

# *Algebra & Number Theory*

Volume 11  
2017  
No. 5



# Algebra & Number Theory

msp.org/ant

## EDITORS

### MANAGING EDITOR

Bjorn Poonen  
Massachusetts Institute of Technology  
Cambridge, USA

### EDITORIAL BOARD CHAIR

David Eisenbud  
University of California  
Berkeley, USA

## BOARD OF EDITORS

Richard E. Borcherds	University of California, Berkeley, USA	Martin Olsson	University of California, Berkeley, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Raman Parimala	Emory University, USA
Brian D. Conrad	Stanford University, USA	Jonathan Pila	University of Oxford, UK
Samit Dasgupta	University of California, Santa Cruz, USA	Anand Pillay	University of Notre Dame, USA
Hélène Esnault	Freie Universität Berlin, Germany	Michael Rapoport	Universität Bonn, Germany
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Victor Reiner	University of Minnesota, USA
Hubert Flenner	Ruhr-Universität, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Christopher Skinner	Princeton University, USA
Joseph Gubeladze	San Francisco State University, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Roger Heath-Brown	Oxford University, UK	J. Toby Stafford	University of Michigan, USA
Craig Huneke	University of Virginia, USA	Pham Huu Tiep	University of Arizona, USA
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Ravi Vakil	Stanford University, USA
János Kollár	Princeton University, USA	Michel van den Bergh	Hasselt University, Belgium
Yuri Manin	Northwestern University, USA	Marie-France Vignéras	Université Paris VII, France
Philippe Michel	École Polytechnique Fédérale de Lausanne	Kei-Ichi Watanabe	Nihon University, Japan
Susan Montgomery	University of Southern California, USA	Shou-Wu Zhang	Princeton University, USA
Shigefumi Mori	RIMS, Kyoto University, Japan		

## PRODUCTION

production@msp.org  
Silvio Levy, Scientific Editor

---

See inside back cover or [msp.org/ant](http://msp.org/ant) for submission instructions.

---

The subscription price for 2017 is US \$325/year for the electronic version, and \$520/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.


---

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

---

ANT peer review and production are managed by EditFLOW<sup>®</sup> from MSP.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2017 Mathematical Sciences Publishers

# Hybrid sup-norm bounds for Maass newforms of powerful level

Abhishek Saha

Let  $f$  be an  $L^2$ -normalized Hecke–Maass cuspidal newform of level  $N$ , character  $\chi$  and Laplace eigenvalue  $\lambda$ . Let  $N_1$  denote the smallest integer such that  $N|N_1^2$  and  $N_0$  denote the largest integer such that  $N_0^2|N$ . Let  $M$  denote the conductor of  $\chi$  and define  $M_1 = M/\gcd(M, N_1)$ . We prove the bound  $\|f\|_\infty \ll_\varepsilon N_0^{1/6+\varepsilon} N_1^{1/3+\varepsilon} M_1^{1/2} \lambda^{5/24+\varepsilon}$ , which generalizes and strengthens previously known upper bounds for  $\|f\|_\infty$ .

This is the first time a hybrid bound (i.e., involving both  $N$  and  $\lambda$ ) has been established for  $\|f\|_\infty$  in the case of nonsquarefree  $N$ . The only previously known bound in the nonsquarefree case was in the  $N$ -aspect; it had been shown by the author that  $\|f\|_\infty \ll_{\lambda, \varepsilon} N^{5/12+\varepsilon}$  provided  $M = 1$ . The present result significantly improves the exponent of  $N$  in the above case. If  $N$  is a squarefree integer, our bound reduces to  $\|f\|_\infty \ll_\varepsilon N^{1/3+\varepsilon} \lambda^{5/24+\varepsilon}$ , which was previously proved by Templier.

The key new feature of the present work is a systematic use of  $p$ -adic representation theoretic techniques and in particular a detailed study of Whittaker newforms and matrix coefficients for  $\mathrm{GL}_2(F)$  where  $F$  is a local field.

## 1. Introduction

**1A. The main result.** Let  $f$  be a Hecke–Maass cuspidal newform on the upper half plane of weight 0, level  $N$ , character  $\chi$ , and Laplace eigenvalue  $\lambda$ . We normalize the volume of  $Y_0(N)$  to be equal to 1 and assume that  $\langle f, f \rangle := \int_{Y_0(N)} |f(z)|^2 dz = 1$ . The problem of bounding the sup-norm  $\|f\|_\infty := \sup_{z \in Y_0(N)} |f(z)|$  in terms of the parameters  $N$  and  $\lambda$  is interesting from several points of view (quantum chaos, spectral geometry, subconvexity of  $L$ -functions, diophantine analysis) and has been much studied recently. For *squarefree* levels  $N$ , there were several results, culminating in the best currently known bound due to Templier [2015], which states that

$$\|f\|_\infty \ll_\varepsilon \lambda^{5/24+\varepsilon} N^{1/3+\varepsilon}.$$

---

The author is supported by EPSRC grant EP/L025515/1.

*MSC2010:* primary 11F03; secondary 11F41, 11F60, 11F72, 11F85, 35P20.

*Keywords:* Maass form, sup-norm, automorphic form, newform, amplification.

The exponent  $\frac{5}{24}$  above for  $\lambda$  has stayed stable since the pioneering work of Iwaniec and Sarnak [1995] (who proved  $\|f\|_\infty \ll_\varepsilon \lambda^{5/24+\varepsilon}$  in the case  $N = 1$ ), and it will likely require some key new idea to improve it. The exponent  $\frac{1}{3}$  for  $N$  in the above bound also appears difficult to improve, at least for squarefree levels, as it seems that the method used so far, primarily due to Harcos and Templier [2012; 2013] and Templier [2010; 2015] has been pushed to its limit. The purpose of the present paper is to show that the situation is very different for *powerful* (nonsquarefree) levels.

To state our result, we introduce a bit of notation. Let  $N_1$  denote the smallest integer such that  $N \mid N_1^2$ . Let  $N_0$  be the largest integer such that  $N_0^2 \mid N$ . Thus  $N_0$  divides  $N_1$  and  $N = N_0 N_1$ .<sup>1</sup> Note that if  $N$  is squarefree, then  $N_1 = N$  and  $N_0 = 1$ . On the other hand, if  $N$  is a perfect square or if  $N$  is highly powerful (a product of high powers of primes) then  $N_1 \asymp N_0 \asymp \sqrt{N}$ . Also, let  $M$  be the conductor of  $\chi$  (so  $M$  divides  $N$ ) and put  $M_1 = M / \gcd(M, N_1)$ . Note that  $M_1$  divides  $N_0$ , and in fact  $M_1$  equals 1 if and only if  $M$  divides  $N_1$ . We will refer to the complementary situation of  $M_1 > 1$  (i.e.,  $M \nmid N_1$ ) as the case when the character  $\chi$  is *highly ramified*.

We prove the following result, which generalizes and strengthens previously known upper bounds for  $\|f\|_\infty$ .

**Theorem** (see Theorem 3.2). *We have*

$$\|f\|_\infty \ll_\varepsilon N_0^{1/6+\varepsilon} N_1^{1/3+\varepsilon} M_1^{1/2} \lambda^{5/24+\varepsilon}.$$

Thus in the squarefree case, our result reduces to that of Templier. However when  $N_1 \asymp N_0 \asymp \sqrt{N}$ , and  $M \mid N_1$  (i.e.,  $\chi$  is not highly ramified), our result gives

$$\|f\|_\infty \ll_\varepsilon N^{1/4+\varepsilon} \lambda^{5/24+\varepsilon}.$$

The exponent of  $\frac{1}{4}$  we obtain in this case is better than the exponent of  $\frac{1}{3}$  in the squarefree case.

We note that the only upper bound known before this for general (i.e., possibly nonsquarefree)  $N$  is due to the present author, and was proved only very recently [Saha 2014]. It was shown that

$$\|f\|_\infty \ll_{\lambda, \varepsilon} N^{5/12+\varepsilon}$$

when  $\chi$  is trivial (no dependence on  $\lambda$  was proved). The results of this paper not only substantially improve those of [Saha 2014] but also use quite different methods. We believe that the approach we take in this paper, characterized by a systematic use of adelic language and local representation-theoretic techniques that separate the difficulties place by place, is the right one to take for powerful levels.

<sup>1</sup>If  $N$  has the prime factorization  $N = \prod_p p^{n_p}$ , then  $N_0$  and  $N_1$  have prime factorizations  $N_0 = \prod_p p^{\lfloor n_p/2 \rfloor}$  and  $N_1 = \prod_p p^{\lceil n_p/2 \rceil}$ .

As for the optimum upper bound for  $\|f\|_\infty$ , it is reasonable to conjecture that

$$\|f\|_\infty \ll_\varepsilon N^\varepsilon \lambda^{1/12+\varepsilon}, \tag{1}$$

if  $M_1 = 1$  (i.e., provided  $\chi$  is *not* highly ramified). If true, (1) is optimal as one can prove *lower bounds* of a similar strength. (But see page 1044.) If  $\chi$  is highly ramified, we cannot expect (1) to hold, for reasons explained in [Saha 2016]. Roughly speaking, in the highly ramified case, the corresponding *local Whittaker newforms* can have large peaks due to a conspiracy of additive and multiplicative characters. This leads to a lower bound for  $\|f\|_\infty$  that is larger than  $N^\varepsilon$  in the  $N$ -aspect. This phenomenon was first observed in Templier [2014] in the case when  $\chi$  is maximally ramified ( $M_1 = N_0$ ) and extended in [Saha 2016] to cover a much bigger range of  $M_1$ . That the factor  $M_1^{1/2}$  is present in our main theorem above (giving worse upper bounds in the highly ramified case) fits nicely with this theme.

In the table below we compare the upper bound provided by this paper with the lower bound provided in [Saha 2016]. We consider newforms of level  $N = p^n$ , for  $1 \leq n \leq 5$ . The second column gives the possible values of  $M$  in each case, and the next three give the corresponding values of  $N_0$ ,  $N_1$  and  $M_1$ . The penultimate column gives the upper bound provided by the theorem on the previous page and should

$N$	$M$	$N_0$	$N_1$	$M_1$	factor $N_0^{1/6} N_1^{1/3} M_1^{1/2}$ in this work's upper bound	factor in lower bound from [Saha 2016]
$p$	1 or $p$	1	$p$	1	$N^{1/3}$	1
$p^2$	1 or $p$	$p$	$p$	1	$N^{1/4}$	1
	$p^2$	$p$	$p$	$p$	$N^{1/2}$	$N^{1/4}$
$p^3$	1, $p$ or $p^2$	$p$	$p^2$	1	$N^{5/18}$	1
	$p^3$	$p$	$p^2$	$p$	$N^{4/9}$	$N^{1/6}$
$p^4$	1, $p$ or $p^2$	$p^2$	$p^2$	1	$N^{1/4}$	1
	$p^3$	$p^2$	$p^2$	$p$	$N^{3/8}$	1
	$p^4$	$p^2$	$p^2$	$p^2$	$N^{1/2}$	$N^{1/4}$
$p^5$	1, $p$ , $p^2$ or $p^3$	$p^2$	$p^3$	1	$N^{4/15}$	1
	$p^4$	$p^2$	$p^3$	$p$	$N^{11/30}$	$N^{1/10}$
	$p^5$	$p^2$	$p^3$	$p^2$	$N^{7/15}$	$N^{1/5}$

**Table 1.** A comparison of upper and lower bounds for  $\|f\|_\infty$ . The penultimate column gives the factor that replaces  $\dots$  in the bound  $\|f\|_\infty \ll_\varepsilon N^\varepsilon \lambda^{5/24+\varepsilon} \times \dots$  given by our main theorem on the previous page. The last column gives the corresponding factor in the previously known lower bound  $\|f\|_\infty \gg_\varepsilon N^{-\varepsilon} \lambda^{1/12-\varepsilon} \times \dots$ .

serve as a nice numerical illustration of our result in the *depth aspect* ( $N = p^n$ ,  $n \rightarrow \infty$ ). The final column gives the corresponding lower bound proved in Theorem 3.3 of [Saha 2016]. The difference between these last two columns reflects the gap in the state of our current knowledge. As the table makes clear, the larger upper bounds for highly ramified  $\chi$  are often matched by larger lower bounds.

Finally, we have colored blue all the quantities on the last column that we (optimistically) conjecture to be in fact the *true size* of  $\|f\|_\infty$  (up to a factor of  $(N\lambda)^\varepsilon$ ) in those cases.

**1B. Organization of this paper.** The remainder of Section 1 is an extended introduction that explains some of the main features of our work. In Section 2, which is the technical heart of this paper, we undertake a detailed analytic study of  $p$ -adic Whittaker newforms and matrix coefficients for representations of  $\mathrm{GL}_2(F)$  where  $F$  is a nonarchimedean local field of characteristic 0. The two main results we prove are related to a) the support and average size of  $p$ -adic Whittaker newforms, b) the size of eigenvalues of certain matrix coefficients. These might be of independent interest. In Section 3, we prove the main result, Theorem 3.2. Perhaps surprisingly, and in contrast to our previous work [Saha 2014], no counting arguments are needed in this paper beyond those supplied by Templier for the squarefree case. Also, in contrast to [Saha 2014], we do not need any powerful version of the “gap principle”. Instead, we rely almost entirely on the  $p$ -adic results of Section 2.

**1C. Squarefree versus powerful levels.** The first bound for  $\|f\|_\infty$  in the  $N$ -aspect was  $\|f\|_\infty \ll_{\lambda, \varepsilon} N^{216/457+\varepsilon}$ , proved by Blomer and Holowinsky [2010]. They also proved the hybrid bound  $\|f\|_\infty \ll (\lambda^{1/2} N)^{1/2-1/2300}$ . These results were only valid under the assumption that  $N$  is squarefree. After that, there was fairly rapid progress (again only assuming  $N$  squarefree) by Harcos and Templier [Harcos and Templier 2012; 2013; Templier 2010; 2015], culminating in the hybrid bound due to Templier described earlier. Note that the  $N$ -exponent in Templier’s case is  $\frac{1}{3}$ , which may be viewed as the “Weyl exponent”, as it is a third of the way from the trivial bound of  $N^{1/2+\varepsilon}$  towards the expected optimum bound<sup>2</sup> of  $N^\varepsilon$ .

For a long time, there was no result at all when  $N$  is not squarefree. Indeed, all the papers of Harcos and Templier rely crucially on using *Atkin–Lehner operators* to move any point of  $\mathbb{H}$  to a point of imaginary part  $\geq \frac{1}{N}$  (which is essentially equivalent to using a suitable Atkin–Lehner operator to move any cusp to infinity). This only works if  $N$  is squarefree. In [Saha 2014], the first (and only previous) result for Maass forms of nonsquarefree level was proved; assuming that  $M = 1$  we showed that  $\|f\|_\infty \ll_{\lambda, \varepsilon} N^{5/12+\varepsilon}$ . A key new idea in [Saha 2014] was to look at the behavior of  $f$  around *cusps of width 1* and to formulate all the geometric and

<sup>2</sup>As mentioned earlier, this optimum bound is only expected to hold when  $\chi$  is not highly ramified.

diophantine results around such a cusp. Apart from this, the overall strategy was not that different from the works of Harcos and Templier and the exponent of  $\frac{5}{12}$  obtained was weaker than the exponent  $\frac{1}{3}$  for the squarefree case.

An initial indication that the exponent  $\frac{1}{3}$  in the  $N$ -aspect might be beaten for powerful levels was given by Marshall [2016], who showed recently that for a newform  $g$  of level  $N$  and trivial character on a *compact arithmetic surface* (i.e., coming from a quaternion division algebra) the bound

$$\|g\|_\infty \ll_\varepsilon \lambda^{1/4+\varepsilon} N_1^{1/2+\varepsilon}$$

holds true. In particular, when  $N$  is sufficiently powerful, this gives a “sub-Weyl” exponent of  $\frac{1}{4}$  in the  $N$ -aspect. Marshall’s proof does not work for the usual Hecke–Maass newforms  $f$  on the upper-half plane of level  $N$  that we consider in this paper (though it does work for certain shifts of these  $f$  when restricted to a *fixed compact set*). Finally, our main result, Theorem 3.2, gives (when  $\chi$  is not highly ramified) the bound  $\|f\|_\infty \ll_\varepsilon N_0^{1/6+\varepsilon} N_1^{1/3+\varepsilon} \lambda^{5/24+\varepsilon}$  which may be viewed as a strengthened analogue of Marshall’s result for cusp forms on the upper-half plane.

As indicated already, the powerful level case has been historically more difficult than the squarefree case. It may thus seem surprising that in the powerful case, we succeed in obtaining better exponents than in the squarefree case. However this seems to be a relatively common phenomenon. For example, for the related problem of quantum unique ergodicity in the level aspect, the known results in the squarefree case [Nelson 2011] give mass equidistribution with no power-savings but for powerful levels one obtains mass equidistribution with power savings [Nelson et al. 2014]. Again, for the problem of proving strong subconvexity bounds in the conductor aspect for Dirichlet  $L$ -functions, one only has a Weyl exponent  $\frac{1}{6}$  when the conductor is squarefree, but Milićević [2016] has shown an improved exponent of  $.1645\dots < \frac{1}{6}$  for high prime powers. The results of this paper continue this surprising pattern (for which we do not attempt to give a general conceptual explanation).

**1D. Fourier expansions and efficient generating domains.** It seems worth noting explicitly the following interesting technical aspect of our work: the method of Fourier (Whittaker) expansion, once one chooses a good (adelic) *generating domain*, leads to the rather strong bound  $\|f\|_\infty \ll_\varepsilon M_1^{1/2} N_1^{1/2+\varepsilon} \lambda^{1/4+\varepsilon}$ . Note that this bound reduces to the “trivial bound” when  $N$  is squarefree, but is almost of the same strength (in the  $N$ -aspect) as our main theorem when  $N$  is sufficiently powerful. In this subsection, we briefly explain the ideas behind this.

It is best to work adelicly here. Let  $\phi$  be the automorphic form associated to  $f$ , and let  $g = g_f g_\infty \in G(\mathbb{A})$ , where  $g_f$  denotes the finite part of  $g$  and  $g_\infty$  denotes the infinite component. Then  $\|f\|_\infty = \sup_{g \in G(\mathbb{A})} |\phi(g)|$ . Because of the invariance properties for  $\phi$ , it suffices to restrict  $g$  to a suitable generating domain  $D \subset G(\mathbb{A})$ .

Roughly speaking,  $D$  can be any subset of  $G(\mathbb{A})$  such that the natural map from  $D$  to  $Z(\mathbb{A})G(\mathbb{Q})\backslash G(\mathbb{A})/\bar{K}$  is a surjection where  $\bar{K}$  is a subgroup of  $G(\mathbb{A})$  generated by a set of elements under which  $|\phi|$  is right-invariant.

The Whittaker expansion for  $\phi$ , which we want to exploit to bound  $|\phi(g)|$ , looks as follows:

$$\phi(g) = \sum_{q \in \mathbb{Q} \neq 0} W_\phi\left(\begin{bmatrix} q & \\ & 1 \end{bmatrix}g\right).$$

The above is an infinite sum, but two things make it tractable. First of all there is an integer  $Q(g_f)$ , depending on  $g_f$ , such that the sum is supported only on those  $q$  whose denominator divides  $Q(g_f)$ . Secondly, the sum decays very quickly after a certain point  $|q| > T(g_\infty)$  due to the exponential decay of the Bessel function. The upshot is that

$$|\phi(g)| \ll \sum_{\substack{n \in \mathbb{Z} \neq 0 \\ |n| < Q(g_f)T(g_\infty)}} W_\phi\left(\begin{bmatrix} n/Q(g_f) & \\ & 1 \end{bmatrix}g\right). \tag{2}$$

The key quantity is the *length*  $Q(g_f)T(g_\infty)$  of the sum above. Indeed, assuming Ramanujan type bounds on average for the local Whittaker newforms and using Cauchy–Schwartz, the expression (2) leads to the inequality<sup>3</sup>  $|\phi(g)| \ll_\varepsilon (Q(g_f)T(g_\infty))^{1/2+\varepsilon}$ . The key point therefore, is to choose an efficient generating domain  $D$  inside  $G(\mathbb{A})$ , such that  $\sup_{g \in D} Q(g_f)T(g_\infty)$  is as small as possible.

Let us look at some examples. Suppose  $\phi$  corresponds to a Hecke–Maass cusp form for  $SL_2(\mathbb{Z})$ . Then it is natural to take  $D$  to be the subset of  $G(\mathbb{A})$  consisting of the elements  $g$  with  $g_f = 1$  and  $g_\infty = \begin{bmatrix} y & x \\ & 1 \end{bmatrix}$  such that  $-\frac{1}{2} \leq x \leq \frac{1}{2}$  and  $y \geq \frac{\sqrt{3}}{2}$ . In this case  $Q(g_f) = 1$  and  $T(g_\infty) = \lambda^{1/2}/y$ , leading to the bound  $|\phi(g)| \ll_\varepsilon \lambda^{1/4+\varepsilon}$  as expected. Next, suppose  $\phi$  corresponds to a newform of level  $N$  where  $N$  is squarefree. In this case one can include the Atkin–Lehner operators inside the symmetry group  $\bar{K}$  above. Harcos and Templier showed that one can take  $D$  to be the subset of  $G(\mathbb{A})$  consisting of the elements with  $g_f = 1$  and for which  $g_\infty = \begin{bmatrix} y & x \\ & 1 \end{bmatrix}$  such that  $y \geq \sqrt{3}/(2N)$  (and some additional properties). For such an element, one again has  $Q(g_f) = 1$  and  $T(g_\infty) = \lambda^{1/2}/y$  leading to the bound  $|\phi(g)| \ll_\varepsilon (\lambda^{1/2}/y)^{1/2+\varepsilon} \ll N^{1/2+\varepsilon} \lambda^{1/4+\varepsilon}$ .

When  $N$  is nonsquarefree, it is not possible to construct a generating domain  $D$  with a finite value of  $\sup_{g \in D} T(g_\infty)$  for which all points have  $g_f = 1$ . Classically, this means that any fundamental domain (for the full symmetry group generated by  $\Gamma_0(N)$  and the Atkin–Lehner operators) must touch the real line. The idea used in [Saha 2014] was to take the infinite part of  $D$  essentially the same as in the squarefree case and take the finite part to be a certain nice subset of  $\prod_{p|N} GL_2(\mathbb{Z}_p)$ .

---

<sup>3</sup>Strictly speaking, this inequality is not completely accurate as one has to add an (usually smaller) error term coming from peaks of the local Whittaker and  $K$ -Bessel functions.



Classically, our choice of generating domain in [Saha 2014] corresponded to taking discs around cusps of width 1. Assuming  $\chi = 1$ , this choice again gave  $Q(g_f) = 1$  and  $T(g_\infty) = \lambda^{1/2}/y$  leading to the same bound  $|\phi(g)| \ll_\varepsilon N^{1/2+\varepsilon} \lambda^{1/4+\varepsilon}$  as earlier. Thus, in all the above papers, the worst case bound obtained by the Whittaker expansion (i.e., for smallest  $y$ ) was just the *trivial bound*  $N^{1/2+\varepsilon} \lambda^{1/4+\varepsilon}$  (also, all these papers restricted to  $\chi = 1$ ).

In this paper we choose a somewhat different generating domain from that of [Saha 2014]. For simplicity, we describe this domain here in the special case when  $N = p^{2n_0}$  and  $M = p^m$ , for some prime  $p$  and some nonnegative integers  $n_0$  and  $m$ . Take  $D$  to consist of the elements  $g_p g_\infty$ , where  $g_\infty = \begin{bmatrix} y & x \\ & 1 \end{bmatrix}$  with  $y \geq \sqrt{3}/2$  and  $g_p \in \text{GL}_2(\mathbb{Z}_p) \begin{bmatrix} p^{n_0} & \\ & 1 \end{bmatrix}$ . It is easy to prove this is a generating domain. The difficulties lie in computing  $Q(g_f)$  and in proving that the required Ramanujan type bounds on average hold. These key technical local results involve intricate calculations that take up a good part of Section 2. We are able to prove that  $\sup_{g \in D} Q(g_f) = p^{\max(m, n_0)} = M_1 \sqrt{N}$ . Also,  $T(g_\infty) = \lambda^{1/2}/y$  as usual. This leads to the surprisingly strong Whittaker expansion bound of

$$|\phi(g)| \ll_\varepsilon M_1^{1/2} N^{1/4+\varepsilon} \lambda^{1/4+\varepsilon}$$

in this case. Classically, the generating domain described above corresponds to taking discs around the cusps of the group

$$\Gamma_0(p^{n_0}, p^{n_0}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}) : p^{n_0} \mid b, p^{n_0} \mid c \right\}.$$

We remark here that the function  $f'(z) := f(z/p^{n_0})$  is a Maass form for  $\Gamma_0(p^{n_0}, p^{n_0})$ .

When  $N$  is not a perfect square, the generating domain we actually use is slightly different than described above. Roughly speaking, we exploit the existence of Atkin–Lehner operators at primes that divide  $N$  to an odd power. This does not change the value of  $\sup_{g \in D} Q(g_f) T(g_\infty)$  and so does not really affect the Whittaker expansion analysis; however it makes it easier to count lattice points for amplification (described in the next subsection). In any case, the Whittaker expansion bound we prove ultimately (see Section 3D) is  $|\phi(g)| \ll_\varepsilon (N_0 M_1 \lambda^{1/2}/y)^{1/2+\varepsilon}$  where  $y \geq N_0/N_1$ , leading to the worst case bound of  $|\phi(g)| \ll_\varepsilon M_1^{1/2} N_1^{1/2+\varepsilon} \lambda^{1/4+\varepsilon}$ . This, as mentioned earlier, is essentially of the same strength (in the  $N$ -aspect) as our main theorem when  $N$  is sufficiently powerful.

It bears repeating that the main tools used for the above bound are local, relating to the representation theory of  $p$ -adic Whittaker functions. This supports the assertion of Marshall [2016] that  $N_1^{1/2+\varepsilon}$  should be viewed as the correct *local bound* in the level aspect (when  $\chi$  is not highly ramified). Our analysis of these  $p$ -adic Whittaker functions also lead to other interesting questions. For example, one can ask for a sup-norm bound for these local Whittaker newforms, and in (1), we predict a Lindelöf type bound when  $\chi$  is not highly ramified (this conjecture was originally

made in [Saha 2016]). One of the key technical results in Section 2 essentially proves an *averaged* version of this conjecture (this is the Ramanujan type bound on average alluded to earlier).

**1E. The pretrace formula and amplification.** Recall our main theorem:

$$\|f\|_\infty \ll_\varepsilon N_0^{1/6+\varepsilon} N_1^{1/3+\varepsilon} M_1^{1/2} \lambda^{5/24+\varepsilon}.$$

As we have seen above, the method of Fourier (Whittaker) expansion gives us the bound  $\|f\|_\infty \ll_\varepsilon N_1^{1/2+\varepsilon} M_1^{1/2} \lambda^{1/4+\varepsilon}$  (with even better bounds when the relevant point on our generating domain has a large value for  $y$ ) so we need to save a further factor of  $(N_1/N_0)^{1/6} \lambda^{1/24}$ . This is done by *amplification*, whereby we choose suitable test functions at each prime to obtain a *pretrace formula* and then estimate its geometric side via some point counting results from [Harcos and Templier 2013; Templier 2015]. The basic idea is that by choosing these local test functions carefully (constructing an amplifier) one should be able to boost the contribution of the newform  $f$  to the resulting pretrace formula. The details for this are given (in a fairly flexible adelic framework) in Sections 3E–3G.

The unramified local test functions that we use in this paper are standard and essentially go back to Iwaniec–Sarnak (the key point is to exploit a simple identity relating the eigenvalues for the Hecke operators  $T(\ell)$  and  $T(\ell^2)$ ). However, our ramified local test functions are very different from the papers of Harcos and Templier or our previous paper [Saha 2014]. In all those past papers, the ramified test functions had been simply chosen to be the characteristic functions of the relevant congruence subgroups. In contrast, we use a variant of the local test function used by Marshall [2016]. The main results about this test function are proved in Sections 2F–2H. Roughly speaking, it is (the restriction to a large compact subgroup of) the *matrix coefficient* for a local vector  $v'$  obtained by translating the local newform. The key property of this test function is that its unique nonzero eigenvalue is fairly large (and  $v'$  is an eigenvector with this eigenvalue).

Our choice of test functions at ramified primes ensures that any pretrace formula involving them averages over relatively few representations of level  $N$ . It may be useful to view this as a ramified analogue of the classical (unramified) amplifier. Indeed, the resulting “trivial bound” obtained via the pretrace formula (by choosing the unramified test functions trivially) matches exactly (on compact subsets) with the strong local bounds obtained via Whittaker expansion. This is an important point because it means that we only need to save a further factor of  $(N_1/N_0)^{1/6} \lambda^{1/24}$  by putting in the unramified amplifier and counting lattice points. This is carried out in Section 3G.

It is worth noting that we do not need any new counting results in this paper beyond those proved by Harcos and Templier. This is because the counting part of

our paper is only concerned with the squarefree integer  $N_1/N_0$ . In particular, the role of amplification in this paper to improve the  $N$  exponent is relatively minor when  $N$  is highly powerful (note that  $N_1/N_0$  approaches a negligible power of  $N$  as  $N$  gets more powerful). Indeed, when  $N$  is a perfect square ( $N_1 = N_0$ ), all our savings in the  $N$ -aspect come from Whittaker expansion and we do not gain anything further by amplification.<sup>4</sup> In contrast, in [Saha 2014] we had a relatively poor bound coming from Whittaker expansion but we then saved a nontrivial power of  $N$  via amplification.

The technical reason why the method of amplification does not improve the  $N$ -aspect too much beyond our strong local bounds is that our ramified test functions have relatively large support. Consequently, we do not have many global congruences related to  $N$ , and congruences are essential for savings via counting. More precisely, our ramified test functions are supported on the maximal compact subgroup at primes that divide  $N$  to an even power, and supported on a (slightly) smaller subgroup at primes that divide  $N$  to an odd power (it is the latter case that leads to the savings of  $(N_1/N_0)^{1/6}$ ). If we were to reduce the support of our test functions further and thus force new congruences, the resulting savings via counting would be eclipsed by the resulting loss due to the fact that our pretrace formula would now be averaging over more representations of level  $N$ . Somehow the ramified and unramified parts of the amplifier seem to work against each other and the key point is to strike the right balance.

It would be an interesting and challenging problem to detect any additional cancellation on the geometric side of our pretrace formula by going beyond counting lattice points and perhaps taking into account the *phases* of the matrix coefficient used to construct the ramified test function. Such a result could potentially push the upper-bound for  $\|f\|_\infty$  below  $N^{1/4}$ .

**1F. Notations.** We collect here some general notations that will be used throughout this paper. Additional notations will be defined where they first appear in the paper.

Given two integers  $a$  and  $b$ , we use  $a \mid b$  to denote that  $a$  divides  $b$ , and we use  $a \mid b^\infty$  to denote that  $a \mid b^n$  for some positive integer  $n$ . For any real number  $\alpha$ , we let  $\lfloor \alpha \rfloor$  denote the greatest integer less than or equal to  $\alpha$  and we let  $\lceil \alpha \rceil$  denote the smallest integer greater than or equal to  $\alpha$ . The symbol  $\mathbb{A}$  denotes the ring of adèles of  $\mathbb{Q}$  and  $\mathbb{A}_f$  denotes the subset of finite adèles. For any two complex numbers  $\alpha$  and  $z$  we let  $K_\alpha(z)$  denote the modified Bessel function of the second kind.

The groups  $GL_2$ ,  $SL_2$ ,  $PSL_2$ ,  $\Gamma_0(N)$  and  $\Gamma_1(N)$  have their usual meanings. The letter  $G$  always stands for the group  $GL_2$ . If  $H$  is any subgroup of  $G$ , and  $R$  is any subring of  $\mathbb{R}$ , then  $H(R)^+$  denotes the subgroup of  $H(R)$  consisting of matrices with positive determinant.

---

<sup>4</sup>However, we always gain a nontrivial savings in the  $\lambda$  aspect via amplification.

We let  $\mathbb{H} = \{x + iy : x \in \mathbb{R}, y \in \mathbb{R}, y > 0\}$  denote the upper half plane. For any  $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  in  $\mathrm{GL}_2(\mathbb{R})^+$ , and any  $z \in \mathbb{H}$ , we define  $\gamma(z)$  or  $\gamma z$  to equal  $(az+b)/(cz+d)$ . This action of  $\mathrm{GL}_2(\mathbb{R})^+$  on  $\mathbb{H}$  extends naturally to the boundary of  $\mathbb{H}$ .

We say that a function  $f$  on  $\mathbb{H}$  is a Hecke–Maass cuspidal newform of weight 0, level  $N$ , character  $\chi$  and Laplace eigenvalue  $\lambda$  if it has the following properties:

- $f$  is a smooth real analytic function on  $\mathbb{H}$ .
- $f$  satisfies  $(\Delta + \lambda)f = 0$  where  $\Delta := y^{-2}(\partial_x^2 + \partial_y^2)$ .
- For all  $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$ ,  $f(\gamma z) = \chi(d)f(z)$ .
- $f$  decays rapidly at the cusps of  $\Gamma_1(N)$ .
- $f$  is orthogonal to all oldforms.
- $f$  is an eigenfunction of all the Hecke and Atkin–Lehner operators.<sup>5</sup>

The study of newforms  $f$  as above is equivalent to the study of corresponding adelic newforms  $\phi$  which are certain functions on  $G(\mathbb{A})$ . For the details of this correspondence, see Remark 3.1.

We use the notation  $A \ll_{x,y,z} B$  to signify that there exists a positive constant  $C$ , depending at most upon  $x, y, z$ , so that  $|A| \leq C|B|$ . The symbol  $\epsilon$  will denote a small positive quantity. The values of  $\epsilon$  and that of the constant implicit in  $\ll_{\epsilon, \dots}$  may change from line to line.

## 2. Local calculations

**2A. Preliminaries.** We begin with fixing some notations that will be used throughout this section. Let  $F$  be a nonarchimedean local field of characteristic zero whose residue field has cardinality  $q$ . Let  $\mathfrak{o}$  be its ring of integers, and  $\mathfrak{p}$  its maximal ideal. Fix a generator  $\varpi$  of  $\mathfrak{p}$ . Let  $|\cdot|$  denote the absolute value on  $F$  normalized so that  $|\varpi| = q^{-1}$ . For each  $x \in F^\times$ , let  $v(x)$  denote the integer such that  $|x| = q^{-v(x)}$ . For a nonnegative integer  $m$ , we define the subgroup  $U_m$  of  $\mathfrak{o}^\times$  to be the set of elements  $x \in \mathfrak{o}^\times$  such that  $v(x - 1) \geq m$ .

Let  $G = \mathrm{GL}_2(F)$  and  $K = \mathrm{GL}_2(\mathfrak{o})$ . For each integral ideal  $\mathfrak{a}$  of  $\mathfrak{o}$ , let

$$K_0(\mathfrak{a}) = K \cap \begin{bmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{a} & \mathfrak{o} \end{bmatrix}, \quad K_1(\mathfrak{a}) = K \cap \begin{bmatrix} 1 + \mathfrak{a} & \mathfrak{o} \\ \mathfrak{a} & \mathfrak{o} \end{bmatrix}, \quad K^0(\mathfrak{a}) = K \cap \begin{bmatrix} \mathfrak{o} & \mathfrak{a} \\ \mathfrak{o} & \mathfrak{o} \end{bmatrix}.$$

For  $x \in F, y \in F^\times$  and  $t \in F^\times$ , write

$$w = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad a(y) = \begin{bmatrix} y & \\ & 1 \end{bmatrix}, \quad n(x) = \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}, \quad z(t) = \begin{bmatrix} t & \\ & t \end{bmatrix},$$

---

<sup>5</sup>Assuming the previous properties, this last property is equivalent to the weaker condition that  $f$  is an eigenfunction of almost all Hecke operators.

Define subgroups  $N = \{n(x) : x \in F\}$ ,  $A = \{a(y) : y \in F^\times\}$ ,  $Z = \{z(t) : t \in F^\times\}$ ,  $B_1 = NA$  and  $B = ZNA = G \cap \begin{bmatrix} * & * \\ * & * \end{bmatrix}$  of  $G$ .

We normalize Haar measures as follows. The measure  $dx$  on the additive group  $F$  assigns volume 1 to  $\mathfrak{o}$ , and transports to a measure on  $N$ . The measure  $d^\times y$  on the multiplicative group  $F^\times$  assigns volume 1 to  $\mathfrak{o}^\times$ , and transports to measures on  $A$  and  $Z$ . We obtain a left Haar measure  $d_L b$  on  $B$  via  $d_L(z(u)n(x)a(y)) = |y|^{-1} d^\times u dx d^\times y$ . Let  $dk$  be the probability Haar measure on  $K$ . The Iwasawa decomposition  $G = BK$  gives a left Haar measure  $dg = d_L b dk$  on  $G$ .

For each irreducible admissible representation  $\sigma$  of  $G$  (resp.  $F^\times$ ) we define  $a(\sigma)$  to be the smallest nonnegative integer such that  $\sigma$  has a  $K_1(\mathfrak{p}^{a(\sigma)})$ -fixed (resp.  $U_{a(\sigma)}$ -fixed) vector.

**2B. Some matrix invariants.** From now on, fix  $\pi$  to be a generic irreducible admissible unitary representation of  $G$ . Let  $n = a(\pi)$ , and let  $\omega_\pi$  denote the central character of  $\pi$ .

It is convenient now to introduce some notation. Define

- $n_1 := \lceil \frac{n}{2} \rceil$ ,
- $n_0 := n - n_1 = \lfloor \frac{n}{2} \rfloor$ ,
- $m = a(\omega_\pi)$ ,
- $m_1 = \max(0, m - n_1)$ .

Note that  $m_1 = 0$  if and only if  $m \leq n_1$ ; this can be viewed as the case when  $\omega_\pi$  is not highly ramified.

Next, for any  $g \in G$ , we define two integers  $t(g)$  and  $l(g)$  which depend on  $g$  and  $n$ . Recall the disjoint double coset decomposition [Saha 2016, Lemma 2.13]:

$$G = \bigsqcup_{t \in \mathbb{Z}} \bigsqcup_{0 \leq l \leq n} \bigsqcup_{v \in \mathfrak{o}^\times / U_{\min(l, n-l)}} ZNa(\varpi^t)wn(\varpi^{-l}v)K_1(\mathfrak{p}^n). \tag{3}$$

Accordingly, given any matrix  $g \in G$ , we define  $t(g)$  and  $l(g)$  to be the unique integers such that

- $0 \leq l(g) \leq n$ ,
- $g \in ZNa(\varpi^{t(g)})wn(\varpi^{-l(g)}v)K_1(\mathfrak{p}^n)$  for some  $v \in \mathfrak{o}^\times$ .

**Remark 2.1.** It is illuminating to restate these matrix invariants slightly differently. Let  $g$  in  $G$ . The Iwasawa decomposition tells us that  $g \in ZNa(y)k$  where  $k = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in K$ . Then one can check that  $l(g) = \min(v(c), n)$ , and  $t(g) = v(y) - 2l(g)$ .

In the sequel, we will often consider matrices  $g$  lying in the set  $Ka(\varpi^{n_1})$ . The next few lemmas explicate some key properties of this set.

**Lemma 2.2.** *Suppose that  $k \in K$  and  $n$  is odd (so  $n_1 = n_0 + 1$ ). Then:*

- (1)  $l(ka(\varpi^{n_1})) \geq n_1$  if and only if  $k \in N(\mathfrak{o})K^0(\mathfrak{p})$ .
- (2)  $l(ka(\varpi^{n_1})) \leq n_0$  if and only if  $k \in wK^0(\mathfrak{p})$ .

*Proof.* We first assume that  $l(ka(\varpi^{n_1})) \geq n_1$  and prove that  $k \in BK^0(\mathfrak{p})$ . For brevity, put  $l = l(ka(\varpi^{n_1}))$ . So we can write  $ka(\varpi^{n_1}) = bwn(\varpi^{-l}v)k'$ , where  $b \in B$ ,  $k' \in K_1(\mathfrak{p}^n)$  and  $n \geq l \geq n_1$ . Therefore  $k = b'wn(\varpi^{n_1-l}v)k_2$ , where  $k_2 = a(\varpi^{n_1})k'a(\varpi^{-n_1}) \in K^0(\mathfrak{p}^{n_1})$  and  $b' \in B$ . To complete the proof that  $k \in BK^0(\mathfrak{p})$ , it suffices to check that there exists a matrix  $b_2 \in B$  such that  $b_2wn(\varpi^{n_1-l}v) \in K^0(\mathfrak{p})$ . By explicit verification,  $b_2 = \begin{bmatrix} \varpi^{n_1-l}v & \\ & \varpi^{l-n_1}v^{-1} \end{bmatrix}$  works. Once we have  $k \in BK^0(\mathfrak{p})$ , it follows immediately that  $k \in B(\mathfrak{o})K^0(\mathfrak{p}) = N(\mathfrak{o})K^0(\mathfrak{p})$ .

The proof that  $l(ka(\varpi^{n_1})) \leq n_0$  implies  $k \in wK^0(\mathfrak{p})$  is similar. The reverse implications follow using  $N(\mathfrak{o})K^0(\mathfrak{p}) \cap wK^0(\mathfrak{p}) = \emptyset$ . □

**Lemma 2.3.** *Suppose that  $k \in K_0(\mathfrak{p})$ ,  $n$  is odd, and  $g \in \{1, \begin{bmatrix} & 1 \\ \varpi & \end{bmatrix}\}$ . Then*

$$kgwa(\varpi^{n_1}) = k'a(\varpi^{n_1})g'z,$$

where  $k' \in K$ ,  $l(k'a(\varpi^{n_1})) \leq n_0$ ,  $g' \in \{1, \begin{bmatrix} & 1 \\ \varpi & \end{bmatrix}\}$ , and  $z \in Z$ .

*Proof.* If  $g = 1$ , then  $kgwa(\varpi^{n_1}) = w(w^{-1}kw)a(\varpi^{n_1})$ . If  $g = \begin{bmatrix} & 1 \\ \varpi & \end{bmatrix}$ , then  $kgwa(\varpi^{n_1}) = w(w^{-1}kw)a(\varpi^{n_1})\begin{bmatrix} & 1 \\ \varpi & \end{bmatrix}z(-\varpi^{n_1-n})$ . Since  $(w^{-1}kw) \in K^0(\mathfrak{p})$ , the result now follows from Lemma 2.2. □

**Lemma 2.4.** *Suppose that  $g \in Ka(\varpi^{n_1})$ . Then  $t(g) = \min(n_1 - 2l(g), -n_1)$ .*

*Proof.* This follows by an explicit computation similar to the proof of Lemma 2.2. We omit the details. □

**2C. Our goal.** It may be worthwhile to declare at this point the output from the rest of Section 2 that will be needed for our main theorem.

In Sections 2D–2E, we will study the local Whittaker newform  $W_\pi$ , which is a certain function on  $G$ . Given a compact subset  $\mathcal{J}$  of  $G$ , we are interested in the following questions:

- (1) For each  $g \in \mathcal{J}$ , provide a good upper bound for the quantity

$$\sup\{|y| : W_\pi(a(y)g) \neq 0\}.$$
<sup>6</sup>

- (2) Prove an average Ramanujan-type bound for the function  $|W_\pi(a(y)g)|$  whenever  $g \in \mathcal{J}$  and  $W_\pi(a(y)g) \neq 0$ .

For our global applications, it will be useful to have the set  $\mathcal{J}$  to be relatively large (so that we can create a generating domain out of it with a relatively small archimedean component) while also making sure that the supremum of the upper

---

<sup>6</sup>This is essentially the local analogue of the quantity  $Q(g_f)$  described in the introduction.

bound above (as  $g$  varies in  $\mathcal{J}$ ) is fairly small (so as to optimize the Whittaker expansion bound). We will choose  $\mathcal{J}$  to equal the set  $Ka(\varpi^{n/2})$  if  $n$  is even and equal to  $\{g \in Ka(\varpi^{n_1}) : l(g) \leq n_0\}$  if  $n$  is odd. For this set  $\mathcal{J}$  we will answer the two questions above in Proposition 2.11. This proposition will be of key importance for our global Whittaker expansion bound.

Next, in Sections 2F–2H, we will study a certain test function  $\Phi'_\pi$ . This test function, viewed as a convolution operator, is essentially idempotent, and therefore has exactly one nonzero positive eigenvalue. In Proposition 2.13, we determine the size of this nonzero eigenvalue, and we also prove that  $a(\varpi^{n_1}) \cdot W_\pi$  is an eigenvector with this eigenvalue. This proposition will be of key importance for our global bound coming from the amplified trace formula.

In view of the technical material coming up, it is worth emphasizing that Propositions 2.11 and 2.13 are the *only* results from the rest of Section 2 that will be used in Section 3.

**2D. The Whittaker newform.** Fix an additive character  $\psi : F \rightarrow S^1$  with conductor  $\mathfrak{o}$ . Then  $\pi$  can be realized as a unique subrepresentation of the space of functions  $W$  on  $G$  satisfying  $W(n(x)g) = \psi(x)W(g)$ . This is the Whittaker model of  $\pi$  and will be denoted  $\mathcal{W}(\pi, \psi)$ .

**Definition 2.5.** The *normalized Whittaker newform*  $W_\pi$  is the unique function in  $\mathcal{W}(\pi, \psi)$  invariant under  $K_1(\mathfrak{p}^n)$  that satisfies  $W_\pi(1) = 1$ .

The following lemma is well known and so we omit its proof.

**Lemma 2.6.** *Suppose that  $W_\pi(a(y)) \neq 0$ . Then  $|y| \leq 1$ , i.e.,  $y \in \mathfrak{o}$ .*

**Lemma 2.7** [Saha 2016, Proposition 2.28]. *Let  $\tilde{\pi}$  denote the contragredient representation of  $\pi$ . Let  $t \in \mathbb{Z}$ ,  $0 \leq l \leq n$ ,  $v \in \mathfrak{o}^\times$ , and assume<sup>7</sup>  $\omega_\pi(\varpi) = 1$ . We have*

$$\begin{aligned} W_{\tilde{\pi}}(a(\varpi^t)wn(\varpi^{-l}v)) \\ = \varepsilon\left(\frac{1}{2}, \pi\right)\omega_\pi(v)\psi(-\varpi^{t+l}v^{-1})W_\pi(a(\varpi^{t+2l-n})wn(-\varpi^{l-n}v)). \end{aligned}$$

Define  $g_{t,l,v} := a(\varpi^t)wn(\varpi^{-l}v)$ . Let  $\tilde{X}$  denote the group of characters  $\mu$  of  $F^\times$  such that  $\mu(\varpi) = 1$ . For each  $\mu \in \tilde{X}$  and each  $x \in F$ , define the Gauss sum  $G(x, \mu) = \int_{\mathfrak{o}^\times} \psi(xy)\mu(y) d^\times y$ .

We will need two additional results for the results of the next subsection. The first one is a key formula from [Saha 2016].

**Lemma 2.8** [Saha 2016, Proposition 2.23]. *Assume that  $\omega_\pi \in \tilde{X}$ , we have*

$$W_\pi(g_{t,l,v}) = \sum_{\substack{\mu: a(\mu) \leq l, \\ \mu \in \tilde{X}}} c_{t,l}(\mu)\mu(v),$$

---

<sup>7</sup>There is no loss of generality in this assumption as we can always twist  $\pi$  by a character of the form  $|\cdot|^{it}$  to ensure this.

where the coefficients  $c_{t,l}(\mu)$  can be read off from the following identity

$$\begin{aligned} &\varepsilon\left(\frac{1}{2}, \mu\pi\right)\left(\sum_{t=-\infty}^{\infty} q^{(t+a(\mu\pi))(1/2-s)} c_{t,l}(\mu)\right)L(s, \mu\pi)^{-1} \\ &= \omega_{\pi}(-1)\left(\sum_{a=0}^{\infty} W_{\pi}(a(\varpi^a))q^{-a(1/2-s)} G(\varpi^{a-l}, \mu^{-1})\right)L(1-s, \mu^{-1}\omega_{\pi}^{-1}\pi)^{-1} \end{aligned} \quad (4)$$

The next result deals with conductors of character twists. While the proof is quite easy, it involves a question that comes up frequently in such problems, see, e.g., Remark 1.9 of [Nelson et al. 2014].

**Lemma 2.9.** *Let  $l \leq n_0$  be a nonnegative integer. For each character  $\mu$  with  $a(\mu) = l$ , we have  $a(\mu\pi) \leq \max(n, l + m)$ . Furthermore, for each  $r \geq 0$ ,*

$$|\{\mu \in \tilde{X} : a(\mu) = l, a(\mu\pi) = \max(n, l + m) - r\}| \leq q^{l-r/2}.$$

*Proof.* If  $\pi$  is supercuspidal we have  $l + m \leq n$ . Writing  $\pi$  as a twist of a minimal supercuspidal, the result follows from Tunnell’s theorem [1978, Proposition 3.4] on conductors of twists of supercuspidal representations. If  $\pi$  is principal series, then it follows from the well-known formula  $a(\chi_1 \boxplus \chi_2) = a(\chi_1) + a(\chi_2)$ . If  $\pi$  is a twist of the Steinberg representations, it follows from the formula  $a(\chi \text{St}) = \max(2a(\chi), 1)$ . □

**2E. The support and average size of  $W_{\pi}$ .** In this subsection we will prove an important technical result (Proposition 2.10) about the size and support of  $W_{\pi}$ . This will then be combined with the results of the previous subsection to deduce Proposition 2.11 which will be needed for our global application. To motivate all these results, we first recall a conjecture made in [Saha 2016].

**Conjecture 1** (local Lindelöf hypothesis for Whittaker newforms). *Suppose that  $a(\omega_{\pi}) \leq n_1$  (i.e.,  $m_1 = 0$ ). Then*

$$1 \ll \sup_{g \in G} |W_{\pi}(g)| \ll_{\varepsilon} q^{n\varepsilon}.$$

This conjecture (originally stated as [Saha 2016, Conjecture 2]) seems to be quite hard as it implies square-root cancellation in sums of twisted  $\text{GL}_{2-\varepsilon}$ -factors. However, for the purpose of this paper, we can prove a bound that is (at least) as strong as the above conjecture on *average*. This is achieved by the second part of the next proposition, which generalizes some results obtained in [Nelson et al. 2014, Section 2], which considered the special case  $\omega_{\pi} = 1$ .

**Proposition 2.10.** (1) *If  $W_{\pi}(g) \neq 0$ , then  $t(g) \geq -\max(2l(g), l(g) + m, n)$ .*



(2) Suppose  $t(g) = -\max(2l(g), l(g) + m, n) + r$  where  $r \geq 0$ . Then we have

$$\left( \int_{v \in \mathfrak{o}^\times} |W_\pi(a(v)g)|^2 d^\times v \right)^{1/2} \ll q^{-r/4}.$$

*Proof.* By twisting  $\pi$  with a character of the form  $| \cdot |^{lr}$  if necessary (which does not change  $|W_\pi|$ ), we may assume  $\omega_\pi \in \tilde{X}$ . Also assume  $n \geq 1$ , as the case  $n = 0$  is trivial. Because of the coset decomposition from earlier, we may further assume that  $g = g_{t,l,v} := a(\varpi^t)wn(\varpi^{-l}v)$ . Finally, because of Lemma 2.7, we can assume (by replacing  $\pi$  by  $\tilde{\pi}$  if necessary) that  $0 \leq l \leq n_0$ . The desired result then is the following:

- Let  $0 \leq l \leq n_0$ . If  $W_\pi(g_{t,l,v}) \neq 0$ , then  $t \geq -\max(n, l + m)$ . Further if  $t = -\max(n, l + m) + r$  where  $r \geq 0$  then

$$\left( \int_{v \in \mathfrak{o}^\times} |W_\pi(g_{t,l,v})|^2 d^\times v \right)^{1/2} \ll q^{-r/4}.$$

In the notation of (4), the above is equivalent to:

**Claim 1.** Let  $0 \leq l \leq n_0$ . If there exists  $\mu \in \tilde{X}$  such that  $a(\mu) \leq l$  and  $c_{t,l}(\mu) \neq 0$  then  $t \geq -\max(n, l + m)$ . Further if  $t = -\max(n, l + m) + r$  where  $r \geq 0$  then  $\sum_{\substack{\mu \in \tilde{X} \\ a(\mu) \leq l}} |c_{t,l}(\mu)|^2 \ll q^{-r/2}$ .

Define the quantities  $d_{t,l}(\mu)$  via the following identity (of polynomials in  $q^{\pm s}$ ):

$$\varepsilon\left(\frac{1}{2}, \mu\pi\right) \left( \sum_{t=-\infty}^{\infty} q^{(t+a(\mu\pi))(1/2-s)} c_{t,l}(\mu) \right) L(s, \mu\pi)^{-1} = \left( \sum_{t=-\infty}^{\infty} q^{(t+a(\mu\pi))(1/2-s)} d_{t,l}(\mu) \right). \quad (5)$$

Note that (for fixed  $l$  and  $\mu$ )  $d_{t,l}(\mu)$  is nonzero for only finitely many  $t$ . Furthermore,  $c_{t,l}(\mu) = \sum_{i=0}^{\infty} \alpha_i d_{t-i,l}(\mu)$  where  $|\alpha_0| = 1$  and  $|\alpha_i| \ll q^{-i/2}$ . (In fact, if  $\pi$  is supercuspidal,  $\alpha_i = 0$  for all  $i > 0$ ). Hence it suffices to prove Claim 1 for the quantities  $d_{t,l}(\mu)$  rather than  $c_{t,l}(\mu)$ . Therefore using (4) it suffices to prove this:

**Claim 2.** Let  $0 \leq l \leq n_0$ . Define the quantities  $d_{t,l}(\mu)$  via the identity

$$\left( \sum_{t=-\infty}^{\infty} q^{(t+a(\mu\pi))(1/2-s)} d_{t,l}(\mu) \right) = \omega_\pi(-1) \left( \sum_{a=0}^{\infty} W_\pi(a(\varpi^a)) q^{-a(1/2-s)} G(\varpi^{a-l}, \mu^{-1}) \right) L(1-s, \mu^{-1}\omega_\pi^{-1}\pi)^{-1}. \quad (6)$$

If there exists  $\mu \in \tilde{X}$  such that  $a(\mu) \leq l$  and  $d_{t,l}(\mu) \neq 0$  then  $t \geq -\max(n, l + m)$ . Further, if  $t = -\max(n, l + m) + r$  with  $r \geq 0$ , then  $\sum_{\substack{\mu \in \tilde{X} \\ a(\mu) \leq l}} |d_{t,l}(\mu)|^2 \ll q^{-r/2}$ .

We only consider the case  $L(s, \pi) = 1$ , as the case  $L(s, \pi) \neq 1$  is similar but easier. (Note that  $L(s, \pi) \neq 1$  if and only if either  $m = n$  or  $n = 1$ .)

Let  $\mu \in \tilde{X}$  be such that  $a(\mu) \leq l$ . As  $L(s, \pi) = 1$ , we can use the well-known formulas stated in [Saha 2016, Equation (6) and Lemma 2.5] to deduce that the quantity on the RHS of (6) lying inside the bracket is a constant of absolute value  $\ll q^{-l/2}$  if  $a(\mu) = l$  or if  $a(\mu) = 0$  and  $l = 1$ ; and is equal to 0 otherwise. Furthermore, there are at most 2 characters  $\mu \in \tilde{X}$  with  $a(\mu) \leq n_0$  and  $L(s, \mu^{-1}\omega_\pi^{-1}\pi) \neq 1$  (this can be checked, for example, using the classification written down in [Saha 2016, Section 2.2]).

We henceforth assume that  $a(\mu) = l$  or  $a(\mu) = 0$  and  $l = 1$ ; else there is nothing to prove as  $d_{t,l}(\mu) = 0$ . Suppose first that  $L(s, \mu^{-1}\omega_\pi^{-1}\pi) = 1$ . Then, by equating coefficients on both sides of (6), we see that  $d_{t,l}(\mu) \neq 0$  implies  $t = -a(\mu\pi) \geq -\max(n, a(\mu) + m) \geq -\max(n, l + m)$ , using Lemma 2.9. Furthermore if  $t = -\max(n, l + m) + r$ , then

$$\sum_{\substack{\mu \in \tilde{X} \\ a(\mu) \in \{l, 0\} \\ L(s, \mu\pi) = 1}} |d_{t,l}(\mu)|^2 \ll \sum_{\substack{\mu \in \tilde{X} \\ a(\mu) \in \{l, 0\} \\ a(\mu\pi) = \max(n, l+m) - r}} q^{-l} \ll q^{-r/2},$$

again using Lemma 2.9.

Suppose next that  $L(s, \mu^{-1}\omega_\pi^{-1}\pi) \neq 1$ . In this case  $\mu \neq 1$  so if  $d_{t,l}(\mu) \neq 0$  we must have  $a(\mu) = l$ . Also, the right side of (6) is of the form  $\alpha_0 + \alpha_1 q^{-1(1/2-s)} + \alpha_2 q^{-2(1/2-s)}$  with  $\alpha_i \ll q^{-(l+i)/2}$ . Furthermore if  $\alpha_2 \neq 0$  then  $a(\mu\pi) = 0 \leq n - 2$  and if  $\alpha_2 = 0$  then  $\alpha_1 \neq 0$  and  $a(\mu\pi) \leq \max(n_0, m) \leq n - 1$ . So again equating coefficients and using Lemma 2.9, we see that  $d_{t,l}(\mu) \neq 0 \Rightarrow t \geq -n \geq -\max(n, l + m)$ , and furthermore if  $t = -\max(n, l + m) + r$ , then

$$\sum_{\substack{\mu \in \tilde{X} \\ a(\mu) = l \\ L(s, \mu\pi) \neq 1}} |d_{t,l}(\mu)|^2 \ll \sum_{i=0}^2 \sum_{\substack{\mu \in \tilde{X} \\ a(\mu) = l \\ a(\mu\pi) = \max(n, l+m) - r - i}} q^{-l-i} \ll q^{-r/2},$$

again using Lemma 2.9.

Putting everything together, the proof of Claim 2 is complete. □

Next, for any  $g \in G$ , define

$$n_0(g) = \min(l(g), n - l(g)), \quad \text{and} \quad q(g) = \max(n_0, n_0(g) - n_1 + m).$$

We note the useful bounds  $0 \leq n_0(g) \leq n_0$  and  $n_0 \leq q(g) \leq n_0 + m_1$ .

**Proposition 2.11.** *Suppose that  $g \in Ka(\varpi^{n_1})$ . Assume further that either  $n$  is even or  $l(g) \leq n_0$ .*

- (1) *If for some  $y \in F^\times$ , we have  $W_\pi(a(y)g) \neq 0$ , then  $v(y) \geq -q(g)$ .*

(2) Suppose  $b = -q(g) + r$  where  $r \geq 0$ . Then we have

$$\left( \int_{v \in \mathfrak{o}^\times} |W_\pi(a(\varpi^b v)g)|^2 d^\times v \right)^{1/2} \ll q^{-r/4}.$$

*Proof.* This follows immediately from Lemma 2.4 and Proposition 2.10. □

**Remark 2.12.** Note that the map on  $\mathfrak{o}^\times$  given by  $v \mapsto |W_\pi(a(vy)g)|$  is  $U_{n_0(g)}$  invariant for all  $y \in F^\times$  and  $g \in G$ . Hence the second part of Proposition 2.11 is equivalent to

$$\frac{1}{|\mathfrak{o}^\times / U_{n_0(g)}|} \sum_{v \in \mathfrak{o}^\times / U_{n_0(g)}} |W_\pi(a(\varpi^b v)g)|^2 d^\times v \ll q^{-r/2}.$$

**2F. Test functions.** We now change gears and start looking at certain local test functions (related to matrix coefficients) that will be used later in the trace formula. We begin with some definitions. Let  $C_c^\infty(G, \omega_\pi^{-1})$  be the space of functions  $\kappa$  on  $G$  with the following properties:

- (1)  $\kappa(z(y)g) = \omega_\pi^{-1}(y)\kappa(g)$ .
- (2)  $\kappa$  is locally constant.
- (3)  $|\kappa|$  is compactly supported on  $Z \backslash G$ .

Given  $\kappa_1, \kappa_2 \in C_c^\infty(G, \omega_\pi^{-1})$  we define the convolution  $\kappa_1 * \kappa_2 \in C_c^\infty(G, \omega_\pi^{-1})$  via

$$(\kappa_1 * \kappa_2)(h) = \int_{Z \backslash G} \kappa_1(g^{-1})\kappa_2(gh) dg, \tag{7}$$

which turns  $C_c^\infty(G, \omega_\pi^{-1})$  into an associative algebra.

Next let  $\sigma$  be a representation of  $G$  with central character equal to  $\omega_\pi$ . Then, for any  $\kappa \in C_c^\infty(G, \omega_\pi^{-1})$  and any vector  $v \in \sigma$ , we define  $R(\kappa)v$  to be the vector in  $\sigma$  given by

$$R(\kappa)v = \int_{Z \backslash G} \kappa(g)(\sigma(g)v) dg. \tag{8}$$

Let  $v_\pi$  be any *newform* in the space of  $\pi$ , i.e., any nonzero vector fixed by  $K_1(\mathfrak{p}^n)$ . Equivalently  $v_\pi$  can be any vector in  $\pi$  corresponding to  $W_\pi$  under some isomorphism  $\pi \simeq \mathcal{W}(\pi, \psi)$ . Thus  $v_\pi$  is unique up to multiples. Put  $v'_\pi = \pi(a(\varpi^{n_1}))v_\pi$ . Note that  $v'_\pi$  is, up to multiples, the unique nonzero vector in  $\pi$  that is invariant under the subgroup  $a(\varpi^{n_1})K_1(\mathfrak{p}^n)a(\varpi^{-n_1})$ .

Let  $\langle \cdot, \cdot \rangle$  be any  $G$ -invariant inner product on  $\pi$  (this is also unique up to multiples). Define a matrix coefficient  $\Phi_\pi$  on  $G$  as follows:

$$\Phi_\pi(g) = \frac{\langle v_\pi, \pi(g)v_\pi \rangle}{\langle v_\pi, v_\pi \rangle};$$

this is clearly independent of the choice of  $v_\pi$  or the normalization of the inner product. Further, let

$$K^0 := K^0(\mathfrak{p}^{n_1-n_0}) = \begin{cases} K & \text{if } n \text{ is even,} \\ K^0(\mathfrak{p}) & \text{if } n \text{ is odd.} \end{cases}$$

Put

$$\Phi'_\pi(g) = \begin{cases} \Phi_\pi(a(\varpi^{-n_1})ga(\varpi^{n_1})) = \frac{\langle v'_\pi, \pi(g)v'_\pi \rangle}{\langle v'_\pi, v'_\pi \rangle} & \text{if } g \in ZK^0, \\ 0 & \text{if } g \notin ZK^0. \end{cases}$$

Then it follows that  $\Phi'_\pi \in C_c^\infty(G, \omega_\pi^{-1})$  and  $\Phi'_\pi(g^{-1}) = \overline{\Phi'_\pi(g)}$ . In particular, the operator  $R(\Phi'_\pi)$  is self-adjoint.

**Proposition 2.13.** *There exists a positive real constant  $\delta_\pi$  depending only on  $\pi$  and satisfying  $\delta_\pi \gg q^{-n_1-m_1}$  such that the following hold:*

- (1)  $R(\Phi'_\pi)v'_\pi = \delta_\pi v'_\pi$ .
- (2)  $\Phi'_\pi * \Phi'_\pi = \delta_\pi \Phi'_\pi$ .

**Remark 2.14.** This is a refinement of a result of Marshall [2016] that holds in the special case  $\omega_\pi = 1$ ; he used a slightly different test function which does not differentiate between  $n$  odd and even.

**Remark 2.15.** In fact with some additional work one can prove  $\delta_\pi \asymp q^{-n_1-m_1}$ .

The rest of this section will be devoted to proving this proposition. We note a useful corollary.

**Corollary 2.16.** *Let  $\sigma$  be a generic irreducible admissible unitarizable representation of  $G$  such that  $\omega_\sigma = \omega_\pi$  and let  $v_\sigma$  be any vector in the space of  $\sigma$ . Suppose that  $R(\Phi'_\pi)v_\sigma = \delta v_\sigma$  for some complex number  $\delta$ . Then  $\delta \in \{0, \delta_\pi\}$ ; in particular,  $\delta$  is a nonnegative real number.*

*Proof.* We have

$$\delta \delta_\pi v_\sigma = \delta_\pi R(\Phi'_\pi)v_\sigma = R(\Phi'_\pi * \Phi'_\pi)v_\sigma = R(\Phi'_\pi)R(\Phi'_\pi)v_\sigma = \delta^2 v_\sigma,$$

implying that  $\delta \in \{0, \delta_\pi\}$ . □

**2G. Some preparatory lemmas.**

**Lemma 2.17.** *Consider the representation  $\pi|_{K^0}$  of  $K^0$  and let  $\pi'$  be the subrepresentation of  $\pi|_{K^0}$  generated by  $v'_\pi$ . Then  $\pi'$  is a finite dimensional irreducible representation of  $K^0$ .*

*Proof.* We know that  $\pi'$  is isomorphic to a direct sum of irreducible representations of  $K^0$ . However if there were more than one summand in the decomposition of  $\pi'$ , then the representation  $\pi|_{K^0}$  (and hence the representation  $\pi$ ) would contain a  $a(\varpi^{n_1})K_1(\mathfrak{p}^n)a(\varpi^{-n_1})$ -fixed subspace of dimension greater than one; by newform

theory this is impossible. Hence  $\pi'$  is irreducible. The finite dimensionality of  $\pi'$  follows from the admissibility of  $\pi$ . □

**Lemma 2.18.** *Let  $\pi'$  be as in Lemma 2.17. Then both claims of Proposition 2.13 hold with the quantity  $\delta_\pi$  defined as follows:*

$$\delta_\pi = \int_{Z \backslash G} |\Phi'_\pi(g)|^2 dg = \int_{K^0} |\Phi'_\pi(g)|^2 dg = \frac{1}{[K : K^0] \dim(\pi')}.$$

*Proof.* Note that  $\langle \cdot, \cdot \rangle$  is an invariant inner product for  $\pi'$ . It follows immediately (from the orthonormality of matrix coefficients) that the last two quantities are equal. The equality of the middle two quantities is immediate from our normalization of Haar measures.

We now show that this quantity satisfies the claims of Proposition 2.13. First of all,  $R(\Phi'_\pi)v'_\pi$  is a vector in  $\pi$  that is invariant under the subgroup  $a(\varpi^{n_1})K_1(\mathfrak{p}^n)a(\varpi^{-n_1})$ . It follows that  $R(\Phi'_\pi)v'_\pi = \delta v'_\pi$  for some constant  $\delta$ . Taking inner products with  $v'_\pi$  immediately shows that  $\delta = \delta_\pi$ . This proves the first assertion of Proposition 2.13. The second assertion is a standard property of convolutions of matrix coefficients. □

*Proof of Proposition 2.13 in the case of nonsupercuspidal representations.* For any nonsupercuspidal representation  $\pi$  it suffices to show that

$$\dim(\pi') \ll q^{n_0+m_1},$$

where  $\pi'$  is as in Lemma 2.17.

We can embed  $\pi$  inside a representation  $\chi_1 \boxplus \chi_2$ , consisting of smooth functions  $f$  on  $G$  satisfying

$$f\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} g\right) = \left|\frac{a}{d}\right|^{1/2} \chi_1(a)\chi_2(d)f(g).$$

Here  $\chi_1$  and  $\chi_2$  are two (not necessarily unitary) characters. Let  $f'$  be the function in  $\chi_1 \boxplus \chi_2$  that corresponds to  $v'_\pi$ . Let  $K'$  be the (normal) subgroup of  $K^0$  consisting of matrices  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  such that  $a \equiv d \equiv 1 \pmod{\mathfrak{p}^{n_0+m_1}}$ ,  $b \equiv 0 \pmod{\mathfrak{p}^{n_1+m_1}}$  and  $c \equiv 0 \pmod{\mathfrak{p}^{n_0+m_1}}$ . Let  $V_{K'}$  be the subspace of  $\chi_1 \boxplus \chi_2$  consisting of the functions  $f$  that satisfy  $f(gk) = \omega_\pi(a)f(g)$  for all  $k = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in K'$ . Then  $f' \in V_{K'}$ . Moreover (and this is the key fact!) if  $k \in K^0$  and  $k' \in K'$ , then the top left entries of  $k'$  and  $kk'k^{-1}$  (both these matrices are elements of  $K'$ ) are equal modulo  $\mathfrak{p}^m$ . Hence the space  $V_{K'}$  is stable under the action of  $K^0$ . So it suffices to prove that  $\dim(V_{K'}) \ll q^{n_0+m_1}$ .

Using the Iwasawa decomposition, it follows that  $|B(F) \backslash G(F) / K'| \asymp q^{n_0+m_1}$ . Fix a set of double coset representatives  $S$  for  $B(F) \backslash G(F) / K'$ . Since any element of  $V_{K'}$  is uniquely determined by its values on  $S$ , it follows that  $\dim(V_{K'}) \ll q^{n_0+m_1}$ . The proof is complete. □

**2H. Proof of Proposition 2.13 in the case of supercuspidal representations.** We now assume that  $\pi$  is supercuspidal. In this case,  $m \leq n_0$ , hence  $m_1 = 0$ . So it suffices to prove that

$$\int_{K^0} |\Phi_\pi(a(\varpi^{-n_1})ga(\varpi^{n_1}))|^2 dg \gg q^{-n_1}. \tag{9}$$

The next proposition gives a formula for  $\Phi_\pi$ , which may be of independent interest.

**Proposition 2.19.** *For  $0 \leq l < n$ , we have*

$$\begin{aligned} \Phi_\pi(n(x)g_{t,l,v}) &= G(-\varpi^{l-n}, 1)G(\varpi^{t+l}v^{-1} - x, 1)\omega_\pi(-v)\delta_{t,-2l} \\ &\quad + \varepsilon\left(\frac{1}{2}, \pi\right)\omega_\pi(v) \sum_{\substack{\mu \in \tilde{X} \\ a(\mu)=n-l \\ a(\mu\tilde{\pi})=n-2l-t}} G(\varpi^{l-n}, \mu)G(vx - \varpi^{t+l}, \mu)\varepsilon\left(\frac{1}{2}, \mu\tilde{\pi}\right). \end{aligned} \tag{10}$$

*Proof.* Using the usual inner product in the Whittaker model, and the fact that  $W_\pi(a(t))$  is supported on  $t \in \mathfrak{o}^\times$ , (as  $\pi$  is supercuspidal) it follows that

$$\Phi_\pi(n(x)g_{t,l,v}) = \int_{\mathfrak{o}^\times} \psi(-ux)\omega_\pi(u)\overline{W_\pi(g_{t,l,vu^{-1}})} d^\times u. \tag{11}$$

On the other hand, by the formula for  $W_\pi$  in [Saha 2016, Proposition 2.30] and using Lemma 2.7 we have

$$\begin{aligned} W_\pi(a(\varpi^t)wn(\varpi^{-l}v)) &= \omega_\pi(-v^{-1})\psi(-\varpi^{t+l}v^{-1})G(\varpi^{l-n}, 1)\delta_{t,-2l} \\ &\quad + \left( \varepsilon\left(\frac{1}{2}, \tilde{\pi}\right)\omega_\pi(v^{-1})\psi(-\varpi^{t+l}v^{-1}) \right. \\ &\quad \left. \times \sum_{\substack{\mu \in \tilde{X} \\ a(\mu)=n-l \\ a(\mu\pi)=n-t-2l}} G(\varpi^{l-n}, \mu^{-1})\varepsilon\left(\frac{1}{2}, \mu^{-1}\pi\right)\mu(-v). \right) \end{aligned}$$

Substituting this into (11), we immediately get the required result. □

To obtain (9), we will need to substitute the formula from Proposition 2.19 and integrate. The following elementary lemma (which is similar to Lemma 2.6 of [Hu 2017]) will be useful; we omit its proof.

**Lemma 2.20.** *Let  $f$  be a function on  $G$  that is right  $K_1(\mathfrak{p}^n)$ -invariant. Then*

$$\int_G f(g) dg = \sum_{k=0}^n A_k \int_B f(bwn(\varpi^{-k})) db,$$

where  $A_0 = (1 + q^{-1})^{-1}$ ,  $A_n = q^n(1 + q^{-1})^{-1}$  and, for  $0 < k < n$ ,  $A_k = q^k(1 - q^{-1})(1 + q^{-1})^{-1}$ .

We now complete the proof of (9). Using Lemma 2.20, it suffices to prove that

$$\int_{\substack{b \in B \\ bwn(\varpi^{-n_1}) \in a(\varpi^{-n_1})K^0a(\varpi^{n_1})}} |\Phi_\pi(bwn(\varpi^{-n_1}))|^2 db \gg q^{-2n_1}. \tag{12}$$

Now, note that the quantity  $z(u)n(x)a(y)wn(\varpi^{-n_1})$  lies in  $a(\varpi^{-n_1})K^0a(\varpi^{n_1})$  if and only if

$$u = \varpi^{n_1}u', \quad y = \varpi^{-2n_1}y' \quad \text{and} \quad x = \varpi^{-n_1}x',$$

for  $y' \in \mathfrak{o}^\times$ ,  $u' \in \mathfrak{o}^\times$ ,  $x' \in \mathfrak{o}$  and  $y' - x' \in \mathfrak{p}^{n_1-n_0}$ . Hence the left side of (12) is equals

$$q^{-n_1} \int_{\substack{y' \in \mathfrak{o}^\times, x' \in \mathfrak{o} \\ x' \in y' + \mathfrak{p}^{n_1-n_0}}} |\Phi_\pi(n(\varpi^{-n_1}x')g_{-2n_1, -n_1, y'-1})|^2 dx' d^\times y'. \tag{13}$$

Now, we can exactly evaluate the integral in (13) using Proposition 2.19. We expand  $|\Phi_\pi(n(\varpi^{-n_1}x')g_{-2n_1, -n_1, y'-1})|^2$  and observe that the main (diagonal) terms are simple to evaluate as we know the modulus-squared of Gauss sums. Indeed, the contribution to (13) from the diagonal terms is simply

$$q^{-n_1} \int_{\substack{y' \in \mathfrak{o}^\times, x' \in \mathfrak{o} \\ x' \in y' + \mathfrak{p}^{n_1-n_0}}} \sum_{\substack{\mu \in \tilde{X} \\ a(\mu) = n_0 \\ a(\mu\tilde{\pi}) = n}} q^{-2n_0} \asymp q^{-2n_1}.$$

On the other hand, the contribution from the cross terms is zero. Indeed, each cross term involves an integral like

$$\int_{\substack{y' \in \mathfrak{o}^\times, x' \in \mathfrak{o} \\ y'^{-1}x' - 1 \in \mathfrak{p}^{n_1-n_0}\mathfrak{o}^\times}} \mu_1^{-1} \mu_2((y'^{-1}x' - 1)\varpi^{n_0-n_1}),$$

which equals 0 because of the orthogonality of characters. This completes the proof of (12). □

### 3. Sup-norms of global newforms

From now on, we move to a global setup and consider newforms on  $GL_2(\mathbb{A})$  where  $\mathbb{A}$  is the ring of adèles over  $\mathbb{Q}$ . For any place  $v$  of  $\mathbb{Q}$ , we will use the notation  $X_v$  for each *local object*  $X$  introduced in the previous section. The corresponding global objects will be typically denoted without the subscript  $v$ . The archimedean place will be denoted by  $v = \infty$ . We will usually denote a nonarchimedean place  $v$  by  $p$ , where  $p$  is a rational prime. The set of all nonarchimedean places (primes) will be denoted by  $f$ .

We fix measures on all our adelic groups (like  $\mathbb{A}$ ,  $\mathrm{GL}_2(\mathbb{A})$ , etc.) by taking the product of the local measures over all places (for the nonarchimedean places, these local measures were normalized in Section 2A; at the archimedean place we fix once and for all a suitable Haar measure). We normalize the Haar measure on  $\mathbb{R}$  to be the usual Lebesgue measure. We give all discrete groups the counting measure and thus obtain a measure on the appropriate quotient groups.

**3A. Statement of result.** As usual, let  $G = \mathrm{GL}_2$ . Let  $\pi = \otimes_v \pi_v$  be an irreducible, unitary, cuspidal automorphic representation of  $G(\mathbb{A})$  with central character  $\omega_\pi = \prod_v \omega_{\pi_v}$ . For each prime  $p$ , let the integers  $n_p, n_{1,p}, n_{0,p}, m_p$ , and  $m_{1,p}$  be defined as in Section 2B. We put  $N = \prod_p p^{n_p}$ ,  $N_0 = \prod_p p^{n_{0,p}}$ ,  $N_1 = \prod_p p^{n_{1,p}}$ ,  $M = \prod_p p^{m_p}$ , and  $M_1 = \prod_p p^{m_{1,p}}$ . Thus,  $N$  is the conductor of  $\pi$ ,  $M$  is the conductor of  $\omega_\pi$ ,  $N_0$  is the largest integer such that  $N_0^2 \mid N$ , and  $N_1 = N/N_0$  is the smallest integer such that  $N \mid N_1^2$ . Let  $N_2 = N_1/N_0 = N/N_0^2$ . Note that  $N_2$  is a squarefree integer and is the product of all the primes  $p$  such that  $p$  divides  $N$  to an odd power. If  $N$  is squarefree, then  $N_2 = N_1 = N$  and  $N_0 = 1$  while if  $N$  is a perfect square then  $N_0 = N_1 = \sqrt{N}$  and  $N_2 = 1$ . Note also that  $M_1 = M/\mathrm{gcd}(M, N_1)$ .

We assume that  $\pi_\infty$  is a spherical principal series representation whose central character is trivial on  $\mathbb{R}^+$ . This means that  $\pi_\infty \simeq \chi_1 \boxplus \chi_2$ ,<sup>8</sup> where for  $i = 1, 2$ , we have  $\chi_i = |y|^{it} \mathrm{sgn}(y)^m$ ,  $\chi_2 = |y|^{-it} \mathrm{sgn}(y)^m$ , with  $m \in \{0, 1\}$ , and  $t \in \mathbb{R} \cup (-\frac{i}{2}, \frac{i}{2})$ .

Let  $K_1(N) = \prod_{p \in f} K_{1,p}(p^{n_p}) = \prod_{p \nmid N} G(\mathbb{Z}_p) \prod_{p \mid N} K_{1,p}(p^{n_p})$  be the standard congruence subgroup of  $G(\widehat{\mathbb{Z}}) = \prod_{p \in f} G(\mathbb{Z}_p)$ ; note that  $K_1(N)G(\mathbb{R})^+ \cap G(\mathbb{Q})$  is equal to the standard congruence subgroup  $\Gamma_1(N)$  of  $\mathrm{SL}_2(\mathbb{Z})$ . Let  $K_\infty = \mathrm{SO}_2(\mathbb{R})$  be the maximal connected compact subgroup of  $G(\mathbb{R})$  (equivalently, the maximal compact subgroup of  $G(\mathbb{R})^+$ ). We say that a nonzero automorphic form  $\phi \in V_\pi$  is a *newform* if  $\phi$  is  $K_1(N)K_\infty$ -invariant. It is well-known that a newform  $\phi$  exists and is unique up to multiples, and corresponds to a factorizable vector  $\phi = \otimes_v \phi_v$ . We define

$$\|\phi\|_2 = \int_{Z(\mathbb{A})G(F)\backslash G(\mathbb{A})} |\phi(g)|^2 dg.$$

**Remark 3.1.** If  $\phi$  is a newform, then the function  $f$  on  $\mathbb{H}$  defined by  $f(g(i)) = \phi(g)$  for each  $g \in \mathrm{SL}_2(\mathbb{R})$  is a Hecke–Maass cuspidal newform of level  $N$  (and character  $\omega_\pi$ ). Precisely, it satisfies the relation

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} z\right) = \left(\prod_{p \mid N} \omega_{\pi,p}(d)\right) f(z), \quad \text{for all } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N). \tag{14}$$

<sup>8</sup>For two characters  $\chi_1$  and  $\chi_2$  on  $\mathbb{R}^\times$ , we let  $\chi_1 \boxplus \chi_2$  denote the principal series representation on  $G(\mathbb{R})$  that is unitarily induced from the corresponding representation of  $B(\mathbb{R})$ ; this consists of smooth functions  $f$  on  $G(\mathbb{R})$  satisfying

$$f\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} g\right) = \left|\frac{a}{d}\right|^{1/2} \chi_1(a)\chi_2(d)f(g).$$



The Laplace eigenvalue  $\lambda$  for  $f$  is given by  $\lambda = \frac{1}{4} + t^2$  where  $t$  is as above. (Note that  $\lambda \asymp (1 + |t|)^2$ .)

Furthermore, any Hecke–Maass cuspidal newform  $f$  is obtained in the above manner from a newform  $\phi$  in a suitable automorphic representation  $\pi$ . The newform  $\phi$  can be directly constructed from  $f$  via strong approximation. It is clear that  $\sup_{g \in G(\mathbb{A})} |\phi(g)| = \sup_{z \in \Gamma_0(N) \backslash \mathbb{H}} |f(z)|$ .

Our main result is as follows.

**Theorem 3.2.** *Let  $\pi$  be an irreducible, unitary, cuspidal automorphic representation of  $G(\mathbb{A})$  such that  $\pi_\infty \simeq \chi_1 \boxplus \chi_2$ , where, for  $i = 1, 2$ , we have  $\chi_1 = |y|^{it} \operatorname{sgn}(y)^m$  and  $\chi_2 = |y|^{-it} \operatorname{sgn}(y)^m$ , with  $m \in \{0, 1\}$  and  $t \in \mathbb{R} \cup (-\frac{i}{2}, \frac{i}{2})$ . Let the integers  $N_0, N_1$  and  $M_1$  be defined as above and let  $\phi \in V_\pi$  be a newform satisfying  $\|\phi\|_2 = 1$ . Then*

$$\sup_{g \in G(\mathbb{A})} |\phi(g)| \ll_\varepsilon N_0^{1/6+\varepsilon} N_1^{1/3+\varepsilon} M_1^{1/2} (1 + |t|)^{5/12+\varepsilon}.$$

**Remark 3.3.** If  $\pi$  has trivial central character and  $N_1 \asymp \sqrt{N}$  (this is the case whenever  $N$  is sufficiently “powerful”), then we get  $\sup_{g \in G(\mathbb{A})} |\phi(g)| \ll_{t,\varepsilon} N^{1/4+\varepsilon}$ , which is a considerable improvement over the best previously known result [Saha 2014]  $\sup_{g \in G(\mathbb{A})} |\phi(g)| \ll_{t,\varepsilon} N^{5/12+\varepsilon}$ , due to the author.

**3B. Atkin–Lehner operators and a generating domain.** Let  $\pi$  be as in Section 3A and  $\phi \in V_\pi$  a newform. In order to prove Theorem 3.2 we will restrict the variable  $g$  to a carefully chosen generating domain inside  $G(\mathbb{A})$ . In order to do this, we will have to consider the newform  $\phi$  along with some of its Atkin–Lehner translates. The object of this section is to explain these ideas and describe our generating domain. The main result in this context is Proposition 3.6 below.

We begin with some definitions. For any integer  $L$ , let  $\mathcal{P}(L)$  denote the set of distinct primes dividing  $L$ . For any subset  $S$  of  $\mathcal{P}(N)$ , let  $\eta_S, h_S \in G(\mathbb{A}_f)$  be defined as follows:  $\eta_{S,p} = \begin{bmatrix} & 1 \\ p^{n_p} & \end{bmatrix}$  if  $p \in S$  and  $\eta_{S,p} = 1$  otherwise;  $h_{S,p} = a(p^{n_{1,p}})$  if  $p \in S$  and  $h_{S,p} = 1$  otherwise. Define

$$K_S = \prod_{p \in S} G(\mathbb{Z}_p) \subset G(\mathbb{A}_f), \quad J_S = K_S h_S \subset G(\mathbb{A}_f).$$

Finally, define

$$\mathcal{J}_S = \{g \in J_S : l(g_p) \leq n_{0,p} \text{ for all } p \in S \text{ such that } n_p \text{ is odd}\}.$$

Using Lemma 2.2, we see that  $g \in \prod_{p \in S} G(\mathbb{Q}_p)$  belongs to  $\mathcal{J}_S$  if and only if  $g_p \in wK_p^0(p)a(p^{n_{1,p}})$  for all  $p \in S$  for which  $n_p$  is odd. If  $L$  divides  $N$ , we abuse notation by denoting

$$h_L = h_{\mathcal{P}(L)}, \quad K_L = K_{\mathcal{P}(L)}, \quad J_L = J_{\mathcal{P}(L)} \quad \text{and} \quad \mathcal{J}_L = \mathcal{J}_{\mathcal{P}(L)}.$$

For any  $0 < c < \infty$ , let  $D_c$  be the subset of  $B_1(\mathbb{R})^+ \simeq \mathbb{H}$  defined by

$$D_c := \{n(x)a(y) : x \in \mathbb{R}, y \geq c\}.$$

Finally, for  $L > 0$ , define

$$\mathcal{F}_L = \{n(x)a(y) \in D_{\sqrt{3}/(2L)} : z = x + iy \text{ satisfies } |cz + d|^2 \geq 1/L, \forall (0, 0) \neq (c, d) \in \mathbb{Z}^2\}.$$

Next, for any subset  $S$  of  $\mathcal{P}(N)$ , let  $\omega_\pi^S = \prod_v \omega_{\pi,v}^S$  be the unique character<sup>9</sup> on  $\mathbb{Q}^\times \backslash \mathbb{A}^\times$  with the following properties:

- (1)  $\omega_{\pi,\infty}^S$  is trivial on  $\mathbb{R}^+$ .
- (2)  $\omega_{\pi,p}^S|_{\mathbb{Z}_p^\times}$  is trivial if  $p \in S$  and equals  $\omega_{\pi,p}|_{\mathbb{Z}_p^\times}$  if  $p \notin S$ .

Note that  $\omega_\pi^{\mathcal{P}(N)} = 1$ ,  $\omega_\pi^\emptyset = \omega_\pi$  and, for each  $S$ ,  $\omega_\pi^S$  has conductor  $\prod_{p \notin S} p^{m_p}$ . Define the irreducible, unitary, cuspidal automorphic representation  $\pi^S$  by  $\pi^S = \tilde{\pi} \otimes \omega_\pi^S = \pi \otimes (\omega_\pi^{-1} \omega_\pi^S)$ . A key observation is that for every  $S$ , the representation  $\pi^S$  has conductor  $N$  and its central character  $\omega_{\pi^S} = \omega_\pi^{-1} (\omega_\pi^S)^2$  has conductor  $M$ . We have  $\pi^\emptyset = \pi$  and  $\pi^{\mathcal{P}(N)} = \tilde{\pi}$ .

**Lemma 3.4.** *The function  $\phi^S$  on  $G(\mathbb{A})$  given by  $\phi^S(g) := (\omega_\pi^{-1} \omega_\pi^S)(\det(g))\phi(g\eta_S)$  is a newform in  $\pi^S$ .*

*Proof.* It is clear that  $\phi^S$  is a vector in  $\pi^S$ , and one can easily check from the defining relation that it is  $K_1(N)K_\infty$  invariant. □

**Remark 3.5.** In the special case  $\omega_\pi = 1$ , one has  $\pi^S = \pi$  for every subset  $S$  of  $\mathcal{P}(N)$ . In this case, for each  $S$ , the involution  $\pi(\eta_S)$  on  $V_\pi$  corresponds to a classical Atkin–Lehner operator, and  $\phi^S = \pm\phi$  with the sign equal to the Atkin–Lehner eigenvalue. We will call the natural map on  $Z(\mathbb{A})G(\mathbb{Q}) \backslash G(\mathbb{A})/K_1(N)K_\infty$  induced by  $g \mapsto g\eta_S$  the adelic Atkin–Lehner operator associated to  $S$ .

Recall that  $\mathcal{J}_N = \prod_{p|N_2} wK_p^0(p)a(p^{n_{1,p}}) \prod_{p|N, p \nmid N_2} G(\mathbb{Z}_p)a(p^{n_{1,p}}) \subset G(\mathbb{A}_f)$ . The next proposition tells us that any point in  $Z(\mathbb{A})G(\mathbb{Q}) \backslash G(\mathbb{A})/K_1(N)K_\infty$  can be moved by an adelic Atkin–Lehner operator to a point whose finite part lies in  $\mathcal{J}_N$  and whose infinite component lies in  $\mathcal{F}_{N_2}$ .

**Proposition 3.6.** *Suppose that  $g \in G(\mathbb{A})$ . Then there exists a subset  $S$  of  $\mathcal{P}(N_2)$  such that*

$$g \in Z(\mathbb{A})G(\mathbb{Q})(\mathcal{J}_N \times \mathcal{F}_{N_2})\eta_S K_1(N)K_\infty.$$

*Proof.* Let  $w_N$  be the diagonal embedding of  $w = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$  into  $K_N$ . The determinant map from  $w_N h_N K_1(N) h_N^{-1} w_N^{-1}$  is surjective onto  $\prod_p \mathbb{Z}_p^\times$ . Hence by strong

---

<sup>9</sup>The existence, as well as uniqueness, of the character  $\omega_\pi^S$  follows from the identity  $\mathbb{A}^\times = \mathbb{Q}^\times \mathbb{R}^+ \prod_p \mathbb{Z}_p^\times$ .

approximation for  $gh_N^{-1}w_N^{-1}$ , we can write  $gh_N^{-1}w_N^{-1} = zg_{\mathbb{Q}}g_{\infty}^+(w_Nh_Nkh_N^{-1}w_N^{-1})$  where  $z \in Z(\mathbb{A})$ ,  $g_{\mathbb{Q}} \in G(\mathbb{Q})$ ,  $g_{\infty}^+ \in G(\mathbb{R})^+$  and  $k \in K_1(N)$ . In other words,

$$g \in Z(\mathbb{A})G(\mathbb{Q})g_{\infty}^+w_Nh_NK_1(N). \tag{15}$$

Using Lemma 1 from [Harcos and Templier 2012], we can find a divisor  $N_3$  of  $N_2$ , and a matrix  $W \in M_2(\mathbb{Z})$  such that

$$W \equiv \begin{bmatrix} 0 & * \\ 0 & 0 \end{bmatrix} \pmod{N_3}, \quad W \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N_2}, \quad \det(W) = N_3, \quad W_{\infty}g_{\infty}^+ \in \mathcal{F}_{N_2}K_{\infty}.$$

$W_{\infty}$  denotes the element  $W$  considered as an element of  $G(\mathbb{R})^+$ . Let  $S$  be the set of primes dividing  $N_3$ . Note that  $W_p \in K_{0,p}(p)\begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix}$  if  $p \in S$ ,  $W_p \in K_{0,p}(p)$  if  $p \mid N_2$  but  $p \notin S$ , and  $W_p \in G(\mathbb{Z}_p)$  if  $p \nmid N_2$ . Since  $W \in G(\mathbb{Q})$ , it follows from above and from (15) that  $g$  is an element of

$$\begin{aligned} Z(\mathbb{A})G(\mathbb{Q})\mathcal{F}_{N_2}K_{\infty} \left( \prod_{p \in S} K_{0,p}(p)\begin{bmatrix} 0 & 1 \\ p & 0 \end{bmatrix} w \right) & \left( \prod_{\substack{p \mid N_2 \\ p \notin S}} K_{0,p}(p) w \right) \left( \prod_{\substack{p \mid N \\ p \nmid N_2}} G(\mathbb{Z}_p) \right) h_N K_1(N) \\ & = Z(\mathbb{A})G(\mathbb{Q})(\mathcal{J}_N \times \mathcal{F}_{N_2})\eta_S K_1(N) K_{\infty}, \end{aligned}$$

where in the last step we have used Lemma 2.3. □

**Corollary 3.7.** *Let  $\pi$  and  $\phi$  be as in Theorem 3.2. Suppose that for all subsets  $S$  of  $\mathcal{P}(N_2)$  and all  $g \in \mathcal{J}_N$ ,  $n(x)a(y) \in \mathcal{F}_{N_2}$ , we have*

$$|\phi^S(gn(x)a(y))| \ll_{\varepsilon} N_1^{1/2+\varepsilon} M_1^{1/2} N_2^{-1/6} (1 + |t|)^{5/12+\varepsilon}.$$

*Then the conclusion of Theorem 3.2 is true.*

*Proof.* This follows from Proposition 3.6 and the fact that

$$|\phi^S(gn(x)a(y))| = |\phi(gn(x)a(y)\eta_S)|. \tag{□}$$

**3C. Sketch of proof modulo technicalities.** We now prove Theorem 3.2 assuming some key bounds whose proofs will take the rest of this paper. For brevity we put  $T = 1 + |t|$ . Also, recall that  $N_2 = N_1/N_0$ . We need to show that for each  $g \in G(\mathbb{A})$ ,

$$|\phi(g)| \ll_{\varepsilon} N_1^{1/2+\varepsilon} M_1^{1/2} N_2^{-1/6} T^{5/12+\varepsilon}.$$

By letting  $\phi$  run over all its various Atkin–Lehner translates  $\phi^S$ , for  $S \subseteq \mathcal{P}(N_2)$ , we may assume (by Corollary 3.7) that  $g \in \mathcal{J}_N \mathcal{F}_{N_2}$ . Therefore, in what follows, we will not explicitly keep track of the set  $S$ , but instead prove the following: *Given an automorphic representation  $\pi$  as in Section 3A (with associated quantities  $N_1$ ,  $N_2$ ,  $T$  and  $M_1$  as defined earlier), a newform  $\phi \in V_{\pi}$  satisfying  $\|\phi\|_2 = 1$ , and elements  $g \in \mathcal{J}_N$  and  $n(x)a(y) \in \mathcal{F}_{N_2}$ , we have*

$$|\phi(gn(x)a(y))| \ll_{\varepsilon} N_1^{1/2+\varepsilon} M_1^{1/2} N_2^{-1/6} T^{5/12+\varepsilon}. \tag{16}$$

As noted, the above statement implies Theorem 3.2. Implicit here is the fact that we are letting  $\pi$  vary among the various  $\pi^S$ , which all have exactly the same values of  $N, N_1, N_2, M_1$  and  $T$  as  $\pi$ , and moreover the corresponding newforms  $\phi^S$  all satisfy  $\|\phi^S\|_2 = \|\phi\|_2$ .

We prove (16) by a combination of two methods. In Proposition 3.8, we use the Whittaker expansion to bound this quantity. Precisely, we prove the following bound:

$$|\phi(gn(x)a(y))| \ll_\varepsilon (NT)^\varepsilon \left( \left( \frac{N_1 M_1 T}{N_2 y} \right)^{1/2} + \left( \frac{N_1 T^{1/3}}{N_2} \right)^{1/2} \right). \tag{17}$$

To prove (17) we rely on Proposition 2.11. Next, in Proposition 3.16, we use the amplification method to bound this quantity. We prove that for each  $\Lambda \geq 1$ , we have

$$|\phi(gn(x)a(y))|^2 \ll_\varepsilon (NT\Lambda)^\varepsilon N_1 M_1 \left[ \frac{T + N_2^{1/2} T^{1/2} y}{\Lambda} + \Lambda^{1/2} T^{1/2} (N_2^{-1/2} + y) + \Lambda^2 T^{1/2} N_2^{-1} \right]. \tag{18}$$

The proof of this bound relies on Proposition 2.13 and some counting arguments due to Harcos and Templier. Combining the two bounds leads to Theorem 3.2, as we explain now.

Choose  $\Lambda = T^{1/6} N_2^{1/3}$ . Then (18) becomes

$$|\phi(gn(x)a(y))|^2 \ll_\varepsilon (NT)^\varepsilon N_1 M_1 [T^{5/6} N_2^{-1/3} + T^{7/12} N_2^{-1/6} y]. \tag{19}$$

If  $y \leq T^{1/4} N_2^{-1/6}$ , then we use (19) to immediately deduce (16). If  $y \geq T^{1/4} N_2^{-1/6}$ , then we use (17) to obtain the bound

$$|\phi(gn(x)a(y))| \ll_\varepsilon (NT)^\varepsilon M_1^{1/2} N_1^{1/2} N_2^{-5/12} T^{3/8}, \tag{20}$$

which is much stronger than (16)! This completes the proof.

**3D. The bound via the Whittaker expansion.** Let  $\pi$  and  $\phi$  be as in Section 3A with  $\|\phi\|_2 = 1$ . The object of this section is to prove the following result.

**Proposition 3.8.** *Let  $x \in \mathbb{R}, y \in \mathbb{R}^+$  and  $g \in \mathcal{J}_N$ . Then*

$$|\phi(gn(x)a(y))| \ll_\varepsilon (NT)^\varepsilon \left( \left( \frac{N_0 M_1 T}{y} \right)^{1/2} + (N_0 T^{1/3})^{1/2} \right).$$

**Remark 3.9.** If we assume Conjecture 1, then we can improve the bound in Proposition 3.8 to

$$(NT)^\varepsilon \left( \left( \frac{N_0 M_1 T}{y} \right)^{1/2} + (T^{1/3})^{1/2} \right).$$

We now begin the proof of Proposition 3.8. One has the usual Fourier expansion at infinity

$$\phi(n(x)a(y)) = y^{1/2} \sum_{n \in \mathbb{Z} \neq 0} \rho_\phi(n) K_{it}(2\pi |n|y) e(nx). \tag{21}$$

Lemma 3.10 notes some key properties about the Fourier coefficients in (21).

**Lemma 3.10.** *The Fourier coefficients  $\rho_\phi(n)$  satisfy the following properties:*

- (1)  $|\rho_\phi(n)| = |\rho_\phi(1)\lambda_\pi(n)|$  where  $\lambda_\pi(n)$  are the coefficients of the  $L$ -function of  $\pi$ .
- (2)  $|\rho_\phi(1)| \ll_\varepsilon (NT)^\varepsilon e^{\pi t/2}$ .
- (3)  $\sum_{1 \leq |n| \leq X} |\lambda_\pi(n)|^2 \ll X(NTX)^\varepsilon$ .

*Proof.* All the parts are standard. The first part is a basic well-known relation between the Fourier coefficients and Hecke eigenvalues. The second part is due to Hoffstein and Lockhart [1994]. The last part follows from the analytic properties of the Rankin–Selberg  $L$ -function (e.g., see [Harcos and Michel 2006]). □

The Fourier expansion (21) is a special case of the more general Whittaker expansion that we describe now. Let  $g_f \in G(\mathbb{A}_f)$ . Then the Whittaker expansion for  $\phi$  says that

$$\phi(g_f n(x)a(y)) = \sum_{q \in \mathbb{Q} \setminus \{0\}} W_\phi(a(q)g_f n(x)a(y)), \tag{22}$$

where  $W_\phi$  is a global Whittaker newform corresponding to  $\phi$  given explicitly by

$$W_\phi(g) = \int_{x \in \mathbb{A}/\mathbb{Q}} \phi(n(x)g)\psi(-x) dx.$$

Putting  $g_f = 1$  in (22) gives us the expansion (21). On the other hand, the function  $W_\phi$  factors as  $W_\phi(g) = c \prod_v W_v(g_v)$  where

- (1)  $W_p = W_{\pi_p}$  at all finite primes  $p$ ,
- (2)  $|W_\infty(a(q)n(x)a(y))| = |qy|^{1/2} |K_{it}(2\pi|q|y)|$ .

The constant  $c$  is related to  $L(1, \pi, \text{Ad})$ ; for further details on this constant, see [Saha 2016, Section 3.4].

For any  $g = \prod_{p|N} g_p \in \mathcal{J}_N$ , define

$$N_0^g = \prod_{p|N} p^{n_0(g_p)} \quad \text{and} \quad Q^g = \prod_{p|N} p^{q(g_p)},$$

where the integers  $n_0(g_p)$  and  $q(g_p)$  are as defined just before Proposition 2.11. Note that the “useful bounds” stated there imply that  $N_0^g | N_0$  and  $Q^g | N_0 M_1$ .

**Lemma 3.11.** *Suppose that  $g \in \mathcal{J}_N$  and  $W_\phi(a(q)gn(x)a(y)) \neq 0$  for some  $q \in \mathbb{Q}$ . Then we have  $q = n/Q^g$  for some  $n \in \mathbb{Z}$ .*

*Proof.* We have  $W_{\pi_p}(a(q)g_p) \neq 0$  for each  $p | N$  and  $W_{\pi_p}(a(q)) \neq 0$  for each  $p \nmid N$ . Now the result follows from Proposition 2.11 and Lemma 2.6. □

Henceforth we fix some  $g \in \mathcal{J}_N$ . By comparing the expansion (22) for  $g_f = g$  with the trivial case  $g_f = 1$ , we conclude that

$$\begin{aligned} &\phi(gn(x)a(y)) \\ &= \sum_{n \in \mathbb{Z} \neq 0} W_\phi(a(n/Q^g)gn(x)a(y)) \\ &= \sum_{n \in \mathbb{Z} \neq 0} \left( \prod_{p|N} W_{\pi_p}(a(n/Q^g)g) \right) \left( c \prod_{p \nmid N} W_{\pi_p}(a(n)) \right) W_\infty(a(n/Q^g)n(x)a(y)) \\ &= \left( \frac{y}{Q^g} \right)^{1/2} \sum_{n \in \mathbb{Z} \neq 0} (|n|, N^\infty)^{1/2} \rho_\phi \left( \frac{n}{(|n|, N^\infty)} \right) \lambda_{\pi_N}(n; g) K_{it} \left( \frac{2\pi|n|y}{Q^g} \right) \chi_n, \end{aligned} \tag{23}$$

where  $\chi_n$  is some complex number of absolute value 1, and for each nonnegative integer  $n$  we define

$$\lambda_{\pi_N}(n; g) := \prod_{p|N} W_{\pi_p}(a(np^{-q(g_p)})g_p).$$

The tail of the sum (23) consisting of the terms with  $2\pi|n|y/Q^g > T + T^{1/3+\varepsilon}$  is negligible because of the exponential decay of the Bessel function. Put

$$R = Q^g \left( \frac{T + T^{1/3+\varepsilon}}{2\pi y} \right) \asymp \frac{Q^g T}{y}.$$

Using the Cauchy–Schwarz inequality and Lemma 3.10, we therefore have

$$\begin{aligned} |\phi(gn(x)a(y))|^2 &\ll_\varepsilon (NT)^\varepsilon e^{\pi t} \left( \frac{y}{Q^g} \right) \left( \sum_{0 < n < R} (|n|, N^\infty) \left| \lambda_\pi \left( \frac{n}{(|n|, N^\infty)} \right) \right|^2 \right) \\ &\quad \times \left( \sum_{0 < n < R} \left| \lambda_{\pi_N}(n; g) K_{it} \left( \frac{2\pi|n|y}{Q^g} \right) \right|^2 \right). \end{aligned} \tag{24}$$

**Lemma 3.12.** *The function  $\lambda_{\pi_N}(n; g)$  satisfies the following properties:*

- (1) *Suppose that  $n_1$  is a positive integer such that  $n_1 | N^\infty$ , and  $n_0, n'_0$  are two integers coprime to  $N$  such that  $n_0 \equiv n'_0 \pmod{N_0^g}$ . Then*

$$|\lambda_{\pi_N}(n_0 n_1; g)| = |\lambda_{\pi_N}(n'_0 n_1; g)|.$$

- (2) *For any integer  $r$  and any  $n_1 | N^\infty$ ,*

$$\sum_{\substack{rN_0^g \leq |n_0| < (r+1)N_0^g \\ (n_0, N) = 1}} |\lambda_{\pi_N}(n_0 n_1; g)|^2 \ll N_0^g n_1^{-1/2}.$$

*Proof.* Let  $p | N$  and  $u_1, u_2 \in \mathbb{Z}_p^\times$ . Then by (3) it follows that, for all  $w \in \mathbb{Q}_p^\times$ ,

$$|W_{\pi_p}(a(wu_1)g_p)| = |W_{\pi_p}(a(wu_2)g_p)|,$$

whenever  $u_1 \equiv u_2 \pmod{(p^{n_0(g_p)})}$ . It follows that if  $n_1 | N^\infty$ , then

$$|\lambda_{\pi_N}(n_0 n_1; g)| = |\lambda_{\pi_N}(n'_0 n_1; g)| \quad \text{if } n_0 \equiv n'_0 \pmod{N_0^g}. \tag{25}$$

Furthermore using the above and the Chinese remainder theorem,

$$\frac{1}{N_0^g} \sum_{\substack{n_0 \bmod N_0^g \\ (n_0, N)=1}} |\lambda_{\pi_N}(n_0 n_1; g)|^2 = \prod_{p|N} \left( \int_{\mathbb{Z}_p^\times} |W_{\pi_p}(a(n_1 v p^{-q(g_p)}) g_p)|^2 d^\times v \right),$$

and hence by Proposition 2.11,

$$\frac{1}{N_0^g} \sum_{\substack{n_0 \bmod N_0^g \\ (n_0, N)=1}} |\lambda_{\pi_N}(n_0 n_1; g)|^2 \ll n_1^{-1/2}. \quad \square$$

**Lemma 3.13.** *We have*

$$\sum_{0 < n < R} t e^{\pi t} \left| \lambda_{\pi_N}(n; g) K_{it} \left( \frac{2\pi |n| y}{Q^g} \right) \right|^2 \ll_\epsilon (NT)^\epsilon \left( N_0^g T^{1/3} + \frac{Q^g T}{y} \right).$$

**Remark 3.14.** If we assume Conjecture 1, then the bound on the right side can be improved to  $(NT)^\epsilon (T^{1/3} + (Q^g T)/y)$ .

*Proof.* Let  $f(y) = \min(T^{1/3}, |y/T - 1|^{-1/2})$ . Then it is known that

$$t e^{\pi t} |K_{it}(y)|^2 \ll f(y),$$

see, e.g., [Templier 2015, (3.1)]. Using the previous lemma, we may write

$$\begin{aligned} t e^{\pi t} \sum_{0 < n < R} \left| \lambda_{\pi_N}(n; g) K_{it} \left( \frac{2\pi |n| y}{Q^g} \right) \right|^2 &\ll \sum_{\substack{1 \leq n_1 \leq R \\ n_1 | N^\infty}} \sum_{\substack{1 \leq |n_0| \leq R/n_1 \\ (n_0, N)=1}} |\lambda_{\pi_N}(n_0 n_1; g)|^2 f \left( \frac{2\pi |n_0 n_1| y}{Q^g} \right) \\ &\ll \sum_{\substack{1 \leq n_1 \leq R \\ n_1 | N^\infty}} \sum_{0 \leq r \leq \lfloor R/(n_1 N_0^g) \rfloor} \sum_{\substack{r N_0^g \leq |n_0| \leq (r+1) N_0^g \\ (n_0, N)=1}} |\lambda_{\pi_N}(n_0 n_1; g)|^2 f \left( \frac{2\pi |n_0 n_1| y}{Q^g} \right) \\ &\ll N_0^g \sum_{\substack{1 \leq n_1 \leq R \\ n_1 | N^\infty}} n_1^{-1/2} \sum_{0 \leq r \leq \lfloor R/(n_1 N_0^g) \rfloor} f \left( \frac{2\pi |n_0^{(r)} n_1| y}{Q^g} \right) \end{aligned}$$

(where  $n_0^{(r)} \in [r N_0^g, (r + 1) N_0^g]$  is the point where  $f(2\pi n_0^{(r)} n_1 y / Q^g)$  is maximum, and where we have used Lemma 3.12)

$$\ll \sum_{\substack{1 \leq n_1 \leq R \\ n_1 | N^\infty}} n_1^{-1/2} N_0^g \left( T^{1/3} + \int_0^{R/(N_0^g n_1)} f \left( \frac{2\pi N_0^g r n_1 y}{Q^g} \right) dr \right)$$

(as  $f$  has  $\ll 1$  turning points)

$$\begin{aligned} &\ll \sum_{\substack{1 \leq n_1 \leq R \\ n_1 \mid N^\infty}} \left( N_0^g T^{1/3} n_1^{-1/2} + n_1^{-3/2} \frac{Q^g}{y} \int_0^{T+T^{1/3+\epsilon}} \left| \frac{s}{T} - 1 \right|^{-1/2} ds \right) \\ &\ll_\epsilon (NT)^\epsilon \left( N_0^g T^{1/3} + \frac{Q^g T}{y} \right). \quad \square \end{aligned}$$

**Lemma 3.15.** *For all  $X > 0$ , we have*

$$\sum_{0 < n < X} (|n|, N^\infty) \left| \lambda_\pi \left( \frac{n}{(|n|, N^\infty)} \right) \right|^2 \ll_\epsilon (NTX)^\epsilon X.$$

*Proof.* This follows from the last part of Lemma 3.10 using a similar (but simpler) argument to Lemma 3.13. □

Finally, by combining (24), Lemma 3.13 and Lemma 3.15, we get the bound

$$|\phi(gn(x)a(y))|^2 \ll_\epsilon (NT)^\epsilon \left( \frac{Q^g T}{y} + N_0^g T^{1/3} \right). \quad (26)$$

Taking square roots, and using that  $Q^g \leq N_0 M_1$  and  $N_0^g \leq N_0$ , we get the conclusion of Proposition 3.8.

**3E. Preliminaries on amplification.** Our aim for the rest of this paper is to prove the following proposition. As explained in Section 3C, this will complete the proof of our main result.

**Proposition 3.16.** *Let  $\Lambda \geq 1$  be a real number. Let  $n(x)a(y) \in \mathcal{F}_{N_2}$ ,  $g \in \mathcal{J}_N$ . Then*

$$\begin{aligned} &|\phi(gn(x)a(y))|^2 \\ &\ll_\epsilon (\Lambda NT)^\epsilon N_1 M_1 \left[ \frac{T + N_2^{1/2} T^{1/2} y}{\Lambda} + \Lambda^{1/2} T^{1/2} (N_2^{-1/2} + y) + \Lambda^2 T^{1/2} N_2^{-1} \right]. \quad (27) \end{aligned}$$

Recall that  $h_N = \prod_{p|N} a(p^{n_{1,p}})$ . Define the vector  $\phi' \in V_\pi$  by

$$\phi'(g) = \phi(gh_N).$$

Then the problem becomes equivalent to bounding the quantity  $\phi'(k_N n(x)a(y))$  where  $k_N \in K_N = \prod_{p|N} G(\mathbb{Z}_p)$  and  $k_N h_N \in \mathcal{J}_N$ . Note that  $\phi'$  is  $K'_1(N)K_\infty$ -invariant where  $K'_1(N) := h_N K_1(N) h_N^{-1}$ .

Define the function  $\Phi'_N$  on  $\prod_{p|N} G(\mathbb{Q}_p)$  by  $\Phi'_N = \prod_{p|N} \Phi'_{\pi_p}$ , with the functions  $\Phi'_{\pi_p}$  defined in Section 2F. By Proposition 2.13, it follows that

$$R(\Phi'_N)\phi' := \int_{(Z \setminus G)(\prod_{p|N} \mathbb{Q}_p)} \Phi'_N(g)(\pi(g)\phi') dg = \delta_N \phi',$$



where  $\delta_N \gg N_1^{-1} M_1^{-1}$ . Note also that if  $g \in \prod_{p|N} G(\mathbb{Q}_p)$  and  $\Phi'_N(g) \neq 0$ , then  $g \in Z(\mathbb{Q}_p)G(\mathbb{Z}_p)$  for each prime  $p$  dividing  $N$  and  $g \in Z(\mathbb{Q}_p)K_p^0(p)$  for each prime  $p$  dividing  $N_2$ . Also, recall that  $R(\Phi'_N)$  is a self-adjoint, essentially idempotent operator.

Next, we consider the primes not dividing  $N$ . Let  $\mathcal{H}_{\text{ur}}$  be the usual global (unramified) convolution Hecke algebra; it is generated by the set of all functions  $\kappa_{\text{ur}}$  on  $\prod_{p \nmid N} G(\mathbb{Q}_p)$  such that for each finite prime  $p$  not dividing  $N$ ,

- (1)  $\kappa_p \in C_c^\infty(G(\mathbb{Q}_p), \omega_{\pi_p}^{-1})$ ,
- (2)  $\kappa_p$  is bi- $G(\mathbb{Z}_p)$ -invariant.

It is well-known that  $\mathcal{H}_{\text{ur}}$  is a commutative algebra and is generated by the various functions  $\kappa_\ell$  (as  $\ell$  varies over integers coprime to  $N$ ) where  $\kappa_\ell = \prod_{p \nmid N} \kappa_{\ell,p}$  and the function  $\kappa_{\ell,p}$  in  $C_c^\infty(G(\mathbb{Q}_p), \omega_{\pi_p}^{-1})$  is defined as follows:

- (1)  $\kappa_{\ell,p}(zka(\ell)k) = |\ell|^{-1/2} \omega_{\pi_p}^{-1}(z)$  for all  $z \in Z(\mathbb{Q}_p)$  and  $k \in G(\mathbb{Z}_p)$ .
- (2)  $\kappa_{\ell,p}(g) = 0$  if  $g \notin Z(\mathbb{Q}_p)G(\mathbb{Z}_p)a(\ell)G(\mathbb{Z}_p)$ .

Then, it follows that for each  $\kappa_{\text{ur}} \in \mathcal{H}_{\text{ur}}$ ,

$$R(\kappa_{\text{ur}})\phi' := \int_{\prod_{p \nmid N} (Z \backslash G)(\mathbb{Q}_p)} \kappa_{\text{ur}}(g)(\pi(g)\phi') dg = \delta_{\text{ur}}\phi',$$

where  $\delta_{\text{ur}}$  is a complex number (depending linearly on  $\kappa_{\text{ur}}$ ). Furthermore,

$$R(\kappa_\ell)\phi' = \lambda_\pi(\ell)\phi',$$

where the Hecke eigenvalues  $\lambda_\pi(\ell)$  were defined earlier in Lemma 3.10. Moreover, we note that as  $\kappa_{\text{ur}}$  varies over  $\mathcal{H}_{\text{ur}}$ , the corresponding operators  $R(\kappa_{\text{ur}})$  form a commuting system of normal operators. Indeed, if we define  $\kappa_\ell^* = (\prod_{p|\ell} \omega_{\pi_p}^{-1}(\ell))\kappa_\ell$ , and extend this via multiplicativity and antilinearity to all of  $\mathcal{H}_{\text{ur}}$ , then we have an involution  $\kappa \mapsto \kappa^*$  on all of  $\mathcal{H}_{\text{ur}}$ . It is well-known that  $\kappa^*(g) = \overline{\kappa(g^{-1})}$  and hence  $R(\kappa^*)$  is precisely the adjoint of  $R(\kappa)$ .

Finally, we consider the infinite place. For  $g \in G(\mathbb{R})^+$ , let  $u(g)$  denote the hyperbolic distance from  $g(i)$  to  $i$ ; precisely  $u(g) = 3D|g(i) - i|^2 / (4 \text{Im}(g(i)))$ . Each bi- $Z(\mathbb{R})K_\infty$ -invariant function  $\kappa_\infty$  in  $C_c^\infty(Z(\mathbb{R}) \backslash G(\mathbb{R})^+)$ , can be viewed as a function on  $\mathbb{R}^+$  via  $\kappa_\infty(g) = \kappa_\infty(u(g))$ . For each irreducible spherical unitary principal series representation  $\sigma$  of  $G(\mathbb{R})$ , we define the Harish-Chandra–Selberg transform  $\hat{\kappa}_\infty(\sigma)$  via

$$\hat{\kappa}_\infty(\sigma) = \int_{Z(\mathbb{R}) \backslash G(\mathbb{R})^+} \kappa_\infty(g) \frac{\langle \sigma(g)v_\sigma, v_\sigma \rangle}{\langle v_\sigma, v_\sigma \rangle} dg,$$

where  $v_\sigma$  is the unique (up to multiples) spherical vector in the representation  $\sigma$ . For all such  $\sigma$  it is known that  $R(\kappa_\infty)v_\sigma = \hat{\kappa}_\infty(\sigma)v_\sigma$ ; in particular  $R(\kappa_\infty)\phi' = \hat{\kappa}_\infty(\pi_\infty)\phi'$ .

By [Templier 2015, Lemma 2.1] there exists such a function  $\kappa_\infty$  on  $G(\mathbb{R})$  with the following properties:

- (1)  $\kappa_\infty(g) = 0$  unless  $g \in G(\mathbb{R})^+$  and  $u(g) \leq 1$ .
- (2)  $\hat{\kappa}_\infty(\sigma) \geq 0$  for all irreducible spherical unitary principal series representations  $\sigma$  of  $G(\mathbb{R})$ .
- (3)  $\hat{\kappa}_\infty(\pi_\infty) \gg 1$ .
- (4) For all  $g \in G(\mathbb{R})^+$ ,  $|\kappa_\infty(g)| \leq T$ . Moreover, if  $u(g) \geq T^{-2}$ , then  $|\kappa_\infty(g)| \leq T^{1/2}/u(g)^{1/4}$ .

Henceforth, we fix a function  $\kappa_\infty$  as above.

**3F. The amplified pretrace formula.** In this subsection, we will use  $L^2(X)$  as a shorthand for  $L^2(G(\mathbb{Q}) \backslash G(\mathbb{A}) / K'_1(N) K_\infty, \omega_\pi)$ .

Let the functions  $\Phi'_N, \kappa_\infty$  be as defined in the previous subsection. Consider the space of functions  $\kappa$  on  $G(\mathbb{A})$  such that  $\kappa = \Phi'_N \kappa_{\text{ur}} \kappa_\infty$  with  $\kappa_{\text{ur}}$  in  $\mathcal{H}_{\text{ur}}$ . We fix an orthonormal basis  $\mathcal{B} = \{\psi\}$  of the space  $L^2(X)$  such that  $\phi' \in \mathcal{B}$  and consisting of eigenfunctions for all the operators  $R(\kappa)$  with  $\kappa$  as above; i.e., for all  $\psi \in \mathcal{B}$ , there exists a complex number  $\lambda_\psi$  satisfying

$$R(\Phi'_N)R(\kappa_{\text{ur}})R(\kappa_\infty)\psi = R(\kappa)\psi := \int_{Z(\mathbb{A}) \backslash G(\mathbb{A})} \kappa(g)(\pi(g)\psi) dg = \lambda_\psi \psi.$$

Such a basis exists because the set of all  $R(\kappa)$  as above form a commuting system of normal operators. The basis  $\mathcal{B}$  naturally splits into a discrete and continuous part, with the continuous part consisting of Eisenstein series and the discrete part consisting of cusp forms and residual functions.

Given a  $\kappa = \Phi'_N \kappa_{\text{ur}} \kappa_\infty$  as above, we define the automorphic kernel  $K_\kappa(g_1, g_2)$  for  $g_1, g_2 \in G(\mathbb{A})$  via

$$K_\kappa(g_1, g_2) = \sum_{\gamma \in Z(\mathbb{Q}) \backslash G(\mathbb{Q})} \kappa(g_1^{-1} \gamma g_2).$$

A standard calculation tells us that if  $\psi = \otimes_v \psi_v$  is an element of  $L^2(X)$  such that  $\psi_v$  is an eigenfunction for  $R(\kappa_v)$  with eigenvalue  $\lambda_v$ , for each place  $v$ , then

$$\int_{Z(\mathbb{A})G(\mathbb{Q}) \backslash G(\mathbb{A})} K_\kappa(g_1, g_2)\psi(g_2) dg_2 = \left(\prod_v \lambda_v\right)\psi(g_1). \tag{28}$$

**Lemma 3.17.** *Suppose that  $\kappa_{\text{ur}} = \kappa'_{\text{ur}} * (\kappa'_{\text{ur}})^*$  for some  $\kappa'_{\text{ur}} \in \mathcal{H}_{\text{ur}}$ . Put  $\kappa = \Phi'_N \kappa_{\text{ur}} \kappa_\infty$ . If  $\psi \in \mathcal{B}$  then*

$$\int_{Z(\mathbb{A})G(\mathbb{Q}) \backslash G(\mathbb{A})} K_\kappa(g_1, g_2)\psi(g_2) dg_2 = \lambda_\psi \psi(g_1),$$

for some  $\lambda_\psi \geq 0$ . Moreover  $\lambda_{\phi'} \geq M_1^{-1} N_1^{-1} |\lambda'_{\text{ur}}|^2 \hat{\kappa}_\infty(\pi_\infty)$  where the quantity  $\lambda'_{\text{ur}}$  is defined by  $R(\kappa'_{\text{ur}})\phi' = \lambda'_{\text{ur}}\phi'$ .

*Proof.* By our assumption that  $\psi \in \mathcal{B}$ , a complex number  $\lambda_\psi$  as above exists. We can write  $\lambda_\psi = \lambda_{\psi,N} \lambda_{\psi,\text{ur}} \lambda_{\psi,\infty}$  using the decomposition  $R(\kappa) = R(\Phi'_N)R(\kappa_{\text{ur}})R(\kappa_\infty)$ . We have  $\lambda_{\psi,\infty} \geq 0$  by our assumption  $\hat{\kappa}_\infty(\sigma) \geq 0$  for all irreducible spherical unitary principal series representations  $\sigma$  of  $G(\mathbb{R})$ . We have  $\lambda_{\psi,N} \geq 0$  by Corollary 2.16. Finally if  $R(\kappa'_{\text{ur}})\psi = \lambda'_{\psi} \psi$  then  $\lambda_{\psi,\text{ur}} = |\lambda'_{\psi}|^2 \geq 0$ . Hence  $\lambda_\psi \geq 0$ . The last assertion is immediate from the results of the previous subsection. □

Henceforth we assume that  $\kappa_{\text{ur}} = \kappa'_{\text{ur}} * (\kappa'_{\text{ur}})^*$  for some  $\kappa'_{\text{ur}} \in \mathcal{H}_{\text{ur}}$  and we put  $\kappa = \Phi'_N \kappa_{\text{ur}} \kappa_\infty$ . Then spectrally expanding  $K_\kappa(g, g)$  along  $\mathcal{B}$  and using Lemma 3.17 we get, for all  $g \in G(\mathbb{A})$ ,

$$M_1^{-1} N_1^{-1} \hat{\kappa}_\infty(\pi_\infty) |\lambda'_{\text{ur}} \phi'(g)|^2 \leq K_\kappa(g, g).$$

Note that  $\hat{\kappa}_\infty(\pi_\infty) \geq 1$ . Next we look at the quantity  $K_\kappa(g, g)$ . Assume that  $g = k_N n(x) a(y)$  with  $k_N = \prod_{p|N} k_p \in K_N$  and  $k_N h_N \in \mathcal{J}_N$ . The second condition means that  $k_p \in wK_p^0(p)$  for all  $p | N_2$ . We have

$$K_\kappa(g, g) = \sum_{\gamma \in Z(\mathbb{Q}) \backslash G(\mathbb{Q})} \Phi'_N(k_N^{-1} \gamma k_N) \kappa_{\text{ur}}(\gamma) \kappa_\infty((n(x) a(y))^{-1} \gamma n(x) a(y)).$$

Above we have  $\Phi'_N(k_N^{-1} \gamma k_N) \leq 1$ , moreover if  $\Phi'_N(k_N^{-1} \gamma k_N) \neq 0$  then we must have

- (a)  $k_p^{-1} \gamma k_p \in Z(\mathbb{Q}_p) G(\mathbb{Z}_p)$  for all primes  $p$  dividing  $N$ , and
- (b)  $k_p^{-1} \gamma k_p \in Z(\mathbb{Q}_p) K_p^0(p)$  for all primes  $p$  dividing  $N_2$ .

Condition (a) implies that  $\gamma \in Z(\mathbb{Q}_p) G(\mathbb{Z}_p)$  for all primes  $p$  dividing  $N$ . Condition (b), together with the fact that  $k_p \in wK_p^0(p)$  for all  $p | N_2$ , implies that  $\gamma \in Z(\mathbb{Q}_p) K_{0,p}(p)$  for all primes  $p$  dividing  $N_2$ .

Finally we have  $\kappa_\infty(g) = 0$  if  $\det(g) < 0$ , and if  $\det(g) > 0$  we can write  $\kappa_\infty(g) = \kappa_\infty(u(g))$  as explained earlier, whence

$$\kappa_\infty((n(x) a(y))^{-1} \gamma n(x) a(y)) = \kappa_\infty(u(z, \gamma z)), \quad z = x + iy,$$

where, for any two points  $z_1$  and  $z_2$  on the upper-half plane,  $u(z_1, z_2)$  denotes the hyperbolic distance between them, i.e.,  $u(z_1, z_2) = |z_1 - z_2|^2 / (4 \text{Im}(z_1) \text{Im}(z_2))$ . Putting everything together, we get the following Proposition.

**Proposition 3.18.** *Let  $\kappa'_{\text{ur}} \in \mathcal{H}_{\text{ur}}$  and suppose that  $R(\kappa'_{\text{ur}})\phi' = \lambda'_{\text{ur}}\phi'$ . Let  $\kappa_{\text{ur}} = \kappa'_{\text{ur}} * (\kappa'_{\text{ur}})^*$  and  $\kappa = \Phi'_N \kappa_{\text{ur}} \kappa_\infty$ . Then for all  $z = x + iy$  and all  $k \in K_N$  such that  $kh_N \in \mathcal{J}_N$ , we have*

$$|\phi'(kn(x) a(y))|^2 \leq \frac{M_1 N_1}{|\lambda'_{\text{ur}}|^2} \sum_{\substack{\gamma \in Z(\mathbb{Q}) \backslash G(\mathbb{Q})^+, \\ \gamma \in Z(\mathbb{Q}_p) K_{0,p}(p) \forall p | N_2 \\ \gamma \in Z(\mathbb{Q}_p) G(\mathbb{Z}_p) \forall p | N}} |\kappa_{\text{ur}}(\gamma) \kappa_\infty(u(z, \gamma z))|.$$

**3G. Conclusion.** We now make a specific choice for  $\kappa_{\text{ur}}$ . Let  $\Lambda \geq 1$  be a real number. We let

$$S = \{\ell : \ell \text{ prime, } (\ell, N) = 1, \Lambda \leq \ell \leq 2\Lambda\}.$$

Define for each integer  $r$ ,

$$c_r = \begin{cases} |\lambda_\pi(r)|/\lambda_\pi(r) & \text{if } r = \ell \text{ or } r = \ell^2, \ell \in S, \\ 0 & \text{otherwise.} \end{cases}$$

We set  $\kappa'_{\text{ur}} = \sum_r c_r \kappa_r$ , and  $\kappa_{\text{ur}} = \kappa'_{\text{ur}} * (\kappa'_{\text{ur}})^*$ . Given this, let us estimate the quantities appearing in Proposition 3.18.

First of all, we have  $\lambda'_{\text{ur}} = \sum_{\ell \in S} (|\lambda_\pi(\ell)| + |\lambda_\pi(\ell^2)|)$ . By the well-known relation  $\lambda_\pi(\ell)^2 - \lambda_\pi(\ell^2) = \omega_{\pi_\ell}(\ell)$ , it follows that  $|\lambda_\pi(\ell)| + |\lambda_\pi(\ell^2)| \geq 1$ . Hence  $\lambda'_{\text{ur}} \gg_\varepsilon \Lambda^{1-\varepsilon}$ .

Next, using the well-known relation

$$\kappa_m * \kappa_n^* = \sum_{t \mid \gcd(m,n)} \left( \prod_{p \mid t} \omega_{\pi_p}(t) \right) \left( \prod_{p \mid n} \omega_{\pi_p}^{-1}(n) \right) \kappa_{mn/t^2},$$

we see that

$$\kappa_{\text{ur}} = \sum_{1 \leq l \leq 16\Lambda^4} y_l \kappa_l$$

where the complex numbers  $y_l$  satisfy:

$$|y_l| \ll \begin{cases} \Lambda, & l = 1, \\ 1, & l = \ell_1 \text{ or } l = \ell_1 \ell_2 \text{ or } l = \ell_1 \ell_2^2 \text{ or } l = \ell_1^2 \ell_2^2 \text{ with } \ell_1, \ell_2 \in S, \\ 0, & \text{otherwise.} \end{cases}$$

We have  $|\kappa_l(\gamma)| \leq l^{-1/2}$ . Moreover  $\kappa_l(\gamma) = 0$  unless  $\gamma \in Z(\mathbb{Q}_p)G(\mathbb{Z}_p)a(\ell)G(\mathbb{Z}_p)$  for all  $p \nmid N$ . We deduce the following bound:

$$|\phi'(kn(x)a(y))|^2 \ll_\varepsilon \Lambda^{-2+\varepsilon} M_1 N_1 \sum_{1 \leq l \leq 16\Lambda^4} \frac{y_l}{\sqrt{l}} \sum_{\substack{\gamma \in Z(\mathbb{Q}) \setminus G(\mathbb{Q})^+, \\ \gamma \in Z(\mathbb{Q}_p)K_{0,p}(p) \forall p \mid N_2 \\ \gamma \in Z(\mathbb{Q}_p)G(\mathbb{Z}_p)a(\ell)G(\mathbb{Z}_p) \forall p \nmid N_2}} |\kappa_\infty(u(z, \gamma z))|. \tag{29}$$

Define

$$M(\ell, N_2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, a, b, c, d \in \mathbb{Z}, a > 0, N_2 \mid c, ad - bc = \ell \right\}.$$

The following lemma follows immediately from strong approximation.

**Lemma 3.19.** *Let  $\gamma \in G(\mathbb{Q})^+$  and  $\ell$  be a positive integer coprime to  $N_2$ . Suppose for each prime  $p$  that  $\gamma \in Z(\mathbb{Q}_p)G(\mathbb{Z}_p)a(\ell)G(\mathbb{Z}_p)$ . Suppose also for each prime  $p \mid N_2$  that  $\gamma \in Z(\mathbb{Q}_p)K_{0,p}(p)$ . Then there exists  $z \in Z(\mathbb{Q})$  such  $z\gamma \in M(\ell, N_2)$ .*

*Proof.* Omitted. □

Let us take another look at (29) in view of Lemma 3.19. The sum in (29) is over all matrices  $\gamma$  in  $Z(\mathbb{Q}) \backslash G(\mathbb{Q})^+$  such that  $\gamma \in Z(\mathbb{Q}_p)K_{0,p}(p)$  for  $p \mid N_2$  and  $\gamma \in Z(\mathbb{Q}_p)G(\mathbb{Z}_p)a(\ell)G(\mathbb{Z}_p)$  for  $p \nmid N_2$ . The latter condition can equally well be taken over all  $p$  as

$$Z(\mathbb{Q}_p)G(\mathbb{Z}_p)a(\ell)G(\mathbb{Z}_p) = Z(\mathbb{Q}_p)G(\mathbb{Z}_p)a(\ell)G(\mathbb{Z}_p) = Z(\mathbb{Q}_p)G(\mathbb{Z}_p)$$

if  $\ell$  and  $p$  are coprime, which is the case when  $p \mid N$ . Therefore Lemma 3.19, together with the fact that the natural map from  $M(\ell, N_2)$  to  $Z(\mathbb{Q}) \backslash G(\mathbb{Q})^+$  is an injection, implies that the sum in (29) can be replaced by a sum over the set  $M(\ell, N_2)$ . Hence, writing  $g = kh_N \in \mathcal{J}_N$  as before, we get

$$|\phi(gn(x)a(y))|^2 = |\phi'(kn(x)a(y))|^2 \ll_{\varepsilon} \Lambda^{-2+\varepsilon} M_1 N_1 \sum_{1 \leq l \leq 16\Lambda^4} \frac{y_l}{\sqrt{l}} \sum_{\gamma \in M(\ell, N_2)} |\kappa_{\infty}(u(z, \gamma z))|. \tag{30}$$

For any  $\delta > 0$ , we define

$$N(z, \ell, \delta, N_2) = |\{\gamma \in M(\ell, N_2) : u(z, \gamma z) \leq \delta\}|.$$

We have the following counting result due to Templier [2015, Proposition 6.1].

**Proposition 3.20.** *Let  $z = x + iy \in \mathcal{F}_{N_2}$ . For any  $0 < \delta < 1$  and positive integer  $\ell$  coprime to  $N_2$ , let the number  $N(z, \ell, \delta, N_2)$  be defined as above.*

*For  $\Lambda \geq 1$ , define*

$$A(z, \Lambda, \delta, N_2) = \sum_{1 \leq l \leq 16\Lambda^4} \frac{y_l}{\sqrt{l}} N(z, \ell, \delta, N_2).$$

*Then*

$$A(z, \Lambda, \delta, N_2) \ll_{\varepsilon} \Lambda^{\varepsilon} N_2^{\varepsilon} [\Lambda + \Lambda N_2^{1/2} \delta^{1/2} y + \Lambda^{5/2} \delta^{1/2} N_2^{-1/2} + \Lambda^{5/2} \delta^{1/2} y + \Lambda^4 \delta N_2^{-1}].$$

*Proof.* This is Proposition 6.1 of [Templier 2015]. □

Now (30) gives us

$$|\phi(gn(x)a(y))|^2 \ll_{\varepsilon} \Lambda^{-2+\varepsilon} M_1 N_1 \int_0^1 |\kappa_{\infty}(\delta)| dA(z, \Lambda, \delta, N_2). \tag{31}$$

Using Proposition 3.20 and the property  $|\kappa_{\infty}(\delta)| \leq \min(T, T^{1/2}/\delta^{1/4})$ , we immediately deduce Proposition 3.16 after a simple integration, as in [Templier 2015, Section 6.2].

### Acknowledgements

I would like to thank Edgar Assing, Simon Marshall, Paul Nelson, and Nicolas Templier for useful discussions and feedback.

**Note added in proof.** Recent work of the author with Yueke Hu suggests that (1) may not hold in general in the case of powerful levels. This is due to the failure of Conjecture 1 in certain cases, which we have recently discovered.

### References

- [Blomer and Holowinsky 2010] V. Blomer and R. Holowinsky, “Bounding sup-norms of cusp forms of large level”, *Invent. Math.* **179**:3 (2010), 645–681. MR Zbl
- [Harcos and Michel 2006] G. Harcos and P. Michel, “The subconvexity problem for Rankin–Selberg  $L$ -functions and equidistribution of Heegner points II”, *Invent. Math.* **163**:3 (2006), 581–655. MR Zbl
- [Harcos and Templier 2012] G. Harcos and N. Templier, “On the sup-norm of Maass cusp forms of large level: II”, *Int. Math. Res. Not.* **2012**:20 (2012), 4764–4774. MR Zbl
- [Harcos and Templier 2013] G. Harcos and N. Templier, “On the sup-norm of Maass cusp forms of large level III”, *Math. Ann.* **356**:1 (2013), 209–216. MR Zbl
- [Hoffstein and Lockhart 1994] J. Hoffstein and P. Lockhart, “Coefficients of Maass forms and the Siegel zero”, *Ann. of Math. (2)* **140**:1 (1994), 161–181. MR Zbl
- [Hu 2017] Y. Hu, “Triple product formula and mass equidistribution on modular curves of level  $N$ ”, *Int. Math. Res. Not.* (2017), art. id. rnw322.
- [Iwaniec and Sarnak 1995] H. Iwaniec and P. Sarnak, “ $L^\infty$  norms of eigenfunctions of arithmetic surfaces”, *Ann. of Math. (2)* **141**:2 (1995), 301–320. MR Zbl
- [Marshall 2016] S. Marshall, “Local bounds for  $L^p$  norms of Maass forms in the level aspect”, *Algebra Number Theory* **10**:4 (2016), 803–812. MR Zbl
- [Milićević 2016] D. Milićević, “Sub-Weyl subconvexity for Dirichlet  $L$ -functions to prime power moduli”, *Compos. Math.* **152**:4 (2016), 825–875. MR
- [Nelson 2011] P. D. Nelson, “Equidistribution of cusp forms in the level aspect”, *Duke Math. J.* **160**:3 (2011), 467–501. MR Zbl
- [Nelson et al. 2014] P. D. Nelson, A. Pitale, and A. Saha, “Bounds for Rankin–Selberg integrals and quantum unique ergodicity for powerful levels”, *J. Amer. Math. Soc.* **27**:1 (2014), 147–191. MR Zbl
- [Saha 2014] A. Saha, “On sup-norms of cusp forms of powerful level”, Preprint, 2014. arXiv
- [Saha 2016] A. Saha, “Large values of newforms on  $GL(2)$  with highly ramified central character”, *Int. Math. Res. Not.* **2016**:13 (2016), 4103–4131. MR
- [Templier 2010] N. Templier, “On the sup-norm of Maass cusp forms of large level”, *Selecta Math. (N.S.)* **16**:3 (2010), 501–531. MR Zbl
- [Templier 2014] N. Templier, “Large values of modular forms”, *Camb. J. Math.* **2**:1 (2014), 91–116. MR Zbl
- [Templier 2015] N. Templier, “Hybrid sup-norm bounds for Hecke–Maass cusp forms”, *J. Eur. Math. Soc. (JEMS)* **17**:8 (2015), 2069–2082. MR Zbl
- [Tunnell 1978] J. B. Tunnell, “On the local Langlands conjecture for  $GL(2)$ ”, *Invent. Math.* **46**:2 (1978), 179–200. MR Zbl

Communicated by Peter Sarnak

Received 2015-10-13    Revised 2016-10-25    Accepted 2016-12-16

abhishek.saha@bristol.ac.uk    *Department of Mathematics, University of Bristol, Bristol, BS81SN, United Kingdom*





# Collinear CM-points

Yuri Bilu, Florian Luca and David Masser

André's celebrated theorem of 1998 implies that each complex straight line  $Ax + By + C = 0$  (apart from obvious exceptions) contains at most finitely many points  $(j(\tau), j(\tau'))$ , where  $\tau, \tau' \in \mathbb{H}$  are algebraic of degree 2. We show that there are only a finite number of such lines which contain more than two such points. As there is a line through any two complex points, this is the best possible result.

1. Introduction	1047
2. Special varieties and the theorem of Pila	1050
3. Main lemma and proof of Theorem 1.1	1053
4. Roots of unity	1055
5. Singular moduli	1056
6. Rational matrices	1062
7. Level, twist, and $q$ -expansion of a $j$ -map	1064
8. Initializing the proof of the main lemma	1065
9. The case $m_2 = m_3$	1068
10. The case $m_2 > m_3$ and $n_2 > n_3$	1073
11. The case $m_2 > m_3$ and $n_2 = n_3$	1076
12. The case $m_2 > m_3$ and $n_3 > n_2$	1079
Acknowledgments	1085
References	1086

## 1. Introduction

André [1998] proved that a nonspecial irreducible plane curve in  $\mathbb{C}^2$  may have at most finitely many CM-points. Here a *plane curve* is a curve defined by an irreducible equation  $F(x, y) = 0$ , where  $F$  is a polynomial with complex coefficients, and a *CM-point* (called also a *special point*) in  $\mathbb{C}^2$  is a point whose coordinates are both singular moduli. Recall that a *singular modulus* is the invariant of an elliptic curve with complex multiplication; in other words, it is an algebraic number of the form  $j(\tau)$ , where  $j$  denotes the standard  $j$ -function on the upper half-plane  $\mathbb{H}$  and

*MSC2010:* primary 11G15; secondary 11G18.

*Keywords:* CM points, André–Oort.

$\tau \in \mathbb{H}$  is an algebraic number of degree 2. Thus, a CM-point is a point of the form  $(j(\tau), j(\tau'))$  with  $\tau, \tau' \in \mathbb{H}$  algebraic of degree 2.

*Special curves* are those of the following types:

- “vertical lines”  $x = j(\tau)$  and “horizontal lines”  $y = j(\tau)$ , where  $j(\tau)$  is a singular modulus, and
- *modular curves*  $Y_0(N)$ , realized as the plane curves  $\Phi_N(x, y) = 0$ , where  $\Phi_N$  is the modular polynomial of level  $N$ .

Recall that the polynomial  $\Phi_N(X, Y) \in \mathbb{C}[X, Y]$  is the  $X$ -monic  $\mathbb{C}$ -irreducible polynomial satisfying  $\Phi_N(j(z), j(Nz)) = 0$ . It is known that actually  $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ ; this and other properties of  $\Phi_N$  can be found, for instance, in [Cox 1989, Theorem 11.18].

Clearly, each special curve contains infinitely many CM-points, and André proved that special curves are characterized by this property.

André’s result was the first nontrivial contribution to the celebrated André–Oort conjecture on the special subvarieties of Shimura varieties; see [Pila 2011] and the references therein.

Several other proofs (some conditional on the GRH) of André’s theorem were suggested [Bilu et al. 2013; Breuer 2001; Edixhoven 1998; Kühne 2012; 2013; Pila 2009]. We specifically mention the argument of Pila [2009], based on an idea of Pila and Zannier [2008]. Pila [2011] extended it to higher dimensions, proving the André–Oort conjecture for subvarieties of  $\mathbb{C}^n$ . To state this result, one needs to introduce the notion of “special variety”; then Pila’s theorem asserts that an algebraic subvariety of  $\mathbb{C}^n$  has at most finitely many maximal special subvarieties. See Section 2 and Theorem 2.4 for the details.

Besides general results, some particular curves were considered. For instance, Kühne [2013, Theorem 5] proved that the straight line  $x + y = 1$  has no CM-points,<sup>1</sup> and a similar result for the hyperbola  $xy = 1$  was obtained in [Bilu et al. 2013]. The same conclusion was obtained in [Habegger et al. 2017] for the quartic curve

$$x^3y - 2x^2y^2 + xy^3 - 1728x^3 + 1216x^2y + 1216xy^2 - 1728y^3 + 3538944x^2 - 2752512xy + 3538944y^2 - 2415919104x - 2415919104y + 549755813888 = 0;$$

this is equivalent to the fact that there are no complex  $t \neq 0, 1, -1$  for which the two elliptic curves  $Y^2 = X(X - 1)(X - t)$  and  $Y^2 = X(X - 1)(X + t)$  both have complex multiplication.

One can ask about CM-points on general straight lines  $Ax + By + C = 0$ . One has to exclude from consideration the *special straight lines*:  $x = j(\tau)$ ,  $y = j(\tau)$  (where  $j(\tau)$  is a singular modulus) and  $x = y$ , the latter being nothing else than the modular

<sup>1</sup>The same result was independently obtained in an earlier version of [Bilu et al. 2013] but did not appear in the final version.

curve  $Y_0(1)$  (the modular polynomial  $\Phi_1$  is  $X - Y$ ). According to the theorem of André, these are the only straight lines containing infinitely many CM-points.

In [Allombert et al. 2015] all CM-points lying on nonspecial straight lines defined over  $\mathbb{Q}$  are listed. More generally, Kühne [2013, p. 5] remarks that, given a positive integer  $\nu$ , at most finitely many CM-points belong to the union of all nonspecial straight lines defined over a number field of degree  $\nu$ ; moreover, for a fixed  $\nu$  all these points can, in principle, be listed explicitly, though the implied calculation does not seem to be feasible.

Here we take a different point of view: instead of restricting the degree of field of definition, we study the (nonspecial) straight lines passing through at least three CM-points.

Such lines do exist [Allombert et al. 2015, Remark 5.3]: since

$$\det \begin{bmatrix} 1728 & -884736000 \\ 287496 & -147197952000 \end{bmatrix} = 0,$$

the three points  $(0, 0)$ ,  $(1728, 287496)$  and  $(-884736000, -147197952000)$  belong to the same straight line  $1331x = 8y$ , and just as well for the points  $(0, 0)$ ,  $(1728, -884736000)$  and  $(287496, -147197952000)$  on  $512000x = -y$ . Here

$$\begin{aligned} j\left(\frac{-1 + \sqrt{-3}}{2}\right) &= 0, & j(\sqrt{-1}) &= 1728, & j(2\sqrt{-1}) &= 287496, \\ j\left(\frac{-1 + \sqrt{-43}}{2}\right) &= -884736000, & j\left(\frac{-1 + \sqrt{-67}}{2}\right) &= -147197952000. \end{aligned}$$

Call an (unordered) triple  $\{P_1, P_2, P_3\}$  of CM-points *collinear* if  $P_1, P_2, P_3$  are pairwise distinct and belong to a nonspecial straight line.

In this paper we prove the following:

**Theorem 1.1.** *There exist at most finitely many collinear triples of CM-points.*

In particular, there exist at most finitely many nonspecial straight lines passing through three or more CM-points. This latter consequence looks formally weaker than Theorem 1.1, but in fact it is equivalent to it, due to the theorem of André.

**Remark 1.2.** The referee drew our attention to the phenomenon of *automatic uniformity*, discovered by Scanlon [2004]. Combining Theorem 4.2 from [Scanlon 2004] with Pila's Theorem 2.4 stated in the next section, one obtains the following "uniform" version of the theorem of André: there is a (noneffective) uniform upper bound  $c_d$  on the number of CM-points on an arbitrary nonspecial curve of geometric degree  $d$  (with an arbitrary field of definition). For every  $d$ , it is a widely open question what the optimal  $c_d$  actually is; moreover, even obtaining an effective upper bound for  $c_d$  seems to be quite difficult. It might be an easier question to ask for an

optimal bound  $c_d^*$  such that *all but finitely many* nonspecial curves of degree  $d$  contain at most  $c_d^*$  special points. In this language our Theorem 1.1 simply asserts that  $c_1^* = 2$ .

The idea of the proof of Theorem 1.1 is simple. Three points  $(x_i, y_i)$  lie on a line if and only if

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{vmatrix} = 0. \quad (1-1)$$

This defines a variety in  $\mathbb{C}^6$  to which we can apply Pila’s André–Oort result. This guarantees finiteness outside the special subvarieties of positive dimension. One easily detects “obvious” positive-dimensional special subvarieties: they correspond to the line being special in two dimensions or the three points not being distinct. The main difficulty is showing that there are no other positive-dimensional special subvarieties: this is the content of the “main lemma”, whose proof occupies the overwhelming part of the article. Along the way we have to solve some auxiliary problems not only of André–Oort type but also of “mixed type” involving roots of unity.

It could be mentioned that, while the main lemma is completely effective, Theorem 1.1 is not because its deduction from the main lemma relies on Pila’s Theorem 2.4, which is noneffective.

For analogous Diophantine assertions about lines proved also using “determinant varieties”, the reader can consult the articles of Evertse, Győry, Stewart and Tijdeman [Evertse et al. 1988] about  $S$ -units or of Schlickewei and Wirsing [1997] about heights. In these papers, one is actually in the multiplicative group  $\mathbb{G}_m^2$  and the appropriate special varieties are much easier to describe.

**Plan of the article.** In Section 2 we recall the general notion of special variety and state the already mentioned theorem of Pila, proving the André–Oort conjecture for subvarieties of  $\mathbb{C}^n$ .

In Section 3 we present the main lemma, which lists all maximal positive-dimensional special subvarieties of the “determinant variety” defined by (1-1), and we deduce Theorem 1.1 from the theorem of Pila and the main lemma.

In Sections 4, 5, 6 and 7 we obtain various auxiliary results used in the sequel. The proof of the main lemma occupies Sections 8 to 12. In Section 8 we collect some preliminary material and show how the proof of the main lemma splits into four cases. These cases are treated in Sections 9 to 12.

## 2. Special varieties and the theorem of Pila

We recall the definition of special varieties from [Pila 2011]. The referee pointed out that this is not the definition used in the standard formulation of the André–Oort

conjecture, and some work is required to show that the two are equivalent. However, this presents no issues for our purposes since the main result that we need, Pila's Theorem 2.4, proved in [Pila 2011], is stated therein in terms of this definition.

To begin, we define sets  $M$  in  $\mathbb{C}^m$  (where  $m \geq 1$ ) as follows. If  $m = 1$ , then  $M = \mathbb{C}$ , while if  $m \geq 2$ , then  $M$  is given by modular equations

$$\Phi_{N(i)}(x_1, x_i) = 0 \quad (i = 2, \dots, m). \tag{2-1}$$

More generally for  $\mathbb{C}^n$  (where  $n \geq 1$ ), one takes a partition  $n = l_0 + m_1 + \dots + m_d$  (where  $d \geq 0$ ) with  $l_0 \geq 0$  and with  $m_1 \geq 1, \dots, m_d \geq 1$  (when  $d \geq 1$ ) and defines sets  $K$  in  $\mathbb{C}^n = \mathbb{C}^{l_0} \times \mathbb{C}^{m_1} \times \dots \times \mathbb{C}^{m_d}$  as  $L_0 \times M_1 \times \dots \times M_d$ , where  $L_0$  (if  $l_0 \geq 1$ ) is a single point whose coordinates are singular moduli and  $M_1, \dots, M_d$  (if  $d \geq 1$ ) are as  $M$  above. Then any irreducible component  $\tilde{K}$  of  $K$ , which necessarily has the form

$$\tilde{K} = L_0 \times \tilde{M}_1 \times \dots \times \tilde{M}_d \tag{2-2}$$

with irreducible components  $\tilde{M}_1, \dots, \tilde{M}_d$  of  $M_1, \dots, M_d$ , is an example of a special variety in the sense of Pila; and one gets all examples by permuting the coordinates. The dimension is  $d$ .

When  $n = 2$  and  $d = 1$ , this agrees with the notion of special curve introduced in Section 1 because the polynomials  $\Phi_N$  are irreducible.

The following property of special varieties is certainly known, but we could not find a suitable reference.

**Proposition 2.1.** *Let  $0 \leq e \leq d \leq n$ . Then every special variety of dimension  $d$  contains a Zariski-dense union of special varieties of dimension  $e$ .*

*Proof.* If  $d = 0$ , there is nothing to prove. Otherwise, by induction, it suffices to treat the case  $e = d - 1$ , with the special variety (2-2).

If  $m_1 = 1$ , then  $\tilde{M}_1 = \mathbb{C}$  and for each singular modulus  $\xi$  the variety  $L_0 \times \{\xi\} \times \tilde{M}_2 \times \dots \times \tilde{M}_d$  is special of dimension  $d - 1$ . As there are infinitely many singular moduli, the union is Zariski-dense in  $\tilde{K}$ .

If  $m_1 \geq 2$  (call it  $m$ ), we note from (2-1) that  $x_1$  is nonconstant on  $\tilde{M}_1$ . Thus, the corresponding projection of  $\tilde{M}_1$  to  $\mathbb{C}$  is dominant. We can therefore find infinitely many singular moduli  $\xi_1$  for which some  $(\xi_1, \xi_2, \dots, \xi_m)$  lies in  $\tilde{M}_1$ . As  $\Phi_{N(i)}(\xi_1, \xi_i) = 0$  for  $i = 2, \dots, m$ , it is clear that  $\xi_2, \dots, \xi_m$  are also singular moduli, and now the corresponding

$$L_0 \times \{(\xi_1, \xi_2, \dots, \xi_m)\} \times \tilde{M}_2 \times \dots \times \tilde{M}_d$$

do the trick. □

Special points are exactly those of the form  $(\xi_1, \dots, \xi_n)$ , where each  $\xi_i$  is a singular modulus. To characterize the special curves in a similar way, it will be

convenient to use the language of “ $j$ -maps”. A map  $f : \mathbb{H} \rightarrow \mathbb{C}$  will be called a  $j$ -map if either  $f(z) = j(\gamma z)$  for some  $\gamma \in \text{GL}_2^+(\mathbb{Q})$  (a *nonconstant  $j$ -map*) or  $f(z) = j(\tau)$  with  $\tau \in \mathbb{H}$  algebraic of degree 2 (a *constant  $j$ -map*). Here  $\text{GL}_2^+(\mathbb{Q})$  is the subgroup of  $\text{GL}_2(\mathbb{Q})$  consisting of matrices with positive determinants. We define a  $j$ -set to be of the form  $\{(f_1(z), \dots, f_n(z)) : z \in \mathbb{H}\}$ , where each  $f_k$  is a  $j$ -map and at least one of them is nonconstant.

**Remark 2.2.** It is worth noting that every  $j$ -map is  $\Gamma(N)$ -automorphic<sup>2</sup> for some positive integer  $N$ . This is trivially true for constant  $j$ -maps, and a nonconstant  $j$ -map  $f = j \circ \gamma$  is  $\gamma^{-1}\Gamma(1)\gamma$ -automorphic. So it remains to note that  $\gamma^{-1}\Gamma(1)\gamma$  contains  $\Gamma(N)$  for a suitable  $N$ . Indeed, write  $A \in \Gamma(N)$  as  $I + NB$ , where  $I$  is the identity matrix and  $B$  is a matrix with entries in  $\mathbb{Z}$ . Then the matrix  $\gamma A \gamma^{-1} = I + N\gamma B \gamma^{-1}$  has entries in  $\mathbb{Z}$  if  $N$  is divisible by the product of the denominators of the entries of  $\gamma$  and  $\gamma^{-1}$ .

It seems to be known (and even used in several places) that every special curve is a  $j$ -set and that the converse is also true. As we could not find a convincing reference, we provide here an argument. We thank the referee for many explanations on this topic.

**Proposition 2.3.** (1) *Any  $j$ -set is a Zariski-closed irreducible algebraic subset of  $\mathbb{C}^n$ .*

(2) *A subset of  $\mathbb{C}^n$  is a  $j$ -set if and only if it is a special curve.*

*Proof.* In the proof of Part (1), we may restrict to the case when all  $f_1, \dots, f_n$  are nonconstant  $j$ -maps. Denote by  $Z \subset \mathbb{C}^n$  the  $j$ -set defined by these maps. According to Remark 2.2, the maps  $f_1, \dots, f_n$  are  $\Gamma(N)$ -automorphic for some positive integer  $N$ . Hence, each  $f_i$  induces a regular map, also denoted by  $f_i$ , of the affine modular curve  $Y(N) = \Gamma(N) \backslash \mathbb{H}$  to  $\mathbb{C}$ , and our  $Z$  is the image of the map  $(f_1, \dots, f_n) : Y(N) \rightarrow \mathbb{C}^n$ .

Furthermore, each  $f_i$  extends to a regular map  $\bar{f}_i : X(N) \rightarrow \mathbb{P}^1(\mathbb{C})$  of projective curves, where  $X(N)$  is the standard compactification of  $Y(N)$ , as explained, for instance, in [Diamond and Shurman 2005, §2.4]. The image  $\bar{Z}$  of the map  $(\bar{f}_1, \dots, \bar{f}_n) : X(N) \rightarrow \mathbb{P}^1(\mathbb{C})^n$  is Zariski-closed in  $\mathbb{P}^1(\mathbb{C})^n$  and irreducible (being the image of an irreducible projective curve under a regular map). But for  $x \in X(N)$ , we have  $\bar{f}_i(x) = \infty$  if and only if  $x \in X(N) \setminus Y(N)$  (we write  $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$  in the obvious sense). Hence,  $Z = \bar{Z} \cap \mathbb{C}^n$ , which shows that  $Z$  is Zariski-closed in  $\mathbb{C}^n$  and irreducible. This proves Part (1).

---

<sup>2</sup>Recall that  $\Gamma(N)$  is the kernel of the mod  $N$  reduction map  $\text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ , and “the function  $f$  is  $\Gamma(N)$ -automorphic” means  $f \circ \eta = f$  for any  $\eta \in \Gamma(N)$ .

Part (2) is an easy consequence of Part (1). If  $f$  and  $g$  are two nonconstant  $j$ -maps, then there exists  $N$  such that  $\Phi_N(f, g) = 0$ . It follows that, up to coordinate permutations, any  $j$ -set is contained in  $L_0 \times M$ , where  $L_0$  is a point whose coordinates are singular moduli and  $M \subseteq \mathbb{C}^m$  is defined as in (2-1). Since our  $j$ -set is irreducible and Zariski-closed, it must be an irreducible component of  $L_0 \times M$ , that is, a special curve. In particular, a  $j$ -set is an irreducible one-dimensional algebraic set defined over  $\overline{\mathbb{Q}}$ .

Conversely, every special curve has (up to coordinate permutations) the shape  $L_0 \times \tilde{M}$ , where  $\tilde{M}$  is an irreducible component of a set  $M \subseteq \mathbb{C}^m$  defined as in (2-1). Recall that two complex numbers  $x, y$  satisfy  $\Phi_N(x, y) = 0$  if and only if  $x$  and  $y$  are  $j$ -invariants of two elliptic curves linked by a cyclic  $N$ -isogeny. Now let  $(\xi_1, \dots, \xi_m)$  be a transcendental point<sup>3</sup> of  $\tilde{M}$ . Then the numbers  $\xi_1, \dots, \xi_m$  are  $j$ -invariants of isogenous elliptic curves. Hence, if we write  $\xi_1 = j(z)$  with some  $z \in \mathbb{H}$ , then there exist  $\gamma_2, \dots, \gamma_m \in \text{GL}_2^+(\mathbb{Q})$  such that  $\xi_i = j(\gamma_i z)$  for  $i = 2, \dots, m$ .

Thus,  $\tilde{M}$  shares a transcendental point with the  $j$ -set defined by the  $j$ -maps  $j, j \circ \gamma_2, \dots, j \circ \gamma_m$ . Since both are Zariski-closed irreducible one-dimensional algebraic sets defined over  $\overline{\mathbb{Q}}$ , they must coincide. □

A similar “parametric” description can be given for higher dimensional special varieties. We do not go into this because we will not need it.

Pila [2011] generalized the theorem of André by proving the following:

**Theorem 2.4** (Pila). *An algebraic set in  $\mathbb{C}^n$  contains at most finitely many maximal special subvarieties.*

“Maximal” is understood here in the set-theoretic sense: let  $V$  be an algebraic set in  $\mathbb{C}^n$  and  $M \subseteq V$  a special variety; we call  $M$  a *maximal special subvariety* of  $V$  if for any special variety  $M'$  such that  $M \subseteq M' \subseteq V$  we have  $M = M'$ .

If an algebraic curve is not special, then its only special subvarieties are special points, and we recover the theorem of André.

### 3. Main lemma and proof of Theorem 1.1

Theorem 1.1 is an easy consequence of Pila’s Theorem 2.4 and the following lemma.

**Lemma 3.1** (main lemma). *Let  $f_1, f_2, f_3, g_1, g_2, g_3$  be  $j$ -maps, not all constant. Assume that the determinant*

$$\det \begin{bmatrix} 1 & 1 & 1 \\ f_1 & f_2 & f_3 \\ g_1 & g_2 & g_3 \end{bmatrix} \tag{3-1}$$

*is identically 0. Then at least one of the following holds:*

---

<sup>3</sup>“Transcendental” means here that the coordinates of this point are not all algebraic over  $\mathbb{Q}$ .

- $f_1 = f_2 = f_3$ ,
- $g_1 = g_2 = g_3$ ,
- for some distinct  $k, \ell \in \{1, 2, 3\}$  we have  $f_k = f_\ell$  and  $g_k = g_\ell$ ,
- $f_k = g_k$  for  $k = 1, 2, 3$ .

In this section we prove Theorem 1.1 assuming the validity of the main lemma. Lemma 3.1 itself will be proved in the subsequent sections.

Consider the algebraic set in  $\mathbb{C}^6$  consisting of the points  $(x_1, x_2, x_3, y_1, y_2, y_3)$  satisfying

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{vmatrix} = 0. \tag{3-2}$$

Then Lemma 3.1 has the following consequence.

**Corollary 3.2.** *The algebraic set (3-2) has exactly six maximal special subvarieties of positive dimension:*

- the subvariety  $R_x$ , defined in  $\mathbb{C}^6$  by  $x_1 = x_2 = x_3$ ,
- the subvariety  $R_y$ , defined in  $\mathbb{C}^6$  by  $y_1 = y_2 = y_3$ ,
- the three subvarieties  $S_{k,\ell}$ , defined in  $\mathbb{C}^6$  by  $x_k = x_\ell$  and  $y_k = y_\ell$ , where  $k, \ell \in \{1, 2, 3\}$  are distinct, and
- the subvariety  $T$ , defined in  $\mathbb{C}^6$  by  $x_k = y_k$  for  $k = 1, 2, 3$ .

*Proof.* Let  $\tilde{K}$  be a special variety in (3-2) of positive dimension. By Proposition 2.1 it contains a Zariski-dense union of special curves. By Proposition 2.3 each such curve is a  $j$ -set. By the main lemma, each  $j$ -set is contained in one of the subvarieties above. The latter are clearly irreducible and also special; for example with  $R_x$  we have  $n = 6, d = 4$ , and the partition with

$$l_0 = 0, \quad m_1 = 3, \quad m_2 = m_3 = m_4 = 1.$$

Taking closures we see that  $\tilde{K}$  itself is also contained in one of them. □

Now we are ready to prove Theorem 1.1. Let

$$P_k = (x_k, y_k) \quad (k = 1, 2, 3)$$

be three special points forming a collinear triple. Then the point  $Q = (x_1, x_2, x_3, y_1, y_2, y_3)$  belongs to the algebraic set (3-2). Moreover, since our points are pairwise distinct,  $Q$  does not belong to any of  $S_{k,\ell}$ , and since the straight line passing through our points is not special,  $Q$  does not belong to any of  $R_x, R_y, T$ .

This shows that  $\{Q\}$  is a zero-dimensional maximal special subvariety of the algebraic set (3-2), and we complete the proof by applying Theorem 2.4. □



The main lemma will be proved in Sections 8–12, after some preparations made in Sections 4–7.

#### 4. Roots of unity

In this section we collect some facts about roots of unity used in the proof of the main lemma.

**Lemma 4.1.** *Let  $\alpha$  be a sum of  $k$  roots of unity and  $N$  a nonzero integer. Assume that  $N \mid \alpha$  (in the ring of algebraic integers). Then either  $\alpha = 0$  or  $k \geq |N|$ .*

*Proof.* Assume  $\alpha \neq 0$ , and write  $\alpha = N\beta$ , where  $\beta$  is a nonzero algebraic integer. Then there exists an embedding  $\mathbb{Q}(\alpha) \xrightarrow{\sigma} \mathbb{C}$  such that  $|\beta^\sigma| \geq 1$ . It follows that  $|N| \leq |\alpha^\sigma|$ . But since  $\alpha$  is a sum of  $k$  roots of unity, we have  $|\alpha^\sigma| \leq k$ .  $\square$

**Lemma 4.2.** *Let  $a, b$  be nonzero rational numbers and  $\eta, \theta$  roots of unity. Assume that  $\alpha = a\eta + b\theta$  is of degree 1 or 2 over  $\mathbb{Q}$ . Then  $\mathbb{Q}(\alpha)$  is one of the fields  $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5})$ , and after a possible swapping of  $a\eta$  and  $b\theta$ , and possible replacing of  $(a, \eta)$  by  $(-a, -\eta)$  and/or  $(b, \theta)$  by  $(-b, -\theta)$ , we have the following:*

- (1) If  $\mathbb{Q}(\alpha) = \mathbb{Q}$ , then
  - (a) either both  $\eta$  and  $\theta$  are  $\pm 1$  or
  - (b)  $\eta$  is a primitive cubic root of unity,  $\theta = \eta^{-1}$ , and  $a = b$ , or
  - (c)  $\theta = -\eta$  and  $a = b$ .
- (2) If  $\mathbb{Q}(\alpha) = \mathbb{Q}(i)$ , then
  - (a) either  $\eta = i$  and  $\theta \in \{1, i\}$  or
  - (b)  $\eta$  is a primitive 12th root of unity,  $\theta = -\eta^{-1}$ , and  $a = b$ .
- (3) If  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-3})$ , then  $\eta$  is a primitive cubic root of unity, and  $\theta$  is a cubic root of unity (primitive or not).
- (4) If  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-2})$ , then  $\eta$  is a primitive 8th root of unity,  $\theta = -\eta^{-1}$ , and  $a = b$ .
- (5) If  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$ , then  $\eta$  is a primitive 8th root of unity,  $\theta = \eta^{-1}$ , and  $a = b$ .
- (6) If  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3})$ , then  $\eta$  is a primitive 12th root of unity, and
  - (a) either  $\theta = \eta^{-1}$  and  $a = b$  or
  - (b)  $\theta = -\eta^3 (= \pm i)$  and  $a = 2b$ .
- (7) If  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$ , then  $\eta$  is a primitive 5th root of unity,  $\theta = \eta^{-1}$ , and  $a = b$ .

*Proof.* Without loss of generality, we may assume that  $a$  and  $b$  are coprime integers. Let  $N$  be the order of the multiplicative group generated by  $\eta$  and  $\theta$ , and  $L = \mathbb{Q}(\eta, \theta)$ ; then  $[L : \mathbb{Q}] = \varphi(N)$ , where  $\varphi$  is Euler's totient function.

If  $\varphi(N) \leq 2$ , then  $N \in \{1, 2, 3, 4, 6\}$ , and we have one of the options (1), (2a), or (3). If  $\alpha = 0$ , then we have option (1c).

From now on we assume that  $\varphi(N) > 2$  and  $\alpha \neq 0$ . Since  $\varphi(N) > 2$ , there exists  $\sigma \in \text{Gal}(L/\mathbb{Q})$  such that  $(\eta^\sigma, \theta^\sigma) \neq (\eta, \theta)$ , but  $\alpha^\sigma = \alpha$ . We obtain

$$a(\eta - \eta^\sigma) = b(\theta^\sigma - \theta). \tag{4-1}$$

By our choice of  $\sigma$ , both sides of (4-1) are nonzero. Since  $a$  and  $b$  are coprime integers, we have  $a \mid (\theta^\sigma - \theta)$ , whence  $|a| \leq 2$  by Lemma 4.1. Similarly,  $|b| \leq 2$ . It follows that  $(a, b) \in \{(\pm 1, \pm 1), (\pm 1, \pm 2), (\pm 2, \pm 1)\}$ . Swapping (if necessary)  $a\eta$  and  $b\theta$ , and replacing (if necessary)  $(a, \eta)$  by  $(-a, -\eta)$  and/or  $(b, \theta)$  by  $(-b, -\theta)$ , we may assume that  $a \in \{1, 2\}$  and  $b = 1$ . The rest of the proof splits into two cases.

The case  $a = 2$  and  $b = 1$ . In this case (4-1) becomes  $2(\eta - \eta^\sigma) = \theta^\sigma - \theta$ . We must have  $\theta^\sigma = -\theta$ ; otherwise all the conjugates of the nonzero algebraic integer  $(\theta^\sigma - \theta)/2$  would be of absolute value strictly smaller than 1. Thus, we obtain  $\eta - \eta^\sigma + \theta = 0$ . Three roots of unity may sum up to 0 only if they are proportional to  $(1, \zeta_3, \zeta_3^{-1})$ , where  $\zeta_3$  is a primitive cubic of unity. We obtain  $\theta/\eta = \zeta_3^{-1}$ , and  $\eta = \alpha(a + b\zeta_3^{-1})^{-1}$  is of degree at most 4 over  $\mathbb{Q}$ . Since  $\theta = \eta^\sigma - \eta \in \mathbb{Q}(\eta)$ , we obtain  $L = \mathbb{Q}(\eta)$ ; in particular,  $\eta$  is a primitive  $N$ -th root of unity.

Thus,  $\varphi(N) = [\mathbb{Q}(\eta) : \mathbb{Q}] \leq 4$ , and in fact  $\varphi(N) = 4$  because  $\varphi(N) > 2$ . Since  $-\eta^\sigma/\eta = \zeta_3$ , we must have  $3 \mid N$ . Together with  $\varphi(N) = 4$ , this implies that  $N = 12$  and  $\eta$  is a primitive 12th root of unity. Hence, we have the option (6b).

The case  $a = b = 1$ . In this case  $\eta - \eta^\sigma + \theta - \theta^\sigma = 0$ . Four roots of unity may sum up to 0 only if two of them sum up to 0 (and the other two sum up to 0 as well). Since  $\eta \neq \eta^\sigma$  and  $\eta \neq -\theta$  (because  $\alpha \neq 0$ ), we have  $\eta = \theta^\sigma$  and  $\eta^\sigma = \theta$ . This implies that  $L = \mathbb{Q}(\eta) = \mathbb{Q}(\theta)$ , both  $\eta$  and  $\theta$  are primitive  $N$ -th roots of unity, and  $\sigma^2 = 1$ .

We claim that the subgroup  $H = \{1, \sigma\}$  is the stabilizer of  $\mathbb{Q}(\alpha)$  in  $G = \text{Gal}(L/\mathbb{Q})$ . Thus, let  $\varsigma \in G$  satisfy  $\alpha^\varsigma = \alpha$ . Since  $\eta + \eta^\sigma - \eta^\varsigma - \eta^{\sigma\varsigma} = 0$  and  $\eta + \eta^\sigma \neq 0$ , we must have either  $\eta = \eta^\varsigma$  or  $\eta = \eta^{\sigma\varsigma}$ . Since  $L = \mathbb{Q}(\eta)$ , in the first case we have  $\varsigma = 1$  and in the second case  $\varsigma = \sigma^{-1} = \sigma$ .

Thus,  $H$  is the stabilizer of  $\mathbb{Q}(\alpha)$ . Since  $|H| = 2$  and  $[G : H] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ , we obtain  $\varphi(N) = |G| = 4$ , which implies that  $N \in \{5, 8, 10, 12\}$ .

Now if  $N = 5$ , then we have option (7). If  $N = 10$ , then replacing  $(a, \eta)$  by  $(-a, -\eta)$  and  $(b, \theta)$  by  $(-b, -\theta)$ , we obtain option (7) as well. If  $N = 8$ , then we have one of the options (4) or (5). Finally, if  $N = 12$ , then we have one of the options (2b) or (6a). □

### 5. Singular moduli

In this section we collect miscellaneous properties of singular moduli used in the sequel. We start by recalling the notion of the *discriminant* of a singular modulus. Let  $\tau \in \mathbb{H}$  be algebraic of degree 2; the endomorphism ring of the lattice  $\mathbb{Z}\tau + \mathbb{Z}$  is an

$\Delta$	-3	-4	-7	-8	-11	-12	-16	-19	-27
$j$	0	1728	-3375	8000	-32768	54000	287496	-884736	-12288000
$\Delta$	-28		-43		-67		-163		
$j$	16581375		-884736000		-147197952000		-262537412640768000		

**Table 1.** Discriminants  $\Delta$  with  $h(\Delta) = 1$  and the corresponding singular moduli.

order in the imaginary quadratic field  $\mathbb{Q}(\tau)$ ; the discriminant  $\Delta = \Delta_\tau$  of this order will be called the *discriminant* of the singular modulus  $j(\tau)$ . This discriminant is a negative integer satisfying  $\Delta \equiv 0, 1 \pmod 4$ .

It is well-known (see, for instance, [Cox 1989, §11]) that

- any singular modulus of discriminant  $\Delta$  is an algebraic integer of degree equal to the class number of  $\Delta$ , denoted  $h(\Delta)$ , and
- the singular moduli of discriminant  $\Delta$  are all conjugate over  $\mathbb{Q}$ ; moreover, they form a complete set of  $\mathbb{Q}$ -conjugates.

A full description of singular moduli of given discriminant  $\Delta$  is well-known as well. Denote by  $T = T_\Delta$  the set of triples of integers  $(a, b, c)$  such that

$$\gcd(a, b, c) = 1, \quad \Delta = b^2 - 4ac, \quad \text{either } -a < b \leq a < c \text{ or } 0 \leq b \leq a = c.$$

Then the map

$$(a, b, c) \mapsto j\left(\frac{b + \sqrt{\Delta}}{2a}\right) \tag{5-1}$$

defines a bijection from  $T_\Delta$  onto the set of singular moduli of discriminant  $\Delta$ . In particular,  $h(\Delta) = |T_\Delta|$ . The proof of this is a compilation of several classical facts, some of which go back to Gauss; see, for instance, [Bilu et al. 2016, §2.2] and the references therein.

It is crucial for us that the set  $T_\Delta$  has only one triple  $(a, b, c)$  with  $a = 1$ . The corresponding singular modulus will be called the *principal* singular modulus of discriminant  $\Delta$ . Note that the principal singular modulus is a real number; in particular,

$$\text{any singular modulus has a real } \mathbb{Q}\text{-conjugate.} \tag{5-2}$$

There exist exactly 13 discriminants  $\Delta$  with  $h(\Delta) = 1$ . The corresponding singular moduli (and only they) are rational integers. The full list of the 13 rational singular moduli is well-known and reproduced in Table 1.

Finally, we use the inequality

$$||j(\tau)| - e^{2\pi \operatorname{Im} \tau}| \leq 2079, \tag{5-3}$$

which holds for every  $\tau \in \mathbb{H}$  satisfying  $\text{Im } \tau \geq \sqrt{3}/2$  [Bilu et al. 2013, Lemma 1]. In particular, if  $(a, b, c) \in T_\Delta$ , then the number

$$\tau(a, b, c) = \frac{b + \sqrt{\Delta}}{2a}$$

satisfies  $\text{Im } \tau(a, b, c) \geq \sqrt{3}/2$  [Bilu et al. 2016, p. 403, (8)]. Hence, (5-3) applies with  $\tau = \tau(a, b, c)$ .

All the facts listed above will be repeatedly used in this section, sometimes without a special reference.

**Lemma 5.1.** *Let  $x$  be a singular modulus, and let  $x'$  be the principal singular modulus of the same discriminant. Then either  $x = x'$  or  $|x'| > |x| + 180000$ .*

*Proof.* Let  $\Delta$  be the common discriminant of  $x$  and  $x'$ . We may assume that  $|\Delta| \geq 15$ ; otherwise,  $h(\Delta) = 1$  and there is nothing to prove. We assume that  $x \neq x'$  and will use (5-3) to estimate  $|x|$  from above and  $|x'|$  from below.

We have  $x = j(\tau)$  and  $x' = j(\tau')$ , where  $\tau = \tau(a, b, c)$  and  $\tau' = \tau(a', b', c')$  for some  $(a, b, c), (a', b', c') \in T_\Delta$ . Since  $x'$  is principal, and  $x$  is not, we have  $a' = 1$  and  $a \geq 2$ . Hence,

$$\text{Im } \tau' = \pi |\Delta|^{1/2}, \quad \text{Im } \tau = \frac{\pi |\Delta|^{1/2}}{a} \leq \frac{\pi |\Delta|^{1/2}}{2}.$$

We obtain

$$|x'| \geq e^{\pi |\Delta|^{1/2}} - 2079, \quad |x| \leq e^{\pi |\Delta|^{1/2}/2} + 2079,$$

which implies

$$|x'| - |x| \geq e^{\pi |\Delta|^{1/2}} - e^{\pi |\Delta|^{1/2}/2} - 4158 \geq e^{\pi \sqrt{15}} - e^{\pi \sqrt{15}/2} - 4158 > 180000,$$

as wanted. □

**Lemma 5.2.** *Let  $x, y$  be singular moduli, and let  $a, b \in \mathbb{Z}$  be such that  $|a|, |b| \leq 90000$ . Assume that  $y \neq b$  and that  $(x - a)/(y - b)$  is a root of unity. Then either  $x = y$  or  $x, y \in \mathbb{Z}$ . In particular, if  $x/y$  is a root of unity (with  $y \neq 0$ ) or if  $(x - 744)/(y - 744)$  is a root of unity, then  $x = y$ .*

*Proof.* Let  $x'$  and  $y'$  be the principal singular moduli of the same discriminants as  $x$  and  $y$ . We may assume that  $|x'| \geq |y'|$ . We may further assume, by conjugating, that  $x = x'$ . Then  $y = y'$  as well since otherwise  $|y| < |y'| - 180000$  by Lemma 5.1, and we obtain

$$|y| + 90000 \geq |y - b| = |x - a| = |x' - a| \geq |x'| - 90000 \geq |y'| - 90000 > |y| + 90000,$$

a contradiction. Thus, both  $x$  and  $y$  are principal singular moduli. In particular, both are real, which implies  $x - a = \pm(y - b)$ .

Now Theorem 1.2 of [Allombert et al. 2015] implies one of the following options:

- (1)  $x = y$  and  $a = b$ ,
- (2)  $x, y \in \mathbb{Z}$ , or
- (3)  $x$  and  $y$  are distinct and of degree 2 over  $\mathbb{Q}$ .

We have to rule out option (3). Thus, assume that to be the case and let  $f(T) = T^2 + AT + C$  and  $g(T) = T^2 + BT + D$  be the  $\mathbb{Q}$ -minimal polynomials of  $x$  and  $y$ . Since  $x$  and  $y$  are both principal and distinct, they are not  $\mathbb{Q}$ -conjugate, which means that the polynomials  $F$  and  $G$  are distinct. We have either  $x + y = a + b$  or  $x - y = a - b$ . Taking  $\mathbb{Q}$ -traces, we obtain  $A + B = 2(a + b)$  or  $A - B = 2(a - b)$ . In particular, we have either  $|A + B| \leq 360000$  or  $|A - B| \leq 360000$ .

However, our  $F$  and  $G$  are among the 29 Hilbert class polynomials associated to the imaginary quadratic orders of class number 2. The full list of such polynomials can be found in Table 2 of [Bilu et al. 2016]. A quick inspection of this table shows that, if  $A$  and  $B$  are middle coefficients of two distinct polynomials from this table, then  $|A + B| > 360000$  and  $|A - B| > 360000$ . Hence, option (3) is impossible. This proves the first statement of the lemma.

In the special cases  $a = b = 0$  or  $a = b = 744$ , we must have either  $x = y$  or

$$x, y \in \mathbb{Z}, \quad x \neq y, \quad x + y \in \{0, 1488\}. \tag{5-4}$$

Inspecting Table 1, we find out that (5-4) is impossible. The lemma is proved.  $\square$

**Lemma 5.3.** *Let  $x$  and  $y$  be distinct principal singular moduli. Then  $||x| - |y|| > 1600$ .*

*Proof.* Denote by  $\Delta_x$  and  $\Delta_y$  the discriminants of  $x$  and  $y$ , respectively. We will assume that  $|\Delta_x| > |\Delta_y|$ . If  $|\Delta_x| \leq 12$ , then  $h(\Delta_x) = 1$ , and the statement follows by inspection of Table 1. And if  $|\Delta_x| \geq 15$ , then

$$\begin{aligned} |x| - |y| &\geq (e^{\pi|\Delta_x|^{1/2}} - 2079) - (e^{\pi|\Delta_y|^{1/2}} + 2079) \\ &\geq e^{\pi|\Delta_x|^{1/2}} - e^{\pi|\Delta_x-1|^{1/2}} - 4158 \\ &\geq e^{\pi\sqrt{15}} - e^{\pi\sqrt{14}} - 4158 \\ &> 60000, \end{aligned}$$

which is much stronger than needed. The lemma is proved.  $\square$

**Lemma 5.4.** *Let  $x$  be a singular modulus, and assume that the number field  $\mathbb{Q}(x)$  is a Galois extension of  $\mathbb{Q}$ . Then the Galois group of  $\mathbb{Q}(x)/\mathbb{Q}$  is 2-elementary, that is, isomorphic to  $(\mathbb{Z}/2\mathbb{Z})^k$  for some  $k$ .*

*Proof.* This is well-known; see, for instance, Corollary 3.3 from [Allombert et al. 2015].  $\square$

**Lemma 5.5.** *Let  $x, y$  be singular moduli and  $\varepsilon, \eta$  roots of unity. Then  $\varepsilon(x - 744) + \eta(y - 744)$  is not a root of unity.*

*Proof.* We will assume that

$$\varepsilon(x - 744) + \eta(y - 744) = 1$$

and derive a contradiction. We clearly have

$$||y| - |x|| \leq 1489. \tag{5-5}$$

We follow the same strategy as in the proof of Lemma 5.2. We denote by  $x'$  and  $y'$  the principal moduli of the same discriminants as  $x$  and  $y$ , respectively, and we may assume that  $|x'| \geq |y'|$  and  $x = x'$ . We claim that  $y = y'$  as well. Indeed, if  $y \neq y'$ , then Lemma 5.1 implies that

$$|y| + 1489 \geq |x| = |x'| \geq |y'| > |y| + 180000,$$

a contradiction.

Thus, we may assume that both  $x$  and  $y$  are principal singular moduli. Lemma 5.3 and inequality (5-5) imply that  $x = y$ . Thus,

$$(\varepsilon + \eta)(x - 744) = 1.$$

In particular  $0 \neq \varepsilon + \eta \in \mathbb{R}$ , which implies  $\eta = \varepsilon^{-1}$ .

Lemma 5.4 implies that the Galois group of the number field  $\mathbb{Q}(x) = \mathbb{Q}(\varepsilon + \varepsilon^{-1})$  is 2-elementary. Since  $\mathbb{Q}(\varepsilon + \varepsilon^{-1})$  is a subfield of degree at most 2 in  $\mathbb{Q}(\varepsilon)$ , the Galois group of  $\mathbb{Q}(\varepsilon)/\mathbb{Q}$  is either 2-elementary or  $\mathbb{Z}/4\mathbb{Z}$  times a 2-elementary group. But this group is  $(\mathbb{Z}/n\mathbb{Z})^\times$ , where  $n$  is the order of the root of unity  $\varepsilon$ . Using the well-known structure of the multiplicative group  $(\mathbb{Z}/n\mathbb{Z})^\times$  (see, for instance, [Ireland and Rosen 1990, Theorem 3 in §4.1]), one easily finds out that any integer  $n$  with the property “the group  $(\mathbb{Z}/n\mathbb{Z})^\times$  is either 2-elementary or  $\mathbb{Z}/4\mathbb{Z}$  times a 2-elementary group” divides either 48 or 120. It follows that  $|\varepsilon + \varepsilon^{-1}| \geq 2 \sin(\pi/60)$  (recall that  $\varepsilon + \varepsilon^{-1} = \varepsilon + \eta \neq 0$ ). Hence,

$$|x - 744| \leq \frac{1}{2 \sin(\pi/60)} < 10.$$

No principal singular modulus satisfies the latter inequality. □

**Lemma 5.6.** *The numbers 744,  $744 \pm 1$ ,  $744 \pm 2$ ,  $744 \pm 196884$ ,  $744 \pm 1 \pm 196884$ ,  $744 \pm 2 \cdot 196884$  are not singular moduli.*

*Proof.* The proof is just by inspection of Table 1. □

**Lemma 5.7.** *Let  $\theta$  be a root of unity. Then  $744 + \theta$  and  $744 + 196884\theta$  are not singular moduli.*

*Proof.* If  $744 + \theta$  or  $744 + 196884\theta$  is a singular modulus, then the cyclotomic field  $\mathbb{Q}(\theta)$  has a real embedding by (5-2), which is possible only if  $\theta = \pm 1$ . Now apply Lemma 5.6. □

**Lemma 5.8.** *Assume that a singular modulus of discriminant  $\Delta$  is a sum of  $k$  roots of unity. Then*

$$|\Delta| \leq \pi^{-2}(\log(k + 2079))^2.$$

*Proof.* We may assume that our modulus (denote it by  $x$ ) is principal and, as in the proof of Lemma 5.1, deduce from this that it satisfies  $|x| \geq e^{\pi|\Delta|^{1/2}} - 2079$ . On the other hand, since  $x$  is a sum of  $k$  roots of unity, we have  $|x| \leq k$ , whence the result.  $\square$

**Lemma 5.9.** *Let  $\eta, \theta$  be roots of unity,  $x$  a singular modulus, and  $a, b, c \in \mathbb{Z}$ . Assume that*

$$x = a\eta + b\theta + c, \quad a, b \neq 0, \quad |a| + |b| + |c| \leq 3400000.$$

*Then one of the following options holds:*

- We have  $x \in \mathbb{Z}$ .
- After possible replacing of  $(a, \eta)$  by  $(-a, -\eta)$  and/or  $(b, \theta)$  by  $(-b, -\theta)$ , we have the following:  $\eta$  is a primitive 5th root of unity,  $\theta = \eta^{-1}$ ,  $a = b$ , and

$$(a, c) \in \{(85995, -52515), (-85995, -138510), (565760, 914880), (-565760, 349120)\}. \quad (5-6)$$

*Proof.* Let  $\Delta$  be the discriminant of the singular modulus  $x$ . Lemma 5.8 implies that

$$|\Delta| \leq \pi^{-2}(\log(3400000 + 2079))^2 < 22.92. \quad (5-7)$$

Assume that  $x \notin \mathbb{Z}$ ; then  $h(\Delta) > 1$ . Among negative quadratic discriminants satisfying (5-7), all but two have class number 1; these two are  $\Delta = -15$  and  $\Delta = -20$ . In both cases  $h(\Delta) = 2$  and  $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{5})$ , so option (7) of Lemma 4.2 applies in both cases. After possible replacing of  $(a, \eta)$  by  $(-a, -\eta)$  and/or  $(b, \theta)$  by  $(-b, -\theta)$ , we obtain the following:  $\eta$  is a primitive 5th root of unity,  $\theta = \eta^{-1}$ , and  $a = b$ , so we have  $x = a(\eta + \eta^{-1}) + c$ .

The two singular moduli of discriminant  $\Delta = -15$  are

$$\begin{aligned} \frac{-191025 \pm 85995\sqrt{5}}{2} &= -\frac{191025}{2} \pm 85995\left(\frac{1}{2} + \eta + \eta^{-1}\right) \\ &= \begin{cases} \text{either} & 85995(\eta + \eta^{-1}) - 52515, \\ \text{or} & -85995(\eta + \eta^{-1}) - 138510, \end{cases} \end{aligned}$$

which gives us the first two options in (5-6)

Similarly, the two singular moduli of discriminant  $\Delta = -20$  are  $632000 \pm 282880\sqrt{5}$ , which gives the other two options.  $\square$

### 6. Rational matrices

In this section we obtain some elementary properties of  $\mathbb{Q}$ -matrices, which will be used in our study of  $j$ -maps in Section 7.

Recall that we denote by  $GL_2^+(\mathbb{Q})$  the subgroup of  $GL_2(\mathbb{Q})$  consisting of matrices of positive determinant. Unless the contrary is stated explicitly, in this section *matrix* refers to an element in  $GL_2^+(\mathbb{Q})$ . We call two matrices  $A$  and  $A'$  *equivalent* (denoted  $A \sim A'$ ) if there exists a matrix  $B \in SL_2(\mathbb{Z})$  and a scalar  $\lambda \in \mathbb{Q}^\times$  such that  $A' = \lambda BA$ .

For  $a, b \in \mathbb{Q}$  we define  $\gcd(a, b)$  as the nonnegative  $\delta \in \mathbb{Q}$  such that  $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$ . Given a matrix  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ , we define the *normalized left content* of  $A$  by

$$\text{nlc}(A) = \frac{\gcd(a, c)^2}{\det A}.$$

Clearly,  $\text{nlc}(A) = \text{nlc}(A')$  if  $A \sim A'$ .

**Proposition 6.1.** *Every matrix  $A$  is equivalent to an upper-triangular matrix of the form  $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$  with  $a > 0$ , where  $a = \text{nlc}(A)$ . We have  $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \sim \begin{bmatrix} a' & b' \\ 0 & 1 \end{bmatrix}$  if and only if  $a = a'$  and  $b \equiv b' \pmod{\mathbb{Z}}$ .*

*Proof.* It suffices to show that  $A$  is equivalent to an upper-triangular matrix; the rest is easy. Let  $\begin{pmatrix} x \\ y \end{pmatrix}$  be the left column of  $A$  and  $\delta = \gcd(x, y)$ . Then  $x/\delta, y/\delta \in \mathbb{Z}$ , and there exist  $u, v \in \mathbb{Z}$  such that  $ux + vy = \delta$ . Multiplying  $A$  on the left by the matrix  $\begin{bmatrix} u & v \\ -y/\delta & x/\delta \end{bmatrix} \in SL_2(\mathbb{Z})$ , we obtain an upper-triangular matrix. □

**Proposition 6.2.** *Let  $A_1, A_2$  be nonequivalent matrices. Then there exists a matrix  $B$  such that  $\text{nlc}(A_1B) \neq \text{nlc}(A_2B)$ .*

*Proof.* We may assume that  $\text{nlc}(A_1) = \text{nlc}(A_2)$  (otherwise there is nothing to prove). Multiplying on the right by  $A_1^{-1}$ , we may assume that  $A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ . We may further assume that  $A_2 = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ . Since  $a = \text{nlc}(A_2) = \text{nlc}(A_1) = 1$ , we have  $A_2 = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ , where  $b \notin \mathbb{Z}$  since  $A_2 \not\sim A_1$ .

Now  $B = \begin{bmatrix} 1 & 0 \\ -b^{-1} & 1 \end{bmatrix}$  would do. Indeed,

$$\text{nlc}(A_1B) = \text{nlc}(B) = \gcd(-b^{-1}, 1)^2, \quad \text{nlc}(A_2B) = \text{nlc} \begin{bmatrix} 0 & b \\ -b^{-1} & 1 \end{bmatrix} = b^{-2},$$

and we have to prove that  $\gcd(-b^{-1}, 1) \neq |b|^{-1}$ . This is equivalent to  $\gcd(1, b) \neq 1$ , which is true because  $b \notin \mathbb{Z}$ . □

One may wonder if the same statement holds true for more than two matrices: *given pairwise nonequivalent matrices  $A_1, \dots, A_n$ , does there exist a matrix  $B \in GL_2^+(\mathbb{Q})$  such that  $\text{nlc}(A_1B), \dots, \text{nlc}(A_nB)$  are pairwise distinct?* The proof of the main lemma could have been drastically simplified if it were the case. Unfortunately, the answer is “no” already for three matrices, as the following example shows.



**Example 6.3.** Let

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 1/2 \\ 0 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix}.$$

We claim that, for any matrix  $B$ , at least two of the numbers

$$\text{nlc}(A_1 B), \quad \text{nlc}(A_2 B), \quad \text{nlc}(A_3 B)$$

are equal. Indeed, write  $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ . After multiplying by a suitable scalar, we may assume that  $c = 2$ . Now

$$\text{nlc}(A_1 B) = \frac{\gcd(a, 2)^2}{\det B}, \quad \text{nlc}(A_2 B) = \frac{\gcd(a + 1, 2)^2}{\det B}, \quad \text{nlc}(A_3 B) = \frac{\gcd(4a, 2)^2}{4 \det B},$$

and we must show that among the three numbers

$$\gcd(a, 2), \quad \gcd(a + 1, 2), \quad \frac{1}{2} \gcd(4a, 2)$$

there are two equal. And this is indeed the case:

- if  $\text{ord}_2(a) > 0$ , then  $\gcd(a + 1, 2) = \frac{1}{2} \gcd(4a, 2)$ ,
- if  $\text{ord}_2(a) = 0$ , then  $\gcd(a, 2) = \frac{1}{2} \gcd(4a, 2)$ , and
- if  $\text{ord}_2(a) < 0$ , then  $\gcd(a, 2) = \gcd(a + 1, 2)$ .

Still, it is possible to prove something.

**Proposition 6.4.** *Let  $A_1, A_2, A_3$  be pairwise nonequivalent matrices. Then there exists a matrix  $B$  such that among the numbers  $\text{nlc}(A_1 B), \text{nlc}(A_2 B), \text{nlc}(A_3 B)$  one is strictly bigger than the two others.*

*Proof.* We may assume that  $A_k = \begin{bmatrix} a_k & * \\ 0 & 1 \end{bmatrix}$  for  $k = 1, 2, 3$ . If the numbers  $a_k$  are pairwise distinct, then there is nothing to prove. Hence, we may assume that  $a_1 = a_2$ . Multiplying on the right by  $A_3^{-1}$  and afterwards by a suitable diagonal matrix, we may assume that

$$A_1 = \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} a^{-1} & 0 \\ 0 & 1 \end{bmatrix},$$

where  $a > 0$ . Since  $A_1 \approx A_2$ , we have  $b_1 \not\equiv b_2 \pmod{\mathbb{Z}}$ , and we may assume  $b_1 \notin \mathbb{Z}$ .

Set  $B = \begin{bmatrix} 1 & 0 \\ -b_1^{-1} & 1 \end{bmatrix}$ . Then

$$\begin{aligned} \text{nlc}(A_1 B) &= b_1^{-2}, \\ \text{nlc}(A_2 B) &= \gcd(1 - b_1^{-1} b_2, b_1^{-1})^2, \\ \text{nlc}(A_3 B) &= a \gcd(a^{-1}, b_1^{-1})^2. \end{aligned} \tag{6-1}$$

Multiplying numbers (6-1) by  $ab_1^2$ , we must show that among the three numbers

$$a, \quad a \gcd(b_1 - b_2, 1)^2, \quad \gcd(b_1, a)^2 \tag{6-2}$$

one is strictly bigger than the others.

If the numbers in (6-2) are pairwise distinct, then there is nothing to prove. Now assume that two of them are equal. Since  $b_1 \not\equiv b_2 \pmod{\mathbb{Z}}$ , then  $\gcd(b_1 - b_2, 1) < 1$ , and in particular, the first two of them are distinct.

Further, the equality  $a = \gcd(b_1, a)^2$  is not possible either. Indeed, in this case for any prime number  $p$  we would have

$$\text{ord}_p(a) = 2 \min\{\text{ord}_p(a), \text{ord}_p(b_1)\},$$

which implies that either  $\text{ord}_p(a) = 2 \text{ord}_p(b_1) > 0$  or  $\text{ord}_p(b_1) \geq \text{ord}_p(a) = 0$ . In particular,  $\text{ord}_p(b_1) \geq 0$  for any  $p$ , contradicting our assumption  $b_1 \notin \mathbb{Z}$ .

Thus, the only possibility is  $a \gcd(b_1 - b_2, 1)^2 = \gcd(b_1, a)^2$ , and we obtain

$$a > a \gcd(b_1 - b_2, 1)^2 = \gcd(b_1, a)^2. \quad \square$$

### 7. Level, twist, and $q$ -expansion of a $j$ -map

In this section we collect some properties of  $j$ -maps used in the sequel.

Given  $\gamma, \gamma' \in \text{GL}_2^+(\mathbb{Q})$ , we have  $j(\gamma z) = j(\gamma' z)$  if and only if the matrices  $\gamma$  and  $\gamma'$  are *equivalent* in the sense of Section 6. Combined with Proposition 6.1, this gives the following:

**Proposition 7.1.** *Let  $f$  be a nonconstant  $j$ -map. Then there exist a unique positive number  $m \in \mathbb{Q}$  and a unique modulo 1 number  $\mu \in \mathbb{Q}$  such that  $f(z) = j(mz + \mu)$ .*

Note that  $m = \text{nlc}(\gamma)$  for any  $\gamma \in \text{GL}_2^+(\mathbb{Q})$  such that  $f(z) = j(\gamma z)$ .

Setting  $q = e^{2\pi iz}$  and  $\varepsilon = e^{2\pi i\mu}$ , the map  $f(z) = j(mz + \mu)$  admits the “ $q$ -expansion”

$$f(z) = \varepsilon^{-1} q^{-m} + 744 + 196884\varepsilon q^m + 21493760\varepsilon^2 q^{2m} + o(q^{2m}), \tag{7-1}$$

where here and below we accept the following convention:

- $O(q^\ell)$  means “terms of  $q$ -degree  $\ell$  or higher” and
- $o(q^\ell)$  means “terms of  $q$ -degree strictly higher than  $\ell$ ”.

We call  $m$  and  $\varepsilon$  the *level* and the *twist* of the nonconstant  $j$ -map  $f$ . For a constant  $j$ -map, we set its level to be 0 and its twist undefined. The following property will be routinely used, usually without special reference:

two nonconstant  $j$ -maps coincide if and only if their levels and twists coincide. (7-2)

We will denote in the sequel  $A = 196884$  and  $B = 21493760$  so that (7-1) reads

$$f(z) = \varepsilon^{-1}q^{-m} + 744 + A\varepsilon q^m + B\varepsilon^2 q^{2m} + O(q^{2m}). \tag{7-3}$$

The following lemma will play an important role in Section 8.

**Lemma 7.2.** *Let  $f_1, f_2, f_3$  be pairwise distinct  $j$ -maps, not all constant. Then there exists  $\gamma \in \text{GL}_2^+(\mathbb{Q})$  such that one of the maps  $f_1 \circ \gamma, f_2 \circ \gamma, f_3 \circ \gamma$  has level strictly bigger than the two others.*

*Proof.* If only one of the maps  $f_k$  is nonconstant, then there is nothing to prove. If exactly two of them, say  $f_1$  and  $f_2$ , are nonconstant, then Proposition 6.2 implies the existence of  $\gamma \in \text{GL}_2^+(\mathbb{Q})$  such that  $f_1 \circ \gamma$  and  $f_2 \circ \gamma$  have distinct levels, and we are done. Finally, if all the three are nonconstant, the result follows from Proposition 6.4. □

We conclude this section with a linear-independence property of nonconstant  $j$ -maps.

**Lemma 7.3.** *Let  $f, g$  be nonconstant  $j$ -maps satisfying a nontrivial linear relation  $af + bg + c = 0$ , where  $(a, b, c) \in \mathbb{C}^3$  and  $(a, b, c) \neq (0, 0, 0)$ . Then  $f = g$  and  $a + b = c = 0$ .*

*Proof.* Any two nonconstant  $j$ -maps parametrize the modular curve  $Y_0(N)$  of a certain level  $N$ ; in other words, we have  $\Phi_N(f, g) = 0$ , where  $\Phi_N(x, y)$  is the  $N$ -th modular polynomial. If we also have  $af + bg + c = 0$ , then the polynomial  $\Phi_N(x, y)$ , being irreducible, must divide the linear polynomial  $ax + by + c$ . It follows that  $N = 1$  since  $\Phi_1(x, y) = x - y$  is the only modular polynomial of degree 1. □

### 8. Initializing the proof of the main lemma

In this section we start the proof of the main lemma. Thus, from now on, let  $f_1, f_2, f_3, g_1, g_2, g_3$  be  $j$ -maps, not all constant and satisfying

$$\begin{vmatrix} 1 & 1 & 1 \\ f_1 & f_2 & f_3 \\ g_1 & g_2 & g_3 \end{vmatrix} = 0. \tag{8-1}$$

This can be rewritten as

$$(f_1 - f_2)(g_2 - g_3) = (f_2 - f_3)(g_1 - g_2). \tag{8-2}$$

If say  $f_1 = f_2$ , then we find from (8-2) that either  $f_2 = f_3$ , in which case  $f_1 = f_2 = f_3$ , or  $g_1 = g_2$ , in which case  $f_1 = f_2$  and  $g_1 = g_2$ . Hence, we may assume in the sequel that

$$f_1, f_2, f_3 \text{ are pairwise distinct, and so are } g_1, g_2, g_3. \tag{8-3}$$

We will show that under this assumption

$$f_k = g_k \quad (k = 1, 2, 3). \tag{8-4}$$

Let  $m_k, n_k$  be the levels of  $f_k, g_k$ , respectively, for  $k = 1, 2, 3$ . If  $f_k$  and/or  $g_k$  is not constant, we denote the corresponding twists by  $\varepsilon_k = e^{2\pi i \mu_k}$  and/or  $\eta_k = e^{2\pi i \nu_k}$ , respectively.

**8A. Some relations for the levels.** Since not all of our six maps are constant, we may assume that the three maps  $f_k$  are not all constant. Lemma 7.2 implies now that, after a suitable variable change, one of the numbers  $m_1, m_2, m_3$  is strictly bigger than the others. After renumbering, we may assume that

$$m_1 > m_2, m_3.$$

We claim that

$$n_1 > n_2, n_3 \tag{8-5}$$

as well, and moreover,

$$m_1 - \max\{m_2, m_3\} = n_1 - \max\{n_2, n_3\}. \tag{8-6}$$

Indeed, assume that, say,  $n_2 \geq n_1, n_3$ . Then the leading terms of the  $q$ -expansion on the left and on the right of (8-2) are of the forms  $cq^{-(m_1+n_2)}$  and  $c'q^{-(\max\{m_2, m_3\}+n_2)}$  with some nonzero  $c$  and  $c'$ . (Precisely,

$$c = \begin{cases} \varepsilon_1^{-1} \eta_2^{-1}, & n_2 > n_3, \\ \varepsilon_1^{-1} (\eta_2^{-1} - \eta_3^{-1}), & n_2 = n_3 > 0, \\ \varepsilon_1^{-1} (g_2 - g_3), & n_2 = n_3 = 0, \end{cases}$$

and it follows from (8-3) that  $c \neq 0$ ; in a similar way one shows that  $c' \neq 0$ .) And this is impossible because  $m_1 + n_2 > \max\{m_2, m_3\} + n_2$ . This proves that  $n_1 > n_2, n_3$ . In particular the three maps  $g_k$  are also not all constant. Again comparing the leading terms of the  $q$ -expansion on the left and on the right of (8-2), we obtain (8-6).

Swapping, if necessary, the functions  $f_k$  and  $g_k$ , we may assume that

$$m_1 \geq n_1, \tag{8-7}$$

and after renumbering, we may assume that

$$m_1 > m_2 \geq m_3. \tag{8-8}$$

Equation (8-6) now becomes

$$m_1 - m_2 = n_1 - \max\{n_2, n_3\}. \tag{8-9}$$

**8B. One more lemma.** Here is a less obvious property, which will be used in the proof several times.

**Lemma 8.1.** *In the above setup we cannot simultaneously have  $f_2 = g_3$  and  $g_2 = f_3$ .*

*Proof.* If  $f_2 = g_3$  and  $g_2 = f_3$ , then

$$0 = \begin{vmatrix} 1 & 1 & 1 \\ f_1 & f_2 & f_3 \\ g_1 & f_3 & f_2 \end{vmatrix} = (f_3 - f_2)(f_1 + g_1 - f_2 - f_3).$$

Since  $f_2 \neq f_3$ , this implies

$$f_1 + g_1 = f_2 + f_3. \tag{8-10}$$

We will see that this leads to a contradiction.

Observe first of all that  $m_2 > 0$ . Indeed, if  $m_2 = 0$ , then  $m_3 = 0$  as well by (8-8). Hence, both  $f_2$  and  $f_3$  are constant, and (8-10) contradicts Lemma 7.3.

Next, we have  $m_3 > 0$  as well. Indeed, if  $f_3$  is constant, then comparing the constant terms in (8-10), we find  $f_3 = 744$ , contradicting Lemma 5.6.

Thus, we have  $m_1 \geq n_1 > n_3 = m_2 \geq m_3 > 0$ . Comparing the  $q$ -expansions

$$f_1 + g_1 = \begin{cases} \varepsilon_1^{-1}q^{-m_1} + \eta_1^{-1}q^{-n_1} + O(1), & m_1 > n_1, \\ (\varepsilon_1^{-1} + \eta_1^{-1})q^{-m_1} + O(1), & m_1 = n_1, \varepsilon_1 \neq -\eta_1, \\ 1488 + 2B\varepsilon_1^2q^{2m_1} + o(q^{2m_1}), & m_1 = n_1, \varepsilon_1 = -\eta_1, \end{cases}$$

$$f_2 + f_3 = \begin{cases} \varepsilon_2^{-1}q^{-m_2} + \varepsilon_3^{-1}q^{-m_3} + O(1), & m_2 > m_3, \\ (\varepsilon_2^{-1} + \varepsilon_3^{-1})q^{-m_2} + O(1), & m_2 = m_3, \varepsilon_2 \neq -\varepsilon_3, \\ 1488 + 2B\varepsilon_2^2q^{2m_2} + o(q^{2m_2}), & m_2 = m_3, \varepsilon_2 = -\varepsilon_3, \end{cases}$$

we immediately derive a contradiction. □

**8C. The determinant  $\mathcal{D}(q)$ .** We will study in the sequel a slightly modified version of the determinant from (8-1):

$$\mathcal{D}(q) = \begin{vmatrix} 1 & 1 & 1 \\ q^{m_1} f_1 & q^{m_1} f_2 & q^{m_1} f_3 \\ q^{n_1} g_1 & q^{n_1} g_2 & q^{n_1} g_3 \end{vmatrix}.$$

The advantage is that it has no negative powers of  $q$ . Equation (8-1) simply means that  $\mathcal{D}(q)$  vanishes as a formal power series in  $q$ . It will be useful to write

$$\mathcal{D}(q) = \begin{vmatrix} 1 & 1 & 1 \\ q^{m_1}(f_1 - 744) & q^{m_1}(f_2 - 744) & q^{m_1}(f_3 - 744) \\ q^{n_1}(g_1 - 744) & q^{n_1}(g_2 - 744) & q^{n_1}(g_3 - 744) \end{vmatrix}. \tag{8-11}$$

This would allow us to eliminate the constant terms in the  $q$ -expansions of  $f_k$  and  $g_k$ .

It will be convenient to use the notation

$$\tilde{f}_k = \begin{cases} \varepsilon_k^{-1}, & m_k > 0, \\ f_k - 744, & m_k = 0, \end{cases} \quad \tilde{g}_k = \begin{cases} \eta_k^{-1}, & n_k > 0, \\ g_k - 744, & n_k = 0 \end{cases} \quad (8-12)$$

so that

$$q^{m_1}(f_k - 744) = \tilde{f}_k q^{m_1 - m_k} + o(q^{m_1}), \quad q^{n_1}(g_k - 744) = \tilde{g}_k q^{n_1 - n_k} + o(q^{n_1}).$$

Lemma 5.6 implies that

$$\tilde{f}_k, \tilde{g}_k \neq 0 \quad (k = 1, 2, 3), \quad (8-13)$$

which will be frequently used, usually without special references.

**8D. The four cases.** According to (8-5) and (8-8), there are four possible cases:

$$\begin{aligned} m_2 &= m_3, \\ m_2 &> m_3, \quad n_2 > n_3, \\ m_2 &> m_3, \quad n_2 &= n_3, \\ m_2 &> m_3, \quad n_3 > n_2. \end{aligned}$$

They are treated in the four subsequent sections, respectively. We will show that in the first two cases we have (8-4) and that the last two cases are impossible. The proofs in the four cases are similar in strategy but differ in technical details.

Most of our arguments are nothing more than careful manipulations with  $q$ -expansions. Still, they are quite technical, and to facilitate reading, we split proofs of each of the cases it into short logically complete steps.

### 9. The case $m_2 = m_3$

In this section we assume that

$$m_1 > m_2 = m_3.$$

We want to prove that in this case we have  $f_k = g_k$  for  $k = 1, 2, 3$ .

Let us briefly describe the strategy of the proof. We already have (8-5), and after renumbering we may assume that

$$n_1 > n_2 \geq n_3.$$

Equation (8-9) now becomes

$$m_1 - m_2 = m_1 - m_3 = n_1 - n_2. \quad (9-1)$$

We start by proving that  $n_2 = n_3$ ; see Section 9A. With this done, setting  $m_2 = m_3 = m$  and  $n_2 = n_3 = n$ , we rewrite (9-1) as

$$m_1 - m = n_1 - n. \tag{9-2}$$

The next step is proving (see Section 9B) that  $m_1 = n_1$ . In view of (9-2) this would imply that  $m = n$  as well. In particular,  $f_k$  and  $g_k$  are of the same level for every  $k = 1, 2, 3$ . After this, we will be ready to prove that  $f_k = g_k$  for  $k = 1, 2, 3$ ; see Section 9C.

**9A. Proof of  $n_2 = n_3$ .** In this subsection we prove that  $n_2 = n_3$ . Set

$$m_1 - m_2 = m_1 - m_3 = n_1 - n_2 = \lambda, \quad n_1 - n_3 = \lambda' \geq \lambda.$$

We want to show that  $\lambda' = \lambda$ .

Assume that  $\lambda' > \lambda$ . Then by (8-7) all the  $m_k$  and  $n_k$  except perhaps  $n_3$  are positive. We consider separately the cases  $n_3 = 0$  and  $n_3 > 0$ .

*The subcase  $n_3 = 0$ .* If  $n_3 = 0$ , then using notation (8-12), we write  $\tilde{g}_3 = g_3 - 744$  and

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^\lambda \\ \eta_1^{-1} & \eta_2^{-1}q^\lambda & \tilde{g}_3q^{\lambda'} \end{vmatrix} + o(q^{n_1}) \\ &= (\varepsilon_1^{-1}\eta_2^{-1} - \varepsilon_2^{-1}\eta_1^{-1} + \varepsilon_3^{-1}\eta_1^{-1})q^\lambda + \varepsilon_3^{-1}\eta_2^{-1}q^{2\lambda} + \varepsilon_1^{-1}\tilde{g}_3q^{\lambda'} + o(q^{n_1}) + O(q^{\lambda+\lambda'}). \end{aligned}$$

The term with  $q^{\lambda'}$  can be eliminated only if  $\lambda' = 2\lambda$  and  $\varepsilon_1^{-1}\tilde{g}_3 = \varepsilon_3^{-1}\eta_2^{-1}$ , that is,  $g_3 = 744 + \varepsilon_1\varepsilon_3^{-1}\eta_2^{-1}$ , contradicting Lemma 5.7.

*The subcase  $n_3 > 0$ .* If  $n_3 > 0$ , then

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^\lambda \\ \eta_1^{-1} & \eta_2^{-1}q^\lambda & \eta_3^{-1}q^{\lambda'} + A\eta_3q^{n_1+n_3} \end{vmatrix} + o(q^{n_1+n_3}) \\ &= (\varepsilon_1^{-1}\eta_2^{-1} - \varepsilon_2^{-1}\eta_1^{-1} + \varepsilon_3^{-1}\eta_1^{-1})q^\lambda - \varepsilon_3^{-1}\eta_2^{-1}q^{2\lambda} - \varepsilon_1^{-1}\eta_3^{-1}q^{\lambda'} \\ &\quad + \varepsilon_2^{-1}\eta_3^{-1}q^{\lambda+\lambda'} - A\varepsilon_1^{-1}\eta_3q^{n_1+n_3} + o(q^{n_1+n_3}). \end{aligned}$$

As  $n_1 + n_3 > \lambda'$ , the term with  $q^{n_1+n_3}$  can be eliminated only if either

$$\lambda < \lambda' < 2\lambda = n_1 + n_3 < \lambda + \lambda', \quad \varepsilon_3^{-1}\eta_2^{-1} = -A\varepsilon_1^{-1}\eta_3,$$

which is impossible because  $A$  is not a root of unity, or

$$\lambda < \lambda', 2\lambda < n_1 + n_3 = \lambda + \lambda', \quad \varepsilon_2^{-1}\eta_3^{-1} = A\varepsilon_1^{-1}\eta_3,$$

which is again impossible by the same reason.

*Conclusion.* Thus, we have proved that  $n_2 = n_3$ . Setting  $m = m_2 = m_3$  and  $n = n_2 = n_3$ , we can summarize our knowledge as

$$\begin{aligned} m_1 > m_2 = m_3 = m, & \quad m_1 - m = n_1 - n = \lambda > 0, \\ n_1 > n_2 = n_3 = n, & \quad m_1 - n_1 = m - n \geq 0. \end{aligned}$$

Together with (8-3) this implies that

$$\tilde{f}_2 \neq \tilde{f}_3, \quad \tilde{g}_2 \neq \tilde{g}_3. \tag{9-3}$$

**9B. Proof of  $m_1 = n_1$ .** Now we want to prove that

$$m_1 = n_1. \tag{9-4}$$

Thus, assume that  $m_1 > n_1$ , in which case we also have  $m > n$ . We consider separately the subcases  $n > 0$  and  $n = 0$ .

*The subcase  $n > 0$ .* If  $n > 0$ , then

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1} q^\lambda & \varepsilon_3^{-1} q^\lambda \\ \eta_1^{-1} & \eta_2^{-1} q^\lambda + A\eta_2 q^{n_1+n} & \eta_3^{-1} q^\lambda + A\eta_3 q^{n_1+n} \end{vmatrix} + o(q^{n_1+n}) \\ &= \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2^{-1} - \varepsilon_3^{-1} \\ \eta_1^{-1} & \eta_2^{-1} - \eta_3^{-1} \end{vmatrix} q^\lambda + \begin{vmatrix} \varepsilon_2^{-1} & \varepsilon_3^{-1} \\ \eta_2^{-1} & \eta_3^{-1} \end{vmatrix} q^{2\lambda} + A\varepsilon_1^{-1}(\eta_2 - \eta_3)q^{n_1+n} + o(q^{n_1+n}) + o(q^{2\lambda}). \end{aligned}$$

Here the coefficient of  $q^\lambda$  must vanish. If  $2\lambda > n_1 + n$ , then that of  $q^{n_1+n}$  must vanish too, but that would contradict (9-3). If  $2\lambda < n_1 + n$ , then the coefficient of  $q^{2\lambda}$  must vanish and then that of  $q^{n_1+n}$ . It follows that  $2\lambda = n_1 + n$  and

$$\begin{vmatrix} \varepsilon_2^{-1} & \varepsilon_3^{-1} \\ \eta_2^{-1} & \eta_3^{-1} \end{vmatrix} = A\varepsilon_1^{-1}(\eta_3 - \eta_2). \tag{9-5}$$

As noted, both sides of (9-5) are nonzero. Since the left-hand side is a sum of two roots of unity, Lemma 4.1 implies that  $196884 = |A| \leq 2$ , a contradiction. This completes the proof of (9-4) in the case  $n > 0$ .

*The subcase  $n = 0$ .* If  $n = 0$ , then  $g_2$  and  $g_3$  are distinct constants, and the other functions are nonconstant. Also, we have  $\lambda = n_1$ , and so

$$m_1 = m + n_1. \tag{9-6}$$



Now, using notation (8-12), we obtain

$$\begin{aligned} \mathcal{D}(q) &= \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^{n_1} + A\varepsilon_2q^{m_1+m} & \varepsilon_3^{-1}q^{n_1} + A\varepsilon_3q^{m_1+m} \\ \eta_1^{-1} + A\eta_1q^{2n_1} & \tilde{g}_2q^{n_1} & \tilde{g}_3q^{n_1} \end{array} \right| \\ &\quad + o(q^{m_1+m}) + o(q^{2n_1}) \\ &= \left| \begin{array}{cc} \varepsilon_1^{-1} & \varepsilon_2^{-1} - \varepsilon_3^{-1} \\ \eta_1^{-1} & \tilde{g}_2 - \tilde{g}_3 \end{array} \right| q^{n_1} + \left| \begin{array}{cc} \varepsilon_2^{-1} & \varepsilon_3^{-1} \\ \tilde{g}_2 & \tilde{g}_3 \end{array} \right| q^{2n_1} + A\eta_1^{-1}(\varepsilon_3 - \varepsilon_2)q^{m_1+m} \\ &\quad + o(q^{m_1+m}) + o(q^{2n_1}). \end{aligned}$$

As  $\varepsilon_3 \neq \varepsilon_2$ , the coefficient of  $q^{m_1+m}$  is nonzero; by Lemma 5.2 so is the coefficient of  $q^{2n_1}$ . This shows that  $2n_1 = m_1 + m$ . Together with (9-6) this implies  $m_1 = 3m$  and  $n_1 = 2m$ ; rescaling  $z$ , we may assume

$$m = 1, \quad n_1 = 2, \quad m_1 = 3.$$

Hence,

$$\begin{aligned} \mathcal{D}(q) &= \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^2 + A\varepsilon_2q^4 + B\varepsilon_2^2q^5 & \varepsilon_3^{-1}q^2 + A\varepsilon_3q^4 + B\varepsilon_3^2q^5 \\ \eta_1^{-1} + A\eta_1q^4 & \tilde{g}_2q^2 & \tilde{g}_3q^2 \end{array} \right| + O(q^6) \\ &= \left| \begin{array}{cc} \varepsilon_1^{-1} & \varepsilon_2^{-1} - \varepsilon_3^{-1} \\ \eta_1^{-1} & \tilde{g}_2 - \tilde{g}_3 \end{array} \right| q^2 + \left( \left| \begin{array}{cc} \varepsilon_2^{-1} & \varepsilon_3^{-1} \\ \tilde{g}_2 & \tilde{g}_3 \end{array} \right| + A\eta_1^{-1}(\varepsilon_3 - \varepsilon_2) \right) q^4 + B\eta_1^{-1}(\varepsilon_3^2 - \varepsilon_2^2)q^5 + O(q^6). \end{aligned}$$

Equating to 0 the coefficient of  $q^5$ , we obtain  $\varepsilon_3 = \pm\varepsilon_2$ , and (9-3) implies that  $\varepsilon_3 = -\varepsilon_2$ . Using this, and equating to 0 the coefficients of  $q^2$  and  $q^4$ , we obtain

$$\varepsilon_1^{-1}(\tilde{g}_2 - \tilde{g}_3) = 2\varepsilon_2^{-1}\eta_1^{-1}, \quad \varepsilon_2^{-1}(\tilde{g}_2 + \tilde{g}_3) = 2A\eta_1^{-1}\varepsilon_2,$$

from which we deduce  $g_2 = \tilde{g}_2 + 744 = \varepsilon_1\varepsilon_2^{-1}\eta_1^{-1} + A\eta_1^{-1}\varepsilon_2^2 + 744$ .

Now Lemma 5.9 implies that  $g_2 \in \mathbb{Z}$ , from which we deduce, using Lemma 4.2, that both roots of unity  $\varepsilon_1\varepsilon_2^{-1}\eta_1^{-1}$  and  $\eta_1^{-1}\varepsilon_2^2$  must be  $\pm 1$ . Hence,  $g_2$  is one of the four numbers  $744 \pm 1 \pm A$ , contradicting Lemma 5.6.

**9C. Proof of  $f_k = g_k$  for  $k = 1, 2, 3$ .** In the previous subsection we proved that

$$m_1 = n_1 > m = n. \tag{9-7}$$

We want to now prove that

$$f_k = g_k \quad (k = 1, 2, 3). \tag{9-8}$$

We again distinguish the subcases  $m = n > 0$  and  $m = n = 0$ . As before, we set  $\lambda = m_1 - m = n_1 - n$ .

The subcase  $m = n > 0$ . If  $m = n > 0$  then

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda + A\varepsilon_2q^{\lambda+2m} & \varepsilon_3^{-1}q^\lambda + A\varepsilon_3q^{\lambda+2m} \\ \eta_1^{-1} & \eta_2^{-1}q^\lambda + A\eta_2q^{\lambda+2m} & \eta_3^{-1}q^\lambda + A\eta_3q^{\lambda+2m} \end{vmatrix} + o(q^{\lambda+2m}) \\ &= \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2^{-1} - \varepsilon_3^{-1} \\ \eta_1^{-1} & \eta_2^{-1} - \eta_3^{-1} \end{vmatrix} q^\lambda + \begin{vmatrix} \varepsilon_2^{-1} & \varepsilon_3^{-1} \\ \eta_2^{-1} & \eta_3^{-1} \end{vmatrix} q^{2\lambda} + A \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2 - \varepsilon_3 \\ \eta_1^{-1} & \eta_2 - \eta_3 \end{vmatrix} q^{\lambda+2m} + o(q^{\lambda+2m}). \end{aligned} \tag{9-9}$$

This implies the equations

$$\begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2^{-1} - \varepsilon_3^{-1} \\ \eta_1^{-1} & \eta_2^{-1} - \eta_3^{-1} \end{vmatrix} = 0, \quad \begin{vmatrix} \varepsilon_2^{-1} & \varepsilon_3^{-1} \\ \eta_2^{-1} & \eta_3^{-1} \end{vmatrix} = 0, \quad \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2 - \varepsilon_3 \\ \eta_1^{-1} & \eta_2 - \eta_3 \end{vmatrix} = 0 \tag{9-10}$$

if  $2\lambda \neq \lambda + 2m$  and the equations

$$\begin{aligned} \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2^{-1} - \varepsilon_3^{-1} \\ \eta_1^{-1} & \eta_2^{-1} - \eta_3^{-1} \end{vmatrix} &= 0, \\ \begin{vmatrix} \varepsilon_2^{-1} & \varepsilon_3^{-1} \\ \eta_2^{-1} & \eta_3^{-1} \end{vmatrix} &= -A \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2 - \varepsilon_3 \\ \eta_1^{-1} & \eta_2 - \eta_3 \end{vmatrix} \end{aligned} \tag{9-11}$$

if  $2\lambda = \lambda + 2m$ . If both sides of (9-11) are nonzero, then Lemma 4.1 implies  $196884 = |A| \leq 2$ , a contradiction. Hence, in any case we have (9-10).

Resolving the first two equations from (9-10) in  $\eta_1^{-1}, \eta_2^{-1}, \eta_3^{-1}$  and using (9-3), we obtain

$$(\eta_1, \eta_2, \eta_3) = \theta(\varepsilon_1, \varepsilon_2, \varepsilon_3)$$

for some  $\theta \in \mathbb{C}$ . Substituting this into the third equation in (9-10) and again using (9-3), we find  $\theta = \pm 1$ . If  $\theta = -1$ , then we get for  $\mathcal{D}(q)$  the value

$$\begin{aligned} &\begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} + A\varepsilon_1q^{2\lambda+2m} & \varepsilon_2^{-1}q^\lambda + A\varepsilon_2q^{\lambda+2m} + B\varepsilon_2^2q^{\lambda+3m} & \varepsilon_3^{-1}q^\lambda + A\varepsilon_3q^{\lambda+2m} + B\varepsilon_3^2q^{\lambda+3m} \\ -\varepsilon_1^{-1} - A\varepsilon_1q^{2\lambda+2m} & -\varepsilon_2^{-1}q^\lambda - A\varepsilon_2q^{\lambda+2m} + B\varepsilon_2^2q^{\lambda+3m} & -\varepsilon_3^{-1}q^\lambda - A\varepsilon_3q^{\lambda+2m} + B\varepsilon_3^2q^{\lambda+3m} \end{vmatrix} \\ &\qquad\qquad\qquad + o(q^{\lambda+3m}) \\ &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} + A\varepsilon_1q^{2\lambda+2m} & \varepsilon_2^{-1}q^\lambda + A\varepsilon_2q^{\lambda+2m} + B\varepsilon_2^2q^{\lambda+3m} & \varepsilon_3^{-1}q^\lambda + A\varepsilon_3q^{\lambda+2m} + B\varepsilon_3^2q^{\lambda+3m} \\ 0 & 2B\varepsilon_2^2q^{\lambda+3m} & 2B\varepsilon_3^2q^{\lambda+3m} \end{vmatrix} \\ &\qquad\qquad\qquad + o(q^{\lambda+3m}) \\ &= 2B\varepsilon_1^{-1}(\varepsilon_2^2 - \varepsilon_3^2)q^{\lambda+3m} + o(q^{\lambda+3m}), \end{aligned}$$

which gives  $\varepsilon_2 = \pm\varepsilon_3$ , and  $\varepsilon_2 = -\varepsilon_3$  by (9-3). Thus, we have  $\varepsilon_2 = \eta_3 = -\varepsilon_3 = -\eta_2$ , which implies that  $f_2 = g_3$  and  $g_2 = f_3$ , contradicting Lemma 8.1.

The only remaining option is  $\theta = 1$ , which, together with (9-7), proves (9-8).

The subcase  $m = n = 0$ . This case can be easily settled using Lemma 7.3. Indeed, in the case  $m = n = 0$  the functions  $f_1, g_1$  are nonconstant,  $f_2, f_3, g_2, g_3$  are constant, and

$$0 = \begin{vmatrix} 1 & 1 & 1 \\ f_1 & f_2 & f_3 \\ g_1 & g_2 & g_3 \end{vmatrix} = (g_2 - g_3)f_1 - (f_2 - f_3)g_1 + \begin{vmatrix} f_2 & f_3 \\ g_2 & g_3 \end{vmatrix}$$

is a nontrivial linear relation for  $f_1, g_1$  (recall that  $f_2 \neq f_3$  and  $g_2 \neq g_3$  by (8-3)). By Lemma 7.3

$$f_1 = g_1, \quad f_2 - f_3 = g_2 - g_3, \quad \begin{vmatrix} f_2 & f_3 \\ g_2 & g_3 \end{vmatrix} = 0.$$

From the last two equations, one easily deduces that  $f_2 = g_2$  and  $f_3 = g_3$ , proving (9-8).

**10. The case  $m_2 > m_3$  and  $n_2 > n_3$**

In this section we assume that

$$m_1 > m_2 > m_3, \quad n_1 > n_2 > n_3. \tag{10-1}$$

As in the previous section, we will prove that in this case  $f_k = g_k$  for  $k = 1, 2, 3$ .

The strategy of the proof is similar to that of the previous section. Equation (8-9) now reads

$$m_1 - m_2 = n_1 - n_2. \tag{10-2}$$

We start with proving that

$$m_1 - m_3 = n_1 - n_3; \tag{10-3}$$

see Section 10A. Then we prove, in Section 10B, that  $m_1 = n_1$ . Since, by this time, we will already know (10-2) and (10-3), this will imply that  $m_k = n_k$  for every  $k = 1, 2, 3$ . After this, we prove that  $f_k = g_k$  for  $k = 1, 2, 3$  in Section 10C.

We set  $m_1 - m_2 = n_1 - n_2 = \lambda$ . We also have  $m_1 \geq n_1$  by (8-7). Let us collect our knowledge:

$$m_1 > m_2 > m_3, \quad n_1 > n_2 > n_3, \quad m_1 - m_2 = n_1 - n_2 = \lambda > 0, \quad m_1 - n_1 = m_2 - n_2 \geq 0.$$

**10A. Proof of  $m_1 - m_3 = n_1 - n_3$ .** Now let us prove that  $m_1 - m_3 = n_1 - n_3$ . Using notation (8-12), we write

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \tilde{f}_3q^{m_1-m_3} \\ \eta_1^{-1} & \eta_2^{-1}q^\lambda & \tilde{g}_3q^{n_1-n_3} \end{vmatrix} + o(q^{n_1}) \\ &= \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2^{-1} \\ \eta_1^{-1} & \eta_2^{-1} \end{vmatrix} q^\lambda + \tilde{f}_3\eta_1^{-1}q^{m_1-m_3} - \varepsilon_1^{-1}\tilde{g}_3q^{n_1-n_3} + o(q^{m_1-m_3}) + o(q^{n_1-n_3}). \end{aligned}$$

If  $m_1 - m_3 \neq n_1 - n_3$ , then we have one of the options

$$\lambda < m_1 - m_3 < n_1 - n_3, \quad \lambda < n_1 - n_3 < m_1 - m_3.$$

In the first case  $q^{m_1 - m_3}$  cannot be eliminated, and in the second case  $q^{n_1 - n_3}$  cannot be eliminated. This proves that  $m_1 - m_3 = n_1 - n_3$ .

We set  $m_1 - m_3 = n_1 - n_3 = \lambda'$ . Thus,

$$\begin{aligned} m_1 > m_2 > m_3, \quad n_1 > n_2 > n_3, \\ m_1 - m_2 = n_1 - n_2 = \lambda > 0, \quad m_1 - m_3 = n_1 - n_3 = \lambda' > \lambda > 0, \quad (10-4) \\ m_1 - n_1 = m_2 - n_2 = m_3 - n_3 \geq 0. \end{aligned}$$

In addition to this, from

$$\mathcal{D}(q) = \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1} q^\lambda & \tilde{f}_3 q^{\lambda'} \\ \eta_1^{-1} & \eta_2^{-1} q^\lambda & \tilde{g}_3 q^{\lambda'} \end{vmatrix} + o(q^{n_1}) = \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2^{-1} \\ \eta_1^{-1} & \eta_2^{-1} \end{vmatrix} q^\lambda - \begin{vmatrix} \varepsilon_1^{-1} & \tilde{f}_3 \\ \eta_1^{-1} & \tilde{g}_3 \end{vmatrix} q^{\lambda'} + o(q^{\lambda'}),$$

we deduce that

$$\begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2^{-1} \\ \eta_1^{-1} & \eta_2^{-1} \end{vmatrix} = \begin{vmatrix} \varepsilon_1^{-1} & \tilde{f}_3 \\ \eta_1^{-1} & \tilde{g}_3 \end{vmatrix} = 0, \quad (10-5)$$

which means that

$$(\eta_1^{-1}, \eta_2^{-1}, \tilde{g}_3) = \theta(\varepsilon_1^{-1}, \varepsilon_2^{-1}, \tilde{f}_3) \quad (10-6)$$

with some root of unity  $\theta$ .

**10B. Proof of  $m_1 = n_1$ .** In this subsection we show that  $m_1 = n_1$ . Thus, assume

$$m_1 > n_1, \quad (10-7)$$

in which case we also have

$$m_2 > n_2, \quad m_3 > n_3. \quad (10-8)$$

We should also have

$$n_3 > 0. \quad (10-9)$$

Indeed, if  $m_3 > n_3 = 0$ , then the second equation in (10-5) reads  $g_3 = 744 + \varepsilon_1 \varepsilon_3^{-1} \eta_1^{-1}$ , which is impossible by Lemma 5.7.

Using (10-6), (10-7), (10-8), and (10-9), we obtain

$$\begin{aligned} \mathfrak{D}(q) &= \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{\lambda'} \\ \eta_1^{-1} & \eta_2^{-1}q^\lambda & \eta_3^{-1}q^{\lambda'} + A\eta_3q^{n_1+n_3} \end{array} \right| + o(q^{n_1+n_3}) \\ &= \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{\lambda'} \\ 0 & 0 & A\eta_3q^{n_1+n_3} \end{array} \right| + o(q^{n_1+n_3}) \\ &= -A\varepsilon_1^{-1}\eta_3q^{n_1+n_3} + o(q^{n_1+n_3}), \end{aligned}$$

a contradiction.

This proves that

$$m_k = n_k \quad (k = 1, 2, 3). \tag{10-10}$$

**10C. Proof of  $f_k = g_k$  for  $k = 1, 2, 3$ .** To prove that  $f_k = g_k$  for  $k = 1, 2, 3$ , we only need to show that

$$\theta = 1,$$

where  $\theta$  is from (10-6). If  $m_3 = n_3 = 0$ , then rewriting the equality  $\tilde{g}_3 = \theta \tilde{f}_3$  as  $(g_3 - 744) = \theta(f_3 - 744)$ , we deduce  $\theta = 1$  from Lemma 5.2.

Now assume that  $m_3 = n_3 > 0$ . In this case

$$\begin{aligned} \mathfrak{D}(q) &= \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{\lambda'} + A\varepsilon_3q^{m_1+m_3} \\ \eta_1^{-1} & \eta_2^{-1}q^\lambda & \eta_3^{-1}q^{\lambda'} + A\eta_3q^{m_1+m_3} \end{array} \right| + o(q^{m_1+m_3}) \\ &= \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{\lambda'} + A\varepsilon_3q^{m_1+m_3} \\ 0 & 0 & A\varepsilon_3(\theta^{-1} - \theta)q^{m_1+m_3} \end{array} \right| + o(q^{m_1+m_3}) \\ &= -A\varepsilon_1^{-1}\varepsilon_3(\theta^{-1} - \theta)q^{m_1+m_3} + o(q^{m_1+m_3}), \end{aligned}$$

which implies  $\theta = \pm 1$ . If  $\theta = -1$ , then we get for  $\mathfrak{D}(q)$  the value

$$\begin{aligned} &\left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} + A\varepsilon_1q^{2m_1} & \varepsilon_2^{-1}q^\lambda + A\varepsilon_2q^{m_1+m_2} & \varepsilon_3^{-1}q^{\lambda'} + A\varepsilon_3q^{m_1+m_3} + B\varepsilon_3^2q^{m_1+2m_3} \\ -\varepsilon_1^{-1} - A\varepsilon_1q^{2m_1} & -\varepsilon_2^{-1}q^\lambda - A\varepsilon_2q^{m_1+m_2} & -\varepsilon_3^{-1}q^{\lambda'} - A\varepsilon_3q^{m_1+m_3} + B\varepsilon_3^2q^{m_1+2m_3} \end{array} \right| \\ &\qquad\qquad\qquad + o(q^{m_1+2m_3}) \\ &= \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} + A\varepsilon_1q^{2m_1} & \varepsilon_2^{-1}q^\lambda + A\varepsilon_2q^{m_1+m_2} & \varepsilon_3^{-1}q^{\lambda'} + A\varepsilon_3q^{m_1+m_3} \\ 0 & 0 & 2B\varepsilon_3^2q^{m_1+2m_3} \end{array} \right| + o(q^{m_1+2m_3}) \\ &= -2B\varepsilon_1^{-1}\varepsilon_3^2q^{m_1+2m_3} + o(q^{m_1+2m_3}), \end{aligned}$$

a contradiction.

Thus, in any case we have  $\theta = 1$  in (10-6). Together with (10-10), this proves that  $f_k = g_k$  for  $k = 1, 2, 3$ .

**11. The case  $m_2 > m_3$  and  $n_2 = n_3$**

In this section we assume that

$$m_1 > m_2 > m_3, \quad n_1 > n_2 = n_3 \tag{11-1}$$

and will show that this is impossible.

Relation (8-9) now becomes  $m_1 - m_2 = n_1 - n_2 = n_1 - n_3$ . We set

$$m_1 - m_2 = n_1 - n_2 = n_1 - n_3 = \lambda. \tag{11-2}$$

First of all, let us rule out the case  $n_2 = n_3 = 0$ . In this case  $n_1 = \lambda < m_1 - m_3$ . Using notation (8-12), we write in this case

$$\mathcal{D}(q) = \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & 0 \\ \eta_1^{-1} & \tilde{g}_2q^\lambda & \tilde{g}_3q^\lambda \end{vmatrix} + o(q^\lambda) = (\varepsilon_1^{-1}\tilde{g}_2 - \varepsilon_1^{-1}\tilde{g}_3 - \varepsilon_2^{-1}\eta_1^{-1})q^\lambda + o(q^\lambda).$$

We obtain  $\varepsilon_1^{-1}\tilde{g}_2 - \varepsilon_1^{-1}\tilde{g}_3 - \varepsilon_2^{-1}\eta_1^{-1} = 0$ , which contradicts Lemma 5.5.

Thus, we may assume in the sequel that

$$n_2 = n_3 > 0. \tag{11-3}$$

Since  $n_2 = n_3$ , we have

$$\eta_2 \neq \eta_3, \tag{11-4}$$

which will be systematically used, sometimes without special reference.

Our principal objective will be to show that  $m_3 = m_1 - 2\lambda$  and  $n_1 = m_1 - \lambda/2$ . The first of these two relations is proved already in Section 11A. The second one is more delicate and will be established in Section 11D, after some preparatory work done in the previous subsections. On the way, we will also prove certain inequalities relating the numbers  $m_k, n_k$ , and  $\lambda$  and certain relations for the twists. After all this is done, obtaining a contradiction will be relatively easy; see Section 11E.

**11A. Proof of  $2\lambda = m_1 - m_3 \leq n_1 + n_2$ .** Using notation (8-12), we write

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \tilde{f}_3q^{m_1-m_3} \\ \eta_1^{-1} & \eta_2^{-1}q^\lambda + A\eta_2q^{n_1+n_2} & \eta_3^{-1}q^\lambda + A\eta_3q^{n_1+n_2} \end{vmatrix} + o(q^{m_1}) + o(q^{n_1+n_2}) \\ &= (\varepsilon_1^{-1}\eta_2^{-1} - \varepsilon_1^{-1}\eta_3^{-1} - \varepsilon_2^{-1}\eta_1^{-1})q^\lambda + \varepsilon_2^{-1}\eta_3^{-1}q^{2\lambda} + \eta_1^{-1}\tilde{f}_3q^{m_1-m_3} \\ &\quad + A\varepsilon_1^{-1}(\eta_2 - \eta_3)q^{n_1+n_2} + o(q^{m_1-m_3}) + o(q^{n_1+n_2}). \end{aligned} \tag{11-5}$$

First of all, this gives

$$\varepsilon_1^{-1}\eta_2^{-1} - \varepsilon_1^{-1}\eta_3^{-1} - \varepsilon_2^{-1}\eta_1^{-1} = 0. \tag{11-6}$$

A sum of three roots of unity can vanish only if they are proportional to the three distinct cubic roots of unity. In particular,

$$\eta_2/\eta_3 \text{ is a primitive 6th root of unity.} \tag{11-7}$$

We have  $m_1 - m_3 \geq 2\lambda$ . Indeed, if  $2\lambda > m_1 - m_3$ , then we must have

$$m_1 - m_3 = n_1 + n_2, \quad \eta_1^{-1}\tilde{f}_3 = -A\varepsilon_1^{-1}(\eta_2 - \eta_3). \tag{11-8}$$

If  $m_3 > 0$ , this gives  $\eta_1^{-1}\varepsilon_3^{-1} = -A\varepsilon_1^{-1}(\eta_2 - \eta_3)$ , which is impossible because  $A$  does not divide a root of unity. And if  $m_3 = 0$ , then  $f_3 = 744 - A\varepsilon_1^{-1}\eta_1(\eta_2 - \eta_3)$ . Lemma 5.9 now implies that  $f_3 \in \mathbb{Z}$ , and we obtain  $f_3 \in \{744 \pm 196884, 744 \pm 2 \cdot 196884\}$ , contradicting Lemma 5.6.

We have  $m_1 - m_3 \leq 2\lambda$ . Indeed, if  $2\lambda < m_1 - m_3$ , then the term with  $q^{2\lambda}$  cancels either a term in  $o(q^{n_1+n_2})$  or the term with  $q^{n_1+n_2}$ . In the first situation the terms with  $q^{m_1-m_3}$  and  $q^{n_1+n_2}$  must cancel each other, and we are back to (11-8). In the second situation we must have

$$2\lambda = n_1 + n_2, \quad \varepsilon_2^{-1}\eta_3^{-1} = -A\varepsilon_1^{-1}(\eta_2 - \eta_3),$$

which is impossible because  $A = 196884$  does not divide a root of unity.

Thus, we proved that  $m_1 - m_3 = 2\lambda$ .

We have  $n_1 + n_2 \geq 2\lambda$ . Indeed, if  $n_1 + n_2 < 2\lambda = m_1 - m_3$ , then the nonzero term  $A\varepsilon_1^{-1}(\eta_2 - \eta_3)q^{n_1+n_2}$  cannot be eliminated. (It is nonzero because of (11-4).)

Thus, we proved that

$$2\lambda = m_1 - m_3 \leq n_1 + n_2. \tag{11-9}$$

**11B. Proof of  $n_1 + n_2 > 2\lambda$ .** We want to show now that the inequality in (11-9) is strict. Thus, assume the contrary, that is,

$$2\lambda = m_1 - m_3 = n_1 + n_2. \tag{11-10}$$

Then (11-5) implies that

$$\varepsilon_2^{-1}\eta_3^{-1} + \eta_1^{-1}\tilde{f}_3 + A\varepsilon_1^{-1}(\eta_2 - \eta_3) = 0. \tag{11-11}$$

This implies that  $m_3 = 0$ . Indeed, if  $m_3 > 0$ , then (11-11) can be rewritten as

$$\varepsilon_2^{-1}\eta_3^{-1} + \eta_1^{-1}\varepsilon_3^{-1} = -A\varepsilon_1^{-1}(\eta_2 - \eta_3). \tag{11-12}$$

Both sides in (11-12) are nonzero by (11-4), and Lemma 4.1 implies that  $2 \geq |A|$ , a contradiction. Thus, we have  $m_3 = 0$ , which, together with (11-2) and (11-10), implies that

$$m_1 = 2\lambda, \quad m_2 = \lambda, \quad n_1 = \frac{3}{2}\lambda, \quad n_2 = n_3 = \frac{1}{2}\lambda.$$

Rescaling, we may assume that  $\lambda = 2$ , which gives

$$m_1 = 4, \quad m_2 = 2, \quad m_3 = 0, \quad n_1 = 3, \quad n_2 = n_3 = 1.$$

Using (11-6) and (11-11), we obtain

$$\begin{aligned} \mathcal{D}(q) &= \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^2 & \tilde{f}_3q^4 \\ \eta_1^{-1} & \eta_2^{-1}q^2 + A\eta_2q^4 + B\eta_2^2q^5 & \eta_3^{-1}q^2 + A\eta_3q^4 + B\eta_3^2q^5 \end{array} \right| + O(q^6) \\ &= B\varepsilon_1^{-1}(\eta_2^2 - \eta_3^2)q^5 + O(q^6), \end{aligned}$$

which gives  $\eta_2 = \pm\eta_3$ , contradicting (11-7).

This proves that

$$2\lambda = m_1 - m_3 < n_1 + n_2. \tag{11-13}$$

**11C. Proof of  $m_3 > 0$ .** In addition to this, we have  $m_3 > 0$ . Indeed, equating to 0 the coefficient of  $q^{2\lambda}$  in (11-5), we obtain

$$\varepsilon_2^{-1}\eta_3^{-1} + \eta_1^{-1}\tilde{f}_3 = 0. \tag{11-14}$$

If  $m_3 = 0$ , then this gives  $f_3 = 744 - \varepsilon_2^{-1}\eta_3^{-1}\eta_1$ , contradicting Lemma 5.7. This proves that

$$m_3 > 0, \tag{11-15}$$

and (11-14) becomes

$$\varepsilon_2^{-1}\eta_3^{-1} = -\varepsilon_3^{-1}\eta_1^{-1}. \tag{11-16}$$

**11D. Proof of  $m_1 + m_3 = n_1 + n_2 < 3\lambda$ .** Our next step is showing that  $m_1 + m_3 = n_1 + n_2 < 3\lambda$ . Using (11-6) and (11-16), we obtain

$$\begin{aligned} \mathcal{D}(q) &= \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{2\lambda} + A\varepsilon_3q^{m_1+m_3} \\ \eta_1^{-1} & \eta_2^{-1}q^\lambda + A\eta_2q^{n_1+n_2} & \eta_3^{-1}q^\lambda + A\eta_3q^{n_1+n_2} \end{array} \right| + o(q^{m_1+m_3}) + o(q^{n_1+n_2}) \\ &= A\varepsilon_3\eta_1^{-1}q^{m_1+m_3} + A\varepsilon_1^{-1}(\eta_2 - \eta_3)q^{n_1+n_2} - \varepsilon_3^{-1}\eta_2^{-1}q^{3\lambda} \\ &\quad + o(q^{m_1+m_3}) + o(q^{n_1+n_2}). \end{aligned} \tag{11-17}$$

We have  $m_1 + m_3 \geq n_1 + n_2$ . Indeed, if  $m_1 + m_3 < n_1 + n_2$ , then we must have  $m_1 + m_3 = 3\lambda$  and  $A\varepsilon_3\eta_1^{-1} = \varepsilon_3^{-1}\eta_2^{-1}$ , which is impossible because  $A$  is not a root of unity.



We have  $m_1 + m_3 \leq n_1 + n_2$ . Similarly, if  $m_1 + m_3 > n_1 + n_2$ , then we must have  $n_1 + n_2 = 3\lambda$  and  $A\varepsilon_1^{-1}(\eta_2 - \eta_3) = \varepsilon_3^{-1}\eta_2^{-1}$ , which is impossible because  $A$  does not divide a root of unity.

We have  $m_1 + m_3 = n_1 + n_2 < 3\lambda$ . Indeed, if  $m_1 + m_3 = n_1 + n_2 > 3\lambda$ , then the  $q^{3\lambda}$  cannot be eliminated. And if  $m_1 + m_3 = n_1 + n_2 = 3\lambda$ , then  $A\varepsilon_3\eta_1^{-1} + A\varepsilon_1^{-1}(\eta_2 - \eta_3) = \varepsilon_3^{-1}\eta_2^{-1}$ , which is impossible because  $A$  does not divide a root of unity.

Thus, we proved that

$$m_1 + m_3 = n_1 + n_2 < 3\lambda. \quad (11-18)$$

Since  $n_2 = n_1 - \lambda$  and  $m_3 = m_1 - 2\lambda$  (see (11-2) and (11-13)), this implies that

$$n_1 = m_1 - \frac{1}{2}\lambda. \quad (11-19)$$

Also, comparing the coefficients in (11-17), we obtain

$$\varepsilon_3\eta_1^{-1} + \varepsilon_1^{-1}\eta_2 - \varepsilon_1^{-1}\eta_3 = 0. \quad (11-20)$$

**11E. Conclusion.** We are almost done. Let us summarize the relations between the levels we already obtained. We deduce from (11-2), (11-15), (11-18), and (11-19)

$$m_2 = m_1 - \lambda, \quad m_3 = m_1 - 2\lambda, \quad n_1 = m_1 - \frac{1}{2}\lambda, \quad n_2 = n_3 = m_1 - \frac{3}{2}\lambda, \quad 2\lambda < m_1 < \frac{5}{2}\lambda.$$

This implies the inequalities

$$2m_1 > m_1 + m_2 = m_1 + m_3 + \lambda = n_1 + n_2 + \lambda > 3\lambda, \quad 2n_1 > 3\lambda, \quad n_1 + 2n_2 > m_1 + 2m_3.$$

It follows that

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{2\lambda} + A\varepsilon_3q^{m_1+m_3} + B\varepsilon_3^2q^{m_1+2m_3} \\ \eta_1^{-1} & \eta_2^{-1}q^\lambda + A\eta_2q^{n_1+n_2} & \eta_3^{-1}q^\lambda + A\eta_3q^{n_1+n_2} \end{vmatrix} \\ &\quad + o(q^{m_1+2m_3}) + o(q^{3\lambda}) \\ &= -\varepsilon_3^{-1}\eta_2^{-1}q^{3\lambda} + B\varepsilon_3^2\eta_1^{-1}q^{m_1+2m_3} + o(q^{m_1+2m_3}) + o(q^{3\lambda}). \end{aligned}$$

We obtain  $3\lambda = m_1 + 2m_3$  and  $\varepsilon_3^{-1}\eta_2^{-1} = B\varepsilon_3^2\eta_1^{-1}$ . But the last equation is impossible because  $B$  is not a root of unity. This proves that (11-1) is impossible in case (11-3).

## 12. The case $m_2 > m_3$ and $n_3 > n_2$

In this section we assume that

$$m_1 > m_2 > m_3, \quad n_1 > n_3 > n_2 \quad (12-1)$$

(as usual with  $m_1 \geq n_1$ ) and will, eventually, arrive at a contradiction. This is the nastiest case, and we beg for the reader's patience.

Relation (8-9) now becomes  $m_1 - m_2 = n_1 - n_3$ . We set  $m_1 - m_2 = n_1 - n_3 = \lambda$ . Using notation (8-12), we write

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \tilde{f}_3q^{m_1-m_3} \\ \eta_1^{-1} & \tilde{g}_2q^{n_1-n_2} & \eta_3^{-1}q^\lambda \end{vmatrix} + o(q^{n_1}) \\ &= \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2^{-1} \\ \eta_1^{-1} & -\eta_3^{-1} \end{vmatrix} q^\lambda + \tilde{f}_3\eta_1^{-1}q^{m_1-m_3} + \varepsilon_1^{-1}\tilde{g}_2q^{n_1-n_2} + \varepsilon_2^{-1}\eta_3^{-1}q^{2\lambda} \\ &\quad - \tilde{f}_3\tilde{g}_2q^{m_1-m_3+n_1-n_2} + o(q^{n_1}). \end{aligned} \tag{12-2}$$

Since  $0 < \lambda < m_1 - m_3, n_1 - n_2$ , this implies that

$$\begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2^{-1} \\ \eta_1^{-1} & -\eta_3^{-1} \end{vmatrix} = 0. \tag{12-3}$$

**12A. Proof of  $m_1 - m_3 = n_1 - n_2$ .** Let us start by proving that

$$m_1 - m_3 = n_1 - n_2. \tag{12-4}$$

Indeed, assume that  $m_1 - m_3 \neq n_1 - n_2$ . Then  $q^{n_1-n_2}$  in (12-2) can be eliminated only if

$$n_1 - n_2 = 2\lambda, \quad \varepsilon_1^{-1}\tilde{g}_2 = -\varepsilon_2^{-1}\eta_3^{-1}. \tag{12-5}$$

This implies also that  $n_2 > 0$ . Indeed, if  $n_2 = 0$ , then the second equality in (12-5) gives  $g_2 = 744 - \varepsilon_1\varepsilon_2^{-1}\eta_3^{-1}$ , contradicting Lemma 5.7.

Using (12-3) and (12-5), we can now write

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \tilde{f}_3q^{m_1-m_3} \\ \eta_1^{-1} & \eta_2^{-1}q^{2\lambda} + A\eta_2q^{n_1+n_2} & \eta_3^{-1}q^\lambda \end{vmatrix} + o(q^{m_1}) + o(q^{n_1+n_2}) \\ &= \tilde{f}_3\eta_1^{-1}q^{m_1-m_3} + A\varepsilon_1^{-1}\eta_2q^{n_1+n_2} + o(q^{m_1-m_3}) + o(q^{n_1+n_2}). \end{aligned}$$

Here the term with  $q^{m_1-m_3}$  cannot be eliminated by  $o(q^{n_1+n_2})$  since then  $m_1 - m_3 > n_1 + n_2$  and after elimination  $q^{n_1+n_2}$  would still be standing. So

$$m_1 - m_3 = n_1 + n_2, \quad \tilde{f}_3\eta_1^{-1} = -A\varepsilon_1^{-1}\eta_2. \tag{12-6}$$

However, the second equality in (12-6) is impossible. Indeed, if  $m_3 > 0$ , then it becomes  $\varepsilon_3^{-1}\eta_1^{-1} = -A\varepsilon_1^{-1}\eta_2$ , which is clearly impossible because  $A = 196884$  is not a root of unity. And if  $m_3 = 0$ , then it becomes  $f_3 = 744 - A\varepsilon_1^{-1}\eta_1\eta_2$ , contradicting Lemma 5.7.

This proves (12-4). We set  $m_1 - m_3 = n_1 - n_2 = \lambda'$ . Since  $m_1 \geq n_1$  by (8-7), we may summarize our present knowledge as

$$\begin{aligned} m_1 &> m_2 > m_3, & n_1 &> n_3 > n_2, \\ m_1 - m_2 &= n_1 - n_3 = \lambda > 0, & m_1 - m_3 &= n_1 - n_2 = \lambda' > \lambda, \\ m_1 - n_1 &= m_2 - n_3 = m_3 - n_2 \geq 0. \end{aligned}$$

**12B. Proof of  $m_3 > 0$ .** In this subsection we prove that  $m_3 > 0$ . We will assume that  $m_3 = 0$  and will arrive at a contradiction.

If  $m_3 = 0$ , then

$$\tilde{m}_1 = n_1 = \lambda', \quad m_2 = n_3, \quad m_3 = n_2 = 0. \tag{12-7}$$

Using (12-3), we obtain

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1} q^\lambda + A\varepsilon_2 q^{m_1+m_2} & \tilde{f}_3 q^{m_1} \\ \eta_1^{-1} & \tilde{g}_2 q^{m_1} & \eta_3^{-1} q^\lambda + A\eta_3 q^{m_1+m_2} \end{vmatrix} + o(q^{m_1+m_2}) \\ &= \begin{vmatrix} \varepsilon_1^{-1} & \tilde{f}_3 \\ -\eta_1^{-1} & \tilde{g}_2 \end{vmatrix} q^{m_1} + \varepsilon_2^{-1} \eta_3^{-1} q^{2\lambda} + A \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2 \\ \eta_1^{-1} & -\eta_3 \end{vmatrix} q^{m_1+m_2} + o(q^{m_1+m_2}). \end{aligned} \tag{12-8}$$

The term with  $q^{m_1+m_2}$  can be eliminated if either

$$\begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2 \\ \eta_1^{-1} & -\eta_3 \end{vmatrix} = 0, \tag{12-9}$$

or  $m_1 + m_2 = 2\lambda$  and

$$A \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_2 \\ \eta_1^{-1} & -\eta_3 \end{vmatrix} = -\varepsilon_2^{-1} \eta_3^{-1}. \tag{12-10}$$

However, (12-10) is impossible because  $A$  does not divide a root of unity. Hence, we have (12-9). Together with (12-3), this implies that

$$(\varepsilon_1, \varepsilon_2) = \theta(\eta_1, -\eta_3), \quad \theta = \pm 1. \tag{12-11}$$

The rest of this subsection splits into three cases depending on the relation between  $m_2$  and  $\lambda$ .

The case  $m_2 > \lambda$ . In this case  $m_1 > 2\lambda$  and  $q^{2\lambda}$  in (12-8) cannot be eliminated.

The case  $m_2 < \lambda$ . In this case  $m_1 < 2\lambda$ , and  $q^{m_1}$  in (12-8) can be eliminated only if  $\varepsilon_1^{-1} \tilde{g}_2 + \eta_1^{-1} \tilde{f}_3 = 0$ , which, combined with (12-11), gives  $\tilde{g}_2 = -\theta \tilde{f}_3$ . Lemma 5.2 implies that  $\theta = -1$  and  $\tilde{f}_3 = \tilde{g}_2$ , that is,  $f_3 = g_2$ . Also, since  $\theta = -1$ , we obtain  $\varepsilon_2 = \eta_3$ , which, together with  $m_2 = n_3$  (see (12-7)), implies that  $f_2 = g_3$ . This contradicts Lemma 8.1.

The case  $m_2 = \lambda$ . In this case  $m_1 = 2\lambda < m_1 + m_2$  and  $\varepsilon_1^{-1}\tilde{g}_2 + \eta_1^{-1}\tilde{f}_3 + \varepsilon_2^{-1}\eta_3^{-1} = 0$ , which contradicts Lemma 5.5.

This completes the proof of impossibility of  $m_3 = 0$ .

**12C. Proof of  $n_2 > 0$ .** Thus, we have  $m_3 > 0$ . Let us now prove that  $n_2 > 0$  as well. Indeed, if  $n_2 = 0$ , then

$$m_1 > n_1 = \lambda', \quad m_2 > n_3, \quad m_3 > n_2 = 0. \tag{12-12}$$

Using (12-3), we obtain

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{n_1} \\ \eta_1^{-1} & \tilde{g}_2q^{n_1} & \eta_3^{-1}q^\lambda \end{vmatrix} + o(q^{n_1}) \\ &= (\varepsilon_1^{-1}\tilde{g}_2 + \varepsilon_3^{-1}\eta_1^{-1})q^{n_1} + \varepsilon_2^{-1}\eta_3^{-1}q^{2\lambda} + o(q^{n_1}). \end{aligned}$$

Now to eliminate  $q^{n_1}$  we need to have one of the following:

$$\varepsilon_1^{-1}\tilde{g}_2 + \varepsilon_3^{-1}\eta_1^{-1} = 0, \tag{12-13}$$

$$\varepsilon_1^{-1}\tilde{g}_2 + \varepsilon_3^{-1}\eta_1^{-1} + \varepsilon_2^{-1}\eta_3^{-1} = 0. \tag{12-14}$$

However, since  $\tilde{g}_2 = g_2 - 744$ , (12-13) contradicts Lemma 5.7. Furthermore, applying Lemma 5.9 to (12-14), we obtain  $g_2 \in \{744, 744 \pm 1, 744 \pm 2\}$ , contradicting Lemma 5.6.

This proves that  $n_2 > 0$ . Let us summarize our present knowledge as

$$\begin{aligned} m_1 > m_2 > m_3 > 0, \quad n_1 > n_3 > n_2 > 0, \\ m_1 - m_2 = n_1 - n_3 = \lambda > 0, \quad m_1 - m_3 = n_1 - n_2 = \lambda' > \lambda, \\ m_1 - n_1 = m_2 - n_3 = m_3 - n_2 \geq 0. \end{aligned}$$

**12D. Proof of  $m_1 = n_1$ .** Next, we show that  $m_1 = n_1$ . Thus, assume that  $m_1 > n_1$ . Then we also have  $m_2 > n_3$  and  $m_3 > n_2$ . Using (12-3), we write

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{\lambda'} \\ \eta_1^{-1} & \eta_2^{-1}q^{\lambda'} + A\eta_2q^{n_1+n_2} & \eta_3^{-1}q^\lambda \end{vmatrix} + o(q^{n_1+n_2}) \\ &= \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_3^{-1} \\ -\eta_1^{-1} & \eta_2^{-1} \end{vmatrix} q^{\lambda'} + \varepsilon_2^{-1}\eta_3^{-1}q^{2\lambda} - \varepsilon_3^{-1}\eta_2^{-1}q^{2\lambda'} + A\varepsilon_1^{-1}\eta_2q^{n_1+n_2} \\ &\quad + o(q^{n_1+n_2}). \end{aligned} \tag{12-15}$$

To eliminate  $q^{n_1+n_2}$  we need one of the following to hold:

$$2\lambda = n_1 + n_2, \quad \varepsilon_2^{-1}\eta_3^{-1} = -A\varepsilon_1^{-1}\eta_2, \tag{12-16}$$

$$2\lambda' = n_1 + n_2, \quad \varepsilon_3^{-1}\eta_2^{-1} = A\varepsilon_1^{-1}\eta_2. \tag{12-17}$$

However, the second equations in both (12-16) and (12-17) cannot be true because  $A$  is not a root of unity.

This proves that  $m_1 = n_1$ . Moreover,

$$m_1 = n_1 > m_2 = n_3 > m_3 = n_2 > 0, \tag{12-18}$$

$$m_1 - m_2 = n_1 - n_3 = \lambda > 0, \quad m_1 - m_3 = n_1 - n_2 = \lambda' > \lambda.$$

**12E. Proof of  $\lambda' = 2\lambda$ .** Our next quest is proving that  $\lambda' = 2\lambda$ . Using (12-3) and (12-18), we obtain

$$\mathcal{D}(q) = \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{\lambda'} \\ \eta_1^{-1} & \eta_2^{-1}q^{\lambda'} & \eta_3^{-1}q^\lambda \end{vmatrix} + o(q^{m_1}) = - \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_3^{-1} \\ \eta_1^{-1} & -\eta_2^{-1} \end{vmatrix} q^{\lambda'} + \varepsilon_2^{-1}\eta_3^{-1}q^{2\lambda} + o(q^{\lambda'}).$$

This already implies that  $\lambda' \leq 2\lambda$ ; otherwise  $q^{2\lambda}$  cannot be eliminated.

The proof of the opposite inequality  $\lambda' \geq 2\lambda$  is much more involved. Thus, assume that  $\lambda' < 2\lambda$ . Then we must have

$$\begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_3^{-1} \\ \eta_1^{-1} & -\eta_2^{-1} \end{vmatrix} = 0.$$

Together with (12-3) this implies that

$$(\eta_1, -\eta_3, -\eta_2) = \theta(\varepsilon_1, \varepsilon_2, \varepsilon_3), \tag{12-19}$$

where  $\theta$  is some root of unity. We obtain

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{\lambda'} + A\varepsilon_3q^{m_1+m_3} \\ \theta^{-1}\varepsilon_1^{-1} & -\theta^{-1}\varepsilon_3^{-1}q^{\lambda'} - A\theta\varepsilon_3q^{m_1+m_3} & -\theta^{-1}\varepsilon_2^{-1}q^\lambda \end{vmatrix} + o(q^{m_1+m_3}) \\ &= -\theta^{-1}\varepsilon_2^{-2}q^{2\lambda} + \theta^{-1}\varepsilon_3^{-2}q^{2\lambda'} + A\varepsilon_3\varepsilon_1^{-1}(\theta^{-1} - \theta)q^{m_1+m_3} + o(q^{m_1+m_3}). \end{aligned}$$

To eliminate  $q^{m_1+m_3}$  one of the following should be satisfied:

$$A\varepsilon_3\varepsilon_1^{-1}(\theta^{-1} - \theta) = \theta^{-1}\varepsilon_2^{-2}, \quad A\varepsilon_3\varepsilon_1^{-1}(\theta^{-1} - \theta) = -\theta^{-1}\varepsilon_3^{-2}, \quad A\varepsilon_3\varepsilon_1^{-1}(\theta^{-1} - \theta) = 0.$$

Since  $A$  does not divide a root of unity, only the third equation is possible, which implies  $\theta = \pm 1$ . If  $\theta = -1$ , then (12-18) and (12-19) imply that  $f_2 = g_3$  and  $f_3 = g_2$ , contradicting Lemma 8.1. Thus,  $\theta = 1$  and

$$(\eta_1, -\eta_3, -\eta_2) = (\varepsilon_1, \varepsilon_2, \varepsilon_3),$$

which gives us the relations

$$\begin{aligned} q^{m_1}(g_1 - 744) &= q^{m_1}(f_1 - 744), \\ q^{m_1}(g_3 - 744) &= -q^{m_1}(f_2 - 744) + O(q^{m_1+2m_2}), \\ q^{m_1}(g_2 - 744) &= -q^{m_1}(f_3 - 744) + 2B\varepsilon_3^2 q^{m_1+2m_3} + o(q^{m_1+2m_3}). \end{aligned}$$

Using this, and the identity

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a & -c+x & -b \end{vmatrix} = c^2 - b^2 + x(a - c),$$

we obtain

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ q^{m_1}(f_1 - 744) & q^{m_1}(f_2 - 744) & q^{m_1}(f_3 - 744) \\ q^{m_1}(f_1 - 744) & -q^{m_1}(f_3 - 744) + 2B\varepsilon_3^2 q^{m_1+2m_3} & -q^{m_1}(f_2 - 744) \end{vmatrix} \\ &\quad + o(q^{m_1+2m_3}) \\ &= 2B\varepsilon_1^{-1} \varepsilon_3^2 q^{m_1+2m_3} + (\varepsilon_3^{-1} q^{m_1-m_3} + A\varepsilon_3 q^{m_1+m_3})^2 \\ &\quad - (\varepsilon_2^{-1} q^{m_1-m_2} + A\varepsilon_2 q^{m_1+m_2})^2 + o(q^{m_1+2m_3}) \\ &= -\varepsilon_2^{-2} q^{2\lambda} + \varepsilon_3^{-2} q^{2\lambda'} + 2B\varepsilon_1^{-1} \varepsilon_3^2 q^{m_1+2m_3} + o(q^{m_1+2m_3}) \end{aligned}$$

(recall that  $\lambda = m_1 - m_2$  and  $\lambda' = m_1 - m_3$ ). We see that to eliminate  $q^{m_1+2m_3}$  we need to have either  $2B\varepsilon_1^{-1} \varepsilon_3^2 = \varepsilon_2^{-2}$  or  $2B\varepsilon_1^{-1} \varepsilon_3^2 = -\varepsilon_3^{-2}$ ; both are clearly impossible.

This proves that  $\lambda' = 2\lambda$ . Thus,

$$m_1 = n_1, \quad m_2 = n_3 = m_1 - \lambda, \quad m_3 = n_2 = m_1 - 2\lambda > 0. \tag{12-20}$$

**12F. Proof of  $2\lambda < m_1 < 3\lambda$ .** Now it is not difficult to show that

$$2\lambda < m_1 < 3\lambda. \tag{12-21}$$

In fact,  $m_1 > 2\lambda$  is already in (12-20). Next, using (12-3), we obtain

$$\begin{aligned} \mathcal{D}(q) &= \begin{vmatrix} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1} q^\lambda & \varepsilon_3^{-1} q^{2\lambda} + A\varepsilon_3 q^{m_1+m_3} \\ \eta_1^{-1} & \eta_2^{-1} q^{2\lambda} + A\eta_2 q^{m_1+m_3} & \eta_3^{-1} q^\lambda \end{vmatrix} + o(q^{m_1+m_3}) \\ &= (\varepsilon_1^{-1} \eta_2^{-1} + \varepsilon_3^{-1} \eta_1^{-1} + \varepsilon_2^{-1} \eta_3^{-1}) q^{2\lambda} - \varepsilon_3^{-1} \eta_2^{-1} q^{4\lambda} - A \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_3 \\ \eta_1^{-1} & -\eta_2 \end{vmatrix} q^{m_1+m_3} \\ &\quad + o(q^{m_1+m_3}). \end{aligned}$$

Since  $m_1 > 2\lambda$ , this gives

$$\varepsilon_1^{-1} \eta_2^{-1} + \varepsilon_3^{-1} \eta_1^{-1} + \varepsilon_2^{-1} \eta_3^{-1} = 0. \tag{12-22}$$

Further, if  $4\lambda < m_1 + m_3$ , then  $q^{4\lambda}$  cannot be eliminated. And if  $4\lambda = m_1 + m_3$ , then

$$-\varepsilon_3^{-1}\eta_2^{-1} = A \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_3 \\ \eta_1^{-1} & -\eta_2 \end{vmatrix},$$

which is impossible because  $A$  does not divide a root of unity.

Thus, we have  $4\lambda > m_1 + m_3 = 2m_1 - 2\lambda$ , that is,  $m_1 < 3\lambda$ , proving (12-21). In addition to this, to eliminate  $q^{m_1+m_3}$  we need to have

$$\begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_3 \\ \eta_1^{-1} & -\eta_2 \end{vmatrix} = 0.$$

Together with (12-3) this implies that

$$(\eta_1^{-1}, -\eta_3^{-1}, -\eta_2) = \theta(\varepsilon_1^{-1}, \varepsilon_2^{-1}, \varepsilon_3) \tag{12-23}$$

for some root of unity  $\theta$ .

**12G. Conclusion.** It follows from (12-21) that  $m_3 < \lambda$ , whence

$$m_1 + 2m_3 < m_1 + m_3 + \lambda = m_1 + m_2 < 2m_1.$$

Using this, (12-3), (12-22), and (12-23), we obtain for  $\mathcal{D}(q)$  the value

$$\begin{aligned} & \left| \begin{array}{ccc} 1 & 1 & 1 \\ \varepsilon_1^{-1} & \varepsilon_2^{-1}q^\lambda & \varepsilon_3^{-1}q^{2\lambda} + A\varepsilon_3q^{m_1+m_3} + B\varepsilon_3^2q^{m_1+2m_3} \\ \eta_1^{-1} & \eta_2^{-1}q^{2\lambda} + A\eta_2q^{m_1+m_3} + B\eta_2^2q^{m_1+2m_3} & \eta_3^{-1}q^\lambda \end{array} \right| \\ & \qquad \qquad \qquad + o(q^{m_1+2m_3}) \\ & = -\varepsilon_3^{-1}\eta_2^{-1}q^{4\lambda} - B \begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_3^2 \\ \eta_1^{-1} & -\eta_2^2 \end{vmatrix} q^{m_1+2m_3} + o(q^{m_1+2m_3}). \end{aligned}$$

Arguing as in Section 12F, we obtain from this  $4\lambda > m_1 + 2m_3$  and

$$\begin{vmatrix} \varepsilon_1^{-1} & \varepsilon_3^2 \\ \eta_1^{-1} & -\eta_2^2 \end{vmatrix} = 0,$$

which, together with (12-23), implies that  $\theta = -1$ . It follows that  $\eta_2 = \varepsilon_3$  and  $\eta_3 = \varepsilon_2$ ; together with (12-18) this implies  $g_2 = f_3$  and  $g_3 = f_2$ , contradicting Lemma 8.1.

This completes the proof of impossibility of (12-1). The main lemma is now fully proved.

### Acknowledgments

Yuri Bilu was supported by the Agence National de la Recherche project ‘‘Hamot’’ (ANR 2010 BLAN-0115-01). We thank Bill Allombert, Qing Liu, Pierre Parent, Jonathan Pila, and Thomas Scanlon for useful discussions. We also thank the referee,

who did the hard job of verifying the proof, detected a number of inaccuracies, and made many helpful suggestions.

### References

- [Allombert et al. 2015] B. Allombert, Yu. Bilu, and A. Pizarro-Madariaga, “CM-points on straight lines”, pp. 1–18 in *Analytic number theory*, edited by C. Pomerance and M. Th. Rassias, Springer, 2015. MR Zbl
- [André 1998] Y. André, “Finitude des couples d’invariants modulaires singuliers sur une courbe algébrique plane non modulaire”, *J. Reine Angew. Math.* **505** (1998), 203–208. MR Zbl
- [Bilu et al. 2013] Yu. Bilu, D. Masser, and U. Zannier, “An effective ‘Theorem of André’ for CM-points on a plane curve”, *Math. Proc. Cambridge Philos. Soc.* **154**:1 (2013), 145–152. MR Zbl
- [Bilu et al. 2016] Yu. Bilu, F. Luca, and A. Pizarro-Madariaga, “Rational products of singular moduli”, *J. Number Theory* **158** (2016), 397–410. MR Zbl
- [Breuer 2001] F. Breuer, “Heights of CM points on complex affine curves”, *Ramanujan J.* **5**:3 (2001), 311–317. MR Zbl
- [Cox 1989] D. A. Cox, *Primes of the form  $x^2 + ny^2$ : Fermat, class field theory, and complex multiplication*, Wiley, 1989. MR Zbl
- [Diamond and Shurman 2005] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics **228**, Springer, 2005. MR Zbl
- [Edixhoven 1998] B. Edixhoven, “Special points on the product of two modular curves”, *Compositio Math.* **114**:3 (1998), 315–328. MR Zbl
- [Evertse et al. 1988] J.-H. Evertse, K. Györy, C. L. Stewart, and R. Tijdeman, “On  $S$ -unit equations in two unknowns”, *Invent. Math.* **92**:3 (1988), 461–477. MR Zbl
- [Habegger et al. 2017] P. Habegger, G. Jones, and D. Masser, “Six unlikely intersection problems in search of effectivity”, *Math. Proc. Cambridge Philos. Soc.* **162**:3 (2017), 447–477. MR
- [Ireland and Rosen 1990] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts in Mathematics **84**, Springer, 1990. MR Zbl
- [Kühne 2012] L. Kühne, “An effective result of André–Oort type”, *Ann. of Math. (2)* **176**:1 (2012), 651–671. MR Zbl
- [Kühne 2013] L. Kühne, “An effective result of André–Oort type, II”, *Acta Arith.* **161** (2013), 1–19. MR Zbl
- [Pila 2009] J. Pila, “Rational points of definable sets and results of André–Oort–Manin–Mumford type”, *Int. Math. Res. Not.* **2009**:13 (2009), 2476–2507. MR Zbl
- [Pila 2011] J. Pila, “O-minimality and the André–Oort conjecture for  $\mathbb{C}^n$ ”, *Ann. of Math. (2)* **173**:3 (2011), 1779–1840. MR Zbl
- [Pila and Zannier 2008] J. Pila and U. Zannier, “Rational points in periodic analytic sets and the Manin–Mumford conjecture”, *Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl.* **19**:2 (2008), 149–162. MR Zbl
- [Scanlon 2004] T. Scanlon, “Automatic uniformity”, *Int. Math. Res. Not.* **2004**:62 (2004), 3317–3326. MR Zbl
- [Schlickewei and Wirsing 1997] H. P. Schlickewei and E. Wirsing, “Lower bounds for the heights of solutions of linear equations”, *Invent. Math.* **129**:1 (1997), 1–10. MR Zbl

Communicated by Jonathan Pila

Received 2016-01-02

Revised 2016-11-27

Accepted 2017-03-31



yuri@math.u-bordeaux.fr

*Institut de Mathématiques de Bordeaux,  
Université de Bordeaux et CNRS, Talence, France*

florian.luca@wits.ac.za

*School of Mathematics,  
University of the Witwatersrand, Johannesburg, South Africa*

david.massar@unibas.ch

*Max Planck Institute for Mathematics, Bonn, Germany*

*Mathematisches Institut, Universität Basel, Basel, Switzerland*



# A uniform classification of discrete series representations of affine Hecke algebras

Dan Ciubotaru and Eric Opdam

We give a new and independent parametrization of the set of discrete series characters of an affine Hecke algebra  $\mathcal{H}_v$ , in terms of a canonically defined basis  $\mathcal{B}_{\text{gm}}$  of a certain lattice of virtual elliptic characters of the underlying (extended) affine Weyl group. This classification applies to all semisimple affine Hecke algebras  $\mathcal{H}$ , and to all  $v \in \mathcal{Q}$ , where  $\mathcal{Q}$  denotes the vector group of positive real (possibly unequal) Hecke parameters for  $\mathcal{H}$ . By analytic Dirac induction we define for each  $b \in \mathcal{B}_{\text{gm}}$  a continuous (in the sense of Opdam and Solleveld (2010)) family  $\mathcal{Q}_b^{\text{reg}} := \mathcal{Q}_b \setminus \mathcal{Q}_b^{\text{sing}} \ni v \rightarrow \text{Ind}_D(b; v)$ , such that  $\epsilon(b; v)\text{Ind}_D(b; v)$  (for some  $\epsilon(b; v) \in \{\pm 1\}$ ) is an irreducible discrete series character of  $\mathcal{H}_v$ . Here  $\mathcal{Q}_b^{\text{sing}} \subset \mathcal{Q}$  is a finite union of hyperplanes in  $\mathcal{Q}$ .

In the nonsimply laced cases we show that the families of virtual discrete series characters  $\text{Ind}_D(b; v)$  are piecewise rational in the parameters  $v$ . Remarkably, the formal degree of  $\text{Ind}_D(b; v)$  in such piecewise rational family turns out to be rational. This implies that for each  $b \in \mathcal{B}_{\text{gm}}$  there exists a universal rational constant  $d_b$  determining the formal degree in the family of discrete series characters  $\epsilon(b; v)\text{Ind}_D(b; v)$ . We will compute the canonical constants  $d_b$ , and the signs  $\epsilon(b; v)$ . For certain geometric parameters we will provide the comparison with the Kazhdan–Lusztig–Langlands classification.

1. Motivation and goals	1090
2. Massive pure elliptic virtual characters	1094
3. One-dimensional algebraic families of discrete series representations, and their limits	1103
4. Explicit results; comparison to the Kazhdan–Lusztig–Langlands classification	1113
References	1132

This research was supported in part by the ERC-advanced grant no. 268105 and the EPSRC grant EP/N033922/1. It is a pleasure to thank Xuhua He and Maarten Solleveld for useful discussions and comments.

*MSC2010*: primary 20C08; secondary 22D25, 43A30.

*Keywords*: Affine Hecke algebra, graded affine Hecke algebra, Dirac operator, discrete series representation.

### 1. Motivation and goals

Let  $\mathcal{R} = (X, R_0, Y, R_0^\vee, F_0)$  be a based root datum. In particular,  $X, Y$  are  $\mathbb{Z}$ -lattices of finite rank in perfect duality,  $R_0 \subset X$  is the set of roots,  $R_0^\vee \subset Y$  is the set of coroots, and  $F_0 \subset R_0$  is the set of simple roots. Define the (extended) affine Weyl group  $W := W_0 \ltimes X$ , where  $W_0 = W(R_0)$  is the finite Weyl group associated with the root system  $R_0$ . Let  $R_{0,+} \supset F_0$  denote the positive roots. We denote by  $S_0$  the set of simple reflections of  $W_0$ . Associated to  $\mathcal{R}$  one has a canonical Laurent polynomial algebra  $\Lambda$  generated by invertible ‘‘Hecke parameters’’, and the generic extended affine Hecke algebra  $\mathcal{H}_\Lambda$  over  $\Lambda$  (see, e.g., [Opdam and Solleveld 2010]). Let  $\mathcal{Q}$  be the real vector group of the algebraic torus associated with  $\Lambda$ . If  $\mathbf{v} \in \mathcal{Q}$  then we denote by  $\mathcal{H}_\mathbf{v}$  the corresponding specialization of  $\mathcal{H}_\Lambda$ .

The Hecke algebra  $\mathcal{H}_\mathbf{v}$  has a natural structure of a normalized Hilbert algebra and an abstract Plancherel formula [Opdam 2004]. It is a fundamental question to classify explicitly the irreducible discrete series characters (the simple summands in the Plancherel decomposition) and compute their formal degrees, i.e., the Plancherel mass of the discrete series characters.

For the Hecke algebras  $\mathcal{H}_\mathbf{v}$  with equal parameters of a simply connected root datum, the classification of the irreducible discrete series modules in terms of the Kazhdan–Lusztig–Langlands parameters was obtained in the seminal paper of Kazhdan and Lusztig [1987] and also by Ginzburg [Chriss and Ginzburg 1997]. This classification was generalized later by Lusztig [2002] for the Hecke algebras that occur in relation with the unipotent representations of quasisimple  $p$ -adic groups with connected center. In the case when the  $p$ -adic group is the split form of  $\mathrm{SO}(2n + 1)$ , the parametrization of irreducible discrete series modules was also determined by Waldspurger [2004]. By applying Clifford theory to Kazhdan–Lusztig theory, Reeder [2002] extended the Kazhdan–Lusztig classification to root data of arbitrary isogeny type in the case when the parameters are equal. For unequal parameters unipotent Hecke algebras, this method was carried out recently by Aubert, Baum, Plymen and Solleveld [Aubert et al. 2017]. In the case of the Hecke algebra of affine type  $C_n$ , a different classification in terms of Kato’s ‘‘exotic geometry’’ was offered in [Ciubotaru and Kato 2011].

Using a different, analytic approach, a complete explicit Plancherel decomposition for affine Hecke algebras of arbitrary isogeny and with arbitrary positive parameters was obtained in [Opdam 2004; 2007]. The program was continued in [Opdam and Solleveld 2010], where a classification of irreducible discrete series in this generality is obtained, except that for root data of type  $E$ , the authors had to also rely on certain results from Kazhdan and Lusztig [1987].

In this paper, we give a new and uniform classification of the set of discrete series modules of  $\mathcal{H}_\mathbf{v}$  in terms of certain canonical orthonormal subset  $\mathcal{B}_{\mathrm{gm}}$  of the elliptic

character lattice of  $W$  for arbitrary positive parameters and arbitrary root data, which is independent of the previous classifications, including the Kazhdan–Lusztig classification. We also give algebraic models for the discrete series modules and we study their formal degrees from the perspective of parameter deformations, in particular, we obtain complete and explicit closed formulas for the formal degrees of all irreducible discrete series modules. At several places in our proofs, we rely on [Opdam 2007] and [Opdam and Solleveld 2010] for the classification of the central characters of irreducible discrete series in terms of residual points, on [Opdam 2004] and [Opdam and Solleveld 2009] for the elements of elliptic theory for affine Hecke algebras, and on [Ciubotaru et al. 2014] for several facts about Dirac induction for graded affine Hecke algebras.

**1A. Uniform classification of the discrete series.** Let  $\bar{\mathcal{R}}_{\mathbb{Z}}(W)$  be the lattice of elliptic virtual characters of  $W$ , equipped with the Euler–Poincaré pairing, and let  $\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)$  denote the lattice of elliptic virtual characters of  $\mathcal{H}_v$ . If  $\pi$  is an element of  $\mathcal{R}_{\mathbb{Z}}(\mathcal{H}_v)$ , let us denote by  $\bar{\pi}$  its image in  $\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)$ .

In this paper we will use a basic tool, the so-called “scaling map”:

$$\begin{aligned} \lim_{v \rightarrow 1} : \bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v) &\rightarrow \bar{\mathcal{R}}_{\mathbb{Z}}(W) \\ [\pi] &\rightarrow \left[ \lim_{\epsilon \rightarrow 0} \pi_{v^\epsilon} \right], \end{aligned} \tag{1}$$

where  $\pi_{v^\epsilon} := \pi \circ j_\epsilon^{-1}$ . Here  $j_\epsilon : \mathcal{H}_v^{\text{an}}(U) \rightarrow \mathcal{H}_{v^\epsilon}^{\text{an}}(\sigma_\epsilon(U))$  ( $\epsilon > 0$ ) is the isomorphism between the analytic localizations  $\mathcal{H}_v^{\text{an}}(U)$  and  $\mathcal{H}_{v^\epsilon}^{\text{an}}(\sigma_\epsilon(U))$  of the affine Hecke algebra as introduced in [Opdam 2004, Theorem 5.3]. It is easy to see that the family of isomorphisms  $\{j_\epsilon^{-1}\}_{\epsilon > 0}$  has a well defined limit at  $\epsilon = 0$ , defining a homomorphism  $i_0 : \mathbb{C}[W] \rightarrow \mathcal{H}_v^{\text{an}}(U)$  (see [Solleveld 2012, Proposition 4.1.2]). This explains the existence of the desired “scaling map”  $\lim_{v \rightarrow 1} : \bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v) \rightarrow \bar{\mathcal{R}}_{\mathbb{Z}}(W)$  as in (1). The isomorphisms  $j_\epsilon$  ( $\epsilon > 0$ ) induce isometric isomorphisms [Opdam and Solleveld 2009, Theorem 3.5(b)]:

$$(j_\epsilon^{-1})^* : \bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v) \rightarrow \bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_{v^\epsilon}). \tag{2}$$

Consequently, the limit  $\lim_{v \rightarrow 1}$  of (1) is an isometry too [Opdam and Solleveld 2009, Theorem 3.5(b)].

Let us denote by  $\mathcal{Y}_v \subset \bar{\mathcal{R}}_{\mathbb{Z}}(W)$  the image of this map, and by  $\mathcal{Y}_{v-m} \subset \mathcal{Y}_v$  the image of the sublattice of  $\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)$  of the virtual discrete series characters of  $\mathcal{H}_v$ . Let  $\mathcal{Y}_{\text{gm}} \subset \bar{\mathcal{R}}_{\mathbb{Z}}(W)$  be the smallest sublattice which contains all lattices  $\mathcal{Y}_{v-m}$  (see Definition 2.5). We call  $\mathcal{Y}_{\text{gm}}$  the lattice of *generically massive* elliptic characters of  $W$ , and  $\mathcal{Y}_{v-m}$  the sublattice of *v-massive* elliptic characters of  $W$ .

The lattice  $\mathcal{Y}_{\text{gm}}$  possesses a distinguished orthonormal basis  $\mathcal{B}_{\text{gm}}$  characterized by a positivity property to be explained below. To each  $b \in \mathcal{B}_{\text{gm}}$  we will assign a

subset (nonempty by definition)  $\mathcal{Q}_b^{\text{reg}} \subset \mathcal{Q}$  of the space of parameters by:

$$\mathcal{Q}_b^{\text{reg}} := \{ \mathbf{v} \in \mathcal{Q} \mid \exists \text{ an irreducible discrete series } \pi \text{ of } \mathcal{H}_{\mathbf{v}} \text{ such that } \lim_{\epsilon \rightarrow 0} \overline{\pi_{\mathbf{v}^\epsilon}} = b \}.$$

According to [Opdam and Solleveld 2010], the complement  $\mathcal{Q}_b^{\text{sing}}$  of  $\mathcal{Q}_b^{\text{reg}}$  is a union of finitely many hyperplanes (depending on  $b$ ). For  $y \in \mathcal{Y}_{\text{gm}}$  in general we put  $\mathcal{Q}_y^{\text{reg}} := \bigcap_{b \in \text{Supp}(y)} \mathcal{Q}_b^{\text{reg}}$ . Combining with the technique of analytic Dirac induction (introduced in [Ciubotaru et al. 2014] in the context of graded affine Hecke algebras) we can associate a family of virtual discrete series characters

$$\mathcal{Q}_y^{\text{reg}} \ni \mathbf{v} \rightarrow \text{Ind}_D(y; \mathbf{v}) \in \mathcal{R}_{\mathbb{Z}}(\mathcal{H}_{\mathbf{v}})$$

(called the Dirac induction of  $y$  at  $\mathbf{v}$ , see Definition 2.7), which depends linearly on  $y$ , for each fixed  $\mathbf{v} \in \mathcal{Q}_y^{\text{reg}}$ . If  $b \in \mathcal{B}_{\text{gm}}$  and  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$  then  $\text{Ind}_D(b; \mathbf{v})$  is an irreducible character up to a sign, characterized by the property  $\lim_{\epsilon \rightarrow 0} \overline{(\text{Ind}_D(b; \mathbf{v}^\epsilon))} = b$ . We will prove (see Proposition 3.8) that the family  $\text{Ind}_D(y; \mathbf{v})$  depends continuously on  $\mathbf{v} \in \mathcal{Q}_y^{\text{reg}}$  in the sense of [Opdam and Solleveld 2010]. The ‘‘Vogan conjecture’’ (see [Ciubotaru et al. 2014]) allows one to compute the generic central character  $W_0 r_b$  of  $\text{Ind}_D(b)$  explicitly, where  $r_b \in T_\Lambda := \text{Hom}(X, \Lambda^\times)$  is a *generic residual point* in the sense of [Opdam and Solleveld 2010].

To such an orbit of generic residual points  $W_0 r_b$  we associated in [Opdam and Solleveld 2010] an explicit rational function  $m_b^{\mathcal{Q}} := m_{W_0 r_b}$  on  $\mathcal{Q}$  which is regular on  $\mathcal{Q}$ , and with the property that  $\mathcal{Q}_b^{\text{reg}} = \{ \mathbf{v} \in \mathcal{Q} \mid m_b(\mathbf{v}) \neq 0 \}$ .

Let  $\mathcal{R}_{\mathbb{Z}, \text{temp}}(\mathcal{H}_{\mathbf{v}})$  denote the Grothendieck group of finite-dimensional tempered  $\mathcal{H}_{\mathbf{v}}$ -representations and let  $\overline{\mathcal{R}}_{\mathbb{Z}, \text{temp}}(\mathcal{H}_{\mathbf{v}})$  denote the image of  $\mathcal{R}_{\mathbb{Z}, \text{temp}}(\mathcal{H}_{\mathbf{v}})$  in  $\overline{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_{\mathbf{v}})$ . As a consequence of the parabolic Langlands classification, it is easy to see that  $\overline{\mathcal{R}}_{\mathbb{Z}, \text{temp}}(\mathcal{H}_{\mathbf{v}}) = \overline{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_{\mathbf{v}})$ . Extend the notion of formal degree  $\text{fdeg}$  linearly to  $\mathcal{R}_{\mathbb{Z}, \text{temp}}(\mathcal{H}_{\mathbf{v}})$ . Observe that in this way, the function  $\text{fdeg}$  naturally descends to  $\overline{\mathcal{R}}_{\mathbb{Z}, \text{temp}}(\mathcal{H}_{\mathbf{v}})$ .

**Theorem 1.1.** *Retain the previous notation.*

(a)  $\mathcal{Y}_{\text{gm}}$  has a **unique orthonormal basis**  $\mathcal{B}_{\text{gm}}$  such that for all  $b \in \mathcal{B}_{\text{gm}}$ , and for all  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$ ,  $d_b(\mathbf{v}) := m_b(\mathbf{v})^{-1} \text{fdeg}(\overline{\text{Ind}_D(b; \mathbf{v})}) > 0$ .

(b)  $\overline{\text{Ind}_D(b; \mathbf{v})}$  is represented by a virtual character  $\text{Ind}_D(b; \mathbf{v})$  of  $\mathcal{H}_{\mathbf{v}}$  which is plus or minus an irreducible discrete series.

(c) The central character of  $\text{Ind}_D(b; \mathbf{v})$  is the specialization at  $\mathbf{v}$  of a  $W_0$ -orbit of generic residual points  $W_0 r_b$ , with  $r_b \in T_\Lambda := \text{Hom}(X, \Lambda^\times)$ .

(d) The family  $\text{Ind}_D(b; \mathbf{v})$  depends continuously on  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$  (in the sense of [Opdam and Solleveld 2010]).

(e) For all  $b \in \mathcal{B}_{\text{gm}}$ , the signature function  $\mathcal{Q}_b^{\text{reg}} \ni \mathbf{v} \rightarrow \epsilon(b; \mathbf{v}) \in \{ \pm 1 \}$  such that  $\epsilon(b; \mathbf{v}) \text{Ind}_D(b; \mathbf{v})$  is an irreducible discrete series character, is locally constant.

(f) For each  $\mathbf{v} \in \mathcal{Q}$ , define  $\mathcal{B}_{\mathbf{v}-m} = \{b \in \mathcal{B}_{\text{gm}} \mid m_b(\mathbf{v}) \neq 0\}$ . The assignment

$$\mathcal{B}_{\mathbf{v}-m} \ni b \rightarrow \epsilon(b; \mathbf{v}) \text{Ind}_D(b; \mathbf{v})$$

yields a canonical bijection between  $\mathcal{B}_{\mathbf{v}-m}$  and the set of irreducible discrete series characters of  $\mathcal{H}_{\mathbf{v}}$ .

(g) For all  $b \in \mathcal{B}_{\text{gm}}$ :  $d_b(\mathbf{v}) = d_b$  is **independent** of  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$  (where  $d_b(\mathbf{v})$  is the positive function defined in (a)), and  $d_b \in \mathbb{Q}_+$ . In other words, for all  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$ ,

$$\text{fdeg}(\text{Ind}_D(b; \mathbf{v})) = d_b m_b(\mathbf{v})$$

(a rational function of  $\mathbf{v}$ , regular in all points of  $\mathcal{Q}$ , with zero locus  $\mathcal{Q}_b^{\text{sing}}$ ).

This represents first of all a new classification of the discrete series of  $\mathcal{H}_{\mathbf{v}}$ , which is uniform in the sense that it applies to all irreducible root data and all parameters  $\mathbf{v} \in \mathcal{Q}$ . It is explicit in the sense that for cases where a classification of discrete series has been given in other terms in the literature (e.g., in terms of Kazhdan–Lusztig–Langlands parameters) the comparison can be explicitly given. The main tool for making this uniform classification explicit in specific cases is the Hecke algebra version of the “Vogan conjecture” established first in [Barbasch et al. 2012] and sharpened to the version that we need here in [Ciubotaru et al. 2014]. This enables the explicit computation in terms of  $b \in \mathcal{B}_{\text{gm}}$  of the central character  $W_0 r_b$ . More precisely, motivated by the ideas of Vogan and Huang and Pandžić for  $(\mathfrak{g}, K)$ -modules of real reductive groups, [Barbasch et al. 2012] introduced the notion of Dirac cohomology of a finite dimensional graded Hecke algebra module  $M$ . The Dirac cohomology is a finite dimensional representation of the pin double cover of the finite Weyl group and the main idea is that if  $M$  has a central character (in particular, if it is a simple module), then the Dirac cohomology, if nonzero, determines its central character. In the present setting, to every  $b \in \mathcal{B}_{\text{gm}}$ , one can attach canonically an irreducible representation of the pin double cover of an “endoscopic” subgroup of  $W_0$  in such a way that this representation occurs in the Dirac cohomology of the graded Hecke algebra module supported on  $\text{Ind}_D(b; \mathbf{v})$ , and this in turn, using the idea just explained, determines the central character of  $\text{Ind}_D(b; \mathbf{v})$ .

Let  $b \in \mathcal{B}_{\text{gm}}$ , let  $C \subset \mathcal{Q}_b$  be a connected component (an open cone in  $\mathcal{Q}$ ), and let  $\mathbf{v}_0 \in \partial(C) \subset \mathcal{Q}_b^{\text{sing}}$ . An underlying issue is the behavior of the families  $\text{Ind}_D(b; \mathbf{v})$  near  $\mathbf{v}_0 \in \mathcal{Q}_b^{\text{sing}}$ . These questions play a technical role in the proof of the above Theorem, and are of independent interest. To be sure, the family  $\text{Ind}_D(b; \mathbf{v})$  is *not* continuous in any neighborhood of  $\mathbf{v}_0$ , which is one of the reasons that Theorem 1.1(g) is surprising and noteworthy. We will show that there is a sense in which the family  $\text{Ind}_D(b; \mathbf{v})$  can be extended along smooth curves in  $\mathcal{Q}_{\mathbb{C}}$  as an algebraic family of genuine characters, provided one lifts the condition that the

characters in the family are discrete series characters. More precisely, consider an affine smooth curve  $\mathcal{C} \subset \mathcal{Q}_{\mathbb{C}}$  which intersects  $\bar{C}$  in a real curve containing  $\mathbf{v}_0 \in \bar{C}$ . Then  $\mathcal{C} \cap C \ni \mathbf{v} \rightarrow \text{Ind}_D(b; \mathbf{v})$  extends as a rational family of generically irreducible genuine characters to a finite branched covering  $\tilde{\mathcal{C}}$  of  $\mathcal{C}$ . Importantly, this family is unramified at points of  $\mathcal{C} \cap \bar{C}$ , and regular at the points of  $\tilde{\mathcal{C}}$  lying above  $\mathbf{v}_0$ . In particular one can define a limit  $\text{Ind}_D(b, C; \mathbf{v}_0)$  at  $\mathbf{v}_0$  of the family of discrete series along  $\mathcal{C}$  “from the direction of  $C$ ”. This “limit of discrete series” is a tempered character, which depends on  $(C, \mathbf{v}_0)$ . We expect that it does not depend on the choice of  $\mathcal{C}$ . Notice that if  $\mathcal{C}$  intersects the boundary of  $C$  transversally at  $\mathbf{v}_0$  then  $\mathcal{C}$  will also intersect the chamber  $C_-$  opposite to  $C$  with respect to  $\mathbf{v}_0$ , and thus there exists also a limit  $\text{Ind}_D(b, C_-, \mathcal{C}; \mathbf{v})$ . It would be interesting to investigate how these two limits are related to each other, in terms of the relevant analytic R-group.

## 2. Massive pure elliptic virtual characters

### 2A. Elliptic virtual characters of affine Weyl groups.

**2A1. Elliptic virtual characters of affine Weyl groups.** We identify  $X$  with the normal subgroup  $\{e\} \times X \subset W$ , and  $W_0$  with the subgroup  $W_0 \times \{0\}$ . Let  $E = \mathbb{R} \otimes X$ ; then  $W$  acts naturally on the Euclidean space  $E$  as a group of affine isometries.

The lattice  $X \subset W$  is the normal subgroup of elements whose conjugacy class is finite. A centralizer of an element  $x \in X$  is called a *Levi subgroup* of  $W$ . There are finitely many Levi subgroups of  $W$ , and this collection is conjugation invariant. Each Levi subgroup  $L \subset W$  is itself an affine Weyl group  $L = W_L \ltimes X$ , where  $W_L$  is a Levi subgroup of  $W_0$  (the isotropy group of  $x$  in  $W_0$ ). Then  $W_L$  is a Coxeter group, and has a unique set of simple reflections  $S_L$  consisting of reflection  $r_\alpha \in W_0$  with  $\alpha \in R_{0,+}$ . Every Levi subgroup is conjugate to a standard Levi subgroup. We call  $L$  *standard* if  $S_L \subset S_0$ .

An element  $w \in W$  is called *elliptic* if  $w$  does not belong to any proper Levi subgroup  $L \subset W$  (see [Opdam and Solleveld 2009]). The following are easily seen to be equivalent:

- (a)  $w \in W$  is elliptic.
- (b) The canonical image of  $w$  in  $W_0$  is elliptic (with respect to the action of  $W_0$  on  $E$ ).
- (c) The centralizer of  $w$  in  $W$  is finite.
- (d) The conjugacy class of  $w$  is a union of left (or equivalently right) cosets of a sublattice of  $X$  of maximal rank.
- (e)  $w$  has isolated fixed points in  $E$ .
- (f)  $w$  has a unique fixed point in  $E$ .



The set of elliptic elements is a finite union of conjugacy classes.

An (extended) *parahoric subgroup* of  $W$  is the pointwise stabilizer of an affine subspace in  $E$ . Given  $e \in E$  consider the isotropy group  $W_e \subset W$ . Then  $W_e$  has a natural faithful linear action on  $T_e(T) \simeq E$ , and an element  $w \in W_e$  is said to be elliptic if  $w$  is elliptic in  $W_e$  with respect to the action on  $T_e(T)$ , in the sense of Reeder [2001].

We denote by  $\mathcal{R}_{\mathbb{Z}}(W)$  the Grothendieck group of the category of  $\mathbb{C}[W]$ -modules of finite length, and by  $\mathcal{R}_{\mathbb{C}}(W)$  its complexification. The character map defines an embedding of  $\mathcal{R}_{\mathbb{C}}(W)$  into the space of complex class functions on  $W$ . Let  $\bar{\mathcal{R}}_{\mathbb{C}}(W)$  denote the complex valued class functions on  $W$  supported on the set of elliptic conjugacy classes. When we compose the character map with the restriction map we obtain a surjective map from  $\mathcal{R}_{\mathbb{C}}(W)$  to  $\bar{\mathcal{R}}_{\mathbb{C}}(W)$ . In [Opdam and Solleveld 2009] it was shown that the kernel of this map is spanned by the set of characters which are induced from proper Levi subgroups. We will identify  $\bar{\mathcal{R}}_{\mathbb{C}}(W)$  with this quotient of  $\mathcal{R}_{\mathbb{C}}(W)$ . We denote by  $\bar{\mathcal{R}}_{\mathbb{Z}}(W) \subset \mathcal{R}_{\mathbb{C}}(W)$  the image of  $\mathcal{R}_{\mathbb{Z}}(W)$ , and refer to this lattice as the group of elliptic virtual characters.

There exists a unique conjugation invariant measure [Opdam and Solleveld 2009, Theorem 3.3(c)]  $\mu_{\text{ell}}$  on  $W$ , which is supported on the elliptic conjugacy classes, and which is defined by  $\mu_{\text{ell}}((1-w)(X)) = |W_0|^{-1}$  if  $(1-w)(X)$  has maximal rank, and  $\mu_{\text{ell}}((1-w)(X)) = 0$  otherwise. This defines an integral positive semidefinite Hermitian pairing, the *elliptic pairing*  $\text{EP}_W$  on  $\mathcal{R}_{\mathbb{C}}(W)$  by integrating  $f\bar{g}$  over  $W$  with respect to the measure  $\mu_{\text{ell}}$ . The Euler–Poincaré pairing on  $\mathcal{R}_{\mathbb{Z}}(W)$  is expressed by  $\text{EP}_W$ . More precisely [Opdam and Solleveld 2009], given virtual representations  $U$  and  $V$  of  $W$ , with characters  $\chi_U$  and  $\chi_V$  respectively, one has

$$\text{EP}_W(U, V) = \int_{w \in W} \chi_U(w) \overline{\chi_V(w)} d\mu_{\text{ell}}(w) = \sum_{i=0}^{\infty} (-1)^i \dim \text{Ext}_W^i(U, V). \quad (3)$$

In particular  $\text{EP}_W$  is integral on  $\mathcal{R}_{\mathbb{Z}}(W)$ . By [Opdam and Solleveld 2009] the radical of  $\text{EP}_W$  is exactly the kernel of the quotient map  $\mathcal{R}_{\mathbb{C}}(W) \rightarrow \bar{\mathcal{R}}_{\mathbb{C}}(W)$ , hence in particular  $\text{EP}_W$  descends to a positive definite integral inner product on  $\bar{\mathcal{R}}_{\mathbb{Z}}(W)$ .

The Weyl group  $W_0$  acts naturally on the algebraic torus  $T = \text{Hom}(X, \mathbb{C}^\times)$ . Clearly  $w \in W_0$  is elliptic if and only if  $w$  has finitely many fixed points on  $T$ . It was shown in [Opdam and Solleveld 2009] that the set of elliptic conjugacy classes of  $W$  and the set of  $W_0$ -orbits of pairs  $(C, t)$  with  $C \in W_t$  an elliptic conjugacy class (with respect to the faithful action of  $W_t$  on  $T_t(T)$ ) and  $t \in T$  have the same cardinality. Here the action of  $W_0$  is defined by  $w(C, t) = (wCw^{-1}, wt)$ .

Elements  $f \in \bar{\mathcal{R}}_{\mathbb{C}}(W)$  can be viewed as tracial functionals  $f \in \mathbb{C}[W]^*$  supported on the set of elliptic conjugacy classes. Hence the center

$$Z(\mathbb{C}[W]) = \mathbb{C}[X]^{W_0} \subset \mathbb{C}[W]$$

acts on  $\bar{\mathcal{R}}_{\mathbb{C}}(W)$  by multiplication, i.e.,  $z.f(a) := f(za)$  for all  $z \in Z(\mathbb{C}[W])$ ,  $f \in \bar{\mathcal{R}}(W)$ , and  $a \in \mathbb{C}[W]$ . Using Mackey theory we showed in [Opdam and Solleveld 2009] that there exists an isometric isomorphism

$$\text{Ind} := \bigoplus_{s \in W_0 \setminus T} \text{Ind}_s : \bigoplus_{s \in W_0 \setminus T} \bar{\mathcal{R}}_{\mathbb{C}}(W_s) \rightarrow \bar{\mathcal{R}}_{\mathbb{C}}(W). \tag{4}$$

Here  $\bar{\mathcal{R}}_{\mathbb{C}}(W_s)$  is equipped with the elliptic inner product [Reeder 2001] for the isotropy group  $W_s$  with respect to its natural faithful representation on the tangent space  $T_s(T)$  of  $T$  at  $s$ , and the direct sum is an orthogonal direct sum. Furthermore  $\text{Ind}_s$  is the linear map on  $\bar{\mathcal{R}}_{\mathbb{C}}(W_s)$  realized by the Mackey induction functor. The image of  $\text{Ind}_s$  equals

$$\text{Im}(\text{Ind}_s) = \bar{\mathcal{R}}_{\mathbb{C}}(W)_{W_0s}, \tag{5}$$

the  $Z(\mathbb{C}[W])$ -eigenspace in  $\bar{\mathcal{R}}_{\mathbb{C}}(W)$  with eigenvalue  $W_0s$ , hence (4) gives the orthogonal decomposition of  $\bar{\mathcal{R}}_{\mathbb{C}}(W)$  as a direct sum of  $Z(\mathbb{C}[W])$ -eigenspaces. By Mackey theory for  $W = W_0 \times X$  this decomposition is compatible with the integral structure. It follows that we also have an orthogonal direct sum decomposition of lattices:

$$\text{Ind} := \bigoplus_{s \in W_0 \setminus T} \text{Ind}_s : \bigoplus_{s \in W_0 \setminus T} \bar{\mathcal{R}}_{\mathbb{Z}}(W_s) \rightarrow \bar{\mathcal{R}}_{\mathbb{Z}}(W). \tag{6}$$

**Definition 2.1** ([Ciubotaru et al. 2014]). Let  $\mathcal{X}$  be a  $\mathbb{Z}$ -lattice equipped with an integral positive definite bilinear form. An element  $x \in \mathcal{X}$  is called *pure* if  $x$  is not a nontrivial orthogonal sum in  $\mathcal{X}$ .

**2B. Affine Hecke algebras and Dirac induction.** Unfortunately we do not know how to define a Dirac-type operator for affine Hecke algebras. Using appropriate versions of Lusztig’s reduction theorems and results of [Ciubotaru et al. 2014; Opdam and Solleveld 2009; 2010], we can nevertheless define Dirac-type induction from a well-defined subspace of the space of elliptic characters of the affine Weyl group to the space of virtual discrete series characters of  $\mathcal{H}_v$ .

For affine Hecke algebras we use the setup and notation of [Opdam and Solleveld 2010, Section 2]. Thus given a based root datum  $\mathcal{R}$  let  $\Lambda$  denote the canonically associated Laurent polynomial ring of Hecke parameters  $v(s)$ , and let  $\mathcal{H}_{\Lambda} = \mathcal{H}_{\Lambda}(\mathcal{R})$  denote the associated affine Hecke algebra defined over  $\Lambda$ . Let  $\mathcal{Q}_c = \text{Hom}(\Lambda, \mathbb{C})$ , the group of complex points of an algebraic torus. Let  $\mathcal{Q} \subset \mathcal{Q}_c$  be the real vector group, the identity component of the group of real points.

We denote the canonical  $\Lambda$ -basis of  $\mathcal{H}_{\Lambda}$  by  $N_w$  (with  $w \in W$ ), where the normalization is such that for affine simple reflections  $s \in S$  we have

$$(N_s - v(s))(N_s + v(s)^{-1}) = 0. \tag{7}$$

An element  $v \in \mathcal{Q}$  is determined by its coordinates  $v(s) := v(s)(v)$  with  $s \in S$ . We denote by  $\mathcal{H}_v = \mathcal{H}_\Lambda(\mathcal{R}) \otimes \mathbb{C}_v$  the corresponding specialized affine Hecke algebra, specialized at  $v$ .

According to the Bernstein–Lusztig–Zelevinski presentation of  $\mathcal{H}_\Lambda$  we have a unique abelian subalgebra  $\mathcal{A} = \mathbb{C}[\theta_x \mid x \in X] \subset \mathcal{H}$  such that  $\theta_x = N_x$  if  $x \in X$  is dominant. Then  $\mathcal{A} \simeq \mathbb{C}[X]$ , and the center  $Z(\mathcal{H}_\Lambda)$  is equal to  $A^{W_0} \simeq \Lambda[X]^{W_0}$ .

Given  $v \in \mathcal{Q}$ , consider the quotient  $\bar{\mathcal{R}}_{\mathbb{C}}(\mathcal{H}_v)$  of the complexified Grothendieck ring  $\mathcal{R}_{\mathbb{C}}(\mathcal{H}_v)$  of finite length representations of  $\mathcal{H}_v$  by the subspace generated by the properly parabolically induced representations. By [Ciubotaru and He 2014] this is a finite dimensional complex vector space for all  $v \in \mathcal{Q}$ . Notice also that  $\bar{\mathcal{R}}_{\mathbb{C}}(\mathcal{H}_{v=1}) = \bar{\mathcal{R}}_{\mathbb{C}}(W)$ . The image of the lattice of virtual characters is denoted by  $\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)$ . The center  $Z(\mathcal{H}_v)$  acts on  $\bar{\mathcal{R}}_{\mathbb{C}}(\mathcal{H}_v)$ , and by Schur’s lemma we have a decomposition

$$\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v) = \bigoplus_{t \in W_0 \backslash T} \bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)_{W_0 t}. \tag{8}$$

If  $v \in \mathcal{Q}$  is a positive parameter then [Opdam and Solleveld 2009] asserts that  $\mathcal{H}_v$  has finite global dimension, and we define an integral bilinear form  $\text{EP}_{\mathcal{H}}$  on  $\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)$  by

$$\text{EP}_{\mathcal{H}}(U, V) = \sum_{i=0}^{\infty} (-1)^i \dim \text{Ext}_{\mathcal{H}_v}^i(U, V). \tag{9}$$

As mentioned above, there exists [Opdam and Solleveld 2009] a “scaling map”  $\lim_{v \rightarrow 1} : \bar{\mathcal{R}}_{\mathbb{C}}(\mathcal{H}_v) \rightarrow \bar{\mathcal{R}}_{\mathbb{C}}(W)$  which is an isometry. In particular  $\text{EP}_{\mathcal{H}}$  is itself symmetric and positive semidefinite. One way to understand  $\lim_{v \rightarrow 1}$  is via Lusztig’s reduction results to graded affine Hecke algebras, combined with Clifford theory, and the restriction map from graded affine Hecke algebra representations to representations of the corresponding Weyl group. This is what we will look into in the next paragraph.

**2B1. Clifford theory for extensions of graded affine Hecke algebras.** Consider  $v \in \mathcal{Q}$ , and let  $V$  be an irreducible representation of  $\mathcal{H}_v$ . Recall the polar decomposition  $T = T_u T_v$ , where  $T_u = \text{Hom}(X, S^1)$  and  $T_v = \text{Hom}(X, \mathbb{R}_{>0})$ . Let the central character of  $V$  be  $W_0 t$  with  $t = sc$  where  $s \in T_u$  is a unitary element, and  $c \in T_v$ . Let  $F_{s,1}$ ,  $R_{s,1}$  and  $\Gamma_s$  be as in [Opdam and Solleveld 2010, Definition 2.5], so that the isotropy group  $W_s$  of  $s$  in  $W_0$  equals  $W_s = W(R_{s,1}) \rtimes \Gamma_s$ , and  $\alpha(t) > 0$  for all  $\alpha \in R_{s,1}$ . We recall that  $\Gamma_s$  is a finite abelian group, acting on  $F_{s,1}$  by diagram automorphisms preserving  $k_{s,1}$ . Lusztig’s reduction theorems [1989a] in the version discussed in [Opdam and Solleveld 2010, Theorems 2.6 and 2.8, Corollary 2.10] imply that the category of finite dimensional representations of  $\mathcal{H}_v$  with central character  $W_0 t$  is equivalent to the category of finite dimensional representations

of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma(t)$  with real central character  $W(R_{s,1})\xi$ . Here  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$  is the graded affine Hecke algebra as defined in [Opdam and Solleveld 2010, Section 2],  $\xi \in T_s(T)$  is the unique vector in the real span of  $R_{s,1}^\vee$  such that  $\alpha(t) = e^{\alpha(\xi)}$  for all  $\alpha \in R_{s,1}$  and  $\Gamma(t) \subset \Gamma_s$  is the isotropy group of the central character  $W(R_{s,1})\xi$  of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$ .

Clifford theory [Ram and Ramage 2003] for the crossed product

$$\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s$$

says that the irreducible characters of this algebra are obtained as follows. Let  $U$  be an irreducible representation of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$ . Let  $\Gamma_U \subset \Gamma_s$  be the isotropy subgroup for the equivalence class  $[U]$  of irreducible representations of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$ . Then twisting  $U$  by elements of  $\Gamma_U$  equips  $U$  with a representation of a twisted group algebra  $\mathbb{C}[\Gamma_U; \eta_U]$  with respect to a 2-cocycle  $\eta_U$  of  $\Gamma_U$  with values in  $\mathbb{C}^\times$ . Consider a simple module  $M$  of  $\mathbb{C}[\Gamma_U; \eta_U^{-1}]$ , then

$$N_{\mathbb{H}}(U, M) := \text{Ind}_{\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_U}^{\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s} (U \otimes M)$$

is an irreducible  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s$ -module, and all its irreducible modules are equivalent to such a module. Moreover,  $N_{\mathbb{H}}(U, M) \simeq N_{\mathbb{H}}(U', M')$  if and only if  $U' \simeq U \circ \gamma^{-1}$  for some  $\gamma \in \Gamma_s$ , and  $M' \simeq M \circ \gamma^{-1}$ .

Observe that when  $U$  has central character  $W(R_{s,1})\xi$  then  $\Gamma_U \subset \Gamma(t)$ . Thus Clifford theory implies that the set of irreducible modules of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s$  with central character  $W_s\xi$  is in natural bijection with the set of irreducible modules of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma(t)$  with central character  $W(R_{s,1})\xi$ . In fact it follows from the proof of Lusztig’s reduction theorem that this bijection between the respective sets of irreducibles arises from a Morita equivalence of the two algebras, formally completed at the appropriate central characters  $W_s\xi$  and  $W(R_{s,1})\xi$  respectively. Therefore, by the above, the category of finite dimensional representations of  $\mathcal{H}_v$  with central character  $W_{0t}$  is naturally equivalent with the category of finite dimensional representations of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s$  with real central character  $W_s\xi$ . In particular we have a natural isomorphism

$$\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)_{W_{0t}} \simeq \bar{\mathcal{R}}_{\mathbb{Z}}(\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s)_{W_s\xi}. \tag{10}$$

It is an interesting question what the central support of  $\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)$  is. Clearly, if  $\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)_{W_{0t}} \neq 0$  then, by the above, one has  $T_s(E)^{W_s} = 0$ .

Since  $\mathbb{C}[W_s] = \mathbb{C}[W(R_{s,1})] \rtimes \Gamma_s$ , we have a similar description of the set of irreducibles of  $\mathbb{C}[W_s]$  as modules of the form  $N_{W_s}(X, M)$  where  $X$  is an irreducible for  $W(R_{s,1})$ .

The restriction functor

$$\text{Res}_{W_s}: \mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s\text{-modules} \rightarrow \mathbb{C}[W_s] = \mathbb{C}[W(R_{s,1})] \rtimes \Gamma_s\text{-modules},$$

induces a homomorphism on the level of the Grothendieck groups of representations of finite length. Via the above correspondences, the “scaling map”  $\lim_{\mathbf{v} \rightarrow 1}$  (more precisely,  $\lim_{\epsilon \rightarrow 0} \pi_{\mathbf{v}^\epsilon}$ ) corresponds to taking the limit  $\epsilon \rightarrow 0$  of the family of twists by linear scaling isomorphisms,

$$\psi_\epsilon : \mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s \rightarrow \mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; \epsilon k_s) \rtimes \Gamma_s,$$

defined by  $\phi_\epsilon(\xi) = \epsilon^{-1}\xi$ . This is the restriction map  $\text{Res}_{W_s}$ . In particular we see:

**Corollary 2.2.** *The map  $[\pi] \rightarrow \lim_{\epsilon \rightarrow 0} [\pi_{\mathbf{v}^\epsilon}]$  respects the lattices of virtual characters, and defines an isometric map  $\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_{\mathbf{v}}) \rightarrow \bar{\mathcal{R}}_{\mathbb{Z}}(W)$  sending  $\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_{\mathbf{v}})_{W_0 t}$  to  $\bar{\mathcal{R}}_{\mathbb{Z}}(W)_{W_0 s}$ , where  $t = sc \in T_u T_v$  as before. More precisely, if  $\pi$  corresponds to the module  $U$  of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s$  via (10), and  $b_s = [U|_{W_s}]$ , then  $\lim_{\epsilon \rightarrow 0} [\pi_{\mathbf{v}^\epsilon}] = \text{Ind}_s(b_s)$ .*

**2B2. Residual points.** Let  $R_1$  be the reduced root subsystem of the inmultiplicable roots of the possibly nonreduced root system

$$R_{\text{nr}} = R_0 \cup \{2\alpha \mid \alpha^\vee \in 2Y \cap R_0^\vee\}. \tag{11}$$

For  $\beta \in R_{\text{nr}}$ , define the parameters  $v_{\beta^\vee}$  in terms of the  $v(s)$  as in [Opdam and Solleveld 2010, (7), (8)]. For every  $\mathbf{v} \in \mathcal{Q}$ , recall the Macdonald  $c$ -function,  $c = \prod_{\alpha \in R_{1,+}} c_\alpha$ , a rational function on  $T$ , where

$$c_\alpha(t, \mathbf{v}) = \frac{(1 + v_{\alpha^\vee}^{-1} \alpha(t)^{-\frac{1}{2}})(1 - v_{\alpha^\vee}^{-1} v_{2\alpha^\vee}^{-2} \alpha(t)^{-\frac{1}{2}})}{1 - \alpha(t)^{-1}}. \tag{12}$$

If  $\alpha \in R_1 \setminus R_0$  then  $\alpha/2$  is a character of  $T$ ; however, if  $\alpha \in R_0 \cap R_1$  then  $v_{2\alpha^\vee} = 1$ , and we interpret the numerator of  $c_\alpha$  as  $(1 - v_{\alpha^\vee}^{-2} \alpha(r)^{-1})$ . Thus for all  $\alpha \in R_1$ , the expression for  $c_\alpha$  defines a rational function on  $T$  indeed. Set  $\eta(t) = (c(t)c(t^{-1}))^{-1}$ . Define the pole order  $i_{\{r\}}$  of  $\eta$  at  $r \in T$  as in [Opdam and Solleveld 2010, (34)]. By [Opdam 2007, Theorem 6.1],  $i_{\{r\}} \geq \text{rk}(R_0)$  for all  $r \in T$ .

**Definition 2.3** ([Opdam and Solleveld 2010, Definitions 2.39 and 2.40]). An element  $r \in T$  is called a *residual point* of  $(\mathcal{R}, \mathbf{v})$  if  $i_{\{r\}} = \text{rk}(R_0)$ . The set of  $(\mathcal{R}, \mathbf{v})$ -residual points is denoted by  $\text{Res}(\mathcal{R}, \mathbf{v})$ .

A  $\mathcal{Q}_c$ -valued point  $r \in T_\Lambda$  is called a  $(\mathcal{Q})$ -generic residual point of  $\mathcal{R}$  if there exists an open dense subset  $U \subset \mathcal{Q}$  such that the points  $r(\mathbf{v}) \in \text{Res}(\mathcal{R}, \mathbf{v})$  for all  $\mathbf{v} \in U$ . The set of generic residual points of  $\mathcal{R}$  is denoted by  $\text{Res}(\mathcal{R})$  (or  $\text{Res}(\mathcal{R}, \mathcal{Q})$  if confusion is possible).

Let  $r$  be a  $\mathcal{Q}$ -generic residual point. As in [Opdam and Solleveld 2010, (40)], we define the mass function  $m_{W_0 r}$  as the rational function on  $\mathcal{Q}$  defined by

$$m_{W_0 r} = m_{W_0 r}^{\mathcal{Q}} = \frac{\prod'_{\alpha \in R_1} (\alpha(r)^{-1} - 1)}{\prod'_{\alpha \in R_1} (v_{\alpha^\vee}^{-1} \alpha(r)^{-\frac{1}{2}} + 1) \prod'_{\alpha \in R_1} (v_{\alpha^\vee}^{-1} v_{2\alpha^\vee}^{-2} \alpha(r)^{-\frac{1}{2}} - 1)}. \tag{13}$$

Here  $\prod'$  means that the factors which are identically zero as functions on  $\mathcal{Q}$  are omitted. The function  $m_{W_0 r}$  is regular on  $\mathcal{Q}$  (see [Opdam and Solleveld 2010, Theorem 2.60, Corollary 4.4, Theorem 4.6]), hence, in particular, continuous. Comments similar to those above concerning the interpretation of the roots  $\alpha(r)^{-\frac{1}{2}}$  apply. Observe that the expression in (13) is independent of the choice of representative  $r$  in its  $W_0$ -orbit.

We will also need the related notions for the graded affine Hecke algebra. Let  $R_1 \subset V^*$  be a semisimple reduced root system and let  $\mathcal{K}$  be the space of  $W_0$ -invariant real valued functions on  $R_1$ .

**Definition 2.4** ([Heckman and Opdam 1997; Opdam and Solleveld 2010, Definition 2.55]). For  $k \in \mathcal{K}$ , a point  $h \in V$  is called  $(R_1, k)$ -residual if

$$|\{\alpha \in R_1 \mid \alpha(h) = k_\alpha\}| = |\{\alpha \in R_1 \mid \alpha(h) = 0\}| + \dim(V). \tag{14}$$

We denote by  $\text{Res}^{\text{lin}}(R_1)$  the set of linear maps  $\xi : \mathcal{K} \rightarrow V$  such that for almost all  $k$ , the point  $\xi(k) \in V$  is  $(R_1, k)$ -residual. The elements  $\xi \in \text{Res}^{\text{lin}}(R_1)$  are called the *generic linear residual points*.

**2B3. Massive elliptic representations.**

**Definition 2.5.** We define

$$\mathcal{Y}_v := \lim_{v \rightarrow 1} (\bar{\mathcal{R}}_{\mathbb{Z}}(\mathcal{H}_v)) \subset \bar{\mathcal{R}}_{\mathbb{Z}}(W), \tag{15}$$

and let  $\mathcal{Y}_{v-m} \subset \mathcal{Y}_v$  be the sublattice generated by the limits  $\lim_{\epsilon \rightarrow 0} \pi_{v^\epsilon}$  of *discrete series representations* of  $\mathcal{H}_v$ . We call  $\mathcal{Y}_{v-m}$  the lattice of  $v$ -massive elliptic representations of  $W$ . Finally let  $\mathcal{Y}_{\text{gm}} \subset \bar{\mathcal{R}}_{\mathbb{Z}}(W)$  be the sublattice generated by  $\bigcup_{v \in \mathcal{Q}} \mathcal{Y}_{v-m}$ , the lattice of *generically massive* elliptic representations of  $W$ . In general,  $\mathcal{Y}_{\text{gm}} \neq \bar{\mathcal{R}}_{\mathbb{Z}}(W)$ .

**Proposition 2.6.** *The lattice  $\mathcal{Y}_{\text{gm}}$  admits an orthonormal basis  $\mathcal{B}_{\text{gm}} \subset \mathcal{Y}_{\text{gm}}$ . If  $b \in \mathcal{B}_{\text{gm}}$  then  $b \in \bar{\mathcal{R}}_{\mathbb{Z}}(W)_{W_0 s}$  for some  $s \in T_u$  such that  $\text{rk}(R_{s,1}) = \dim(T_u)$ .*

*Proof.* It follows from the classification [Opdam and Solleveld 2010, Section 5] that an irreducible discrete series  $(V, \pi_v)$  of  $\mathcal{H}_v$  has central character  $W_0 r(v)$  for some generic residual point  $r$ , and we can write  $r = sc$  with  $s \in T_u$  and  $c = \exp(\xi)$ , where  $\xi$  is a generic linear residual point for  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$  whose evaluation at  $k_s$  is residual. In particular, the rank of  $R_{s,1}$  is equal to the dimension of  $T_u$ .

By [Opdam and Solleveld 2010] it also follows that  $\pi$  corresponds via (10) to the representation of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s$  induced by the irreducible representation  $U \otimes M$  of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_U$ , where  $U$  is an irreducible discrete series character of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$  (here we also use the discussion in the text above). In Corollary 2.2 we have seen that the limit  $b := \lim_{\epsilon \rightarrow 0} \bar{\pi}_{v^\epsilon}$  equals  $b = \text{Ind}_s(b_s)$  with  $b_s = \overline{U|_{W_s}}$ . By the results of [Ciubotaru et al. 2014]

and of [Opdam and Solleveld 2010] we see that the algebraic Dirac induction for  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$  of  $b_s$  yields an elliptic representation supported by the central character  $W(R_{s,1})\xi(k_s)$ , which is (by [Opdam and Solleveld 2010]) residual for all  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$ , a complement in  $\mathcal{Q}$  of finitely many hyperplanes. Recall that, by [Opdam 2007], a central character  $W(R_{s,1})\xi(k_s)$  for  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$  is residual if and only if  $W_s\xi(k_s)$  is residual for  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_s$ . (This is because of the invariance of residual central characters under Dynkin diagram automorphisms.)

Let  $\mathbf{v}' \in \mathcal{Q}_b^{\text{reg}}$ . By the main result of [Ciubotaru et al. 2014], since  $W_s\xi(k'_s)$  is residual there exists a virtual discrete series character  $U'$  of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k'_s)$  with  $\overline{U'|_{W_s}} = b_s$  ( $U'$  is the analytic Dirac induction of  $b_s$ ). Again using the classification of the discrete series of [Opdam and Solleveld 2010], and (10), there exists a virtual discrete series character  $\pi'_{\mathbf{v}'}$  of  $\mathcal{H}_{\mathbf{v}'}$  with  $b = \text{Ind}_s(b_s) = \lim_{\epsilon \rightarrow 0} \overline{\pi_{\mathbf{v}'\epsilon}}$ . Since  $\mathcal{Y}_{\text{gm}} \subset \overline{\mathcal{R}_{\mathbb{Z}}(W)}$  it is clear that  $\mathcal{Y}_{\text{gm}}$  is finitely generated. Choose a finite collection of (irreducible) discrete series  $\pi_i$  of  $\mathcal{H}_{\mathbf{v}_i}$  such that the corresponding limits  $b_i$  are linearly independent and generate  $\mathcal{Y}_{\text{gm}}$ . By the arguments above, if  $\mathbf{v} \in \bigcap_i \mathcal{Q}_{b_i}^{\text{reg}}$  then there exist virtual discrete series characters  $\pi'_i$  of  $\mathcal{H}_{\mathbf{v}}$  with

$$b_i := \lim_{\epsilon \rightarrow 0} \overline{\pi'_{i,\mathbf{v}\epsilon}}.$$

Consequently,  $\mathcal{Y}_{\text{gm}} = \mathcal{Y}_{\mathbf{v}-m}$ . Since the limit map is an isometry and since (by [Opdam and Solleveld 2009]) the irreducible discrete series form an orthonormal set with respect to  $\text{EP}_{\mathcal{H}}$ ,  $\mathcal{Y}_{\mathbf{v}-m}$  (and thus  $\mathcal{Y}_{\text{gm}}$ ) admits an orthonormal basis.  $\square$

At this point, the basis  $\mathcal{B}_{\text{gm}}$  from Proposition 2.6 is not unique. The canonical choice for the basis  $\mathcal{B}_{\text{gm}}$  is obtained in Corollary 3.19.

**2B4. Dirac induction for affine Hecke algebras.**

**Definition 2.7.** Given  $b \in \mathcal{B}_{\text{gm}}$  and  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$ , we define  $\text{Ind}_D(b; \mathbf{v})$  (the ‘‘Dirac induction of  $b$ ’’) as the unique virtual discrete series character of  $\mathcal{H}_{\mathbf{v}}$  whose scaling limit satisfies  $\lim_{\epsilon \rightarrow 0} \text{Ind}_D(b; \mathbf{v}\epsilon) = b$ . Up to a sign  $\epsilon(b; \mathbf{v}) \in \{\pm 1\}$ ,  $\text{Ind}_D(b; \mathbf{v})$  is an irreducible discrete series character. For all  $\mathbf{v} \in \mathcal{Q}$  this defines a bijection

$$\mathcal{B}_{\mathbf{v}-m} \ni b \rightarrow \epsilon(b; \mathbf{v}) \text{Ind}(b; \mathbf{v}) \in \Delta_{\mathbf{v}},$$

where  $\Delta_{\mathbf{v}} := \Delta(\mathcal{H}_{\mathbf{v}})$  denotes the set of isomorphism classes of irreducible discrete series representations of  $\mathcal{H}_{\mathbf{v}}$ .

In the proof of Proposition 2.6 we have seen that  $\text{Ind}_D(b; \mathbf{v})$  is not directly constructed as the index of a Dirac-type operator but rather, it corresponds via (10) and a Morita equivalence to the discrete series  $U \otimes M$  of  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s) \rtimes \Gamma_U$ , with  $U = \text{Ind}_D^{\text{an}}(b_s, k_s)$  the analytic Dirac induction (defined in [Ciubotaru et al. 2014]) of  $b_s$  for  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$ . The existence of  $\text{Ind}_D(b; \mathbf{v})$  follows

from this construction. It also follows from this construction that  $\pm \text{Ind}_D(b; \mathbf{v})$  is irreducible.

**2B5.** *The generic Vogan central character map.* Let  $\mathcal{B}_{\text{gm}}$  be an orthonormal basis of  $\mathcal{Y}_{\text{gm}}$ . As we have seen, given  $b \in \mathcal{B}_{\text{gm}}$  the set  $\mathcal{Q}_b^{\text{reg}} = \{\mathbf{v} \mid b \in \mathcal{B}_{\mathbf{v}-m}\}$  is the complement of finitely many hyperplanes in  $\mathcal{Q}$ . As in the proof of Proposition 2.6, to each  $b \in \mathcal{B}_{\text{gm}}$  we have a canonically associated orbit of generic residual points  $W_0 r_b$ , with  $r_b = s \exp \xi_s$ , and  $\xi_s$  the generic linear residual point associated to  $b_s \in \overline{R_{\mathbb{Z}}(W_s)}$  by the generic version of ‘‘Vogan’s conjecture’’ (see [Ciubotaru et al. 2014, Theorem 3.2]). Strictly speaking, the results of [Ciubotaru et al. 2014] apply to give a residual central character of a nonextended graded affine Hecke algebra, but as already noted in the proof of Proposition 2.6, one may use the invariance [Opdam 2007] of these central characters under diagram automorphisms to obtain the desired central character in our more general setting.

Let us denote the resulting generic central character map (see [Opdam and Solleveld 2010]) by:

$$\begin{aligned} \text{gcc}_B : \mathcal{B}_{\text{gm}} &\rightarrow W_0 \setminus \text{Hom}(X, \Lambda^\times) = W_0 \setminus T_\Lambda, \\ b &\rightarrow W_0(s \exp \xi_s) \end{aligned}$$

(the generic Vogan central character map). From the proof of Proposition 2.6 and Definition 2.7 we obtain:

**Corollary 2.8.** *For all  $b \in \mathcal{B}_{\text{gm}}$  and  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$  we have*

$$\text{gcc}_{\mathbf{v}}(\text{Ind}_D(b; \mathbf{v})) = \text{gcc}_B(b) = W_0 r_b.$$

Moreover,  $W_0 r_b(1) = W_0 s$  if and only if  $b$  can be written as  $b = \text{Ind}_s(b_s)$ .

**Definition 2.9.** We put  $m_b := m_{W_0 r_b}$ , where  $m_{W_0 r_b}$  denotes the mass function associated to the orbit of  $\mathcal{Q}$ -generic residual points  $\text{gcc}_B(b) = W_0 r_b$  in (13). By [Opdam and Solleveld 2010], and we have for all  $b \in \mathcal{B}$  that

$$\mathcal{Q}_b^{\text{reg}} = \{\mathbf{v} \in \mathcal{Q} \mid m_b(\mathbf{v}) \neq 0\}.$$

When  $\mathcal{Q}'$  is a subtorus of  $\mathcal{Q}$ , we will write  $m_b^{\mathcal{Q}'}$  for the function  $m_{W_0 r'_b}$  defined with respect to the  $\mathcal{Q}'$ -generic residual point  $r'_b$  obtained from  $r_b$  by base change to  $\mathcal{Q}'$ . Notice that  $m_b^{\mathcal{Q}'} = d' m_b|_{\mathcal{Q}'}$  for some  $d' \in \mathbb{Q}$ , with  $d' \neq 0$  if and only if  $\mathcal{Q}_b^{\text{reg}} \cap \mathcal{Q}' \neq \emptyset$ .

**Theorem 2.10.** *The generic Vogan central character map  $\text{gcc}_B$  is a surjection  $\text{gcc}_B : \mathcal{B}_{\text{gm}} \rightarrow W_0 \setminus \text{Res}(\mathcal{R})$ .*

*Proof.* In [Opdam 2004] it was shown (also see [Opdam and Solleveld 2010]) that for any  $\mathbf{v} \in \mathcal{Q}$ , every orbit of residual points of  $\mathcal{H}_{\mathbf{v}}$  is the specialization at  $\mathbf{v}$  of a generic orbit of residual points  $W_0 r$  at  $\mathbf{v}$ . The main theorem of [Opdam 2004] states that for any  $\mathbf{v} \in \mathcal{Q}$ , and any orbit of residual cosets  $W_0 r(\mathbf{v})$ , there exists a discrete



series character  $\pi$  of  $\mathcal{H}_v$  such that  $W_0r(v)$  is the central character of  $\pi$ . The set  $W_0 \setminus \text{Res}(\mathcal{R})$  is finite, hence

$$\mathcal{Q}^{\text{gen}} := \left\{ v \in \bigcap_{W_0r \in W_0 \setminus \text{Res}(\mathcal{R})} \mathcal{Q}_{W_0r}^{\text{reg}} \mid \text{For all } r, r' \in \text{Res}(\mathcal{R}): W_0r(v) = W_0r'(v) \text{ only if } Wr = W_0r' \right\}$$

is open and dense in  $\mathcal{Q}$ . Let  $v \in \mathcal{Q}^{\text{gen}}$  and  $W_0r \in W_0 \setminus \text{Res}(\mathcal{R})$ . By the above there exists a  $\pi \in \Delta_v$  such that  $cc(\pi) = W_0r(v)$ . Since  $v \in \mathcal{Q}^{\text{gen}}$  this implies that  $\text{gcc}_v(\pi) = W_0r$ . (For the definition of the generic central character map  $\text{gcc}_v$ , see [Opdam and Solleveld 2010, Definition 5.4].) Put  $b := \lim_{\epsilon \rightarrow 0} \pi_{v^\epsilon}$ . By Corollary 2.8 we have  $\text{gcc}_B(b) = W_0r$ .  $\square$

Denote by  $\mathcal{B}_{W_0r} \subset \mathcal{B}_{\text{gm}}$  the fiber  $\text{gcc}_B^{-1}(W_0r)$  of the map from Theorem 2.10.

### 3. One-dimensional algebraic families of discrete series representations, and their limits

**3A. One-dimensional algebraic families of discrete series.** Given a generic residual point  $r \in \text{Hom}(X, \Lambda^\times)$  we know that  $r(v)$  is a residual point for all  $v \in \mathcal{Q}_{W_0r}^{\text{reg}}$ , which is the complement of finitely many hyperplanes in  $\mathcal{Q}$ . By [Opdam and Solleveld 2010, Corollary 5.9]) we have a nonempty set of irreducible discrete series characters of  $\mathcal{H}_v$  with *generic central character*  $W_0r$ . Denote this nonempty set by:

$$\text{DS}_{W_0r, v} := \{ \pi \in \Delta(\mathcal{H}_v) \mid \text{gcc}(\pi) = b \}.$$

Hence  $W_0r(v)$  is the central character of the following nonempty union:

$$\text{DS}_{W_0r(v)} := \bigcup_{\{W_0r' \mid W_0r'(v) = W_0r(v)\}} \text{DS}_{W_0r', v}.$$

Let  $v \in \mathcal{Q}_{\mathbb{C}}$ . For each  $r'(v) \in W_0r(v)$ , choose a convex open neighborhood  $U_{r'(v)}$  of  $r'(v) \in T$  such that the only residual cosets of the  $\mu$ -function  $\mu_{\mathcal{R}, v}$  of  $\mathcal{H}_v$  which intersect  $U_{r'(v)}$  in fact contain  $r'(v)$ . Let  $U_{r'(v)}^{\text{reg}} = U_{r'(v)} \cap T^{\text{reg}}$  be the complement in  $U_{r'(v)}$  of the union of the set of residual cosets of  $\mu_{\mathcal{R}, v}$  in  $T$ . The choice of  $U_{r'(v)}$  as above implies that  $U_{r'(v)}^{\text{reg}}$  is homeomorphic to the complement of a central hyperplane arrangement in a complex vector space with origin  $r'(v)$ . In particular, the homology group  $H_n(U_{r'(v)}^{\text{reg}}, \mathbb{Z})$  only depends on the local structure of the pole hyperplane arrangement at  $r'(v)$ , and if we would shrink  $U_{r'(v)}$  to a smaller convex open neighborhood  $U_{r'(v)}^{\prime, \text{reg}} \subset U_{r'(v)}^{\text{reg}}$  of  $r'(v)$  this would induce a canonical isomorphism  $H_n(U_{r'(v)}^{\prime, \text{reg}}, \mathbb{Z}) = H_n(U_{r'(v)}^{\text{reg}}, \mathbb{Z})$ . Let us denote the direct limit  $\varinjlim H_n(U_{r'(v)}^{\prime, \text{reg}}, \mathbb{Z})$  by  $H_{n, r'(v)}(\mathbb{Z})$ .

In general, if  $U \subset T$  is homeomorphic to a complex ball  $B \subset \mathfrak{t}$ , via the exponential mapping of the complex algebraic torus  $T$ , then  $U^{\text{reg}} := U \cap T^{\text{reg}}$  is homeomorphic to the intersection of  $B$  with the complement of an affine hyperplane arrangement. In this section we will need some basic facts about the topology of hyperplane arrangements, see [Orlik and Terao 1992; Schechtman and Varchenko 1991]. By [Schechtman and Varchenko 1991, Paragraph 4.4] it easily follows that  $H_n(U^{\text{reg}}, \mathbb{Z})$  is in a canonical way a *direct sum* of the  $H_{n,p}(\mathbb{Z})$  where  $p$  runs over the set of points of  $U$  which lie in the intersection lattice generated by the codimension one residual cosets of  $\mu_{\mathcal{R},v}$ . Let  $\pi_p : H_n(U^{\text{reg}}, \mathbb{Z}) \rightarrow H_{n,p}(\mathbb{Z})$  denote the corresponding projection.

Let us denote the collection of open sets  $\{U_{r'(\mathbf{v})}\}_{r' \in W_0r}$  by  $\mathcal{U}$ . Let  $\mathcal{O}_{\mathcal{U},v} \subset \mathcal{Q}_{\mathbb{C}}$  be an open ball with center  $\mathbf{v}$  with the property that for all  $\mathbf{v}' \in \mathcal{O}_{\mathcal{U},v}$  and all  $r' \in W_0r$  we have  $r'(\mathbf{v}') \in U_{r'(\mathbf{v})}$ . Given  $\mathbf{v} \in \mathcal{Q}_{\mathbb{C}}$  and a homology class  $[\xi_{r'(\mathbf{v})}] \in H_n(U_{r'(\mathbf{v})}, \mathbb{Z})$  for each  $r'(\mathbf{v}) \in W_0r(\mathbf{v})$ , this defines for all  $\mathbf{v}' \in \mathcal{O}_{\mathcal{U},v}$  a unique class  $\pi_{r'(\mathbf{v}')}([\xi_{r'(\mathbf{v}')}] \in H_{n,r'(\mathbf{v}')}(\mathbb{Z})$ . It is easy to see that this procedure defines a topology basis of the étale space of a sheaf  $\mathcal{F}_{n,r'}^H$  of abelian groups over  $\mathcal{Q}_{\mathbb{C}}$ , with stalks  $H_{n,r'(\mathbf{v})}(\mathbb{Z})$ . Let  $\mathcal{Q}_{W_0r,\mathbb{C}}^{\text{gen}} \subset \mathcal{Q}_{\mathbb{C}}$  be the Zariski-open set of  $\mathbf{v} \in \mathcal{Q}_{\mathbb{C}}$  such that  $|W_0r(\mathbf{v}')|$  is locally constant at  $\mathbf{v}$ , and such that if  $r'$  is a generic residual point such that  $W_0r(\mathbf{v}) = W_0r'(\mathbf{v})$  then  $W_0r = W_0r'$ .<sup>1</sup> Clearly, the sheaf  $\mathcal{F}_{n,r}^H$  is locally trivial in the analytic topology on  $\mathbf{v} \in \mathcal{Q}_{W_0r,\mathbb{C}}^{\text{gen}}$ . We have shown:

**Lemma 3.1.** *For each generic residual point  $r$ , the homology groups  $H_{n,r(\mathbf{v})}(\mathbb{Z})$  ( $\mathbf{v} \in \mathcal{Q}_{\mathbb{C}}$ ) are the stalks of a sheaf  $\mathcal{F}_{n,r}^H$  (in the analytic topology) of finitely generated abelian groups on  $\mathcal{Q}_{\mathbb{C}}$ , which is locally trivial on the Zariski-open set  $\mathcal{Q}_{W_0r,\mathbb{C}}^{\text{gen}}$ .*

The main results of [Opdam 2004] and of [Opdam and Solleveld 2010] show that for each  $\mathbf{v} \in \mathcal{Q}_{W_0r}^{\text{reg}}$  we can choose, for each  $r'(\mathbf{v}) \in W_0r(\mathbf{v})$ , classes  $\xi_{r'(\mathbf{v})} \in H_{n,r'(\mathbf{v})}(\mathbb{Z})$  and, for each  $\chi \in \text{DS}_{W_0r(\mathbf{v})}$ , constants  $c_{\chi,C} \in \mathbb{Q}_+$  depending only on the connected component  $C = C_{\chi,v} \subset \mathcal{Q}_{\text{gcc}_v}^{\text{reg}}(\chi)$  to which  $\mathbf{v}$  belongs (where  $\text{gcc}_v(\chi) = W_0r''$  denotes the generic central character [Opdam 2004, Definition 5.4] of  $\chi$ ), such that for all  $h \in \mathcal{H}_v$ ,

$$\sum_{\chi \in \text{DS}_{W_0r(\mathbf{v})}} c_{\chi,C} \chi_v(h) = m_{W_0r}(\mathbf{v})^{-1} \sum_{r'(\mathbf{v}) \in W_0r(\mathbf{v})} \int_{t \in \xi_{r'(\mathbf{v})}} K_v(h, t), \tag{16}$$

where  $K_v(h, t) = E_t(\mathbf{v}; h) \Delta(t)^{-1} \mu_{\mathcal{R},v} dt$  is a rational  $(n, 0)$ -form in  $t \in T$ , with  $\Delta(t) := \prod_{\alpha > 0} (1 - \alpha(t)^{-1})$  and with  $E_t(\mathbf{v}; h)$  a linear functional in  $h \in \mathcal{H}_v$ , which is regular on  $(t, \mathbf{v}) \in T \times \mathcal{Q}_{\mathbb{C}}$ , and such that  $E_t(\mathbf{v}; a) = a(t) \Delta(t)$  for all  $a \in \mathcal{A}$ .

We now prove a fundamental continuity property of (16) (or even the full Plancherel decomposition of the trace of  $\mathcal{H}_v$ ) with respect to the topology of the sheaves  $\mathcal{F}_{n,r}^H$ .

<sup>1</sup>Using the results of [Opdam 2007] it is easy to see that  $\mathcal{Q}_{W_0r,\mathbb{C}}^{\text{gen}} \cap \mathcal{Q} = \mathcal{Q}_{W_0r}^{\text{gen}}$ , in the notation of [Opdam and Solleveld 2010].

**Lemma 3.2.** *Let  $r$  be a generic residual point and let  $\mathbf{v} \in \mathcal{Q}_{W_0 r}^{\text{reg}}$ . For  $r' \in W_0 r$  and for  $\mathbf{v}'$  in a sufficiently small neighborhood of  $\mathbf{v}$ , the local homology classes  $[\xi_{r'}(\mathbf{v}')] \in H_{n,r'}(\mathbb{Z})$  in (16) form a local section of  $\mathcal{F}_{n,r'}^H$ .*

*Proof.* We use the analogous construction to the above of sheaves  $\mathcal{F}_{n,r_L}^H(\mathbb{Z})$  for all  $r_L \in T_L$  a generic residual point. Recall the residue lemma [Opdam 2004, Lemma 3.4]. By [Opdam 2004, Proposition 3.7] we can realize the local traces  $\mathfrak{X}_c$  defined in [Opdam 2004, Lemma 3.4] “explicitly” by a system of local cycles  $\xi_{L(\mathbf{v})} \subset \mathcal{B}_{L(\mathbf{v})}(r_L(\mathbf{v}), \delta) \subset T_{L(\mathbf{v})}$  (for all quiresidual cosets  $L(\mathbf{v}) \subset T$ ) such that for  $t_0 \in T_v$  deep in the negative Weyl chamber, the cycles  $t_0 T_u$  and  $\bigcup_L \xi_{L(\mathbf{v})} \times T_u^L$  are homologous. Moreover, the  $\xi_{L(\mathbf{v})}$  satisfy certain local properties (see [Opdam 2004, Proposition 3.7], items (i), (ii) and (iii)) which guarantee that for all  $h \in \mathcal{H}_v$ , the functional

$$\mathbb{C}[T] \ni f \rightarrow \int_{\xi_{L(\mathbf{v})} \times T_u^L} f(t) K_v(h, t)$$

can be written as a distribution on  $r_L(\mathbf{v})T_u$  with support in  $L(\mathbf{v})^{\text{temp}} = r_L(\mathbf{v})T_u^L$ , applied to  $f$  (which is zero if  $L_v$  is not a residual coset).

The definition of the local sections of the sheaves  $\mathcal{F}_{n,r_{L'}}^H$  is such that the local properties ((i), (ii) and (iii) mentioned in [Opdam 2004, Proposition 3.7]) can be satisfied by cycles

$$\xi_{L'(\mathbf{v}')} \subset \mathcal{B}_{L'(\mathbf{v}')} (r_{L'}(\mathbf{v}'), \delta) \subset T_{L'(\mathbf{v}')}$$

representing the classes  $[\xi_{L'(\mathbf{v}')}] \in H_{n,r_{L'}(\mathbf{v}')}(\mathbb{Z})$  for  $\mathbf{v}'$  in a small neighborhood of  $\mathbf{v}$ . Moreover, it is automatic that  $t_0 T_u$  is homologous to the union of  $\bigcup_L \xi_{L(\mathbf{v}')} \times T_u^L$  (union over the generic residual cosets  $L$ ) with a collection of cycles of the form  $\xi_{L'(\mathbf{v}')} \times T_u^{L'}$ , where  $L'(\mathbf{v}')$  is quiresidual (which are irrelevant). This implies the result. □

**Corollary 3.3.** *For  $\mathbf{v} \in \mathcal{Q}_{W_0 r}^{\text{reg}}$ , the left-hand side of (16) extends to a central functional on  $\mathcal{H}_{\mathbf{v}'}$  for all  $\mathbf{v}'$  in a Zariski-open neighborhood of  $\mathbf{v}$  in  $\mathcal{Q}_{\mathbb{C}}$ . For  $h \in \mathcal{H}_{\Lambda}$  this functional takes values in the quotient field  $\mathcal{Q}_{\Lambda}$  of  $\Lambda$ . The values of this functional restrict to continuous functions on the connected component  $C$  of  $\mathbf{v}$  in  $\bigcap_{\chi \in \text{DS}_{W_0 r}(\mathbf{v})} \mathcal{Q}_{\text{gcc}_v(\chi)}^{\text{reg}}$ .*

*Proof.* We extend the left-hand side in a neighborhood of  $\mathbf{v}$  by taking local sections of classes  $[\xi_{r'}(\mathbf{v})]$  in  $\mathcal{F}_{n,r'}^H$ , and use the right-hand side of (16) to define the left-hand side. We know from [Opdam and Solleveld 2010] that the left-hand side extends, for all  $h \in \mathcal{H}_{\Lambda}$ , continuously on  $\bigcap_{\chi \in \text{DS}_{W_0 r}(\mathbf{v})} \mathcal{Q}_{\text{gcc}_v(\chi)}^{\text{reg}}$ . Let  $\chi \in \text{DS}_{W_0 r}(\mathbf{v})$  and let  $\text{gcc}_v(\chi) := W_0 r'$ . Let

$$\mathbf{v}' \in \bigcap_{\chi \in \text{DS}_{W_0 r}(\mathbf{v})} C_{\chi, \mathbf{v}} \cap \mathcal{Q}_{\text{gcc}_v(\chi)}^{\text{gen}}$$

Then the left-hand side of (16) can be written as  $\sum_{\{W_{0r'}|W_{0r'}(v)=W_{0r}(v)\}} \Sigma_{W_{0r'}}(h; v')$ , with

$$\Sigma_{W_{0r'}}(h; v') := \sum_{\chi \in \text{DS}_{W_{0r'}, v'}} c_{\chi, C} \chi_{v'}(h). \tag{17}$$

We have

$$\Sigma_{W_{0r'}}(h; v') = m_{W_{0r'}}(v')^{-1} \sum_{r''(v') \in W_{0r'}(v')} \int_{t \in \xi_{r''}(v')} K_{v'}(h, t),$$

where, for  $v'$  in a sufficiently small neighborhood of  $v$ , the class  $[\xi_{r''}(v')]$  is equal to the image  $\pi_{r''(v')}( \xi_{r''}(v) ) \in H_{n, r''(v')}( \mathbb{Z} )$  of the constant cycle  $\xi_{r''}(v)$ , by Lemmas 3.1 and 3.2. It follows that in a small analytic neighborhood of  $v$  the expression  $\Sigma_{W_{0r'}}(h; v')$  is given by an element of  $\mathcal{Q}_\Lambda$ . This extends  $v' \rightarrow \Sigma_{W_{0r'}}(h; v')$  to a rational function on a Zariski-open set of  $\mathcal{Q}_\mathbb{C}$ .

The continuity of the values of  $\Sigma_{W_{0r'}}(h; v')$  in the connected component  $C \subset \mathcal{Q}_{W_{0r'}}^{\text{reg}}$  of  $v'$  follows from [Opdam and Solleveld 2010, Theorem 3.4, Proposition 3.7], and this implies the continuity assertion in the theorem.  $\square$

**Remark 3.4.** We note that  $\Sigma_{W_{0r}}(h; \cdot)$  is not rational on  $\bigcap_{\chi \in \text{DS}_{W_{0r}(v)}} \mathcal{Q}_{\text{gcc}_v(\chi)}^{\text{reg}}$ . The rational functions of Corollary 3.3 depend on the connected component of  $v$  in  $\bigcap_{\chi \in \text{DS}_{W_{0r}(v)}} \mathcal{Q}_{\text{gcc}_v(\chi)}^{\text{reg}}$ .

Let  $\mathcal{C} \subset \mathcal{Q}$  be (the set of complex points of) an irreducible real algebraic curve which is not contained in  $\bigcup_{W_{0r}} \mathcal{Q}_{W_{0r}}^{\text{sing}}$ . Let  $\mathfrak{R}$  be the ring of regular functions of  $\mathcal{C}$ , with quotient field  $\mathfrak{K}$ . Thus  $\mathfrak{R}$  is a quotient of  $\Lambda$ , and we can form  $\mathcal{H}_{\mathfrak{R}} := \mathcal{H}_\Lambda \otimes_\Lambda \mathfrak{R}$ . Let  $P = v_0 \in \mathcal{C}$  be a smooth point of  $\mathcal{C}$ , and let  $C \subset \mathcal{Q}_{W_{0r}}^{\text{reg}}$  be a connected component such that  $v_0 \in \bar{C}$ . Let  $v' \in C \cap \mathcal{Q}_{W_{0r}}^{\text{gen}}$ , and consider  $\Sigma_{W_{0r}}(h; v')$ . According to Corollary 3.3, this positive rational linear combination of the discrete series characters with central character  $W_{0r}(v')$  extends as a rational function in  $v'$  which is continuous on  $C$ . By Corollary 3.3 we can restrict the values of  $\Sigma_{W_{0r}}(h; v')$  to  $v' \in \mathcal{C} \cap C$ . By the argument of [Kollár and Nowak 2015, Proposition 7] it is clear that this restriction defines a rational function on  $\mathcal{C}$  which we will denote by  $\Sigma_{W_{0r}, C}^{\mathcal{C}}(h) \in \mathfrak{R}$ , depending linearly on  $h \in \mathcal{H}_{\mathfrak{R}}$ . These rational functions are continuous on  $\mathcal{C} \cap C$ .

**Lemma 3.5.** *Assume that  $\mathcal{C} \cap \bar{C}$  consists of smooth points and let  $P = v_0 \in \mathcal{C} \cap \bar{C}$ . For all  $h \in \mathcal{H}_{\mathfrak{R}}$  we have: The rational function  $\Sigma_{W_{0r}, C}^{\mathcal{C}}(h)$  is regular in  $P = v_0$ . There exists a Zariski-open neighborhood  $\mathfrak{U} \subset \mathcal{C}$  of  $\mathcal{C} \cap \bar{C}$  such that  $\Sigma_{W_{0r}, C}^{\mathcal{C}}(h) \in \mathfrak{R}(\mathfrak{U})$  for all  $h \in \mathcal{H}_{\mathfrak{R}(\mathfrak{U})}$ .*

*Proof.* Since  $\Sigma_{W_{0r}, C}^{\mathcal{C}}(h)$  is rational and  $P$  is a smooth point of the curve  $\mathcal{C}$ , it is enough to show that  $v \rightarrow \Sigma_{W_{0r}, C}^{\mathcal{C}}(h; v)$  is bounded in a neighborhood of  $v_0 = P \in \mathcal{C}$  for  $v \in \mathcal{C} \cap C$ . But  $\Sigma_{W_{0r}}(\cdot; v)$  is a positive functional on  $\mathcal{H}_v$  for all  $v \in C$ , and if  $v \in \mathcal{C} \cap C$  then  $\Sigma_{W_{0r}}(T_e; v) = \sum_{\chi \in \text{DS}_{W_{0r}, v}} c_{\chi, C} \deg(\chi) = C \in \mathbb{Q}_+$  is constant.

By [Opdam 2004, Corollary 2.17(i)] we see that  $|\Sigma_{W_{0r},C}^{\mathfrak{C}}(h; \mathbf{v})| \leq C \|h\|_o$ . This implies the regularity at  $P$  of the rational function  $\mathbf{v} \rightarrow \Sigma_{W_{0r},C}^{\mathfrak{C}}(h; \mathbf{v})$  for all  $h \in \mathcal{H}_{\mathfrak{R}}$ . Note that for  $z \in \mathcal{Z} \subset \mathcal{H}_{\mathfrak{R}}$  we have  $\Sigma_{W_{0r},C}^{\mathfrak{C}}(zh; \mathbf{v}) = z(W_{0r}(\mathbf{v}))\Sigma_{W_{0r},C}^{\mathfrak{C}}(h; \mathbf{v})$ , while  $\mathbf{v} \rightarrow z(W_{0r}(\mathbf{v})) \in \mathfrak{R}$  is regular on  $\mathfrak{C}$ . Since  $\mathcal{H}_{\mathfrak{R}}$  is finitely generated over  $\mathcal{Z}$  it follows that we can find an open neighborhood  $\mathfrak{U}$  of  $\mathfrak{C} \cap \bar{C}$  on which  $\mathbf{v} \rightarrow \Sigma_{W_{0r},C}^{\mathfrak{C}}(h; \mathbf{v})$  is regular for all  $h \in \mathcal{H}_{\mathfrak{R}}$ .  $\square$

From now on we will assume that  $\mathfrak{C} \cap \bar{C}$  consists of smooth points of  $\mathfrak{C}$ , and that  $\mathfrak{U} \subset \mathfrak{C}$  is as in Lemma 3.5. We have shown that

$$\Sigma_{W_{0r},C}^{\mathfrak{C}} \in \mathcal{H}_{\mathfrak{R}(\mathfrak{U})}^* := \text{Hom}_{\mathfrak{R}(\mathfrak{U})}(\mathcal{H}_{\mathfrak{R}(\mathfrak{U})}, \mathfrak{R}(\mathfrak{U}))$$

is a central functional in the  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})} \otimes_{\mathfrak{R}(\mathfrak{U})} \mathcal{H}_{\mathfrak{R}(\mathfrak{U})}^{\text{op}}$ -module  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})}^*$ , supported by the central character  $W_{0r}$ .

**Definition 3.6.**  $M_{W_{0r},C}^{\mathfrak{U}} \subset \mathcal{H}_{\mathfrak{R}(\mathfrak{U})}^*$  denotes the  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})} \otimes \mathcal{H}_{\mathfrak{R}(\mathfrak{U})}^{\text{op}}$ -submodule generated by  $\Sigma_{W_{0r},C}^{\mathfrak{C}}$ .

We will now show that a generic family  $\chi$  of discrete series characters as discussed in [Opdam and Solleveld 2010] always admits an algebraic model when we restrict the parameter space to a curve  $\mathfrak{C}$  in  $\mathcal{Q}$ . Moreover, we can find such models that are regular at the intersection of the curve with the boundary of the connected component  $C \subset \mathcal{Q}_{\text{gcc}(\chi)}^{\text{reg}}$  (an open cone) on which  $\chi$  lives. More precisely:

**Proposition 3.7.** (i)  $M_{W_{0r},C}^{\mathfrak{U}}$  is an  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})} \otimes_{\mathfrak{R}(\mathfrak{U})} \mathcal{H}_{\mathfrak{R}(\mathfrak{U})}^{\text{op}}$ -module. The central subalgebra  $\mathcal{Z}_{\mathfrak{R}(\mathfrak{U})} \otimes_{\mathfrak{R}(\mathfrak{U})} \mathcal{Z}_{\mathfrak{R}(\mathfrak{U})}$  acts via scalar multiplication via the character  $(z_1 \otimes z_2) \rightarrow (z_1 z_2)(W_{0r}) \in \mathfrak{R}(\mathfrak{U})$ .

(ii)  $M_{W_{0r},C}^{\mathfrak{U}}$  is a locally free  $\mathfrak{R}(\mathfrak{U})$ -module of finite rank.

(iii)  $M_{W_{0r},C}^{\mathfrak{U}}$  has a canonical  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})}$ -algebra structure such that, if we put  $e = m_{W_{0r}} \Sigma_{W_{0r},C}^{\mathfrak{C}} \in M_{W_{0r},C}^{\mathfrak{U}} \subset \mathcal{H}_{\mathfrak{R}(\mathfrak{U})}^*$ , the map  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})} \ni h \rightarrow he$  is an algebra homomorphism.

(iv) If  $\mathbf{v} \in \mathfrak{U} \cap C$  then

$$M_{W_{0r},C}^{\mathfrak{U}} \otimes \mathbb{C}_{\mathbf{v}} \simeq \bigoplus_{\chi \in \text{DS}_{W_{0r},\mathbf{v}}} \text{End}_{\mathbb{C}}(V_{\chi_{\mathbf{v}}}),$$

where  $V_{\chi_{\mathbf{v}}}$  is a vector space on which the discrete series character  $\chi_{\mathbf{v}}$  is realized.

(v) We may assume without loss of generality that  $\mathfrak{U}$  is smooth. There exists a Zariski-open subset  $\mathfrak{U}^* \subset \mathfrak{U}$  with  $\mathfrak{C} \cap C \subset \mathfrak{U}^*$  such that

$$M_{W_{0r},C}^{\mathfrak{U}^*} := M_{W_{0r},C}^{\mathfrak{U}} \otimes_{\mathfrak{R}(\mathfrak{U})} \mathfrak{R}(\mathfrak{U}^*)$$

is a locally free separable  $\mathfrak{R}(\mathfrak{U}^*)$ -algebra of finite rank.

(vi) There exists a branched covering  $\phi: \tilde{\mathfrak{U}} \rightarrow \mathfrak{U}$  such that the following holds true. Let  $\mathfrak{L} \supset \mathfrak{K}$  denote the function field of  $\tilde{\mathfrak{U}}$ , and let  $\tilde{\mathfrak{R}}(\mathfrak{U}) := \mathfrak{R}(\tilde{\mathfrak{U}})$  be the integral

closure of  $\mathfrak{R}(\mathfrak{U})$  in  $\mathfrak{L}$ . Put  $\tilde{M}_{W_0r,C}^{\mathfrak{U}} := M_{W_0r,C}^{\mathfrak{U}} \otimes \tilde{\mathfrak{R}}(\mathfrak{U})$ . There exists a finite set of projective  $\tilde{\mathfrak{R}}(\mathfrak{U})$ -modules of finite rank  $\{L_i\}_{i \in \mathcal{I}}$ , such that

$$\tilde{M}_{W_0r,C}^{\mathfrak{U}} \subset \tilde{M}_{W_0r,C}^{\mathfrak{U},\max} \simeq \bigoplus_{i \in \mathcal{I}} \text{End}_{\tilde{\mathfrak{R}}(\mathfrak{U})}(L_i)$$

is an  $\tilde{\mathfrak{R}}(\mathfrak{U})$ -order. This turns  $L_i$  into an  $\mathcal{H}_{\tilde{\mathfrak{R}}(\mathfrak{U})}$ -module, for each  $i \in \mathcal{I}$ .

(vii) With  $\mathfrak{U}^*$  as in (v), define  $\tilde{\mathfrak{U}}^* := \phi^{-1}(\mathfrak{U}^*)$  and let  $\mathfrak{R}(\tilde{\mathfrak{U}}^*) \subset \mathfrak{L}$  be the integral closure of  $\mathfrak{R}(\mathfrak{U}^*)$  (which is the localization of  $\mathfrak{R}(\mathfrak{U}^*)$  at  $\tilde{\mathfrak{U}}^*$ ). Put  $\tilde{M}_{W_0r,C}^{\mathfrak{U}^*} := M_{W_0r,C}^{\mathfrak{U}^*} \otimes_{\mathfrak{R}(\mathfrak{U}^*)} \mathfrak{R}(\tilde{\mathfrak{U}}^*)$ . Then we have an isomorphism

$$\tilde{M}_{W_0r,C}^{\mathfrak{U}^*} = \tilde{M}_{W_0r,C}^{\mathfrak{U}^*,\max} \simeq \bigoplus_{i \in \mathcal{I}} \text{End}_{\tilde{\mathfrak{R}}(\mathfrak{U})}(L_i^*),$$

with  $L_i^* := L_i \otimes_{\tilde{\mathfrak{R}}(\mathfrak{U})} \mathfrak{R}(\tilde{\mathfrak{U}}^*)$ .

(viii) The covering  $\phi$  (as in (vi)) is not branched at points of  $\mathfrak{C} \cap C$ . Let  $\mathbf{v} \in \mathfrak{C} \cap C$  and let  $\tilde{\mathbf{v}}$  be a closed point lying above  $\mathbf{v} \in \mathfrak{C} \cap C$ . There exists a unique bijection  $i \rightarrow \chi_i$  from  $\mathcal{I}$  onto  $\text{DS}_{W_0r,\mathbf{v}}$  such that  $L_{i,\tilde{\mathbf{v}}} := L_i \otimes \mathbb{C}_{\tilde{\mathbf{v}}} \simeq V_{\chi_i,\mathbf{v}}$  as representation of  $\mathcal{H}_{\mathbf{v}}$ , via the canonical isomorphism  $\mathcal{H}_{\mathbf{v}} \simeq \mathcal{H}_{\tilde{\mathfrak{R}}(\mathfrak{U}),\tilde{\mathbf{v}}}$ .

*Proof.* Assertion (i): This is immediate from the definition.

Assertion (ii): Since  $\Sigma_{W_0r,C}^{\mathfrak{C}}$  is central and is a  $\mathcal{Z}^{\mathfrak{U}}$ -eigenfunction with eigenvalue  $W_0r$ , it is clear that  $M_{W_0r,C}^{\mathfrak{U}}$  is finitely generated over  $\mathfrak{R}(\mathfrak{U})$ . It is also obviously torsion free over  $\mathfrak{R}(\mathfrak{U})$ , implying that the localization  $M_{W_0r,C,Q}^{\mathfrak{U}}$  is free over  $\mathfrak{R}_Q$  for all  $Q \in \mathfrak{U}$  (since the local rings are principal ideal domains). Since  $M_{W_0r,C}^{\mathfrak{U}}$  is finitely generated, this implies that it is a locally free module.

Assertion (iii): We need to verify that the kernel of the surjective  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})}$ -module homomorphism  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})} \ni h \rightarrow he \in M_{W_0r,C}^{\mathfrak{R}(\mathfrak{U})}$  is a two-sided ideal. This is a trivial consequence of the centrality of  $e$ . This turns  $M_{W_0r,C}^{\mathfrak{R}(\mathfrak{U})}$  into an  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})}$ -algebra.

Assertions (iv) and (v): We have already established that  $M_{W_0r,C}^{\mathfrak{R}(\mathfrak{U})}$  is a locally free  $\mathcal{H}_{\mathfrak{R}(\mathfrak{U})}$ -algebra of finite rank. When we specialize at  $\mathbf{v} \in C \cap \mathfrak{U}$ , we may use the fact [Delorme and Opdam 2008, Corollary 5.8] that  $e_{\mathbf{v}} \in \mathcal{S}_{\mathbf{v}} \subset \mathcal{H}_{\mathbf{v}}^*$  is a central idempotent of the Schwartz algebra  $\mathcal{S}_{\mathbf{v}}$  to see that the specialization  $M_{W_0r,C,\mathbf{v}} = M_{W_0r,C}^{\mathfrak{U}} \otimes \mathbb{C}_{\mathbf{v}}$  equals the finite dimensional semisimple algebra as stated in (iv). Hence the trace form of  $M_{W_0r,C}^{\mathfrak{U}}$  is nondegenerate over  $\mathfrak{R}$ , and by shrinking  $\mathfrak{U}^*$  sufficiently we may assume that the discriminant of the trace form of  $M_{W_0r,C}^{\mathfrak{U}}$  is nonvanishing on  $\mathfrak{U}^*$ . We arrive at the conclusion of (v) (see, e.g., [Artin 1999, Section IV.3]).

Assertion (vi): By (v) it follows that  $M_{W_0r,C}^{\mathfrak{R}} := M_{W_0r,C}^{\mathfrak{U}} \otimes_{\mathfrak{R}(\mathfrak{U})} \mathfrak{R}$  is a finite separable  $\mathfrak{R}$ -algebra. Hence  $M_{W_0r,C}^{\mathfrak{R}}$  is isomorphic to a finite direct sum of central simple algebras over finite separable field extensions  $\mathfrak{R}_i$  of  $\mathfrak{R}$  (see [Artin 1999, Section IV.3]). Tsen's Theorem [Artin 1999, Section III.15] implies that in fact  $M_{W_0r,C}^{\mathfrak{R}}$  is a direct sum

of full matrix algebras  $\text{Mat}_{d_i \times d_i}(\mathfrak{K}_i)$ . Consider the compositum  $\mathfrak{L}$  of the  $\mathfrak{K}_i$ . It is easy to see that for all  $i$ , the tensor product  $\mathfrak{K}_i \otimes_{\mathfrak{K}} \mathfrak{L}$  is isomorphic to a finite direct sum of copies of  $\mathfrak{L}$ . It follows that  $\mathfrak{L}$  is a finite separable extension of  $\mathfrak{K}$  such that  $M_{W_0r,C}^{\mathfrak{L}} := M_{W_0r,C}^{\mathfrak{L}} \otimes_{\mathfrak{R}(\mathfrak{L})} \mathfrak{L} = M_{W_0r,C}^{\mathfrak{K}} \otimes_{\mathfrak{K}} \mathfrak{L}$  is isomorphic to a finite direct sum of full matrix algebras  $M_{W_0r,C,i}^{\mathfrak{L}} \simeq \text{End}_{\mathfrak{L}}(\mathfrak{L}^{d_i})$  over  $\mathfrak{L}$ . Let  $\Pi_i$  denote the projection homomorphism  $M_{W_0r,C}^{\mathfrak{L}} \rightarrow M_{W_0r,C,i}^{\mathfrak{L}}$ . Let  $\tilde{\mathfrak{R}}(\mathfrak{L})$  be the integral closure of  $\mathfrak{R}(\mathfrak{L})$  in  $\mathfrak{L}$ , which is a Dedekind domain with fraction field  $\mathfrak{L}$ . The inclusion  $\mathfrak{R}(\mathfrak{L}) \subset \tilde{\mathfrak{R}}(\mathfrak{L})$  gives rise to a ramified covering  $\phi : \tilde{\mathfrak{U}} \rightarrow \mathfrak{U}$ . We may assume, by shrinking  $\mathfrak{U}^*$  (as in (v)) if necessary, that  $\phi : \tilde{\mathfrak{U}}^* := \phi^{-1}(\mathfrak{U}^*) \rightarrow \mathfrak{U}^*$  is finite étale.

Now  $\tilde{M}_{W_0r,C}^{\mathfrak{L}} := M_{W_0r,C}^{\mathfrak{L}} \otimes_{\mathfrak{R}(\mathfrak{L})} \tilde{\mathfrak{R}}(\mathfrak{L}) \subset M_{W_0r,C}^{\mathfrak{L}}$  is clearly an  $\tilde{\mathfrak{R}}(\mathfrak{L})$ -order in  $M_{W_0r,C}^{\mathfrak{L}}$ . Hence the projection  $\Pi_i(\tilde{M}_{W_0r,C}^{\mathfrak{L}})$  is an  $\tilde{\mathfrak{R}}(\mathfrak{L})$ -order in  $M_{W_0r,C,i}^{\mathfrak{L}} \simeq \text{End}_{\mathfrak{L}}(\mathfrak{L}^{d_i})$ . By [Artin 1999, Theorem IV.4.1, Proposition IV.4.7] this is contained in a maximal  $\tilde{\mathfrak{R}}(\mathfrak{L})$ -order in  $M_{W_0r,C,i}^{\mathfrak{L}}$  which must be a trivial Azumaya algebra of the form  $\text{End}_{\tilde{\mathfrak{R}}(\mathfrak{L})}(L_i)$  where  $L_i \subset \mathfrak{L}^{d_i}$  denotes an  $\tilde{\mathfrak{R}}(\mathfrak{L})$ -lattice. Hence we have

$$\tilde{M}_{W_0r,C}^{\mathfrak{L}} \subset \bigoplus_i \Pi_i(\tilde{M}_{W_0r,C}^{\mathfrak{L}}) \subset \bigoplus_i \text{End}_{\tilde{\mathfrak{R}}(\mathfrak{L})}(L_i) =: \tilde{M}_{W_0r,C}^{\mathfrak{L},\max}$$

This turns  $L_i$  into an  $\mathcal{H}_{\tilde{\mathfrak{R}}(\mathfrak{L})}$ -module, and proves (vi).

Assertions (vii) and (viii): Localizing at  $\tilde{\mathfrak{U}}^*$  we obtain  $\tilde{M}_{W_0r,C}^{\mathfrak{L}^*} \subset \bigoplus_i \text{End}_{\tilde{\mathfrak{R}}(\mathfrak{L}^*)}(L_i^*)$ , where  $L_i^* := L_i \otimes_{\tilde{\mathfrak{R}}(\mathfrak{L})} \tilde{\mathfrak{R}}(\mathfrak{L}^*)$  is an  $\tilde{\mathfrak{R}}(\mathfrak{L}^*)$ -lattice in  $\mathfrak{L}^{d_i}$ . Since  $\tilde{M}_{W_0r,C}^{\mathfrak{L}^*}$  is separable, by (v), we have  $\tilde{M}_{W_0r,C}^{\mathfrak{L}^*} = (\tilde{M}_{W_0r,C}^{\mathfrak{L}^*})^* := \text{Hom}_{\tilde{\mathfrak{R}}(\mathfrak{L}^*)}(\tilde{M}_{W_0r,C}^{\mathfrak{L}^*}, \tilde{\mathfrak{R}}(\mathfrak{L}^*))$ . As in the proof of [Artin 1999, Corollary IV.4.5] this implies that  $\tilde{M}_{W_0r,C}^{\mathfrak{L}^*}$  is a maximal  $\tilde{\mathfrak{R}}(\mathfrak{L}^*)$ -order, hence we actually have  $\tilde{M}_{W_0r,C}^{\mathfrak{L}^*} = \bigoplus_i \text{End}_{\tilde{\mathfrak{R}}(\mathfrak{L}^*)}(L_i^*)$ , proving (vii). When we take  $\tilde{v}$  lying above a  $v \in \mathfrak{U}^* \cap C$ , then specializing at  $\tilde{v}$  and comparing (iv) and (vii) we obtain (viii). Observe that the structural result (vi) implies that  $\phi$  can not be ramified at  $v$ . Indeed, when assuming the contrary then (vi) would imply that the number of discrete series characters of  $\mathcal{H}_v$  with generic central character  $W_0r$  would be strictly smaller than the number of such discrete series characters of  $\mathcal{H}_{v'}$  with  $v' \in C$  in a small neighborhood of  $v$ . This contradicts [Opdam and Solleveld 2010, Corollary 5.11].  $\square$

**Proposition 3.8.** *Let  $b \in \mathcal{B}_{\text{gm}}$ . The family  $\mathcal{Q}_b^{\text{reg}} \ni v \rightarrow \epsilon(b; v) \text{Ind}_D(b; v)$  is continuous (in the sense of [Opdam and Solleveld 2010, Section 3]).*

*Proof.* The discrete series character  $\epsilon(b; v) \text{Ind}_D(b; v)$  of  $\mathcal{H}_v$  has generic central character  $\text{gcc}_v(\pi_v) = W_0r$  with  $r = r_b$  by Corollary 2.8. By [Opdam and Solleveld 2010, Definition 5.10] we know therefore that  $\epsilon(b; v) \text{Ind}_D(b; v)$  is also the specialization at  $v$  of a unique continuous family of generic irreducible discrete series characters  $\chi \in \Delta_{W_0r_b}^{\text{gen}}(\mathcal{R})$  with generic central character  $W_0r_b$  on  $\mathcal{Q}_b^{\text{gen}}$ . By [Opdam and Solleveld 2010, Corollary 5.8]  $\Delta_{W_0r_b}(\mathcal{R})$ , is a constant sheaf with finite fiber. Let  $C$  be a connected component of  $\mathcal{Q}_b^{\text{reg}}$ , and let  $\mathcal{C}$  be any irreducible real curve in

$\mathcal{Q}$  which intersects  $C$ . Let  $I_{\mathcal{C}} \subset \mathcal{C} \cap C$  be connected. By the above it is enough to show that  $\epsilon(b; \mathbf{v}) \text{Ind}_D(b; \mathbf{v})$  and  $\chi_{\mathbf{v}}$  are equivalent when  $\mathbf{v} \in I_{\mathcal{C}}$ . In other words, it is enough to show that for all  $\mathbf{v} \in I_{\mathcal{C}}$  we have  $\lim_{\epsilon \rightarrow 0} [\chi_{\mathbf{v}^\epsilon}] = b$ . By Proposition 3.7, the restriction of  $\chi$  to  $\mathcal{C} \cap C$  is realized by an algebraic model  $L$  defined over some Zariski-open set  $\tilde{\mathcal{U}}$  of a ramified cover  $\tilde{\mathcal{C}}$  of  $\mathcal{C}$ , such that  $I_{\mathcal{C}} \subset \tilde{\mathcal{U}}$  and there is no ramification at the points of  $I_{\mathcal{C}}$ . Choose a lift  $\tilde{I}_{\mathcal{C}}$  of  $I_{\mathcal{C}}$ .

By Corollary 2.8 we know that  $b = \text{Ind}_s(b_s)$ , where  $\text{gcc}_B(b) = W_0 r$  for some generic residual point  $r = sc$  with  $s \in T_u$  a fixed special point, and  $c = \exp(\xi)$  with  $\xi$  a generic linear residual point for  $\mathbb{H}(R_{s,1}, T_s(E), F_{s,1}; k_s)$ . By Proposition 3.7 we know that  $\epsilon(b, C) \text{Ind}_D(b, C; \mathbf{v})$  is realized by an algebraic family  $L$  defined over  $\mathfrak{R}(\tilde{\mathcal{U}}^*)$ . By shrinking  $\mathcal{U}^*$  if necessary, we may assume that for all  $\tilde{\mathbf{v}} \in \tilde{\mathcal{U}}^*$  we have, for all  $r, r' \in W_0 r$ , that  $sW_s c \neq s'W_{s'} c'$  (with  $r' = s'c'$ ) if and only if  $sW_s c(\mathbf{v}) \cap s'W_{s'} c'(\mathbf{v}) = \emptyset$  with  $\mathbf{v} = \phi(\tilde{\mathbf{v}})$ . Let  $m_s$  be the ideal in  $\mathfrak{R}(\tilde{\mathcal{U}}^*)[X]$  corresponding to the finite set  $sW_s c$  of  $\mathfrak{R}(\tilde{\mathcal{U}}^*)$ -points of  $T$ . By our choice of  $\mathfrak{R}(\tilde{\mathcal{U}}^*)$ , we have that  $m_s + m'_s = \mathfrak{R}(\tilde{\mathcal{U}}^*)[X]$  whenever  $sW_s c \neq s'W_{s'} c'$ . Hence by the Chinese remainder theorem we have

$$(\mathfrak{R}(\tilde{\mathcal{U}}^*)[X])_{\widehat{W_0 r}} \simeq \bigoplus_{s' \in W_0 s} (\mathfrak{R}(\tilde{\mathcal{U}}^*)[X])_{\widehat{s'W_{s'} c'}}$$

Let  $1 = \sum_{s' \in W_0 s} e_{s'}$  be the corresponding decomposition into orthogonal idempotents of  $1 \in (\mathfrak{R}(\tilde{\mathcal{U}}^*)[X])_{\widehat{W_0 r}}$ . Let  $\mathcal{H}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)} = \mathcal{H}_\Lambda \otimes_\Lambda \mathfrak{R}(\tilde{\mathcal{U}}^*)$ . Since  $\mathcal{H}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)}$  contains the Bernstein subalgebra  $\mathcal{A}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)} \simeq \mathfrak{R}(\tilde{\mathcal{U}}^*)[X]$ , we can define the idempotents  $e_s \in (\mathcal{H}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)})_{\widehat{W_0 r}}$ . Since  $\text{gcc}(L_b) = W_0 r$ , we can consider  $L$  as a module over  $(\mathcal{H}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)})_{\widehat{W_0 r}}$ . Hence the  $e_s$  act on  $L$ , and are mapped to idempotent elements in  $\text{End}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)}(L)$  such that  $\text{Id} = \sum_{s' \in W_0 s} e_{s'}$ .

Following Lusztig [1989a, Lemmas 8.14, 8.15] we know that

$$\mathcal{H}_{s, \mathfrak{R}(\tilde{\mathcal{U}}^*)} := (\mathcal{H}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)}(\mathcal{R}_s))_{\widehat{W_s c}} \rtimes \Gamma_s$$

is isomorphic to the algebra  $(\mathcal{H}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)})_{s, W_0 r} := e_s (\mathcal{H}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)})_{\widehat{W_0 r}} e_s$ , via the map (in the notation of [loc. cit.])  $f.T_{w,s}.\gamma \rightarrow f.e_s.T_w.e_s.T_\gamma.e_s$ . Hence the finite, locally free  $\mathfrak{R}(\tilde{\mathcal{U}}^*)$  module  $L_s := e_s L$  is a module over  $\mathcal{H}_{s, \mathfrak{R}(\tilde{\mathcal{U}}^*)}$ , and in particular over the finite-type Hecke subalgebra

$$\mathcal{H}_{s, \mathfrak{R}(\tilde{\mathcal{U}}^*), 0} := \mathcal{H}_{\mathfrak{R}(\tilde{\mathcal{U}}^*)}(W(R_{1,s})) \rtimes \Gamma_s$$

in the obvious way. By shrinking  $\mathfrak{R}(\tilde{\mathcal{U}}^*)$  if necessary we may assume that  $L_s$  is actually a free  $\mathfrak{R}(\tilde{\mathcal{U}}^*)$ -module. Let  $\chi_s$  denote the character of  $L_s$  (considered as a function of  $\mathbf{v} \in I_{\mathcal{C}}$ ). By Corollary 2.2 we see that for each  $\mathbf{v} \in I_{\mathcal{C}}$  we have  $\lim_{\epsilon \rightarrow 0} [\chi_{\mathbf{v}^\epsilon}] = \text{Ind}_s(b_{\mathbf{v},s})$ , where  $b_{\mathbf{v},s} = \lim_{\epsilon \rightarrow 0} [\chi_{s, \mathbf{v}^\epsilon}]$ . This limit clearly only depends on the restriction of  $L_s$  to  $\mathcal{H}_{s, \mathfrak{R}(\tilde{\mathcal{U}}^*), 0}$ . Now it is well known that (see, e.g.,



[Opdam 1995, Theorem 5])<sup>2</sup> the irreducible characters of  $\mathcal{H}_{s, \mathfrak{R}(\tilde{\mathcal{U}}^*), 0}$  take values in  $\Lambda$ . This implies that  $b_{v,s}$  is independent of  $v \in I_{\mathcal{C}}$ , as desired.  $\square$

**Corollary 3.9.**  $\epsilon(b, \cdot)$  is locally constant on  $\mathcal{Q}_b^{\text{reg}}$ .

*Proof.* The continuity of  $\mathcal{Q}_b^{\text{reg}} \ni v \rightarrow \epsilon(b; v) \text{Ind}_D(b; v)$  implies that on each connected component  $C$  of  $\mathcal{Q}_b^{\text{reg}}$  the sign  $C \ni v \rightarrow \epsilon(b, v)$  is continuous, hence constant.  $\square$

**Definition 3.10.** If  $C \subset \mathcal{Q}_b^{\text{reg}}$  is a connected component, we define  $\epsilon(b, C) := \epsilon(b, v) \in \{\pm 1\}$  for any choice of  $v \in C$ .

**3B. Limits of discrete series.** Let  $b \in \mathcal{B}_{\text{gm}}$  let  $C \subset \mathcal{Q}_b^{\text{reg}}$  be a connected component, and let  $v_0 \in \partial C$ . Choose a connected real algebraic curve  $\mathcal{C}_r = \mathcal{C} \cap \mathcal{Q} \subset \mathcal{Q}$  which meets  $C$ , and contains  $v_0 \in \mathcal{C}_r$  as a smooth point of  $\mathcal{C}_r$ . Extend  $\mathcal{C}_r$  to a complex affine algebraic curve  $\mathcal{C} \subset \mathcal{Q}_{\mathbb{C}}$ . Assume we have chosen the structures as in Proposition 3.7 with respect to  $W_0r = \text{gcc}_B(b)$ ,  $v_0$ ,  $C$  and  $\mathcal{C}$ . Let  $v$  be a point in  $\mathcal{C} \cap C$  such that  $v_0$  and  $v$  are in the same connected component of  $\mathcal{C} \cap \bar{C}$ . Given a  $\tilde{v} \in \tilde{\mathcal{U}}^*$  above  $v \in \mathcal{C} \cap C$ , let us denote by  $L_b$  the unique  $\mathfrak{R}(\mathcal{U})$ -lattice as in Proposition 3.7(vi) such that  $L_{i, \tilde{v}} \simeq V_{\chi_{b,v}}$  (according to Proposition 3.7(viii)), where  $\chi_{b,v} = \epsilon(b; v) \text{Ind}_D(b; v)$ . The interval  $I_{\mathcal{C}} \subset \mathcal{C}_r$  connecting  $v$  to  $v_0$  has a unique lift  $\tilde{I}_{\mathcal{C}}$  starting at  $\tilde{v} \in \tilde{\mathcal{U}}^*$ . Let  $\tilde{v}_0 \in \tilde{\mathcal{U}}$  be the unique endpoint of this lifted interval lying above  $v_0$ .

**Definition 3.11.** We denote by  $\text{Ind}_D(b, C; v_0)$  the unique virtual character of  $\mathcal{H}_{v_0}$  such that  $\epsilon(b, C) \text{Ind}_D(b, C; v_0)$  is realized by  $L_{b, \tilde{v}_0}$ . We call this representation the *limit of the family of discrete series*  $\chi_b = \epsilon(b; v) \text{Ind}_D(b; v)$  along  $\mathcal{C}$  from  $C$  at  $v_0$ .

**Remark 3.12.** A priori  $\text{Ind}_D(b, C; v_0)$  may depend on the chosen curve and the model  $L_b$  of  $\epsilon(b; v) \text{Ind}_D(b)$  defined over  $\mathfrak{R}(\mathcal{U})$ , but we suppress this from the notation.

**Corollary 3.13.**  $\epsilon(b, C) \text{Ind}_D(b, C; v_0)$  is a genuine tempered character.

*Proof.* Since the limit  $\epsilon(b, C) \text{Ind}_D(b, C; v_0)$  was defined by specializing the  $\mathfrak{R}(\mathcal{U})$ -module  $L_b$  at  $\tilde{v} = \tilde{v}_0$ , it is by definition a genuine character.

The central character of  $L_b(\tilde{v})$  is  $W_0r(v)$  (with  $v = \phi(\tilde{v})$ ), hence for all  $z \in \mathcal{Z}_{\mathfrak{R}(\mathcal{U})}$  we have  $z(W_0r) \in \mathfrak{R}(\mathcal{U})$ . Recall that  $\mathcal{Z}_{\mathfrak{R}(\mathcal{U})} = \mathcal{A}_{\mathfrak{R}(\mathcal{U})}^{W_0}$ , hence the generalized  $\mathcal{A}_{\mathfrak{R}(\mathcal{U})}$  weight spaces belongs to the set  $W_0r \subset T(\mathfrak{R}(\mathcal{U}))$ .

Let  $r'(v_0) \in W_0r(v_0)$ , and let  $\tilde{v} \in \tilde{I}_{\mathcal{C}}$  be close to  $\tilde{v}_0$ . Choose a basis  $\{x_1, \dots, x_n\}$  of  $X$ , and consider the corresponding commuting elements  $\theta_i \in \mathcal{A}$  acting in  $L_b(\tilde{v})$ . For each  $i$  consider the set  $S_{i, r'(v_0)} := \{r'' \in W_0r \mid x_i(r''(v_0)) = x_i(r'(v_0))\}$  of

<sup>2</sup>For a discussion of the rationality properties of characters for finite Hecke algebras, see also [Geck and Pfeiffer 2000, Section 9.3], and the references therein.

generalized eigenvalues of  $\theta_i$  (acting in  $L_b(\tilde{\mathbf{v}})$ ) which coalesce to  $x_i(r'(\mathbf{v}_0))$  at  $\mathbf{v} = \mathbf{v}_0$ . Then the projection  $\Pi_{r',\tilde{\mathbf{v}}}$  onto the direct sum of the generalized  $\mathcal{A}$ -weight spaces in  $L_b(\tilde{\mathbf{v}})$  which coalesce to  $r'(\mathbf{v}_0)$  is the composition of the commuting projection operators  $\Pi_{i,r',\tilde{\mathbf{v}}}$  onto the direct sum of the generalized eigenspaces  $r''(\mathbf{v})$  of  $\theta_i(\tilde{\mathbf{v}})$  with  $r'' \in S_{i,r'(\mathbf{v}_0)}$ . By holomorphic functional calculus we have

$$\Pi_{i,r',\tilde{\mathbf{v}}} = \frac{1}{2\pi i} \int_{\partial D_i} (z \text{Id} - \theta_i(\tilde{\mathbf{v}}))^{-1} dz,$$

where  $D_i$  is a fixed disk around  $x_i(r'(\mathbf{v}_0))$  such that  $x_i(r''(\mathbf{v})) \in D_i$  if and only if  $r'' \in S_{i,r'(\mathbf{v}_0)}$  (such  $D_i$  clearly exist, provided  $\mathbf{v}$  is sufficiently close to  $\mathbf{v}_0$ ). Hence the  $\Pi_{i,r',\tilde{\mathbf{v}}}$  are continuous in  $\tilde{\mathbf{v}}$ . In particular  $\Pi_{r',\tilde{\mathbf{v}}}$  is continuous in  $\tilde{\mathbf{v}}$ , implying that the dimension of its image is independent of  $\mathbf{v}$ . Therefore  $r'(\mathbf{v}_0)$  is a generalized  $\mathcal{A}$ -weight of  $L_b(\tilde{\mathbf{v}}_0)$  if and only if for some  $\mathbf{v} \in I_{\mathcal{C}}$  sufficiently close to  $\mathbf{v}_0$ , there exists a  $r''(\mathbf{v})$  with  $r''(\mathbf{v}_0) = r'(\mathbf{v}_0)$  (i.e.,  $r'' \in \bigcap_i S_{i,r'(\mathbf{v}_0)}$ ) such that  $r''(\mathbf{v})$  is a generalized  $\mathcal{A}$ -weight of the discrete series representation  $L_b(\tilde{\mathbf{v}})$ . In particular,  $r'(\mathbf{v})$  is a limit of  $\mathcal{A}$ -weights which meet the Casselman condition for temperedness [Opdam 2004, Lemma 2.20]. This is a closed condition, hence the generalized  $\mathcal{A}$ -weights of  $L_b(\tilde{\mathbf{v}}_0)$  satisfy the Casselman conditions themselves. The mentioned lemma implies that  $L_b(\tilde{\mathbf{v}}_0) = \epsilon(b, C) \text{Ind}_D(b, C; \mathbf{v}_0)$  is tempered.  $\square$

**Corollary 3.14.** *The tempered character  $\epsilon(b, C) \text{Ind}_D(b, C; \mathbf{v}_0)$  is a member of an algebraic family of characters of  $\mathcal{H}_{\tilde{\mathfrak{X}}(\mathfrak{A})}$ -characters with values in  $\tilde{\mathfrak{X}}(\mathfrak{A})$ . For generic element  $\tilde{\mathbf{v}} \in \tilde{\mathfrak{X}}$  this character is irreducible, and for  $\tilde{\mathbf{v}} \in \tilde{\mathfrak{X}}^* \cap C$  it is an irreducible discrete series.*

**Remark 3.15.** The limit  $\epsilon(b, C) \text{Ind}_D(b, C; \mathbf{v}_0)$  may be irreducible or not. In the case of the Hecke algebras of type  $C_n^{(1)}$  the limits of discrete series were constructed using the geometric model [Kato 2009] of characters of the generic affine Hecke algebra of this type. In this situation it is known that the limits of the discrete series at nontrivial singular parameters are always irreducible [Ciubotaru et al. 2012]. In general the limit to the trivial parameter  $\mathbf{v} = 1$  will be a reducible character of the affine Weyl group (the only exceptions being the “one  $W$ -type” discrete series characters).

**Proposition 3.16.**  $\lim_{\epsilon \rightarrow 0} [\text{Ind}_D(b, C; \mathbf{v}_0^\epsilon)] = b \in \mathcal{B}_{\text{gm}} \subset \bar{\mathcal{R}}_{\mathbb{Z}}(W).$

*Proof.* The proof is exactly the same as the proof of Proposition 3.8.  $\square$

**Corollary 3.17.** *The covering  $\phi$  is not ramified at the points of  $\mathcal{C} \cap \bar{C}$ .*

*Proof.* The argument of Proposition 3.8 proves that  $b_s = \lim_{\epsilon \rightarrow 0} [\chi_{s, \mathbf{v}^\epsilon}]$  for any  $\mathbf{v}$  in a neighborhood of  $\mathbf{v}_0$ . On the other hand, the discrete series of  $\mathcal{H}_{\mathbf{v}}$  are parametrized by the  $b \in \mathcal{B}_{\mathbf{v}-\text{gm}} = \mathcal{B}_{\text{gm}} \cap \mathcal{Y}_{\mathbf{v}-\text{gm}}$  by Corollary 2.2, Proposition 2.6 and Section 2B4. Moreover, for  $b$  in the image of  $\text{Ind}_s$ , the limit map  $b \rightarrow b_s$  is an isometry by

Corollary 2.2. Hence the generic discrete series with generic central character  $W_0r$  are also parametrized by the corresponding elliptic class  $b_s$  of  $W_s$ . Therefore the algebraic continuation of the discrete series characters  $\epsilon(b, C) \text{Ind}_D(b; \mathbf{v})$  (realized by  $L_b$ ) on  $\tilde{\mathfrak{U}}^*$  can not have monodromy around  $\mathbf{v}_0$ , by the above. We conclude that the character values are regular functions in a neighborhood of  $\mathbf{v}_0 \in \mathfrak{U}$ .  $\square$

**3C. The rationality of the generic formal degree.**

**3C1.** *The universality of the rational factors of the generic formal degree.* The following result follows now simply from [Ciubotaru and Opdam 2015, Corollary 5.7; Ciubotaru et al. 2014; Opdam and Solleveld 2010]:

**Theorem 3.18.** *Fix  $b \in \mathcal{B}_{\text{gm}}$ . The formal degree of a continuous family of virtual discrete series characters  $\mathcal{Q}_b^{\text{reg}} \ni \mathbf{v} \rightarrow \text{Ind}_D(b; \mathbf{v})$  as a function of  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$  is a rational function of the form  $d_b m_b$ , with  $d_b \in \mathbb{Q}^\times$ .*

*Proof.* By [Ciubotaru and Opdam 2015, Corollary 5.7] the formal degree of  $\text{Ind}_D(b; \mathbf{v})$  is a linear combination of rational functions of the  $\mathbf{v}_s$ , which only depends on the elliptic class  $\lim_{\epsilon \rightarrow 0} \text{Ind}_D(b; \mathbf{v}^\epsilon)$ . This is, by definition,  $b$  (and therefore independent of  $\mathbf{v}$ ). On the other hand we have shown that this family is continuous and (by [Ciubotaru et al. 2014]) has generic central character  $W_0r_b$ . By [Opdam and Solleveld 2010, Theorem 4.6] we conclude that the formal degree has the form  $d_b(C) m_b$  for some constants  $d_b(C)$  depending on the connected component  $C$  of  $\mathcal{Q}_b^{\text{reg}}$  in which  $\mathbf{v}$  lies. But the rationality implies that these constants need to be equal on all chambers.  $\square$

**Corollary 3.19.** *We can choose the basis vector  $b \in \mathcal{B}_{\text{gm}}$  uniquely such that  $d_b > 0$ . With this choice,  $\epsilon(b, C)$  will be equal to the sign of  $m_b(\mathbf{v})$  for  $\mathbf{v} \in C$ .*

**3D. Proof of Theorem 1.1.** The proof of Theorem 1.1 is all completed now, and we point out where the various parts of it have been proved. Part (a) is in Proposition 2.6 and Corollary 3.19. Part (b) is in Section 2B4. Part (c) is Corollary 2.8. Part (d) is in Proposition 3.8. Part (e) is Corollary 3.9. Part (f) follows from Corollary 2.2, Proposition 2.6, and Section 2B4. Part (g) is Theorem 3.18.

**4. Explicit results; comparison with the Kazhdan–Lusztig–Langlands classification**

In this section we will compare the uniform classification of the discrete series with the Kazhdan–Lusztig–Langlands classification when an affine Hecke algebra arises in the context of a unipotent type of an unramified simple group defined over a nonarchimedean local field. We will also compute, for all affine Hecke algebras of simple type, the canonically positive basis  $\mathcal{B}_{\text{gm}}$  and the fundamental rational constants  $d_b$  appearing in the generic Plancherel measure. We will moreover

explain how the general semisimple case can be reduced to the case of simple type. In addition, we will show that in each connected component of  $\mathcal{Q}_b^{\text{reg}}$  the generic discrete series character  $\epsilon(b; \mathbf{v}) \text{Ind}_D(b; \mathbf{v})$  takes values in  $\mathcal{Q}_\Lambda$ , the quotient field of  $\Lambda$ . Needless to say, the results in this section are based on case-by-case methods.

**4A. Determination of the canonically positive basis  $\mathcal{B}_{\text{gm}}$ .**

**4A1.** *The sign of  $m_b(\mathbf{v})$ .* In light of Corollary 3.19, we need to analyze the sign of  $m_b(\mathbf{v})$ . Specialize

$$\mathbf{v}(s) = \mathbf{v}^{f_s}, \quad \text{with } \mathbf{v} > 1, f_s \in \mathbb{R}.$$

Write  $r = sc$  as before and let  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$  denote the corresponding graded affine Hecke algebra. Recall that the parameter function  $k_s$  is given by [Opdam and Solleveld 2010, (26)]

$$k_s(\alpha) = \begin{cases} \log_{\mathbf{v}}(v_{\alpha^\vee}^2) & \text{if } \alpha \in R_0 \cap R_1, \text{ or if } \alpha = 2\beta, \beta \in R_0 \text{ and } \beta(s) = 1, \\ \log_{\mathbf{v}}(v_{\alpha^\vee}^2 v_{2\alpha^\vee}^4) & \text{if } \alpha = 2\beta, \beta \in R_0, \beta(s) = -1. \end{cases} \tag{18}$$

Write  $c = \mathbf{v}^{\bar{c}}$ . The following proposition says that the sign of the function  $m_{W_0,r}$  can in fact be detected at the graded Hecke algebra level.

**Proposition 4.1.** *The sign of  $m_{W_0,r}$  from (13) equals the sign of the expression*

$$\bar{m}_{W_0\bar{c}} = \frac{\prod'_{\alpha \in R_{s,1}} \alpha(\bar{c})}{\prod'_{\alpha \in R_{s,1}} (\alpha(\bar{c}) - k_s(\alpha))}. \tag{19}$$

*This expression is a polynomial which equals the product of  $n$  rational linear forms in the parameters  $k_s(\alpha)$  (where  $n$  is the rank of  $R_0$ ).*

*Proof.* For every  $\alpha \in R_1$ ,  $\alpha(s)$  is a root of unity. Write  $R_1 = R_{s,1} \sqcup R_1^{s,-1} \sqcup R_1^{s,z}$ , where  $R_1^{s,-1} = \{\alpha \in R_1 \mid \alpha(s) = -1\}$  and  $R_1^{s,z} = \{\alpha \in R_1 \mid \alpha(s)^2 \neq 1\}$ . If  $\alpha$  is a root in  $R_1 \setminus R_0$ , then  $\alpha$  is a root of type  $A_1$  in  $B_n$  and from the classification of isolated semisimple elements  $s$  in this situation, we see that  $\alpha \in R_{s,1}$ .

We break up the product expression for  $m_{W_0r}$  according to the three types of roots:  $R_{s,1}$ ,  $R_1^{s,-1}$ ,  $R_1^{s,z}$ . Take  $R_1^{s,-1}$  first and we analyze the contribution of its numerator and denominator. The numerator is a product of expressions  $(-\alpha(c) - 1)(-\alpha(c)^{-1} - 1) > 0$ , since  $\alpha(c) > 0$ , one factor for each positive root  $\alpha \in R_1^{s,-1}$ . For the denominator, for each positive root  $\alpha \in R_1^{s,-1}$  (which by the remark above it is in  $R_0$ ), we have a factor  $(-v_{\alpha^\vee}^{-2}\alpha(c)^{-1} - 1)(-v_{\alpha^\vee}^{-2}\alpha(c) - 1) > 0$ . Therefore, the part of the expression corresponding to  $R_1^{s,-1}$  is positive.

Consider now  $R_1^{s,z}$ . Its contribution equals

$$\frac{\prod'_{\alpha \in R_1^{s,z}} (\alpha(s)\alpha(c) - 1)}{\prod'_{\alpha \in R_1^{s,z}} (\alpha(s)v_{\alpha^\vee}^{-2}\alpha(c) - 1)}.$$

The argument in [Opdam 2004, Theorem 3.27(v)] shows that both the numerator and the denominator are polynomial expressions in  $\mathbf{v}$  with rational (in fact integer) coefficients. Moreover, since  $\alpha(s)$  is not real, these polynomials do not afford real roots in  $\mathbf{v}$ . It follows that they are always positive or always negative for real  $\mathbf{v}$ . But it is clear that for  $\mathbf{v} = 0$  the fraction above equals  $1 > 0$ , and therefore it is always positive.

In conclusion, the sign of  $m_{W_0r}$  equals the sign of the expression

$$m_{W_0r} = \frac{\prod'_{\alpha \in R_{s,1}} (\alpha(c)^{-1} - 1)}{\prod'_{\alpha \in R_{s,1}} (v_{\alpha^\vee}^{-1} \alpha(c)^{-1/2} + 1) \prod'_{\alpha \in R_{s,1}} (v_{\alpha^\vee}^{-1} v_{2\alpha^\vee}^{-2} \alpha(c)^{-1/2} - 1)}.$$

The numerator can be rewritten as  $\prod_{\alpha \in R_{s,1}^+} \alpha(c)^{-1} (-1)(\alpha(c) - 1)^2$  and therefore its sign is  $(-1)^{n_s}$ , where  $n_s = \#\{\alpha \in R_{s,1}^+ \mid \alpha(c) \neq 1\} = \#\{\alpha \in R_{s,1}^+ \mid \alpha(\bar{c}) \neq 0\}$ . But this is also the sign of the numerator in (19).

Let  $\alpha \in R_0^+ \cap R_{s,1}$  be given. Then  $\alpha$  and  $-\alpha$  give a contribution in the denominator of  $v_{\alpha^\vee}^{-4} (\alpha(c)^{-1} - v_{\alpha^\vee}^2) (\alpha(c) - v_{\alpha^\vee}^2) = v_{\alpha^\vee}^{-4} (\mathbf{v}^{-\alpha(\bar{c})} - \mathbf{v}^{k_s(\alpha)}) (\mathbf{v}^{\alpha(\bar{c})} - \mathbf{v}^{k_s(\alpha)})$ . Clearly, the sign of this expression is the same as the sign of  $(-\alpha(\bar{c}) - k_s(\alpha)) (\alpha(\bar{c}) - k_s(\alpha))$ .

Now suppose that  $\alpha = 2\beta$  with  $\beta \in R_0$ . If  $\beta(s) = 1$ , the factors of the form  $(v_{\alpha^\vee}^{-1} \alpha(r)^{-1/2} + 1) = (v_{\alpha^\vee} \beta(c)^{-1} + 1)$  are all positive and can be ignored. So the contribution in the denominator comes from the factors  $(v_{\alpha^\vee}^{-1} v_{2\alpha^\vee}^{-2} \alpha(r)^{-1/2} - 1) = (\mathbf{v}^{-k_s(\alpha)/2} \beta(c)^{-1} - 1)$ . Grouping together the factors corresponding to  $\alpha$  and  $-\alpha$  as before and multiplying by powers of  $\mathbf{v}$ , we see that the contribution to the sign is given by  $(\mathbf{v}^{\alpha(\bar{c})/2} - \mathbf{v}^{k_s(\alpha)/2}) (\mathbf{v}^{-\alpha(\bar{c})/2} - \mathbf{v}^{k_s(\alpha)/2})$ . But this has the same sign as  $(-\alpha(\bar{c}) - k_s(\alpha)) (\alpha(\bar{c}) - k_s(\alpha))$ .

Finally, if  $\beta(s) = -1$ , then the factor

$$(v_{\alpha^\vee}^{-1} v_{2\alpha^\vee}^{-2} \alpha(r)^{-1/2} - 1) = -(v_{\alpha^\vee}^{-1} v_{2\alpha^\vee}^{-2} \beta(c)^{-1} + 1)$$

is negative and the contributions of these factors for  $\alpha$  and  $-\alpha$  cancel out. Thus we remain with the factor  $(v_{\alpha^\vee}^{-1} \alpha(r)^{-1/2} + 1) = (-\mathbf{v}^{-k_s(\alpha)/2} \beta(c) + 1)$  and the same analysis as in the previous case applies.

The regularity of  $m_{W_0r}$  on  $\mathcal{Q}$  implies that  $\bar{m}_{W_0\bar{c}}$  is bounded if the  $k_s(\alpha)$  take arbitrary real values. At the same time,  $\bar{m}_{W_0\bar{c}}$  is a rational function whose numerator and denominator are products of *rational* linear expressions in the  $k_s(\alpha)$ , with (as follows from Definition 2.3) exactly  $n$  more factors in the numerator than in the denominator. It follows that the denominator divides the numerator, leaving a polynomial in the  $k_s(\alpha)$  of degree  $n$  of the desired form.  $\square$

**Example 4.2.** Consider the affine Hecke algebra of type  $G_2$  with parameters  $k_1$  and  $k_2$  as in Section 4B3 below and in Table 1. In particular, let

$$\bar{c}_1 = [k_1, k_2], \quad \bar{c}_2 = [k_1, -k_1 + k_2], \quad \text{and} \quad \bar{c}_3 = \left[ k_1, \frac{1}{2}(-k_1 + k_2) \right],$$

be the three generic linear residual points in the graded affine Hecke algebra of type  $G_2$ . The corresponding polynomials in Proposition 4.1 are:

$$\begin{aligned} \bar{m}_{W_0\bar{c}_1} &= \frac{1}{36}(k_1 + 2k_2)(2k_1 + 3k_2), \\ \bar{m}_{W_0\bar{c}_2} &= -\frac{1}{36}(2k_1 - 3k_2)(k_1 - 2k_2), \\ \bar{m}_{W_0\bar{c}_3} &= \frac{1}{36}k_1k_2. \end{aligned} \tag{20}$$

Notice that the zeros of these polynomials give precisely the sets  $\mathcal{Q}_{b_i}^{\text{sing}}$ ,  $1 \leq i \leq 3$ , see [Heckman and Opdam 1997, Proposition 4.15; Opdam and Solleveld 2010, Table 4].

**Remark 4.3.** Fix  $b \in \mathcal{B}_{\text{gm}}$  and suppose  $\mathbf{v}_0 \in \mathcal{Q}_b^{\text{reg}} \setminus \mathcal{Q}_b^{\text{gen}}$  is a nongeneric, but regular parameter. By definition,  $b$  is in  $\mathcal{B}_{\mathbf{v}_0-m}$  and let  $r_0 = \lim_{\mathbf{v} \rightarrow \mathbf{v}_0} r_b(\mathbf{v})$ . The irreducible discrete series at  $\mathbf{v}_0$  in the family defined by  $b$  is  $\text{ds}(b, \mathbf{v}_0) = \epsilon(b; \mathbf{v}_0) \text{Ind}_D(b; \mathbf{v}_0)$ . By Theorem 1.1, the sign  $\epsilon(b; \mathbf{v})$  is locally constant and therefore taking  $\lim_{\mathbf{v} \rightarrow \mathbf{v}_0}$  in the formula of Theorem 1.1(g), we see that  $\epsilon(b; \mathbf{v}_0)$  equals the sign of  $m_{W_0r}(\mathbf{v}_0) = \lim_{\mathbf{v} \rightarrow \mathbf{v}_0} m_{W_0r_b}(\mathbf{v})$ , where  $m_{W_0r_b}$  is defined by (13). This equals the sign of  $\bar{m}_{W_0\bar{c}_b}$ .

**4B. Tables.** We present the explicit form of the canonically positive basis  $\mathcal{B}_{\text{gm}}$ , as well as the generic residual central characters  $W_0r_b$ , the constants  $d_b$  in the case when  $\mathcal{R}$  is a simple root datum of type  $C_n^{(1)}$  (with three parameters),  $B_n^{(1)}$ ,  $C_n$  adjoint,  $G_2$ , and  $F_4$  (with two parameters). For the affine Hecke algebra of a simple, nonsimply laced root datum of arbitrary isogeny, one may deduce the relevant information from the cases listed above, by specializing the parameters appropriately and by the use of induction and restriction (see Section 4E).

**4B1.**  $C_n^{(1)}$ . Let

$$X = \mathbb{Z}^n = \langle \epsilon_1, \dots, \epsilon_n \rangle, \quad R_0 = \{ \pm \epsilon_i \pm \epsilon_j, i \neq j, \pm \epsilon_i \}, \quad F_0 = \{ \epsilon_i - \epsilon_{i+1}, \epsilon_n \}.$$

For simplicity of notation, we use the coordinates  $\epsilon_i$  for the basis of  $Y$  as well. We have  $W = X \rtimes W_0 = \mathbb{Z}R_0 \rtimes W_0$ . The affine simple roots are

$$F = \{ (\epsilon_i - \epsilon_{i+1}, 0) \cup \{ (2\epsilon_n, 0) \} \cup (-2\epsilon_1, 1) \}$$

and the affine Dynkin diagram (with parameters) is

$$v_0 \implies v_1 \text{ --- } v_1 \text{ --- } \dots \text{ --- } v_1 \longleftarrow v_2. \tag{21}$$

Here the affine simple root is  $\alpha_0 = (-2\epsilon_1, 1)$  and it gets the label  $v_0$ . Let  $\mathcal{H}(v_0, v_1, v_2)$  be the affine Hecke algebra with generators  $N_0, N_1, \dots, N_n$ . We need to switch to the Bernstein presentation. The algebra  $\mathcal{H}(v_0, v_1, v_2)$  is generated by  $N_1, \dots, N_n$

and  $\theta_1^{\pm 1}, \dots, \theta_n^{\pm 1}$  (here  $\theta_i = \theta_{\epsilon_i}$ ) subject to the relations

$$\begin{aligned} \theta_i N_i - N_i \theta_{i+1} &= (v_1 - v_1^{-1})\theta_i, & 1 \leq i \leq n - 1, \\ \theta_i N_j &= N_j \theta_i, & |i - j| \geq 2, \\ \theta_n N_n - N_n \theta_n^{-1} &= (v_2 - v_2^{-1})\theta_n + (v_0 - v_0^{-1}), \end{aligned} \tag{22}$$

the usual Hecke relations and the commutation of the  $\theta_i$ 's. In the change of presentation, we set  $\theta_i = N_0 N_{s_{\epsilon_i}}$ , where  $s_{\epsilon_i} \in W_0$  is the reflection corresponding to the root  $\epsilon_i$ .

It is immediate that the assignment  $N_0 \mapsto -v_0^{-1}$  gives a surjective algebra homomorphism onto the finite Hecke algebra  $\mathcal{H}_f(C_n, v_1, v_2)$  of type  $C_n$  with parameters  $v_1, v_2$ . Translating to the Bernstein presentation, we find that the assignment

$$N_i \mapsto N_i, \quad \theta_i \mapsto -v_0^{-1} N_{s_{\epsilon_i}}, \quad 1 \leq i \leq n, \tag{23}$$

extends to a surjective algebra homomorphism onto the Hecke algebra  $\mathcal{H}_f(C_n, v_1, v_2)$  of finite type. This allows us to lift every simple  $\mathcal{H}_f(C_n, v_1, v_2)$ -module to a simple module of the affine Hecke algebra. The simple  $\mathcal{H}_f(C_n, v_1, v_2)$ -modules are parametrized by bipartitions  $(\lambda, \mu)$  of  $n$ . It is particularly useful to use Hoefsmit's construction of such modules, see [Geck and Pfeiffer 2000, pages 322–325], since in that realization the  $N_{s_{\epsilon_i}}$  act diagonally.

We recall the construction. Denote by  $V_{(\lambda, \mu)}(v)$  the simple module of  $\mathcal{H}_f(C_n)$  parametrized by  $(\lambda, \mu)$ . Its basis is indexed by left-justified decreasing standard tableaux of shape  $(\lambda, \mu)$ . Let  $\dagger$  denote such a Young tableau. Then

$$N_{s_{\epsilon_j}} \cdot \dagger = \text{ct}(\dagger, n - j + 1)\dagger, \quad \text{where } \text{ct}(\dagger, k) = \begin{cases} v_1^{2(y-x)} v_2 & \text{if } k \text{ occurs in } \lambda, \\ -v_1^{2(y-x)} v_2^{-1} & \text{if } k \text{ occurs in } \mu, \end{cases}$$

where  $(x, y)$  are the coordinates of the box in which  $k$  occurs. (The coordinates  $(x, y)$  of a box in the Young tableau increase to the right in  $y$  and down in  $x$ .)

This means that in  $\tilde{V}_{(\lambda, \mu)}(v)$ , the lift of  $V_{(\lambda, \mu)}$  to the affine Hecke algebra, we have

$$\theta_j \cdot \dagger = -v_0^{-1} \text{ct}(\dagger, n - j + 1)\dagger. \tag{24}$$

The condition that a simple module is a discrete series module is that the eigenvalues of the product  $\theta_1 \cdot \theta_2 \cdots \theta_j$  are all smaller than 1 in absolute value, for all  $j = 1, \dots, n$ . From (24), we see that when the absolute value of the specialization of  $v_0$  is much larger than that of  $v_1$  and  $v_2$ , every  $V_{(\lambda, \mu)}(v)$  is a discrete series module. Moreover, the central characters of these modules are all distinct at generic values of the parameters, and since, by [Opdam and Solleveld 2010], the dimension of the space  $\bar{\mathcal{R}}_{\mathbb{Z}}(W)$  equals the number of bipartitions of  $n$ , it follows that the set  $\{\lim_{v \rightarrow 1} \tilde{V}_{(\lambda, \mu)}(v)\}$  is an orthonormal basis of  $\mathcal{Y}_{\text{gm}} = \bar{\mathcal{R}}_{\mathbb{Z}}(W)$ . In order to determine

the canonically positive basis  $\mathcal{B}_{\text{gm}}$ , it remains therefore to determine the signs  $\epsilon(b, \mathbf{v})$  for each  $b = \lim_{v \rightarrow 1} \tilde{V}_{(\lambda, \mu)}(v)$ .

To this end, we need to examine the formal degrees of these modules. Denote by  $R_0^{\text{sh}} = \{\pm \epsilon_i\}$ , the short roots, and by  $R_0^{\text{lo}} = \{\pm \epsilon_i \pm \epsilon_j\}$ , the long roots. Specialize

$$v_1 = v, \quad v_2 = v^{k_+ + k_-}, \quad v_0 = v^{k_+ - k_-},$$

where  $v > 1$  and  $k_-, k_+ \in \mathbb{R}$ . Notice that  $R_1 \setminus R_0 = \{\pm 2\epsilon_i\}$ . The formula for the generic formal degree [Opdam and Solleveld 2010, Theorem 4.6 and (40)] gives in our particular case that the formal degree of a discrete series  $\pi(b, \mathbf{v})$  with central character  $W_0 r_b(\mathbf{v})$  is

$$\text{fdeg}(\pi(b, \mathbf{v})) = \frac{d_b \epsilon(b, k_+, k_-) \prod'_{\alpha \in R_1} (\alpha(r_b(\mathbf{v}))^{-1} - 1)}{\prod'_{\alpha \in R_0^{\text{lo}}} (v^{-2} \alpha(r_b(\mathbf{v}))^{-1} - 1)} \cdot \frac{1}{\prod'_{\alpha \in R_0^{\text{sh}}} (v^{-2k_+} \alpha(r_b(\mathbf{v}))^{-1} - 1) \prod'_{\alpha \in R_0^{\text{sh}}} (v^{-2k_-} \alpha(r_b(\mathbf{v}))^{-1} + 1)},$$

where  $\epsilon(b, k_+, k_-)$  is a sign to be made explicit (see (28)). From [Ciubotaru et al. 2012, Theorem 4.7] (see the remark in the proof of [Opdam 2016, Theorem 4.12]), we know that

$$d_b = 1. \tag{25}$$

Fix a bipartition  $(\lambda, \mu)$ . The corresponding central character  $W_0 r_b(\mathbf{v})$  is the  $W_0$ -orbit of the string

$$r_{(\lambda, \mu)} = ((-v^{2(y-x)} v^{2k_-} \mid (x, y) \in \lambda); (v^{2(y'-x')} v^{-2k_+} \mid (x', y') \in \mu)). \tag{26}$$

and therefore

$$\bar{c}_{(\lambda, \mu)} = (\bar{c}_\lambda(k_-), \bar{c}_\mu(-k_+)), \quad \text{where } \bar{c}_\lambda(k) = ((y-x) + k \mid (x, y) \in \lambda).$$

We will use Proposition 4.1 to compute the signs. Denote by  $B_{|\lambda|}$  the root subsystem of  $R_0$  given by the roots that involve only coordinates  $\epsilon_i$ ,  $1 \leq i \leq |\lambda|$ . Similarly, let  $B_{|\mu|}$  be the root subsystem in coordinates  $\epsilon_j$ ,  $|\lambda| < j \leq n$ . Let  $D_{|\lambda|} = B_{|\lambda|} \cap R_0^{\text{lo}}$  and  $A_1^{|\lambda|} = B_{|\lambda|} \cap R_0^{\text{sh}}$ , and similarly for  $\mu$ . Notice that  $\mathbb{H}(R_{s,1}, T_s(T), F_{s,1}; k_s)$  is isomorphic to the product of graded affine Hecke algebras  $\mathbb{H}(B_{|\lambda|}, k_-) \times \mathbb{H}(B_{|\mu|}, k_+)$ , where by  $\mathbb{H}(B_\ell, k)$  we denote the graded affine Hecke algebra of type  $B_\ell$  with parameters 1 on the long roots and  $m$  on the short roots. Define for  $\lambda$  (and similarly for  $\mu$ ):

$$\bar{m}_\lambda(k) = \frac{\prod'_{\alpha \in B_{|\lambda|}} \alpha(\bar{c}_\lambda(k))}{\prod'_{\alpha \in D_{|\lambda|}} (\alpha(\bar{c}_\lambda(k)) - 1) \prod'_{\alpha \in A_1^{|\lambda|}} (\alpha(\bar{c}_\lambda(k)) - k)}, \tag{27}$$

$\epsilon(\lambda, k)$  = the sign of  $\bar{m}_\lambda(k)$ .



Then from Proposition 4.1,  $\bar{m}_\lambda(k)$  is a degree  $n$  polynomial and

$$\epsilon(b, k_+, k_-) = \epsilon(\lambda, k_-)\epsilon(\mu, -k_+) = \epsilon(\lambda, k_-)\epsilon(\mu^T, k_+), \tag{28}$$

where  $\mu^T$  denotes the transpose partition to  $\mu$ .

As noticed before, in the chamber where  $k_- \gg k_+ \gg 0$ , the discrete series are  $V_{(\lambda, \mu)}(\mathfrak{v})$ . Let  $\epsilon(\lambda, \mu) = \lim_{k_\pm \rightarrow \infty} \epsilon(b, k_+, k_-)$ . In conclusion, we have proved:

**Proposition 4.4.** *For the affine Hecke algebra of type  $C_n^{(1)}$ , the canonically positive basis  $\mathcal{B}_{\text{gm}, C}$  of  $\mathcal{Y}_{\text{gm}} = \bar{\mathcal{R}}_{\mathbb{Z}}(W)$  is*

$$\mathcal{B}_{\text{gm}, C} = \{b_{(\lambda, \mu)} := \epsilon(\lambda, \mu)\tilde{V}_{(\lambda, \mu)}(1) \mid (\lambda, \mu) \text{ bipartition of } n\},$$

where  $\tilde{V}_{(\lambda, \mu)}(1)$  is the irreducible  $W$ -representation with central character  $W_{0S_{(\lambda, \mu)}}$ ,

$$s_{(\lambda, \mu)} = (\underbrace{-1, \dots, -1}_{|\lambda|}, \underbrace{1, \dots, 1}_{|\mu|}),$$

and whose restriction to  $W_0$  is the irreducible  $W_0$ -representation labeled by the bipartition  $(\lambda, \mu)$ .

**4B2.**  $B_n^{(1)}$ ,  $C_n$  adjoint. The Iwahori–Hecke algebra of  $\text{Spin}_{2n+1}(F)$  is associated with the root datum of type  $B_n^{(1)}$ , for which the parameter space  $\mathcal{Q}$  is two dimensional. This two parameter family is isogenous to a specialization  $\mathcal{H}_B$  of the generic affine Hecke algebra  $\mathcal{H}_C$  of type  $C_n^{(1)}$  discussed in the previous section, namely  $\mathcal{H}_B = \mathcal{H}_C|_{v_0=1}$  (or equivalently  $k_- = k_+$ ). Observe that  $\mathcal{H}_B$  is associated with the extended diagram of type  $B_n^{(1)}$ , i.e.,  $R_0$  has type  $C_n$ , and  $X$  is its weight lattice. The Iwahori–Hecke algebra of  $\text{PGSp}_{2n}(F)$  is associated with the extended diagram of type  $C_n^{(1)}$ , and has a root datum with  $R_0$  of type  $B_n$  with  $X$  its weight lattice. The generic affine Hecke algebra  $\mathcal{H}_{C, \text{ad}}$  of this type has a two dimensional parameter space  $\mathcal{Q}_{\text{ad}} \subset \mathcal{Q}$  given by  $v_0 = v_2$ . Clearly,  $\mathcal{H}_{C, \text{ad}}$  is isogenous to the specialization  $\mathcal{H}_{C, \mathcal{Q}_{\text{ad}}} = \mathcal{H}_C|_{v_0=v_2}$  (or equivalently  $k_- = 0$ ) of the generic affine Hecke algebra  $\mathcal{H}_C$  of type  $C_n^{(1)}$ . To find the bases  $\mathcal{B}_{\text{gm}}$  of these two parameter generic Hecke algebras, we use some general results on isogeny (see Section 4E) in conjunction with the following remark:

**Remark 4.5.** Consider an arbitrary generic affine Hecke algebra  $\mathcal{H}_\Lambda$  over the parameter ring  $\Lambda$  as in Section 2B, with parameter space  $\mathcal{Q}$  and canonically positive basis  $\mathcal{B}_{\text{gm}}$ . Suppose that we have a quotient  $\Lambda'$  of  $\Lambda$  corresponding to a subtorus  $\mathcal{Q}' \subset \mathcal{Q}$ , and let  $\mathcal{B}'_{\text{gm}}$  be the corresponding basis for  $\mathcal{H}_{\Lambda'}$ . For any  $b \in \mathcal{B}_{\text{gm}}$  we have  $m_b^{\mathcal{Q}'} = d'_b m_b|_{\mathcal{Q}'}$  (see Definition 2.9) with

$$\pm b \in \mathcal{B}'_{\text{gm}} \iff \mathcal{Q}_b^{\text{reg}} \cap \mathcal{Q}' \neq \emptyset \iff d'_b \neq 0,$$

and

$$\mathcal{B}'_{\text{gm}} = \{\text{sign}(d'_b)b \mid b \in \mathcal{B}_{\text{gm}} \text{ and } \mathcal{Q}_b^{\text{reg}} \cap \mathcal{Q}' \neq \emptyset\}. \tag{29}$$

**Proposition 4.6.** (1) *The canonically positive basis of  $\mathcal{H}_B$  is  $\mathcal{B}_{\text{gm},B} = \mathcal{B}_{\text{gm},C}$ .*

(2) *The canonically positive basis of  $\mathcal{H}_{C, \mathcal{Q}_{\text{ad}}}$  is (see [Opdam and Solleveld 2010, Proposition 6.4] for the notion of  $\lambda$ -regular)*

$$\mathcal{B}_{\text{gm},C, \mathcal{Q}_{\text{ad}}} = \{ \epsilon_{C, \mathcal{Q}_{\text{ad}}}(\lambda) b_{(\lambda, \mu)} \mid 0 \text{ is } \lambda\text{-regular} \},$$

where  $\epsilon_{C, \mathcal{Q}_{\text{ad}}}(\lambda)$  is the sign of  $\bar{m}_\lambda^{C, \mathcal{Q}_{\text{ad}}}(0) \cdot \bar{m}_\lambda(0)$ .

*Proof.* By Remark 4.5 and formula (28) we need to compute the sign

$$\text{sign} \left( \lim_{(k_+, k_-) \rightarrow (k_{0,+}, k_{0,-})} \bar{m}'_\lambda(k_-) \bar{m}'_{\mu^T}(k_+) \right) \cdot \epsilon(\lambda, k_{0,-}) \epsilon(\mu^T, k_{0,+}),$$

where  $k_{0,+} = k_{0,-} = k$  in the first case, and  $k_{0,+} = k, k_{0,-} = 0$  in the second case (here  $k$  is a generic real number), and  $\bar{m}'$  denotes the polynomial  $\bar{m}_\lambda^B$  (in the first case) or  $\bar{m}_\lambda^{C, \mathcal{Q}_{\text{ad}}}$  (in the second case) defined as  $\bar{m}$ , but with  $\bar{c}$  generic on the relevant 2-dimensional parameter space instead of the 3-dimensional parameter space of  $\mathcal{H}_C$ . The combinatorial condition that 0 is  $\lambda$ -regular is precisely designed so that  $\bar{m}_\lambda(0) \neq 0$ .

It is obvious that in the first case the sign is +1. Since in the second case the contribution of  $k_+$  is +1 again, the claim follows.  $\square$

**Remark 4.7.** Let  $\lambda$  be an arbitrary partition. The signs  $\epsilon_{C, \mathcal{Q}_{\text{ad}}}(\lambda)$  that appear in Proposition 4.6 can be computed in the terms of the diagram of the partition. We need to count the signs contributed by the nonzero linear factors that appear in  $\bar{m}_\lambda(k)$ ,  $k$  generic but which become zero at  $k = 0$ . These are all factors of the form  $\pm k, \pm 2k$ . One combinatorial answer is that the resulting sign is  $(-1)^\ell$ , where  $\ell$  is the number of pairs of distinct boxes  $\{x_1, x_2\}$  in the Young diagram of  $\lambda$  that are “almost symmetric” with respect to the main diagonal. I.e., suppose  $x_1$  is the box on or below the diagonal and  $x'_1$  is the flip of  $x_1$  with respect to the diagonal, then  $x_2$  is one unit away from  $x'_1$  in one of the four directions.

**4B3.**  $G_2, F_4$ . For the affine Hecke algebras of types  $G_2$  and  $F_4$ , we work with the following coordinates. For  $G_2$ , the affine diagram is

$$\alpha_0 \text{ --- } \alpha_1 \implies \alpha_2,$$

with parameters  $v(s_i) = v^{2k_i}, i = 1, 2$ , while for  $F_4$ , it is

$$\alpha_0 \text{ --- } \alpha_1 \text{ --- } \alpha_2 \implies \alpha_3 \text{ --- } \alpha_4,$$

with parameters  $v(s_1) = v^{2k_1}, v(s_3) = v^{2k_2}$ . In both cases,  $v > 1$  and  $k_i \in \mathbb{R}$ .

Let  $\omega_i^\vee$  denote the fundamental coweights. A central character is of the form  $r_b = sc$ , where  $c = v^{\sum_i a_i \omega_i^\vee}$ , where  $s$  is a compact element of the torus. The generic residual central characters are listed in Tables 1 and 2 (Parts 1 and 2). In these

$b$	$s$	$W_0c$	$d_b$	$G_2$	$\epsilon$
$b_1$	1	$[k_1, k_2]$	1	$[G_2, 1]$	1
$b_2$	1	$[k_1, -k_1 + k_2]$	1	$[G_2(a_1), (21)]$	-1
$b_3$	1	$[k_1, \frac{1}{2}(-k_1 + k_2)]$	1/2	$[G_2(a_1), (3)]$	1
$b_4$	$2A_1$	$[-\frac{1}{2}k_1 - \frac{3}{2}k_2, k_2]$	1/2	$[2A_1, 1]$	1
$b_5$	$A_2$	$[k_1, -k_1]$	1/3	$[A_2, 1]$	1

$b$	$E_6 \subset E_8$	$\epsilon$	${}^3E_6$	$\epsilon$
$b_1$	$[A_2E_6, \theta]$	1	$E_6$	1
$b_2$	$[A_2E_6(a_1), \theta]$	-1	$E_6(a_1)$	-1
$b_3$	$[A_2E_6(a_3), \theta]$	1	$E_6(a_3)$	1
$b_4$	$[A_1A_2A_5, \theta]$	1	$A_1A_5$	1
$b_5$	$[A_8, \theta]$	1	$A_2^3$	1

**Table 1.**  $G_2$ .

tables, if  $s \neq 1$ , we specify it by the type of its centralizer in the second column. In the third column, we give  $c$  in the form  $[a_i]$ .

For each generic residual central character  $W_0r_b$ , we compute the function  $m_b(\mathbf{v})$  using formula (40) from [Opdam and Solleveld 2010]. To obtain the constant  $d_b$ , we compute the limits of  $m_b(\mathbf{v})$  in equal parameter case, e.g.,  $k_1 \rightarrow 1, k_2 \rightarrow 1$  and also in the unequal parameter cases that appear in  $E_8$ . Then we compare the results with the formulas for formal degrees in [Reeder 2000; 1994]. To complete the determination of the Langlands parameter, i.e., the representation of the component group, we computed, when needed, the  $W_0$ -structure of the specialization of the family of discrete series and compared it with the  $K$ -structure of the representations in Reeder’s tables. The relevant unequal parameter cases that appear in  $E_8$  are: the affine Hecke algebra of type  $F_4$  that controls the subcategory of unipotent representations where the parahoric subgroup is  $D_4$  in  $E_8$ , and the affine Hecke algebra of type  $G_2$  for the subcategories of unipotent representations where the parahoric subgroup is  $E_6$  in  $E_8$ . For this comparison, we need to multiply the specialization of the formal degree in the unequal parameters Hecke algebra by the factor  $\rho(1)/P_J(v^2)$ , where  $\rho$  is the appropriate cuspidal unipotent representation (whose dimension is given in the tables of [Carter 1985]) and  $P_J(v^2)$  is the Poincaré polynomial of the finite Hecke algebra corresponding to the parahoric  $J$ .

In addition, the Iwahori–Hecke algebra for the quasisplit exceptional  $p$ -adic group  ${}^3E_6$  (respectively,  ${}^2E_7$ ) is isomorphic to a direct sum of three (respectively, two) copies of an affine Hecke algebra with unequal parameters of type  $G_2$  (respectively,  $F_4$ ). To compare the formal degrees in these cases against the results of [Reeder 1994], we need to multiply the specialization of formal degrees for the affine Hecke

$b$	$s$	$W_0c$	$d_b$	$F_4$	$\epsilon$
$b_1$	1	$[k_1, k_1, k_2, k_2]$	1	$[F_4, 1]$	1
$b_2$	1	$[k_1, k_1, k_2 - k_1, k_2]$	1	$[F_4(a_1), -]$	-1
$b_3$	1	$[k_1, k_1, k_2 - k_1, k_1]$	1	$[F_4(a_1), +]$	1
$b_4$	1	$[k_1, k_1, k_2 - 2k_1, k_2]$	1	$[F_4(a_3), (211)]$	1
$b_5$	1	$[k_1, k_1, k_2 - 2k_1, 2k_1]$	1	$[F_4(a_2), +]$	1
$b_6$	1	$[k_1, k_1, k_2 - 2k_1, k_1]$	1	$[F_4(a_3), (31)]$	-1
$b_7$	1	$[k_1, k_1, k_2 - 2k_1, -2k_2]$	1	$[F_4(a_2), -]$	-1
$b_8$	1	$[0, k_1, 0, k_2 - k_1]$	1/6	$[F_4(a_3), (4)]$	1
$b_9$	1	$[0, k_1, 0, k_2 - k_1]$	1/3	$[F_4(a_3), (22)]$	1
$b_{10}$	$B_4$	$[k_1/2, k_1, k_2, -3k_1 - 2k_2]$	1/2	$[B_4, +]$	1
$b_{11}$	$B_4$	$[2k_1, -k_1, k_2, -k_1 - 2k_2]$	1/2	non-ds	
$b_{12}$	$B_4$	$[0, k_1, -k_1 + k_2, -2k_2]$	1/2	$[B_4(531), \epsilon'']$	-1
$b_{13}$	$B_4$	$[k_1, k_1, -2k_1 + k_2, k_1 - 2k_2]$	1/2	$[B_4(531), 1]$	1
$b_{14}$	$B_4$	$[k_1, k_1, -3k_1 + k_2, 3k_1 - 2k_2]$	1/2	$[B_4(531), \epsilon']$	-1
$b_{15}$	$C_3A_1$	$[-2k_1 - 3k_2, k_1, k_2, k_2]$	1/2	$[C_3 \times A_1, +]$	1
$b_{16}$	$C_3A_1$	$[-2k_1, k_1, -k_2, 2k_2]$	1/2	$[C_3(42) \times A_1, ++]$	1
$b_{17}$	$C_3A_1$	$[-2k_1 + 3k_2, k_1, -k_2, -k_2]$	1/2	$[C_3(42) \times A_1, +-]$	-1
$b_{18}$	$2A_2$	$[k_1, -k_1 - 2k_2, k_2, k_2]$	1/3	$[2A_2, 1]$	1
$b_{19}$	$A_3A_1$	$[k_1, k_1, -3k_1/2 - k_2/2, k_2]$	1/4	$[A_1A_3, 1]$	1

**Table 2.** (Part 1)  $F_4$ .

algebra by the factor

$$\frac{(q^{1/2} - q^{-1/2})^{n+1}}{|\Omega| \prod_O (q^{|O|/2} - q^{-|O|/2})},$$

where  $n + 1$  is the number of nodes in the affine Dynkin diagram, and  $O$  ranges over the Galois orbits in the affine Dynkin diagram. See [Opdam 2016, (25)] for more details. For the nonsplit inner forms, this procedure allows us to find the L-packet to which the representation should belong, but it is not sufficient to enable us to attach the representation of the component group.<sup>3</sup>

**4C. Relation with Kazhdan–Lusztig parameters.** Let  $\mathcal{R}$  be a semisimple root datum. Let  $G$  be the connected complex semisimple group with root datum  $\mathcal{R}$ . Consider the generic affine Hecke algebra  $\mathcal{H}$  with root datum  $\mathcal{R}$  and equal parameters, i.e.,  $v(s) = v(s') = v$  for all  $s, s' \in S$ . If  $G$  is simply connected, the Kazhdan–Lusztig classification [Kazhdan and Lusztig 1987] applies to give a

<sup>3</sup>This is a subtle question, see [Opdam 2016] for results in this sense. We plan to return to this question in future work.

$b$	$D_4 \subset E_8$	$\epsilon$	${}^2E_7$	$\epsilon$
$b_1$	$[A_1E_7, -]$	1	$E_7$	1
$b_2$	$[A_1E_7(a_4), --]$	-1	$E_7(a_1)$	-1
$b_3$	$[A_1E_7(a_2), -]$	1	$E_7(a_2)$	1
$b_4$	$[A_1E_7(a_3), +-]$	1	$E_7(a_3)$	1
$b_5$	$[A_1E_7(a_3), -+]$	-1	$E_7(a_3)$	-1
$b_6$	$[A_1E_7(a_4), +-]$	1	$E_7(a_4)$	1
$b_7$	$[A_1E_7(a_1), -]$	-1	$E_7(a_4)$	-1
$b_8$	$[A_1E_7(a_5), -3]$	1	$E_7(a_5)$	1
$b_9$	$[A_1E_7(a_5), -21]$	1	$E_7(a_5)$	1
$b_{10}$	$[D_8, -]$	1	$A_1D_6$	1
$b_{11}$	$[D_8(5, 11), -]$	1	$A_1D_6(3, 9)$	-1
$b_{12}$	$[D_8(1, 3, 5, 7), r]$	1	$A_1D_6(5, 7)$	-1
$b_{13}$	$[D_8(7, 9), -]$	-1	non-ds	
$b_{14}$	$[D_8(3, 13), -]$	-1	non-ds	
$b_{15}$	$[A_3D_5, -1]$	1	$A_1D_6$	1
$b_{16}$	$[A_3D_5(3, 7), -1]$	-1	$A_1D_6(5, 7)$	1
$b_{17}$	non-ds		$A_1D_6(3, 9)$	-1
$b_{18}$	$[A_1A_2A_5, -1]$	1	$A_2A_5$	1
$b_{19}$	$[A_1A_7, -]$	1	$A_1A_3^2$	1

**Table 2.** (Part 2)  $F_4$ .

parametrization of the simple discrete series  $\mathcal{H}_{v_0}$ -modules,  $v_0 > 1$ , in terms of

$$DS_{KL}(\mathcal{R}) = G \setminus \{(x, \phi) \mid x \in G \text{ elliptic, } \phi \in \widehat{A(x)} \text{ such that } H^{\text{top}}(\mathcal{B}_x)^\phi \neq 0\}. \quad (30)$$

This result has been extended by Reeder [2002] (also see [Aubert et al. 2017]) to the case where  $\mathcal{R}$  has arbitrary isogeny type. Recall that we say that  $x$  is elliptic in  $G$  if the conjugacy class of  $x$  does not meet any proper Levi subgroup of  $G$ . Here we denote by  $A(x) = Z_G(x)/Z_G(x)^0 Z(G)$  the component group of the centralizer of  $x$  in  $G$  (mod the center of  $G$ ), by  $\mathcal{B}_x$  the Springer fiber of  $x$  in  $G$ , and by  $H^{\text{top}}(\mathcal{B}_x)^\phi$  the  $\phi$ -isotypic component of  $A(x)$  in the top cohomology of  $\mathcal{B}_x$ .

As is well known, by the construction of Springer extended by Lusztig and Kato in the simply connected case (see, for example, [Reeder 2000, Section 8]), and further extended by Reeder [2002, Section 3] to the arbitrary semisimple case, the full cohomology groups  $H^\bullet(\mathcal{B}_x)^\phi$  carry an action of  $W$ . We define

$$\mathcal{B}_{DS}^{KL} = \{h_{x,\phi} := H^\bullet(\mathcal{B}_x)^\phi \otimes \varepsilon \mid (x, \phi) \in DS_{KL}(\mathcal{R})\}, \quad (31)$$

where  $\varepsilon$  is the sign character of  $W$ .

Let  $x$  be an elliptic parameter as above and write  $x = su$  for the Jordan decomposition, with  $s \in T_u$ . Let  $\psi : \mathrm{SL}(2, \mathbb{C}) \rightarrow G$  be the Lie homomorphism such that  $\phi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = u$ . Set

$$\tau = s\phi\left(\begin{pmatrix} v^{-1} & 0 \\ 0 & v \end{pmatrix}\right) \in T_u T_v \quad \text{and} \quad q = v^2.$$

The following Proposition follows easily from the work of Kazhdan and Lusztig [Kazhdan and Lusztig 1987; Lusztig 1995; 1989b] and the definitions.

**Proposition 4.8.** *Let  $\pi_{v,h_x,\phi}$  be the Kazhdan–Lusztig representation of  $\mathcal{H}$  associated to the elliptic Kazhdan–Lusztig parameter  $(x, \phi)$ . Then*

$$\pi_{v,h_x,\phi} = \mathrm{Ind}_D(h_x, \phi, v). \tag{32}$$

*In particular,  $\pi_{v,h_x,\phi}$  is a discrete series character with central character  $W_0\tau$ .*

*Proof.* By [Kazhdan and Lusztig 1987], the representation  $\pi_{v,h_x,\phi}$  is an irreducible discrete series with central character  $W_0\tau$ . We know by [Reeder 2001, Theorem 5.11.1] that  $\lim_{v \rightarrow 1} \pi_{v,h_x,\phi} = h_x, \phi$ , hence (32) follows directly from Definition 2.7.  $\square$

If  $\mathcal{R}$  is of simply connected type then the formal degree is given by the formula [Opdam 2016; Reeder 2000]:

$$\mathrm{fdeg}(\pi_{v,h_x,\phi}) = \frac{\phi(1)}{|A(x)||Z(G)|} m_v^{\mathrm{KL}}(\tau), \tag{33}$$

where

$$m_v^{\mathrm{KL}}(\tau) = q^{|R|/2} \frac{\prod'_{\alpha \in R} (\alpha(\tau) - 1)}{\prod'_{\alpha \in R} (q\alpha(\tau) - 1)}.$$

**Proposition 4.9.** *Equation (33) holds for all semisimple root data  $\mathcal{R}$ .*

*Proof.* Let  $G'$  be an arbitrary connected complex semisimple group with root datum  $\mathcal{R}'$ , and let  $1 \rightarrow C \rightarrow G \rightarrow G' \rightarrow 1$  be the universal covering of  $G'$ . Consider  $x' = s'u' \in G'$  elliptic, and let  $x = su \in G$  be a lifting of  $x'$ . Let  $A(x), A(x') \subset G_{\mathrm{ad}}$  be the centralizers of the unramified Langlands parameters associated to  $x$  and  $x'$  as in the text above Proposition 4.9 (these are finite subgroups, since  $x$  and  $x'$  are elliptic). We define a homomorphism  $A(x') \rightarrow C$  by  $a \rightarrow asa^{-1}s^{-1} \in C$ , whose image we denote by  $C_x$ . Similar to [Reeder 2002, Section 3.3], this give rise to an exact sequence:

$$1 \rightarrow A(x) \rightarrow A(x') \rightarrow C_x \rightarrow 1$$

(more precisely,  $A(x)$  and  $A(x')$  are the images in  $G_{\mathrm{ad}}$  of Reeder’s  $A_{\tau,u}$  and  $A_{\tau,u}^+$  respectively). Let  $(x, \phi) \in \mathrm{DS}_{\mathrm{KL}}(\mathcal{R})$ . Let  $C_{x,\phi} \subset C_x$  be the isotropy group of  $\phi$  with respect to the natural action of  $C_x$  on the set of equivalence classes of irreducible characters of  $A(x)$ . Let  $\mu$  denote the complex 2-cocycle of  $C_{x,\phi}$  associated to  $\phi$ ,

and  $E_{x,\phi} = \mathbb{C}[C_{x,\phi}, \mu]$  the corresponding twisted group algebra. By Mackey theory (see [Reeder 2002, Section 3.3]) we have

$$E_{x,\phi} \simeq \text{End}_{\mathbb{C}[A(x')]}(\text{Ind}_{A(x)}^{A(x')} \phi),$$

and thus

$$\text{Ind}_{A(x)}^{A(x')} \phi = \bigoplus_{\psi \in \text{Irr}(E_{x,\phi})} \psi \otimes \rho_\phi^\psi, \tag{34}$$

with  $\rho_\phi^\psi \in \text{Irr}(A(x'))$  as  $E_{x,\phi} \otimes \mathbb{C}[A(x')]$ -module. Moreover, all irreducible characters  $\rho$  of  $A(x')$  appear as some  $\rho \simeq \rho_\phi^\psi$ , and  $\rho_\phi^\psi \simeq \rho_{\phi'}^{\psi'}$  if and only if  $\phi'$  is a twist of  $\phi$  by an element of  $C_x$ , and  $\psi'$  and  $\psi$  correspond accordingly via this twist. By counting the multiplicity of  $\rho_\phi^\psi$  in the regular representation of  $A(x')$  using (34) we see:

$$\dim(\rho_\phi^\psi) = \frac{|C_x|}{|C_{x,\phi}|} \dim(\phi) \dim(\psi). \tag{35}$$

On the other hand we consider the affine Hecke algebras  $\mathcal{H}_v$  and  $\mathcal{H}'_v$ . Reeder [Reeder 2002, Section 1.5, Lemma 3.5.2] showed  $\mathcal{H}'_v = (\mathcal{H}_v)^C$ , and

$$\pi_{v,h_{x,\phi}}|_{\mathcal{H}'_v} = \bigoplus_{\psi \in \text{Irr}(E_{x,\phi})} \psi \otimes \pi_{v,h_{x',\rho_\phi^\psi}}. \tag{36}$$

Now  $\pi_{v,h_{x',\rho_\phi^\psi}}$  will arise as a summand of  $\pi_{v,h_{\tilde{x},\tilde{\phi}}}|_{\mathcal{H}'_v}$  if and only if  $(\tilde{x}, \tilde{\phi})$  is a twist of  $(x, \phi)$  by an element of  $C$ . The Plancherel decomposition of the trace  $\tau'$  of the normalized Hecke algebra  $\mathcal{H}'_v$  is obtained by restricting the Plancherel decomposition of the trace  $\tau$  of  $\mathcal{H}_v$ , since (see [Opdam 2016, Paragraph 2.4.1]) we have  $\tau' = \tau|_{\mathcal{H}'_v}$ . The above shows that in this restriction, the character of  $\pi_{v,h_{x',\rho_\phi^\psi}}$  will appear with formal degree equal to the formal degree of  $\pi_{v,h_{x,\phi}}$  with respect to  $\mathcal{H}_v$ , multiplied by the multiplicity

$$\frac{|C|}{|C_{x,\phi}|} \dim(\psi). \tag{37}$$

Considering that clearly  $m_v^{\text{KL}}(\tau) = m_v^{\text{KL}}(\tau')$ , and using (33), (34), (35), and (37), we see that

$$\text{fdeg}(\pi_{v,h_{x',\rho_\phi^\psi}}) = \frac{\rho_\phi^\psi(1)}{|A(x')||Z(G')|} m_v^{\text{KL}}(\tau'),$$

as was to be proved. □

By [Reeder 2000, Proposition 7.2],  $m_v^{\text{KL}}(\tau) = q^{\dim \mathcal{B}_u} (q - 1)^\ell |M_0^s| R(q)$ , where  $\ell = \dim T$ ,  $M_0^s$  is as in [Reeder 2000, Lemma 7.1], and  $R(q)$  is a rational function in  $q$  that has the property that  $R(0) = 1$  and  $R(1) \neq 0$ . On the other hand, we know by [Opdam 2004, Proposition 3.27(v)] that  $m_v^{\text{KL}}(\tau) q^{-\dim \mathcal{B}_u}$  must equal a scalar times a rational function in cyclotomic polynomials in  $q$ . This means that  $R(q)$  is a scalar times a rational function where both the numerator and the denominator are products of cyclotomic polynomials  $\Phi_n(q)$  with  $n \geq 2$ . Since  $R(0) = 1$ , the scalar

must be in fact 1. But then  $R(q) > 0$  whenever  $q$  is specialized to any real number greater than  $-1$ , which implies that  $m_v^{\text{KL}}(\tau) > 0$  whenever  $q > 1$ .

Notice that the same conclusion follows from our sign formula (19). In the equal parameter case, we have  $k_s \equiv 1$ , and therefore the number of contributions of  $(-1)$  in (19) equals the number of roots  $\alpha(\bar{c}) < 0$  plus the number of roots  $\alpha(\bar{c}) < 1$ . Because of integrality of the central character  $\bar{c}$  and the fact that the roots of  $\bar{c}$  that vanish come in pairs, it follows, that this is an even number, thus the sign of  $\bar{m}_{W_0\bar{c}}$  is positive.

**Proposition 4.10.** *Suppose  $\mathcal{R}$  is a semisimple root datum and let  $\mathbf{v}_0$  denote the specialization in the equal parameters case.*

- (a)  $\mathcal{B}_{\mathbf{v}_0-m} = \{b_{x,\phi} := \epsilon(x, \phi)h_{x,\phi} \mid h_{x,\phi} \in \mathcal{B}_{\text{DS}}^{\text{KL}}\}$ , where  $\epsilon(x, \phi) = \epsilon(b_{x,\phi}; \mathbf{v}_0)$  is the sign of  $m_{W_0r_b}^{\ominus}(\mathbf{v}_0)$  (see Remark 4.3).
- (b) If  $\mathcal{R}$  is simply laced, then  $\mathcal{B}_{\text{gm}} = \mathcal{B}_{\text{DS}}^{\text{KL}}$  and

$$d_{b_{x,\phi}} = \frac{\phi(1)}{|A(x)||Z(G)|} \quad \text{for all } b_{x,\phi} \in \mathcal{B}_{\text{gm}}.$$

- (c) Suppose  $\mathcal{R}$  is a root datum of type  $G_2$  or  $F_4$ . Then

$$\mathcal{B}_{\text{gm}}(G_2) = \{\epsilon(x, \phi)h_{x,\phi} \mid h_{x,\phi} \in \mathcal{B}_{\text{DS}}^{\text{KL}}\}$$

and

$$\mathcal{B}_{\text{gm}}(F_4) = \{\epsilon(x, \phi)h_{x,\phi} \mid h_{x,\phi} \in \mathcal{B}_{\text{DS}}^{\text{KL}}\} \cup \{b_{11} = H^\bullet(\mathcal{B}_{x_{B_4}})^{\text{triv}} \otimes \varepsilon\},$$

with  $x_{B_4} = s_{B_4}u_{(711)}$ , where  $Z_G(s_{B_4})$  is of type  $B_4$  and  $u_{(711)}$  is a representative of the subregular unipotent class in  $B_4$ . The explicit signs  $\epsilon(x, \phi)$  are given in the sixth column in Tables 1 and 2 (Part 1), while the constants  $d_{b_{x,\phi}}$  are listed in the fourth column of the tables.

*Proof.* As in Remark 4.3, for every  $b \in \mathcal{B}_{\mathbf{v}_0-m}$ ,  $\text{ds}(b; \mathbf{v}_0) = \epsilon(b; \mathbf{v}_0) \text{Ind}(b; \mathbf{v}_0)$  and we know that the sign  $\epsilon(b, \mathbf{v}_0)$  is given by the sign of the generic  $m$ -function. Applying the restriction map, we get that  $\text{Res}(\text{ds}(b; \mathbf{v}_0)) = \epsilon(b; \mathbf{v}_0) \text{Ind}(b; \mathbf{v}_0)$ . On the other hand, as explained above  $\text{Res}(\text{ds}(b; \mathbf{v}_0))$  equals an  $h_{x,\phi}$  for some  $(x, \phi) \in \text{DS}_{\text{KL}}(\mathcal{R})$ . This is the claim in part (a).

Part (b) follows immediately from (a) by Proposition 4.9 and the discussion preceding the present proposition: in the simply laced case, the generic  $m$ -function equals  $m_v^{\text{KL}}(\tau)$ , which is positive.

Part (c) is contained in Section 4B3, where Tables 1 and 2 were computed.  $\square$

**Remark 4.11.** If  $\mathcal{R}$  is a simply connected root datum of type  $B$  or  $C$ , then one can relate the elements of  $\mathcal{B}_{\text{DS}}^{\text{KL}}$  to the bipartitions in the basis  $\mathcal{B}_{\text{gm}}$  from Proposition 4.4 using the combinatorial algorithms of Slooten [2008], see also [Opdam 2016]. If



$(x, \phi)$  is a discrete Kazhdan–Lusztig parameter as above, let  $(\lambda(x, \phi), \mu(x, \phi))$  be the bipartition associated by the algorithms in [loc. cit.]. Then

$$\mathcal{B}_{\text{DS}}^{\text{KL}} = \{ \epsilon(\lambda(x, \phi), \mu(x, \phi)) \cdot b_{(\lambda(x, \phi), \mu(x, \phi))} \mid (x, \phi) \in \text{DS}_{\text{KL}}(\mathcal{R}) \},$$

where  $\epsilon(\lambda(x, \phi), \mu(x, \phi))$  equals the sign of  $\lim_{k_s(\alpha) \rightarrow 1} \bar{m}_{W_0 \bar{c}}$  from (19).

**4D. Pin cover of the Weyl group.** Suppose  $\mathcal{W}$  is a finite Weyl group with its reflection representation  $\mathcal{E}$ . Fix a positive definite  $\mathcal{W}$ -invariant symmetric bilinear form on  $\mathcal{E}$ . Define the Clifford algebra  $C(\mathcal{E})$  and the pin cover  $p : \tilde{\mathcal{W}} \rightarrow \mathcal{W}$  as in [Ciubotaru et al. 2014, Section 3.1]. Let  $\det$  be the determinant character of  $\tilde{\mathcal{W}}$  acting on  $\mathcal{E}$ . As in [Ciubotaru et al. 2014, Section 4.1], define  $\tilde{\mathcal{W}}'$  to be equal to  $\tilde{\mathcal{W}}$ , when  $\dim \mathcal{E}$  is odd, and to equal  $\ker \det$  (an index two subgroup), when  $\dim \mathcal{E}$  is even.

If  $\dim \mathcal{E}$  is odd, then  $C(\mathcal{E})$  has two nonisomorphic simple complex modules; we denote them  $S^+$  and  $S^-$ . When  $\dim \mathcal{E}$  is even,  $C(\mathcal{E})$  has a unique simple complex module whose restriction to the even part  $C_0(\mathcal{E})$  splits into a direct sum of two nonisomorphic modules, denoted again  $S^+$  and  $S^-$ . We fix the choice of  $S^+$  (and  $S^-$ ) in both cases once and for all.

An irreducible  $\tilde{\mathcal{W}}'$ -representation is said to be genuine if it does not factor through  $p(\tilde{\mathcal{W}}')$ . Two nonisomorphic irreducible  $\tilde{\mathcal{W}}'$ -representations are said to be associate if one is the det-dual of the other, when  $\dim \mathcal{E}$  is odd, and if they both occur in the restriction to  $\tilde{\mathcal{W}}'$  of an irreducible  $\tilde{\mathcal{W}}$ -module, when  $\dim \mathcal{E}$  is even. For example  $\{S^+, S^-\}$  is a pair of associate  $\tilde{\mathcal{W}}'$ -representations. Denote by  $\text{Irr}^2 \tilde{\mathcal{W}}'$  the set of associate genuine pairs.

We apply these constructions in the case when  $\mathcal{R}$  is a semisimple, simply connected root datum,  $\mathcal{W} = W_s$ , with  $s$  an isolated element of  $T_u$  and  $\mathcal{E} = T_s(T) \cong E$ . For the connections with elliptic theory, see [Ciubotaru et al. 2014, Section 4] for example. Given  $\{\tilde{\sigma}^+, \tilde{\sigma}^-\}$ , let  $\xi_s(\tilde{\sigma}^+) = \xi_s(\tilde{\sigma}^-)$  be a representative of the generic central character defined by [Ciubotaru et al. 2014, Theorem 3.2]. Let

$$\text{Irr}_{\text{gm}}^2 \tilde{W}'_s = \{ \{\tilde{\sigma}^+, \tilde{\sigma}^-\} \in \text{Irr}^2 \tilde{W}'_s \mid \xi_s(\tilde{\sigma}^+) \text{ is generically residual for } (R_{s,1}, k_s) \}$$

and

$$\text{Irr}_{\text{KL}}^2 \tilde{W}'_s = \{ \{\tilde{\sigma}^+, \tilde{\sigma}^-\} \in \text{Irr}_{\text{gm}}^2 \tilde{W}'_s \mid \xi_s(\tilde{\sigma}^+)(1) \text{ is residual for } (R_{s,1}, k_s = 1) \},$$

where  $\xi_s(\tilde{\sigma}^+)(1)$  denotes the specialization at the equal parameter case  $k_s = 1$ .

Write  $\mathcal{B}_{\text{gm}} = \bigsqcup_s \text{Ind}_s(\mathcal{B}_{\text{gm},s})$  for the canonically positive basis, where  $\mathcal{B}_{\text{gm},s}$  is a certain orthonormal subset of  $\bar{R}_{\mathbb{Z}}(W_s)$ . By [Ciubotaru et al. 2014, Theorem 4.2], for each  $b_s \in \mathcal{B}_{\text{gm},s}$  there exists a pair  $(\tilde{\sigma}_{b_s}^+, \tilde{\sigma}_{b_s}^-)$  of associate genuine irreducible  $\tilde{W}'_s$ -representations such that

$$b_s = \Delta(\tilde{\sigma}_{b_s}^+, \tilde{\sigma}_{b_s}^-) := \frac{\tilde{\sigma}_{b_s}^+ - \tilde{\sigma}_{b_s}^-}{S^+ - S^-} \quad \text{in } \bar{R}_{\mathbb{Z}}(W_s).$$

Moreover, as explained in Section 2B4,  $\xi_s(\tilde{\sigma}_{b_s}^+) = r_{b_s}$ ; in particular,

$$\{\tilde{\sigma}_{b_s}^+, \tilde{\sigma}_{b_s}^-\} \in \text{Irr}_{\text{gm}}^2 \widetilde{W}_s'.$$

By the same results in [loc. cit.], the assignment  $b_s \mapsto \{\tilde{\sigma}_{b_s}^+, \tilde{\sigma}_{b_s}^-\}$  is injective. Thus if we define  $\text{Irr}_{\text{gm}}^2 \widetilde{W}_s' = \{(\tilde{\sigma}_{b_s}^+, \tilde{\sigma}_{b_s}^-) \mid b_s \in \mathcal{B}_{\text{gm},s}\}$ , then the map  $\Delta$  defines a bijection

$$\Delta : \text{Irr}_{\text{gm}}^2 \widetilde{W}_s' \rightarrow \mathcal{B}_{\text{gm},s}.$$

In fact,  $\text{Irr}_{\text{gm}}^2 \widetilde{W}_s'$  is just  $\text{Irr}_{\text{gm}}^2 \widetilde{W}_s'$  with a particular choice of  $\tilde{\sigma}^+$  versus  $\tilde{\sigma}^-$ .

We can explain this choice independently in the case of  $\text{Irr}_{\text{KL}}^2 \widetilde{W}_s'$ . Since  $\xi_s(\tilde{\sigma}^+)(1)$  is a residual point, we know by [Opdam 2004] that  $\xi_s(\tilde{\sigma}^+)(1)$  satisfies the same combinatorial condition as the Bala–Carter condition for half of the middle element of a distinguished Lie triple in  $Z_G(s)$ . Thus, the pair  $\{\tilde{\sigma}^+, \tilde{\sigma}^-\} \in \text{Irr}_{\text{KL}}^2 \widetilde{W}_s'$  determines the (conjugacy class of an) element  $u$ , and therefore the elliptic element  $x = su$  in the Kazhdan–Lusztig parametrization. To formalize this, denote by  $u(\{\tilde{\sigma}^+, \tilde{\sigma}^-\})$  a representative of the unipotent class attached in this way.

Let  $\Omega_{\widetilde{W}_s}$  be the Casimir element of  $\widetilde{W}_s$ , e.g., [Ciubotaru et al. 2014, (3.2.5)]. The scalar  $\tilde{\sigma}^+(\Omega_{\widetilde{W}_s})$  by which  $\Omega_{\widetilde{W}_s}$  acts in  $\tilde{\sigma}^+$  (which does not depend on the choice of  $\tilde{\sigma}^+$  versus  $\tilde{\sigma}^-$ ) equals the squared norm of  $\xi_s(\tilde{\sigma}^+)$ .

It remains to discuss how to associate a representation  $\phi$  of the component group  $A(x)$ . This will also lead to the desired canonical choice for  $\tilde{\sigma}^\pm$ . Let  $x = su$  be an elliptic element of  $G$ . Recall that this means that  $u$  is distinguished in  $Z_G(s)$ . Let  $X_s(u, \phi)$  and  $\sigma_s(u, \phi)$  denote the standard and irreducible  $W_s$ -representations afforded via Springer theory by  $H^\bullet(\mathcal{B}_u^s)^\phi \otimes \varepsilon$  and  $H^{2d_u^s}(\mathcal{B}_u^s)^\phi \otimes \varepsilon$  respectively, where  $\mathcal{B}_u^s$  is the Springer fiber of  $u$  in  $Z_G(s)$  and  $d_u^s = \dim \mathcal{B}_u^s$ . As above, there exist associate irreducible representations  $\tilde{\sigma}_s(u, \phi)^\pm$  such that

$$X_s(u, \phi) \otimes (S^+ - S^-) = \tilde{\sigma}_s(u, \phi)^+ - \tilde{\sigma}_s(u, \phi)^-.$$

As noticed in [Ciubotaru and Trapa 2013; Ciubotaru and He 2015], if we write

$$X_s(u, \phi) = \sigma_s(u, \phi) + \sum_{u' > u} a_{(u', \phi')} X_s(u', \phi')$$

(by the results of Borho and Macpherson), then one can deduce that  $\tilde{\sigma}_s(u, \phi)^\pm$  can only appear in  $\sigma_s(u, \phi) \otimes S^\pm$  and in no other  $X_s(u', \phi') \otimes S^\pm$ . Moreover, by the Dirac theory, the scalar  $\tilde{\sigma}_s(u, \phi)^\pm(\Omega_{\widetilde{W}_s})$  equals the squared norm of half a middle element for a Lie triple of  $u$ , and this is the *minimal* such scalar that may appear for an irreducible constituent of  $\sigma_s(u, \phi) \otimes S^\pm$ . By [Ciubotaru 2012] (case-by-case) or [Ciubotaru and He 2015] (uniformly),  $\tilde{\sigma}_s(u, \phi)^+$  appears with multiplicity one in  $\sigma_s(u, \phi) \otimes S^+$  (and similarly for the  $-$  case).

The conclusion is that  $\tilde{\sigma}_s(u, \phi)^+$  is characterized by the property that it is the unique irreducible constituent of  $\sigma_s(u, \phi) \otimes S^+$  for which the scalar by which  $\Omega_{\widetilde{W}_s}$

acts in it is minimal among all the constituents of the tensor product. Moreover,  $\tilde{\sigma}_s(u, \phi)^+$  does not appear as such a “minimal representation” in any other tensor product of this form. This gives a one-to-one correspondence between the sets  $\{\sigma_s(u, \phi)\}$  and  $\{\tilde{\sigma}_s(u, \phi)^+\}$ . Given a  $\tilde{\sigma}^+$  in the latter set, denote by  $\phi(\tilde{\sigma}^+)$  the local system  $\phi$  for the Springer representation in the former set. In particular, we have a preferred representation  $\tilde{\sigma}^+$  in any pair belonging to  $\text{Irr}_{\text{KL}}^2 \widetilde{W}_s'$ . Thus we get a set  $\text{Irr}_{\text{KL}}^2 \widetilde{W}_s'$  of ordered pairs. In summary we have:

**Proposition 4.12.** *Suppose  $\mathcal{R}$  is a simply connected semisimple root datum. Then, with the canonical choice of representations  $\tilde{\sigma}^+$  as above,*

$$\bigsqcup_s \text{Ind}_s \circ \Delta(\text{Irr}_{\text{KL}}^2 \widetilde{W}_s') = \mathcal{B}_{\text{DS}}^{\text{KL}}.$$

Given a pair  $(\tilde{\sigma}^+, \tilde{\sigma}^-) \in \text{Irr}_{\text{KL}}^2(\widetilde{W}_s')$ , the Kazhdan–Lusztig parameter  $(x = su, \phi)$  is given by  $u = u(\{\tilde{\sigma}^+, \tilde{\sigma}^-\})$  and  $\phi = \phi(\tilde{\sigma}^+)$  with the notation as in the previous paragraph.

**Remark 4.13.** If, in addition  $\mathcal{R}$  is simply laced, this also implies that

$$\mathcal{B}_{\text{gm}} = \bigsqcup_s \text{Ind}_s \circ \Delta(\text{Irr}_{\text{KL}}^2 \widetilde{W}_s').$$

When  $\mathcal{R}$  is not simply laced, the relation between  $\mathcal{B}_{v_0-m}$  and  $\mathcal{B}_{\text{DS}}^{\text{KL}}$  (and therefore  $\bigsqcup_s \text{Ind}_s \circ \Delta(\text{Irr}_{\text{KL}}^2 \widetilde{W}_s')$ ) was given in Section 4C.

**Remark 4.14.** The case of root data of type  $E$  is particularly interesting. Suppose  $\mathcal{R}$  is a simply connected, type  $E$ , root datum. Let  $\{\tilde{\sigma}^+, \tilde{\sigma}^-\} \in \text{Irr}^2(\widetilde{W}_s')$  be given, with the notation as above. We know a priori that  $\xi_s(\tilde{\sigma}^+)$  equals  $k/2$  times the middle element of a Lie triple of a quasidistinguished unipotent element  $u$  of  $Z_G(s)$  (see [Ciubotaru et al. 2014, Section 5]). By [Opdam 2004, Appendix] (also see [Opdam and Solleveld 2010]), this is a residual point for  $(R_s, k)$  if and only if  $u$  is distinguished in  $Z_G(s)$ . The key, empirical, observation is that for the root systems  $R_s$  occurring in a type  $E$  root system, the squared norms of the middle element of a quasidistinguished Lie triple uniquely identifies the unipotent class. In particular, the scalar by which  $\Omega_{\tilde{W}_s}$  acts in  $\tilde{\sigma}^+$  already identifies uniquely the unipotent class of  $u(\{\tilde{\sigma}^+, \tilde{\sigma}^-\})$ , and in particular if  $\{\tilde{\sigma}^+, \tilde{\sigma}^-\} \in \text{Irr}_{\text{gm}}^2(\widetilde{W}_s')$ . In this way we can effectively determine the base  $\mathcal{B}_{\text{DS}}^{\text{KL}} = \mathcal{B}_{\text{gm}}$  of Proposition 4.12, and for each  $b \in \mathcal{B}_{\text{gm}}$ , the central character  $W_0\tau$  (with  $\tau = s \exp(\xi_s)$ ) of  $\text{Ind}_D(b; v)$ . This recovers the classification of the discrete series characters of  $\mathcal{H}$  starting from the Springer theory of  $W_s$ .

**4E. The general semisimple case.** Let us consider the determination of the basis  $\mathcal{B}_{\text{gm}}$  for an arbitrary semisimple root datum  $\mathcal{R}$ . Recall that if  $\mathcal{H} \subset \mathcal{H}'$  are isogenous extended affine Hecke algebras such that  $R_{\text{nr}} = R'_{\text{nr}}$  (see (11)), so that in particular

we have a canonical identification  $\mathcal{Q} = \mathcal{Q}'$ , then the functors induction  $\text{Ind}_{\mathcal{H}}^{\mathcal{H}'}$  and restriction  $\text{Res}_{\mathcal{H}}^{\mathcal{H}'}$  respect the discrete series [Delorme and Opdam 2011, Lemma 6.3] in the sense that an irreducible discrete series is mapped to a finite direct sum of irreducible discrete series. From this we easily obtain:

**Proposition 4.15.** *Let  $b \in \mathcal{B}_{\text{gm}}$  (respectively  $b' \in \mathcal{B}'_{\text{gm}}$ ), and let  $\mathbf{v} \in \mathcal{Q}_b^{\text{reg}}$  (respectively  $\mathbf{v} \in \mathcal{Q}_{b'}^{\text{reg}}$ ). Let  $\delta'$  (respectively  $\delta$ ) be an irreducible summand of  $\text{Ind}_D^{\mathcal{H}'}(\text{Ind}_D(b; \mathbf{v}))$  (respectively  $\text{Res}_{\mathcal{H}}^{\mathcal{H}'}(\text{Ind}_D(b'; \mathbf{v}))$ ). Then  $\lim_{\mathbf{v} \rightarrow 1} \delta'$  is an element of  $\mathcal{B}'_{\text{gm}}$  and all elements of  $\mathcal{B}'_{\text{gm}}$  are of this form, and similarly,  $\lim_{\mathbf{v} \rightarrow 1} \delta$  is an element of  $\mathcal{B}_{\text{gm}}$  and all elements of  $\mathcal{B}_{\text{gm}}$  are of this form.*

The following result reduces the explicit computation of the restrictions and inductions of discrete series to the case of restriction and induction of representations of the extended affine Weyl groups  $W \subset W'$ .

**Proposition 4.16.** *We have  $\text{Ind}_{\mathcal{H}}^{\mathcal{H}'}(\text{Ind}_D(b; \mathbf{v})) = \text{Ind}_D(\text{Ind}_W^{W'}(b); \mathbf{v})$  and similarly  $\text{Res}_{\mathcal{H}}^{\mathcal{H}'}(\text{Ind}_D(b; \mathbf{v})) = \text{Ind}_D(\text{Res}_W^{W'}(b); \mathbf{v})$ .*

*Proof.* This follows easily from Definition 2.7 and the proof of [Delorme and Opdam 2011, Lemma 6.3], by taking the limit  $\lim_{\mathbf{v} \rightarrow 1}$  on both sides. □

**Remark 4.17.** From Propositions 4.15 and 4.16, it follows that for every  $b \in \mathcal{B}_{\text{gm}}$ , the induced character  $\text{Ind}_W^{W'}(b)$  is a positive integral linear combination of elements of  $\mathcal{B}'_{\text{gm}}$ . Therefore, in practice, in order to obtain the elements of  $\mathcal{B}'_{\text{gm}}$  that lie in the support of  $\text{Ind}_W^{W'}(b)$ , it is sufficient to decompose  $\text{Ind}_W^{W'}(b)$  as a positive integral linear combination of unit vectors in  $\bar{R}(W')$ . The resulting unit vectors are all in  $\mathcal{B}'_{\text{gm}}$  automatically by the canonical positivity property of  $\mathcal{B}'_{\text{gm}}$ .

The same analysis holds for the restrictions  $\text{Res}_W^{W'}(b)$ .

By the results of Sections 4B, 4C, and 4D we have determined the basis  $\mathcal{B}_{\text{gm}}$  for at least one representative of each isogeny class of irreducible root data. Using Remark 4.17 it is now easy to determine  $\mathcal{B}_{\text{gm}}$  for an arbitrary irreducible root datum.

Now suppose that  $\mathcal{R}$  is an arbitrary semisimple based root datum. The finite abelian group  $\Omega$  acts faithfully on the affine Coxeter diagram of  $\mathcal{R}$  by special affine diagram automorphisms, and it is easy to see that the special affine diagram automorphisms respect the irreducible components of the diagram of  $\mathcal{R}$ . Let  $D_i$  with  $i = 1, 2, \dots, e$  denote the irreducible components of the affine Coxeter diagram of  $\mathcal{R}$ , and let  $\Omega_i$  denote the image of  $\Omega$  in the group of special affine diagram automorphisms of  $D_i$ . Then  $\Omega \subset \Omega_1 \times \dots \times \Omega_e$ . Let  $\mathcal{R}' = \mathcal{R}_1 \times \mathcal{R}_2 \dots \times \mathcal{R}_e$  be the root datum which is isogenous to  $\mathcal{R}$ , such that  $\Omega' = \Omega_1 \times \dots \times \Omega_e$ .

**Proposition 4.18.** *We have  $\mathcal{Q} = \mathcal{Q}' = \mathcal{Q}_1 \times \dots \times \mathcal{Q}_e$ . In particular, Propositions 4.15 and 4.16 apply to the isogeny  $\mathcal{H} \subset \mathcal{H}'$ .*

*Proof.* We need to verify that  $R_{nr} = R'_{nr}$ . But this reduces to the actions of the groups  $\Omega$  and  $\Omega'$  on the irreducible components. The result follows easily from the definition of  $R_{nr}$  (see, e.g., [Opdam and Solleveld 2010, Section 2]).  $\square$

In the notation of Proposition 4.18, we have  $\mathcal{B}' = \mathcal{B}'_1 \times \cdots \times \mathcal{B}'_e$ , which can be determined explicitly since the factors are of irreducible type. Hence we can determine  $\mathcal{B}$  using Propositions 4.15 and 4.16.

**4F. Rationality of characters of discrete series.** In this subsection, we discuss the character value ring for the families of generic discrete series considered before. In light of Corollary 3.3, we know that for every generic residual central character  $W_{0r}$  and for every  $\mathbf{v} \in \mathcal{Q}_{W_{0r}}^{\text{reg}}$ , the central functional given by the “stable combination” of generic characters (16) takes values in  $\mathcal{Q}_\Lambda$ , the quotient field of  $\Lambda$ , i.e.,

$$\sum_{\chi \in \text{DS}_{W_{0r}(\mathbf{v})}} c_{\chi,C} \chi_{\mathbf{v}}(h) \in \mathcal{Q}_\Lambda, \quad \text{for all } h \in \mathcal{H}_\Lambda. \tag{38}$$

**Proposition 4.19.** *Suppose the root datum  $\mathcal{R}$  of the generic affine Hecke algebra  $\mathcal{H}_\Lambda$  is simple and not simply laced. Let  $W_{0r}$  be a generic residual central character and let  $\mathbf{v} \in \mathcal{Q}_{W_{0r}}^{\text{reg}}$  be given. Then for every discrete series character  $\chi \in \text{DS}_{W_{0r}(\mathbf{v})}$ , we have  $\chi_{\mathbf{v}}(h) \in \mathcal{Q}_\Lambda$ , for all  $h \in \mathcal{H}_\Lambda$ .*

*Proof.* By the classification of generic discrete series families [Opdam 2004; Opdam and Solleveld 2010], we know that, when  $\mathcal{R}$  is not simply laced, the cardinality of  $\text{DS}_{W_{0r}(\mathbf{v})}$  is always 1, except if  $\mathcal{R} = F_4$  and  $W_{0r}$  is the central character  $[0, k_1, 0, k_2 - k_1]$  from Table 2. Therefore, with this exception, the claim immediately follows from (38).

Let’s consider now this exceptional residual central character in  $F_4$ . In the same coordinates as in Table 2, we have  $r = v^{2[0, k_1, 0, k_2 - k_1]}$  and

$$\mathcal{Q}_{W_{0r}}^{\text{reg}} = \{k_1, k_2 \in \mathbb{R} \mid k_1 k_2 \neq 0\}.$$

There are always two families of discrete series  $\pi_{\mathbf{v},\text{I}} = \epsilon(b_8; \mathbf{v}) \text{Ind}_D(b_8; \mathbf{v})$  and  $\pi_{\mathbf{v},\text{II}} = \epsilon(b_9; \mathbf{v}) \text{Ind}_D(b_9; \mathbf{v})$  for  $\mathbf{v} \in \mathcal{Q}_{W_{0r}}^{\text{reg}}$ , where  $b_8, b_9$  are as in Table 2. From (38), we know that  $\pi_{\mathbf{v},\text{I}} + \pi_{\mathbf{v},\text{II}}$  takes values in  $\mathcal{Q}_\Lambda$ , so it suffices to show that  $\pi_{\mathbf{v},\text{II}}$  has the same property. Assume first that  $k_1 > 0$  and  $k_2 > 0$ . Then  $\pi_{\mathbf{v},\text{II}}$  is a 10-dimensional module that has the property that it is  $\mathcal{A}$ -semisimple, i.e., each generalized weight space under the action of Bernstein’s abelian subalgebra  $\mathcal{A}$  is one-dimensional. This claim follows from [Reeder 2000, page 80], where the weight diagram of this module is given under the label  $[A_1 E_7(a_5), -21]$ . Let  $\text{Wt}(\pi_{\mathbf{v},\text{II}})$  denote the set of weights. As it is well known, we may choose a basis of the module consisting of weight vectors  $\dagger_\lambda, \lambda \in \text{Wt}(\pi_{\mathbf{v},\text{II}})$  such that for every  $s \in S_0$ , the action of  $N_s$  is given

by

$$N_s \cdot \dagger_\lambda = \begin{cases} \frac{v(s) - v(s)^{-1}}{1 - \theta_{-\alpha}(\lambda)} \dagger_\lambda, & \text{if } s(\lambda) \notin \text{Wt}(\pi_{v,\text{II}}), \\ \frac{v(s) - v(s)^{-1}}{1 - \theta_{-\alpha}(\lambda)} \dagger_\lambda + \left( v(s)^{-1} + \frac{v(s) - v(s)^{-1}}{1 - \theta_{-\alpha}(\lambda)} \right) \dagger_{s(\lambda)} & \text{if } s(\lambda) \in \text{Wt}(\pi_{v,\text{II}}), \end{cases}$$

where  $s = s_\alpha$ . This means that both types of generators,  $\theta_x$  and  $N_s$  act in this basis via matrices with entries in  $Q_\Lambda$ , and the claim follows.

To treat the other three quadrants in  $k_1, k_2$ , notice that the affine Hecke algebra of type  $F_4$  has three involutions of the form  $N_s \mapsto -N_s^{-1}$ , where  $s$  ranges over the long simple reflections, the short simple reflections, and all the simple reflections, respectively. (The last one is the Iwahori–Matsumoto involution.) Applying these involutions to the modules  $\pi_{v,\text{I}}$  and  $\pi_{v,\text{II}}$  from the  $k_1 > 0, k_2 > 0$  case, we obtain the discrete series in the other three cases.  $\square$

## References

- [Artin 1999] M. Artin, “Noncommutative rings”, course notes, University of California, Berkeley, 1999.
- [Aubert et al. 2017] A.-M. Aubert, P. Baum, R. Plymen, and M. Solleveld, “The principal series of  $p$ -adic groups with disconnected center”, *Proc. London Math. Soc.* **114**:5 (2017), 798–854.
- [Barbasch et al. 2012] D. Barbasch, D. Ciubotaru, and P. E. Trapa, “Dirac cohomology for graded affine Hecke algebras”, *Acta Math.* **209**:2 (2012), 197–227. MR Zbl
- [Carter 1985] R. W. Carter, *Finite groups of Lie type: conjugacy classes and complex characters*, Wiley, New York, 1985. MR Zbl
- [Chriss and Ginzburg 1997] N. Chriss and V. Ginzburg, *Representation theory and complex geometry*, Birkhäuser, Boston, 1997. MR Zbl
- [Ciubotaru 2012] D. Ciubotaru, “Spin representations of Weyl groups and the Springer correspondence”, *J. Reine Angew. Math.* **671** (2012), 199–222. MR Zbl
- [Ciubotaru and He 2014] D. Ciubotaru and X. He, “Cocenters and representations of affine Hecke algebras”, preprint, 2014. To appear in *J. Eur. Math. Soc.* arXiv
- [Ciubotaru and He 2015] D. Ciubotaru and X. He, “Green polynomials of Weyl groups, elliptic pairings, and the extended Dirac index”, *Adv. Math.* **283** (2015), 1–50. MR Zbl
- [Ciubotaru and Kato 2011] D. Ciubotaru and S. Kato, “Tempered modules in exotic Deligne–Langlands correspondence”, *Adv. Math.* **226**:2 (2011), 1538–1590. MR Zbl
- [Ciubotaru and Opdam 2015] D. Ciubotaru and E. Opdam, “Formal degrees of unipotent discrete series representations and the exotic Fourier transform”, *Proc. Lond. Math. Soc.* (3) **110**:3 (2015), 615–646. MR Zbl
- [Ciubotaru and Trapa 2013] D. M. Ciubotaru and P. E. Trapa, “Characters of Springer representations on elliptic conjugacy classes”, *Duke Math. J.* **162**:2 (2013), 201–223. MR Zbl
- [Ciubotaru et al. 2012] D. Ciubotaru, M. Kato, and S. Kato, “On characters and formal degrees of discrete series of affine Hecke algebras of classical types”, *Invent. Math.* **187**:3 (2012), 589–635. MR Zbl
- [Ciubotaru et al. 2014] D. Ciubotaru, E. M. Opdam, and P. E. Trapa, “Algebraic and analytic Dirac induction for graded affine Hecke algebras”, *J. Inst. Math. Jussieu* **13**:3 (2014), 447–486. MR Zbl

- [Delorme and Opdam 2008] P. Delorme and E. M. Opdam, “The Schwartz algebra of an affine Hecke algebra”, *J. Reine Angew. Math.* **625** (2008), 59–114. MR Zbl
- [Delorme and Opdam 2011] P. Delorme and E. Opdam, “Analytic  $R$ -groups of affine Hecke algebras”, *J. Reine Angew. Math.* **658** (2011), 133–172. MR Zbl
- [Geck and Pfeiffer 2000] M. Geck and G. Pfeiffer, *Characters of finite Coxeter groups and Iwahori–Hecke algebras*, London Mathematical Society Monographs (N.S.) **21**, Oxford University Press, New York, 2000. MR Zbl
- [Heckman and Opdam 1997] G. J. Heckman and E. M. Opdam, “Yang’s system of particles and Hecke algebras”, *Ann. of Math. (2)* **145**:1 (1997), 139–173. MR Zbl
- [Kato 2009] S. Kato, “An exotic Deligne–Langlands correspondence for symplectic groups”, *Duke Math. J.* **148**:2 (2009), 305–371. MR Zbl
- [Kazhdan and Lusztig 1987] D. Kazhdan and G. Lusztig, “Proof of the Deligne–Langlands conjecture for Hecke algebras”, *Invent. Math.* **87**:1 (1987), 153–215. MR Zbl
- [Kollár and Nowak 2015] J. Kollár and K. Nowak, “Continuous rational functions on real and  $p$ -adic varieties”, *Math. Z.* **279**:1–2 (2015), 85–97. MR Zbl
- [Lusztig 1989a] G. Lusztig, “Affine Hecke algebras and their graded version”, *J. Amer. Math. Soc.* **2**:3 (1989), 599–635. MR Zbl
- [Lusztig 1989b] G. Lusztig, “Cells in affine Weyl groups, IV”, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **36**:2 (1989), 297–328. MR Zbl
- [Lusztig 1995] G. Lusztig, “Cuspidal local systems and graded Hecke algebras, II”, pp. 217–275 in *Representations of groups* (Banff, AB, 1994), edited by B. N. Allison and G. H. Cliff, CMS Conf. Proc. **16**, Amer. Math. Soc., Providence, RI, 1995. MR Zbl
- [Lusztig 2002] G. Lusztig, “Cuspidal local systems and graded Hecke algebras, III”, *Represent. Theory* **6** (2002), 202–242. MR Zbl
- [Opdam 1995] E. M. Opdam, “A remark on the irreducible characters and fake degrees of finite real reflection groups”, *Invent. Math.* **120**:3 (1995), 447–454. MR Zbl
- [Opdam 2004] E. M. Opdam, “On the spectral decomposition of affine Hecke algebras”, *J. Inst. Math. Jussieu* **3**:4 (2004), 531–648. MR Zbl
- [Opdam 2007] E. Opdam, “The central support of the Plancherel measure of an affine Hecke algebra”, *Mosc. Math. J.* **7**:4 (2007), 723–741. MR Zbl
- [Opdam 2016] E. Opdam, “Spectral transfer morphisms for unipotent affine Hecke algebras”, *Selecta Math. (N.S.)* **22**:4 (2016), 2143–2207. MR Zbl
- [Opdam and Solleveld 2009] E. Opdam and M. Solleveld, “Homological algebra for affine Hecke algebras”, *Adv. Math.* **220**:5 (2009), 1549–1601. MR Zbl
- [Opdam and Solleveld 2010] E. Opdam and M. Solleveld, “Discrete series characters for affine Hecke algebras and their formal degrees”, *Acta Math.* **205**:1 (2010), 105–187. MR Zbl
- [Orlik and Terao 1992] P. Orlik and H. Terao, *Arrangements of hyperplanes*, Grundlehren der Mathematischen Wissenschaften **300**, Springer, 1992. MR Zbl
- [Ram and Ramagge 2003] A. Ram and J. Ramagge, “Affine Hecke algebras, cyclotomic Hecke algebras, and Clifford theory”, pp. 428–466 in *A tribute to C. S. Seshadri: a collection of articles on geometry and representation theory* (Chennai, 2002), edited by V. Lakshmibai et al., Trends Math., Birkhäuser, Basel, 2003. MR Zbl
- [Reeder 1994] M. Reeder, “On the Iwahori-spherical discrete series for  $p$ -adic Chevalley groups; formal degrees and  $L$ -packets”, *Ann. Sci. École Norm. Sup. (4)* **27**:4 (1994), 463–491. MR Zbl

- [Reeder 2000] M. Reeder, “Formal degrees and  $L$ -packets of unipotent discrete series representations of exceptional  $p$ -adic groups”, *J. Reine Angew. Math.* **520** (2000), 37–93. MR Zbl
- [Reeder 2001] M. Reeder, “Euler–Poincaré pairings and elliptic representations of Weyl groups and  $p$ -adic groups”, *Compositio Math.* **129**:2 (2001), 149–181. MR Zbl
- [Reeder 2002] M. Reeder, “Isogenies of Hecke algebras and a Langlands correspondence for ramified principal series representations”, *Represent. Theory* **6** (2002), 101–126. MR Zbl
- [Schechtman and Varchenko 1991] V. V. Schechtman and A. N. Varchenko, “Arrangements of hyperplanes and Lie algebra homology”, *Invent. Math.* **106**:1 (1991), 139–194. MR Zbl
- [Slooten 2008] K. Slooten, “Induced discrete series representations for Hecke algebras of types  $B_n^{\text{aff}}$  and  $C_n^{\text{aff}}$ ”, *Int. Math. Res. Not.* **2008**:10 (2008), art. id. rnn023, 41 pp. MR Zbl
- [Solleveld 2012] M. Solleveld, “On the classification of irreducible representations of affine Hecke algebras with unequal parameters”, *Represent. Theory* **16** (2012), 1–87. MR Zbl
- [Waldspurger 2004] J.-L. Waldspurger, “Représentations de réduction unipotente pour  $\text{SO}(2n+1)$ : quelques conséquences d’un article de Lusztig”, pp. 803–910 in *Contributions to automorphic forms, geometry, and number theory*, edited by H. Hida et al., Johns Hopkins Univ. Press, Baltimore, 2004. MR Zbl

Communicated by Marie-France Vignéras

Received 2016-04-21

Revised 2016-09-06

Accepted 2016-12-04

Dan.Ciubotaru@maths.ox.ac.uk

*Mathematical Institute, University of Oxford,  
Andrew Wiles Building, Oxford, OX2 6GG, United Kingdom*

e.m.opdam@uva.nl

*Korteweg-de Vries Institute for Mathematics,  
Universiteit van Amsterdam, Science Park 105-107,  
1098 XG Amsterdam, Netherlands*



# An explicit bound for the least prime ideal in the Chebotarev density theorem

Jesse Thorner and Asif Zaman

We prove an explicit version of Weiss' bound on the least norm of a prime ideal in the Chebotarev density theorem, which is a significant improvement on the work of Lagarias, Montgomery, and Odlyzko. As an application, we prove the first explicit, nontrivial, and unconditional upper bound for the least prime represented by a positive-definite primitive binary quadratic form. We also consider applications to elliptic curves and congruences for the Fourier coefficients of holomorphic cuspidal modular forms.

## 1. Introduction and statement of results

In 1837, Dirichlet proved that if  $a, q \in \mathbb{Z}$  and  $\gcd(a, q) = 1$ , then there are infinitely many primes  $p \equiv a \pmod{q}$ . In light of this result, it is natural to ask how big the first such prime, say  $P(a, q)$ , is. Assuming the generalized Riemann hypothesis (GRH) for Dirichlet  $L$ -functions, Lamzouri, Li, and Soundararajan [Lamzouri et al. 2015] proved that for all  $q \geq 4$ ,

$$P(a, q) \leq (\varphi(q) \log q)^2, \quad (1-1)$$

where  $\varphi$  is Euler's totient function. Nontrivial, unconditional upper bounds are significantly harder to prove. The first such bound on  $P(a, q)$  is due to Linnik [1944a; 1944b], who proved that for some absolute constant  $c_1 > 0$ ,

$$P(a, q) \ll q^{c_1} \quad (1-2)$$

with an absolute and computable implied constant. Admissible values of  $c_1$  are now known explicitly. Building on the work of Heath-Brown [1992], Xylouris [2011] proved that one may take  $c_1 = 5.2$  unconditionally. (Xylouris improved this to  $c_1 = 5$  in his Ph.D. thesis.) For a detailed history of the unconditional progress toward (1-1), see [Heath-Brown 1992, Section 1].

---

*MSC2010:* primary 11R44; secondary 11M41, 14H52.

*Keywords:* Chebotarev density theorem, least prime ideal, Linnik's theorem, binary quadratic forms, elliptic curves, modular forms, log-free zero density estimate.

A broad generalization of (1-2) lies in the context of the Chebotarev density theorem. Let  $L/F$  be a Galois extension of number fields with Galois group  $G$ . To each prime ideal  $\mathfrak{p}$  of  $F$  which is unramified in  $L$ , there corresponds a certain conjugacy class of automorphisms in  $G$  which are attached to the prime ideals of  $L$  lying above  $\mathfrak{p}$ . We denote this conjugacy class using the Artin symbol  $\left[\frac{L/F}{\mathfrak{p}}\right]$ . For a conjugacy class  $C \subset G$ , let

$$\pi_C(x, L/F) := \#\left\{\mathfrak{p} : \mathfrak{p} \text{ is unramified in } L, \left[\frac{L/F}{\mathfrak{p}}\right] = C, N_{F/\mathbb{Q}} \mathfrak{p} \leq x\right\}.$$

The Chebotarev density theorem asserts that

$$\pi_C(x, L/F) \sim \frac{|C|}{|G|} \int_2^x \frac{dt}{\log t}.$$

In analogy with (1-2), it is natural to bound the quantity

$$P(C, L/F) := \min\left\{N_{F/\mathbb{Q}} \mathfrak{p} : \mathfrak{p} \text{ unramified in } L, \left[\frac{L/F}{\mathfrak{p}}\right] = C, N_{F/\mathbb{Q}} \mathfrak{p} \text{ a rational prime}\right\}. \quad (1-3)$$

Under GRH for Hecke  $L$ -functions, Lagarias and Odlyzko [1977] proved a bound for  $P(C, L/F)$ ; Bach and Sorenson [1996] made this bound explicit, proving that

$$P(C, L/F) \leq (4 \log D_L + 2.5[L : \mathbb{Q}] + 5)^2, \quad (1-4)$$

where  $D_L = |\text{disc}(L/\mathbb{Q})|$ . (This can be improved assuming Artin’s conjecture; see work of V. K. Murty [1994, Equation 2].) We note that if  $L = \mathbb{Q}(e^{2\pi i/q})$  for some integer  $q \geq 1$  and  $F = \mathbb{Q}$ , then one recovers a bound of the same analytic quality as (1-1), though the constants are slightly larger.

The first nontrivial, unconditional bound on  $P(C, L/F)$  is due to Lagarias, Montgomery, and Odlyzko [Lagarias et al. 1979]; they proved  $P(C, L/F) \leq 2D_L^{c_2}$  for some absolute constant  $c_2 > 0$ . Recently, Zaman [2017b] explicitly bounded  $c_2$ , proving that<sup>1</sup>

$$P(C, L/F) \ll D_L^{40}. \quad (1-5)$$

The bound (1-5), up to quality of the exponent, is commensurate with the best known bounds when  $L$  is a quadratic extension of  $F = \mathbb{Q}$ , which reduces to the problem of bounding the least quadratic nonresidue. We observe, however, that if  $q$  is prime,  $L = \mathbb{Q}(e^{2\pi i/q})$ , and  $F = \mathbb{Q}$ , then (1-5) states that  $P(a, q) \ll q^{40(q-2)}$ , which is much worse than (1-2).

Weiss [1983] significantly improved the results in [Lagarias et al. 1979]. Let  $A$  be any abelian subgroup of  $G$  such that  $A \cap C$  is nonempty, let  $\hat{A}$  be the character

---

<sup>1</sup>Unless mentioned otherwise, all implied constants in all asymptotic inequalities  $f \ll g$  or  $f = O(g)$  are absolute and computable.

group of  $A$ , and let  $K = L^A$  be the subfield of  $L$  fixed by  $A$ . Let the  $K$ -integral ideal  $\mathfrak{f}_\chi$  be the conductor of a character  $\chi \in \hat{A}$ , and let

$$\mathcal{Q}(L/K) = \max\{N_{K/\mathbb{Q}} \mathfrak{f}_\chi : \chi \in \hat{A}\}. \tag{1-6}$$

Weiss proved that for certain absolute constants  $c_3 > 0$  and  $c_4 > 0$ ,

$$P(C, L/F) \leq 2[K : \mathbb{Q}]^{c_3[K:\mathbb{Q}]} (D_K \mathcal{Q}(L/K))^{c_4}. \tag{1-7}$$

To see how (1-7) compares to (1-5), we observe that if  $A$  is a cyclic subgroup of  $G$ , then

$$D_L^{1/|A|} \leq D_K \mathcal{Q}(L/K) \leq D_L^{1/\varphi(|A|)}.$$

(See [Bach and Sorenson 1996, Lemma 4.2] for a proof of the upper bound; the lower bound holds for all  $A$  and follows from the conductor-discriminant formula.) Furthermore, if  $F = \mathbb{Q}$  and  $L = \mathbb{Q}(e^{2\pi i/q})$ , then one may take  $\hat{A}$  to be the full group of Dirichlet characters modulo  $q$ , in which case  $K = F = \mathbb{Q}$  and  $\mathcal{Q}(L/K) = q$ . Thus Weiss proves a bound on  $P(C, L/F)$ , which provides a “continuous transition” from (1-2) to (1-5). In particular, (1-2) follows from (1-7).

In this paper, we prove the following bound on  $P(C, L/F)$ , which makes (1-7) explicit.

**Theorem 1.1.** *Let  $L/F$  be a Galois extension of number fields with Galois group  $G$ , let  $C \subset G$  be a conjugacy class, and let  $P(C, L/F)$  be defined by (1-3). Let  $A \subset G$  be an abelian subgroup such that  $A \cap C$  is nonempty,  $K = L^A$  be the fixed field of  $A$ , and  $\mathcal{Q} = \mathcal{Q}(L/K)$  be defined by (1-6). Then*

$$P(C, L/F) \ll D_K^{694} \mathcal{Q}^{521} + D_K^{232} \mathcal{Q}^{367} [K : \mathbb{Q}]^{290[K:\mathbb{Q}]}.$$

**Remarks.** • Theorem 1.1 immediately implies that  $P(a, q) \ll q^{521}$ . For historical context, this is slightly better than Jutila’s bound [1970] on  $P(a, q)$ , which was over 25 years after Linnik’s original theorem.

- The bound we obtain on  $P(C, L/F)$  follows immediately from the effective lower bound on  $\pi_C(x, L/F)$  given by (3-2), which is of independent interest. See [Zaman 2017a, Theorem 1.3.1] for a related lower bound.
- If  $[K : \mathbb{Q}] \leq 2(\log D_K) / \log \log D_K$ , then  $P(C, L/F) \ll D_K^{694} \mathcal{Q}^{521}$ . Situations where  $[K : \mathbb{Q}] > 2(\log D_K) / \log \log D_K$  are rare; the largest class of known examples involve infinite  $p$ -class tower extensions, which were first studied by Golod and Šafarevič [1964].
- If  $L/K$  is unramified, then  $\mathcal{Q} = 1$  and  $D_K = D_L^{1/|A|}$ . Thus

$$P(C, L/F) \ll D_L^{694/|A|} + D_L^{232/|A|} [K : \mathbb{Q}]^{290[K:\mathbb{Q}]}.$$

If  $[K : \mathbb{Q}] \leq 2(\log D_K) / \log \log D_K$ , this improves (1-5) when  $|A| \geq 18$ .

We now consider some specific applications of Theorem 1.1, the first of which is a bound on the least prime represented by a positive-definite primitive binary quadratic form  $Q(x, y) \in \mathbb{Z}[x, y]$  of discriminant  $D$ . It follows from (1-7) that the least such prime  $p$  satisfies  $p \ll |D|^{c_5}$  for some positive absolute constant  $c_5$ ; see Kowalski and Michel [2002] for a similar observation. Ditchen [2013] proved, on average over  $D \not\equiv 0 \pmod{8}$ , that  $p \ll_\epsilon |D|^{20/3+\epsilon}$ , and Zaman [2016b] showed  $p \ll_\epsilon |D|^{9.5+\epsilon}$  in an exceptional case. However, a nontrivial unconditional explicit bound on the least prime represented by  $Q$  for *all* such quadratic forms has not been calculated before now. Such a bound follows immediately from Theorem 1.1.

**Theorem 1.2.** *Let  $Q(x, y) \in \mathbb{Z}[x, y]$  be a positive-definite primitive binary quadratic form of discriminant  $D$ . There exists a prime  $p \nmid D$  represented by  $Q(x, y)$  such that  $p \ll |D|^{694}$ . In particular, if  $n$  is a fixed positive integer, there exists a prime  $p \nmid n$  represented by  $x^2 + ny^2$  such that  $p \ll n^{694}$ .*

We now consider applications to the study of the group of points on an elliptic curve over a finite field. Let  $E/\mathbb{Q}$  be an elliptic curve without complex multiplication (CM), and let  $N_E$  be the conductor of  $E$ . The order and group structure of  $E(\mathbb{F}_p)$ , the group of  $\mathbb{F}_p$ -rational points on  $E$ , frequently appears when doing arithmetic over  $E$ . Thus we are interested in understanding the distribution of values and divisibility properties of  $\#E(\mathbb{F}_p)$ .

V. K. Murty [1994] and Li [2012] proved unconditional and GRH-conditional bounds on the least prime that does not split completely in a number field. This yields bounds on the least prime  $p \nmid \ell N_E$  such that  $\ell \nmid \#E(\mathbb{F}_p)$ , where  $\ell \geq 11$  is prime. As an application of Theorem 1.1, we prove a complementary result on the least  $p \nmid \ell N_E$  such that  $\ell \mid \#E(\mathbb{F}_p)$ . To state the result, we define  $\omega(N_E) = \#\{p : p \mid N_E\}$  and  $\text{rad}(N_E) = \prod_{p \mid N_E} p$ .

**Theorem 1.3.** *Let  $E/\mathbb{Q}$  be a non-CM elliptic curve of conductor  $N_E$ , and let  $\ell \geq 11$  be prime. There exists a prime  $p \nmid \ell N_E$  such that*

$$p \ll \ell^{(5300+1600\omega(N_E))\ell^2} \text{rad}(N_E)^{1900\ell^2} \quad \text{and} \quad \ell \mid \#E(\mathbb{F}_p).$$

**Remark.** The proof is easily adapted to allow for elliptic curves over other number fields; we omit further discussion for brevity.

One of the first significant results in the study of the distribution of values of  $\#E(\mathbb{F}_p)$  is due to Hasse, who proved that if  $p \nmid N_E$ , then  $|p + 1 - \#E(\mathbb{F}_p)| < 2\sqrt{p}$ . For a prime  $\ell$ , the distribution of the primes  $p$  such that  $\#E(\mathbb{F}_p) \equiv p + 1 \pmod{\ell}$  can also be studied using the mod  $\ell$  Galois representations associated to  $E$ .

**Theorem 1.4.** *Let  $E/\mathbb{Q}$  be a non-CM elliptic curve of squarefree conductor  $N_E$ , and let  $\ell \geq 11$  be prime. There exists a prime  $p \nmid \ell N_E$  such that*

$$\#E(\mathbb{F}_p) \equiv p + 1 \pmod{\ell} \quad \text{and} \quad p \ll \ell^{(4600+1200\omega(N_E))\ell} N_E^{2100\ell}.$$

Theorem 1.4 will follow from a more general result on congruences for the Fourier coefficients of certain holomorphic cuspidal modular forms. Let

$$f(z) = \sum_{n=1}^{\infty} a_f(n)e^{2\pi inz}$$

be a cusp form of integral weight  $k_f \geq 2$ , level  $N_f \geq 1$ , and nebentypus  $\chi_f$ . Suppose further that  $f$  is a normalized eigenform for the Hecke operators. We call such a cusp form  $f$  a newform; for each newform  $f$ , the map  $n \mapsto a_f(n)$  is multiplicative. Suppose  $a_f(n) \in \mathbb{Z}$  for all  $n \geq 1$ . In this case,  $\chi_f$  is trivial when  $f$  does not have CM, and  $\chi_f$  is a nontrivial real character when  $f$  does have CM. Moreover, when  $k_f = 2$ ,  $f$  is the newform associated to an isogeny class of elliptic curves  $E/\mathbb{Q}$ . In this case,  $N_f = N_E$ , and for any prime  $p \nmid N_E$ , we have that  $a_f(p) = p + 1 - \#E(\mathbb{F}_p)$ .

**Theorem 1.5.** *Let  $f(z) = \sum_{n=1}^{\infty} a_f(n)e^{2\pi inz} \in \mathbb{Z}[[e^{2\pi iz}]]$  be a non-CM newform of even integral weight  $k_f \geq 2$ , level  $N_f$ , and trivial nebentypus. Let  $\ell \geq 3$  be a prime such that (12-1) holds and  $\gcd(k_f - 1, \ell - 1) = 1$ . For any residue class  $a$  modulo  $\ell$ , there exists a prime  $p \nmid \ell N_f$  such that*

$$a_f(p) \equiv a \pmod{\ell} \quad \text{and} \quad p \ll \ell^{(4600+1200\omega(N_f))\ell} \text{rad}(N_f)^{2100\ell}.$$

**Remarks.** • Equation (12-1) is a fairly mild condition regarding whether the modulo  $\ell$  reduction of a certain representation is surjective. This condition is satisfied by all but finitely many choices of  $\ell$ . See Section 12 for further details.

- The proofs of Theorems 1.3–1.5 are easily adapted to allow composite moduli  $\ell$  as well as elliptic curves and modular forms with CM. Moreover, the proofs can be easily modified to study the mod  $\ell$  distribution of the trace of Frobenius for elliptic curves over number fields other than  $\mathbb{Q}$ . We omit further discussion for brevity.
- Using (1-5), the least prime  $p$  such that  $a_f(p) \equiv a \pmod{\ell}$  satisfies the bound  $p \ll \ell^{120\ell^3(1+\omega(N_f))} \text{rad}(N_f)^{40(\ell^3-1)}$  for any choice of  $a$ . Thus Theorem 1.5 constitutes an improvement over (1-5) for  $\ell \geq 11$ .
- If  $r_{24}(n)$  is the number of representations of  $n$  as a sum of 24 squares, then  $691r_{24}(p) = 16(p^{11} + 1) + 33152\tau(p)$ , where Ramanujan’s function  $\tau(n)$  is the  $n$ -th Fourier coefficient of  $\Delta(z)$ , the unique non-CM newform of weight 12 and level 1. If  $\ell \notin \{2, 3, 5, 7, 23, 691\}$  is such that  $\ell \not\equiv 1 \pmod{11}$ , then by Theorem 1.5, there exists  $p \neq \ell$  such that

$$691r_{24}(p) \equiv 16(p^{11} + 1) \pmod{\ell} \quad \text{and} \quad p \ll \ell^{4600\ell}.$$

## 2. Notation and auxiliary estimates

**2A. Notation.** We use the following notation throughout the paper.

- $K$  is a number field.
- $\mathcal{O}_K$  is the ring of integers of  $K$ .
- $n_K = [K : \mathbb{Q}]$  is the degree of  $K/\mathbb{Q}$ .
- $D_K$  is the absolute value of the discriminant of  $K$ .
- $N = N_{K/\mathbb{Q}}$  is the absolute field norm of  $K$ .
- $\zeta_K(s)$  is the Dedekind zeta function of  $K$ .
- $\mathfrak{q}$  is an integral ideal of  $K$ .
- $\text{Cl}(\mathfrak{q}) = I(\mathfrak{q})/P_{\mathfrak{q}}$  is the narrow ray class group of  $K$  modulo  $\mathfrak{q}$ .
- $\chi$ , or  $\chi \pmod{\mathfrak{q}}$ , is a character of  $\text{Cl}(\mathfrak{q})$ , referred to as a Hecke character or ray class character of  $K$ .
- $\delta(\chi)$  is the indicator function of the trivial character.
- $\mathfrak{f}_{\chi}$  is the conductor of  $\chi$ ; that is, it is the maximal integral ideal such that  $\chi$  is induced from a primitive character  $\chi^* \pmod{\mathfrak{f}_{\chi}}$ .
- $D_{\chi} = D_K N_{\mathfrak{f}_{\chi}}$ .
- $L(s, \chi)$  is the Hecke  $L$ -function associated to  $\chi$ .
- $H$ , or  $H \pmod{\mathfrak{q}}$ , is a subgroup of  $\text{Cl}(\mathfrak{q})$ , or equivalently of  $I(\mathfrak{q})$ , containing  $P_{\mathfrak{q}}$ . The group  $H$  is referred to as a congruence class group of  $K$ .
- $\chi \pmod{H}$  is a character  $\chi \pmod{\mathfrak{q}}$  satisfying  $\chi(H) = 1$ .
- $Q = Q_H = \max\{N_{\mathfrak{f}_{\chi}} : \chi \pmod{H}\}$  is the maximum conductor of  $H$ .
- $\mathfrak{f}_H = \text{lcm}\{\mathfrak{f}_{\chi} : \chi \pmod{H}\}$  is the conductor of  $H$ .
- $H^* \pmod{\mathfrak{f}_H}$  is the primitive congruence class group inducing  $H$ .
- $h_H = [I(\mathfrak{q}) : H]$ .

We also adhere to the convention that all implied constants in all asymptotic inequalities  $f \ll g$  or  $f = O(g)$  are absolute with respect to  $H$  and  $K$ . If an implied constant depends on a parameter, such as  $\epsilon$ , then we use  $\ll_{\epsilon}$  and  $O_{\epsilon}$  to denote that the implied constant depends at most on  $\epsilon$ . All implied constants will be effectively computable. Finally, all sums over integral ideals of  $K$  will be over nonzero integral ideals.

**2B. Hecke  $L$ -functions.** For a more detailed reference on Hecke  $L$ -functions, see [Lagarias et al. 1979]. Strictly speaking, a Hecke character  $\chi$  is a function on  $\text{Cl}(\mathfrak{q})$  but, by pulling back the domain of  $\chi$  and extending it by zero, we regard  $\chi$  as a function on integral ideals of  $K$ . We use this convention throughout the paper.

The Hecke  $L$ -function of  $\chi$ , denoted  $L(s, \chi)$ , is defined as

$$L(s, \chi) = \sum_{\mathfrak{n}} \chi(\mathfrak{n}) N_{\mathfrak{n}}^{-s} = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N_{\mathfrak{p}}^s}\right)^{-1} \quad (2-1)$$

for  $\text{Re}\{s\} > 1$ , where the sum is over integral ideals  $\mathfrak{n}$  of  $K$  and the product is over prime ideals  $\mathfrak{p}$  of  $K$ . Recall that the Dedekind zeta function  $\zeta_K(s)$  is the primitive Hecke  $L$ -function associated to the trivial character  $\chi_0$ ; that is,

$$\zeta_K(s) = \sum_{\mathfrak{n}} (\mathfrak{N}\mathfrak{n})^{-s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathfrak{N}\mathfrak{p}^s}\right)^{-1} \tag{2-2}$$

for  $\text{Re}\{s\} > 1$ . Returning to  $L(s, \chi)$ , assume that  $\chi$  is primitive for the remainder of this subsection, unless otherwise specified. Define the *completed Hecke  $L$ -function*  $\xi(s, \chi)$  by

$$\xi(s, \chi) = [s(s-1)]^{\delta(\chi)} D_\chi^{s/2} \gamma_\chi(s) L(s, \chi), \tag{2-3}$$

where  $D_\chi = D_K \mathfrak{N}\mathfrak{f}_\chi$ ,  $\delta(\chi)$  is the indicator function of the trivial character, and  $\gamma_\chi(s)$  is the *gamma factor of  $\chi$*  defined by

$$\gamma_\chi(s) = \left[\pi^{-s/2} \Gamma\left(\frac{s}{2}\right)\right]^{a(\chi)} \cdot \left[\pi^{-(s+1)/2} \Gamma\left(\frac{s+1}{2}\right)\right]^{b(\chi)}. \tag{2-4}$$

Here  $a(\chi)$  and  $b(\chi)$  are certain nonnegative integers satisfying

$$a(\chi) + b(\chi) = n_K. \tag{2-5}$$

It is a classical fact that  $\xi(s, \chi)$  is entire of order 1 and satisfies the functional equation

$$\xi(s, \chi) = w(\chi) \xi(1-s, \bar{\chi}), \tag{2-6}$$

where  $w(\chi) \in \mathbb{C}$  is the *root number* of  $\chi$  satisfying  $|w(\chi)| = 1$ . The zeros of  $\xi(s, \chi)$  are the *nontrivial zeros*  $\rho$  of  $L(s, \chi)$  and are known to satisfy  $0 < \text{Re}\{\rho\} < 1$ . The *trivial zeros*  $\omega$  of  $L(s, \chi)$  are given by

$$\text{ord}_{s=\omega} L(s, \chi) = \begin{cases} a(\chi) - \delta(\chi) & \text{if } \omega = 0, \\ b(\chi) & \text{if } \omega = -1, -3, -5, \dots, \\ a(\chi) & \text{if } \omega = -2, -4, -6, \dots, \end{cases} \tag{2-7}$$

and arise as poles of the gamma factor of  $L(s, \chi)$ . Since  $\xi(s, \chi)$  is entire of order 1, it admits a Hadamard product factorization given by

$$\xi(s, \chi) = e^{A(\chi)+B(\chi)s} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho}. \tag{2-8}$$

**Lemma 2.1.** *Let  $\chi$  be a primitive Hecke character. Then*

$$-\text{Re}\left\{\frac{L'}{L}(s, \chi)\right\} = \frac{1}{2} \log D_\chi + \text{Re}\left\{\frac{\delta(\chi)}{s-1} + \frac{\delta(\chi)}{s}\right\} - \sum_{\rho} \text{Re}\left\{\frac{1}{s-\rho}\right\} + \text{Re}\left\{\frac{\gamma'_\chi(s)}{\gamma_\chi(s)}\right\},$$

where the sum is over all nontrivial zeros  $\rho$  of  $L(s, \chi)$ .

*Proof.* See [Lagarias and Odlyzko 1977, Lemma 5.1], for example. □

By similar arguments, there exists an explicit formula for higher derivatives of  $-\frac{L'}{L}(s, \chi)$ .

**Lemma 2.2.** *Let  $\chi$  be a Hecke character (not necessarily primitive) and  $k \geq 1$  be a positive integer. Then*

$$\begin{aligned} (-1)^{k+1} \frac{d^k}{ds^k} \frac{L'}{L}(s, \chi) &= \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} (\log N\mathfrak{p}) \chi(\mathfrak{p}) \frac{(\log N\mathfrak{p}^m)^k}{(N\mathfrak{p}^m)^s} \\ &= \frac{\delta(\chi)k!}{(s-1)^{k+1}} - \sum_{\omega} \frac{k!}{(s-\omega)^{k+1}} \end{aligned}$$

for  $\text{Re}\{s\} > 1$ , where the first sum is over prime ideals  $\mathfrak{p}$  of  $K$  and the second sum is over all zeros  $\omega$  of  $L(s, \chi)$ , including trivial ones, counted with multiplicity.

*Proof.* By standard arguments, this follows from the Hadamard product (2-8) of  $\xi(s, \chi)$  and the Euler product of  $L(s, \chi)$ . See [Lagarias et al. 1979, (5.2) and (5.3)], for example. □

**2C. Explicit  $L$ -function estimates.** In order to obtain explicit results, we must have explicit bounds on a few important quantities. First, we record a bound for  $L(s, \chi)$  in the critical strip  $0 < \text{Re}\{s\} < 1$  via a Phragmén–Lindelöf type convexity estimate due to Rademacher.

**Lemma 2.3** [Rademacher 1959]. *Let  $\chi$  be a primitive Hecke character and take  $\eta \in (0, \frac{1}{2}]$ . Then for  $s = \sigma + it$ ,*

$$|L(s, \chi)| \ll \left| \frac{1+s}{1-s} \right|^{\delta(\chi)} \zeta_{\mathbb{Q}}(1+\eta)^{n_K} \left( \frac{D_{\chi}}{(2\pi)^{n_K}} (3+|t|)^{n_K} \right)^{(1+\eta-\sigma)/2}$$

uniformly in the strip  $-\eta \leq \sigma \leq 1 + \eta$ .

Next, we record an explicit bound on the digamma function and  $\frac{\gamma'_{\chi}}{\gamma_{\chi}}(s)$ .

**Lemma 2.4.** *Let  $s = \sigma + it$  with  $\sigma > 1$  and  $t \in \mathbb{R}$ . Then  $\text{Re}\left\{\frac{\Gamma'}{\Gamma}(s)\right\} \leq \log |s| + \sigma^{-1}$  and, for any Hecke character  $\chi$ ,*

$$\text{Re}\left\{\frac{\gamma'_{\chi}}{\gamma_{\chi}}(s)\right\} \leq \frac{n_K}{2}(\log(|s| + 1) + \sigma^{-1} - \log \pi).$$

*In particular, for  $1 < \sigma \leq 6.2$  and  $|t| \leq 1$ , we have  $\text{Re}\left\{\frac{\gamma'_{\chi}}{\gamma_{\chi}}(s)\right\} \leq 0$ .*

*Proof.* The first estimate follows from [Ono and Soundararajan 1997, Lemma 4]. The second estimate is a straightforward consequence of the first combined with the definition of  $\gamma_{\chi}(s)$  in (2-4). The third estimate is contained in [Ahn and Kwon 2014, Lemma 3]. □

Next, we establish some bounds on the number of zeros of  $L(s, \chi)$  in a circle.



**Lemma 2.5.** *Let  $\chi$  be a Hecke character. Let  $s = \sigma + it$  with  $\sigma > 1$  and  $t \in \mathbb{R}$ . For  $r > 0$ , denote*

$$N_\chi(r; s) := \#\{\rho = \beta + i\gamma : 0 < \beta < 1, L(\rho, \chi) = 0, |s - \rho| \leq r\}. \tag{2-9}$$

If  $0 < r \leq 1$ , then

$$N_\chi(r; s) \leq \{4 \log D_K + 2 \log \text{Nf}_\chi + 2n_K \log(|t| + 3) + 4 + 4\delta(\chi)\} \cdot r + 4 + 4\delta(\chi).$$

*Proof.* Without loss, we may assume  $\chi$  is primitive. Observe that

$$N_\chi(r; s) \leq N_\chi(r; 1 + it) \leq N_\chi(2r; 1 + r + it),$$

so it suffices to bound the latter quantity. Now, if  $s_0 = 1 + r + it$ , notice

$$N_\chi(2r; s_0) \leq 4r \sum_{|s_0 - \rho| \leq 2r} \text{Re}\left\{\frac{1}{s_0 - \rho}\right\} \leq 4r \sum_{\rho} \text{Re}\left\{\frac{1}{s_0 - \rho}\right\}.$$

Applying Lemmas 2.1 and 2.4 twice and noting  $\text{Re}\left\{\frac{L'}{L}(s_0, \chi)\right\} \leq -\frac{\xi'_K}{\xi_K}(1 + r)$  via their respective Euler products, the above is

$$\begin{aligned} &\leq 4r \left( \text{Re}\left\{\frac{L'}{L}(s_0, \chi)\right\} + \frac{1}{2} \log D_\chi + \text{Re}\left\{\frac{\gamma'_\chi}{\gamma_\chi}(s_0)\right\} + \delta(\chi) \text{Re}\left\{\frac{1}{s_0} + \frac{1}{s_0 - 1}\right\} \right) \\ &\leq \{4 \log D_K + 2 \log \text{Nf}_\chi + 2n_K \log(|t| + 3) + 4 + 4\delta(\chi)\} \cdot r + 4 + 4\delta(\chi) \end{aligned}$$

as  $D_\chi = D_K \text{Nf}_\chi$ . For details on estimating  $-\frac{\xi'_K}{\xi_K}(1 + r)$ , see Lemma 2.10.  $\square$

To improve the bound in Lemma 2.5, we exhibit an explicit inequality involving the logarithmic derivative of  $L(s, \chi)$  comparable with [Kadiri and Ng 2012, Theorem 2] for the Dedekind zeta function.

**Proposition 2.6.** *Let  $0 < \epsilon < \frac{1}{4}$ ,  $T \geq 1$ , and  $s = \sigma + it$ . For a primitive Hecke character  $\chi$ , define a multiset of nontrivial zeros of  $L(s, \chi)$  by*

$$\mathcal{Z}_{r,t} = \{\rho = \beta + i\gamma : L(\rho, \chi) = 0, |1 + it - \rho| \leq r\}.$$

Then, for  $0 < r < \epsilon$ ,

$$\begin{aligned} -\text{Re}\left\{\frac{L'}{L}(s, \chi)\right\} &\leq \left(\frac{1}{4} + \frac{\epsilon}{\pi} + 5\epsilon^{10}\right) \mathcal{L}_\chi + (4\epsilon^2 + 80\epsilon^{10}) \mathcal{L}'_\chi \\ &\quad + \delta(\chi) \text{Re}\left\{\frac{1}{s-1}\right\} - \sum_{\rho \in \mathcal{Z}_{r,t}} \text{Re}\left\{\frac{1}{s-\rho}\right\} + O_\epsilon(n_K) \end{aligned} \tag{2-10}$$

and

$$-\text{Re}\left\{\frac{L'}{L}(s, \chi)\right\} \leq \left(\frac{1}{4} + \frac{\epsilon}{\pi} + 5\epsilon^{10}\right) \mathcal{L}_\chi + \delta(\chi) \text{Re}\left\{\frac{1}{s-1}\right\} + O_\epsilon(n_K) \tag{2-11}$$

uniformly in the region  $1 < \sigma \leq 1 + \epsilon$  and  $|t| \leq T$ , where  $\mathcal{L}_\chi = \log D_\chi + n_K \log(T + 3)$  and  $\mathcal{L}'_\chi = \log D_K + \mathcal{L}_\chi$ .

*Proof.* This result is a modified version of [Zaman 2016a, Lemma 4.3] which is motivated by [Heath-Brown 1992, Lemma 3.1]. The main improvements are the valid range of  $\sigma$  and  $t$ . Consequently, we sketch the argument found in [Zaman 2016a] highlighting the necessary modifications. Assume  $\chi$  is nontrivial. Apply [Heath-Brown 1992, Lemma 3.2] with  $f(z) = L(z, \chi)$ ,  $a = s$ , and  $R = 1 - \eta$ , where  $\eta = \eta_{s, \chi} \in (0, \frac{1}{10})$  is chosen sufficiently small so that  $L(w, \chi)$  has no zeros on the circle  $|w - s| = R$ . Then

$$-\operatorname{Re}\left\{\frac{L'}{L}(s, \chi)\right\} = - \sum_{|s-\rho|<R} \operatorname{Re}\left\{\frac{1}{s-\rho} - \frac{s-\rho}{R^2}\right\} - J, \tag{2-12}$$

where

$$J := \int_0^{2\pi} \frac{\cos \theta}{\pi R} \cdot \log |L(s + Re^{i\theta}, \chi)| d\theta.$$

To bound  $J$  from below, write

$$J = \int_0^{\pi/2} + \int_{\pi/2}^{3\pi/2} + \int_{3\pi/2}^{2\pi} = J_1 + J_2 + J_3,$$

say, so we may consider each contribution separately. For  $J_1$ , notice by [Zaman 2016a, Lemma 2.5],

$$\log |L(s + Re^{i\theta}, \chi)| \leq \log \zeta_K(\sigma + R \cos \theta) \ll n_K \log\left(\frac{1}{\sigma - 1 + R \cos \theta}\right).$$

Write  $[0, \frac{\pi}{2}] = [0, \frac{\pi}{2} - (\sigma - 1)] \cup [\frac{\pi}{2} - (\sigma - 1), \frac{\pi}{2}] = I_1 \cup I_2$ , say. Then

$$\begin{aligned} J_1 &= \int_{I_1} + \int_{I_2} \\ &\ll n_K \int_{I_1} \cos \theta \log\left(\frac{1}{\cos \theta}\right) d\theta + n_K \log\left(\frac{1}{\sigma - 1}\right) \int_{I_2} \cos \theta d\theta \ll_\epsilon n_K. \end{aligned}$$

A similar argument holds for  $J_3$  so  $J_1 + J_3 \ll_\epsilon n_K$ . For  $J_2$ , consider  $\theta \in [\frac{\pi}{2}, \frac{3\pi}{2}]$ . As  $1 < \sigma \leq 1 + \epsilon$  and  $R < 1$ , we have  $0 < \sigma + R \cos \theta \leq 1 + \epsilon$ . Hence, by Lemma 2.3,

$$\log |L(s + Re^{i\theta}, \chi)| \leq \frac{1}{2} \mathcal{L}_\chi(-R \cos \theta + \epsilon) + O_\epsilon(n_K).$$

Thus,

$$J_2 \geq \frac{\mathcal{L}_\chi}{2\pi R} \int_{\pi/2}^{3\pi/2} (-R \cos^2 \theta + \epsilon \cos \theta) d\theta + O_\epsilon(n_K),$$

yielding overall

$$J \geq -\left(\frac{1}{4} + \frac{\epsilon}{\pi R}\right) \mathcal{L}_\chi + O_\epsilon(n_K). \tag{2-13}$$

For the sum over zeros in (2-12), observe that the terms are nonnegative, so (2-11) follows immediately from (2-12) and (2-13) after taking  $\eta \rightarrow 0$ , which implies  $R \rightarrow 1$ . To prove (2-10), consider  $0 < r < \epsilon$ . By the same observation, we may restrict our

sum over zeros from  $|s - \rho| < R$  to a smaller circle within it:  $|1 + it - \rho| \leq r$ . As  $r < \epsilon < \frac{1}{4}$  by assumption, we discard the zeros outside this smaller circle. For such zeros  $\rho$  satisfying  $|1 + it - \rho| \leq r$ , notice  $\operatorname{Re}\{s - \rho\} = \sigma - \beta \leq \epsilon + r < 2\epsilon$ . This implies, by Lemma 2.5, that

$$\sum_{|1+it-\rho|\leq r} \operatorname{Re}\left\{\frac{s-\rho}{R^2}\right\} \leq \frac{2\epsilon}{R^2} \cdot \{(2\mathcal{L}'_\chi + 8)r + 8\} \leq \frac{4\epsilon^2}{R^2} \mathcal{L}'_\chi + O(1). \quad (2-14)$$

Thus, (2-10) immediately follows<sup>2</sup> upon combining (2-12), (2-13), and (2-14), and taking  $\eta \rightarrow 0$ , which implies  $R \rightarrow 1$ . This completes the proof for  $\chi$  nontrivial.

For  $\chi = \chi_0$  trivial, similarly proceed with [Heath-Brown 1992, Lemma 3.2] with  $f(z) = ((z - 1)/(z + 1))\zeta_K(z)$  and  $a = z$ , but the choice of  $R$  is different due to the simple pole of the Dedekind zeta function. Observe that the circles  $|w - 1| = \epsilon^{10}$  and  $|w - s| = R$  are disjoint for at least one of the following:

- (i) all  $R \in (1 - \epsilon^{10}, 1)$ , or
- (ii) all  $R \in (1 - 5\epsilon^{10}, 1 - 4\epsilon^{10})$ .

In the case of (i), choose  $R = 1 - \eta$  for  $\eta = \eta_{s,\chi}$  sufficiently small so that  $L(w, \chi)$  has no zeros on the circle  $|w - s| = R$ . Similarly for (ii), take  $R = 1 - 4\epsilon^{10} - \eta$ .

Continuing with the same arguments, the only difference occurs when bounding  $J_1$  and similarly  $J_3$ , in which case one must estimate

$$\int_0^{\pi/2} \frac{\cos \theta}{\pi R} \log \left| \frac{s-1+Re^{i\theta}}{s+1+Re^{i\theta}} \right| d\theta.$$

By our choice of  $R$ , the quantity in the logarithm is  $\asymp_\epsilon 1$ , and hence the above is  $O_\epsilon(1)$ . The remainder of the argument is the same, except at the final step one must take  $R \rightarrow 1$  in case (i) and  $R \rightarrow 1 - 4\epsilon^{10}$  in case (ii). The latter case yields the additional  $\epsilon^{10}$  terms appearing in (2-10).  $\square$

**Lemma 2.7.** *Let  $\chi$  be a Hecke character and  $0 < r < \epsilon < \frac{1}{4}$ . If  $s = \sigma + it$  with  $1 < \sigma < 1 + \epsilon$  and  $N_\chi(r; s)$  by (2-9), then, letting  $\phi = 1 + \frac{4}{\pi}\epsilon + 16\epsilon^2 + 340\epsilon^{10}$ ,*

$$N_\chi(r; s) \leq \phi(2 \log D_K + \log \operatorname{Nf}_\chi + n_K \log(|t| + 3) + O_\epsilon(n_K)) \cdot r + 4 + 4\delta(\chi).$$

*Proof.* This is analogous to Lemma 2.5 except that we bound  $N_\chi(r; 1 + it)$  instead of  $N_\chi(2r; 1 + r + it)$ , and further, we apply Proposition 2.6 in place of Lemmas 2.1 and 2.4.  $\square$

<sup>2</sup>One actually obtains (2-10) without the extra  $\epsilon^{10}$  terms.

**2D. Arithmetic sums.** We estimate various sums over integral ideals of  $K$ , which requires some additional notation. It is well-known that the Dedekind zeta function  $\zeta_K(s)$ , defined by (2-2), has a simple pole at  $s = 1$ . Thus, we may define

$$\kappa_K := \operatorname{Res}_{s=1} \zeta_K(s) \quad \text{and} \quad \gamma_K := \kappa_K^{-1} \lim_{s \rightarrow 1} \left( \zeta_K(s) - \frac{\kappa_K}{s-1} \right) \tag{2-15}$$

so the Laurent expansion of  $\zeta_K(s)$  at  $s = 1$  is given by

$$\zeta_K(s) = \frac{\kappa_K}{s-1} + \kappa_K \gamma_K + O_K(|s-1|).$$

We refer to  $\gamma_K$  as the *Euler–Kronecker constant of  $K$* . (See [Ihara 2006] for details on  $\gamma_K$ .)

**Lemma 2.8.** *For  $x > 0$  and  $0 < \epsilon < \frac{1}{2}$ ,*

$$\left| \sum_{\mathfrak{Nn} < x} \frac{1}{\mathfrak{Nn}} \left( 1 - \frac{\mathfrak{Nn}}{x} \right)^{n_K} - \kappa_K \left( \log x - \sum_{j=1}^{n_K} \frac{1}{j} \right) - \kappa_K \gamma_K \right| \ll_{\epsilon} (n_K^{n_K} D_K)^{1/4+\epsilon} x^{-1/2}.$$

*Proof.* The quantity we wish to bound equals

$$\begin{aligned} \frac{1}{2\pi i} \int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty} \zeta_K(s+1) \frac{x^s}{s} \frac{n_K!}{\prod_{j=1}^{n_K} (s+j)} ds \\ = \frac{n_K!}{2\pi i} \int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty} \zeta_K(s+1) \frac{\Gamma(s)}{\Gamma(n_K+1+s)} x^s ds. \end{aligned}$$

Applying Lemma 2.3, Stirling’s formula, and  $\zeta_{\mathbb{Q}}(1+\epsilon)^{n_K} \ll e^{O_{\epsilon}(n_K)}$ , the result follows. □

**Corollary 2.9.** *Let  $\epsilon > 0$  be arbitrary. If  $x \geq 3(n_K^{n_K} D_K)^{1/2+\epsilon}$ , then*

$$\sum_{\mathfrak{Nn} < x} \frac{1}{\mathfrak{Nn}} \geq \left\{ 1 - \frac{1}{1+2\epsilon} + O_{\epsilon} \left( \frac{1}{\log x} \right) \right\} \cdot \kappa_K \log x.$$

*Proof.* It suffices to assume that  $\kappa_K \geq 1/\log x$ . From Lemma 2.8, it follows that

$$\frac{1}{\kappa_K} \sum_{\mathfrak{Nn} < x} \frac{1}{\mathfrak{Nn}} \geq \log x - \sum_{j=1}^{n_K} \frac{1}{j} + \gamma_K + O_{\epsilon}(x^{-\epsilon/8} \log x),$$

by our assumption on  $x$ . By [Ihara 2006, Proposition 3],

$$\gamma_K \geq -\frac{1}{2} \log D_K + \frac{\gamma_{\mathbb{Q}} + \log 2\pi}{2} \cdot n_K - 1,$$

where  $\gamma_{\mathbb{Q}} = 0.5772\dots$  is Euler’s constant. Since  $\sum_{1 \leq j \leq n_K} j^{-1} \leq \log n_K + 1$ ,

$$\begin{aligned} \frac{1}{\kappa_K} \sum_{Nn < x} \frac{1}{Nn} &\geq (\log x) \{1 + O_{\epsilon}(x^{-\epsilon/8})\} - \frac{1}{2} \log D_K + \frac{\gamma_{\mathbb{Q}} + \log 2\pi}{2} \cdot n_K - \log n_K - 2 \\ &\geq (\log x) \left\{1 - \frac{1}{1+2\epsilon} + O_{\epsilon}((\log x)^{-1})\right\}, \end{aligned}$$

by our assumption on  $x$ . □

Taking the logarithmic derivative of  $\zeta_K(s)$  yields in the usual way

$$-\frac{\zeta'_K(s)}{\zeta_K(s)} = \sum_{n \subseteq \mathcal{O}_K} \frac{\Lambda_K(n)}{(Nn)^s} \tag{2-16}$$

for  $\text{Re}\{s\} > 1$ , where  $\Lambda_K(\cdot)$  is the von Mangoldt  $\Lambda$ -function of the field  $K$  defined by

$$\Lambda_K(n) = \begin{cases} \log Np & \text{if } n \text{ is a power of a prime ideal } p, \\ 0 & \text{otherwise.} \end{cases} \tag{2-17}$$

Using this identity, we prove an elementary lemma.

**Lemma 2.10.** *For  $y \geq 3$  and  $0 < r < 1$ ,*

- (i)  $-\frac{\zeta'_K}{\zeta_K}(1+r) = \sum_n \frac{\Lambda_K(n)}{Nn^{1+r}} \leq \frac{1}{2} \log D_K + \frac{1}{r} + 1$ , and
- (ii)  $\sum_{Nn \leq y} \frac{\Lambda_K(n)}{Nn} \leq e \log(e D_K^{1/2} y)$ .

*Proof.* Part (i) follows from Lemmas 2.1 and 2.4, (2-16), and  $\text{Re}\{(1+r-\rho)^{-1}\} \geq 0$ . Part (ii) follows from (i) by taking  $r = (\log y)^{-1}$ . □

Finally, we end this section with a bound for  $h_H$  in terms of  $n_K$ ,  $D_K$ , and  $Q = Q_H$ , and a comparison between  $Q$  and  $Nf_H$ .

**Lemma 2.11.** *Let  $H$  be a congruence class group of  $K$ . For  $\epsilon > 0$ ,*

$$h_H \leq e^{O_{\epsilon}(n_K)} D_K^{1/2+\epsilon} Q^{1+\epsilon}.$$

*Proof.* Observe, by the definitions of  $Q$  and  $f_H$  in Section 2A, that for a Hecke character  $\chi \pmod{H}$  we have  $f_{\chi} \mid f_H$  and  $Nf_{\chi} \leq Q$ . Hence,

$$h_H = \sum_{\chi \pmod{H}} 1 \leq \sum_{\substack{Nf \leq Q \\ f \mid f_H}} \sum_{\chi \pmod{f}} 1 = \sum_{\substack{Nf \leq Q \\ f \mid f_H}} \#\text{Cl}(f).$$

Recall the classical bound  $\#\text{Cl}(f) \leq 2^{n_K} h_K Nf$ , where  $h_K$  is the (broad) class number of  $K$ . (See [Milne 2013, Theorem 1.7], for example.) Bounding the class number

using Minkowski’s bound (see [Weiss 1983, Lemma 1.12], for example), we deduce that

$$h_H \leq \sum_{\substack{N\mathfrak{f} \leq Q \\ \mathfrak{f} | \mathfrak{f}_H}} e^{O_\epsilon(n_K)} D_K^{1/2+\epsilon} N\mathfrak{f} \leq e^{O_\epsilon(n_K)} D_K^{1/2+\epsilon} Q^{1+\epsilon} \sum_{\mathfrak{f} | \mathfrak{f}_H} \frac{1}{(N\mathfrak{f})^\epsilon}.$$

For the remaining sum, notice  $\sum_{\mathfrak{f} | \mathfrak{f}_H} (N\mathfrak{f})^{-\epsilon} \leq \prod_{\mathfrak{p} | \mathfrak{f}_H} (1 - N\mathfrak{p}^{-\epsilon})^{-1} \leq e^{O(\omega(\mathfrak{f}_H))}$ , where  $\omega(\mathfrak{f}_H)$  is the number of prime ideals  $\mathfrak{p}$  dividing  $\mathfrak{f}_H$ . From [Weiss 1983, Lemma 1.13], we have  $\omega(\mathfrak{f}_H) \ll O_\epsilon(n_K) + \epsilon \log(D_K Q)$ , whence the desired estimate follows after rescaling  $\epsilon$ .  $\square$

**Remark.** Weiss [1983, Lemma 1.16] achieves a comparable bound with  $Q^{1+\epsilon}$  replaced by  $N\mathfrak{f}_H$ . This seemingly minor difference will in fact improve the range of  $T$  in Theorem 3.2.

**Lemma 2.12.** *Let  $H$  be a congruence class group of  $K$ . Then  $Q \leq N\mathfrak{f}_H \leq Q^2$ .*

**Remark.** The lower bound is achieved when  $H = P_{\mathfrak{f}_H}$ . We did not investigate the tightness of the upper bound, as this estimate is sufficient for our purposes.

*Proof.* The arguments here are motivated by [Weiss 1983, Lemma 1.13]. Without loss, we may assume  $H$  is primitive. Since  $Q = Q_H = \max\{N\mathfrak{f}_\chi : \chi \pmod{H}\}$  and  $\mathfrak{f}_H = \text{lcm}\{\mathfrak{f}_\chi : \chi \pmod{H}\}$ , the lower bound is immediate. For the upper bound, we apply arguments similar to [Weiss 1983, Lemma 1.13]. Consider any  $\mathfrak{m} | \mathfrak{f}_H$ . Let  $H_{\mathfrak{m}}$  denote the image of  $H$  under the map  $I(\mathfrak{f}_H)/P_{\mathfrak{f}_H} \rightarrow I(\mathfrak{m})/P_{\mathfrak{m}}$ . This induces a map  $I(\mathfrak{f}_H)/H \rightarrow I(\mathfrak{m})/H_{\mathfrak{m}}$ , which, since  $H$  is primitive, must have nontrivial kernel. Hence, characters of  $I(\mathfrak{m})/H_{\mathfrak{m}}$  induce characters of  $I(\mathfrak{f}_H)/H$ .

Now, for  $\mathfrak{p} | \mathfrak{f}_H$ , choose  $e = e_{\mathfrak{p}} \geq 1$  maximal so that  $\mathfrak{p}^e | \mathfrak{f}_H$ . Define  $\mathfrak{m}_{\mathfrak{p}} := \mathfrak{f}_H \mathfrak{p}^{-1}$  and consider the induced map  $I(\mathfrak{f}_H)/H \rightarrow I(\mathfrak{m}_{\mathfrak{p}})/H_{\mathfrak{m}_{\mathfrak{p}}}$  with kernel  $V_{\mathfrak{p}}$ . Since  $H$  is primitive,  $V_{\mathfrak{p}}$  must be nontrivial and hence  $\#V_{\mathfrak{p}} \geq 2$ . Observe that the characters  $\chi$  of  $I(\mathfrak{f}_H)/H$  such that  $\mathfrak{p}^e \nmid \mathfrak{f}_\chi$  are exactly those which are trivial on  $V_{\mathfrak{p}}$  and hence are  $h_H/\#V_{\mathfrak{p}}$  in number. For a given  $\mathfrak{p}$ , this yields

$$\frac{h_H}{2} \leq h_H \left(1 - \frac{1}{\#V_{\mathfrak{p}}}\right) = \sum_{\substack{\chi \pmod{H} \\ \mathfrak{p}^{e_{\mathfrak{p}}} \nmid \mathfrak{f}_\chi}} 1.$$

Multiplying both sides by  $\log(N\mathfrak{p}^{e_{\mathfrak{p}}})$  and summing over  $\mathfrak{p} | \mathfrak{f}_H$ , we have

$$\begin{aligned} \frac{1}{2} h_H \log N\mathfrak{f}_H &= \frac{h_H}{2} \sum_{\mathfrak{p} | \mathfrak{f}_H} \log(N\mathfrak{p}^{e_{\mathfrak{p}}}) \leq \sum_{\mathfrak{p} | \mathfrak{f}_H} \sum_{\substack{\chi \pmod{H} \\ \mathfrak{p}^{e_{\mathfrak{p}}} \nmid \mathfrak{f}_\chi}} \log N\mathfrak{p}^{e_{\mathfrak{p}}} \\ &\leq \sum_{\chi \pmod{H}} \log N\mathfrak{f}_\chi \leq h_H \log Q. \end{aligned}$$

Comparing both sides, we deduce  $N\mathfrak{f}_H \leq Q^2$  as desired.  $\square$

**Lemma 2.13.** *Let  $H$  be a congruence subgroup of  $K$  and  $\epsilon > 0$  be arbitrary. Then*

$$\sum_{\mathfrak{p} \mid \mathfrak{f}_H} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \leq (2\epsilon)^{-1} n_K + \epsilon \log Q.$$

*Proof.* This follows from [Zaman 2016a, Lemma 2.4] and Lemma 2.12. □

### 3. Proof of Theorem 1.1 and Linnik’s three principles

**3A. Proof of Theorem 1.1.** The primary goal in this paper is to prove the following result, from which Theorem 1.1 follows.

**Theorem 3.1.** *Let  $K$  be a number field, let  $H \pmod{\mathfrak{q}}$  be a congruence class group of  $K$ , and let  $\mathfrak{f}_H$  be the conductor of  $H$ . Let  $I(\mathfrak{q})$  be the group of fractional ideals of  $K$  which are coprime to  $\mathfrak{q}$  and let  $C \in I(\mathfrak{q})/H$  be arbitrary. Let  $\chi \pmod{H}$  be a character of  $I(\mathfrak{q})/H$  of conductor  $\mathfrak{f}_\chi$ . Finally, let  $h_H = [I(\mathfrak{q}) : H]$ ,  $Q = \max\{N_{K/\mathbb{Q}}\mathfrak{f}_\chi : \chi \pmod{H}\}$ , and  $\mathfrak{m}$  be the product of prime ideals dividing  $\mathfrak{q}$  but not  $\mathfrak{f}_H$ . If*

$$x \geq D_K^{694} Q^{521} + D_K^{232} Q^{367} n_K^{290n_K} + (D_K Q n_K^{n_K})^{1/1000} N_{K/\mathbb{Q}} \mathfrak{m}, \tag{3-1}$$

and  $D_K Q [K : \mathbb{Q}]^{[K:\mathbb{Q}]}$  is sufficiently large, then

$$\#\{\mathfrak{p} \in C : \deg(\mathfrak{p}) = 1, N_{K/\mathbb{Q}} \mathfrak{p} \leq x\} \gg (D_K Q n_K^{n_K})^{-5} \frac{x}{h_H \log x}.$$

Assuming Theorem 3.1, we now prove Theorem 1.1.

*Proof of Theorem 1.1.* The proof proceeds exactly as in [Weiss 1983, Theorem 6.1]. Let  $L/F$  be a finite Galois extension of number fields with Galois group  $G$ , and let  $C \subset G$  be a given conjugacy class. Let  $A \subset G$  be an abelian subgroup such that  $A \cap C$  is nonempty, and let  $K = L^A$  be the fixed field of  $A$ . Let  $\mathfrak{f}_{L/K}$  be the conductor of  $L/K$ , and let  $\mathfrak{m}$  be the product of prime ideals  $\mathfrak{P}$  in  $K$  which are unramified in  $L$  but such that the prime  $\mathfrak{p}$  of  $F$  lying under  $\mathfrak{P}$  is ramified in  $L$ . If  $\left[\frac{L/K}{\mathfrak{P}}\right]$  denotes the Artin symbol, then the Artin map  $\mathfrak{P} \mapsto \left[\frac{L/K}{\mathfrak{P}}\right]$  induces a group homomorphism  $I(\mathfrak{m}\mathfrak{f}_{L/K}) \rightarrow A$  because the conjugacy classes in  $A$  are singletons; thus if  $H$  is the kernel of the homomorphism, then the canonical map  $\omega : I(\mathfrak{m}\mathfrak{f}_{L/K})/H \rightarrow A$  is an isomorphism. Moreover,  $H$  is a congruence class group modulo the ideal  $\mathfrak{m}\mathfrak{f}_{L/K}$  of  $K$  with  $\mathfrak{f}_H = \mathfrak{f}_{L/K}$ .

Choose  $\sigma_0 \in C \cap A$ . Using  $\omega$ ,  $\sigma_0$  determines a coset of  $I(\mathfrak{m}\mathfrak{f}_H)/H$ ; thus by Theorem 3.1, if (3-1) holds and  $D_K Q n_K^{n_K}$  is sufficiently large, then

$$\#\left\{N_{K/\mathbb{Q}} \mathfrak{P} \leq x : \deg(\mathfrak{P}) = 1, \left[\frac{L/K}{\mathfrak{P}}\right] = \{\sigma_0\}\right\} \gg (D_K Q n_K^{n_K})^{-5} \frac{x}{h_H \log x}.$$

Let  $\mathfrak{p}$  be a prime ideal of  $F$  lying under  $\mathfrak{P}$ . By the definition of  $\mathfrak{m}$ ,  $\mathfrak{p}$  is unramified in  $L$  and  $N_{K/\mathbb{Q}} \mathfrak{P} = N_{F/\mathbb{Q}} \mathfrak{p}$  because  $\deg(\mathfrak{P}) = 1$ . Furthermore,  $[L/F, \mathfrak{p}] = C$ . Thus

if  $x$  satisfies (3-1),

$$\#\left\{ \mathfrak{p} : \deg(\mathfrak{p}) = 1, \left[ \frac{L/F}{\mathfrak{p}} \right] = C, N_{F/\mathbb{Q}} \mathfrak{p} \leq x \right\} \gg (D_K Q n_K^{n_K})^{-5} \frac{x}{h_H \log x}.$$

As in [Weiss 1983, Theorem 6.1],  $N_{K/\mathbb{Q}} \mathfrak{m} \leq D_K$  and  $h_H = [L : K]$ . By the definition of  $Q$  and the definition of  $H$ , we have that  $Q = \mathcal{Q}$ , so

$$\pi_C(x, L/F) \gg (D_K Q n_K^{n_K})^{-5} \frac{x}{[L : K] \log x} \tag{3-2}$$

whenever  $D_K Q n_K^{n_K}$  is sufficiently large and  $x \geq D_K^{694} Q^{521} + D_K^{232} Q^{367} n_K^{290n_K} + D_K Q n_K^{n_K}$ . Since  $D_K Q n_K^{n_K} \leq D_L n_L^{n_L}$  and there are only finitely many number fields  $L$  with  $D_L n_L^{n_L}$  not sufficiently large, we may enlarge the implied constant in Theorem 1.1 to allow for those exceptions and complete the proof.  $\square$

**3B. The key ingredients.** To outline our proof of Theorem 3.1, we recall the modern approach to proving Linnik’s bound on the least prime in an arithmetic progression. In order to obtain small explicit values of  $c_1$  in (1-2), one typically requires three principles, explicit versions of which are recorded in [Heath-Brown 1992, Section 1]:

- A zero-free region for Dirichlet  $L$ -functions: if  $q$  is sufficiently large, then the product  $\prod_{\chi \pmod{q}} L(s, \chi)$  has at most one zero in the region

$$s = \sigma + it, \quad \sigma \geq 1 - \frac{0.10367}{\log(q(2+|t|))}. \tag{3-3}$$

If such a zero exists, it is real and simple and its associated character is also real.

- A “log-free” zero density estimate: if  $q$  is sufficiently large,  $\epsilon > 0$ , and we define  $N(\sigma, T, \chi) = \#\{\rho = \beta + i\gamma : L(\rho, \chi) = 0, |\gamma| \leq T, \beta \geq \sigma\}$ , then

$$\sum_{\chi \pmod{q}} N(\sigma, T, \chi) \ll_{\epsilon} (qT)^{(12/5+\epsilon)(1-\sigma)}, \quad T \geq 1. \tag{3-4}$$

- The zero repulsion phenomenon: if  $q$  is sufficiently large,  $\lambda > 0$  is sufficiently small,  $\epsilon > 0$ , and the exceptional zero in the region (3-3) exists and equals  $1 - \lambda / \log q$ , then  $\prod_{\chi \pmod{q}} L(s, \chi)$  has no other zeros in the region

$$\sigma \geq 1 - \frac{(\frac{2}{3} - \epsilon)(\log \lambda^{-1})}{\log(q(2+|t|))}. \tag{3-5}$$

If such an exceptional zero exists, then it is real and simple and it corresponds with a nontrivial real character  $\chi$ .

Number field variants of these principles were proved by Fogels [1962a; 1962b], but his proof did not maintain the necessary field uniformity. To prove (1-7), Weiss



developed variants of these principles with effective number field dependence; the effective field dependence is critical for the proof of (1-7). To prove Theorem 3.1, we make Weiss' field-uniform results explicit.

**3C. The zero density estimate.** In Sections 4–6, we prove an explicit version of Weiss' variant of (3-4) for Hecke characters using the power sum method. Assume the notation in the previous section, and define

$$N(\sigma, T, \chi) := \#\{\rho = \beta + i\gamma : L(\rho, \chi) = 0, \sigma < \beta < 1, |\gamma| \leq T\},$$

where the nontrivial zeros  $\rho$  of  $L(s, \chi)$  are counted with multiplicity. Weiss [1983, Corollary 4.4] proved that there exists an absolute constant  $c_6 > 0$  such that if  $\frac{1}{2} \leq \sigma < 1$  and  $T \geq n_K^2 h_H^{1/n_K}$ , then

$$\sum_{\chi \pmod{H}} N(\sigma, T, \chi) \ll (e^{O(n_K)} D_K^2 Q T^{n_K})^{c_6}. \tag{3-6}$$

We prove the following.

**Theorem 3.2.** *Let  $H$  be a congruence class group of a number field  $K$ . If  $\frac{1}{2} \leq \sigma < 1$  and  $T \geq \max\{n_K^{5/6} (D_K^{4/3} Q^{4/9})^{-1/n_K}, 1\}$ , then*

$$\sum_{\chi \pmod{H}} N(\sigma, T, \chi) \ll \{e^{O(n_K)} D_K^2 Q T^{n_K+2}\}^{81(1-\sigma)}. \tag{3-7}$$

If  $1 - 10^{-3} \leq \sigma < 1$ , then one may replace 81 with 73.5.

**Remarks.** • Theorem 3.2 noticeably improves Weiss' density estimate (3-6) in the range of  $T$ . If  $n_K \leq 2(\log D_K) / \log \log D_K$ , then Theorem 3.2 holds for  $T \geq 1$ . Thus we may take  $T \geq 1$  for most choices of  $K$ .

- We see from Minkowski's lower bound for  $D_K$  and the valid range of  $T$  that the  $e^{O(n_K)}$  factor is always negligible, regardless of how  $n_K$  compares to  $(\log D_K) / \log \log D_K$ .

It is instructive to compare the two primary methods for proving log-free zero density estimates. The basic idea behind the proof of (3-4) (the so-called mollifier method) is to construct a Dirichlet polynomial which detects zeros by assuming large values at the zeros of a Dirichlet  $L$ -function. The optimal Dirichlet polynomial for this task looks like a smoothed version of  $\mu(n)$ , where

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n \text{ is squarefree with } r \text{ prime factors,} \\ 0 & \text{otherwise,} \end{cases}$$

is the usual Möbius function. In order to efficiently sum the large values contributed by each of the detected zeros, one relies on the fact that the partial sums of  $\mu(n)$  exhibit significant cancellation. To see why this is true, observe that the prime number theorem (with the error term of Hadamard and de la Vallée Poussin) is

equivalent to the statement that there exists an absolute constant  $c_7 > 0$  such that if  $x$  is sufficiently large, then

$$\sum_{n \leq x} \mu(n) \ll x \exp(-c_7(\log x)^{1/2}). \quad (3-8)$$

The fact that (3-8) is a part of the proofs of the log-free zero density estimates in [Graham 1977; Heath-Brown 1992; Iwaniec and Kowalski 2004; Jutila 1977] may not be immediately obvious. After summing the mollified Dirichlet polynomials over all characters  $\chi \pmod{q}$  and applying duality, one must ultimately minimize the quadratic form

$$S(x) = \sum_{n \leq x} \left( \sum_{d|n} \lambda_d \right)^2$$

subject to the constraint

$$\lambda_d = \begin{cases} \mu(d) \min \left\{ 1, \frac{\log(z_2/d)}{\log(z_2/z_1)} \right\} & \text{if } 1 \leq d \leq z_2, \\ 0 & \text{if } d > z_2, \end{cases}$$

where  $1 < z_1 < z_2$  are given real numbers. (For example, see [Iwaniec and Kowalski 2004, pp. 430–431].) Each of [Graham 1977; Heath-Brown 1992; Iwaniec and Kowalski 2004; Jutila 1977] uses the work of Graham [1978] to estimate  $S(x)$  with this choice of  $\lambda_d$ ; Graham proved that

$$S(x) \leq \frac{x}{\log(z_2/z_1)} \left( 1 + O\left( \frac{1}{\log(z_2/z_1)} \right) \right). \quad (3-9)$$

At several points in the proof, Graham uses the asymptotic prime number theorem in the form (3-8).

For a number field  $K$ , let  $\mu_K(\mathfrak{n})$  be the extension of the Möbius function to the prime ideals of  $K$ . For the sake of simplicity, suppose that the Dedekind zeta function  $\zeta_K(s)$  has no Landau–Siegel zero. The effective form of the prime ideal theorem proven in [Lagarias and Odlyzko 1977] is equivalent to the statement that there exists an absolute constant  $c_8 > 0$  such that if  $\log x \gg n_K(\log D_K)^2$ , then

$$\sum_{N\mathfrak{n} \leq x} \mu_K(\mathfrak{n}) \ll x \exp\left(-c_8 \left( \frac{\log x}{n_K} \right)^{1/2}\right).$$

Therefore, to generalize (3-9) to the Möbius function of  $K$ ,  $x$  needs to be larger than any polynomial in  $D_K$  before the partial sums of  $\mu_K(\mathfrak{n})$  up to  $x$  begin to exhibit cancellation. Thus if one extends the preceding arguments to prove an analogue of (3-4) for the Hecke characters of  $K$ , then the ensuing log-free zero density estimate will not have the  $K$ -uniformity which is necessary to prove Theorem 3.1.

Turán developed an alternative formulation of log-free zero density estimates. The idea is to take high derivatives of  $L'/L(s, \chi)$ . This produces a large sum of complex

numbers involving zeros of  $L(s, \chi)$ , which can be bounded below by the Turán power sum method (see Proposition 5.1). The integral of a certain zero-detecting polynomial (which is not defined in terms of the Möbius function) gives an upper bound for these high derivatives. Thus, when a certain zero-detecting polynomial (which is not defined in terms of the Möbius function) encounters a zero of  $L(s, \chi)$ , its integral will be bounded away from zero because of the lower bound given by the power sum method. The contributions from the detected zeros up to height  $T$  are summed efficiently using a particular large sieve inequality (see Section 4).

The advantage of using the power sum method in our proofs lies in the fact that Turán’s lower bound for power sums is a purely Diophantine result, independent of the number fields in our proofs; this allows for noticeably better field uniformity than the mollifier method. The disadvantage is that the lower bound in the power sum method is quite small, which, for example, would inflate the constant  $\frac{12}{5}$  in (3-4). To our knowledge, the power sum method is the only tool available that produces a  $K$ -uniform log-free zero density estimate of the form (3-4) which is strong enough to deduce a conclusion as strong as Theorem 1.1. Limitations to the power sum method indicate a genuine obstacle to any substantive improvements in the constants in Theorem 1.1 when using these methods.

To prove the large sieve inequality (4-4) used in the proof of Theorem 3.2, we use bounds in Section 2 for certain sums over integral ideals, which require smoothing with a kernel that is  $n_K$  times differentiable. Unfortunately, the smoothing introduces the powers of  $n_K^{n_K}$  (see the comments immediately preceding [Weiss 1983, Section 1]). As mentioned after Theorem 1.1, the factor of  $n_K^{n_K}$  is negligible if  $n_K$  is small compared to  $(\log D_K)/\log \log D_K$ , which is expected to be the case in most applications.

**3D. Zero repulsion.** In Section 7, we prove an explicit variant of the zero repulsion phenomenon for Hecke  $L$ -functions, also known as the Deuring–Heilbronn phenomenon.

**Theorem 3.3.** *Let  $H$  be a congruence class group of  $K$ . Let  $\psi \pmod{H}$  be a real Hecke character and suppose  $L(s, \psi)$  has a real zero  $\beta_1$ . Let  $T \geq 1$  be arbitrary,  $\chi \pmod{H}$  an arbitrary Hecke character, and  $\rho' = \beta' + i\gamma'$  a zero of  $L(s, \chi)$  satisfying  $\frac{1}{2} \leq \beta' < 1$  and  $|\gamma'| \leq T$ . Then, for  $\epsilon > 0$  arbitrary,*

$$\beta' \leq 1 - \frac{\log\left(\frac{c_\epsilon}{(1 - \beta_1) \log(D_K \cdot Q \cdot T^{n_K} e^{O_\epsilon(n_K)})}\right)}{b_1 \log D_K + b_2 \log Q + b_3 n_K \log T + O_\epsilon(n_K)}$$

for some absolute, effective constant  $c_\epsilon > 0$  and

$$(b_1, b_2, b_3) = \begin{cases} (48 + \epsilon, 60 + \epsilon, 24 + \epsilon) & \text{if } \psi \text{ is quadratic,} \\ (24 + \epsilon, 12 + \epsilon, 12 + \epsilon) & \text{if } \psi \text{ is trivial.} \end{cases}$$

**Remark.** Other versions of the zero repulsion phenomenon by Kadiri and Ng [2012] and Zaman [2016a] apply for an asymptotically smaller range of  $\beta'$  and  $|\gamma'| \leq 1$ .

In Section 8, we collect all existing results and our new theorems on the distribution of zeros of Hecke  $L$ -functions and package them into versions required for the proof of Theorem 3.1. The necessary explicit zero-free regions for Hecke  $L$ -functions have already been established in previous work of Zaman [2016a; 2017a], which improved on [Ahn and Kwon 2014; Kadiri 2012], and are valid in a certain neighborhood of  $s = 1$ . In Sections 9–11, we use Theorems 3.2 and 3.3, along with the aforementioned work of Zaman, to prove Theorem 3.1. In Section 12, we prove Theorems 1.2–1.5 using Theorem 1.1.

### 4. Mean values of Dirichlet polynomials

Gallagher [1970] proved the following mean value results for Dirichlet polynomials.

**Theorem.** Let  $\{a_n\}$  be a sequence of complex numbers such that  $\sum_{n \geq 1} n|a_n|^2 < \infty$ .

(1) If  $T \geq 1$ , then

$$\sum_{\chi \pmod{q}} \int_{-T}^T \left| \sum_{n=1}^{\infty} a_n \chi(n) n^{it} \right|^2 dt \ll \sum_{n=1}^{\infty} (qT + n) |a_n|^2. \tag{4-1}$$

(2) Let  $R \geq 2$ , and assume  $a_n = 0$  if  $n$  has any prime factor less than  $R$ . If  $T \geq 1$ , then

$$\sum_{q \leq R} \log \frac{R}{q} \sum_{\chi \pmod{q}}^* \int_{-T}^T \left| \sum_{n=1}^{\infty} a_n \chi(n) n^{it} \right|^2 dt \ll \sum_{n=1}^{\infty} (R^2 T + n) |a_n|^2. \tag{4-2}$$

Here,  $\sum^*$  denotes the restriction to primitive characters  $\chi \pmod{q}$ .

In (4-2), the  $\log(R/q)$  weighting on the left-hand side (which arises from the support of  $a_n$ ) turns out to be decisive in some applications, such as the proof of (1-2). To prove Theorem 3.2, we need a  $K$ -uniform analogue of (4-1) when  $a_n$  is supported as in (4-2). Weiss used the Selberg sieve to prove such a result in his Ph.D. thesis [1980, Theorem 3', p. 98].

**Theorem (Weiss).** Let  $b(\cdot)$  be a complex-valued function on the integral ideals  $\mathfrak{n}$  of  $K$ , and suppose that  $\sum_{\mathfrak{n}} (\mathfrak{N}\mathfrak{n}) |b(\mathfrak{n})|^2 < \infty$ . Let  $T \gg 1$ . Suppose that  $b(\mathfrak{n}) = 0$  when  $\mathfrak{n}$  has a prime ideal factor  $\mathfrak{p}$  with  $\mathfrak{N}\mathfrak{p} \leq z$ , and define  $V(z) = \sum_{\mathfrak{N}\mathfrak{n} \leq z} \mathfrak{N}\mathfrak{n}^{-1}$ . If  $0 < \epsilon < \frac{1}{2}$ , then

$$\begin{aligned} \sum_{\chi(H)=1} \int_{-T}^T \left| \sum_{\mathfrak{n}} b(\mathfrak{n}) \chi(\mathfrak{n}) \mathfrak{N}\mathfrak{n}^{-it} \right|^2 dt \\ \ll \sum_{\mathfrak{n}} |b(\mathfrak{n})|^2 \left( \frac{\kappa_K}{V(z)} \mathfrak{N}\mathfrak{n} + c(\epsilon) (n_K^{\kappa_K} D_K Q T^{\kappa_K} z^4)^{1/2+\epsilon} h_H T \right) \end{aligned}$$

for some constant  $c(\epsilon) > 0$  depending only on  $\epsilon$ .

**Remark.** Assuming the Lindelöf hypothesis for Hecke  $L$ -functions, the upper bound improves to

$$\ll \sum_n |b(n)|^2 \left( \frac{K_K}{V(z)} Nn + c(\epsilon)(D_K Q)^\epsilon h_H T^{1+\epsilon n_K} z^{2+\epsilon} \right).$$

This appears to be optimal when using the Selberg sieve, considering that when  $K = \mathbb{Q}$ , the second term is roughly  $(qTz^2)^{1+\epsilon}$ . For related unconditional results, see [Duke 1989, Section 1].

This result is interesting in its own right, but to make the result more practical for the applications at hand, Weiss chose  $b(n)$  to be supported on the prime ideals  $\mathfrak{p}$  such that  $y < N\mathfrak{p} \leq y^{c_9}$ . Then, Weiss set  $z = y^{1/3}$  and chose  $\log y \geq c_{10} \log(D_K Q T^{n_K})$  and  $\epsilon = \frac{1}{3}$ . By Corollary 2.9 and taking  $c_9$  and  $c_{10}$  to be sufficiently large, Weiss' result reduces to

$$\sum_{\chi(H)=1} \int_{-T}^T \left| \sum_{y < N\mathfrak{p} \leq y^{c_9}} b(\mathfrak{p}) \chi(n) Nn^{-it} \right|^2 dt \ll \frac{1}{\log y} \sum_{y < \mathfrak{p} \leq y^{c_9}} |b(\mathfrak{p})|^2 N\mathfrak{p}.$$

Weiss [1983, Corollary 3.8] recast this estimate with more generality.

**Corollary 4.1** (Weiss). *Let  $b(\cdot)$  be a complex-valued function on the prime ideals  $\mathfrak{p}$  of  $K$  such that  $\sum_{\mathfrak{p}} (N\mathfrak{p}) |b(\mathfrak{p})|^2 < \infty$  and  $b(\mathfrak{p}) = 0$  whenever  $N\mathfrak{p} \leq y$ . Let  $H$  be a primitive congruence class group of  $K$ . If  $y \geq (h_H n_K^{2n_K} D_K Q T^{2n_K})^8$ , then*

$$\sum_{\chi(H)=1} \int_{-T}^T \left| \sum_{\mathfrak{p}} b(\mathfrak{p}) \chi(n) Nn^{-it} \right|^2 dt \ll \frac{1}{\log y} \sum_{\mathfrak{p}} |b(\mathfrak{p})|^2 N\mathfrak{p}.$$

The exponent 8 in the range of  $y$  in Corollary 4.1 is large enough to influence the value of  $c_6$  in (3-6), which affects  $c_3$  and  $c_4$  in (1-7). In this section, we improve Corollary 4.1 so that it does not influence the exponents in Theorem 3.2.

**Theorem 4.2.** *Let  $v \geq \epsilon > 0$  be arbitrary. Let  $b(\cdot)$  be a complex-valued function on the prime ideals  $\mathfrak{p}$  of  $K$  such that  $\sum_{\mathfrak{p}} (N\mathfrak{p}) |b(\mathfrak{p})|^2 < \infty$  and  $b(\mathfrak{p}) = 0$  whenever  $N\mathfrak{p} \leq y$ . Let  $H$  be a primitive congruence class group of  $K$ . If  $T \geq 1$  and*

$$y \geq C_\epsilon \{ h_H n_K^{(5/4+v)n_K} D_K^{3/2+v} Q^{1/2} T^{n_K/2+1} \}^{1+\epsilon} \tag{4-3}$$

for some sufficiently large  $C_\epsilon > 0$ , then

$$\begin{aligned} \sum_{\chi \pmod{H}} \int_{-T}^T \left| \sum_{\mathfrak{p}} b(\mathfrak{p}) \chi(\mathfrak{p}) N\mathfrak{p}^{-it} \right|^2 dt \\ \leq \left( \frac{5\pi \{1 - \frac{1}{1+v}\}^{-1}}{\frac{1}{1+\epsilon} \log(\frac{y}{h_H}) - \mathcal{L}'} + O_\epsilon(y^{-\epsilon/2}) \right) \sum_{\mathfrak{p}} N\mathfrak{p} |b(\mathfrak{p})|^2, \end{aligned} \tag{4-4}$$

where  $\mathcal{L}' = \frac{1}{2} \log D_K + \frac{1}{2} \log Q + \frac{1}{4} n_K \log n_K + (\frac{1}{2} n_K + 1) \log T + O_\epsilon(1)$ .

**Remark.** Taking  $v = \epsilon$  and using Lemma 2.11, we improve the range of  $y$  in Corollary 4.1 to

$$y \gg e^{O_\epsilon(n_K)} \{n_K^{5/4n_K} D_K^2 Q^{3/2} T^{n_K/2+1}\}^{1+\epsilon}.$$

**4A. Preparing for the Selberg sieve.** To apply the Selberg sieve, we require several weighted estimates involving Hecke characters. Before we begin, we highlight the necessary properties of our weight  $\Psi$ .

**Lemma 4.3.** For  $T \geq 1$ , let  $A = T \sqrt{2n_K}$ . Define

$$\widehat{\Psi}(s) = \left[ \frac{\sinh(s/A)}{s/A} \right]^{2n_K}$$

and let

$$\Psi(x) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \widehat{\Psi}(s) x^{-s} ds$$

be the inverse Mellin transform of  $\widehat{\Psi}(s)$ . Then:

- (i)  $0 \leq \Psi(x) \leq A/2$  and  $\Psi(x)$  is a compactly supported function vanishing outside the interval  $e^{-2n_K/A} \leq x \leq e^{2n_K/A}$ .
- (ii)  $\widehat{\Psi}(s)$  is an entire function.
- (iii) For all complex  $s = \sigma + it$ ,  $|\widehat{\Psi}(s)| \leq (A/|s|)^{2n_K} e^{|\sigma|/A}$ .
- (iv) For  $|s| \leq A$ ,  $|\widehat{\Psi}(s)| \leq (1 + |s|^2/(5A^2))^{2n_K}$ .
- (v) Uniformly for  $|\sigma| \leq A/\sqrt{2n_K}$ ,  $|\widehat{\Psi}(s)| \ll 1$ .
- (vi) Let  $\{b_m\}_{m \geq 1}$  be a sequence of complex numbers with  $\sum_m |b_m| < \infty$ . Then

$$\int_{-T}^T \left| \sum_m b_m m^{-it} \right|^2 dt \leq \frac{5\pi}{2} \int_0^\infty \left| \sum_m b_m \Psi\left(\frac{x}{m}\right) \right|^2 \frac{dx}{x}.$$

*Proof.* For (i)–(v), see [Weiss 1983, Lemma 3.2]; in his notation,  $\Psi(x) = H_{2n_K}(x)$  with parameter  $A = T \sqrt{2n_K}$ . Statement (vi) follows easily from the proof of [Weiss 1983, Corollary 3.3]. □

For the remainder of this section, assume:

- $H \pmod{\mathfrak{q}}$  is an arbitrary primitive congruence class group of  $K$ .
- $0 < \epsilon < \frac{1}{2}$  and  $T \geq 1$  is arbitrary.
- $\Psi$  is the weight function of Lemma 4.3.

Next, we establish improved analogues of [Weiss 1983, Lemmas 3.4 and 3.6 and Corollary 3.5].

**Lemma 4.4.** *Let  $\chi \pmod H$  be a Hecke character. For  $x > 0$ ,*

$$\left| \sum_{\mathfrak{n}} \frac{\chi(\mathfrak{n})}{N\mathfrak{n}} \cdot \Psi\left(\frac{x}{N\mathfrak{n}}\right) - \delta(\chi) \frac{\varphi(\mathfrak{q})}{N\mathfrak{q}} \kappa_K \right| \ll_{\epsilon} \{n_K^{n_K/4} D_K^{1/2} Q^{1/2} T^{n_K/2+1}\}^{1+\epsilon}.$$

*Proof.* The quantity we wish to bound equals

$$\frac{1}{2\pi i} \int_{-1-i\infty}^{-1+i\infty} L(s+1, \chi) \widehat{\Psi}(s) x^s ds. \tag{4-5}$$

If  $\chi \pmod{\mathfrak{q}}$  is induced by the primitive character  $\chi^* \pmod{\mathfrak{f}_{\chi}}$ , then

$$L(s, \chi) = L(s, \chi^*) \prod_{\mathfrak{p}|\mathfrak{q}, \mathfrak{p} \nmid \mathfrak{f}_{\chi}} (1 - \chi^*(\mathfrak{p}) N\mathfrak{p}^{-s}).$$

Thus  $|L(it, \chi)| \leq 2^{\omega(\mathfrak{q})} |L(it, \chi^*)|$ , where  $\omega(\mathfrak{q})$  is the number of distinct prime ideal divisors of  $\mathfrak{q}$ . Since  $H \pmod{\mathfrak{q}}$  is primitive,  $\omega(\mathfrak{q}) \leq 6e^{4/\epsilon} n_K + \frac{\epsilon}{2} \log(D_K Q)$  by [Weiss 1983, Lemma 1.13]. So, for  $\text{Re}\{s\} = -1$ ,

$$|L(s+1, \chi)| \ll e^{O_{\epsilon}(n_K)} (D_K Q)^{\epsilon/2} |L(s+1, \chi^*)|.$$

Thus, by Lemma 2.3, (4-5) is

$$\ll e^{O_{\epsilon}(n_K)} (D_K Q)^{1/2+\epsilon} x^{-1} \int_0^{\infty} (1+|t|)^{(1/2+\epsilon)n_K} |\widehat{\Psi}(-1+it)| dt$$

as  $D_{\chi} \leq D_K Q$ . By Lemma 4.3(iii) and (iv), this integral is

$$\ll \int_0^{A/2} (1+|t|)^{(1/2+\epsilon)n_K} |\widehat{\Psi}(-1+it)| dt + \int_{A/2}^{\infty} (1+|t|)^{(1/2+\epsilon)n_K} |\widehat{\Psi}(-1+it)| dt,$$

which is  $\ll e^{O(n_K)} A^{(1/2+\epsilon)n_K+1}$ . Collecting the above estimates, the claimed bound, up to a factor of  $\epsilon$ , follows upon recalling  $A = T\sqrt{2n_K}$  and noting  $e^{O(n_K)} \ll_{\epsilon} (n_K^{n_K})^{\epsilon}$ . □

**Corollary 4.5.** *Let  $C$  be a coset of  $H$ , and let  $\mathfrak{d}$  be an integral ideal coprime to  $\mathfrak{q}$ . For all  $x > 0$ , we have*

$$\left| \sum_{\mathfrak{n} \in C, \mathfrak{d}|\mathfrak{n}} \frac{1}{N\mathfrak{n}} \Psi\left(\frac{x}{N\mathfrak{n}}\right) - \frac{\varphi(\mathfrak{q})}{N\mathfrak{q}} \frac{\kappa_K}{h_H} \cdot \frac{1}{N\mathfrak{d}} \right| \ll_{\epsilon} \{n_K^{n_K/4} D_K^{1/2} Q^{1/2} T^{n_K/2+1}\}^{1+\epsilon} \cdot \frac{1}{x}.$$

*Proof.* The proof is essentially the same as that of [Weiss 1983, Corollary 3.5], except for the fact that we have an improved bound in Lemma 4.4. □

We now apply the Selberg sieve. For  $z \geq 1$ , define

$$S_z = \{\mathfrak{n} : \mathfrak{p} | \mathfrak{n} \Rightarrow N\mathfrak{p} > z\} \quad \text{and} \quad V(z) = \sum_{N\mathfrak{n} \leq z} \frac{1}{N\mathfrak{n}}. \tag{4-6}$$

**Lemma 4.6.** *Let  $C$  be a coset of  $H$ . For  $x > 0$  and  $z \geq 1$ ,*

$$\sum_{\mathfrak{n} \in C \cap S_z} \frac{1}{N\mathfrak{n}} \Psi\left(\frac{x}{N\mathfrak{n}}\right) \leq \frac{\kappa_K}{h_H V(z)} + O_\epsilon\left(\frac{\{n_K^{n_K/4} D_K^{1/2} Q^{1/2} T^{n_K/2+1}\}^{1+\epsilon} z^{2+2\epsilon}}{x}\right).$$

*Proof.* The proof is essentially the same as that of [Weiss 1983, Lemma 3.6], except for the fact that we have an improved bound in Lemma 4.4. □

**4B. Proof of Theorem 4.2.** Let  $z$  be a parameter satisfying  $1 \leq z \leq y$ , which we will specify later. Extend  $b(\mathfrak{n})$  to all integral ideals  $\mathfrak{n}$  of  $K$  by zero. Applying Lemma 4.3 and writing

$$b_m = \sum_{N\mathfrak{n}=m} b(\mathfrak{n})\chi(\mathfrak{n}),$$

for each Hecke character  $\chi \pmod{H}$ , it follows that

$$\begin{aligned} \sum_{\chi \pmod{H}} \int_{-T}^T \left| \sum_{\mathfrak{n}} b(\mathfrak{n})\chi(\mathfrak{n})N\mathfrak{n}^{-it} \right|^2 dt \\ \leq \frac{5\pi}{2} \int_0^\infty \sum_{\chi \pmod{H}} \left| \sum_{\mathfrak{n}} b(\mathfrak{n})\chi(\mathfrak{n})\Psi\left(\frac{x}{N\mathfrak{n}}\right) \right|^2 \frac{dx}{x}. \end{aligned} \tag{4-7}$$

By the orthogonality of characters and the Cauchy–Schwarz inequality,

$$\begin{aligned} \sum_{\chi \pmod{H}} \left| \sum_{\mathfrak{n}} b(\mathfrak{n})\chi(\mathfrak{n})\Psi\left(\frac{x}{N\mathfrak{n}}\right) \right|^2 \\ \leq h_H \sum_{C \in I(\mathfrak{q})/H} \left( \sum_{\mathfrak{n} \in C} N\mathfrak{n}|b(\mathfrak{n})|^2 \Psi\left(\frac{x}{N\mathfrak{n}}\right) \right) \sum_{\mathfrak{n} \in C \cap S_z} \frac{\Psi(x/N\mathfrak{n})}{N\mathfrak{n}} \end{aligned}$$

since  $z \leq y$  and  $b(\mathfrak{n})$  is supported on prime ideals with norm greater than  $y$ . For  $\delta = \delta(\epsilon) > 0$  sufficiently small and  $B_\delta > 0$  sufficiently large, denote

$$M'_\delta = M_\delta z^{2+2\delta} \quad \text{and} \quad M_\delta = B_\delta \{n_K^{n_K/4} D_K^{1/2} Q^{1/2} T^{n_K/2+1}\}^{1+\delta}.$$

By Lemma 4.6, the right-hand side of the preceding inequality is therefore at most

$$\begin{aligned} \sum_{C \in I(\mathfrak{q})/H} \sum_{\mathfrak{n} \in C} N\mathfrak{n}|b(\mathfrak{n})|^2 \Psi\left(\frac{x}{N\mathfrak{n}}\right) \left( \frac{\kappa_K}{V(z)} + \frac{h_H M'_\delta}{x} \right) \\ \leq \sum_{\mathfrak{n}} N\mathfrak{n}|b(\mathfrak{n})|^2 \Psi\left(\frac{x}{N\mathfrak{n}}\right) \left( \frac{\kappa_K}{V(z)} + \frac{h_H M'_\delta}{x} \right), \end{aligned}$$

By Lemma 4.3(v), if we insert the above estimates into (4-7), then we obtain the bound



$$\begin{aligned} & \sum_{\chi \pmod{H}} \int_{-T}^T \left| \sum_{\mathfrak{p}} b(\mathfrak{p}) \chi(\mathfrak{p}) N\mathfrak{p}^{-it} \right|^2 dt \\ & \leq \frac{5\pi}{2} \sum_{\mathfrak{n}} N\mathfrak{n} |b(\mathfrak{n})|^2 \left( \frac{\kappa_K}{V(z)} \int_0^\infty \Psi\left(\frac{x}{N\mathfrak{n}}\right) \frac{dx}{x} + h_H M'_\delta \int_0^\infty \frac{1}{x} \Psi\left(\frac{x}{N\mathfrak{n}}\right) \frac{dx}{x} \right) \\ & \leq \frac{5\pi}{2} \sum_{\mathfrak{n}} N\mathfrak{n} |b(\mathfrak{n})|^2 \left( \frac{\kappa_K}{V(z)} |\widehat{\Psi}(0)| + \frac{h_H M'_\delta}{N\mathfrak{n}} |\widehat{\Psi}(1)| \right). \end{aligned}$$

Since  $b(\mathfrak{n})$  is supported on prime ideals whose norm is greater than  $y$ , the last line of the previous display is

$$\leq \frac{5\pi}{2} \left( \frac{\kappa_K}{V(z)} + O(h_H M_\delta z^{2+2\delta} y^{-1}) \right) \sum_{\mathfrak{p}} N\mathfrak{p} |b(\mathfrak{p})|^2.$$

Now, select  $z$  satisfying

$$z = \left( \frac{y^{(1+\delta)/(1+\epsilon)}}{h_H M_\delta} \right)^{1/(2+2\delta)}, \tag{4-8}$$

so  $1 \leq z \leq y$  and hence

$$\begin{aligned} & \sum_{\chi \pmod{H}} \int_{-T}^T \left| \sum_{\mathfrak{p}} b(\mathfrak{p}) \chi(\mathfrak{p}) N\mathfrak{p}^{-it} \right|^2 dt \\ & \leq \frac{5\pi}{2} \left( \frac{\kappa_K}{V(z)} + O_\epsilon(y^{-\epsilon/2}) \right) \sum_{\mathfrak{p}} N\mathfrak{p} |b(\mathfrak{p})|^2 \tag{4-9} \end{aligned}$$

for  $\delta = \delta(\epsilon) > 0$  sufficiently small. If  $C_\epsilon$  in (4-3) is sufficiently large, then (4-3) and (4-8) imply  $z \geq 3(n_K^{n_K} D_K)^{1/2+\nu/2}$ . Applying Corollary 2.9 to (4-9), it follows that

$$\begin{aligned} & \sum_{\chi \pmod{H}} \int_{-T}^T \left| \sum_{\mathfrak{p}} b(\mathfrak{p}) \chi(\mathfrak{p}) N\mathfrak{p}^{-it} \right|^2 dt \\ & \leq \left( \frac{5\pi \nu}{2\{1+\nu\} \log z + O_\epsilon(1)} + O_\epsilon(y^{-\epsilon/2}) \right) \sum_{\mathfrak{p}} N\mathfrak{p} |b(\mathfrak{p})|^2 \end{aligned}$$

since  $\nu \geq \epsilon > 0$ . Finally, by (4-3) and (4-8),

$$\begin{aligned} 2 \log z & \geq \frac{1}{1+\epsilon} \log\left(\frac{y}{h_H}\right) \\ & \quad - \frac{1}{2} \left\{ \log D_K + \log Q + \frac{1}{2} n_K \log n_K + (n_K + 2) \log T + O_\epsilon(1) \right\}. \end{aligned}$$

Putting this estimate into the previous inequality gives the conclusion. □

**5. Detecting the zeros of Hecke  $L$ -functions**

**5A. Notation.** We first specify some additional notation to be used throughout this section.

*Arbitrary quantities.*

- Let  $H \pmod{q}$  be a primitive congruence class group.
- Let  $\epsilon \in (0, \frac{1}{8})$  and  $\phi = 1 + \frac{4}{\pi}\epsilon + 16\epsilon^2 + 340\epsilon^{10}$ .
- Let  $T \geq 1$ . Define  $Q = Q_H$  and

$$\mathcal{L} = \mathcal{L}_{T,\epsilon} := \log D_K + \frac{1}{2} \log Q + \left(\frac{1}{2}n_K + 1\right) \log(T + 3) + \Theta n_K, \tag{5-1}$$

where  $\Theta = \Theta(\epsilon) \geq 1$  is sufficiently large depending on  $\epsilon$ .

- Let  $\lambda_0 > \frac{1}{20}$ . Suppose  $\tau \in \mathbb{R}$  and  $\lambda > 0$  satisfy

$$\lambda_0 \leq \lambda \leq \frac{1}{16}\mathcal{L} \quad \text{and} \quad |\tau| \leq T. \tag{5-2}$$

Furthermore, let  $r = \frac{\lambda}{\mathcal{L}}$ .

*Fixed quantities.*

- Let  $\alpha, \eta, \omega \in (0, 1)$  be fixed.
- Define  $A \geq 1$ , so that  $A_1 = \sqrt{A^2 + 1}$  satisfies

$$A_1 = 2\left(4e\left(1 + \frac{1}{\alpha}\right)\right)^\alpha (1 + \eta). \tag{5-3}$$

- Let  $x = e^{X\mathcal{L}}$  and  $y = e^{Y\mathcal{L}}$  with  $X, Y > 0$  given by

$$Y = Y_\lambda = \frac{1}{eA_1} \cdot \frac{1}{\alpha} \left\{ 2\phi A + \frac{8}{\lambda} \right\},$$

$$X = X_\lambda = \frac{2 \log\left(\frac{2A_1}{1-\omega}\right)}{(1-\omega)} \cdot \frac{1+\alpha}{\alpha} \left\{ 2\phi A + \frac{8}{\lambda} \right\}, \tag{5-4}$$

and  $\alpha, \eta, \omega$  chosen so that  $2 < Y < X$ . Notice  $X = X_\lambda$  and  $Y = Y_\lambda$  depend on the arbitrary quantities  $\epsilon$  and  $\lambda$ , but they are uniformly bounded above and below in terms of  $\alpha, \eta$ , and  $\omega$ , i.e.,  $X \asymp 1$  and  $Y \asymp 1$ . For this reason, while  $X$  and  $Y$  are technically not fixed quantities, they may be treated as such.

**5B. Statement of results.**

*Detecting zeros.* The first goal of this section is to prove the following proposition.

**Proposition 5.1.** *Let  $\chi \pmod{H}$  be a Hecke character. Suppose  $L(s, \chi)$  has a nontrivial zero  $\rho$  satisfying*

$$|1 + i\tau - \rho| \leq r = \frac{\lambda}{\mathcal{L}}. \tag{5-5}$$

Further assume

$$J(\lambda) := \frac{W_1\lambda + W_2}{A_1(1 + \eta)^{k_0}} < 1, \tag{5-6}$$

where

$$\begin{aligned} X &= X_\lambda, & Y &= Y_\lambda, \\ k_0 &= k_0(\lambda) = \alpha^{-1}(2\phi A\lambda + 8), \\ W_1 &= W_1(\lambda) = 8A_1\left(1 + \frac{1}{k_0}\right) + 2eA_1\left(Y + \frac{1}{2} + \{2X + 1\}e^{-\omega\lambda X}\right) + O(\epsilon), \\ W_2 &= W_2(\lambda) = 2e\omega^{-1}A_1e^{-\omega\lambda X} + 18 + O(\epsilon). \end{aligned}$$

If  $\lambda < \frac{\epsilon}{A_1}\mathcal{L}$  and  $2 < Y < X$ , then

$$\begin{aligned} r^4 \log\left(\frac{x}{y}\right) \int_y^x \left| \sum_{y \leq \mathfrak{N}\mathfrak{p} < u} \frac{\chi(\mathfrak{p}) \log \mathfrak{N}\mathfrak{p}}{\mathfrak{N}\mathfrak{p}^{1+i\tau}} \right|^2 \frac{du}{u} + \delta(\chi) \mathbf{1}_{\{|\tau| < Ar\}}(\tau) \\ \geq \left(\frac{\alpha/(1 + \alpha)}{8e2^{1/\alpha}}\right)^{4\phi A\lambda + 16} \frac{(1 - J(\lambda))^2}{4}. \end{aligned}$$

**Remark.** Note that  $W_j(\lambda) \ll 1$  for  $j = 1, 2$ .

The proof of Proposition 5.1 is divided into two main steps, with the final arguments culminating in Section 5E. The method critically hinges on the following power sum estimate due to Kolesnik and Straus.

**Theorem 5.2** [Kolesnik and Straus 1983]. *For any integer  $M \geq 0$  and complex numbers  $z_1, \dots, z_N$ , there is an integer  $k$  with  $M + 1 \leq k \leq M + N$  such that*

$$|z_1^k + \dots + z_N^k| \geq 1.007 \left(\frac{N}{4e(M + N)}\right)^N |z_1|^k.$$

Makai [1964] showed that the constant  $4e$  is essentially optimal.

*Explicit zero density estimate.* Using Theorem 4.2 and Proposition 5.1, the second and primary goal of this section is to establish an explicit log-free zero density estimate. Recall, for a Hecke character  $\chi$ ,

$$N(\sigma, T, \chi) = \#\{\rho : L(\rho, \chi) = 0, \sigma < \operatorname{Re}\{\rho\} < 1, |\operatorname{Im}(\rho)| \leq T\}, \tag{5-7}$$

where  $\sigma \in (0, 1)$  and  $T \geq 1$ .

**Theorem 5.3.** *Let  $\xi \in (1, \infty)$  and  $\nu \in (0, \frac{1}{10}]$  be fixed and set  $\sigma = 1 - \frac{\lambda}{\xi}$ . Suppose*

$$\begin{aligned} \lambda_0 \leq \lambda < \frac{\epsilon}{\xi A_1}\mathcal{L}, & \quad X > Y > 4.6, \\ \text{and } T \geq \max\{n_K^{5/6} (D_K^{4/3} Q^{4/9})^{-1/n_K}, 1\}, & \tag{5-8} \end{aligned}$$

where  $X = X_{\xi\lambda}$  and  $Y = Y_{\xi\lambda}$ . Then

$$\sum_{\chi \pmod{H}} N(\sigma, T, \chi) \leq \frac{4\xi}{\sqrt{\xi^2 - 1}} \cdot (C_4\lambda^4 + C_3\lambda^3 + C_1\lambda + C_0)e^{B_1\lambda + B_2} \cdot \{1 - J(\xi\lambda)\}^{-2},$$

where  $J(\cdot)$  is defined by (5-6) satisfying  $J(\xi\lambda) < 1$ , and

$$\begin{aligned}
 B_1 &= 4\phi A\xi \log(4e\alpha^{-1}(1+\alpha)2^{(1+\alpha)/\alpha}), \\
 B_2 &= 16 \log(4e\alpha^{-1}(1+\alpha)2^{(1+\alpha)/\alpha}), \\
 C_4 &= \frac{5\pi e\phi X(X-Y)^2(X+Y+1+\epsilon)\xi^4}{(1-\frac{1}{1+\nu})(\frac{1}{1+\epsilon}Y-4)}, \\
 C_3 &= \frac{4}{\phi\xi}C_4, \quad C_1 = 4\phi A\xi, \quad C_0 = 16A + \epsilon.
 \end{aligned}
 \tag{5-9}$$

**Remark.** • In Sections 6 and 8E, we will employ Theorem 5.3 with various choices of parameters  $\alpha, \eta, \nu, \epsilon, \omega$ , and  $\xi$  depending on the range of  $\sigma$ . Consequently, this result is written without any explicit choice of the fixed or arbitrary quantities found in Section 5A.

- The quantities  $C_4$  and  $C_3$  are technically not constants with respect to  $\lambda$  or  $\epsilon$ , but one can see that both are bounded absolutely according to the definitions in Section 5A.

Sections 5C and 5D are dedicated to preparing for the proof of Proposition 5.1 which is contained in Section 5E. The proof of Theorem 5.3 is finalized in Section 5F.

**5C. A large derivative.** Suppose  $\chi \pmod H$  is induced from the primitive character  $\chi^*$ . Define  $F(s) := \frac{L'}{L}(s, \chi^*)$  and  $z := 1 + r + i\tau$ . Using Theorem 5.2, the goal of this subsection is to show  $F(s)$  has a large high-order derivative, which we establish in the following lemma.

**Lemma 5.4.** *Keep the above notation and suppose  $L(s, \chi)$  has a zero  $\rho$  satisfying (5-5). If  $\lambda < \frac{\epsilon}{A_1}\mathcal{L}$  and  $\mathbf{1}_S$  is the indicator function of a set  $S$ , then*

$$\begin{aligned}
 \delta(\chi)\mathbf{1}_{\{|\tau| < Ar\}}(\tau) + \left| \frac{r^{k+1}}{k!} F^{(k)}(z) \right| \\
 \geq \frac{\left(\frac{\alpha}{4e(1+\alpha)}\right)^{2\phi A\lambda+8}}{2^{k+1}} \left\{ 1 - \frac{\{8(1+\frac{1}{k})A_1 + O(\epsilon)\}\lambda + 18}{A_1(1+\eta)^k} \right\}
 \end{aligned}$$

for some integer  $k$  in the range  $\frac{1}{\alpha} \cdot (2\phi A\lambda + 8) \leq k \leq \frac{1+\alpha}{\alpha} \cdot (2\phi A\lambda + 8)$ .

*Proof.* By [Weiss 1983, Lemma 1.10],

$$F(s) + \frac{\delta(\chi)}{s-1} = \sum_{|1+i\tau-\rho| < 1/2} \frac{1}{s-\rho} + G(s)$$

uniformly in the region  $|1+i\tau-s| < \frac{1}{2}$ , where  $G(s)$  is analytic and  $|G(s)| \ll \mathcal{L}$  in this region. Differentiating the above formula  $k$  times and evaluating at  $z = 1 + r + i\tau$ ,

we deduce

$$\frac{(-1)^k}{k!} \cdot F^{(k)}(z) + \frac{\delta(\chi)}{(z-1)^{k+1}} = \sum_{|1+i\tau-\rho| < 1/2} \frac{1}{(z-\rho)^{k+1}} + O(4^k \mathcal{L})$$

since  $r = \frac{\lambda}{\mathcal{L}} < \frac{1}{16}$  by assumption (5-2). The error term arises from bounding  $G^{(k)}(z)$  using Cauchy’s integral formula with a circle of radius  $\frac{1}{4}$ . For zeros  $\rho$  that satisfy  $Ar < |1+i\tau-\rho| < \frac{1}{2}$ , notice

$$(A^2 + 1)r^2 < r^2 + |1+i\tau-\rho|^2 \leq |z-\rho|^2 \leq (r + |1+i\tau-\rho|)^2 \leq (r + \frac{1}{2})^2 < 1.$$

Recalling  $A_1 = \sqrt{A^2 + 1}$ , it follows by partial summation that

$$\begin{aligned} \sum_{Ar < |1+i\tau-\rho| < 1/2} \frac{1}{|z-\rho|^{k+1}} &\leq \int_{A_1 r}^1 u^{-k-1} dN_\chi(u; z) \\ &= (k+1) \int_{A_1 r}^1 \frac{N_\chi(u; z)}{u^{k+2}} du + O(\mathcal{L}), \end{aligned}$$

where we bounded  $N_\chi(1; z) \ll \mathcal{L}$  using [Lagarias et al. 1979, Lemma 2.2]. By Lemma 2.5, the above is therefore

$$\leq (k+1) \int_{A_1 r}^\infty \frac{4u\mathcal{L} + 8}{u^{k+2}} du + O(\mathcal{L}) \leq \frac{4\{1 + \frac{1}{k}\}A_1 r \mathcal{L} + 8}{(A_1 r)^{k+1}} + O(\mathcal{L}).$$

By considering cases, one may bound the  $\delta(\chi)$ -term as follows:

$$r^{k+1} \cdot \left| \frac{\delta(\chi)}{(z-1)^{k+1}} \right| \leq \delta(\chi) \cdot \mathbf{1}_{\{|\tau| < Ar\}}(\tau) + \frac{1}{A_1^{k+1}}. \tag{5-10}$$

The above results now yield

$$\begin{aligned} &\delta(\chi) \mathbf{1}_{\{|\tau| < Ar\}}(\tau) + \left| \frac{r^{k+1} F^{(k)}(z)}{k!} \right| \\ &\geq \left| \sum_{|1+i\tau-\rho| \leq Ar} \frac{r^{k+1}}{(z-\rho)^{k+1}} \right| - \left[ \frac{4\{1 + \frac{1}{k}\}A_1 r \mathcal{L} + 9}{A_1^{k+1}} + O((4r)^{k+1} \mathcal{L}) \right]. \end{aligned} \tag{5-11}$$

To bound the remaining sum over zeros from below, we wish to apply Theorem 5.2.

Let

$$N = N_\chi(Ar; 1+i\tau) = \#\{\rho : L(\rho, \chi) = 0, |1+i\tau-\rho| \leq Ar\}.$$

Since  $\lambda < \frac{\epsilon}{A_1} \mathcal{L} < \frac{\epsilon}{A} \mathcal{L}$  and  $\epsilon < \frac{1}{8}$ , Lemma 2.7 and (5-1) imply that  $N \leq 2\phi A \lambda + 8$ . Define  $M := \lfloor (2\phi A \lambda + 8)/\alpha \rfloor$ . Thus, from Theorem 5.2 and assumption (5-5),

$$\left| \sum_{|1+i\tau-\rho| \leq Ar} \frac{1}{(z-\rho)^{k+1}} \right| \geq \left( \frac{\alpha}{4e(1+\alpha)} \right)^{2\phi A \lambda + 8} \frac{1}{(2r)^{k+1}} \tag{5-12}$$

for some  $M + 1 \leq k \leq M + N$ . To simplify the right-hand side of (5-11), observe that

$$(4r)^{k+1} \mathcal{L} \leq 4\lambda(4r)^k \ll \lambda(4\epsilon)^k A_1^{-k} \ll \epsilon \lambda A_1^{-k}, \tag{5-13}$$

since

$$r = \frac{\lambda}{\mathcal{L}} < \frac{\epsilon}{A_1} < \frac{1}{4A_1}$$

by assumption. Moreover, our choice of  $A_1$  in (5-3) implies

$$\begin{aligned} A_1^{-(k+1)} &= \left(\frac{\alpha}{4e(1+\alpha)}\right)^{\alpha k} \frac{1}{2^k} \cdot \frac{1}{A_1(1+\eta)^k} \\ &\leq \left(\frac{\alpha}{4e(1+\alpha)}\right)^{2\phi A\lambda+8} \frac{1}{2^{k+1}} \cdot \frac{2}{A_1(1+\eta)^k}, \end{aligned} \tag{5-14}$$

since  $\alpha k \geq \alpha(M + 1) \geq 2\phi A\lambda + 8$ . Incorporating (5-12)–(5-14) into (5-11) yields the desired result. The range of  $k$  in Lemma 5.4 is determined by the above choice of  $M$  and  $N$ . □

**5D. Short sum over prime ideals.** Continuing with the discussion and notation of Section 5C, from the Euler product for  $L(s, \chi^*)$ , we have

$$F(s) = \frac{L'}{L}(s, \chi^*) = - \sum_{\mathfrak{n}} \chi^*(\mathfrak{n}) \Lambda_K(\mathfrak{n}) (\mathfrak{N}\mathfrak{n})^{-s}$$

for  $\text{Re}\{s\} > 1$  and where  $\Lambda_K(\cdot)$  is given by (2-17). Differentiating the above formula  $k$  times, we deduce

$$\frac{(-1)^{k+1} r^{k+1}}{k!} \cdot F^{(k)}(z) = \sum_{\mathfrak{n}} \frac{\Lambda_K(\mathfrak{n}) \chi^*(\mathfrak{n})}{\mathfrak{N}\mathfrak{n}^{1+r+i\tau}} \cdot r E_k(r \log \mathfrak{N}\mathfrak{n}) \tag{5-15}$$

for any integer  $k \geq 1$ , where  $z = 1 + r + i\tau$  and  $E_k(u) = u^k/k!$ . From Stirling’s bound (see [DLM 2010]) in the form

$$k^k e^{-k} \sqrt{2\pi k} \leq k! \leq k^k e^{-k} \sqrt{2\pi k} e^{1/12k},$$

one can verify

$$E_k(u) \leq \begin{cases} A_1^{-k} e^u & \text{if } u \leq \frac{k}{eA_1}, \\ A_1^{-k} e^{(1-\omega)u} & \text{if } u \geq \frac{2}{1-\omega} \log\left(\frac{2A_1}{1-\omega}\right)k, \end{cases} \tag{5-16}$$

for any  $k \geq 1$  and  $A_1 > 1, \omega \in (0, 1)$  defined in Section 5A. The goal of this subsection is to bound the infinite sum in (5-15) by an integral average of short sums over prime ideals.

**Lemma 5.5.** *Suppose the integer  $k$  is in the range given in Lemma 5.4. If  $\lambda < \frac{\epsilon}{A_1} \mathcal{L}$  then*

$$\begin{aligned} & \left| \sum_n \frac{\chi^*(n) \Lambda_K(n)}{Nn^{1+r+i\tau}} \cdot r E_k(r \log Nn) \right| \\ & \leq r^2 \int_y^x \left| \sum_{y \leq Np < u} \frac{\chi^*(p) \log Np}{Np^{1+i\tau}} \right| \frac{du}{u} \\ & \quad + \left( e \left[ Y + \frac{1}{2} + \{2X + 1\} e^{-\omega \lambda X} + O(\epsilon) \right] \lambda + \frac{e^{1-\omega \lambda X}}{\omega} \right) A_1^{-k}, \end{aligned}$$

where  $x = e^{X\mathcal{L}}$  and  $y = e^{Y\mathcal{L}}$  with  $X = X_\lambda$  and  $Y = Y_\lambda$  defined by (5-4).

*Proof.* First, divide the sum on the left-hand side into four sums:

$$\sum_n = \sum_{Np < y} + \sum_{y \leq Np < x} + \sum_{Np \geq x} + \sum_{n \text{ not prime}} = S_1 + S_2 + S_3 + S_4.$$

Observe that (5-4) and (5-16), along with the range of  $k$  in Lemma 5.4, imply that

$$E_k(r \log Nn) \leq \begin{cases} A_1^{-k} (Nn)^r & \text{if } Nn \leq y, \\ A_1^{-k} (Nn)^{(1-\omega)r} & \text{if } Nn \geq x. \end{cases} \tag{5-17}$$

Hence, for  $S_1$ , it follows by Lemma 2.10 that

$$\begin{aligned} |S_1| & \leq r A_1^{-k} \sum_{Np < y} \frac{\log Np}{Np} \\ & \leq r A_1^{-k} \cdot e \log(e D_K^{1/2} y) \leq e \left( \lambda Y + \frac{\lambda}{2} + \epsilon \right) A_1^{-k}, \end{aligned}$$

since  $r = \frac{\lambda}{\mathcal{L}} < \epsilon$ ,  $\log D_K \leq \mathcal{L}$ , and  $y = e^{Y\mathcal{L}}$ . Similarly, for  $S_3$ , apply partial summation using Lemma 2.10 to deduce

$$\begin{aligned} |S_3| & \leq r A_1^{-k} \sum_{Np \geq x} \frac{\log Np}{(Np)^{1+\omega r}} \\ & \leq r A_1^{-k} \int_x^\infty \frac{\omega r e \log(e D_K^{1/2} t)}{t^{1+\omega r}} dt \leq \left( \left\{ X + \frac{1}{2} \right\} \lambda + \omega^{-1} + \epsilon \right) \frac{e^{1-\omega \lambda X}}{A_1^k}. \end{aligned}$$

For  $S_4$ , since  $\frac{u^k}{k!} \leq e^u$  for  $u > 0$ , observe

$$E_k(r \log Nn) = \frac{1}{k!} (2r)^k \left( \frac{1}{2} \log Nn \right)^k \leq (2r)^k (Nn)^{1/2}.$$

Thus, by Lemma 2.10,

$$\begin{aligned} |S_4| &\leq r \sum_{\mathfrak{p}} \sum_{m \geq 2} \frac{\log N\mathfrak{p}}{(N\mathfrak{p}^m)^{1+r}} E_k(r \log N\mathfrak{p}^m) \\ &\leq (2r)^k r \sum_{\mathfrak{p}} \sum_{m \geq 2} \frac{\log N\mathfrak{p}}{(N\mathfrak{p}^m)^{1/2+r}} \\ &\ll (2r)^k r \sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{1+2r}} \ll \lambda \epsilon A_1^{-k}, \end{aligned}$$

since  $\log D_K \leq \mathcal{L}$  and  $\mathcal{L}^{-1} \ll r = \frac{\lambda}{\mathcal{L}} < \frac{\epsilon}{A_1}$ . Also note that  $\epsilon \in (0, \frac{1}{8})$  implies  $(2\epsilon)^k \ll \epsilon$ . Finally, for the main term  $S_2$ , define

$$W(u) = W_\chi(u; \tau) := \sum_{y \leq N\mathfrak{p} < u} \frac{\chi(\mathfrak{p}) \log N\mathfrak{p}}{N\mathfrak{p}^{1+i\tau}},$$

so by partial summation,

$$S_2 = rW(x)x^{-r} E_k(r \log x) - r^2 \int_y^x W(u) \frac{d}{dt} [e^{-t} E_k(t)] \Big|_{t=r \log u} \frac{du}{u} \quad (5-18)$$

as  $W(y) = 0$ . Similar to  $S_1$ ,  $S_3$ , and  $S_4$ , from (5-17) and Lemma 2.10 it follows

$$\begin{aligned} |rW(x)x^{-r} E_k(r \log x)| &\leq rA_1^{-k} x^{-\omega r} \sum_{y \leq N\mathfrak{p} < x} \frac{\Lambda_K(\mathfrak{n})}{N\mathfrak{n}} \\ &\leq e\left(\left\{X + \frac{1}{2}\right\}\lambda + \epsilon\right) e^{-\omega\lambda X} A_1^{-k}. \end{aligned}$$

Observe

$$\left| \frac{d}{dt} (e^{-t} E_k(t)) \right| = |e^{-t} E_{k-1}(t) - e^{-t} E_k(t)| \leq e^{-t} [E_{k-1}(t) + E_k(t)] \leq 1$$

from the definition of  $E_k(t)$  and since  $\sum_{k=0}^\infty E_k(t) = e^t$ . Hence,

$$|S_2| \leq r^2 \int_y^x |W(u)| \frac{du}{u} + e\left(\left\{X + \frac{1}{2}\right\}\lambda + \epsilon\right) e^{-\omega\lambda X} A_1^{-k}.$$

Collecting all of our estimates, we conclude the desired result as  $\lambda \geq \lambda_0 \gg 1$ .  $\square$

**5E. Proof of Proposition 5.1.** If  $\delta(\chi)\mathbf{1}_{\{\tau < Ar\}}(\tau) = 1$ , then the inequality in Proposition 5.1 holds trivially, as the right-hand side is certainly less than 1. Thus, we may assume otherwise.

Combining Lemmas 5.4 and 5.5 via (5-15), it follows that

$$r^2 \int_y^x \left| \sum_{y \leq N\mathfrak{p} < u} \frac{\chi^*(\mathfrak{p}) \log N\mathfrak{p}}{N\mathfrak{p}^{1+i\tau}} \right| \frac{du}{u} \geq \left( \frac{\alpha}{4e(1+\alpha)} \right)^{2\phi A\lambda+8} \cdot \frac{1}{2^{k+1}} \{1 - J(\lambda)\}, \quad (5-19)$$



after bounding  $A_1^{-k}$  as in (5-14) and noting  $k \geq k_0$  in the range of Lemma 5.4. By assumption,  $J(\lambda) < 1$  and hence the right-hand side of (5-19) is positive. Therefore, squaring both sides and applying Cauchy–Schwarz to the left-hand side gives

$$r^4 \log\left(\frac{x}{y}\right) \int_y^x \left| \sum_{y \leq \mathfrak{N}\mathfrak{p} < u} \frac{\chi^*(\mathfrak{p}) \log \mathfrak{N}\mathfrak{p}}{\mathfrak{N}\mathfrak{p}^{1+i\tau}} \right|^2 \frac{du}{u} \geq \left(\frac{\alpha}{4e(1+\alpha)}\right)^{4\phi A\lambda+16} \cdot \frac{1}{2^{2k+2}} \{1 - J(\lambda)\}^2.$$

By assumption,  $y = e^{Y\mathcal{L}} > e^{2\mathcal{L}} \geq \mathfrak{N}\mathfrak{f}_\chi$ , so it follows that  $\chi^*(\mathfrak{p}) = \chi(\mathfrak{p})$  for  $y \leq \mathfrak{N}\mathfrak{p} < x$ . So we may replace  $\chi^*$  with  $\chi$  in the above sum over prime ideals. Finally, we note  $k \leq \frac{1+\alpha}{\alpha}(2\phi A\lambda + 8)$  since  $k$  is in the range of Lemma 5.4, yielding the desired result.  $\square$

**5F. Proof of Theorem 5.3.** For  $\chi \pmod{H}$ , consider zeros  $\rho = \beta + i\gamma$  of  $L(s, \chi)$  such that

$$1 - \frac{\lambda}{\mathcal{L}} \leq \beta < 1, \quad |\gamma| \leq T. \tag{5-20}$$

Let  $\lambda^* = \xi\lambda$  and  $r^* = \frac{\lambda^*}{\mathcal{L}} = \xi(1 - \sigma)$ , so by (5-8) we have  $r^* < \frac{\epsilon}{A_1}$ . For any zero  $\rho = \beta + i\gamma$  of  $L(s, \chi)$ , define  $\Phi_{\rho, \chi}(\tau) := \mathbf{1}_{\{|1+i\tau-\rho| \leq r^*\}}(\tau)$ . If  $\rho$  satisfies (5-20) then one can verify by elementary arguments that

$$\frac{1}{r^*} \int_{-T}^T \Phi_{\rho, \chi}(\tau) d\tau \geq \frac{\sqrt{\xi^2 - 1}}{\xi}.$$

Applying Proposition 5.1 to such zeros  $\rho$ , it follows that

$$\begin{aligned} & \int_{-T}^T \frac{1}{r^*} \Phi_{\rho, \chi}(\tau) \\ & \times \left[ (r^*)^4 \log\left(\frac{x}{y}\right) \int_y^x \left| \sum_{y \leq \mathfrak{N}\mathfrak{p} < u} \frac{\chi(\mathfrak{p}) \log \mathfrak{N}\mathfrak{p}}{\mathfrak{N}\mathfrak{p}^{1+i\tau}} \right|^2 \frac{du}{u} + \delta(\chi) \mathbf{1}_{\{|\tau| < Ar^*\}}(\tau) \right] d\tau \\ & \geq \frac{\sqrt{\xi^2 - 1}}{4\xi} \left(\frac{\alpha}{4e(1+\alpha)2^{(1+\alpha)/\alpha}}\right)^{2\phi A\xi\lambda+16} \{1 - J(\xi\lambda)\} =: w(\lambda). \end{aligned}$$

Note  $x = e^{X\mathcal{L}}$  and  $y = e^{Y\mathcal{L}}$ , where  $X = X_{\lambda^*}$  and  $Y = Y_{\lambda^*}$ . Summing over all zeros  $\rho$  of  $L(s, \chi)$  satisfying (5-20), we have that

$$\begin{aligned} & w(\lambda)N(\sigma, T, \chi) \\ & \leq (X - Y)(2\phi r^* \mathcal{L} + 8)(r^*)^3 \mathcal{L} \int_y^x \left( \int_{-T}^T \left| \sum_{y \leq \mathfrak{N}\mathfrak{p} < u} \frac{\chi(\mathfrak{p}) \log \mathfrak{N}\mathfrak{p}}{\mathfrak{N}\mathfrak{p}^{1+i\tau}} \right|^2 d\tau \right) \frac{du}{u} \\ & \quad + \delta(\chi)(4\phi Ar^* \mathcal{L} + 16A) \tag{5-21} \end{aligned}$$

since, for  $|\tau| \leq T$  and  $r^* < \epsilon$ ,

$$\sum_{\rho: L(\rho, \chi)=0} \Phi_{\rho, \chi}(\tau) = N_{\chi}(r^*; 1 + i\tau) \leq 2\phi r^* \mathcal{L} + 8$$

by Lemma 2.7. From the conditions on  $Y$  and  $T$  in (5-8) and the definition of  $\mathcal{L}$  in (5-1), observe that, for  $\nu = \nu(\epsilon) > 0$  sufficiently small, Lemma 2.11 implies

$$y = e^{Y\mathcal{L}} \geq C_{\nu} \{h_H n_K^{(5/4+2\nu)n_K} D_K^{3/2+2\nu} Q^{1/2 T^{n_K/2+1}}\}^{1+\nu}$$

since  $\nu \leq \frac{1}{10}$  and  $\Theta = \Theta(\epsilon) \geq 1$  is sufficiently large. Therefore, we may sum (5-21) over  $\chi \pmod{H}$  and apply Theorem 4.2 with  $b(\mathfrak{p}) = (\log N\mathfrak{p})/N\mathfrak{p}$  for  $y \leq N\mathfrak{p} < u$  to deduce

$$\begin{aligned} w(\lambda) & \sum_{\chi \pmod{H}} N(\sigma, T, \chi) \\ & \leq \left( C'(2\phi r^* \mathcal{L} + 8)(r^*)^3 + O_{\epsilon} \left( \frac{(r^*)^4 \mathcal{L}^2}{e^{\epsilon Y \mathcal{L}/2}} \right) \right) \int_y^x \sum_{y \leq N\mathfrak{p} < u} \frac{(\log N\mathfrak{p})^2}{N\mathfrak{p}} \frac{du}{u} \\ & \qquad \qquad \qquad + 4A\phi r^* \mathcal{L} + 16A, \end{aligned} \tag{5-22}$$

where

$$C' = 5\pi(X - Y) \left(1 - \frac{1}{1+\nu}\right)^{-1} \left(\frac{1}{1+\epsilon} Y - 4\right)^{-1}.$$

To calculate  $C'$ , we replaced  $\mathcal{L}'$  (as found in Theorem 4.2) by observing from Lemma 2.11 that  $\mathcal{L}' + \frac{1}{1+\epsilon} \log h_H \leq 4\mathcal{L}$  (since  $T \geq \max\{n_K^{5/6} (D_K^{4/3} Q^{4/9})^{-1/n_K}, 1\}$  and  $\Theta = \Theta(\epsilon)$  is sufficiently large). For the remaining integral in (5-22), notice by Lemma 2.10 that

$$\begin{aligned} \int_y^x \sum_{y \leq N\mathfrak{p} < u} \frac{(\log N\mathfrak{p})^2}{N\mathfrak{p}} \frac{du}{u} & \leq \log x \int_y^x e \log(e D_K^{1/2} u) \frac{du}{u} \\ & \leq \frac{e}{2} X(X - Y) \left(X + Y + 1 + \frac{2}{\mathcal{L}}\right) \mathcal{L}^3. \end{aligned}$$

Substituting this estimate in (5-22) and recalling  $r^* = \frac{\lambda^*}{\mathcal{L}} = \frac{\xi \lambda}{\mathcal{L}}$ , we have shown

$$\begin{aligned} w(\lambda) & \sum_{\chi \pmod{H}} N(\sigma, T, \chi) \\ & \leq 2\phi C'' \xi^4 \cdot \lambda^4 + 8C'' \xi^3 \cdot \lambda^3 + 4\phi A \xi \cdot \lambda + 16A + O_{\epsilon}(\lambda^3 \mathcal{L} e^{-\epsilon \mathcal{L}}), \end{aligned}$$

where

$$C'' = \frac{e}{2} X(X - Y) \left(X + Y + 1 + \frac{2}{\mathcal{L}}\right) C'.$$

Since  $\mathcal{L} \geq \Theta$  and  $\Theta$  is sufficiently large depending on  $\epsilon$ , the big-O error term above and the quantity  $\frac{2}{\mathcal{L}}$  in  $C''$  may both be bounded by  $\epsilon$ . This completes the proof of Theorem 5.3. □

### 6. Log-free zero density estimate

Having established Theorem 5.3, in this section we prove Theorem 3.2.

**Proof of Theorem 3.2:** Without loss, we may assume  $H \pmod{q}$  is primitive because  $Q = Q_H = Q_{H'}, h_H = h_{H'}$  and

$$\sum_{\chi \pmod{H}} N(\sigma, T, \chi) = \sum_{\chi \pmod{H'}} N(\sigma, T, \chi)$$

if  $H'$  induces  $H$ . Suppose  $\frac{1}{2} \leq \sigma \leq 1 - \frac{0.05}{4}$ . By a naive application of [Lagarias et al. 1979, Lemma 2.1], one can verify that for  $T \geq 1$ ,

$$\begin{aligned} \sum_{\chi \pmod{H}} N(\sigma, T, \chi) &\ll h_H T \log(D_K Q T^{n_K}) \\ &\ll (e^{O(n_K)} D_K^2 Q T^{n_K+2})^{81(1-\sigma)} \end{aligned} \tag{6-1}$$

after bounding  $h_H$  with Lemma 2.11.

Now, let  $\epsilon \in (0, \frac{1}{8})$  be fixed and define  $\mathcal{L}$  as in (5-1). Suppose  $1 - \frac{\epsilon}{4} < \sigma < 1$ . Let  $R \geq 1$  be fixed and sufficiently large. By applying the bound in Lemma 2.11 to [Weiss 1983, Theorem 4.3], we deduce that for  $T \geq 1$ ,

$$\sum_{\chi \pmod{H}} N\left(1 - \frac{R}{\mathcal{L}}, T, \chi\right) \ll 1, \tag{6-2}$$

so it suffices to bound  $\sum_{\chi(H)=1} N(\sigma, T, \chi)$  in the range

$$1 - \frac{\epsilon}{4} < \sigma < 1 - \frac{R}{\mathcal{L}}, \tag{6-3}$$

or equivalently, if  $\sigma = 1 - \frac{\lambda}{\mathcal{L}}$ , in the range

$$R < \lambda < \frac{\epsilon}{4} \mathcal{L}.$$

According to Theorem 5.3 and the notation defined in Section 5A, select

$$\xi = 1 + 10^{-5}, \quad v = 10^{-5}, \quad \eta = 10^{-5}, \quad \omega = 10^{-5}, \quad \text{and} \quad \alpha = 0.15.$$

It follows that the constants  $B_2, C_0, C_1, C_3, C_4$  in Theorem 5.3 are bounded absolutely,

$$X > Y > 4.6, \quad B_1 \leq 146.15\phi, \quad \text{and} \quad \xi A_1 < 4,$$

where  $\phi = 1 + \frac{4}{\pi}\epsilon + 16\epsilon^2 + 340\epsilon^{10}$ . Moreover, since  $\lambda > R$ ,

$$J(\xi\lambda) \ll \frac{\lambda}{(1+10^{-5})^\lambda} \ll \frac{R}{(1+10^{-5})^R},$$

and therefore  $J(\xi\lambda) < \frac{1}{2}$  for  $R$  sufficiently large. Thus, by Theorem 5.3,

$$\sum_{\chi \pmod{H}} N(\sigma, T, \chi) \ll \lambda^4 e^{146.15\phi\lambda} \ll e^{146.2\phi\lambda} = e^{146.2\phi(1-\sigma)\mathcal{L}} \tag{6-4}$$

for  $\sigma$  satisfying (6-3) and  $T \geq \max\{n_K^{5/6} D_K^{-4/3n_K} Q^{-4/9n_K}, 1\}$ . To complete the proof of Theorem 3.2, it remains to choose  $\epsilon$  in (6-4). If  $\epsilon = 0.05$  then  $146.2\phi < 162 = 2 \cdot 81$ , yielding the desired result when combined with (6-1). If  $\epsilon = 10^{-3}$  then  $146.2\phi < 147 = 2 \cdot 73.5$  as claimed.  $\square$

### 7. Zero repulsion: the Deuring–Heilbronn phenomenon

In this section, we prove Theorem 3.3 and establish the Deuring–Heilbronn phenomenon for  $L$ -functions of Hecke characters  $\chi \pmod{H}$  where  $H \pmod{\mathfrak{q}}$  is a (not necessarily primitive) congruence class group. We will critically use the following power sum inequality.

**Theorem 7.1** (Lagarias–Montgomery–Odlyzko). *Let  $\epsilon > 0$  and a sequence of complex numbers  $\{z_n\}_n$  be given. Suppose that  $|z_n| \leq |z_1|$  for all  $n \geq 1$ . Define  $M := \frac{1}{|z_1|} \sum_n |z_n|$ . Then there exists  $m_0$  with  $1 \leq m_0 \leq (12 + \epsilon)M$  such that*

$$\operatorname{Re} \left\{ \sum_{n=1}^{\infty} z_n^{m_0} \right\} \geq \frac{\epsilon}{48 + 5\epsilon} |z_1|^{m_0}.$$

*Proof.* This is a modified version of [Lagarias et al. 1979, Theorem 4.2]; see [Zaman 2017b, Theorem 2.3] for details.  $\square$

We prepare for the application of this result by establishing a few preliminary estimates and then end this section with the proof of Theorem 3.3.

#### 7A. Preliminaries.

**Lemma 7.2.** *Let  $\chi \pmod{\mathfrak{q}}$  be a Hecke character. For  $\sigma \geq 2$  and  $t \in \mathbb{R}$ ,*

$$-\operatorname{Re} \left\{ \frac{L'}{L}(\sigma + it, \chi) \right\} \leq -\operatorname{Re} \left\{ \frac{L'}{L}(\sigma + it, \chi^*) \right\} + \frac{1}{2^{\sigma-1}} (n_K + \log N\mathfrak{q}),$$

where  $\chi^*$  is the primitive character inducing  $\chi$ .

*Proof.* By definition,

$$L(s, \chi) = P(s, \chi) L(s, \chi^*), \quad \text{where } P(s, \chi) = \prod_{\mathfrak{p}|\mathfrak{q}, \mathfrak{p} \nmid \mathfrak{f}_\chi} \left( 1 - \frac{\chi^*(\mathfrak{p})}{N\mathfrak{p}^s} \right),$$

so it suffices to show  $\left| \frac{P'}{P}(s, \chi) \right| \leq \frac{1}{2^{\sigma-1}}(n_K + \log Nq)$ . Observe, by elementary arguments,

$$\begin{aligned} \left| \frac{P'}{P}(s, \chi) \right| &= \left| \sum_{p|q, p \nmid f_\chi} \sum_{k=1}^{\infty} \frac{\chi^*(p^k) \log Np^k}{k(Np^k)^s} \right| \\ &\leq \sum_{p|q} \frac{\log Np}{Np^\sigma - 1} \leq \frac{1}{1 - 2^{-\sigma}} \cdot \frac{1}{2^{\sigma-1}} \sum_{p|q} \frac{\log Np}{Np}. \end{aligned}$$

From [Zaman 2016a, Lemma 2.4],

$$\sum_{p|q} \frac{\log Np}{Np} \leq \sqrt{n_K \log Nq} \leq \frac{n_K}{2} + \frac{\log Nq}{2}.$$

Combining this fact with the previous inequality gives the desired estimate.  $\square$

**Lemma 7.3.** *Let  $\chi \pmod{q}$  be a Hecke character. For  $\sigma > 1$  and  $t \in \mathbb{R}$ ,*

$$\sum_{\omega \text{ trivial}} \frac{1}{|\sigma + it - \omega|^2} \leq \begin{cases} \left(\frac{1}{2\sigma} + \frac{1}{\sigma^2}\right) \cdot n_K & \text{if } \chi \text{ is primitive,} \\ \left(\frac{1}{2\sigma} + \frac{1}{\sigma^2}\right) \cdot n_K \\ \quad + \left(\frac{1}{2\sigma} + \frac{2}{\sigma^2 \log 2}\right) \cdot \log Nq & \text{unconditionally,} \end{cases}$$

where the sum is over all trivial zeros  $\omega$  of  $L(s, \chi)$  counted with multiplicity.

*Proof.* Suppose  $\chi \pmod{q}$  is induced by the primitive character  $\chi^* \pmod{f_\chi}$ . Then

$$L(s, \chi) = P(s, \chi)L(s, \chi^*), \quad \text{where } P(s, \chi) = \prod_{p|q, p \nmid f_\chi} \left(1 - \frac{\chi^*(p)}{Np^s}\right),$$

for all  $s \in \mathbb{C}$ . Thus, the trivial zeros of  $L(s, \chi)$  are either zeros of the finite Euler product  $P(s, \chi)$  or trivial zeros of  $L(s, \chi^*)$ . We consider each separately. From (2-7) and (2-5), observe

$$\begin{aligned} \sum_{\substack{\omega \text{ trivial} \\ L(\omega, \chi^*)=0}} \frac{1}{|\sigma + it - \omega|^2} &\leq a(\chi) \sum_{k=0}^{\infty} \frac{1}{(\sigma + 2k)^2 + t^2} + b(\chi) \sum_{k=0}^{\infty} \frac{1}{(\sigma + 2k + 1)^2 + t^2} \\ &\leq n_K \sum_{k=0}^{\infty} \frac{1}{(\sigma + 2k)^2} \leq \left(\frac{1}{2\sigma} + \frac{1}{\sigma^2}\right)n_K. \end{aligned}$$

Now, if  $\chi$  is primitive then  $P(s, \chi) \equiv 1$  and hence never vanishes. Otherwise, notice the zeros of each  $p$ -factor in the Euler product of  $P(s, \chi)$  are totally imaginary and are given by  $a_\chi(p)i + 2\pi i\mathbb{Z}/\log Np$  for some  $0 \leq a_\chi(p) < 2\pi/\log Np$ . Translating

these zeros  $\omega \mapsto \omega + it$  amounts to choosing another representative  $0 \leq b_\chi(\mathfrak{p}; t) < 2\pi / \log N\mathfrak{p}$ . Therefore,

$$\begin{aligned} \sum_{\substack{\omega \text{ trivial} \\ P(\omega, \chi)=0}} \frac{1}{|\sigma + it - \omega|^2} &\leq 2 \sum_{\mathfrak{p}|\mathfrak{q}, \mathfrak{p} \nmid \mathfrak{f}_\chi} \sum_{k=0}^{\infty} \frac{1}{\sigma^2 + (2\pi k / \log N\mathfrak{p})^2} \\ &\leq \left( \frac{1}{2\sigma} + \frac{2}{\sigma^2 \log 2} \right) \log N\mathfrak{q}, \end{aligned}$$

as required. □

**Lemma 7.4.** *Let  $H \pmod{\mathfrak{q}}$  be a congruence class group of  $K$ . Suppose  $\psi \pmod{H}$  is real and  $\chi \pmod{H}$  is arbitrary. For  $\sigma = \alpha + 1$  with  $\alpha \geq 1$  and  $t \in \mathbb{R}$ ,*

$$\begin{aligned} \sum_{\xi_K(\rho)=0} \frac{1}{|\sigma - \rho|^2} + \sum_{L(\rho, \psi)=0} \frac{1}{|\sigma - \rho|^2} + \sum_{L(\rho, \chi)=0} \frac{1}{|\sigma + it - \rho|^2} + \sum_{L(\rho, \psi\chi)=0} \frac{1}{|\sigma + it - \rho|^2} \\ \leq \frac{1}{\alpha} \cdot \left[ \frac{1}{2} \log(D_K^3 Q^2 D_\psi) + \left( \log(\alpha + 2) + \frac{2}{\alpha + 1} + \frac{1}{2^{\alpha+1} - 1} - 2 \log \pi \right) n_K \right. \\ \left. + n_K \log(\alpha + 2 + |t|) + \frac{2}{2^{\alpha+1} - 1} \log Q + \frac{4}{\alpha} + \frac{4}{\alpha + 1} \right], \end{aligned}$$

where the sums are over all nontrivial zeros of the corresponding  $L$ -functions.

**Remark.** If  $\psi$  is trivial, notice that the left-hand side equals

$$2 \left( \sum_{\xi_K(\rho)=0} \frac{1}{|\sigma - \rho|^2} + \sum_{L(\rho, \chi)=0} \frac{1}{|\sigma + it - \rho|^2} \right).$$

This additional factor of 2 will be useful to us later.

*Proof.* Suppose  $\psi$  and  $\chi$  are induced from the primitive characters  $\psi^*$  and  $\chi^*$ , respectively. From the identity  $0 \leq (1 + \psi^*(n))(1 + \operatorname{Re}\{\chi^*(n)(Nn)^{-it}\})$ , it follows that

$$0 \leq -\operatorname{Re} \left\{ \frac{\xi'_K}{\xi_K}(\sigma) + \frac{L'}{L}(\sigma, \psi^*) + \frac{L'}{L}(\sigma + it, \chi^*) + \frac{L'}{L}(\sigma + it, \psi^* \chi^*) \right\}. \tag{7-1}$$

The first three  $L$ -functions are primitive, but  $\xi := \psi^* \chi^*$  is a character modulo  $[\mathfrak{f}_\chi, \mathfrak{f}_\psi]$ , the least common multiple of  $\mathfrak{f}_\psi$  and  $\mathfrak{f}_\chi$ , and hence is not necessarily primitive. Thus, by Lemma 7.2, we deduce

$$\begin{aligned} 0 \leq -\operatorname{Re} \left\{ \frac{\xi'_K}{\xi_K}(\sigma) + \frac{L'}{L}(\sigma, \psi^*) + \frac{L'}{L}(\sigma + it, \chi^*) + \frac{L'}{L}(\sigma + it, \xi^*) \right\} \\ + \frac{n_K + \log N[\mathfrak{f}_\chi, \mathfrak{f}_\psi]}{2^\sigma - 1}. \end{aligned}$$

Note  $N[f_\chi, f_\psi] \leq Q^2$  since  $\psi$  and  $\chi$  are both characters trivial on the congruence subgroup  $H$ , and therefore the norms of their respective conductors are bounded by  $Q$ . Using this bound, we apply Lemmas 2.1 and 2.4 to each of the primitive  $L$ -function terms, yielding

$$0 \leq \frac{1}{2} \log(D_K D_\psi D_\chi D_\xi) + \frac{2}{2^\sigma - 1} \log Q + n_K \log(\sigma + 1 + |t|) + A_\sigma n_K - \operatorname{Re} \left\{ \sum_{\substack{\rho \\ \zeta_K(\rho)=0}} \frac{1}{\sigma - \rho} + \sum_{\substack{\rho \\ L(\rho, \psi)=0}} \frac{1}{\sigma - \rho} + \sum_{\substack{\rho \\ L(\rho, \chi)=0}} \frac{1}{\sigma + it - \rho} + \sum_{\substack{\rho \\ L(\rho, \psi\chi)=0}} \frac{1}{\sigma + it - \rho} \right\} + \frac{1 + \delta(\psi)}{\alpha} + \frac{1 + \delta(\psi)}{\alpha + 1} + \operatorname{Re} \left\{ \frac{\delta(\chi) + \delta(\chi\psi)}{\alpha + it} + \frac{\delta(\chi) + \delta(\chi\psi)}{\alpha + 1 + it} \right\}, \quad (7-2)$$

where  $A_\sigma = \log(\sigma + 1) + \frac{2}{\sigma} + \frac{1}{2^{\sigma-1}} - 2 \log \pi$ . Since  $0 < \beta < 1$ , we notice

$$\operatorname{Re} \left\{ \frac{1}{\sigma + it - \rho} \right\} \geq \frac{\alpha}{|\sigma + it - \rho|^2} \quad \text{and} \quad \operatorname{Re} \left\{ \frac{1}{\alpha + it} + \frac{1}{\alpha + 1 + it} \right\} \leq \frac{1}{\alpha} + \frac{1}{\alpha + 1}.$$

Further,  $D_\chi$  and  $D_\xi$  are both  $\leq D_K Q$ , since  $\xi = \psi^* \chi^*$  induces the character  $\psi\chi \pmod{q}$ , which is trivial on  $H$ . Rearranging (7-2) and employing all of the subsequent observations gives the desired conclusion.  $\square$

**7B. Proof of Theorem 3.3.** If  $\tilde{H} \pmod{m}$  induces  $H \pmod{q}$ , then a character  $\chi \pmod{H}$  is induced by a character  $\tilde{\chi} \pmod{\tilde{H}}$ . It follows that

$$L(s, \chi) = L(s, \tilde{\chi}) \prod_{\substack{p|q, p \nmid m}} \left( 1 - \frac{\tilde{\chi}(p)}{Np^s} \right)$$

for all  $s \in \mathbb{C}$ . This implies that the nontrivial zeros of  $L(s, \chi)$  are the same nontrivial zeros of  $L(s, \tilde{\chi})$ . Therefore, without loss of generality, we may assume  $H \pmod{q}$  is primitive.

We divide the proof according to whether  $\psi$  is quadratic or trivial. The arguments in each case are similar but require some minor differences.

*Case 1:  $\psi$  is quadratic.* Let  $m$  be a positive integer,  $\alpha \geq 1$ , and  $\sigma = \alpha + 1$ . From the inequality  $0 \leq (1 + \psi^*(n))(1 + \operatorname{Re}\{\chi^*(n)(Nn)^{-i\gamma'}\})$  and Lemma 2.2 with  $s = \sigma + i\gamma'$ , it follows that

$$\operatorname{Re} \left\{ \sum_{n=1}^{\infty} z_n^m \right\} \leq \frac{1}{\alpha^m} - \frac{1}{(\alpha + 1 - \beta_1)^{2m}} + \operatorname{Re} \left\{ \frac{\delta(\chi) + \delta(\psi\chi)}{(\alpha + i\gamma')^{2m}} - \frac{\delta(\chi) + \delta(\psi\chi)}{(\alpha + 1 + i\gamma' - \beta_1)^{2m}} \right\}, \quad (7-3)$$

where  $z_n = z_n(\gamma')$  satisfies  $|z_1| \geq |z_2| \geq \dots$  and runs over the multisets

$$\begin{aligned} & \{(\sigma - \omega)^{-2} : \omega \text{ is any zero of } \zeta_K(s)\}, \\ & \{(\sigma - \omega)^{-2} : \omega \neq \beta_1 \text{ is any zero of } L(s, \psi^*)\}, \\ & \{(\sigma + i\gamma' - \omega)^{-2} : \omega \neq \beta_1 \text{ is any zero of } L(s, \chi^*)\}, \\ & \{(\sigma + i\gamma' - \omega)^{-2} : \omega \neq \beta_1 \text{ is any zero of } L(s, \psi^* \chi^*)\}. \end{aligned} \tag{7-4}$$

Note that the multisets include trivial zeros of the corresponding  $L$ -functions, and  $\psi^* \chi^*$  is a Hecke character (not necessarily primitive) modulo the least common multiple of  $f_\chi$  and  $f_\psi$ . With this choice, it follows that

$$\left(\alpha + \frac{1}{2}\right)^{-2} \leq (\alpha + 1 - \beta')^{-2} \leq |z_1| \leq \alpha^{-2}. \tag{7-5}$$

The right-hand side of (7-3) may be bounded via the observation

$$\begin{aligned} \left| \frac{1}{(\alpha + it)^{2m}} - \frac{1}{(\alpha + it + 1 - \beta_1)^{2m}} \right| & \leq \alpha^{-2m} \left| 1 - \frac{1}{\left(1 + \frac{1 - \beta_1}{\alpha + it}\right)^{2m}} \right| \\ & \ll \alpha^{-2m-1} m(1 - \beta_1), \end{aligned}$$

whence

$$\operatorname{Re} \left\{ \sum_{n=1}^{\infty} z_n^m \right\} \ll \alpha^{-2m-1} m(1 - \beta_1). \tag{7-6}$$

On the other hand, by Theorem 7.1, for  $\epsilon > 0$ , there exists some  $m_0 = m_0(\epsilon)$  with  $1 \leq m_0 \leq (12 + \epsilon)M$  such that

$$\operatorname{Re} \left\{ \sum_{n=1}^{\infty} z_n^{m_0} \right\} \geq \frac{\epsilon}{50} |z_1|^{m_0} \geq \frac{\epsilon}{50} (\alpha + 1 - \beta')^{-2m_0} \geq \frac{\epsilon}{50} \alpha^{-2m_0} \exp\left(-\frac{2m_0}{\alpha}(1 - \beta')\right),$$

where  $M = |z_1|^{-1} \sum_{n=1}^{\infty} |z_n|$ . Comparing with (7-6) for  $m = m_0$ , it follows that

$$\exp\left(-\frac{2m_0}{\alpha}(1 - \beta')\right) \ll_{\epsilon} \frac{M}{\alpha} (1 - \beta_1). \tag{7-7}$$

Therefore, it suffices to bound  $\frac{M}{\alpha}$  and optimize over  $\alpha \geq 1$ .

By (7-4),  $M$  is a sum involving nontrivial and trivial zeros of certain  $L$ -functions. For the nontrivial zeros, we employ Lemma 7.4 with  $D_\psi = D_K N f_\psi \leq D_K Q$  since  $\psi$  is quadratic. For the trivial zeros, apply Lemma 7.3 in the “primitive” case for  $\zeta_K(s), L(s, \psi^*), L(s, \chi^*)$  and in the “unconditional” case for  $L(s, \psi^* \chi^*)$ . In the latter case, we additionally observe that, as  $H \pmod{q}$  is primitive,  $\log Nq \leq 2 \log Q$



by Lemma 2.12. Combining these steps along with (7-5), it follows that

$$\begin{aligned} \frac{M}{\alpha} \leq & \frac{(\alpha+1/2)^2}{\alpha^2} \cdot \left[ 2 \log D_K + \left( \frac{3}{2} + \frac{2\alpha}{2\alpha+2} + \frac{4\alpha}{(\alpha+1)^2 \log 2} + \frac{2}{2^{\alpha+1}-1} \right) \log Q \right. \\ & + \left( \log(\alpha+2) + \log(\alpha+3) + 2 - 2 \log \pi + \frac{4\alpha}{(\alpha+1)^2} + \frac{1}{2^{\alpha+1}-1} \right) n_K \\ & \left. + n_K \log T + \frac{4}{\alpha} + \frac{4}{\alpha+1} \right], \quad (7-8) \end{aligned}$$

for  $\alpha \geq 1$ . Note that, in applying Lemma 7.4, we used that  $\log(\alpha+2+T) \leq \log(\alpha+3) + \log T$  for  $T \geq 1$ . Finally, select  $\alpha$  sufficiently large, depending on  $\epsilon > 0$ , so the right-hand side of (7-8) is

$$\leq \left( 2 + \frac{\epsilon}{100} \right) \log D_K + \left( 2.5 + \frac{\epsilon}{100} \right) \log Q + \left( 1 + \frac{\epsilon}{100} \right) n_K \log T + O_\epsilon(n_K).$$

Incorporating the resulting bounds into (7-7) completes the proof of Theorem 3.3 for  $\psi$  quadratic.

*Case 2:  $\psi$  is trivial.* Begin with the inequality  $0 \leq 1 + \operatorname{Re}\{\chi^*(n)(Nn)^{-i\gamma'}\}$ . This similarly implies

$$\begin{aligned} \operatorname{Re} \left\{ \sum_{n=1}^{\infty} z_n^m \right\} \leq & \frac{1}{\alpha^m} - \frac{1}{(\alpha+1-\beta_1)^{2m}} \\ & + \operatorname{Re} \left\{ \frac{\delta(\chi)}{(\alpha+i\gamma')^{2m}} - \frac{\delta(\chi)}{(\alpha+1+i\gamma'-\beta_1)^{2m}} \right\} \quad (7-9) \end{aligned}$$

for a new choice  $z_n = z_n(\gamma')$  satisfying  $|z_1| \geq |z_2| \geq \dots$  and which runs over the multisets

$$\begin{aligned} & \{(\sigma - \omega)^{-2} : \omega \neq \beta_1 \text{ is any zero of } \zeta_K(s)\}, \\ & \{(\sigma + i\gamma' - \omega)^{-2} : \omega \neq \beta_1 \text{ is any zero of } L(s, \chi^*)\}. \end{aligned} \quad (7-10)$$

Following the same arguments as before, we may arrive at (7-7) for the new quantity  $M = |z_1|^{-1} \sum_{n=1}^{\infty} |z_n|$ . To bound the nontrivial zeros arising in  $M$ , apply Lemma 7.4 with  $D_\psi = D_K$  since  $\psi$  is trivial. For the trivial zeros, apply Lemma 7.3 in the “primitive” case for both  $\zeta_K(s)$  and  $L(s, \chi^*)$ . It follows from (7-5) that, for  $\alpha \geq 1$ ,

$$\begin{aligned} \frac{M}{\alpha} \leq & \frac{(\alpha+1/2)^2}{\alpha^2} \cdot \left[ \log D_K + \left( \frac{1}{2} + \frac{1}{2^{\alpha+1}-1} \right) \log Q \right. \\ & + \frac{1}{2} n_K \log T + \frac{2}{\alpha} + \frac{2}{\alpha+1} + \left( \frac{1}{2} \log(\alpha+2) + \frac{1}{2} \log(\alpha+3) + 1 \right. \\ & \left. \left. - \log \pi + \frac{2\alpha}{(\alpha+1)^2} + \frac{1/2}{2^{\alpha+1}-1} \right) n_K \right]. \quad (7-11) \end{aligned}$$

Again, we select  $\alpha$  sufficiently large, depending on  $\epsilon > 0$ , so the right-hand side of (7-11) is

$$\leq \left(1 + \frac{\epsilon}{50}\right) \log D_K + \left(0.5 + \frac{\epsilon}{50}\right) \log Q + \left(0.5 + \frac{\epsilon}{50}\right) n_K \log T + O_\epsilon(n_K).$$

Incorporating the resulting bound into (7-7) completes the proof of Theorem 3.3.  $\square$

**Remark.** To obtain a more explicit version of Theorem 3.3, the only difference in the proof is selecting an explicit value of  $\alpha$  in the final step of each case. The possible choice of  $\alpha$  is somewhat arbitrary because the coefficients of  $\log D_K$ ,  $\log Q$ , and  $n_K$  in (7-8) and (7-11) cannot be simultaneously minimized. Hence, in the interest of having relatively small coefficients of comparable size for all quantities, one could choose the value  $\alpha = 18$ .

### 8. Zeros in low-lying rectangles

Analogous to [Heath-Brown 1992] for the classical case, most of the key numerical estimates we use to prove Theorem 3.1 pertain to zeros in a “low-lying” rectangle. In this section, we record the relevant existing results and establish some new ones. These encompass the required three principles in Section 3 and will be applied in the final arguments for the proof of Theorem 3.1. We begin with some notation.

**8A. Logarithmic quantity.** Let  $\delta_0 > 0$  be fixed and sufficiently small. For the remainder of the paper, define

$$\mathcal{L} := \begin{cases} \left( \frac{1}{3} + \delta_0 \right) \log D_K + \left( \frac{19}{36} + \delta_0 \right) \log Q \\ \quad + \left( \frac{5}{12} + \delta_0 \right) n_K \log n_K & \text{if } n_K^{5n_K/6} \geq D_K^{4/3} Q^{4/9}, \\ \left( 1 + \delta_0 \right) \log D_K + \left( \frac{3}{4} + \delta_0 \right) \log Q \\ \quad + \delta_0 n_K \log n_K & \text{otherwise.} \end{cases} \tag{8-1}$$

Notice that

$$\begin{aligned} \mathcal{L} &\geq (1 + \delta_0) \log D_K + \left(\frac{3}{4} + \delta_0\right) \log Q + \delta_0 n_K \log n_K, \\ \mathcal{L} &\geq \left(\frac{5}{12} + \delta_0\right) n_K \log n_K, \end{aligned} \tag{8-2}$$

unconditionally. For  $T_\star \geq 1$  fixed,<sup>3</sup> set  $T_0 := \max\{n_K^{5/6} (D_K^{4/3} Q^{4/9})^{-1/n_K}, T_\star\}$ . We compare  $\mathcal{L} = \mathcal{L}_{T_0, \delta_0}$  given by (5-1) with  $\mathcal{L}$  and deduce  $\mathcal{L} \leq \mathcal{L}$  for  $\mathcal{L}$  sufficiently large. This observation implies that

$$N\left(1 - \frac{\lambda}{\mathcal{L}}, T, \chi\right) \leq N\left(1 - \frac{\lambda}{\mathcal{L}}, T, \chi\right) \tag{8-3}$$

for  $\lambda > 0$  and  $N(\sigma, T, \chi)$  defined in (5-7). We will utilize this fact in Section 8E.

<sup>3</sup>For the purposes of this paper, setting  $T_\star = 1$  would suffice, but we avoid this choice to make the results of Section 8 more widely applicable.

**8B. Low-lying zeros.** Next we specify some important zeros of  $\prod_{\chi \pmod{H}} L(s, \chi)$  which will be used for the remainder of the paper. Consider the multiset of zeros given by

$$\mathcal{Z} := \left\{ \rho \in \mathbb{C} : \prod_{\chi \pmod{H}} L(\rho, \chi) = 0, 0 < \operatorname{Re}\{\rho\} < 1, |\operatorname{Im}(\rho)| \leq T_\star \right\}. \quad (8-4)$$

We select three important zeros in  $\mathcal{Z}$  as follows:

- Choose  $\rho_1 \in \mathcal{Z}$  such that  $\operatorname{Re}\{\rho_1\}$  is maximal. Let  $\chi_1$  be its associated Hecke character, so  $L(\rho_1, \chi_1) = 0$ . Let

$$\rho_1 = \beta_1 + i\gamma_1 = \left(1 - \frac{\lambda_1}{\mathcal{L}}\right) + i \frac{\mu_1}{\mathcal{L}},$$

where  $\beta_1 = \operatorname{Re}\{\rho_1\}$ ,  $\gamma_1 = \operatorname{Im}\{\rho_1\}$ ,  $\lambda_1 > 0$ , and  $\mu_1 \in \mathbb{R}$ .

- Choose  $\rho' \in \mathcal{Z} \setminus \{\rho_1, \bar{\rho}_1\}$  satisfying  $L(\rho', \chi_1) = 0$  such that  $\operatorname{Re}\{\rho'\}$  is maximal.<sup>4</sup> Similarly, let

$$\rho' = \beta' + i\gamma' = \left(1 - \frac{\lambda'}{\mathcal{L}}\right) + i \frac{\mu'}{\mathcal{L}}.$$

- Let  $\mathcal{Z}_1$  be the multiset of zeros of  $L(s, \chi_1)$  contained in  $\mathcal{Z}$ . Choose  $\rho_2 \in \mathcal{Z} \setminus \mathcal{Z}_1$  such that  $\operatorname{Re}\{\rho_2\}$  is maximal. Let  $\chi_2$  be its associated Hecke character, so  $L(\rho_2, \chi_2) = 0$ . Similarly, let

$$\rho_2 = \beta_2 + i\gamma_2 = \left(1 - \frac{\lambda_2}{\mathcal{L}}\right) + i \frac{\mu_2}{\mathcal{L}}.$$

**8C. Zero-free regions.** With the above notation, we may introduce the first of three principles. We record the current best-known existing explicit result regarding zero-free regions of Hecke  $L$ -functions.

**Theorem 8.1** (Zaman). *For  $\mathcal{L}$  sufficiently large, we have  $\min\{\lambda', \lambda_2\} > 0.2866$ . If  $\lambda_1 < 0.0875$  then  $\rho_1$  is a simple real zero of  $\prod_{\chi \pmod{H}} L(s, \chi)$  and is associated with a real character  $\chi_1$ .*

*Proof.* When  $T_\star = 1$  and  $H = P_q$ , in which case  $Q = Nq$ , this is implied by [Zaman 2016a, Theorems 1.1 and 1.3] since  $\mathcal{L}$  satisfies (8-2). For general congruence subgroups  $H$  and any fixed  $T_\star \geq 1$ , the argument, which occurs in [Zaman 2017a], is achieved by modifying [Zaman 2016a] as follows:

- Assume  $H \pmod{q}$  is primitive, i.e.,  $\mathfrak{f}_H = q$ .
- Restrict to characters  $\chi \pmod{q}$  satisfying  $\chi(H) = 1$  throughout.
- Redefine  $\mathcal{L}$  and  $\mathcal{L}^*$  in [Zaman 2016a, (3.2)] to replace  $\log Nq$  with  $\log Q$ .

---

<sup>4</sup>If  $\rho_1$  is real then  $\rho' \in \mathcal{Z} \setminus \{\rho_1\}$  instead with the other conditions remaining the same.

- Substitute applications of [Zaman 2016a, Lemma 2.4] with Lemma 2.13 since  $q = f_H$ . When estimating certain sums, this allows one to transfer from imprimitive characters  $\chi \pmod{H}$  to primitive ones.
- Modify [Zaman 2016a, Lemma 3.2] so that the special value  $T_0(q)$ , in that lemma’s notation, instead satisfies  $T_\star \leq T_0(q) \leq \frac{1}{10} T_\star \mathcal{T}$ ; one can achieve this by analogously supposing, for a contradiction, that each region  $\alpha \leq \sigma \leq 1$  and  $T_\star 10^j \leq |t| \leq T_\star 10^{j+1}$  for  $0 \leq j < J$  with  $J = \lceil \log \mathcal{T} / \log 10 \rceil$  contains at least one zero of  $\prod_{\chi \pmod{H}} L(s, \chi)$ . After applying [Zaman 2016a, (3.4)] with  $T = T_\star \mathcal{T}$ , the rest of the argument follows similarly.  $\square$

**8D. Zero repulsion.** Here we record two explicit estimates for zero repulsion when an exceptional zero exists.

**Theorem 8.2** (Zaman). *If  $\lambda_1 < 0.0875$  then unconditionally, for  $\mathcal{L}$  sufficiently large,  $\min\{\lambda', \lambda_2\} > 0.44$ . If  $\eta \leq \lambda_1 < 0.0875$  then, for  $\mathcal{L}$  sufficiently large depending on  $\eta > 0$ ,  $\min\{\lambda', \lambda_2\} > 0.2103 \log(1/\lambda_1)$ .*

*Proof.* When  $T_\star = 1$  and  $H = P_q$ , this is contained in [Zaman 2016a, Theorem 1.4] since  $\mathcal{L}$  satisfies (8-2). Similarly to the proof of Theorem 8.1, one may modify [Zaman 2016a] to deduce the same theorem for general congruence subgroups  $H$  and any fixed  $T_\star \geq 1$ .  $\square$

Theorem 8.2 is not equipped to deal with exceptional zeros  $\rho_1$  extremely close to 1 due to the requirement  $\lambda_1 \geq \eta$ . Thus, we require a more widely applicable version of zero repulsion; this is precisely the purpose of Theorem 3.3, which we restate here in the current notation.

**Theorem 8.3.** *Let  $T \geq 1$  be arbitrary. Suppose  $\chi_1$  is a real character and  $\rho_1$  is a real zero. For  $\chi \pmod{H}$ , let  $\rho \neq \rho_1$  be any nontrivial zero of  $L(s, \chi)$  satisfying  $\frac{1}{2} \leq \text{Re}\{\rho\} = 1 - \frac{\lambda}{\mathcal{L}} < 1$  and  $|\text{Im}\{\rho\}| \leq T$ . For  $\mathcal{L}$  sufficiently large depending on  $\epsilon > 0$  and  $T$ , we have  $\lambda > \log(c_\epsilon/\lambda_1)/(80 + \epsilon)$ , where  $c_\epsilon > 0$  is an effective constant depending only on  $\epsilon$ .*

*Proof.* This follows immediately from Theorem 3.3 since

$$(48 + \epsilon) \log D_K + (60 + \epsilon) \log Q + (24 + \epsilon)n_K \log T + O_\epsilon(n_K) \leq (80 + 2\epsilon)\mathcal{L}$$

for  $\mathcal{L}$  sufficiently large depending on  $\epsilon$  and  $T$ .  $\square$

The repulsion constant  $\frac{1}{80+\epsilon} \approx 0.0125$  in Theorem 8.3 is much smaller than 0.2103 in Theorem 8.2. This deficiency follows from using power sum arguments; see the remarks following Theorem 3.3. We now quantify how close an exceptional zero  $\rho_1$  can be to 1.

**Theorem 8.4** [Stark 1974]. *Unconditionally,  $\lambda_1 \gg e^{-24\mathcal{L}/5}$ .*

*Proof.* This follows from (8-1), (8-2), and the proof of [Stark 1974, Theorem 1', p. 148].  $\square$

**8E. Log-free zero density estimates.** First, we restate a slightly weaker form of Theorem 3.2 in the current notation.

**Theorem 8.5.** *Let  $T \geq 1$  be arbitrary. If  $0 < \lambda < \mathcal{L}$  then*

$$\sum_{\chi \pmod{H}} N\left(1 - \frac{\lambda}{\mathcal{L}}, T, \chi\right) \ll e^{162\lambda}$$

*provided  $\mathcal{L}$  is sufficiently large depending on  $T$ .*

*Proof.* This follows from (8-1) and Theorem 3.2.  $\square$

In addition to Theorem 8.5, we require a completely explicit zero density estimate for “low-lying” zeros. Define<sup>5</sup>

$$\begin{aligned} \mathcal{N}(\lambda) = \mathcal{N}_H(\lambda) &:= \sum_{\chi \pmod{H}} N\left(1 - \frac{\lambda}{\mathcal{L}}, T_\star, \chi\right) \\ &= \sum_{\chi \pmod{H}} \#\left\{\rho : L(\rho, \chi) = 0, 1 - \frac{\lambda}{\mathcal{L}} < \operatorname{Re}\{\rho\} < 1, |\operatorname{Im}\{\rho\}| \leq T_\star\right\}. \end{aligned} \quad (8-5)$$

By Theorem 8.1, observe that  $\mathcal{N}(0.0875) \leq 1$  and  $\mathcal{N}(0.2866) \leq 2$ . In light of these bounds, we exhibit explicit numerical estimates for  $\mathcal{N}(\lambda)$  in the range with  $0.287 \leq \lambda \leq 1$ . For each fixed value of  $\lambda$ , we apply Theorem 5.3 with  $\nu = 0.1$  and  $\epsilon \in (0, 10^{-5})$  assumed to be fixed and sufficiently small, and obtain a bound for  $\mathcal{N}(\lambda\mathcal{L}/\mathcal{L})$ . By (8-3), the same bound holds for  $\mathcal{N}(\lambda)$ . By performing numerical experimentation over the remaining parameters  $(\alpha, \eta, \omega, \xi)$  using MATLAB, we roughly optimize the bound in Theorem 5.3 and generate Table 1. Note that we have verified  $J(\xi\lambda) < 1$  and  $X_{\xi\lambda} > Y_{\xi\lambda} > 4.6$  in each case.

Based on Table 1, we may also establish an explicit estimate for  $\mathcal{N}(\lambda)$  by specifying parameters in Theorem 5.3.

**Theorem 8.6.** *Let  $\epsilon_0 > 0$  be fixed and sufficiently small. If  $0 < \lambda < \epsilon_0\mathcal{L}$  then  $\mathcal{N}(\lambda) \leq e^{162\lambda+188}$  for  $\mathcal{L}$  sufficiently large. If  $0 < \lambda \leq 1$  then  $\mathcal{N}(\lambda)$  is also bounded as in Table 1.*

*Proof.* For  $\lambda \leq 0.2866$ , the result is immediate as  $\mathcal{N}(0.2866) \leq 2$  by Theorem 8.1. For  $0.2866 \leq \lambda \leq 1$ , one can directly verify the desired bound by using Table 1. Now, consider  $\lambda \geq 1$ . Apply Theorem 5.3 with

$$\begin{aligned} T = T_0, & \quad \lambda_0 = 1, & \quad \alpha = 0.1549, & \quad \eta = 0.05722, \\ \epsilon = 10^{-5}, & \quad \nu = 0.1, & \quad \xi = 1.0030, & \quad \omega = 0.02074. \end{aligned}$$

---

<sup>5</sup>Note  $\mathcal{N}(\lambda)$  defined here is *not* the same as  $N(\lambda)$  as defined in [Zaman 2016a]. Instead, one has  $N(\lambda) \leq \mathcal{N}(\lambda)$ .

$\lambda$	$\log N(\lambda) \leq$	$\alpha$	$\eta$	$\omega$	$\xi$	$J(\xi\lambda)$	$Y_{\xi\lambda}$	$X_{\xi\lambda}$
0.287	198.1	0.3448	0.09955	0.03466	1.0082	0.46	5.8	993
0.288	198.3	0.3444	0.09943	0.03462	1.0082	0.46	5.8	991
0.289	198.5	0.3441	0.09931	0.03458	1.0082	0.46	5.8	988
0.290	198.7	0.3437	0.09918	0.03454	1.0082	0.46	5.8	986
0.291	198.9	0.3433	0.09906	0.03450	1.0082	0.46	5.8	984
0.292	199.1	0.3429	0.09894	0.03446	1.0081	0.46	5.8	982
0.293	199.3	0.3426	0.09882	0.03442	1.0081	0.46	5.8	979
0.294	199.5	0.3422	0.09870	0.03439	1.0081	0.46	5.8	977
0.295	199.8	0.3418	0.09859	0.03435	1.0081	0.46	5.8	975
0.296	200.0	0.3415	0.09847	0.03431	1.0081	0.46	5.8	973
0.297	200.2	0.3411	0.09835	0.03427	1.0080	0.46	5.8	970
0.298	200.4	0.3408	0.09823	0.03423	1.0080	0.46	5.8	968
0.299	200.6	0.3404	0.09811	0.03420	1.0080	0.46	5.8	966
0.300	200.8	0.3400	0.09800	0.03416	1.0080	0.46	5.8	964
0.325	205.9	0.3316	0.09518	0.03326	1.0075	0.47	5.8	914
0.350	211.0	0.3240	0.09257	0.03242	1.0071	0.47	5.7	871
0.375	216.0	0.3171	0.09014	0.03163	1.0067	0.47	5.7	833
0.400	220.9	0.3108	0.08787	0.03090	1.0064	0.48	5.7	800
0.425	225.7	0.3054	0.08678	0.02878	1.0061	0.46	5.6	769
0.450	230.4	0.2998	0.08373	0.02956	1.0059	0.48	5.6	744
0.475	235.1	0.2948	0.08184	0.02895	1.0056	0.48	5.6	720
0.500	239.8	0.2903	0.08006	0.02837	1.0054	0.49	5.6	699
0.550	249.0	0.2821	0.07677	0.02729	1.0050	0.49	5.5	661
0.600	258.0	0.2748	0.07379	0.02631	1.0046	0.50	5.5	629
0.650	266.9	0.2684	0.07109	0.02542	1.0043	0.50	5.4	602
0.700	275.6	0.2627	0.06862	0.02460	1.0041	0.50	5.4	579
0.750	284.3	0.2576	0.06634	0.02383	1.0039	0.51	5.4	559
0.800	292.9	0.2529	0.06424	0.02313	1.0037	0.51	5.4	541
0.850	301.4	0.2486	0.06230	0.02247	1.0035	0.51	5.3	525
0.900	309.8	0.2447	0.06049	0.02186	1.0033	0.51	5.3	510
0.950	318.2	0.2412	0.05880	0.02128	1.0032	0.52	5.3	497
1.000	326.5	0.2378	0.05722	0.02074	1.0030	0.52	5.3	486

**Table 1.** Bounds for  $\mathcal{N}(\lambda)$  using Theorem 5.3 with  $\nu = 0.1$  and  $\epsilon \in (0, 10^{-5}]$ .

This choice of values is motivated by the last row of Table 1, but with a more suitable choice for  $\alpha$ . With this selection, one can check that for any  $\lambda \geq 1$ ,

$$4.61 \leq Y_{\xi\lambda} \leq 9.2, \quad 264 \leq X_{\xi\lambda} \leq 526, \quad J(\xi\lambda) \leq 0.272.$$

These inequalities can be verified by elementary arguments involving the definitions in Section 5A and (5-6). In particular, for any  $\lambda \geq 1$ , the assumptions of Theorem 5.3 are satisfied for all  $1 \leq \lambda < \epsilon_0 \mathcal{L}$ .

Now with these estimates, we may deduce upper bounds for  $C_4, C_3, C_1, C_0, B_2,$  and  $B_1$  in Theorem 5.3 as follows:

$$\begin{aligned} C_4 = C_4(\lambda) &\leq 6.0 \times 10^{13}, & C_1 &\leq 17, & B_2 &\leq 154, \\ C_3 = C_3(\lambda) &\leq 2.4 \times 10^{14}, & C_0 &\leq 65, & B_1 &\leq 156, \end{aligned}$$

for  $\lambda \geq 1$ . Thus, by Theorem 5.3, for  $1 \leq \lambda \leq \epsilon_0 \mathcal{L}$ ,

$$N(\lambda) \leq 52(6.0 \times 10^{13} \cdot \lambda^4 + 2.4 \times 10^{14} \cdot \lambda^3 + 17 \cdot \lambda + 65)e^{156\lambda+154}.$$

To simplify the expression on the right-hand side, we crudely observe that the above is

$$\begin{aligned} &\leq 52 \cdot 65 \left( 6.0 \times 10^{13} \cdot \frac{24}{6^4 \cdot 65} \cdot \frac{(6\lambda)^4}{4!} \right. \\ &\quad \left. + 2.4 \times 10^{14} \cdot \frac{6}{6^3 \cdot 65} \cdot \frac{(6\lambda)^3}{3!} + 6\lambda + 1 \right) e^{156\lambda+154} \\ &\leq 52 \cdot 6.7 \times 10^{12} \cdot \left( \frac{(6\lambda)^4}{4!} + \frac{(6\lambda)^3}{3!} + 6\lambda + 1 \right) e^{156\lambda+154} \leq e^{162\lambda+188}, \end{aligned}$$

as desired. □

### 9. Proof of Theorem 3.1: preliminaries

We may finally begin the proof of Theorem 3.1. The arguments below are motivated by [Heath-Brown 1992, Section 10] and mostly follow the structure of [Zaman 2017b, Section 4]. Recall that we retain the notation introduced in Section 8 for the remainder of the paper.

**9A. Choice of weight.** We define a weight function (see [Zaman 2017b, Lemmas 2.6 and 2.7]) and describe its properties.

**Lemma 9.1.** *For real numbers  $A, B > 0$  and a positive integer  $\ell \geq 1$  satisfying  $B > 2\ell A$ , define*

$$F(z) = F_\ell(z; B, A) = e^{-(B-2\ell A)z} \left( \frac{1-e^{-Az}}{Az} \right)^{2\ell}, \tag{9-1}$$

and let  $f(t)$  be the inverse Laplace transform of  $F(z)$ . Then:

- (i)  $0 \leq f(t) \leq A^{-1}$  for all  $t \in \mathbb{R}$ .
- (ii) The support of  $f$  is contained in  $[B - 2\ell A, B]$ .
- (iii) For  $x > 0$  and  $y \in \mathbb{R}$ ,

$$|F(x + iy)| \leq e^{-(B-2\ell A)x} \left( \frac{1-e^{-Ax}}{Ax} \right)^{2\ell} \leq e^{-(B-2\ell A)x}.$$

For the entirety of this section, select real numbers  $A, B > 0$  and an integer  $\ell \geq 1$  satisfying  $B > 2\ell A$ , and let  $F(\cdot) = F_\ell(\cdot; B, A)$ . The inverse Laplace transform of  $F(z)$  is written as  $f(t)$ , so that  $F(z) = \int_0^\infty f(t)e^{-zt} dt$ . To motivate our choice of  $f$ , we note that the parameter  $\ell$  is chosen to be of size  $O(n_K)$ , so that  $f(t)$  is  $O(n_K)$ -times differentiable and hence  $F(x + iy)$  decays like  $|y|^{-O(n_K)}$  for fixed  $x > 0$  and as  $|y| \rightarrow \infty$ . This decay rate is necessary when applying log-free zero density estimates such as Theorem 3.2 to bound the contribution of zeros which are high in the critical strip.

**9B. A weighted sum of prime ideals.** For the congruence class group  $H \pmod{\mathfrak{q}}$ , let  $\mathcal{C}$  be an element of the class group of  $H$ ; that is,  $\mathcal{C} \in I(\mathfrak{q})/H$ . Using the compactly supported weight  $f$ , define

$$S := \sum_{\substack{\mathfrak{p} \nmid \mathfrak{q}\mathfrak{D}_K \\ \text{Np is a rational prime}}} \frac{\log \text{Np}}{\text{Np}} f\left(\frac{\log \text{Np}}{\mathcal{L}}\right) \cdot \mathbf{1}_{\mathcal{C}}(\mathfrak{p}), \tag{9-2}$$

where  $\mathbf{1}_{\mathcal{C}}(\cdot)$  is an indicator function for the coset  $\mathcal{C}$ ,  $\mathfrak{D}_K$  is the different of  $K$ , and the sum is over degree 1 prime ideals  $\mathfrak{p}$  of  $K$  not dividing  $\mathfrak{q}\mathfrak{D}_K$ . We reduce the proof of Theorem 3.1 to verifying the following lemma.

**Lemma 9.2.** *Let  $\eta > 0$  be sufficiently small and let  $\mathfrak{m}$  be the product of prime ideals dividing  $\mathfrak{q}$  but not  $\mathfrak{f}_H$ . If  $h_H \mathcal{L}^{-1} S \gg_\eta \min\{1, \lambda_1\}$  for*

$$B \geq \max\left\{693.5, \frac{\log \text{Nm}}{\mathcal{L}} + 8\eta\right\}, \quad A = \frac{4}{\mathcal{L}}, \quad \ell = \lfloor \eta \mathcal{L} \rfloor \tag{9-3}$$

and  $\mathcal{L}$  is sufficiently large then Theorem 3.1 holds.

*Proof.* Select  $B = (\log x)/\mathcal{L}$  with  $A = 4/\mathcal{L}$  and  $\ell = \lfloor \eta \mathcal{L} \rfloor$ . From the definition (8-1) of  $\mathcal{L}$  and the condition on  $x$  in (3-1), one can verify that  $B$  satisfies (9-3). Now, since  $f$  is supported in  $[B - 2\ell A, B]$  and  $|f| \leq A^{-1} \leq \mathcal{L}$  by Lemma 9.1,

$$S \leq \mathcal{L} e^{8\eta \mathcal{L}} x^{-1} \log x \#\{\mathfrak{p} : \text{Np} \leq x, \text{deg}(\mathfrak{p}) = 1, \mathfrak{p} \in \mathcal{C}\}.$$

Multiplying both sides by  $h_H \mathcal{L}^{-1}$  and noting  $B$  satisfies (9-3), we conclude

$$\#\{\mathfrak{p} : \text{Np} \leq x, \text{deg}(\mathfrak{p}) = 1, \mathfrak{p} \in \mathcal{C}\} \geq \frac{4S}{\mathcal{L}} \cdot \frac{x e^{-8\eta \mathcal{L}}}{\log x} \gg_\eta e^{-5\mathcal{L}} \cdot \frac{x}{h_H \log x}.$$

by Theorems 8.1 and 8.4. Fixing  $\eta$  and noting  $\mathcal{L} \leq \log(D_K Q n_K^{n_K})$  yields the conclusion of Theorem 3.1. □



Now, by orthogonality of characters,

$$S = \frac{1}{h_H} \sum_{\chi \pmod{H}} \bar{\chi}(C) S_\chi, \quad \text{where } S_\chi := \sum_{\substack{p \nmid q\mathfrak{D}_K \\ Np \text{ is a rational prime}}} \frac{\log Np}{Np} \chi(p) f\left(\frac{\log Np}{\mathcal{L}}\right). \quad (9-4)$$

We wish to write  $S_\chi$  as a contour integral involving a logarithmic derivative of a primitive Hecke  $L$ -function. Before doing so, we define

$$\mathfrak{m} = \prod_{p \mid q, p \nmid f_H} p. \quad (9-5)$$

**Lemma 9.3.** *If  $B - 2\ell A > \max\{1, (\log Nm)/\mathcal{L}\}$  then*

$$\mathcal{L}^{-1} S_\chi = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} -\frac{L'}{L}(s, \chi^*) F((1-s)\mathcal{L}) ds + O(A^{-1} e^{-(B-2\ell A)\mathcal{L}/2}),$$

where  $\chi^*$  is the primitive Hecke character inducing  $\chi \pmod{H}$ .

*Proof.* Observe

$$\begin{aligned} \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} -\frac{L'}{L}(s, \chi^*) F((1-s)\mathcal{L}) ds \\ = \mathcal{L}^{-1} \sum_n \frac{\Lambda(n)}{Nn} \chi^*(n) f\left(\frac{\log Nn}{\mathcal{L}}\right) = \mathcal{L}^{-1} \tilde{S}_\chi, \end{aligned}$$

say. Thus, we must show  $\tilde{S}_\chi$  equals  $S_\chi$  up to a negligible contribution from prime ideal powers, prime ideals whose norms are not rational primes, and prime ideals dividing  $q\mathfrak{D}_K$ . For simplicity, denote  $X = e^{(B-2\ell A)\mathcal{L}}$ .

*Prime ideal powers.* By Lemma 9.1, the contribution of such ideals in  $\tilde{S}_\chi$  is bounded by

$$\sum_p \sum_{m \geq 2} \frac{\log Np}{Np^m} f\left(\frac{\log Np^m}{\mathcal{L}}\right) \leq A^{-1} \sum_p \sum_{\substack{m \geq 2 \\ Np^m \geq X}} \frac{\log Np}{Np^m}.$$

Since a rational prime  $p$  splits into at most  $n_K$  prime ideals in  $K$ , the right-hand side is

$$\leq A^{-1} \sum_{p \text{ rational}} \sum_{(p) \subseteq \mathfrak{p}} \sum_{\substack{m \geq 2 \\ Np^m \geq X}} \frac{\log Np}{Np^m} \leq A^{-1} \sum_{\substack{p \text{ rational} \\ p \geq X^{1/2}}} \frac{1}{p^2} \sum_{(p) \subseteq \mathfrak{p}} \log Np \ll A^{-1} \mathcal{L} X^{-1/2}$$

by partial summation and noting  $n_K \ll \mathcal{L}$  from Minkowski's bound.

*Prime ideals with norm not equal to a rational prime.* By Lemma 9.1,

$$\sum_{\substack{\mathfrak{p} \\ N\mathfrak{p} \text{ not a rational prime}}} \sum_{m=1}^{\infty} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^m} f\left(\frac{\log N\mathfrak{p}^m}{\mathcal{L}}\right) \ll A^{-1} \sum_{\substack{N\mathfrak{p} \geq X \\ N\mathfrak{p} \text{ not a rational prime}}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}}.$$

For  $\mathfrak{p}$  appearing in the right-hand sum and lying above the rational prime  $p$ , notice  $N\mathfrak{p} \geq p^2$ . Thus, arguing as in the previous case, we deduce

$$\ll A^{-1} \sum_{\substack{p \geq X^{1/2} \\ p \text{ rational prime}}} \frac{1}{p^2} \sum_{(p) \subseteq \mathfrak{p}} \log N\mathfrak{p} \ll A^{-1} \mathcal{L} X^{-1/2}.$$

*Prime ideals dividing  $\mathfrak{q}\mathfrak{D}_K$ .* As  $B - 2\ell A > \max\{1, (\log Nm)/\mathcal{L}\}$ ,  $N\mathfrak{D}_K \leq D_K \leq e^{-\mathcal{L}}$  by (8-2), and  $f$  is supported in  $[B - 2\ell A, B]$ , we have  $f((\log N\mathfrak{p})/\mathcal{L}) = 0$  for  $\mathfrak{p} \mid m\mathfrak{D}_K$ . As  $\chi(\mathfrak{p}) = \chi^*(\mathfrak{p})$  for all  $\mathfrak{p} \nmid m$ , this implies that

$$\chi(\mathfrak{p}) f\left(\frac{\log N\mathfrak{p}}{\mathcal{L}}\right) = \chi^*(\mathfrak{p}) f\left(\frac{\log N\mathfrak{p}}{\mathcal{L}}\right)$$

for all prime ideals  $\mathfrak{p}$ . Combining all of these contributions to compare  $S_\chi$  with  $\tilde{S}_\chi$  yields the desired result.  $\square$

Applying Lemma 9.3 to (9-4), we deduce

$$\mathcal{L}^{-1} S = \frac{1}{h_H} \sum_{\chi \pmod{H}} \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} -\frac{L'}{L}(s, \chi^*) F((1-s)\mathcal{L}) ds + O(A^{-1} e^{-(B-2\ell A)\mathcal{L}/2}), \tag{9-6}$$

provided  $B - 2\ell A > \max\{1, (\log Nm)/\mathcal{L}\}$ .

**9C. A sum over low-lying zeros.** The next step is to shift the contour in (9-6) and pick up the arising poles. Our objective in this subsection is to reduce the analysis to the “low-lying” zeros of Hecke  $L$ -functions.

**Lemma 9.4.** *Let  $T_\star \geq 1$  be fixed, and let  $\rho_1$  and  $\chi_1$  be as in Section 8B. If the inequalities  $B - 2\ell A > \max\{162, (\log Nm)/\mathcal{L}\}$ ,  $\ell > (81n_K + 162)/4$ , and  $A > 1/\mathcal{L}$  hold and  $\mathcal{L}$  is sufficiently large, then*

$$\begin{aligned} & |h_H \mathcal{L}^{-1} S - F(0) + \bar{\chi}_1(C) F((1 - \rho_1)\mathcal{L})| \\ & \leq \sum_{\chi \pmod{H}} \sum'_{\rho} |F((1 - \rho)\mathcal{L})| + O\left(\left(\frac{2}{AT_\star \mathcal{L}}\right)^{2\ell} T_\star^{40.5n_K} + e^{-78\mathcal{L}}\right), \end{aligned}$$

where the sum  $\sum'$  indicates a restriction to nontrivial zeros  $\rho \neq \rho_1$  of  $L(s, \chi)$ , counted with multiplicity, satisfying  $0 < \text{Re}\{\rho\} < 1$  and  $|\text{Im}\{\rho\}| \leq T_\star$ .

*Proof.* Shift the contour in (9-6) to the line  $\text{Re}\{s\} = -\frac{1}{2}$ . For each primitive character  $\chi^*$ , this picks up the nontrivial zeros of  $L(s, \chi)$ , the simple pole at  $s = 1$  when  $\chi$  is trivial, and the trivial zero at  $s = 0$  of  $L(s, \chi)$  of order  $r(\chi)$ . To bound the remaining contour, by [Lagarias et al. 1979, Lemma 2.2] and Lemma 9.1(iii) with [Zaman 2017b, Lemma 2.7], for  $\text{Re}\{s\} = -\frac{1}{2}$  we have

$$-\frac{L'}{L}(s, \chi^*) \ll \mathcal{L} + n_K \log(|s| + 2) \quad \text{and} \quad |F((1-s)\mathcal{L})| \ll e^{-\frac{3}{2}(B-2\ell A)\mathcal{L}} \cdot |s|^{-2}$$

since  $A > 1/\mathcal{L}$ . It follows that

$$\frac{1}{2\pi i} \int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty} -\frac{L'}{L}(s, \chi^*) F((1-s)\mathcal{L}) ds \ll \mathcal{L} e^{-\frac{3}{2}(B-2\ell A)\mathcal{L}}.$$

Overall, (9-6) becomes

$$\frac{h_H S}{\mathcal{L}} - F(0) + \sum_{\chi \pmod{H}} \bar{\chi}(C) \sum_{\rho} F((1-\rho)\mathcal{L}) \ll \sum_{\chi \pmod{H}} r(\chi) F(\mathcal{L}) + \frac{\mathcal{L}}{e^{(B-2\ell A)\mathcal{L}/2}}, \quad (9-7)$$

where the inner sum over  $\rho$  is over all nontrivial zeros of  $L(s, \chi)$ . From (2-5) and (2-7), notice  $r(\chi) \leq n_K$ . Thus, by Lemma 9.1 and Minkowski's bound  $n_K \ll \mathcal{L}$ ,

$$\frac{1}{h_H} \sum_{\chi \pmod{H}} r(\chi) F(\mathcal{L}) \ll \mathcal{L} e^{-(B-2\ell A)\mathcal{L}}.$$

Since  $h_H \ll e^{2\mathcal{L}}$  by Lemma 2.11 and (8-2), it follows from (9-7) that

$$h_H \mathcal{L}^{-1} S = F(0) - \sum_{\chi \pmod{H}} \bar{\chi}(C) \sum_{\rho} F((1-\rho)\mathcal{L}) + O(\mathcal{L} e^{-(B-2\ell A-4)\mathcal{L}/2}).$$

The error term is bounded by  $O(e^{-78\mathcal{L}})$  as  $B - 2\ell A > 162$ . Therefore, it suffices to show

$$Z := \sum_{\chi \pmod{H}} \sum_{k=0}^{\infty} \sum_{\substack{\rho \\ 2^k T_{\star} \leq \text{Im}\{\rho\} < 2^{k+1} T_{\star}}} |F((1-\rho)\mathcal{L})| \ll \left(\frac{2}{AT_{\star}\mathcal{L}}\right)^{2\ell} T_{\star}^{40.5n_K}.$$

From Lemma 9.1, writing  $\rho = \beta + i\gamma$  with  $\beta \geq \frac{1}{2}$ , observe

$$|F(\rho\mathcal{L})| + |F((1-\rho)\mathcal{L})| \leq 2e^{-(B-2\ell A)(1-\beta)\mathcal{L}} \left(\frac{2}{A|\gamma|\mathcal{L}}\right)^{2\ell},$$

and moreover, from Theorem 3.2,

$$\tilde{N}(\sigma) := \sum_{\chi \pmod{H}} N(\sigma, 2T, \chi) \ll (e^{162\mathcal{L}} T^{81n_K + 162})^{(1-\sigma)}$$

for  $\frac{1}{2} \leq \sigma \leq 1$ ,  $T \geq 1$ , and  $\mathcal{L}$  sufficiently large. Thus, by partial summation,

$$\begin{aligned} \sum_{\chi \pmod{H}} \sum_{\substack{\rho \\ T \leq |\text{Im}\{\rho\}| \leq 2T}} |F((1-\rho)\mathcal{L})| &\ll \left(\frac{2}{A\mathcal{L}}\right)^{2\ell} \int_1^{1/2} e^{-(B-2\ell A)(1-\sigma)\mathcal{L}} d\tilde{N}(\sigma) \\ &\ll \left(\frac{2}{A\mathcal{L}}\right)^{2\ell} T^{40.5n_K+81-2\ell} \end{aligned}$$

since  $B > 2\ell A + 162$ . Note we have used that the zeros of  $\prod_{\chi \pmod{H}} L(s, \chi)$  are symmetric across the critical line  $\text{Re}\{s\} = \frac{1}{2}$ . Overall, we deduce

$$Z \ll \left(\frac{2}{A\mathcal{L}}\right)^{2\ell} T_\star^{40.5n_K+81-2\ell} \sum_{k=0}^{\infty} (2^k)^{40.5n_K+81-2\ell} \ll \left(\frac{2}{A\mathcal{L}}\right)^{2\ell} T_\star^{40.5n_K},$$

since  $\ell > \frac{1}{4}(81n_K + 162)$  and  $T_\star$  is fixed, as desired. □

We further restrict the sum over zeros in Lemma 9.4 to zeros  $\rho$  close to the line  $\text{Re}\{s\} = 1$ . To simplify the statement, we also select parameters  $\ell$  and  $A$  for the weight function.

**Lemma 9.5.** *Let  $T_\star \geq 1$  and  $\eta \in (0, 1)$  be fixed and  $1 \leq R \leq \mathcal{L}$  be arbitrary. Suppose*

$$B - 2\ell A > \max\left\{162, \frac{\log Nm}{\mathcal{L}}\right\}, \quad A = \frac{4}{\mathcal{L}}, \quad \ell = \lfloor \eta \mathcal{L} \rfloor. \tag{9-8}$$

If  $\mathcal{L}$  is sufficiently large then

$$\begin{aligned} &|h_{H\mathcal{L}^{-1}} S - F(0) + \bar{\chi}_1(C)F((1-\rho_1)\mathcal{L})| \\ &\leq \sum_{\chi \pmod{H}} \sum_{\rho}^* |F((1-\rho)\mathcal{L})| + O(e^{-(B-2\ell A-162)R} + (2T_\star)^{-2\eta\mathcal{L}} e^{\eta\mathcal{L}} + e^{-78\mathcal{L}}) \end{aligned}$$

where the marked sum  $\sum^*$  runs over zeros  $\rho \neq \rho_1$  of  $L(s, \chi)$ , counting with multiplicity, satisfying  $1 - R/\mathcal{L} < \text{Re}\{\rho\} < 1$  and  $|\text{Im}\{\rho\}| \leq T_\star$ .

*Proof.* For  $\mathcal{L}$  sufficiently large depending on  $\epsilon$  and  $\eta$ , the quantities  $B$ ,  $A$ , and  $\ell$  satisfy the assumptions of Lemma 9.4. Denote  $B' = B - 2\ell A$ . We claim it suffices to show

$$\sum_{\chi \pmod{H}} \sum'_{\text{Re}\{\rho\} \leq 1-R/\mathcal{L}} |F((1-\rho)\mathcal{L})| \ll e^{-(B'-162)R}, \tag{9-9}$$

where  $\sum'$  is defined in Lemma 9.4. To see the claim, we need only show that the error term in Lemma 9.4 is absorbed by that of Lemma 9.5. For  $\mathcal{L}$  sufficiently large, notice  $T_\star^{40.5n_K} \leq e^{\eta\mathcal{L}}$  as  $n_K \log T_\star = o(\mathcal{L})$ ; hence, for our choices of  $A$  and  $\ell$ , we have

$$\left(\frac{2}{A\mathcal{L}}\right)^{2\ell} T_\star^{40.5n_K} \leq \left(\frac{1}{2T_\star}\right)^{2\eta\mathcal{L}} e^{\eta\mathcal{L}}.$$

This proves the claim. Now, to establish (9-9), define the multiset of zeros

$$\mathcal{R}_m(\chi) := \left\{ \rho : L(\rho, \chi) = 0, 1 - \frac{m+1}{\mathcal{L}} \leq \operatorname{Re}\{\rho\} \leq 1 - \frac{m}{\mathcal{L}}, |\operatorname{Im}\{\rho\}| \leq T_\star \right\}$$

for  $1 \leq m \leq \mathcal{L}$ . By Theorem 8.5 and Lemma 9.1, it follows that

$$\sum_{\chi \pmod{H}} \sum_{\rho \in \mathcal{R}_m(\chi)} |F((1-\rho)\mathcal{L})| \leq e^{-B'm} \sum_{\chi \pmod{H}} \#\mathcal{R}_m(\chi) \ll e^{-(B'-162)m}$$

for  $\mathcal{L}$  sufficiently large. Summing over  $m \geq R$  yields the desired conclusion.  $\square$

### 10. Proof of Theorem 3.1: exceptional case

For this section, we assume  $\lambda_1 < 0.0875$ . By Theorem 8.1,  $\rho_1$  is a simple real zero and  $\chi_1$  is a real Hecke character. For fixed  $\eta \in (0, 10^{-3})$  sufficiently small, assume  $\mathcal{L}$  is sufficiently large and that

$$B \geq \max\left\{163, \frac{\log Nm}{\mathcal{L}} + 8\eta\right\}, \quad \ell = \lfloor \eta\mathcal{L} \rfloor, \quad \text{and} \quad A = \frac{4}{\mathcal{L}}.$$

Thus  $B, \ell$ , and  $A$  satisfy (9-8) and  $B' := B - 2\ell A > 162$ . For the moment, we do not make any additional assumptions on the minimum size of  $B$  and hence  $B'$ . To prove Theorem 3.1 when  $\rho_1$  is an exceptional zero, it suffices to show, by Lemma 9.2, that  $h_H \mathcal{L}^{-1} S \gg \min\{1, \lambda_1\}$  for  $B \geq \max\{593, (\log Nm)/\mathcal{L} + 8\eta\}$  and  $\mathcal{L}$  sufficiently large.

For a nontrivial zero  $\rho$  of a Hecke  $L$ -function, write  $\rho = \beta + i\gamma = (1 - \frac{\lambda}{\mathcal{L}}) + i\gamma$ , so that by Lemma 9.1,  $|F((1-\rho)\mathcal{L})| \leq e^{-B'\lambda}$ . From Lemma 9.5, with  $T_\star \geq 1$  fixed and  $1 \leq R \leq \mathcal{L}$  arbitrary, it follows that if we define

$$\Delta = \begin{cases} \eta & \text{if } T_\star = 1 \\ & \text{and } R = R(\eta) \text{ is sufficiently large,} \\ O(e^{-(B'-162)R} + e^{-78\mathcal{L}}) & \text{if } T_\star = T_\star(\eta) \text{ is sufficiently large} \\ & \text{and } 1 \leq R \leq \mathcal{L}, \end{cases} \quad (10-1)$$

then

$$h_H \mathcal{L}^{-1} S \geq 1 - \chi_1(\mathcal{C})e^{-B'\lambda_1} - \sum_{\chi \pmod{H}} \sum_{\rho}^* e^{-B'\lambda} - \Delta, \quad (10-2)$$

where the restricted sum  $\sum^*$  is over zeros  $\rho \neq \rho_1$ , counted with multiplicity, satisfying  $0 < \lambda \leq R$  and  $|\gamma| \leq T_\star$ .

Suppose the arbitrary parameter  $\lambda^* > 0$  satisfies

$$\lambda > \lambda^* \quad \text{for every zero } \rho \text{ occurring in the restricted sum of (10-2).} \quad (10-3)$$

It remains for us to divide into cases according to the range of  $\lambda_1$  and value of  $\chi_1(\mathcal{C}) \in \{\pm 1\}$ . In each case, we make a suitable choice for  $\lambda^*$ .

**10A. Moderate exceptional zero ( $\eta \leq \lambda_1 < 0.0875$  or  $\chi_1(C) = -1$ ).** For the moment, we do not make any assumptions on the size of  $\lambda_1$  other than that  $0 < \lambda_1 < 0.0875$ . Select  $T_\star = 1$  and  $R = R(\eta)$  sufficiently large so  $\Delta = \eta$  according to (10-1). By partial summation, our choice of  $\lambda^\star$  in (10-2), and Theorem 8.6,

$$\begin{aligned} \sum_{\chi \pmod{H}} \sum_{\rho}^\star e^{-B'\lambda} &\leq \int_{\lambda^\star}^R e^{-B'\lambda} d\mathcal{N}(\lambda) \\ &\leq e^{-(B'-162)R+188} + \int_{\lambda^\star}^\infty B' e^{-(B'-162)\lambda+188} d\lambda. \end{aligned}$$

As  $R = R(\eta)$  is sufficiently large and  $B' > 162$ , the above is

$$\leq \left(1 - \frac{162}{B'}\right)^{-1} e^{188-(B'-162)\lambda^\star} + \eta.$$

Comparing with (10-2), we have

$$h_H \mathcal{L}^{-1} S \geq 1 - \chi_1(C) e^{-B'\lambda_1} - \left(1 - \frac{162}{B'}\right)^{-1} e^{-(B'-162)\lambda^\star+188} - 2\eta. \quad (10-4)$$

Finally, we further subdivide into cases according to the size of  $\lambda_1$  and value of  $\chi_1(C) \in \{\pm 1\}$ . Recall  $\eta > 0$  is sufficiently small.

*Case 1:  $\lambda_1$  medium ( $10^{-3} \leq \lambda_1 < 0.0875$ ).* Here we also assume  $B \geq 593$ , in which case  $B' \geq 592$ . Select  $\lambda^\star = 0.44$ , which, by Theorem 8.2, satisfies (10-3) for the specified range of  $\lambda_1$ . Incorporating this estimate into (10-4) and noting  $|\chi_1(C)| \leq 1$ , we deduce

$$h_H \mathcal{L}^{-1} S \geq 1 - e^{-592 \times 10^{-3}} - \frac{592}{430} e^{-430 \times 0.44 + 188} - 2\eta \geq 0.032 - 2\eta$$

for  $\lambda \in [10^{-3}, 0.0875]$ . Hence, for  $\eta$  sufficiently small,  $h_H \mathcal{L}^{-1} S \gg 1$  in this subcase, as desired.

*Case 2:  $\lambda_1$  small ( $\eta \leq \lambda_1 < 10^{-3}$ ).* Here we also assume  $B \geq 297$ , in which case  $B' \geq 296.5$ . Select  $\lambda^\star = 0.2103 \log(1/\lambda_1)$ , which, by Theorem 8.2, satisfies (10-3). For  $\lambda < 10^{-3}$ , this implies  $\lambda^\star > 1.45$ . Applying both of these facts in (10-4) and noting  $|\chi_1(C)| \leq 1$ , we see

$$\begin{aligned} h_H \mathcal{L}^{-1} S &\geq 1 - e^{-296.5\lambda_1} - \frac{296}{134} e^{-(134.5-188/1.45)\lambda^\star} - 2\eta \\ &\geq 1 - e^{-296.5\lambda_1} - \frac{296}{134} \lambda_1 - 2\eta \end{aligned}$$

since  $4.84 \times 0.2103 = 1.017 \dots > 1$ . As  $1 - e^{-x} \geq x - \frac{x^2}{2}$  for  $x \geq 0$ , the above is

$$\geq 296.5\lambda_1 - \frac{(296.5)^2}{2} \lambda_1^2 - \frac{296}{134} \lambda_1 - 2\eta \geq 294.2\lambda_1(1 - 150\lambda_1) - 2\eta \geq 250\eta$$

because  $\eta \leq \lambda_1 < 10^{-3}$ . Therefore,  $h_H \mathcal{L}^{-1} S \gg 1$ , completing the proof of this subcase.

Case 3:  $\lambda_1$  very small ( $\lambda_1 < \eta$ ) and  $\chi_1(C) = -1$ . Here we also assume  $B \geq 163$ , in which case  $B' > 162.5$ . From (10-4), it follows that

$$h_H \mathcal{L}^{-1} S \geq 1 + e^{-162.5\lambda_1} - 325e^{-0.5\lambda^* + 188} - 2\eta \geq 2 - O(e^{-0.5\lambda^*} + \eta + \lambda_1).$$

By Theorem 8.3, the choice  $\lambda^* = \frac{1}{81} \log(c_{11}/\lambda_1)$  satisfies (10-3) for some absolute constant  $c_{11} > 0$ . Since  $\lambda_1 < \eta$ , the above is therefore

$$\geq 2 - O(\eta^{0.5/81} + \eta) \geq 2 - O(\eta^{1/162}).$$

As  $\eta$  is fixed and sufficiently small, we conclude  $h_H \mathcal{L}^{-1} S \gg 1$  as desired. This completes the proof for a “moderate” exceptional zero.

**10B. Truly exceptional zero ( $\lambda_1 < \eta$  and  $\chi_1(C) = +1$ ).** Select  $T_\star = T_\star(\eta)$  sufficiently large and let  $R = \frac{1}{80.1} \log(c_{12}/\lambda_1)$ , where  $c_{12} > 0$  is a sufficiently small absolute constant. By Theorem 8.3, it follows that the restricted sum over zeros  $\rho$  in (10-2) is empty and therefore, by (10-2) and (10-1),

$$h_H \mathcal{L}^{-1} S \geq 1 - e^{-B'\lambda_1} - O(\lambda_1^{(B'-162)/80.1} + e^{-78\mathcal{L}})$$

as  $\chi_1(C) = 1$ . Additionally assuming  $B \geq 243$ , in which case  $B' \geq 242.2$ , and noting  $1 - e^{-x} \geq x - \frac{x^2}{2}$  for  $x \geq 0$ , we conclude that

$$\begin{aligned} h_H \mathcal{L}^{-1} S &\geq 242.2\lambda_1 - O(\lambda_1^2 + \lambda_1^{80.2/80.1} + e^{-78\mathcal{L}}) \\ &\geq \lambda_1(242.2 - O(\lambda_1^{0.001} + e^{-73\mathcal{L}})) \end{aligned}$$

since  $\lambda_1 \gg e^{-4.8\mathcal{L}}$  by Theorem 8.4. As  $\lambda_1 \leq \eta$  for fixed  $\eta > 0$  sufficiently small, we conclude  $h_H \mathcal{L}^{-1} S \gg \lambda_1$  as desired.

Comparing all cases, we see that the most stringent condition is  $B \geq 593$ , thus completing the proof of Theorem 3.1 in the exceptional case.  $\square$

**Remark.** When  $H \pmod{q}$  is primitive, the “truly exceptional” subcase considered in Section 10B is implied by a numerically much stronger result of Zaman [2016b, Theorem 1.1] using entirely different methods.

### 11. Proof of Theorem 3.1: nonexceptional case

For this section, we assume  $\lambda_1 \geq 0.0875$ . Thus, we no longer have any additional information as to whether  $\rho_1$  is real or not, or whether  $\chi_1$  is real or not. We proceed in a similar fashion as the exceptional case, but require a slightly more refined analysis due to the absence of the Deuring–Heilbronn phenomenon. Assume  $\lambda^* > 0$  satisfies  $\lambda^* < \min\{\lambda', \lambda_2\}$ , where  $\lambda'$  and  $\lambda_2$  are defined in Section 8B. For  $0 < \eta \leq 10^{-3}$  fixed, suppose  $B \geq \max\{693.5, (\log Nm)/\mathcal{L} + 8\eta\}$ ,  $\ell = \lfloor \eta\mathcal{L} \rfloor$ , and  $A = 4/\mathcal{L}$ . Thus  $B, \ell$ , and  $A$  satisfy (9-8). By Lemma 9.2, it suffices to show  $h_H \mathcal{L}^{-1} S \gg 1$ . For simplicity, denote  $B' = B - 2\ell A \geq 693$ . For a nontrivial zero

$\rho$  of a Hecke  $L$ -function, as usual, write  $\rho = \beta + i\gamma = (1 - \lambda/\mathcal{L}) + i\mu/\mathcal{L}$ . From Lemma 9.5, as  $F(0) = 1$ , it follows that

$$h_H \mathcal{L}^{-1} S \geq 1 - |F(\lambda_1 + i\mu_1)| - |F(\lambda_1 - i\mu_1)| - \sum_{\chi \pmod{H}} \sum_{\rho}^{\dagger} |F(\lambda + i\mu)| - \eta,$$

where the marked sum  $\sum^{\dagger}$  runs over nontrivial zeros  $\rho \neq \rho_1$  (or  $\rho \neq \rho_1, \bar{\rho}_1$  if  $\rho_1$  is complex) of  $L(s, \chi)$ , counted with multiplicity, satisfying  $\lambda^* \leq \lambda \leq R$  and  $|\gamma| \leq 1$  for some  $R = R(\eta) \geq 1$  sufficiently large. By Lemma 9.1, this implies

$$h_H \mathcal{L}^{-1} S \geq 1 - 2e^{-B'\lambda_1} - \sum_{\chi \pmod{H}} \sum_{\substack{\lambda^* \leq \lambda \leq R \\ |\gamma| \leq 1}} e^{-B'\lambda} - \eta. \tag{11-1}$$

Let  $\Lambda > 0$  be a fixed parameter to be specified later. To bound the remaining sum over zeros, we apply partial summation using the quantity  $\mathcal{N}(\lambda)$ , defined in (8-5), over two different ranges: (i)  $\lambda^* \leq \lambda \leq \Lambda$  and (ii)  $\Lambda < \lambda \leq R$ .

For (i), partition the interval  $[\lambda^*, \Lambda]$  into  $M$  subintervals with sample points

$$\lambda^* = \Lambda_0 < \Lambda_1 < \Lambda_2 < \dots < \Lambda_M = \Lambda.$$

By partial summation, we see

$$\begin{aligned} Z_1 &:= \sum_{\chi \pmod{H}} \sum_{\substack{\lambda^* < \lambda \leq \Lambda \\ |\gamma| \leq 1}} e^{-B'\lambda} = \sum_{j=1}^M \sum_{\chi \pmod{H}} \sum_{\Lambda_{j-1} < \lambda \leq \Lambda_j} e^{-B'\lambda} \\ &\leq e^{-B'\Lambda_{M-1}} \mathcal{N}(\Lambda_M) + \sum_{j=1}^{M-1} (e^{-B'\Lambda_{j-1}} - e^{-B'\Lambda_j}) \mathcal{N}(\Lambda_j). \end{aligned}$$

By Theorem 8.1, we may choose  $\lambda^* = 0.2866$ . Furthermore, we select

$$\Lambda = 1, \quad M = 32, \quad \Lambda_r = \begin{cases} 0.286 + 0.001r, & 1 \leq r \leq 14, \\ 0.300 + 0.025(r - 14), & 15 \leq r \leq 22, \\ 0.5 + 0.05(r - 22), & 23 \leq r \leq 32, \end{cases}$$

and incorporate the estimates from Table 1 to bound  $\mathcal{N}(\cdot)$ , yielding  $Z_1 \leq 0.9926$ .

For (ii), apply partial summation along with Theorem 8.6. Since  $B' \geq 693 > 162$  and  $R = R(\eta)$  is sufficiently large, it follows that

$$Z_2 := \sum_{\chi \pmod{H}} \sum_{\substack{\Lambda < \lambda \leq R \\ |\gamma| \leq 1}} e^{-B'\lambda} \leq e^{188 - (B' - 162)R} + B' \int_{\Lambda}^{\infty} e^{188 - (B' - 162)\lambda} d\lambda$$

for  $\mathcal{L}$  sufficiently large depending on  $\eta$ . Evaluating the right-hand side with  $B' \geq 693$  and  $\Lambda = 1$ , we deduce  $Z_2 \leq 10^{-400}$ .



Incorporating (i) and (ii) into (11-1), we conclude

$$h_H \mathcal{L}^{-1} S \geq 1 - 2e^{-B'\lambda_1} - 0.9926 - 10^{-400} - 2\eta \geq 0.0073 - 2\eta$$

as  $\lambda_1 > 0.0875$  and  $B' \geq 693$ . Since  $\eta \in (0, 10^{-3}]$  is fixed and sufficiently small, we conclude  $h_H \mathcal{L}^{-1} S \gg 1$ . This completes the proof of Theorem 3.1.  $\square$

### 12. Proofs of Theorems 1.2–1.5

*Proof of Theorem 1.2.* Let  $Q(x, y) \in \mathbb{Z}[x, y]$  be a positive-definite primitive binary quadratic form of discriminant  $D$ . Let  $K = \mathbb{Q}(\sqrt{D})$ , and let  $L$  be the ring class field of the order of discriminant  $D$  in  $K$ . By Theorem 9.12 of [Cox 1989], the rational primes  $p \nmid D$  represented by  $Q$  are the primes which split in  $K$  that satisfy a certain Chebotarev condition in  $L$ . We have that  $D_K Q \leq |D|$ . The result follows.  $\square$

We now state a slightly weaker version of (3-2) and Theorem 1.1 which will be convenient for the remaining proofs. For positive integers  $n$ , let  $\omega(n) = \#\{p : p \mid n\}$  and  $\text{rad}(n) = \prod_{p \mid n} p$ .

**Theorem 12.1.** *Let  $L/F$  be a Galois extension of number fields with Galois group  $G$  and  $L \neq \mathbb{Q}$ , and let  $C$  be any conjugacy class of  $G$ . Let  $H$  be an abelian subgroup of  $G$  such that  $H \cap C$  is nonempty, and let  $K \neq \mathbb{Q}$  be the subfield of  $L$  fixed by  $H$ . Define*

$$M(L/K) := [L : K]^{3/2} n_K^{\omega(D_L)} \text{rad}(D_L)^{5/2}.$$

If  $(M(L/K)n_K)^{n_K}$  is sufficiently large and

$$x \gg [L : K]^{n_K} \text{rad}(D_L)^{n_K - 694} M(L/K)^{694n_K},$$

then

$$\pi_C(x, L/F) \gg \frac{(M(L/K)n_K)^{-15n_K/2}}{[L : K]} \frac{x}{\log x}.$$

Consequently, for all  $L/F$ , we have that

$$P(C, L/F) \ll [L : K]^{n_K} \text{rad}(D_L)^{n_K - 694} M(L/K)^{694n_K}.$$

*Proof.* Let  $\mathcal{P}(L/K)$  be the set of rational primes  $p$  such that there is a prime ideal  $\mathfrak{p}$  of  $K$  such that  $\mathfrak{p} \mid p$  and  $\mathfrak{p}$  ramifies in  $L$ . By [Serre 1981, Proposition 6],  $D_K \leq (n_K)^{n_K \omega(D_K)} \text{rad}(D_K)^{n_K - 1}$ . Since  $L/K$  is abelian, we have by [Murty et al. 1988, Proposition 2.5] that

$$Q \leq \left( [L : K] \prod_{p \in \mathcal{P}(L/K)} p \right)^{2n_K}.$$

The primes in  $\mathcal{P}(L/K)$  and the primes dividing  $D_K$  all divide  $D_L$ . Since  $K \neq \mathbb{Q}$ , we have  $\omega(D_K) \geq 1$  and  $n_K \geq 2$ . Thus the result follows from Theorem 1.1, and in particular (3-2).  $\square$

**Remark.** For comparison, if one uses [Serre 1981, Proposition 6] to bound  $D_L$ , then (1-5) implies that  $P(C, L/F) \ll (n_L^{\omega(D_L)} \text{rad}(D_L))^{40n_L}$ . We can replace  $\omega(D_L)$  with 1 if  $L/\mathbb{Q}$  is Galois.

**12A.  $\text{GL}_2$  extensions.** We now review some facts about  $\text{GL}_2$  extensions of  $\mathbb{Q}$  and class functions to prove Theorems 1.3–1.5. Let

$$f(z) = \sum_{n=1}^{\infty} a_f(n)e^{2\pi inz} \in \mathbb{Z}[[e^{2\pi iz}]]$$

be a non-CM newform of even weight  $k \geq 2$  and level  $N \geq 1$ . Let  $\ell$  be a prime, and let  $\mathbb{F}_\ell$  be the finite field of  $\ell$  elements. By [Deligne 1971], there exists a representation

$$\rho_{f,\ell} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$$

with the property that if  $p \nmid \ell N$  and  $\sigma_p$  is a Frobenius element at  $p$  in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , then  $\rho_{f,\ell}$  is unramified at  $p$ ,  $\text{tr } \rho_{f,\ell}(\sigma_p) \equiv a_f(p) \pmod{\ell}$ , and  $\det \rho_{f,\ell}(\sigma_p) \equiv p^{k-1} \pmod{\ell}$ . Let  $L = L_{f,\ell}$  be the subfield of  $\overline{\mathbb{Q}}$  fixed by the kernel of  $\rho_{f,\ell}$ . Then  $L/\mathbb{Q}$  is a Galois extension unramified outside  $\ell N$  whose Galois group  $\text{Gal}(L/\mathbb{Q})$  is isomorphic to a subgroup of

$$G = G_{k,\ell} = \{A \in \text{GL}_2(\mathbb{F}_\ell) : \det A \text{ is a } (k-1)\text{-th power in } \mathbb{F}_\ell^\times\}.$$

If  $\ell$  is sufficiently large, then the representation is surjective, in which case

$$\text{Gal}(L/\mathbb{Q}) \cong G. \tag{12-1}$$

When  $k = 2$  and the level is  $N$ ,  $f$  is necessarily the newform of a non-CM elliptic curve  $E/\mathbb{Q}$  of conductor  $N$ . In this case, we write  $\rho_{f,\ell} = \rho_{E,\ell}$ , and  $L$  is the  $\ell$ -division field  $\mathbb{Q}(E[\ell])$ . It is conjectured that  $\text{Gal}(L/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_\ell)$  for all  $\ell > 37$ . When  $E/\mathbb{Q}$  is non-CM and has squarefree level, it follows from the work of Mazur [1978] that  $\ker \tilde{\rho}_{E,\ell} \cong \text{GL}_2(\mathbb{F}_\ell)$  for all  $\ell \geq 11$ .

**Lemma 12.2.** *Let  $L/\mathbb{Q}$  be a  $\text{GL}_2(\mathbb{F}_\ell)$  extension which is unramified outside of  $\ell N$  for some  $N \geq 1$ . Let  $C \subset \text{GL}_2(\mathbb{F}_\ell)$  be a conjugacy class intersecting the subgroup  $D$  of diagonal matrices. There exists a prime  $p \nmid \ell N$  such that*

$$p \ll \ell^{(5209+1542\omega(N))\ell^2} \text{rad}(N)^{1737\ell(\ell+1)} \quad \text{and} \quad \left[ \frac{L/\mathbb{Q}}{p} \right] = C.$$

*Proof.* If  $K = L^D$  is the subfield of  $L$  fixed by  $D$ , then  $[L : K] = (\ell - 1)^2$  and  $[K : \mathbb{Q}] = \ell(\ell + 1)$ . Moreover,  $\text{rad}(D_L) \mid \ell \text{rad}(N)$ . The result now follows immediately from Theorem 12.1. □

*Proof of Theorem 1.3.* It follows from the proof of [Murty 1994, Theorem 4] and Mazur’s torsion theorem [1978] that it suffices to consider  $\ell \geq 11$ . Let  $L = \mathbb{Q}(E[\ell])$

be the  $\ell$ -division field of  $E/\mathbb{Q}$ . For  $p \nmid \ell N_E$ , we have that  $E(\mathbb{F}_p)$  has an element of order  $\ell$  if and only if

$$\text{tr } \rho_{\ell,E}(\sigma_p) \equiv \det \rho_{\ell,E}(\sigma_p) + 1 \pmod{\ell}, \tag{12-2}$$

where  $\sigma_p$  is a Frobenius automorphism at  $p$  in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . If  $\text{Gal}(L/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_\ell)$ , then the  $\rho_{\ell,E}(\sigma_p) \in \text{GL}_2(\mathbb{F}_\ell)$  which satisfy (12-2) form a union of conjugacy classes in  $\text{GL}_2(\mathbb{F}_\ell)$  which includes the identity element. The subgroup  $D$  of diagonal matrices is a maximal abelian subgroup of  $\text{GL}_2(\mathbb{F}_\ell)$ . Thus  $\pi_{\{\text{id}\}}(x, L/\mathbb{Q})$  is a lower bound for the function that counts the primes  $p \leq x$  such that  $p \nmid \ell N_E$  and  $\ell \mid \#E(\mathbb{F}_p)$ . Since  $\text{rad}(D_L) \mid \ell \text{rad}(N)$ , Lemma 12.2 implies the claimed result.

Suppose now that  $\text{Gal}(L/\mathbb{Q})$  is not isomorphic to  $\text{GL}_2(\mathbb{F}_\ell)$ . The possible cases are described in the proof of [Murty 1994, Theorem 4]. Applying similar analysis to all of these cases, one sees that the above case gives the largest upper bound for the least prime  $p$  such that  $\ell \mid \#E(\mathbb{F}_p)$ .  $\square$

We require some basic results on class functions (see [Serre 1981]) for the proof of Theorem 1.5. Let  $L/F$  be a Galois extension of number fields with Galois group  $G$ , and let  $\phi : G \rightarrow \mathbb{C}$  be a class function. For each prime ideal  $\mathfrak{p}$  of  $F$ , choose any prime ideal  $\mathfrak{P}$  of  $L$  dividing  $\mathfrak{p}$ . Let  $D_{\mathfrak{P}}$  and  $I_{\mathfrak{P}}$  be the decomposition and inertia subgroups of  $G$  at  $\mathfrak{p}$ , respectively. We then have a distinguished Frobenius element  $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}/I_{\mathfrak{P}}$ . For each  $m \geq 1$ , let

$$\phi(\text{Frob}_{\mathfrak{p}}^m) = \frac{1}{|I_{\mathfrak{P}}|} \sum_{\substack{g \in D_{\mathfrak{P}} \\ g I_{\mathfrak{P}} = \sigma_{\mathfrak{P}}^m \in D_{\mathfrak{P}}/I_{\mathfrak{P}}}} \phi(g).$$

Note that  $\phi(\text{Frob}_{\mathfrak{p}}^m)$  is independent of the aforementioned choice of  $\mathfrak{P}$ . If  $\mathfrak{p}$  is unramified in  $L$ , this definition agrees with the value of  $\phi$  on the conjugacy class  $\text{Frob}_{\mathfrak{p}}^m$  of  $G$ . For  $x \geq 2$ , we define

$$\pi_{\phi}(x) = \sum_{\substack{\mathfrak{p} \text{ unramified in } L \\ N_{F/\mathbb{Q}} \mathfrak{p} \leq x}} \phi(\text{Frob}_{\mathfrak{p}}), \quad \tilde{\pi}_{\phi}(x) = \sum_{\substack{\mathfrak{p} \text{ unramified in } L \\ N_{F/\mathbb{Q}} \mathfrak{p}^m \leq x}} \frac{1}{m} \phi(\text{Frob}_{\mathfrak{p}}^m).$$

Let  $C \subset G$  be stable under conjugation, and let  $\mathbf{1}_C : G \rightarrow \{0, 1\}$  be the class function given by the indicator function of  $C$ . Now, define  $\pi_C(x, L/F) = \pi_{\mathbf{1}_C}(x)$  and  $\tilde{\pi}_C(x, L/F) = \tilde{\pi}_{\mathbf{1}_C}(x)$ . Serre [1981, Proposition 7] proved that if  $x \geq 2$ , then

$$|\pi_C(x, L/F) - \tilde{\pi}_C(x, L/F)| \leq 4n_F((\log D_L)/n_L + \sqrt{x}). \tag{12-3}$$

By arguments similar to the proof of Theorem 1.1, we have that if  $A$  is an abelian subgroup of  $G$  such that  $A \cap C$  is nonempty, then  $\tilde{\pi}_C(x, L/F) = \tilde{\pi}_{\text{Ind}_A^G C}(x, L/L^A)$ .

*Proof of Theorem 1.5.* Let  $\ell$  be an odd prime such that (12-1) is satisfied. Assuming  $\gcd(k - 1, \ell - 1) = 1$ , we have  $G \cong \text{GL}_2(\mathbb{F}_\ell)$ . To prove the theorem, we consider

$$\pi_f(x; \ell, a) := \#\{p \leq x : p \nmid \ell N, a_f(p) \equiv a \pmod{\ell}, \\ \ell \text{ splits in } \mathbb{Q}((a_f(p)^2 - 4p^{k-1})^{1/2})\}.$$

Note that for  $p \nmid \ell N$ ,  $a_f(p)^2 - 4p^{k-1} = \text{tr}(\rho_{f,\ell}(\sigma_p)) - 4 \det(\rho_{f,\ell}(\sigma_p))^2$ , where  $\sigma_p$  is Frobenius at  $p$  in  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . The subset  $C \subset G$  given by

$$C = \{A \in G : \text{tr}(A) \equiv a \pmod{\ell}, \text{tr}(A)^2 - 4 \det(A) \text{ is a square in } \mathbb{F}_\ell^\times\}$$

is a conjugacy-invariant subset of  $G$ , so we bound  $\tilde{\pi}_C(x, L/\mathbb{Q})$ . Let  $B \subset G$  denote the subgroup of upper triangular matrices; the condition that  $\text{tr}(A)^2 - 4 \det(A)$  is a square in  $\mathbb{F}_\ell^\times$  means that  $\sigma_p$  is conjugate to an element in  $B$ . If  $\Gamma$  is a maximal set of elements  $\gamma \in B$  which are nonconjugate in  $G$  with  $\text{tr}(\gamma) \equiv a \pmod{q}$ , then  $C = \bigsqcup_{\gamma \in \Gamma} C_G(\gamma)$ , where  $C_G(\gamma)$  denotes the conjugacy class of  $\gamma$  in  $G$ . Since  $B$  is a subgroup of  $G$  with the property that every element of  $C$  is conjugate to an element of  $B$ , it follows from [Zywina 2015, Lemma 2.6] that

$$\tilde{\pi}_C(x, L/\mathbb{Q}) = \sum_{\gamma \in \Gamma} \frac{\tilde{\pi}_{C_B(\gamma)}(x, L/L^B)}{[\text{Cent}_G(\gamma) : \text{Cent}_B(\gamma)]},$$

where  $\text{Cent}_G(\gamma)$  denotes the centralizer of  $\gamma$  in  $G$  (and similarly for  $B$ ). If  $C_1 = \bigsqcup_{\gamma \in \Gamma \text{ nonscalar}} C_B(\gamma)$ , then it follows that  $\tilde{\pi}_C(x; L/\mathbb{Q}) \geq \frac{1}{|G|} \tilde{\pi}_{C_1}(x, L/L^B)$  for all  $x \geq 2$ .

*Case 1:  $\ell N$  sufficiently large,  $a \not\equiv 0 \pmod{\ell}$ .* Let  $U$  be the normal subgroup of  $B$  consisting of the matrices whose diagonal entries are both 1. We observe that  $U \cdot C_1 \subset C_1$ ; therefore, using arguments from [Zywina 2015, Lemma 2.6], we have that  $\tilde{\pi}_{C_1}(x, L/L^B) = \tilde{\pi}_{C_2}(x, L^U/L^B)$  for  $x \geq 2$ , where  $C_2$  is the image of  $C_1 \cap B$  in  $B/U$ . It follows from (12-3) and Theorem 12.1 that if  $\ell N$  is sufficiently large and  $x$  is bounded below as in Theorem 12.1, then

$$\tilde{\pi}_{C_2}(x, L^U/L^B) > 0 \quad \text{if and only if} \quad \pi_{C_2}(x, L^U/L^B) > 0. \tag{12-4}$$

It is straightforward to compute  $n_{L^B} = \ell + 1$  and  $[L^U : L^B] = (\ell - 1)^2$ . Since  $L^U/L^B$  is abelian and all of the ramified primes divide  $\ell N$ , the theorem now follows from Theorem 12.1.

*Case 2:  $\ell N$  sufficiently large,  $a \equiv 0 \pmod{\ell}$ .* Let  $H$  be the normal subgroup of  $B$  consisting of matrices whose eigenvalues are both equal. We have that  $H \cdot C_1 \subset C_1$  since multiplying a trace zero matrix by a scalar does not change the trace. Let  $C_3$  be the image of  $C_1 \cap B$  in  $B/H$ . The arguments are now the same as in the previous case, with  $L^H$  replacing  $L^U$ . In fact, since  $B/H \cong \mathbb{F}_\ell^\times$  is abelian of order

$\ell - 1$  and  $C_3$  is a singleton, we obtain a slightly better exponent than what is stated in Theorem 1.5 when  $a \equiv 0 \pmod{\ell}$ .

*Case 3:  $\ell N$  not sufficiently large.* Let  $A_2 = U$  and  $A_3 = H$ . The lower bound for  $\pi_{C_i}(x, L^{A_i}/L^B)$  ( $i = 2$  or  $3$ ) given by Theorem 12.1 only holds when  $\ell N$  is sufficiently large. Therefore, when  $\ell N$  is not sufficiently large, we cannot verify (12-4) using Theorem 12.1. For these finitely many exceptional cases, we use Weiss' lower bound on  $\pi_{C_i}(x, L^{A_i}/L^B)$  that follows from [Weiss 1983, Theorem 5.2], which holds uniformly for all choices of  $N$  and  $\ell$ . Continuing the proof as in Case 1 (this requires us to take  $c_{10}$  sufficiently small and  $c_{11}$  to be sufficiently large in [Weiss 1983, Theorem 5.2]), we see that the least prime  $p \nmid \ell N$  such that  $a_f(p) \equiv a \pmod{\ell}$  is absolutely bounded in all of the finitely many exceptional cases. This proves the theorem.  $\square$

### Acknowledgements

The authors thank John Friedlander, V. Kumar Murty, Robert Lemke Oliver, Ken Ono, David Zureick-Brown, and the anonymous referee for their comments and suggestions. Thorner conducted work on this paper while visiting Centre de Recherches Mathématiques (hosted by Chantal David, Andrew Granville, and Dimitris Koukoulopoulos) and Stanford University (hosted by Robert Lemke Oliver and Kannan Soundararajan); he is grateful to these departments and hosts for providing a vibrant work environment. Zaman was supported in part by an NSERC PGS-D scholarship.

### References

- [Ahn and Kwon 2014] J.-H. Ahn and S.-H. Kwon, "Some explicit zero-free regions for Hecke  $L$ -functions", *J. Number Theory* **145** (2014), 433–473. MR Zbl
- [Bach and Sorenson 1996] E. Bach and J. Sorenson, "Explicit bounds for primes in residue classes", *Math. Comp.* **65**:216 (1996), 1717–1735. MR Zbl
- [Cox 1989] D. A. Cox, *Primes of the form  $x^2 + ny^2$ : Fermat, class field theory and complex multiplication*, Wiley, New York, 1989. MR Zbl
- [Deligne 1971] P. Deligne, "Formes modulaires et représentations  $l$ -adiques", exposé 355, pp. 139–172 in *Séminaire Bourbaki*, 1968/1969, Lecture Notes in Math. **175**, Springer, Berlin, 1971. MR Zbl
- [Ditchen 2013] J. Ditchen, "On the average distribution of primes represented by binary quadratic forms", preprint, 2013. arXiv
- [DLM 2010] F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller, and B. V. Saunders (editors), "Digital library of mathematical functions", electronic reference, National Institute of Standards and Technology, 2010, available at <http://dlmf.nist.gov/>.
- [Duke 1989] W. Duke, "Some problems in multidimensional analytic number theory", *Acta Arith.* **52**:3 (1989), 203–228. MR Zbl

- [Fogels 1962a] E. Fogels, “On the zeros of Hecke’s  $L$ -functions, I”, *Acta Arith.* **7**:2 (1962), 87–106. MR Zbl
- [Fogels 1962b] E. Fogels, “On the zeros of Hecke’s  $L$ -functions, II”, *Acta Arith.* **7**:2 (1962), 131–147. MR Zbl
- [Gallagher 1970] P. X. Gallagher, “A large sieve density estimate near  $\sigma = 1$ ”, *Invent. Math.* **11** (1970), 329–339. MR Zbl
- [Golod and Šafarevič 1964] E. S. Golod and I. R. Šafarevič, “On the class field tower”, *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), 261–272. In Russian. MR Zbl
- [Graham 1977] S. W. Graham, *Applications of sieve methods*, Ph.D. thesis, University of Michigan, 1977, available at <http://search.proquest.com/docview/302861551>.
- [Graham 1978] S. Graham, “An asymptotic estimate related to Selberg’s sieve”, *J. Number Theory* **10**:1 (1978), 83–94. MR Zbl
- [Heath-Brown 1992] D. R. Heath-Brown, “Zero-free regions for Dirichlet  $L$ -functions, and the least prime in an arithmetic progression”, *Proc. London Math. Soc.* (3) **64**:2 (1992), 265–338. MR Zbl
- [Ihara 2006] Y. Ihara, “On the Euler–Kronecker constants of global fields and primes with small norms”, pp. 407–451 in *Algebraic geometry and number theory*, edited by V. Ginzburg, Progr. Math. **253**, Birkhäuser, Boston, 2006. MR Zbl
- [Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004. MR Zbl
- [Jutila 1970] M. Jutila, “A new estimate for Linnik’s constant”, *Ann. Acad. Sci. Fenn. Ser. A I Math.* **471** (1970), 1–8. MR Zbl
- [Jutila 1977] M. Jutila, “On Linnik’s constant”, *Math. Scand.* **41**:1 (1977), 45–62. MR Zbl
- [Kadiri 2012] H. Kadiri, “Explicit zero-free regions for Dedekind zeta functions”, *Int. J. Number Theory* **8**:1 (2012), 125–147. MR Zbl
- [Kadiri and Ng 2012] H. Kadiri and N. Ng, “Explicit zero density theorems for Dedekind zeta functions”, *J. Number Theory* **132**:4 (2012), 748–775. MR Zbl
- [Kolesnik and Straus 1983] G. Kolesnik and E. G. Straus, “On the sum of powers of complex numbers”, pp. 427–442 in *Studies in pure mathematics*, edited by P. Erdős, Birkhäuser, Basel, 1983. MR Zbl
- [Kowalski and Michel 2002] E. Kowalski and P. Michel, “Zeros of families of automorphic  $L$ -functions close to 1”, *Pacific J. Math.* **207**:2 (2002), 411–431. MR Zbl
- [Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, “Effective versions of the Chebotarev density theorem”, pp. 409–464 in *Algebraic number fields:  $L$ -functions and Galois properties* (Durham, UK, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR Zbl
- [Lagarias et al. 1979] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, “A bound for the least prime ideal in the Chebotarev density theorem”, *Invent. Math.* **54**:3 (1979), 271–296. MR Zbl
- [Lamzouri et al. 2015] Y. Lamzouri, X. Li, and K. Soundararajan, “Conditional bounds for the least quadratic non-residue and related problems”, *Math. Comp.* **84**:295 (2015), 2391–2412. MR Zbl
- [Li 2012] X. Li, “The smallest prime that does not split completely in a number field”, *Algebra Number Theory* **6**:6 (2012), 1061–1096. MR Zbl
- [Linnik 1944a] U. V. Linnik, “On the least prime in an arithmetic progression, I: The basic theorem”, *Rec. Math. [Mat. Sbornik] N.S.* **15(57)**:2 (1944), 139–178. MR Zbl
- [Linnik 1944b] U. V. Linnik, “On the least prime in an arithmetic progression, II: The Deuring–Heilbronn phenomenon”, *Rec. Math. [Mat. Sbornik] N.S.* **15(57)**:3 (1944), 347–368. MR Zbl

- [Makai 1964] E. Makai, “On a minimum problem, II”, *Acta Math. Acad. Sci. Hungar.* **15** (1964), 63–66. MR Zbl
- [Mazur 1978] B. Mazur, “Rational isogenies of prime degree”, *Invent. Math.* **44**:2 (1978), 129–162. MR Zbl
- [Milne 2013] J. S. Milne, “Class field theory (version 4.02)”, course notes, 2013, available at <http://www.jmilne.org/math/CourseNotes/CFT.pdf>.
- [Murty 1994] V. K. Murty, “The least prime which does not split completely”, *Forum Math.* **6**:5 (1994), 555–565. MR Zbl
- [Murty et al. 1988] M. R. Murty, V. K. Murty, and N. Saradha, “Modular forms and the Chebotarev density theorem”, *Amer. J. Math.* **110**:2 (1988), 253–281. MR Zbl
- [Ono and Soundararajan 1997] K. Ono and K. Soundararajan, “Ramanujan’s ternary quadratic form”, *Invent. Math.* **130**:3 (1997), 415–454. MR Zbl
- [Rademacher 1959] H. Rademacher, “On the Phragmén–Lindelöf theorem and some applications”, *Math. Z.* **72**:1 (1959), 192–204. MR Zbl
- [Serre 1981] J.-P. Serre, “Quelques applications du théorème de densité de Chebotarev”, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. MR Zbl
- [Stark 1974] H. M. Stark, “Some effective cases of the Brauer–Siegel theorem”, *Invent. Math.* **23** (1974), 135–152. MR Zbl
- [Weiss 1980] A. R. Weiss, *The least prime ideal with prescribed decomposition behaviour*, Ph.D. thesis, Ohio State University, 1980, available at <http://search.proquest.com/docview/303045630>.
- [Weiss 1983] A. Weiss, “The least prime ideal”, *J. Reine Angew. Math.* **338** (1983), 56–94. MR Zbl
- [Xylouris 2011] T. Xylouris, “On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet  $L$ -functions”, *Acta Arith.* **150**:1 (2011), 65–91. MR Zbl
- [Zaman 2016a] A. Zaman, “Explicit estimates for the zeros of Hecke  $L$ -functions”, *J. Number Theory* **162** (2016), 312–375. MR Zbl
- [Zaman 2016b] A. Zaman, “On the least prime ideal and Siegel zeros”, *Int. J. Number Theory* **12**:8 (2016), 2201–2229. MR Zbl
- [Zaman 2017a] A. Zaman, *Analytic estimates for the Chebotarev density theorem and their applications*, Ph.D. thesis, University of Toronto, 2017, available at <http://tinyurl.com/zamanthesis>.
- [Zaman 2017b] A. Zaman, “Bounding the least prime ideal in the Chebotarev density theorem”, *Funct. Approx. Comment. Math.* (online publication March 2017).
- [Zywina 2015] D. Zywina, “Bounds for the Lang–Trotter conjectures”, pp. 235–256 in *SCHOLAR: a scientific celebration highlighting open lines of arithmetic research*, edited by A. C. Cojocaru et al., Contemp. Math. **655**, American Mathematical Society, Providence, RI, 2015. MR Zbl

Communicated by Andrew Granville

Received 2016-05-12

Revised 2016-10-25

Accepted 2017-03-10

[jthorner@stanford.edu](mailto:jthorner@stanford.edu)

*Department of Mathematics, Stanford University,  
Building 380, Sloan Mathematical Center,  
Stanford, CA 94305, United States*

[asif@math.toronto.edu](mailto:asif@math.toronto.edu)

*Department of Mathematics, University of Toronto,  
Room 6290, 40 St. George St., Toronto, ON M5S 2E4, Canada*





# Modular curves of prime-power level with infinitely many rational points

Andrew V. Sutherland and David Zywina

For each open subgroup  $G$  of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  containing  $-I$  with full determinant, let  $X_G/\mathbb{Q}$  denote the modular curve that loosely parametrizes elliptic curves whose Galois representation, which arises from the Galois action on its torsion points, has image contained in  $G$ . Up to conjugacy, we determine a complete list of the 248 such groups  $G$  of prime power level for which  $X_G(\mathbb{Q})$  is infinite. For each  $G$ , we also construct explicit maps from each  $X_G$  to the  $j$ -line. This list consists of 220 modular curves of genus 0 and 28 modular curves of genus 1. For each prime  $\ell$ , these results provide an explicit classification of the possible images of  $\ell$ -adic Galois representations arising from elliptic curves over  $\mathbb{Q}$  that is complete except for a finite set of exceptional  $j$ -invariants.

## 1. Introduction

Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and denote its  $j$ -invariant by  $j_E$ . For each positive integer  $N$ , let  $E[N]$  denote the  $N$ -torsion subgroup of  $E(\bar{\mathbb{Q}})$ , where  $\bar{\mathbb{Q}}$  is a fixed algebraic closure of  $\mathbb{Q}$ . The natural action of the absolute Galois group  $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  on  $E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$  induces a Galois representation

$$\rho_{E,N} : \mathrm{Gal}_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

After choosing compatible bases for the torsion subgroups  $E[N]$ , these representations determine a Galois representation

$$\rho_E : \mathrm{Gal}_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

whose composition with the projection  $\mathrm{GL}_2(\hat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  given by reduction modulo  $N$  is equal to  $\rho_{E,N}$  for each  $N$ . The images of  $\rho_{E,N}$  and  $\rho_E$  are uniquely determined up to conjugacy in  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  and  $\mathrm{GL}_2(\hat{\mathbb{Z}})$ , respectively. If  $E$  does not have complex multiplication (CM), then  $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$  is an open subgroup of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$ , by Serre's [1972] open image theorem, hence of finite index in  $\mathrm{GL}_2(\hat{\mathbb{Z}})$ .

---

Sutherland was supported by NSF grants DMS-1115455 and DMS-1522526.

*MSC2010:* primary 14G35; secondary 11F80, 11G05.

*Keywords:* modular curves, elliptic curves, Galois representations.

Let  $G$  be an open subgroup of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  that satisfies  $\det(G) = \hat{\mathbb{Z}}^\times$  and  $-I \in G$ . Let  $N$  be the least positive integer such that  $G$  is the inverse image of its image under the reduction map  $\mathrm{GL}_2(\hat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ ; we call  $N$  the *level* of  $G$ .

Associated to  $G$  is a modular curve  $X_G/\mathbb{Q}$ ; one can define  $X_G$  as the generic fiber of the smooth proper  $\mathbb{Z}[1/N]$ -scheme that is the coarse moduli space for the algebraic stack  $\mathcal{M}_{\bar{G}}[1/N]$  in the sense of [Deligne and Rapoport 1973, §IV], where  $\bar{G}$  denotes the image of  $G$  under reduction modulo  $N$ . See Section 2 for some background on  $X_G$  and an alternate description; in particular, it is a smooth projective geometrically integral curve defined over  $\mathbb{Q}$ .

When  $G = \mathrm{GL}_2(\hat{\mathbb{Z}})$ , the modular curve  $X_G$  is the  $j$ -line  $\mathbb{P}_{\mathbb{Q}}^1 = \mathbb{A}_{\mathbb{Q}}^1 \cup \{\infty\}$ . If  $G$  and  $G'$  are open subgroups of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  with  $\det(G) = \det(G') = \hat{\mathbb{Z}}^\times$  and  $-I \in G, G'$  such that  $G \subseteq G'$ , then there is a natural morphism  $X_G \rightarrow X_{G'}$  of degree  $[G' : G]$ . In particular, with  $G' = \mathrm{GL}_2(\hat{\mathbb{Z}})$ , we have a morphism

$$\pi_G : X_G \rightarrow \mathbb{P}_{\mathbb{Q}}^1 = \mathbb{A}_{\mathbb{Q}}^1 \cup \{\infty\}$$

of degree  $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : G]$  from  $X_G$  to the  $j$ -line.

The key property for our applications is that for an elliptic curve  $E/\mathbb{Q}$  with  $j_E \notin \{0, 1728\}$ , the group  $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$  is conjugate in  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  to a subgroup of  $G$  if and only if  $j_E$  is an element of  $\pi_G(X_G(\mathbb{Q}))$ ; see Proposition 2.7. This property requires  $-I \in G$ , since there is always an elliptic curve  $E$  with any given rational  $j$ -invariant such that  $-I \in \rho_E(\mathrm{Gal}_{\mathbb{Q}})$ ; it also requires  $\det(G) = \hat{\mathbb{Z}}^\times$ , since  $\det(\rho_E(\mathrm{Gal}_{\mathbb{Q}})) = \hat{\mathbb{Z}}^\times$ , and that  $G$  contain an element corresponding to complex conjugation.

We are interested in those groups  $G$  for which  $X_G$  has infinitely many rational points; equivalently, for which there are infinitely many elliptic curves  $E/\mathbb{Q}$ , with distinct  $j$ -invariants, such that  $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$  is conjugate to a subgroup of  $G$ . We need only consider modular curves  $X_G$  of genus 0 or 1 since otherwise  $X_G(\mathbb{Q})$  is finite by Faltings' theorem [1983].

In this article, we give an explicit description of all such subgroups  $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$  for which the modular curve  $X_G$  has infinitely many rational points in the special case where the level  $N$  of  $G$  is a *prime power*; we also give an explicit model for  $X_G$  and the morphism  $\pi_G$ . We need only describe the groups  $G$  up to conjugacy in  $\mathrm{GL}_2(\hat{\mathbb{Z}})$ . For notational simplicity, we define the genus of  $G$  to be the genus of the corresponding curve  $X_G$ .

**Theorem 1.1.** *Up to conjugacy, there are 248 open subgroups  $G$  of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  of prime power level satisfying  $-I \in G$  and  $\det(G) = \hat{\mathbb{Z}}^\times$  for which  $X_G$  has infinitely many rational points. Of these 248 groups, there are 220 of genus 0 and 28 of genus 1.*

The 220 subgroups of genus 0 in Theorem 1.1 are given in Tables 1, 2 and 3 of the online supplement. For such a group  $G$  of genus 0, we also describe the

morphism  $\pi_G$ . More precisely, we give a rational function  $J(t) \in \mathbb{Q}(t)$  such that the function field of  $X_G$  is of the form  $\mathbb{Q}(t)$  and the morphism from  $X_G$  to the  $j$ -line is given by the equation  $j = J(t)$ . In particular, if  $E/\mathbb{Q}$  is an elliptic curve with  $j_E \notin \{0, 1728\}$ , then  $\rho_E(\text{Gal}_{\mathbb{Q}})$  is conjugate to a subgroup of  $G$  if and only if  $j_E = J(t_0)$  for some  $t_0 \in \mathbb{Q} \cup \{\infty\}$ .

The 28 subgroups of genus 1 in Theorem 1.1 are listed in Table 4 of the online supplement; their levels are all powers of 2 except for a group of level 11 whose image in  $\text{GL}_2(\mathbb{Z}/11\mathbb{Z})$  is the normalizer of a nonsplit Cartan subgroup. For such a group  $G$  of genus 1, we give a Weierstrass model for  $X_G$  and the morphism  $\pi_G$  to the  $j$ -line.

**Example 1.2.** Up to conjugacy, there is a unique subgroup  $G \subseteq \text{GL}_2(\hat{\mathbb{Z}})$  of genus 0 and level 27 given by Theorem 1.1. It has label  $27A^0\text{-}27a$  in our classification, and we may choose it so that the image of  $G$  in  $\text{GL}_2(\mathbb{Z}/27\mathbb{Z})$  is generated by the matrices  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ,  $\begin{pmatrix} 2 & 1 \\ 9 & 5 \end{pmatrix}$  and  $\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$ . Using Table 1 of the online supplement, associated to  $G$  is the rational function

$$J(t) = F_3(F_2(F_1(t))) = \frac{(t^3 + 3)^3(t^9 + 9t^6 + 27t^3 + 3)^3}{t^3(t^6 + 9t^3 + 27)},$$

where  $F_1(t) = t^3$ ,  $F_2(t) = t(t^2 + 9t + 27)$  and  $F_3(t) = (t + 3)^3(t + 27)/t$ . That  $J(t)$  is the composition of three rational functions reflects the fact that the morphism  $\pi_G$  factors as  $X_G \rightarrow X_{G'} \rightarrow X_{G''} \rightarrow \mathbb{P}_{\mathbb{Q}}^1$  for some groups  $G \subsetneq G' \subsetneq G'' \subsetneq \text{GL}_2(\hat{\mathbb{Z}})$ . The groups  $G'$  and  $G''$  have labels  $9B^0\text{-}9a$  and  $3B^0\text{-}3a$ , respectively, and can also be found in Table 1 of the online supplement.

**Remark 1.3.** In contrast to the case of prime power level, in general there are infinitely many open subgroups  $G$  of  $\text{GL}_2(\hat{\mathbb{Z}})$  satisfying  $-I \in G$  and  $\det(G) = \hat{\mathbb{Z}}^\times$  for which the modular curve  $X_G$  has infinitely many rational points. Let us explicitly construct just one of several infinite families of such groups  $G$ .

Let  $D$  be the discriminant of a quadratic number field and let  $\chi_D : \hat{\mathbb{Z}}^\times \rightarrow \{\pm 1\}$  be the continuous quadratic character arising from the corresponding Dirichlet character. Let  $\varepsilon : \text{GL}_2(\hat{\mathbb{Z}}) \rightarrow \{\pm 1\}$  be the character obtained by composing the reduction map  $\text{GL}_2(\hat{\mathbb{Z}}) \rightarrow \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$  with the unique nontrivial homomorphism  $\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \{\pm 1\}$ . Define the group

$$G_D := \{A \in \text{GL}_2(\hat{\mathbb{Z}}) : \varepsilon(A) = \chi_D(\det(A))\};$$

it is an open subgroup of  $\text{GL}_2(\hat{\mathbb{Z}})$  of index 2 containing  $-I$  with  $\det(G_D) = \hat{\mathbb{Z}}^\times$  whose level is  $|D|$  or  $2|D|$ , depending on whether  $D \equiv 0 \pmod{4}$  or  $D \equiv 1 \pmod{4}$ . For  $D \neq D'$ , the groups  $G_D$  and  $G_{D'}$  are not conjugate in  $\text{GL}_2(\hat{\mathbb{Z}})$ .

The modular curve  $X_{G_D}$  has genus 0 and a rational point (it has a unique, hence rational, cusp); the function field of  $X_{G_D}$  is of the form  $\mathbb{Q}(t)$  with the map to the  $j$ -line given by  $J(t) = Dt^2 + 1728$ . Each  $X_{G_D}$  is a  $\mathbb{Q}(\sqrt{D})$ -twist of the modular curve

$X_G$  corresponding to the unique index 2 subgroup  $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$  whose reduction has index 2 in  $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ ; it has label  $2A^0-2a$  in our classification and can be found in Table 3 (see the online supplement), along with its map to the  $j$ -line, which is  $J(t) = t^2 + 1728$ .

In general, if  $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$  is a fixed congruence subgroup of level  $N$  and index  $m$  containing  $-I$ , there are infinitely many nonconjugate open subgroups  $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$  of index  $M$  containing  $-I$  with  $\det(G) = \hat{\mathbb{Z}}^\times$  whose reductions modulo  $N$  coincide with that of  $\Gamma$  upon intersection with  $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ . The levels  $M$  of these groups  $G$  may be arbitrarily large multiples of  $N$  (and divisible by arbitrarily large primes). The corresponding modular curves  $X_G/\mathbb{Q}$  are nonisomorphic, but for each  $X_G$  there is a cyclotomic field  $\mathbb{Q}(\zeta_M)$  over which  $X_G$  becomes isomorphic to the modular curve  $X_\Gamma/\mathbb{Q}(\zeta_N)$  (the quotient of the extended upper half plane by the action of  $\Gamma$ ) after base change; as in our example, the  $X_G$  form an infinite family of twists.

**1A.  $\ell$ -adic representations.** Fix a prime  $\ell$ . Define the set

$$\mathcal{J}_\ell := \bigcup_G (\pi_G(X_G(\mathbb{Q})) \cap \mathbb{Q})$$

of rational numbers, where  $G$  varies over the open subgroups of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  whose level is a power of  $\ell$  and satisfies  $-I \in G$  and  $\det(G) = \hat{\mathbb{Z}}^\times$ , and for which  $X_G(\mathbb{Q})$  is finite. Note that the set  $\mathcal{J}_\ell$  contains the 13  $j$ -invariants of CM elliptic curves over  $\mathbb{Q}$ : for  $n \geq 1$  each CM  $j$ -invariant corresponds to points on at least one of the modular curves  $X_s^+(\ell^n)$ ,  $X_{\mathrm{ns}}^+(\ell^n)$ ,  $X_0(\ell^n)$ , and for sufficiently large  $n$  these curves have genus at least 2, hence finitely many rational points (by Faltings' theorem).

For an elliptic curve  $E/\mathbb{Q}$ , let

$$\rho_{E,\ell^\infty} : \mathrm{Gal}_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

be the representation describing the Galois action on the  $\ell$ -power torsion points; it is the composition of  $\rho_E$  with the natural projection  $\mathrm{GL}_2(\hat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ . After excluding a finite number of  $j$ -invariants, we will describe the possible images of the  $\ell$ -adic representation arising from elliptic curves over  $\mathbb{Q}$ . Denote by  $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$  the group generated by  $-I$  and  $\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$ .

The following theorem describes the possibilities for  $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$ , up to conjugacy, when  $j_E$  is not in the (finite!) set  $\mathcal{J}_\ell$ .

**Theorem 1.4.**

- (i) *The set  $\mathcal{J}_\ell$  is finite.*
- (ii) *If  $E/\mathbb{Q}$  is an elliptic curve with  $j_E \notin \mathcal{J}_\ell$ , then  $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$  is conjugate in  $\mathrm{GL}_2(\mathbb{Z}_\ell)$  to the  $\ell$ -adic projection of a unique group  $G$  from Theorem 1.1 with  $\ell$ -power level. Moreover,  $G$  does not have genus 1, level 16, and index 24 in  $\mathrm{GL}_2(\hat{\mathbb{Z}})$ .*

(iii) *Let  $G$  be a group from Theorem 1.1 with  $\ell$ -power level that does not have genus 1, level 16, and index 24 in  $\mathrm{GL}_2(\hat{\mathbb{Z}})$ . Then there are infinitely many elliptic curves  $E/\mathbb{Q}$ , with distinct  $j$ -invariants, such that  $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$  is conjugate in  $\mathrm{GL}_2(\mathbb{Z}_\ell)$  to the  $\ell$ -adic projection of  $G$ .*

**Remark 1.5.** (i) Serre [1981, p. 399] has asked whether  $\rho_{E,\ell}$  is surjective for all non-CM elliptic curves  $E/\mathbb{Q}$  and all primes  $\ell > 37$ . For  $\ell > 37$ , this would imply that the set  $\mathcal{J}_\ell$  consists of only the 13  $j$ -invariants of CM elliptic curves over  $\mathbb{Q}$ .

(ii) It would be nice to explicitly know the finite sets  $\mathcal{J}_\ell$ ; the proof that  $\mathcal{J}_\ell$  is finite relies on [Zywina 2015b], which is ineffective since it applies Faltings’ theorem several times.

Theorem 1.4 describes the subgroups of  $\mathrm{GL}_2(\mathbb{Z}_\ell)$ , up to conjugacy, that occur as  $\pm\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$  for infinitely many elliptic curves  $E/\mathbb{Q}$  with distinct  $j$ -invariants.

Theorem 1.4 also allows us to determine the subgroups of  $\mathrm{GL}_2(\mathbb{Z}_\ell)$ , up to conjugacy, that occur as  $\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$  for infinitely many elliptic curves  $E/\mathbb{Q}$  with distinct  $j$ -invariants. They are precisely the subgroups  $H$  of the  $\ell$ -adic projection  $G$  of a group from Theorem 1.4 with  $\ell$ -power level such that  $\pm H = G$ . Indeed if  $G = \pm\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$ , then for any such  $H$  there is a quadratic twist of  $E$  such that  $H$  is conjugate to  $\rho_{E',\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$ , see [Zywina 2015a, §5.1; Sutherland 2016, §5.6]; when  $H$  is properly contained in  $G$  this quadratic twist is unique up to isomorphism and can be explicitly determined.

**Corollary 1.6.** *For  $\ell = 2, 3, 5, 7, 11, 13$  there are respectively 1201, 47, 23, 15, 2, 11 subgroups  $H$  of  $\mathrm{GL}_2(\mathbb{Z}_\ell)$  that arise as  $\rho_{E,\ell^\infty}(\mathrm{Gal}_{\mathbb{Q}})$  for infinitely many elliptic curves  $E/\mathbb{Q}$  with distinct  $j$ -invariants. For  $\ell > 13$  the only such subgroup is  $H = \mathrm{GL}_2(\mathbb{Z}_\ell)$ .*

A list of the groups  $H$  appearing in Corollary 1.6 can be found in electronic form at [Sutherland and Zywina 2016].

**1B. Overview.** We now give a brief overview of the contents of this paper. As already noted, the groups  $G$  from Theorem 1.1, along with the corresponding modular curves  $X_G$  and morphisms  $\pi_G$ , can be found in the online supplement.

In Section 2, we review the background material we need concerning the modular curves  $X_G$ . If  $G$  has level  $N$ , then we can identify the function field of  $X_G$  with a subfield of the field  $\mathcal{F}_N$  of modular functions on  $\Gamma(N)$  whose Fourier coefficients lie in the cyclotomic field  $\mathbb{Q}(\zeta_N)$ . As a working definition of  $X_G$ , we define it in terms of its function field.

In Section 3, we determine up to conjugacy the open subgroups  $G$  of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  with genus at most 1 that satisfy  $\det(G) = \hat{\mathbb{Z}}^\times$ ,  $-I \in G$ , and contain an element that “looks like complex conjugation”; this last condition is necessary, since otherwise

$X_G(\mathbb{R})$ , and therefore  $X_G(\mathbb{Q})$ , is empty. We are left with 220 groups of genus 0 and 250 groups of genus 1 that include all the groups that appear in Theorem 1.1. These computations make use of the tables of Cummins and Pauli [2003] of congruence subgroups of low genus.

Let  $\Gamma$  be a congruence subgroup of  $\mathrm{SL}_2(\mathbb{Z})$  and let  $X_\Gamma$  be the smooth compact Riemann surface obtained by taking the quotient of the complex upper-half plane by  $\Gamma$  and adjoining cusps. Assume further that  $X_\Gamma$  has genus 0. In Section 4, we describe how to explicitly construct a *hauptmodul* for  $\Gamma$ ; it is a meromorphic function  $h$  on  $X_\Gamma$  that has a unique pole at the cusp at  $\infty$ . We describe  $h$  in terms of *Siegel functions*; its Fourier coefficients are computable and lie in the field  $\mathbb{Q}(\zeta_N) \subseteq \mathbb{C}$ .

In Section 5, we prove the part of Theorem 1.1 concerning genus 0 groups. Let  $G$  be one of the genus 0 groups from Section 3 and let  $J(t) \in \mathbb{Q}(t)$  be the corresponding rational function from the online supplement. We need to verify that the function field  $\mathbb{Q}(X_G)$  of  $X_G$  is of the form  $\mathbb{Q}(f)$ , for some modular function  $f$  for which  $J(f)$  coincides with the modular  $j$ -function. Using our work in Section 4, we can construct an explicit modular function  $h$  such that  $\mathbb{Q}(\zeta_N)(X_G) = \mathbb{Q}(\zeta_N)(h)$ , along with a rational function  $J'(t) \in \mathbb{Q}(\zeta_N)(t)$  such that  $J'(h) = j$ . The function  $f$  must satisfy  $f = \psi(h)$  for some  $\psi(t) \in \mathbb{Q}(\zeta_N)(t)$  of degree 1, and therefore  $J'(h) = j = J(f) = J(\psi(h))$ ; this in turn implies that  $J'(t) = J(\psi(t))$ . We then directly test all the modular functions  $f := \psi(h)$ , where  $\psi(t) \in \mathbb{Q}(\zeta_N)(t)$  is one of the finitely many degree 1 rational functions that satisfy  $J'(t) = J(\psi(t))$ .

In Section 6, we prove the part of Theorem 1.1 concerning genus 1 groups. Let  $G$  be one of the genus 1 groups from Section 3. One can show that  $X_G$  has good reduction at all primes  $p \nmid N$  and its modular interpretation gives a way to compute  $\#X_G(\mathbb{F}_p)$  directly from the group  $G$ , without requiring an explicit model. By computing  $\#X_G(\mathbb{F}_p)$  for enough primes  $p \nmid N$ , one can determine the Jacobian  $J_G$  of  $X_G$  up to isogeny. This allows us to compute the rank of  $J_G(\mathbb{Q})$  which is an isogeny invariant of  $J_G$ . We need only consider groups for which  $J_G(\mathbb{Q})$  has positive rank since otherwise  $X_G(\mathbb{Q})$  is finite; this leaves the 28 genus 1 groups in Theorem 1.1. These 28 groups  $G$  of genus 1 and a description of their morphisms  $\pi_G$  already appear in the literature; our contribution lies in proving that there are no others.

In Section 7, we complete the proof of Theorem 1.4, and in Section 8 we explain how we found the rational functions  $J(t) \in \mathbb{Q}(t)$  whose verification is described in Section 5.

The online supplement lists the 248 groups  $G$  that appear in Theorem 1.1, along with explicit maps from  $X_G$  to the  $j$ -line; for the 220 groups of genus 0 these are rational functions  $J(t)$ , and for the 28 groups of genus 1 these are morphisms  $J(x, y)$  from an explicit Weierstrass model for  $X_G$  as an elliptic curve of positive rank. One

can use these maps to explicitly construct infinite families of elliptic curves  $E/\mathbb{Q}$  with distinct  $j$ -invariants whose  $\ell$ -adic Galois images match the groups  $G$  listed in Theorem 1.4 and the groups  $H$  listed in Corollary 1.6 by choosing appropriate quadratic twists.

**1C. Related results.** Contemporaneous with our work, Rouse and Zureick-Brown [2015] independently computed explicit models for all modular curves  $X_G/\mathbb{Q}$  of 2-power level that have a noncuspidal rational point, including all those for which  $X_G(\mathbb{Q})$  is infinite. The  $X_G$  of 2-power level in our list agree with theirs, although we generally obtain different (but isomorphic) models (note our groups are transposed relative to theirs; in our choice of the isomorphism  $\text{Aut}(E[N]) \simeq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  we view matrices in  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  as acting on the left, rather than the right).

**Notation and terminology.** For each integer  $n \geq 1$ , we denote by  $\zeta_n$  the  $n$ -th root of unity  $e^{2\pi i/n}$  in  $\mathbb{C}$ , and let  $K_n := \mathbb{Q}(\zeta_n)$  denote the corresponding cyclotomic field. For any nonconstant function  $f \in K(t)$ , where  $K$  is a field, the *degree* of  $f$  is its degree as a morphism  $\mathbb{P}_K^1 \rightarrow \mathbb{P}_K^1$ .

For any ring  $R$ , we denote by  $M_2(R)$  the ring of  $2 \times 2$  matrices with coefficients in  $R$ . We denote by  $\hat{\mathbb{Z}}$  the profinite completion of  $\mathbb{Z}$ , and view the profinite group

$$\text{GL}_2(\hat{\mathbb{Z}}) \simeq \varprojlim_N \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{\ell} \text{GL}_2(\mathbb{Z}_{\ell})$$

as a topological group in the profinite topology. If  $G$  is an open subgroup of  $\text{GL}_2(\hat{\mathbb{Z}})$ , we define its *level* to be the least positive integer  $N$  for which  $G$  is the inverse image of a subgroup of  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  under the natural projection  $\text{GL}_2(\hat{\mathbb{Z}}) \rightarrow \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ . If  $G$  is a subgroup of  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ , its level is defined to be the level of its inverse image in  $\text{GL}_2(\hat{\mathbb{Z}})$ , which is necessarily a divisor of  $N$ . For convenience we may identify the level  $N$  subgroups of  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  with their inverse images in  $\text{GL}_2(\hat{\mathbb{Z}})$ , and conversely. By the *genus* of an open subgroup  $G$  of  $\text{GL}_2(\hat{\mathbb{Z}})$  satisfying  $-I \in G$  and  $\det(G) = \hat{\mathbb{Z}}^{\times}$ , we mean the genus of the modular curve  $X_G$  defined in Section 2.

For sets  $S$  and  $T$  we use  $S - T$  to denote the set of elements that lie in  $S$  but not  $T$ .

## 2. Modular functions and modular curves

In this section, we summarize the background we need concerning modular curves.

**2A. Congruence subgroups.** Fix a congruence subgroup  $\Gamma$  of  $\text{SL}_2(\mathbb{Z})$ , i.e., a subgroup of  $\text{SL}_2(\mathbb{Z})$  containing

$$\Gamma(N) := \{A \in \text{SL}_2(\mathbb{Z}) : A \equiv I \pmod{N}\}$$

for some integer  $N \geq 1$ . The smallest such  $N$  is the *level* of  $\Gamma$ .

The group  $\Gamma$  acts on the complex upper half plane  $\mathbb{H}$  by linear fractional transformations, and the quotient  $Y_\Gamma = \Gamma \backslash \mathbb{H}$  is a smooth Riemann surface. By adding *cusps*, we can extend  $Y_\Gamma$  to a smooth compact Riemann surface  $X_\Gamma$ . We denote by  $X(N)$  the Riemann surface  $X_{\Gamma(N)}$ . The *genus* of  $\Gamma$  is the genus of the Riemann surface  $X_\Gamma$ .

**2B. Cusps.** Define the extended upper half plane by  $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ . The action of  $\Gamma$  extends to  $\mathbb{H}^*$  and we can identify the quotient  $\Gamma \backslash \mathbb{H}^*$  with  $X_\Gamma$ . In particular, the cusps correspond to the  $\Gamma$ -orbits of  $\mathbb{Q} \cup \{\infty\}$ .

**Lemma 2.1.** *Let  $a/b$  and  $\alpha/\beta$  be elements of  $\mathbb{Q} \cup \{\infty\}$  satisfying  $\gcd(a, b) = 1$  and  $\gcd(\alpha, \beta) = 1$  (where we take  $\infty = \pm 1/0$ ). Then  $\Gamma \cdot a/b = \Gamma \cdot \alpha/\beta$  if and only if  $\gamma \begin{pmatrix} a \\ b \end{pmatrix} \equiv \pm \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \pmod{N}$  for some  $\gamma \in \Gamma$ .*

*Proof.* For the case  $\Gamma = \Gamma(N)$ , see [Shimura 1971, Lemma 1.42]. The general case follows easily. □

Let  $\pm\Gamma$  be the congruence subgroup generated by  $-I$  and  $\Gamma$ . From Lemma 2.1, we find that the cusps of  $X_\Gamma$  correspond with the orbits of  $\pm\Gamma$  on the set of  $\begin{pmatrix} a \\ b \end{pmatrix} \in (\mathbb{Z}/N\mathbb{Z})^2$  of order  $N$ . Using this, it is straightforward to find representatives of the cusps of  $X_\Gamma$ .

**2C. Modular functions.** A *modular function* for  $\Gamma$  is a meromorphic function of  $X_\Gamma$ ; they correspond to meromorphic functions  $f$  of  $\mathbb{H}$  that satisfy  $f(\gamma\tau) = f(\tau)$  for all  $\gamma \in \Gamma$  and are meromorphic at the cusps. The function field  $\mathbb{C}(X_\Gamma)$  of  $X_\Gamma$  consists of the meromorphic functions of  $X_\Gamma$ .

Let  $\tau$  be a variable of the upper half plane. Let  $w$  be the width of the cusp at  $\infty$ , i.e., the smallest positive integer for which  $\begin{pmatrix} 1 & w \\ 0 & 1 \end{pmatrix}$  is an element of  $\Gamma$ ; it is a divisor of  $N$ . For any rational number  $m$ , define  $q^m := e^{2\pi im\tau}$ . Then any modular function  $f$  for  $\Gamma$  has a unique  $q$ -expansion

$$f(\tau) = \sum_{n \in \mathbb{Z}} c_n q^{n/w},$$

where the  $c_n$  are complex numbers that are 0 for all but finitely many  $n < 0$ . We will often refer to the  $c_n$  as the *coefficients* of  $f$ .

**2D. Field of modular functions.** Fix a positive integer  $N$ . Denote by  $\mathcal{F}_N$  the field of meromorphic functions of the Riemann surface  $X(N)$  whose  $q$ -expansions have coefficients in  $K_N := \mathbb{Q}(\zeta_N)$ . For example,  $\mathcal{F}_1 = \mathbb{Q}(j)$ , where  $j$  is the modular  $j$ -invariant.

For  $f \in \mathcal{F}_N$  and  $\gamma \in \text{SL}_2(\mathbb{Z})$ , let  $f|_\gamma \in \mathcal{F}_N$  denote the modular function satisfying  $f|_\gamma(\tau) = f(\gamma\tau)$ .



For each  $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ , let  $\sigma_d$  be the automorphism of  $K_N$  satisfying  $\sigma_d(\zeta_N) = \zeta_N^d$ . We extend  $\sigma_d$  to an automorphism of the field  $\mathcal{F}_N$  by defining

$$\sigma_d(f) := \sum_n \sigma_d(c_n)q^{n/N},$$

where  $f$  has expansion  $\sum_n c_n q^{n/N}$ . We now recall some facts about the extension  $\mathcal{F}_N$  of  $\mathcal{F}_1 = \mathbb{Q}(j)$ .

**Proposition 2.2.** *The extension  $\mathcal{F}_N$  of  $\mathbb{Q}(j)$  is Galois. There is a unique isomorphism*

$$\theta_N : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \xrightarrow{\sim} \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$$

such that the following hold for all  $f \in \mathcal{F}_N$ :

- (a) For  $g \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ , we have  $\theta_N(g)f = f|_{\gamma^t}$ , where  $\gamma$  is any matrix in  $\mathrm{SL}_2(\mathbb{Z})$  that is congruent to  $g$  modulo  $N$  and  $\gamma^t$  is the transpose of  $\gamma$ .
- (b) For  $g = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ , we have  $\theta_N(g)f = \sigma_d(f)$ .

Moreover, the algebraic closure of  $\mathbb{Q}$  in  $\mathcal{F}_N$  is  $\mathbb{Q}(\zeta_N)$ ; it corresponds to the subgroup  $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ .

*Proof.* This is well known; see [Kubert and Lang 1981, Chapter 2, §2] for a summary (where the action given is a right action obtained as above but without the transpose in (a)). □

Throughout the rest of the paper, we let  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  act on  $\mathcal{F}_N$  via the homomorphism  $\theta_N$  of Proposition 2.2. We set  $g_*(f) := \theta_N(g)(f)$  for  $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  and  $f \in \mathcal{F}_N$ .

**Remark 2.3.** There are other natural actions of  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  on  $\mathcal{F}_N$ ; for example, one could replace  $\gamma^t$  in condition (a) by  $\gamma^{-1}$  or just act on the right. Our choice is motivated by Proposition 2.6 below.

**2E. Modular curves.** Let  $G$  be a subgroup of  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  satisfying  $-I \in G$  and  $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ . Let  $\mathcal{F}_N^G$  be the subfield of  $\mathcal{F}_N$  fixed by the action of  $G$  from Proposition 2.2. Proposition 2.2 and the assumption  $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$  imply that  $\mathbb{Q}$  is algebraically closed in  $\mathcal{F}_N^G$ .

The modular curve  $X_G$  associated with  $G$  is the smooth projective curve with function field  $\mathcal{F}_N^G$ . The curve  $X_G$  is defined over  $\mathbb{Q}$  and is geometrically irreducible. The inclusion of fields  $\mathcal{F}_N^G \supseteq \mathcal{F}_1 = \mathbb{Q}(j)$  gives rise to a nonconstant morphism

$$\pi_G : X_G \rightarrow \mathrm{Spec} \mathbb{Q}[j] \cup \{\infty\} = \mathbb{P}_{\mathbb{Q}}^1$$

of degree  $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$ . Moreover, given another group  $G \subseteq G' \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ , the inclusion  $\mathcal{F}_N^{G'} \subseteq \mathcal{F}_N^G$  induces a nonconstant morphism  $X_G \rightarrow X_{G'}$  of degree  $[G' : G]$ . Composing  $X_G \rightarrow X_{G'}$  with  $\pi_{G'}$  gives the morphism  $\pi_G$ .

Let  $\Gamma$  be the congruence subgroup consisting of  $\gamma \in \mathrm{SL}_2(\mathbb{Z})$  for which  $\gamma^t$  modulo  $N$  lies in  $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ . The level of  $\Gamma$  divides, but need not equal,  $N$ .

**Lemma 2.4.** (i) *The field  $K_N(X_G)$ , i.e., the function field of the base extension of  $X_G$  to  $K_N$ , is the field consisting of  $f \in \mathcal{F}_N$  satisfying  $f|_\gamma = f$  for all  $\gamma \in \Gamma$ .*  
 (ii) *The genus of the modular curve  $X_G$  is equal to the genus of  $\Gamma$ .*

*Proof.* Proposition 2.2 implies that  $K_N$  is algebraically closed in  $\mathcal{F}_N$  and that we have an isomorphism  $\mathrm{Gal}(\mathcal{F}_N/K_N(j)) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ . Thus  $K_N(X_G)$  is the subfield of  $\mathcal{F}_N$  fixed by  $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ . Part (i) is now clear.

Since  $K_N$  is algebraically closed in  $\mathcal{F}_N$  and  $\mathbb{Q}$  is algebraically closed in  $\mathbb{Q}(X_G)$ , we have

$$[\mathbb{C} \cdot K_N(X_G) : \mathbb{C}(j)] = [K_N(X_G) : K_N(j)] = [\mathbb{Q}(X_G) : \mathbb{Q}(j)] = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G].$$

Since  $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ , we deduce that  $[\mathbb{C} \cdot K_N(X_G) : \mathbb{C}(j)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ .

Clearly each  $f \in K_N(X_G)$  is a modular function for  $\Gamma$ , thus  $\mathbb{C} \cdot K_N(X_G) \subseteq \mathbb{C}(X_\Gamma)$ . We in fact have  $\mathbb{C} \cdot K_N(X_G) = \mathbb{C}(X_\Gamma)$ , since  $[\mathbb{C} \cdot K_N(X_G) : \mathbb{C}(j)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = [\mathbb{C}(X_\Gamma) : \mathbb{C}(j)]$ . The curve  $X_G$  has the same genus as the Riemann surface  $X_\Gamma$  because  $\mathbb{C}(X_G) = \mathbb{C}(X_\Gamma)$ .  $\square$

**Remark 2.5.** Another natural congruence subgroup to study is the congruence subgroup  $\Gamma'$  consisting of  $\gamma \in \mathrm{SL}_2(\mathbb{Z})$  such that  $\gamma$  modulo  $N$  lies in  $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ , which we use later in the paper. Observe that the congruence subgroups  $\Gamma$  and  $\Gamma'$  are conjugate in  $\mathrm{SL}_2(\mathbb{Z})$ ; indeed, we have  $B^{-1}\gamma B = (\gamma^t)^{-1}$  for all  $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ , where  $B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ . Thus  $\Gamma$  and  $\Gamma'$  have the same genus.

The following proposition is crucial to our application.

**Proposition 2.6.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  with  $j_E \notin \{0, 1728\}$ . Then  $\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$  is conjugate in  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  to a subgroup of  $G$  if and only if  $j_E$  belongs to  $\pi_G(X_G(\mathbb{Q}))$ .*

*Proof.* See [Zywina 2015a, §3] for a proof.  $\square$

**2F. Modular curves and open subgroups.** Fix an open subgroup  $G$  of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  that satisfies  $-I \in G$  and  $\det(G) = \hat{\mathbb{Z}}^\times$ . Let  $N \geq 1$  be an integer that is divisible by the level of  $G$ . Define the modular curve

$$X_G := X_{\bar{G}},$$

where  $\bar{G} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  is the image of  $G$  modulo  $N$ . Observe that the modular curve  $X_G$  and its function field do not depend on the initial choice of  $N$ .

Every (open) subgroup  $G'$  of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  that contains  $G$  satisfies  $-I \in G'$  and  $\det(G') = \hat{\mathbb{Z}}^\times$ , and we have a morphism  $X_G \rightarrow X_{G'}$ . With  $G' = \mathrm{GL}_2(\hat{\mathbb{Z}})$ , we obtain a morphism  $\pi_G : X_G \rightarrow X_{G'} = \mathbb{P}_{\mathbb{Q}}^1$  to the  $j$ -line that agrees with  $\pi_{\bar{G}}$ . The following is equivalent to Proposition 2.6.

**Proposition 2.7.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  with  $j_E \notin \{0, 1728\}$ . Then  $\rho_E(\text{Gal}_{\mathbb{Q}})$  is conjugate in  $\text{GL}_2(\hat{\mathbb{Z}})$  to a subgroup of  $G$  if and only if  $j_E$  belongs to  $\pi_G(X_G(\mathbb{Q}))$ .  $\square$*

**2G. Complex conjugation.** Fix a subgroup  $G$  of  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  satisfying  $-I \in G$  and  $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ . For our curve  $X_G$  to have rational points, we need  $G$  to contain an element that “looks like” complex conjugation.

**Lemma 2.8.** *For any elliptic curve  $E/\mathbb{Q}$  and integer  $N > 1$ , the group  $\rho_{E,N}(\text{Gal}_{\mathbb{Q}})$  contains an element that is conjugate in  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  to  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  or  $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ .*

*Proof.* This follows from of [Zywina 2015b, Proposition 3.5] (and its proof for the cases  $j_E \in \{0, 1728\}$ ).  $\square$

Note that  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  and  $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$  are conjugate to each other in  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  if  $N$  is odd. If  $G$  does not contain an element that is conjugate in  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  to  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  or  $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ , then  $X_G(\mathbb{Q})$  must be empty since  $X_G(\mathbb{R})$  is finite (by [Zywina 2015b, Proposition 3.5]), hence empty, since  $X_G$  is nonsingular.

### 3. Group theoretic computations

We define an *admissible group* to be an open subgroup  $G$  of  $\text{GL}_2(\hat{\mathbb{Z}})$  for which the following conditions hold:

- $G$  has prime power level.
- $-I \in G$  and  $\det(G) = \hat{\mathbb{Z}}^\times$ .
- $G$  contains an element that is conjugate in  $\text{GL}_2(\hat{\mathbb{Z}})$  to  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  or  $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ .

The condition  $\det(G) = \hat{\mathbb{Z}}^\times$  is needed for Proposition 2.7 since  $\det(\rho_E(\text{Gal}_{\mathbb{Q}})) = \hat{\mathbb{Z}}^\times$ . If we were interested in elliptic curves defined over other number fields, then we could loosen this restriction which could increase the base field of the modular curve  $X_G$ .

The condition  $-I \in G$  is also needed in Proposition 2.7. For an elliptic curve  $E/\mathbb{Q}$ , there is a quadratic twist  $E'/\mathbb{Q}$ , which automatically has the same  $j$ -invariant as  $E$ , such that  $-I \in \rho_E(\text{Gal}_{\mathbb{Q}})$ .

The last condition on  $G$  is necessary in order for  $X_G(\mathbb{Q})$  to be nonempty, as explained in Section 2G.

**Proposition 3.1.** *Let  $G$  be an admissible group of genus 0. The set  $X_G(\mathbb{Q})$  is infinite.*

*Proof.* We have  $X_G(\mathbb{R}) \neq \emptyset$  by [Zywina 2015b, Proposition 3.5]. For primes  $p$  not dividing its prime power level the modular curve  $X_G$  has good reduction at  $p$  and  $X_G(\mathbb{Q}_p) \neq \emptyset$ , since the reduction of  $X_G$  to  $\mathbb{F}_p$  necessarily has rational points that can be lifted to  $\mathbb{Q}_p$  via Hensel’s lemma. Thus  $X_G$  has rational points locally

at all but at most one place of  $\mathbb{Q}$ . The product formula for Hilbert symbols and the Hasse–Minkowski theorem then imply that  $X_G$  has a rational point and is thus isomorphic to  $\mathbb{P}^1$  and has infinitely many rational points.  $\square$

**Remark 3.2.** As shown by Proposition 3.1, our three criteria for admissibility rule out genus 0 curves with no rational points. There are ten groups  $G$  of 2-power level that satisfy our first two criteria but not the third; these give rise to the ten pointless conics  $X_G$  found in [Rouse and Zureick-Brown 2015]. There are three such groups of 3-power level, three of 5-power level, and none of higher prime-power level.

Fix an integer  $g \geq 0$ . In this section, we explain how to enumerate all admissible subgroups  $G$  of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$ , up to conjugacy, that have genus at most  $g$ . We shall apply these methods with  $g = 1$  to verify Theorem 3.3 below, and to find explicit representatives of these conjugacy classes of groups; Magma [Bosma et al. 1997] scripts that perform this enumeration can be found in [Sutherland and Zywina 2016].

**Theorem 3.3.**

- (i) *Up to conjugacy in  $\mathrm{GL}_2(\hat{\mathbb{Z}})$ , there are 220 admissible subgroups of genus 0.*
- (ii) *Up to conjugacy in  $\mathrm{GL}_2(\hat{\mathbb{Z}})$ , there are 250 admissible subgroups of genus 1.*

**Remark 3.4.** The 220 admissible subgroups  $G$  of genus 0, up to conjugacy, are precisely those given in Tables 1–3 of the online supplement. More precisely, for each entry of the table, we have an integer  $N$  and a set of generators that generates the image in  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  of an admissible group of level  $N$  and genus 0.

**Remark 3.5.** The 28 admissible subgroups  $G$  of genus 1 that have infinitely many rational points, up to conjugacy, are precisely those given in Table 4 of the online supplement, of which 27 have level 16 and 1 has level 11. The levels arising among the remaining 222 are 7, 8, 9, 11, 16, 17, 19, 27, 32, and 49.

For a fixed admissible group  $G$  of level  $N$ , let  $\Gamma$  be the congruence subgroup of  $\mathrm{SL}_2(\mathbb{Z})$  consisting of matrices whose image modulo  $N$  lies in the image of  $G \bmod N$ ; the level of  $\Gamma$  necessarily divides  $N$ , and  $\Gamma$  contains  $-I$ . By Lemma 2.4(ii) and Remark 2.5, the modular curve  $X_G$  has the same genus as  $\Gamma$ .

The basic idea of our computation is to reverse the process above; we start with a congruence subgroup  $\Gamma$  of genus at most  $g$  and prime power level, and then enumerate the possible groups  $G$  that could produce  $\Gamma$ .

Let  $S_g$  be the set of congruence subgroups of  $\mathrm{SL}_2(\mathbb{Z})$  of prime power level that contain  $-I$  and have genus at most  $g$ . We know that the set  $S_g$  is finite from a theorem of Dennin [1974]. When  $g \leq 24$ , and in particular, for  $g = 1$ , we can explicitly determine the elements of  $S_g$  from the tables of Cummins and Pauli [2003] (their methods can also be extended to larger  $g$ ).

Let  $L_g$  be the set of primes that divide the level of some congruence subgroup

$\Gamma \in S_g$ . The set  $L_g$  is finite, since  $S_g$  is finite, and we have  $L_1 = \{2, 3, 5, 7, 11, 13, 17, 19\}$ . If  $G$  is an admissible group of genus at most  $g$ , then its level must be a power of a prime  $\ell \in L_g$ . For the rest of the section, we fix a prime  $\ell \in L_g$ . Since  $L_g$  is finite, it suffices to explain how to compute the admissible groups  $G$  with genus at most  $g$  whose level is a power of  $\ell$ , and we need only consider levels strictly greater than 1 since  $\text{GL}_2(\hat{\mathbb{Z}})$  is the only admissible group of level 1.

Fix a prime power  $N := \ell^n > 1$ , and consider any congruence subgroup  $\Gamma \in S_g$  whose level divides  $N$ . By enumerating subgroups of  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  one can explicitly determine those subgroups  $G_N$  that satisfy the following conditions:

- (1)  $G_N$  has level  $N$ ,
- (2)  $G_N \cap \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$  is equal to the image of  $\Gamma$  modulo  $N$ ,
- (3)  $\det(G_N) = (\mathbb{Z}/N\mathbb{Z})^\times$ ,
- (4)  $G_N$  contains an element that is conjugate in  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  to  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  or  $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ .

Let  $H$  be the image of  $\Gamma$  in  $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ . The group  $H = G_N \cap \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$  is normal in  $G_N$  and hence  $G_N$  is a subgroup of the normalizer  $K$  of  $H$  in  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ . So rather than searching for  $G_N$  in  $K$ , we can work in the quotient  $K/H$  where the image of  $G_N$  is an abelian group isomorphic to  $(\mathbb{Z}/N\mathbb{Z})^\times$ . Using Magma, we can efficiently enumerate all abelian subgroups  $A$  of  $K/H$  of order  $\#(\mathbb{Z}/N\mathbb{Z})^\times$ . For each such subgroup  $A$  we then test whether its inverse image  $G_N$  in  $K$  satisfies conditions (1)–(4) above.

Let  $G$  be the subgroup of  $\text{GL}_2(\hat{\mathbb{Z}})$  consisting of those matrices whose image modulo  $N$  lies in a fixed group  $G_N$  satisfying the conditions (1)–(4). The group  $G$  is admissible of level  $N$  and has genus at most  $g$ . Moreover, it is clear that every admissible group of level  $N$  and genus at most  $g$  arises in this manner.

Fix an integer  $e \geq 1$ . By applying the above method with  $1 \leq n \leq e$ , we obtain all admissible groups  $G$  of genus at most  $g$  and level dividing  $\ell^e$ . Our algorithm proceeds by applying this procedure to increasing values of  $e$ . In order for it to terminate we need to know that there are only finitely many admissible groups  $G$  of  $\ell$ -power level and genus at most  $g$ , and we need an explicit way to determine when we have reached an  $e$  that is large enough to guarantee that we have found them all. Proposition 3.6 below addresses both issues.

**Proposition 3.6.**

- (i) *There are only finitely many admissible groups  $G$  with genus at most  $g$  whose level is a power of  $\ell$ .*
- (ii) *Take any integer  $n \geq 2$  with  $n \neq 2$  if  $\ell = 2$ . Define  $N := \ell^n$ . Suppose that there is no subgroup  $G_N$  of  $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  that satisfies conditions (1)–(4) for some  $\Gamma \in S_g$  with level dividing  $N$ . Then any admissible group  $G$  of genus at most  $g$  with level a power of  $\ell$  has level at most  $N$ .*

The remainder of this section is devoted to proving Proposition 3.6. We will need the following basic lemma.

**Lemma 3.7.** *Let  $\ell$  be a prime and let  $G$  be an open subgroup of  $\mathrm{GL}_2(\mathbb{Z}_\ell)$ . For each integer  $m \geq 1$ , let  $i_m$  be the index of the image of  $G$  in  $\mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$ . If  $i_{n+1} = i_n$  for an integer  $n \geq 1$ , with  $n \neq 1$  if  $\ell = 2$ , then  $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G] = i_n$ .*

*Proof.* Since  $G$  is an open subgroup, it suffices to prove  $i_{m+1} = i_m$  for all  $m \geq n$ ; we proceed by induction on  $m$ . The base case is given, so we assume  $i_{m+1} = i_m$  for some  $m \geq n$ ; we need to show that  $i_{m+2} = i_{m+1}$ . Let  $G_m$  denote the image of  $G$  in  $\mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$ . Reduction modulo  $\ell^m$  gives exact sequences related by inclusions

$$\begin{array}{ccccccc}
 1 & \longrightarrow & K_{m+1} & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/\ell^{m+1}\mathbb{Z}) & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z}) \longrightarrow 1 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 1 & \longrightarrow & H_{m+1} & \longrightarrow & G_{m+1} & \longrightarrow & G_m \longrightarrow 1.
 \end{array}$$

The inductive hypothesis  $i_{m+1} = i_m$  implies that the kernels  $H_{m+1}$  and  $K_{m+1}$  coincide; in particular,  $H_{m+1}$  is as large as possible (i.e., it has order  $\ell^4$ ). It thus suffices to show that the kernel  $H_{m+2}$  of the reduction map from  $G_{m+2}$  to  $G_{m+1}$  also has order  $\ell^4$ . We have  $|H_{m+2}| \leq \ell^4$ , so it suffices to give an injective map  $H_{m+1} \rightarrow H_{m+2}$ .

Let  $M$  be an element of  $G$  whose image in  $G_{m+1}$  lies in  $H_{m+1}$ ; then  $M = I + \ell^m A$  for some  $A \in \mathrm{M}_2(\mathbb{Z}_\ell)$ . Since  $m \geq 1$ , with  $m \geq 2$  if  $\ell = 2$ , we have

$$(1 + \ell^m A)^\ell = 1 + \binom{\ell}{1} \ell^m A + \binom{\ell}{2} \ell^{2m} A^2 + \dots \equiv 1 + \ell^{m+1} A \pmod{\ell^{m+2}}.$$

The  $\ell$ -power map thus induces an injection  $H_{m+1} \rightarrow H_{m+2}$ . □

**Remark 3.8.** Lemma 3.7 holds more generally. One can replace  $\mathrm{GL}_2(\mathbb{Z}_\ell)$  with the unit group of any (unital associative)  $\mathbb{Z}_\ell$ -algebra  $\mathcal{A}$  that is torsion-free and finitely generated as a  $\mathbb{Z}_\ell$ -module (in the lemma,  $\mathcal{A} = \mathrm{M}_2(\mathbb{Z}_\ell)$ ); the proof is exactly the same.

*Proof of Proposition 3.6(i).* Let  $\mathcal{G}$  be the set of admissible groups of genus at most  $g$  whose level is a power of  $\ell$ . Note that if  $G'$  is a subgroup of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  containing some  $G \in \mathcal{G}$ , then  $G' \in \mathcal{G}$ . We wish to show that  $\mathcal{G}$  is finite.

We claim that any admissible group  $G$  has only finitely many maximal subgroups that are also admissible and whose level is a power of  $\ell$ . It suffices to show that an open subgroup  $H$  of  $\mathrm{GL}_2(\mathbb{Z}_\ell)$  has only finitely many open maximal subgroups. Let  $\Phi(H)$  be the Frattini subgroup of  $H$ ; it is the intersection of the maximal closed proper subgroups of  $H$ . By the proposition in [Serre 1997, §10.5],  $\Phi(H)$  is an open subgroup of  $H$ . This proves the claim.

Now suppose that  $\mathcal{G}$  is infinite. The claim implies that  $\mathcal{G}$  contains an infinite descending chain  $G_1 \supsetneq G_2 \supsetneq G_3 \supsetneq \dots$  (let  $G_1 = \mathrm{GL}_2(\hat{\mathbb{Z}}) \in \mathcal{G}$ , let  $G_2 \in \mathcal{G}$  be one of the finitely many maximal subgroups of  $G_1$  in  $\mathcal{G}$  that has infinitely many subgroups

in  $\mathcal{G}$ , and continue in this fashion). For each  $i \geq 1$ , let  $\Gamma_i$  be the congruence subgroup associated to  $G_i$  (i.e.,  $\Gamma_i$  consists of the matrices in  $\mathrm{SL}_2(\mathbb{Z})$  whose image modulo  $N$  lies in the image modulo  $N$  of  $G_i$ , where  $N$  is the level of  $G_i$ ); then  $\Gamma_i \in S_g$ . Since  $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : G_i] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_i]$ , we have inclusions  $\Gamma_1 \supseteq \Gamma_2 \supseteq \Gamma_3 \supseteq \dots$ . This contradicts the finiteness of  $S_g$  and the proposition follows.  $\square$

*Proof of Proposition 3.6(ii).* Fix an integer  $n \geq 1$  as in the statement of part (ii). Suppose there is an integer  $m > n$  such that there is an admissible group  $G$  of level  $\ell^m$  and genus at most  $g$ .

With  $N := \ell^n$ , let  $G_N$  be the image of  $G$  in  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ . The curve  $X_{G_N}$  has genus at most  $g$  since it is dominated by  $X_G$ . Therefore, conditions (2), (3), and (4) hold for some  $\Gamma \in S_g$  with level dividing  $N$ . Our assumption on  $n$  implies that the level of  $G_N$  is a proper divisor of  $N$ . This implies that the index  $i_n := [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G_N]$  agrees with  $i_{n-1} := [\mathrm{GL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z}) : G_{\ell^{n-1}}]$ , where  $G_{\ell^{n-1}}$  is the image of  $G$  in  $\mathrm{GL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z})$ . Since  $i_n = i_{n-1}$ , Lemma 3.7 implies that  $[\mathrm{GL}_2(\mathbb{Z}_\ell) : G] = i_{n-1}$ . However, this means that  $G$  has level dividing  $\ell^{n-1}$  which is impossible since, by assumption,  $G$  has level  $\ell^m > \ell^{n-1}$ . Therefore, no such admissible group  $G$  exists.  $\square$

#### 4. Construction of hauptmoduls

Fix a congruence subgroup  $\Gamma$  of genus 0 and level  $N$ . The function field of  $X_\Gamma$  is then of the form  $\mathbb{C}(h)$ , where the function  $h : X_\Gamma \rightarrow \mathbb{C} \cup \{\infty\}$  gives an isomorphism between  $X_\Gamma$  and the Riemann sphere; in particular,  $h$  has a unique (simple) pole.

We may choose  $h$  so that its unique pole is at the cusp  $\infty$ ; we will call such an  $h$  a *hauptmodul* of  $\Gamma$ . Every hauptmodul of  $\Gamma$  is then of the form  $ah + b$  for some complex numbers  $a \neq 0$  and  $b$ . For example, the familiar modular  $j$ -invariant

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots$$

is a hauptmodul for  $\mathrm{SL}_2(\mathbb{Z})$ . If  $h$  is a hauptmodul for  $\Gamma$ , then we have an inclusion of function fields  $\mathbb{C}(j) \subseteq \mathbb{C}(h)$  and hence  $J(h) = j$  for a unique rational function  $J(h) \in \mathbb{C}(t)$ .

The main task of Section 4 is to describe how to find an *explicit* hauptmodul  $h$  of  $\Gamma$  in terms of Siegel functions when  $N$  is a prime power. Our  $h$  will have coefficients in  $K_N$ . In Section 4D, we explain how to compute the rational function  $J(t)$  corresponding to  $h$ .

**4A. Siegel functions.** Take any pair  $a = (a_1, a_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ . We define the *Siegel function*  $g_a(\tau)$  to be the holomorphic function  $\mathbb{H} \rightarrow \mathbb{C}^\times$  defined by the series

$$-q^{1/2B_2(a_1)} \cdot e(a_2(a_1 - 1)/2) \cdot (1 - e(a_2)q^{a_1}) \prod_{n=1}^{\infty} (1 - e(a_2)q^{n+a_1})(1 - e(-a_2)q^{n-a_1}),$$

where  $e(z) = e^{2\pi iz}$  and  $B_2(x) = x^2 - x + \frac{1}{6}$ .

Recall that the *Dedekind eta function* is the holomorphic function on  $\mathbb{H}$  given by

$$\eta(\tau) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

For each  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ , there is a unique 12-th root of unity  $\varepsilon(\gamma) \in \mathbb{C}^\times$  such that

$$\eta(\gamma\tau)^2 = \varepsilon(\gamma)(c\tau + d)\eta(\tau)^2. \tag{4-1}$$

We can characterize the map  $\varepsilon : \text{SL}_2(\mathbb{Z}) \rightarrow \mathbb{C}^\times$  by the property that it is a homomorphism satisfying  $\varepsilon\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = \zeta_{12}$  and  $\varepsilon\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = \zeta_4$ ; see [Kubert and Lang 1981, Chapter 3, §5]. Moreover, the kernel of  $\varepsilon$  is a congruence subgroup of level 12 and agrees with the commutator subgroup of  $\text{SL}_2(\mathbb{Z})$ .

The following lemma gives several key properties of Siegel functions.

**Lemma 4.1.** *For any  $\gamma \in \text{SL}_2(\mathbb{Z})$ ,  $a \in \mathbb{Q}^2 - \mathbb{Z}^2$ , and  $b \in \mathbb{Z}^2$ , the following hold:*

- (i)  $g_{-a} = -g_a$ ,
- (ii)  $g_{a+b} = (-1)^{b_1+b_2+b_1b_2} \cdot e((b_2a_1 - b_1a_2)/2) \cdot g_a$ ,
- (iii)  $g_a|_\gamma = \varepsilon(\gamma) \cdot g_{a\gamma}$ , where we view  $a$  as a row vector.

*Proof.* In [Kubert and Lang 1981, Chapter 2, §1], we see that  $g_a(\tau) = \mathfrak{k}_a(\tau)\eta(\tau)^2$ , where  $\mathfrak{k}_a(\tau)$  is a Klein form (with  $W = W_\tau$  in the notation the previous work). Part (ii) follows directly from property K2 in [loc. cit.].

Take any  $\gamma \in \text{SL}_2(\mathbb{Z})$  and let  $(c, d)$  be the last row of  $\gamma$ . From properties K0 and K1 of the above reference, we find that

$$\mathfrak{k}_a(\gamma\tau) = (c\tau + d)^{-1}\mathfrak{k}_{a\gamma}(\tau). \tag{4-2}$$

From (4-1) and (4-2), we deduce that  $g_a(\gamma\tau) = \varepsilon(\gamma) \cdot g_{a\gamma}(\tau)$ , which proves part (iii). Finally, part (i) follows from part (iii) with  $\gamma = -I$ , since  $\varepsilon(-I) = -1$ .  $\square$

For an integer  $N > 1$ , let  $\mathcal{A}_N$  be the set of pairs  $(a_1, a_2) \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2$  that satisfy one of the following conditions:

- $0 < a_1 < \frac{1}{2}$  and  $0 \leq a_2 < 1$ ,
- $a_1 = 0$  and  $0 < a_2 \leq \frac{1}{2}$ ,
- $a_1 = \frac{1}{2}$  and  $0 \leq a_2 \leq \frac{1}{2}$ .

The set  $\mathcal{A}_N$  is chosen so that every nonzero coset of  $(N^{-1}\mathbb{Z}^2)/\mathbb{Z}^2$  is represented by an element of the form  $a$  or  $-a$  for a unique  $a \in \mathcal{A}_N$ . So for any  $a \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}^2$ , we can use parts (i) and (ii) of Lemma 4.1 to show that

$$g_a = \epsilon \cdot \zeta \cdot g_{a'}$$



for an explicit sign  $\epsilon \in \{\pm 1\}$ ,  $N$ -th root of unity  $\zeta$ , and pair  $a' \in \mathcal{A}_N$ .

**4B. Siegel orbits.** Now fix a congruence subgroup  $\Gamma$  of level  $N > 1$ . For each  $a \in \mathcal{A}_N$  and  $\gamma \in \text{SL}_2(\mathbb{Z})$ , let  $a * \gamma$  be the unique element of  $\mathcal{A}_N$  such that  $a * \gamma$  or  $-a * \gamma$  lies in the coset  $a\gamma + \mathbb{Z}^2$ . The map

$$\mathcal{A}_N \times \text{SL}_2(\mathbb{Z}) \rightarrow \mathcal{A}_N, \quad (a, \gamma) \mapsto a * \gamma$$

then gives a right action of  $\text{SL}_2(\mathbb{Z})$  on  $\mathcal{A}_N$ . In particular, this gives a right action of  $\Gamma$  on  $\mathcal{A}_N$ .

Fix a  $\Gamma$ -orbit  $\mathcal{O}$  of  $\mathcal{A}_N$  and define

$$g_{\mathcal{O}} := \prod_{a \in \mathcal{O}} g_a;$$

it is a holomorphic function  $\mathbb{H} \rightarrow \mathbb{C}^\times$ .

**Lemma 4.2.** *The function  $g_{\mathcal{O}}^{12N}$  is a modular function for  $\Gamma$ . Every pole and zero of  $g_{\mathcal{O}}^{12N}$  on  $X_\Gamma$  is a cusp.*

*Proof.* Take any  $\gamma \in \Gamma$  and  $a \in \mathcal{A}_N$ . By Lemma 4.1(iii), we have  $g_a^{12N}|_\gamma = g_{a\gamma}^{12N}$ . We have  $a\gamma = \epsilon \cdot (a * \gamma + b)$  for some  $\epsilon \in \{\pm 1\}$  and  $b \in \mathbb{Z}^2$ . By parts (i) and (ii) of Lemma 4.1, we find that  $g_a^{12N}|_\gamma = g_{a\gamma}^{12N}$  is equal to  $g_{a*\gamma}^{12N}$ . Therefore,

$$g_{\mathcal{O}}^{12N}|_\gamma = \prod_{a \in \mathcal{O}} g_a^{12N}|_\gamma = \prod_{a \in \mathcal{O}} g_{a*\gamma}^{12N} = g_{\mathcal{O}}^{12N},$$

where the last equality uses the fact that the map  $\mathcal{O} \rightarrow \mathcal{O}$ ,  $a \mapsto a * \gamma$  is a bijection (since  $\mathcal{O}$  is a  $\Gamma$ -orbit). The remaining statement about the poles and zeros of  $g_{\mathcal{O}}^{12N}$  follows immediately since each  $g_a$  is holomorphic and nonzero on  $\mathbb{H}$ .  $\square$

Let  $P_1, \dots, P_r$  be the cusps of  $X_\Gamma$ . Choose a representative  $s_j \in \mathbb{Q} \cup \{\infty\}$  of each cusp  $P_j$  and a matrix  $A_j \in \text{SL}_2(\mathbb{Z})$  satisfying  $A_j \cdot \infty = s_j$ . Let  $w_j$  be the width of the cusp  $P_j$ ; it is the smallest positive integer  $b$  such that  $A_j \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} A_j^{-1}$  is an element of  $\Gamma$ .

For a nonzero meromorphic function  $f$  of  $\mathbb{H}$  given by a  $q$ -expansion, we define  $\text{ord}_q(f)$  to be the smallest rational number  $m$  such that there is a nonzero term of the form  $q^m$  in the expansion of  $f$ . For each cusp  $P_j$ , define the map

$$v_{P_j} : \mathbb{C}(X_\Gamma)^\times \rightarrow \mathbb{Z}, \quad f \mapsto w_j \cdot \text{ord}_q(f|_{A_j});$$

it is a surjective homomorphism and agrees with the valuation giving the order of vanishing of a function at  $P_j$ . We extend  $\text{ord}_q$  and  $v_{P_j}$  by setting  $\text{ord}_q(0) = +\infty$  and  $v_{P_j}(0) = +\infty$ .

We now give a computable expression for the divisor of  $g_{\mathcal{O}}^{12N}$  on  $X_\Gamma$ .

**Lemma 4.3.** *With notation as above, we have*

$$\operatorname{div}(g_{\mathcal{O}}^{12N}) = \sum_{j=1}^r \left( 6N w_j \sum_{a \in \mathcal{O}} B_2(\langle (aA_j)_1 \rangle) \right) \cdot P_j,$$

where  $B_2(x) = x^2 - x + \frac{1}{6}$ ,  $(aA_j)_1$  is the first coordinate of the row vector  $aA_j$ , and  $\langle x \rangle$  denotes the positive fractional part of the real number  $x$ , chosen so  $0 \leq \langle x \rangle < 1$  and  $x - \langle x \rangle \in \mathbb{Z}$ .

*Proof.* For any  $a \in (N^{-1}\mathbb{Z}^2) - \mathbb{Z}^2$ , we have  $\operatorname{ord}_q(g_a) = \frac{1}{2} \cdot B_2(\langle a_1 \rangle)$ ; see [Kubert and Lang 1981, p. 31]. We have

$$v_{P_j}(g_{\mathcal{O}}^{12N}) = \sum_{a \in \mathcal{O}} v_{P_j}(g_a^{12N}) = \sum_{a \in \mathcal{O}} w_j \operatorname{ord}_q(g_a^{12N}|_{A_j}) = \sum_{a \in \mathcal{O}} w_j \operatorname{ord}_q(g_{aA_j}^{12N}),$$

where the last equality uses Lemma 4.1(iii). Therefore,

$$v_{P_j}(g_{\mathcal{O}}^{12N}) = \sum_{a \in \mathcal{O}} 12N w_j \operatorname{ord}_q(g_{aA_j}) = 6N w_j \sum_{a \in \mathcal{O}} B_2(\langle (aA_j)_1 \rangle).$$

Since all poles and zeros of  $g_{\mathcal{O}}^{12N}$  are cusps, we have  $\operatorname{div}(g_{\mathcal{O}}^{12N}) = \sum_{i=1}^r v_{P_i}(g_{\mathcal{O}}^{12N}) \cdot P_i$ , and the lemma follows immediately. □

**4C. Constructing hauptmoduls of prime power level.** Fix a congruence subgroup  $\Gamma$  of  $\operatorname{SL}_2(\mathbb{Z})$  of prime power level  $N > 1$  that has genus 0. Let  $P_1, \dots, P_r$  be the cusps of  $\Gamma$ ; we choose our cusps so that  $P_1$  is the cusp at  $\infty$ .

In this section, we explain how to construct an explicit hauptmodul of  $\Gamma$  whose  $q$ -expansion has coefficients in  $K_N$ . Moreover, our hauptmodul will be of the form

$$\sum_{i=1}^M \zeta_{2N^2}^{e_i} \prod_{a \in \mathcal{A}_N} g_a^{m_{a,i}} \tag{4-3}$$

with integers  $m_{a,i}$  and  $e_i$ .

*Case 1: multiple cusps.* First assume that  $\Gamma$  has at least two cusps. We will use the following lemma to construct a hauptmodul for certain genus 0 congruence subgroups.

Let  $\mathcal{O}_1, \dots, \mathcal{O}_n$  be the distinct  $\Gamma$ -orbits of  $\mathcal{A}_N$ . For each  $\mathcal{O}_i$ , define the divisor  $D_i := \operatorname{div}(g_{\mathcal{O}_i}^{12N})$  on  $X_\Gamma$ . By Lemma 4.3, the divisors  $D_1, \dots, D_n$  are supported on  $\{P_1, \dots, P_r\}$  and are straightforward to compute.

**Lemma 4.4.** *Suppose there is an  $n$ -tuple  $m \in \mathbb{Z}^n$  such that*

$$\sum_{i=1}^n m_i D_i = -12N \cdot P_1 + 12N \cdot P_2.$$

Let  $0 \leq e < 2N^2$  be the integer satisfying  $e \equiv \sum_{i=1}^n m_i \sum_{a \in \mathcal{O}_i} Na_2(N - Na_1) \pmod{2N^2}$ . Then

$$h := \zeta_{2N^2}^e \prod_{i=1}^n g_{\mathcal{O}_i}^{m_i}$$

is a hauptmodul for  $\Gamma$  whose  $q$ -expansion has coefficients in  $K_N$ . On  $X_\Gamma$ , we have  $\text{div}(h) = -P_1 + P_2$ .

*Proof.* Since  $X_\Gamma$  has genus 0, there is a meromorphic function  $f$  on  $X_\Gamma$  with  $\text{div}(f) = -P_1 + P_2$ . Lemma 4.2 implies that  $f^{12N}/h^{12N}$  defines a function on  $X_\Gamma$ ; it has divisor

$$12N \text{div}(f) - \sum_{i=1}^n m_i \text{div}(g_{\mathcal{O}_i}^{12N}) = 12N(-P_1 + P_2) - \sum_{i=1}^n m_i D_i = 0,$$

where the last equality uses our assumption on  $m$ . Therefore,  $f^{12N}/h^{12N}$  is constant. Since  $f$  and  $h$  are meromorphic functions on the upper half-plane, we deduce that  $f/h$  is a (nonzero) constant. In particular,  $h$  is modular for  $\Gamma$  and  $\text{div}(h) = -P_1 + P_2$ . The function  $h$  on  $X_\Gamma$  is a hauptmodul for  $\Gamma$  since its only pole is the simple pole at  $P_1$ , i.e., the cusp at  $\infty$ .

It remains to show that the coefficients of  $h$  lie in  $K_N$ . Take any  $a \in \mathcal{A}_N$ . From the series defining  $g_a$ , we find that  $a$  equals the root of unity  $e(\frac{1}{2}a_2(a_1 - 1)) = \zeta_{2N^2}^{Na_2(Na_1 - N)}$  times a Laurent series in  $q^{1/(6N^2)}$  with coefficients in  $K_N$ . Set

$$e' := \sum_{i=1}^n m_i \sum_{a \in \mathcal{O}_i} Na_2(Na_1 - N).$$

The coefficients of  $\zeta_{2N^2}^{-e'} \prod_{i=1}^n g_{\mathcal{O}_i}^{m_i}$  thus all lie in  $K_N$ . The lemma follows since  $e \equiv -e' \pmod{2N^2}$ . □

Using the Cummins–Pauli classification of genus 0 congruence subgroups [Cummins and Pauli 2003], we have explicitly verified that the  $n$ -tuple  $m$  from Lemma 4.4 always exists. Using Lemma 4.3, the existence of  $m$  comes down to finding integral solutions to  $r$  linear equations with integer coefficients in  $n$  variables. Using Lemma 4.4, we can thus find an explicit hauptmodul for  $\Gamma$  of the form (4-3) with  $M = 1$  (we have  $m_{a,i} = m_i$  if  $a \in \mathcal{O}_i$ ).

**Remark 4.5.** One can also abstractly prove the existence of the  $n$ -tuple  $m$ . If  $N$  is an odd prime power, then any modular function of level  $N$  whose zeros and poles are all cusps can be expressed as a constant times a product of Siegel functions  $g_a$  with  $a \in N^{-1}\mathbb{Z}^2 - \mathbb{Z}$ ; see [Kubert and Lang 1981, Chapter 5, Theorem 1.1(i)].

If  $N \geq 4$  is a power of 2, this can also be deduced from [loc. cit.]. (One needs to be a little careful here since  $g_a$  has a different definition in [Kubert and Lang 1981, Chapter 4, §1] when  $2a \in \mathbb{Z}$ . For the alternate  $g_a$  from the previous work

with  $2a \in \mathbb{Z}$ , one can express them as a constant times a product of Siegel functions  $g_{a'}$  with  $a' \in \mathcal{A}_4 \subseteq \mathcal{A}_N$ .)

The case  $N = 2$  can be handled directly. For example, one can show that

$$g_{(1/2,0)}^8 \cdot g_{(1/2,1/2)}^4 \quad \text{and} \quad g_{(1/2,0)}^{12} \cdot g_{(1/2,1/2)}^{12}$$

are hauptmoduls for  $\Gamma(2)$  and  $\Gamma_0(2)$ , respectively (note that  $\Gamma_{\text{ns}}(2)$  has a single cusp and does not fall into this case; it falls into case 2 below).

*Case 2: a single cusp and  $N \neq 11$ .* Now assume that  $X_\Gamma$  has a single cusp and that  $N \neq 11$ . There are no nonconstant modular functions for  $\Gamma$  whose zeros and poles are only at the cusps of  $X_\Gamma$ . In particular, a hauptmodul of  $\Gamma$  is never be equal to a product of Siegel functions.

Using the Cummins–Pauli classification, we find that there is a congruence subgroup  $\Gamma'$  that is a proper normal subgroup of  $\Gamma$ , also of level  $N$  and containing  $-I$ , such that  $X_{\Gamma'}$  has genus 0 and has exactly  $[\Gamma : \Gamma']$  cusps (this is where we use  $N \neq 11$ ).

Since  $X_{\Gamma'}$  has multiple cusps, we know from Case 1 how to construct a hauptmodul  $h'$  of  $\Gamma'$  with coefficients in  $K_N$  that is of the form (4-3). Using that  $\Gamma'$  is normal in  $\Gamma$ , we find that  $h'|_\gamma$  is modular for  $\Gamma'$  for all  $\gamma \in \Gamma$  and the function depends only on the coset  $\Gamma' \cdot \gamma$ . Define

$$h := \sum_{\gamma \in \Gamma \backslash \Gamma} h'|_\gamma;$$

it is a modular function for  $\Gamma$ . Since  $X_\Gamma$  has only one cusp and  $X_{\Gamma'}$  has  $[\Gamma : \Gamma']$  cusps, we deduce that the modular functions  $\{h'|_\gamma\}_{\gamma \in \Gamma \backslash \Gamma}$  on  $X_{\Gamma'}$  each have their unique (simple) pole at different cusps. This implies that  $h$  has a simple pole at the unique cusp of  $X_\Gamma$  and is holomorphic elsewhere. Therefore,  $h$  is a hauptmodul for  $\Gamma$ .

Since  $h'$  is modular for  $\Gamma(N)$  and has coefficients in  $K_N$ , so does  $h'|_\gamma$  for all  $\gamma \in \text{SL}_2(\mathbb{Z})$ ; see Proposition 2.2. Therefore, the coefficients of  $h$  lie in  $K_N$ .

Finally, it remains to show that  $h$  is of the form (4-3). It suffices to show that  $h'|_\gamma$  is of the form (4-3) for a fixed  $\gamma \in \Gamma$ . We know that  $h'$  is equal to some product  $\zeta_{2N^2}^e \prod_{a \in \mathcal{A}_N} g_a^{m_a}$ , so

$$h|_\gamma = \varepsilon(\gamma)^b \zeta_{2N^2}^e \prod_{a \in \mathcal{A}_N} g_{a\gamma}^{m_a}$$

with  $b := \sum_{a \in \mathcal{A}_N} m_a$  by Lemma 4.1(iii). Recall that for each  $a \in \mathcal{A}_N$ , there is a unique  $a * \gamma \in \mathcal{A}_N$  such that  $a\gamma$  lies in the same coset of  $(N^{-1}\mathbb{Z}^2)/\mathbb{Z}^2$  as  $a * \gamma$  or  $-a * \gamma$ . From Lemma 4.1(i) and (ii), the functions  $g_{a\gamma}^{m_a}$  and  $g_{a*\gamma}^{m_a}$  agree up to a multiplication by some computable root of unity  $-\zeta_N^{e'}$ . Therefore,  $h|_\gamma$  is equal to  $\varepsilon(\gamma)^b$  times a function of the form (4-3) with  $M = 1$ .

It remains only to show that  $\varepsilon(\gamma)^b$  is a power of a  $2N^2$ -th root of unity. Kubert and Lang [1981, Chapter 3, §5] give a necessary and sufficient condition for the

product  $\prod_{a \in \mathcal{A}_N} g_a^{m_a}$  to be modular for  $\Gamma(N)$ ; these conditions hold since  $h'$  is modular for  $\Gamma' \supseteq \Gamma(N)$ . If  $N$  is a power of a prime  $\ell \geq 5$ , then [Kubert and Lang 1981, Chapter 3, Theorem 5.2] implies that  $b \equiv 0 \pmod{12}$  and hence  $\varepsilon(\gamma)^b = 1$ . If  $N$  is a power of 3, then [Kubert and Lang 1981, Chapter 3, Theorem 5.3] implies that  $b \equiv 0 \pmod{4}$  and hence  $\varepsilon(\gamma)^b$  is a power of  $\zeta_3$ . If  $N$  is a power of 2, then [Kubert and Lang 1981, Chapter 3, Theorem 5.3] implies that  $b \equiv 0 \pmod{3}$  and hence  $\varepsilon(\gamma)^b$  is a power of  $\zeta_4$ . Therefore,  $\varepsilon(\gamma)^b$  is indeed a power of a  $2N^2$ -th root of unity.

*Case 3:*  $N = 11$ . The remaining case is when  $X_\Gamma$  has a single cusp and  $N = 11$ . We include this case only for completeness; we will not need it for our application.

Define the function

$$f(\tau) := \prod_{(a_1, a_2) \in B} g_{(a_1/11, a_2/11)}(\tau),$$

where

$$B := \{(0, 1), (0, 2), (0, 3), (1, 0), (1, 2), (1, 5), (1, 7), (2, 1), (2, 2), (2, 4), (2, 5), (2, 6), (2, 7), (2, 8), (2, 9), (2, 10), (3, 0), (3, 2), (3, 4), (3, 5), (3, 6), (3, 8), (3, 10), (4, 0), (4, 1), (4, 2), (4, 4), (4, 5), (4, 6), (5, 1), (5, 4), (5, 5), (5, 6), (5, 7), (5, 8), (5, 9)\}.$$

One can verify that

$$\sum_{(a_1, a_2) \in B} a_1^2 \equiv \sum_{(a_1, a_2) \in B} a_2^2 \equiv \sum_{(a_1, a_2) \in B} a_1 a_2 \equiv 0 \pmod{11}$$

and that  $|B| = 36 \equiv 0 \pmod{12}$ . Theorem 5.2 of [Kubert and Lang 1981, Chapter 3, §5] implies that  $f$  is a modular function for  $\Gamma(11)$ . Using

$$\sum_{(a_1, a_2) \in B} \frac{1}{11} a_2 \cdot \frac{\frac{1}{11} a_1 - 1}{2} = -\frac{60}{11}$$

and the  $q$ -expansion of Siegel functions from Section 4A, we find that all the coefficients of  $f$  lie in  $K_{11}$ . Therefore,  $f \in \mathcal{F}_{11}$ .

Using that  $\Gamma(11)$  is normal in  $\Gamma$ , we find that  $f|_\gamma$  is modular for  $\Gamma(11)$  for all  $\gamma \in \Gamma$  and the function depends only on the coset  $\Gamma(11) \cdot \gamma$ . Define

$$h := \sum_{\gamma \in \Gamma(11) \backslash \Gamma} f|_\gamma;$$

it is a modular function for  $\Gamma$ . That  $h$  is of the form (4-3) follows as in the previous case.

We claim that  $h$  is a hauptmodul for  $\Gamma$ . From our description of  $h$  in terms of Siegel functions, we find that  $h$  has no poles except possibly at the unique cusp

(at  $\infty$ ). From [Cummins and Pauli 2003], there is a unique genus 0 congruence subgroup of  $\mathrm{SL}_2(\mathbb{Z})$  of level 11 up to conjugacy in  $\mathrm{GL}_2(\mathbb{Z})$  (the one labeled  $11A^0$ ). We have computed all the possible  $\Gamma$  and shown that  $h$  has a simple pole at  $\infty$ , and is therefore a hauptmodul.

**Remark 4.6.** The set  $B$  comes from Section 5.3 of [Chua et al. 2004]. That work gives methods to compute hauptmoduls for genus 0 congruence subgroups (unfortunately, the accompanying hauptmodul tables are no longer available). The authors use “generalized Dedekind eta functions”, which are essentially Siegel functions.

**4D. The rational function  $J(t)$ .** For a hauptmodul  $h$  of  $\Gamma$ , there is a unique function  $J(t) \in \mathbb{C}(t)$  such that  $J(h) = j$ ; it has degree  $d := [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma]$ .

Let us briefly explain how to compute  $J(t)$  assuming that one can compute sufficiently many terms of the expansion of  $f$ . Let  $K \subseteq \mathbb{C}$  be a field containing all the coefficients of  $h$ . Consider the equation

$$(a_d h^d + \cdots + a_1 h + a_0) - j \cdot (b_d h^d + \cdots + b_1 h + b_0) = 0 \tag{4-4}$$

with unknowns  $a_i, b_i \in K$ , where  $d := [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma]$ . Computing the  $q$ -expansion coefficients of the left-hand side of (4-4) yields a system of homogeneous linear equations in the unknowns  $a_i$  and  $b_i$ . The existence and uniqueness of  $J$  ensure that the solutions  $(a_1, \dots, a_d, b_1, \dots, b_d) \in K^{2d}$  form a one-dimensional subspace. By computing sufficiently many coefficients of (4-4) one can find a nonzero solution  $(a_1, \dots, a_d, b_1, \dots, b_d) \in K^{2d}$ , unique up to scaling by  $K^\times$ , and

$$J(t) = \frac{a_d t^d + \cdots + a_1 t + a_0}{b_d t^d + \cdots + b_1 t + b_0} \in K(t)$$

is then the unique rational function for which  $J(h) = j$ . Note that if the hauptmodul  $h$  is constructed as in the previous section then we have  $J(t) \in K_N(t)$ , where  $N$  is the level of  $\Gamma$ .

### 5. Modular curves of genus 0

Fix the following:

- An integer  $N > 1$  that is a prime power.
- A subgroup  $G$  of  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  satisfying  $-I \in G$  and  $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ .
- A rational function  $J(t) \in \mathbb{Q}(t)$ .

In this section, we explain how to determine if the function field of  $X_G$  is of the form  $\mathbb{Q}(f)$  for some modular function  $f \in \mathcal{F}_N$  satisfying  $J(f) = j$ . We will use this to verify the entries of Tables 1–3, found in the online supplement.

If such an  $f$  exists, then  $X_G \simeq \mathbb{P}_{\mathbb{Q}}^1$  and the isomorphism  $\pi_G : X_G \rightarrow \mathbb{P}_{\mathbb{Q}}^1$  is given

by the relation  $j = J(f)$  in their function fields. We may assume the necessary condition that  $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G] = \deg \pi_G$  agrees with the degree of  $J(t)$ .

**Remark 5.1.** In Section 8 we explain how the  $J(t)$  listed in Tables 1–3 of the online supplement, were actually found, which involves the use of a Monte Carlo algorithm and assumes the generalized Riemann hypothesis (GRH). The purpose of this section is to explain how we can unconditionally verify a given  $J(t)$ , regardless of how it was found.

**5A. Construction of possible  $f$ .** Let  $\Gamma$  be the congruence subgroup consisting of  $\gamma \in \mathrm{SL}_2(\mathbb{Z})$  for which  $\gamma^t$  modulo  $N$  lies in  $G$  (equivalently, in  $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ ). By Lemma 2.4(ii), we may assume that  $\Gamma$  has genus 0 since otherwise  $X_G$  has positive genus and its function field cannot be of the form  $\mathbb{Q}(f)$ .

The group  $\Gamma$  acts on the right on the field  $\mathcal{F}_N$ ; let  $\mathcal{F}_N^\Gamma$  be subfield fixed by this action. By Lemma 2.4(i), we have  $K_N(X_G) = \mathcal{F}_N^\Gamma$ .

In Section 4C, we described how to compute an explicit hauptmodul  $h$  for  $\Gamma$  such that coefficients of its  $q$ -expansion all lie in  $K_{N'} \subseteq K_N$ , where the level  $N'$  of  $\Gamma$  divides  $N$ . Therefore, we have

$$K_N(X_G) = \mathcal{F}_N^\Gamma = K_N(h).$$

Moreover, we can express  $h$  in terms of Siegel functions and hence we can compute as many of its coefficients as we desire. In Section 4D, we described how to compute the unique rational function  $J'(t) \in K_N(t)$  for which  $j = J'(h)$ . The degree of  $J'(t)$  agrees with  $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$ , thus  $J(t)$  and  $J'(t)$  have the same degree.

**Remark 5.2.** The rational function  $J'(t)$  gives a map to the  $j$ -line from  $X_\Gamma$ , which is defined over  $K_N = \mathbb{Q}(\zeta_N)$ , while the rational function  $J(t)$  gives a map to the  $j$ -line from  $X_G$ , which is defined over  $\mathbb{Q}$ . We use  $J'(t)$  in our procedure to verify  $J(t)$ , but note that  $J'(t)$  does not determine  $J(t)$ ; in general there will be multiple nonconjugate subgroups  $G$  corresponding to  $\Gamma$  and a different rational function  $J(t)$  for each of the corresponding  $X_G$  (in total we have 220 modular curves  $X_G$  of genus 0 corresponding to 73 modular curves  $X_\Gamma$ ).

**Lemma 5.3.** *The modular functions  $f \in K_N(X_G)$  that satisfy  $K_N(X_G) = K_N(f)$  and  $J(f) = j$  are precisely those of the form  $\psi(h)$ , where  $\psi(t) \in K_N(t)$  is a degree 1 function satisfying  $J'(t) = J(\psi(t))$ .*

*Proof.* First take any  $\psi(t) \in K_N(t)$  of degree 1 satisfying  $J'(t) = J(\psi(t))$ . Define  $f := \psi(h)$ . We have  $K_N(f) = K_N(h) = K_N(X_G)$ , since  $\psi$  has an inverse, and  $J(f) = J(\psi(h)) = J'(h) = j$ .

Now suppose that  $K_N(X_G) = K_N(f)$  for some  $f \in K_N(X_G)$  satisfying  $J(f) = j$ . Since  $K_N(f) = K_N(X_G) = K_N(h)$ , we have  $f = \psi(h)$  for a unique  $\psi(t) \in K_N(t)$

of degree 1. We then have  $j = J(f) = J(\psi(h))$  and therefore  $J'(t) = J(\psi'(t))$ , since  $J'(t)$  is the unique element of  $K_N(t)$  that satisfies  $J'(h) = j$ .  $\square$

**5B. Finding possible  $f$ .** Define  $\Psi$  to be the set of  $\psi(t) \in K_N(t)$  of degree 1 for which  $J'(t) = J(\psi'(t))$ ; these  $\psi$  arise in Lemma 5.3. We now explain how to compute  $\Psi$ .

Choose three distinct elements  $\beta_1, \beta_2, \beta_3 \in K_N \cup \{\infty\}$ . For  $1 \leq i \leq 3$ , define the set

$$R_i := \{ \alpha \in K_N \cup \{\infty\} : J'(\beta_i) = J(\alpha) \text{ and } \text{ord}_{\beta_i}(J') = \text{ord}_{\alpha}(J) \},$$

where  $\text{ord}_{\beta_i}(J')$  is the order of vanishing of  $J'(t)$  at  $t = \beta_i$ . Let  $R$  be the set of triples  $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in R_1 \times R_2 \times R_3$  such that  $\alpha_1, \alpha_2$ , and  $\alpha_3$  are distinct. Let  $\psi_\alpha \in K_N(t)$  be the *unique* rational function of degree 1 such that  $\psi_\alpha(\beta_i) = \alpha_i$  for all  $1 \leq i \leq 3$ .

Take any  $\psi \in \Psi$ . We have  $J'(\beta_i) = J(\psi'(\beta_i))$  and  $\text{ord}_{\beta_i}(J') = \text{ord}_{\psi(\beta_i)}(J)$  for each  $1 \leq i \leq 3$ . Therefore,  $\psi(\beta_i) \in R_i$  for each  $1 \leq i \leq 3$  and hence  $\psi = \psi_\alpha$  for some  $\alpha \in R$ . So we have

$$\Psi = \{ \psi_\alpha : \alpha \in R, J'(t) = J(\psi'(t)) \}.$$

Since  $R$  is finite, this gives us a way to compute the (finite) set  $\Psi$ .

By Lemma 5.3, the set

$$\{ \psi(h) : \psi \in \Psi \}$$

is the set of modular functions  $f \in K_N(X_G)$  that satisfy  $K_N(X_G) = K_N(f)$  and  $J(f) = j$ .

**5C. Checking each  $f$ .** Let  $f$  be one of the finite number of functions that satisfy  $K_N(X_G) = K_N(f)$  and  $J(f) = j$ . We just saw how to compute all such  $f$ ; they are of the form  $\psi(h)$  for a degree 1 function  $\psi(t) \in K_N(t)$  and a modular function  $h$  satisfying  $K_N(X_G) = K_N(h)$  that is expressed in terms of Siegel functions. Recall from Section 2D that each  $A \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$  acts on  $\mathcal{F}_N$  via the isomorphism  $\theta_N : \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \xrightarrow{\sim} \text{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$  of Proposition 2.2, and for  $f \in \mathcal{F}_N$  we use  $A_*(f) := \theta_N(A)(f)$  to denote this action.

**Lemma 5.4.** (i) We have  $\mathbb{Q}(X_G) = \mathbb{Q}(f)$  if and only if  $f \in \mathbb{Q}(X_G)$ .

(ii) For a matrix  $A \in G$ , we have  $A_*(f) = f$  if and only if  $\text{ord}_q(A_*(f) - f) > 2w/N'$ , where  $w$  is the width of the cusp  $\infty$  of  $X_\Gamma$  and  $N'$  is the level of  $\Gamma$ .

*Proof.* We first prove part (i); only one implication needs proof. Suppose that  $f \in \mathbb{Q}(X_G)$ . Then  $\mathbb{Q}(f) \subseteq \mathbb{Q}(X_G)$  and it suffices to show that these two fields have the same degree over  $\mathbb{Q}(j)$ . This is true since we have been assuming that  $\text{deg } \pi_G$  is equal to the degree of  $J(t)$ .



For part (ii), again only one implication needs proof. Suppose  $\text{ord}_q(A_*(f) - f) > 2w/N'$ . As meromorphic functions on  $X_\Gamma$ ,  $f$  and  $A_*(f)$  have a unique (simple) pole since  $h$  has this property and  $\psi$  has degree 1. Therefore, the function  $A_*(f) - f$  on  $X_\Gamma$  is zero or has at most two poles (and hence at most two zeros). Our assumption  $\text{ord}_q(A_*(f) - f) > 2w/N'$  implies that  $A_*(f) - f$  has a zero of order 3 at the cusp  $\infty$  and thus  $A_*(f) - f = 0$ .  $\square$

By Lemma 5.4(i), we have  $\mathbb{Q}(X_G) = \mathbb{Q}(f)$  if and only if  $A_*(f) = f$  for all  $A \in G$  in a set of generators of  $G$ ; it suffices to consider  $A \in G$  for which  $\det(A)$  generate  $(\mathbb{Z}/N\mathbb{Z})^\times$  since  $h$  and hence  $f$  is fixed by  $G \cap \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ . It remains to describe how to determine whether  $A_*(f)$  is equal to  $f$ . By Lemma 5.4(ii), it suffices to compute enough terms of the  $q$ -expansion of  $A_*(f) - f$  to determine whether  $\text{ord}_q(A_*(f) - f) > 2w/N'$  holds.

Finally, let us briefly explain how to compute terms in the  $q$ -expansion of  $A_*(f) - f$ . Let  $d$  be an odd integer congruent to  $\det(A)$  modulo  $N$ . Choose a matrix  $\gamma \in \text{SL}_2(\mathbb{Z})$  so that  $A^t \equiv \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \gamma \pmod{N}$ . We thus have

$$A_*(f) - f = \sigma_d(f)|_\gamma - f = \sigma_d(\psi)(\sigma_d(h)|_\gamma) - \psi(h), \tag{5-1}$$

where  $\sigma_d(\psi)$  is the rational function with  $\sigma_d$  applied to the coefficients of its numerator and denominator. Our hauptmodul  $h$  is of the form  $\sum_{i=1}^M \zeta_{2N^2}^{e_i} \prod_{a \in \mathcal{A}_N} g_a^{m_{a,i}}$  for certain integers  $e_i$  and  $m_{a,i}$ , so

$$\sigma_d(h)|_\gamma = \sum_{i=1}^M \zeta_{2N^2}^{e_i d} \prod_{a \in \mathcal{A}_N} (\sigma_d(g_a)|_\gamma)^{m_{a,i}}.$$

From the series expansion of  $g_a$ , one easily checks that  $\sigma_d(g_{(a_1, a_2)}) = g_{(a_1, da_2)}$ . From Lemma 4.1(iii), we have  $\sigma_d(g_a)|_\gamma = \varepsilon(\gamma)g_{(a_1, da_2)\gamma}$  and hence

$$\sigma_d(h)|_\gamma = \sum_{i=1}^M \zeta_{2N^2}^{e_i d} \cdot \prod_{a \in \mathcal{A}_N} \varepsilon(\gamma)^{m_{a,i}} \cdot \prod_{a \in \mathcal{A}_N} g_{(a_1, da_2)\gamma}^{m_{a,i}}.$$

Thus by computing enough terms in the  $q$ -expansion of the functions  $\{g_a\}_{a \in \mathcal{A}_N}$ , we are able to compute the  $q$ -expansion of  $h$  and  $\sigma_d(h)|_\gamma$  to as many terms as we desire. This allows us to compute terms in the  $q$ -expansion of  $A_*(f) - f$  via (5-1).

**Remark 5.5.** Suppose that  $X_\Gamma$  has at least 3 cusps. We then have  $A_*(f) = f$  if and only if  $A_*(f)$  and  $f$  take the same value at any three of the cusps (as in the proof of Lemma 5.4, this implies that  $A_*(f) - f$  has at least three zeros and hence is the zero function). In the case of at least three cusps, our hauptmodul  $h$  was given as a constant times a product of Siegel functions; so its value at the cusp  $\infty$  is determined by the first term of the  $q$ -expansion of  $h$ . The value at any other cusp  $c$  can be determined by the first term of the  $q$ -expansion of  $h|_\gamma$  with  $\gamma \in \text{SL}_2(\mathbb{Z})$

satisfying  $\gamma\infty = c$ . This approach is quicker since fewer terms of the  $q$ -expansions are required.

**5D. Verifying the entries of our tables.** We now explain how to verify the validity of our genus 0 tables. Magma scripts that perform these verifications can be found in [Sutherland and Zywina 2016].

In the online supplement, each row of Tables 1–3 gives a set of generators of a subgroup  $G$  of  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  that satisfies  $-I \in G$  and  $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$  for a prime power  $N$ . We may assume that  $N > 1$ . By composing rational maps, we obtain a corresponding rational function  $J(t) \in \mathbb{Q}(t)$ .

Using the earlier parts of Section 5, we can construct a modular function  $f \in \mathcal{F}_N$  such that  $\mathbb{Q}(X_G) = \mathbb{Q}(f)$  and  $J(f) = j$ . So  $X_G$  is isomorphic to  $\mathbb{P}_{\mathbb{Q}}^1$  and the morphism  $\pi_G : X_G \rightarrow \mathbb{P}_{\mathbb{Q}}^1$  is given by the relation  $j = J(f)$  in their function fields. (We also note that there is no harm in replacing  $G$  by a conjugate group; this is useful because one can reuse the hauptmodul computations for different groups in the tables.)

Fix a group  $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  as above, and a modular function  $f \in \mathcal{F}_N$  satisfying  $\mathbb{Q}(X_G) = \mathbb{Q}(f)$  and  $J(f) = j$ .

Now fix another group  $G' \subseteq \mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z})$  from our table so that  $N$  divides  $N'$  and the image of  $G'$  in  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  is conjugate to a subgroup of  $G$ . In the above computations, we have constructed a modular function  $f'$  satisfying  $\mathbb{Q}(X_{G'}) = \mathbb{Q}(f')$  and  $J'(f') = j$  for a rational function  $J'(t) \in \mathbb{Q}(t)$  also arising from the tables.

Take any subgroup  $\tilde{G} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  conjugate to  $G'$  whose image modulo  $N$  lies in  $G$ . Choose any  $A \in \mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z})$  for which  $\tilde{G} := A G' A^{-1}$  and define  $\tilde{f} := A_*(f')$ . We have an inclusion of fields

$$\mathbb{Q}(\tilde{f}) = \mathbb{Q}(X_{\tilde{G}}) \supseteq \mathbb{Q}(X_G) = \mathbb{Q}(f).$$

The extension  $\mathbb{Q}(\tilde{f})/\mathbb{Q}(f)$  has degree  $i := [\mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z}):G']/[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}):G]$ . Therefore,  $\varphi(\tilde{f}) = f$  for a unique  $\varphi(t) \in \mathbb{Q}(t)$  of degree  $i$ . We can compute  $\varphi(t)$  using the method from Section 4D; the coefficients of  $f$  and  $\tilde{f}$  can be computed as in Section 5C.

The rational function  $\varphi$  is not unique, it depends on the choices of  $\tilde{G}$ ,  $f$ ,  $f'$ , and  $A$ . However, any other rational function occurring would be of the form  $\psi'(\varphi(\psi(t)))$ , where  $\psi, \psi' \in \mathbb{Q}(t)$  are degree 1 functions satisfying  $J(\psi(t)) = J(t)$  and  $J'(\psi'(t)) = J'(t)$ . Note that all the possible  $\psi$  and  $\psi'$  can be computed as in Section 5B (with  $J = J'$ ). We have checked that the rational function relating  $G$  and  $G'$  in our tables, when given, is indeed of the form  $\psi'(\varphi(\psi(t)))$ .

### 6. Modular curves of genus 1

We now consider the open subgroups  $G$  of  $\mathrm{GL}_2(\hat{\mathbb{Z}})$  with genus 1 and prime power level  $N = \ell^e$  that satisfy  $-I \in G$  and  $\det(G) = \hat{\mathbb{Z}}^\times$ . We are interested in describing those  $G$  for which  $X_G(\mathbb{Q})$  is infinite. There is no harm in replacing  $G$  by a conjugate. So by Theorem 3.3(ii), there are 250 cases that need to be checked.

Let  $J_G$  be the Jacobian of the curve  $X_G$ . Using the methods of [Zywina 2015b], we can compute the rank of  $J_G(\mathbb{Q})$ . From [Deligne and Rapoport 1973, §IV], we find that the curve  $X_G$  has good reduction at all primes  $p \nmid N = \ell^e$ . Therefore,  $J_G$  is an elliptic curve defined over  $\mathbb{Q}$  whose conductor is a power of  $\ell$ . The primes  $\ell$  that arise are small enough to ensure that  $J_G$  is isomorphic to one of the elliptic curves in Cremona’s [2016] tables; this gives a finite number of candidates for  $J_G$  up to isogeny.

For each prime  $p \nmid 6\ell$ , we can compute  $\#J_G(\mathbb{F}_p) = \#X_G(\mathbb{F}_p)$  from the modular interpretation of  $X_G$ ; see [Zywina 2015b, §3.6] for details. In particular, we can compute  $\#J_G(\mathbb{F}_p)$  directly from the group  $G$  without computing a model for  $X_G$  (or its reduction modulo  $p$ ). By computing several values of  $\#J_G(\mathbb{F}_p)$  with  $p \neq \ell$ , we can quickly distinguish the isogeny class of  $J_G$  among the finite set of candidates. We then compute the rank of  $J_G(\mathbb{Q})$ , which we note is an isogeny invariant.

Running this procedure on each of the 250 genus 1 groups  $G$  given by Theorem 3.3, we find that  $J_G(\mathbb{Q})$  has rank 0 for 222 groups and  $J_G(\mathbb{Q})$  has positive rank for 28 groups; a Magma script that performs this computation can be found in [Sutherland and Zywina 2016]. We need only consider the 28 groups  $G$  for which  $J_G(\mathbb{Q})$  has positive rank, since  $X_G(\mathbb{Q})$  is finite if  $J_G(\mathbb{Q})$  has rank 0.

Now let  $G$  be one of the 28 groups for which  $J_G(\mathbb{Q})$  has positive rank; they are precisely the 28 genus 1 groups in Theorem 1.1 and can be found in Table 4 of the online supplement. For each of these groups  $G$ , if  $X_G(\mathbb{Q})$  is nonempty then it must be infinite, since the Abel–Jacobi map then gives a bijection from  $X_G(\mathbb{Q})$  to  $J_G(\mathbb{Q})$ . We initially verified that  $X_G(\mathbb{Q})$  is nonempty by finding an elliptic curve  $E/\mathbb{Q}$  with  $\rho_E(\mathrm{Gal}_{\mathbb{Q}}) \subseteq G$  using an extension of the algorithm in [Sutherland 2016].

For each of these 28 groups  $G$ , a model for  $X_G$  and the morphism  $\pi_G$  can already be found in the literature (and are equivalent to the ones we give in the online supplement). For the 27 groups  $G$  of level 16 these curves and morphisms were constructed in [Rouse and Zureick-Brown 2015]; the models and morphisms we give in Table 4 for these groups are slightly different (we constructed them by taking fiber products of our genus 0 curves), but we have verified that they are isomorphic (note that their groups are transposed relative to ours). The remaining group  $G$  has level 11 and its image in  $\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$  is the normalizer of a nonsplit Cartan subgroup. An explicit model for  $X_G = X_{\mathrm{ns}}^+(11)$  and the morphism to the  $j$ -line can be found in [Halberstadt 1998]; these are reproduced in the online supplement.

### 7. Proof of Theorem 1.4

If  $\ell \leq 13$ , then the set  $\mathcal{J}_\ell$  is finite by [Zywina 2015b, Proposition 4.8]. If  $\ell > 13$ , this follows from [Zywina 2015b, Proposition 4.9]; note that  $\rho_{E, \ell^\infty}$  is surjective if and only if  $\rho_{E, \ell}$  is surjective, since  $\ell \geq 5$ , by [Serre 1968, §IV, Lemma 3]. This proves (i).

For a group  $G$  from Theorem 1.1, define the set

$$\mathcal{S}_G := \bigcup_{G'} \pi_{G', G}(X_{G'}(\mathbb{Q})),$$

where  $G'$  varies over the proper subgroups of  $G$  that are conjugate to one of the groups in Theorem 1.1 of  $\ell$ -power level and  $\pi_{G', G} : X_{G'} \rightarrow X_G$  is the natural morphism induced by the inclusion  $G' \subseteq G$ . Note that this is a finite union.

Suppose first that  $G$  has genus 0. Then  $X_G \simeq \mathbb{P}_{\mathbb{Q}}^1$  and  $\mathcal{S}_G$  is a *thin* subset of  $X_G(\mathbb{Q})$ , in the language of [Serre 1997, §9]. The field  $\mathbb{Q}$  is Hilbertian, and in particular  $\mathbb{P}_1(\mathbb{Q}) \simeq X_G(\mathbb{Q})$  is not thin; this implies that the complement  $X_G(\mathbb{Q}) - \mathcal{S}_G$  cannot be thin and must be infinite.

Suppose that  $G$  has genus 1. If  $G$  does not have level 16 and index 24, then there are no proper subgroups  $G'$  of  $G$  that are conjugate to a group from Theorem 1.1, and therefore  $\mathcal{S}_G$  is empty and  $X_G(\mathbb{Q}) - \mathcal{S}_G$  is infinite.

Now suppose that  $G$  has genus 1, level 16, and index 24. There are 7 such  $G$ , labeled

$$16C^1-16c, 16C^1-16d, 16B^1-16a, 16B^1-16c, 16D^1-16d, 8D^1-16b, 8D^1-16c$$

and explicitly described in Table 4 of the online supplement. Each of these  $G$  contains either two or four index 2 subgroups  $G'$  that are conjugate to one of the groups in Theorem 1.1. In every case we have  $\mathcal{S}_G = X_G(\mathbb{Q})$ , so that  $X_G(\mathbb{Q}) - \mathcal{S}_G$  is empty; see [Rouse and Zureick-Brown 2015, Example 6.11, Remark 6.3].

Let  $E/\mathbb{Q}$  be an elliptic curve with  $j_E \notin \mathcal{J}_\ell$ . The group  $\pm \rho_{E, \ell^\infty}(\text{Gal}_{\mathbb{Q}})$  is conjugate in  $\text{GL}_2(\mathbb{Z}_\ell)$  to the  $\ell$ -adic projection of a unique group  $G$  from Theorem 1.1 with  $\ell$ -power level. Using Proposition 2.6, we can also characterize  $G$  as the unique group from Theorem 1.1 with  $\ell$ -power level such that  $j_E \in \pi_G(X_G(\mathbb{Q}) - \mathcal{S}_G)$ . Parts (ii) and (iii) follow by noting that  $\pi_G(X_G(\mathbb{Q}) - \mathcal{S}_G)$  is empty when  $G$  has genus 1, level 16, and index 24, and it is infinite otherwise.

### 8. How the $J(t)$ were found

Let  $G$  be one of the genus 0 subgroups of  $\text{GL}_2(\hat{\mathbb{Z}})$  from Theorem 1.1; they are listed in Tables 1–3 of the online supplement and were determined using the algorithm described in Section 3. For each  $G$ , we also have a rational function  $J(t) \in \mathbb{Q}(t)$

such that the function field of  $X_G$  is of the form  $\mathbb{Q}(f)$  and  $j = J(f)$ , where  $j$  is the modular  $j$ -invariant; the verification of this property is described in Section 5.

In this section, we explain how we found  $J(t)$ ; note that the method we used to verify the correctness of  $J(t)$  does not depend on how it was found! None of our theorems depend on the techniques described in this section. All that matters is that they eventually produced functions  $J(t)$  whose correctness we could verify using the procedure described in Section 5D.

We used an extension of the algorithm in [Sutherland 2016] to search for elliptic curves  $E/\mathbb{Q}$  for which  $\rho_E(\text{Gal}_{\mathbb{Q}})$  is conjugate to a subgroup of  $G$ . This was initially done by simply checking elliptic curves in Cremona’s [2016] tables and the LMFDB [LMFDB Collaboration 2013] (but see Remark 8.1 below). After enough searching, we find elliptic curves  $E_1, E_2, E_3$  defined over  $\mathbb{Q}$  with distinct  $j$ -invariants  $j_1, j_2, j_3$  for which we believe that  $\rho_{E_i}(\text{Gal}_{\mathbb{Q}})$  is conjugate in  $\text{GL}_2(\hat{\mathbb{Z}})$  to a subgroup of  $G$ ; in particular, we expect that  $j_1, j_2, j_3 \in \pi_G(X_G(\mathbb{Q}))$ . We ran the Monte Carlo algorithm in [Sutherland 2016] using parameters that ensure the error probability is less than  $2^{-100}$ , under the GRH.

Now suppose that  $j_1, j_2, j_3$  are indeed elements of  $\pi_G(X_G(\mathbb{Q}))$ . The curve  $X_G$  has genus 0 and rational points, so it is isomorphic to  $\mathbb{P}_{\mathbb{Q}}^1$ . We can choose an isomorphism  $X_G \simeq \mathbb{P}_{\mathbb{Q}}^1$  such that there are points  $P_1, P_2, P_3 \in X_G(\mathbb{Q})$  satisfying  $\pi_G(P_i) = j_i$  which map to  $0, 1, \infty$ , respectively. There is thus a rational function  $J(t) \in \mathbb{Q}(t)$  such that  $J(0) = j_1, J(1) = j_2, J(\infty) = j_3$  and such that  $\mathbb{Q}(X_G) = \mathbb{Q}(f)$  for a modular function  $f$  satisfying  $J(f) = j$ ; the function  $f$  is obtained by composing our isomorphism  $\mathbb{P}_{\mathbb{Q}}^1 \simeq X_G$  with  $\pi_G$ .

We can now find all such potential  $J$ . As explained in Section 5, we can construct a modular function  $h \in \mathcal{F}_N$  and a rational function  $J'(t) \in K_N(t)$  such that  $K_N(X_G) = K_N(h)$  and  $j = J'(h)$ , where  $N$  is the level of  $G$ . We thus have

$$J(t) = J'(\psi(t))$$

for some degree 1 function  $\psi(t) \in K_N(t)$  satisfying  $\psi(0) \in R_1, \psi(1) \in R_2$ , and  $\psi(\infty) \in R_3$ , where

$$R_i := \{\alpha \in K_N \cup \{\infty\} : J'(\alpha) = j_i\}.$$

Since the sets  $R_i$  are finite and disjoint, there are only finitely many  $\psi(t) \in \mathbb{Q}(t)$  of degree 1 satisfying  $\psi(0) \in R_1, \psi(1) \in R_2, \psi(\infty) \in R_3$ . For each such  $\psi(t)$ , we check whether  $J'(\psi(t))$  lies in  $\mathbb{Q}(t)$ .

Consider any  $\psi$  as above for which  $J'(\psi(t)) \in \mathbb{Q}(t)$ . Set  $J(t) := J'(\psi(t))$  and  $f := \psi^{-1}(h) \in K_N(X_G)$ . We have  $J(f) = J'(h) = j$ . The field  $\mathbb{Q}(f)$  is thus the function field of a modular curve  $X_{G'}$ , where  $G'$  is an open subgroup of  $\text{GL}_2(\hat{\mathbb{Z}})$  of level  $N$  satisfying  $\det(G') = \hat{\mathbb{Z}}^\times$  and  $-I \in G'$ ; it consists of matrices whose reductions modulo  $N$  fix  $f$ . We can then check whether  $G$  is equal to  $G'$ . Since

$[\mathrm{GL}_2(\hat{\mathbb{Z}}) : G] = \deg \pi_G = \deg J = [\mathrm{GL}_2(\hat{\mathbb{Z}}) : G']$ , it suffices to determine whether  $G$  is a subgroup of  $G'$ ; equivalently, whether  $G$  fixes  $f$ . A method for determining whether  $f$  is fixed by  $G$  is described in Section 5C.

We will eventually find a  $\psi$  for which we have  $G = G'$  (provided that our initial  $j$ -invariants  $j_i$  are valid). This then proves that  $\mathbb{Q}(X_G) = \mathbb{Q}(f)$  for some  $f$  satisfying  $J(f) = j$ , where  $J(t) := J'(\psi(t)) \in \mathbb{Q}(t)$ .

Note this rational function  $J(t)$  is not unique since  $J(\varphi(t))$  would also work for any  $\varphi(t) \in \mathbb{Q}(t)$  of degree 1. Using similar reasoning, it is easy to determine if two  $J_1, J_2 \in \mathbb{Q}(t)$  satisfy  $J_2(t) = J_2(\varphi(t))$  for some degree 1 function  $\varphi \in \mathbb{Q}(t)$ . We have chosen our rational functions so that they are relatively compact when written down.

**Remark 8.1.** Having run this procedure to obtain functions  $J(t)$  for each of the groups  $G$  where we were able to find suitable  $E_1, E_2, E_3$  in Cremona's tables, we then address the remaining groups  $G$  by picking a group  $G'$  that contains a subgroup conjugate to  $G$  for which we already know a function  $J'(t) \in \mathbb{Q}(t)$ ; such a  $G'$  existed for every  $G$  not addressed in our initial search of Cremona's tables. Using the function  $J'(t)$  we can quickly obtain a large list of elliptic curves  $E$  for which  $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$  is a subgroup of  $G'$ . By running the algorithm in [Sutherland 2016] on several thousand (or even millions) of these curves we are eventually able to find  $E_1, E_2, E_3$  with distinct  $j$ -invariants for which it is highly probable that  $\rho_{E_i}(\mathrm{Gal}_{\mathbb{Q}})$  is actually conjugate to a subgroup of the smaller group  $G$  contained in  $G'$ . We then proceed as above to compute the function  $J(t)$  for  $G$ .

### Acknowledgements

We thank Jeremy Rouse and David Zureick-Brown for the feedback on an early draft of this article, and the referees for their careful review and helpful comments.

### References

- [Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl
- [Chua et al. 2004] K. S. Chua, M. L. Lang, and Y. Yang, "On Rademacher's conjecture: congruence subgroups of genus zero of the modular group", *J. Algebra* **277**:1 (2004), 408–428. MR Zbl
- [Cremona 2016] J. E. Cremona, "Elliptic curve data", electronic reference, University of Warwick, 2016, available at <http://johncremona.github.io/ecdata/>.
- [Cummins and Pauli 2003] C. J. Cummins and S. Pauli, "Congruence subgroups of  $\mathrm{PSL}(2, \mathbb{Z})$  of genus less than or equal to 24", *Experiment. Math.* **12**:2 (2003), 243–255. A database containing the tables is available at <http://www.uncg.edu/mat/faculty/pauli/congruence/>. MR Zbl
- [Deligne and Rapoport 1973] P. Deligne and M. Rapoport, "Les schémas de modules de courbes elliptiques", pp. 143–316 in *Modular functions of one variable, II* (Antwerp, 1972), edited by P. Deligne and W. Kuyk, Lecture Notes in Math. **349**, Springer, Berlin, 1973. MR Zbl
- [Dennin 1974] J. B. Dennin, Jr., "The genus of subfields of  $K(p^n)$ ", *Illinois J. Math.* **18** (1974), 246–264. MR Zbl

- [Faltings 1983] G. Faltings, “Endlichkeitssätze für abelsche Varietäten über Zahlkörpern”, *Invent. Math.* **73**:3 (1983), 349–366. Correction in **75**: 2 (1984), 381. MR Zbl
- [Halberstadt 1998] E. Halberstadt, “Sur la courbe modulaire  $X_{\text{ndép}}(11)$ ”, *Experiment. Math.* **7**:2 (1998), 163–174. MR Zbl
- [Kubert and Lang 1981] D. S. Kubert and S. Lang, *Modular units*, Grundlehren Math. Wissenschaften **244**, Springer, Berlin, 1981. MR Zbl
- [LMFDB Collaboration 2013] LMFDB Collaboration, “The  $L$ -functions and modular forms database”, electronic reference, 2013, available at <http://www.lmfdb.org>.
- [Rouse and Zureick-Brown 2015] J. Rouse and D. Zureick-Brown, “Elliptic curves over  $\mathbb{Q}$  and 2-adic images of Galois”, *Res. Number Theory* **1** (2015), art. id. 12. MR
- [Serre 1968] J.-P. Serre, *Abelian  $l$ -adic representations and elliptic curves*, W. A. Benjamin, New York, 1968. MR Zbl
- [Serre 1972] J.-P. Serre, “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”, *Invent. Math.* **15**:4 (1972), 259–331. MR Zbl
- [Serre 1981] J.-P. Serre, “Quelques applications du théorème de densité de Chebotarev”, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. MR Zbl
- [Serre 1997] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, 3rd ed., Friedr. Vieweg & Sohn, Braunschweig, 1997. MR Zbl
- [Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures **1**, Iwanami Shoten, Tokyo, 1971. MR Zbl
- [Sutherland 2016] A. V. Sutherland, “Computing images of Galois representations attached to elliptic curves”, *Forum Math. Sigma* **4** (2016), art. id. e4. MR Zbl
- [Sutherland and Zywina 2016] A. V. Sutherland and D. Zywina, Magma scripts associated to “Modular curves of prime-power level with infinitely many rational points”, 2016, available at <http://math.mit.edu/~drew/SZ16>.
- [Zywina 2015a] D. Zywina, “On the possible images of the mod  $l$  representations associated to elliptic curves over  $\mathbb{Q}$ ”, preprint, 2015. arXiv
- [Zywina 2015b] D. Zywina, “Possible indices for the Galois image of elliptic curves over  $\mathbb{Q}$ ”, preprint, 2015. arXiv

Communicated by Joseph H. Silverman

Received 2016-05-20

Revised 2017-02-10

Accepted 2017-03-10

drew@math.mit.edu

*Department of Mathematics,  
Massachusetts Institute of Technology,  
77 Massachusetts Ave., Cambridge, MA 02139, United States*

zywina@math.cornell.edu

*Department of Mathematics, Cornell University,  
Ithaca, NY 14853, United States*





# Some sums over irreducible polynomials

David E. Speyer

We prove a number of conjectures due to Dinesh Thakur concerning sums of the form  $\sum_P h(P)$  where the sum is over monic irreducible polynomials  $P$  in  $\mathbb{F}_q[T]$ , the function  $h$  is a rational function and the sum is considered in the  $T^{-1}$ -adic topology. As an example of our results, in  $\mathbb{F}_2[T]$ , the sum  $\sum_P 1/(P^k - 1)$  always converges to a rational function, and is 0 for  $k = 1$ .

## 1. Introduction

Our goal is to explain some identities experimentally discovered by Dinesh Thakur, involving sums over irreducible polynomials in finite fields. We begin by stating the simplest of these identities: Let  $\mathcal{P}$  be the set of irreducible polynomials in  $\mathbb{F}_2[T]$ . Then

$$\sum_{P \in \mathcal{P}} \frac{1}{P-1} = 0.$$

Here the sum must be interpreted as a sum of power series in  $T^{-1}$ . For example, the first five summands are

$$\begin{aligned} \frac{1}{T-1} &= T^{-1} + T^{-2} + T^{-3} + \dots \\ \frac{1}{(T+1)-1} &= T^{-1} \\ \frac{1}{(T^2+T+1)-1} &= T^{-2} + T^{-3} + \dots \\ \frac{1}{(T^3+T+1)-1} &= T^{-3} + \dots \\ \frac{1}{(T^3+T^2+1)-1} &= T^{-3} + \dots \end{aligned}$$

As the reader can see, only finitely many terms contribute to the coefficient of each power of  $T^{-1}$ , and the coefficient of  $T^{-j}$  is 0 for each  $j$ .

*MSC2010:* primary 11M38; secondary 05E05, 11M32.

*Keywords:* zeta function, special value, function field.

We now introduce the notation necessary to state our general results. To aid the reader’s comprehension, we adopt the following conventions: Integers will always be denoted by lower case Roman letters ( $k, p, q, \dots$ ); polynomials over finite fields will always be denoted by capital Roman letters ( $A, F, P, \dots$ ), sets of such polynomials will always be denoted by calligraphic letters ( $\mathcal{A}, \mathcal{P}, \mathcal{R}, \dots$ ), symmetric polynomials will be denoted by bold letters ( $\mathbf{e}_k, \mathbf{p}_k, \dots$ ). Of course, there will be other sorts of mathematical objects as well, which we trust the reader to accommodate as they occur.

Let  $p$  be a prime and  $q$  a power of  $p$ . Let  $\mathbb{F}_q$  be the field with  $q$  elements. Let  $\mathcal{R}$  be the polynomial ring  $\mathbb{F}_q[T]$ . Let  $\mathcal{K}$  be the fraction field  $\mathbb{F}_q(T)$  and let  $\widehat{\mathcal{K}}$  be the  $T^{-1}$ -adic completion of  $\mathcal{K}$ . All infinite sums will be understood in the  $T^{-1}$ -adic topology.

Let  $\mathcal{P}$  be the set of irreducible polynomials in  $\mathcal{R}$ ; let  $\mathcal{P}_1$  be the set of monic irreducible polynomials. Here is our main result for the case  $p = 2$ .

**Theorem 1.1.** *If  $p = 2$  then, for any positive integer  $k \equiv 0 \pmod{q - 1}$ , the sum*

$$\sum_{P \in \mathcal{P}_1} \frac{1}{P^k - 1}$$

*is in  $\mathcal{K}$ .*

The reader may wonder what happens if we sum over all irreducible polynomials rather than monic ones; that is an easy corollary:

**Corollary 1.2.** *Let  $p = 2$ . For any positive integer  $k$ , the sum*

$$\sum_{P \in \mathcal{P}} \frac{1}{P^k - 1}$$

*is in  $\mathcal{K}$ .*

*Proof.* We rewrite the sum as  $\sum_{P \in \mathcal{P}_1} \sum_{a \in \mathbb{F}_q^\times} 1/((aP)^k - 1)$ . The corollary then follows from the identity

$$\sum_{a \in \mathbb{F}_q^\times} \frac{1}{(aX)^k - 1} = \frac{1}{X^{\text{LCM}(k, q-1)} - 1}$$

in  $\mathbb{F}_q(U)$ . To prove this identity, write

$$\frac{1}{(aX)^k - 1} = \sum_{j=1}^{\infty} 1/(aX)^{kj}$$

and recall that

$$\sum_{a \in \mathbb{F}_q^\times} a^m = \begin{cases} 1, & m \equiv 0 \pmod{q - 1}, \\ 0, & \text{otherwise.} \end{cases}$$

□

We now discuss the case of a general prime. Define the rational function  $G_p(U)$  by

$$G_p(U) = \frac{(1 - U^p) - (1 - U)^p}{p(1 - U)^p}.$$

When  $p = 2$ , we have  $G_2(U) = (2U - 2U^2)/(2(1 - U)^2) = U/(1 - U)$ , so  $G_2(1/P) = 1/(P - 1)$ . When  $p$  is odd, we have the following alternate expressions for  $G_p$ :

**Proposition 1.3.** *If  $p$  is odd, then, as rational functions in  $\mathbb{F}_p(U)$ , we have*

$$G_p(U) = \frac{\sum_{j=1}^{p-1} U^j/j}{(1 - U)^p} = \sum_{\substack{0 \leq j < \infty \\ j \not\equiv 0 \pmod p}} \frac{U^j}{j}.$$

*Proof.* If  $p$  is odd, then  $(1 - U^p) - (1 - U)^p = \sum_{j=1}^{p-1} (-1)^{j-1} \binom{p}{j} U^j$ . We have

$$\frac{(-1)^{j-1}}{p} \binom{p}{j} = \frac{(-1)^{j-1} (p-1)(p-2) \cdots (p-j+1)}{1 \cdots 2 \cdots (j-1)j} \equiv \frac{1}{j} \pmod p.$$

This proves the first equality, and the second is immediate. □

**Theorem 1.4.** *For any positive integer  $k \equiv 0 \pmod{q-1}$ , the sum*

$$\sum_{P \in \mathcal{P}_1} G_p(1/P^k)$$

*is in  $\mathcal{K}$ .*

As we noted,  $G_2(1/X) = 1/(X - 1)$ , so Theorem 1.4 implies Theorem 1.1.

**Remark 1.5.** When  $p = 2$ , we do *not* have  $G_2(U) = \sum_{j \not\equiv 0 \pmod p} U^j/j$ ; the latter sum is  $H(U) := U/(1 - U^2)$ . However, it is true that  $\sum_{P \in \mathcal{P}_1} H(1/P^k)$  is in  $\mathcal{K}$ , because  $H(U) = G(U) - G(U^2)$ .

Once again, we have a trivial variant where we sum over  $\mathcal{P}$ :

**Corollary 1.6.** *For any positive integer  $k$ , the sum*

$$\sum_{P \in \mathcal{P}} G_p(1/P^k)$$

*is in  $\mathcal{K}$ .*

*Proof.* If  $p = 2$ , we proved this in Corollary 1.2, so we may (and do) assume  $p$  is odd. As in the proof of Corollary 1.2, we rewrite the sum as  $\sum_{P \in \mathcal{P}_1} \sum_{a \in \mathbb{F}_q^\times} G_p(1/(aP)^k)$ . We now need the identity

$$\sum_{a \in \mathbb{F}_q^\times} G_p((aU)^k) = \text{GCD}(q-1, k) G_p(U^{\text{LCM}(q-1, k)})$$

in  $\mathbb{F}_q(U)$ . To prove this identity, we use the formula  $G_p(U) = \sum_{j \not\equiv 0 \pmod p} U^j/j$  and the identity

$$\sum_{a \in \mathbb{F}_q^\times} a^m = \begin{cases} q-1, & m \equiv 0 \pmod{q-1}, \\ 0, & \text{otherwise.} \end{cases}$$

So

$$\sum_{a \in \mathbb{F}_q^\times} G_p(1/(aU)^k) = \sum_{j \not\equiv 0 \pmod p} \sum_{a \in \mathbb{F}_q^\times} \frac{1}{j(aU)^{kj}} = (q-1) \sum_{\substack{j \not\equiv 0 \pmod p \\ kj \equiv 0 \pmod{q-1}}} \frac{1}{jU^{kj}}.$$

Putting  $kj = \text{LCM}(q-1, k)\ell$ , this is

$$\begin{aligned} (q-1) \sum_{\ell \not\equiv 0 \pmod p} \frac{k}{\text{LCM}(q-1, k)\ell U^{\text{LCM}(q-1, k)\ell}} &= \frac{k(q-1)}{\text{LCM}(q-1, k)} G_p(U^{\text{LCM}(q-1, k)}) \\ &= \text{GCD}(q-1, k) G_p(U^{\text{LCM}(q-1, k)}), \end{aligned}$$

as required. □

We also compute explicit values for the sum when  $k$  is not too large.

**Theorem 1.7.** *Let  $k = (q-1)\ell$ . If  $1 \leq \ell \leq q/p$ , then  $\sum_{P \in \mathcal{P}_1} G_p(1/P^k) = 0$ . If  $q/p + 1 < \ell \leq 2q/p$ , then*

$$\sum_{P \in \mathcal{P}_1} G_p(1/P^k) = \ell \frac{(T^q - T)^{q+1}}{(T^{q^2} - T^q)(T^{q^2} - T)}.$$

In principle, our methods are capable of computing  $\sum_{P \in \mathcal{P}_1} G_p(1/P^k)$  for any  $k \equiv 0 \pmod{q-1}$ , but they become impractical beyond  $\ell = 2q/p$ .

**History of the problem.** Dinesh Thakur suspected such relations should exist, based on heuristics concerning  $\zeta$  deformation. He experimentally discovered most of the relations described above in characteristic two, and suspected there should be similar results in odd characteristic. Thakur [2015] published these computations in a preprint entitled ‘‘Surprising symmetries in distribution of prime polynomials’’. At Thakur’s suggestion, Terence Tao [2015] promoted the problem in posts on his blog and on the Polymath blog. I am grateful to Thakur for finding such an elegant problem and to Tao for bringing it to my attention. My thanks also to all who participated in the discussion on the Polymath blog: Noam Elkies, Ian Finn, Ofir Gorodetsky, Jesse, Gil Kalai, David Lowry-Duda, Dustin G. Mixon, John Nicol, Partha Solapurkar, John Voight, Victor Wang, Qiaochu Yuan, Joshua Zelinsky, and additional thanks to Ofir Gorodetsky for suggesting several improvements to the manuscript.

The author is supported by NSF grant DMS-1600223.

**2. The Carlitz exponential, and symmetric polynomials**

The main tool in our proofs is the theory of the Carlitz exponential. Put

$$D_i = (T^{q^i} - T)(T^{q^i} - T^q)(T^{q^i} - T^{q^2}) \dots (T^{q^i} - T^{q^{i-1}}).$$

Define

$$e_C(Z) = \sum_{j=0}^{\infty} \frac{Z^{q^j}}{D_j},$$

this sum is  $T^{-1}$ -adically convergent for any  $Z \in \widehat{\mathcal{K}}$ . We will make use of the product identity

$$\frac{e_C(\bar{\pi} Z)}{\bar{\pi} Z} = \prod_{A \in \mathcal{R} \setminus \{0\}} \left(1 + \frac{Z}{A}\right),$$

where  $\bar{\pi} \in \widehat{\mathcal{K}}(\sqrt[q-1]{-T})$  is given by

$$\bar{\pi} = \frac{T \sqrt[q-1]{-T}}{\prod_{A \in \mathcal{R} \setminus \{0\}} (1 - (TA)^{-1})}.$$

See, for example, [Goss 1996, Theorem 3.2.8]. This identity should be thought of as similar to Euler’s identity,

$$\frac{\sin(\pi z)}{\pi z} = \prod_{a \in \mathbb{Z} \setminus \{0\}} \left(1 + \frac{z}{a}\right).$$

We introduce the notations  $\mathcal{A}$  for the nonzero polynomials of  $\mathcal{R}$ , and  $\mathcal{A}_1$  for the monic polynomials.

Writing  $e_k$  for the elementary symmetric function of degree  $k$ , this implies

$$e_k(1/A)_{A \in \mathcal{A}} = \begin{cases} \bar{\pi}^k / D_j, & k = q^j - 1, \\ 0, & \text{otherwise.} \end{cases}$$

Since the ring of symmetric polynomials is generated by the  $e_k$ , we deduce:

**Proposition 2.1.** *If  $f$  is a homogenous symmetric polynomial of degree  $k$ , then  $f(1/A)_{A \in \mathcal{A}}$  is in  $\bar{\pi}^k \mathcal{K}$ .*

Here we note that  $f(1/A)_{A \in \mathcal{A}}$  is always defined, since only finitely many terms contribute to the coefficient of any particular power of  $T^{-1}$ .

The above considers symmetric polynomials in  $\{1/A\}_{A \in \mathcal{A}}$ , but we would rather restrict to the case of  $A$  monic. To this end, we have

**Proposition 2.2.**

$$e_\ell(1/A^{q-1})_{A \in \mathcal{A}_1} = \begin{cases} (-1)^\ell \bar{\pi}^{\ell(q-1)} / D_j, & \ell = (q^j - 1)/(q - 1), \\ 0, & \text{otherwise.} \end{cases}$$

*Proof.* Grouping together scalar multiples of the same polynomial in the Carlitz product identity, we have

$$\frac{e_C(\bar{\pi} Z)}{\bar{\pi} Z} = \prod_{A \in \mathcal{A}_1} \left(1 - \frac{Z^{q-1}}{A^{q-1}}\right).$$

Equate coefficients of  $Z^{\ell(q-1)}$  on both sides. □

**Corollary 2.3.** *If  $f$  is a homogenous symmetric polynomial of degree  $\ell$ , then  $f(1/A^{q-1})_{A \in \mathcal{A}_1}$  is in  $\bar{\pi}^{\ell(q-1)}\mathcal{K}$ .*

### 3. Proofs of rationality

We now have enough background to prove Theorem 1.4 and, hence, Theorem 1.1. Throughout, let  $k \equiv 0 \pmod{q-1}$ .

Consider the symmetric polynomial

$$g_p(X_1, X_2, \dots) := \frac{1}{p} \left( \left( \sum X_i \right)^p - \sum X_i^p \right).$$

The polynomial  $g_p$  has integer coefficients, so we may discuss plugging elements of  $\mathcal{K}$  into it.

Let  $C$  be the cyclic group of order  $p$ , and let  $C$  act on  $\mathcal{A}_1^p$  by rotating coordinates. Let  $\Delta$  denote the diagonal:  $\Delta := \{(A, A, \dots, A)\} \subset \mathcal{A}_1^p$ . Then

$$g_p(1/A^k)_{A \in \mathcal{A}_1} = \sum_{(A_1, \dots, A_p) \in (\mathcal{A}_1^p \setminus \Delta) / C} \frac{1}{A_1^k A_2^k \dots A_p^k}.$$

The sum is over cosets for the free action of  $C$  on  $\mathcal{A}^p \setminus \Delta$ .

Let

$$\Phi = \{(A_1, \dots, A_p) \in \mathcal{A}_1^p : \text{GCD}(A_1, \dots, A_p) = 1\}.$$

Any  $(A_1, \dots, A_p) \in \mathcal{A}_1^p$  can be uniquely factored as  $A_i = DB_i$  for some  $D \in \mathcal{A}_1$  and  $(B_1, \dots, B_p) \in \Phi$ . So we can factor the above sum as

$$g_p(1/A^k)_{A \in \mathcal{A}_1} = \left( \sum_{D \in \mathcal{A}_1} \frac{1}{D^{kp}} \right) \left( \sum_{(B_1, \dots, B_p) \in (\Phi \setminus \{(1, \dots, 1)\}) / C} \frac{1}{B_1^k B_2^k \dots B_p^k} \right).$$

Now, from Corollary 2.3,  $g_p(1/A^k)_{A \in \mathcal{A}_1}$  is in  $\bar{\pi}^{pk}\mathcal{K}$ . Also from Corollary 2.3,  $\sum_{D \in \mathcal{A}_1} 1/D^{kp}$  is in  $\bar{\pi}^{pk}\mathcal{K}$ , and a quick computation shows that this sum is 1 plus terms in  $T^{-1}\mathbb{F}_q[[T^{-1}]]$ , so it is not zero. We deduce that

$$\sum_{(B_1, \dots, B_p) \in (\Phi \setminus \{(1, \dots, 1)\}) / C} \frac{1}{B_1^k B_2^k \dots B_p^k} \in \mathcal{K}.$$

For  $B \in \mathcal{A}_1$ , let  $\Psi(B)$  be the set of  $p$ -tuples  $(B_1, B_2, \dots, B_p)$  for which  $\prod B_i = B$  and  $\text{GCD}(B_1, \dots, B_p) = 1$ . Let  $\psi(B) = \#\Psi(B)$ . So we have shown that

$$\sum_{B \in \mathcal{A}_1 \setminus \{1\}} \frac{\psi(B)/p}{B^k} \in \mathcal{K}.$$

Here, to interpret the numerator, we must divide  $\psi(B)$  by  $p$  as integers and only then consider the quotient in  $\mathbb{F}_p$ .

If  $B = P_1^{k_1} P_2^{k_2} \dots P_r^{k_r}$  then there is an easy bijection between  $\Psi(B)$  and  $\Psi(P_1^{k_1}) \times \Psi(P_2^{k_2}) \times \dots \times \Psi(P_r^{k_r})$ , so  $\psi(B) = \prod \psi(P_i^{k_i})$ . If  $P$  is irreducible then  $\psi(P^r)$  is divisible by  $p$  for any  $r > 0$ , since  $C$  acts freely on  $\Psi(P^r)$ . So, if  $B$  is divisible by two different irreducible polynomials, then  $\psi(B)$  is divisible by  $p^2$ . So we can rewrite the sum as

$$\sum_{P \in \mathcal{P}_1} \sum_{r=1}^{\infty} \frac{\psi(P^r)/p}{P^{rk}}.$$

We now compute  $\psi(P^r)$ ; which is the number of  $p$ -tuples  $(P^{r_1}, \dots, P^{r_p})$  with  $\prod P^{r_i} = P^r$  and  $\text{GCD}(P^{r_1}, \dots, P^{r_p}) = 1$ . In other words, we must count  $(r_1, \dots, r_p) \in \mathbb{Z}_{\geq 0}^p$  with  $\sum r_i = r$  and  $\min(r_1, \dots, r_p) = 0$ . The number of  $(r_1, \dots, r_p) \in \mathbb{Z}_{\geq 0}^p$  with  $\sum r_i = r$  is the coefficient of  $U^r$  in  $1/(1-U)^p$ . In order to impose  $\min(r_1, \dots, r_p) = 0$ , we subtract off the terms with  $\min(r_1, \dots, r_p) > 0$ . These are in bijection with  $(s_1, \dots, s_p) \in \mathbb{Z}_{\geq 0}^p$  with  $p + \sum s_i = r$ . So  $\psi(P^r)$  is the coefficient of  $U^r$  in  $1/(1-U)^p - U^p/(1-U)^p$ . In other words,  $\sum_{r=0}^{\infty} \psi(P^r)U^r = (1-U^p)/(1-U)^p$ . So

$$\sum_{r=1}^{\infty} \frac{\psi(P^r)}{p} U^r = \frac{1}{p} \left( \frac{1-U^p}{(1-U)^p} - 1 \right) = G_p(U).$$

We deduce that  $\sum_{r=1}^{\infty} (\psi(P^r)/p)/P^{rk} = G_p(1/P^k)$ . We have now shown that  $\sum_{P \in \mathcal{P}_1} G_p(1/P^k) \in \mathcal{K}$ , as claimed. □

We record the specific formula we have proved:

**Proposition 3.1.** *Let  $k$  be a positive integer. Then*

$$\sum_{P \in \mathcal{P}_1} G_p(1/P^k) = \frac{\mathbf{g}_p(1/A^k)_{A \in \mathcal{A}_1}}{\sum_{A \in \mathcal{A}_1} 1/A^{pk}}.$$

We will rewrite this formula in various ways in Section 5. We remark that this formula is correct even if  $k$  is not divisible by  $q - 1$ , although we have only shown the ratio is in  $\mathcal{K}$  when  $k \equiv 0 \pmod{q - 1}$ . The denominator of this formula is  $\zeta(pk) = \zeta(k)^p$ , where  $\zeta$  is the Goss  $\zeta$ -function [1979].

### 4. Vanishing

We will now prove the claim in Theorem 1.7 that the sum vanishes when  $k = (q - 1)\ell$  for  $1 \leq \ell \leq q/p$ . From Proposition 3.1, it is equivalent to show that  $\mathbf{g}_p(1/A^{\ell(q-1)})_{A \in \mathcal{A}_1} = 0$ . To this end, we must explicitly write  $\mathbf{g}_p(1/A^{\ell(q-1)})$  as a polynomial in the  $\mathbf{e}_k(1/A^{q-1})$ .

The variables  $\lambda$  or  $\mu$  will always denote partitions, meaning weakly decreasing sequences  $(\lambda_1, \lambda_2, \dots, \lambda_r)$  of positive integers; sums over  $\lambda$  or  $\mu$  implicitly contain the condition that the summation variable is a partition.

We define  $\mathbf{e}_\lambda = \prod_s \mathbf{e}_{\lambda_s}$ . The symmetric polynomials  $\mathbf{e}_\lambda$  form an integer basis for the symmetric polynomials with integer coefficients.

**Lemma 4.1.** *Write*

$$\mathbf{g}_p(X_1^\ell, X_2^\ell, \dots) = \sum_{|\lambda|=p\ell} c_\lambda \mathbf{e}_\lambda(X_1, X_2, \dots)$$

for some integers  $c_\lambda$ . Then  $c_{11\dots 1} = 0$ .

*Proof.* Note that  $\mathbf{e}_{11\dots 1}$  is the only  $\mathbf{e}_\lambda$  with a nonzero coefficient of  $X_1^{p\ell}$ . The coefficient of  $X_1^{p\ell}$  in  $\mathbf{g}_p(X_1^\ell, X_2^\ell, \dots)$  is clearly 0. □

Now, suppose that  $\ell \leq q/p$ , so we have  $p\ell < q + 1$ . So any partition  $(\lambda_1, \dots, \lambda_r)$  of  $p\ell$  other than  $(1, 1, \dots, 1)$  contains a  $\lambda_i$  between 2 and  $q$ . By Proposition 2.2,  $\mathbf{e}_m(1/A^{q-1})_{A \in \mathcal{A}_1} = 0$  for  $2 \leq m \leq q$ , so  $\mathbf{e}_\lambda(1/A^{q-1})_{A \in \mathcal{A}_1} = 0$  whenever  $\lambda$  is a partition of  $p\ell$  other than  $(1, 1, \dots, 1)$ . We deduce that  $\mathbf{g}_p(1/A^{q-1})_{A \in \mathcal{A}_1} = 0$  as desired. □

### 5. Computations for small $k$

In this section, we will discuss the computation of  $\sum_{P \in \mathcal{P}_1} G_p(1/P^k)$  for  $k \equiv 0 \pmod{q-1}$  and, in particular, prove the remaining half of Theorem 1.7. Our strategy is to combine Propositions 3.1 and 2.2. We must compute  $\mathbf{g}_p(1/A^{\ell(q-1)})_{A \in \mathcal{A}_1}$  and  $\sum_{A \in \mathcal{A}_1} 1/A^{p\ell}$ . Note the latter is  $(\mathbf{p}_\ell(1/A^{q-1})_{A \in \mathcal{A}_1})^p$ , where  $\mathbf{p}_d(X_1, X_2, \dots)$  is the power sum symmetric function  $\sum X_i^d$ . We write  $k = (q - 1)\ell$ .

Put

$$\begin{aligned} \mathbf{g}_p(X_1^\ell, X_2^\ell, \dots) &= \sum_{|\lambda|=\ell p} c_\lambda \mathbf{e}_\lambda(X_1, X_2, \dots), \\ \mathbf{p}_\ell(X_1, X_2, \dots) &= \sum_{|\mu|=\ell} d_\mu \mathbf{e}_\mu(X_1, X_2, \dots). \end{aligned}$$

Note that  $\mathbf{e}_m(1/A^{q-1})_{A \in \mathcal{A}_1} = 0$  unless  $m$  is of the form  $(q^j - 1)/(q - 1)$ . So we only need to sum over partitions where all the parts of  $\lambda$  are of the form  $(q^j - 1)/(q - 1)$ .

**From now on, we now impose that  $q/p + 1 \leq \ell \leq 2q/p$ .** So  $\ell < q + 1$ . Any partition of  $\ell$  cannot contain any parts of size  $(q^j - 1)/(q - 1)$ , for  $j > 1$ . Similarly,



$p\ell < 2q + 2$ , so a partition of  $p\ell$  can contain at most one part of size  $q + 1 = (q^2 - 1)/(q - 1)$  and no parts of size  $(q^j - 1)/(q - 1)$  for  $j > 2$ . We deduce that the only terms which contribute to our final answer come from  $\lambda = (1, 1, \dots, 1)$  or  $\lambda = (q + 1, 1, 1, \dots, 1)$  when computing  $\mathbf{g}_p(1/A^{\ell(q-1)})_{A \in \mathcal{A}_1}$ , and from  $\mu = (1, 1, \dots, 1)$  in computing  $(\mathbf{p}_\ell(1/A^{q-1}))_{A \in \mathcal{A}_1}^p$ . Moreover, from Lemma 4.1, the coefficient  $c_{(1,1,\dots,1)}$  is zero.

We deduce that

$$\begin{aligned} \sum_{P \in \mathcal{P}_1} G_p(1/P^k) &= \frac{c_{(q+1,1^{p\ell-q-1})} \mathbf{e}_{(q+1,1^{p\ell-q-1})}(1/A^{q-1})_{A \in \mathcal{A}_1}}{(d_{1^\ell} \mathbf{e}_{1^\ell}(1/A^{q-1})_{A \in \mathcal{A}_1})^p} \\ &= \frac{c_{(q+1,1^{p\ell-q-1})} \mathbf{e}_{q+1}(1/A^{q-1})_{A \in \mathcal{A}_1} (\mathbf{e}_1(1/A^{q-1})_{A \in \mathcal{A}_1})^{p\ell-q-1}}{d_{1^\ell} (\mathbf{e}_1(1/A^{q-1})_{A \in \mathcal{A}_1})^{p\ell}} \\ &= \frac{c_{(q+1,1^{p\ell-q-1})} \mathbf{e}_{q+1}(1/A^{q-1})_{A \in \mathcal{A}_1}}{d_{1^\ell} (\mathbf{e}_1(1/A^{q-1})_{A \in \mathcal{A}_1})^{q+1}}. \end{aligned}$$

Here  $1^r$  is shorthand for the partition with  $r$  parts equal to 1.

We now use Proposition 2.2. The powers of  $\bar{\pi}$  and  $(-1)$  cancel to give

$$\sum_{P \in \mathcal{P}_1} G_p(1/P^k) = \frac{c_{(q+1,1^{p\ell-q-1})}}{d_{1^\ell}} \frac{D_1^{q+1}}{D_2} = \frac{c_{(q+1,1^{p\ell-q-1})}}{d_{1^\ell}} \frac{(T^q - T)^{q+1}}{(T^{q^2} - T^q)(T^{q^2} - T)}.$$

To finish the computation, we must find  $c_{q+1,1^{ps-1}}$  and  $d_{1^\ell}$ . The latter is easy: Comparing coefficients of  $X_1^\ell$  on both sides of

$$\mathbf{p}_\ell(X_1, X_2, \dots) = \sum_{|\mu|=\ell} d_\mu \mathbf{e}_\mu(X_1, X_2, \dots),$$

we deduce that  $d_{1^\ell} = 1$ .

To compute  $c_{(q+1,1^{p\ell-q-1})}$ , we begin with the formula

$$\mathbf{g}_p(X_1^\ell, X_2^\ell, \dots) = \frac{1}{p} (\mathbf{p}_\ell(X_1, X_2, \dots)^p - \mathbf{p}_{p\ell}(X_1, X_2, \dots)).$$

For brevity, we write  $\mathbf{f}(X)$  to indicate that the inputs to a symmetric polynomial are  $(X_1, X_2, \dots)$ . Note that we are working with symmetric polynomials with integer coefficients, so it makes sense to divide by  $p$ .

We rewrite the right hand side of the previous equation as

$$\frac{1}{p} \left( (\mathbf{e}_1(X)^\ell + \dots)^p - (\mathbf{e}_1(X)^{p\ell} + d_{q+1,1^{p\ell-q-1}} \mathbf{e}_{q+1}(X) \mathbf{e}_1(X)^{p\ell-q-1} + \dots) \right).$$

Here the ellipses denote terms  $\mathbf{e}_\lambda$  where  $\lambda$  has some part that is not of the form  $(q^j - 1)/(q - 1)$ . We deduce that

$$c_{q+1,1^{p\ell-q-1}} = -\frac{1}{p} d_{q+1,1^{p\ell-q-1}}.$$

Now, observe the identity

$$\begin{aligned} \sum_j \frac{(-1)^{j-1} \mathbf{p}_j(X) U^j}{j} &= \sum_i \log(1 + X_i U) \\ &= \log \prod_i (1 + X_i U) = \log \left( 1 + \sum_{m=1}^{\infty} \mathbf{e}_m(X) U^m \right). \end{aligned}$$

The coefficient of  $U^{p\ell}$  on the left is  $((-1)^{p\ell}/p\ell) \mathbf{p}_{p\ell}$ . Expanding the log on the right hand side as a Taylor series, only one term contributes to  $U^{p\ell} \mathbf{e}_{q+1} \mathbf{e}_1^{p\ell-q-1}$ . So we obtain

$$\frac{(-1)^{p\ell-1}}{p\ell} \mathbf{p}_{p\ell}(X) = \frac{(-1)^{p\ell-q-1}}{p\ell-q} \binom{p\ell-q}{1} \mathbf{e}_{q+1}(X) \mathbf{e}_1^{p\ell-q-1}(X) + \dots,$$

where the ellipses denote a sum of  $\mathbf{e}_\lambda$  other than  $\mathbf{e}_{q+1}(X) \mathbf{e}_1^{p\ell-q-1}(X)$ . So

$$d_{q+1, 1^{p\ell-q-1}} = (-1)^q p\ell \quad \text{and} \quad c_{q+1, 1^{ps-1}} = (-1)^{q-1} \ell.$$

Plugging into our previous formula, and using that  $(-1)^{q-1} \equiv 1 \pmod p$ ,

$$\sum_{P \in \mathcal{P}_1} G_p(1/P^k) = \ell \frac{(T^q - T)^{q+1}}{(T^{q^2} - T^q)(T^{q^2} - T)}.$$

This concludes the proof of Theorem 1.7. □

We conclude by verifying one of Thakur’s conjectures which goes beyond the range  $\ell \leq 2q/p$ . Let  $p = q = 2$ . Thakur conjectures

$$\sum_{P \in \mathcal{P}_1} \frac{1}{P^3 - 1} = \frac{1}{T^4 + T^2}.$$

We begin by computing

$$\begin{aligned} \mathbf{p}_3(X) &= \mathbf{e}_1(X)^3 + 3\mathbf{e}_3(X) - 3\mathbf{e}_2(X)\mathbf{e}_1(X), \\ \mathbf{p}_3(X)^2 &= \mathbf{e}_1(X)^6 + 6\mathbf{e}_1(X)^3\mathbf{e}_3(X) + 9\mathbf{e}_3(X)^2 + \dots \end{aligned}$$

Here and in the following equations, the ellipses denote  $\mathbf{e}_\lambda$  terms where  $\lambda$  contains a part other than 1 and 3. (Note that  $(2^3 - 1)/(2 - 1) = 7$ , too large to contribute to a symmetric polynomial of degree 6.) Similarly,

$$\mathbf{p}_6(X) = \mathbf{e}_1(X)^6 + 6\mathbf{e}_1(X)^3\mathbf{e}_3(X) + 3\mathbf{e}_3(X)^2 + \dots$$

So

$$\mathbf{g}_2(X_1^3, X_2^3, \dots) = \frac{1}{2}(\mathbf{p}_3(X)^2 - \mathbf{p}_6(X)) = 3\mathbf{e}_3(X)^2 + \dots$$

and (recall that we are working modulo 2)

$$\mathbf{g}_2(1/A^3)_{A \in \mathcal{A}_1} = (\mathbf{e}_3(1/A)_{A \in \mathcal{A}_1})^2 = \frac{\bar{\pi}^6}{D_2^2} = \frac{\bar{\pi}^6}{(T^4 - T^2)^2 (T^4 - T)^2}.$$

Similarly,

$$\begin{aligned} p_6(1/A)_{A \in \mathcal{A}_1} &= (e_1(1/A)_{A \in \mathcal{A}_1})^6 + (e_3(1/A)_{A \in \mathcal{A}_1})^2 \\ &= \left(\frac{\bar{\pi}}{D_1}\right)^6 + \left(\frac{\bar{\pi}^3}{D_2}\right)^2 \\ &= \bar{\pi}^6 \left( \left(\frac{1}{T^2 - T}\right)^6 + \left(\frac{1}{(T^4 - T^2)(T^4 - T)}\right)^2 \right). \end{aligned}$$

We verify Thakur's claim:

$$\sum_{P \in \mathcal{P}_1} \frac{1}{P^3 - 1} = \frac{1/((T^4 - T^2)^2(T^4 - T)^2)}{1/(T^2 - T)^6 + 1/((T^4 - T^2)^2(T^4 - T)^2)} = \frac{1}{T^4 + T^2}.$$

### References

- [Goss 1979] D. Goss, “ $v$ -adic zeta functions,  $L$ -series and measures for function fields”, *Invent. Math.* **55**:2 (1979), 107–119. MR Zbl
- [Goss 1996] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik (3) **35**, Springer, 1996. MR Zbl
- [Tao 2015] T. Tao, “Polymath proposal: explaining identities for irreducible polynomials”, 2015, Available at <https://polymathprojects.org/2015/12/28/>.
- [Thakur 2015] D. S. Thakur, “Surprising symmetries in distribution of prime polynomials”, preprint, 2015. arXiv

Communicated by Kiran S. Kedlaya

Received 2016-10-17      Accepted 2017-04-03

speyer@umich.edu

*Department of Mathematics, University of Michigan,  
2844 East Hall, 530 Church Street,  
Ann Arbor, MI 48109-1043, United States*



## Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

**Originality.** Submission of a manuscript acknowledges that the manuscript is original and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

**Language.** Articles in *ANT* are usually in English, but articles written in other languages are welcome.

**Length** There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

**Required items.** A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

**Format.** Authors are encouraged to use  $\LaTeX$  but submissions in other varieties of  $\TeX$ , and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

**References.** Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of Bib $\TeX$  is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

**Figures.** Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to [graphics@msp.org](mailto:graphics@msp.org) with details about how your graphics were generated.

**White space.** Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

**Proofs.** Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

# Algebra & Number Theory

Volume 11    No. 5    2017

---

Hybrid sup-norm bounds for Maass newforms of powerful level ABHISHEK SAHA	1009
Collinear CM-points YURI BILU, FLORIAN LUCA and DAVID MASSER	1047
A uniform classification of discrete series representations of affine Hecke algebras DAN CIUBOTARU and ERIC OPDAM	1089
An explicit bound for the least prime ideal in the Chebotarev density theorem JESSE THORNER and ASIF ZAMAN	1135
Modular curves of prime-power level with infinitely many rational points ANDREW V. SUTHERLAND and DAVID ZYWINA	1199
Some sums over irreducible polynomials DAVID E. SPEYER	1231



1937-0652(2017)11:5;1-G