ESSENTIAL NUMBER THEORY

2022

vol. 1 no. 1

msp

ESSENTIAL NUMBER THEORY

msp.org/ent

See inside back cover or msp.org/ent for submission instructions.

Essential Number Theory (ISSN 2834-4634 electronic, 2834-4626 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ENT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
https://msp.org/

Essential Number Theory
Vol. 1, No. 1, 2022
https://doi.org/10.2140/ent.2022.1.1

The cubic case of Vinogradov's mean value theorem

D. R. Heath-Brown

We present a self-contained proof of the cubic case of Vinogradov's mean value theorem, based on Wooley's "efficient congruencing" approach.

1. Introduction

In a remarkable series of papers, Wooley [2012; 2013; 2015; 2016; 2017], and in collaboration with Ford [Ford and Wooley 2014], has made dramatic progress with Vinogradov's mean value theorem. This culminated in the full proof of the main conjecture, by Bourgain, Demeter and Guth [Bourgain et al. 2016], using rather different methods — but see [Wooley 2019] for a subsequent treatment by the original approach. Wooley's survey article [2014] gives an excellent introduction to his results and their applications.

The mean value theorem concerns the integer $J_{s,k}(X)$ defined as the number of solutions $(x_1,\dots,x_{2s})\in\mathbb{N}^{2s}$ of the simultaneous equations

$$x_1^j+\cdots+x_s^j=x_{s+1}^j+\cdots+x_{2s}^j \quad (1\le j\le k) \tag{1}$$

with $x_1,\dots,x_{2s}\le X$. Here $X\ge 1$ is an arbitrary real number, and s and k are positive integers, which one treats as being fixed. The key feature of this system is that if $(x_1,\dots,x_{2s})$ is a solution, so is any translate $(x_1+c,\dots,x_{2s}+c)$.

The various forms of the Vinogradov mean value theorem give upper bounds for $J_{s,k}(X)$. It is not hard to see that

$$J_{s,k}(X)\gg_{s,k} X^s+X^{2s-k(k+1)/2},$$

for $X\ge 1$, and the central conjecture is that

$$J_{s,k}(X)\ll_{s,k,\varepsilon} X^{\varepsilon}(X^s+X^{2s-k(k+1)/2})$$

for any $\varepsilon>0$. "Classically" this was known for $k=1$ and 2, for $s\le k+1$, and for $s\ge s_0(k)$ with a value $s_0(k)\ll k^2\log k$. However Wooley [2012] showed that one may take $s_0(k)=k^2+k$. Moreover, in [Wooley 2016], he showed that the full conjecture holds for $k=3$.

MSC2020: primary 11L15; secondary 11D45, 11L07.
Keywords: exponential sum, mean value, cubic, Vinogradov.

The purpose of this paper is to present a much simplified version of Wooley's methods, sufficient to handle the case $k = 3$.

Theorem. *We have*

$$J_{6,3}(X) \ll_\varepsilon X^{6+\varepsilon}$$

for any fixed $\varepsilon > 0$.

It is trivial from (2) below that if s and t are any positive integers then we will have $J_{s+t,k}(X) \le X^{2t} J_{s,k}(X)$ and $J_{s,k}(X) \le J_{s+t,k}(X)^{s/(s+t)}$. Thus for $k = 3$ we can deduce the general case of the conjecture immediately from the theorem.

It should be stressed that, while the argument of the present paper appears cleaner and shorter than that presented by Wooley [2016], the underlying principles are the same.

2. Outline of the proof

Investigations into the mean value theorem depend crucially on an alternative interpretation of $J_{s,k}(X)$ in terms of exponential sums. If $\boldsymbol{\alpha} \in \mathbb{R}^k$ we write

$$f_k(\boldsymbol{\alpha};\, X) = f(\boldsymbol{\alpha}) = \sum_{x \le X} e(\alpha_1 x + \cdots + \alpha_k x^k),$$

whence

$$J_{s,k}(X) = \int_{(0,1]^k} |f(\boldsymbol{\alpha})|^{2s}\, d\boldsymbol{\alpha}. \tag{2}$$

Our version of the efficient congruencing method will also use the exponential sums

$$f_k(\boldsymbol{\alpha};\, X, \xi, a) = f_a(\boldsymbol{\alpha};\, \xi) = \sum_{\substack{x \le X \\ x \equiv \xi \pmod{p^a}}} e(\alpha_1 x + \cdots + \alpha_k x^k),$$

where p is prime and a is a positive integer exponent. The prime $p \ge 5$ will be chosen to be a small power of X. Since it will not change during the argument we will not include it explicitly among the parameters for $f_a(\boldsymbol{\alpha};\, \xi)$. Taking s and k as fixed we will write

$$I_m(X;\, \xi, \eta;\, a, b) = \int_{(0,1]^k} |f_a(\boldsymbol{\alpha};\, \xi)|^{2m} |f_b(\boldsymbol{\alpha};\, \eta)|^{2(s-m)}\, d\boldsymbol{\alpha}, \quad (0 \le m \le s-1),$$

which counts solutions of (1) in which

$$x_i \equiv \xi \pmod{p^a} \quad (1 \le i \le m \text{ and } s+1 \le i \le s+m),$$

and

$$x_i \equiv \eta \pmod{p^b} \quad (m+1 \le i \le s \text{ and } s+m+1 \le i \le 2s).$$

We will use this notation even when p^a or p^b is larger than X. We observe that when $m = 0$ we have

$$I_0(X;\xi,\eta;a,b) = \int_{(0,1]^k} |f_b(\boldsymbol{\alpha};\eta)|^{2s}\, d\boldsymbol{\alpha},$$

which is independent of ξ and a.

We will also work with $I_m(X;a,b)$ defined by

$$I_0(X;a,b) = \max_{\eta \pmod{p^b}} I_0(X;\xi,\eta;a,b)$$

and

$$I_m(X;a,b) = \max_{\xi\not\equiv\eta \pmod{p}} I_m(X;\xi,\eta;a,b) \quad (1 \le m \le s-1).$$

The condition $\xi \not\equiv \eta \pmod{p}$ is the last remaining vestige of Wooley's "conditioning" step. Wooley [2016, page 538] uses functions $I^m_{a,b}(X)$ and $K^m_{a,b}(X)$, both of which correspond to our function $I_m(X;a,b)$. We are able to work with a single (simpler) function because we have a simpler version of the conditioning process.

Although many of our results can be proved for general s and k we shall now specialize to the case $s=6$, $k=3$, and write $J(X) = J_{6,3}(X)$ for brevity. We proceed to present a series of estimates relating $J(X)$ and $I_m(X;a,b)$ for $m = 0, 1, 2$, with various values of a and b. Iterating these will ultimately establish our theorem. The lemmas below will be proved in the next section. For the time being we content ourselves with stating the results, and showing how they lead to the theorem.

When $m = 0$ we can relate $I_0(X;a,b)$ to $J(X)$ as follows.

Lemma 1. *If $p^b \le X$ we have*

$$I_0(X;a,b) \le J(2X/p^b).$$

Our next result shows how to bound $J(X)$ in terms of $I_2(X;1,1)$.

Lemma 2. *If $p \le X$ we have*

$$J(X) \ll pJ(2X/p) + p^{12} I_2(X;1,1).$$

One way to compare values of $I_1(X;a,b)$ and $I_2(X;a,b)$ is by applying Hölder's inequality. We give two such estimates.

Lemma 3. *We have*

$$I_2(X;a,b) \le I_2(X;b,a)^{1/3} I_1(X;a,b)^{2/3}$$

irrespective of the size of p.

Lemma 4. *If $p^b \le X$ we have*

$$I_1(X;a,b) \le I_2(X;b,a)^{1/4} J(2X/p^b)^{3/4}.$$

Next we show how successively larger values of a and b arise.

Lemma 5. *For any p we have*

$$I_1(X; a, b) \le p^{3b-a} I_1(X; 3b, b)$$

if $1 \le a \le 3b$.

Lemma 6. *For any prime p we have*

$$I_2(X; a, b) \le 2bp^{4(b-a)} I_2(X; 2b-a, b)$$

whenever $1 \le a \le b$.

We are now ready to assemble all these results to prove the following recursive estimate for I_2.

Lemma 7. *If* $1 \le a \le b$ *and* $p^b \le X$ *we have*

$$I_2(X; a, b) \le 2bp^{-10a/3+14b/3} I_2(X; b, 2b-a)^{1/3} I_2(X; b, 3b)^{1/6} J(2X/p^b)^{1/2}.$$

The reader may note that the above inequality is a neat form of the bound in Lemma 5.2 of [Wooley 2016].

For the proof we successively apply Lemmas 6, 3, 5 and 4, giving

$$\begin{aligned}
&I_2(X; a, b)\\
&\qquad \le 2bp^{4(b-a)} I_2(X; 2b-a, b)\\
&\qquad \le 2bp^{4(b-a)} I_2(X; b, 2b-a)^{1/3} I_1(X; 2b-a, b)^{2/3}\\
&\qquad \le 2bp^{4(b-a)} I_2(X; b, 2b-a)^{1/3} \{p^{3b-(2b-a)} I_1(X; 3b, b)\}^{2/3}\\
&\qquad \le 2bp^{4(b-a)+2(a+b)/3} I_2(X; b, 2b-a)^{1/3} \{I_2(X; b, 3b)^{1/4} J(2X/p^b)^{3/4}\}^{2/3}\\
&\qquad = 2bp^{-10a/3+14b/3} I_2(X; b, 2b-a)^{1/3} I_2(X; b, 3b)^{1/6} J(2X/p^b)^{1/2}.
\end{aligned}$$

Here we should observe that, in applying Lemma 5 to $I_1(X; 2b-a, b)$, the necessary condition "$a \le 3b$" is satisfied, since $2b-a \le 3b$.

Everything is now in place to complete the proof of the theorem. We note the trivial upper bound $J(X) \ll X^{12}$ and the trivial lower bound $J(X) \ge [X]^6 \gg X^6$ (coming from the obvious diagonal solutions $x_i = x_{6+i}$ for $i \le 6$). Thus we may define a real number $\Delta \in [0, 6]$ by setting

$$\Delta = \inf\{\delta \in \mathbb{R} : J(X) \ll X^{6+\delta} \text{ for } X \ge 1\}. \tag{3}$$

It follows that we will have $J(X) \ll_\varepsilon X^{6+\Delta+\varepsilon}$ for any $\varepsilon > 0$. Our goal of course is to show that $\Delta = 0$.

We observe that

$$I_2(X; a, b) \le J(X) \ll_\varepsilon X^{6+\Delta+\varepsilon}$$

for $1 \le a \le b$, and hence that

$$I_2(X;a,b) \ll_\varepsilon X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{3(3b-a)}, \tag{4}$$

since $3(3b-a) \ge 2a+4b$ for $a \le b$. We now proceed to use Lemma 7 to prove, by induction on n, that

$$I_2(X;a,b) \ll_{\varepsilon,n,a,b} X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{(3-n\Delta/6)(3b-a)} \tag{5}$$

for any integer $n \ge 0$, provided that

$$1 \le a \le b \tag{6}$$

and

$$p^{3^n b} \le X. \tag{7}$$

The base case $n = 0$ is exactly the bound (4). The reader may be puzzled by the choice of the exponent for p in (5). We shall discuss this further in the final section.

Given (5) we have

$$\begin{aligned} I_2(X;b,2b-a) &\ll_{\varepsilon,n,a,b} X^{6+\Delta+\varepsilon} p^{-2b-4(2b-a)} p^{(3-n\Delta/6)(3(2b-a)-b)} \\ &= X^{6+\Delta+\varepsilon} p^{4a-10b} p^{(3-n\Delta/6)(5b-3a)}. \end{aligned}$$

Note that the conditions corresponding to (6) and (7) are satisfied if

$$p^{3^{n+1}b} \le X.$$

since we will have $1 \le b \le 2b-a$ whenever $1 \le a \le b$, and

$$p^{3^n(2b-a)} \le p^{3^{n+1}b} \le X.$$

In a similar way, (5) implies that

$$\begin{aligned} I_2(X;b,3b) &\ll_{\varepsilon,n,b} X^{6+\Delta+\varepsilon} p^{-2b-12b} p^{(3-n\Delta/6)(9b-b)} \\ &= X^{6+\Delta+\varepsilon} p^{-14b} p^{(3-n\Delta/6)(8b)} \end{aligned}$$

the conditions corresponding to (6) and (7) holding whenever $b \ge 1$.

Finally we have

$$J(2X/p^b) \ll_\varepsilon X^{6+\Delta+\varepsilon} p^{-6b-\Delta b}$$

provided that $p^b \le X$. Feeding these estimates into Lemma 7 we deduce that

$$\begin{aligned} I_2(X;a,b) \ll_{\varepsilon,n,a,b} & \; p^{-10a/3+14b/3}\{X^{6+\Delta+\varepsilon} p^{4a-10b} p^{(3-n\Delta/6)(5b-3a)}\}^{1/3} \\ & \times \{X^{6+\Delta+\varepsilon} p^{-14b} p^{(3-n\Delta/6)(8b)}\}^{1/6}\{X^{6+\Delta+\varepsilon} p^{-6b-\Delta b}\}^{1/2} \\ = & \; X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{(3-n\Delta/6)(3b-a)} p^{-\Delta b/2} \\ \le & \; X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{(3-(n+1)\Delta/6)(3b-a)}, \end{aligned}$$

since $b/2 \ge (3b-a)/6$. This provides the required induction step.

Having established (5) we apply it with $a = b = 1$, and p chosen to lie in the range

$$\tfrac{1}{2}X^{1/3^n} \le p \le X^{1/3^n}.$$

There will always be a suitable $p \ge 5$ if

$$X \ge 10^{3^n}.$$

We then deduce from Lemma 2 that

$$J(X) \ll pJ(2X/p) + p^{12}I_2(X;\, 1,\, 1) \ll_{\varepsilon,n} p(X/p)^{6+\Delta+\varepsilon} + X^{6+\Delta+\varepsilon}p^{12-n\Delta/3}.$$

If Δ were strictly positive we could choose n sufficiently large that $n\Delta \ge 39$, and would then conclude that

$$J(X) \ll_{\varepsilon,n} X^{6+\Delta+\varepsilon}p^{-1} \ll_{\varepsilon,n} X^{6+\Delta-3^{-n}+\varepsilon},$$

contradicting the definition (3). We must therefore have $\Delta = 0$, as required for the theorem.

The reader will probably feel that the final stages of the argument, from (5) onward, are lacking in motivation. The final section of the paper will offer an explanation for the route chosen.

3. Proof of the lemmas

We begin by examining Lemma 1. We observe that there is an $\eta \in (0, p^b]$ such that $I_0(X; a, b)$ counts solutions to (1) in which each x_i takes the shape $\eta + p^b y_i$, with integer variables y_i. We will have $0 \le y_i \le X/p^b$. Thus if we set $z_i = y_i + 1$ we find that $1 \le z_i \le 1 + X/p^b \le 2X/p^b$, in view of our condition $p^b \le X$. Moreover we know that if the x_i satisfy (1) then so too will the y_i and the z_i. It follows that $I_0(X; a, b) \le J_{s,k}(2X/p^b)$ as claimed.

To prove Lemma 2 we split solutions of (1) into congruence classes for which $x_i \equiv \xi_i \pmod{p}$ for $1 \le i \le 12$. The number of solutions in which

$$x_1 \equiv \cdots \equiv x_{12} \pmod{p}$$

is at most

$$\sum_{\eta \pmod{p}} I_0(X;\, 0, \eta;\, 1,\, 1) \le pI_0(X;\, 1,\, 1) \le pJ(2X/p),$$

by Lemma 1. For the remaining solutions to (1) there is always a pair of variables that are incongruent modulo p, and it follows that there exist $\xi \not\equiv \eta \pmod{p}$ such that

$$J(X) \le pJ(2X/p) + \binom{12}{2}p(p-1)\int_{(0,1]^3} |f_1(\boldsymbol{\alpha};\, \xi)f_1(\boldsymbol{\alpha};\, \eta)f(\boldsymbol{\alpha})^{10}|\, d\boldsymbol{\alpha}.$$

By Hölder's inequality we have

$$\begin{aligned}&\int_{(0,1]^3}|f_1(\boldsymbol{\alpha};\xi)f_1(\boldsymbol{\alpha};\eta)f(\boldsymbol{\alpha})^{10}|\,d\boldsymbol{\alpha}\\ &\quad\le\left\{\int_{(0,1]^3}|f_1(\boldsymbol{\alpha};\xi)|^4|f_1(\boldsymbol{\alpha};\eta)|^8\,d\boldsymbol{\alpha}\right\}^{1/12}\left\{\int_{(0,1]^3}|f_1(\boldsymbol{\alpha};\xi)|^8|f_1(\boldsymbol{\alpha};\eta)|^4\,d\boldsymbol{\alpha}\right\}^{1/12}\\ &\qquad\times\left\{\int_{(0,1]^3}|f(\boldsymbol{\alpha})|^{12}\,d\boldsymbol{\alpha}\right\}^{5/6},\end{aligned}$$

whence

$$J(X)\ll pJ(2X/p)+p^2I_2(X;1,1)^{1/12}I_2(X;1,1)^{1/12}J(X)^{5/6}.$$

We deduce that

$$J(X)\ll pJ(2X/p)+p^{12}I_2(X;1,1),$$

as required for the lemma.

Lemma 3 is a trivial application of Hölder's inequality. We have

$$\begin{aligned}&I_2(X;\xi,\eta;a,b)\\ &\quad=\int_{(0,1]^3}|f_a(\boldsymbol{\alpha};\xi)|^4|f_b(\boldsymbol{\alpha};\eta)|^8\,d\boldsymbol{\alpha}\\ &\quad\le\left\{\int_{(0,1]^3}|f_a(\boldsymbol{\alpha};\xi)|^8|f_b(\boldsymbol{\alpha};\eta)|^4\,d\boldsymbol{\alpha}\right\}^{1/3}\left\{\int_{(0,1]^3}|f_a(\boldsymbol{\alpha};\xi)|^2|f_b(\boldsymbol{\alpha};\eta)|^{10}\,d\boldsymbol{\alpha}\right\}^{2/3}\\ &\quad\le I_2(X;b,a)^{1/3}I_1(X;a,b)^{2/3},\end{aligned}$$

and the lemma follows.

For Lemma 4 we note that

$$\begin{aligned}&I_1(X;\xi,\eta;a,b)\\ &\qquad=\int_{(0,1]^3}|f_a(\boldsymbol{\alpha};\xi)|^2|f_b(\boldsymbol{\alpha};\eta)|^{10}\,d\boldsymbol{\alpha}\\ &\qquad\le\left\{\int_{(0,1]^3}|f_b(\boldsymbol{\alpha};\xi)|^4|f_a(\boldsymbol{\alpha};\eta)|^8\,d\boldsymbol{\alpha}\right\}^{1/4}\left\{\int_{(0,1]^3}|f_b(\boldsymbol{\alpha};\eta)|^{12}\,d\boldsymbol{\alpha}\right\}^{3/4}\\ &\qquad\le I_2(X;b,a)^{1/4}I_0(X;b,b)^{3/4}\\ &\qquad\le I_2(X;b,a)^{1/4}J(2X/p^b)^{3/4},\end{aligned}$$

by Hölder's inequality and Lemma 1.

Turning next to Lemma 5 we note that $I_1(X;\xi,\eta;a,b)$ counts solutions of (1) in which $x_i=\xi+p^ay_i$ for $i=1$ and $i=7$, and $x_i=\eta+p^by_i$ for the remaining indices i. If we set $\nu = \xi - \eta$ we deduce that the variables

$$z_i = \begin{cases} \nu + p^a y_i & i = 1 \text{ or } 7, \\ p^b y_i & \text{otherwise}, \end{cases}$$

also satisfy (1). In particular, the equation of degree $j = 3$ yields

$$(\nu + p^a z_1)^3 \equiv (\nu + p^a z_7)^3 \pmod{p^{3b}}.$$

Now, crucially, we use the fact that $\xi \not\equiv \eta \pmod{p}$, whence $p \nmid \nu$. It follows that we must have $\nu + p^a z_1 \equiv \nu + p^a z_7 \pmod{p^{3b}}$, and hence $z_1 \equiv z_7 \pmod{p^{3b-a}}$. We therefore have $x_1 \equiv x_7 \equiv \xi' \pmod{p^{3b}}$ for one of p^{3b-a} possible values of ξ', so that

$$I_1(X; \xi, \eta; a, b) \le p^{3b-a} I_1(X; 3b, b),$$

which suffices for the lemma.

Finally we must handle Lemma 6. We note that $I_2(X; \xi, \eta; a, b)$ counts solutions of (1) in which $x_i = \xi + p^a y_i$ for $i = 1, 2, 7$ and 8, and $x_i = \eta + p^b y_i$ for the remaining indices i. As in the proof of Lemma 5 we set $\nu = \xi - \eta$ and $z_i = x_i - \eta$, so that the z_i also satisfy (1). We will have $p^b \mid z_i$ for $3 \le i \le 6$ and $9 \le i \le 12$, whence

$$(\nu + p^a y_1)^j + (\nu + p^a y_2)^j \equiv (\nu + p^a y_7)^j + (\nu + p^a y_8)^j \pmod{p^{bj}} \quad (1 \le j \le 3)$$

with $\nu = \xi - \eta \not\equiv 0 \pmod{p}$. We shall use only the congruences for $j = 2$ and 3. On expanding these we find that

$$2\nu S_1 + p^a S_2 \equiv 0 \pmod{p^{2b-a}} \tag{8}$$

and

$$3\nu^2 S_1 + 3\nu p^a S_2 + p^{2a} S_3 \equiv 0 \pmod{p^{3b-a}},$$

where

$$S_j = y_1^j + y_2^j - y_7^j - y_8^j \quad (j = 1, 2, 3).$$

Eliminating S_1 from these yields

$$3\nu p^a S_2 + 2p^{2a} S_3 \equiv 0 \pmod{p^{2b-a}},$$

whence

$$3\nu S_2 + 2p^a S_3 \equiv 0 \pmod{p^{2b-2a}}.$$

Moreover (8) trivially implies that

$$2\nu S_1 + p^a S_2 \equiv 0 \pmod{p^{2b-2a}}.$$

It appears that we have wasted some information here, but the above congruences are sufficient.

We now call on the following result, which we shall prove at the end of this section.

Lemma 8. *With the notations above for S_j, let $N(p;a,c)$ denote the number of solutions (y_1,y_2,y_7,y_8) modulo p^c of the congruences*

$$2\nu S_1+p^aS_2\equiv 3\nu S_2+2p^aS_3\equiv 0 \pmod{p^c}.$$

Then if $a\geq 1$ and $c\geq 0$ we will have $N(p;a,c)\leq (c+1)p^{2c}$.

If $y_i\equiv y_{i0} \pmod{p^{2(b-a)}}$ for $i=1,2,7,8$ then $x_i\equiv \xi_i \pmod{p^{2b-a}}$, with $\xi_i=\xi+p^ay_{i0}$. The number of solutions to (1) counted by $I_2(X;\xi,\eta;a,b)$ for which $y_i\equiv y_{i0} \pmod{p^{2(b-a)}}$ is then given by

$$\begin{aligned}
\int_{(0,1]^3} & f_{2b-a}(\boldsymbol{\alpha};\xi_1)f_{2b-a}(\boldsymbol{\alpha};\xi_2)\overline{f_{2b-a}(\boldsymbol{\alpha};\xi_7)f_{2b-a}(\boldsymbol{\alpha};\xi_8)}|f_b(\boldsymbol{\alpha};\eta)|^8\,d\boldsymbol{\alpha}\\
&\leq \int_{(0,1]^3}\Big|\prod_{i=1,2,6,7} f_{2b-a}(\boldsymbol{\alpha};\xi_i)\Big||f_b(\boldsymbol{\alpha};\eta)|^8\,d\boldsymbol{\alpha}\\
&\leq \prod_{i=1,2,6,7}\left\{\int_{(0,1]^3}|f_{2b-a}(\boldsymbol{\alpha};\xi_i)|^4|f_b(\boldsymbol{\alpha};\eta)|^8\,d\boldsymbol{\alpha}\right\}^{1/4}\\
&\leq \prod_{i=1,2,6,7} I_2(X;\xi_i,\eta;2b-a,b)^{1/4}\\
&\leq I_2(X;2b-a,b),
\end{aligned}$$

by Holder's inequality. It then follows from Lemma 8 that

$$I_2(X;a,b)\leq N\big(p;a,2(b-a)\big)I_2(X;2b-a,b)\leq 2bp^{4(b-a)}I_2(X;2b-a,b)$$

as required.

It remains to prove Lemma 8, for which we use induction on c. The base case $c=0$ is trivial. When $c=1$ we have $p\mid S_1$ and $p\mid S_2$ and the number of solutions is $2p^2-p$, which is also satisfactory. In general we shall say that a solution (y_1,y_2,y_7,y_8) is singular if

$$y_1\equiv y_2\equiv y_7\equiv y_8 \pmod{p},$$

and nonsingular otherwise. For a nonsingular solution the vectors

$$\nabla(2\nu S_1+p^aS_2)\quad\text{and}\quad\nabla(3\nu S_2+2p^aS_3)$$

are not proportional modulo p, since $a\geq 1$ and $p\nmid 6\nu$. It follows that a nonsingular solution (y_1,y_2,y_7,y_8) of the congruences modulo p^c will lift to exactly p^2 solutions modulo p^{c+1}. Thus if we write $N_0(p;a,c)$ for the number of nonsingular solutions modulo p^c we will have $N_0(p;a,c)\leq 2p^{2c}$, by induction.

For a singular solution we have

$$y_1\equiv y_2\equiv y_7\equiv y_8\equiv\beta \pmod{p},$$

say. If we write $y_i = \beta + pu_i$ and

$$S'_j = u_1^j + u_2^j - u_7^j - u_8^j$$

we find that

$$2\nu S_1 + p^a S_2 = 2(\nu + \beta p^a)pS'_1 + p^{a+2}S'_2$$

and

$$3\nu S_2 + 2p^a S_3 = 6\beta(\nu + \beta p^a)pS'_1 + 3(\nu + 2\beta p^a)p^2 S'_2 + 2p^{a+3}S'_3.$$

Hence

$$2\nu' pS'_1 + p^{a+2}S'_2 \equiv 6\beta\nu' pS'_1 + 3(\nu' + \beta p^a)p^2 S'_2 + 2p^{a+3}S'_3 \equiv 0 \pmod{p^c}$$

with $\nu' = \nu + \beta p^a \not\equiv 0 \pmod{p}$. Eliminating S'_1 from the second expression yields

$$3\nu' p^2 S'_2 + 2p^{3+a}S'_3 \equiv 0 \pmod{p^c}$$

and we deduce that

$$2\nu' S'_1 + p^{a+1}S'_2 \equiv 0 \pmod{p^{c-1}} \tag{9}$$

and

$$3\nu' S'_2 + 2p^{a+1}S'_3 \equiv 0 \pmod{p^{c-2}}. \tag{10}$$

Since we are counting values of y_i modulo p^c we have to count values of u_i modulo p^{c-1}. However any solution of

$$2\nu' S'_1 + p^{a+1}S'_2 \equiv 3\nu' S'_2 + 2p^{a+1}S'_3 \equiv 0 \pmod{p^{c-2}}$$

modulo p^{c-2} lifts to exactly p^3 solutions of the two congruences (9) and (10) modulo p^{c-1}, since

$$\nabla(2\nu' S'_1 + p^{a+1}S'_2) \equiv 2\nu'(1, 1, -1, -1) \not\equiv 0 \pmod{p}.$$

It follows that (9) and (10) have $p^3 N(p; a+1, c-2)$ solutions for each of the p possible choices of β, provided of course that $c \geq 2$.

We are therefore able to conclude that

$$N(p; a, c) \leq N_0(p; a, c) + p^4 N(p; a+1, c-2) \leq 2p^{2c} + p^4 N(p; a+1, c-2)$$

for $c \geq 2$, and the lemma then follows by induction on c.

We conclude this section by remarking that in this final inductive argument, we have estimates of the same order of magnitude for both the number of singular solutions and the number of nonsingular solutions. When one tries to generalize the argument to systems of more congruences the singular solutions can dominate the count in an unwelcome way. It is for this reason that Wooley's approach requires a "conditioning" step in general, in order to remove singular solutions at the outset. Fortunately we just manage to avoid this in our situation.

4. Remarks on the conclusion to the proof

This final section is intended to shed some light on the argument that leads from Lemma 7 to the theorem. In particular the reader may be curious as to how one is led to formulate the induction hypothesis (5). The issue is that repeated applications of Lemma 7, starting from $I_2(X; 1, 1)$ for example, produce values of $I_2(X; a, b)$ with a large number of different pairs a, b; and one wants an induction hypothesis that will apply successfully to all of them.

Suppose one assumes that $J(X) \ll_\varepsilon X^{\theta+\varepsilon}$ for any $\varepsilon > 0$ and that for any positive integers $a \leq b$ one has

$$I_2(X; a, b) \ll_\varepsilon X^{\theta+\varepsilon} p^{\alpha a+\beta b} \tag{11}$$

for some constants α and β, for a suitable range $p \leq X^{\delta(\alpha,\beta)}$, say.

Then Lemma 7 yields

$$I_2(X; a, b) \ll_b X^\theta p^{\alpha' a+\beta' b}$$

for $a \leq b$, with new constants

$$\alpha' = -\tfrac{10}{3} - \tfrac{1}{3}\beta, \quad \beta' = \tfrac{14}{3} + \tfrac{1}{2}\alpha + \tfrac{7}{6}\beta - \tfrac{1}{2}\theta.$$

We can express this by writing

$$\binom{\alpha'}{\beta'} = \boldsymbol{c} + M\binom{\alpha}{\beta},$$

with

$$\boldsymbol{c} = \binom{-10/3}{14/3-\theta/2}, \quad M = \begin{pmatrix} 0 & -1/3 \\ 1/2 & 7/6 \end{pmatrix}.$$

Starting with $\alpha = \beta = 0$, for example, we obtain inductively a succession of bounds of the shape (11), with

$$\binom{\alpha}{\beta} = \binom{\alpha_n}{\beta_n} = \boldsymbol{c} + M\boldsymbol{c} + \cdots + M^n\boldsymbol{c}.$$

The matrix M has eigenvalues 1 and $\frac{1}{6}$, and can be diagonalized as PDP^{-1} with

$$P = \begin{pmatrix} -1 & -2 \\ 3 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{6} \end{pmatrix}.$$

It then follows that

$$\binom{\alpha_n}{\beta_n} = nP\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P^{-1}\boldsymbol{c} + O(1) = \frac{(6-\theta)n}{5}\binom{-1}{3} + O(1)$$

as n tends to infinity. For any starting pair a, b we will have $3b - a \geq 2b \geq 2$. Thus if $\theta > 6$ we will eventually have $\alpha_n a + \beta_n b < -1$, say, for suitably large n.

We therefore obtain

$$I_2(X; a, b) \ll_\varepsilon X^{\theta+\varepsilon} p^{-1}$$

for $p \le X^\delta$, for some $\delta = \delta_n$ depending on θ. This leads to a contradiction, as in Section 2.

We therefore see that the crucial feature of Lemma 7 is that it leads to a matrix M having its largest eigenvalue equal to 1. The corresponding eigenvector is $(\alpha, \beta) = (-1, 3)$, and the argument of Section 2 has therefore been expressed in terms of the linear combination $3b - a$.

References

[Bourgain et al. 2016] J. Bourgain, C. Demeter, and L. Guth, "Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three", *Ann. of Math.* (2) **184**:2 (2016), 633–682. MR Zbl

[Ford and Wooley 2014] K. Ford and T. D. Wooley, "On Vinogradov's mean value theorem: strongly diagonal behaviour via efficient congruencing", *Acta Math.* **213**:2 (2014), 199–236. MR Zbl

[Wooley 2012] T. D. Wooley, "Vinogradov's mean value theorem via efficient congruencing", *Ann. of Math.* (2) **175**:3 (2012), 1575–1627. MR Zbl

[Wooley 2013] T. D. Wooley, "Vinogradov's mean value theorem via efficient congruencing, II", *Duke Math. J.* **162**:4 (2013), 673–730. MR Zbl

[Wooley 2014] T. D. Wooley, "Translation invariance, exponential sums, and Waring's problem", pp. 505–529 in *Proceedings of the International Congress of Mathematicians* (Seoul, 2014), vol. II, edited by S. Y. Jang et al., Kyung Moon Sa, Seoul, South Korea, 2014. MR Zbl

[Wooley 2015] T. D. Wooley, "Multigrade efficient congruencing and Vinogradov's mean value theorem", *Proc. Lond. Math. Soc.* (3) **111**:3 (2015), 519–560. MR Zbl

[Wooley 2016] T. D. Wooley, "The cubic case of the main conjecture in Vinogradov's mean value theorem", *Adv. Math.* **294** (2016), 532–561. MR Zbl

[Wooley 2017] T. D. Wooley, "Approximating the main conjecture in Vinogradov's mean value theorem", *Mathematika* **63**:1 (2017), 292–350. MR Zbl

[Wooley 2019] T. D. Wooley, "Nested efficient congruencing and relatives of Vinogradov's mean value theorem", *Proc. Lond. Math. Soc.* (3) **118**:4 (2019), 942–1016. MR Zbl

Received 6 Jul 2021. Revised 14 Sep 2021.

D. R. HEATH-BROWN:

rhb@maths.ox.ac.uk
University of Oxford, Mathematical Institute, Oxford, United Kingdom

Essential Number Theory
Vol. 1, No. 1, 2022
https://doi.org/10.2140/ent.2022.1.13

Exceptional zeros, sieve parity, Goldbach

John B. Friedlander and Henryk Iwaniec

We survey connections between the possible existence of exceptional real zeros of Dirichlet L-functions and the sieve parity barrier and then show how recent work tying them to the Goldbach problem can be viewed in a considerably generalized framework.

1. Introduction

A fundamental problem in analytic number theory is that of establishing excellent upper and lower bounds in general sieve methods, most especially in the linear sieve. Following a great deal of progress, stretching now over a century, one gradually became aware of a general "parity barrier" which governs the limitations of what one can hope to accomplish, at least in general.

A fundamental problem in analytic number theory is that of establishing zero-free regions for Dirichlet L-functions. In case the corresponding character $\chi \pmod q$ is complex or, alternatively, for all complex zeros $\rho = \beta + i\gamma$ with $\gamma \neq 0$, one has long known how to produce zero-free regions of the type

$$\sigma \geq 1 - c/\log q(|t|+1) \tag{1-1}$$

where $s = \sigma + it$ with a positive constant c. In the remaining situation, where both χ and s are real, much less is known, nothing more recent than a famous "ineffective" estimate of Siegel for the L-function at $s = 1$ which enables a bound like (1-1) but only with the replacement of $\log q$ by q^{ε} with arbitrary $\varepsilon > 0$ and a numerically uncomputable c depending on ε. This exponentially weaker result has been a serious impediment to progress in many basic questions.

It is not unfair to claim that much progress in mathematics proceeds by analogy. The two problems above, in many aspects, ring familiar to each other. The first purpose of this paper is to illustrate ways in which this has been found to be true. Our second purpose is to, in the case of one close recently discovered connection, carry forward this investigation to a new, deeper and more general setting.

Friedlander was supported in part by NSERC grant A5123.
MSC2020: 11M20, 11N05, 11N35, 11P32.
Keywords: primes, sieves, exceptional zeros, Goldbach conjecture.

We recall, that an "exceptional" zero is a real zero β that does lie in the region (1-1) for a constant c. If however there were only a finite number of these we could (since the L-functions do not vanish at $s = 1$) adjust the constant c to exclude them all from the region. Thus the name is really not a very good one for an individual zero since the concept requires an infinite sequence of these. Nevertheless, it is ingrained in the literature; when we use it we are thinking of such a sequence. It is known, essentially due to Landau, that such a sequence of moduli, should one exist, must be very lacunary; the zeros would all be simple, at most one per modulus and indeed with the exceptional moduli q_i satisfying

$$\frac{\log q_{i+1}}{\log q_i} \to \infty.$$

Failing a proof of their nonexistence, it is the lack of any examples of exceptional zeros that leads to the ineffectivity in results such as that of Siegel. Specific real (or nearly real) zeros can and do lead to computationally effective results, even when, as first realized in [Friedlander 1976], they are all the way over at $s = \frac{1}{2}$, a location where the GRH does not prohibit their appearance.

In the absence of a solution to the problem of whether there exist exceptional zeros, there have naturally been attempts to relate the question to other very difficult problems. One class of results of this type deals with showing that the assumption of the existence of exceptional zeros leads to consequences for prime number distribution that are beyond current reach, but are nevertheless expected to be true. There have been in recent years quite a number of such results, several by the current authors; see [Heath-Brown 1983; Friedlander and Iwaniec 2003; 2004; 2005; Merikoski 2021].

These statements, although conditional, can be quite deep and spectacular. For example, in the case of [Friedlander and Iwaniec 2003], we derived asymptotics for the counting of primes $p \le x$ in arithmetic progressions of modulus $q < x^{1/2+\delta}$, so beyond the reach of the generalized Riemann hypothesis. An essential ingredient for this was our asymptotic formula for the divisor function $\tau_3(n)$, $n \le x$ in progressions to modulus $q \le x^{1/2+\delta'}$, which we deduced [Friedlander and Iwaniec 1985] from the expected estimates for exponential sums over relevant varieties, proofs of which were provided for us by Birch and Bombieri, using in turn the Riemann hypothesis for varieties, proved by Deligne. The type of applications of Deligne's work, pioneered in [Friedlander and Iwaniec 1985], has since been extensively developed, for example by Y. Zhang [2014] and, especially, in a whole series of papers by E. Fouvry, E. Kowalski and P. Michel.

Results of this type are not however the primary concern in this paper. On the contrary, we are here highlighting an admittedly smaller class of examples, wherein the assumption of exceptional zeros leads to consequences that are beyond current reach, but are nevertheless expected to be *false*. If one does not believe in the existence of exceptional zeros, then one can dream that this is more promising.

One early example of this class we here consider, by now folklore, shows that the nonexistence of such zeros would follow from improvements, seductively small, in the Brun–Titchmarsh theorem which gives uniform upper bounds for the number of primes in an arithmetic progression. We shall recall this situation in more detail in Section 3.

In more recent years, results have been obtained showing how relatively good bounds for exceptional zeros would follow from assumptions about the less obviously related Goldbach conjecture. The latter famous statement predicts that every even integer exceeding two can be written as the sum of two primes. Hardy and Littlewood [1923] put forth a conjectured asymptotic formula for the number of representations of n as the sum of two primes. Following the normal practice in the subject, we find it simpler to consider a weighted sum over the representations involving the von Mangoldt function, one which leads to an entirely equivalent conjecture. Let

$$G(n) = \sum_{\substack{m_1+m_2=n \\ 2\nmid m_1 m_2}} \Lambda(m_1)\Lambda(m_2). \tag{1-2}$$

The Hardy–Littlewood conjecture predicts that, for n even, we have $G(n) \sim \mathfrak{S}(n)n$ where $\mathfrak{S}(n)$ is a certain positive product over the primes, to be defined in (4-2), and easily large enough to imply Goldbach for all sufficiently large even n.

In Section 4 we recall how even a much weakened form of this conjectured asymptotic completely eliminates the possible existence of any exceptional zeros. Then, in the subsequent sections, we are going to generalize considerably the results of Section 4, for the purpose of showing clearly that the questions are linked to the parity barrier of sieve theory.

But first, in the next section, we give a review of that barrier.

2. Parity problem and the asymptotic sieve

We are interested in counting prime numbers. Beginning from the very earliest works, but especially over the past century, a significant component of this exercise has been the development of sieve methods.

Already from Brun's early successes, a striking achievement was the attainment of upper bounds of the correct order for the number of primes in interesting subsequences of the positive integers.

The attainment of a positive lower bound however seemed always a bit beyond reach. What one could succeed in getting was a lower bound for the number of integers having no more than k prime factors for some value of k, fairly small but invariably greater than one. These results created an interest in the so-called "almost primes".

Gradually, around the middle of the last century, it began to be noticed that the constant factor in the upper bound was never better than twice the expected, though, in the most favorable situations, it could come very close to that.

Analogously, although the lower bound the machinery spewed out for the number of primes was never positive, here too, in the most favorable situations, it could come very close to being so. This has in places been attributed to the incapability of the sieve to distinguish between integers with an odd number of prime factors and those having an even number. The apparent inevitability of this situation has led to the name "parity phenomenon", a name which will seem more clearly appropriate in what follows.

In the same way that, for reasons which are both elementary (think Chebyshev) and analytic (think Riemann), it turns out to be both convenient and elegant to study the primes using the von Mangoldt function, the study of almost primes of order k is facilitated with the introduction of its generalization, given by the Dirichlet convolution

$$\Lambda_k = \mu * \log^k, \tag{2-1}$$

which, as its progenitor ($k = 1$), is supported on integers having at most k distinct prime factors, satisfies (by induction) the recurrence

$$\Lambda_{k+1} = \Lambda_k \cdot \log + \Lambda_k * \Lambda, \tag{2-2}$$

obeys the bounds

$$0 \le \Lambda_k(n) \le (\log n)^k \tag{2-3}$$

and yields the asymptotic formula

$$\sum_{n \le x} \Lambda_k(n) \sim kx(\log x)^{k-1}. \tag{2-4}$$

In case $k = 1$ this last result is of course the prime number theorem and from that and (2-2) one can easily obtain the others. However, it turns out, due to Selberg, that for $k = 2$ and hence for larger k, the formula admits an elementary proof.

In retrospect, we can see that this difference in the levels of difficulty between $k = 1$ and larger k is mirrored in the analytic behavior of their generating functions. The Dirichlet series for Λ_k, namely

$$\sum_{n \ge 1} \Lambda_k(n) n^{-s} = (-1)^k \frac{\zeta^{(k)}(s)}{\zeta(s)}, \tag{2-5}$$

has a pole of order k at $s = 1$. As soon as $k \geq 2$ this pole has multiple order and its effect cannot be canceled out by a simple real zero. Still, it does seem strange that zeta in particular feels the need to worry that she might have an exceptional zero.

It is interesting to note that, although for $k = 1$ the contribution to the sum in (2-4) comes entirely from the integers with an odd number of distinct prime factors, on the contrary, for each $k \geq 2$ the contribution comes half from odd and half from even.

The original motivation for Selberg's discovery was that it could then be combined with other arguments (which he implemented, as did Erdös) leading to elementary proofs for the prime number theorem itself. But that is not the issue here (although perhaps some day it could be).

We are concerned with the counting of primes in more general sequences and, with rare exceptions, we are still far from this goal. It was Bombieri [1976] (see also [Friedlander and Iwaniec 1978; 1996; 2010]) who made breakthroughs in enormously generalizing the elementary results for $k \geq 2$ with his asymptotic sieve. To avoid using excessive space and notation we shall give only the flavor of these results.

We consider a sequence (a_n) of nonnegative reals which satisfies certain basic axioms of linear sieve type. Without the possibility of providing an exhaustive list (see [Friedlander and Iwaniec 2010]) we mention the most essential ones.

We consider, for given $d \geq 1$, the congruence sum

$$A_d(x) = \sum_{\substack{n \leq x \\ n \equiv 0 \pmod{d}}} a_n \tag{2-6}$$

and assume it satisfies the approximation

$$A_d(x) = A_1(x)g(d) + r_d(x) \tag{2-7}$$

where the function $g(d)$ in the "main term" is multiplicative and satisfies the linear sieve condition

$$\sum_{p \leq y} g(p) \log p = \log y + c_g + O_A((\log y)^{-A}) \tag{2-8}$$

for arbitrary A and all $y \leq x$.

For the same A and y the "remainder terms" $r_d(y)$ are assumed to satisfy, for every $\varepsilon > 0$, $D = x^{1-\varepsilon}$, the bound

$$\sum_{d \leq D} |r_d(y)| \ll A_1(x)(\log D)^{-A}. \tag{2-9}$$

We remark that, of these conditions, that for the main term, i.e., (2-8), is known to hold for many interesting sequences. On the other hand, the latter assumption (2-9), although expected to hold for many of those natural sequences that are not very sparse (in that they satisfy $A_1(x) \gg x(\log x)^{-B}$ for some B), is in most cases quite difficult to prove.

By weakening the assumption (2-9), requiring it to hold only for some smaller value of D (the"level of distribution"), one can verify it for many sequences and still can get useful results (see [Friedlander and Iwaniec 1978]), but then the connection to the parity principle rapidly falls off.

We now loosely describe the main thrusts of Bombieri's results [1976].

By heuristic arguments, one is led to the conjecture that for a nice sequence (a_n) satisfying (2-8) one might expect, in place of (2-4), the asymptotic formula

$$\sum_{n\le x} a_n \Lambda_k(n) \sim kH \sum_{n\le x} a_n (\log n)^{k-1} \sim kHA_1(x)(\log x)^{k-1}, \tag{2-10}$$

where H is given by the product

$$H = \prod_p (1-g(p))\Big(1-\frac{1}{p}\Big)^{-1}. \tag{2-11}$$

Bombieri shows in particular that, given a sequence (a_n) satisfying (2-8), (2-9) and some quite mild additional conditions, for each $k \ge 2$ the asymptotic formula (2-10) holds. In fact, one gets more precise information which describes, apart from one glaring loophole, a rather precise picture of the contribution to these sums coming from the integers having a specified number of prime factors.

Given our sequence (a_n) having these properties, there exists a function $\delta(x)$, defined up to $o(1)$, such that the following happens. For each integer $r \ge 1$ let $\sum^r$ denote a sum restricted to positive integers with precisely r distinct prime factors. We fix some $k \ge 2$ and some r with $1 \le r \le k$. Then we have

$$\sum_{n\le x}{}^{r}\, a_n \Lambda_k(n) \sim \delta(x) kH \sum_{n\le x}{}^{r}\, a_n (\log n)^{k-1}. \tag{2-12}$$

Moreover, the same formula holds with the same value of $\delta(x)$ for every other $r \le k$ having the same parity and with the value $2-\delta(x)$ for every $r \le k$ having the opposite parity.

In particular, we see that $0 \le \delta(x) \le 2$. As it happens, for each such real number, one can give examples of sequences satisfying the axioms which give rise to that particular value. We noted earlier that, for each $k \ge 2$, the contribution to the sum in (2-4) comes half from those integers with an odd number of distinct prime factors and half from those with an even number. We can now say that this happens for the more general sequence (a_n) provided that $\delta(x) = 1$.

Bombieri goes on to show that results of the same type apply to sums over a_n weighted by functions far more general, supported on almost primes. To do this he first studies convolutions of the various Λ_k and finite linear combinations of these. He then shows, using the Weierstrass approximation theorem, that quite general normalized smooth functions f, defined at squarefree $n = p_1 \cdots p_r$ by

$$f_r(n) = F_r\left(\frac{\log p_1}{\log n}, \dots, \frac{\log p_r}{\log n}\right), \tag{2-13}$$

with $F_r(u_1, \dots, u_r)$ continuous and symmetric, one for each value of r, can be closely approximated by these linear combinations. This allows him to deduce statements for the sums

$$\sum_{n \le x}{}^{r} a_n F_r\left(\frac{\log p_1}{\log n}, \dots, \frac{\log p_r}{\log n}\right), \tag{2-14}$$

similar to that for the special case (2-12). One needs some growth conditions on the weight function (2-14) which imply that the small prime factors of n do not make an essential contribution. For example, $F_r(u_1, \dots, u_r) \ll u_1 \cdots u_r$ is fine.

3. Primes in arithmetic progressions

That there are relations between the parity barrier and the existence of exceptional zeros becomes particularly evident in connection with the study of the distribution of primes in an arithmetic progression.

Analytic methods have so far succeeded to prove, for example,

$$\psi(x; q, a) = \sum_{\substack{n \le x \\ n \equiv a \pmod q}} \Lambda(n) = \frac{x}{\varphi(q)} - \frac{\chi(a)}{\varphi(q)} \frac{x^\beta}{\beta} + O(x \exp(-c\sqrt{\log x})). \tag{3-1}$$

Here the second term is to be deleted if there is no exceptional zero β. When combined with Siegel's bound, this gives the asymptotic formula, but only with a uniformity in q bounded by an arbitrary fixed power of $\log x$.

For numerous applications it is desirable to have a much wider uniformity so it is of great utility that one has at least an upper bound with that feature, the Brun–Titchmarsh theorem, which is provided by sieve methods.

That upper bound, after years of successive improvement by a constant factor, is

$$\pi(x; q, a) = \sum_{\substack{p \le x \\ p \equiv a \pmod q}} 1 \le \frac{(2+\varepsilon)x}{\varphi(q)\log(x/q)}. \tag{3-2}$$

The Selberg sieve and the beta sieve (see [Friedlander and Iwaniec 2010]) both give this constant 2 and fail to do significantly better. This failure seems inevitable when one considers that the replacement of 2 by $2 - \eta$ with a fixed positive η in a range $x > q^{A(\eta)}$, would lead to the banishment of exceptional zeros. The proof of this result (in somewhat weaker form) is found in [Siebert 1983] with a deeper, more precise, statement in [Granville 2020]. The basic idea is to combine (3-1) and (3-2), the latter having been adjusted to a bound for $\psi(x; q, a)$.

Moreover, using more sophisticated ideas, Siebert and then, in definitive form, Granville show this result to be a special case of the following more general statement.

The linear sieve produces specific upper and lower bound functions $F(s)$ and $f(s)$ respectively, first discovered by Jurkat and Richert [1965], (see Section 12.1 of [Friedlander and Iwaniec 2010]), which apply when we are dealing with a sequence (a_n), $n \le x$ satisfying the linear sieve axiom (2-8) and we are sieving by a set of primes $p \le D^{1/s}$. It is known that these functions F, f are optimal in general, although the specific sequences which provide a counterexample do not resemble arithmetic progressions. Siebert, respectively Granville, show that a fixed improvement of the value of either $F(s)$, $f(s)$ *for any value of* s, again in the case of arithmetic progressions and with x larger than a sufficiently large power of q, implies that exceptional zeros do not exist.

We should mention as well that Granville considers also, and in considerable detail, the corresponding problem in which one sieves by small primes, the integers in a short interval.

Before we leave the topic of arithmetic progressions, we draw attention to an interesting feature of Bombieri's sieve in this case. Naturally enough, the results of the last section are applicable in particular to this most basic sequence $\{n \le x; n \equiv a \pmod{q}\}$. Moreover, for this particular sequence, the level of distribution axiom (2-9) holds uniformly in the modulus q in a much wider range than $q \ll (\log x)^A$, which was our limit for $k = 1$. Hence, we have the following result.

For each integer $k \ge 2$ and $(a, q) = 1$ there holds the asymptotic formula

$$\sum_{\substack{n \le x \\ n \equiv a \ (\mathrm{mod}\, q)}} \Lambda_k(n) \sim k \frac{x}{\varphi(q)} (\log x)^{k-1}, \tag{3-3}$$

now valid for q in the much larger range

$$\log q = o(\log x).$$

The proof of this is to be found in [Friedlander 1981] for $k = 2$ and extends easily to larger k. As was the situation with $\zeta(s)$, for $k \ge 2$ the principal L-function has a pole of multiple order, whereas any potential exceptional zero must be simple. This fact offers an analytic explanation for the resulting extra level of uniformity as compared to that for $k = 1$.

4. The Goldbach problem

In relation to this problem Hardy and Littlewood [1923] conjectured the following asymptotic formula for the sum (1-2).

$$G(n) = \sum_{\substack{m_1+m_2=n \\ 2\nmid m_1m_2}} \Lambda(m_1)\Lambda(m_2) \sim \mathfrak{S}(n)n, \tag{4-1}$$

for n even, where

$$\mathfrak{S}(n) = 2\prod_{p>2}\Big(1-\frac{1}{(p-1)^2}\Big)\prod_{\substack{p\,|\,n \\ p>2}}\Big(1+\frac{1}{p-2}\Big). \tag{4-2}$$

A rather weakened (though still seemingly far from reach) form of the Hardy–Littlewood conjecture which features in our work is as follows.

Weak Hardy–Littlewood–Goldbach conjecture. *For all sufficiently large even n, we have*

$$\delta\mathfrak{S}(n)n < G(n) < (2-\delta)\mathfrak{S}(n)n, \tag{4-3}$$

for some fixed $0 < \delta < 1$.

In [Friedlander and Iwaniec 2021; Friedlander et al. 2022] the following result is proved.

Theorem. *Assume that the Weak Hardy–Littlewood–Goldbach conjecture holds for all sufficiently large even n. Then, there are no zeros of any Dirichlet L-function in the region* (1-1) *with a positive constant c which is now allowed to depend on δ.*

Earlier results in this direction had been given in [Fei 2016; Bhowmik et al. 2019; Bhowmik and Halupczok 2021; Jia 2022; Goldston and Suriajaya 2021]. Those works had narrowed the escape window for the exceptional zeros but did not close it tightly.

In the following sections we are going to consider the arguments that lead to this theorem but in considerably more general form.

5. A generalized Goldbach problem

We let $a(\ell)$, $b(m)$ be given sequences of real numbers having some interesting arithmetical structure and, for every $n \geq 2$ we consider

$$F(n) = \sum_{\ell+m=n} a(\ell)b(m). \tag{5-1}$$

For example, if $a(\ell) = \Lambda(\ell)$, $b(m) = \Lambda(m)$ for $2\nmid \ell m$ then $F(n)$ reduces to the sum $G(n)$ in (1-2). We shall, in any case, be interested in the representations $\ell + m = n$

with ℓ, m being almost primes, hence having a number of prime factors bounded by a fixed quantity, say $r \geq 1$. From now on, some of the constants implied in our estimates may depend on r.

In the appendix we employ heuristic arguments to predict an asymptotic formula

$$F(n) \sim \mathfrak{S}(n)\Phi(n), \tag{5-2}$$

as $n \to \infty$, n even and where $\Phi(n)$ will be defined in (12-2). Then, in Section 14, we mention somewhat weaker estimates

$$\delta\mathfrak{S}(n)\Phi(n) < F(n) < (2-\delta)\mathfrak{S}(n)\Phi(n), \tag{5-3}$$

with a fixed $0 < \delta < 1$ for all even n sufficiently large. The punchline of this heuristic thinking, as it was in [Friedlander et al. 2022], is the following.

Conclusion. The region $s = \sigma + it$ with

$$\sigma \geq 1 - c/\log q(|t|+1) \tag{5-4}$$

is free of zeros of $L(s, \chi)$ for all characters $\chi \pmod q$ and all $q \geq 3$, where $c = c(\delta)$ is a positive constant computable in terms of δ.

Remarks. Although our results are more general than those in [Friedlander et al. 2022] we shall appeal to some of the statements there without change. In particular, the Bombieri version of zero density estimates is a key input to both works; see (4.3) in [Friedlander et al. 2022].

Our generalization from $G(n)$ to $F(n)$ lets us see the parity issue of sieve methods in a more transparent, picturesque context. The arguments we provide are amenable to still further generalization than we have given in this work. However, this would have made the paper more complicated and the extra results would have drifted the topic away from this very connection.

Incidentally, one should not lose hope of proving the original Goldbach conjecture before killing off the exceptional characters because, to this end, when one is not worried about quantitative bounds, one can skip counting many inconvenient representations. Ironically, the existence of exceptional characters might conceivably help to solve the original Goldbach problem, as it does for the twin prime problem and for other questions about prime numbers. In this connection, see as we have mentioned earlier, [Heath-Brown 1983; Friedlander and Iwaniec 2003; 2004; 2005; Merikoski 2021].

6. A series of $F(n)$

Let $N \geq q \geq 3$. We are going to consider the series

$$S(N,q) = \sum_{n \equiv 0 \pmod q} F(n) e^{-n/N} \tag{6-1}$$

by means of L-functions, similarly to [Goldston and Suriajaya 2021; Friedlander and Iwaniec 2021; Friedlander et al. 2022]. First, we detect the congruence $n = \ell + m \equiv 0 \pmod q$ by characters $\chi \pmod q$, getting

$$S(N,q) = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \chi(-1) A(N,\chi) B(N,\bar{\chi}) + E(N,q) \tag{6-2}$$

where

$$A(N,\chi) = \sum_{\ell} \chi(\ell) a(\ell) e^{-\ell/N}, \quad B(N,\bar{\chi}) = \sum_{m} \bar{\chi}(m) b(m) e^{-m/N} \tag{6-3}$$

and $E(N,q)$ is the contribution from the terms ℓ, m with $(\ell m, q) \neq 1$, that is

$$E(N,q) = \sum\sum_{\substack{\ell+m \equiv 0 \pmod q \\ (\ell m, q) \neq 1}} a(\ell) b(m) e^{-(\ell+m)/N}. \tag{6-4}$$

Remark. Naturally, one may think that the main part of (6-2) comes from the principal character χ_0, but the exceptional character χ_1 cannot be dismissed. All the other characters will be shown to yield a negligible contribution. The last term (6-4) will also turn out to be negligible due to the properties of $a(\ell)$.

7. Properties of $a(\ell)$

We assume throughout that $a(\ell)$ is supported on squarefree almost primes and that $a(\ell)$ is quite small if ℓ has a small prime factor. We express this latter property in the following fashion:

$$a(\ell) \ll \log p, \quad \text{for all } p \mid \ell. \tag{7-1}$$

We assume that $a(1) \ll 1$. As for $\ell > 1$, the examples

$$a(\ell) = \Lambda(\ell), \quad a(\ell) = \Lambda_r(\ell)(\log \ell)^{1-r}$$

and the r-fold convolution

$$a(\ell) = (\Lambda * \cdots * \Lambda)(\ell)(\log \ell)^{1-r},$$

all satisfy (7-1); see (2-3). Our assumption means that $a(\ell)$ is majorized by

$$\mathcal{C}(\ell)=\sum_{\substack{p_1\cdots p_r=\ell\\ p_1<\cdots<p_r}}\log p_1,\quad \text{if } \omega(\ell)=r\geq 1, \tag{7-2}$$

where $\omega(\ell)$ as usual denotes the number of distinct prime factors of ℓ. For $\ell=1$ we set $\mathcal{C}(1)=1$. Note that the subsequence $a(d\ell)$ also satisfies (7-1).

Remark. We do not assume that $a(\ell)$ is positive nor that it is equidistributed over reduced residue classes except for the heuristic arguments in the Appendix. The arguments in that section are loose and lacking in mathematical rigor. They serve in this presentation as a motivation to expect the asymptotic formula (12-1), (12-2) (a generalization of the Hardy–Littlewood formula for $G(n)$), which we use in Section 13 to build a reliable model $R(N,q)$ for $S(N,q)$ and then to compare the two in the discussions of Section 14.

Lemma 7.1. *For $x\geq 2$ we have*

$$\sum_{\ell\leq x}|a(\ell)|\ell^{-1}\ll\log x. \tag{7-3}$$

Proof. For the sum over ℓ prime we have the bound

$$\sum_{p\leq x}\frac{\log p}{p}\ll\log x. \tag{7-4}$$

For the sum over ℓ having $r\geq 2$ prime factors we use the bound

$$\sum_{\substack{p_1\cdots p_r\leq x\\ p_1<\cdots<p_r}}(p_1\cdots p_r)^{-1}\log p_1\ll\log x, \tag{7-5}$$

which follows by repeated application of (7-4). □

Actually, we can derive from (7-1) the following bound.

Lemma 7.2. *We have*

$$\sum_{x<\ell\leq qx}|a(\ell)|\ell^{-1}\ll\log q. \tag{7-6}$$

Proof. If $x\leq q^r$ the result follows from (7-3). If ℓ is prime the result follows from

$$\sum_{x<\ell\leq qx}\frac{\log p}{p}=\log q+O(1).$$

Now, let $\ell=p\ell'$, $x<\ell\leq qx$ where ℓ' has all of its $r-1$ prime factors smaller than p. Then, for $x>q^r$ we have $\ell'\leq(qx)^{1-1/r}\leq x^{1-1/r^2}$. Hence, the contribution to the sum (7-6) is bounded by

$$\sum_{\ell'\leq x^{1-1/r^2}} \frac{\mathcal{C}(\ell')}{\ell'} \sum_{x/\ell'<p\leq qx/\ell'} \frac{1}{p} \ll \frac{\log q}{\log x} \sum_{\ell'\leq x} \frac{\mathcal{C}(\ell')}{\ell'} \ll \log q;$$

see (7-3) for the function(7-2) . □

Lemma 7.3. *For $x \geq 2$ we have*

$$\sum_{\ell\leq x} |a(\ell)| \ll x. \tag{7-7}$$

Proof. For the sum over ℓ prime we have the bound $O(x)$. For the sum over ℓ having $r \geq 2$ prime factors, $\sqrt{x} < \ell \leq x$, we estimate as follows:

$$\sum_{\substack{\sqrt{x}<p_1\cdots p_r\leq x\\ p_1<\cdots<p_r}} \log p_1 \ll \sum_{\substack{p_1\cdots p_{r-1}\leq x^{1-1/(2r)}\\ p_1<\cdots<p_{r-1}}} \frac{\log p_1}{p_1\cdots p_{r-1}} \frac{rx}{\log x} \ll x.$$

The contribution of $\ell \leq \sqrt{x}$ is negligible. □

By similar arguments one shows that (use the Brun–Titchmarsh theorem) that

$$\sum_{\substack{\ell\leq x\\ \ell\equiv\alpha \pmod q}} |a(\ell)| \ll \frac{x}{\varphi(q)} \quad \text{if } (\alpha, q) = 1 \text{ and } x \geq q^{r+1}. \tag{7-8}$$

Lemma 7.4. *For $x \geq 2$ and p prime, we have*

$$\sum_{\substack{p\neq\ell\leq x\\ \ell\equiv 0 \pmod p}} |a(\ell)| \ll \frac{x}{p}. \tag{7-9}$$

Proof. The contribution of those ℓ having all prime factors $\geq p$ is bounded by (apply the sieve over the range $P(p)$: the product of all primes less than p)

$$\sum_{\substack{p<\ell\leq x/p\\ (\ell,P(p))=1}} \log p \ll \frac{x}{p} \frac{\log p}{\log p} = \frac{x}{p}.$$

If p is not the smallest prime divisor of ℓ then $a(\ell p)$ with $1 \leq \ell \leq x/p$ satisfies (7-1) so, as in the proof of (7-7), we get a contribution $\ll x/p$. □

Lemma 7.5. *Let $r \geq 1$. For $x \geq 2$ and p prime we have*

$$\sum_{\substack{\ell\leq x\\ \ell\equiv 0 \pmod p\\ \omega(\ell)=r+1}} |a(\ell)| \ll \frac{x}{p} \frac{\log p}{\log x} \left(\log\left(1 + \frac{\log x}{\log p}\right)\right)^{r-1}, \tag{7-10}$$

where, we recall that $\omega(\ell)$ denotes the number of distinct prime factors of ℓ.

Proof. If $p > \sqrt{x}$, then (7-10) follows from (7-9). If $p \leq \sqrt{x}$, and $r = 1$ then (7-10) is obvious. If $p \leq \sqrt{x}$, and $r \geq 2$, then, using (7-5), we see that the sum is bounded by

$$\begin{aligned}\sum_{\substack{p_1\cdots p_r \leq x/p \\ p_1 < \cdots < p_r}} \min(\log p, \log p_1) &\ll \frac{x}{p \log x} \sum_{p_1 < \cdots < p_{r-1} < x} \frac{\min(\log p, \log p_1)}{p_1 \cdots p_{r-1}} \\ &\ll \frac{x}{p} \frac{\log p}{\log x} \sum_{0 \leq j < r} \Big(\sum_{p < p' < x} \frac{1}{p'} \Big)^j \\ &\ll \frac{x}{p} \frac{\log p}{\log x} \Big(\log \frac{\log x}{\log p} \Big)^{r-1}.\end{aligned}$$

□

Corollary 7.6. *Suppose $a(\ell)$ is supported on squarefree numbers having at most r prime factors and that* (7-1) *holds. Then, for $x \geq 2$ and $z \geq 2$ we have*

$$\sum_{p \leq z} \sum_{\substack{\ell \leq x \\ \ell \equiv 0 \pmod p}} |a(\ell)| \ll x \frac{\log z}{\log x} \Big(\log\Big(1 + \frac{\log x}{\log z}\Big)\Big)^{r-1}. \tag{7-11}$$

Actually, for $r \geq 2$ we can take the stronger exponent $r - 2$ rather than $r - 1$.

Lemma 7.7. *For $x \geq 2$ and $q \geq 2$ we have*

$$\sum_{\substack{\ell \leq x \\ (\ell, q) \neq 1}} |a(\ell)| \ll \frac{x}{\log x} (\log\log 2x)^{r-1} \log\log 2q. \tag{7-12}$$

Here, $r \geq 1$ is the bound for the number of prime divisors of ℓ.

Proof. This follows from (7-10) and the easy bound

$$\sum_{p \mid q} \frac{\log p}{p} \ll \log\log 2q.$$

□

Lemma 7.8. *Let $d = (\alpha, q) \neq 1$. For $x \geq q^{2r+2}$ we have*

$$\sum_{\substack{\ell \leq x \\ \ell \equiv \alpha \pmod q}} |a(\ell)| \ll \frac{x \log p(d)}{\varphi(q) \log x} \Big(\log \frac{\log x}{\log p(d)} \Big)^{r-1}, \tag{7-13}$$

where $p(d)$ denotes the smallest prime divisor of d and the implied constant depends only on r.

Proof. The contribution of $\ell \le q^{2r}$ is negligible by (7-7). Let $q^{2r} \le \ell \le x$. We write $\ell = p\ell'$ with ℓ' having at most $r-1$ prime divisors, each of them smaller than p. Therefore $p > q^2$, $\ell' < x^{1-1/r}$ and $a(\ell) \ll \mathcal{C}(\ell')$, $d \mid \ell'$, where we recall the definition (7-2). Since $d \ne 1$, $r \ge 2$. The contribution of these terms to (7-13) is estimated as follows:

$$\sum_{\substack{\ell' < x^{1-1/r} \\ \ell' \equiv 0 \ (\mathrm{mod}\, d)}} \mathcal{C}(\ell') \sum_{\substack{q < p \le x/\ell' \\ p\ell' \equiv \alpha \ (\mathrm{mod}\, q)}} 1 \ll \frac{x}{\varphi(q/d) \log x} \sum_{\substack{\ell' \le x \\ \ell' \equiv 0 \ (\mathrm{mod}\, d)}} \frac{\mathcal{C}(\ell')}{\ell'}$$

by the Brun–Titchmarsh theorem for primes $p \equiv \beta \ (\mathrm{mod}\, q/d)$ where $\beta\ell' \equiv \alpha \ (\mathrm{mod}\, q)$. Note that $(\beta, q/d) = 1$ because $p \nmid q$. The above sum of $\mathcal{C}(\ell')/\ell'$ is estimated using the arrangements as in the proof of (7-10). Let $p(d)$ denote the least prime divisor of d. Then, the sum of $\mathcal{C}(\ell')/\ell'$ over $\ell' \equiv 0 \ (\mathrm{mod}\, d)$, $\ell' \le x$ is estimated by

$$\frac{1}{d} \sum_{\substack{\ell \le x \\ \omega(\ell) \le r-2}} \frac{\mathcal{C}(d\ell)}{\ell} \le \frac{1}{d} \sum_{0 \le s \le r-2} \Biggl(\sum_{p_1 < \cdots < p_s \le p(d)} \frac{\log p_1}{p_1 \cdots p_s} \Biggr) \Biggl(\sum_{p(d) < p \le x} \frac{1}{p} \Biggr)^{r-2-s}$$
$$\ll \frac{\log p(d)}{d} \biggl(\log \frac{\log x}{\log p(d)} \biggr)^{r-2}.$$

Here, if $s = 0$ the sum over $p_1 < \cdots < p_s$ is taken to have the value 1.

This completes the proof of (7-13), using $d\varphi(q/d) \ge \varphi(q)$. □

8. Properties of $b(m)$

We could work with $b(m)$ as with $a(\ell)$ but for simplicity (in order to apply (3.3) of [Friedlander et al. 2022] without modification) we shall assume that

$$b(m) = \sum_{hk=m} \lambda(h)\Lambda(k), \tag{8-1}$$

where $\lambda(h)$ is supported on squarefree almost primes and

$$\lambda(h) \ll \log p \quad \text{for all } p \mid h. \tag{8-2}$$

We take $\lambda(1) = 1$. If $h > 1$, for example, $\lambda(h) = \Lambda_r(h)(\log h)^{1-r}$ is good. Note that $\lambda(h)$ satisfies (7-3)–(7-13). Moreover, we have

$$\sum_{m \le x} |b(m)| \ll x \log x \tag{8-3}$$

for every $x \ge 2$, because

$$\sum_{h \le x} |\lambda(h)| h^{-1} \ll \log x, \tag{8-4}$$

by (7-3) for the lambda function. Actually, we have the stronger result

$$\sum_{x<h\leq qx} |\lambda(h)|h^{-1} \ll \log q, \tag{8-5}$$

for every $x \geq 2$; see (7-6) for the lambda function.

Remark. Many interesting functions supported on almost primes can be well-approximated by sums of functions like $\lambda * \Lambda$. For example, we can take

$$b(m) = F_r\left(\frac{\log p_1}{\log m}, \dots, \frac{\log p_r}{\log m}\right)(\log m)^2$$

if $m = p_1 \cdots p_r$, where we recall F_r in (2-13) is as in Bombieri's asymptotic sieve; see Chapters 3 and 16 of [Friedlander and Iwaniec 2010].

In the case $b(m) = \Lambda(m)$ we have $\lambda(h) = 0$ except for $\lambda(1) = 1$. Therefore, in this special case some of our estimates can be improved by a log factor from those displayed. In particular, in (8-3) the factor $\log x$ can be removed and in (8-4) the "sum" is bounded. In the arguments of the following sections, this special case is therefore much easier, yet the need for these slightly stronger bounds would complicate the exposition. Since the results for this particular example are anyway just those already given in [Friedlander et al. 2022], we omit them from this presentation.

9. Evaluation of $S(N, q)$, first steps

Let $\chi_1 \pmod q$ be a real primitive character of modulus q such that $L(s, \chi_1)$ has a simple real zero β_1 close to $s = 1$. We single out the contributions of χ_0 and χ_1 to (6-2) and estimate the remaining parts as follows:

$$Q(N, q) = \sum_{\chi\neq\chi_0,\chi_1} \chi(-1)A(N, \chi)B(N, \bar{\chi}) = S(H, N, q) + T(H, N, q), \tag{9-1}$$

say, where $S(H, N, q)$ is the partial sum restricted to $h \leq H$ and $T(H, N, q)$ is the complementary partial sum. The first one is bounded by

$$\left(\sum_{\ell} |a(\ell)|e^{-\ell/N}\right) \sum_{h\leq H} |\lambda(h)| \sum_{\chi\neq\chi_0,\chi_1} \left|\sum_k \chi(k)\Lambda(k)e^{-hk/N}\right|. \tag{9-2}$$

The sum over ℓ in (9-2) is bounded by $O(N)$; see (7-7). The sum over k is (3.3) from [Friedlander et al. 2022], so it satisfies

$$\sum_{\chi\neq\chi_0,\chi_1} \left|\sum_k \chi(k)\Lambda(k)e^{-hk/N}\right| \ll \frac{N}{h}(1-\beta_1)\log q, \tag{9-3}$$

provided that $Nh^{-1} \geq q^b$ for a suitably large b; see (5.1) and (3.5) of [Friedlander et al. 2022]. This condition is satisfied for $N \geq Hq^b$. Hence, we get

$$S(H, N, q) \ll N^2(1-\beta_1)(\log q)(\log H). \tag{9-4}$$

Recall that (9-3) exploits the Bombieri zero density theorem with the repulsion effect of the exceptional zero β_1. We do not apply this effect, nor do we need it, for the estimation of $T(H, N, q)$. We write

$$T(H,N,q) = \sum_{\chi \neq \chi_0, \chi_1} \chi(-1)\biggl(\sum_{\ell} a(\ell)\chi(\ell)e^{-\ell/N}\biggr) \sum_{h>H} \sum_{k} \overline{\chi}(hk)\lambda(h)\Lambda(k)e^{-hk/N}.$$

Hence, inserting the corresponding sum for the missing two characters and using orthogonality, we find that

$$\begin{aligned} &T(H,N,q) \\ &= \varphi(q) \sum\sum\sum_{\substack{\ell+hk\equiv 0 \pmod q \\ (\ell,q)=1,\, h>H}} a(\ell)\lambda(h)\Lambda(k)e^{-(\ell+hk)/N} + O\biggl(N^2 \sum_{h>H} |\lambda(h)|h^{-1}e^{-h/2N}\biggr), \end{aligned}$$

on using the trivial bound for the contribution of the two additional characters. Using (7-8), we see that the above main term is also bounded by the above error term. Moreover, this error term is $\ll N^2 \log(N/H)$, as seen by applying (8-5) for $x = H, qH, q^2H, \ldots$. Choosing $H = Nq^{-b}$ we conclude that

$$T(H, N, q) \ll N^2 \log q. \tag{9-5}$$

On adding these estimates (9-4) and(9-5), we see that the sum in (9-1) satisfies $Q(N, q) \leq \varepsilon(N, q)N^2 \log N$ where

$$\varepsilon(N, q) \ll (1-\beta_1)\log q + \frac{\log q}{\log N}. \tag{9-6}$$

We still need to estimate $E(N, q)$ in (6-2) which is given by (6-4). This term is negligible and is actually smaller than the main term by a saving factor $\log N$. Nevertheless, we give simpler arguments producing an estimate somewhat weaker, yet still sufficient for our applications; see (9-7) and (9-8). Recall that $a(\ell)$, $\lambda(h)$ are supported on squarefree numbers having at most r prime divisors. By (7-13) we obtain

$$\begin{aligned} |E(N,q)| &\leq \sum_{\substack{d \mid q \\ d \neq 1}} \sum\sum_{\substack{\ell+m\equiv 0 \pmod q \\ (m,q)=d}} |a(\ell)b(m)|e^{-(\ell+m)/N} \\ &\ll \frac{N}{\varphi(q)} \frac{(\log\log N)^{r-1}}{\log N} \sum_{\substack{d \mid q \\ d \neq 1}} (\log p(d))W(N, d) \end{aligned}$$

where

$$W(N,d)=\sum_{m\equiv 0 \ (\mathrm{mod}\, d)}|b(m)|e^{-m/N}\le\sum_{uv=d}\sum_{\substack{h\equiv 0 \ (\mathrm{mod}\, u)\\ k\equiv 0 \ (\mathrm{mod}\, v)}}\sum\lambda(h)\Lambda(k)e^{-hk/N}.$$

Since k is prime we have $v=1$ or $v=k$. The sum with $v=1$ contributes

$$\begin{aligned}W_1(N,d)&=\sum_{h\equiv 0 \ (\mathrm{mod}\, d)}\lambda(h)\sum_k\Lambda(k)e^{-hk/N}\\&\ll\sum_{h\equiv 0 \ (\mathrm{mod}\, d)}|\lambda(h)|h^{-1}e^{-h/2N}\\&\ll\frac{\log d}{d}N(\log\log N)^{r-1},\end{aligned}$$

by the trivial bound $\lambda(h)\ll\log d$. Then we need, here and later, the easy bound

$$\sum_{d\,|\,q}(\log d)^2d^{-1}\ll(\log\log q)^3.$$

Next, the sum with $v=k$ contributes

$$W_2(N,d)=\sum_{uv=d}\Lambda(v)\sum_{h\equiv 0 \ (\mathrm{mod}\, u)}|\lambda(h)|e^{-hv/N}.$$

The partial sum of $W_2(N,d)$ with $u=1$ is

$$W_{21}(N,d)=\Lambda(d)\sum_h|\lambda(h)|e^{-dh/N}\ll\frac{\Lambda(d)}{d}N;$$

see (7-7) for the λ function. The remaining part of $W_2(N,d)$ is

$$W_{22}(N,d)=\sum_{\substack{uv=d\\ u\neq 1}}\Lambda(v)\sum_{h\equiv 0 \ (\mathrm{mod}\, u)}|\lambda(h)|e^{-hv/N}.$$

Hence,

$$\begin{aligned}\sum_{d\,|\,q}(\log p(d))W_{22}(N,d)&\le\sum_{uv\,|\,q}\Lambda^2(v)\sum_{\substack{u\,|\,h\\ (h,q)\neq 1}}|\lambda(h)|e^{-hv/N}\\&\ll\sum_{v\,|\,q}\Lambda^2(v)\sum_{(h,q)\neq 1}|\lambda(h)|e^{-hv/N}\end{aligned}$$

because $\tau(h)\ll_r 1$. Applying (7-12), we find this is bounded by

$$\biggl(\sum_{v\,|\,q}\frac{\Lambda^2(v)}{v}\biggr)\frac{N}{\log N}(\log\log N)^r\ll\frac{N}{\log N}(\log\log N)^{r+3}.$$

Gathering the above estimates, we obtain

$$E(N,q) \ll \frac{N^2}{\varphi(q)} \frac{(\log\log N)^{2r+2}}{\log N}. \tag{9-7}$$

This is stronger than we needed, namely

$$E(N,q) \ll N^2 \frac{\log q}{\varphi(q)}. \tag{9-8}$$

Now, (6-2) becomes

$$\begin{aligned}&\varphi(q)S(N,q)\\ &\quad = A(N,\chi_0)B(N,\chi_0) + \chi_1(-1)A(N,\chi_1)B(N,\chi_1) + (\varepsilon(N,q)N^2\log N).\end{aligned} \tag{9-9}$$

The coprimality of ℓ, m with q in the main term $A(N,\chi_0)B(N,\chi_0)$ can be dropped within the existing error term, specifically

$$A(N,\chi_0) = A(N,1) + O\left(N\frac{(\log\log N)^r}{\log N}\right) \tag{9-10}$$

and

$$B(N,\chi_0) = B(N,1) + O(N(\log\log N)^r), \tag{9-11}$$

by direct applications of (7-12) for $a(\ell)$ and $b(m)/\log N$ respectively. Note that $(\log\log N)^r \ll (\log(\log N/\log q))^r \log q$.

10. Evaluation of $A(N,\chi_1)$ and $B(N,\chi_1)$

The exceptional character pretends to be the Möbius function on squarefree numbers, so we are able to replace

$$A(N,\chi_1) = \sum_{\ell} \chi_1(\ell)a(\ell)e^{-\ell/N} \tag{10-1}$$

by

$$A(N,\mu) = \sum_{\ell} \mu(\ell)a(\ell)e^{-\ell/N}. \tag{10-2}$$

In this section we use the Linnik zero repulsion phenomenon (see [Bombieri 1987]) to estimate the error caused in making this replacement. For ℓ squarefree we have

$$|\chi_1(\ell) - \mu(\ell)| \le \sum_{p\mid\ell}(1+\chi_1(p)). \tag{10-3}$$

Hence

$$|A(N,\chi_1) - A(N,\mu)| \le \sum_{p}(1+\chi_1(p)) \sum_{\ell\equiv 0 \pmod p} |a(\ell)|e^{-\ell/N}. \tag{10-4}$$

The contribution of $\ell = p$ is bounded by $\Psi(N)$, where

$$\Psi(y) = \sum_p (1 + \chi_1(p))(\log p)e^{-p/y}. \tag{10-5}$$

For $y \geq z = q^b$ we have (apply (5.3) of [Friedlander et al. 2022]):

$$\Psi(y) \ll (1 - \beta_1)y \log y + y(\log y)^{-1}. \tag{10-6}$$

For $p > z$ and $N > z$ we write

$$e^{-\ell/N} \leq e^{-\ell/2N}e^{-p/2N} \leq 6e^{-\ell/2N}(e^{-p/2N} - e^{-p/z}).$$

Hence, the terms ℓ, p with $\ell \neq p > z$ contribute to (10-4) at most

$$\frac{N}{\log N}\left(\log\left(1 + \frac{\log N}{\log z}\right)\right)^{r-1} \sum_p (1 + \chi_1(p))\frac{\log p}{p}(e^{-p/2N} - e^{-p/z}) \tag{10-7}$$

by (7-10). The sum over all p above is equal to

$$\int_z^{2N} \Psi(y)y^{-2}dy \ll (1 - \beta_1)(\log N)^2 + \log\left(\frac{\log 2N}{\log z}\right)$$

by (10-6). Hence (10-7) is bounded by

$$N\left(\log\left(1 + \frac{\log N}{\log z}\right)\right)^r \left((1 - \beta_1)\log N + \frac{1}{\log N}\right). \tag{10-8}$$

For $p \leq z$ we use (7-11) obtaining a contribution to (10-4) at most

$$N\frac{\log z}{\log N}\left(\log\left(1 + \frac{\log N}{\log z}\right)\right)^r. \tag{10-9}$$

Combining estimates (10-6), (10-7), (10-9), we conclude that, if $N \geq q^b$, then

$$|A(N, \chi_1) - A(N, \mu)| \ll \eta(N, q)N \tag{10-10}$$

where

$$\eta(N, q) \ll \left((1 - \beta_1)\log N + \frac{\log q}{\log N}\right)\left(\log \frac{\log N}{\log q}\right)^r. \tag{10-11}$$

Similarly, we can replace $B(N, \chi_1)$ by $B(N, \mu)$. Since the function $b(m)/\log N$ satisfies, for $m \leq N^{2021}$, the same conditions as $a(\ell)$, hence the same arguments as those between (10-3) and (10-11) yield

$$|B(N, \chi_1) - B(N, \mu)| \ll \eta(N, q)N\log N, \tag{10-12}$$

where $\eta(N, q)$ satisfies (10-11), the contribution of $m > N^{2021}$ being microscopic.

11. Evaluation of $S(N, q)$, conclusion

Collecting the results of the last two sections we formulate our basic result:

Proposition 11.1. *Let $a(\ell)$ and $b(m)$ be supported on squarefree numbers having at most r prime factors. Suppose* (7-1), (8-1), (8-2) *hold. Then, for $N \geq q^b$ with a suitable constant b, we have*

$$\varphi(q)S(N,q) = A(N,1)B(N,1) + \chi_1(-1)A(N,\mu)B(N,\mu) + \eta(N,q)N^2\log N \tag{11-1}$$

with

$$\eta(N,q) \ll \left((1-\beta_1)\log N + \frac{\log q}{\log N}\right)\left(\log\frac{\log N}{\log q}\right)^r, \tag{11-2}$$

the implied constant depending on r and where χ_1 $(\mathrm{mod}\, q)$ *is the exceptional character and β_1 is the zero of $L(s,\chi_1)$ in the segment*

$$1 - c(\log q)^{-1} < \beta_1 < 1 \tag{11-3}$$

with c a small positive constant.

Proof. In (9-9) use (9-10), (9-11) to replace χ_0 by 1, use (10-10) and (10-12) to replace χ_1 by μ. □

In case $b(m) = \Lambda(m)$ we have $\lambda(h) = 0$ except for $\lambda(1) = 1$ and, as mentioned in Section 8, in this special, much easier case some of our estimates can be improved by a log factor from those displayed. As an upshot, our final formula (11-1) holds with the error term $\eta(N,q)N^2$.

For $N = q^A$ with A a large exponent we have

$$\eta(N,q) \ll (A(1-\beta_1)\log q + A^{-1})(\log A)^r. \tag{11-4}$$

Given $\delta > 0$ we can make

$$|\eta(N,q)| < \delta \tag{11-5}$$

if the exceptional zero satisfies (11-3) with c sufficiently small:

$$A \asymp \frac{1}{\delta}\left(\log\frac{1}{\delta}\right)^r, \quad c \leq A^{-2}. \tag{11-6}$$

We can write (11-1) in the form

$$\varphi(q)S(N,q) = \sum_{\ell}\sum_{m}(1+\chi_1(-1)\mu(\ell m))a(\ell)b(m)e^{-(\ell+m)/N} + \eta(N,q)N^2\log N, \tag{11-7}$$

where $\eta(N,q)$ satisfies (11-2).

Remarks. Our conditions on $a(\ell)$ and $\lambda(h)$ imply that $A(N,1) \ll N$ and $B(N,1) \ll N\log N$. However, the formula (11-1) is meaningful if

$$A(N,1) \asymp N, \quad B(N,1) \asymp N\log N, \quad \text{for } N \geq q^b. \tag{11-8}$$

As we have already mentioned, the factor $\log N$ in the error term of (11-1) can be deleted if $b(m) = \Lambda(m)$. This is the case of $\lambda(h) = \Lambda_0(h)$, which function vanishes except for $\lambda(1) = \Lambda_0(1) = 1$.

12. Asymptotic formula for $F(n)$: prediction

Recall that $F(n)$ is given by (5-1) with $a(\ell)$ satisfying (7-1) and $b(m)$ given by (8-1) with $\lambda(h)$ satisfying (8-2). As such, $F(n)$ is a generalization of the Goldbach sum so it is too much to be expected to evaluate it unconditionally. Nevertheless, in the Appendix we show heuristic arguments which permit us to predict the following generalization of the Hardy–Littlewood conjecture (4-1).

Corollary. *Under the above-mentioned* (*in Sections 7 and 8*) *conditions on the sequences* $a(\ell)$, $b(m) = (\lambda * \Lambda)(m)$, *we have*

$$F(n) = \sum_{\ell+m=n} a(\ell)b(m) \sim \mathfrak{S}(n)\Phi(n) \tag{12-1}$$

as $n \to \infty$, *n even*, *where* $\mathfrak{S}(n)$ *is given by* (4-2) *and*

$$\Phi(n) = \sum\sum_{\ell+h<n} a(\ell)\lambda(h)h^{-1}. \tag{12-2}$$

Examples. If $b(m) = \Lambda(m)$, we have $\lambda(1) = 1$, $\lambda(h) = 0$ for $h > 1$. Hence

$$\Phi(n) = \sum_{\ell<n-1} a(\ell).$$

Moreover, if $a(\ell) = \Lambda(\ell)$ then we have $\Phi(n) \sim n$ and

$$F(n) = G(n) = \sum_{\ell+m=n} \Lambda(\ell)\Lambda(m) \sim \mathfrak{S}(n)n, \tag{12-3}$$

recovering (4-1). More generally, keeping $b(m) = \Lambda(m)$ but choosing $a(\ell) = \Lambda_k(\ell)/(\log n)^{k-1}$, we have

$$F(n) = \sum_{\ell+m=n} a(\ell)\Lambda(m) \sim k\mathfrak{S}(n)n. \tag{12-4}$$

13. Evaluation of $R(N, q)$

Injecting the asymptotic formula (12-1) into the series (6-1) we obtain the following model for $S(N, q)$:

$$\begin{aligned} R(N,q) &= \sum_{n\equiv 0 \ (\mathrm{mod}\, q)} \mathfrak{S}(n)\Phi(n)e^{-n/N} \\ &= \sum_{\ell}\sum_{h} a(\ell)\lambda(\ell)h^{-1} \sum_{\substack{n\equiv 0 \ (\mathrm{mod}\, q)\\ \ell+h<n,\, n \text{ even}}} \mathfrak{S}(n)e^{-n/N}. \end{aligned} \tag{13-1}$$

Using (6.5) of [Friedlander et al. 2022] one can derive the asymptotic formula

$$\sum_{\substack{n\equiv 0 \ (\mathrm{mod}\, q)\\ n\le x,\, n \text{ even}}} \mathfrak{S}(n) \sim \frac{x}{\varphi(q)}.$$

Hence, the last sum over n in (13-1) is asymptotic to

$$\sim \frac{1}{\varphi(q)}\int_{\ell+h}^{\infty} e^{-x/N}dx = \frac{N}{\varphi(q)}e^{-(\ell+h)/N}$$

and

$$\varphi(q)R(N,q) \sim N\Bigl(\sum_{\ell} a(l)e^{-\ell/N}\Bigr)\Bigl(\sum_{h}\lambda(h)h^{-1}e^{-h/N}\Bigr). \tag{13-2}$$

On the other hand, we have

$$B(N,1) = \sum_{m} b(m)e^{-m/N} = \sum_{h}\lambda(h)\sum_{k}\Lambda(k)e^{-hk/N} \sim N\sum_{h}\lambda(h)h^{-1}e^{-h/N}.$$

Hence, (13-2) becomes

$$\varphi(q)R(N,q) \sim A(N,1)B(N,1). \tag{13-3}$$

This should be compared with (11-1) subject to the conditions (11-8).

14. Exceptional zero effects

It is instructive to observe what happens if we compare the legitimate formula (11-1) with the heuristic (13-3) in the range $N = q^A$. Take A sufficiently large and assume, as we may, that the exceptional constant $c \le A^{-2}$ so that $\eta(N, q)$ is negligible. It follows that $A(N, \mu)B(N, \mu)$ is significantly smaller than $A(N, 1)B(N, 1)$. This observation is attractive if the coefficients $a(\ell)$, $b(m)$ are each supported on almost primes having a fixed parity in the number of their prime divisors, because the

Möbius function is then constant and

$$A(N,\mu)=\mu_A A(N,1)\quad\text{where } \mu_A=\pm 1,$$
$$B(N,\mu)=\mu_B B(N,1)\quad\text{where } \mu_B=\pm 1.$$

Hence

$$|A(N,\mu)B(N,\mu)|=|A(N,1)B(N,1)|$$

and

$$\varphi(q)S(N,q)=\nu A(N,1)B(N,1)+o(N^2\log N)$$

with $\nu=0$ or 2. This inconsistency with (13-3) implies that the exceptional character does not exist! Indeed, it means that one may, a fortiori, kill the exceptional character by assuming the weaker conjecture (5-3) with any $0<\delta<1$, under suitable conditions on the coefficients $a(\ell)$, $b(m)$, as has been done in [Friedlander and Iwaniec 2021] and [Friedlander et al. 2022] for $a(\ell)=\Lambda(\ell)$, $b(m)=\Lambda(m)$.

If, on the other hand, we choose instead $a(\ell)=\Lambda_a(\ell)(\log\ell)^{1-a}$ and $\lambda(h)=\Lambda_b(h)(\log h)^{1-b}$ with numbers $a+b>2$, that is not both 1, then the effect on the exceptional zero no longer shows itself in our arguments. The point is that the series

$$\sum_{\ell}\Lambda_a(\ell)\ell^{-s}=(-1)^a\frac{\zeta(s)^{(a)}}{\zeta(s)}$$

has a pole at $s=1$ of order a, while the series

$$\sum_{\ell}\mu(\ell)\Lambda_a(\ell)\ell^{-s}=\zeta(s)\sum_{n}\frac{\mu(n)}{n^s}(\log n)^a\prod_{p\,|\,n}\Bigl(1-\frac{1}{p^s}\Bigr)$$

has only a simple pole at $s=1$ for any $a\geq 1$. Hence $A(N,\mu)$ is smaller than $A(N,1)$ by a factor $(\log N)^{a-1}$, so it yields a negligible contribution if $a\geq 2$. Similarly for $B(N,\mu)$ if $b\geq 2$. This is the same feature which, in the case of arithmetic progressions, led to the wider range of uniformity in Selberg's formula (2-4) and, more generally, in (3-3).

In view of the above, our formula (11-1) is relevant to the issue of exceptional characters only if its coefficients $a(\ell)$, $b(m)$, can be approximated, via the Weierstrass theorem, by linear combinations of scaled down $\Lambda_a(\ell)$, $\Lambda_b(m)$, in which $a=b=1$ appears (cannot be canceled out). The components with $a+b>2$ can be dismissed in (the highest order term of) $A(N,\mu)B(N,\mu)$.

We encourage the reader to learn the Bombieri approximations by the von Mangoldt functions from the original paper [Bombieri 1976] and to look at Chapters 3 and 16 of [Friedlander and Iwaniec 2010]; see also [Friedlander and Iwaniec 1985], especially Section 20.

Appendix: Heuristic arguments

Again we recall that $F(n)$ is given by (5-1) with $a(\ell)$ satisfying (7-1) and $b(m)$ given by (8-1) with $\lambda(\ell)$ satisfying (8-2). The coefficients $a(\ell)$, $b(m)$ are small if ℓ, m have small prime divisors so we can assume that ℓ, m are odd and that $n = \ell + m$ is even. We write

$$\Lambda(k) = -\sum_{d \mid k} \mu(d) \log d$$

and replace $b = \lambda * \Lambda$ by

$$-\sum_{\substack{dh \mid m \\ d<y}} \lambda(h)\mu(d) \log d,$$

where y is neither too small nor too large. Next, we interpret the equation $\ell + m = n$ by the congruence $\ell \equiv n \pmod{dh}$ with $(\ell, n) = 1$, $\ell < n$ and $(dh, n) = 1$. Arguing by the randomness of $\mu(n)$, we replace $F(n)$ by

$$-\sum_{\substack{d<y \\ (d,n)=1}} \mu(d) \log d \sum_{\substack{h<n/d \\ (h,n)=1}} \lambda(h) \sum_{\substack{\ell<n-dh,\, (\ell,n)=1 \\ \ell \equiv n \pmod{dh}}} a(\ell).$$

Next, assuming the equidistribution of $a(\ell)$ over reduced residue classes, we replace the sum over ℓ by

$$\frac{1}{\varphi(dh)} \sum_{\substack{\ell<n-dh, \\ (\ell,n)=1}} a(\ell).$$

We may think of $\ell < n$ as being not very close to n because otherwise $m = n - \ell$ would be very small, hence so would $b(m)$. Similarly, $h < n - \ell$ should not be close to $n - \ell$ because otherwise $k = (n - \ell)/h$ would be very small. Therefore, the sum over d,

$$-\sum_{\substack{d<y,\, dh<n-\ell \\ (d,n)=1}} \frac{\mu(d)}{\varphi(d)} \log d,$$

is not short, so it is reasonable to replace it by the infinite series

$$-\sum_{(d,n)=1} \frac{\mu(d)}{\varphi(d)} \log d = \mathfrak{S}(n);$$

see for example Lemma 19.3 of [Iwaniec and Kowalski 2004]. Now, we can drop the restriction $(\ell h, n) = 1$ because $a(\ell)$, $\lambda(h)$ are supported on almost primes and are relatively small if ℓ, h have any small prime divisors. For the same reason, we have already replaced $\varphi(dh)$ by $\varphi(d)h$.

The above lines show how we are led to the conjecture (12-1). The arguments of Hardy and Littlewood are rather different. They approach the issue by way of the circle method rather than using the randomness of the Möbius function.

Acknowledgement

We thank D.A. Goldston and A.I. Suriajaya whose preprint [Goldston and Suriajaya 2021] sparked our interest in the relevence to the Goldbach problem of the question of exceptional zeros, leading to the joint paper [Friedlander et al. 2022] and to the current work.

We thank Lillian Pierce for having invited us to submit this work on the occasion of the inauguration of her exciting new journal.

We thank the referees for many interesting suggestions.

References

[Bhowmik and Halupczok 2021] G. Bhowmik and K. Halupczok, "Conditional bounds on Siegel zeros", pp. 25–39 in *Combinatorial and additive number theory IV*, edited by M. B. Nathanson, Springer Proc. Math. Stat. **347**, Springer, 2021. MR

[Bhowmik et al. 2019] G. Bhowmik, K. Halupczok, K. Matsumoto, and Y. Suzuki, "Goldbach representations in arithmetic progressions and zeros of Dirichlet L-functions", *Mathematika* **65**:1 (2019), 57–97. MR Zbl

[Bombieri 1976] E. Bombieri, "The asymptotic sieve", *Rend. Accad. Naz. XL* (5) **1(2)** (1976), 243–269. MR Zbl

[Bombieri 1987] E. Bombieri, "Le grand crible dans la théorie analytique des nombres", pp. i+87 Astérisque **18**, Soc. Mat. de France, Paris, 1987. 2ieme ed. MR Zbl

[Fei 2016] J. Fei, "An application of the Hardy–Littlewood conjecture", *J. Number Theory* **168** (2016), 39–44. MR Zbl

[Friedlander 1976] J. B. Friedlander, "On the class numbers of certain quadratic extensions", *Acta Arith.* **28**:4 (1976), 391–393. MR

[Friedlander 1981] J. B. Friedlander, "Selberg's formula and Siegel's zero", pp. 15–23 in *Recent progress in analytic number theory* (Durham, 1979), vol. 1, edited by H. Halberstam and C. Hooley, Academic Press, London, 1981. MR

[Friedlander and Iwaniec 1978] J. Friedlander and H. Iwaniec, "On Bombieri's asymptotic sieve", *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **5**:4 (1978), 719–756. MR

[Friedlander and Iwaniec 1985] J. B. Friedlander and H. Iwaniec, "Incomplete Kloosterman sums and a divisor problem", *Ann. of Math.* (2) **121**:2 (1985), 319–350. With an appendix by Bryan J. Birch and Enrico Bombieri. MR

[Friedlander and Iwaniec 1996] J. Friedlander and H. Iwaniec, "Bombieri's sieve", pp. 411–430 in *Analytic number theory* (Allerton Park, IL, 1995), vol. 1, edited by B. C. Berndt et al., Progr. Math. **138**, Birkhäuser, Boston, 1996. MR Zbl

[Friedlander and Iwaniec 2003] J. B. Friedlander and H. Iwaniec, "Exceptional characters and prime numbers in arithmetic progressions", *Int. Math. Res. Not.* **2003**:37 (2003), 2033–2050. MR

[Friedlander and Iwaniec 2004] J. B. Friedlander and H. Iwaniec, "Exceptional characters and prime numbers in short intervals", *Selecta Math.* (*N.S.*) **10**:1 (2004), 61–69. MR

[Friedlander and Iwaniec 2005] J. B. Friedlander and H. Iwaniec, “The illusory sieve”, *Int. J. Number Theory* **1**:4 (2005), 459–494. MR

[Friedlander and Iwaniec 2010] J. Friedlander and H. Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications **57**, American Mathematical Society, Providence, RI, 2010. MR Zbl

[Friedlander and Iwaniec 2021] J. Friedlander and H. Iwaniec, “Note on a note of Goldston and Suriajaya”, preprint, 2021. arXiv 2105.09038

[Friedlander et al. 2022] J. B. Friedlander, D. A. Goldston, H. Iwaniec, and A. I. Suriajaya, “Exceptional zeros and the Goldbach problem”, *J. Number Theory* **233** (2022), 78–86. MR

[Goldston and Suriajaya 2021] D. A. Goldston and A. I. Suriajaya, “Note on the Goldbach conjecture and Landau–Siegel zeros”, preprint, 2021. arXiv 2104.09407v1

[Granville 2020] A. Granville, “Sieving intervals and Siegel zeros”, preprint, 2020. arXiv 2010.01211

[Hardy and Littlewood 1923] G. H. Hardy and J. E. Littlewood, “Some problems of ‘Partitio numerorum’; III: On the expression of a number as a sum of primes”, *Acta Math.* **44**:1 (1923), 1–70. MR Zbl

[Heath-Brown 1983] D. R. Heath-Brown, “Prime twins and Siegel zeros”, *Proc. London Math. Soc.* (3) **47**:2 (1983), 193–224. 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

[Jia 2022] C. H. Jia, “On the conditional bounds for Siegel zeros”, *Acta Math. Sin.* (*Engl. Ser.*) **38**:5 (2022), 869–876. MR Zbl

[Jurkat and Richert 1965] W. B. Jurkat and H.-E. Richert, “An improvement of Selberg’s sieve method, I”, *Acta Arith.* **11** (1965), 217–240. MR Zbl

[Merikoski 2021] J. Merikoski, “Exceptional characters and prime numbers in sparse sets”, preprint, 2021. arXiv 2108.01355

[Siebert 1983] H. Siebert, “Sieve methods and Siegel’s zeros”, pp. 659–668 in *Studies in pure mathematics*, edited by P. Erdős, Birkhäuser, Basel, 1983. MR Zbl

[Zhang 2014] Y. Zhang, “Bounded gaps between primes”, *Ann. of Math.* (2) **179**:3 (2014), 1121–1174. MR Zbl

Received 24 Aug 2021. Revised 22 Dec 2021.

JOHN B. FRIEDLANDER:

frdlndr@math.toronto.edu
Department of Mathematics, University of Toronto, Toronto, ON, Canada

HENRYK IWANIEC:

iwaniec@comcast.net
Department of Mathematics, Rutgers University, Piscataway, NJ, United States

Essential Number Theory
Vol. 1, No. 1, 2022
https://doi.org/10.2140/ent.2022.1.41

A note on Tate's conjectures for abelian varieties

Chao Li and Wei Zhang

In this mostly expository note, we explain a proof of Tate's two conjectures for algebraic cycles of arbitrary codimension on certain products of elliptic curves and abelian surfaces over number fields.

1. Statement

Let X be a smooth projective variety over a finitely generated field F. Let $\mathrm{Ch}^r(X)$ be the Chow group of codimension r algebraic cycles of X defined over F modulo rational equivalence. Let $\bar{F}$ be a separable algebraic closure of F and $\Gamma_F := \mathrm{Gal}(\bar{F}/F)$. Tate [1965, Conjecture 1] made the following far-reaching conjecture (often known as *the Tate conjecture*), relating algebraic cycles and Γ_F-invariants of the ℓ-adic cohomology of X.

Conjecture 1.1 (Tate I). *For any $1 \le r \le \dim X$ and for any prime $\ell \ne \mathrm{char}(F)$, the ℓ-adic cycle class map*

$$\mathrm{Ch}^r(X) \otimes \mathbb{Q}_\ell \to \mathrm{H}^{2r}(X_{\bar{F}}, \mathbb{Q}_\ell(r))^{\Gamma_F}$$

is surjective.

Let $\mathrm{Ch}^r_{\mathrm{hom}}(X)$ be the quotient group of $\mathrm{Ch}^r(X)$ modulo ℓ-adic homological equivalence. It is further conjectured (and known when $\mathrm{char}(F) = 0$) that $\mathrm{Ch}^r_{\mathrm{hom}}(X)$ is independent of ℓ, and the ℓ-adic cycle class map is injective on $\mathrm{Ch}^r_{\mathrm{hom}}(X) \otimes \mathbb{Q}_\ell$; see [Tate 1965, page 97]. In particular, when $\mathrm{char}(F) = 0$, Tate I implies an isomorphism $\mathrm{Ch}^r_{\mathrm{hom}}(X) \otimes \mathbb{Q}_\ell \simeq \mathrm{H}^{2r}(X_{\bar{F}}, \mathbb{Q}_\ell(r))^{\Gamma_F}$ and thus

$$\mathrm{rank}\, \mathrm{Ch}^r_{\mathrm{hom}}(X) = \dim \mathrm{H}^{2r}(X_{\bar{F}}, \mathbb{Q}_\ell(r))^{\Gamma_F} \tag{1.1.1}$$

for any prime ℓ.

Tate [1965, Conjecture 2] further made a conjecture relating algebraic cycles to poles of zeta functions (often known as *the strong Tate conjecture*). When F is a number field, we denote by $L(\mathrm{H}^{2r}(X)(r), s)$ the (incomplete) L-function associated to the compatible system $\{\mathrm{H}^{2r}(X_{\bar{F}}, \overline{\mathbb{Q}}_\ell(r))\}$ of Γ_F-representations, which

MSC2020: primary 11G40, 14G10; secondary 11G10, 14C25.
Keywords: Tate conjecture, abelian varieties, algebraic cycles, poles of zeta functions, potential automorphy.

converges absolutely for $\Re(s) > 1$. Then Conjecture 2 of [Tate 1965] specializes to the following.

Conjecture 1.2 (Tate II). *Assume that F is a number field. Then for any $1 \leq r \leq \dim X$,*

$$\operatorname{rank} \mathrm{Ch}^r_{\mathrm{hom}}(X) = -\operatorname{ord}_{s=1} L(\mathrm{H}^{2r}(X)(r), s).$$

Tate I for divisors ($r = 1$) is known for various X, including abelian varieties over any finitely generated fields [Faltings 1983; Zarhin 1975; Tate 1966]. Much less is known when $r > 1$. We refer to the surveys [Totaro 2017; Milne 2007; Tate 1994; Ramakrishnan 1989] for a nice summary of known results. The goal of this short note is to present some examples of abelian varieties X over number fields for which Tate's conjectures hold for algebraic cycles in *arbitrary* codimension r.

Theorem 1.3 (Tate I). *Assume that F is finitely generated with* $\mathrm{char}(F) = 0$. *Then Tate I holds for any abelian variety X over F with simple factors all having dimension ≤ 2.*

Theorem 1.4 (Tate II). *Assume that F is a number field. Let E_1, E_2, E_3, E_4 be elliptic curves over F. Let A be an abelian surface over F. Then Tate II holds for the following cases*:

(i) *F is totally real or imaginary CM and $X = E_1^{n_1} \times E_2^{n_2}$ for any $n_1 \geq 1, n_2 \geq 0$.*

(ii) *F is totally real or imaginary CM and $X = E_1^{n_1} \times E_2^{n_2} \times E_3$ for any $n_1 \geq 1$ and $1 \leq n_2 \leq 2$.*

(iii) *F is totally real or imaginary CM and $X = E_1^{n_1} \times E_2^{n_2} \times E_3 \times E_4$ for any $1 \leq n_1, n_2 \leq 2$.*

(iv) *F is totally real and $X = A$, $X = A^2$.*

Remark 1.5. It is worth mentioning that the special case when $X = E^n$ is a power of an elliptic curve was considered by Tate himself [Tate 1965, page 106], and played an important role in his formulation of the Sato–Tate conjecture.

Theorem 1.3 (Tate I) can be deduced from recent theorems on the Hodge conjecture and the Mumford–Tate conjecture [Ramón Marí 2008; Lombardo 2016], as mentioned, e.g., in [Moonen 2017, page 284]. Theorem 1.4 (Tate II) can be deduced from more recent potential automorphy theorems [Allen et al. 2018; Boxer et al. 2021] and known cases of Langlands functionality, and should also be known to the experts. All these ingredients are available in more generality, but to illustrate the ideas we do not aim for maximal generality in the statement of the theorems.

2. Proof of Theorem 1.3 (Tate I)

Choose an embedding $F \hookrightarrow \mathbb{C}$ and view F as a subfield of $\mathbb{C}$. Since all simple factors of X have dimension ≤ 2, the Hodge conjecture for $X_{\mathbb{C}}$ holds (in any codimension r) by [Ramón Marí 2008, Theorem 3.15]. In fact in this case all Hodge classes on $X_{\mathbb{C}}$ are generated by products of divisor classes. Also by [Lombardo 2016, Corollary 1.2], the Mumford–Tate conjecture for X holds.

Now the desired result follows due to the well-known general fact (see, e.g., [Farfán 2016, Section 6]) that the Mumford–Tate conjecture for the abelian variety X over F together with the Hodge conjecture for $X_{\mathbb{C}}$ (in codimension r) implies Tate I (Conjecture 1.1) for X (in codimension r). In particular all Tate classes on X are also generated by products of divisor classes.

Remark 2.1. We refer to [Ramón Marí 2008; Lombardo 2016] for discussions about related previous works on the Hodge and Mumford–Tate conjectures. When X is a product of elliptic curves, the Hodge conjecture was proved in [Murty 1990] (see also [Gordon 1999, Appendix B, Section 3]) and the same method should also apply to prove Tate I.

3. Potential automorphy

Let F be a number field. Let $V = \{V_\ell\}$ and $W = \{W_\ell\}$ be compatible systems of semisimple ℓ-adic Γ_F-representations (e.g., in the sense of strictly compatible systems of ℓ-adic representations of Γ_F defined over $\mathbb{Q}$ of [Boxer et al. 2021, Section 2.8]). Recall that V is *potentially automorphic* if there exists a finite Galois extension L/F such that the restriction $V|_{\Gamma_L}$ is automorphic (e.g., in the sense of [Boxer et al. 2021, Definition 9.1.1]). We introduce the following variants of potential automorphy.

Definition 3.1. Let S be a nonempty set of rational primes. Let L/F be a finite Galois extension.

We say that V is *S-strongly automorphic over L*, if for any subextension L'/F of L/F with L/L' solvable, the following conditions are satisfied:

(i) $V|_{\Gamma_{L'}}$ is automorphic.

(ii) Let π be an isobaric automorphic representation on $\mathrm{GL}_n(\mathbb{A}_{L'})$ associated to $V|_{\Gamma_{L'}}$ ($n = \dim V$ and $\mathbb{A}_{L'}$ is the ring of adèles of L'). Write $\pi = \boxplus_{i=1}^k \pi_i$ as an isobaric direct sum of cuspidal automorphic representations on $\mathrm{GL}_{n_i}(\mathbb{A}_{L'})$ $\big(n = \sum_{i=1}^k n_i\big)$. Write $V|_{\Gamma_{L'}} = \oplus_{i=1}^k V_i$ as the corresponding direct sum decomposition into compatible systems of $\Gamma_{L'}$-representations. Then the ℓ-adic $\Gamma_{L'}$-representation $V_{i,\ell}$ ($i = 1, \dots, k$) is irreducible for any $\ell \in S$. (Notice that the irreducibility of $V_{i,\ell}$ is conjectured but not known in general).

We say that V is *S-strongly potentially automorphic*, if V is S-strongly automorphic over L for some finite Galois extension L/F. We say that V is *strongly potentially automorphic*, if V is S-strongly potentially automorphic for some Dirichlet density one set S.

We say that V and W are *jointly S-strongly potentially automorphic*, if V and W are both S-strongly automorphic over L for some finite Galois extension L/F. We say that V and W are *jointly strongly potentially automorphic*, if V and W are jointly S-strongly potentially automorphic for some Dirichlet density one set S.

Lemma 3.2. *Let $V = \{V_\ell\}$ and $W = \{W_\ell\}$ be compatible systems of semisimple ℓ-adic Γ_F-representations. Let S be a nonempty set of rational primes*:

(i) *Assume that V is S-strongly potentially automorphic. Then $L(V, s)$ has meromorphic continuation to all of $\mathbb{C}$, and for any $\ell \in S$,*

$$\dim V_\ell^{\Gamma_F} = -\operatorname{ord}_{s=1} L(V, s).$$

(ii) *Assume that V and W are jointly S-strongly potentially automorphic. Then $L(V \otimes W, s)$ has meromorphic continuation to all of $\mathbb{C}$, and for any $\ell \in S$,*

$$\dim (V_\ell \otimes W_\ell)^{\Gamma_F} = -\operatorname{ord}_{s=1} L(V \otimes W, s).$$

(iii) *Assume that V has a finite direct sum decomposition $V \simeq \oplus_{i=1}^k V_i \otimes W_i$ into tensor products of compatible systems of Γ_F-representations. Assume that V_i and W_i are jointly S-strongly potentially automorphic for each i. Then $L(V, s)$ has meromorphic continuation to all of $\mathbb{C}$, and for any $\ell \in S$,*

$$\dim V_\ell^{\Gamma_F} = -\operatorname{ord}_{s=1} L(V, s).$$

Remark 3.3. Lemma 3.2 should be known to the experts and the proof idea, using Brauer's induction theorem and known properties of automorphic L-functions, is an old one; see, e.g., [Taylor 2002; Harris et al. 2010; Harris 2009]. Notice that (i) also follows as a special case of (iii). We keep (i) to illustrate the ideas.

Proof. (i) Let L/F be a finite Galois extension such that V is S-strongly automorphic over L. By Brauer's induction theorem, we may find a virtual decomposition

$$\mathbf{1}_{\Gamma_F} = \sum_{j=1}^{k} c_j \operatorname{Ind}_{\Gamma_{L_j}}^{\Gamma_F} \psi_i,$$

where $c_j \in \mathbb{Z}$, $F \subseteq L_j \subseteq L$ with L/L_j solvable, and ψ_j is a 1-dimensional representation of $\mathrm{Gal}(L/L_j)$ $(j = 1, \dots, k)$. Since V is S-strongly automorphic over L, we know that for each j there exists an isobaric direct sum of cuspidal automorphic representations $\pi_{L_j} = \boxplus_{i=1}^{m_i} \pi_{L_j,i}$ of $\mathrm{GL}_n(\mathbb{A}_{L_j})$ and a direct sum decomposition

$V|_{\Gamma_{L_j}} = \oplus_{i=1}^{m_j} V_{L_j,i}$ into Γ_{L_j}-representations such that

$$L(V|_{\Gamma_{L_j}}, s) = L(s, \pi_{L_j}) \quad L(V_{L_j,i}, s) = L(s, \pi_{L_j,i}),$$

and each ℓ-adic representation $V_{L_j,i,\ell}$ is irreducible for any $\ell \in S$. Here $L(s, \pi_{L_j})$ is the (incomplete) standard L-function as in [Godement and Jacquet 1972] and has meromorphic continuation to all of $\mathbb{C}$. Hence

$$L(V \otimes \mathrm{Ind}_{\Gamma_{L_j}}^{\Gamma_F} \psi_j, s) = L(V|_{\Gamma_{L_j}} \otimes \psi_j, s) = \prod_{i=1}^{m_j} L(V_{L_j,i} \otimes \psi_j, s) = \prod_{i=1}^{m_j} L(s, \pi_{L_j,i} \otimes \chi_j),$$

where χ_j is the automorphic character on $\mathrm{GL}_1(\mathbb{A}_{L_j})$ associated to ψ_j. It follows that

$$L(V, s) = L(V \otimes \mathbf{1}_{\Gamma_F}, s) = \prod_{j=1}^{k} \prod_{i=1}^{m_j} L(s, \pi_{L_j,i} \otimes \chi_j)^{c_j}$$

and thus $L(V, s)$ has meromorphic continuation to all of $\mathbb{C}$.

Since $\pi_{L_j,i} \otimes \chi_j$ is cuspidal, by [Jacquet and Shalika 1976] we know that $L(s, \pi_{L_j,i} \otimes \chi_j)$ has no zero or pole at $s = 1$, unless $\pi_{L_j,i} \otimes \chi_j$ is the trivial representation in which case it has a simple pole at $s = 1$. Hence $-\mathrm{ord}_{s=1} L(V, s)$ equals the number of trivial representations among $\pi_{L_j,i} \otimes \chi_j$ weighted by c_j, and so we obtain

$$-\mathrm{ord}_{s=1} L(V, s) = \sum_{j=1}^{k} \sum_{i=1}^{m_j} c_j \dim \mathrm{Hom}_{\Gamma_{L_j}}(\mathbf{1}_{\Gamma_{L_j}}, V_{L_j,i,\ell} \otimes \psi_{j,\ell}),$$

for any $\ell \in S$ by the irreducibility of $V_{L_j,i,\ell}$. This evaluates to

$$\sum_{j=1}^{k} c_j \dim \mathrm{Hom}_{\Gamma_{L_j}}(\mathbf{1}_{\Gamma_{L_j}}, V_\ell|_{\Gamma_{L_j}} \otimes \psi_{j,\ell}),$$

which by the Frobenius reciprocity equals

$$\dim \mathrm{Hom}_{\Gamma_F}(\mathbf{1}_{\Gamma_F}, V_\ell) = \dim V_\ell^{\Gamma_F}.$$

(ii) Let L/F be a finite Galois extension such that both V and W are S-strongly automorphic over L. By the same notation and argument in the proof of (i), we know that for each j there exists an isobaric direct sum of cuspidal representations $\pi_{L_j} = \boxplus_{i=1}^{m_j} \pi_{L_j,i}$ (resp. $\Pi_{L_j} = \boxplus_{i'=1}^{m'_j} \Pi_{L_j,i'}$), together with a corresponding decomposition into Γ_{L_j}-representations $V|_{\Gamma_{L_j}} \simeq \oplus_{i=1}^{m_j} V_{L_j,i}$ $\big($resp. $W|_{\Gamma_{L_j}} \simeq \bigoplus_{i'=1}^{m'_j} W_{L_j,i'}\big)$ such that each ℓ-adic representation $V_{L_j,i,\ell}$ (resp. $W_{L_j,i',\ell}$) is irreducible for any $\ell \in S$.

It follows that

$$L(V\otimes W,s)=\prod_{j=1}^{k}L(V\otimes W\otimes\mathbf{1}_{\Gamma_F},s)=\prod_{j=1}^{k}\prod_{i=1}^{m_j}\prod_{i'=1}^{m'_j}L(s,\pi_{L_j,i}\times(\Pi_{L_j,i'}\otimes\chi_j))^{c_j},$$

where $L(s,\pi_{L_j,i}\times(\Pi_{L_j,i'}\otimes\chi_j))$ is the (incomplete) Rankin–Selberg L-function as in [Jacquet et al. 1983], and thus $L(V\otimes W,s)$ has meromorphic continuation to all of $\mathbb{C}$.

Since $\pi_{L_j,i}$ and $\Pi_{L_j,i}\otimes\chi_j$ are cuspidal, we know that $L(s,\pi_{L_j,i}\times(\Pi_{L_j,i}\otimes\chi_j))$ has no zero at $s=1$ by [Shahidi 1980]; see also [Moreno 1985, Lemma 3.1; Sarnak 2004, page 721]. Also by [Jacquet and Shalika 1981, (4.6) and (4.11)] (see also [Mœglin and Waldspurger 1989, Appendice; Cogdell and Piatetski-Shapiro 2004, Theorem 2.4]), it has no pole at $s=1$, unless $\pi_{L_j,i}\simeq(\Pi_{L_j,i'}\otimes\chi_j)^\vee$ in which case it has a simple pole at $s=1$. The latter happens if and only if $V_{L_j,i}\simeq(W_{L_j,i'}\otimes\psi_j)^\vee$. Hence

$$-\operatorname{ord}_{s=1}L(V,s)=\sum_{j=1}^{k}\sum_{i=1}^{m_j}\sum_{i'=1}^{m'_j}c_j\dim\operatorname{Hom}_{\Gamma_{L_j}}(\mathbf{1}_{\Gamma_{L_j}},V_{L_j,i,\ell}\otimes W_{L_j,i',\ell}\otimes\psi_{j,\ell})$$

for any $\ell\in S$ by the irreducibility of $V_{L_j,i,\ell}$ and $W_{L_j,i',\ell}$. This evaluates to

$$\sum_{j=1}^{k}c_j\dim\operatorname{Hom}_{\Gamma_{L_j}}(\mathbf{1}_{\Gamma_{L_j}},(V_\ell\otimes W_\ell)|_{\Gamma_{L_j}}\otimes\psi_{j,\ell}),$$

which by the Frobenius reciprocity equals

$$\dim\operatorname{Hom}_{\Gamma_F}(\mathbf{1}_{\Gamma_F},V_\ell\otimes W_\ell)=\dim(V_\ell\otimes W_\ell)^{\Gamma_F}.$$

(iii) It follows directly from (ii) and the factorization $L(V,s)=\prod_{i=1}^{k}L(V_i\otimes W_i,s)$. □

Lemma 3.4. *Assume that F is a number field. Let E_1, E_2, E_3, E_4 be elliptic curves over F. Let A be an abelian surface over F:*

(i) *If F is totally real or imaginary CM, then $\{\operatorname{Sym}^{k_1}\mathrm{H}^1(E_{1,\overline{F}},\overline{\mathbb{Q}}_\ell)\}$ and $\{\operatorname{Sym}^{k_2}\mathrm{H}^1(E_{2,\overline{F}},\overline{\mathbb{Q}}_\ell)\}$ are jointly strongly potentially automorphic for any $k_1,k_2\geq 0$.*

(ii) *If F is totally real or imaginary CM, then $\{\operatorname{Sym}^{k_1}\mathrm{H}^1(E_{1,\overline{F}},\overline{\mathbb{Q}}_\ell)\}$ and $\{\operatorname{Sym}^{k_2}\mathrm{H}^1(E_{2,\overline{F}},\overline{\mathbb{Q}}_\ell)\otimes\operatorname{Sym}^{k_3}\mathrm{H}^1(E_{3,\overline{F}},\overline{\mathbb{Q}}_\ell)\}$ are jointly strongly potentially automorphic for any $k_1\geq 0$, $0\leq k_2\leq 2$, and $0\leq k_3\leq 1$.*

(iii) *If F is totally real or imaginary CM, then*

$$\{\operatorname{Sym}^{k_1}\mathrm{H}^1(E_{1,\overline{F}},\overline{\mathbb{Q}}_\ell)\otimes\operatorname{Sym}^{k_3}\mathrm{H}^1(E_{3,\overline{F}},\overline{\mathbb{Q}}_\ell)\}$$

and

$$\{\mathrm{Sym}^{k_2}\,\mathrm{H}^1(E_{2,\bar{F}},\overline{\mathbb{Q}}_\ell)\otimes\mathrm{Sym}^{k_4}\,\mathrm{H}^1(E_{4,\bar{F}},\overline{\mathbb{Q}}_\ell)\}$$

are jointly strongly potentially automorphic for any $0\le k_1,k_2\le 2$ *and* $0\le k_3,k_4\le 1$.

(iv) *If F is totally real, then* $\{\mathrm{H}^{k_1}(A_{\bar{F}},\overline{\mathbb{Q}}_\ell)\}$ *and* $\{\mathrm{H}^{k_2}(A_{\bar{F}},\overline{\mathbb{Q}}_\ell)\}$ *are jointly strongly potentially automorphic for any* $0\le k_1,k_2\le 4$.

Proof. (i) If one of E_1 or E_2 has CM, say E_1 has CM, then $\{\mathrm{Sym}^{k_1}\,\mathrm{H}^1(E_{1,\bar{F}},\overline{\mathbb{Q}}_\ell)\}$ is automorphic, as an isobaric direct sum of automorphic characters on $\mathrm{GL}_1(\mathbb{A}_F)$, and possibly automorphic inductions of automorphic characters on $\mathrm{GL}_1(\mathbb{A}_K)$ for a quadratic extension K/F. In particular, we know that $\{\mathrm{Sym}^{k_1}\,\mathrm{H}^1(E_{1,\bar{F}},\overline{\mathbb{Q}}_\ell)\}|_{\Gamma_L}$ is S-strongly automorphic over any finite Galois extension L/F and any nonempty set S of primes. The result follows if E_2 also has CM. If E_2 has no CM, then $\{\mathrm{H}^1(E_{2,\bar{F}},\overline{\mathbb{Q}}_\ell)\}$ is strongly irreducible in the sense defined before [Allen et al. 2018, Lemma 7.1.1] (i.e., for any finite extension F'/F, the representation $\mathrm{H}^1(E_{2,\bar{F}},\overline{\mathbb{Q}}_\ell)|_{\Gamma_{F'}}$ is irreducible for ℓ in a Dirichlet density one set of primes), and we can apply [loc. cit., Corollary 7.1.11] to $\{\mathrm{Sym}^{k_2}\,\mathrm{H}^1(E_{2,\bar{F}},\overline{\mathbb{Q}}_\ell)\}$ together with [loc. cit., Proposition 6.5.13] to obtain the desired joint S-strong potential automorphy for a Dirichlet density one set S of primes. If neither of E_1 and E_2 has CM, then the desired result follows from the more general [loc. cit., Theorem 7.1.10] together with [loc. cit., Proposition 6.5.13]. (In the case $F=\mathbb{Q}$, we may also directly apply [Newton and Thorne 2021, Theorem A (non-CM case) and Theorem A.1 (CM case)]).

(ii) By the same argument in (i), there are a finite Galois extension L/F and a Dirichlet density one set S of primes such that $\{\mathrm{Sym}^{k_i}\,\mathrm{H}^1(E_{i,\bar{F}},\overline{\mathbb{Q}}_\ell)\}$ is S-strongly automorphic over L for any $1\le i\le 3$. Hence by the functorial products for $\mathrm{GL}(2)\times\mathrm{GL}(2)\to\mathrm{GL}(4)$ [Ramakrishnan 2000, Theorem M] and $\mathrm{GL}(2)\times\mathrm{GL}(3)\to\mathrm{GL}(6)$ [Kim and Shahidi 2002, Theorem A], we know that $\{\mathrm{Sym}^{k_2}\,\mathrm{H}^1(E_{2,\bar{F}},\overline{\mathbb{Q}}_\ell)\otimes\mathrm{Sym}^{k_3}\,\mathrm{H}^1(E_{3,\bar{F}},\overline{\mathbb{Q}}_\ell)\}$ is also S-strongly automorphic over L for any $0\le k_2\le 2$ and $0\le k_3\le 1$. The result then follows.

(iii) By the same argument in (ii), there are a finite Galois extension L/F and a Dirichlet density one set S of primes such that $\{\mathrm{Sym}^{k_i}\,\mathrm{H}^1(E_{i,\bar{F}},\overline{\mathbb{Q}}_\ell)\otimes\mathrm{Sym}^{k_j}\,\mathrm{H}^1(E_{j,\bar{F}},\overline{\mathbb{Q}}_\ell)\}$ is S-strongly automorphic over L for any $0\le k_i\le 2$ and $0\le k_j\le 1$, which gives the result.

(iv) The result follows from [Boxer et al. 2021, Theorem 9.3.1] and its proof. □

Remark 3.5. For each item of Lemma 3.4, the proof supplies a Dirichlet density one set S of primes such that the joint S-strong potential automorphy holds. Since compatible systems in Lemma 3.4 come from elliptic curves and abelian surfaces, one should also be able to prove directly that the irreducible conditions required in Definition 3.1(ii) hold for all primes ℓ, and hence the joint S-strong potential automorphy holds for the set S of all primes. For the purpose of the proof of Theorem 1.4 (Tate II) below, any nonempty S suffices.

4. Proof of Theorem 1.4 (Tate II)

Let $1 \le r \le \dim X$. Let $V = \{\mathrm{H}^{2r}(X_{\overline{F}}, \overline{\mathbb{Q}}_\ell(r))\}$. By Theorem 1.3 (Tate I), we know from (1.1.1) that $\operatorname{rank}\mathrm{Ch}^r_{\mathrm{hom}}(X) = \dim V_\ell^{\Gamma_F}$ for any prime ℓ. Thus it remains to show that $\dim V_\ell^{\Gamma_F} = -\operatorname{ord}_{s=1} L(V, s)$ for some prime ℓ:

(i) By the Künneth formula and the decomposition of $\mathrm{H}^1(E_{i,\overline{F}}, \overline{\mathbb{Q}}_\ell)^{\otimes k_i}$ into symmetric powers of $\mathrm{H}^1(E_{i,\overline{F}}, \overline{\mathbb{Q}}_\ell)$ ($i = 1, 2$), we have an isomorphism of semisimple Γ_F-representations

$$\begin{aligned}&\mathrm{H}^{2r}(X_{\overline{F}}, \overline{\mathbb{Q}}_\ell(r)) \\ &\qquad \simeq \bigoplus_{\substack{0\le k_i\le n_i\\ i=1,2}} m_{k_1,k_2}(\mathrm{Sym}^{k_1}\mathrm{H}^1(E_{1,\overline{F}}, \overline{\mathbb{Q}}_\ell)\otimes \mathrm{Sym}^{k_2}\mathrm{H}^1(E_{2,\overline{F}}, \overline{\mathbb{Q}}_\ell))\tfrac{1}{2}(k_1+k_2),\end{aligned}$$

where $m_{k_1,k_2} \ge 0$ are certain multiplicities (nonzero only if $k_1 + k_2 \le 2r$ is even). The result then follows from Lemma 3.2 (iii) and Lemma 3.4 (i).

(ii) Similarly, if we set $n_3 = 1$ then we have an isomorphism of semisimple Γ_F-representations

$$\mathrm{H}^{2r}(X_{\overline{F}}, \overline{\mathbb{Q}}_\ell(r)) \simeq \bigoplus_{\substack{0\le k_i\le n_i\\ 1\le i\le 3}} m_{k_1,k_2,k_3}(\otimes_{1\le i\le 3}\mathrm{Sym}^{k_i}\mathrm{H}^1(E_{i,\overline{F}}, \overline{\mathbb{Q}}_\ell))\tfrac{1}{2}(k_1+k_2+k_3),$$

where $m_{k_1,k_2,k_3} \ge 0$ are certain multiplicities (nonzero only if $k_1 + k_2 + k_3 \le 2r$ is even). The result then follows from Lemma 3.2(iii) and Lemma 3.4(ii).

(iii) Similarly, the result follows from Lemma 3.2(iii) and Lemma 3.4(iii).

(iv) For $X = A$, the result follows from Lemma 3.2(i) and Lemma 3.4(iv). For $X = A^2$, by the Künneth formula, we have an isomorphism of semisimple Γ_F-representations

$$\mathrm{H}^{2r}(X_{\overline{F}}, \overline{\mathbb{Q}}_\ell(r)) \simeq \bigoplus_{\substack{k_1+k_2=2r\\ 0\le k_1,k_2\le 4}} (\mathrm{H}^{k_1}(A_{\overline{F}}, \overline{\mathbb{Q}}_\ell)\otimes \mathrm{H}^{k_2}(A_{\overline{F}}, \overline{\mathbb{Q}}_\ell))(r).$$

The result then follows from Lemma 3.2(iii) and Lemma 3.4(iv).

Remark 4.1. When X is an abelian surface of the type $\mathrm{Res}_{K/F} E$, where F is totally real, K/F is a quadratic CM extension and E is an elliptic curve over K, Tate II was proved in [Virdol 2015] using a similar argument. We also refer to [Johansson 2017; Taylor 2020] for more detailed analysis for L-functions of abelian surfaces.

Acknowledgments

The authors are grateful to G. Boxer, F. Calegari, T. Gee and the anonymous referee for helpful comments. C. L. was partially supported by the NSF grant DMS-2101157. W. Z. was partially supported by the NSF grant DMS-1901642.

References

[Allen et al. 2018] P. B. Allen, F. Calegari, A. Caraiani, T. Gee, D. Helm, B. V. L. Hung, J. Newton, P. Scholze, R. Taylor, and J. A. Thorne, "Potential automorphy over CM fields", preprint, 2018. arXiv 1812.09999

[Boxer et al. 2021] G. Boxer, F. Calegari, T. Gee, and V. Pilloni, "Abelian surfaces over totally real fields are potentially modular", *Publ. Math. Inst. Hautes Études Sci.* **134** (2021), 153–501. MR Zbl

[Cogdell and Piatetski-Shapiro 2004] J. W. Cogdell and I. I. Piatetski-Shapiro, "Remarks on Rankin–Selberg convolutions", pp. 255–278 in *Contributions to automorphic forms*, *geometry*, *and number theory*, edited by H. Hida et al., Johns Hopkins Univ. Press, Baltimore, MD, 2004. MR Zbl

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR Zbl

[Farfán 2016] V. C. Farfán, "A survey around the Hodge, Tate and Mumford–Tate conjectures for abelian varieties", preprint, 2016. arXiv 1602.08354

[Godement and Jacquet 1972] R. Godement and H. Jacquet, *Zeta functions of simple algebras*, Lecture Notes in Mathematics **260**, Springer, 1972. MR Zbl

[Gordon 1999] B. B. Gordon, *A survey of the Hodge conjecture for abelian varieties*, American Mathematical Society, Providence, RI, 1999. Appendix B to J. D. Lewis, , "A survey of the Hodge conjecture", *CRM Monograph Series* **10** (1999), xvi+368. MR

[Harris 2009] M. Harris, "Potential automorphy of odd-dimensional symmetric powers of elliptic curves and applications", pp. 1–21 in *Algebra*, *arithmetic*, *and geometry*: *in honor of Yu. I. Manin*, vol. II, edited by Y. Tschinkel and Y. Zarhin, Progr. Math. **270**, Birkhäuser, Boston, 2009. MR Zbl

[Harris et al. 2010] M. Harris, N. Shepherd-Barron, and R. Taylor, "A family of Calabi–Yau varieties and potential automorphy", *Ann. of Math.* (2) **171**:2 (2010), 779–813. MR Zbl

[Jacquet and Shalika 1976] H. Jacquet and J. A. Shalika, "A non-vanishing theorem for zeta functions of GL_n", *Invent. Math.* **38**:1 (1976), 1–16. MR Zbl

[Jacquet and Shalika 1981] H. Jacquet and J. A. Shalika, "On Euler products and the classification of automorphic representations, I", *Amer. J. Math.* **103**:3 (1981), 499–558. MR Zbl

[Jacquet et al. 1983] H. Jacquet, I. I. Piatetskii-Shapiro, and J. A. Shalika, "Rankin–Selberg convolutions", *Amer. J. Math.* **105**:2 (1983), 367–464. MR Zbl

[Johansson 2017] C. Johansson, "On the Sato–Tate conjecture for non-generic abelian surfaces", *Trans. Amer. Math. Soc.* **369**:9 (2017), 6303–6325. MR Zbl

[Kim and Shahidi 2002] H. H. Kim and F. Shahidi, "Functorial products for $\mathrm{GL}_2 \times \mathrm{GL}_3$ and the symmetric cube for GL_2", *Ann. of Math.* (2) **155**:3 (2002), 837–893. MR Zbl

[Lombardo 2016] D. Lombardo, "On the ℓ-adic Galois representations attached to nonsimple abelian varieties", *Ann. Inst. Fourier* (*Grenoble*) **66**:3 (2016), 1217–1245. MR Zbl

[Milne 2007] J. S. Milne, "The Tate conjecture over finite fields (AIM talk)", 2007. arXiv 0709.3040

[Mœglin and Waldspurger 1989] C. Mœglin and J.-L. Waldspurger, "Le spectre résiduel de $\mathrm{GL}(n)$", *Ann. Sci. École Norm. Sup.* (4) **22**:4 (1989), 605–674. MR

[Moonen 2017] B. Moonen, "Families of motives and the Mumford–Tate conjecture", *Milan J. Math.* **85**:2 (2017), 257–307. MR Zbl

[Moreno 1985] C. J. Moreno, "Analytic proof of the strong multiplicity one theorem", *Amer. J. Math.* **107**:1 (1985), 163–206. MR Zbl

[Murty 1990] V. K. Murty, "Computing the Hodge group of an abelian variety", pp. 141–158 in *Séminaire de Théorie des Nombres*, *Paris* 1988–1989, edited by C. Goldstein, Progr. Math. **91**, Birkhäuser, Boston, 1990. MR Zbl

[Newton and Thorne 2021] J. Newton and J. A. Thorne, "Symmetric power functoriality for holomorphic modular forms, II", *Publ. Math. Inst. Hautes Études Sci.* **134** (2021), 117–152. MR Zbl

[Ramakrishnan 1989] D. Ramakrishnan, "Regulators, algebraic cycles, and values of L-functions", pp. 183–310 in *Algebraic K-theory and algebraic number theory*, edited by M. R. Stein and R. K. Dennis, Contemp. Math. **83**, Amer. Math. Soc., Providence, RI, 1989. MR Zbl

[Ramakrishnan 2000] D. Ramakrishnan, "Modularity of the Rankin–Selberg L-series, and multiplicity one for SL(2)", *Ann. of Math.* (2) **152**:1 (2000), 45–111. MR Zbl

[Ramón Marí 2008] J. J. Ramón Marí, "On the Hodge conjecture for products of certain surfaces", *Collect. Math.* **59**:1 (2008), 1–26. MR

[Sarnak 2004] P. Sarnak, "Nonvanishing of L-functions on $\mathfrak{R}(s) = 1$", pp. 719–732 in *Contributions to automorphic forms*, *geometry*, *and number theory*, edited by H. Hida et al., Johns Hopkins Univ. Press, Baltimore, MD, 2004. MR Zbl

[Shahidi 1980] F. Shahidi, "On nonvanishing of L-functions", *Bull. Amer. Math. Soc.* (*N.S.*) **2**:3 (1980), 462–464. MR Zbl

[Tate 1965] J. T. Tate, "Algebraic cycles and poles of zeta functions", pp. 93–110 in *Arithmetical algebraic geometry* (Purdue Univ., 1963), edited by O. F. G. Schilling, Harper & Row, New York, 1965. MR Zbl

[Tate 1966] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.* **2** (1966), 134–144. MR Zbl

[Tate 1994] J. Tate, "Conjectures on algebraic cycles in l-adic cohomology", pp. 71–83 in *Motives* (Seattle, WA, 1991), edited by U. Jannsen et al., Proc. Sympos. Pure Math. **55**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Taylor 2002] R. Taylor, "Remarks on a conjecture of Fontaine and Mazur", *J. Inst. Math. Jussieu* **1**:1 (2002), 125–143. MR Zbl

[Taylor 2020] N. Taylor, "Sato–Tate distributions on Abelian surfaces", *Trans. Amer. Math. Soc.* **373**:5 (2020), 3541–3559. MR Zbl

[Totaro 2017] B. Totaro, "Recent progress on the Tate conjecture", *Bull. Amer. Math. Soc.* (*N.S.*) **54**:4 (2017), 575–590. MR Zbl

[Virdol 2015] C. Virdol, "Tate conjecture for some abelian surfaces over totally real or CM number fields", *Funct. Approx. Comment. Math.* **52**:1 (2015), 57–63. MR Zbl

[Zarhin 1975] J. G. Zarhin, "Endomorphisms of Abelian varieties over fields of finite characteristic", *Izv. Akad. Nauk SSSR Ser. Mat.* **39**:2 (1975), 272–277, 471. In Russian; translated in *Math. USSR Isvestija* **9**:2 (1975), 255–260. MR

Received 9 Jan 2022. Revised 9 May 2022.

CHAO LI:
chaoli@math.columbia.edu
Department of Mathematics, Columbia University, New York, NY, United States

WEI ZHANG:
weizhang@mit.edu
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, United States

msp

Essential Number Theory
Vol. 1, No. 1, 2022
https://doi.org/10.2140/ent.2022.1.51

A Diophantine problem about Kummer surfaces

William Duke

Upper and lower bounds are given for the number of rational points of bounded height on a double cover of projective space ramified over a Kummer surface.

1. Introduction

Let $F(x) = F(x_0, \dots, x_n)$ with $n \geq 2$ be an integral form with $\deg F \geq 2$ and set

$$N_F(T) = \#\{x \in \mathbb{Z}^{n+1} \mid F(x) = z^2 \text{ for some } z \in \mathbb{Z}, \gcd(x_0, \dots, x_n) = 1 \text{ and } \|x\| \leq T\}, \tag{1-1}$$

where $\|x\| = \max_j(|x_j|)$. The behavior of $N_F(T)$ for large T is of basic Diophantine interest. When $\deg F$ is even, $N_F(T)$ counts rational points of bounded height on a double cover of $\mathbb{P}^n_{\mathbb{Q}}$ ramified over the hypersurface given by $F(x) = 0$.

Assume that $\deg F$ is even and that $z^2 - F(x)$ is irreducible over $\mathbb{C}$. It follows from Theorem 3 on page 178 of [Serre 1989] that for any $\epsilon > 0$

$$N_F(T) \ll T^{n+1/2+\epsilon}. \tag{1-2}$$

As discussed after Theorem 3 in [Serre 1989], it is reasonable to expect that

$$N_F(T) \ll T^{n+\epsilon}. \tag{1-3}$$

Broberg [2003] improved $\frac{5}{2}$ to $\frac{9}{4}$ in (1-2) when $n = 2$. For $n \geq 3$, various improvements and generalizations of (1-2) are given in [Munshi 2009; Heath-Brown and Pierce 2012; Bonolis 2021], assuming that $F(x) = 0$ is nonsingular. Certain nonhomogeneous F are treated in [Heath-Brown and Pierce 2012].

In this note I will consider the problem of estimating $N_F(T)$ from above *and below* when $n = 3$ for a special class of quartic F, namely those for which $F(x) = 0$ define certain Kummer surfaces. These surfaces have singularities (nodes).

For our purpose we will define a Kummer surface in terms of an integral sextic polynomial $P(t)$. For fixed $a, b, c, d, e, f, g \in \mathbb{Z}$ with $a \neq 0$ let

$$P(t) = at^6 + bt^5 + ct^4 + dt^3 + et^2 + ft + g.$$

Research supported by NSF grant DMS 1701638 and Simons Foundation Award Number 554649.
MSC2020: 11Dxx, 11E76.
Keywords: Diophantine equations, Kummer surfaces, rational points.

Suppose that the discriminant of P is not zero. Define the symmetric matrices

$$S_0 = \begin{pmatrix} a & \frac{b}{2} & 0 & 0 \\ \frac{b}{2} & c & \frac{d}{2} & 0 \\ 0 & \frac{d}{2} & e & \frac{f}{2} \\ 0 & 0 & \frac{f}{2} & g \end{pmatrix} \tag{1-4}$$

and

$$S_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & 0 \\ 0 & -\frac{1}{2} & 0 & 0 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \end{pmatrix}, \quad S_3 = \begin{pmatrix} 0 & 0 & -\frac{1}{2} & 0 \\ 0 & 1 & 0 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{1-5}$$

For $x = (x_0, x_1, x_2, x_3)$ define the matrix

$$S_x = x_0 S_0 + x_1 S_1 + x_2 S_2 + x_3 S_3.$$

For a row vector v let $S(v) = vSv^t$ denote the quadratic form associated to a symmetric matrix S. It is easy to check that *for any x* we have the identity

$$x_0 P(t) = S_x(t^3, t^2, t, 1).$$

Define the associated quartic form F by

$$F(x) := 16 \det S_x. \tag{1-6}$$

Over $\mathbb{C}$ the surface given by $F(x) = 0$ is a Kummer surface, a special determinantal quartic surface that is singular with sixteen nodes, including the points $(t^3, t^2, t, 1)$ where t is a root of $P(t) = 0$. The Jacobian variety of the genus two hyperelliptic curve $y^2 = P(t)$ is a double cover of the Kummer surface ramified over these nodes. For details on the geometry of Kummer surfaces; see, e.g., [Hudson 1990; Dolgachev 2012]. Some arithmetic aspects of Kummer surfaces are considered in [Cassels and Flynn 1996]. The construction of a Kummer surface using the S_j from (1-4) and (1-5) occurs in a slightly different form in [Baker 1907, page 69]; see also [Cassels and Flynn 1996, page 42].

Our main result is the following.

Theorem 1. *Suppose that $P(t) = at^6 + bt^5 + ct^4 + dt^3 + et^2 - 2t$ with integral a, b, c, d, e has nonzero discriminant and $a \neq 0$. Let F be defined in* (1-6) *and $N_F(T)$ in* (1-1). *Then for any $\epsilon > 0$*

$$T^2 \ll N_F(T) \ll T^{3+\epsilon}, \tag{1-7}$$

where the first implied constant depends only on P and the second depends only on P and ϵ.

Our approach to these estimates relies on the special form of the Kummer surfaces we consider. In particular, for the upper bound we use that in P we assume that $g = 0$. For the lower bound we use that $g = 0$ and $f = -2$. The upper bound coincides with that given in (1-3). An example of an equation to which Theorem 1 applies, when $P(t) = t^6 - 2t$, is

$$z^2 = x_3^2(x_1^2 + 8x_0x_2) + x_3(-16x_0^3 - 2x_1x_2^2) - 4x_0x_1^3 - 8x_0^2x_1x_2 + x_2^4.$$

Numerical calculations in this case show that we seem to have $N_F(T) \gg T^{3-\epsilon}$. It would be of interest to find the correct order of magnitude of $N_F(T)$ for some P.

Remark. Most research on $N_F(T)$ in (1-1) has concentrated on giving upper bounds for $N_F(T)$ for quite general F, where $F(x) = 0$ is usually assumed to be nonsingular. The proofs often make use of intricate estimates of character and exponential sums; for example, see [Heath-Brown and Pierce 2012]. In contrast, the proof of the upper bound of (1-7) is rather straightforward. Although it is likely not sharp, the lower bound of (1-7) is probably more interesting and certainly deeper. Its proof uses a remarkable and not well-known identity of Schottky to explicitly produce solutions to $F(x) = z^2$. Along somewhat similar lines, invariant theory was recently applied to asymptotically count integer points on quadratic twists of certain elliptic curves and give a class number formula for binary quartic forms [Duke 2021]. It is reasonable to hope that some other classical identities of algebraic geometry and syzygies of invariant theory, some of which are beautifully presented in [Dolgachev 2012], could have still undiscovered applications to the problem of finding lower bounds for counting functions like $N_F(T)$.

2. Proof of the theorem

Upper bound. The mechanism behind the proof of the upper bound in (1-7) is that a quadratic Diophantine equation in two variables has “few” solutions. The argument relies on the fact that for $P(t)$ of the assumed form (so that in particular $g = 0$), the associated F has the property that it is quadratic in one of its variables. It will become clear that similar arguments can be applied to other F with this property.

For a general $P(t)$ we have the explicit formula

$$\begin{aligned} F(x) = {} & x_0^4(16aceg - 4acf^2 - 4ad^2g - 4b^2eg + b^2f^2) \\ & - 2x_0^3(-8acgx_1 + 2adfx_1 - 4adgx_2 - 8aegx_3 + 2af^2x_3 + 2b^2gx_1 \\ & \qquad + bdfx_2 + 2bdgx_3) \\ & + x_0^2(-4aex_1^2 + 4afx_1x_2 + 16agx_1x_3 - 4agx_2^2 - 4bex_1x_2 - 2bfx_1x_3 \\ & + 2bfx_2^2 + 4bgx_2x_3 - 4cex_2^2 - 4cfx_2x_3 - 4cgx_3^2 + d^2x_2^2) \\ & -2x_0(2ax_1^3 + 2bx_1^2x_2 + 2cx_1x_2^2 + dx_1x_2x_3 + dx_2^3 + 2ex_2^2x_3 + 2fx_2x_3^2 + 2gx_3^3) \\ & + (x_2^2 - x_1x_3)^2. \end{aligned}$$

For $P(t) = at^6 + bt^5 + ct^4 + dt^3 + et^2 - 2t$ we have that F has an expansion that is quadratic in x_3:

$$\begin{aligned}F(x) = x_3^2(x_1^2 + 8x_2x_0) &\\ &+ x_3(-16ax_0^3 + 4bx_0^2x_1 + 8cx_0^2x_2 - 2dx_0x_1x_2 - 4ex_0x_2^2 - 2x_1x_2^2)\\ &+ 4b^2x_0^4 - 16acx_0^4 + 8adx_0^3x_1 - 4aex_0^2x_1^2 - 4ax_0x_1^3 + 4bdx_0^3x_2\\ &- 8ax_0^2x_1x_2 - 4bex_0^2x_1x_2 - 4bx_0x_1^2x_2 - 4bx_0^2x_2^2 + d^2x_0^2x_2^2\\ &- 4cex_0^2x_2^2 - 4cx_0x_1x_2^2 - 2dx_0x_2^3 + x_2^4.\end{aligned} \tag{2-1}$$

Thus given a solution x of $z^2 = F(x)$, upon completing the square we will get a solution (y, z) of

$$y^2 - (x_1^2 + 8x_2x_0)z^2 = k(x_0, x_1, x_2) \tag{2-2}$$

where

$$k(x_0, x_1, x_2) = 8x_0x_2^5 - 64a^2x_0^5 + \cdots$$

is a homogeneous integral form of degree 6 that is not identically zero, and where

$$y = (x_1^2+8x_2x_0)x_3+(8ax_0^3-2bx_0^2x_1-4cx_0^2x_2+dx_0x_1x_2+2ex_0x_2^2+x_1x_2^2). \tag{2-3}$$

The number of x_0, x_1, x_2 with $|x_0|, |x_1|, |x_2| \le T$ where either

$$k(x_0, x_1, x_2) = 0 \quad \text{or} \quad x_1^2 + 8x_2x_0 = 0$$

is $\ll T^2$. For such x_0, x_1, x_2, by (2-2) and (2-3) the total number of solutions of $F(x) = z^2$ with $|x_3| \le T$ is $\ll T^3$.

For any other x_0, x_1, x_2 with $|x_0|, |x_1|, |x_2| \le T$ we can apply the well-known estimate

$$d(k) \ll k^\epsilon$$

for the divisor function and [Hooley 1986, Lemma 1], which follows from [Hooley 1967, Lemma 5], to conclude that the total number of solutions of $F(x) = z^2$ with $|x_1|, |x_2|, |x_3|, |x_0| \le T$ is $\ll T^{3+\epsilon}$.

Lower bound. The tool used to obtain the lower bound of (1-7) is an explicit parametrization of solutions given by an identity of Schottky. This identity has a form that is similar to many of those coming from syzygies connecting covariants and invariants of forms. However, Schottky's identity has a different origin and does not appear to come from invariant theory.

The Jacobian of S_0, S_1, S_2, S_3 as given in (1-4) and (1-5) is

$$J(x) = J_{S_0,S_1,S_2,S_3}(x) = \det\begin{pmatrix}\partial_1 S_0 & \partial_2 S_0 & \partial_3 S_0 & \partial_4 S_0\\ \partial_1 S_1 & \partial_2 S_1 & \partial_3 S_1 & \partial_4 S_1\\ \partial_1 S_2 & \partial_2 S_2 & \partial_3 S_2 & \partial_4 S_2\\ \partial_1 S_3 & \partial_2 S_3 & \partial_3 S_3 & \partial_4 S_3\end{pmatrix} = 2gx_3^3x_0 - 2ax_3x_0^3 + \cdots .$$

In case $f=-2$ and $g=0$ this is given in full by

$$\begin{aligned} J(x)=2(&-ax_3x_0^3+3ax_0^2x_1x_2-2ax_0x_1^3-bx_3x_0^2x_1+bx_0^2x_2^2+bx_0x_1^2x_2-bx_1^4\\ &-cx_3x_0x_1^2+2cx_0x_1x_2^2-cx_1^3x_2-dx_3x_1^3+dx_0x_2^3+ex_3x_0x_2^2\\ &-2ex_3x_1^2x_2+ex_1x_2^3-2x_3^2x_0x_2+2x_3^2x_1^2+2x_3x_1x_2^2-2x_2^4). \end{aligned} \tag{2-4}$$

The surface defined by $J(x)=0$ is a Weddle surface. A variant of the following identity connecting the Weddle and Kummer surfaces, which can be checked directly, is apparently due to Schottky [1889, page 241]. He obtained it via theta functions and used it to show that the Kummer and Weddle surfaces are birationally equivalent over $\mathbb{C}$. It is stated (in a somewhat different form) in [Baker 1907, page 152, Example 8].

Proposition 2. *For F in* (1-6) (*and in* (2-1)) *when $P(t)=at^6+bt^5+ct^4+dt^3+et^2-2t$, we have identically*

$$F(-S_3(x),-2S_2(x),2S_1(x),S_0(x))=J^2(x), \tag{2-5}$$

where $J(x)$ is given in (2-4).

Note the order of the parametrizing quadrics S_j. It is not obvious (to me) how to modify (2-5) so that it holds for a general $P(t)$ or even if that is possible without changing its basic form.

Proof of Theorem 1. Let $\mathcal{S}$ be the set of six points $\alpha_j\in\mathbb{P}^3_{\mathbb{C}}$ represented by $(t_j^3,t_j^2,t_j,1)$, where $P(t_j)=0$ for $j=1,\dots,6$. Recall from the discussion around (1-6) that $S_i(\alpha_j)=0$ for each i,j. In order to apply Proposition 2 to prove the lower bound of (1-7), we must first examine the map

$$\alpha\mapsto(-S_3(\alpha),-2S_2(\alpha),2S_1(\alpha),S_0(\alpha)) \tag{2-6}$$

from $\mathbb{P}^3_{\mathbb{C}}\setminus\mathcal{S}$ to $\mathbb{P}^3_{\mathbb{C}}$. Let V be the space spanned by $\{S_0,S_1,S_2,S_3\}$, which is clearly four dimensional. We need to control the degree of the map (2-6). Suppose that $\beta_1,\beta_2,\beta_3\in\mathbb{P}^3_{\mathbb{C}}\setminus\mathcal{S}$ are distinct and all have the same image in $\mathbb{P}^3_{\mathbb{C}}$ under the map (2-6). Then three independent $S,S',S''\in V$ will vanish at the nine distinct points $\{\alpha_1,\dots,\alpha_6,\beta_1,\beta_2,\beta_3\}$. This is impossible by Bezout's theorem and shows that there are at most two points in $\mathbb{P}^3_{\mathbb{C}}\setminus\mathcal{S}$ with the same image in $\mathbb{P}^3_{\mathbb{C}}$ under the map (2-6).

Therefore by Proposition 2, the lower bound of (1-7) will follow from

$$\#\{x\in\mathbb{Z}^4:\gcd(x_1,x_2,x_3,x_4)=1,\ |S_j(x)|\le T,\ j=1,2,3,4\}\gg T^2.$$

This estimate is easily established since there is a ball in $\mathbb{R}^4$ centered at the origin of positive radius, all of whose points x satisfy $|S_j(x)|\le 1$ for $j=1,2,3,4$. Thus a standard lattice point count gives the result. □

References

[Baker 1907] H. F. Baker, *An introduction to the theory of multiply periodic functions*, Cambridge University Press, 1907. Zbl

[Bonolis 2021] D. Bonolis, "A polynomial sieve and sums of Deligne type", *Int. Math. Res. Not.* **2021**:2 (2021), 1096–1137. MR Zbl

[Broberg 2003] N. Broberg, "Rational points on finite covers of $\mathbb{P}^1$ and $\mathbb{P}^2$", *J. Number Theory* **101**:1 (2003), 195–207. MR Zbl

[Cassels and Flynn 1996] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, 1996. Zbl

[Dolgachev 2012] I. V. Dolgachev, *Classical algebraic geometry*, Cambridge University Press, 2012. MR Zbl

[Duke 2021] W. Duke, "On elliptic curves and binary quartic forms", *International Mathematics Research Notices* (2021).

[Heath-Brown and Pierce 2012] D. R. Heath-Brown and L. B. Pierce, "Counting rational points on smooth cyclic covers", *J. Number Theory* **132**:8 (2012), 1741–1757. MR Zbl

[Hooley 1967] C. Hooley, "On binary cubic forms", *J. Reine Angew. Math.* **226** (1967), 30–87. MR Zbl

[Hooley 1986] C. Hooley, "On binary quartic forms", *J. Reine Angew. Math.* **366** (1986), 32–52. MR Zbl

[Hudson 1990] R. W. H. T. Hudson, *Kummer's quartic surface*, Cambridge University Press, 1990. MR Zbl

[Munshi 2009] R. Munshi, "Density of rational points on cyclic covers of $\mathbb{P}^n$", *J. Théor. Nombres Bordeaux* **21**:2 (2009), 335–341. MR Zbl

[Schottky 1889] F. Schottky, "Ueber die Beziehungen zwischen den sechzehn Thetafunctionen von zwei Variabeln", *J. Reine Angew. Math.* **105** (1889), 233–249. MR Zbl

[Serre 1989] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects Math. **E15**, Vieweg & Sohn, Braunschweig, Germany, 1989. MR Zbl

Received 21 Sep 2021. Revised 9 Dec 2021.

WILLIAM DUKE:

wdduke@ucla.edu
Mathematics Department, UCLA, Los Angeles, CA, United States

Essential Number Theory
Vol. 1, No. 1, 2022
https://doi.org/10.2140/ent.2022.1.57

Quartic index form equations and monogenizations of quartic orders

Shabnam Akhtari

Some upper bounds for the number of monogenizations of quartic orders are established by considering certain classical Diophantine equations, namely index form equations in quartic number fields, and cubic and quartic Thue equations.

1. Introduction

Let K be an algebraic number field and O_K its ring of integers. Let O be an order in K (a subring of O_K with quotient field K). We call the ring O *monogenic* if it is generated by one element as a $\mathbb{Z}$-algebra, i.e., $O = \mathbb{Z}[\alpha]$ for some $\alpha \in O$; the element α is called a *monogenizer* of O. If α is a monogenizer of O, than so is $\pm\alpha + c$ for any $c \in \mathbb{Z}$. We call two monogenizers α and α' of O *equivalent* if $\alpha' = \pm\alpha + c$ for some $c \in \mathbb{Z}$. Then by a *monogenization* of O, we mean an equivalence class of monogenizers of O. By fundamental work of Győry [1976], we know that any order in an algebraic number field can have at most finitely many monogenizations and that effectively computable upper bounds on the number of these monogenizations can be determined. It is a difficult computational problem to find or even count the monogenizations of a given order (many computational examples, interesting special cases and efficient algorithms in low degree number fields may be found in [Gaál 2019]).

We are interested in counting the number of monogenizations of a given order. An overview of various results on estimates for the number of monogenizations of orders in number fields is given in [Evertse 2011]. There are further extensions and generalizations of such results in [Evertse and Győry 2017] (in particular, see the relevant results in Section 9.1).

Monogenicity of algebraic number rings has a long history. It is an interesting problem to decide whether a given number field K is monogenic, that is, whether its ring of integers O_K, which is the maximal order in K, is monogenic. It is well known that quadratic number fields are monogenic. Dedekind [1878] gave the first example of a nonmonogenic cubic field. It is an open conjecture that most of

MSC2020: 11D25, 11D45, 11R04, 11R16.
Keywords: monogenizations of a quartic order, index form equations, Thue equations.

number fields of degree greater than 2 are not monogenic. For recent progress in this direction in the cases of cubic and quartic number fields, we refer the reader to the work of Alpöge, Bhargava, and Shnidman [Alpöge et al. 2021a; 2021b].

In this article we focus on the problem of counting the number of monogenizations of a quartic order. Evertse and Győry [1985] proved explicit upper bounds for the number of monogenizations of an order in a number field K. These bounds depend only on the degree of K. The best known result for $n \geq 4$ is due to Evertse [2011], who proved in that an order $\mathcal{O}$ in a number field K of degree n can have at most $2^{4(n+5)(n-2)}$ monogenizations. In the case $n = 4$, Evertse's result shows that an order in a quartic field can have at most 2^{72} monogenizations. Recently, Bhargava [2022] gave an improved bound in, showing that an order in a quartic number field can have at most 2760 monogenizations (and even fewer when the discriminant of the order is large enough). We give another proof for Theorem 1.1 of [Bhargava 2022].

Theorem 1.1. *Let $\mathcal{O}$ be an order in a quartic number field. The number of monogenizations of $\mathcal{O}$ is at most* 2760. *If the absolute value of the discriminant of $\mathcal{O}$ is sufficiently large*, *the number of monogenizations of $\mathcal{O}$ is at most* 182. *Moreover*, *if the discriminant of $\mathcal{O}$ is negative and has sufficiently large absolute value*, *the number of monogenizations of $\mathcal{O}$ is at most* 70.

In the above theorem the assumptions about the size of the discriminant are the result of such assumptions to overcome certain technical difficulties in some approximation methods used to prove Propositions 2.3, 2.5, and 2.6. These restrictions can be expressed explicitly. For instance, assuming the absolute value of the discriminant is at least 10^{500} will suffice; see [Akhtari 2009; 2012], where such explicit values are established but no effort has been made to optimize them. It is known that there are only finitely many quartic number fields with the absolute value of their discriminants bounded by a constant; see [Birch and Merriman 1972; Evertse and Győry 1991]. By the identity in (2), which relates the discriminant of an order to that of the underlying number field, Theorem 1.1 implies that with at most finitely many exceptions, a quartic order with positive discriminant can have at most 182 monogenizations and a quartic order with negative discriminant can have at most 70 monogenizations.

Our approach involves refining and modifying an algorithmic method developed by Gaál, Pethő and Pohst [Gaál et al. 1996] to solve an index form equation $I(X, Y, Z) = \pm 1$ in a quartic number field. Using this method, we will be able to associate explicit polynomials and binary and ternary forms to a monogenic order and a fixed monogenizer of that, and eventually reduce our problem to the resolution of a number of Thue equations of degree 3 and 4. The proof in [Bhargava 2022] uses a more abstract viewpoint by utilizing two ways of parametrizing quartic rings, one established by Bhargava [2004] and another one established by Wood [2012].

2. Preliminaries: discriminants, Thue equations, discriminant and index form equations

2A. ***Discriminants.*** We recall the definitions of discriminants of orders, polynomials, algebraic numbers, and binary forms which will be frequently used throughout this manuscript. We will also refer to the discriminant of number fields. The discriminant of a number field K is the discriminant of its maximal order, the ring of integers O_K. For $K = \mathbb{Q}(\alpha)$, the discriminant of K can be expressed in terms of the discriminant of the algebraic number α and its index in $\mathbb{Q}(\alpha)$. The index of an algebraic integer and the discriminant of orders are defined in Section 2B.

Let $\boldsymbol{P}(T) \in \mathbb{Z}[T]$ be a polynomial of degree n and leading coefficient $a \in \mathbb{Z}$. The discriminant $\mathrm{Disc}(\boldsymbol{P})$ of $\boldsymbol{P}(T)$ is

$$\mathrm{Disc}(\boldsymbol{P}) = a^{2n-2} \prod_{i<j} (\gamma_i - \gamma_j)^2,$$

where $\gamma_1, \dots, \gamma_n \in \mathbb{C}$ are the roots of $\boldsymbol{P}(T)$.

The discriminant of an algebraic number is defined as the discriminant of its minimal polynomial.

Let $F(U, V) \in \mathbb{Z}[U, V]$ be a binary form of degree n that factors over $\mathbb{C}$ as

$$\prod_{i=1}^{n} (\alpha_i U - \beta_i V).$$

The discriminant $D(F)$ of F is given by

$$D(F) = \prod_{i<j} (\alpha_i \beta_j - \alpha_j \beta_i)^2. \tag{1}$$

We note that the discriminant of the polynomial $F(U, 1) \in \mathbb{Z}[U]$ is equal to the discriminant of the binary form $F(U, V) \in \mathbb{Z}[U, V]$.

2B. ***Discriminant and index form equations.*** Let K be an algebraic number field of degree n. Let $\alpha_1, \dots, \alpha_n$ a linearly independent set of n elements of K. Let $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ be all the embeddings of K into $\mathbb{C}$. The discriminant of $(\alpha_1, \dots, \alpha_n)$ is defined as the square of the determinant of an $n \times n$ matrix:

$$D_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) := (\det(\sigma_i(\alpha_j)))^2,$$

where $i, j \in \{1, \dots, n\}$.

If $\{\beta_1, \dots, \beta_n\}$ forms a basis for O_K, then the discriminant of K is

$$D_K = D_{K/\mathbb{Q}}(\beta_1, \dots, \beta_n).$$

Let $\gamma_1, \gamma_2, \dots, \gamma_n$ be an integral basis for an order O in a number field K of degree n (we note that by definition an order is a full-rank $\mathbb{Z}$-module in O_K). The discriminant of O is defined as $D_{K/\mathbb{Q}}(\gamma_1, \dots, \gamma_n)$ and is independent of the choice of the integral basis $\gamma_1, \gamma_2, \dots, \gamma_n$; see [Koch 1997], or any introductory text in algebraic number theory.

The following basic well-known lemmas are due to Hensel [1908].

Lemma 2.1. *Let $\alpha_1, \dots, \alpha_n \in O_K$ be linearly independent over $\mathbb{Q}$ and set*

$$O = \mathbb{Z}[\alpha_1, \dots, \alpha_n].$$

then

$$D_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = J^2 D_K, \tag{2}$$

where O_K^+ and O^+ are the additive groups of the modules O_K and O, respectively, and $J = (O_K^+ : O^+)$ is the module index.

For every $\gamma \in K$, we denote the algebraic conjugates of γ by $\gamma^{(i)}$ $(1 \le i \le n)$. Let $\{1, \omega_2, \dots, \omega_n\}$ be an integral basis of K. Let

$$\boldsymbol{X} = (X_1, \dots, X_n),$$

and

$$L(\boldsymbol{X}) = X_1 + \omega_2 X_2 + \cdots + \omega_n X_n, \tag{3}$$

with algebraic conjugates

$$L^{(i)}(\boldsymbol{X}) = X_1 + \omega_2^{(i)} X_2 + \cdots + \omega_n^{(i)} X_n,$$

$(1 \le i \le n)$. Kronecker and Hensel called the form $L(\boldsymbol{X})$ the *Fundamentalform* and

$$D_{K/\mathbb{Q}}(L(\boldsymbol{X})) = \prod_{1 \le i < j \le n} (L^{(i)}(\boldsymbol{X}) - L^{(j)}(\boldsymbol{X}))^2 \tag{4}$$

the *Fundamentaldiskriminante*.

Lemma 2.2. *We have*

$$D_{K/\mathbb{Q}}(L(\boldsymbol{X})) = (I(X_1, \dots, X_n))^2 D_K,$$

where D_K is the discriminant of the field K, the linear form $L(\boldsymbol{X})$ and its discriminant are defined in (3) *and* (4), *and $I(X_1, \dots, X_n)$ is a homogeneous form in $n-1$ variables of degree $n(n-1)/2$ with integer coefficients.*

The form $I(X_1, \dots, X_n)$ in the statement of Lemma 2.2 is called the index form corresponding to the integral basis $\{1, \omega_2, \dots, \omega_n\}$. An important property of the index form is that for any algebraic integer

$$\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n,$$

with $K = \mathbb{Q}(\alpha)$, by Lemma 2.2 we have

$$I(\alpha) = |I(x_2, \dots, x_n)|,$$

where $I(\alpha)$ is the index of the module $\mathbb{Z}[\alpha]$ in O_K. The index form is independent of the variable X_1, for if $\beta = \alpha + a$, where $a \in \mathbb{Z}$, then $I(\alpha) = I(\beta)$.

We remark that in a cubic number field an index form equation is in fact a cubic Thue equation (see Section 2C for the definition)

$$I(X_2, X_3) = \pm m,$$

where $m \in \mathbb{Z}$. In [Akhtari 2020] we have discussed some results about cubic Thue equations and their consequences in resolving index form equations and counting the number of monogenizations of a cubic ring.

2C. ***Upper bounds on the number of solutions of cubic and quartic Thue equations.*** Let $F(U, V) \in \mathbb{Z}[U, V]$ be a binary form of degree at least 3. If $F(U, V)$ is irreducible over $\mathbb{Q}$, for any integer m, it is shown in [Thue 1909] that the equation

$$F(U, V) = m$$

has at most finitely many solutions in integers U, V. These equations are called *Thue equations*. We will summarize some useful results on the number of integer solutions of binary cubic and quartic Thue equations. In Propositions 2.3–2.6, two pairs of solutions (u, v), $(-u, -v) \in \mathbb{Z}^2$ are considered as one solution.

The following is the combination of main results due to Bennett [2001] and Okazaki [2002]; see also [Akhtari 2009].

Proposition 2.3. *A cubic Thue equation $F(U, V) = \pm 1$ has at most 10 integer solutions. If the absolute value of the discriminant of $F(U, V)$ is sufficiently large then $F(U, V) = \pm 1$ has at most 7 integer solutions.*

The following result was established independently by Delone [1930] and Nagell [1928].

Proposition 2.4. *Let $F(U, V) \in \mathbb{Z}[U, V]$ be a cubic binary form with negative discriminant. The Thue equation $F(U, V) = \pm 1$ has at most 5 integers solutions.*

The following is Theorem A.1 of [Bhargava 2022], where results from [Akhtari 2015; 2012; Bennet and Rechnitzer ≥ 2022] are combined to obtain upper bounds for the number of integral solutions to quartic Thue equations.

Proposition 2.5. *A quartic Thue equation $F(U, V) = \pm 1$ has at most 276 integer solutions. If the absolute value of the discriminant of $F(U, V)$ is sufficiently large then the quartic Thue equation $F(U, V) = \pm 1$ has at most 26 integer solutions.*

The following is part of the main theorem in [Akhtari 2012].

Proposition 2.6. *Let $F(U, V) \in \mathbb{Z}[U, V]$ be a quartic binary form with negative discriminant. If the absolute value of the discriminant of $F(U, V)$ is sufficiently large, the Thue equation $F(U, V) = \pm 1$ has at most 14 integer solutions.*

2D. ***Matrix actions on binary forms.*** We summarize some trivial facts about matrix actions on binary forms that are well known to those in the field. Let $F(U, V) \in \mathbb{Z}[U, V]$ and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be a 2×2 matrix with integer entries. We define the binary form

$$F_A(U, V) \in \mathbb{Z}[U, V]$$

by

$$F_A(U, V) = F(aU + bV, cU + dV).$$

Via the definition (1), we observe that for any 2×2 matrix A with integer entries

$$D(F_A) = (\det A)^{n(n-1)} D(F). \tag{5}$$

We say that two integral binary forms F and G are *equivalent* if $G = \pm F_A$ for some $A \in \mathrm{GL}_2(\mathbb{Z})$. This is in fact an equivalence relationship. Moreover, the discriminants of two equivalent forms are equal.

For $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, and any $(u, v) \in \mathbb{Z}^2$, we clearly have

$$A^{-1} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

and

$$F_A(du - bv, -cu + av) = \pm F(u, v).$$

Therefore, there is a one-to-one correspondence between the possible solutions of the Thue equation $F(U, V) = \pm 1$ and those of the Thue equation $F_A(U, V) = \pm 1$.

3. Index form equations in quartic number fields

Let ξ be a quartic algebraic integer with the minimal polynomial

$$\boldsymbol{P}(T) = T^4 + a_1 T^3 + a_2 T^2 + a_3 T + a_4 \in \mathbb{Z}[T]. \tag{6}$$

Let $K = \mathbb{Q}(\xi)$. Suppose that $\omega_1 = 1$, ω_2, ω_3 and ω_4 form an integral basis for the quartic number field K. We write σ_1, σ_2, σ_3 and σ_4 for the distinct embeddings of K into $\mathbb{C}$. For $i = 1, 2, 3, 4$, we define the linear forms

$$l_i(X, Y, Z) = X\omega_2^{(i)} + Y\omega_3^{(i)} + Z\omega_4^{(i)},$$

where $\omega_j^{(i)} = \sigma_i(\omega_j)$.

The *discriminant form* corresponding to the integral basis $\{1, \omega_2, \omega_3, \omega_4\}$ is defined by

$$D_{K/\mathbb{Q}}(X\omega_2 + Y\omega_3 + Z\omega_4) = \prod_{1\le i<j\le 4} (l_i(X, Y, Z) - l_j(X, Y, Z))^2.$$

We have

$$D_{K/\mathbb{Q}}(X\omega_2 + Y\omega_3 + Z\omega_4) = (I(X, Y, Z))^2 D_K, \tag{7}$$

where D_K is the discriminant of the number field K and $I(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ is the *index form* corresponding to the fixed integral basis $\{1, \omega_2, \omega_3, \omega_4\}$. The integral ternary form $I(X, Y, Z)$ has degree 6. For any algebraic integer $\alpha = a + x\omega_2 + y\omega_3 + z\omega_4$, with $a, x, y, z \in \mathbb{Z}$, the index $I(\alpha)$ is equal to $|I(x, y, z)|$, where $I(\alpha)$ is the module index of $\mathbb{Z}[\alpha]$ in O_K, the ring of integers of K. In this section we consider the *index form equation*

$$I(X, Y, Z) = \pm m \tag{8}$$

where $m \in \mathbb{Z}$.

We follow a simple and efficient algorithm given by Gaál, Pethő and Pohst [1996], where they reduce the problem of solving an index form equation in a quartic number field to the problem of finding all solutions $(u_i, v_i) \in \mathbb{Z}^2$ of a cubic Thue equation $F(U, V) = \pm h$, with $h \in \mathbb{Z}$, and the resolution of corresponding systems of quadratic equations $\boldsymbol{Q}_1(X, Y, Z) = u_i$, $\boldsymbol{Q}_2(X, Y, Z) = v_i$, where $F(U, V) \in \mathbb{Z}[U, V]$ is a cubic form, and $\boldsymbol{Q}_1(X, Y, Z)$ and $\boldsymbol{Q}_2(X, Y, Z)$ are integral ternary quadratic forms. We state this reduction more precisely in Proposition 3.1.

We denote by I_0 the index of the algebraic integer ξ. Then

$$I_0 = I(\xi) = |I(x_0, y_0, z_0)|,$$

where $\xi = a_\xi + x_0\omega_2 + y_0\omega_3 + z_0\omega_4$, and $a_\xi, x_0, y_0, z_0 \in \mathbb{Z}$. Once again we remark that the algebraic integers ξ and $\xi - a_\xi$ have the same index in O_K. Since I_0 is the index of $\mathbb{Z}[\xi]$ in O_K, for every algebraic integer $\alpha \in O_K$, we have

$$I_0\alpha \in \mathbb{Z}[\xi].$$

Assume that $(x_1, y_1, z_1) \in \mathbb{Z}^3$ satisfies (8). Let

$$\alpha = x_1\omega_2 + y_1\omega_3 + z_1\omega_4, \tag{9}$$

and

$$\alpha' = I_0\alpha = a'_\alpha + x'_1\xi + y'_1\xi^2 + z'_1\xi^3 \in \mathbb{Z}[\xi]. \tag{10}$$

We have

$$I(\alpha') = I(x'\xi + y'\xi^2 + z'\xi^3) = \pm I_0^6 m. \tag{11}$$

We denote by $\xi^{(i)}$ and $\alpha'^{(i)}$ the algebraic conjugates of ξ and α', for $i = 1, 2, 3, 4$. Dividing both sides of the (11) by $I(\xi) = I_0$, we obtain

$$\prod_{(i,j,k,l)} \left(\frac{\alpha'^{(i)} - \alpha'^{(j)}}{\xi^{(i)} - \xi^{(j)}}\right)\left(\frac{\alpha'^{(k)} - \alpha'^{(l)}}{\xi^{(k)} - \xi^{(l)}}\right) = \pm\frac{I_0^6 m}{I_0} = \pm I_0^5 m, \tag{12}$$

where the above product is taken for $(i, j, k, l) = (1, 2, 3, 4), (1, 3, 2, 4), (1, 4, 2, 3)$. For each (i, j, k, l), via (10), we have

$$\left(\frac{\alpha'^{(i)} - \alpha'^{(j)}}{\xi^{(i)} - \xi^{(j)}}\right)\left(\frac{\alpha'^{(k)} - \alpha'^{(l)}}{\xi^{(k)} - \xi^{(l)}}\right) = \boldsymbol{Q}_1(x'_1, y'_1, z'_1) - \xi_{i,j,k,l}\boldsymbol{Q}_2(x'_1, y'_1, z'_1), \tag{13}$$

where

$$\xi_{i,j,k,l} = \xi^{(i)}\xi^{(j)} + \xi^{(k)}\xi^{(l)},$$

$$\boldsymbol{Q}_1(X, Y, Z) = \\ X^2 - a_1XY + a_2Y^2 + (a_1^2 - 2a_2)XZ + (a_3 - a_1a_2)YZ + (-a_1a_3 + a_2^2 + a_4)Z^2, \tag{14}$$

and

$$\boldsymbol{Q}_2(X, Y, Z) = Y^2 - XZ - a_1YZ + a_2Z^2. \tag{15}$$

The coefficients of the quadratic forms $\boldsymbol{Q}_1(X, Y, Z)$ and $\boldsymbol{Q}_2(X, Y, Z)$ are expressed in terms of the coefficients of $\boldsymbol{P}(T)$, the minimal polynomial of ξ given in (6). For each $(i, j, k, l) = (1, 2, 3, 4), (1, 3, 2, 4), (1, 4, 2, 3)$, we define the linear form

$$\mathcal{P}(i, j, k, l) = \mathcal{P}(i, j, k, l)(U, V) = U - \xi_{1,2,3,4}V.$$

Taking $U = \boldsymbol{Q}_1(X, Y, Z)$ and $V = \boldsymbol{Q}_2(X, Y, Z)$, by (12) and (13), we obtain

$$\prod_{(i,j,k,l)} \mathcal{P}(i, j, k, l) = (U - \xi_{1,2,3,4}V)(U - \xi_{1,3,2,4}V)(U - \xi_{1,4,2,3}V) = \pm I_0^5 m, \tag{16}$$

where the product is taken over $(i, j, k, l) = (1, 2, 3, 4), (1, 3, 2, 4), (1, 4, 2, 3)$.

The left-hand side of (16) is a cubic binary form in U and V whose coefficients are symmetric polynomials of $\xi^{(1)}, \xi^{(2)}, \xi^{(3)}, \xi^{(4)}$. Simple and routine calculations show that this integral cubic binary form is

$$\begin{aligned}\prod_{(i,j,k,l)} \mathcal{P}(i, j, k, l)(U, V) &\\ &= F(U, V)\\ &= U^3 - a_2U^2V + (a_1a_3 - 4a_4)UV^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)V^3. \end{aligned}\tag{17}$$

The cubic polynomial

$$F(T, 1) = T^3 - a_2T^2 + (a_1a_3 - 4a_4)T + (4a_2a_4 - a_3^2 - a_1^2a_4)$$

is called the *cubic resolvent polynomial* of $\boldsymbol{P}(T)$, the minimal polynomial of ξ. The discriminant of $\boldsymbol{P}(T) \in \mathbb{Z}[T]$ is equal to the discriminant of $F(T, 1) \in \mathbb{Z}[T]$ and therefore to the discriminant of $F(U, V) \in \mathbb{Z}[U, V]$. Since the discriminant of the minimal polynomial $\boldsymbol{P}(T)$ is not zero, we conclude that $F(U, V)$ will factor into three pairwise nonproportional linear factors over $\mathbb{C}$. This, together with (16), implies that the three cubic algebraic integers $\xi_{1,2,3,4}$, $\xi_{1,3,2,4}$, and $\xi_{1,4,2,3}$ are distinct algebraic conjugates over $\mathbb{Q}$. The above argument can be found in [Gaál 2019] and [Gaál et al. 1996], and implies the following.

Proposition 3.1. *Let ξ be a quartic algebraic integer and*

$$I_0 = I(\xi).$$

Assume that $I(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ is an index form in the quartic number field $\mathbb{Q}(\xi)$. The triple $(x, y, z) \in \mathbb{Z}^3$ is a solution of the index form equation

$$I(X, Y, Z) = \pm m,$$

with $m \in \mathbb{Z}$, if and only if there exists a solution $(u, v) \in \mathbb{Z}^2$ of the cubic Thue equation

$$F(U, V) = \pm I_0^5 m \tag{18}$$

such that (x, y, z) satisfies the system of quadratic ternary equations

$$\boldsymbol{Q}_1(X, Y, Z) = u, \qquad \boldsymbol{Q}_2(X, Y, Z) = v, \tag{19}$$

where $F(U, V)$ is an integral cubic binary form and $\boldsymbol{Q}_1(X, Y, Z)$ and $\boldsymbol{Q}_2(X, Y, Z)$ are integral quadratic ternary forms, respectively defined in (17), (14) *and* (15) *with coefficients expressed in terms of the coefficients of the minimal polynomial of the fixed generator ξ.*

Proposition 3.1 provides a general algorithm to find algebraic integers with index m in the quartic number field K by fixing any algebraic integer ξ that generates K. So in general the quantities I_0 and m need not to be related. Using an argument of Mordell [1969], in [Gaál et al. 1996] it is shown that all solutions of an index form equation in a quartic number field can be found through solving finitely many cubic and quartic Thue equations; see Theorems 1 and 2, as well as equations (8), (9) and (10) of [loc. cit.]. In Section 4 we will modify the argument in [loc. cit.] and apply our modification to an index form equation of the shape $I(X, Y, Z) = \pm 1$ connected to the quartic ring generated by an algebraic integer ξ. This will enable us to count these Thue equations more efficiently. Moreover, it turns out that in this case the right-hand sides of our Thue equations are ± 1, and therefore we may apply absolute upper bounds for the number of integer solutions recorded in Section 2C. This way we can provide an absolute upper bound for the number of solutions of the index form equation that we study. These solutions will correspond to different monogenizations of the quartic order $\mathbb{Z}[\xi]$.

We end this section by recording another important relation between the ternary quadratic forms $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$, defined in (14) and (15), and the integer values represented by the cubic form $F(U, V)$. For $(u_0, v_0) \in \mathbb{Z}^2$, we define

$$\boldsymbol{Q}(X, Y, Z) = u_0 \boldsymbol{Q}_2(X, Y, Z) - v_0 \boldsymbol{Q}_1(X, Y, Z). \tag{20}$$

Let $M_{\boldsymbol{Q}}$ be the 3×3 symmetric Gram matrix of the quadratic form $\boldsymbol{Q}(X, Y, Z)$. We have

$$4|\mathrm{Det}(M_{\boldsymbol{Q}})| = |F(u_0, v_0)|, \tag{21}$$

where $F(U, V)$ is defined in (17). The identity (21) can be verified easily and is established as an implication of Lemma 1 of [Gaál et al. 1996]. Its proof can also be found in Lemma 6.1.1 of [Gaál 2019]. The identity (21) is not used in our proofs, but it is crucial in confirming that the ternary quadratic forms $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$ form a pair that parametrizes a quartic ring in the sense of Bhargava [2004]. Such a parametrization is used in Bhargava's proof of Theorem 1.1 [Bhargava 2022]. Another ingredient in [Bhargava 2022] is a beautiful parametrization due to Wood [2012] for quartic rings. We do not use any of these two parametrizations. However, in light of identities (20) and (21), one could view our discussion in the following section as an explicit way of expressing polynomials and binary forms that are appearing (implicitly) in Bhargava's and Wood's methods of parametrization.

4. Proof of Theorem 1.1

When treating a general index form equation in a quartic number field, one needs to consider the identity (10) in order to have integer values for x'_1, y'_1 and z'_1. In Theorem 1.1 we are interested in finding other possible monogenizers for a monogenized ring $\mathbb{Z}[\xi]$. Therefore, we are looking for algebraic integers $\alpha \in \mathbb{Z}[\xi]$ that satisfy the index form (8). In this case, under the assumption $\alpha \in \mathbb{Z}[\xi]$, we may express (10) as

$$\alpha = a_\alpha + x\xi + y\xi^2 + z\xi^3, \tag{22}$$

with $x, y, z \in \mathbb{Z}$. This will simplify some of the equations introduced in Section 3. Another simple observation is that if $\mathbb{Z}[\xi] = \mathbb{Z}[\alpha]$, then the algebraic integers α and ξ have the same index in the ring of integers of the underlying number field $\mathbb{Q}(\alpha) = \mathbb{Q}(\xi)$, and therefore in the index form (11) and (12), we may take $I_0 = m$.

Let K be a quartic number field and ξ an algebraic integer in K of index $I_0 = m$. We are interested in finding other monogenizers of $\mathbb{Z}[\xi]$. After replacing (10) by

(22), for $\alpha \in \mathbb{Z}[\xi]$ the identity (12) becomes

$$\prod_{(i,j,k,l)} \left(\frac{\alpha^{(i)} - \alpha^{(j)}}{\xi^{(i)} - \xi^{(j)}}\right)\left(\frac{\alpha^{(k)} - \alpha^{(l)}}{\xi^{(k)} - \xi^{(l)}}\right) = \pm 1. \tag{23}$$

Therefore, in Proposition 3.1, we may consider the cubic Thue equation

$$F(U, V) = \pm 1. \tag{24}$$

In fact, we obtain the following modification of Proposition 3.1.

Lemma 4.1. *The algebraic integer $x\xi + y\xi^2 + z\xi^3$, with $x, y, z \in \mathbb{Z}$ is a monogenizer of $\mathbb{Z}[\xi]$ if and only if there is a solution $(u, v) \in \mathbb{Z}^2$ of the cubic Thue equation*

$$F(U, V) = \pm 1 \tag{25}$$

such that (x, y, z) satisfies the system of quadratic ternary equations

$$\boldsymbol{Q}_1(X, Y, Z) = u, \quad \boldsymbol{Q}_2(X, Y, Z) = v. \tag{26}$$

4A. *The trivial solution of $F(U, V) = 1$.* First we notice that $F(U, V)$ is monic and therefore $(u, v) = (1, 0)$ satisfies the equation $F(U, V) = \pm 1$. This corresponds to the system of equations

$$\begin{aligned} \boldsymbol{Q}_1(X, Y, Z) &= 1 \\ \boldsymbol{Q}_2(X, Y, Z) &= 0, \end{aligned} \tag{27}$$

where the ternary quadratic forms $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$ are defined in (14) and (15).

A special solution to the system of equations (27) is $(x, y, z) = (1, 0, 0)$ as ξ is trivially a monogenizer of $\mathbb{Z}[\xi]$; see (10).

Assume $x, y, z \in \mathbb{Z}$ satisfy (27). Then

$$\boldsymbol{Q}_2(x, y, z) = y^2 - xz - a_1 yz + a_2 z^2 = 0. \tag{28}$$

If $z = 0$ then $y = 0$. Since x, y, z also satisfy $\boldsymbol{Q}_1(X, Y, Z) = 1$, we conclude that $x = 1$.

Now assume that $z \neq 0$. From (28), we conclude that $z \mid y^2$. Let $q = \gcd(z, y)$, $y = qy'$ and $z = qz'$, with $\gcd(y', z') = 1$. We may rewrite (28) as

$$\boldsymbol{Q}_2(x, y, z) = y'^2 q^2 - xz'q - a_1 y'z'q^2 + a_2 z'^2 q^2 = 0$$

to conclude that $q \mid xz'$ and $z' \mid q$. Since (x, y, z) satisfies the system (27), in particular $\boldsymbol{Q}_1(x, y, z) = 1$, we have $\gcd(q, x) = 1$ and therefore $q \mid z'$. So we have $z' = \pm q$ and $q^2 = \pm z$. Since (x, y, z) and $(-x, -y, -z)$ give the same monogenization, we may assume $z \geq 0$ and $q^2 = z$. Now we can express x, y and z in terms of two integers q and p as follows:

$$x = p^2 - a_1 pq + a_2 q^2, \quad y = pq, \quad z = q^2. \tag{29}$$

The parametrization (29) can be done for any $(x, y, z) \neq (1, 0, 0)$ that satisfies (28). Substituting the parametrized values for variables X, Y and Z in (14), we may express the ternary quadratic form $\boldsymbol{Q}_1(X, Y, Z)$ as a quartic binary form in variables P, Q, where

$$X(P, Q) = P^2 - a_1 PQ + a_2 Q^2, \quad Y(P, Q) = PQ, \quad Z(P, Q) = Q^2. \tag{30}$$

We note that each $X(P, Q)$, $Y(P, Q)$ and $Z(P, Q)$ is a binary quadratic form in variables P and Q. The parametrization (29) was considered for $z \neq 0$, however the trivial (and special) solution $(x, y, z) = (1, 0, 0)$ also corresponds to a solution of the quartic Thue equation

$$\boldsymbol{Q}_1(X(P, Q), Y(P, Q), Z(P, Q)) = 1,$$

namely $(p, q) = (1, 0)$.

Let us define the quartic binary form

$$\mathcal{Q}_{(1,0)}(P, Q) = \mathcal{Q}(P, Q) = \boldsymbol{Q}_1(X(P, Q), Y(P, Q), Z(P, Q)). \tag{31}$$

We have shown that the number of solutions $(X, Y, Z) \in \mathbb{Z}^3$ of the system of ternary equations (27) is equal to the number of integer solutions (p, q) of the quartic Thue equation

$$\mathcal{Q}(P, Q) = 1.$$

Via (27), we may substitute the parameter X by $(Y^2 - a_1 YZ + a_2 Z^2)/Z^2$ in $\boldsymbol{Q}_1(X, Y, Z)$ to get

$$\boldsymbol{Q}_1(X, Y, Z) = Z^4 \boldsymbol{P}\big(\tfrac{Y}{Z} - a_1\big),$$

where $\boldsymbol{P}(T)$ is the minimal polynomial of ξ defined in (6). In other words,

$$\mathcal{Q}(P, Q) = Q^4 \boldsymbol{P}\big(\tfrac{P}{Q} - a_1\big).$$

Since $a_1 \in \mathbb{Z}$, we conclude that the discriminant of the quartic form $\mathcal{Q}(P, Q)$ is equal to the discriminant of ξ, and therefore, to the discriminant of the cubic form $F(U, V)$.

We also note that $\mathcal{Q}(P, Q)$ is a monic binary form, i.e., the coefficient of the term P^4 equals 1. This confirms the existence of the trivial solution $(p, q) = (1, 0)$ of the Thue equation $\mathcal{Q}(P, Q) = 1$.

We conclude that the trivial solution $(1, 0)$ of the cubic Thue equation $F(U, V) = 1$ corresponds to a quartic Thue equation, namely $\mathcal{Q}_{(1,0)}(P, Q) = 1$, defined in (31). Moreover, by (29), each pair of solution $(p, q) \in \mathbb{Z}^2$ corresponds to the monogenizer

$$X(p, q)\xi + Y(p, q)\xi^2 + Z(p, q)\xi^3$$

of the order $\mathbb{Z}[\xi]$. Clearly, the monogenizer ξ is produced by the solution $(p, q) = (1, 0)$ of the quartic Thue equation.

4B. ***Nontrivial solutions of $F(U, V) = 1$.*** For nontrivial solutions of the Thue equation (24), in [Gaál et al. 1996] the system of ternary quadratic equations (32) is reduced to a quartic Thue equation with a parametrization similar to (30); see equations (8) and (10) of [Gaál et al. 1996]. We simplify such a parametrization with help of a $\mathrm{GL}_2(\mathbb{Z})$ matrix that maps any given primitive solution of a Thue equation to the trivial solution $(1, 0)$ of an equivalent Thue equation. More precisely, assume that $(u_0, v_0) \in \mathbb{Z}^2$, with $(u_0, v_0) \neq (1, 0)$, satisfies (24). We have $\gcd(u_0, v_0) = 1$ and therefore we may choose fixed $s, t \in \mathbb{Z}$ so that

$$su_0 + tv_0 = 1.$$

Consequently, if $(x, y, z) \in \mathbb{Z}^3$ satisfies the system of equations in (19) with $(u, v) = (u_0, v_0)$, then (x, y, z) will satisfy

$$\begin{aligned} \mathbf{Q}'_1(X, Y, Z) &= s\boldsymbol{Q}_1(X, Y, Z) + t\boldsymbol{Q}_2(X, Y, Z) = 1 \\ \mathbf{Q}'_2(X, Y, Z) &= v_0\boldsymbol{Q}_1 - u_0\boldsymbol{Q}_2 = 0. \end{aligned} \tag{32}$$

The next step is to express this system as an equation of a quartic binary form to 1, via the parametrization (30).

Let $A = \begin{pmatrix} s & t \\ -v_0 & u_0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. Clearly we have

$$A\begin{pmatrix} u_0 \\ v_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The matrix $A^{-1} \in \mathrm{GL}_2(\mathbb{Z})$ acts on the binary cubic form $F(U, V)$ to produce the equivalent binary form $F_{A^{-1}}(U, V)$. The solution (u_0, v_0) of $F(U, V) = 1$ corresponds to the solution $(1, 0)$ of the cubic equation $F_{A^{-1}}(U, V) = 1$.

Since $(1, 0)$ satisfies the equation $F_{A^{-1}}(U, V) = 1$, the cubic binary form $F_{A^{-1}}(U, V)$ is monic. Similar to (31), and via parametrization (30), we obtain the binary quartic form

$$\mathcal{Q}_{(u_0,v_0)}(P, Q) = \mathbf{Q}'_1(X(P, Q), Y(P, Q), Z(P, Q)), \tag{33}$$

with $\mathbf{Q}'_1$ defined in (32). Therefore, in order to solve the system of ternary equations (32) one can solve the quartic Thue equation

$$\mathcal{Q}_{(u_0,v_0)}(P, Q) = 1 \tag{34}$$

in integers P, Q.

4C. ***Conclusion.*** Let ξ be an algebraic integer of degree 4 with the minimal polynomial given in (6). In order to count the number of monogenizations of $\mathbb{Z}[\xi]$, we defined the integral cubic form $F(u, v)$ in (17), and the integral quadratic forms $\boldsymbol{Q}_1(X, Y, Z)$ and $\boldsymbol{Q}_2(X, Y, Z)$ in (14) and (15), respectively. The coefficients of these forms are all expressed in terms of the coefficients of the minimal polynomial of ξ. We showed that the following three numbers are equal:

(1) The number of solutions to the cubic Thue equation $F(U, V) = \pm 1$ in (24).

(2) The number of systems of ternary quadratic equations (32).

(3) The number of quartic Thue equations (34).

We have also shown that for any fixed solution $(u, v) \in \mathbb{Z}^2$ of the cubic Thue equation $F(U, V) = \pm 1$ in (24), each solution (p, q) of the corresponding quartic Thue equation (34) provides a monogenizer $X(p, q)\xi + Y(p, q)\xi^2 + Z(p, q)\xi^3$, with the integral binary quadratic forms $X(P, Q)$, $Y(P, Q)$ and $Z(P, Q)$ defined in (30).

Therefore, the number of monogenizations of $\mathbb{Z}[\xi]$ is bounded by an upper bound for the number of integer solutions to cubic Thue equations multiplied by an upper bound for the number of integer solutions to quartic Thue equations. Proposition 2.3 provides upper bounds for the number of solutions of cubic Thue equations and Proposition 2.5 provides upper bounds for the number of solutions of quartic Thue equations.

Acknowledgements

I am grateful to the anonymous referee for many helpful comments and suggestions, which improved an earlier version of this article significantly.

I thank *Professor Manjul Bhargava* for inspiring and insightful conversations about the general topic of this article. I thank *Professor Kálmán Győry* for encouragement, sharing his beautiful work, and comments on an earlier version of this article.

During the completion of this project I visited the department of mathematics at Cornell University and was supported by the Ruth I. Michler Memorial Prize. I am grateful to *Professor Michler's family* and AWM for creating this invaluable opportunity and to the Cornell math department for their hospitality. In particular, I thank *Professor Ravi Ramakrishna* for warmly welcoming me and making me feel at home in Ithaca.

This research has been supported in part by *the Simons Foundation Collaboration Grants*, Award Number 635880, and by *the National Science Foundation* Award DMS-2001281.

References

[Akhtari 2009] S. Akhtari, "Cubic Thue equations", *Publ. Math. Debrecen* **75**:3-4 (2009), 459–483. MR Zbl

[Akhtari 2012] S. Akhtari, "Upper bounds for the number of solutions to quartic Thue equations", *Int. J. Number Theory* **8**:2 (2012), 335–360. MR Zbl

[Akhtari 2015] S. Akhtari, "Representation of small integers by binary forms", *Q. J. Math.* **66**:4 (2015), 1009–1054. MR Zbl

[Akhtari 2020] S. Akhtari, "Counting monogenic cubic orders", pp. 13–24 in *Combinatorial and additive number theory*, *III*, edited by M. B. Nathanson, Springer Proc. Math. Stat. **297**, Springer, 2020. MR Zbl

[Alpöge et al. 2021a] L. Alpöge, M. Bhargava, and A. Shnidman, "A positive proportion of cubic fields are not monogenic yet have no local obstruction to being so", preprint, 2021. arXiv 2011.01186

[Alpöge et al. 2021b] L. Alpöge, M. Bhargava, and A. Shnidman, "A positive proportion of quartic fields are not monogenic yet have no local obstruction to being so", preprint, 2021. arXiv 2107.05514

[Bennet and Rechnitzer $\geq$ 2022] M. Bennet and A. Rechnitzer, "Tabulating binary quartic forms over $\mathbb{Z}$ by discriminant", in preparation.

[Bennett 2001] M. A. Bennett, "On the representation of unity by binary cubic forms", *Trans. Amer. Math. Soc.* **353**:4 (2001), 1507–1534. MR Zbl

[Bhargava 2004] M. Bhargava, "Higher composition laws, III: The parametrization of quartic rings", *Ann. of Math.* (2) **159**:3 (2004), 1329–1360. MR Zbl

[Bhargava 2022] M. Bhargava, "On the number of monogenizations of a quartic order", *Publ. Math. Debrecen* **100**:3-4 (2022), 513–531. MR Zbl

[Birch and Merriman 1972] B. J. Birch and J. R. Merriman, "Finiteness theorems for binary forms with given discriminant", *Proc. London Math. Soc.* (3) **24** (1972), 385–394. MR Zbl

[Dedekind 1878] R. Dedekind, "Ueber den Zusammenhang zwischen der Theorie der ideale und der Theorie der höheren Congruenzen", *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen* **23** (1878), 3–38.

[Delaunay 1930] B. Delaunay, "Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante", *Math. Z.* **31**:1 (1930), 1–26. MR Zbl

[Evertse 2011] J.-H. Evertse, "A survey on monogenic orders", *Publ. Math. Debrecen* **79**:3-4 (2011), 411–422. MR Zbl

[Evertse and Győry 1985] J.-H. Evertse and K. Győry, "On unit equations and decomposable form equations", *J. Reine Angew. Math.* **358** (1985), 6–19. MR Zbl

[Evertse and Győry 1991] J.-H. Evertse and K. Győry, "Effective finiteness results for binary forms with given discriminant", *Compositio Math.* **79**:2 (1991), 169–204. MR Zbl

[Evertse and Győry 2017] J.-H. Evertse and K. Győry, *Discriminant equations in Diophantine number theory*, New Mathematical Monographs **32**, Cambridge University Press, 2017. MR Zbl

[Gaál 2019] I. Gaál, *Diophantine equations and power integral bases*, Birkhäuser, Boston, 2019. MR

[Gaál et al. 1996] I. Gaál, A. Pethő, and M. Pohst, "Simultaneous representation of integers by a pair of ternary quadratic forms—with an application to index form equations in quartic number fields", *J. Number Theory* **57**:1 (1996), 90–104. MR Zbl

[Győry 1976] K. Győry, "Sur les polynômes à coefficients entiers et de discriminant donné, III", *Publ. Math. Debrecen* **23**:1-2 (1976), 141–165. MR Zbl

[Hensel 1908] K. Hensel, "Theorie der algebraischen Zahlen, Band 1", 1908. Zbl

[Koch 1997] H. Koch, *Algebraic number theory*, Springer, 1997. MR Zbl

[Mordell 1969] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics **30**, Academic Press, London, 1969. MR Zbl

[Nagell 1928] T. Nagell, "Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante", *Math. Z.* **28**:1 (1928), 10–29. MR Zbl

[Okazaki 2002] R. Okazaki, “Geometry of a cubic Thue equation”, *Publ. Math. Debrecen* **61**:3-4 (2002), 267–314. MR Zbl

[Thue 1909] A. Thue, “Über Annäherungswerte algebraischer Zahlen”, *J. Reine Angew. Math.* **135** (1909), 284–305. MR Zbl

[Wood 2012] M. M. Wood, “Quartic rings associated to binary quartic forms”, *Int. Math. Res. Not.* **2012**:6 (2012), 1300–1320. MR Zbl

Received 18 Mar 2022. Revised 22 Jun 2022.

SHABNAM AKHTARI:

akhtari@uoregon.edu
Department of Mathematics, University of Oregon, Eugene, OR, United States

Essential Number Theory
Vol. 1, No. 1, 2022
https://doi.org/10.2140/ent.2022.1.73

Modularity lifting theorems

Toby Gee

Updated lecture notes from 2013 Arizona winter school.

1. Introduction

The main aim of these notes is to explain modularity/automorphy lifting theorems for two-dimensional p-adic representations, using wherever possible arguments that go over to the (essentially conjugate self-dual) n-dimensional case. In particular, we use improvements on the original Taylor–Wiles method due to Diamond, Fujiwara and Kisin, and we explain (in the case $n = 2$) Taylor's arguments [2008] that avoid the use of Ihara's lemma. For the most part I ignore the issues which are local at p, focusing on representations which satisfy the Fontaine–Laffaille condition.

1.1. ***Notation.*** Much of this notation will also be introduced in the text, but I have tried to collect together various definitions here, for ease of reading. Throughout these notes, $p > 2$ is a prime greater than two. In the earlier stages of the notes, we discuss n-dimensional p-adic and mod p representations, before specialising to the case $n = 2$. When we do so, we assume that $p \nmid n$. (Of course, in the case $n = 2$, this follows from our assumption that $p > 2$.)

If M is a field, we let G_M denote its absolute Galois group $\mathrm{Gal}(\overline{M}/M)$, where $\overline{M}$ is some choice of separable closure of M. We write ε_p (or just ε) for the p-adic cyclotomic character. We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and regard all algebraic extensions of $\mathbb{Q}$ as subfields of $\overline{\mathbb{Q}}$. For each prime p we fix an algebraic closure $\overline{\mathbb{Q}}_p$

MSC2020: 11S37.
Keywords: automorphic forms, modularity lifting, Langlands program.

of $\mathbb{Q}_p$, and we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. In this way, if v is a finite place of a number field F, we have a homomorphism $G_{F_v} \hookrightarrow G_F$. We also fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. If $L/\mathbb{Q}_p$ is algebraic, then we write $\mathcal{O}_L$ for the ring of integers of L, and $k(L)$ for its residue field.

We normalize the definition of Hodge–Tate weights so that all the Hodge–Tate weights of the p-adic cyclotomic character ε_p are -1.

If R is a local ring, we write $\mathfrak{m}_R$ for the maximal ideal of R.

We let ζ_p be a primitive p-th root of unity.

We use the terms "modularity lifting theorem" and "automorphy lifting theorem" more or less interchangeably.

2. Galois representations

Modularity lifting theorems prove that certain Galois representations are modular, in the sense that they come from modular forms. We begin in this first chapter by introducing Galois representations, and explaining some of their basic properties.

2.1. ***Basics of Galois representations (and structure of Galois groups).*** Let K'/K be a (not necessarily finite) normal and separable extension of fields. Then the Galois group $\mathrm{Gal}(K'/K)$ is the group

$$\{\sigma \in \mathrm{Aut}(K') : \sigma|_K = \mathrm{id}_K\}.$$

This has a natural topology, making it a compact Hausdorff totally disconnected topological group; equivalently, it is a profinite group. This can be expressed by the topological isomorphism

$$\mathrm{Gal}(K'/K) \cong \varprojlim_{\substack{K''/K \text{ finite normal} \\ K'' \subseteq K'}} \mathrm{Gal}(K''/K),$$

where the finite groups $\mathrm{Gal}(K''/K)$ have the discrete topology. Then Galois theory gives a bijective correspondence between intermediate fields $K' \supset K'' \supset K$ and closed subgroups $H \subset \mathrm{Gal}(K'/K)$, with K'' corresponding to $\mathrm{Gal}(K'/K'')$ and H corresponding to K^H; see, e.g., Section 1.6 of [Gruenberg 1967].

Fix a separable closure $\overline{K}$ of K, and write $G_K := \mathrm{Gal}(\overline{K}/K)$. Let L be a topological field; then a *Galois representation* is a continuous homomorphism $\rho : G_K \to \mathrm{GL}_n(L)$ for some n. The nature of these representations depends on the topology on L. For example, if L has the discrete topology, then the image of ρ is finite, and ρ factors through a finite Galois group $\mathrm{Gal}(K''/K)$.

Exercise 2.2. If $L = \mathbb{C}$ with the usual topology, then $\rho(G_K)$ is finite, and ρ is conjugate to a representation valued in $\mathrm{GL}_n(\overline{\mathbb{Q}})$.

On the other hand, if $L/\mathbb{Q}_p$ is a finite extension with the p-adic topology, then there can be examples with infinite image. The rest of these notes will be concerned with these p-adic representations. For example, if $p \neq \operatorname{char} K$, we have the p-adic cyclotomic character $\varepsilon_p : G_K \to \mathbb{Z}_p^\times$, which is uniquely determined by the requirement that if $\sigma \in G_K$ and $\zeta \in \overline{K}$ with $\zeta^{p^m} = 1$ for some n, then $\sigma(\zeta) = \zeta^{\varepsilon_p(\sigma) \pmod{p^m}}$. More interesting examples arise from geometry, as we explain in Section 2.21 below.

Fact 2.3. If $L/\mathbb{Q}_p$ is an algebraic extension, and $\rho : G_K \to \mathrm{GL}_n(L)$ is a continuous representation, then $\rho(G_K) \subseteq \mathrm{GL}_n(M)$ for some $L \supset M \supset \mathbb{Q}_p$ with $M/\mathbb{Q}_p$ finite.

Proof. This follows from the Baire category theorem; see, e.g., the proof of Corollary 5 of [Dickinson 2001b] for the details. □

Exercise 2.4. If $L/\mathbb{Q}_p$ is an algebraic extension, and $\rho : G_K \to \mathrm{GL}_n(L)$ is a continuous representation, then ρ is conjugate to a representation in $\mathrm{GL}_n(\mathcal{O}_L)$.

Any finite-dimensional Galois representation has a Jordan–Hölder sequence, and thus a well-defined semisimplification.

Fact 2.5. Two Galois representations $\rho, \rho' : G_K \to \mathrm{GL}_n(L)$ have isomorphic semisimplifications if and only if $\rho(g), \rho'(g)$ have the same characteristic polynomials for each $g \in G_K$. If $\operatorname{char} L = 0$ (or indeed if $\operatorname{char} L > n$), then this is equivalent to $\operatorname{tr} \rho(g) = \operatorname{tr} \rho'(g)$ for all $g \in G_K$.

Proof. This is a consequence of the Brauer–Nesbitt theorem, [Curtis and Reiner 1962, 30.16] □

As a corollary of the previous exercise and fact, we see that p-adic representations have well-defined semisimplified reductions modulo p. Indeed, given $\rho : G_K \to \mathrm{GL}_n(L)$ with $L/\mathbb{Q}_p$ algebraic, we may conjugate ρ to be valued in $\mathrm{GL}_n(\mathcal{O}_L)$, reduce modulo the maximal ideal and semisimplify to get a semisimple representation $\bar{\rho} : G_K \to \mathrm{GL}_n(k(L))$, whose characteristic polynomials are determined by those of ρ.

Remark 2.6. We really do have to semisimplify here; to see why, think about the reductions modulo p of the matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right)$.

2.7. ***Local representations with p ≠ l: the monodromy theorem.*** In this section we will let $K/\mathbb{Q}_l$ be a finite extension, for some prime $l \neq p$. In order to study the representations of G_K, we firstly recall something of the structure of G_K itself; see, e.g., [Serre 1979] for further details. Let ϖ_K be a uniformizer of $\mathcal{O}_K$, let $k = k(K)$ denote the residue field of K, and let $\mathrm{val}_K : K^\times \twoheadrightarrow \mathbb{Z}$ be the ϖ_K-adic valuation. Let $|\cdot|_K := (\#k)^{-\mathrm{val}_K(\cdot)}$ be the corresponding norm. The action of G_K on K preserves

val_K, and thus induces an action on k, so that we have a homomorphism $G_K \to G_k$, and in fact a short exact sequence

$$0 \to I_K \to G_K \to G_k \to 0$$

defining the inertia subgroup I_K. We let $\mathrm{Frob}_K = \mathrm{Frob}_k \in G_k$ be the geometric Frobenius element, a topological generator of $G_k \cong \hat{\mathbb{Z}}$.

Then we define the Weil group W_K via the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & I_K \arrow[r] & G_K \arrow[r] & G_k \arrow[r] & 0 \\
0 \arrow[r] & I_K \arrow[r] \arrow[u, equal] & W_K \arrow[r] \arrow[u, hook] & \mathrm{Frob}_k^{\mathbb{Z}} \arrow[r] \arrow[u, hook] & 0
\end{tikzcd}$$

so that W_K is the subgroup of G_K consisting of elements which map to an integral power of the Frobenius in G_k. The group W_K is a topological group, but its topology is not the subspace topology of G_K; rather, the topology is determined by decreeing that I_K is open, and has its usual topology.

Let $K^{\mathrm{ur}} = \overline{K}^{I_K}$ be the maximal unramified extension of K, and let $K^{\mathrm{tame}} = \bigcup_{(m,l)=1} K^{\mathrm{ur}}(\varpi_K^{1/m})$ be the maximal tamely ramified extension. Then the wild inertia subgroup $P_K := \mathrm{Gal}(\overline{K}/K^{\mathrm{tame}})$ is the unique Sylow pro-l subgroup of I_K. Let $\zeta = (\zeta_m)_{(m,l)=1}$ be a compatible system of primitive roots of unity (i.e., $\zeta_{ab}^a = \zeta_b$). Then we have a character

$$t_\zeta : I_K/P_K \xrightarrow{\sim} \prod_{p \neq l} \mathbb{Z}_p,$$

defined by

$$\frac{\sigma(\varpi_K^{1/m})}{\varpi_K^{1/m}} = \zeta_m^{(t_\zeta(\sigma) \pmod{m})}.$$

Exercise 2.8. Any other compatible system of roots of unity is of the form ζ^u for some $u \in \prod_{p \neq l} \mathbb{Z}_p^\times$, and we have $t_{\zeta^u} = u^{-1} t_\zeta$.

If $\sigma \in W_K$, then $t_\zeta(\sigma\tau\sigma^{-1}) = \varepsilon(\sigma) t_\zeta(\tau)$, where ε is the cyclotomic character. We let $t_{\zeta,p}$ be the composite of t_ζ and the projection to $\mathbb{Z}_p$.

Local class field theory is summarized in the following statement. (See, for example, [Tate 1979] for this and the other facts about class field theory recalled below.)

Theorem 2.9. *Let W_K^{ab} denote the group $W_K/\overline{[W_K, W_K]}$. Then there are unique isomorphisms $\mathrm{Art}_K : K^\times \xrightarrow{\sim} W_K^{\mathrm{ab}}$ such that*

(1) *if K'/K is a finite extension, then* $\mathrm{Art}_{K'} = \mathrm{Art}_K \circ N_{K'/K}$, *and*

(2) *we have a commutative square*

$$\begin{tikzcd}
K^\times \arrow[r, "\mathrm{Art}_K"] \arrow[d, "\mathrm{val}_K"] & W_K^{\mathrm{ab}} \arrow[d] \\
\mathbb{Z} \arrow[r] & \mathrm{Frob}_K^{\mathbb{Z}}
\end{tikzcd}$$

where the bottom arrow is the isomorphism sending $a \mapsto \mathrm{Frob}_K^a$.

The continuous irreducible representations of the group W_K^{ab} are just the continuous characters of W_K, and local class field theory gives a simple description of them, as representations of $K^\times = \mathrm{GL}_1(K)$. The local Langlands correspondence for GL_n (see Section 4.1) is a kind of n-dimensional generalization of this, giving a description of certain representations of $\mathrm{GL}_n(K)$ in terms of the n-dimensional representations of W_K.

Definition 2.10. Let L be a field of characteristic 0. A *representation* of W_K over L is a representation (on a finite-dimensional L-vector space) which is continuous if L has the discrete topology (i.e., a representation with open kernel).

A *Weil–Deligne* representation of W_K on a finite-dimensional L-vector space V is a pair (r, N) consisting of a representation $r : W_K \to \mathrm{GL}(V)$, and an endomorphism $N \in \mathrm{End}(V)$ such that for all $\sigma \in W_K$,

$$r(\sigma)Nr(\sigma)^{-1} = (\#k)^{-v_K(\sigma)}N,$$

where $v_K : W_K \to \mathbb{Z}$ is determined by $\sigma|_{K^{\mathrm{ur}}} = \mathrm{Frob}_K^{v_K(\sigma)}$.

Remark 2.11. (1) Since I_K is compact and open in W_K, if r is a representation of W_K then $r(I_K)$ is finite.

(2) N is necessarily nilpotent.

Exercise 2.12. (1) Show that if (r, V) is a representation of W_K and $m \geq 1$ then the following defines a Weil–Deligne representation $\mathrm{Sp}_m(r)$ with underlying vector space V^m: we let W_K act via

$$r|\mathrm{Art}_K^{-1}|_K^{m-1} \oplus r|\mathrm{Art}_K^{-1}|_K^{m-2} \oplus \cdots \oplus r,$$

and let N induce an isomorphism from $r|\mathrm{Art}_K^{-1}|_K^{i-1}$ to $r|\mathrm{Art}_K^{-1}|_K^{i}$ for each $i < m-1$, and be 0 on $r|\mathrm{Art}_K^{-1}|_K^{m-1}$.

(2) Show that every Weil–Deligne representation (r, V) for which r is semisimple is isomorphic to a direct sum of representations $\mathrm{Sp}_{m_i}(r_i)$.

(3) Show that if (r, V, N) is a Weil–Deligne representation of W_K, and K'/K is a finite extension, then $(r|_{W_{K'}}, V, N)$ is a Weil–Deligne representation of $W_{K'}$.

(4) Suppose that r is a representation of W_K. Show that if $\sigma \in W_K$ then for some positive integer n, $r(\sigma^n)$ is in the center of $r(W_K)$.

(5) Assume further that $\sigma \notin I_K$. Show that for any $\tau \in W_K$ there exists $n \in \mathbb{Z}$ and $m > 0$ such that $r(\sigma^n) = r(\tau^m)$.

(6) Show that for a representation r of W_K, the following conditions are equivalent:
   (a) r is semisimple.
   (b) $r(\sigma)$ is semisimple for all $\sigma \in W_K$.
   (c) $r(\sigma)$ is semisimple for some $\sigma \notin I_K$.

(7) Let (r, N) be a Weil–Deligne representation of W_K. Set $\tilde{r}(\sigma) = r(\sigma)^{\mathrm{ss}}$, the semisimplification of $r(\sigma)$. Prove that $(\tilde{r}, N)$ is also a Weil–Deligne representation of W_K.

Definition 2.13. We say that a Weil–Deligne representation (r, N) is *Frobenius semisimple* if r is semisimple. With notation as in Exercise 2.12(7), we say that $(\tilde{r}, N)$ is the *Frobenius semisimplification* of (r, N).

Definition 2.14. If L is an algebraic extension of $\mathbb{Q}_p$, then we say that an element $A \in \mathrm{GL}_n(L)$ is *bounded* if it has determinant in $\mathcal{O}_L^\times$, and characteristic polynomial in $\mathcal{O}_L[X]$.

Exercise 2.15. A is bounded if and only if it stabilizes an $\mathcal{O}_L$-lattice in L^n.

Definition 2.16. Let L be an algebraic extension of $\mathbb{Q}_p$. Then we say that r is *bounded* if $r(\sigma)$ is bounded for all $\sigma \in W_K$.

Exercise 2.17. Show r is bounded if and only if $r(\sigma)$ is bounded for some $\sigma \notin I_K$.

The reason for all of these definitions is the following theorem, which in practice gives us a rather concrete classification of the p-adic representations of G_K.

Proposition 2.18 (Grothendieck's monodromy theorem). *Suppose that $l \neq p$, that $K/\mathbb{Q}_l$ is finite, and that V is a finite-dimensional L-vector space, with L an algebraic extension of $\mathbb{Q}_p$. Fix $\varphi \in W_K$ a lift of* Frob$_K$ *and a compatible system $(\zeta_m)_{(m,l)=1}$ of primitive roots of unity. If $\rho : G_K \to \mathrm{GL}(V)$ is a continuous representation then there is a finite extension K'/K and a uniquely determined nilpotent $N \in \mathrm{End}(V)$ such that for all $\sigma \in I_{K'}$,*

$$\rho(\sigma) = \exp(N t_{\zeta,p}(\sigma)).$$

For all $\sigma \in W_K$, we have $\rho(\sigma)N\rho(\sigma)^{-1} = \#k^{-v_K(\sigma)}N$. In fact, we have an equivalence of categories $\mathrm{WD} = \mathrm{WD}_{\zeta,\varphi}$ *from the category of continuous representations of G_K on finite-dimensional L-vector spaces to the category of bounded Weil–Deligne representations on finite-dimensional L-vector spaces, taking*

$$\rho \mapsto (V, r, N), \quad r(\tau) := \rho(\tau)\exp(-t_{\zeta,p}(\varphi^{-v_K(\tau)}\tau)N).$$

The functors $\mathrm{WD}_{\zeta',\varphi'}$ *and* $\mathrm{WD}_{\zeta,\varphi}$ *are naturally isomorphic.*

Remark 2.19. Note that since N is nilpotent, the exponential here is just a polynomial — there are no convergence issues!

The proof is contained in the following exercise.

Exercise 2.20. (1) By Exercise 2.4 there is a G_K-stable $\mathcal{O}_L$-lattice $\Lambda \subset V$. Show that if $G_{K'}$ is the kernel of the induced map $G_K \to \mathrm{Aut}(\Lambda/p\Lambda)$, then K'/K is a finite extension, and $\rho(G_{K'})$ is pro-p. Show that $\rho|_{I_{K'}}$ factors through $t_{\zeta,p} : I_{K'} \to \mathbb{Z}_p$.

(2) Choose $\sigma \in I_{K'}$ such that $t_{\zeta,p}(\sigma)$ topologically generates $t_{\zeta,p}(I_{K'})$. By considering the action of conjugation by φ, show that the eigenvalues of $\rho(\sigma)$ are all p-power roots of unity. Hence show that one may make a further finite extension K''/K' such that the elements of $\rho(I_{K''})$ are all unipotent.

(3) Deduce the existence of a unique nilpotent $N \in \mathrm{End}(V)$ such that for all $\sigma \in I_{K''}$, $\rho(\sigma) = \exp(Nt_{\zeta,p}(\sigma))$. [Hint: use the logarithm map (why are there no convergence issues?).]

(4) Complete the proof of the proposition, by showing that (r, N) is a Weil–Deligne representation. Where does the condition that r is bounded come in?

One significant advantage of Weil–Deligne representations over Galois representations is that there are no subtle topological issues: the topology on the Weil–Deligne representation is the discrete topology. This allows one to describe representations in a way that is "independent of L", and is necessary to make sense of the notion of a compatible system of Galois representations (or at least to make sense of it at places at which the Galois representation is ramified); see Definition 2.32 below.

2.21. ***Local representations with p = l: p-adic Hodge theory.*** The case $l = p$ is far more complicated than the case $l \neq p$, largely because wild inertia can act in a highly nontrivial fashion, so there is no simple analogue of Grothendieck's monodromy theorem. (There is still an analogue, though, it's just much harder to state and prove, and doesn't apply to all p-adic Galois representations.) The study of representations $G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ with $K/\mathbb{Q}_p$ finite is part of what is called *p-adic Hodge theory*, a subject initially developed by Fontaine in the 1980s. For an introduction to the part of p-adic Hodge theory concerned with Galois representations, the reader could consult [Berger 2004]. There is a lot more to p-adic Hodge theory than the study of Galois representations, and an excellent overview of some recent developments in the more geometric part of the theory can be found in [Bhatt 2021]. We will content ourselves with some terminology, some definitions, and some remarks intended to give intuition and motivation.

Fix $K/\mathbb{Q}_p$ finite. In some sense, "most" p-adic Galois representations $G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ will not be relevant for us, because they do not arise in geometry, or in the Galois representations associated to automorphic representations. Instead, there is a hierarchy of classes of representations

$$\{\text{crystalline}\} \subsetneq \{\text{semistable}\} \subsetneq \{\text{de Rham}\} \subsetneq \{\text{Hodge–Tate}\}.$$

For any of these classes X, we say that ρ is *potentially* X if there is a finite extension K'/K such that $\rho|_{G_{K'}}$ is X. A representation is potentially de Rham if and only if it is de Rham, and potentially Hodge–Tate if and only if it is Hodge–Tate; the corresponding statements for crystalline and semistable representations are false, as we will see concretely in the case $n = 1$ later on. The p-adic analogue of Grothendieck's monodromy theorem is the following deep theorem of Berger.

Theorem 2.22 (the p-adic monodromy theorem). *A representation is de Rham if and only if it is potentially semistable.*

The notion of a de Rham representation is designed to capture the representations arising in geometry; it does so by the following result of Tsuji (building on the work of many people).

Theorem 2.23. *If X/K is a smooth projective variety, then each $H^i_{\text{ét}}(X \times_K \overline{K}, \overline{\mathbb{Q}}_p)$ is a de Rham representation.*

Similarly, the definitions of crystalline and semistable are designed to capture the notions of good and semistable reduction, and one has (again as a consequence of Tsuji's work); see Section 2.5 of [Berger 2004].

Theorem 2.24. *If X/K is a smooth projective variety with good (respectively, semistable) reduction, then each $H^i_{\text{ét}}(X \times_K \overline{K}, \overline{\mathbb{Q}}_p)$ is a crystalline (respectively, semistable) representation.*

Thus the p-adic monodromy theorem can be thought of as a Galois-theoretic incarnation of Grothendieck's semistable reduction theorem.

The case that $n = 1$ is particularly simple, as we now explain. In this case, every semistable character is crystalline, and the de Rham characters are exactly the Hodge–Tate characters. In the case $K = \mathbb{Q}_p$, these are precisely the characters whose restrictions to inertia are of the form $\psi\varepsilon_p^m$ where ψ has finite order and $m \in \mathbb{Z}$, while the crystalline characters are those for which ψ is trivial. A similar description exists for general K, with ε_p^m replaced by a product of so-called *Lubin–Tate characters*.

Fact 2.25. A character $\chi : G_K \to \overline{\mathbb{Q}}_p^\times$ is de Rham if and only if there is an open subgroup U of $K^\times$ and an integer n_τ for each $\tau : K \hookrightarrow \overline{\mathbb{Q}}_p$ such that $(\chi \circ \mathrm{Art}_K)(\alpha) = \prod_\tau \tau(\alpha)^{-n_\tau}$ for each $\alpha \in U$, and it is crystalline if and only if we can take $U = \mathcal{O}_K^\times$. See Exercise 6.4.3 of [Brinon and Conrad 2009].

As soon as $n > 1$, there are noncrystalline semistable representations, and non-de Rham Hodge–Tate representations. A useful heuristic when comparing to the $l \neq$

p case is that crystalline representations correspond to unramified representations, semistable representations correspond to representations for which inertia acts unipotently, and de Rham representations correspond to all representations.

Suppose that $\rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ is a Hodge–Tate representation. Then for each $\tau : K \hookrightarrow \overline{\mathbb{Q}}_p$ there is a multiset of *τ-labeled Hodge–Tate weights* (defined for example in the notation section of [Barnet-Lamb et al. 2014], where they are called "Hodge–Tate numbers") $\mathrm{HT}_\tau(\rho)$ associated to ρ; this is a multiset of integers, and in the case of a de Rham character χ as above, $\mathrm{HT}_\tau(\chi) = n_\tau$. In particular, the p-adic cyclotomic character ε_p has all Hodge–Tate weights equal to -1. If K'/K is a finite extension, and $\tau' : K' \hookrightarrow \overline{\mathbb{Q}}_p$ extends $\tau : K \hookrightarrow \overline{\mathbb{Q}}_p$, then

$$\mathrm{HT}_{\tau'}(\rho|_{G_{K'}}) = \mathrm{HT}_\tau(\rho).$$

If furthermore ρ is potentially semistable (equivalently, de Rham) then a construction of Fontaine associates a Weil–Deligne representation $\mathrm{WD}(\rho) = (r, N)$ of W_K to ρ. If K'/K is a finite extension, then $\mathrm{WD}(\rho|_{G_{K'}}) = (r|_{W_{K'}}, N)$. It is known that ρ is semistable if and only if r is unramified, and that ρ is crystalline if and only if r is unramified and $N = 0$. Thus ρ is potentially crystalline if and only $N = 0$.

2.26. ***Number fields.*** We now consider the case that K is a number field (that is, a finite extension of $\mathbb{Q}$). If v is a finite place of K, we let K_v denote the completion of K at v. If K'/K is a finite Galois extension, then $\mathrm{Gal}(K'/K)$ transitively permutes the places of K' above v; if we choose one such place w, then we define the *decomposition group*

$$\mathrm{Gal}(K'/K)_w := \{\sigma \in \mathrm{Gal}(K'/K) \mid w\sigma = w\}.$$

Then we have a natural isomorphism $\mathrm{Gal}(K'/K)_w \xrightarrow{\sim} \mathrm{Gal}(K'_w/K_v)$, and since $\mathrm{Gal}(K'/K)_{w\sigma} = \sigma^{-1}\,\mathrm{Gal}(K'/K)_w\sigma$, we see that the definition extends to general algebraic extensions, and in particular we have an embedding $G_{K_v} \hookrightarrow G_K$ which is well-defined up to conjugacy (alternatively, up to a choice of embedding $\overline{K} \hookrightarrow \overline{K}_v$). (Note that you need to be slightly careful with taking completions in the case that K'/K is infinite, as then the extension K'_w/K_v need not be algebraic; we can for example define $\mathrm{Gal}(K'_w/K_v)$ to be the group of continuous automorphisms of K'_w which fix K_v pointwise.)

If K'/K is Galois and unramified at v, and w is a place of K' lying over v, then we define

$$\mathrm{Frob}_w := \mathrm{Frob}_{K_v} \in \mathrm{Gal}(K'_w/K_v) \xrightarrow{\sim} \mathrm{Gal}(K'/K)_w \hookrightarrow \mathrm{Gal}(K'/K).$$

We have $\mathrm{Frob}_{w\sigma} = \sigma^{-1}\,\mathrm{Frob}_w\,\sigma$, and thus a well-defined conjugacy class $[\mathrm{Frob}_v] = \{\mathrm{Frob}_w\}_{w\,|\,v}$ in $\mathrm{Gal}(K'/K)$.

Fact 2.27 (Chebotarev density theorem). If K'/K is a Galois extension which is unramified outside of a finite set S of places of K, then the union of the conjugacy classes $[\mathrm{Frob}_v]$, $v \notin S$ is dense in $\mathrm{Gal}(K'/K)$.

We briefly recall a statement of global class field theory. Let $\mathbb{A}_K$ denote the adeles of K, and write $K_\infty = \prod_{v \mid \infty} K_v$. Let $K^{\mathrm{ab}} = \overline{K}^{[G_K, G_K]}$ be the maximal abelian extension of K. Then there is a homomorphism $\mathrm{Art}_K : \mathbb{A}_K^\times/(K_\infty^\times)^\circ \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, defined in the following way: for each finite place v of K, the restriction of Art_K to $K_v^\times$ agrees with the local Artin maps Art_{K_v}, and similarly at the infinite places, it agrees with the obvious isomorphisms $\mathrm{Art}_{K_v} : K_v^\times/(K_v^\times)^\circ \xrightarrow{\sim} \mathrm{Gal}(\overline{K}_v/K_v)$. (In both cases, the symbol ° refers to the connected component of the identity.) Then global class field theory states that Art_K induces an isomorphism

$$\mathrm{Art}_K : \mathbb{A}_K^\times/\overline{K^\times(K_\infty^\times)^\circ} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

The global Galois representations that we will care about are those that Fontaine and Mazur call *geometric*. Let $L/\mathbb{Q}_p$ be an algebraic extension.

Definition 2.28. If K is a number field, then a continuous representation $\rho : G_K \to \mathrm{GL}_n(L)$ is *geometric* if it is unramified outside of a finite set of places of K, and if for each place $v \mid p$, $\rho|_{G_{K_v}}$ is de Rham.

Remark 2.29. It is known that both conditions are necessary; that is, there are examples of representations which are unramified outside of a finite set of places of K but not de Rham at places lying over p, and examples of representations which are de Rham at all places lying over p, but are ramified at infinitely many places. (As we will see in Theorem 2.43, these examples require $n > 1$.)

In practice (and conjecturally always), geometric Galois representations arise as part of a *compatible system* of Galois representations. There are a number of different definitions of a compatible system in the literature, all of which are conjecturally equivalent (although proving the equivalence of the definitions is probably very hard). The following definition, taken from [Barnet-Lamb et al. 2014], is simultaneously a strong enough set of assumptions under which one can hope to employ automorphy lifting theorems to study a compatible system, and is weak enough that the conditions can be verified in interesting examples.

Definition 2.30. Suppose that K and M are number fields, that S is a finite set of places of K and that n is a positive integer. By a *weakly compatible system* of n-dimensional p-adic representations (for varying p) of G_K defined over M and unramified outside S we mean a family of continuous semisimple representations

$$r_\lambda : G_K \to \mathrm{GL}_n(\overline{M}_\lambda),$$

where λ runs over the finite places of M, with the following properties:

- If $v \notin S$ is a finite place of K, then for all λ not dividing the residue characteristic of v, the representation r_λ is unramified at v and the characteristic polynomial of $r_\lambda(\mathrm{Frob}_v)$ lies in $M[X]$ and is independent of λ.
- Each representation r_λ is de Rham at all places above the residue characteristic of λ, and in fact crystalline at any place $v \notin S$ which divides the residue characteristic of λ.
- For each embedding $\tau : K \hookrightarrow \overline{M}$ the τ-labeled Hodge–Tate weights of r_λ are independent of λ.

Remark 2.31. By the Chebotarev density theorem and the Brauer–Nesbitt theorem, each r_λ is determined by the characteristic polynomials of the $r_\lambda(\mathrm{Frob}_v)$ for $v \notin S$, and in particular the compatible system is determined by a single r_λ. Note that for a general element $\sigma \in G_K$, there will be no relationship between the characteristic polynomials of the $r_\lambda(\sigma)$ as λ varies (and they won't even lie in $M[X]$, so there will be no way of comparing them).

There are various other properties one could demand; for example, we have the following definition (again following [Barnet-Lamb et al. 2014], although we have slightly strengthened the definition made there by allowing λ to divide the residue characteristic of v).

Definition 2.32. We say that a weakly compatible system is *strictly compatible* if for each finite place v of K there is a Weil–Deligne representation WD_v of W_{K_v} over $\overline{M}$ such that for each finite place λ of M and every M-linear embedding $\varsigma : \overline{M} \hookrightarrow \overline{M}_\lambda$ we have $\varsigma\, \mathrm{WD}_v \cong \mathrm{WD}(r_\lambda|_{G_{K_v}})^{\text{F-ss}}$.

Conjecturally, every weakly compatible system is strictly compatible, and even satisfies further properties, such as purity; see, e.g., Section 5 of [Barnet-Lamb et al. 2014]. We also have the following consequence of the Fontaine–Mazur conjecture (Conjecture 2.38 below) and standard conjectures on the étale cohomology of algebraic varieties over number fields.

Conjecture 2.33. *Any semisimple geometric representation* $G_K \to \mathrm{GL}_n(L)$ *is part of a strictly compatible system of Galois representations.*

In practice, most progress on understanding these conjectures has been made by using automorphy lifting theorems to prove special cases of the following conjecture.

Conjecture 2.34. *Any weakly compatible system of Galois representations is strictly compatible, and is in addition automorphic, in the sense that there is an algebraic automorphic representation* (*in the sense of* [Clozel 1990]) π *of* $\mathrm{GL}_n(\mathbb{A}_K)$ *with the property that* $\mathrm{WD}_v \cong \mathrm{rec}_{K_v}(\pi_v|\det|^{(1-n)/2})$ *for each finite place* v *of* K, *where* rec_{K_v} *is the local Langlands correspondence as in Section 4.1 below.*

2.35. ***Sources of Galois representations.*** The main source (and conjecturally the only source) of compatible systems of Galois representations is the étale cohomology of algebraic varieties. We have the following result, a consequence of Theorem 2.23 and "independence of l" results in étale cohomology [Katz and Messing 1974].

Theorem 2.36. *Let K be a number field, and let X/K be a smooth projective variety. Then for any i, j, the $H^i_{\text{ét}}(X \times_K \overline{K}, \mathbb{Q}_p)^{\text{ss}}(j)$ (the (j) denoting a Tate twist) form a weakly compatible system (defined over $\mathbb{Q}$) as p varies.*

Remark 2.37. Conjecturally, it is a strictly compatible system, and there is no need to semisimplify the representations. Both of these properties are known if X is an abelian variety; see Section 2.4 of [Fontaine 1994].

Conjecture 2.38 (the Fontaine–Mazur conjecture [Fontaine and Mazur 1995]). *Any irreducible geometric representation $\rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ is (the extension of scalars to $\overline{\mathbb{Q}}_p$ of) a subquotient of a representation arising from étale cohomology as in Theorem 2.36.*

Remark 2.39. The *Fontaine–Mazur–Langlands conjecture* is a somewhat ill-defined conjecture, which is essentially the union of Conjectures 2.33 and 2.34, expressing the expectation that an irreducible geometric Galois representation is automorphic.

When $n = 1$, all of these conjectures are essentially known, as we will now explain. For $n > 1$, we know very little (although the situation when $K = \mathbb{Q}$ and $n = 2$ is pretty good), and the main results that are known are as a consequence of automorphy lifting theorems (as discussed in these notes) and of potential automorphy theorems (which are not discussed in these notes, but should be accessible given the material we develop here; for a nice introduction, see [Buzzard 2012]).

Definition 2.40. A *Grössencharacter* is a continuous character $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$. We say that χ is *algebraic* (or "type A_0") if for each $\tau : K \hookrightarrow \mathbb{C}$ there is an integer n_τ, such that for each $\alpha \in (K_\infty^\times)^\circ$, we have $\chi(\alpha) = \prod_\tau (\tau(\alpha))^{-n_\tau}$.

Definition 2.41. Let L be a field of characteristic zero such that for each embedding $\tau : K \hookrightarrow \bar{L}$, we have $\tau(K) \subseteq L$. Then an *algebraic character* $\chi_0 : \mathbb{A}_K^\times \to \bar{L}^\times$ is a character with open kernel such that for each $\tau : K \hookrightarrow L$ there is an integer n_τ with the property that for all $\alpha \in K^\times$, we have $\chi_0(\alpha) = \prod_\tau (\tau(\alpha))^{n_\tau}$.

Exercise 2.42. Show that if χ_0 is an algebraic character, then χ_0 takes values in some number field. [Hint: show that $\mathbb{A}_K^\times / (K^\times \ker \chi_0)$ is finite, and that $\chi_0(K^\times \ker \chi_0)$ is contained in a number field.]

Theorem 2.43. *Let E be a number field containing the normal closure of K. Fix embeddings $\iota_\infty : \bar{E} \hookrightarrow \mathbb{C}$, $\iota_p : \bar{E} \hookrightarrow \overline{\mathbb{Q}}_p$. Then the following are in natural bijection:*

(1) *Algebraic characters $\chi_0 : \mathbb{A}_K^\times \to \bar{E}^\times$.*

(2) *Algebraic Grössencharacters $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$.*

(3) *Continuous representations* $\rho : G_K \to \overline{\mathbb{Q}}_p^\times$ *which are de Rham at all* $v \mid p$.

(4) *Geometric representations* $\rho : G_K \to \overline{\mathbb{Q}}_p^\times$.

Exercise 2.44. Prove Theorem 2.43 as follows; see, e.g., Section 1 of [Fargues 2011] for more details. Firstly, use Fact 2.25, together with global class field theory, to show that (3) and (4) are equivalent. For the correspondence between (1) and (2), show that we can pair up χ_0 and χ by

$$\chi(\alpha) = \iota_\infty\Biggl(\chi_0(\alpha) \prod_{\tau : K \hookrightarrow \mathbb{C}} \tau(\alpha_\infty)^{-n_{\iota_\infty^{-1}\tau}}\Biggr).$$

For the correspondence between (1) and (3), show that we can pair up χ_0 and ρ by

$$(\rho \circ \mathrm{Art}_K)(\alpha) = \iota_p\Biggl(\chi_0(\alpha) \prod_{\tau : K \hookrightarrow \overline{\mathbb{Q}}_p} \tau(\alpha_p)^{-n_{\iota_p^{-1}\tau}}\Biggr).$$

3. Galois deformations

The “lifting” in “modularity lifting theorems” refers to deducing the modularity of a p-adic Galois representation from the modularity of its reduction modulo p; so we “lift” the modularity property from characteristic p to characteristic zero. In this section we consider the Galois-theoretic aspects of this lifting, which are usually known as “Galois deformation theory”.

There are a number of good introductions to the material in this section, and for the most part we will simply give basic definitions and motivation, and refer elsewhere for proofs. In particular, [Mazur 1997] is a very nice introduction to Galois deformations (although slightly out of date, as it does not treat liftings/framed deformations), and [Böckle 2013] is a thorough modern treatment.

3.1. ***Generalities.*** Take $L/\mathbb{Q}_p$ finite with ring of integers $\mathcal{O} = \mathcal{O}_L$ and maximal ideal λ, and write $\mathbb{F} = \mathcal{O}/\lambda$. Let G be a profinite group which satisfies the following condition (Mazur’s condition Φ_p): for each open subgroup Δ of G, then $\Delta/\langle[\Delta, \Delta], \Delta^p\rangle$ is finite. Equivalently (see, e.g., Exercise 1.8.1 of [Böckle 2013]), for each Δ the maximal pro-p quotient of Δ is topologically finitely generated. If G is topologically finitely generated, then Φ_p holds, but we will need to use the condition for some G (the global Galois groups $G_{K,S}$ defined below) which are not known to be topologically finitely generated.

In particular, using class field theory or Kummer theory, it can be checked that Φ_p holds if $G = G_K = \mathrm{Gal}(\overline{K}/K)$ for some prime l (possibly equal to p) and some finite extension $K/\mathbb{Q}_l$, or if $G = G_{K,S} = \mathrm{Gal}(K_S/K)$ where K is a number field, S is a finite set of finite places of K, and K_S/K is the maximal extension unramified outside of S and the infinite places; see, e.g., the proof of Theorem 2.41 of [Darmon et al. 1997].

Fix a continuous representation $\bar{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$. Let $\mathcal{C}_{\mathcal{O}}$ be the category of complete local Noetherian $\mathcal{O}$-algebras with residue field $\mathbb{F}$, and consider the functor $\mathcal{C}_{\mathcal{O}} \to \underline{Sets}$ which sends A to the set of continuous representations $\rho : G \to \mathrm{GL}_n(A)$ such that $\rho \bmod \mathfrak{m}_A = \bar{\rho}$ (that is, to the set of *lifts* of $\bar{\rho}$ to A).

Lemma 3.2. *This functor is represented by a representation* $\rho^{\square} : G \to \mathrm{GL}_n(R^{\square}_{\bar{\rho}})$.

Proof. This is straightforward; see Proposition 1.3.1(a) of [Böckle 2013] for a closely related result (showing the prorepresentability of the functor restricted to Artinian algebras), or to [Dickinson 2001a] for a complete proof of a more general result. □

Definition 3.3. We say that $R^{\square}_{\bar{\rho}}$ is the *universal lifting ring* (or in Kisin's terminology, the *universal framed deformation ring*). We say that $\rho^{\square}$ is the *universal lifting* of $\bar{\rho}$.

If $\mathrm{End}_{\mathbb{F}[G]}\,\bar{\rho} = \mathbb{F}$ we will say that $\bar{\rho}$ is *Schur*. By Schur's lemma, if $\bar{\rho}$ is absolutely irreducible, then $\bar{\rho}$ is Schur. In this case, there is a very useful (and historically earlier) variant on the above construction.

Definition 3.4. Suppose that $\bar{\rho}$ is Schur. Then a *deformation* of $\bar{\rho}$ to $A \in \mathrm{ob}\,\mathcal{C}_{\mathcal{O}}$ is an equivalence class of liftings, where $\rho \sim \rho'$ if and only if $\rho' = a\rho a^{-1}$ for some $a \in \ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}))$ (or equivalently, for some $a \in \mathrm{GL}_n(A)$).

Lemma 3.5. *If $\bar{\rho}$ is Schur, then the functor $\mathcal{C}_{\mathcal{O}} \to \underline{Sets}$ sending A to the set of deformations of $\bar{\rho}$ to A is representable by some* $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R^{\mathrm{univ}}_{\bar{\rho}})$.

Proof. See Proposition 1.3.1(b) of [Böckle 2013], or Theorem 2.36 of [Darmon et al. 1997] for a more hands-on approach. □

Definition 3.6. We say that ρ^{univ} (or more properly, its equivalence class) is the *universal deformation* of $\bar{\rho}$, and $R^{\mathrm{univ}}_{\bar{\rho}}$ is the *universal deformation ring*.

Deformations are representations considered up to conjugation, so it is reasonable to hope that deformations can be studied by considering their traces. In the case that $\bar{\rho}$ is absolutely irreducible, universal deformations are determined by traces in the following rather strong sense. This result is essentially due to Carayol [1994].

Lemma 3.7. *Suppose that $\bar{\rho}$ is absolutely irreducible. Let R be an object of $\mathcal{C}_{\mathcal{O}}$, and $\rho : G \to \mathrm{GL}_n(R)$ a lifting of $\bar{\rho}$*:

(1) *If $a \in \mathrm{GL}_n(R)$ and $a\rho a^{-1} = \rho$ then $a \in R^{\times}$.*

(2) *If $\rho' : G \to \mathrm{GL}_n(R)$ is another continuous lifting of $\bar{\rho}$ and $\mathrm{tr}\,\rho = \mathrm{tr}\,\rho'$, then there is some $a \in \ker(\mathrm{GL}_n(R) \to \mathrm{GL}_n(\mathbb{F}))$ such that $\rho' = a\rho a^{-1}$.*

(3) *If $S \subseteq R$ is a closed subring with $S \in \mathrm{ob}\,\mathcal{C}_{\mathcal{O}}$ and $\mathfrak{m}_S = \mathfrak{m}_R \cap S$, and if $\mathrm{tr}\,\rho(G) \subseteq S$, then there is some $a \in \ker(\mathrm{GL}_n(R) \to \mathrm{GL}_n(\mathbb{F}))$ such that $a\rho a^{-1} : G \to \mathrm{GL}_n(S)$.*

Proof. See Lemmas 2.1.8 and 2.1.10 of [Clozel et al. 2008], or Theorem 2.2.1 of [Böckle 2013]. □

Exercise 3.8. Deduce from Lemma 3.7 that if $\bar{\rho}$ is absolutely irreducible, then $R^{\mathrm{univ}}_{\bar{\rho}}$ is topologically generated over $\mathcal{O}$ by the values $\operatorname{tr} \rho^{\mathrm{univ}}(g)$ as g runs over any dense subset of G.

Exercise 3.9. Show that if $\bar{\rho}$ is absolutely irreducible, then $R^{\square}_{\bar{\rho}}$ is isomorphic to a power series ring in (n^2-1) variables over $R^{\mathrm{univ}}_{\bar{\rho}}$. Hint: let ρ^{univ} be a choice of universal deformation, and consider the homomorphism

$$\rho^{\square} : G \to \mathrm{GL}_n(R^{\mathrm{univ}}_{\bar{\rho}}[\![X_{i,j}]\!]_{i,j=1,\dots,n}/(X_{1,1}))$$

given by $\rho^{\square} = (1_n + (X_{i,j}))\rho^{\mathrm{univ}}(1_n + (X_{i,j}))^{-1}$. Show that this is the universal lifting.

3.10. *Tangent spaces.* The tangent spaces of universal lifting and deformation rings have a natural interpretation in terms of liftings and deformations to the ring of dual numbers, $\mathbb{F}[\varepsilon]/(\varepsilon^2)$.

Exercise 3.11. Show that we have natural bijections between:

(1) $\mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}_{R^{\square}_{\bar{\rho}}}/(\mathfrak{m}^2_{R^{\square}_{\bar{\rho}}}, \lambda), \mathbb{F})$.

(2) $\mathrm{Hom}_{\mathcal{O}}(R^{\square}_{\bar{\rho}}, \mathbb{F}[\varepsilon]/(\varepsilon^2))$.

(3) The set of liftings of $\bar{\rho}$ to $\mathbb{F}[\varepsilon]/(\varepsilon^2)$.

(4) The set of cocycles $Z^1(G, \operatorname{ad}\bar{\rho})$.

Show that if $\bar{\rho}$ is absolutely irreducible, then we also have a bijection between $\mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}_{R^{\mathrm{univ}}_{\bar{\rho}}}/(\mathfrak{m}^2_{R^{\mathrm{univ}}_{\bar{\rho}}}, \lambda), \mathbb{F})$ and $H^1(G, \operatorname{ad}\bar{\rho})$.

Hint: given $f \in \mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}_{R^{\square}_{\bar{\rho}}}/(\mathfrak{m}^2_{R^{\square}_{\bar{\rho}}}, \lambda), \mathbb{F})$, define an element of $\mathrm{Hom}_{\mathcal{O}}(R^{\square}_{\bar{\rho}}, \mathbb{F}[\varepsilon]/(\varepsilon^2))$ by sending $a + x$ to $a + f(x)\varepsilon$ whenever $a \in \mathcal{O}$ and $x \in \mathfrak{m}_{R^{\square}_{\bar{\rho}}}$. Given a cocycle $\phi \in Z^1(G, \operatorname{ad}\bar{\rho})$, define a lifting $\rho : G \to \mathrm{GL}_n(\mathbb{F}[\varepsilon]/(\varepsilon^2))$ by $\rho(g) := (1 + \phi(g)\varepsilon)\bar{\rho}(g)$.

Corollary 3.12. *We have*

$$\dim_{\mathbb{F}} \mathfrak{m}_{R^{\square}_{\bar{\rho}}}/(\mathfrak{m}^2_{R^{\square}_{\bar{\rho}}}, \lambda) = \dim_{\mathbb{F}} H^1(G, \operatorname{ad}\bar{\rho}) + n^2 - \dim_{\mathbb{F}} H^0(G, \operatorname{ad}\bar{\rho}).$$

Proof. This follows from the exact sequence

$$0 \to (\operatorname{ad}\bar{\rho})^G \to \operatorname{ad}\bar{\rho} \to Z^1(G, \operatorname{ad}\bar{\rho}) \to H^1(G, \operatorname{ad}\bar{\rho}) \to 0. \qquad \square$$

In particular, if $d := \dim_{\mathbb{F}} Z^1(G, \operatorname{ad}\bar{\rho})$, then we can choose a surjection $\phi : \mathcal{O}[\![x_1, \dots, x_d]\!] \twoheadrightarrow R^{\square}_{\bar{\rho}}$. Similarly, if $\bar{\rho}$ is absolutely irreducible, we can choose a surjection $\phi' : \mathcal{O}[\![x_1, \dots, x_{d'}]\!] \twoheadrightarrow R^{\mathrm{univ}}_{\bar{\rho}}$, where $d' := \dim_{\mathbb{F}} H^1(G, \operatorname{ad}\bar{\rho})$.

Lemma 3.13. *If $J = \ker\phi$ or $J = \ker\phi'$, then there is an injection*

$$\mathrm{Hom}_{\mathbb{F}}(J/\mathfrak{m}J, \mathbb{F}) \hookrightarrow H^2(G, \operatorname{ad}\bar{\rho}),$$

where $\mathfrak{m}$ denotes the maximal ideal of $\mathcal{O}[\![x_1, \dots, x_d]\!]$ or $\mathcal{O}[\![x_1, \dots, x_{d'}]\!]$ respectively.

Proof. See the proof of Proposition 2 of [Mazur 1989]. □

Corollary 3.14. *If $H^2(G, \operatorname{ad}\bar{\rho}) = 0$, then $R^{\square}_{\bar{\rho}}$ is formally smooth of relative dimension* $\dim_{\mathbb{F}} Z^1(G, \operatorname{ad}\bar{\rho})$ *over $\mathcal{O}$.*

In any case, the Krull dimension of $R^{\square}_{\bar{\rho}}$ is at least

$$1 + n^2 - \dim_{\mathbb{F}} H^0(G, \operatorname{ad}\bar{\rho}) + \dim_{\mathbb{F}} H^1(G, \operatorname{ad}\bar{\rho}) - \dim_{\mathbb{F}} H^2(G, \operatorname{ad}\bar{\rho}).$$

If $\bar{\rho}$ is absolutely irreducible, then the Krull dimension of $R^{\mathrm{univ}}_{\bar{\rho}}$ is at least

$$1 + \dim_{\mathbb{F}} H^1(G, \operatorname{ad}\bar{\rho}) - \dim_{\mathbb{F}} H^2(G, \operatorname{ad}\bar{\rho}).$$

3.15. ***Deformation conditions.*** In practice, we frequently want to impose additional conditions on the liftings and deformations we consider. For example, if we are trying to prove the Fontaine–Mazur conjecture, we would like to be able to restrict to global deformations which are geometric. There are various ways in which to impose extra conditions; we will use the formalism of *deformation problems* introduced in [Clozel et al. 2008].

Definition 3.16. By a *deformation problem* $\mathcal{D}$ we mean a collection of liftings (R, ρ) of $(\mathbb{F}, \bar{\rho})$ (with R an object of $\mathcal{C}_{\mathcal{O}}$), satisfying the following properties:

- $(\mathbb{F}, \bar{\rho}) \in \mathcal{D}$.
- If $f : R \to S$ is a morphism in $\mathcal{C}_{\mathcal{O}}$ and $(R, \rho) \in \mathcal{D}$, then $(S, f \circ \rho) \in \mathcal{D}$.
- If $f : R \hookrightarrow S$ is an injective morphism in $\mathcal{C}_{\mathcal{O}}$ then $(R, \rho) \in \mathcal{D}$ if and only if $(S, f \circ \rho) \in \mathcal{D}$.
- Suppose that $R_1, R_2 \in \operatorname{ob}\mathcal{C}_{\mathcal{O}}$ and I_1, I_2 are closed ideals of R_1, R_2 respectively such that there is an isomorphism $f : R_1/I_1 \xrightarrow{\sim} R_2/I_2$. Suppose also that $(R_1, \rho_1), (R_2, \rho_2) \in \mathcal{D}$, and that $f(\rho_1 \bmod I_1) = \rho_2 \bmod I_2$. Then $(\{(a, b) \in R_1 \oplus R_2 : f(a \bmod I_1) = b \bmod I_2\}, \rho_1 \oplus \rho_2) \in \mathcal{D}$.
- If (R, ρ) is a lifting of $(\mathbb{F}, \bar{\rho})$ and $I_1 \supset I_2 \supset \cdots$ is a sequence of ideals of R with $\cap_j I_j = 0$, and $(R/I_j, \rho \bmod I_j) \in \mathcal{D}$ for all j, then $(R, \rho) \in \mathcal{D}$.
- If $(R, \rho) \in \mathcal{D}$ and $a \in \ker(\mathrm{GL}_n(R) \to \mathrm{GL}_n(\mathbb{F}))$, then $(R, a\rho a^{-1}) \in \mathcal{D}$.

In practice, when we want to impose a condition on our deformations, it will be easy to see that it satisfies these requirements. (An exception is that these properties are hard to check for certain conditions arising in p-adic Hodge theory, but we won't need those conditions in these notes.)

The relationship of this definition to the universal lifting ring is as follows. Note that each element $a \in \ker(\mathrm{GL}_n(R^{\square}_{\bar{\rho}}) \to \mathrm{GL}_n(\mathbb{F}))$ acts on $R^{\square}_{\bar{\rho}}$, via the universal property and by sending $\rho^{\square}$ to $a^{-1}\rho^{\square}a$. [Warning: this *isn't* a group action, though!]

Lemma 3.17. (1) *If $\mathcal{D}$ is a deformation problem then there is a* $\ker(\mathrm{GL}_n(R^{\square}_{\bar\rho}) \to \mathrm{GL}_n(\mathbb{F}))$*-invariant ideal $I(\mathcal{D})$ of $R^{\square}_{\bar\rho}$ such that $(R, \rho) \in \mathcal{D}$ if and only if the map $R^{\square}_{\bar\rho} \to R$ induced by ρ factors through the quotient $R^{\square}_{\bar\rho}/I(\mathcal{D})$.*

(2) *Let $\tilde{L}(\mathcal{D}) \subseteq Z^1(G, \operatorname{ad}\bar\rho) \cong \operatorname{Hom}(\mathfrak{m}_{R^{\square}_{\bar\rho}}/(\lambda, \mathfrak{m}^2_{R^{\square}_{\bar\rho}}), \mathbb{F})$ denote the annihilator of the image of $I(\mathcal{D})$ in $\mathfrak{m}_{R^{\square}_{\bar\rho}}/(\lambda, \mathfrak{m}^2_{R^{\square}_{\bar\rho}})$. Then $\tilde{L}(\mathcal{D})$ is the preimage of some subspace $L(\mathcal{D}) \subseteq H^1(G, \operatorname{ad}\bar\rho)$.*

(3) *If I is a* $\ker(\mathrm{GL}_n(R^{\square}_{\bar\rho}) \to \mathrm{GL}_n(\mathbb{F}))$*-invariant ideal of $R^{\square}_{\bar\rho}$ with $\sqrt{I} = I$ and $I \neq \mathfrak{m}_{R^{\square}_{\bar\rho}}$, then*

$$\mathcal{D}(I) := \{(R, \rho) : R^{\square}_{\bar\rho} \to R \text{ factors through } R^{\square}_{\bar\rho}/I\}$$

is a deformation problem. Furthermore, we have $I(\mathcal{D}(I)) = I$ and $\mathcal{D}(I(\mathcal{D})) = \mathcal{D}$.

Proof. See Lemma 2.2.3 of [Clozel et al. 2008] and Lemma 3.2 of [Barnet-Lamb et al. 2011] (and for (2), use that $I(\mathcal{D})$ is $\ker(\mathrm{GL}_n(R^{\square}_{\bar\rho}) \to \mathrm{GL}_n(\mathbb{F}))$-invariant). □

3.18. ***Fixing determinants.*** For technical reasons, we will want to fix the determinants of our Galois representations; see Remark 5.12 of [Calegari and Geraghty 2018]. To this end, let $\chi : G \to \mathcal{O}^\times$ be a continuous homomorphism such that $\chi \bmod \lambda = \det\bar\rho$. Then it makes sense to ask that a lifting has determinant χ, and we can define a universal lifting ring $R^{\square}_{\bar\rho,\chi}$ for lifts with determinant χ, and when $\bar\rho$ is Schur, a universal fixed determinant deformation ring $R^{\mathrm{univ}}_{\bar\rho,\chi}$.

Exercise 3.19. Check that the material developed in the previous section goes over unchanged, except that $\operatorname{ad}\bar\rho$ needs to be replaced with $\operatorname{ad}^0\bar\rho := \{x \in \operatorname{ad}\bar\rho : \operatorname{tr} x = 0\}$.

Note that since we are assuming throughout that $p \nmid n$, $\operatorname{ad}^0\bar\rho$ is a direct summand of $\operatorname{ad}\bar\rho$ (as a G-representation).

3.20. ***Global deformations with local conditions.*** Now fix a finite set S, and for each $v \in S$, a profinite group G_v satisfying Φ_p, together with a continuous homomorphism $G_v \to G$, and a deformation problem $\mathcal{D}_v$ for $\bar\rho|_{G_v}$. [In applications, G will be a global Galois group, and the G_v will be decomposition groups at finite places.]

Also fix $\chi : G \to \mathcal{O}^\times$, a continuous homomorphism such that $\chi \bmod \lambda = \det\bar\rho$. Assume that $\bar\rho$ is absolutely irreducible, and fix some subset $T \subseteq S$.

Definition 3.21. Fix $A \in \operatorname{ob}\mathcal{C}_{\mathcal{O}}$. A *$T$-framed deformation* of $\bar\rho$ of *type* $\mathcal{S} := (S, \{\mathcal{D}_v\}_{v\in S}, \chi)$ to A is an equivalence class of tuples $(\rho, \{\alpha_v\}_{v\in T})$, where $\rho : G \to \mathrm{GL}_n(A)$ is a lift of $\bar\rho$ such that $\det\rho = \chi$ and $\rho|_{G_v} \in \mathcal{D}_v$ for all $v \in S$, and α_v is an element of $\ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}))$.

The equivalence relation is defined by decreeing that for each $\beta \in \ker(\mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}))$, we have $(\rho, \{\alpha_v\}_{v\in T}) \sim (\beta\rho\beta^{-1}, \{\beta\alpha_v\}_{v\in T})$.

The point of considering T-framed deformations is that it allows us to study absolutely irreducible representations $\bar{\rho}$ for which some of the $\bar{\rho}|_{G_v}$ are reducible, because if $(\rho, \{\alpha_v\}_{v\in T})$ is a T-framed deformation of type $\mathcal{S}$, then $\alpha_v^{-1}\rho|_{G_v}\alpha_v$ is a well-defined element of $\mathcal{D}_v$ (independent of the choice of representative of the equivalence class). The following lemma should be unsurprising.

Lemma 3.22. *The functor $\mathcal{C}_{\mathcal{O}} \to \underline{\mathrm{Sets}}$ sending A to the set of T-framed deformations of $\bar{\rho}$ of type $\mathcal{S}$ is represented by a universal object $\rho^{\square_T} : G \to \mathrm{GL}_n(R_{\mathcal{S}}^{\square_T})$.*

Proof. See Proposition 2.2.9 of [Clozel et al. 2008]. □

If $T = \varnothing$ then we will write $R_{\mathcal{S}}^{\mathrm{univ}}$ for $R_{\mathcal{S}}^{\square_T}$.

3.23. ***Presenting global deformation rings over local lifting rings.*** Continue to use the notation of the previous subsection. Since $\alpha_v^{-1}\rho^{\square_T}|_{G_v}\alpha_v$ is a well-defined element of $\mathcal{D}_v$, we have a tautological homomorphism $R^{\square}_{\bar{\rho}|_{G_v},\chi}/I(\mathcal{D}_v) \to R_{\mathcal{S}}^{\square_T}$. Define

$$R^{\mathrm{loc}}_{\mathcal{S},T} := \widehat{\bigotimes}_{v\in T}(R^{\square}_{\bar{\rho}|_{G_v},\chi}/I(\mathcal{D}_v)).$$

Then we have a natural map $R^{\mathrm{loc}}_{\mathcal{S},T} \to R_{\mathcal{S}}^{\square_T}$.

We now generalize Corollary 3.14 by considering presentations of $R_{\mathcal{S}}^{\square_T}$ over $R^{\mathrm{loc}}_{\mathcal{S},T}$. In order to compute how many variables are needed to present $R_{\mathcal{S}}^{\square_T}$ over $R^{\mathrm{loc}}_{\mathcal{S},T}$, we must compute $\dim_{\mathbb{F}} \mathfrak{m}_{R_{\mathcal{S}}^{\square_T}}/(\mathfrak{m}^2_{R_{\mathcal{S}}^{\square_T}}, \mathfrak{m}_{R^{\mathrm{loc}}_{\mathcal{S},T}}, \lambda)$. Unsurprisingly, in order to compute this, we will compute a certain H^1.

We define a complex as follows. As usual, given a group G and an $\mathbb{F}[G]$-module M, we let $C^i(G, M)$ be the space of functions $G^i \to M$, and we let $\partial : C^i(G, M) \to C^{i+1}(G, M)$ be the usual coboundary map. We define a complex $C^i_{\mathcal{S},T,\mathrm{loc}}(G, \mathrm{ad}^0\bar{\rho})$ by

$$C^0_{\mathcal{S},T,\mathrm{loc}}(G, \mathrm{ad}^0\bar{\rho}) = \oplus_{v\in T}C^0(G_v, \mathrm{ad}\,\bar{\rho}) \oplus \oplus_{v\in S\setminus T}0,$$
$$C^1_{\mathcal{S},T,\mathrm{loc}}(G, \mathrm{ad}^0\bar{\rho}) = \oplus_{v\in T}C^1(G_v, \mathrm{ad}^0\bar{\rho}) \oplus \oplus_{v\in S\setminus T}C^1(G_v, \mathrm{ad}^0\bar{\rho})/\tilde{L}(\mathcal{D}_v),$$

and for $i \geq 2$,

$$C^i_{\mathcal{S},T,\mathrm{loc}}(G, \mathrm{ad}^0\bar{\rho}) = \oplus_{v\in S}C^i(G_v, \mathrm{ad}^0\bar{\rho}).$$

Let $C^0_0(G, \mathrm{ad}^0\bar{\rho}) := C^0(G, \mathrm{ad}\,\bar{\rho})$, and set $C^i_0(G, \mathrm{ad}^0\bar{\rho}) = C^i(G, \mathrm{ad}^0\bar{\rho})$ for $i > 0$. Then we let $H^i_{\mathcal{S},T}(G, \mathrm{ad}^0\bar{\rho})$ denote the cohomology of the complex

$$C^i_{\mathcal{S},T}(G, \mathrm{ad}^0\bar{\rho}) := C^i_0(G, \mathrm{ad}^0\bar{\rho}) \oplus C^{i-1}_{\mathcal{S},T,\mathrm{loc}}(G, \mathrm{ad}^0\bar{\rho})$$

where the coboundary map is given by

$$(\phi, (\psi_v)) \mapsto (\partial\phi, (\phi|_{G_v} - \partial\psi_v)).$$

Then we have an exact sequence of complexes

$$0 \to C^{i-1}_{\mathcal{S},T,\mathrm{loc}}(G, \mathrm{ad}^0\bar{\rho}) \to C^i_{\mathcal{S},T}(G, \mathrm{ad}^0\bar{\rho}) \to C^i_0(G, \mathrm{ad}^0\bar{\rho}) \to 0,$$

and the corresponding long exact sequence in cohomology is

$$\begin{tikzcd}
0 \arrow[r] & H^0_{S,T}(G,\mathrm{ad}^0\bar\rho) \arrow[r] & H^0(G,\mathrm{ad}\bar\rho) \arrow[r] & \oplus_{v\in T}H^0(G_v,\mathrm{ad}\bar\rho) \arrow[dll, rounded corners] \\
 & H^1_{S,T}(G,\mathrm{ad}^0\bar\rho) \arrow[r] & H^1(G,\mathrm{ad}^0\bar\rho) \arrow[r] & \oplus_{v\in T}H^1(G_v,\mathrm{ad}^0\bar\rho)\oplus_{v\in S\setminus T}H^1(G_v,\mathrm{ad}^0\bar\rho)/L(\mathcal{D}_v) \arrow[dll, rounded corners] \\
 & H^2_{S,T}(G,\mathrm{ad}^0\bar\rho) \arrow[r] & H^2(G,\mathrm{ad}^0\bar\rho) \arrow[r] & \oplus_{v\in S}H^2(G_v,\mathrm{ad}^0\bar\rho) \arrow[dll, rounded corners] \\
 & H^3_{S,T}(G,\mathrm{ad}^0\bar\rho) \arrow[r] & \cdots &
\end{tikzcd}$$

Taking Euler characteristics, we see that if we define the negative Euler characteristic χ by $\chi(G,\mathrm{ad}^0\bar\rho)=\sum_i(-1)^{i-1}\dim_{\mathbb{F}}H^i(G,\mathrm{ad}^0\bar\rho)$, we have

$$\begin{aligned}\chi_{S,T}(G,\mathrm{ad}^0\bar\rho) = -1+\chi(G,\mathrm{ad}^0\bar\rho) - \sum_{v\in S}\chi(G_v,\mathrm{ad}^0\bar\rho)&\\ +\sum_{v\in T}(\dim_{\mathbb{F}}H^0(G_v,\mathrm{ad}\,\bar\rho)-\dim_{\mathbb{F}}H^0(G_v,\mathrm{ad}^0\bar\rho))&\\ +\sum_{v\in S\setminus T}(\dim_{\mathbb{F}}L(\mathcal{D}_v)-\dim_{\mathbb{F}}H^0(G_v,\mathrm{ad}^0\bar\rho)).&\end{aligned}$$

From now on for the rest of the notes, we specialize to the case that F is a number field, S is a finite set of finite places of F including all the places lying over p, and we set $G=G_{F,S}$, $G_v=G_{F_v}$ for $v\in S$. (Since $G=G_{F,S}$, note in particular that all deformations we are considering are unramified outside of S.) We then employ standard results on Galois cohomology that can be found in [Milne 2006]. In particular, we have $H^i(G_{F_v},\mathrm{ad}\,\bar\rho)=0$ if $i\ge 3$, and

$$H^i(G_{F,S},\mathrm{ad}^0\bar\rho)\cong\oplus_{v\ \mathrm{real}}H^i(G_{F_v},\mathrm{ad}^0\bar\rho)=0$$

if $i\ge 3$ (the vanishing of the local cohomology groups follows as $p>2$, so G_{F_v} has order coprime to that of $\mathrm{ad}^0\bar\rho$). Consequently, $H^i_{S,T}(G_{F,S},\mathrm{ad}^0\bar\rho)=0$ if $i>3$.

We now employ the local and global Euler characteristic formulas. For simplicity, assume from now on that T contains all the places of S lying over p. The global formula gives

$$\chi(G_{F,S},\mathrm{ad}^0\bar\rho)=-\sum_{v\,|\,\infty}\dim_{\mathbb{F}}H^0(G_{F_v},\mathrm{ad}^0\bar\rho)+[F:\mathbb{Q}](n^2-1),$$

and the local formula gives

$$\sum_{v\in S}\chi(G_{F_v},\mathrm{ad}^0\bar\rho)=\sum_{v\,|\,p}(n^2-1)[F_v:\mathbb{Q}_p]=(n^2-1)[F:\mathbb{Q}],$$

so that

$$\begin{aligned}&\chi_{\mathcal{S},T}(G_{F,S},\operatorname{ad}^0\bar{\rho})\\&=-1+\#T-\sum_{v\,|\,\infty}\dim_{\mathbb{F}}H^0(G_{F_v},\operatorname{ad}^0\bar{\rho})+\sum_{v\in S\setminus T}(\dim_{\mathbb{F}}L(\mathcal{D}_v)-\dim_{\mathbb{F}}H^0(G_{F_v},\operatorname{ad}^0\bar{\rho})).\end{aligned}$$

Assume now that $\bar{\rho}$ is absolutely irreducible; then $H^0(G_{F,S},\operatorname{ad}\bar{\rho})=\mathbb{F}$, so $H^0_{\mathcal{S},T}(G_{F,S},\operatorname{ad}^0\bar{\rho})=\mathbb{F}$. To say something sensible about $H^1_{\mathcal{S},T}(G_{F,S},\operatorname{ad}^0\bar{\rho})$ we still need to control the $H^2_{\mathcal{S},T}$ and $H^3_{\mathcal{S},T}$. Firstly, the above long exact sequence gives us in particular the exact sequence

$$\begin{tikzcd}
 & H^1(G_{F,S},\operatorname{ad}^0\bar{\rho}) \arrow[r] & \oplus_{v\in T}H^1(G_{F_v},\operatorname{ad}^0\bar{\rho})\oplus_{v\in S\setminus T}H^1(G_{F_v},\operatorname{ad}^0\bar{\rho})/L(\mathcal{D}_v) \arrow[dll, rounded corners] \\
H^2_{\mathcal{S},T}(G_{F,S},\operatorname{ad}^0\bar{\rho}) \arrow[r] & H^2(G_{F,S},\operatorname{ad}^0\bar{\rho}) \arrow[r] & \oplus_{v\in S}H^2(G_{F_v},\operatorname{ad}^0\bar{\rho}) \arrow[dll, rounded corners] \\
H^3_{\mathcal{S},T}(G_{F,S},\operatorname{ad}^0\bar{\rho}) \arrow[r] & 0. &
\end{tikzcd}$$

On the other hand, from the Poitou–Tate exact sequence [Milne 2006, Proposition 4.10, Chapter 1] we have an exact sequence

$$\begin{tikzcd}
H^1(G_{F,S},\operatorname{ad}^0\bar{\rho}) \arrow[r] & \oplus_{v\in S}H^1(G_{F_v},\operatorname{ad}^0\bar{\rho}) \arrow[r] & H^1(G_{F,S},(\operatorname{ad}^0\bar{\rho})^\vee(1))^\vee \arrow[dll, rounded corners] & \\
H^2(G_{F,S},\operatorname{ad}^0\bar{\rho}) \arrow[r] & \oplus_{v\in S}H^2(G_{F_v},\operatorname{ad}^0\bar{\rho}) \arrow[r] & H^0(G_{F,S},(\operatorname{ad}^0\bar{\rho})^\vee(1))^\vee \arrow[r] & 0.
\end{tikzcd}$$

Note that $\operatorname{ad}^0\bar{\rho}$ is self-dual under the trace pairing, so we can and do identify $(\operatorname{ad}^0\bar{\rho})^\vee(1)$ and $(\operatorname{ad}^0\bar{\rho})(1)$. If we let $L(\mathcal{D}_v)^\perp\subseteq H^1(G_{F_v},(\operatorname{ad}^0\bar{\rho})(1))$ denote the annihilator of $L(\mathcal{D}_v)$ under the pairing coming from Tate local duality, and we define

$$\begin{aligned}&H^1_{\mathcal{S},T}(G_{F,S},(\operatorname{ad}^0\bar{\rho})(1))\\&\qquad:=\ker(H^1(G_{F,S},(\operatorname{ad}^0\bar{\rho})(1))\to\oplus_{v\in S\setminus T}(H^1(G_{F_v},(\operatorname{ad}^0\bar{\rho})(1))/L(\mathcal{D}_v)^\perp)),\end{aligned}$$

then we deduce that we have an exact sequence

$$\begin{tikzcd}
 & H^1(G_{F,S},\operatorname{ad}^0\bar{\rho}) \arrow[r] & \oplus_{v\in T}H^1(G_{F_v},\operatorname{ad}^0\bar{\rho})\oplus_{v\in S\setminus T}H^1(G_{F_v},\operatorname{ad}^0\bar{\rho})/L(\mathcal{D}_v) \arrow[dll, rounded corners] \\
H^1_{\mathcal{S},T}(G_{F,S},\operatorname{ad}^0\bar{\rho}(1))^\vee \arrow[r] & H^2(G_{F,S},\operatorname{ad}^0\bar{\rho}) \arrow[r] & \oplus_{v\in S}H^2(G_{F_v},\operatorname{ad}^0\bar{\rho}) \arrow[dll, rounded corners] \\
H^0(G_{F,S},\operatorname{ad}^0\bar{\rho}(1))^\vee \arrow[r] & 0, &
\end{tikzcd}$$

and comparing with the diagram above shows that

$$\begin{aligned}H^3_{\mathcal{S},T}(G_{F,S},\operatorname{ad}^0\bar{\rho})&\cong H^0(G_{F,S},\operatorname{ad}^0\bar{\rho}(1))^\vee,\\H^2_{\mathcal{S},T}(G_{F,S},\operatorname{ad}^0\bar{\rho})&\cong H^1_{\mathcal{S},T}(G_{F,S},\operatorname{ad}^0\bar{\rho}(1))^\vee.\end{aligned}$$

Combining all of this, we see that

$$\begin{aligned}\dim_{\mathbb{F}} H^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}) = \#T - \sum_{v \mid \infty} &\dim_{\mathbb{F}} H^0(G_{F_v}, \operatorname{ad}^0 \bar{\rho}) \\ &+ \sum_{v \in S \setminus T} (\dim_{\mathbb{F}} L(\mathcal{D}_v) - \dim_{\mathbb{F}} H^0(G_{F_v}, \operatorname{ad}^0 \bar{\rho})) \\ &+ \dim_{\mathbb{F}} H^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}(1)) \\ &- \dim_{\mathbb{F}} H^0(G_{F,S}, \operatorname{ad}^0 \bar{\rho}(1)).\end{aligned}$$

Now, similar arguments to those we used above give us the following result; see Section 2.2 of [Clozel et al. 2008].

Proposition 3.24. (1) *There is a canonical isomorphism*

$$\operatorname{Hom}(\mathfrak{m}_{R^{\square_T}_{\mathcal{S}}}/(\mathfrak{m}^2_{R^{\square_T}_{\mathcal{S}}}, \mathfrak{m}_{R^{\mathrm{loc}}_{\mathcal{S},T}}, \lambda), \mathbb{F}) \cong H^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho}).$$

(2) $R^{\square_T}_{\mathcal{S}}$ *is the quotient of a power series ring in* $\dim_{\mathbb{F}} H^1_{\mathcal{S},T}(G_{F,S}, \operatorname{ad}^0 \bar{\rho})$ *variables over* $R^{\mathrm{loc}}_{\mathcal{S},T}$.

(3) *The Krull dimension of* $R^{\mathrm{univ}}_{\mathcal{S}}$ *is at least*

$$\begin{aligned}1 + \sum_{v \in S} &(\operatorname{Krull} \dim(R^{\square}_{\bar{\rho}|_{G_{F_v}}, \chi}/I(\mathcal{D}_v)) - n^2) \\ &- \sum_{v \mid \infty} \dim_{\mathbb{F}} H^0(G_{F_v}, \operatorname{ad}^0 \bar{\rho}) - \dim_{\mathbb{F}} H^0(G_{F,S}, \operatorname{ad}^0 \bar{\rho}(1)).\end{aligned}$$

3.25. ***Finiteness of maps between global deformation rings.*** Suppose that F'/F is a finite extension of number fields, and that S' is the set of places of F' lying over S. Assume that $\bar{\rho}|_{G_{F',S'}}$ is absolutely irreducible. Then restricting the universal deformation ρ^{univ} of $\bar{\rho}$ to $G_{F',S'}$ gives a ring homomorphism $R^{\mathrm{univ}}_{\bar{\rho}|_{G_{F',S'}}} \to R^{\mathrm{univ}}_{\bar{\rho}}$. The following very useful fact is due to Khare and Wintenberger.

Proposition 3.26. *The ring* $R^{\mathrm{univ}}_{\bar{\rho}}$ *is a finitely generated* $R^{\mathrm{univ}}_{\bar{\rho}|_{G_{F',S'}}}$*-module.*

Proof. See, e.g., Lemma 1.2.3 of [Barnet-Lamb et al. 2014]. □

3.27. ***Local deformation rings with l = p.*** For proving modularity lifting theorems, we typically need to consider local deformation rings when $l = p$ which capture certain properties in p-adic Hodge theory (for example being crystalline with fixed Hodge–Tate weights). These deformation rings are one of the most difficult and interesting parts of the subject; for example, a detailed computation of deformation rings with $l = p = 3$ was at the heart of the eventual proof of the Taniyama–Shimura–Weil conjecture.

For the most part, the relevant deformation rings when $l = p$ are still not well understood; we don't have a concrete description of the rings in most cases, or even basic information such as the number of irreducible components of the generic fiber. In these notes, we will ignore all of these difficulties, and work only with the "Fontaine–Laffaille" case, where the deformation rings are formally smooth. This is already enough to have important applications.

Assume that $K/\mathbb{Q}_p$ is a finite unramified extension, and assume that L is chosen large enough to contain the images of all embeddings $K \hookrightarrow \overline{\mathbb{Q}}_p$. For each $\sigma : K \hookrightarrow L$, let H_σ be a set of n distinct integers, such that the difference between the maximal and minimal elements of H_σ is less than or equal to $p-2$.

Theorem 3.28. *There is a unique reduced, p-torsion free quotient $R^{\square}_{\bar{\rho},\chi,\mathrm{cr},\{H_\sigma\}}$ of $R^{\square}_{\bar{\rho},\chi}$ with the property that a continuous homomorphism $\psi : R^{\square}_{\bar{\rho},\chi} \to \overline{\mathbb{Q}}_p$ factors through $R^{\square}_{\bar{\rho},\chi,\mathrm{cr},\{H_\sigma\}}$ if and only if $\psi \circ \rho^{\square}$ is crystalline, and for each $\sigma : K \hookrightarrow L$, we have $\mathrm{HT}_\sigma(\psi \circ \rho^{\square}) = H_\sigma$.*

Furthermore it has Krull dimension given by

$$\dim R^{\square}_{\bar{\rho},\chi,\mathrm{cr},\{H_\sigma\}} = n^2 + [K : \mathbb{Q}_p]\tfrac{1}{2}n(n-1),$$

and in fact $R^{\square}_{\bar{\rho},\chi,\mathrm{cr},\{H_\sigma\}}$ is formally smooth over $\mathcal{O}$, i.e., it is isomorphic to a power series ring in $n^2 - 1 + [K : \mathbb{Q}_p]\frac{1}{2}n(n-1)$ variables over $\mathcal{O}$.

In fact, if we remove the assertion of formal smoothness, Theorem 3.28 still holds without the assumption that $K/\mathbb{Q}_p$ is unramified, and without any assumption on the difference between the maximal and minimal elements of the H_σ, but in this case it is a much harder theorem of Kisin [2008]. In any case, the formal smoothness will be important for us.

Theorem 3.28 is essentially a consequence of Fontaine–Laffaille theory [Fontaine and Laffaille 1982], which is a form of integral p-adic Hodge theory; it classifies the Galois-stable lattices in crystalline representations, under the assumptions we've made above. The first proof of Theorem 3.28 was essentially in Ramakrishna's thesis [1993], and the general result is the content of Section 2.4 of [Clozel et al. 2008].

3.29. ***Local deformation rings with $p \neq l$.*** In contrast to the situation when $l = p$, we will need to consider several deformation problems when $l \neq p$. We will restrict ourselves to the two-dimensional case. Let $K/\mathbb{Q}_l$ be a finite extension, with $l \neq p$, and fix $n = 2$. As we saw in Section 2.7, there is essentially an incompatibility between the wild inertia subgroup of G_K and the p-adic topology on $\mathrm{GL}_2(\mathcal{O})$, which makes it possible to explicitly describe the p-adic representations of G_K, and consequently the corresponding universal deformation rings. This was done in varying degrees of generality over a long period of time; in particular, in the general n-dimensional case we highlight Section 2.4.4 of [Clozel et al. 2008] and [Choi 2009], and in the 2-dimensional setting [Pilloni 2008] and [Shotton 2016]. In fact [Shotton 2016] gives a complete description of the deformation rings for a fixed inertial type.

We will content ourselves with recalling some of the basic structural results, and with giving a sketch of how the results are proved in one particular case; see Exercise 3.34 below.

3.30. ***Deformations of fixed type.*** Recall from Proposition 2.18 that given a representation $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ there is a Weil–Deligne representation $\mathrm{WD}(\rho)$ associated to ρ. If $\mathrm{WD} = (r, N)$ is a Weil–Deligne representation, then we write $\mathrm{WD}\,|_{I_K}$ for $(r|_{I_K}, N)$, and call it an *inertial* WD-*type*.

Fix $\bar{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$. Then (assuming as usual that L is sufficiently large) we have the following general result on $R^{\square}_{\bar{\rho},\chi}$; see, e.g., Theorem 3.3.1 of [Böckle 2013].

Theorem 3.31. *$R^{\square}_{\bar{\rho},\chi}$ is equidimensional of Krull dimension* 4, *and the generic fiber $R^{\square}_{\bar{\rho},\chi}[1/p]$ has Krull dimension* 3. *Furthermore*:

(a) *The function which takes a $\overline{\mathbb{Q}}_p$-point $x : R^{\square}_{\bar{\rho},\chi}[1/p] \to \overline{\mathbb{Q}}_p$ to* (*the isomorphism class of*) $\mathrm{WD}(x \circ \rho^{\square})|_{I_K}$ (*forgetting N*) *is constant on the irreducible components of $R^{\square}_{\bar{\rho},\chi}[1/p]$.*

(b) *The irreducible components of $R^{\square}_{\bar{\rho},\chi}[1/p]$ are all regular*, *and there are only finitely many of them.*

In light of Theorem 3.31, we make the following definition. Let τ be an inertial WD-type. Then there is a unique reduced, p-torsion free quotient $R^{\square}_{\bar{\rho},\chi,\tau}$ of $R^{\square}_{\bar{\rho},\chi}$ with the property that a continuous homomorphism $\psi : R^{\square}_{\bar{\rho},\chi} \to \overline{\mathbb{Q}}_p$ factors through $R^{\square}_{\bar{\rho},\chi,\tau}$ if and only if $\psi \circ \rho^{\square}$ has inertial Weil–Deligne type τ. (Of course, for all but finitely many τ, we will just have $R^{\square}_{\bar{\rho},\chi,\tau} = 0$.) By Theorem 3.31 we see that if $R^{\square}_{\bar{\rho},\chi,\tau}$ is nonzero then it has Krull dimension 4.

3.32. ***Taylor–Wiles deformations.*** As the name suggests, the deformations that we consider in this subsection will be of crucial importance for the Taylor–Wiles–Kisin method. Assume that $\bar{\rho}$ is unramified, that $\bar{\rho}(\mathrm{Frob}_K)$ has distinct eigenvalues, and that $\#k \equiv 1 \pmod{p}$. Suppose also that χ is unramified.

Lemma 3.33. *Suppose that* $(\#k - 1)$ *is exactly divisible by p^m. Then* $R^{\square}_{\bar{\rho},\chi} \cong \mathcal{O}[[x, y, B, u]]/((1+u)^{p^m} - 1)$. *Furthermore*, *if $\varphi \in G_K$ is a lift of* Frob_K, *then $\rho^{\square}(\varphi)$ is conjugate to a diagonal matrix.*

Exercise 3.34. Prove this lemma as follows. Note firstly that $\rho^{\square}(P_K) = \{1\}$, because $\bar{\rho}(P_K) = \{1\}$, so $\rho^{\square}(P_K)$ is a pro-l-subgroup of the pro-p-group $\ker(\mathrm{GL}_2(R^{\square}_{\bar{\rho},\chi}) \to \mathrm{GL}_2(\mathbb{F}))$.

Let φ be a fixed lift of Frob_K to G_K/P_K, and σ a topological generator of I_K/P_K, which as in Section 2.7 we can choose so that $\varphi^{-1}\sigma\varphi = \sigma^{\#k}$. Write $\bar{\rho}(\varphi) = \left(\begin{smallmatrix}\bar{\alpha} & 0\\ 0 & \bar{\beta}\end{smallmatrix}\right)$, and fix lifts $\alpha, \beta \in \mathcal{O}$ of $\bar{\alpha}, \bar{\beta}$.

Then we will show that we can take

$$\rho^{\square}(\varphi) = \begin{pmatrix} 1 & y \\ x & 1 \end{pmatrix}^{-1} \begin{pmatrix} \alpha + B & 0 \\ 0 & \chi(\varphi)/(\alpha + B) \end{pmatrix} \begin{pmatrix} 1 & y \\ x & 1 \end{pmatrix},$$

$$\rho^{\square}(\sigma) = \begin{pmatrix} 1 & y \\ x & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1+u & 0 \\ 0 & (1+u)^{-1} \end{pmatrix} \begin{pmatrix} 1 & y \\ x & 1 \end{pmatrix}.$$

(1) Let $\rho : G_K \to \mathrm{GL}_2(A)$ be a lift of $\bar{\rho}$. By Hensel's lemma, there are $a, b \in \mathfrak{m}_A$ such that $\rho(\varphi)$ has characteristic polynomial $(X-(\alpha+a))(X-(\beta+b))$. Show that there are $x, y \in \mathfrak{m}_A$ such that

$$\rho(\varphi)\begin{pmatrix} 1 \\ x \end{pmatrix} = (\alpha + a)\begin{pmatrix} 1 \\ x \end{pmatrix} \quad \text{and} \quad \rho(\varphi)\begin{pmatrix} y \\ 1 \end{pmatrix} = (\beta + b)\begin{pmatrix} y \\ 1 \end{pmatrix}$$

(2) Since $\bar{\rho}$ is unramified, $\bar{\rho}(\sigma) = 1$, so we may write

$$\begin{pmatrix} 1 & y \\ x & 1 \end{pmatrix}^{-1} \rho(\sigma) \begin{pmatrix} 1 & y \\ x & 1 \end{pmatrix} = \begin{pmatrix} 1+u & v \\ w & 1+z \end{pmatrix}$$

with $u, v, w, z \in \mathfrak{m}_A$. Use the commutation relation between $\rho(\varphi)$ and $\rho(\sigma)$ to show that $v = w = 0$.

(3) Use the fact that χ is unramified to show that $1 + z = (1+u)^{-1}$.

(4) Show that $(1+u)^{\#k} = 1+u$, and deduce that $(1+u)^{\#k-1} = 1$.

(5) Deduce that $(1+u)^{p^m} = 1$.

(6) Complete the proof of the lemma.

3.35. ***Taylor's "Ihara avoidance" deformations.*** The following deformation rings are crucial to Taylor's arguments [2008] which avoid the use of Ihara's lemma in proving automorphy lifting theorems. When $n = 2$ these arguments are not logically necessary, but they are crucial to all applications of automorphy lifting theorems when $n > 2$. They are used in order to compare Galois representations with differing ramification at places not dividing p.

Continue to let $K/\mathbb{Q}_l$ be a finite extension, and assume that $\bar{\rho}$ is the trivial 2-dimensional representation, that $\#k \equiv 1 \pmod{p}$, that χ is unramified, and that $\bar{\chi}$ is trivial. Again, we see that $\rho^{\square}(P_K)$ is trivial, so that $\rho^{\square}$ is determined by the two matrices $\rho^{\square}(\sigma)$ and $\rho^{\square}(\varphi)$, as in Exercise 3.34. A similar analysis then yields the following facts. (For the proof of the analogous results in the n-dimensional case, see Section 3 of [Taylor 2008].)

Definition 3.36. (1) Let $\mathcal{P}_{\mathrm{ur}}$ be the minimal ideal of $R^{\square}_{\bar{\rho},\chi}$ modulo which $\rho^{\square}(\sigma) = 1_2$.

(2) For any root of unity ζ which is trivial modulo λ, we let $\mathcal{P}_\zeta$ be the minimal ideal of $R^{\square}_{\bar{\rho},\chi}$ modulo which $\rho^{\square}(\sigma)$ has characteristic polynomial $(X-\zeta)(X-\zeta^{-1})$.

(3) Let $\mathcal{P}_{\mathrm{m}}$ be the minimal ideal of $R^{\square}_{\bar{\rho},\chi}$ modulo which $\rho^{\square}(\sigma)$ has characteristic polynomial $(X-1)^2$, and $\#k(\operatorname{tr}\rho^{\square}(\varphi))^2 = (1+\#k)^2 \det \rho^{\square}(\varphi)$.

[The motivation for the definition of $\mathcal{P}_{\mathrm{m}}$ is that we are attempting to describe the unipotent liftings, and if you assume that $\rho^{\square}(\sigma) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, this is the relation forced on $\rho^{\square}(\varphi)$.]

Proposition 3.37. *The minimal primes of $R^{\square}_{\bar{\rho},\chi}$ are precisely $\sqrt{\mathcal{P}_{\mathrm{ur}}}$, $\sqrt{\mathcal{P}_{\mathrm{m}}}$, and the $\sqrt{\mathcal{P}_{\zeta}}$ for $\zeta \neq 1$. We have $\sqrt{\mathcal{P}_1} = \sqrt{\mathcal{P}_{\mathrm{ur}}} \cap \sqrt{\mathcal{P}_{\mathrm{m}}}$.*

Write $R^{\square}_{\bar{\rho},\chi,1}$, $R^{\square}_{\bar{\rho},\chi,\zeta}$, $R^{\square}_{\bar{\rho},\chi,\mathrm{ur}}$, $R^{\square}_{\bar{\rho},\chi,\mathrm{m}}$ for the corresponding quotients of $R^{\square}_{\bar{\rho},\chi}$.

Theorem 3.38. *We have $R^{\square}_{\bar{\rho},\chi,1}/\lambda = R^{\square}_{\bar{\rho},\chi,\zeta}/\lambda$. Furthermore:*

(1) *If $\zeta \neq 1$ then $R^{\square}_{\bar{\rho},\chi,\zeta}[1/p]$ is geometrically irreducible of dimension* 3.

(2) *$R^{\square}_{\bar{\rho},\chi,\mathrm{ur}}$ is formally smooth over $\mathcal{O}$ (and thus geometrically irreducible) of relative dimension* 3.

(3) *$R^{\square}_{\bar{\rho},\chi,\mathrm{m}}[1/p]$ is geometrically irreducible of dimension* 3.

(4) *Both*

$$\operatorname{Spec} R^{\square}_{\bar{\rho},\chi,1} = \operatorname{Spec} R^{\square}_{\bar{\rho},\chi,\mathrm{ur}} \cup \operatorname{Spec} R^{\square}_{\bar{\rho},\chi,\mathrm{m}}$$

and

$$\operatorname{Spec} R^{\square}_{\bar{\rho},\chi,1}/\lambda = \operatorname{Spec} R^{\square}_{\bar{\rho},\chi,\mathrm{ur}}/\lambda \cup \operatorname{Spec} R^{\square}_{\bar{\rho},\chi,\mathrm{m}}/\lambda$$

are unions of two irreducible components, and have relative dimension 3.

Proof. See Proposition 3.1 of [Taylor 2008] for an n-dimensional version of this result. In the 2-dimensional case it can be proved by explicitly computing equations for the lifting rings; see [Shotton 2016]. □

4. Modular and automorphic forms, and the Langlands correspondence

We now turn to the automorphic side of the Langlands correspondence, and define the spaces of modular forms to which our modularity lifting theorems pertain.

4.1. *The local Langlands correspondence (and the Jacquet–Langlands correspondence).*

Weil–Deligne representations are the objects on the "Galois" side of the local Langlands correspondence. We now describe the objects on the "automorphic" side. These will be representations (π, V) of $\mathrm{GL}_n(K)$ on (usually infinite-dimensional) $\mathbb{C}$-vector spaces, where as above $K/\mathbb{Q}_l$ is a finite extension for some prime l.

Definition 4.2. We say that (π, V) is *smooth* if for any vector $v \in V$, the stabilizer of v in $\mathrm{GL}_n(K)$ is open. We say that (π, V) is *admissible* if it is smooth, and for any compact open subgroup $U \subset \mathrm{GL}_n(K)$, V^U is finite-dimensional.

For example, a smooth one-dimensional representation of $K^\times$ is the same thing as a continuous character (for the discrete topology on $\mathbb{C}$).

Fact 4.3. (1) If π is smooth and irreducible then it is admissible.

(2) Schur's lemma holds for admissible smooth representations, and in particular if π is smooth, admissible and irreducible then it has a central character $\chi_\pi : K^\times \to \mathbb{C}^\times$.

In general these representations are classified in terms of the (super)cuspidal representations. We won't need the details of this classification, and accordingly we won't define the cuspidal representations; see, for example, Chapter IV of [Bushnell and Henniart 2006].

Let B be the subgroup of $\mathrm{GL}_2(K)$ consisting of upper-triangular matrices. Define $\delta : B \to K^\times$ by

$$\delta\left(\begin{pmatrix} a & * \\ 0 & d \end{pmatrix}\right) = ad^{-1}.$$

Given two continuous characters $\chi_1, \chi_2 : K^\times \to \mathbb{C}^\times$, we may view $\chi_1 \otimes \chi_2$ as a representation of B by

$$\chi_1 \otimes \chi_2 : \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \mapsto \chi_1(a)\chi_2(d).$$

Then we define a representation $\chi_1 \times \chi_2$ of $\mathrm{GL}_2(K)$ by *normalized induction*:

$$\begin{aligned}\chi_1 \times \chi_2 &= \text{n-Ind}_B^{\mathrm{GL}_2(K)}(\chi_1 \otimes \chi_2) \\ &:= \{\varphi : \mathrm{GL}_2(K) \to \mathbb{C} \mid \varphi(hg) = (\chi_1 \otimes \chi_2)(h)|\delta(h)|_K^{1/2}\varphi(g) \\ &\qquad\qquad \text{for all } h \in B,\ g \in \mathrm{GL}_2(K)\}\end{aligned}$$

where $\mathrm{GL}_2(K)$ acts by $(g\varphi)(g') = \varphi(g'g)$, and we only allow smooth φ, i.e., functions for which there is an open subgroup U of $\mathrm{GL}_2(K)$ such that $\varphi(gu) = \varphi(g)$ for all $g \in \mathrm{GL}_2(K)$, $u \in U$.

The representation $\chi_1 \times \chi_2$ has length at most 2, but is not always irreducible. It is always the case that $\chi_1 \times \chi_2$ and $\chi_2 \times \chi_1$ have the same Jordan-Hölder factors. If $\chi_1 \times \chi_2$ is irreducible then we say that it is a *principal series* representation.

Fact 4.4. (1) $\chi_1 \times \chi_2$ is irreducible unless $\chi_1/\chi_2 = |\cdot|_K^{\pm 1}$.

(2) $\chi \times \chi|\cdot|_K$ has a one-dimensional irreducible subrepresentation, and the corresponding quotient is irreducible. We denote this quotient by $\mathrm{Sp}_2(\chi)$.

We will let $\chi_1 \boxplus \chi_2$ denote $\chi_1 \times \chi_2$ unless $\chi_1/\chi_2 = |\cdot|_K^{\pm 1}$, and we let

$$\chi \boxplus \chi|\cdot|_K = \chi|\cdot|_K \boxplus \chi = (\chi|\cdot|_K^{1/2}) \circ \det.$$

(While this notation may seem excessive, we remark that a similar construction is possible for n-dimensional representations, which is where the notation comes from.) These representations, and the $\mathrm{Sp}_2(\chi)$, are all the noncuspidal irreducible admissible representations of $\mathrm{GL}_2(K)$. We say that an irreducible smooth representation π of $\mathrm{GL}_2(K)$ is *discrete series* if it is of the form $\mathrm{Sp}_2(\chi)$ or is cuspidal.

The local Langlands correspondence provides a unique family of bijections rec_K from the set of isomorphism classes of irreducible smooth representations of $\mathrm{GL}_n(K)$ to the set of isomorphism classes of n-dimensional Frobenius semisimple Weil–Deligne representations of W_K over $\mathbb{C}$, satisfying a list of properties. In order to be uniquely determined, one needs to formulate the correspondence for all n at once, and the properties are expressed in terms of L- and ε-factors, neither of which we have defined. Accordingly, we will not make a complete statement of the local Langlands correspondence, but will rather state the properties of the correspondence that we will need to use. (Again, the reader could look at the book [Bushnell and Henniart 2006] for these properties, and many others.) It is also possible to define the correspondence in global terms, as we will see later, and indeed at present the only proof of the correspondence is global.

Fact 4.5. We now list some properties of rec_K for $n = 1, 2$:

(1) If $n = 1$ then $\mathrm{rec}_K(\pi) = \pi \circ \mathrm{Art}_K^{-1}$.

(2) If χ is a smooth character, $\mathrm{rec}_K(\pi \otimes (\chi \circ \det)) = \mathrm{rec}_K(\pi) \otimes \mathrm{rec}_K(\chi)$.

(3) $\mathrm{rec}_K(\mathrm{Sp}_2(\chi)) = \mathrm{Sp}_2(\mathrm{rec}_K(\chi))$; see Exercise 2.12 for this notation.

(4) $\mathrm{rec}_K(\chi_1 \boxplus \chi_2) = \mathrm{rec}_K(\chi_1) \oplus \mathrm{rec}_K(\chi_2)$.

(5) If $n = 2$, then $\mathrm{rec}_K(\pi)$ is unramified (i.e., $N = 0$ and the restriction to I_K is trivial) if and only if $\pi = \chi_1 \boxplus \chi_2$ with χ_1, χ_2 both unramified characters (i.e., trivial on $\mathcal{O}_K^\times$). These conditions are equivalent to $\pi^{\mathrm{GL}_2(\mathcal{O}_K)} \neq 0$, in which case it is one-dimensional.

(6) π is discrete series if and only if $\mathrm{rec}_K(\pi)$ is indecomposable, and cuspidal if and only if $\mathrm{rec}_K(\pi)$ is irreducible.

4.6. ***Hecke operators.*** Consider the set of compactly supported $\mathbb{C}$-valued functions on $\mathrm{GL}_2(\mathcal{O}_K)\backslash \mathrm{GL}_2(K)/\mathrm{GL}_2(\mathcal{O}_K)$. Concretely, these are functions which vanish outside of a finite number of double cosets $\mathrm{GL}_2(\mathcal{O}_K)g\,\mathrm{GL}_2(\mathcal{O}_K)$. The set of such functions is in fact a ring, with the multiplication being given by convolution. To be precise, we fix μ the (left and right) Haar measure on $\mathrm{GL}_2(K)$ such that $\mu(\mathrm{GL}_2(\mathcal{O}_K)) = 1$, and we define

$$(\varphi_1 * \varphi_2)(x) = \int_{\mathrm{GL}_2(K)} \varphi_1(g)\varphi_2(g^{-1}x)\, d\mu_g.$$

Of course, this integral is really just a finite sum. One can check without too much difficulty that the ring $\mathcal{H}$ of these Hecke operators is just $\mathbb{C}[T, S^{\pm 1}]$, where T is the characteristic function of

$$\mathrm{GL}_2(\mathcal{O}_K)\begin{pmatrix}\varpi_K & 0\\ 0 & 1\end{pmatrix}\mathrm{GL}_2(\mathcal{O}_K)$$

and S is the characteristic function of

$$\mathrm{GL}_2(\mathcal{O}_K)\begin{pmatrix}\varpi_K & 0\\ 0 & \varpi_K\end{pmatrix}\mathrm{GL}_2(\mathcal{O}_K).$$

The algebra $\mathcal{H}$ acts on an irreducible admissible $\mathrm{GL}_2(K)$-representation π. Given $\varphi \in \mathcal{H}$, we obtain a linear map $\pi(\varphi) : \pi \to \pi^{\mathrm{GL}_2(\mathcal{O}_K)}$, by

$$\pi(\varphi)(v) = \int_{\mathrm{GL}_2(K)} \varphi(g)\pi(g)v d\mu_g.$$

In particular, if π is unramified then $\pi(\varphi)$ acts via a scalar on the one-dimensional $\mathbb{C}$-vector space $\pi^{\mathrm{GL}_2(\mathcal{O}_K)}$. We will now compute this scalar explicitly.

Exercise 4.7. (1) Show that we have decompositions

$$\mathrm{GL}_2(\mathcal{O}_K)\begin{pmatrix}\varpi_K & 0\\ 0 & \varpi_K\end{pmatrix}\mathrm{GL}_2(\mathcal{O}_K) = \begin{pmatrix}\varpi_K & 0\\ 0 & \varpi_K\end{pmatrix}\mathrm{GL}_2(\mathcal{O}_K),$$

and

$$\mathrm{GL}_2(\mathcal{O}_K)\begin{pmatrix}\varpi_K & 0\\ 0 & 1\end{pmatrix}\mathrm{GL}_2(\mathcal{O}_K)$$
$$= \Big(\coprod_{\alpha\in\mathcal{O}_K \pmod{\varpi_K}} \begin{pmatrix}\varpi_K & \alpha\\ 0 & 1\end{pmatrix}\mathrm{GL}_2(\mathcal{O}_K)\Big) \coprod \begin{pmatrix}1 & 0\\ 0 & \varpi_K\end{pmatrix}\mathrm{GL}_2(\mathcal{O}_K).$$

(2) Suppose that $\pi = (\chi|\cdot|^{1/2})\circ\det$ with χ unramified. Show that $\pi^{\mathrm{GL}_2(\mathcal{O}_K)} = \pi$, and that S acts via $\chi(\varpi_K)^2(\#k)^{-1}$, and that T acts via $(\#k^{1/2}+\#k^{-1/2})\chi(\varpi_K)$.

(3) Suppose that χ_1, χ_2 are unramified characters and that $\chi_1 \neq \chi_2|\cdot|_K^{\pm 1}$. Let $\pi = \chi_1 \boxplus \chi_2$. Using the Iwasawa decomposition $\mathrm{GL}_2(K) = B(K)\,\mathrm{GL}_2(\mathcal{O}_K)$, check that $\pi^{\mathrm{GL}_2(\mathcal{O}_K)}$ is one-dimensional, and is spanned by a function φ_0 with $\varphi_0\big(\big(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\big)\big) = \chi_1(a)\chi_2(d)|a/d|^{1/2}$. Show that S acts on $\pi^{\mathrm{GL}_2(\mathcal{O}_K)}$ via $(\chi_1\chi_2)(\varpi_K)$, and that T acts via $\#k^{1/2}(\chi_1(\varpi_K) + \chi_2(\varpi_K))$.

4.8. ***Modular forms and automorphic forms on quaternion algebras.*** Let F be a totally real field, and let D/F be a quaternion algebra with center F, i.e., a central simple F-algebra of dimension 4. Letting $S(D)$ be the set of places v of F at which D is ramified, i.e., for which $D \otimes_F F_v$ is a division algebra (equivalently, is not isomorphic to $M_2(F_v)$), it is known that $S(D)$ classifies D up to isomorphism, and that $S(D)$ can be any finite set of places of F of even cardinality (so for example $S(D)$ is empty if and only if $D = M_2(F)$). We will now define some spaces of automorphic forms on $D^\times$.

For each $v \mid \infty$ fix $k_v \geq 2$ and $\eta_v \in \mathbb{Z}$ such that $k_v + 2\eta_v - 1 = w$ is independent of v. These will be the weights of our modular forms. Let G_D be the algebraic group over $\mathbb{Q}$ such that for any $\mathbb{Q}$-algebra R, $G_D(R) = (D \otimes_{\mathbb{Q}} R)^\times$. For each place $v \mid \infty$ of F, we define a subgroup U_v of $(D \otimes_F F_v)^\times$ as follows: if $v \in S(D)$ we let $U_v = (D \otimes_F F_v)^\times \cong \mathbb{H}^\times$ (where $\mathbb{H}$ denotes the Hamilton quaternions), and if $v \notin S(D)$, so that $(D \otimes_F F_v)^\times \cong \mathrm{GL}_2(\mathbb{R})$, we take $U_v = \mathbb{R}^\times \mathrm{SO}(2)$. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ and $z \in \mathbb{C} - \mathbb{R}$, we let $j(\gamma, z) = cz + d$. One checks easily that $j(\gamma\delta, z) = j(\gamma, \delta z) j(\delta, z)$.

We now define a representation (τ_v, W_v) of U_v over $\mathbb{C}$ for each $v \mid \infty$. If $v \in S(D)$, we have $U_v \hookrightarrow \mathrm{GL}_2(\bar{F}_v) \cong \mathrm{GL}_2(\mathbb{C})$ which acts on $\mathbb{C}^2$, and we let (τ_v, W_v) be the representation

$$(\mathrm{Sym}^{k_v - 2}\, \mathbb{C}^2) \otimes (\wedge^2 \mathbb{C}^2)^{\eta_v}.$$

If $v \notin S(D)$, then we have $U_v \cong \mathbb{R}^\times \mathrm{SO}(2)$, and we take $W_v = \mathbb{C}$, with

$$\tau_v(\gamma) = j(\gamma, i)^{k_v} (\det \gamma)^{\eta_v - 1}.$$

We write $U_\infty = \prod_{v \mid \infty} U_v$, $W_\infty = \otimes_{v \mid \infty} W_v$, $\tau_\infty = \otimes_{v \mid \infty} \tau_v$. Let $\mathbb{A} = \mathbb{A}_{\mathbb{Q}}$ be the adeles of $\mathbb{Q}$, and let $\mathbb{A}^\infty$ be the finite adeles. We then define $S_{D,k,\eta}$ (where k, η reflect the dependence on the integers k_v, η_v) to be the space of functions $\varphi : G_D(\mathbb{Q}) \backslash G_D(\mathbb{A}) \to W_\infty$ which satisfy:

(1) $\varphi(g u_\infty) = \tau_\infty(u_\infty)^{-1} \varphi(g)$ for all $u_\infty \in U_\infty$ and $g \in G_D(\mathbb{A})$.

(2) There is a nonempty open subset $U^\infty \subset G_D(\mathbb{A}^\infty)$ such that $\varphi(gu) = \varphi(g)$ for all $u \in U^\infty$, $g \in G_D(\mathbb{A})$.

(3) Let S_∞ denote the infinite places of F. If $g \in G_D(\mathbb{A}^\infty)$ then the function

$$(\mathbb{C} - \mathbb{R})^{S_\infty - S(D)} \to W_\infty$$

defined by

$$h_\infty(i, \ldots, i) \mapsto \tau_\infty(h_\infty) \phi(g h_\infty)$$

is holomorphic. [Note that this function is well-defined by the first condition, as U_∞ is the stabilizer of $(i, \ldots, i)$.]

(4) If $S(D) = \varnothing$ then for all $g \in G_D(\mathbb{A}) = \mathrm{GL}_2(\mathbb{A}_F)$, we have

$$\int_{F \backslash \mathbb{A}_F} \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g \right) dx = 0.$$

If in addition we have $F = \mathbb{Q}$, then we furthermore demand that for all $g \in G_D(\mathbb{A}^\infty)$, $h_\infty \in \mathrm{GL}_2(\mathbb{R})^+$ the function $\varphi(gh_\infty)|\mathrm{Im}(h_\infty i)|^{k/2}$ is bounded on $\mathbb{C} - \mathbb{R}$.

There is a natural action of $G_D(\mathbb{A}^\infty)$ on $S_{D,k,\eta}$ by right-translation, i.e., $(g\varphi)(x) := \varphi(xg)$.

Exercise 4.9. While this definition may at first sight appear rather mysterious, it is just a generalization of the familiar spaces of cuspidal modular forms. For example, take $F = \mathbb{Q}$, $S(D) = \varnothing$, $k_\infty = k$, and $\eta_\infty = 0$. Define

$$U_1(N) = \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \;\middle|\; g \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

(1) Let $\mathrm{GL}_2(\mathbb{Q})^+$ be the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ consisting of matrices with positive determinant. Show that the intersection of $\mathrm{GL}_2(\mathbb{Q})^+$ and $U_1(N)$ inside $\mathrm{GL}_2(\mathbb{A}^\infty)$ is $\Gamma_1(N)$, the matrices in $\mathrm{SL}_2(\mathbb{Z})$ congruent to $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}$. [Hint: what is $\hat{\mathbb{Z}}^\times \cap \mathbb{Q}^\times$?]

(2) Use the facts that $\mathrm{GL}_2(\mathbb{A}) = \mathrm{GL}_2(\mathbb{Q})U_1(N)\,\mathrm{GL}_2(\mathbb{R})^+$ [which follows from strong approximation for SL_2 and the fact that $\det U_1(N) = \hat{\mathbb{Z}}^\times$] and that $\mathbb{A}^\times = \mathbb{Q}^\times\hat{\mathbb{Z}}^\times\mathbb{R}^\times_{>0}$ to show that $S^{U_1(N)}_{D,k,0}$ can naturally be identified with a space of functions

$$\varphi : \Gamma_1(N)\backslash \mathrm{GL}_2(\mathbb{R})^+ \to \mathbb{C}$$

satisfying

$$\varphi(gu_\infty) = j(u_\infty, i)^{-k}\varphi(g)$$

for all $g \in \mathrm{GL}_2(\mathbb{R})^+$, $u_\infty \in \mathbb{R}^\times_{>0}\,\mathrm{SO}(2)$.

(3) Show that the stabilizer of i in $\mathrm{GL}_2(\mathbb{R})^+$ is $\mathbb{R}^\times_{>0}\,\mathrm{SO}(2)$. Hence deduce a natural isomorphism between $S^{U_1(N)}_{D,k,0}$ and $S_k(\Gamma_1(N))$, which takes a function φ as above to the function $(gi \mapsto j(g,i)^k\varphi(g))$, $g \in \mathrm{GL}_2(\mathbb{R})^+$.

The case that $S_\infty \subset S(D)$ is particularly simple; then if $U \subset G_D(\mathbb{A}^\infty)$ is an open subgroup, then $S^U_{D,2,0}$ is just the set of $\mathbb{C}$-valued functions on

$$G_D(\mathbb{Q})\backslash G_D(\mathbb{A})/G_D(\mathbb{R})U,$$

which is a finite set. When proving modularity lifting theorems, we will be able to reduce to the case that $S_\infty \subset S(D)$; when this condition holds, we say that D is a *definite* quaternion algebra.

We will now examine the action of Hecke operators on these spaces. Choose an $\mathcal{O}_F$-order $\mathcal{O}_D \subset D$ (that is, an $\mathcal{O}_F$-subalgebra of D which is finitely generated as a $\mathbb{Z}$-module and for which $\mathcal{O}_D \otimes_{\mathcal{O}_F} F \xrightarrow{\sim} D$). For example, if $D = M_2(F)$, one may take $\mathcal{O}_D = M_2(\mathcal{O}_F)$.

For all but finite many finite places v of F we can choose an isomorphism $D_v \cong M_2(F_v)$ such that this isomorphism induces an isomorphism $\mathcal{O}_D \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v} \xrightarrow{\sim} M_2(\mathcal{O}_{F_v})$. Then $G_D(\mathbb{A}^\infty)$ is the subset of elements $g = (g_v) \in \prod_{v \nmid \infty} G_D(F_v)$ such that $g_v \in \mathrm{GL}_2(\mathcal{O}_{F_v})$ for almost all v.

We now wish to describe certain irreducible representations of $G_D(\mathbb{A}^\infty)$ in terms of irreducible representations of the $GL_2(F_v)$. More generally, we have the following construction. Let I be an indexing set and for each $i \in I$, let V_i be a $\mathbb{C}$-vector space. Suppose that we are given $0 \neq e_i \in V_i$ for almost all i (that is, all but finitely many i). Then we define the *restricted tensor product*

$$\otimes'_{\{e_i\}} V_i := \varinjlim_{J \subseteq I} \otimes_{i \in J} V_i,$$

where the colimit is over the finite subsets $J \subseteq I$ containing all the places for which e_i is not defined, and where the transition maps for the colimit are given by "tensoring with the e_i". It can be checked that $\otimes'_{\{e_i\}} V_i \cong \otimes'_{\{f_i\}} V_i$ if for almost all i, e_i and f_i span the same line.

Definition 4.10. We call a representation (π, V) of $G_D(\mathbb{A}^\infty)$ *admissible* if

(1) for any $x \in V$, the stabilizer of x is open, and

(2) for any $U \subset G_D(\mathbb{A}^\infty)$ an open subgroup, $\dim_{\mathbb{C}} V^U < \infty$.

Fact 4.11 [Flath 1979]. If π_v is an irreducible smooth (so admissible) representation of $(D \otimes_F F_v)^\times$ with $\pi_v^{\mathrm{GL}_2(\mathcal{O}_{F_v})} \neq 0$ for almost all v, then $\otimes' \pi_v := \otimes'_{\{\pi_v^{\mathrm{GL}_2(\mathcal{O}_{F_v})}\}} \pi_v$ is an irreducible admissible smooth representation of $G_D(\mathbb{A}^\infty)$, and any irreducible admissible smooth representation of $G_D(\mathbb{A}^\infty)$ arises in this way for unique π_v.

We have a global Hecke algebra, which decomposes as a restricted tensor product of the local Hecke algebras in the following way. For each finite place v of F we choose $U_v \subset (D \otimes_F F_v)^\times$ a compact open subgroup, such that $U_v = \mathrm{GL}_2(\mathcal{O}_{F_v})$ for almost all v. Let μ_v be a Haar measure on $(D \otimes_F F_v)^\times$, chosen such that for almost all v we have $\mu_v(\mathrm{GL}_2(\mathcal{O}_{F_v})) = 1$. Then there is a unique Haar measure μ on $G_D(\mathbb{A}^\infty)$ such that for any U_v as above, if we set $U = \prod_v U_v \subset G_D(\mathbb{A}^\infty)$, then $\mu(U) = \prod_v \mu_v(U_v)$. Then there is a decomposition

$$\mathcal{C}_c(U \backslash G_D(\mathbb{A}^\infty)/U)\mu \cong \otimes'_{\{1_{U_v}\mu_v\}} \mathcal{C}_c(U_v \backslash (D \otimes_F F_v)^\times / U_v)\mu_v,$$

and the actions of these Hecke algebras are compatible with the decomposition $\pi = \otimes' \pi_v$. For the following fact, see Lemma 1.3 of [Taylor 2006].

Fact 4.12. $S_{D,k,\eta}$ is a semisimple admissible representation of $G_D(\mathbb{A}^\infty)$.

Definition 4.13. The irreducible constituents of $S_{D,k,\eta}$ are called the *cuspidal automorphic representations* of $G_D(\mathbb{A}^\infty)$ of weight (k, η).

Remark 4.14. Note that these automorphic representations do not include Maass forms or weight one modular forms; they are the class of *regular algebraic* or *cohomological* cuspidal automorphic representations.

For the following facts, the reader could consult [Gelbart 1975].

Fact 4.15 (strong multiplicity one (and multiplicity one) for GL_2). Suppose that $S(D)=\varnothing$. Then every irreducible constituent of $S_{D,k,\eta}$ has multiplicity one. In fact if π (respectively π') is a cuspidal automorphic representation of weight (k,η) (respectively (k',η')) such that $\pi_v\cong\pi'_v$ for almost all v then $k=k'$, $\eta=\eta'$, and $\pi=\pi'$.

Fact 4.16 (the theory of newforms). Suppose that $S(D)=\varnothing$. If $\mathfrak{n}$ is an ideal of $\mathcal{O}_F$, write

$$U_1(\mathfrak{n})=\left\{g\in\mathrm{GL}_2(\hat{\mathcal{O}}_F)\;\middle|\; g\equiv\begin{pmatrix}* & *\\ 0 & 1\end{pmatrix}\pmod{\mathfrak{n}}\right\}.$$

If π is a cuspidal automorphic representation of $G_D(\mathbb{A}^\infty)$ then there is a unique ideal $\mathfrak{n}$ such that $\pi^{U_1(\mathfrak{n})}$ is one-dimensional, and $\pi^{U_1(\mathfrak{m})}\neq 0$ if and only if $\mathfrak{n}\mid\mathfrak{m}$. We call $\mathfrak{n}$ the *conductor* (or sometimes the *level*) of π.

Analogous to the theory of admissible representations of $\mathrm{GL}_2(K)$, $K/\mathbb{Q}_p$ finite that we sketched above, there is a theory of admissible representations of $M^\times$, M a nonsplit quaternion algebra over K. Since $M^\times/K^\times$ is compact, any irreducible smooth representation of $M^\times$ is finite-dimensional. There is a bijection JL, the *local Jacquet–Langlands correspondence*, from the irreducible smooth representations of $M^\times$ to the discrete series representations of $\mathrm{GL}_2(K)$, determined by a character identity.

Fact 4.17 (the global Jacquet–Langlands correspondence). We have the following facts about $G_D(\mathbb{A}^\infty)$:

(1) The only finite-dimensional cuspidal automorphic representations of $G_D(\mathbb{A}^\infty)$ are 1-dimensional representations which factor through the reduced norm; these only exist if $D\neq M_2(F)$.

(2) There is a bijection JL from the infinite-dimensional cuspidal automorphic representations of $G_D(\mathbb{A}^\infty)$ of weight (k,η) to the cuspidal automorphic representations of $\mathrm{GL}_2(\mathbb{A}_F^\infty)$ of weight (k,η) which are discrete series for all finite places $v\in S(D)$. Furthermore if $v\notin S(D)$ then $\mathrm{JL}(\pi)_v=\pi_v$, and if $v\in S(D)$ then $\mathrm{JL}(\pi)_v=\mathrm{JL}(\pi_v)$.

Remark 4.18. We will use the global Jacquet–Langlands correspondence together with base change (see below) to reduce ourselves to considering the case that $S(D)=S_\infty$ when proving automorphy lifting theorems.

4.19. *Galois representations associated to automorphic representations.*

Fact 4.20 (the existence of Galois representations associated to regular algebraic cuspidal automorphic representations). Let π be a regular algebraic cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F^\infty)$ of weight (k, η). Then there is a CM field L_π which contains the eigenvalues of T_v and S_v on $\pi_v^{\mathrm{GL}_2(\mathcal{O}_{F_v})}$ for each finite place v at which π_v is unramified. Furthermore, for each finite place λ of L_π there is a continuous irreducible Galois representation

$$r_\lambda(\pi) : G_F \to \mathrm{GL}_2(\bar{L}_{\pi,\lambda})$$

such that:

(1) If π_v is unramified and v does not divide the residue characteristic of λ, then $r_\lambda(\pi)|_{G_{F_v}}$ is unramified, and the characteristic polynomial of Frob_v is $X^2 - t_v X + (\#k(v))s_v$, where t_v and s_v are the eigenvalues of T_v and S_v respectively on $\pi_v^{\mathrm{GL}_2(\mathcal{O}_{F_v})}$, and $k(v)$ is the residue field of F_v. [Note that by the Chebotarev density theorem, this already characterizes $r_\lambda(\pi)$ up to isomorphism.]

(2) More generally, for all finite places v not dividing the residue characteristic of λ, $\mathrm{WD}(r_\lambda(\pi)|_{G_{F_v}})^{F-\mathrm{ss}} \cong \mathrm{rec}_{F_v}(\pi_v \otimes |\det|^{-1/2})$.

(3) If v divides the residue characteristic of λ then $r_\lambda(\pi)|_{G_{F_v}}$ is de Rham with τ-Hodge–Tate weights $\eta_\tau, \eta_\tau + k_\tau - 1$, where $\tau : F \hookrightarrow \bar{L}_\pi \subset \mathbb{C}$ is an embedding lying over v. If π_v is unramified then $r_\lambda(\pi)|_{G_{F_v}}$ is crystalline.

(4) If c_v is a complex conjugation, then $\det r_\lambda(\pi)(c_v) = -1$.

Remark 4.21. The representations $r_\lambda(\pi)$ in fact form a strictly compatible system; see Section 5 of [Barnet-Lamb et al. 2014] for a discussion of this in a more general context.

Remark 4.22. Using the Jacquet–Langlands correspondence, we get Galois representations for the infinite-dimensional cuspidal automorphic representations of $G_D(\mathbb{A}^\infty)$ for any D. In fact, the proof actually uses the Jacquet–Langlands correspondence; in most cases, you can transfer to a D for which $S(D)$ contains all but one infinite place, and the Galois representations are then realized in the étale cohomology of the associated Shimura curve. The remaining Galois representations are constructed from these ones via congruences.

Fact 4.23 (cyclic base change). Let E/F be a cyclic extension of totally real fields of prime degree. Let $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ and let $\mathrm{Gal}(E/F)^\vee = \langle\delta_{E/F}\rangle$ (here $\mathrm{Gal}(E/F)^\vee$ is the dual abelian group of $\mathrm{Gal}(E/F)$). Let π be a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F^\infty)$ of weight (k, η). Then there is a cuspidal automorphic representation $\mathrm{BC}_{E/F}(\pi)$ of $\mathrm{GL}_2(\mathbb{A}_E^\infty)$ of weight $(\mathrm{BC}_{E/F}(k), \mathrm{BC}_{E/F}(\eta))$ such that:

(1) For all finite places v of E, $\mathrm{rec}_{E_v}(\mathrm{BC}_{E/F}(\pi)_v) = (\mathrm{rec}_{F_{v|F}}(\pi_{v|F}))|_{W_{E_v}}$. In particular, $r_\lambda(BC_{E/F}(\pi)) \cong r_\lambda(\pi)|_{G_E}$.

(2) $\mathrm{BC}_{E/F}(k)_v = k_{v|F}$, $\mathrm{BC}_{E/F}(\eta)_v = \eta_{v|F}$.

(3) $\mathrm{BC}_{E/F}(\pi) \cong \mathrm{BC}_{E/F}(\pi')$ if and only if $\pi \cong \pi' \otimes (\delta^i_{E/F} \circ \mathrm{Art}_F \circ \det)$ for some i.

(4) A cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_E^\infty)$ is in the image of $\mathrm{BC}_{E/F}$ if and only if $\pi \circ \sigma \cong \pi$.

Definition 4.24. We say that $r : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ is *modular* (of weight (k, η)) if it is isomorphic to $r_\lambda(\pi)$ for some cuspidal automorphic representation π (of weight (k, η)) and some place λ of L_π lying over p.

Proposition 4.25. *Suppose that $r : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ is a continuous representation, and that E/F is a finite solvable Galois extension of totally real fields. Then $r|_{G_E}$ is modular if and only if r is modular.*

Exercise 4.26. Prove the above proposition as follows:

(1) Use induction to reduce to the case that E/F is cyclic of prime degree.

(2) Suppose that $r|_{G_E}$ is modular, say $r|_{G_E} \cong r_\lambda(\pi)$. Use strong multiplicity one to show that $\pi \circ \sigma \cong \pi$. Deduce that there is an automorphic representation π' such that $\mathrm{BC}_{E/F}(\pi') = \pi$.

(3) Use Schur's lemma to deduce that there is a character χ of G_F such that $r \cong r_\lambda(\pi') \otimes \chi$. Conclude that r is modular.

We can make use of this result to make considerable simplifications in our proofs of modularity lifting theorems. It is frequently employed in conjunction with the following fact from class field theory.

Fact 4.27 [Taylor 2003, Lemma 2.2]. Let K be a number field, and let S be a finite set of places of K. For each $v \in S$, let L_v be a finite Galois extension of K_v. Then there is a finite solvable Galois extension M/K such that for each place w of M above a place $v \in S$ there is an isomorphism $L_v \cong M_w$ of K_v-algebras.

Note that we are allowed to have infinite places in S, so that if K is totally real we may choose to make L totally real by an appropriate choice of the L_v.

5. The Taylor–Wiles–Kisin method

In this section we prove our modularity lifting theorem, using the Taylor–Wiles–Kisin patching method. Very roughly, the idea of this method is to patch together spaces of modular forms of varying levels, allowing more and more ramification at places away from p, in such a way as to "smooth out" the singularities of global deformation rings, reducing the problem to one about local deformation rings. This patching procedure is (at least on first acquaintance) somewhat strange, as it involves making many noncanonical choices to identify spaces of modular forms with level structures at different primes.

5.1. Our aim now is to prove the following theorem. Let $p > 3$ be a prime, and let $L/\mathbb{Q}_p$ be a finite extension with ring of integers $\mathcal{O}$, maximal ideal λ, and residue field $\mathbb{F} = \mathcal{O}/\lambda$. Let F be a totally real number field, and assume that L is sufficiently large that L contains the images of all embeddings $F \hookrightarrow \bar{L}$.

Theorem 5.2. *Let $\rho, \rho_0 : G_F \to \mathrm{GL}_2(\mathcal{O})$ be two continuous representations, such that $\bar{\rho} = \rho \pmod{\lambda} = \rho_0 \pmod{\lambda}$. Assume that ρ_0 is modular, that ρ is geometric, and that $p > 3$. Assume further that the following properties hold*:

(1) *For all $\sigma : F \hookrightarrow L$, $\mathrm{HT}_\sigma(\rho) = \mathrm{HT}_\sigma(\rho_0)$, and contains two distinct elements.*

(2)
- *For all $v \mid p$, $\rho|_{G_{F_v}}$ and $\rho_0|_{G_{F_v}}$ are crystalline.*
- *p is unramified in F.*
- *For all $\sigma : F \hookrightarrow L$, the elements of $\mathrm{HT}_\sigma(\rho)$ differ by at most $p-2$.*

(3) $\mathrm{Im}\,\bar{\rho} \supseteq \mathrm{SL}_2(\mathbb{F}_p)$.

Then ρ is modular.

5.3. ***The integral theory of automorphic forms.*** In order to prove Theorem 5.2, we will need to study congruences between automorphic forms. This is easier to do if we work with automorphic forms on $G_D(\mathbb{A}^\infty)$, where $S(D) = S_\infty$. In order to do this, assume that $[F : \mathbb{Q}]$ is even. (We will reduce to this case by base change.) Then such a D exists, and we have $G_D(\mathbb{A}^\infty) \cong \mathrm{GL}_2(\mathbb{A}_F^\infty)$, and $(D \otimes_\mathbb{Q} \mathbb{R})^\times/(F \otimes_\mathbb{Q} \mathbb{R})^\times$ is compact.

Fix an isomorphism $\imath : \bar{L} \xrightarrow{\sim} \mathbb{C}$, and some $k \in \mathbb{Z}_{\geq 2}^{\mathrm{Hom}(F,\mathbb{C})}$, $\eta \in \mathbb{Z}^{\mathrm{Hom}(F,\mathbb{C})}$ with $w := k_\tau + 2\eta_\tau - 1$ independent of τ. Let $U = \prod_v U_v \subset \mathrm{GL}_2(\mathbb{A}_F^\infty)$ be a compact open subgroup, and let S be a finite set of finite places of F, not containing any of the places lying over p, with the property that if $v \notin S$, then $U_v = \mathrm{GL}_2(\mathcal{O}_{F_v})$.

Let $U_S := \prod_{v\in S} U_v$, write $U = U_S U^S$, let $\psi : U_S \to \mathcal{O}^\times$ be a continuous homomorphism (which implies that it has open kernel), and let $\chi_0 : \mathbb{A}_F^\times/F^\times \to \mathbb{C}^\times$ be an algebraic Grössencharacter with the properties that

- χ_0 is unramified outside S,
- for each place $v \mid \infty$, $\chi_0|_{(F_v^\times)^\circ}(x) = x^{1-w}$, and
- $\chi_0|_{\left(\prod_{v\in S} F_v^\times\right)\cap U_S} = \imath \circ \psi^{-1}$.

As in Theorem 2.43, this gives us a character

$$\chi_{0,\imath} : \mathbb{A}_F^\times/\overline{F^\times (F_\infty^\times)^\circ} \to \bar{L}^\times,$$
$$x \mapsto \Big(\prod_{\tau:F\hookrightarrow L} \tau(x_p)^{1-w}\Big)\imath^{-1}\Big(\prod_{\tau:F\hookrightarrow \mathbb{C}} \tau(x_\infty)\Big)^{w-1} \chi_0(x).$$

Our spaces of (p-adic) algebraic automorphic forms will be defined in a similar way to the more classical spaces defined in Section 4.8, but with the role of the infinite places being played by the places lying over p. Accordingly, we define coefficient systems in the following way. Assume that L is sufficiently large that it contains the image of $\chi_{0,\iota}$.

Let $\Lambda = \Lambda_{k,\eta,\iota} = \otimes_{\tau:F\hookrightarrow\mathbb{C}} \operatorname{Sym}^{k_\tau-2}(\mathcal{O}^2) \otimes (\wedge^2\mathcal{O}^2)^{\otimes\eta_\tau}$, and let $\mathrm{GL}_2(\mathcal{O}_{F,p}) := \prod_{v\,|\,p} \mathrm{GL}_2(\mathcal{O}_{F_v})$ act on Λ via $\iota^{-1}\tau$ on the τ-factor. In particular, $\Lambda \otimes_{\mathcal{O},\iota} \mathbb{C} \cong \otimes_{\tau:F\hookrightarrow\mathbb{C}} \operatorname{Sym}^{k_\tau-2}(\mathbb{C}^2) \otimes (\wedge^2\mathbb{C}^2)^{\otimes\eta_\tau}$, which has an obvious action of $\mathrm{GL}_2(F_\infty)$, and the two actions of $\mathrm{GL}_2(\mathcal{O}_{F,(p)})$ (via its embeddings into $\mathrm{GL}_2(\mathcal{O}_{F,p})$ and $\mathrm{GL}_2(F_\infty)$) are compatible.

Let A be a finite $\mathcal{O}$-module. Since D is fixed, we drop it from the notation from now on. We define $S(U, A) = S_{k,\eta,\iota,\psi,\chi_0}(U, A)$ to be the space of functions

$$\phi : D^\times \backslash \mathrm{GL}_2(\mathbb{A}_F^\infty) \to \Lambda \otimes_{\mathcal{O}} A$$

such that for all $g \in \mathrm{GL}_2(\mathbb{A}_F^\infty)$, $u \in U$, $z \in (\mathbb{A}_F^\infty)^\times$, we have

$$\phi(guz) = \chi_{0,\iota}(z)\psi(u_S)^{-1}u_p^{-1}\phi(g).$$

Since $D^\times \backslash \mathrm{GL}_2(\mathbb{A}_F^\infty)/U(\mathbb{A}_F^\infty)^\times$ is finite, we see in particular that $S(U, \mathcal{O})$ is a finite free $\mathcal{O}$-module. It has a Hecke action in the obvious way: let $\tilde{\mathbb{T}} := \mathcal{O}[T_v, S_v : v\nmid p, v \notin S]$, let ϖ_v be a uniformizer of F_v, and let T_v, S_v act via the usual double coset operators corresponding to $\left(\begin{smallmatrix}\varpi_v & 0\\ 0 & 1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\varpi_v & 0\\ 0 & \varpi_v\end{smallmatrix}\right)$. Let $\mathbb{T}_U$ be the image of $\tilde{\mathbb{T}}$ in $\operatorname{End}_{\mathcal{O}}(S(U, \mathcal{O}))$, so that $\mathbb{T}_U$ is a commutative $\mathcal{O}$-algebra which acts faithfully on $S(U, \mathcal{O})$, and is finite free as an $\mathcal{O}$-module.

As in [Taylor 2006, Lemma 1.3], to which we refer for more details, there is an isomorphism

$$S(U, \mathcal{O}) \otimes_{\mathcal{O},\iota} \mathbb{C} \xrightarrow{\sim} \operatorname{Hom}_{U_S}(\mathbb{C}(\psi^{-1}), S_{k,\eta}^{U^S,\chi_0}),$$

with the map being

$$\phi \mapsto (g \mapsto g_\infty^{-1}\iota(g_p\phi(g^\infty))),$$

where g_p acts on $\Lambda \otimes_{\mathcal{O},\iota} \mathbb{C}$ via the obvious extension of the action of $\mathrm{GL}_2(\mathcal{O}_{F,(p)})$ defined above, and the target of the isomorphism is the elements $\phi' \in S_{k,\eta}$ with $z\phi' = \chi_0(z)\phi'$ for all $z \in (\mathbb{A}_F^\infty)^\times$, $u\phi' = \psi(u_S)^{-1}\phi'$ for all $u \in U$. This isomorphism is compatible with the actions of $\tilde{\mathbb{T}}$ on each side. The target is isomorphic to

$$\oplus_\pi \operatorname{Hom}_{U_S}(\mathbb{C}(\psi^{-1}), \pi_S) \otimes \otimes'_{v\notin S}\pi_v^{\mathrm{GL}_2(\mathcal{O}_{F_v})},$$

where the sum is over the cuspidal automorphic representations π of $G_D(\mathbb{A}^\infty)$ of weight (k, η), which have central character χ_0 and are unramified outside of S (so that in particular, for $v \notin S$, $\pi_v^{\mathrm{GL}_2(\mathcal{O}_{F_v})}$ is a one-dimensional $\mathbb{C}$-vector space).

By strong multiplicity one, this means that we have an isomorphism

$$\mathbb{T}_U \otimes_{\mathcal{O},\iota} \mathbb{C} \cong \prod_{\pi \text{ as above, with } \mathrm{Hom}_{U_S}(\mathbb{C}(\psi^{-1}),\pi_S)\neq 0} \mathbb{C}$$

sending T_v, S_v to their eigenvalues on $\pi_v^{\mathrm{GL}_2(\mathcal{O}_{F_v})}$. (Note in particular that this shows that $\mathbb{T}_U$ is reduced.) This shows that there is a bijection between ι-linear ring homomorphisms $\theta : \mathbb{T}_U \to \mathbb{C}$ and the set of π as above, where π corresponds to the character taking T_v, S_v to their corresponding eigenvalues.

Each π has a corresponding Galois representation. Taking the product of these representations, we obtain a representation

$$\rho^{\mathrm{mod}} : G_F \to \prod_{\pi} \mathrm{GL}_2(\bar{L}) = \mathrm{GL}_2(\mathbb{T}_U \otimes_{\mathcal{O}} \bar{L}),$$

which is characterized by the properties that it is unramified outside of $S \cup \{v \mid p\}$, and for any $v \notin S$, $v \nmid p$, we have $\operatorname{tr} \rho^{\mathrm{mod}}(\mathrm{Frob}_v) = T_v$, $\det \rho^{\mathrm{mod}}(\mathrm{Frob}_v) = \#k(v) S_v$.

Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_U$. Then if $\mathfrak{p} \subsetneq \mathfrak{m}$ is a minimal prime, then there is an injection $\theta : \mathbb{T}_U/\mathfrak{p} \hookrightarrow \bar{L}$, which corresponds to some π as above. (This follows from the going-up and going-down theorems, and the fact that $\mathbb{T}_U$ is finitely generated and free over $\mathcal{O}$.) The semisimple mod p Galois representation corresponding to π can be conjugated to give a representation $\bar{\rho}_{\mathfrak{m}} : G_F \to \mathrm{GL}_2(\mathbb{T}_U/\mathfrak{m})$ (because the trace and determinant are valued in $\mathbb{T}_U/\mathfrak{m}$, which is a finite field, and thus has trivial Brauer group, so the Schur index is trivial). This is well defined (up to isomorphism) independently of the choice of $\mathfrak{p}$ and θ (by the Chebotarev density theorem).

Since $\mathbb{T}_U$ is finite over the complete local ring $\mathcal{O}$, it is semilocal, and we can write $\mathbb{T}_U = \prod_{\mathfrak{m}} \mathbb{T}_{U,\mathfrak{m}}$. Suppose now that $\bar{\rho}_{\mathfrak{m}}$ is absolutely irreducible. Then we have the representation

$$\rho_{\mathfrak{m}}^{\mathrm{mod}} : G_F \to \mathrm{GL}_2(\mathbb{T}_{U,\mathfrak{m}} \otimes_{\mathcal{O}} \bar{L}) = \prod_{\pi} \mathrm{GL}_2(\bar{L}),$$

where the product is over the π as above with $\bar{\rho}_{\pi,\iota} \cong \bar{\rho}_{\mathfrak{m}}$. Each representation to $\mathrm{GL}_2(\bar{L})$ can be conjugated to lie in $\mathrm{GL}_2(\mathcal{O}_{\bar{L}})$, and after further conjugation (so that the residual representations are equal to $\bar{\rho}_{\mathfrak{m}}$, rather than just conjugate to it), the image of $\rho_{\mathfrak{m}}^{\mathrm{mod}}$ lies in the subring of $\prod_{\pi} \mathrm{GL}_2(\mathcal{O}_{\bar{L}})$ consisting of elements whose image modulo the maximal ideal of $\mathcal{O}_{\bar{L}}$ lie in $\mathbb{T}_U/\mathfrak{m}$. We can then apply Lemma 3.7 to see that $\rho_{\mathfrak{m}}^{\mathrm{mod}}$ can be conjugated to lie in $\mathrm{GL}_2(\mathbb{T}_{U,\mathfrak{m}})$. We will write $\rho_{\mathfrak{m}}^{\mathrm{mod}} : G_F \to \mathrm{GL}_2(\mathbb{T}_{U,\mathfrak{m}})$ for the resulting representation from now on.

We will sometimes want to consider Hecke operators at places in S. To this end, let $T \subseteq S$ satisfy $\psi|_{U_T} = 1$, and choose $g_v \in \mathrm{GL}_2(F_v)$ for each $v \in T$. Set $W_v = [U_v g_v U_v]$, and define $\mathbb{T}_U \subseteq \mathbb{T}'_U \subseteq \mathrm{End}_{\mathcal{O}}(S(U, \mathcal{O}))$ by adjoining the W_v for

$v \in T$. This is again commutative, and finite and flat over $\mathcal{O}$. However, it need not be reduced; indeed, we have

$$\mathbb{T}'_U \otimes_{\mathcal{O},\iota} \mathbb{C} \cong \oplus_\pi \otimes_{v\in T} \{\text{ subalgebra of } \mathrm{End}_{\mathbb{C}}(\pi_v^{U_v}) \text{ generated by } W_v\},$$

so that there is a bijection between ι-linear homomorphisms $\mathbb{T}'_U \to \mathbb{C}$ and tuples $(\pi, \{\alpha_v\}_{v\in T})$, where α_v is an eigenvalue of W_v on $\pi_v^{U_v}$. (Note that we will not explicitly use the notation $\mathbb{T}'_U$ again for a Hecke algebra, but that for example the Hecke algebras $\mathbb{T}_{U_Q}$ used in the patching argument below, which incorporate Hecke operators at the places in Q, are an example of this construction.)

We can write

$$\mathrm{GL}_2(\mathbb{A}_F^\infty) = \coprod_{i\in I} D^\times g_i U (\mathbb{A}_F^\infty)^\times$$

for some finite indexing set I, and so we have an injection $S(U, A) \hookrightarrow \oplus_{i\in I}(\Lambda \otimes_{\mathcal{O}} A)$, by sending $\phi \mapsto (\phi(g_i))$. To determine the image, we need to consider when we can have $g_i = \delta g_i u z$ for $\delta \in D^\times$, $z \in (\mathbb{A}_F^\infty)^\times$, $u \in U$ (because then $\phi(g_i) = \phi(\delta g_i u z) = \chi_{0,\iota}(z)\psi(u_S)^{-1}u_p^{-1}\phi(g_i)$). We see in this way that we obtain an isomorphism

$$S(U, A) \xrightarrow{\sim} \oplus_{i\in I}(\Lambda \otimes A)^{(U(\mathbb{A}_F^\infty)^\times \cap g_i^{-1} D^\times g_i)/F^\times}.$$

We need to have some control on these finite groups

$$G_i := (U(\mathbb{A}_F^\infty)^\times \cap g_i^{-1} D^\times g_i)/F^\times.$$

(Note that they are finite, because $D^\times$ is discrete in $G_D(\mathbb{A}^\infty)$.) Since we have assumed that $p > 3$ and p is unramified in F, we see that $[F(\zeta_p) : F] > 2$. Then we claim that G_i has order prime to p. To see this, note that if $g_i^{-1}\delta g_i$ is in this group, with $\delta \in D^\times$, then $\delta^2/\det\delta \in D^\times \cap g_i U g_i^{-1}(\det U)$, the intersection of a discrete set and a compact set, so $\delta^2/\det\delta$ has finite order, i.e., is a root of unity. However any element of D generates an extension of F of degree at most 2, so by the assumption that $[F(\zeta_p) : F] > 2$, it must be a root of unity of degree prime to p, and there is some $p \nmid N$ with $\delta^{2N} \in F^\times$, so that $g_i^{-1}\delta g_i$ has order prime to p, as required.

Proposition 5.4. (1) *We have $S(U, \mathcal{O}) \otimes_{\mathcal{O}} A \xrightarrow{\sim} S(U, A)$.*

(2) *If V is an open normal subgroup of U with $\#(U/V)$ a power of p, then $S(V, \mathcal{O})$ is a free $\mathcal{O}[U/V(U \cap (\mathbb{A}_F^\infty)^\times)]$-module.*

Proof. (1) This is immediate from the isomorphism $S(U, A) \xrightarrow{\sim} \oplus_{i\in I}(\Lambda \otimes A)^{G_i}$, because the fact that the G_i have order prime to p means that $(\Lambda \otimes A)^{G_i} = (\Lambda)^{G_i} \otimes A$.

(2) Write $U = \coprod_{j\in J} u_j V(U \cap (\mathbb{A}_F^\infty)^\times)$. We claim that we have $\mathrm{GL}_2(\mathbb{A}_F^\infty) = \coprod_{i\in I, j\in J} D^\times g_i u_j V(\mathbb{A}_F^\infty)^\times$, from which the result is immediate. To see this, we need to show that if $g_i u_j = \delta g_{i'} u_{j'} v z$ then $i = i'$ and $j = j'$.

That $i = i'$ is immediate from the definition of I, so we have $u_{j'}vu_j^{-1}z = g_i^{-1}\delta^{-1}g_i$. As above, there is some positive integer N coprime to p such that $\delta^N \in F^\times$, thus $(u_{j'}vu_j^{-1})^N \in (\mathbb{A}_F^\infty)^\times$. Since V is normal in U, we can write $(u_{j'}vu_j^{-1})^N = (u_{j'}u_j^{-1})^N v'$ for some $v' \in V$, so that $(u_{j'}u_j^{-1})^N \in V(U \cap (\mathbb{A}_F^\infty)^\times)$. Since $\#(U/V)$ is a power of p, we see that in fact $u_{j'}u_j^{-1} \in V(U \cap (\mathbb{A}_F^\infty)^\times)$, so that $j = j'$ by the definition of J. □

5.5. ***Base change.*** We begin the proof of Theorem 5.2 by using base change to reduce to a special case. By Facts 4.23 and 4.27, we can replace F by a solvable totally real extension which is unramified at all primes above p, and assume that:

- $[F : \mathbb{Q}]$ is even.
- $\bar{\rho}$ is unramified outside p.
- For all places $v \nmid p$, both $\rho(I_{F_v})$ and $\rho_0(I_{F_v})$ are unipotent (possibly trivial).
- If ρ or ρ_0 are ramified at some place $v \nmid p$, then $\bar{\rho}|_{G_{F_v}}$ is trivial, and $\#k(v) \equiv 1 \pmod{p}$.
- $\det \rho = \det \rho_0$. [To see that we can assume this, note that the assumption that ρ, ρ_0 are crystalline with the same Hodge–Tate weights for all places dividing p implies that $\det \rho / \det \rho_0$ is unramified at all places dividing p. Since we have already assumed that $\rho(I_{F_v})$ and $\rho_0(I_{F_v})$ are unipotent for all places $v \nmid p$, we see that the character $\det \rho / \det \rho_0$ is unramified at all places, and thus has finite order. Since it is residually trivial, it has p-power order, and is thus trivial on all complex conjugations; so the extension cut out by its kernel is a finite, abelian, totally real extension which is unramified at all places dividing p.]

We will assume from now on that all of these conditions hold. Write χ for $\det \rho = \det \rho_0$; then we have $\chi \varepsilon_p = \chi_{0,\imath}$ for some algebraic Grössencharacter χ_0.

From now on, we will assume without further comment that the coefficient field L is sufficiently large, in the sense that L contains a primitive p-th root of unity, and for all $g \in G_F$, $\mathbb{F}$ contains the eigenvalues of $\bar{\rho}(g)$.

5.6. ***Patching.*** Having used base change to impose the additional conditions of the previous section, we are now in a position to begin the main patching argument.

We let D/F be a quaternion algebra ramified at exactly the infinite places (which exists by our assumption that $[F : \mathbb{Q}]$ is even). By the Jacquet–Langlands correspondence, we can and will work with automorphic representations of $G_D(\mathbb{A}^\infty)$ from now on.

Let T_p be the set of places of F lying over p, let T_r be the set of places not lying over p at which ρ or ρ_0 is ramified, and let $T = T_p \coprod T_r$. If $v \in T_r$, write σ_v for a choice of topological generator of I_{F_v}/P_{F_v}. By our assumptions above, if $v \in T_r$ then $\bar{\rho}|_{G_{F_v}}$ is trivial, $\rho|_{I_{F_v}}$, $\rho_0|_{I_{F_v}}$ are unipotent, and $\#k(v) \equiv 1 \pmod{p}$.

The patching argument will involve the consideration of various finite sets Q of auxiliary finite places. We will always assume that if $v \in Q$, then

- $v \notin T$,
- $\#k(v) \equiv 1 \pmod{p}$, and
- $\bar{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues, which we denote $\bar{\alpha}_v$ and $\bar{\beta}_v$.

For each set Q of places satisfying these conditions, we define deformation problems $\mathcal{S}_Q = (T \cup Q, \{\mathcal{D}_v\}, \chi)$ and $\mathcal{S}'_Q = (T \cup Q, \{\mathcal{D}'_v\}, \chi)$ as follows. (The reason for considering both problems is that the objects without a prime are the ones that we ultimately wish to study, but the objects with a prime have the advantage that the ring $(R^{\mathrm{loc},'})^{\mathrm{red}}$ defined below is irreducible. We will exploit this irreducibility, and the fact that the two deformation problems agree modulo p.) Let ζ be a fixed primitive p-th root of unity in L:

- If $v \in T_p$, then $\mathcal{D}_v = \mathcal{D}'_v$ is chosen so that $R^{\square}_{\bar{\rho}|_{G_{F_v}},\chi}/I(\mathcal{D}_v) = R^{\square}_{\bar{\rho}|_{G_{F_v}},\chi,\mathrm{cr},\{\mathrm{HT}_\sigma(\rho)\}}$.
- If $v \in Q$, then $\mathcal{D}_v = \mathcal{D}'_v$ consists of all lifts of $\bar{\rho}|_{G_{F_v}}$ with determinant χ.
- If $v \in T_r$, then $\mathcal{D}_v$ consists of all lifts of $\bar{\rho}|_{G_{F_v}}$ with $\mathrm{char}_{\rho(\sigma_v)}(X) = (X-1)^2$, while $\mathcal{D}'_v$ consists of all lifts with $\mathrm{char}_{\rho(\sigma_v)}(X) = (X-\zeta)(X-\zeta^{-1})$.

(In particular, the difference between $\mathcal{S}_Q$ and $\mathcal{S}_\varnothing$ is that we have allowed our deformations to ramify at places in Q.) We write

$$R^{\mathrm{loc}} = \widehat{\otimes}_{v\in T,\mathcal{O}} R^{\square}_{\bar{\rho}|_{G_{F_v}},\chi}/I(\mathcal{D}_v), \qquad R^{\mathrm{loc},'} = \widehat{\otimes}_{v\in T,\mathcal{O}} R^{\square}_{\bar{\rho}|_{G_{F_v}},\chi}/I(\mathcal{D}'_v).$$

Then $R^{\mathrm{loc}}/\lambda = R^{\mathrm{loc},'}/\lambda$, because $\zeta \equiv 1 \pmod{\lambda}$. In addition, we see from Theorems 3.28 and 3.38 that

- $(R^{\mathrm{loc},'})^{\mathrm{red}}$ is irreducible, $\mathcal{O}$-flat, and has Krull dimension $1 + 3\#T + [F:\mathbb{Q}]$,
- $(R^{\mathrm{loc}})^{\mathrm{red}}$ is $\mathcal{O}$-flat, equidimensional of Krull dimension $1+3\#T+[F:\mathbb{Q}]$, and reduction modulo λ gives a bijection between the irreducible components of $\operatorname{Spec} R^{\mathrm{loc}}$ and those of $\operatorname{Spec} R^{\mathrm{loc}}/\lambda$.

We have the global analogues $R^{\mathrm{univ}}_Q := R^{\mathrm{univ}}_{\bar{\rho},\mathcal{S}_Q}$, $R^{\mathrm{univ},'}_Q := R^{\mathrm{univ}}_{\bar{\rho},\mathcal{S}'_Q}$, $R^{\square}_Q := R^{\square_T}_{\bar{\rho},\mathcal{S}_Q}$, $R^{\square,'}_Q := R^{\square_T}_{\bar{\rho},\mathcal{S}'_Q}$, and we have $R^{\mathrm{univ}}_Q/\lambda = R^{\mathrm{univ},'}_Q/\lambda$, $R^{\square}_Q/\lambda = R^{\square,'}_Q/\lambda$. There are obvious natural maps $R^{\mathrm{loc}} \to R^{\square}_Q$, $R^{\mathrm{loc},'} \to R^{\square,'}_Q$, and these maps agree after reduction $\bmod \lambda$.

We can and do fix representatives ρ^{univ}_Q, $\rho^{\mathrm{univ},'}_Q$ for the universal deformations of $\bar{\rho}$ over R^{univ}_Q, $R^{\mathrm{univ},'}_Q$ respectively, which are compatible with the choices of $\rho^{\mathrm{univ}}_\varnothing$, $\rho^{\mathrm{univ},'}_\varnothing$, and so that the induced surjections

$$R^{\mathrm{univ}}_Q \twoheadrightarrow R^{\mathrm{univ}}_\varnothing, \;\; R^{\mathrm{univ},'}_Q \twoheadrightarrow R^{\mathrm{univ},'}_\varnothing$$

are identified modulo λ.

Fix a place $v_0 \in T$, and set $\mathcal{J} := \mathcal{O}[[X_{v,i,j}]]_{v\in T, i,j=1,2}/(X_{v_0,1,1})$. Let $\mathfrak{a}$ be the ideal of $\mathcal{J}$ generated by the $X_{v,i,j}$. Then our choice of ρ_Q^{univ} gives an identification $R_Q^{\square} \xrightarrow{\sim} R_Q^{\mathrm{univ}}\widehat{\otimes}_{\mathcal{O}}\mathcal{J}$, corresponding to the universal T-framed deformation $(\rho_Q^{\mathrm{univ}}, \{1+(X_{v,i,j})\}_{v\in T})$.

Now, by Exercise 3.34, for each place $v \in Q$ we have an isomorphism $\rho_Q^{\mathrm{univ}}|_{G_{F_v}} \cong \chi_\alpha \oplus \chi_\beta$, where $\chi_\alpha, \chi_\beta : G_{F_v} \to (R_Q^{\mathrm{univ}})^\times$, where $(\chi_\alpha \bmod \mathfrak{m}_{R_Q^{\mathrm{univ}}})(\mathrm{Frob}_v) = \bar{\alpha}_v$, $(\chi_\beta \bmod \mathfrak{m}_{R_Q^{\mathrm{univ}}})(\mathrm{Frob}_v) = \bar{\beta}_v$.

Let Δ_v be the maximal p-power quotient of $k(v)^\times$ (which we sometimes regard as a subgroup of $k(v)^\times$). Then $\chi_\alpha|_{I_{F_v}}$ factors through the composite

$$I_{F_v} \twoheadrightarrow I_{F_v}/P_{F_v} \twoheadrightarrow k(v)^\times \twoheadrightarrow \Delta_v,$$

and if we write $\Delta_Q = \prod_{v\in Q}\Delta_v$, $\left(\prod \chi_\alpha\right) : \Delta_Q \to (R_Q^{\mathrm{univ}})^\times$, then we see that $(R_Q^{\mathrm{univ}})_{\Delta_Q} = R_{\varnothing}^{\mathrm{univ}}$.

The isomorphism $R_Q^{\square} \xrightarrow{\sim} R_Q^{\mathrm{univ}}\widehat{\otimes}_{\mathcal{O}}\mathcal{J}$ and the homomorphism $\Delta_Q \to (R_Q^{\mathrm{univ}})^\times$ together give a homomorphism $\mathcal{J}[\Delta_Q] \to R_Q^{\square}$. In the same way, we have a homomorphism $\mathcal{J}[\Delta_Q] \to R_Q^{\square,\prime}$, and again these agree modulo λ. If we write $\mathfrak{a}_Q := \langle \mathfrak{a}, \delta - 1\rangle_{\delta\in\Delta_Q} \lhd \mathcal{J}[\Delta_Q]$, then we see that $R_Q^{\square}/\mathfrak{a}_Q = R_{\varnothing}^{\mathrm{univ}}$, and that $R_Q^{\square,\prime}/\mathfrak{a}_Q = R_{\varnothing}^{\mathrm{univ},\prime}$, and again these agree modulo λ.

We now examine the spaces of modular forms that we will patch. We have our fixed isomorphism $\imath : \bar{L} \xrightarrow{\sim} \mathbb{C}$, and an algebraic Grössencharacter χ_0 such that $\chi\varepsilon_p = \chi_{0,\imath}$. Define k, η by $\mathrm{HT}_\tau(\rho_0) = \{\eta_{\imath\tau}, \eta_{\imath\tau} + k_{\imath\tau} - 1\}$. We define compact open subgroups $U_Q = \prod U_{Q,v}$, where

- $U_{Q,v} = \mathrm{GL}_2(\mathcal{O}_{F_v})$ if $v \notin Q \cup T_r$,
- $U_{Q,v} = U_0(v) = \left\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{v}\right\}$ if $v \in T_r$, and
- $U_{Q,v} = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in U_0(v) \mid a/d \pmod{v} \in k(v)^\times \mapsto 1 \in \Delta_v\right\}$ if $v \in Q$.

We let $\psi : \prod_{v\in Q\cup T_r} U_{Q,v} \to \mathcal{O}^\times$ be the trivial character. Similarly, we set $U_Q' = U_Q$, and we define $\psi' : \prod_{v\in Q\cup T_r} U_{Q,v} \to \mathcal{O}^\times$ in the following way. For each $v \in T_r$, we have a homomorphism $U_{Q,v} \to k(v)^\times$ given by sending $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to $a/d \pmod{v}$, and we compose these characters with the characters $k(v)^\times \to \mathcal{O}^\times$ sending the image of σ_v to ζ, where σ_v is a generator of I_{F_v}/P_{F_v}. We let ψ' be trivial at the places in Q.

We obtain spaces of modular forms $S(U_Q, \mathcal{O})$, $S(U_Q', \mathcal{O})$ and corresponding Hecke algebras $\mathbb{T}_{U_Q}$, $\mathbb{T}_{U_Q'}$, generated by the Hecke operators T_v, S_v with $v \notin T \cup Q$, together with Hecke operators U_{ϖ_v} for $v \in Q$ (depending on a chosen uniformizer ϖ_v) defined by

$$U_{\varpi_v} = \left[U_{Q,v}\begin{pmatrix} \varpi_v & 0 \\ 0 & 1 \end{pmatrix}U_{Q,v}\right].$$

Note that $\psi = \psi' \pmod{\lambda}$, so we have $S(U_{\varnothing}, \mathcal{O})/\lambda = S(U_{\varnothing}', \mathcal{O})/\lambda$. We let $\mathfrak{m}_{\varnothing} \lhd \mathbb{T}_{U_{\varnothing}}$ be the ideal generated by λ and the $\operatorname{tr}\bar{\rho}(\mathrm{Frob}_v) - T_v$, $\det\bar{\rho}(\mathrm{Frob}_v) - \#k(v)S_v$,

$v \notin T$. This is a maximal ideal of $\mathbb{T}_{U_\varnothing}$, because it is the kernel of the homomorphism $\mathbb{T}_{U_\varnothing} \to \mathcal{O} \twoheadrightarrow \mathbb{F}$, where the map $\mathbb{T}_{U_\varnothing} \to \mathcal{O}$ is the one coming from the automorphicity of ρ_0, sending $T_v \mapsto \operatorname{tr} \rho_0(\mathrm{Frob}_v)$, $S_v \mapsto \#k(v)^{-1} \det \rho_0(\mathrm{Frob}_v)$.

Write $\mathbb{T}_\varnothing := \mathbb{T}_{U_\varnothing, \mathfrak{m}_\varnothing}$. We have a lifting $\rho^{\mathrm{mod}} : G_F \to \mathrm{GL}_2(\mathbb{T}_\varnothing)$ of type $\mathcal{S}_\varnothing$, so by the universal property of $R^{\mathrm{univ}}_\varnothing$, we have a surjection $R^{\mathrm{univ}}_\varnothing \twoheadrightarrow \mathbb{T}_\varnothing$ (it is surjective because local-global compatibility shows that the Hecke operators generating $\mathbb{T}_\varnothing$ are in the image). Similarly, we have a surjection $R^{\mathrm{univ},'}_\varnothing \twoheadrightarrow \mathbb{T}'_\varnothing := \mathbb{T}_{U'_\varnothing, \mathfrak{m}_\varnothing}$. Set $S_\varnothing := S(U_\varnothing, \mathcal{O})_{\mathfrak{m}_\varnothing}$, $S'_\varnothing := S(U'_\varnothing, \mathcal{O})_{\mathfrak{m}_\varnothing}$. Then the identification $R^{\mathrm{univ}}_\varnothing/\lambda \cong R^{\mathrm{univ},'}_\varnothing/\lambda$ is compatible with $S_\varnothing/\lambda = S'_\varnothing/\lambda$.

Lemma 5.7. *If* $\mathrm{Supp}_{R^{\mathrm{univ}}_\varnothing}(S_\varnothing) = \mathrm{Spec}\, R^{\mathrm{univ}}_\varnothing$, *then* ρ *is modular.*

Proof. Suppose that $\mathrm{Supp}_{R^{\mathrm{univ}}_\varnothing}(S_\varnothing) = \mathrm{Spec}\, R^{\mathrm{univ}}_\varnothing$. Since $S_\varnothing$ is a faithful $\mathbb{T}_\varnothing$-module by definition, we see that $\ker(R^{\mathrm{univ}}_\varnothing \to \mathbb{T}_\varnothing)$ is nilpotent, so that $(R^{\mathrm{univ}}_\varnothing)^{\mathrm{red}} \xrightarrow{\sim} \mathbb{T}_\varnothing$. Then ρ corresponds to some homomorphism $R^{\mathrm{univ}}_\varnothing \to \mathcal{O}$, and thus to a homomorphism $\mathbb{T}_\varnothing \to \mathcal{O}$, and the composite of this homomorphism with $\imath : \mathcal{O} \hookrightarrow \mathbb{C}$ corresponds to a cuspidal automorphic representation π of $G_D(\mathbb{A}^\infty)$ of weight (k, η), which by construction has the property that $\rho \cong \rho_{\pi,\imath}$, as required. □

To show that $\mathrm{Supp}_{R^{\mathrm{univ}}_\varnothing}(S_\varnothing) = \mathrm{Spec}\, R^{\mathrm{univ}}_\varnothing$, we will study the above constructions as Q varies. Let $\mathfrak{m}_Q \lhd \mathbb{T}_{U_Q}$ be the maximal ideal generated by λ, the $\operatorname{tr} \bar{\rho}(\mathrm{Frob}_v) - T_v$ and $\det \bar{\rho}(\mathrm{Frob}_v) - \#k(v) S_v$ for $v \notin T \cup Q$, and the $U_{\varpi_v} - \bar{\alpha}_v$ for $v \in Q$.

Write $S_Q = S_{U_Q} := S(U_Q, \mathcal{O})_{\mathfrak{m}_Q}$ and $\mathbb{T}_Q := (\mathbb{T}_{U_Q})_{\mathfrak{m}_Q}$. We have a homomorphism $\Delta_Q \to \mathrm{End}(S_Q)$, given by sending $\delta \in \Delta_v$ to $\left(\begin{smallmatrix} \delta & 0 \\ 0 & 1 \end{smallmatrix}\right) \in U_0(v)$. We also have another homomorphism $\Delta_Q \to \mathrm{End}(S_Q)$, given by the composite

$$\Delta_Q \to R^{\mathrm{univ}}_Q \twoheadrightarrow \mathbb{T}_Q \to \mathrm{End}(S_Q).$$

Let $U_{Q,0} := \prod_{v \notin Q} U_{Q,v} \prod_{v \in Q} U_0(v)$. Then U_Q is a normal subgroup of $U_{Q,0}$, and $U_{Q,0}/U_Q = \Delta_Q$.

We now examine the consequences of local-global compatibility at the places in Q.

Proposition 5.8. (1) *The two homomorphisms* $\Delta_Q \to \mathrm{End}(S_Q)$ (*the other one coming via* R^{univ}_Q) *are equal.*

(2) S_Q *is finite free over* $\mathcal{O}[\Delta_Q]$.

Proof. A homomorphism $\theta : \mathbb{T}_Q \to \bar{L} \xrightarrow{\sim} \mathbb{C}$ corresponds to a cuspidal automorphic representation π, and for each $v \in Q$ the image α_v of U_{ϖ_v} is such that α_v is an eigenvalue of U_{ϖ_v} on $\pi_v^{U_{Q,v}}$.

It can be checked that since $\pi_v^{U_{Q,v}} \neq 0$, π_v is necessarily a subquotient of $\chi_1 \times \chi_2$ for some tamely ramified characters $\chi_1, \chi_2 : F_v^\times \to \mathbb{C}^\times$. Then one checks explicitly that

$$(\chi_1 \times \chi_2)^{U_{Q,v}} \cong \mathbb{C}\phi_1 \oplus \mathbb{C}\phi_w,$$

where $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\phi_1(1) = \phi_w(w) = 1$, and $\operatorname{Supp}\phi_1 = B(F_v)U_{Q,v}$, $\operatorname{Supp}\phi_w = B(F_v)wU_{Q,v}$.

Further explicit calculation shows that

$$U_{\varpi_v}\phi_1 = \#k(v)^{1/2}\chi_1(\varpi_v)\phi_1 + X\phi_w$$

for some X, which is 0 if χ_1/χ_2 is ramified, and

$$U_{\varpi_v}\phi_w = \#k(v)^{1/2}\chi_2(\varpi_v)\phi_w.$$

By local-global compatibility $\iota^{-1}(\#k(v)^{1/2}\chi_1(\varpi_v))$ and $\iota^{-1}(\#k(v)^{1/2}\chi_2(\varpi_v))$ are the eigenvalues of $\rho_{\pi,\iota}(\mathrm{Frob}_v)$, so one of them is a lift of $\bar{\alpha}_v$, and one is a lift of $\bar{\beta}_v$. As a consequence, we see that $\chi_1/\chi_2 \neq |\cdot|^{\pm 1}$ (as if this equality held, we would have $\bar{\alpha}_v/\bar{\beta}_v \equiv \#k(v)^{\pm 1} \equiv 1 \pmod{\lambda}$, contradicting our assumption that $\bar{\alpha}_v \neq \bar{\beta}_v$). Consequently we have $\pi_v = \chi_1 \times \chi_2 \cong \chi_2 \times \chi_1$, so that without loss of generality we have $\bar{\chi}_1(\varpi_v) = \bar{\beta}_v$, $\bar{\chi}_2(\varpi_v) = \bar{\alpha}_v$.

It is also easily checked that

$$\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}\phi_1 = \chi_1(\delta)\phi_1, \quad \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}\phi_w = \chi_2(\delta)\phi_w.$$

We see that $S_Q \otimes_{\mathcal{O},\iota} \mathbb{C} = \oplus_\pi \otimes_{v\in Q} X_v$, where X_v is the 1-dimensional space where U_{ϖ_v} acts via a lift of $\bar{\alpha}_v$. Since this space is spanned by ϕ_w, we see that Δ_v acts on S_Q via $\chi_2 = \chi_\alpha \circ \mathrm{Art}$. This completes the proof of the first part.

Finally, the second part is immediate from Proposition 5.4(2). □

Fix a place $v \in Q$. Since $\bar{\alpha}_v \neq \bar{\beta}_v$, by Hensel's lemma we may write

$$\operatorname{char} \rho_{\varnothing}^{\mathrm{mod}}(\mathrm{Frob}_v) = (X - A_v)(X - B_v)$$

for some $A_v, B_v \in \mathbb{T}_\varnothing$ with $A_v \equiv \bar{\alpha}_v$, $B_v \equiv \bar{\beta}_v \pmod{\mathfrak{m}_\varnothing}$.

Proposition 5.9. *We have an isomorphism* $\prod_{v\in Q}(U_{\varpi_v} - B_v) : S_\varnothing \xrightarrow{\sim} S(U_{Q,0}, \mathcal{O})_{\mathfrak{m}_Q}$ (*with the morphism being defined by viewing the source and target as submodules of* $S(U_{Q,0}, \mathcal{O})_{\mathfrak{m}_\varnothing}$).

Proof. We claim that it is enough to prove that the map is an isomorphism after tensoring with L, and an injection after tensoring with $\mathbb{F}$. To see this, write $X := S_\varnothing$, $Y := S(U_{Q,0}, \mathcal{O})_{\mathfrak{m}_Q}$, and write Q for the cokernel of the map $X \to Y$. Then X, Y are finite free $\mathcal{O}$-modules, and if the map $X \otimes L \to Y \otimes L$ is injective, then so is the map $X \to Y$, so that we have a short exact sequence $0 \to X \to Y \to Q \to 0$. Tensoring with L, we have $Q \otimes L = 0$. Tensoring with $\mathbb{F}$, we obtain an exact sequence $0 \to Q[\lambda] \to X \otimes \mathbb{F} \to Y \otimes \mathbb{F} \to Q \otimes \mathbb{F} \to 0$, so we have $Q[\lambda] = 0$. Thus $Q = 0$, as required.

In order to check that we have an isomorphism after tensoring with L, it is enough to check that the induced map $\prod_{v\in Q}(U_{\varpi_v} - B_v) : S_\varnothing \otimes_{\mathcal{O},\iota} \mathbb{C} \to S(U_{Q,0}, \mathcal{O})_{\mathfrak{m}_Q} \otimes_{\mathcal{O},\iota} \mathbb{C}$

is an isomorphism. This is easily checked: $S_\varnothing \otimes \mathbb{C} \cong \oplus_\pi \otimes_{v\in Q} (\chi_{1,v} \times \chi_{2,v})^{\mathrm{GL}_2(\mathcal{O}_{F_v})}$, and $(\chi_{1,v} \times \chi_{2,v})^{\mathrm{GL}_2(\mathcal{O}_{F_v})} = \mathbb{C}\phi_0$, where ϕ_0 is as in Exercise 4.7(3). Similarly, $S(U_{Q,0}, \mathcal{O})_{\mathfrak{m}_Q} \otimes_{\mathcal{O},\iota} \mathbb{C} = \oplus_\pi \otimes_{v\in Q} M_v$, where M_v is the subspace of $(\chi_{1,v} \times \chi_{2,v})^{U_0(v)}$ on which U_{ϖ_v} acts via a lift of $\bar{\alpha}_v$, which is spanned by ϕ_w. Since the natural map $(\chi_{1,v} \times \chi_{2,v})^{\mathrm{GL}_2(\mathcal{O}_{F_v})} \to (\chi_{1,v} \times \chi_{2,v})^{U_0(v)}$ sends $\phi_0 \mapsto \phi_1 + \phi_w$ (as $\phi_0(1) = \phi_0(w) = 1$), the result follows.

It remains to check injectivity after tensoring with $\mathbb{F}$. The kernel of the map, if nonzero, would be a nonzero finite module for the Artinian local ring $\mathbb{T}_\varnothing/\lambda$, and would thus have nonzero $\mathfrak{m}_\varnothing$-torsion, so it suffices to prove that the induced map

$$\prod_{v\in Q} (U_{\varpi_v} - B_v) : (S_\varnothing \otimes \mathbb{F})[\mathfrak{m}_\varnothing] \to S(U_{Q,0}, \mathcal{O})_{\mathfrak{m}_Q} \otimes \mathbb{F}$$

is an injection. By induction on $\#Q$, it suffices to prove this in the case that $Q = \{v\}$. Suppose for the sake of contradiction that there is a nonzero $x \in (S_\varnothing \otimes \mathbb{F})[\mathfrak{m}_\varnothing]$ with $(U_{\varpi_v} - \bar{\beta}_v)x = 0$. Since $x \in S_\varnothing \otimes \mathbb{F}$, we also have $T_v x = (\bar{\alpha}_v + \bar{\beta}_v)x$, and we will show that these two equations together lead to a contradiction.

Now, x is just a function $D^\times \backslash \mathrm{GL}_2(\mathbb{A}_F^\infty) \to \Lambda \otimes \mathbb{F}$, on which $\mathrm{GL}_2(\mathbb{A}_F^\infty)$ acts by right translation. If we make the action of the Hecke operators explicit, we find that there are g_i such that

$$U_v = \coprod_i g_i U_{Q,v}$$

and

$$T_v = \left(\coprod_i g_i \,\mathrm{GL}_2(\mathcal{O}_{F_v})\right) \coprod \begin{pmatrix} 1 & 0 \\ 0 & \varpi_v \end{pmatrix} \mathrm{GL}_2(\mathcal{O}_{F_v}),$$

so that we have $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \varpi_v \end{smallmatrix}\right)x = T_v x - U_{\varpi_v} x = \bar{\alpha}_v x$. Then $\left(\begin{smallmatrix} \varpi_v & 0 \\ 0 & 1 \end{smallmatrix}\right)x = w\left(\begin{smallmatrix} 1 & 0 \\ 0 & \varpi_v \end{smallmatrix}\right)wx = \bar{\alpha}_v x$, and $U_{\varpi_v} x = \sum_{a\in k(v)} \left(\begin{smallmatrix} \varpi_v & a \\ 0 & 1 \end{smallmatrix}\right)x = \sum_{a\in k(v)} \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \varpi_v & 0 \\ 0 & 1 \end{smallmatrix}\right)x = \#k(v)\bar{\alpha}_v x = \bar{\alpha}_v x$. But $U_{\varpi_v} x = \bar{\beta}_v x$, so $\bar{\alpha}_v = \bar{\beta}_v$, a contradiction. □

Set $S_Q^\square := S_Q \otimes_{R_Q^{\mathrm{univ}}} R_Q^\square$. Then we have $S_Q^\square/\mathfrak{a}_Q = S(U_{Q,0}, \mathcal{O})_{\mathfrak{m}_Q} \xrightarrow{\sim} S_\varnothing$, compatibly with the isomorphism $R_Q^\square/\mathfrak{a}_Q \xrightarrow{\sim} R_\varnothing^{\mathrm{univ}}$. Also, $S_Q^\square$ is finite free over $\mathcal{J}[\Delta_Q]$.

We now return to the Galois side. By Proposition 3.24, we can and do choose a presentation

$$R^{\mathrm{loc}}[\![x_1, \ldots, x_{h_Q}]\!] \twoheadrightarrow R_Q^\square,$$

where $h_Q = \#T + \#Q - 1 - [F : \mathbb{Q}] + \dim_{\mathbb{F}} H_Q^1(G_{F,T}, (\mathrm{ad}^0 \bar{\rho})(1))$, and

$$H_Q^1(G_{F,T}, (\mathrm{ad}^0 \bar{\rho})(1)) = \ker\big(H^1(G_{F,T}, (\mathrm{ad}^0 \bar{\rho})(1)) \to \oplus_{v\in Q} H^1(G_{k(v)}, (\mathrm{ad}^0 \bar{\rho})(1))\big).$$

The following result will provide us with the sets Q that we will use.

Proposition 5.10. *Let* $r = \max(\dim H^1(G_{F,T}, (\mathrm{ad}^0 \bar{\rho})(1)), 1 + [F : \mathbb{Q}] - \#T)$. *For each* $N \geq 1$, *there exists a set* Q_N *of places of* F *such that*:

- $Q_N \cap T = \varnothing$.
- *If* $v \in Q_N$, *then* $\bar{\rho}(\mathrm{Frob}_v)$ *has distinct eigenvalues* $\bar{\alpha}_v \neq \bar{\beta}_v$.
- *If* $v \in Q_N$, *then* $\#k(v) \equiv 1 \pmod{p^N}$.
- $\#Q_N = r$.
- $R^{\square}_{Q_N}$ (*respectively* $R^{\square,'}_{Q_N}$) *is topologically generated over* R^{loc} (*respectively* $R^{\mathrm{loc},'}$) *by* $\#T - 1 - [F : \mathbb{Q}] + r$ *elements.*

Proof. The last condition may be replaced by

- $H^1_{Q_N}(G_{F,T}, (\mathrm{ad}^0 \bar{\rho})(1)) = 0$.

Therefore, it is enough to show that for each $0 \neq [\phi] \in H^1(G_{F,T}, (\mathrm{ad}^0 \bar{\rho})(1))$, there are infinitely many $v \notin T$ such that:

- $\#k(v) \equiv 1 \pmod{p^N}$.
- $\bar{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues $\bar{\alpha}_v, \bar{\beta}_v$.
- $\mathrm{Res}[\phi] \in H^1(G_{k(v)}, (\mathrm{ad}^0 \bar{\rho})(1))$ is nonzero.

This then gives us some set of places Q with the given properties, except that $\#Q$ may be too large; but then we can pass to a subset of cardinality r, while maintaining the injectivity of the map $H^1(G_{F,T}, (\mathrm{ad}^0 \bar{\rho})(1)) \to \oplus_{v \in Q} H^1(G_{k(v)}, (\mathrm{ad}^0 \bar{\rho})(1))$.

We will use the Chebotarev density theorem to do this; note that the condition that $\#k(v) \equiv 1 \pmod{p^N}$ is equivalent to v splitting completely in $F(\zeta_{p^N})$, and the condition that $\bar{\rho}(\mathrm{Frob}_v)$ has distinct eigenvalues is equivalent to asking that $\mathrm{ad}\,\bar{\rho}(\mathrm{Frob}_v)$ has an eigenvalue not equal to 1.

Set $E = \bar{F}^{\ker \mathrm{ad}\,\bar{\rho}}(\zeta_{p^N})$. We claim that we have $H^1(\mathrm{Gal}(E/F), (\mathrm{ad}^0 \bar{\rho})(1)) = 0$. In order to see this, we claim firstly that $\zeta_p \notin \bar{F}^{\ker \mathrm{ad}\,\bar{\rho}}$. This follows from the classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$: we have assumed that $\mathrm{Im}\,\bar{\rho} \supseteq \mathrm{SL}_2(\mathbb{F}_p)$, and this implies that $\mathrm{Im}\,\mathrm{ad}\,\bar{\rho} = \mathrm{PGL}_2(\mathbb{F}_{p^s})$ or $\mathrm{PSL}_2(\mathbb{F}_{p^s})$ for some s, and in particular $(\mathrm{Im}\,\mathrm{ad}\,\bar{\rho})^{\mathrm{ab}}$ is trivial or cyclic of order 2. Since $p \geq 5$ and p is unramified in F, we have $[F(\zeta_p) : F] \geq 4$, so $\zeta_p \notin \bar{F}^{\ker \mathrm{ad}\,\bar{\rho}}$, as claimed.

The extension $E/\bar{F}^{\ker \mathrm{ad}\,\bar{\rho}}$ is abelian, and we let E_0 be the intermediate field such that $\mathrm{Gal}(E/E_0)$ has order prime to p, while $\mathrm{Gal}(E_0/\bar{F}^{\ker \mathrm{ad}\,\bar{\rho}})$ has p-power order. Write $\Gamma_1 = \mathrm{Gal}(E_0/F)$, $\Gamma_2 = \mathrm{Gal}(E/E_0)$. Then the inflation-restriction exact sequence is in part

$$0 \to H^1(\Gamma_1, (\mathrm{ad}^0 \bar{\rho})(1)^{\Gamma_2}) \to H^1(\mathrm{Gal}(E/F), (\mathrm{ad}^0 \bar{\rho})(1)) \to H^1(\Gamma_2, (\mathrm{ad}^0 \bar{\rho})(1))^{\Gamma_1},$$

so in order to show that $H^1(\mathrm{Gal}(E/F), (\mathrm{ad}^0 \bar{\rho})(1)) = 0$, it suffices to prove that $H^1(\Gamma_1, (\mathrm{ad}^0 \bar{\rho})(1)^{\Gamma_2}) = H^1(\Gamma_2, (\mathrm{ad}^0 \bar{\rho})(1))^{\Gamma_1} = 0$.

In fact, we claim that $(\mathrm{ad}^0 \bar{\rho})(1)^{\Gamma_2}$ and $H^1(\Gamma_2, (\mathrm{ad}^0 \bar{\rho})(1))$ both vanish. For the first of these, note that Γ_2 acts trivially on $\mathrm{ad}^0 \bar{\rho}$ (since E_0 contains $\bar{F}^{\ker \mathrm{ad}\,\bar{\rho}}$), but that $\zeta_p \notin E_0$ (as $[E_0 : \overline{F}^{\ker \operatorname{ad} \bar\rho}]$ is a power of p). For the second term, note that Γ_2 has prime-to-p order.

Suppose that $\# k(v) \equiv 1 \pmod p$, and that $\bar\rho(\mathrm{Frob}_v) = \left(\begin{smallmatrix}\bar\alpha_v & 0\\ 0 & \bar\beta_v\end{smallmatrix}\right)$. Then $\operatorname{ad}^0 \bar\rho$ has the basis $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0 & 0\\ 1 & 0\end{smallmatrix}\right)$ of eigenvectors for Frob_v, with eigenvalues 1, $\bar\alpha_v/\bar\beta_v$, $\bar\beta_v/\bar\alpha_v$ respectively. Consequently, we see that there is an isomorphism $H^1(G_{k(v)}, (\operatorname{ad}^0 \bar\rho)(1)) \cong \mathbb{F}$ (since in general for a (pro)cyclic group, the first cohomology is given by passage to coinvariants), which we can write explicitly as $[\phi] \mapsto \pi_v \circ \phi(\mathrm{Frob}_v) \circ i_v$, where i_v is the injection of $\mathbb{F}$ into the $\bar\alpha_v$-eigenspace of Frob_v, and π_v is the Frob_v-equivariant projection onto that subspace.

Let σ_0 be an element of $\mathrm{Gal}(E/F)$ such that:

- $\sigma_0(\zeta_{p^N}) = \zeta_{p^N}$.
- $\bar\rho(\sigma_0)$ has distinct eigenvalues $\bar\alpha$, $\bar\beta$.

(To see that such a σ_0 exists, note that $\mathrm{Gal}(\overline{F}^{\ker\bar\rho}/F(\zeta_{p^N})\cap\overline{F}^{\ker\bar\rho})$ contains $\mathrm{PSL}_2(\mathbb{F}_p)$, and so we can choose σ_0 so that its image in this group is an element whose adjoint has an eigenvalue other than 1.) Let $\tilde{E}/E$ be the extension cut out by all the $[\phi] \in H^1(G_{F,T}, (\operatorname{ad}^0 \bar\rho)(1))$. In order to complete the proof, it suffices to show that we can choose some $\sigma \in \mathrm{Gal}(\tilde{E}/F)$ with $\sigma|_E = \sigma_0$, and such that in the notation above, we have $\pi_{\sigma_0} \circ \phi(\sigma) \circ i_{\sigma_0} \neq 0$, because we can then choose v to have $\mathrm{Frob}_v = \sigma$ by the Chebotarev density theorem.

To this end, choose any $\tilde\sigma_0 \in \mathrm{Gal}(\tilde{E}/F)$ with $\tilde\sigma_0|_E = \sigma_0$. If $\tilde\sigma_0$ does not work, then we have $\pi_{\sigma_0} \circ \phi(\tilde\sigma_0) \circ i_{\sigma_0} = 0$. In this case, take $\sigma = \sigma_1\tilde\sigma_0$ for some $\sigma_1 \in \mathrm{Gal}(\tilde{E}/E)$. Then $\phi(\sigma) = \phi(\sigma_1\tilde\sigma_0) = \phi(\sigma_1) + \sigma_1\phi(\tilde\sigma_0) = \phi(\sigma_1) + \phi(\tilde\sigma_0)$, so $\pi_{\sigma_0} \circ \phi(\sigma) \circ i_{\sigma_0} = \pi_{\sigma_0} \circ \phi(\sigma_1) \circ i_{\sigma_0}$.

Note that $\phi(\mathrm{Gal}(\tilde{E}/E))$ is a $\mathrm{Gal}(E/F)$-invariant subset of $\operatorname{ad}^0 \bar\rho$, which is an irreducible $\mathrm{Gal}(E/F)$-module, since the image of $\bar\rho$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. Thus the $\mathbb{F}$-span of $\phi(\mathrm{Gal}(\tilde{E}/E))$ is all of $\operatorname{ad}^0 \bar\rho(1)$, from which it is immediate that we can choose σ_1 so that $\pi_{\sigma_0} \circ \phi(\sigma_1) \circ i_{\sigma_0} \neq 0$. □

We are now surprisingly close to proving the main theorem! Write $h := \# T - 1 - [F : \mathbb{Q}] + r$, and $R_\infty := R^{\mathrm{loc}}\llbracket x_1, \dots, x_h \rrbracket$. For each set Q_N as above, choose a surjection $R_\infty \twoheadrightarrow R^{\square}_{Q_N}$. Let $\mathcal{J}_\infty := \mathcal{J}\llbracket y_1, \dots, y_r \rrbracket$. Choose a surjection $\mathcal{J}_\infty \twoheadrightarrow \mathcal{J}[\Delta_{Q_N}]$, given by writing $Q_N = \{v_1, \dots, v_r\}$ and mapping y_i to $(\gamma_i - 1)$, where γ_i is a generator of Δ_{v_i}. Choose a homomorphism $\mathcal{J}_\infty \to R_\infty$ so that the composites $\mathcal{J}_\infty \to R_\infty \twoheadrightarrow R^{\square}_{Q_N}$ and $\mathcal{J}_\infty \to \mathcal{J}[\Delta_{Q_N}] \to R^{\square}_{Q_N}$ agree, and write $\mathfrak{a}_\infty := (\mathfrak{a}, y_1, \dots, y_r)$. Then $S^{\square}_{Q_N}/\mathfrak{a}_\infty = S_\varnothing$, $R^{\square}_{Q_N}/\mathfrak{a}_\infty = R^{\mathrm{univ}}_\varnothing$.

Write $\mathfrak{b}_N := \ker(\mathcal{J}_\infty \to \mathcal{J}[\Delta_{Q_N}])$, so that $S^{\square}_{Q_N}$ is finite free over $\mathcal{J}_\infty/\mathfrak{b}_N$. Since all the elements of Q_N are congruent to 1 modulo p^N, we see that

$$\mathfrak{b}_N \subseteq ((1+y_1)^{p^N} - 1, \dots, (1+y_r)^{p^N} - 1).$$

We can and do choose the same data for $R^{\mathrm{loc},\prime}$, in such a way that the two sets of data are compatible modulo λ.

Now choose open ideals $\mathfrak{c}_N \lhd \mathcal{J}_\infty$ such that:

- $\mathfrak{c}_N \cap \mathcal{O} = (\lambda^N)$.
- $\mathfrak{c}_N \supseteq \mathfrak{b}_N$.
- $\mathfrak{c}_N \supseteq \mathfrak{c}_{N+1}$.
- $\cap_N \mathfrak{c}_N = 0$.

(For example, we could take $\mathfrak{c}_N = ((1+X_{v,i,j})^{p^N} - 1, (1+y_i)^{p^N} - 1, \lambda^N)$.) Note that since $\mathfrak{c}_N \supseteq \mathfrak{b}_N$, $S^{\square}_{Q_N}/\mathfrak{c}_N$ is finite free over $\mathcal{J}_\infty/\mathfrak{c}_N$. Also choose open ideals $\mathfrak{d}_N \lhd R^{\mathrm{univ}}_{\varnothing}$ such that:

- $\mathfrak{d}_N \subseteq \ker(R^{\mathrm{univ}}_{\varnothing} \to \mathrm{End}(S_\varnothing/\lambda^N))$.
- $\mathfrak{d}_N \supseteq \mathfrak{d}_{N+1}$.
- $\cap_N \mathfrak{d}_N = 0$.

If $M \geq N$, write $S_{M,N} = S^{\square}_{Q_M}/\mathfrak{c}_N$, so that $S_{M,N}$ is finite free over $\mathcal{J}_\infty/\mathfrak{c}_N$ of rank equal to the $\mathcal{O}$-rank of $S_\varnothing$; indeed $S_{M,N}/\mathfrak{a}_\infty \xrightarrow{\sim} S_\varnothing/\lambda^N$. Then we have a commutative diagram

$$\begin{tikzcd}
\mathcal{J}_\infty \arrow[r] & R_\infty \arrow[r, two heads] \arrow[d, phantom, "\circlearrowright"] & R^{\mathrm{univ}}_{\varnothing}/\mathfrak{d}_N \arrow[d, phantom, "\circlearrowright"] \\
 & S_{M,N} \arrow[r, two heads] & S_\varnothing/\mathfrak{d}_N
\end{tikzcd}$$

where $S_{M,N}$, $S_\varnothing/\mathfrak{d}_N$ and $R^{\mathrm{univ}}_{\varnothing}/\mathfrak{d}_N$ all have finite cardinality. Because of this finiteness, we see that there is an infinite subsequence of pairs (M_i, N_i) such that $M_{i+1} > M_i$, $N_{i+1} > N_i$, and the induced diagram

$$\begin{tikzcd}
\mathcal{J}_\infty \arrow[r] & R_\infty \arrow[r, two heads] \arrow[d, phantom, "\circlearrowright"] & R^{\mathrm{univ}}_{\varnothing}/\mathfrak{d}_{N_i} \arrow[d, phantom, "\circlearrowright"] \\
 & S_{M_{i+1},N_{i+1}}/\mathfrak{c}_{N_i} \arrow[r, two heads] & S_\varnothing/\mathfrak{d}_{N_i}
\end{tikzcd}$$

is isomorphic to the diagram for (M_i, N_i).

Then we can take the projective limit over this subsequence, to obtain a commutative diagram

$$\begin{tikzcd}
\mathcal{J}_\infty \arrow[r] & R_\infty \arrow[r, two heads] \arrow[d, phantom, "\circlearrowright"] & R^{\mathrm{univ}}_{\varnothing} \arrow[d, phantom, "\circlearrowright"] \\
 & S_\infty \arrow[r, two heads] & S_\varnothing
\end{tikzcd}$$

where S_∞ is finite free over $\mathcal{J}_\infty$. Furthermore, we can simultaneously carry out the same construction in the $'$ world, compatibly with this picture modulo λ.

This is the key picture, and the theorem will now follow from it by purely commutative algebra arguments. We have (ultimately by the calculations of the dimensions of the local deformation rings in Theorems 3.28 and 3.31)

$$\dim R_\infty = \dim R'_\infty = \dim \mathcal{J}_\infty = 4\#T + r,$$

and since S_∞, S'_∞ are finite free over the power series ring $\mathcal{J}_\infty$ (from Proposition 5.8), we have

$$\operatorname{depth}_{\mathcal{J}_\infty}(S_\infty) = \operatorname{depth}_{\mathcal{J}_\infty}(S'_\infty) = 4\#T + r.$$

(This is the "numerical coincidence" on which the Taylor–Wiles method depends; see [Calegari and Geraghty 2018] for a further discussion of this point, and of a more general "numerical coincidence".) Since the action of $\mathcal{J}_\infty$ on S_∞ factors through R_∞, we see that

$$\operatorname{depth}_{R_\infty}(S_\infty) \geq 4\#T + r,$$

and similarly

$$\operatorname{depth}_{R'_\infty}(S'_\infty) \geq 4\#T + r.$$

Now, if $\mathcal{P} \lhd R'_\infty$ is a minimal prime in the support of S'_∞, then we see that

$$4\#T + r = \dim R'_\infty \geq \dim R'_\infty/\mathcal{P} \geq \operatorname{depth}_{R'_\infty} S'_\infty \geq 4\#T + r,$$

so equality holds throughout, and $\mathcal{P}$ is a minimal prime of R'_∞. But R'_∞ has a unique minimal prime, so in fact

$$\operatorname{Supp}_{R'_\infty}(S'_\infty) = \operatorname{Spec} R'_\infty.$$

By the same argument, we see that $\operatorname{Supp}_{R_\infty}(S_\infty)$ is a union of irreducible components of $\operatorname{Spec} R_\infty$. We will show that it is all of $\operatorname{Spec} R_\infty$ by reducing modulo λ and comparing with the situation for S'_∞.

To this end, note that since $\operatorname{Supp}_{R'_\infty}(S'_\infty) = \operatorname{Spec} R'_\infty$, we certainly have

$$\operatorname{Supp}_{R'_\infty/\lambda}(S'_\infty/\lambda) = \operatorname{Spec} R'_\infty/\lambda.$$

This implies that $\operatorname{Supp}_{R_\infty/\lambda}(S_\infty/\lambda) = \operatorname{Spec} R_\infty/\lambda$, by the compatibility between the two pictures. Thus $\operatorname{Supp}_{R_\infty}(S_\infty)$ is a union of irreducible components of $\operatorname{Spec} R_\infty$, which contains the entirety of $\operatorname{Spec} R_\infty/\lambda$. Since (by Theorem 3.38) the irreducible components of $\operatorname{Spec} R_\infty/\lambda$ are in bijection with the irreducible components of $\operatorname{Spec} R_\infty$, this implies that $\operatorname{Supp}_{R_\infty}(S_\infty) = \operatorname{Spec} R_\infty$. Then

$$\operatorname{Supp}_{R_\infty/\mathfrak{a}_\infty}(S_\infty/\mathfrak{a}_\infty) = R_\infty/\mathfrak{a}_\infty,$$

i.e., $\operatorname{Supp}_{R_\varnothing^{\mathrm{univ}}} S_\varnothing = R_\varnothing^{\mathrm{univ}}$, which is what we wanted to prove.

6. Relaxing the hypotheses

The hypotheses in our main theorem are not optimal. We will now briefly indicate the "easy" relaxations of the assumptions that could be made, and discuss the generalizations that are possible with (a lot) more work.

Firstly, it is possible to relax the assumption that $p \geq 5$, and that $\operatorname{Im}\bar{\rho} \supseteq \mathrm{SL}_2(\mathbb{F}_p)$. These assumptions cannot be completely removed, but they can be considerably relaxed. The case $p = 2$ is harder in several ways, but important theorems have been proved in this case, for example the results of Kisin [2009b] which completed the proof of Serre's conjecture.

On the other hand, the case $p = 3$ presents no real difficulties. The main place that we assumed that $p > 3$ was in the proof that the finite groups G_i in Section 5.3 have order prime to p; this argument could also break down for cases when $p > 3$ if we allowed p to ramify in F, which in general we would like to do. Fortunately, there is a simple solution to this problem, which is to introduce an auxiliary prime v to the level. This prime is chosen in such a way that all deformations of $\bar{\rho}|_{G_{F_v}}$ are automatically unramified, so none of the global Galois deformation rings that we work with are changed when we relax the conditions at v. The existence of an appropriate v follows from the Chebotarev density theorem and some elementary group theory; see Lemma 4.11 of [Darmon et al. 1997] and the discussion immediately preceding it.

We now consider the possibility of relaxing the assumption that $\operatorname{Im}\bar{\rho} \supseteq \mathrm{SL}_2(\mathbb{F}_p)$. We should certainly assume that $\bar{\rho}$ is absolutely irreducible, because otherwise many of our constructions don't even make sense; we always had to assume this in constructing universal deformation rings, in constructing the universal modular deformation, and so on. (Similar theorems have been proved in the case that $\bar{\rho}$ is reducible, in particular by Skinner and Wiles [1999], but the arguments are considerably more involved, and at present involve a number of serious additional hypotheses, in particular ordinarity — although see [Pan 2022] for a theorem without an ordinarity hypothesis.) Examining the arguments made above, we see that the main use of the assumption that $\operatorname{Im}\bar{\rho} \supseteq \mathrm{SL}_2(\mathbb{F}_p)$ is in the proof of Proposition 5.10. Looking more closely at the proof, the key assumption is really that $\bar{\rho}|_{G_{F(\zeta_p)}}$ is absolutely irreducible; this is known as the "Taylor–Wiles assumption". (Note that by elementary group theory, this is equivalent to the absolute irreducibility of $\bar{\rho}|_{G_K}$, where K/F is the unique quadratic subextension of $F(\zeta_p)/F$; in particular, over $\mathbb{Q}$ the condition is equivalent to the absolute irreducibility of $\bar{\rho}|_{G_{\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})}}$, which is how the condition is stated in the original papers.)

Unfortunately this condition isn't quite enough in complete generality, but it comes very close; the only exception is certain cases when $p = 5$, F contains $\mathbb{Q}(\sqrt{5})$, and the projective image of $\bar{\rho}$ is $\mathrm{PGL}_2(\mathbb{F}_5)$. See [Kisin 2009c, (3.2.3)] for the definitive statement (and see the work of Khare and Thorne [2017] for some improvements in this exceptional case). If $\bar{\rho}$ is absolutely irreducible, but $\bar{\rho}|_{G_{F(\zeta_p)}}$ is (absolutely) reducible, it is sometimes possible to prove modularity lifting theorems, but considerably more work is needed (and there is no general approach in higher dimension); see [Skinner and Wiles 2001] in the ordinary case, which uses similar arguments to those of [Skinner and Wiles 1999], and also [Thorne 2016; Pan 2022].

The other conditions that we could hope to relax are the assumptions on $\rho|_{G_{F_v}}$ and $\rho_0|_{G_{F_v}}$ at places $v \mid p$. We've hardly discussed where some of these assumptions come from, as we swept most issues with p-adic Hodge theory under the carpet. There are essentially two problems here. First, we have assumed that p is unramified in F, that the Galois representations are crystalline, and that the gaps between the Hodge–Tate weights are "small"; this is the Fontaine–Laffaille condition. There is also the assumption that ρ, ρ_0 have the same Hodge–Tate weights. Both conditions can be considerably (although by no means completely) relaxed (of course subject to the necessary condition that ρ is geometric). As already alluded to above, very general results are available in the ordinary case (even in arbitrary dimension), in particular those of Geraghty [2019]. In the case that $F_v = \mathbb{Q}_p$ there are again very general results, using the p-adic local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$; see in particular [Emerton 2011; Kisin 2009a; Pan 2022]. However, beyond this case, the situation is considerably murkier, and at present there are no generally applicable results.

6.1. ***Further generalizations.*** Other than the results discussed in the previous subsection, there are a number of obvious generalizations that one could hope to prove. One obvious step, already alluded to above, is to replace 2-dimensional representations with n-dimensional representations; we could also hope to allow F to be a more general number field. At present it seems to be necessary to assume that F is a CM field, as otherwise we do not know how to attach Galois representations to automorphic representations; but if F is CM, then automorphy lifting theorems analogous to our main theorem are now known (for arbitrary n), and we refer to [Calegari 2021] for both the history of such results and the state of the art.

Another natural condition to relax would be the condition that the Hodge–Tate weights are distinct; for example, one could ask that they all be equal, and hope to prove Artin's conjecture, or that some are equal, to prove modularity results for abelian varieties. The general situation where some Hodge–Tate weight occurs with multiplicity greater than 2 seems to be completely out of reach (because there is no known way to relate the automorphic representations expected to correspond to such Galois representations to the automorphic representations which contribute to the cohomology of Shimura varieties, which is the only technique we have for constructing the maps $R \to \mathbb{T}$), but there has been considerable progress for small dimensional cases, for which we again refer the reader to [Calegari 2021].

Finally, we would of course like to be able to dispose of the hypothesis that $\bar{\rho}$ is modular (that is, to dispose of ρ_0). This is the problem of Serre's conjecture and its generalizations, and has only been settled in the case that $F = \mathbb{Q}$ and $n = 2$. The proof in that case (by Khare and Wintenberger [2009a; 2009b] and Kisin [2009b]) makes essential use of modularity lifting theorems. The proof inductively reduces to the case that $p \leq 5$ and $\bar{\rho}$ has very little ramification, when direct arguments using discriminant bounds can be made. The more general modularity lifting theorems mentioned above make it plausible that the inductive steps could be generalized, but the base case of the induction seems specific to the case of $\mathrm{GL}_2 /\mathbb{Q}$, and proving the modularity of $\bar{\rho}$ in greater generality is one of the biggest open problems in the field.

Acknowledgements

These notes are based in part on a lecture course given by Richard Taylor at Harvard University in 2009, and I am extremely grateful to him both for the many things I learned from his course, and for giving me permission to present them here.

These notes were originally written for the 2013 Arizona Winter School, and I would like to thank the organizers (Bryden Cais, Mirela Çiperiani, Matthew Papanikolas, Rachel Pries, David Savitt, and Romyar Sharifi) for the invitation to speak, and the participants for their feedback. I would like to thank Ana Caraiani for encouraging me to belatedly publish these notes. In revising for publication I removed some material relating to the Arizona Winter School project, and for the most part removed the outdated section on more recent developments (the reader disappointed by this change should read Calegari's excellent survey [2021]). I have otherwise maintained the feel of the original notes.

I would also like to thank Kevin Buzzard, Frank Calegari, Ana Caraiani, Kęstutis Česnavičius, Matthew Emerton, Jessica Fintzen, Jeff Hatley, Florian Herzig, Christian Johansson, Keenan Kidwell, Alexander Kutzim, Jack Lamplugh, Heejong Lee, Tom Lovering, Judith Ludwig, James Newton, Sug Woo Shin and Jack Shotton for their helpful comments on earlier versions of these notes.

Finally, I am extremely grateful to the anonymous referee for their many helpful corrections and suggestions.

References

[Barnet-Lamb et al. 2011] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor, "A family of Calabi–Yau varieties and potential automorphy II", *Publ. Res. Inst. Math. Sci.* **47**:1 (2011), 29–98. MR Zbl

[Barnet-Lamb et al. 2014] T. Barnet-Lamb, T. Gee, D. Geraghty, and R. Taylor, "Potential automorphy and change of weight", *Ann. of Math.* (2) **179**:2 (2014), 501–609. MR Zbl

[Berger 2004] L. Berger, “An introduction to the theory of p-adic representations”, pp. 255–292 in *Geometric aspects of Dwork theory*, vol. 1, edited by A. Adolphson et al., de Gruyter, Berlin, 2004. MR Zbl

[Bhatt 2021] B. Bhatt, “Algebraic geometry in mixed characteristic”, preprint, 2021. To appear in the proceedings of the 2022 ICM. arXiv 2112.12010

[Böckle 2013] G. Böckle, “Deformations of Galois representations”, pp. 21–115 in *Elliptic curves, Hilbert modular forms and Galois deformations*, edited by H. Darmon et al., Birkhäuser, Basel, 2013. MR Zbl

[Brinon and Conrad 2009] O. Brinon and B. Conrad, “CMI summer school notes on p-adic Hodge theory”, 2009, available at http://math.stanford.edu/∼conrad/.

[Bushnell and Henniart 2006] C. J. Bushnell and G. Henniart, *The local Langlands conjecture for* GL(2), Grundl. Math. Wissen. **335**, Springer, 2006. MR Zbl

[Buzzard 2012] K. Buzzard, “Potential modularity—a survey”, pp. 188–211 in *Non-abelian fundamental groups and Iwasawa theory*, edited by J. Coates et al., London Math. Soc. Lecture Note Ser. **393**, Cambridge Univ. Press, 2012. MR Zbl

[Calegari 2021] F. Calegari, “Reciprocity in the Langlands program since Fermat’s last theorem”, preprint, 2021. arXiv 2109.14145

[Calegari and Geraghty 2018] F. Calegari and D. Geraghty, “Modularity lifting beyond the Taylor–Wiles method”, *Invent. Math.* **211**:1 (2018), 297–433. MR Zbl

[Carayol 1994] H. Carayol, “Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet”, pp. 213–237 in *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture* (Boston, MA, 1991), edited by B. Mazur and G. Stevens, Contemp. Math. **165**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Choi 2009] S. H. Choi, *Local deformation lifting spaces of mod l Galois representations*, Ph.D. thesis, Harvard University, 2009, available at https://www.proquest.com/docview/304892280. MR

[Clozel 1990] L. Clozel, “Motifs et formes automorphes: Applications du principe de fonctorialité”, pp. 77–159 in *Automorphic forms, Shimura varieties, and L-functions* (Ann Arbor, MI, 1988), vol. 1, edited by L. Clozel and J. S. Milne, Perspectives in Mathematics **10**, Academic Press, Boston, MA, 1990. MR Zbl

[Clozel et al. 2008] L. Clozel, M. Harris, and R. Taylor, “Automorphy for some l-adic lifts of automorphic mod l Galois representations”, *Publ. Math. Inst. Hautes Études Sci.* 108 (2008), 1–181. MR Zbl

[Curtis and Reiner 1962] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics **XI**, Interscience Publishers, New York, 1962. MR Zbl

[Darmon et al. 1997] H. Darmon, F. Diamond, and R. Taylor, “Fermat’s last theorem”, pp. 2–140 in *Elliptic curves, modular forms & Fermat’s last theorem* (Hong Kong, 1993), edited by J. Coates and S. T. Yau, Int. Press, Cambridge, MA, 1997. MR Zbl

[Dickinson 2001a] M. Dickinson, “A criterion for existence of a universal deformation ring”, pp. 339–343 in *Arithmetic algebraic geometry* (Park City, UT, 1999), edited by B. Conrad and K. Rubin, IAS/Park City Math. Ser. **9**, Amer. Math. Soc., Providence, RI, 2001. Appendix 1 of F. Gouvêa, “Deformations of Galois representations”, pp. 233–406. MR

[Dickinson 2001b] M. Dickinson, “On the modularity of certain 2-adic Galois representations”, *Duke Math. J.* **109**:2 (2001), 319–382. MR Zbl

[Emerton 2011] M. Emerton, “Local-global compatibility in the p-adic Langlands programme for $\mathrm{GL}_{2/\mathbb{Q}}$”, 2011, available at http://www.math.uchicago.edu/∼emerton/pdffiles/lg.pdf.

[Fargues 2011] L. Fargues, “Motives and automorphic forms: the (potentially) abelian case”, 2011, available at https://webusers.imj-prg.fr/~laurent.fargues/Motifs_abeliens.pdf.

[Flath 1979] D. Flath, “Decomposition of representations into tensor products”, pp. 179–183 in *Automorphic forms, representations and L-functions* (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math., XXXIII **1**, Amer. Math. Soc., Providence, R.I., 1979. MR Zbl

[Fontaine 1994] J.-M. Fontaine, “Représentations l-adiques potentiellement semi-stables”, pp. 321–347 in *Périodes p-adiques* (Bures-sur-Yvette, 1988), Astérisque **223**, Société Mathématique de France, Paris, 1994. MR Zbl

[Fontaine and Laffaille 1982] J.-M. Fontaine and G. Laffaille, “Construction de représentations p-adiques”, *Ann. Sci. École Norm. Sup.* (4) **15**:4 (1982), 547–608. MR Zbl

[Fontaine and Mazur 1995] J.-M. Fontaine and B. Mazur, “Geometric Galois representations”, pp. 41–78 in *Elliptic curves, modular forms, & Fermat’s last theorem* (Hong Kong, 1993), edited by J. H. Coates and S.-T. Yau, Series in Number Theory **1**, International Press, Cambridge, MA, 1995. MR Zbl

[Gelbart 1975] S. S. Gelbart, *Automorphic forms on adèle groups*, Annals of Mathematics Studies **83**, Princeton University Press, Princeton, N.J., 1975. MR Zbl

[Geraghty 2019] D. Geraghty, “Modularity lifting theorems for ordinary Galois representations”, *Math. Ann.* **373**:3-4 (2019), 1341–1427. MR Zbl

[Gruenberg 1967] K. Gruenberg, “Profinite groups”, pp. 116–127 in *Algebraic Number Theory* (Proc. Instructional Conf., Brighton, 1965), edited by J. W. S. Cassels and A. Fröhlich, Thompson, Washington, D.C., 1967. MR Zbl

[Katz and Messing 1974] N. M. Katz and W. Messing, “Some consequences of the Riemann hypothesis for varieties over finite fields”, *Invent. Math.* **23** (1974), 73–77. MR Zbl

[Khare and Thorne 2017] C. B. Khare and J. A. Thorne, “Automorphy of some residually S_5 Galois representations”, *Math. Z.* **286**:1-2 (2017), 399–429. MR Zbl

[Khare and Wintenberger 2009a] C. Khare and J.-P. Wintenberger, “Serre’s modularity conjecture, I”, *Invent. Math.* **178**:3 (2009), 485–504. MR Zbl

[Khare and Wintenberger 2009b] C. Khare and J.-P. Wintenberger, “Serre’s modularity conjecture, II”, *Invent. Math.* **178**:3 (2009), 505–586. MR Zbl

[Kisin 2008] M. Kisin, “Potentially semi-stable deformation rings”, *J. Amer. Math. Soc.* **21**:2 (2008), 513–546. MR Zbl

[Kisin 2009a] M. Kisin, “The Fontaine–Mazur conjecture for GL_2”, *J. Amer. Math. Soc.* **22**:3 (2009), 641–690. MR Zbl

[Kisin 2009b] M. Kisin, “Modularity of 2-adic Barsotti–Tate representations”, *Invent. Math.* **178**:3 (2009), 587–634. MR Zbl

[Kisin 2009c] M. Kisin, “Moduli of finite flat group schemes, and modularity”, *Ann. of Math.* (2) **170**:3 (2009), 1085–1180. MR Zbl

[Mazur 1989] B. Mazur, “Deforming Galois representations”, pp. 385–437 in *Galois groups over* $\mathbf{Q}$ (Berkeley, CA, 1987), edited by Y. Ihara et al., Math. Sci. Res. Inst. Publ. **16**, Springer, 1989. MR Zbl

[Mazur 1997] B. Mazur, “An introduction to the deformation theory of Galois representations”, pp. 243–311 in *Modular forms and Fermat’s last theorem* (Boston, MA, 1995), edited by G. Cornell et al., Springer, 1997. MR Zbl

[Milne 2006] J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006. MR Zbl

[Pan 2022] L. Pan, “The Fontaine–Mazur conjecture in the residually reducible case”, *J. Amer. Math. Soc.* **35**:4 (2022), 1031–1169. MR Zbl

[Pilloni 2008] V. Pilloni, “The study of 2-dimensional p-adic Galois deformations in the $\ell \neq p$ case”, 2008, available at http://perso.ens-lyon.fr/vincent.pilloni/Defo.pdf.

[Ramakrishna 1993] R. Ramakrishna, “On a variation of Mazur’s deformation functor”, *Compositio Math.* **87**:3 (1993), 269–286. MR Zbl

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer, 1979. MR Zbl

[Shotton 2016] J. Shotton, “Local deformation rings for GL_2 and a Breuil–Mézard conjecture when $\ell \neq p$”, *Algebra Number Theory* **10**:7 (2016), 1437–1475. MR Zbl

[Skinner and Wiles 1999] C. M. Skinner and A. J. Wiles, “Residually reducible representations and modular forms”, *Inst. Hautes Études Sci. Publ. Math.* 89 (1999), 5–126. MR Zbl

[Skinner and Wiles 2001] C. M. Skinner and A. J. Wiles, “Nearly ordinary deformations of irreducible residual representations”, *Ann. Fac. Sci. Toulouse Math.* (6) **10**:1 (2001), 185–215. MR Zbl

[Tate 1979] J. Tate, “Number theoretic background”, pp. 3–26 in *Automorphic forms, representations and L-functions, II* (Corvallis, OR, 1977), edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, American Mathematical Society, Providence, RI, 1979. MR Zbl

[Taylor 2003] R. Taylor, “On icosahedral Artin representations, II”, *Amer. J. Math.* **125**:3 (2003), 549–566. MR Zbl

[Taylor 2006] R. Taylor, “On the meromorphic continuation of degree two L-functions”, *Doc. Math.* Extra Vol. (2006), 729–779. MR

[Taylor 2008] R. Taylor, “Automorphy for some l-adic lifts of automorphic mod l Galois representations, II”, *Publ. Math. Inst. Hautes Études Sci.* 108 (2008), 183–239. MR Zbl

[Thorne 2016] J. A. Thorne, “Automorphy of some residually dihedral Galois representations”, *Math. Ann.* **364**:1-2 (2016), 589–648. MR Zbl

Received 9 Feb 2022. Revised 4 Sep 2022.

TOBY GEE:

toby.gee@imperial.ac.uk
Mathematics Department, Imperial College London, London, United Kingdom

msp

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the submission page.

Originality. Submission of a manuscript acknowledges that the manuscript is original and 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 are usually in English or French, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not refer to bibliography keys. 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 a Mathematics Subject Classification for the article, and, for each author, affiliation (if appropriate) and email address.

Format. Authors are encouraged to use LaTeX and the standard amsart class, but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should normally 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 BibTeX 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 with as many details as you can about how your graphics were generated.

Bundle your figure files into a single archive (using zip, tar, rar or other format of your choice) and upload on the link you been provided at acceptance time. Each figure should be captioned and numbered so that it can float. Small figures occupying no more than three lines of vertical space can be kept in the text ("the curve looks like this:"). It is acceptable to submit a manuscript with all figures at the end, if their placement is specified in the text by means of comments such as "Place Figure 1 here". The same considerations apply to tables.

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.

ESSENTIAL NUMBER THEORY

2022 vol. 1 no. 1