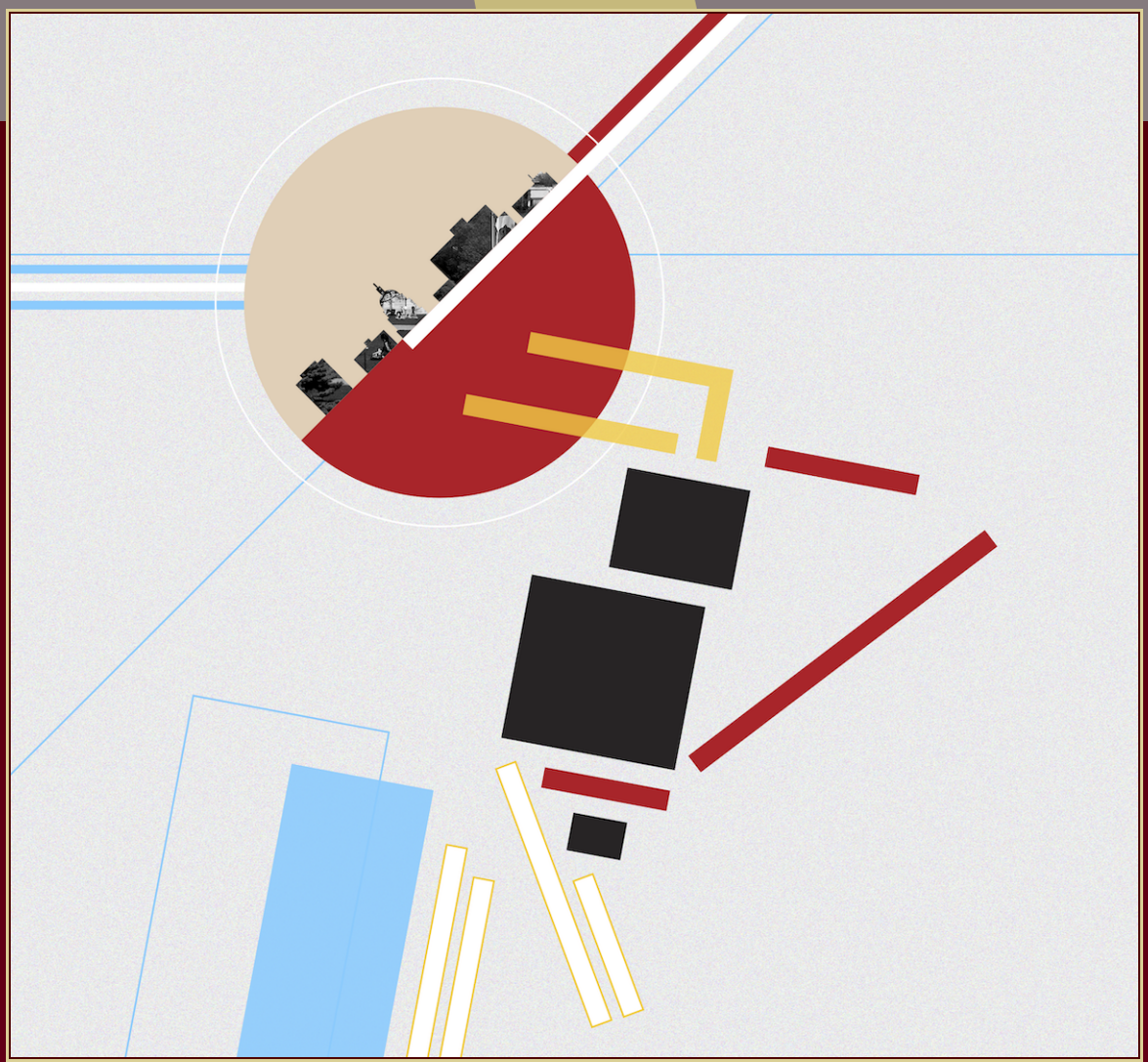
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Generating subgroups of ray class groups with small prime ideals

Benjamin Wesolowski



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.461

Generating subgroups of ray class groups with small prime ideals

Benjamin Wesolowski

Explicit bounds are given on the norms of prime ideals generating arbitrary subgroups of ray class groups of number fields, assuming the extended Riemann hypothesis. These are the first explicit bounds for this problem and are significantly better than previously known asymptotic bounds. Applied to the integers, they express that any subgroup of index i of the multiplicative group of integers modulo m is generated by prime numbers smaller than $16(i \log m)^2$, subject to the Riemann hypothesis. Two particular consequences relate to mathematical cryptology. Applied to cyclotomic fields, they provide explicit bounds on generators of the relative class group, needed in some previous work on the shortest vector problem on ideal lattices. Applied to Jacobians of hyperelliptic curves, they allow one to derive bounds on the degrees of isogenies required to make their horizontal isogeny graphs connected. Such isogeny graphs are used to study the discrete logarithm problem on said Jacobians.

1. Introduction

1A. ***Motivation.*** In 1990, Bach [1] computed explicit bounds for the norms of prime ideals generating the class groups of number fields, assuming the extended Riemann hypothesis (henceforth, ERH). These bounds made explicit the earlier work of Lagarias, Montgomery and Odlyzko [11], and have proved to be a crucial tool in the design and analysis of many number-theoretic algorithms. However, these bounds do not tell anything about the norms of prime ideals generating any particular subgroup of the class group. Indeed, a generating set for the full group might not contain any element of the subgroup.

Let K be a number field of degree n, and let Δ be the absolute value of its discriminant. The results of [11] show that the class group $\mathrm{Cl}(K)$ is generated by prime ideals of norm bounded by $O((\log \Delta)^2)$. Now, let H be an arbitrary subgroup of the class group $\mathrm{Cl}(K)$. Some asymptotic bounds on the norm of prime ideals generating H have already been computed in [10] by analyzing spectral properties of the underlying Cayley graphs. They are of the form $O((n[\mathrm{Cl}(K) : H] \log \Delta)^{2+\varepsilon})$ for an arbitrary $\varepsilon > 0$. Taking H to be the full class group reveals a clear gap with the bounds of [11]. The explicit bounds provided in the present paper eliminate this gap, as they are asymptotically $O(([\mathrm{Cl}(K) : H] \log \Delta)^2)$.

MSC2010: primary 11R29; secondary 11M06, 11R37, 14K02.
Keywords: class group, ray class group, prime ideal, isogeny graph.

Situations where proper subgroups of class groups have to be considered have already arisen in two distinct regions of mathematical cryptology. One is related to lattice-based cryptography. Cryptographic schemes based on ideal lattices are typically instantiated over the ring of integers $\mathcal{O}_K$ of a cyclotomic field K. The field K has a Hermitian vector space structure induced by its Minkowski embedding, and ideals of $\mathcal{O}_K$ are also lattices in this vector space. It was shown in [3; 4; 5] that in principal ideals of $\mathcal{O}_K$, an unusually short vector can be found in quantum polynomial time, under some heuristic assumptions (this short vector is actually a generator of the ideal). This led to the break of a multitude of cryptographic schemes using principal ideals (including [4; 8; 14; 20]).

A recent result [6] shows how to extend the algorithm to find short vectors in arbitrary ideals of $\mathcal{O}_K$ by transferring the problem to a principal ideal. Let n be the degree of K, K_0 the maximal real subfield of K, and $\mathrm{Cl}^-(K)$ the relative class group (i.e., the kernel of the norm map $\mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$). The transferring method of [6] crucially relies on the assumption that $\mathrm{Cl}^-(K)$ is generated by a small number (polynomial in $\log n$) of prime ideals of small norm (polynomial in n) and all their Galois conjugates. On one hand, very little is known about the structure of $\mathrm{Cl}^-(K)$, and it seems difficult to prove that it can always be generated by such a small number of Galois orbits of ideals (yet there is convincing numerical evidence; see [19] for the case where K has prime conductor). On the other hand it can be shown, assuming the ERH, that the constraint on the norms can be satisfied, and the present work provides the best asymptotic bounds, and the first explicit ones (see Theorem 1.2 and Remark 2).

The second situation is related to hyperelliptic curves. Let $\mathcal{A}$ be the Jacobian of a hyperelliptic curve over a finite field $\mathbb{F}_q$. Isogeny graphs around $\mathcal{A}$ are a central tool to study the difficulty of the underlying discrete logarithm problem (see for instance [7; 9; 10; 21]). When $\mathcal{A}$ is ordinary and absolutely simple — as required for applications in cryptography — its endomorphism algebra is a complex multiplication field K (with maximal real subfield K_0) and its endomorphism ring is isomorphic to an order $\mathcal{O}$ in K. Any abelian variety isogenous to $\mathcal{A}$ has the same endomorphism algebra, and an isogeny that also preserves the endomorphism ring is called a *horizontal* isogeny. The horizontal isogeny graphs of $\mathcal{A}$ are closely related to Cayley graphs of the kernel $\mathcal{P}(\mathcal{O})$ of the norm map

$$N_{K/K_0} : \mathrm{Cl}(\mathcal{O}) \longrightarrow \mathrm{Cl}^+(\mathcal{O} \cap K_0),$$

where $\mathrm{Cl}^+(\mathcal{O} \cap K_0)$ is the narrow class group of $\mathcal{O} \cap K_0$. More precisely, for any bound $B > 0$, there is a graph isomorphism between

(1) the Cayley graph of $\mathcal{P}(\mathcal{O})$ with generators the ideals of prime norm smaller than B, and

(2) the isogeny graph consisting of all principally polarizable abelian varieties isogenous to $\mathcal{A}$ and with same endomorphism ring, and all isogenies between them of prime degree smaller than B.

When the Jacobian $\mathcal{A}$ is an elliptic curve, the situation is well understood since $K_0 = \mathbb{Q}$; hence $\mathcal{P}(\mathcal{O}) = \mathrm{Cl}(K)$. As a result, Bach's bounds have successfully been used to analyse various algorithms dealing with elliptic curve isogenies. In higher genus, however, $\mathcal{P}(\mathcal{O})$ is typically a proper subgroup of the class

group, and Bach's bounds are not sufficient to obtain connected isogeny graphs. New explicit bounds guaranteeing the connectedness are provided in Theorem 1.4.

1B. ***Setting.*** Throughout this paper, K denotes a number field of degree n, with r_1 embeddings into $\mathbb{R}$ and $2r_2$ embeddings into $\mathbb{C}$. Let $\mathcal{I}(K)$ denote the group of fractional ideals of the ring of integers $\mathcal{O}_K$. A modulus $\mathfrak{m}$ of K is a formal product of a finite part $\mathfrak{m}_0$ (an ideal in $\mathcal{O}_K$), and an infinite part $\mathfrak{m}_\infty$ (a subset of the set of real embeddings of K). Then, $\mathcal{I}_\mathfrak{m}(K)$ denotes the subgroup generated by ideals coprime to $\mathfrak{m}_0$.

The notion of ray class group can now be recalled. Let $P_{K,1}^\mathfrak{m}$ be the subgroup of $\mathcal{I}_\mathfrak{m}(K)$ generated by principal ideals of the form $\alpha\mathcal{O}_K$, where $\mathrm{ord}_\mathfrak{p}(\alpha-1) \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{m}_0)$ for all primes $\mathfrak{p}$ dividing $\mathfrak{m}_0$, and $\iota(\alpha) > 0$ for all $\iota \in \mathfrak{m}_\infty$. The *ray class group* of K modulo $\mathfrak{m}$ is the quotient

$$\mathrm{Cl}_\mathfrak{m}(K) = \mathcal{I}_\mathfrak{m}(K)/P_{K,1}^\mathfrak{m}.$$

For any ideal $\mathfrak{a}$ such that $(\mathfrak{a},\mathfrak{m}) = 1$, let $[\mathfrak{a}]_\mathfrak{m}$ denote its class in $\mathrm{Cl}_\mathfrak{m}(K)$. The *narrow class group* of K is the group $\mathrm{Cl}_\mathfrak{m}(K)$, where $\mathfrak{m}$ is the set of all the real embeddings.

Our main tools to study these groups will be ray class characters. We call a *ray class character modulo* $\mathfrak{m}$ what Neukirch [16, Definition VII.6.8] calls a (generalized) Dirichlet character modulo $\mathfrak{m}$, that is, a Größencharakter $\chi : \mathcal{I}_\mathfrak{m}(K) \to \mathbb{C}^\times$ that factors through the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$ via the canonical projection.

1C. ***Main theorem.*** Let K be a number field of degree n, and $\mathfrak{m}$ a modulus on K. Consider any subgroup H of the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$ and any character χ that is not trivial on that subgroup. The main theorem generalizes [1] by providing explicit bounds on the smallest prime ideal $\mathfrak{p}$ whose class is in H and such that $\chi(\mathfrak{p}) \neq 1$. Note that all statements containing "(ERH)" assume the extended Riemann hypothesis (recalled in Section 2). The following theorem is proved in Section 3.

Theorem 1.1 (ERH). *Let K be any number field, and Δ the absolute value of the discriminant of K. Let $\mathfrak{m}$ be a modulus of K, with finite part $\mathfrak{m}_0$ and infinite part $\mathfrak{m}_\infty$. Let H be any subgroup of the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$. Let χ be a ray class character modulo $\mathfrak{m}$ that is not trivial on H. Then there is a prime ideal $\mathfrak{p}$ such that $(\mathfrak{p},\mathfrak{m}_0) = 1$, the class of $\mathfrak{p}$ in $\mathrm{Cl}_\mathfrak{m}(K)$ is in the subgroup H, $\chi(\mathfrak{p}) \neq 1$, $\deg(\mathfrak{p}) = 1$ and*

$$N(\mathfrak{p}) \leq \big([\mathrm{Cl}_\mathfrak{m}(K) : H](2.71\log(\Delta N(\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{m}_0)) + 4.13\big)^2,$$

where $\omega(\mathfrak{m}_0)$ denotes the number of distinct prime ideals dividing $\mathfrak{m}_0$.

Remark 1. When H is the full group and $n \geq 2$, the above bound can be compared to Bach's bound $N(\mathfrak{p}) \leq 18(\log(\Delta^2 N(\mathfrak{m}_0)))^2$ given by [1, Theorem 4]. Let us put the expression of Theorem 1.1 in a comparable form. From [1, Lemma 7.1], we have

$$|\mathfrak{m}_\infty| \leq n \leq \frac{\log(\Delta N(\mathfrak{m}_0)) + \frac{3}{2}}{\log(2\pi) - \psi(2)} \leq 0.71\log(\Delta N(\mathfrak{m}_0)) + 1.07,$$

where ψ is the logarithmic derivative of the gamma function. Moreover, we have the bound $\omega(\mathfrak{m}_0) \leq \log(\Delta N(\mathfrak{m}_0))/\log 2$. The bound of Theorem 1.1 becomes $N(\mathfrak{p}) \leq (5.62\log(\Delta N(\mathfrak{m}_0)) + 5.52)^2$. Whenever $\Delta N(\mathfrak{m}_0) < 12$, the corresponding ray class group is trivial, so we can suppose that $\log(\Delta N(\mathfrak{m}_0)) \geq \log(12) \geq 2.48$. These estimates lead to

$$N(\mathfrak{p}) \leq (5.62 + 5.52/2.48)^2(\log(\Delta N(\mathfrak{m}_0)))^2 \leq 62(\log(\Delta N(\mathfrak{m}_0)))^2. \tag{1-1}$$

Even in this form, direct comparison with [1, Lemma 7.1] is not obvious. With the unrefined estimate $\Delta^2 N(\mathfrak{m}_0) \leq (\Delta N(\mathfrak{m}_0))^2$, Bach's bound becomes $N(\mathfrak{p}) \leq 72(\log(\Delta N(\mathfrak{m}_0)))^2$. The constant factor is slightly worse than in the bound (1-1), but this comparison does not do justice to either theorem.

1D. ***Consequences.*** In Section 4, a series of notable consequences is derived from Theorem 1.1. Foremost, it allows us to obtain sets of small prime ideals generating any given subgroup of a ray class group. This is made precise in the following theorem.

Theorem 1.2 (ERH). *Let K be any number field and Δ the absolute value of the discriminant of K. Let $\mathfrak{m}$ be a modulus of K, with finite part $\mathfrak{m}_0$ and infinite part $\mathfrak{m}_\infty$. Let $\mathfrak{h}$ be any ideal in K. Let H be a nontrivial subgroup of the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$. Then H is generated by the classes of the prime ideals in*

$$\{\mathfrak{p} \text{ prime ideal in } K \mid (\mathfrak{p}, \mathfrak{h}\mathfrak{m}_0) = 1,\ [\mathfrak{p}]_\mathfrak{m} \in H, \deg(\mathfrak{p}) = 1 \text{ and } N(\mathfrak{p}) < B\},$$

where $B = \big([\mathrm{Cl}_\mathfrak{m}(K) : H](2.71\log(\Delta N(\mathfrak{h}\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{h}\mathfrak{m}_0)) + 4.13\big)^2$, and $[\mathfrak{p}]_\mathfrak{m}$ denotes the class of $\mathfrak{p}$ in $\mathrm{Cl}_\mathfrak{m}(K)$.

Remark 2. In particular, Theorem 1.2 implies that the relative class group of a cyclotomic field K of degree n and discriminant Δ is generated by ideals of prime norm smaller than $(2.71h_{K_0}\log\Delta + 4.13)^2$, where h_{K_0} is the class number of the maximal real subfield of K. This is an important improvement for [6] over the previously known bound $O((h_{K_0}n\log\Delta)^{2+\varepsilon})$ derived from [10].

Applying Theorem 1.1 to Dirichlet characters, one can obtain new results on subgroups of the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$. Let m be a positive integer and H a nontrivial subgroup of $G = (\mathbb{Z}/m\mathbb{Z})^\times$. It is already known that, assuming the ERH, H contains a prime number smaller than $O(([G : H]\log m)^2)$ (see [2; 13]). But these bounds do not provide a generating set for H: they only guarantee the existence of one such prime number. The following theorem gives a set of generators of H whose norms are also asymptotically $O(([G : H]\log m)^2)$.

Theorem 1.3 (ERH). *Let m be a positive integer, and H a nontrivial subgroup of $G = (\mathbb{Z}/m\mathbb{Z})^\times$. Then H is generated by the set of prime numbers p such that $p \bmod m \in H$ and $p \leq 16([G : H]\log m)^2$.*

Finally, we derive bounds on the degrees of cyclic isogenies required to connect all isogenous principally polarizable abelian varieties over a finite field sharing the same endomorphism ring.

Theorem 1.4 (ERH). *Let $\mathcal{A}$ be a principally polarized, absolutely simple, ordinary abelian variety over a finite field $\mathbb{F}_q$, with endomorphism algebra K and endomorphism ring isomorphic to an order $\mathcal{O}$ in K.*

Let K_0 be the maximal real subfield of K and $\mathfrak{f}$ the conductor of $\mathcal{O}$. For any $B > 0$, let $\mathcal{G}(B)$ be the isogeny graph whose vertices are the principally polarizable varieties isogenous to $\mathcal{A}$ and with the same endomorphism ring, and whose edges are isogenies connecting them, of prime degree smaller than B. Then, if $\mathcal{O}_0 = \mathcal{O} \cap K_0$ is the ring of integers of K_0, the graph

$$\mathcal{G}(26(h^+_{\mathcal{O}_0} \log(\Delta N(\mathfrak{f})))^2)$$

is connected, with Δ the absolute value of the discriminant of K and $h^+_{\mathcal{O}_0}$ the narrow class number of $\mathcal{O}_0$.

Remark 3. In particular, the above holds in dimension 2, where *principally polarized* translates to *Jacobian of a genus-2 hyperelliptic curve* (see [15, Theorem 4.1]).

1E. ***Notation.*** An inequality such as $x \leq y$ between complex numbers means that the relation holds between the real parts. The function log denotes the natural logarithm.

2. Ray class characters

This section summarizes the definitions, notation and facts related to ray class characters that will be used throughout the paper.

Recall that a ray class character modulo $\mathfrak{m}$ is a Größencharakter $\chi : \mathcal{I}_{\mathfrak{m}}(K) \to \mathbb{C}^\times$ that factors through the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ (via the canonical projection). A character is *principal* if it takes only the value 1. Let $\delta(\chi)$ be 1 if χ is principal and 0 otherwise. A ray class character is *primitive modulo* $\mathfrak{m}$ if it does not factor through $\mathrm{Cl}_{\mathfrak{m}'}(K)$ for any modulus $\mathfrak{m}'$ smaller[1] than $\mathfrak{m}$. The conductor $\mathfrak{f}_\chi$ of χ is the smallest modulus $\mathfrak{f}$ such that χ is the restriction of a ray class character modulo $\mathfrak{f}$. Let $\beta_\chi = |\mathfrak{f}_\infty|$ be the number of infinite places in the conductor $\mathfrak{f}$. From [16, Proposition 6.9], any ray class character χ is the restriction of a primitive ray class character of modulus $\mathfrak{f}_\chi$, which is also primitive as a Größencharakter.

The Hecke L-function associated to a character χ modulo $\mathfrak{m}$ is defined as

$$L_\chi(s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

for $\Re\mathfrak{e}(s) > 1$, where the sum is taken over all ideals of $\mathcal{O}_K$. Note that χ is implicitly extended to all ideals by defining $\chi(\mathfrak{a}) = 0$ whenever $(\mathfrak{a}, \mathfrak{m}_0) \neq 1$. When χ is the trivial character on $\mathcal{I}(K)$, we obtain the Dedekind zeta function of K, $\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$. These L-functions are extended meromorphically on the complex plane with at most a simple pole at $s = 1$, which occurs if and only if χ is principal. Let R_χ be the set of zeros of L_χ on the critical strip $0 < \Re\mathfrak{e}(s) < 1$. The ERH implies that all Hecke L-functions are zero-free in the half-plane $\Re\mathfrak{e}(s) > \frac{1}{2}$.

We will extensively use the logarithmic derivatives L'_χ/L_χ. When $\Re\mathfrak{e}(s) > 1$, they admit the absolutely convergent representation

$$\frac{L'_\chi}{L_\chi}(s) = -\sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})\chi(\mathfrak{a})}{N(\mathfrak{a})^s}, \tag{2-1}$$

[1] A modulus $\mathfrak{m}'$ is (strictly) smaller than $\mathfrak{m}$ if $\mathfrak{m}'_0 \mid \mathfrak{m}_0$, $\mathfrak{m}'_\infty \subseteq \mathfrak{m}_\infty$ and $\mathfrak{m}' \neq \mathfrak{m}$.

place	residue of ζ_K'/ζ_K	residue of L_χ'/L_χ
1	-1	0
$\rho \in R_1$	1	0 if $\rho \notin R_\chi$, 1 otherwise
$\rho \in R_\chi$	0 if $\rho \notin R_1$, 1 otherwise	1
0	$r_1 + r_2 - 1$	$r_1 + r_2 - \beta_\chi$
$-2n+1,\ n \in \mathbb{N}_{>0}$	r_2	$r_2 + \beta_\chi$
$-2n,\ n \in \mathbb{N}_{>0}$	$r_1 + r_2$	$r_1 + r_2 - \beta_\chi$

Table 1. Residues of the logarithmic derivative of Hecke L-functions, when χ is a primitive ray class character [1, p. 361].

where Λ is the von Mangoldt function (i.e., $\Lambda(\mathfrak{a}) = \log N(\mathfrak{p})$ if $\mathfrak{a}$ is a power of a prime ideal $\mathfrak{p}$, and 0 otherwise). The residues of L_χ'/L_χ when χ is primitive modulo $\mathfrak{m}$ are summarized in Table 1, which comes from [1, p. 361] (with the observation that β in [1] coincides with $\beta_\chi = |\mathfrak{m}_\infty|$ for characters χ which are primitive modulo $\mathfrak{m}$).

Let ψ be the logarithmic derivative of the gamma function, and for any ray class character χ on K, define

$$\psi_\chi(s) = \frac{r_1 + r_2 - \beta_\chi}{2}\psi\left(\frac{s}{2}\right) + \frac{r_2 + \beta_\chi}{2}\psi\left(\frac{s+1}{2}\right) - \frac{n\log\pi}{2}. \tag{2-2}$$

The main reason to introduce these functions is the following formula: for any complex number s, if χ is primitive then

$$-\Re\mathfrak{e}\frac{L_\chi'}{L_\chi}(s) = \tfrac{1}{2}\log(\Delta N(\mathfrak{f}_\chi)) + \Re\mathfrak{e}\left(\delta(\chi)\left(\frac{1}{s} + \frac{1}{s-1}\right) - \sum_{\rho\in R_\chi}\frac{1}{s-\rho} + \psi_\chi(s)\right). \tag{2-3}$$

A proof can be found in [12, Lemma 5.1].

3. Proof of the main theorem

Throughout this section, consider a ray class character χ modulo $\mathfrak{m}$ that is not trivial on a given subgroup H of $G = \mathrm{Cl}_\mathfrak{m}(K)$.

3A. ***Outline of the proof.*** For any $0 < a < 1,\ x > 0$, and ideal $\mathfrak{a}$, let

$$P(\mathfrak{a}, x) = \Lambda(\mathfrak{a})\left(\frac{N(\mathfrak{a})}{x}\right)^a \log\left(\frac{x}{N(\mathfrak{a})}\right).$$

Let us start by recalling a lemma that is the starting point of the original proof of Bach's bounds.

Lemma 3.1 [1, Lemma 4.2]. *For $0 < a < 1$ and any character η,*

$$\sum_{N(\mathfrak{a})<x}\eta(\mathfrak{a})P(\mathfrak{a}, x) = -\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{x^s}{(s+a)^2}\cdot\frac{L_\eta'}{L_\eta}(s)\,ds.$$

Bach then considers the difference between two instances of this equality at $\eta = 1$ and at $\eta = \chi$, and proves the bounds by estimating the right-hand side as $x + O(\sqrt{x})$, while the left-hand side is zero if the character is trivial on all prime ideals of norm smaller than x; therefore such an x cannot be too large.

The proof of Theorem 1.1 follows the same strategy. It exploits the series of lemmata provided in [1, Section 5], interlacing them with a game of characters of G/H in order to account for the new condition $[\mathfrak{a}]_{\mathfrak{m}} \in H$. Consider the group of characters of the quotient G/H, namely $\widehat{G/H} = \mathrm{Hom}(G/H, \mathbb{C}^\times)$. Given any character $\theta \in \widehat{G/H}$, let θ^* be the primitive ray class character such that $\theta^*(\mathfrak{a}) = \theta([\mathfrak{a}]_{\mathfrak{m}} H)$ whenever $(\mathfrak{a}, \mathfrak{m}_0) = 1$. For any $\theta \in \widehat{G/H}$, write L_θ for the L-function of θ^*. For any ray class character η and any $\theta \in \widehat{G/H}$, let η_θ denote the primitive character inducing the product $\eta\theta^*$.

Lemma 3.2. *Let $\mathfrak{a}$ be any ideal in K. Let $\mathfrak{n}_0$ be the largest divisor of $\mathfrak{m}_0$ coprime to $\mathfrak{a}$, and $\mathfrak{n} = \mathfrak{n}_0\mathfrak{m}_\infty$. Let $\pi : \mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Cl}_{\mathfrak{n}}(K)$ be the natural projection. Then,*

$$\sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}) = \begin{cases} [\mathrm{Cl}_{\mathfrak{n}}(K) : \pi(H)] & \text{if } [\mathfrak{a}]_{\mathfrak{n}} \in \pi(H), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $\Theta_{\mathfrak{a}} = \{\theta \in \widehat{G/H} \mid \theta^*(\mathfrak{a}) \neq 0\} = \{\theta \in \widehat{G/H} \mid (\mathfrak{f}_{\theta^*}, \mathfrak{a}) = 1\}$. This set is naturally in bijection with the group X of characters of $\mathrm{Cl}_{\mathfrak{n}}(K)/\pi(H)$. We obtain

$$\sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}) = \sum_{\theta \in \Theta_{\mathfrak{a}}} \theta^*(\mathfrak{a}) = \sum_{\nu \in X} \nu([\mathfrak{a}]_{\mathfrak{n}}) = \begin{cases} [\mathrm{Cl}_{\mathfrak{n}}(K) : \pi(H)] & \text{if } [\mathfrak{a}]_{\mathfrak{n}} \in \pi(H), \\ 0 & \text{otherwise.} \end{cases}$$ □

Lemma 3.3. *For any $0 < a < 1$, we have*

$$\mathcal{S}_{\mathfrak{m}}(x) + \mathcal{S}_H(x) = -\frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} I(x, \theta),$$

where

$$\mathcal{S}_H(x) = \sum_{\substack{N(\mathfrak{a}) < x \\ [\mathfrak{a}]_{\mathfrak{m}} \in H}} (1 - \chi(\mathfrak{a})) P(\mathfrak{a}, x),$$

$$\mathcal{S}_{\mathfrak{m}}(x) = \frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a}, \mathfrak{m}) \neq 1}} (\theta^*(\mathfrak{a}) - \chi_\theta(\mathfrak{a})) P(\mathfrak{a}, x), \text{ and}$$

$$I(x, \theta) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2} \left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}} \right)(s)\, ds.$$

Proof. From Lemma 3.2, for any ray class character η, we have

$$\sum_{\substack{N(\mathfrak{a}) < x \\ [\mathfrak{a}]_{\mathfrak{m}} \in H}} \eta(\mathfrak{a}) P(\mathfrak{a}, x) = \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a}, \mathfrak{m}) = 1}} \frac{\sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a})}{[G:H]} \eta(\mathfrak{a}) P(\mathfrak{a}, x) = \frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a}, \mathfrak{m}) = 1}} \eta_\theta(\mathfrak{a}) P(\mathfrak{a}, x).$$

Subtracting two instances of this equality, for $\eta = 1$ and $\eta = \chi$, we get

$$\mathcal{S}_H(x) = \frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} \sum_{N(\mathfrak{a}) < x} (\theta^*(\mathfrak{a}) - \chi_\theta(\mathfrak{a}))P(\mathfrak{a}, x) - \mathcal{S}_{\mathfrak{m}}(x)$$

and conclude by applying Lemma 3.1. □

Lemma 3.4. *For $0 < a < 1$, and with the notation from Lemma 3.3,*

$$\frac{x}{(a+1)^2} = [G:H](\mathcal{S}_H(x) + \mathcal{S}_{\mathfrak{m}}(x)) + \sum_{\theta \in \widehat{G/H}} (I_{1/2}(x,\theta) + I_0(x,\theta) + I_-(x,\theta)),$$

where

$$I_-(x,\theta) = (\beta_{\chi_\theta} - \beta_\theta) \sum_{k=2}^{\infty} \frac{(-1)^k}{(a-k)^2 x^k},$$

$$I_{1/2}(x,\theta) = \sum_{\rho \in R_\theta} \frac{x^\rho}{(\rho+a)^2} - \sum_{\rho \in R_{\chi_\theta}} \frac{x^\rho}{(\rho+a)^2}, \text{ and}$$

$$I_0(x,\theta) = \frac{\log x}{x^a}\left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(-a) + \frac{1}{x^a}\left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)'(-a) + (\beta_{\chi_\theta} - \beta_\theta)\left(\frac{1}{a^2} - \frac{1}{x(a-1)^2}\right) - \frac{\delta(\theta)}{a^2}.$$

Recall that for any character η, R_η is the set of zeros of L_η on the strip $0 < \mathfrak{Re}(s) < 1$.

Proof. This lemma is an analogue of [1, Lemma 4.4]. Evaluating each integral $I(x,\theta)$ by residue using Table 1 yields

$$I(x,\theta) = I_{1/2}(x,\theta) + I_0(x,\theta) + I_-(x,\theta) - \frac{\delta(\theta)x}{(a+1)^2}.$$

The residue calculations can be justified as in the proof of [12, Theorem 28]. The result follows from Lemma 3.3. □

3B. ***Explicit estimates.*** This section adopts the notation from Lemmas 3.3 and 3.4. The remainder of the proof consists in evaluating each term in the formula of Lemma 3.4. More precisely, we bound the quantities

(1) $I_{1/2}$ in Lemma 3.7,

(2) I_0 in Lemma 3.9,

(3) $\mathcal{S}_{\mathfrak{m}}$ in Lemma 3.10,

(4) $\mathcal{S}_H$ in Lemma 3.12.

The quantity I_- remains, which is easy to bound thanks to [1, Lemma 5.1]. All these estimates are combined in Lemma 3.11. Let

$$\mathcal{R}(a,\chi) = \sum_{\theta \in \widehat{G/H}} \left(\sum_{\rho \in R_\theta} \frac{1}{|\rho + a|^2} + \sum_{\rho \in R_{\chi_\theta}} \frac{1}{|\rho + a|^2} \right).$$

We bound that quantity in Lemma 3.6, but first, we need the following lemma.

Lemma 3.5. *For $\Re\mathfrak{e}(s) > 1$, we have*

$$\sum_{\theta\in\widehat{G/H}}\left(\frac{L'_\theta}{L_\theta}+\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(s)\le 0.$$

Proof. Equation (2-1) yields

$$\sum_{\theta\in\widehat{G/H}}\left(\frac{L'_\theta}{L_\theta}+\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(s)=-\sum_{\theta\in\widehat{G/H}}\sum_{\mathfrak{a}}\frac{\Lambda(\mathfrak{a})(\chi_\theta(\mathfrak{a})+\theta^*(\mathfrak{a}))}{N(\mathfrak{a})^s}=-\sum_{\mathfrak{a}}\frac{\Lambda(\mathfrak{a})}{N(\mathfrak{a})^s}\sum_{\theta\in\widehat{G/H}}(\chi_\theta(\mathfrak{a})+\theta^*(\mathfrak{a})).$$

Fix an ideal $\mathfrak{a}$. If $\chi_\theta(\mathfrak{a})=0$ for all θ, Lemma 3.2 implies

$$\sum_{\theta\in\widehat{G/H}}(\chi_\theta(\mathfrak{a})+\theta^*(\mathfrak{a}))\ge 0.$$

Now suppose that there exists an $\eta\in\widehat{G/H}$ such that $\chi_\eta(\mathfrak{a})\neq 0$. The fact that any given character is induced by a unique primitive character implies that for any $\theta\in\widehat{G/H}$, we have $\chi_\theta(\mathfrak{a})=\chi_\eta(\mathfrak{a})(\theta\eta^{-1})^*(\mathfrak{a})$. Indeed, if $(\theta\eta^{-1})^*(\mathfrak{a})\neq 0$, the equality follows from the fact that χ_θ is the primitive character inducing $\chi_\eta\cdot(\theta\eta^{-1})^*$, and if $(\theta\eta^{-1})^*(\mathfrak{a})=0$, then one must have $\chi_\theta(\mathfrak{a})=0$ because $(\theta\eta^{-1})^*$ is the primitive character inducing χ_θ/χ_η. We deduce that

$$\sum_{\theta\in\widehat{G/H}}(\chi_\theta(\mathfrak{a})+\theta^*(\mathfrak{a}))=\chi_\eta(\mathfrak{a})\sum_{\theta\in\widehat{G/H}}\left(\frac{\theta}{\eta}\right)^*(\mathfrak{a})+\sum_{\theta\in\widehat{G/H}}\theta^*(\mathfrak{a})=(\chi_\eta(\mathfrak{a})+1)\sum_{\theta\in\widehat{G/H}}\theta^*(\mathfrak{a}),$$

whose real part is nonnegative (using again Lemma 3.2). □

Lemma 3.6 (ERH). *Let $0<a<1$. The sum $\mathcal{R}(a,\chi)$ is at most*

$$\frac{2[G:H]}{2a+1}\left(\log(\Delta N(\mathfrak{m}_0))+n(\psi(a+1)-\log(2\pi))-\frac{|\mathfrak{m}_\infty|}{2}\left(\psi\left(\frac{a+1}{2}\right)-\psi\left(\frac{a+2}{2}\right)\right)\right)+\frac{2}{2a+1}\left(\frac{1}{a+1}+\frac{1}{a}\right).$$

Proof. Writing $\sigma=1+a$, we have

$$\frac{2a+1}{|\rho+a|^2}=\frac{1}{\sigma-\rho}+\frac{1}{\sigma-\overline{\rho}}$$

for any $\Re\mathfrak{e}(\rho)=\frac{1}{2}$ (as observed in [1, Lemma 5.5]), so for any ray class character η

$$\sum_{\rho\in R_\eta}\frac{1}{|\rho+a|^2}=\frac{1}{2a+1}\sum_{\rho\in R_\eta}\left(\frac{1}{\sigma-\rho}+\frac{1}{\sigma-\overline{\rho}}\right).$$

As in [12, Lemma 5.1], we get from (2-3) that

$$\sum_{\rho\in R_\eta}\left(\frac{1}{\sigma-\rho}+\frac{1}{\sigma-\overline{\rho}}\right)=2\Re\mathfrak{e}\frac{L'_\eta}{L_\eta}(\sigma)+\log(\Delta N(\mathfrak{f}_\eta))+2\delta(\eta)\left(\frac{1}{\sigma}+\frac{1}{\sigma-1}\right)+2\psi_\eta(\sigma).$$

Then, $\mathcal{R}(a,\eta)$ is at most

$$\frac{1}{2a+1}\sum_{\theta\in\widehat{G/H}}\left(2\mathfrak{Re}\left(\frac{L'_\theta}{L_\theta}+\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(\sigma)+\log(\Delta^2 N(\mathfrak{f}_\theta\mathfrak{f}_{\chi_\theta}))+2\delta(\theta)\left(\frac{1}{\sigma}+\frac{1}{\sigma-1}\right)+2(\psi_\theta(\sigma)+\psi_{\chi_\theta}(\sigma))\right). \quad (3\text{-}1)$$

From Lemma 3.5, we have $\sum_{\theta\in\widehat{G/H}}(L'_\theta/L_\theta + L'_{\chi_\theta}/L_{\chi_\theta})(\sigma)\le 0$, and the corresponding term can be discarded from the expression in (3-1). Also, with $\alpha_{\chi_\theta}=r_1-\beta_{\chi_\theta}$,

$$\begin{aligned}2(\psi_\theta(\sigma)+\psi_{\chi_\theta}(\sigma)) &= (n+\alpha_{\chi_\theta}-\beta_\theta)\psi\left(\frac{a+1}{2}\right)+(n-\alpha_{\chi_\theta}+\beta_\theta)\psi\left(\frac{a+2}{2}\right)-2n\log\pi\\ &= 2n(\psi(a+1)-\log(2\pi))+(\alpha_{\chi_\theta}-\beta_\theta)\left(\psi\left(\frac{a+1}{2}\right)-\psi\left(\frac{a+2}{2}\right)\right)\\ &\le 2n(\psi(a+1)-\log(2\pi))-|\mathfrak{m}_\infty|\left(\psi\left(\frac{a+1}{2}\right)-\psi\left(\frac{a+2}{2}\right)\right),\end{aligned}$$

where the first equality uses the expression (2-2) and the second one follows from the duplication formula $(\psi(z/2)+\psi((z+1)/2)=2(\psi(z)-\log 2))$. □

Lemma 3.7 (ERH). *For $0<a<1$ and $x\ge 1$, we have $\sum_{\theta\in\widehat{G/H}}|I_{1/2}(x,\theta)|\le\sqrt{x}\cdot\mathcal{R}(a,\chi)$.*

Proof. From the ERH, for any ray class character η and any zero $\rho\in R_\eta$ of L_η on the critical strip, we have $\mathfrak{Re}(\rho)\le\frac{1}{2}$. Therefore $|x^\rho|=|x|^{\mathfrak{Re}(\rho)}\le\sqrt{x}$. □

Lemma 3.8. *For any s,*

$$\begin{aligned}\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(s) &= \sum_{\rho\in R_\theta}\left(\frac{1}{s-\rho}-\frac{1}{2-\rho}\right)-\sum_{\rho\in R_{\chi_\theta}}\left(\frac{1}{s-\rho}-\frac{1}{2-\rho}\right)\\ &\quad-\frac{\beta_{\chi_\theta}-\beta_\theta}{2}\left(\psi\left(\frac{s}{2}\right)-\psi\left(\frac{s+3}{2}\right)-\psi(1)+\psi\left(\frac{3}{2}\right)\right)\\ &\quad-\frac{\beta_{\chi_\theta}-\beta_\theta}{s+1}+\delta(\theta)\left(\frac{3}{2}-\frac{1}{s}-\frac{1}{s-1}\right)+\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(2),\end{aligned}$$

and

$$\begin{aligned}\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)'(s) &= \sum_{\rho\in R_{\chi_\theta}}\frac{1}{(s-\rho)^2}-\sum_{\rho\in R_\theta}\frac{1}{(s-\rho)^2}\\ &\quad-\frac{\beta_{\chi_\theta}-\beta_\theta}{4}\left(\psi'\left(\frac{s}{2}\right)-\psi'\left(\frac{s+3}{2}\right)\right)+\frac{\beta_{\chi_\theta}-\beta_\theta}{(s+1)^2}+\delta(\theta)\left(\frac{1}{s^2}+\frac{1}{(s-1)^2}\right).\end{aligned}$$

Proof. This is essentially the same proof as [1, Lemma 5.2], with an additional use of the recurrence relations $\psi(z)=\psi(z+1)-1/z$ and $\psi'(z)=\psi'(z+1)+1/z^2$. □

Lemma 3.9 (ERH). *Let* $0 < a < 1$ *and* $x \geq 1$. *Then*,

$$\sum_{\theta \in \widehat{G/H}} I_0(x,\theta) \leq \frac{(2+a)\log x + 1}{x^a} \cdot \mathcal{R}(a,\chi) + \frac{[G:H]|\mathfrak{m}_\infty|}{a^2} - \frac{1}{a^2} + \frac{\log x}{x^a}\left(\frac{3}{2} + \frac{1}{a} + \frac{1}{a+1}\right) + \frac{1}{x^a}\left(\frac{1}{a^2} + \frac{1}{(a+1)^2}\right) + \frac{[G:H]|\mathfrak{m}_\infty|}{x}\left(\frac{1}{(1-a)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2 x^{a-1}}\right).$$

Proof. For any $0 < a < 1$, Lemma 3.8 implies

$$\sum_{\theta \in \widehat{G/H}} \left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(-a) \leq (2+a)\cdot \mathcal{R}(a,\chi) + \frac{3}{2} + \frac{1}{a} + \frac{1}{a+1} - \sum_{\theta \in \widehat{G/H}} \frac{\beta_{\chi_\theta} - \beta_\theta}{1-a}$$

and

$$\sum_{\theta \in \widehat{G/H}} \left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)'(-a) \leq \mathcal{R}(a,\chi) + \frac{1}{a^2} + \frac{1}{(a+1)^2} + \sum_{\theta \in \widehat{G/H}} \frac{\beta_{\chi_\theta} - \beta_\theta}{(1-a)^2}.$$

We used the facts that $\psi(-a/2) - \psi((3-a)/2) - \psi(1) + \psi\left(\frac{3}{2}\right) \geq 0$, and $\psi'(-a/2) - \psi'((3-a)/2) \geq 0$, which are easily derived from the recurrence relations $\psi(z) = \psi(z+1) - 1/z$ and $\psi'(z) = \psi'(z+1) + 1/z^2$, and the monotonicity of ψ and ψ'. From [1, Lemma 5.3], for any $0 < a < 1$, we have

$$\left(\frac{\log x}{(a-1)x^{a-1}} + \frac{1}{(a-1)^2 x^{a-1}} - \frac{1}{(1-a)^2}\right) \leq 0;$$

therefore

$$\sum_{\theta \in \widehat{G/H}} \frac{\beta_{\chi_\theta} - \beta_\theta}{x}\left(\frac{\log x}{(a-1)x^{a-1}} + \frac{1}{(a-1)^2 x^{a-1}} - \frac{1}{(1-a)^2}\right) \leq \frac{[G:H]|\mathfrak{m}_\infty|}{x}\left(\frac{1}{(1-a)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2 x^{a-1}}\right).$$

The result follows by applying these estimates to $I_0(x,\theta)$ (as defined in Lemma 3.4). □

Lemma 3.10. *For any* $0 < a < 1$,

$$\mathcal{S}_{\mathfrak{m}}(x) \leq \frac{2\log x}{ea}\omega(\mathfrak{m}_0) \leq \frac{2\log x}{ea\log 2}\log(N(\mathfrak{m}_0)),$$

where $\omega(\mathfrak{m}_0)$ *is the number of distinct prime ideals dividing* $\mathfrak{m}_0$.

Proof. We have

$$\mathcal{S}_{\mathfrak{m}}(x) = \frac{1}{[G:H]} \sum_{\substack{N(\mathfrak{a})<x \\ (\mathfrak{a},\mathfrak{m})\neq 1}} \left(\sum_{\theta \in \widehat{G/H}} (\theta^*(\mathfrak{a}) - \chi_\theta(\mathfrak{a}))\right) P(\mathfrak{a},x) \leq \sum_{\substack{N(\mathfrak{a})<x \\ (\mathfrak{a},\mathfrak{m})\neq 1}} 2P(\mathfrak{a},x),$$

and the result follows from [1, Lemma 5.7]. □

Lemma 3.11 (ERH). *For any $0 < a < 1$, the fraction $\sqrt{x}/(a+1)^2$ is at most*

$$[G:H]\left(s_1(x)\log(\Delta N(\mathfrak{m}_0)) + s_5(x)n + s_4(x)|\mathfrak{m}_\infty| + s_3(x)\omega(\mathfrak{m}_0) + \frac{\mathcal{S}_H(x)}{\sqrt{x}}\right) + s_2(x),$$

where

$$s_1(x) = \frac{2}{2a+1}\left(1 + \frac{(2+a)\log x + 1}{x^{a+1/2}}\right),$$

$$s_2(x) = s_1(x)\left(\frac{1}{a} + \frac{1}{a+1}\right) + \frac{\log x}{x^{a+1/2}}\left(\frac{3}{2} + \frac{1}{a} + \frac{1}{a+1}\right) + \frac{1}{x^{a+1/2}}\left(\frac{1}{a^2} + \frac{1}{(a+1)^2}\right),$$

$$s_3(x) = \frac{2\log x}{ea\sqrt{x}},$$

$$s_4(x) = \frac{1}{(a-2)^2x^{5/2}} - \frac{s_1(x)}{2}\left(\psi\left(\frac{a+1}{2}\right) - \psi\left(\frac{a+2}{2}\right)\right) + \frac{1}{a^2\sqrt{x}} + \frac{1}{x^{3/2}}\left(\frac{1}{(1-a)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2x^{a-1}}\right),$$

$$s_5(x) = s_1(x)(\psi(a+1) - \log(2\pi)).$$

Proof. As in [1, Lemma 5.1], we have

$$0 \le \sum_{k=2}^{\infty} \frac{(-1)^k}{(a-k)^2x^k} \le \frac{1}{(a-2)^2x^2}.$$

We deduce that

$$I_-(x,\theta) \le \frac{|\beta_{\chi_\theta} - \beta_\theta|}{(a-2)^2x^2} \le \frac{|\mathfrak{m}_\infty|}{(a-2)^2x^2}.$$

Together with Lemma 3.7, the bound from Lemma 3.4 becomes

$$\frac{\sqrt{x}}{(a+1)^2} \le \frac{[G:H]|\mathfrak{m}_\infty|}{(a-2)^2x^{5/2}} + \mathcal{R}(a,\chi) + \frac{1}{\sqrt{x}}\sum_{\theta\in\widehat{G/H}} I_0(x,\theta) + [G:H]\frac{\mathcal{S}_H(x) + \mathcal{S}_{\mathfrak{m}}(x)}{\sqrt{x}}.$$

The result then follows from Lemmas 3.6, 3.9 and 3.10. □

Lemma 3.12. *Suppose that $\chi(\mathfrak{p}) = 1$ for all prime ideals $\mathfrak{p}$ such that $N(\mathfrak{p}) < x$, $[\mathfrak{p}]_{\mathfrak{m}} \in H$, and $\deg(\mathfrak{p}) = 1$. Then, for any $0 < a < 1$,*

$$\mathcal{S}_H(x) \le \frac{2n}{ea}\sum_{m<\sqrt{x}} \Lambda(m).$$

Proof. We start as in [1, Lemma 5.7] by observing that when $t \ge 1$, the function $t^{-a}\log t$ is bounded above by $1/(ea)$. We deduce

$$\mathcal{S}_H(x) = \sum_{\substack{N(\mathfrak{a})<x\\ [\mathfrak{a}]_{\mathfrak{m}}\in H}} (1-\chi(\mathfrak{a}))P(\mathfrak{a},x) \le \frac{2}{ea}\sum_{\substack{N(\mathfrak{a})<x\\ [\mathfrak{a}]_{\mathfrak{m}}\in H\\ \chi(\mathfrak{a})\ne 1}} \Lambda(\mathfrak{a}). \tag{3-2}$$

Fix a prime ideal $\mathfrak{p}$ (above a rational prime p) of norm smaller than x and consider the contribution of its powers to the above sum. First suppose that $\deg(\mathfrak{p}) > 1$. Then,

$$\sum_{\substack{N(\mathfrak{p}^k)<x\\ [\mathfrak{p}^k]_{\mathfrak{m}}\in H\\ \chi(\mathfrak{p}^k)\neq 1}} \Lambda(\mathfrak{p}^k) \le \sum_{N(\mathfrak{p}^k)<x} \deg(\mathfrak{p})\Lambda(p^k) \le \deg(\mathfrak{p}) \sum_{p^k<\sqrt{x}} \Lambda(p^k).$$

Now suppose that $\deg(\mathfrak{p}) = 1$, and let ℓ be the smallest integer such that $[\mathfrak{p}^\ell]_{\mathfrak{m}} \in H$. If $\ell = 1$, then $\chi(\mathfrak{p}^k) = 1$ for any integer k, so the contribution of $\mathfrak{p}$ is zero. Suppose that $\ell \ge 2$. Then,

$$\sum_{\substack{N(\mathfrak{p}^k)<x\\ [\mathfrak{p}^k]_{\mathfrak{m}}\in H\\ \chi(\mathfrak{p}^k)\neq 1}} \Lambda(\mathfrak{p}^k) \le \sum_{N(\mathfrak{p}^{k\ell})<x} \Lambda(\mathfrak{p}^{k\ell}) \le \deg(\mathfrak{p}) \sum_{p^k<\sqrt{x}} \Lambda(p^k).$$

Summing over all rational primes p and ideals $\mathfrak{p}$ above p, we obtain

$$\sum_{p}\sum_{\mathfrak{p}\mid p}\sum_{\substack{N(\mathfrak{p}^k)<x\\ [\mathfrak{p}^k]_{\mathfrak{m}}\in H\\ \chi(\mathfrak{p}^k)\neq 1}} \Lambda(\mathfrak{p}^k) \le \sum_{p}\sum_{\mathfrak{p}\mid p} \deg(\mathfrak{p}) \sum_{p^k<\sqrt{x}} \Lambda(p^k) \le n \sum_{m<\sqrt{x}} \Lambda(m).$$

We conclude by applying this inequality to (3-2). □

Lemma 3.13. *For any $x > 0$,*

$$\lim_{a\to 1}\left(\frac{1}{(1-a)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2x^{a-1}}\right) = \frac{(\log x)^2}{2}.$$

Proof. A simple application of L'Hôpital's rule yields

$$\begin{aligned}\lim_{a\to 1}\left(\frac{1}{(1-a)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2x^{a-1}}\right) &= \lim_{b\to 0}\left(\frac{x^b - b\log x - 1}{b^2x^b}\right) = \lim_{b\to 0}\left(\frac{x^b\log x - \log x}{bx^b(b\log(x)+2)}\right)\\ &= \lim_{b\to 0}\left(\frac{(\log x)^2}{b^2(\log x)^2 + 4b\log x + 2}\right) = \frac{(\log x)^2}{2}.\end{aligned}$$

□

3C. ***Proof of Theorem 1.1.*** Let x be the norm of the smallest prime ideal $\mathfrak{p}$ such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$, $\deg(\mathfrak{p}) = 1$ and $\chi(\mathfrak{p}) \neq 1$. First suppose that $x \le 95$, and consider the quantity

$$B = \big([G:H](2.71\log(\Delta N(\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{m}_0)) + 4.13\big)^2.$$

We want to show that $x \le B$.

Suppose $n = 1$. For the ray class group G to be nontrivial, one must have either $|\mathfrak{m}_\infty| = 1$ and $N(\mathfrak{m}_0) \ge 3$, in which case

$$B \ge (2.71\log(3) + 1.29 + 1.38 + 4.13)^2 = 95.59\ldots \ge x,$$

or $|\mathfrak{m}_\infty| = 0$ and $N(\mathfrak{m}_0) \ge 5$, in which case

$$B \ge (2.71\log(5) + 1.38 + 4.13)^2 = 97.44\ldots \ge x.$$

Suppose $n = 2$. Suppose that $\Delta N(\mathfrak{m}_0) \geq 8$. Then

$$B \geq (2.71 \log(8) + 4.13)^2 = 95.36\ldots \geq x.$$

Now, one must investigate the cases where $\Delta N(\mathfrak{m}_0) \leq 7$. All quadratic fields with a discriminant of absolute value at most 7 have a trivial (narrow) class group. Therefore, one must have $N(\mathfrak{m}_0) \geq 2$. There is only one quadratic field of discriminant of absolute value at most 3, namely $\mathbb{Q}(\sqrt{-3})$. It has discriminant of absolute value 3 and no ideal of norm 2, so the condition $\Delta N(\mathfrak{m}_0) \leq 7$ is impossible.

Suppose $n > 2$. From [1, Lemma 7.1], we get

$$\log(\Delta N(\mathfrak{f})) \geq n(\log(2\pi) - \psi(2)) - \tfrac{3}{2} \geq 2.74,$$

and we deduce

$$B \geq (2.71 \cdot 2.74 + 4.13)^2 = 133.52\ldots \geq x.$$

It remains to consider the case $x > 95$. From Lemma 3.12 and [18, Theorem 12],

$$\mathcal{S}_H(x) \leq \frac{2n}{ea} \sum_{m < \sqrt{x}} \Lambda(m) \leq \frac{2nC\sqrt{x}}{ea},$$

where $C = 1.03883$. We now apply Lemma 3.11 with $a \to 1$. From Lemma 3.13 (applied to the term s_4), and the facts that, for $x \geq 95$, $(s_5(x) + 2C/(ea))$ is negative and s_1, s_2, s_3 and s_4 are decreasing, we get

$$\begin{aligned} x &\leq 2^4\big([G:H]\big(s_1(95)\log(\Delta N(\mathfrak{m}_0)) + s_4(95)|\mathfrak{m}_\infty| + s_3(95)\omega(\mathfrak{m}_0)\big) + s_2(95)\big)^2 \\ &\leq \big([G:H]\big(2.71\log(\Delta N(\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{m}_0)\big) + 4.13\big)^2, \end{aligned}$$

which proves the theorem. □

4. Consequences

With Theorem 1.1 at hand, we can now derive a few important consequences. The first, Theorem 1.2, asserts that a subgroup H of the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ is always generated by ideals of bounded prime norm.

4A. ***Proof of Theorem 1.2.*** Recall that K is a number field, Δ is the absolute value of the discriminant of K, and $\mathfrak{m}$ is a modulus of K, with finite part $\mathfrak{m}_0$ and infinite part $\mathfrak{m}_\infty$. Also, $\mathfrak{h}$ is an ideal in K, and H is a nontrivial subgroup of the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$. Let

$$\begin{aligned} B &= \big([G:H](2.71\log(\Delta N(\mathfrak{h}\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{h}\mathfrak{m}_0)) + 4.13\big)^2, \\ \mathcal{N} &= \{\mathfrak{p} \in \mathcal{I}_{\mathfrak{m}}(K) \mid \mathfrak{p} \text{ is prime}, (\mathfrak{p}, \mathfrak{h}) = 1, [\mathfrak{p}]_{\mathfrak{m}} \in H, \deg(\mathfrak{p}) = 1 \text{ and } N(\mathfrak{p}) < B\}, \end{aligned}$$

and N be the subgroup of H generated by $\mathcal{N}$. By contradiction, suppose $N \neq H$. Then, there is a nontrivial character of H that is trivial on N. Since G is abelian, this character on H extends to a character on G, thereby defining a ray class character χ modulo $\mathfrak{m}$ that is not trivial on H. From Theorem 1.1, there is a

prime ideal $\mathfrak{p} \in \mathcal{I}_{\mathfrak{hm}}(K)$ such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$, $\chi(\mathfrak{p}) \neq 1$, $\deg(\mathfrak{p}) = 1$ and $N(\mathfrak{p}) \leq B$. All these conditions imply $\mathfrak{p} \in \mathcal{N} \subseteq N$, whence $\chi(\mathfrak{p}) = 1$, a contradiction. □

The next consequence, Theorem 1.3, is a specialization of Theorem 1.2 to the field of rational numbers, and asserts that a subgroup H of a group of the form $(\mathbb{Z}/m\mathbb{Z})^\times$ is generated by prime numbers bounded polynomially in the subgroup index and $\log(m)$.

4B. ***Proof of Theorem 1.3.*** Recall that m is a positive integer, and H is a nontrivial subgroup of $G = (\mathbb{Z}/m\mathbb{Z})^\times$. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0 = m\mathbb{Z}$ and $\mathfrak{m}_\infty$ is the real embedding of $\mathbb{Q}$. Then, $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q})$ is isomorphic to $G = (\mathbb{Z}/m\mathbb{Z})^\times$. An isomorphism is given by the map sending the class of $a\mathbb{Z}$ to $a \bmod m$. The subgroup H of $(\mathbb{Z}/m\mathbb{Z})^\times$ corresponds to a subgroup H' of $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q})$ through this isomorphism. From Theorem 1.2, H' is generated by prime numbers smaller than

$$B = \big([G : H](2.71\log(m) + 1.29 + 1.38\omega(m)) + 4.13\big)^2,$$

and so is H. If H is the full group, then the theorem follows from [1, Theorem 3], and for $m \leq 11000$, the result is easy to check by an exhaustive computation. So we can assume that $m/|H| \geq 2$ and $m > 11000$. From [1, Lemma 6.4],

$$\frac{\omega(m)}{\log m} \leq \frac{\mathrm{li}(\log m) + 0.12\sqrt{\log m}}{\log m} \leq \frac{\mathrm{li}(\log 11000) + 0.12\sqrt{\log 11000}}{\log 11000} \leq 0.67,$$

where li is the logarithmic integral function. We get

$$B \leq \left([G : H]\log(m)\left(2.71 + \frac{1.29 + 4.13/2}{\log 11000} + 1.38 \cdot 0.67\right)\right)^2,$$

and we conclude by computing the constant. □

The third consequence is a bound on the degrees of the cyclic isogenies required to connect all isogenous principally polarizable abelian varieties over a finite field sharing the same endomorphism ring.

4C. ***Proof of Theorem 1.4.*** Recall that $\mathcal{A}$ is a principally polarized, absolutely simple, ordinary abelian variety over a finite field $\mathbb{F}_q$, with endomorphism algebra K and endomorphism ring isomorphic to an order $\mathcal{O}$ in K. The field K_0 is the maximal real subfield of K, and $\mathfrak{f}$ is the conductor of $\mathcal{O}$. For any $B > 0$, $\mathcal{G}(B)$ is the isogeny graph whose vertices are the principally polarizable varieties isogenous to $\mathcal{A}$ and with the same endomorphism ring, and whose edges are isogenies connecting them, of prime degree (therefore cyclic) smaller than B. By the theory of complex multiplication, the graph $\mathcal{G}(B)$ is isomorphic to the Cayley graph of

$$\mathcal{P}(\mathcal{O}) = \ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}^+(\mathcal{O} \cap K_0))$$

with set of generators the classes of ideals of prime norm smaller than B (see [10, Section 2.5] for a detailed discussion of this isomorphism). Let $g \geq 2$ be the dimension of $\mathcal{A}$ and $n = 2g$ the degree of its endomorphism algebra K. The natural map $\pi : \mathrm{Cl}_{\mathfrak{f}}(K) \to \mathrm{Cl}(\mathcal{O})$ is a surjection (see for instance [10,

Section 2.2]), so it is sufficient to find a generating set for $H = \pi^{-1}(\mathcal{P}(\mathcal{O}))$. From [10, Lemma 2.1], we have the inequality

$$[\mathrm{Cl}_{\mathfrak{f}}(K) : H] \leq [\mathrm{Cl}(\mathcal{O}) : \mathcal{P}(\mathcal{O})] \leq h^+_{\mathcal{O}_0}.$$

From Theorem 1.2, $\mathcal{G}(B)$ is connected for

$$B = \left(2.71 + 1.38\frac{\omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} + \frac{4.13}{\log(\Delta N(\mathfrak{f}))}\right)^2 (h^+_{\mathcal{O}_0} \log(\Delta N(\mathfrak{f})))^2, \tag{4-1}$$

and it remains to show that the constant factor in this expression is at most 26. First, we need a lower bound on the quantity $\log(\Delta N(\mathfrak{f}))$. From [17, Table 3], if $n = 4$, then $\log(\Delta N(\mathfrak{f})) \geq 4\log(3.263) \geq 4.73$ (this result assumes the ERH). For $n \geq 6$, [1, Lemma 7.1] implies

$$\log(\Delta N(\mathfrak{f})) \geq n(\log(2\pi) - \psi(2)) - \tfrac{3}{2} \geq 6.99.$$

Therefore for any degree $n \geq 4$, we have $\log(\Delta N(\mathfrak{f})) \geq 4.73$. Now, for $n = 2$, smaller values of $\log(\Delta N(\mathfrak{f}))$ are possible. One can easily check that the constant factor in the expression (4-1) is at most 26 for all pairs $(\Delta, N(\mathfrak{f}))$ such that $\log(\Delta N(\mathfrak{f})) < 4.73$ by an exhaustive computation. There are however five exceptions: when the field is $\mathbb{Q}(\sqrt{-1})$ and $N(\mathfrak{f}) \in \{1, 2\}$, when the field is $\mathbb{Q}(\sqrt{-3})$ and $N(\mathfrak{f}) \in \{1, 3\}$, and when the field is $\mathbb{Q}(\sqrt{5})$ and $N(\mathfrak{f}) = 1$. Since $\mathfrak{f}$ is the conductor of an order in a quadratic field, it is generated by an integer, so $N(\mathfrak{f})$ must be a square. This discards the cases $N(\mathfrak{f}) \in \{2, 3\}$. When $N(\mathfrak{f}) = 1$, the order $\mathcal{O}$ is the ring of integers, which has a trivial (narrow) class group for $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{5})$.

Then, irrespective of the value of n, we can assume in the rest of the proof that $\log(\Delta N(\mathfrak{f})) \geq 4.73$. If $\omega(\mathfrak{f}) \leq 5$, then

$$\frac{\omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} \leq \frac{5}{4.73} \leq 1.06.$$

If $\omega(\mathfrak{f}) > 5$, then $N(\mathfrak{f}) \geq 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13^{\omega(\mathfrak{f})-5}$, and

$$\frac{\omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} \leq \frac{\omega(\mathfrak{f})}{\log(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13^{\omega(\mathfrak{f})-5})} \leq \frac{5}{\log(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11)} + \frac{1}{\log(13)} \leq 1.06.$$

Then,

$$\left(2.71 + \frac{1.38 \cdot \omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} + \frac{4.13}{\log(\Delta N(\mathfrak{f}))}\right)^2 \leq (2.71 + 1.38 \cdot 1.06 + 4.13/4.73)^2 \leq 26,$$

which concludes the proof. □

Acknowledgements

The author wishes to thank Arjen K. Lenstra and Rob Granger, as well as the anonymous referees, for their helpful feedback. Part of this work was supported by the Swiss National Science Foundation under grant number 200021-156420.

References

[1] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no.191, 355–380. MR 1023756

[2] Eric Bach and Jonathan Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. **65** (1996), no. 216, 1717–1735. MR 1355006

[3] Jean-François Biasse and Fang Song, *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields*, Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms (New York), ACM, 2016, pp. 893–902. MR 3478440

[4] P. Campbell, M. Groves, and D. Shepherd, *Soliloquy: a cautionary tale*, notes from ETSI 2nd Quantum-Safe Crypto Workshop, 2014.

[5] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev, *Recovering short generators of principal ideals in cyclotomic rings*, Advances in cryptology—EUROCRYPT 2016, II, Lecture Notes in Comput. Sci., no. 9666, Springer, 2016, pp. 559–585. MR 3516414

[6] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski, *Short Stickelberger class relations and application to ideal–SVP*, Advances in cryptology—EUROCRYPT 2017, I, Lecture Notes in Comput. Sci., no. 10210, Springer, 2017, pp. 324–348. MR 3652108

[7] Steven D. Galbraith, Florian Hess, and Nigel P. Smart, *Extending the GHS Weil descent attack*, Advances in cryptology—EUROCRYPT 2002, Lecture Notes in Comput. Sci., no. 2332, Springer, 2002, pp. 29–44. MR 1975526

[8] Sanjam Garg, Craig Gentry, and Shai Halevi, *Candidate multilinear maps from ideal lattices*, Advances in cryptology—EUROCRYPT 2013, Lecture Notes in Comput. Sci., no. 7881, Springer, 2013, pp. 1–17. MR 3095515

[9] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan, *Expander graphs based on GRH with an application to elliptic curve cryptography*, J. Number Theory **129** (2009), no. 6, 1491–1504. MR 2521489

[10] D. Jetchev and B. Wesolowski, *Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem*, Cryptology ePrint Archive, report 2017/053, 2017.

[11] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), no. 3, 271–296. MR 553223

[12] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham), Academic, London, 1977, pp. 409–464. MR 0447191

[13] Youness Lamzouri, Xiannan Li, and Kannan Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Math. Comp. **84** (2015), no. 295, 2391–2412. MR 3356031

[14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld, *GGHLite: more efficient multilinear maps from ideal lattices*, Advances in cryptology—EUROCRYPT 2014, Lecture Notes in Comput. Sci., no. 8441, Springer, 2014, pp. 239–256. MR 3213223

[15] Daniel Maisner and Enric Nart, *Abelian surfaces over finite fields as Jacobians*, Experiment. Math. **11** (2002), no. 3, 321–337. MR 1959745

[16] Jürgen Neukirch, *Algebraic number theory*, Grundl. Math. Wissen., no. 322, Springer, 1999. MR 1697859

[17] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sém. Théor. Nombres Bordeaux **2** (1990), no. 1, 119–141. MR 1061762

[18] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR 0137689

[19] René Schoof, *Minus class groups of the fields of the lth roots of unity*, Math. Comp. **67** (1998), no. 223, 1225–1245. MR 1458225

[20] Nigel P. Smart and Frederik Vercauteren, *Fully homomorphic encryption with relatively small key and ciphertext sizes*, Public key cryptography—PKC 2010, Lecture Notes in Comput. Sci., no. 6056, Springer, 2010, pp. 420–443. MR 2660756

[21] Benjamin Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, J. Cryptology **22** (2009), no. 4, 505–529. MR 2525710

Received 12 Feb 2018. Revised 14 Jun 2018.

BENJAMIN WESOLOWSKI: benjamin.wesolowski@epfl.ch
École Polytechnique Fédérale de Lausanne, EPFL IC LACAL, Switzerland

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine