THE LARGE SIEVE AND GALOIS REPRESENTATIONS

DAVID ZYWINA

ABSTRACT. We describe a generalization of the large sieve to situations where the underlying groups are nonabelian, and give several applications to the arithmetic of abelian varieties. In our applications, we sieve the set of primes via the system of representations arising from the Galois action on the torsion points of an abelian variety. The resulting upper bounds require explicit character sum calculations, with stronger results holding if one assumes the Generalized Riemann Hypothesis.

1. INTRODUCTION

1.1. **Overview.** In this paper, we explain how a sieve theoretic method called the *large sieve* can be suitably generalized to study various sequences of primes occurring in arithmetic geometry.

In §1.2–1.4, we shall give some applications of our sieve (proofs can be found in §4–6). These examples can be read independently of the rest of the paper and make no explicit reference to sieve theory or Galois representations. Our choice of applications is not meant to be exhaustive but simply demonstrate a few basic problems that can be attacked with sieve theoretic methods.

The large sieve is an important tool from analytic number theory (see [Bom74] and [Mon78] for background on the classical theory); our abstract form of the large sieve will be given in §2. The proof is similar to the classical version except one needs to be slightly careful since the underlying groups may not be abelian. E. Kowalski has independently come up with similar methods and has greatly generalized the large sieve (while adapting several of the ideas from an early version of this paper). The reader is strongly encouraged to look at [Kow08], which complements the material presented here.

In §3, we will specialize to the case of sieving primes by conditions indexed by a collection of independent Galois representations. The proof requires estimating various character sums, with stronger results being obtained if one assumes the Generalized Riemann Hypothesis. One of the merits of the large sieve is that these analytic number theory calculations need only be done once and we hope that Theorem 3.3 will be of practical use for others.

Our applications will be proved in a common manner. We first express the problem in terms of an independent system of strictly compatible Galois representations; these Galois representations give constraints on the set of primes that we are interested in. The large sieve allows us to combine these constraints intelligently. The reader interested in applying the sieve can skip directly to §3.

A quick remark is in order for analytic number theorists. By *large sieve*, we are referring to the sieve theoretic method of that name and not to the related inequalities. The large sieve inequalities in this paper are all proved in a straightforward manner. Since the large sieve inequality deals with "on average" behaviour, one would hope to be able to prove stronger unconditional versions (due to the nonabelian nature of the our examples, it seems difficult to generalize the usual harmonic analysis arguments). Any significant improvement on our unconditional bounds would be of great interest.

We introduce some notation that will hold throughout; further notation and conventions can be found in §1.6. For a number field k, denote its ring of integers by $\mathcal{O}_k$. Let Σ_k be the set of non-zero prime ideals of $\mathcal{O}_k$. For each prime $\mathfrak{p} \in \Sigma_k$, we have a residue field $\mathbb{F}_\mathfrak{p} = \mathcal{O}_k/\mathfrak{p}$ whose cardinality we denote by $N(\mathfrak{p})$. Let $\Sigma_k(x)$ be the set of primes $\mathfrak{p}$ in Σ_k with $N(\mathfrak{p}) \leq x$.

1.2. Application: The Koblitz conjecture.

Let E be an elliptic curve without complex multiplication defined over a number field k. Let S_E be the set of primes of k for which E has bad reduction. For each $\mathfrak{p} \in \Sigma_k - S_E$, denote the reduction of E modulo $\mathfrak{p}$ by $E_\mathfrak{p}$; it is an elliptic curve over $\mathbb{F}_\mathfrak{p}$. We have a finite group $E_\mathfrak{p}(\mathbb{F}_\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma_k - S_E$.

The following function is motivated by elliptic curve cryptography where the discrete logarithm problem for $E_\mathfrak{p}(\mathbb{F}_\mathfrak{p})$ is hardest when its cardinality is divisible by a large prime. Fix a positive integer t, define

$$P_{E,t}(x) := |\{\mathfrak{p} \in \Sigma_k(x) - S_E : |E_\mathfrak{p}(\mathbb{F}_\mathfrak{p})|/t \text{ is an integer and prime}\}|.$$

The following conjecture, in the case $t = 1$, is due to Koblitz [Kob88]; the extended version with a corrected constant can be found in [Zyw11].

Conjecture 1.1. Let E be an elliptic curve over a number field k without complex multiplication and fix an integer $t \geq 1$. There is an explicit constant $\mathcal{C}_{E,t} \geq 0$ such that

$$P_{E,t}(x) = \mathcal{C}_{E,t} \frac{x}{(\log x)^2} + o\left(\frac{x}{(\log x)^2}\right)$$

as $x \to \infty$.

The constant $\mathcal{C}_{E,t}$ will be described explicitly in §4. In the case where $\mathcal{C}_{E,t} = 0$, we shall observe in §4 that $P_{E,t}(x)$ is a bounded function of x. In general, there are no cases for which $\lim_{x \to \infty} P_{E,t}(x) = \infty$ has been proved. Using the large sieve, we obtain the following upper bounds for $P_{E,t}(x)$.

Theorem 1.2. Let E be an elliptic curve without complex multiplication defined over a number field k. Fix a positive integer t and suppose that $\mathcal{C}_{E,t} \neq 0$.

(i) Then
$$P_{E,t}(x) \leq (24 + o(1))\mathcal{C}_{E,t} \frac{x}{(\log x)(\log \log x)}.$$

(ii) Assuming the Generalized Riemann Hypothesis (GRH),
$$P_{E,t}(x) \leq (22 + o(1))\mathcal{C}_{E,t} \frac{x}{(\log x)^2}.$$

In both parts, the $o(1)$ term depends only on E/k and t.

Remark 1.3. Suppose $E/\mathbb{Q}$ is a non-CM elliptic curve. In [Coj05], Cojocaru proves that $P_{E,1}(x) \ll x/(\log x)^2$ assuming GRH[1]. The implicit constant depends on the conductor of E, but the exact dependency is not worked out. Cojocaru's bound is proved using the Selberg sieve.

Unconditionally, Cojocaru proves $P_{E,1}(x) \ll x/((\log x)(\log \log \log x))$. Though our unconditional bound is stronger, it is still not good enough to prove the analogue of Brun's theorem concerning the convergence of the sum of the reciprocal of twin primes. More precisely, it is unknown whether the sum $\sum_{p,|E_p(\mathbb{F}_p)| \text{ prime}} p^{-1}$ is always convergent. Using our upper bound and partial summation, we are only able to show that the sum has very slow growth:

$$\sum_{p \leq x, |E_p(\mathbb{F}_p)| \text{ prime}} p^{-1} \ll \log \log \log x.$$

---

[1] More precisely, Cojocaru needs only the θ-quasi GRH for some $1/2 \leq \theta < 1$; i.e., no Dedekind zeta function has a zero with real part greater that θ. If we assume only the θ-quasi GRH, then our methods yield Theorem 1.2(ii) with 22 replaced by a larger constant depending on θ.

1.3. **Application: Elliptic curves and thin sets.**

1.3.1. *Thin sets.* We recall the notion of a thin set, for more details see [Ser92, §3] or [Ser97, §9]. Fix a positive integer n.

Definition 1.4. A set $\Omega \subseteq \mathbb{Q}^n = \mathbb{A}^n(\mathbb{Q})$ is *thin* if there exists a variety X defined over $\mathbb{Q}$ and a morphism $\pi\colon X \to \mathbb{A}^n_{\mathbb{Q}}$ with the following properties:

(i) $\Omega \subseteq \pi(X(\mathbb{Q}))$,
(ii) The fibre of π over the generic point of $\mathbb{A}^n_{\mathbb{Q}}$ is finite and π has no rational section defined over $\mathbb{Q}$.

There are two special types of thin sets:

Type 1: Ω is contained in a proper closed subvariety of $\mathbb{A}^n_{\mathbb{Q}}$.
Type 2: $\Omega \subseteq \pi(X(\mathbb{Q}))$ where X is an irreducible variety over $\mathbb{Q}$ of dimension n and $\pi\colon X \to \mathbb{A}^n_{\mathbb{Q}}$ is a dominant morphism of degree $d \geq 2$.

Every thin subset of $\mathbb{Q}^n$ is contained in a finite union of thin sets of Type 1 and Type 2.

1.3.2. *Bounds.* Let E be an elliptic curve defined over a number field k. For each prime $\mathfrak{p} \in \Sigma_k$, let $a_{\mathfrak{p}}(E)$ be the corresponding *trace of Frobenius*. If E has good reduction at $\mathfrak{p}$, then $a_{\mathfrak{p}}(E) = N(\mathfrak{p}) + 1 - |E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})|$.

Theorem 1.5. *Let $E_1, \ldots, E_n$ be elliptic curves without complex multiplication defined over a number field k and assume that the E_i are pairwise non-isogenous over $\bar{k}$. Let Ω be a thin subset of $\mathbb{Z}^{n+1}$, and let $\Pi(x)$ be the set of $\mathfrak{p} \in \Sigma_k(x)$ for which $(a_{\mathfrak{p}}(E_1), \ldots, a_{\mathfrak{p}}(E_n), N(\mathfrak{p}))$ belongs to Ω. Then*

$$\Pi(x) \ll \begin{cases} x(\log\log x)^{1+1/(9n+3)}/(\log x)^{1+1/(18n+6)} \\ x^{1-1/(14n+8)}(\log x)^{2/(7n+4)} \end{cases} \qquad \text{assuming GRH.}$$

If Ω is a thin set of Type 1, then

$$\Pi(x) \ll \begin{cases} x((\log\log x)^2 \log\log\log x)^{1/(3n+1)}/(\log x)^{1+1/(3n+1)} \\ x^{1-1/(6n+2)}/(\log x)^{1-2/(3n+1)} \end{cases} \qquad \text{assuming GRH.}$$

The implicit constants depend on the E_i, k, and Ω.

Remark 1.6.

(i) Absorbing the extra factors, our theorem gives bounds of the form $x/(\log x)^{1+\gamma}$ (and $x^{1-\delta}$ under GRH) with explicit values $\gamma, \delta > 0$. Note that while the implicit constant of Theorem 1.5 depends on the thin set Ω, the function of x does not. It is natural to ask what the optimal function of x could be? The example of §1.5 suggests that the general bound is at best $x^{3/4}/(\log x)$.
(ii) Theorem 1.5 was inspired by published remarks of Serre. Remark 2 of [Ser92, §3.6] states (but does not prove) the unconditional case of the theorem for a single elliptic curve defined over $\mathbb{Q}$ (and does not describe the exponent). A similar remark for the Lang-Trotter conjecture of Example 1.7 is given in [Ser81, §8.2 Remark 4].
(iii) Theorem 1.5 in the case of a thin set of Type 1 is not proven using the large sieve. In this case, instead of sieving by many primes it is better to sieve by a single well chosen prime.

Let us consider a few special cases of Theorem 1.5.

Example 1.7. Let $E/\mathbb{Q}$ be a non-CM elliptic curve and K an imaginary quadratic extension of $\mathbb{Q}$. For each prime p of good reduction of E, let π_p be the Frobenius endomorphism of E_p (it is a root of $t^2 - a_p(E)t + p$). Define $\Pi_{E,K}(x) := |\{p \leq x : E \text{ has good reduction at } p, \mathbb{Q}(\pi_p) \cong K\}|$. The *Lang-Trotter conjecture* [LT76] predicts that there is a constant $C > 0$, depending on E and K, such that $\Pi_{E,K}(x) \sim C\frac{x^{1/2}}{\log x}$ as $x \to \infty$.

Define the set $\Omega = \{(a,b) \in \mathbb{Z}^2 : a^2 - 4b = D_K c^2 \text{ for some } c \in \mathbb{Q}^\times\}$ where D_K is the discriminant of K. Define $X = \mathrm{Spec}(\mathbb{Q}[x,y,z]/(x^2 - 4y - D_K z^2))$ and the morphism $\pi \colon X \to \mathrm{Spec}\,\mathbb{Q}[x,y] = \mathbb{A}_\mathbb{Q}^2$, $(x,y,z) \mapsto (x,y)$. The set $\Omega \subseteq \mathbb{Q}^2$ is thin of Type 2 since $\Omega \subseteq \pi(X(\mathbb{Q}))$, X is irreducible of dimension 2, and π is a dominant map of degree 2. We have $\Pi_{E,K}(x) = |\{p \leq x : (a_p(E), p) \in \Omega\}| + O(1)$. Theorem 1.5 implies that

$$\Pi_{E,K}(x) \ll \begin{cases} x(\log\log x)^{13/12}/(\log x)^{25/24} \\ x^{21/22}(\log x)^{2/11} \end{cases} \qquad \text{assuming GRH.}$$

Better bounds for this particular example can be found in [CD08] or [Zyw10].

Example 1.8. Let E and E' be non-CM elliptic curves over a number field k which are non-isogenous over $\bar{k}$. Define the set $\Omega = \{(a,b,c) \in \mathbb{Z}^3 : a = b\}$ which is thin of Type 1. Theorem 1.5 becomes

$$|\{\mathfrak{p} \in \Sigma_k(x) : a_\mathfrak{p}(E) = a_\mathfrak{p}(E')\}| \ll \begin{cases} x(\log\log x \cdot \log\log\log x)^{1/4}/(\log x)^{9/8} \\ x^{13/14}/(\log x)^{5/7} \end{cases} \qquad \text{assuming GRH.}$$

This gives an explicit version of a theorem of Faltings which shows that the values $a_\mathfrak{p}(E)$ determine the isogeny class of E. (That such a theorem can be deduced is not surprising given that work of Faltings is needed in the proof to describe the image of the corresponding Galois representations.)

1.4. **Application: Abelian varieties and Galois groups of characteristic polynomials.**

Definition 1.9. Fix a polynomial $P(T) \in \mathbb{Q}[T]$. The *Galois group* of P is defined to be $\mathrm{Gal}(P(T)) := \mathrm{Gal}(L/\mathbb{Q})$ where L is the splitting field of $P(T)$ in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

1.4.1. *Abelian varieties over finite fields.* Let A be an abelian variety of dimension g defined over a finite field $\mathbb{F}$ with q elements. Let π_A be the q-power Frobenius endomorphism of A. There is a unique polynomial $P_A(T) \in \mathbb{Z}[T]$ of degree $2g$ such that the isogeny $r - \pi_A$ of A has degree $P_A(r)$ for $r \in \mathbb{Z}$. The polynomial $P_A(T)$ satisfies the functional equation, $P_A(q/T)/(q/T)^g = P_A(T)/T^g$. From the functional equation we find that if π is a root of $P_A(T)$, then so is q/π. Let $\pi_1, \ldots, \pi_{2r}$ be the distinct non-rational roots of $P_A(T)$ in $\overline{\mathbb{Q}}$; we may assume that they are numbered so that $\pi_{2i-1}\pi_{2i} = q$ or $\{\pi_{2i-1}, \pi_{2i}\} = \{\pm\sqrt{q}\}$ for $1 \leq i \leq r$. The Galois group $\mathrm{Gal}(P_A(T))$ acts on the roots of $P_A(T)$ and induces an action on the r pairs $\{\pi_1, \pi_2\}, \ldots, \{\pi_{2r-1}, \pi_{2r}\}$.

Definition 1.10. Let W_{2r} be the group of permutations of $\{1, \ldots, 2r\}$ which induce a permutation of the set $\big\{\{1,2\}, \{3,4\}, \ldots, \{2r-1, 2r\}\big\}$.

The numbering of the π_i induces an injective homomorphism $\mathrm{Gal}(P_A(T)) \hookrightarrow W_{2r}$. In particular, we find that $\mathrm{Gal}(P_A(T))$ is isomorphic to a subgroup of W_{2g}. So W_{2g} is the largest possible Galois group for the polynomial $P_A(T)$. The group W_{2g} has order $2^g g!$ and is isomorphic to the Weyl group of $\mathrm{Sp}(2g)$.

1.4.2. *Explicit Chavdarov.* Fix an abelian variety A defined over a number field k and let $S_A \subseteq \Sigma_k$ be the set of prime ideals for which A has bad reduction. For each $\mathfrak{p} \in \Sigma_k - S_A$, let $A_\mathfrak{p}$ be the abelian variety over $\mathbb{F}_\mathfrak{p}$ obtained by reduction modulo $\mathfrak{p}$. For an integer $n \geq 1$, let $\mathbb{F}_\mathfrak{p}^{(n)}$ be the degree n field extension of $\mathbb{F}_\mathfrak{p}$ and let $A_\mathfrak{p} \times \mathbb{F}_\mathfrak{p}^{(n)}$ be the base extension of $A_\mathfrak{p}$ by $\mathbb{F}_\mathfrak{p}^{(n)}$.

We define Π_A to be the set of $\mathfrak{p} \in \Sigma_k - S_A$ such that

$$\mathrm{Gal}\big(P_{A_\mathfrak{p} \times \mathbb{F}_\mathfrak{p}^{(n)}}(T)\big) \not\cong W_{2g}$$

for some $n \geq 1$. The following result of Chavdarov [Cha97, Corollary 6.9] shows that Π_A has natural density 0 for certain abelian varieties.

Theorem 1.11 (Chavdarov). *Let A be an abelian variety of dimension g defined over a number field k. Suppose that g is either 2, 6 or odd, and $\mathrm{End}_{\bar{k}}(A) = \mathbb{Z}$. Then $\Pi_A(x)$ has natural density 0. Equivalently, the set of primes $\mathfrak{p} \in \Sigma_k - S_A$ for which $\mathrm{Gal}\big(P_{A_\mathfrak{p} \times \mathbb{F}_\mathfrak{p}^{(n)}}(T)\big) \cong W_{2g}$ for all $n \geq 1$, has natural density 1.*

The following theorem, which will be proven with the large sieve, gives an explicit version of Chavdarov's theorem. Define $\Pi_A(x) = \Pi_A \cap \Sigma_k(x)$.

Theorem 1.12. *Let A be an abelian variety of dimension g defined over a number field k. Suppose that g is either 2, 6 or odd, and $\mathrm{End}_{\bar{k}}(A) = \mathbb{Z}$. Then*

$$|\Pi_A(x)| \ll \frac{x(\log \log x)^{1+1/(6g^2+3g+3)}}{(\log x)^{1+1/(12g^2+6g+6)}},$$

and assuming the Generalized Riemann Hypothesis

$$|\Pi_A(x)| \ll x^{1-1/(8g^2+6g+8)}(\log x)^{2/(4g^2+3g+4)}.$$

The implicit constants depend only on A/k.

Remark 1.13.

(i) Theorem 1.12 can be used to bound the number of $\mathfrak{p}$ for which $A_\mathfrak{p}$ is not geometrically simple. Fix a prime $\mathfrak{p} \in \Sigma_k - (S \cup \Pi_A)$. For each $n \geq 1$, the polynomial $P_{A_\mathfrak{p} \times \mathbb{F}_\mathfrak{p}^{(n)}}(T)$ is irreducible since $\mathrm{Gal}(P_{A_\mathfrak{p} \times \mathbb{F}_\mathfrak{p}^{(n)}}(T)) \cong W_{2g}$ acts transitively on its $2g$ roots. We also deduce that $\mathbb{Q}(\pi_{A_\mathfrak{p}}^n) = \mathbb{Q}(\pi_{A_\mathfrak{p}})$ for all $n \geq 1$.

By [MW71, Theorem 8], for each $n \geq 1$ we have $\mathrm{End}_{\mathbb{F}_\mathfrak{p}^{(n)}}(A_\mathfrak{p}) \otimes_\mathbb{Z} \mathbb{Q} = \mathbb{Q}(\pi_{A_\mathfrak{p}}^n)$ and hence $\mathrm{End}_{\mathbb{F}_\mathfrak{p}^{(n)}}(A_\mathfrak{p}) \otimes_\mathbb{Z} \mathbb{Q} = \mathbb{Q}(\pi_{A_\mathfrak{p}})$. We deduce that $\mathrm{End}_{\overline{\mathbb{F}}_\mathfrak{p}}(A_\mathfrak{p}) \otimes_\mathbb{Z} \mathbb{Q} = \mathbb{Q}(\pi_{A_\mathfrak{p}})$ and thus $A_\mathfrak{p}/\mathbb{F}_\mathfrak{p}$ is geometrically simple. We thus obtain the following inequality

$$|\{\mathfrak{p} \in \Sigma_k(x) - S_A : A_\mathfrak{p} \text{ } not \text{ geometrically simple}\}| \leq |\Pi_A(x)|$$

and Theorem 1.12 gives an explicit upper bound.

(ii) The dimension assumptions on the abelian varieties are needed only to invoke a theorem of Serre which says that $\mathrm{Gal}(k(A[\ell])/k) \cong \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for all sufficiently large primes ℓ. This condition will hold for a "random" abelian variety A/k of any dimension g. See Hall [Hal08] which gives a nice sufficient condition to have $\mathrm{Gal}(k(A[\ell])/k) \cong \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for almost all ℓ.

(iii) The majority of [Cha97] deals with the function field setting in which Galois representations can be identified with representations of étale fundamental groups. The large sieve method is applicable in this context as well and this has already been studied in a paper of Kowalski [Kow06] (also see Chapter 8 of [Kow08]). The large sieve presented in this paper would need to be altered slightly to deal properly with both the arithmetic and geometric fundamental groups. In the function field setting one can prove strong unconditional bounds since one may use the full force of the Weil conjectures.

The large sieve of this paper has been used to give a generalization of Theorem 1.12 to an arbitrary geometrically simple abelian variety A/k, cf. [Zyw11, §9].

1.5. An explanatory example.

We shall now illustrate the basic concepts underlying the paper with a simple (but nontrivial!) example. The reader may safely skip ahead.

Fix an elliptic curve E defined over $\mathbb{Q}$ and assume that E does not have complex multiplication. Let S_E be the set of places of k for which E has bad reduction. For each prime $p \notin S_E$, let $a_p(E)$ be the integer such that $|E_p(\mathbb{F}_p)| = p - a_p(E) + 1$ where $E_p/\mathbb{F}_p$ is the reduction of E at p. In this example, we will study the set

$$\mathcal{A} := \{p \notin S_E : a_p(E) \text{ is a square}\}.$$

The set $\mathcal{A}$ is infinite (Elkies has shown that there are infinitely many p with $a_p(E) = 0$ [Elk87]). For each real number x, let $\mathcal{A}(x)$ be the set of $p \in \mathcal{A}$ with $p \leq x$. We will see that $\mathcal{A}$ has natural density zero; what is more interesting is to find explicit bounds for $|\mathcal{A}(x)|$. Crude heuristics suggest that there is a constant $C > 0$, depending on E, such that $|\mathcal{A}(x)| \sim Cx^{3/4}/\log x$ as $x \to \infty$. Proving anything like this is exceedingly difficult; we will focus on finding upper bounds for $|\mathcal{A}(x)|$.

The basic idea is to study the integers $a_p(E)$ modulo several small primes ℓ and then combine this local information to find an explicit upper bound for $|\mathcal{A}(x)|$. To understand the distribution of the $a_p(E)$ modulo ℓ, it is advantageous to express everything in terms of Galois representations. For each prime ℓ, let $E[\ell]$ be the group of ℓ-torsion points in $E(\overline{\mathbb{Q}})$. The absolute Galois group of $\mathbb{Q}$, $\mathcal{G}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, acts on the group $E[\ell]$ which gives a representation

$$\rho_{E,\ell} \colon \mathcal{G}_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

From Serre (Theorem 3.5 with $g = 1$), we know that there is a positive integer B such that

$$(1.1) \qquad \Big(\prod_{\ell \nmid B} \rho_{E,\ell}\Big)(\mathcal{G}_{\mathbb{Q}}) = \prod_{\ell \nmid B} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Fix a prime $\ell \nmid B$ and take any prime $p \notin S_E \cup \{\ell\}$. The Galois representation $\rho_{E,\ell}$ is unramified at p, so we obtain a well-defined conjugacy class $\rho_{E,\ell}(\mathrm{Frob}_p)$ of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. The connection with the integer $a_p(E)$ is the congruence $\mathrm{tr}(\rho_\ell(\mathrm{Frob}_p)) \equiv a_p(E) \bmod \ell$. Now take any prime $p \in \mathcal{A}(x)$ with $p \neq \ell$. Since $a_p(E)$ is a square, the trace of the Frobenius conjugacy class $\rho_{E,\ell}(\mathrm{Frob}_p)$ is a square in $\mathbb{Z}/\ell\mathbb{Z}$. Therefore,

$$\rho_{E,\ell}(\mathrm{Frob}_p) \subseteq C_\ell := \{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(A) \text{ is a square in } \mathbb{Z}/\ell\mathbb{Z}\}.$$

One readily checks that

$$(1.2) \qquad |C_\ell|/|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})| = 1/2 + O(1/\ell).$$

Let us now describe our example in a sieve theoretic fashion. Let $Q = Q(x)$ be a positive function such that $Q(x) \ll \sqrt{x}$; we will make a specific choice later. Let $\Lambda(Q)$ be the set of primes $\ell \nmid B$ with $\ell \leq Q$. We now sieve the set $\Sigma_{\mathbb{Q}}(x) - S_E$ by the primes $\ell \in \Lambda(Q)$. More precisely, for each $\ell \in \Lambda(Q)$ we remove those primes p for which $\mathrm{tr}(\rho_\ell(\mathrm{Frob}_p))$ is a *non-square* in $\mathbb{Z}/\ell\mathbb{Z}$. We are then left with the set

$$\mathscr{S}(x) = \{p \in \Sigma_{\mathbb{Q}}(x) - S_E : p = \ell \ \text{ or } \ \rho_\ell(\mathrm{Frob}_p)) \subseteq C_\ell \text{ for all } \ell \in \Lambda(Q)\}.$$

The set $\mathscr{S}(x)$ contains $\mathcal{A}(x)$, so it suffices to consider upper bounds for $|\mathscr{S}(x)|$.

Intuitively, the Chebotarev density theorem and (1.2) tell us that sieving $\Sigma_{\mathbb{Q}}(x) - S_E$ by a prime $\ell \in \Lambda(Q)$ will remove roughly half the elements, while (1.1) shows that our sieving conditions (indexed by the primes $\ell \in \Lambda(Q)$) are independent of each other. Let Q be a constant function. The Chebotarev density theorem gives us

$$\limsup_{x \to \infty} \frac{|\mathscr{S}(x)|}{x/\log x} \leq \prod_{\ell \in \Lambda(Q)} \frac{|C_\ell|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} \leq \prod_{\ell \in \Lambda(Q)} \left(\frac{1}{2} + O\left(\frac{1}{\ell}\right)\right).$$

Since this holds for every constant Q, we deduce that the $\mathcal{A}$ has natural density 0.

In the same manner, we can apply effective versions of the Chebotarev density theorem (as in Appendix A) to obtain explicit upper bounds for $|\mathcal{A}(x)|$. However, the resulting bounds will be weaker that those coming from the sieve theoretic methods discussed in this paper. In particular, assuming the Generalized Riemann Hypothesis (GRH), they will not be strong enough to prove that there is a value $\delta > 0$ for which $|\mathcal{A}(x)| \ll x^{1-\delta}$. This direct approach requires equidistribution of the conjugacy classes $\{(\prod_{\ell \in \Lambda(Q)} \rho_\ell)(\mathrm{Frob}_p)\}_p$ in the conjugacy classes of $\prod_{\ell \in \Lambda(Q)} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, with respect to the measure induces by Haar measure. The prime number theorem shows that the order of this group grows quickly as a function of Q,

$$(1.3) \qquad \left| \prod_{\ell \in \Lambda(Q)} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \right| = e^{4Q + o(Q)}.$$

So in order for the Frobenius elements $\{(\prod_{\ell \in \Lambda(Q)} \rho_\ell)(\mathrm{Frob}_p)\}_{p \leq x}$ to be well equidistributed, we need the function $Q(x)$ to grow quite slowly as a function of x.

Let us now discuss what the large sieve method will give. (We will be applying the large sieve as in Theorem 3.3. The details are similar to those given in §4 for our application to a conjecture of Koblitz.) The advantage over the direct approach just given is that it allows one to limit the size of the groups considered. Let $\mathcal{Z}(Q)$ be the set of finite subsets $D \subseteq \Lambda(Q)$ for which $\prod_{\ell \in D} \ell \leq Q$, and define

$$L(Q) = \sum_{D \in \mathcal{Z}(Q)} \prod_{\ell \in D} \frac{1 - |C_\ell|/|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}{|C_\ell|/|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}.$$

Using (1.2) one shows that $L(Q) \gg Q$. Assuming GRH, our large sieve will give the bound

$$|\mathcal{S}(x)| \ll (x/\log x + Q^{11} x^{1/2} \log x)/L(Q) \ll (x/\log x + Q^{11} x^{1/2} \log x)/Q.$$

Setting $Q(x) = x^{1/22}/(\log x)^{2/11}$ (this choice makes the two terms in the numerator of our bound equal), we have $|\mathcal{A}(x)| \leq |\mathcal{S}(x)| \ll \frac{x^{21/22}}{(\log x)^{9/11}}$. Unconditionally, with $Q(x) \approx (\log x/(\log\log x)^2)^{1/24}$, our large sieve will give

$$|\mathcal{A}(x)| \ll (x/\log x)/L(Q) \ll x(\log\log x)^{1/12}/(\log x)^{25/24}.$$

An examination of the proof of the large sieve shows that, for our example, we use equidistribution results only for the groups $\prod_{\ell \in D \cup D'} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with $D, D' \in \mathcal{Z}(Q)$. For $D, D' \in \mathcal{Z}(Q)$,

$$\left| \prod_{\ell \in D \cup D'} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \right| \leq \prod_{\ell \in D \cup D'} \ell^4 \leq Q^8.$$

Thus to give a bound for $|\mathcal{A}(x)|$ using the primes $\ell \in \Lambda(Q)$, the large sieve uses equidistribution for groups of size at most Q^8; this should be contrasted with (1.3).

1.6. **Notation.** For each field k, let $\bar{k}$ be an algebraic closure of k and let $\mathcal{G}_k := \mathrm{Gal}(\bar{k}/k)$ be the absolute Galois group of k.

Let L be a Galois extension of a number field k. For each $\mathfrak{p} \in \Sigma_k$ that is unramified in L, let $\mathrm{Frob}_\mathfrak{p}$ be the Frobenius conjugacy class of $\mathfrak{p}$ in $\mathrm{Gal}(L/k)$ (though the notation does not indicate it, the extension L will always be clear from context).

Suppose that f and g are complex valued functions of a real variable x. By $f \ll g$ (or $g \gg f$), we shall mean that there are positive constants C_1 and C_2 such that for all $x \geq C_1$, $|f(x)| \leq C_2 |g(x)|$. The dependence of the implied constants will not always be given but will be made precise in the statement of each of the main theorems. We shall use $O(f)$ to denote an unspecified function g with $g \ll f$. We shall write $f = o(g)$ if g is nonzero for sufficiently large x and $f(x)/g(x) \to 0$ as $x \to \infty$.

For $x \geq 2$, define the logarithmic integral $\operatorname{Li} x = \int_2^x (\log t)^{-1} dt$. The function $\operatorname{Li} x$ is useful when counting primes; it satisfies $\operatorname{Li} x = (1 + o(1)) x / \log x$ as $x \to \infty$.

For a finite group G, the set of conjugacy classes of G will be denoted by $G^\sharp$. We denote by $\operatorname{Irr}(G)$ the set of characters of G which come from irreducible linear representations of G over $\mathbb{C}$. Let $(\ ,\ )$ be the inner product on the the space of complex-valued class functions of G for which $\operatorname{Irr}(G)$ is an orthonormal basis. For the basic notions of representation theory see [Ser77].

Finally, ℓ and p will denote rational primes.

2. A GENERAL LARGE SIEVE

2.1. **Setup and statement.** Let X and Λ be finite sets. We will sieve subsets of X via conditions indexed by Λ. For each $\lambda \in \Lambda$, fix a finite group G_λ and a map $\rho_\lambda \colon X \to G_\lambda^\sharp$. Let μ_λ be the probability measure on $G_\lambda^\sharp$ induced by the counting (Haar) measure on G_λ. More concretely, we have $\mu_\lambda(U) = |G_\lambda|^{-1} \sum_{C \in U} |C|$ for every subset $U \subseteq G_\lambda^\sharp$.

Consider a set $\mathscr{S} \subseteq X$. The goal of our sieve is to find an upper bound for $|\mathscr{S}|$ in terms of the values $\mu_\lambda(\rho_\lambda(\mathscr{S}))$.

We now introduce some more notation. For each $D \subseteq \Lambda$, define the group $G_D = \prod_{\lambda \in D} G_\lambda$. For a subset $E \subseteq D$, composition with the projection $G_D \to G_E$ induces an injective map $\operatorname{Irr}(G_E) \hookrightarrow \operatorname{Irr}(G_D)$. We say that a character $\chi \in \operatorname{Irr}(G_D)$ is *imprimitive* if it comes from a character in $\operatorname{Irr}(G_E)$ for some proper subset E of D; otherwise we say that χ is *primitive*. Let $\operatorname{Prim}(G_D)$ denote the set of primitive characters in $\operatorname{Irr}(G_D)$. Define $\rho_D := (\prod_{\lambda \in D} \rho_\lambda) \colon X \to G_D^\sharp$. Finally, let $\mathcal{P}(\Lambda)$ be the set of all subsets of Λ.

Theorem 2.1 (Large sieve)**.** *Fix notation as above, and let $\mathcal{Z}$ be a subset of $\mathcal{P}(\Lambda)$. Let $\Delta(X, \rho, \mathcal{Z}) \geq 0$ be the least real number for which the inequality*

$$(2.1) \qquad \sum_{D \in \mathcal{Z}} \sum_{\chi \in \operatorname{Prim}(G_D)} \left| \sum_{v \in X} a_v \chi(\rho_D(v)) \right|^2 \leq \Delta(X, \rho, \mathcal{Z}) \sum_{v \in X} |a_v|^2$$

holds for every sequence $(a_v)_{v \in X}$ of complex numbers.

Let $\mathscr{S}$ be a subset of X. For each $\lambda \in \Lambda$, fix a real number $0 < \delta_\lambda \leq 1$ such that

$$(2.2) \qquad \mu_\lambda(\rho_\lambda(\mathscr{S})) \leq \delta_\lambda.$$

Define

$$L(\mathcal{Z}) = \sum_{D \in \mathcal{Z}} \prod_{\lambda \in D} \frac{1 - \delta_\lambda}{\delta_\lambda}.$$

Then

$$L(\mathcal{Z}) |\mathscr{S}| \leq \Delta(X, \rho, \mathcal{Z}).$$

Remark 2.2.

(i) In classical versions of the large sieve, the groups G_λ are abelian and the set Λ usually consists of prime numbers. Theorem 2.1 shows that the basic sieve theoretic principle underlying the large sieve can be fruitfully generalized.

(ii) Note that $\Delta(X, \rho, \mathcal{Z})$ does not depend on the set $\mathscr{S}$ and the dependency of $L(\mathcal{Z})$ on $\mathscr{S}$ is only in terms of the δ_λ.

(iii) An inequality of the form (2.1) is called a *large sieve inequality*. The study of such inequalities has been very important for analytic number theory (cf. [IK04, §7]). Quite often in the literature, the term "large sieve" refers to the study of large sieve type inequalities, even when no actual sieving is involved! Proposition 2.3 below gives a very basic upper bound on $\Delta(X, \rho, \mathcal{Z})$. In the abelian case one can often prove stronger large sieve equalities using harmonic analysis.

(iv) Theorem 2.1 can be further generalized but this version will more than suffice for our applications. For example, in the proof of Theorem 2.1 we do not explicitly need the group structure of the groups G_λ. The main fact we need is that the characters $\mathrm{Irr}(G_\lambda)$ form an orthonormal basis for the Hilbert space of class functions on G_λ. We refer to [Kow08] for further studies in this direction.

Proposition 2.3. *With notation as in Theorem 2.1,*

$$\Delta(X, \rho, \mathcal{Z}) \leq \max_{\substack{D' \in \mathcal{Z} \\ \chi' \in \mathrm{Prim}(G_{D'})}} \sum_{D \in \mathcal{Z}} \sum_{\chi \in \mathrm{Prim}(G_D)} \left| \sum_{v \in X} \chi(\rho_D(v)) \overline{\chi'(\rho_{D'}(v))} \right|.$$

A proof of the proposition can be found in §2.4.

Remark 2.4. Thinking of the elements $\{\rho_{D \cup D'}(v)\}_{v \in X}$ as being equidistributed in $G_{D \cup D'}^\sharp$ with respect to the measure $\prod_{\lambda \in D \cup D'} \mu_\lambda$, we would expect the following expression to be small:

$$\sum_{v \in X} \chi(\rho_D(v)) \overline{\chi'(\rho_{D'}(v))} - \begin{cases} |X| & \text{if } \chi = \chi', \\ 0 & \text{otherwise.} \end{cases}$$

The large sieve and Proposition 2.3 then gives an explicit bound of the form

$$|\mathscr{S}| \leq (|X| + E(\mathcal{Z}))/L(\mathcal{Z})$$

where one can think of $E(\mathcal{Z})$ as being an "error term". Taking $\mathcal{Z} = \mathcal{P}(\Lambda)$, we find that $L(\mathcal{Z}) = \prod_{\lambda \in \Lambda}(1 + (1 - \delta_\lambda)/\delta_\lambda) = (\prod_{\lambda \in \Lambda} \delta_\lambda)^{-1}$. Thus the "main term" of our bound is $|X|/L(\mathcal{P}(\Lambda)) = (\prod_{\lambda \in \Lambda} \delta_\lambda)|X|$; i.e., what one would naively expect after sieving X by independent conditions, indexed by $\lambda \in \Lambda$, each with probability δ_λ. Unfortunately, taking $\mathcal{Z} = \mathcal{P}(\Lambda)$ in most applications will not be useful since the "error term" will be too large. The set $\mathcal{Z}$ is called the *sieve support* and should be chosen to optimize or simplify the bounds in a given application.

2.2. **The classical large sieve.** As a simple example, let us show how the large sieve of Theorem 2.1 relates to the familiar case of sieving integers. Fix a natural number N and real numbers M and $Q \geq 2$. Define the sets

$$X = \{n \in \mathbb{Z} : M < n \leq M + N\} \quad \text{and} \quad \Lambda = \{\ell : \ell \text{ prime and } \ell \leq Q\}.$$

For each $\ell \in \Lambda$, let G_ℓ be the group $\mathbb{Z}/\ell\mathbb{Z}$ and let $\rho_\ell \colon X \to G_\ell^\sharp = \mathbb{Z}/\ell\mathbb{Z}$ be reduction modulo ℓ. The set $\mathcal{P}(\Lambda)$ can be identified with the squarefree natural numbers whose prime factors have size at most Q (identify a squarefree natural number with the set of its prime divisors). For each $d \in \mathcal{P}(\Lambda)$, $G_d = \prod_{\ell | d} G_\ell = \mathbb{Z}/d\mathbb{Z}$ and ρ_d is simply reduction modulo d. The irreducible characters of $G_d = \mathbb{Z}/d\mathbb{Z}$ are those of form $x \mapsto e^{2\pi i \cdot ax/d}$ for $a \in \mathbb{Z}/d\mathbb{Z}$. The set $\mathrm{Prim}(G_d)$ consists of those characters with $a \in (\mathbb{Z}/d\mathbb{Z})^\times$.

The classical choice for $\mathcal{Z}$ is the set $\{d \in \mathcal{P}(\Lambda) : d \leq Q\}$; the squarefree natural numbers less than or equal to Q. The following lemma shows that in the above setting, $\Delta(X, \rho, \mathcal{Z}) \leq N + Q^2$; it is a consequence of [Bom74, Théorème 4].

Lemma 2.5. *For any sequence of complex numbers $(a_n)_{n \in X}$,*

$$\sum_{d \leq Q} \sum_{a \in (\mathbb{Z}/d\mathbb{Z})^\times} \left| \sum_{n \in X} a_n e^{2\pi i \cdot an/d} \right| \leq (N + Q^2) \sum_{n \in X} |a_n|^2.$$

In the present case, Theorem 2.1 specializes to the following familiar version of the large sieve.

Theorem 2.6. *Let $\mathscr{S}$ be a set of integers contained in an interval of length $N \geq 1$. Let $Q \geq 2$ be a real number. For each prime $\ell \leq Q$, fix a number $0 < \delta_\ell \leq 1$ such that $|\{n \bmod \ell : n \in \mathscr{S}\}| \leq \delta_\ell \ell$. Then*

$$|\mathscr{S}| \leq (N + Q^2) \Big(\sum_{d \leq Q \text{ squarefree}} \prod_{\ell | d} \frac{1 - \delta_\ell}{\delta_\ell} \Big)^{-1}.$$

2.3. **Proof of Theorem 2.1.**

Lemma 2.7. *For any $D \subseteq \Lambda$, we have*

$$\Big(\prod_{\lambda \in D} \frac{1 - \delta_\lambda}{\delta_\lambda} \Big) \Big| \sum_{v \in X} a_v \Big|^2 \leq \sum_{\chi \in \mathrm{Prim}(G_D)} \Big| \sum_{v \in X} a_v \chi(\rho_D(v)) \Big|^2$$

where $(a_v)_{v \in X}$ is any sequence of complex numbers such that $a_v = 0$ for all $v \in X - \mathscr{S}$.

Proof. We proceed by induction on the cardinality of the set D.
• If $|D| = 0$, then $D = \emptyset$ and the lemma is trivial. Note that $\mathrm{Prim}(G_\emptyset) = \{1\}$.
• If $|D| = 1$, then $D = \{\lambda\}$ for some $\lambda \in \Lambda$.
We first use the Cauchy-Schwarz inequality and our assumption that $a_v = 0$ for $v \notin \mathscr{S}$.

$$\Big| \sum_{v \in X} a_v \Big|^2 = \Big| \sum_{C \in \rho_\lambda(\mathscr{S})} \sum_{\substack{v \in X \\ \rho_\lambda(v) = C}} a_v \Big|^2 \leq \Big(\sum_{C \in \rho_\lambda(\mathscr{S})} |C| \Big) \sum_{C \in \rho_\lambda(\mathscr{S})} \frac{1}{|C|} \Big| \sum_{\substack{v \in X \\ \rho_\lambda(v) = C}} a_v \Big|^2$$

From (2.2) we have $\sum_{C \in \rho_\lambda(\mathscr{S})} |C| = \mu_\lambda(\rho_\lambda(\mathscr{S}))|G_\lambda| \leq \delta_\lambda |G_\lambda|$, so

$$\Big| \sum_{v \in X} a_v \Big|^2 \leq \delta_\lambda |G_\lambda| \sum_{C \in G_\lambda^\sharp} \frac{1}{|C|} \Big| \sum_{\substack{v \in X \\ \rho_\lambda(v) = C}} a_v \Big|^2.$$

The characteristic function of a conjugacy class $C \in G_\lambda^\sharp$ in G_λ has Fourier expansion

$$\sum_{\chi \in \mathrm{Irr}(G_\lambda)} \Big(\frac{1}{|G_\lambda|} \sum_{g \in C} \overline{\chi(g)} \Big) \chi = \sum_{\chi \in \mathrm{Irr}(G_\lambda)} \frac{|C|}{|G_\lambda|} \overline{\chi(C)} \cdot \chi.$$

We now substitute this into our previous inequality and expand.

$$\delta_\lambda^{-1}\Big|\sum_{v\in X} a_v\Big|^2 \le |G_\lambda|\sum_{C\in G_\lambda^\sharp}\frac{1}{|C|}\Big|\sum_{\substack{v\in X\\ \rho_\lambda(v)=C}} a_v\Big|^2$$

$$= |G_\lambda|\sum_{C\in G_\lambda^\sharp}\frac{1}{|C|}\Big|\sum_{v\in X}\Big(\sum_{\chi\in\mathrm{Irr}(G_\lambda)}\frac{|C|}{|G_\lambda|}\overline{\chi(C)}\cdot\chi(\rho_\lambda(v))\Big)a_v\Big|^2$$

$$= |G_\lambda|\sum_{C\in G_\lambda^\sharp}\frac{1}{|C|}\sum_{v,v'\in X}\sum_{\chi,\chi'\in\mathrm{Irr}(G_\lambda)}\frac{|C|^2}{|G_\lambda|^2}\overline{\chi(C)}\chi'(C)\chi(\rho_\lambda(v))\overline{\chi'(\rho_\lambda(v'))}a_v\overline{a_{v'}}$$

$$= \sum_{\chi,\chi'\in\mathrm{Irr}(G_\lambda)}\Big(\frac{1}{|G_\lambda|}\sum_{C\in G_\lambda^\sharp}|C|\overline{\chi(C)}\chi'(C)\Big)\sum_{v\in X}a_v\chi(\rho_\lambda(v))\overline{\sum_{v'\in X}a_{v'}\chi'(\rho_\lambda(v'))}$$

$$= \sum_{\chi,\chi'\in\mathrm{Irr}(G_\lambda)}(\chi,\chi')\sum_{v\in X}a_v\chi(\rho_\lambda(v))\overline{\sum_{v'\in X}a_{v'}\chi'(\rho_\lambda(v'))}$$

Since the irreducible characters of G_λ are orthonormal,

$$\delta_\lambda^{-1}\Big|\sum_{v\in X}a_v\Big|^2 \le \sum_{\chi\in\mathrm{Irr}(G_\lambda)}\Big|\sum_{v\in X}a_v\chi(\rho_\lambda(v))\Big|^2 = \sum_{\chi\in\mathrm{Irr}(G_\lambda)-\{1\}}\Big|\sum_{v\in X}a_v\chi(\rho_\lambda(v))\Big|^2 + \Big|\sum_{v\in X}a_v\Big|^2.$$

The lemma for $D = \{\lambda\}$ follows by noting that $\mathrm{Prim}(G_\lambda) = \mathrm{Irr}(G_\lambda) - \{1\}$ and collecting both sides; i.e.,

$$\frac{1-\delta_\lambda}{\delta_\lambda}\Big|\sum_{v\in X}a_v\Big|^2 \le \sum_{\chi\in\mathrm{Prim}(G_\lambda)}\Big|\sum_{v\in X}a_v\chi(\rho_\lambda(v))\Big|^2.$$

• Suppose that $|D| \ge 2$. Then $D = E \cup E'$, where E and E' are disjoint proper subsets of D. We have a bijection

$$\mathrm{Irr}(G_E)\times\mathrm{Irr}(G_{E'}) \leftrightarrow \mathrm{Irr}(G_D),\ (\chi,\chi')\mapsto \chi\chi',$$

where $(\chi\chi')(g,g') = \chi(g)\chi(g')$ for $(g,g')\in G_E\times G_{E'} = G_D$. This also induces a bijection between $\mathrm{Prim}(G_E)\times\mathrm{Prim}(G_{E'})$ and $\mathrm{Prim}(G_D)$. Using the inductive hypothesis for E and E', we have:

$$\sum_{\chi\in\mathrm{Prim}(G_D)}\Big|\sum_{v\in X}a_v\chi(\rho_D(v))\Big|^2 = \sum_{\alpha\in\mathrm{Prim}(G_E)}\sum_{\beta\in\mathrm{Prim}(G_{E'})}\Big|\sum_{v\in X}a_v\alpha(\rho_E(v))\beta(\rho_{E'}(v))\Big|^2$$

$$\ge \Big(\prod_{\lambda\in E'}\frac{1-\delta_\lambda}{\delta_\lambda}\Big)\sum_{\alpha\in\mathrm{Prim}(G_E)}\Big|\sum_{v\in X}a_v\alpha(\rho_E(v))\Big|^2$$

$$\ge \Big(\prod_{\lambda\in E'}\frac{1-\delta_\lambda}{\delta_\lambda}\Big)\Big(\prod_{\lambda\in E}\frac{1-\delta_\lambda}{\delta_\lambda}\Big)\Big|\sum_{v\in X}a_v\Big|^2 = \Big(\prod_{\lambda\in D}\frac{1-\delta_\lambda}{\delta_\lambda}\Big)\Big|\sum_{v\in X}a_v\Big|^2 \quad \square$$

We now complete the proof of Theorem 2.1. Let $(a_v)_{v\in X}$ be a sequence of complex numbers with $a_v = 0$ for $v \notin \mathscr{S}$. Using Lemma 2.7 and summing over all $D \in \mathcal{Z}$ we obtain

$$\Big(\sum_{D\in\mathcal{Z}}\prod_{\lambda\in D}\frac{1-\delta_\lambda}{\delta_\lambda}\Big)\Big|\sum_{v\in X}a_v\Big|^2 \le \sum_{D\in\mathcal{Z}}\sum_{\chi\in\mathrm{Prim}(G_D)}\Big|\sum_{v\in X}a_v\chi(\rho_D(v))\Big|^2.$$

The large sieve inequality (2.1) then gives

(2.3)
$$\Big(\sum_{D\in\mathcal{Z}}\prod_{\lambda\in D}\frac{1-\delta_\lambda}{\delta_\lambda}\Big)\Big|\sum_{v\in X}a_v\Big|^2 \le \Delta(X,\rho,\mathcal{Z})\sum_{v\in X}|a_v|^2.$$

11

In the special case where $a_v = 1$ for $v \in \mathscr{S}$, we have

$$\Big(\sum_{D \in \mathcal{Z}} \prod_{\lambda \in D} \frac{1 - \delta_\lambda}{\delta_\lambda} \Big) |\mathscr{S}|^2 \leq \Delta(X, \rho, \mathcal{Z}) |\mathscr{S}|.$$

The theorem follows by cancelling $|\mathscr{S}|$ from both sides (the theorem is trivial if $|\mathscr{S}| = 0$).

Remark 2.8. Equation (2.3) can be useful in practice because it allows one to work with *smoothed sums*. We will not use this in the present paper.

2.4. **Duality principle.**

Lemma 2.9 (Duality principle)**.** *Let I and J be finite sets and let $\{c_{i,j}\}_{i \in I, j \in J}$ be a sequence of complex numbers. Then the following assertions concerning a real number Δ are equivalent:*

(i) *For any sequence $\{x_i\}_{i \in I}$ of complex numbers,*

$$\sum_{j \in J} \Big| \sum_{i \in I} c_{i,j} x_i \Big|^2 \leq \Delta \sum_{i \in I} |x_i|^2.$$

(ii) *For any sequence $\{y_j\}_{j \in J}$ of complex numbers,*

$$\sum_{i \in I} \Big| \sum_{j \in J} c_{i,j} y_j \Big|^2 \leq \Delta \sum_{j \in J} |y_j|^2.$$

Proof. This is a special case of [Mon78, Lemma 2]. $\square$

Lemma 2.10. *Let I and J be finite sets and let $\{c_{i,j}\}_{i \in I, j \in J}$ be a sequence of complex numbers. Then for any sequence $\{x_i\}_{i \in I}$ of complex numbers, we have*

$$\sum_{j \in J} \Big| \sum_{i \in I} c_{i,j} x_i \Big|^2 \leq \Big(\max_{j' \in J} \sum_{j \in J} \Big| \sum_{i \in I} c_{i,j} \overline{c_{i,j'}} \Big| \Big) \sum_{i \in I} |x_i|^2.$$

Proof. Take any sequence $\{y_j\}_{j \in J}$ of complex numbers.

$$\sum_{i \in I} \Big| \sum_{j \in J} c_{i,j} y_j \Big|^2 = \sum_{j,j' \in J} \sum_{i \in I} c_{i,j} \overline{c_{i,j'}} y_j \overline{y_{j'}}$$

$$\leq \sum_{j,j' \in J} \Big| \sum_{i \in I} c_{i,j} \overline{c_{i,j'}} \Big| |y_j| |y_{j'}|$$

$$\leq \sum_{j, j'} \Big| \sum_i c_{i,j} \overline{c_{i,j'}} \Big| \frac{|y_j|^2 + |y_{j'}|^2}{2}$$

$$= \sum_{j, j'} \Big| \sum_i c_{i,j} \overline{c_{i,j'}} \Big| |y_{j'}|^2 \leq \Big(\max_{j'} \sum_j \Big| \sum_i c_{i,j} \overline{c_{i,j'}} \Big| \Big) \sum_{j'} |y_{j'}|^2$$

The lemma is now an immediate consequence of Lemma 2.9. $\square$

Proof of Proposition 2.3. Define $I := X$ and $J := \bigcup_{D \in \mathcal{Z}} \mathrm{Prim}(G_D)$. For a character $\chi \in J$, let D_χ be the element of $\mathcal{Z}$ for which $\chi \in \mathrm{Prim}(G_{D_\chi})$. For $v \in I$ and $\chi \in J$, define $c_{v,\chi} := \chi(\rho_{D_\chi}(v))$. The proposition then follows directly from Lemma 2.10. $\square$

Remark 2.11. Let $C = (c_{i,j})$ be an $m \times n$ matrix with complex entries. For a (not necessarily prime!) value p with $1 \leq p \leq \infty$, we can endow $\mathbb{C}^n$ with the usual p-norm $\|\cdot\|_p$. We then define $\|C\|_p$ to be the supremum of $\|Cy\|_p / \|y\|_p$ over all non-zero $y \in \mathbb{C}^n$. In particular, note that $\|C\|_2$ is the smallest nonnegative number such that

$$\sum_{i=1}^m \Big| \sum_{j=1}^n c_{i,j} y_j \Big|^2 \leq \|C\|_2^2 \sum_{j=1}^n |y_j|^2$$

holds for all $y \in \mathbb{C}^n$. Lemma 2.9 is thus equivalent to $\|C\|_2 = \|C^*\|_2$ where C^* is the conjugate transpose of C. For a complex matrix A, one has $\|A\|_\infty = \max_i \sum_j |a_{i,j}|$. In particular,

$$\|C^*C\|_\infty = \max_{j'} \sum_j \left| \sum_i \overline{c_{i,j'}} c_{i,j} \right|.$$

Lemma 2.10 is thus equivalent to $\|C\|_2^2 \leq \|C^*C\|_\infty$.

3. The large sieve for Galois representations

3.1. Galois representations.

Definition 3.1. Let k be a number field and let H be a (Hausdorff) topological group. A homomorphism $\rho\colon \mathcal{G}_k \to H$ is a *Galois representation* of k if it is continuous (where $\mathcal{G}_k = \mathrm{Gal}(\bar{k}/k)$ is endowed with the Krull topology).

Let $\rho\colon \mathcal{G}_k \to H$ be a Galois representation. The group $\ker(\rho)$ is a closed normal subgroup of $\mathcal{G}_k$ whose fixed field we denote by $k(\rho)$. The representation ρ thus factors through an injective homomorphism $\mathrm{Gal}(k(\rho)/k) \hookrightarrow H$. The representation ρ is *unramified* at a prime $\mathfrak{p} \in \Sigma_k$ if $\mathfrak{p}$ is unramified in the field extension $k(\rho)/k$.

Fix a prime $\mathfrak{p} \in \Sigma_k$ for which ρ is unramified at $\mathfrak{p}$ and take any place $\mathfrak{P}$ of $k(\rho)$ which extends $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified in $k(\rho)$, we have a well-defined element $\rho(\mathrm{Frob}_\mathfrak{P}) \in H$. The conjugacy class of $\rho(\mathrm{Frob}_\mathfrak{P})$ in $\rho(\mathcal{G}_k)$ does not depend on the choice of $\mathfrak{P}$ and we shall denote it by $\rho(\mathrm{Frob}_\mathfrak{p})$.

Definition 3.2. Let $\{\rho_\lambda\colon \mathcal{G}_k \to H_\lambda\}_{\lambda \in \Lambda}$ be a collection of Galois representations. We say that the representations $\{\rho_\lambda\}_{\lambda \in \Lambda}$ are *independent* if

$$\left(\prod_{\lambda \in \Lambda} \rho_\lambda \right)(\mathcal{G}_k) = \prod_{\lambda \in \Lambda} \rho_\lambda(\mathcal{G}_k).$$

An equivalent definition of independence is that the fields $k(\rho_\lambda)$ are linearly disjoint over k.

3.2. Statement of the large sieve.

Theorem 3.3. *Let F be a number field and let Λ be a set of nonzero ideals of $\mathcal{O}_F$ which are pairwise relatively prime. Let k be a number field and suppose we have a collection of independent Galois representations*

$$\left\{ \rho_\lambda\colon \mathcal{G}_k \to H_\lambda \right\}_{\lambda \in \Lambda}.$$

Assume that all the groups $G_\lambda := \rho_\lambda(\mathcal{G}_k)$ are finite and that there exists a real number $r \geq 1$ such that $|G_\lambda| \leq N(\lambda)^r$ for all but finitely many $\lambda \in \Lambda$. Assume further that there is a finite set $S \subseteq \Sigma_k$ such that each ρ_λ is unramified away from $S_\lambda := S \cup \{\mathfrak{p} \in \Sigma_k : \mathfrak{p}|N(\lambda)\}$.

For every $\lambda \in \Lambda$, fix a non-empty subset C_λ of G_λ that is stable under conjugation. Let $Q = Q(x)$ be a positive function of a real variable x such that $Q(x) \ll \sqrt{x}$ and let $\Lambda(Q)$ be the set of $\lambda \in \Lambda$ with $N(\lambda) \leq Q$. Define the set

$$\mathscr{S}(x) := \left\{ \mathfrak{p} \in \Sigma_k(x) : \ \mathfrak{p} \in S_\lambda \ \ or \ \ \rho_\lambda(\mathrm{Frob}_\mathfrak{p}) \subseteq C_\lambda \ for \ all \ \lambda \in \Lambda(Q) \right\}.$$

Choose subsets $\mathcal{Z}(Q) \subseteq \{D : D \subseteq \Lambda, \prod_{\lambda \in D} N(\lambda) \leq Q\}$ and define

$$L(Q) = \sum_{D \in \mathcal{Z}(Q)} \prod_{\lambda \in D} \frac{1 - |C_\lambda|/|G_\lambda|}{|C_\lambda|/|G_\lambda|}.$$

For each $D \subseteq \Lambda$, define $G_D = \prod_{\lambda \in D} G_\lambda$.

(i) *Let $B > 0$ be a real number. If $Q(x) := c\big(\log x/(\log\log x)^2\big)^{1/(6r)}$ for a sufficiently small constant $c > 0$, then*

$$|\mathscr{S}(x)| \leq \Big(\operatorname{Li} x + O(x/(\log x)^{1+B})\Big)L(Q)^{-1}.$$

(ii) *Assuming the Generalized Riemann Hypothesis,*

$$|\mathscr{S}(x)| \leq \Big(\operatorname{Li} x + O\big(\max_{D'\in\mathcal{Z}(Q)}|G_{D'}| \cdot \sum_{D\in\mathcal{Z}(Q)} |G_D^\sharp||G_D| \cdot x^{1/2}\log x\big)\Big)L(Q)^{-1}.$$

(iii) *Assuming Artin's Holomorphy Conjecture for the extensions $k(\rho_{D\cup D'})/k$ for $D, D' \in \mathcal{Z}(Q)$ and assuming the Generalized Riemann Hypothesis,*

$$|\mathscr{S}(x)| \leq \left(\operatorname{Li} x + O\Big(\max_{D'\in\mathcal{Z}(Q),\,\chi'\in\operatorname{Irr}(G_{D'})}\chi'(1) \sum_{D\in\mathcal{Z}(Q),\,\chi\in\operatorname{Irr}(G_D)}\chi(1)\cdot x^{1/2}\log x\Big)\right)L(Q)^{-1}.$$

The implicit constants depend on k, the representations $\{\rho_\lambda\}_{\lambda\in\Lambda}$ and in part (i) also on r and B.

Remark 3.4.

(i) If $L(Q) = 0$, then one should interpret the theorem as giving the trivial bound $|\mathscr{S}(x)| \leq +\infty$.

(ii) The dependence of the bounds in Theorem 3.3 on the sets C_λ are only in terms of the ratios $|C_\lambda|/|G_\lambda|$. For each $\lambda \in \Lambda$, fix a real number $0 < \delta_\lambda \leq 1$ such that $|C_\lambda|/|G_\lambda| \leq \delta_\lambda$. Then

$$L(Q) \geq \sum_{D\in\mathcal{Z}(Q)}\prod_{\lambda\in D}\frac{1-\delta_\lambda}{\delta_\lambda}.$$

The smaller the values of δ_λ are, the stronger our bound on $|\mathscr{S}(x)|$ is. The "large" in the large sieve refers to the fact that one may take δ_λ to be relatively small (at least smaller than earlier sieve methods); i.e., a *large* number of elements G_λ are not hit by the conjugacy classes $\rho_\lambda(\operatorname{Frob}_{\mathfrak{p}})$.

The example of §1.5 is typical of a large sieve where we have $\delta_\ell = 1/2 + O(1/\ell)$. In our application to the Koblitz conjecture, we will have $\delta_\ell = (1 - 1/\ell) + O(1/\ell^2)$ which is typical of so-called "small sieves".

(iii) There is flexibility in what the set $\mathcal{Z}(Q)$ can be. The choice $\mathcal{Z}(Q) = \{D : D \subseteq \Lambda, \prod_{\lambda\in D}N(\lambda) \leq Q\}$ is usually appropriate, but as we will see other subtle choices may be useful.

(iv) Suppose that s is a number such that $|G_\lambda^\sharp| \leq N(\lambda)^s$ for all but finitely many $\lambda \in \Lambda$ (one can always take $s = r$). Assuming GRH, the bound in Theorem 3.3(ii) gives the simpler expression $|\mathscr{S}(x)| \leq (\operatorname{Li} x + O(Q^{2r+s+1}x^{1/2}\log x))L(Q)^{-1}$. Choosing $Q(x) = \big(x^{1/2}/(\log x)^2\big)^{1/(2r+s+1)}$, we obtain the bound

$$|\mathscr{S}(x)| \ll \frac{x/\log x}{L\big(x^{1/(4r+2s+2)}/(\log x)^{2/(2r+s+1)}\big)}.$$

(v) In many arithmetic situations (including those considered in this paper) we have $G_\lambda \subseteq \mathbb{G}(\mathcal{O}_F/\lambda)$ where $\mathbb{G}$ is a group scheme of finite type over $\operatorname{Spec}\mathcal{O}_F$. In Theorem 3.3, one can then take r to be any value greater than the dimension of $\mathbb{G}$.

3.3. **Abelian varieties.** We now recall some basic facts concerning Galois representations associated to abelian varieties; these will supply us with interesting examples that satisfy the conditions of Theorem 3.3. In particular, these representations will be needed for our applications.

Let A be an abelian variety of dimension $g \geq 1$ defined over a number field k. For each integer $m \geq 1$, the absolute Galois group of k acts on the m-torsion points $A[m]$ of $A(\bar{k})$ inducing a Galois representation $\rho_{A,m} \colon \mathcal{G}_k \to \operatorname{Aut}(A[m]) \cong \operatorname{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$.

Let S_A be the set of $\mathfrak{p} \in \Sigma_k$ for which A has bad reduction. The representation $\rho_{A,m}$ is unramified outside of $S_A \cup \{\mathfrak{p} \in \Sigma_k : \mathfrak{p}|m\}$. For every prime ideal $\mathfrak{p} \in \Sigma_k - S_A$, there is a unique polynomial $P_{A_\mathfrak{p}}(T) \in \mathbb{Z}[T]$ such that $P_{A_\mathfrak{p}}(T) \equiv \det(TI - \rho_{A,m}(\operatorname{Frob}_\mathfrak{p})) \bmod m$ for all positive m with $\mathfrak{p} \nmid m$. This agrees with the definition of $P_{A_\mathfrak{p}}(T)$ given in §1.4.1.

Now fix a polarization $\phi \colon A \to A^\vee$. Combining this polarization with the Weil pairing gives an alternating bilinear form $e_m \colon A[m] \times A[m] \to \mu_m$. For $x, y \in A[m]$ and $\sigma \in \mathcal{G}_k$, we have

$$e_m(\sigma x, \sigma y) = \sigma(e_m(x, y)) = e_m(x, y)^{\chi_{k,m}(\sigma)}$$

where $\chi_{k,m} \colon \mathcal{G}_k \to (\mathbb{Z}/m\mathbb{Z})^\times$ is the cyclotomic character of k modulo m.

Let $\operatorname{GSp}(A[m], e_m)$ be the group of $C \in \operatorname{Aut}(E[m])$ for which there exists an $\mathrm{m}(C) \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $e_m(Cx, Cy) = e_m(x, y)^{\mathrm{m}(C)}$ for all $x, y \in A[m]$. Our Galois representation thus becomes

$$\rho_{A,m} \colon \mathcal{G}_k \to \operatorname{GSp}(A[m], e_m).$$

If m is relatively prime to the degree of ϕ, then the pairing e_m is non-degenerate. In this case, the isomorphism class of the pair $(A[m], e_m)$ depends only on g and m, and we denote the corresponding abstract group by $\operatorname{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$.

We now give some examples of abelian varieties for which we can describe the image of $\rho_{A,m}$.

Theorem 3.5 (Serre)**.** *Let A be an abelian variety of dimension g defined over a number field k. Suppose that $\operatorname{End}_{\bar{k}}(A) = \mathbb{Z}$ and that g is either 2, 6, or odd. Then $\rho_{A,m}(\mathcal{G}_k)$ is a subgroup of $\operatorname{GSp}(A[m], e_m)$ whose index is bounded independent of m. In particular, there exists a positive integer B such that $\rho_{A,m}(\mathcal{G}_k) \cong \operatorname{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ for all m relatively prime to B.*

Proof. In the case of non-CM elliptic curves (i.e., $g = 1$), this is a well-known result of Serre [Ser72] (we may choose ϕ to be a principal polarization and then $\operatorname{GSp}(A[m], e_m) \cong \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})$).

In the general case, Théorème 3 from the *Résumé des cours de 1985-1986* in [Ser00] implies that there is a B such that $\rho_{A,\ell}$ is surjective for all $\ell \nmid B$. For an overview of the proof, see the letters at the beginning of [Ser00] especially the one to Marie-France Vignéras. The theorem then follows from the group theoretic Lemmas 1 and 2 in Serre's letter to Vignéras. $\qquad\square$

The following describes the image of the Galois representations when A is a product of non-CM elliptic curves that are pairwise non-isogenous.

Theorem 3.6. *Let $E_1, \ldots, E_n$ be elliptic curves without complex multiplication defined over a number field k. Assume that the curves E_i are pairwise non-isogenous over $\bar{k}$. Then there exists a positive integer B such that $\left(\prod_{i=1}^n \rho_{E_i,m} \right)(\mathcal{G}_k) = \left\{ (A_i) \in \operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})^n : \det(A_1) = \cdots = \det(A_n) \right\}$ for all m relatively prime to B.*

Proof. This follows from [Rib75, Theorem 3.5] (from Faltings we know that Ribet's hypothesis is equivalent to the curves E_i being pairwise non-isogenous over $\bar{k}$). $\qquad\square$

Remark 3.7.

  (i) Let A be an abelian variety over a number field k. In contrast to the abelian varieties occurring in Theorems 3.5 and 3.6, there need not exist an integer B for which the Galois representations $\{\rho_{A,\ell} \colon \mathcal{G}_k \to \operatorname{Aut}(A[\ell])\}_{\ell \nmid B}$ are independent. However, there does exists a finite extension K/k such that the representations $\{\rho_{A,m} \colon \mathcal{G}_K \to \operatorname{Aut}(A[m])\}_{m \in \Lambda}$ are independent for any set Λ of relatively prime natural numbers (see Serre's letter to Ribet [Ser00, p56]).

(ii) Conjecturally many other systems of Galois representations will satisfy the conditions of Theorem 3.3. See [Ser94, §2] for a discussion of ℓ-adic representations associated to motives.

3.4. **Proof of Theorem 3.3.** Fix notation as in Theorem 3.3. We first explain how to apply our abstract large sieve (Theorem 2.1). For each finite set $D \subseteq \Lambda$, define the Galois representation

$$\rho_D := \Big(\prod_{\lambda \in D} \rho_\lambda \Big) \colon \mathcal{G}_k \to \prod_{\lambda \in D} H_\lambda.$$

By our ramification assumptions, we find that ρ_D is unramified at all $\mathfrak{p} \in \Sigma_k(x) - S_D$ where $S_D := S \cup \{\mathfrak{p} \in \Sigma_k : \mathfrak{p} \mid \prod_{\lambda \in D} N(\lambda)\} = \bigcup_{\lambda \in D} S_\lambda$. That the representations $\{\rho_\lambda\}_{\lambda \in \Lambda}$ are independent implies that $G_D = \prod_{\lambda \in D} G_\lambda$ is the image of ρ_D and hence ρ_D induces an isomorphism $\mathrm{Gal}(k(\rho_D)/k) \xrightarrow{\sim} G_D$.

Define $X = \Sigma_k(x)$. For each $\lambda \in \Lambda(Q)$, fix a function $\rho_\lambda \colon X \to G_\lambda^\sharp$ such that the following conditions hold:

- $\rho_\lambda(\mathfrak{p}) = \rho_\lambda(\mathrm{Frob}_\mathfrak{p})$ if $\mathfrak{p} \in \Sigma_k(x) - S_\lambda$,
- $\rho_\lambda(\mathfrak{p}) \subseteq C_\lambda$ if $\mathfrak{p} \in \Sigma_k(x) \cap S_\lambda$

(the second condition is imposed simply to match the set-up of our abstract large sieve). It will be clear from context which function ρ_λ we are using. For $D \subseteq \Lambda(Q)$, define the function $\rho_D := \Big(\prod_{\lambda \in D} \rho_\lambda \Big) \colon X \to G_D^\sharp$. We may now define sets of primitive characters $\mathrm{Prim}(G_D)$ just as in §2.1.

For every $\lambda \in \Lambda(Q)$, define μ_λ to be the measure on G_λ as in §2.1. We have $\rho_\lambda(\mathfrak{p}) \subseteq C_\lambda$ for all $\mathfrak{p} \in \mathscr{S}(x)$ and hence $\mu_\lambda(\rho_\lambda(\mathscr{S}(x))) \leq |C_\lambda|/|G_\lambda|$.

We may now apply our abstract large (Theorem 2.1), which gives

(3.1) $$L(Q) \cdot |\mathscr{S}(x)| \leq \Delta(X, \rho, \mathcal{Z}(Q))$$

where $L(Q) = \sum_{D \in \mathcal{Z}(Q)} \prod_{\lambda \in D} \frac{1 - |C_\lambda|/|G_\lambda|}{|C_\lambda|/|G_\lambda|}$. It remains to bound $\Delta(X, \rho, \mathcal{Z}(Q))$. From Proposition 2.3 we have

(3.2) $$\Delta(X, \rho, \mathcal{Z}(Q)) \leq \max_{\substack{D' \in \mathcal{Z}(Q) \\ \chi' \in \mathrm{Prim}(G_{D'})}} \sum_{D \in \mathcal{Z}(Q)} \sum_{\chi \in \mathrm{Prim}(G_D)} \Big| \sum_{\mathfrak{p} \in \Sigma_k(x)} \chi(\rho_D(\mathfrak{p})) \overline{\chi'(\rho_{D'}(\mathfrak{p}))} \Big|,$$

and to bound this quantity we will make use of the character sums worked out in Appendix A.

Lemma 3.8. *With assumptions as above; fix $D, D' \in \mathcal{Z}(Q)$ and characters $\chi \in \mathrm{Irr}(G_D)$, $\chi' \in \mathrm{Irr}(G_{D'})$.*

(i) *Let $B > 0$ be a constant. If $Q(x) := c\big(\log x/(\log \log x)^2\big)^{1/(6r)}$ for a constant $c > 0$ sufficiently small, then*

$$\sum_{\mathfrak{p} \in \Sigma_k(x)} \chi(\rho_D(\mathfrak{p})) \overline{\chi'(\rho_{D'}(\mathfrak{p}))} = \delta_{\chi,\chi'} \, \mathrm{Li}\, x + O\Big(\frac{x}{(\log x)^{1+B}} \Big).$$

(ii) *Assuming GRH,*

$$\sum_{\mathfrak{p} \in \Sigma_k(x)} \chi(\rho_D(\mathfrak{p})) \overline{\chi'(\rho_{D'}(\mathfrak{p}))} = \delta_{\chi,\chi'} \, \mathrm{Li}\, x + O\Big(|G_D||G_{D'}| x^{1/2} \log x \Big).$$

(iii) *Assuming AHC for the extension $k(\rho_{D \cup D'})/k$ and assuming GRH,*

$$\sum_{\mathfrak{p} \in \Sigma_k(x)} \chi(\rho_D(\mathfrak{p})) \overline{\chi'(\rho_{D'}(\mathfrak{p}))} = \delta_{\chi,\chi'} \, \mathrm{Li}\, x + O\Big(\chi(1)\chi'(1) x^{1/2} \log x \Big).$$

16

Proof. To ease notation, define $T := \sum_{\mathfrak{p} \in \Sigma_k(x)} \chi(\rho_D(\mathfrak{p}))\overline{\chi'(\rho_{D'}(\mathfrak{p}))}$ and $L := k(\rho_{D \cup D'})$. We may view χ (resp. χ') as an irreducible character of $G_{D \cup D'}$ by composing with the projection maps from $G_{D \cup D'}$ to G_D (resp. $G_{D'}$). The Galois representation $\rho_{D \cup D'}$ is unramified at all $\mathfrak{p} \notin S_{D \cup D'} :=$ $S \cup \{\mathfrak{p} \in \Sigma_k : \mathfrak{p} | \prod_{\lambda \in D \cup D'} N(\lambda)\}$. In particular, $\rho_D(\mathfrak{p}) = \rho_D(\text{Frob}_{\mathfrak{p}})$ and $\rho_{D'}(\mathfrak{p}) = \rho_{D'}(\text{Frob}_{\mathfrak{p}})$ for all $\mathfrak{p} \in \Sigma_k(x) - S_{D \cup D'}$. Since $D, D' \in \mathcal{Z}(Q)$ and $Q(x) \ll \sqrt{x}$, we have

$$|S_{D \cup D'}| \ll |S| + \sum_{\lambda \in D \cup D'} \log N(\lambda) \leq |S| + \log(\prod_{\lambda \in D} N(\lambda) \cdot \prod_{\lambda \in D'} N(\lambda))$$
$$\leq |S| + \log(Q \cdot Q) \ll \log x.$$

Therefore,

(3.3)
$$T = \sum_{\mathfrak{p} \in \Sigma_k(x), \text{ unramified in } L} (\chi\overline{\chi'})(\rho_{D \cup D'}(\text{Frob}_{\mathfrak{p}})) + O(\chi(1)\chi'(1)|S_{D \cup D'}|)$$
$$= \sum_{\mathfrak{p} \in \Sigma_k(x) \text{ unramified in } L} (\chi\overline{\chi'})(\rho_{D \cup D'}(\text{Frob}_{\mathfrak{p}})) + O(\chi(1)\chi'(1) \log x).$$

Before considering the different cases, we first bound some quantities that will show up in our character sums. For any $D \in \mathcal{Z}(Q)$, we have $|G_D| \ll \prod_{\lambda \in D} N(\lambda)^r \leq Q^r$. Thus

$$[L : k] \leq |G_D||G_{D'}| \ll Q^{2r}.$$

Let $P(L/k)$ be the set of primes p for which there exists a $\mathfrak{p} \in \Sigma_k$ such that $\mathfrak{p}|p$ and $\mathfrak{p}$ is ramified in L. From our ramification assumptions,

$$\prod_{p \in P(L/k)} p \leq \prod_{\lambda \in S_{D \cup D'}} N(\lambda) \ll \prod_{\lambda \in D} N(\lambda) \prod_{\lambda \in D'} N(\lambda) \leq Q^2.$$

Therefore

$$M(L/k) := [L : k]d_k^{1/[k:\mathbb{Q}]} \prod_{p \in P(L/k)} p \ll Q^{2r+2}.$$

In particular, $\log M(L/k) \ll \log x$, since we have assumed that $Q(x) \ll \sqrt{x}$.

(iii) Assume AHC and GRH. Applying Proposition A.4(ii) to (3.3), we have

$$T = (\chi\overline{\chi'}, 1) \text{Li}\, x + O\Big(\chi(1)\chi'(1)[k : \mathbb{Q}]x^{1/2} \log(M(L/k)x)\Big)$$
$$= \delta_{\chi,\chi'} \text{Li}\, x + O\Big(\chi(1)\chi'(1)x^{1/2} \log x\Big).$$

(ii) Assume GRH. Applying Proposition A.4(i) to (3.3), we have

$$T = (\chi\overline{\chi'}, 1) \text{Li}\, x + O\Big(\Big(\sum_{g \in G_{D \cup D'}} |\chi(g)||\chi'(g)|\Big)[k : \mathbb{Q}]x^{1/2} \log(M(L/k)x)\Big)$$
$$= \delta_{\chi,\chi'} \text{Li}\, x + O\Big(\sum_{g \in G_{D \cup D'}} |\chi(g)||\chi'(g)|x^{1/2} \log x\Big).$$

By the Cauchy-Schwartz inequality and the irreducibility of the characters χ and χ',

$$\sum_{g \in G_{D \cup D'}} |\chi(g)||\chi'(g)| \leq \Big(\sum_{g \in G_{D \cup D'}} |\chi(g)|^2\Big)^{1/2}\Big(\sum_{g \in G_{D \cup D'}} |\chi'(g)|^2\Big)^{1/2} = |G_{D \cup D'}|.$$

Therefore,

$$T = \delta_{\chi,\chi'} \text{Li}\, x + O\Big(|G_{D \cup D'}|x^{1/2} \log x\Big) = \delta_{\chi,\chi'} \text{Li}\, x + O\Big(|G_D||G_{D'}|x^{1/2} \log x\Big).$$

(i) By Lemma A.2, $\log d_L \le [L : \mathbb{Q}] \log M(L/k) \ll Q^{2r} \log Q$, and hence $10[L : \mathbb{Q}](\log d_L)^2 \ll Q^{6r}(\log Q)^2$. So for $Q(x) := c\left(\frac{\log x}{(\log \log x)^2}\right)^{\frac{1}{6r}}$, with a sufficiently small constant $c > 0$, we will have $\log x \ge 10[L : \mathbb{Q}](\log d_L)^2$ for x sufficiently large. Applying Proposition A.8 to (3.3), we have

$$T - \delta_{\chi,\chi'} \operatorname{Li} x \ll \chi(1)\chi'(1) \operatorname{Li}(x^{\beta_L}) + \chi(1)\chi'(1)|G^{\sharp}_{D \cup D'}|x \exp\left(-c_1[L : \mathbb{Q}]^{-1/2}(\log x)^{1/2}\right),$$

where the $\chi(1)\chi'(1) \operatorname{Li}(x^{\beta_L})$ term is present only when the exceptional zero β_L exists. The trivial bounds $|G^{\sharp}_{D \cup D'}| \le |G_{D \cup D'}| \ll Q^{2r}$, $\chi(1) \le |G_D|^{1/2} \ll Q^{r/2}$, and $\chi'(1) \le |G_{D'}|^{1/2} \ll Q^{r/2}$ give

$$T - \delta_{\chi,\chi'} \operatorname{Li} x \ll Q^r \operatorname{Li}(x^{\beta_L}) + Q^{3r}x \exp\left(-\frac{c'_1}{[k : \mathbb{Q}]^{1/2}Q^r}(\log x)^{1/2}\right),$$

for some constant $c' > 0$. The second term is easily bounded:

$$Q^{3r}x \exp\left(-\frac{c'_1}{[k : \mathbb{Q}]^{1/2}Q^r}(\log x)^{1/2}\right)$$
$$\le c^{3r}(\log x)^{1/2}x \exp\left(-\frac{c'_1}{c^r[k : \mathbb{Q}]^{1/2}}(\log x)^{1/3}(\log \log x)^{1/3}\right) \ll_B \frac{x}{(\log x)^{1+B}}.$$

Finally, consider the term containing the exceptional zero. We have $Q^r \operatorname{Li}(x^{\beta_L}) \ll x^{\beta_L}$ so it suffices to show that $x^{\beta_L} \ll x/(\log x)^{1+B}$. By Proposition A.5(ii), there is a field F with $k \subseteq F \subseteq L$ such that $[F : k] \le 2$ and $\zeta_F(\beta_L) = 0$. By Proposition A.5(iii),

$$1 - \beta_L \gg \min\left\{([F : \mathbb{Q}]! \log d_F)^{-1}, d_F^{-1/[F:\mathbb{Q}]}\right\}$$
$$\ge \min\left\{((2[k : \mathbb{Q}] - 1)! \log d_F^{1/[F:\mathbb{Q}]})^{-1}, d_F^{-1/[F:\mathbb{Q}]}\right\} \gg d_F^{-1/[F:\mathbb{Q}]}.$$

By Lemma A.2, $d_F^{1/[F:\mathbb{Q}]} \le M(F/k)$. Using $P(F/k) \subseteq P(L/k)$,

$$d_F^{1/[F:\mathbb{Q}]} \ll \prod_{p \in P(L/k)} p \ll Q^2 \ll (\log x)^{1/(3r)},$$

and hence $1 - \beta_L \gg (\log x)^{-1/(3r)}$. Thus for x sufficiently large, $(1 - \beta_L) \log x \ge (1 + B) \log \log x$, or equivalently $x^{\beta_L} \le x/(\log x)^{1+B}$. $\qquad\square$

We now bound $\Delta(X, \rho, \mathcal{Z}(Q))$. Theorem 3.3 will follow by combining these bounds with (3.1). (i) Fix any $B > 1/3$. By (3.2) and Lemma 3.8(i),

$$\Delta(X, \rho, \mathcal{Z}(Q)) \le \max_{\substack{D' \in \mathcal{Z}(Q) \\ \chi' \in \operatorname{Prim}(G_{D'})}} \sum_{D \in \mathcal{Z}(Q)} \sum_{\chi \in \operatorname{Prim}(G_D)} \left|\sum_{\mathfrak{p} \in X} \chi(\rho_D(\mathfrak{p}))\overline{\chi'(\rho_{D'}(\mathfrak{p}))}\right|$$
$$= \max_{\substack{D' \in \mathcal{Z}(Q) \\ \chi' \in \operatorname{Prim}(G_{D'})}} \sum_{D \in \mathcal{Z}(Q)} \sum_{\chi \in \operatorname{Prim}(G_D)} \left(\delta_{\chi,\chi'} \operatorname{Li} x + O\left(\frac{x}{(\log x)^{1+B}}\right)\right)$$
$$= \operatorname{Li} x + O\left(\sum_{D \in \mathcal{Z}(Q)} |\operatorname{Prim}(G_D)| \frac{x}{(\log x)^{1+B}}\right).$$

Now use the bound $\sum_{D \in \mathcal{Z}(Q)} |\operatorname{Prim}(G_D)| \le \sum_{D \in \mathcal{Z}(Q)} |G_D| \ll Q^{r+1} \ll (\log x)^{1/3}$:

$$\Delta(X, \rho, \mathcal{Z}(Q)) \le \operatorname{Li} x + O\left(\frac{x}{(\log x)^{1+(B-1/3)}}\right).$$

(ii) Assume GRH. By (3.2) and Lemma 3.8(ii),

$$\Delta(X,\rho,\mathcal{Z}(Q)) \leq \max_{\substack{D'\in\mathcal{Z}(Q)\\\chi'\in\mathrm{Prim}(G_{D'})}} \sum_{D\in\mathcal{Z}(Q)}\sum_{\chi\in\mathrm{Prim}(G_D)}\left|\sum_{\mathfrak{p}\in X}\chi(\rho_D(\mathfrak{p}))\overline{\chi'(\rho_{D'}(\mathfrak{p}))}\right|$$

$$= \max_{\substack{D'\in\mathcal{Z}(Q)\\\chi'\in\mathrm{Prim}(G_{D'})}} \sum_{D\in\mathcal{Z}(Q)}\sum_{\chi\in\mathrm{Prim}(G_D)}\left(\delta_{\chi,\chi'}\,\mathrm{Li}\,x + O(|G_D||G_{D'}|x^{1/2}\log x)\right)$$

$$= \mathrm{Li}\,x + O\left(\max_{D'\in\mathcal{Z}(Q)}|G_{D'}|\cdot\sum_{D\in\mathcal{Z}(Q)}|\mathrm{Prim}(G_D)||G_D|\cdot x^{1/2}\log x\right),$$

and then use the inequality $|\mathrm{Prim}(G_D)| \leq |\mathrm{Irr}(G_D)| = |G_D^\sharp|$.
(iii) Assume AHC and GRH. By (3.2) and Lemma 3.8(iii),

$$\Delta(X,\rho,\mathcal{Z}(Q)) \leq \max_{\substack{D'\in\mathcal{Z}(Q)\\\chi'\in\mathrm{Prim}(G_{D'})}} \sum_{D\in\mathcal{Z}(Q)}\sum_{\chi\in\mathrm{Prim}(G_D)}\left|\sum_{\mathfrak{p}\in X}\chi(\rho_D(\mathfrak{p}))\overline{\chi'(\rho_{D'}(\mathfrak{p}))}\right|$$

$$= \max_{\substack{D'\in\mathcal{Z}(Q)\\\chi'\in\mathrm{Prim}(G_{D'})}} \sum_{D\in\mathcal{Z}(Q)}\sum_{\chi\in\mathrm{Prim}(G_D)}\left(\delta_{\chi,\chi'}\,\mathrm{Li}\,x + O(\chi(1)\chi'(1)x^{1/2}\log x)\right)$$

$$= \mathrm{Li}\,x + O\left(\max_{\substack{D'\in\mathcal{Z}(Q)\\\chi'\in\mathrm{Irr}(G_{D'})}} \chi'(1)\sum_{D\in\mathcal{Z}(Q),\chi\in\mathrm{Irr}(G_D)}\chi(1)\cdot x^{1/2}\log x\right).$$

4. The Koblitz Conjecture

The purpose of this section is to prove Theorem 1.2. Fix an integer $t \geq 1$. We maintain the notation introduced in §1.2. For each integer $m \geq 1$, let G_m be the image of $\rho_{E,m}\colon \mathcal{G}_k \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and define the set $C_m := \{A \in G_m : \det(I - A) \in t\cdot(\mathbb{Z}/m\mathbb{Z})^\times\}$. The constant $\mathcal{C}_{E,t}$ for Conjecture 1.1, as given in [Zyw11], is

$$\lim_m \frac{|C_m|/|G_m|}{\prod_{\ell\mid m}(1 - 1/\ell)}$$

where the limit runs over positive integers ordered by divisibility. By Theorem 3.5, there exists a positive integer M such that the following conditions hold:

- $(\rho_{E,M} \times \prod_{\ell\nmid M}\rho_{E,\ell})(\mathcal{G}_k) = G_M \times \prod_{\ell\nmid M}\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,
- if ℓ divides t, then $v_\ell(t) < v_\ell(M)$ where v_ℓ is the ℓ-adic valuation.

One can show that

$$\mathcal{C}_{E,t} = \frac{|C_M|/|G_M|}{\prod_{\ell\mid M}\left(1 - \frac{1}{\ell}\right)}\prod_{\ell\nmid M}\frac{|C_\ell|/|G_\ell|}{\left(1 - \frac{1}{\ell}\right)}.$$

Suppose $\mathcal{C}_{E,t} = 0$; equivalently, $C_M = \emptyset$. Take any prime $\mathfrak{p} \in \Sigma_k - S_E$ for which $\mathfrak{p} \nmid M$ and $|E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})|/t$ is an integer and prime. We find that the integer $|E(\mathbb{F}_{\mathfrak{p}})|/t$ modulo M/t is not an invertible element of $\mathbb{Z}/(M/t)\mathbb{Z}$. So $|E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})|$ must be a prime divisor of M, and this can happen for only finitely many $\mathfrak{p}$ since $|E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})| \geq N(\mathfrak{p}) - 2N(\mathfrak{p})^{1/2} + 1$. Therefore, $\mathcal{C}_{E,t} = 0$ implies that $P_{E,t}(x)$ is a bounded function of x.

For the rest of §4, we shall assume that $\mathcal{C}_{E,t} \neq 0$.

4.1. **Sieve setup.** Fix a positive function $Q = Q(x)$ with $Q(x) \ll \sqrt{x}$; we will make a specific choice later. We will bound the cardinality of the set

$$\mathcal{S}(x) := \{\mathfrak{p} \in \Sigma_k - S_E : ((tQ(x))^{1/2} + 1)^2 < N(\mathfrak{p}) \leq x,\ |E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})|/t \text{ is an integer and prime}\}.$$

Observe that $P_{E,t}(x) = |\mathcal{S}(x)| + O(Q(x)) = |\mathcal{S}(x)| + O(\sqrt{x})$, so it suffices to bound $|\mathcal{S}(x)|$.

For each $\mathfrak{p} \in \mathcal{S}(x)$, the Hasse bound gives

$$|E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})|/t \geq (N(\mathfrak{p}) - 2N(\mathfrak{p})^{1/2} + 1)/t = (N(\mathfrak{p})^{1/2} - 1)^2/t > Q(x).$$

So the primality of $|E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})|/t$ implies that

$$(4.1) \qquad\qquad |E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})| \bmod m \in t \cdot (\mathbb{Z}/m\mathbb{Z})^{\times}$$

for $m \leq Q$.

Define the set $\Lambda = \{M\} \cup \{\ell : \ell \nmid M\}$ and let $\Lambda(Q)$ be the set of $m \in \Lambda$ with $m \leq Q$. By our choice of M, the Galois representations $\{\rho_{E,m}\}_{m \in \Lambda}$ are independent. For $m \in \Lambda(Q)$ and $\mathfrak{p} \in \mathcal{S}(x)$, we have $\mathfrak{p}|m$ or $\det(I - \rho_{E,m}(\mathrm{Frob}_{\mathfrak{p}})) \equiv |E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})| \bmod m$ and hence by (4.1), we have $\rho_{E,m}(\mathrm{Frob}_{\mathfrak{p}}) \subseteq C_m$. With our setup matching that of Theorem 3.3, we define

$$\mathscr{S}(x) := \big\{\mathfrak{p} \in \Sigma_k(x) - S_E : \mathfrak{p}|m \ \text{ or } \ \rho_{E,m}(\mathrm{Frob}_{\mathfrak{p}}) \subseteq C_m \text{ for all } m \in \Lambda(Q)\big\}.$$

Note that $\mathcal{S}(x) \subseteq \mathscr{S}(x)$, so it suffices to give upper bounds for $|\mathscr{S}(x)|$. Define

$$\mathcal{Z}(Q) = \{D : D \subseteq \Lambda(Q), \textstyle\prod_{m \in D} m \leq Q\} \quad \text{and} \quad L(Q) = \sum_{D \in \mathcal{Z}(Q)} \prod_{m \in D} \frac{1 - |C_m|/|G_m|}{|C_m|/|G_m|}.$$

For $D \in \mathcal{Z}(Q)$, define $G_D = \prod_{m \in D} G_m$. Before applying the large sieve, we will first carefully consider the asymptotics of $L(Q)$ as a function of Q.

4.2. Asymptotics of $L(Q)$.

Lemma 4.1. *Suppose ℓ is a prime such that $G_\ell = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $\ell \nmid t$. Then*

$$\frac{1 - |C_\ell|/|G_\ell|}{|C_\ell|/|G_\ell|} = \frac{1}{\ell} + \frac{2\ell^2 - \ell - 3}{\ell^4 - 2\ell^3 - \ell^2 + 3\ell}.$$

Proof. In this case, $|C_\ell|$ is the number of matrices $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ that do not have 1 as an eigenvalue; this can be counted directly, for example by using [Lan02, XVIII Table 12.4]. We find that $|C_\ell| = \ell^4 - 2\ell^3 - \ell^2 + 3\ell$ and $|\mathrm{GL}_2(\mathbb{F}_\ell)| = \ell(\ell-1)^2(\ell+1)$. The lemma is now a direct computation. $\qquad\square$

We introduce the Dirichlet series

$$h(s) := \prod_{m \in \Lambda} \left(1 + \frac{1 - |C_m|/|G_m|}{|C_m|/|G_m|} m^{-s}\right) = \sum_{n=1}^{\infty} b_n/n^s;$$

the significance is that $L(Q) = \sum_{n \leq Q} b_n$. For each prime ℓ, define

$$c_\ell = (2\ell^2 - \ell - 3)/(\ell^4 - 2\ell^3 - \ell^2 + 3\ell).$$

Instead of $h(s)$, it will be more convenient to work with the Dirichlet series

$$(4.2) \qquad g(s) := \prod_\ell \left(1 + (1/\ell + c_\ell)\ell^{-s}\right) = \frac{\prod_{\ell|M}(1 + (\frac{1}{\ell} + c_\ell)\ell^{-s})}{1 + \frac{1 - |C_M|/|G_M|}{|C_M|/|G_M|} M^{-s}} \cdot h(s),$$

where the expression in terms of $h(s)$ follows from Lemma 4.1. The Dirichlet series $g(s)$ converges to a non-vanishing holomorphic function on the domain $\mathrm{Re}(s) > 0$.

Lemma 4.2. *The function $g(s)$ has an analytic continuation to a nonvanishing function on a neighbourhood of $\mathrm{Re}(s) \geq 0$ except for a simple pole at $s = 0$. The residue of $g(s)$ at $s = 0$ is $\prod_\ell \big((1 + (\frac{1}{\ell} + c_\ell))(1 - \frac{1}{\ell})\big)$.*

Proof. For $\operatorname{Re}(s) > 0$,

$$g(s)\zeta(s+1)^{-1} = \prod_\ell \left(\left(1 + \left(\frac{1}{\ell} + c_\ell \right)\ell^{-s} \right)\left(1 - \ell^{-s-1} \right) \right) = \prod_\ell (1 + c_\ell\ell^{-s} - c_\ell\ell^{-2s-1} - \ell^{-2s-2}).$$

Since $c_\ell = 2/\ell^2 + O(1/\ell^3)$, this Euler product converges absolutely and is nonvanishing in a neighbourhood of $\operatorname{Re}(s) \geq 0$. The first statement of the lemma is now immediate. The second statement follows by setting $s = 0$ in the product and noting that $\zeta(s + 1)$ has a simple pole at $s = 0$ with residue 1. $\qquad\square$

By Lemma 4.2 and (4.2), we find that $h(s)$ analytically continues to a neighbourhood of $\operatorname{Re}(s) \geq 0$, except for a simple pole at $s = 0$. The residue of $h(s)$ at $s = 0$ is

$$\left(1 + \frac{1 - |C_M|/|G_M|}{|C_M|/|G_M|} \right) \prod_{\ell \mid M} \left(1 - \frac{1}{\ell} \right) \prod_{\ell \nmid M} \left(\left(1 + \frac{1 - |C_\ell|/|G_\ell|}{|C_\ell|/|G_\ell|} \right) \left(1 - \frac{1}{\ell} \right) \right)$$

$$= \left(\frac{|C_M|/|G_M|}{\prod_{\ell \mid M} \left(1 - \frac{1}{\ell} \right)} \prod_{\ell \nmid M} \frac{|C_\ell|/|G_\ell|}{\left(1 - \frac{1}{\ell} \right)} \right)^{-1} = \mathcal{C}_{E,t}^{-1}.$$

Applying the Wiener-Ikehara theorem [Lan94, XV Theorem 1] to the Dirichlet series $h(s - 1)$, which has a simple pole at $s = 1$, we find that $\sum_{n \leq Q} nb_n = \mathcal{C}_{E,t}^{-1}Q + o(Q)$. By partial summation ([Mur01, Theorem 2.1.1]),

$$(4.3) \qquad\qquad L(Q) = \sum_{n \leq Q} b_n = \mathcal{C}_{E,t}^{-1}\log Q + o(\log Q).$$

4.3. **Proof of Theorem 1.2.** We finally apply the large sieve. First consider the unconditional case. For all $m \in \Lambda$, $|G_m| \leq |\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})| \leq m^4$; so set $r = 4$. By Theorem 3.3(i), with $Q(x) := c \left(\log x/(\log\log x)^2 \right)^{1/24}$ we have $|\mathscr{S}(x)| \leq (x/\log x + o(x/\log x))/L(Q)$. From (4.3),

$$L(Q) = \mathcal{C}_{E,t}^{-1}\log Q + o(\log Q) = (24\mathcal{C}_{E,t})^{-1}\log\log x + o(\log\log x).$$

Therefore,

$$|\mathscr{S}(x)| \leq (24 + o(1))\mathcal{C}_{E,t}\frac{x}{(\log x)(\log\log x)}.$$

Now assume GRH. For $D \in \mathcal{Z}(Q)$, we have $|G_D| \leq \prod_{m \in D} m^4 \leq Q^4$. By Lemma B.3, $|\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})^\sharp| = \ell^2 - 1 \leq \ell^2$ and thus for $D \in \mathcal{Z}(Q)$, $|G_D^\sharp| \ll Q^2$.

$$\sum_{D \in \mathcal{Z}(Q)} |G_D^\sharp||G_D| \ll \sum_{d \leq Q} Q^6 \leq Q^7$$

By Theorem 3.3(ii) and (4.3),

$$|\mathscr{S}(x)| \leq (\operatorname{Li} x + O(Q^{11}x^{1/2}\log x))/L(Q) \leq (\mathcal{C}_{E,t} + o(1))(\operatorname{Li} x + O(Q^{11}x^{1/2}\log x))/\log Q.$$

For a fixed constant $\delta > 0$, define $Q(x) := x^{1/22}/(\log x)^{(2+\delta)/11}$. Therefore

$$|\mathscr{S}(x)| \leq (\operatorname{Li} x + O(x/(\log x)^{1+\delta}))/((22\mathcal{C}_{E,t})^{-1}\log x + o(\log x)) \leq (22 + o(1))\mathcal{C}_{E,t}\frac{x}{(\log x)^2}.$$

5. Elliptic curves and thin sets

The goal of this section is to prove Theorem 1.5.

5.1. Reduction of thin sets.

Definition 5.1. Let Ω be a subset of $\mathbb{Z}^n$. For each prime ℓ, let $\Omega_\ell \subseteq (\mathbb{Z}/\ell\mathbb{Z})^n$ be the reduction of Ω modulo ℓ.

Lemma 5.2. *Let $\Omega \subseteq \mathbb{Z}^n$ be a thin set.*

   (i) *There are thin sets $\Omega_1, \ldots, \Omega_m \subseteq \mathbb{Z}^n$, a set of primes $\Lambda \subseteq \Sigma_\mathbb{Q}$ with positive natural density, and a real number $0 < c < 1$ such that $\Omega = \bigcup_{i=1}^m \Omega_i$, and $|\Omega_{i,\ell}| \le c\ell^n$ for all $1 \le i \le m$ and $\ell \in \Lambda$.*

   (ii) *Suppose Ω is a thin set of Type 1. Then $|\Omega_\ell| \ll \ell^{n-1}$ for all $\ell \in \Sigma_\mathbb{Q}$, where the implied constant depends on Ω and n.*

Proof. Part (i) is a consequence of [Ser97, §13 Theorem 5]. Part (ii) follows from the Lang-Weil bounds [LW54]. $\square$

5.2. Proof of Theorem 1.5.

We are interested in bounding the cardinality of the set $\mathcal{S}(x) := \{\mathfrak{p} \in \Sigma_k(x) : (a_\mathfrak{p}(E_1), \ldots, a_\mathfrak{p}(E_n), N(\mathfrak{p})) \in \Omega\}$. By Lemma 5.2, we need only consider the case where there is a set $\Lambda \subseteq \Sigma_k$ of positive density and a number $0 < c < 1$ such that $|\Omega_\ell| \le c\ell^{n+1}$ for all $\ell \in \Lambda$. Let $\mathbb{G}/\operatorname{Spec}\mathbb{Z}$ be the algebraic subgroup of $(\mathrm{GL}_2)^n$ such that

$$\mathbb{G}(R) = \{(A_1, \ldots, A_n) \in \mathrm{GL}_2(R)^n : \det(A_1) = \cdots = \det(A_n)\}$$

for each commutative ring R. For every integer $m \ge 1$, we have a Galois representation

$$\rho_m := \prod_{i=1}^n \rho_{E_i,m} : \mathcal{G}_k \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})^n.$$

By Theorem 3.6, there is an integer B such that $\rho_m(\mathcal{G}_k) = \mathbb{G}(\mathbb{Z}/m\mathbb{Z})$ for all m relatively prime to B. We may assume that $\ell \nmid B$ for all $\ell \in \Lambda$ and hence the Galois representations $\{\rho_\ell\}_{\ell \in \Lambda}$ are independent. Let S be a finite subset of Σ_k such that the elliptic curves $E_1, \ldots, E_n$ have good reduction outside S. For each prime $\ell \in \Lambda$, define the set

$$C_\ell = \{(A_i) \in \mathbb{G}(\mathbb{Z}/\ell\mathbb{Z}) : (\operatorname{tr}(A_1), \ldots, \operatorname{tr}(A_n), \det(A_1)) \in \Omega_\ell\}.$$

For all $\ell \in \Lambda$ and $\mathfrak{p} \in \mathcal{S}(x)$, either $\mathfrak{p} \in S_\ell := S \cup \{\mathfrak{p} : \mathfrak{p}|\ell\}$ or $\rho_\ell(\mathrm{Frob}_\mathfrak{p}) \subseteq C_\ell$.

Fix a positive function $Q = Q(x)$ with $Q(x) \ll \sqrt{x}$, we will make a specific choice later. With our setup matching that of Theorem 3.3, we define

$$\mathscr{S}(x) = \big\{\mathfrak{p} \in \Sigma_k(x) : \mathfrak{p} \in S_\ell \text{ or } \rho_\ell(\mathrm{Frob}_\mathfrak{p}) \subseteq C_\ell \text{ for all } \ell \in \Lambda(Q)\big\}.$$

Note that $\mathcal{S}(x) \subseteq \mathscr{S}(x)$, so it suffices to bound $|\mathscr{S}(x)|$. Before applying the large sieve, we first calculate some related quantities. The calculations reduce to counting various elements of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, see Lemma B.3. For any $\ell \in \Lambda(Q)$:

$$|\mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})| = (\ell-1)|\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})|^n = \ell^n(\ell-1)^{n+1}(\ell+1)^n$$

$$|C_\ell| = \sum_{(t_1,\ldots,t_n,d)\in\Omega_\ell} \prod_{i=1}^n |\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \operatorname{tr}(A) = t_i, \det(A) = d\}|$$

$$\le \sum_{(t_1,\ldots,t_n,d)\in\Omega_\ell} (\ell(\ell+1))^n = |\Omega_\ell|(\ell(\ell+1))^n \le c\ell^{2n+1}(\ell+1)^n$$

$$|C_\ell|/|\mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})| \le c(1 + (\ell-1)^{-1})^{n+1}$$

After possibly removing finitely many primes from Λ, there is a constant $c' < 1$ such that $|C_\ell|/|\mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})| \le c'$ for all $\ell \in \Lambda$. By Lemma B.1(iii), $|\mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})^\sharp| \le (\ell-1)|\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^\sharp|^n$, and by Lemma B.2 there is an absolute constant $\kappa \ge 1$ such that $|\mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})^\sharp| \le \kappa^n \ell^{n+1} \le (\kappa\ell)^{n+1}$.

Define $\mathcal{Z}(Q) = \{D : D \subseteq \Lambda(Q), \prod_{\ell \in D} \kappa\ell \leq Q\}$ and $L(Q) = \sum_{D \in \mathcal{Z}(Q)} \prod_{\ell \in D}(1 - c')/c'$. Since Λ has positive density, we have

$$L(Q) \geq \sum_{\ell \in \Lambda, \, \ell \leq Q/\kappa} \frac{1 - c'}{c'} \gg \frac{Q}{\log Q}.$$

For $D \in \mathcal{Z}(Q)$, define $G_D = \prod_{\ell \in D} \mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})$.

$$|G_D| = \prod_{\ell \in D} |\mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})| \leq \left(\prod_{\ell \in D} \ell\right)^{3n+1} \leq (Q/\kappa^{|D|})^{3n+1} \leq Q^{3n+1}$$

$$|G_D^\sharp| = \prod_{\ell \in D} |\mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})^\sharp| \leq \left(\prod_{\ell \in D} \kappa\ell\right)^{n+1} \leq Q^{n+1}$$

$$\sum_{D \in \mathcal{Z}(Q)} |G_D^\sharp||G_D| \leq |\mathcal{Z}(Q)|Q^{4n+2} \leq Q^{4n+3}$$

Applying Theorem 3.3(i) with $r = 3n + 1$,

$$L(Q) \gg Q/\log Q \gg \frac{(\log x)^{1/(6r)}}{(\log \log x)^{1+1/(3r)}}$$

and hence

$$|\mathscr{S}(x)| \ll (x/\log x)/L(Q) \ll \frac{x(\log \log x)^{1+1/(9n+3)}}{(\log x)^{1+1/(18n+6)}}.$$

Assuming GRH, by Theorem 3.3(ii)

$$|\mathscr{S}(x)| \ll (x/\log x + Q^{7n+4}x^{1/2}\log x)/(Q/\log Q);$$

choosing $Q(x) = (x^{1/2}/(\log x)^2)^{1/(7n+4)}$ gives $|\mathscr{S}(x)| \ll x^{1-1/(14n+8)}(\log x)^{2/(7n+4)}$.

5.2.1. *Thin sets of Type* 1. Now assume that Ω is thin of type 1; i.e., Ω is not Zariski dense in $\mathbb{A}_{\mathbb{Q}}^{n+1}$. By Lemma 5.2, there is a constant $C > 0$ such that $|\Omega_\ell| \leq C\ell^n$ for all primes ℓ. For each ℓ, define $C_\ell = \{(A_i) \in \mathbb{G}(\mathbb{Z}/\ell\mathbb{Z}) : (\mathrm{tr}(A_1), \ldots, \mathrm{tr}(A_n), \det(A_1)) \in \Omega_\ell\}$. Arguing as before, we find the following bounds.

$$|C_\ell| = \sum_{(t_1,\ldots,t_n,d) \in \Omega_\ell} \prod_{i=1}^{n} |\{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{tr}(A) = t_i, \det(A) = d\}|$$

$$\leq \sum_{(t_1,\ldots,t_n,d) \in \Omega_\ell} (\ell(\ell+1))^n = |\Omega_\ell|(\ell(\ell+1))^n \leq C\ell^{2n}(\ell+1)^n$$

By possibly increasing the value of C, we always have $|C_\ell|/|\mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})| \leq C/\ell$. Take any prime $\ell \nmid B$, where B is the constant from Theorem 3.6. Let L_ℓ be the fixed field of $\ker(\rho_\ell)$ in $\bar{k}$; there is an isomorphism

$$\rho_\ell \colon \mathrm{Gal}(L_\ell/k) \xrightarrow{\sim} \mathbb{G}(\mathbb{Z}/\ell\mathbb{Z}),$$

which we will use as an identification. For all $\mathfrak{p} \in \Sigma_k - S$ with $\mathfrak{p} \nmid \ell$, $\rho_\ell(\mathrm{Frob}_\mathfrak{p}) \subseteq C_\ell$. Therefore,

$$|\{\mathfrak{p} \in \Sigma_k(x) : (a_\mathfrak{p}(E_1), \ldots, a_\mathfrak{p}(E_n), N(\mathfrak{p})) \in \Omega\}| \leq \pi_{C_\ell}(x, L_\ell/k) + O(1);$$

see §A.1 for notation. It thus suffices to bound $\pi_{C_\ell}(x, L_\ell/k)$, and this can be done using the effective versions of the Chebotarev density theorem given in Appendix A. We first calculate $M(L_\ell/k)$ (see Definition A.1).

$$M(L_\ell/k) = [L_\ell : k]d_k^{1/[k:\mathbb{Q}]} \prod_{p \in P(L/k)} p \leq \ell^{3n+1}d_k^{1/[k:\mathbb{Q}]} \cdot \ell \prod_{\mathfrak{p} \in S} N(\mathfrak{p}) \ll \ell^{3n+2}$$

23

Assuming GRH (and assuming, say, $\ell \le x$), by Proposition A.3(i),

$$\pi_{C_\ell}(x, L_\ell/k) \le \frac{|C_\ell|}{|\mathbb{G}(\mathbb{Z}/\ell\mathbb{Z})|} \operatorname{Li} x + O(|C_\ell| x^{1/2} \log x) \ll \frac{1}{\ell} \frac{x}{\log x} + \ell^{3n} x^{1/2} \log x.$$

Choose $\ell \nmid B$ such that

$$\left(x^{1/2}/(\log x)^2\right)^{1/(3n+1)} \le \ell \le 2\left(x^{1/2}/(\log x)^2\right)^{1/(3n+1)}$$

(this can be done assuming x is sufficiently large). With this choice of ℓ,

$$\pi_{C_\ell}(x, L_\ell/k) \ll \frac{x^{1-1/(6n+2)}}{(\log x)^{1-2/(3n+1)}}.$$

Now consider the unconditional case. By Proposition A.7, $\pi_{C_\ell}(x, L_\ell/k) \ll \ell^{-1} x/\log x$, assuming that

$$(5.1) \qquad\qquad \log x \ge c_2 (\log d_{L_\ell})(\log\log d_{L_\ell})(\log\log\log 6 d_{L_\ell}),$$

where c_2 is some absolute constant. By Lemma A.2 and the above bound for $M(L_\ell/k)$,

$$\log d_{L_\ell} \le [L_\ell : \mathbb{Q}] \log M(L_\ell/k) \ll \ell^{3n+1} \log \ell,$$

and hence

$$(5.2) \qquad\qquad (\log d_{L_\ell})(\log\log d_{L_\ell})(\log\log\log 6 d_{L_\ell}) \ll \ell^{3n+1} (\log \ell)^2 (\log\log \ell).$$

Let $c > 0$ be a constant which will be chosen sufficiently small, and suppose we have $\ell \nmid B$ with

$$c\left(\frac{\log x}{(\log\log x)^2 (\log\log\log x)}\right)^{1/(3n+1)} \le \ell \le 2c\left(\frac{\log x}{(\log\log x)^2 (\log\log\log x)}\right)^{1/(3n+1)}.$$

For $c > 0$ sufficiently small, the bound (5.2) shows that (5.1) will hold. With such an ℓ,

$$\pi_{C_\ell}(x, L_\ell/k) \ll \frac{1}{\ell} \frac{x}{\log x} \ll \frac{x(\log\log x)^{2/(3n+1)} (\log\log\log x)^{1/(3n+1)}}{(\log x)^{1+1/(3n+1)}}.$$

Such a prime ℓ will exist assuming x is sufficiently large.

Remark 5.3. If we assume GRH and AHC, then for $\ell \le x$, Proposition A.3(ii) gives

$$\pi_{C_\ell}(x, L_\ell/k) \ll \frac{1}{\ell} \frac{x}{\log x} + \ell^{3n/2} x^{1/2} \log x.$$

Choosing $\ell \approx (x^{1/2}/(\log x)^2)^{2/(3n+2)}$ gives the bound

$$|\{\mathfrak{p} \in \Sigma_k(x) : (a_{\mathfrak{p}}(E_1), \ldots, a_{\mathfrak{p}}(E_n), N(\mathfrak{p})) \in \Omega\}| \ll \frac{x^{1-1/(3n+2)}}{(\log x)^{1-4/(3n+2)}}.$$

6. Explicit Chavdarov

The purpose of this section is to prove Theorem 1.12. We keep the notation introduced in §1.4.

6.1. **Group theory of $\mathfrak{S}_n$.** For a positive integer n, let $\mathfrak{S}_n$ be the symmetric group on $\{1, 2, \ldots, n\}$. A *partition* of n is a sequence $\sigma = (\sigma_1, \ldots, \sigma_k)$ of integers such that $n = \sum_i \sigma_i$ and $\sigma_1 \geq \cdots \geq \sigma_k \geq 1$. The *cycle type* of a permutation $\tau \in \mathfrak{S}_n$ is the partition $\sigma = (\sigma_1, \ldots, \sigma_k)$ of n for which τ can be written as a product of disjoint cycles of lengths $\sigma_1, \ldots, \sigma_k$.

Let $f(T) \in \mathbb{Z}[T]$ be a separable polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$ in $\overline{\mathbb{Q}}$. The numbering of the roots induces an injective homomorphism $\mathrm{Gal}(f(T)) \hookrightarrow \mathfrak{S}_n$. This homomorphism, up to an inner automorphism of $\mathfrak{S}_n$, is independent of the choice of numbering.

Definition 6.1. Let $f(T) \in \mathbb{Z}[T]$ be a polynomial of degree n and let $\sigma = (\sigma_1, \ldots, \sigma_k)$ be a partition of n. We say that σ is a *cycle type* of f if f is separable and the image of $\mathrm{Gal}(f(T)) \hookrightarrow \mathfrak{S}_n$ contains a permutation with cycle type σ. An equivalent condition (by the Chebotarev density theorem) is that there exists a prime ℓ such that $f(T) \bmod \ell \in \mathbb{F}_\ell[T]$ factors into distinct irreducibles of degrees $\sigma_1, \ldots, \sigma_k$.

Lemma 6.2. *Let $f(T) \in \mathbb{Z}[T]$ be a polynomial of degree n. Suppose that σ is a cycle type of $f(T)$ for each partition σ of n. Then $\mathrm{Gal}(f(T)) \cong \mathfrak{S}_n$.*

Proof. The cycle type of a permutation in $\mathfrak{S}_n$ induces a bijection between partitions of n and conjugacy classes of $\mathfrak{S}_n$. Our assumption implies that the image of $\mathrm{Gal}(f(T)) \hookrightarrow \mathfrak{S}_n$ meets every conjugacy class of $\mathfrak{S}_n$. A classical lemma of Jordan, says that for each proper subgroup H of a finite group G, there is a conjugacy class $C \in G^\sharp$ such that $H \cap C = \emptyset$. Therefore, $\mathrm{Gal}(f(T)) \cong \mathfrak{S}_n$. $\quad\square$

6.2. **Group theory of W_{2g}.** Fix an integer $g \geq 1$. Recall that W_{2g} is the subgroup of $\mathfrak{S}_{2g}$ which induces an permutation on the set of pairs $\{\{1, 2\}, \{3, 4\}, \ldots, \{2g-1, 2g\}\}$. The action of W_{2g} on these g pairs gives an exact sequence $1 \to H \to W_{2g} \xrightarrow{\phi} \mathfrak{S}_g \to 1$. The group H is generated by the transpositions $(1, 2), \ldots, (2g-1, 2g)$, and hence is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g$. In particular, $|W_{2g}| = 2^g g!$.

Lemma 6.3. *Let G be a subgroup of W_{2g}. If G contains a transposition and $\phi(G) = \mathfrak{S}_g$, then $G = W_{2g}$.*

Proof. From the assumption $\phi(G) = \mathfrak{S}_g$, it suffices to show that $H \subseteq G$. In particular, it suffices to show that G contains every transposition of the form $(2i-1, 2i)$.

By assumption, G contains a transposition. This transposition must be an element of H, and we may assume that it is $(1, 2)$. Since $\phi(G) = \mathfrak{S}_g$, there exists a $\tau \in G$ which switches the pairs $\{1, 2\}$ and $\{2i-1, 2i\}$, and leaves the other pairs fixed. The permutation $\tau(1, 2)\tau^{-1}$ is thus $(2i-1, 2i)$. $\quad\square$

6.3. **Abelian varieties over finite fields.**

Definition 6.4. Let A be an abelian variety of dimension $g \geq 1$ over a finite field $\mathbb{F}_q$. Let $Q_A(T) \in \mathbb{Z}[T]$ be the unique polynomial such that $P_A(T) = T^g Q_A(T + q/T)$. (The existence of $Q_A(T)$ is a direct consequence of the functional equation $P_A(q/T)/(q/T)^g = P_A(T)/T^g$.)

Lemma 6.5. *Let A be an abelian variety of dimension g over $\mathbb{F}_q$. Suppose that $P_A(T)$ has cycle types $(2g)$ and $(2, 1, 1, \ldots, 1)$, and $Q_A(T)$ has cycle type σ for each partition σ of g. Then $\mathrm{Gal}(P_A(T)) \cong W_{2g}$.*

Proof. The polynomial $P_A(T)$ is irreducible since it has cycle type $(2g)$. Let $\pi_1, \ldots, \pi_{2g}$ be the roots of $P_A(T)$ in $\overline{\mathbb{Q}}$, they are non-rational and distinct since $P_A(T)$ is irreducible. We may assume that the π_i are numbered such that the product of any of the pairs $\{\pi_1, \pi_2\}, \ldots, \{\pi_{2g-1}, \pi_{2g}\}$ is q (since $P_A(T)$ is irreducible of degree $2g$, $\pm\sqrt{q}$ can be roots only when $g = 1$, in which case the lemma is trivial). The numbering of the π_i induces an injective homomorphism $\mathrm{Gal}(P_A(T)) \hookrightarrow W_{2g}$; let G be the image of this map. Since $P_A(T)$ has cycle type $(2, 1, 1, \ldots, 1)$, the group $G \subseteq \mathfrak{S}_{2g}$ contains a transposition.

The polynomial $Q_A(T)$ is monic of degree g. Since the value of $T + q/T$ at any element of a pair $\{\pi_{2i-1}, \pi_{2i}\}$ is the same, we find that roots of $Q_A(T)$ correspond with our g pairs of roots of $P_A(T)$. By Lemma 6.2, $\mathrm{Gal}(Q_A(T)) \cong \mathfrak{S}_g$. Thus $\phi(G) = \mathfrak{S}_g$, where ϕ is the map from (**??**). By Lemma 6.3, $\mathrm{Gal}(P_A(T)) \cong G = W_{2g}$ as desired. $\square$

Definition 6.6. Let $P(T) \in \mathbb{Q}[T]$ be a monic polynomial of degree n, and let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be the roots of $P(T)$. For each integer $m > 0$, define $P^{(m)}(T) := \prod_i (T - \alpha_i^m)$ which is a well-defined element of $\mathbb{Q}[T]$.

Let A be an abelian variety over the finite field $\mathbb{F}_q$ with q elements. Then for all $m \geq 1$, $P_A^{(m)}(T) = P_{A \times \mathbb{F}_{q^m}}(T)$. The next lemma gives a useful criterion to test whether $\mathrm{Gal}(P_A^{(m)}(T)) \cong \mathrm{Gal}(P_A(T))$ for all $m \geq 1$.

Lemma 6.7. *Let $P(T) \in \mathbb{Q}[T]$ be an irreducible polynomial of degree n with Galois group G. There is an integer $s = s(n) > 0$, depending only on the degree of $P(T)$, such that if the polynomial $P^{(s)}(T)$ is separable, then the polynomial $P^{(m)}(T) \in \mathbb{Q}[T]$ is irreducible and has Galois group G for all integers $m \geq 1$.*

Proof. This follows from [Cha97, Lemma 5.3]. $\square$

6.4. **Proof of Theorem 1.12.** Fix a positive function $Q = Q(x)$ with $Q \ll \sqrt{x}$ which will be specifically chosen later. Define the set $\Lambda = \{\ell : \ell \nmid B\}$, where B is the constant from Theorem 3.5. Thus the representations $\{\rho_{A,\ell}\}_{\ell \in \Lambda}$ are independent. Let $\Lambda(Q)$ be the set of elements in Λ which are at most Q.

- Let $\mathcal{S}_1(x)$ be the set of $\mathfrak{p} \in \Sigma_k(x) - S_A$ such that $P_{A_\mathfrak{p}}(T)$ does not have cycle type $(2g)$.
- Let $\mathcal{S}_2(x)$ be the set of $\mathfrak{p} \in \Sigma_k(x) - S_A$ such that $P_{A_\mathfrak{p}}(T)$ does not have cycle type $(2, 1, 1 \ldots, 1)$.
- Let $\mathcal{S}_3(x)$ be the set of $\mathfrak{p} \in \Sigma_k(x) - S_A$ such that $P_{A_\mathfrak{p}}^{(s)}(T)$ is not separable, where $s = s(2g)$ is the integer from Lemma 6.7.
- For each partition σ of g, let $\mathcal{S}_\sigma(x)$ be the set of $\mathfrak{p} \in \Sigma_k(x) - S_A$ such that $Q_{A_\mathfrak{p}}(T)$ does not have cycle type σ.

Lemma 6.8. *There is an inclusion $\Pi_A(x) \subseteq \mathcal{S}_1(x) \cup \mathcal{S}_2(x) \cup \mathcal{S}_3(x) \cup \bigcup_\sigma \mathcal{S}_\sigma(x)$, and hence*

$$|\Pi_A(x)| \leq |\mathcal{S}_1(x)| + |\mathcal{S}_2(x)| + |\mathcal{S}_3(x)| + \sum_\sigma |\mathcal{S}_\sigma(x)|.$$

Proof. Take any $\mathfrak{p} \in \Sigma_k(x) - S_A$ with $\mathfrak{p} \notin \mathcal{S}_1(x) \cup \mathcal{S}_2(x) \cup \mathcal{S}_3(x) \cup \bigcup_\sigma \mathcal{S}_\sigma(x)$. Since $\mathfrak{p} \notin \mathcal{S}_1(x) \cup \mathcal{S}_2(x)$, $P_{A_\mathfrak{p}}(T)$ has cycle types $(2g)$ and $(2, 1, 1, \ldots, 1)$. For each partition σ of g, $\mathfrak{p} \notin \mathcal{S}_\sigma(x)$ imples that $Q_{A_\mathfrak{p}}(T)$ has cycle type σ. By Lemma 6.5, $\mathrm{Gal}(P_{A_\mathfrak{p}}(T)) \cong W_{2g}$. Since $\mathfrak{p} \notin \mathcal{S}_3(x)$, we find by Lemma 6.7 that

$$\mathrm{Gal}(P_{A_\mathfrak{p}}^{(m)}(T)) \cong \mathrm{Gal}(P_{A_\mathfrak{p}}(T)) \cong W_{2g}$$

for all $m \geq 1$. Therefore, $\mathfrak{p} \notin \Pi_A(x)$. $\square$

For each prime ℓ, define the following sets:
- Let C_ℓ^1 be the set of $B \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ such that $\det(TI - B) \in \mathbb{F}_\ell[T]$ is reducible.
- Let C_ℓ^2 be the set $B \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ such that $\det(TI - B) \in \mathbb{F}_\ell[T]$ is not the product of an irreducible quadratic and $2g - 2$ distinct linear terms.
- Let $s = s(2g)$ be the integer of Lemma 6.7. Let C_ℓ^3 be the set of $B \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ such that $P^{(s)}(T) \in \mathbb{F}_\ell[T]$ is not separable, where $P(T) = \det(TI - B)$.

- For each partition $\sigma = (\sigma_1, \ldots, \sigma_k)$ of g, let C_ℓ^σ be the set of $B \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ such that $Q(T)$ does not factor into distinct irreducible polynomials of degree $\sigma_1, \ldots, \sigma_k$, where $Q(T) \in \mathbb{F}_\ell[T]$ is the unique polynomial such that $\det(TI - B) = T^g Q(T + \mathrm{m}(B)/T)$.

Lemma 6.9. *There are constants $B' > 0$ and $0 < \delta < 1$, depending only on g, such that for all primes $\ell \geq B'$,*

$$(6.1) \qquad \max_{i=1,2,3} \frac{|C_\ell^i|}{|\mathrm{GSp}_{2g}(\mathbb{F}_\ell)|} \leq \delta \quad \text{and} \quad \max_{\sigma \text{ partition of } g} \frac{|C_\ell^\sigma|}{|\mathrm{GSp}_{2g}(\mathbb{F}_\ell)|} \leq \delta.$$

Proof. These bounds follow from the computations done in [Cha97] (in particular, see Corollary 3.6, Lemma 5.7, Lemma 5.4, and Lemma 5.9). Chavdarov's bounds are done for the $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ cosets of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, our lemma follows by combining these bounds. Also note that the formulation of some of these results looks slightly different in [Cha97] because the characteristic polynomials there are the reverse of ours. $\qquad \square$

We have reduced to the case of bounding the following cardinalities separately: $|\mathcal{S}_1(x)|, |\mathcal{S}_2(x)|, |\mathcal{S}_3(x)|$, and $|\mathcal{S}_\sigma(x)|$ for each partition σ of g. For purely notational reasons we only bound $|\mathcal{S}_1(x)|$; the arguments in the other cases are identical. For any $\ell \in \Lambda(Q)$ and $\mathfrak{p} \in \mathcal{S}_1(x)$, either $\mathfrak{p}|\ell$ or $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \subseteq C_\ell^1$. So $\mathcal{S}_1(x) \subseteq \mathscr{S}_1(x)$, where

$$\mathscr{S}_1(x) := \big\{ \mathfrak{p} \in \Sigma_k(x) - S_A : \mathfrak{p}|\ell \ \text{ or } \ \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \subseteq C_\ell \ \text{for all } \ell \in \Lambda(Q) \big\}.$$

We will now use the large sieve as in Theorem 3.3 to bound $|\mathscr{S}_1(x)|$.

By possibly increasing B, we may assume that (6.1) holds for all $\ell \nmid B$. By Lemma B.2, there is a constant $\kappa \geq 1$ such that $|\mathrm{GSp}_{2g}(\mathbb{F}_\ell)^\sharp| \leq (\kappa\ell)^{g+1}$. Define

$$\mathcal{Z}(Q) = \{D : D \subseteq \Lambda(Q), \ \textstyle\prod_{\ell \in D} \kappa\ell \leq Q\} \quad \text{and} \quad L(Q) = \sum_{D \in \mathcal{Z}(Q)} \prod_{\ell \in D} \frac{1 - \delta}{\delta},$$

where δ is the constant from Lemma 6.9. Note that

$$L(Q) \geq \sum_{\ell \in \Lambda, \ \ell \leq Q/\kappa} \frac{1 - \delta}{\delta} \gg \frac{Q}{\log Q}.$$

For $D \in \mathcal{Z}(Q)$, define $G_D = \prod_{\ell \in D} \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. We shall use Lemma B.2 in the following bounds.

$$|G_D| = \prod_{\ell \in D} |\mathrm{GSp}_{2g}(\mathbb{F}_\ell)| \leq \Big(\prod_{\ell \in D} \ell \Big)^{2g^2 + g + 1} \leq (Q/\kappa^{|D|})^{2g^2 + g + 1} \leq Q^{2g^2 + g + 1}$$

$$|G_D^\sharp| = \prod_{\ell \in D} |\mathrm{GSp}_{2g}(\mathbb{F}_\ell)^\sharp| \leq \Big(\prod_{\ell \in D} \kappa\ell \Big)^{g+1} \leq Q^{g+1}$$

$$\sum_{D \in \mathcal{Z}(Q)} |G_D^\sharp||G_D| \ll |\mathcal{Z}(Q)| Q^{2g^2 + 2g + 2} \ll Q^{2g^2 + 2g + 3}$$

Applying Theorem 3.3(i) with $r = 2g^2 + g + 1$ gives

$$L(Q) \gg Q/\log Q \gg \frac{(\log x)^{1/(6r)}}{(\log \log x)^{1 + 1/(3r)}}$$

and hence

$$|\mathcal{S}_1(x)| \leq |\mathscr{S}_1(x)| \ll (x/\log x)/L(Q) \ll \frac{x(\log \log x)^{1 + 1/(6g^2 + 3g + 3)}}{(\log x)^{1 + 1/(12g^2 + 6g + 6)}}.$$

Assuming GRH, by Theorem 3.3(ii)

$$|\mathscr{S}_1(x)| \ll (x/\log x + Q^{4g^2 + 3g + 4} x^{1/2} \log x)/(Q/\log Q);$$

choosing $Q(x) = (x^{1/2}/(\log x)^2)^{1/(4g^2+3g+4)}$ gives

$$|\mathcal{S}_1(x)| \leq |\mathscr{S}_1(x)| \ll x^{1-1/(8g^2+6g+8)}(\log x)^{2/(4g^2+3g+4)}.$$

Identical bounds will hold for all the $|\mathcal{S}_2(x)|$, $|\mathcal{S}_3(x)|$ and $|\mathcal{S}_\sigma(x)|$. So by Lemma 6.8, we have

$$|\Pi_A(x)| \ll \begin{cases} x(\log\log x)^{1+1/(6g^2+3g+3)}/(\log x)^{1+1/(12g^2+6g+6)} \\[2mm] x^{1-1/(8g^2+6g+8)}(\log x)^{2/(4g^2+3g+4)} \end{cases} \qquad \text{assuming GRH.}$$

Appendix A. Character sums and the Chebotarev density theorem

A.1. **Notation.** Let L/k be a Galois extension of number fields with Galois group G and let C be a subset of G stable under conjugation. Define

$$\pi_C(x, L/k) := |\{\mathfrak{p} \in \Sigma_k(x) : \mathfrak{p} \text{ unramified in } L, \ \text{Frob}_\mathfrak{p} \subseteq C\}|.$$

The *Chebotarev density theorem* says that

$$\pi_C(x, L/k) \sim \frac{|C|}{|G|} \operatorname{Li} x$$

as $x \to \infty$. An effective version would give an explicit bound for $\pi_C(x, L/k) - |C|/|G| \operatorname{Li} x$.

The extension L/k is said to satisfy *Artin's Holomorphy Conjecture* (AHC) if for each $\chi \in \operatorname{Irr}(G) - \{1\}$, the Artin L-series $L(s, \chi)$ has analytic continuation to the whole complex plane. The *Generalized Riemann Hypothesis* (GRH) asserts that for any number field L, the Dedekind zeta function $\zeta_L(s)$ has no zeros with real part $> 1/2$.

Definition A.1. Let L/k be an extension of number fields. Define

$$M(L/k) := [L : k]d_k^{1/[k:\mathbb{Q}]} \prod_{p \in P(L/k)} p$$

where d_k is the absolute discriminant of k and $P(L/k)$ is the set of rational primes p for which there exist a prime $\mathfrak{p} \in \Sigma_k$ such that $\mathfrak{p}|p$ and $\mathfrak{p}$ is ramified in L.

Lemma A.2. *Let L/k be a Galois extension of number fields. Then $\log d_L \leq [L : \mathbb{Q}] \log M(L/k)$.*

Proof. This follows by combining equations (3) and (6) of [Ser81]. $\qquad\square$

A.2. **Conditional versions.**

Proposition A.3. *Let L/k be a Galois extension of number fields with Galois group G and let C be a subset of G stable under conjugation.*

(i) *Assume GRH. Then*

$$\pi_C(x, L/k) = \frac{|C|}{|G|} \operatorname{Li} x + O\Big(|C|x^{1/2}[k : \mathbb{Q}] \log\big(M(L/k)x\big)\Big).$$

(ii) *Assume GRH and assume AHC for the extension L/k. Then*

$$\pi_C(x, L/k) = \frac{|C|}{|G|} \operatorname{Li} x + O\Big(|C|^{1/2}x^{1/2}[k : \mathbb{Q}] \log\big(M(L/k)x\big)\Big).$$

In both cases, the implicit constants are absolute.

Proof. Part (i) is equation (20_R) of [Ser81]. Part (ii) is a consequence of [MMS88, Proposition 3.12]. $\qquad\square$

Proposition A.4. *Let L/k be a Galois extension of number fields with Galois group G and let χ be a character of G.*

(i) *Assume GRH. Then*

$$\sum_{\substack{\mathfrak{p} \in \Sigma_k(x) \\ \mathfrak{p} \text{ unramified in } L}} \chi(\mathrm{Frob}_\mathfrak{p}) = (\chi, 1)\operatorname{Li} x + O\Big(\Big(\sum_{g \in G}|\chi(g)|\Big)[k:\mathbb{Q}]x^{1/2}\log\big(M(L/k)x\big)\Big).$$

(ii) *Assume GRH and assume AHC for the extension L/k. Then*

$$\sum_{\substack{\mathfrak{p} \in \Sigma_k(x) \\ \mathfrak{p} \text{ unramified in } L}} \chi(\mathrm{Frob}_\mathfrak{p}) = (\chi, 1)\operatorname{Li} x + O\Big(\chi(1)[k:\mathbb{Q}]x^{1/2}\log\big(M(L/k)x\big)\Big).$$

In both cases, the implicit constants are absolute.

Proof. Part (i) follows from equation (33_R) of [Ser81] and Lemma A.2. We now consider part (ii). By additivity it suffices to prove the proposition for an irreducible χ. Let $\mathscr{F}_\chi$ be the Artin conductor of χ and define $A_\chi = d_k^{\chi(1)} N_{k/\mathbb{Q}}(\mathscr{F}_\chi)$. See [MMS88, Proposition 3.5] for a sketch that

$$\sum_{\substack{\mathfrak{p} \in \Sigma_k(x) \\ \mathfrak{p} \text{ unramified in } L}} \chi(\mathrm{Frob}_\mathfrak{p}) = (\chi, 1)\operatorname{Li} x + O\Big(x^{1/2}(\log A_\chi + \chi(1)[k:\mathbb{Q}]\log x)\Big)$$
$$+ O\Big(\chi(1)[k:\mathbb{Q}]\log\Big([L:k]d_k^{1/[k:\mathbb{Q}]}\prod_{p \in P(L/k)}p\Big)\Big).$$

By Proposition 2.5 of [MMS88], $\log(N_{k/\mathbb{Q}}(\mathscr{F}_\chi)) \leq 2\chi(1)[k:\mathbb{Q}]\log\Big([L:k]\prod_{p \in P(L/k)}p\Big)$ and hence

$$\log A_\chi \leq 2\chi(1)[k:\mathbb{Q}]\log\Big([L:k]\prod_{p \in P(L/k)}p\Big) + \chi(1)\log d_k$$
$$\leq 2\chi(1)[k:\mathbb{Q}]\log\Big([L:k]d_k^{1/[k:\mathbb{Q}]}\prod_{p \in P(L/k)}p\Big).$$

Combining everything we obtain

$$\sum_{\substack{\mathfrak{p} \in \Sigma_k(x) \\ \mathfrak{p} \text{ unramified in } L}} \chi(\mathrm{Frob}_\mathfrak{p}) = (\chi, 1)\operatorname{Li} x + O\Big(x^{1/2}\chi(1)[k:\mathbb{Q}]\log\Big([L:k]d_k^{1/[k:\mathbb{Q}]}x\prod_{p \in P(L/k)}p\Big)\Big). \quad \square$$

A.3. **Exceptional zeros.**

Proposition A.5.

(i) *Let $L \neq \mathbb{Q}$ be a number field. Then $\zeta_L(s)$ has at most one real zero in the interval $1 - (4\log d_L)^{-1} \leq \sigma < 1$. Such a zero of $\zeta_L(s)$, if it exists, is simple.*

(ii) *Let L/k be a Galois extension of number fields and suppose that $\beta \geq 1/2$ is a real simple zero of $\zeta_L(s)$. Then there is a field F with $k \subseteq F \subseteq L$ such that $[F:k] \leq 2$ and $\zeta_F(\beta) = 0$.*

(iii) *Let $F \neq \mathbb{Q}$ be a number field and suppose β is a real zero of $\zeta_F(s)$. Then*

$$1 - \beta \gg \min\big\{([F:\mathbb{Q}]!\log d_F)^{-1}, d_F^{-1/[F:\mathbb{Q}]}\big\},$$

where the implicit constant is absolute.

Proof. For part (i), see [Sta74, Lemma 3]. Part (ii) is due to Heilbronn, see [Sta74, Theorem 3] for a generalized version. The estimate in part (iii) can be found in the proof of [Sta74, Theorem $1'$]. $\quad \square$

Definition A.6. Let $L \neq \mathbb{Q}$ be a number field. If the simple real zero of $\zeta_L(s)$ described in Proposition A.5(i) exists, then we call it the *exceptional zero* of L and denote it by β_L. Note that $\zeta_\mathbb{Q}(s)$ has no real zeros in the interval $0 \leq \sigma \leq 1$.

A.4. **Unconditional versions.**

Proposition A.7. *Let L/k be a Galois extension of number fields with Galois group G. Let C be a subset of G that is stable under conjugacy and let $\widetilde{C}$ be the set of conjugacy classes of G which are subsets of C.*

   (i) *There is an absolute constant $c_1 > 0$ such that if $\log x \geq 10[L:\mathbb{Q}](\log d_L)^2$, then*

$$\left| \pi_C(x, L/k) - \frac{|C|}{|G|} \operatorname{Li} x \right| \leq \frac{|C|}{|G|} \operatorname{Li}(x^{\beta_L}) + O\left(|\widetilde{C}| x \exp(-c_1[L:\mathbb{Q}]^{-1/2}(\log x)^{1/2}) \right),$$

   where the $\frac{|C|}{|G|} \operatorname{Li}(x^{\beta_L})$ term is present only when the exceptional zero β_L exists.

   (ii) *There is an absolute constant $c_2 > 0$ such that if $\log x \geq c_2 (\log d_L)(\log \log d_L)(\log \log \log 6d_L)$, then*

$$\pi_C(x, L/k) \ll \frac{|C|}{|G|} \frac{x}{\log x}.$$

Proof. Part (i) is a consequence of [LO77, Theorem 1.3]. Part (ii) is stated as in [Ser81, Théorème 3] and is a result of Lagarias, Montgomery, and Odlyzko. $\square$

Proposition A.8. *Let L/k be a Galois extension of number fields with Galois group G and let χ be a character of G. If $\log x \geq 10[L:\mathbb{Q}](\log d_L)^2$, then*

$$\sum_{\substack{\mathfrak{p} \in \Sigma_k(x) \\ \mathfrak{p} \text{ unramified in } L}} \chi(\operatorname{Frob}_\mathfrak{p}) = (\chi, 1) \operatorname{Li} x + O(\chi(1) \operatorname{Li}(x^{\beta_L}))$$
$$+ O\left(\chi(1) |G^\sharp| x \exp(-c_1[L:\mathbb{Q}]^{-1/2}(\log x)^{1/2}) \right)$$

where the $\chi(1) \operatorname{Li}(x^{\beta_L})$ term is present only when the exceptional zero β_L exists, and the constant $c_1 > 0$ and the implicit constants are absolute.

Proof. It suffices to prove the proposition for an irreducible character χ. We first write the character sum in terms of the $\pi_C(x, L/k)$,

$$\sum_{\mathfrak{p} \in \Sigma_k(x),\, \mathfrak{p} \text{ unramified in } L} \chi(\operatorname{Frob}_\mathfrak{p}) = \sum_{C \in G^\sharp} \chi(C) \pi_C(x, L/k).$$

Using $\sum_{C \in G^\sharp} \chi(C)|C|/|G| = (\chi, 1)$ and $\max_{C \in G^\sharp} |\chi(C)| = \chi(1)$, the proposition follows directly from Proposition A.7(i). $\square$

Appendix B. Group theory for $\mathrm{GS}p_{2g}$

B.1. **Symplectic groups.** Fix a field k, a finite dimensional vector space V of dimension $2g$ over k, and a nondegenerate alternating bilinear form $\langle\,,\,\rangle \colon V \times V \to k$. We define $\operatorname{GSp}(V, \langle\,,\,\rangle)$ to be the group of $A \in \operatorname{Aut}(V)$ such that for some $\mathrm{m}(A) \in k^\times$, we have $\langle Av, Aw \rangle = \mathrm{m}(A)\langle v, w \rangle$ for all $v, w \in V$. Define $\operatorname{Sp}(V, \langle\,,\,\rangle)$ to be the group of automorphisms of V which preserve the pairing. We call $\operatorname{GSp}(V, \langle\,,\,\rangle)$ (resp. $\operatorname{Sp}(V, \langle\,,\,\rangle)$) the *group of symplectic similitudes* (resp. the *symplectic group*). The element $\mathrm{m}(A) \in k^\times$ is called the *multiplier* of A, and gives an exact sequence: $1 \to \operatorname{Sp}(V, \langle\,,\,\rangle) \to \operatorname{GSp}(V, \langle\,,\,\rangle) \xrightarrow{\mathrm{m}} k^\times \to 1$.

Up to isomorphism, V has a unique non-degenerate alternating bilinear form; with this in mind, we may unambiguously use the notation $\operatorname{GSp}_{2g}(k)$ and $\operatorname{Sp}_{2g}(k)$. Note that for $g = 1$, $\operatorname{GSp}_2(k) = \operatorname{GL}_2(k)$ and $\operatorname{Sp}_2(k) = \operatorname{SL}_2(k)$. For any $A \in \operatorname{GSp}_{2g}(k)$, we have the relation

$$P(\mathrm{m}(A)/T)/(\mathrm{m}(A)/T)^g = P(T)/T^g,$$

where $P(T) = \det(TI - A) \in k[T]$.

B.2. **Bounds on group orders and number of conjugacy classes.**

Lemma B.1. [Gal70] *Let N be a normal subgroup of a finite group G. Then $|G^\sharp| \leq |(G/N)^\sharp||N^\sharp|$.*

Lemma B.2. *Fix a prime power q.*

    (i) $|\operatorname{Sp}_{2g}(\mathbb{F}_q)| = q^{g^2} \prod_{i=1}^{g}(q^{2i} - 1)$.

    (ii) $|\operatorname{GSp}_{2g}(\mathbb{F}_q)| = (q - 1)q^{g^2} \prod_{i=1}^{g}(q^{2i} - 1) \leq q^{2g^2+g+1}$.

    (iii) *We have $|\operatorname{Sp}_{2g}(\mathbb{F}_q)^\sharp| \leq \kappa_g q^g$ and $|\operatorname{GSp}_{2g}(\mathbb{F}_q)^\sharp| \leq \kappa_g q^{g+1}$ where κ_g depends only on g.*

Proof. Part (i) can be found in [Art88, Chapter III §6], with part (ii) following immediately since $|\operatorname{GSp}_{2g}(\mathbb{F}_q)| = (q - 1)|\operatorname{Sp}_{2g}(\mathbb{F}_q)|$. We now consider part (iii). By Lemma B.1, it suffices to prove the bound for $|\operatorname{Sp}_{2g}(\mathbb{F}_q)^\sharp|$; this follows from [LP97]. $\qquad\square$

Lemma B.3. *Let q be a prime power.*

    (i) $|\operatorname{GL}_2(\mathbb{F}_q)| = q(q - 1)^2(q + 1)$.

    (ii) $|\operatorname{GL}_2(\mathbb{F}_q)^\sharp| = q^2 - 1$.

    (iii) *For $t \in \mathbb{F}_q^\times$, $|\{A \in \operatorname{GL}_2(\mathbb{F}_q) : \operatorname{tr}(A) = t\}| = q(q^2 - q - 1)$.*

    (iv) *Assume q is an odd prime and let $\left(\frac{\cdot}{q}\right)$ be the Legendre symbol. For all $t \in \mathbb{F}_q$ and $d \in \mathbb{F}_q^\times$,*

$$|\{A \in \operatorname{GL}_2(\mathbb{F}_q) : \det(A) = d, \operatorname{tr}(A) = t\}| = q\left(q + \left(\frac{t^2-4d}{q}\right)\right).$$

Proof. One has an explicit description of the conjugacy classes of $\operatorname{GL}_2(\mathbb{F}_q)$, see for example [Lan02, XVIII Table 12.4]. The lemma is then a direct computation. $\qquad\square$

References

[Art88]   E. Artin, *Geometric algebra*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1988. Reprint of the 1957 original; A Wiley-Interscience Publication. ↑B.2

[Bom74]   Enrico Bombieri, *Le grand crible dans la théorie analytique des nombres*, Société Mathématique de France, Paris, 1974. Avec une sommaire en anglais; Astérisque, No. 18. ↑1.1, 2.2

[Bom78]   _____, *On exponential sums in finite fields. II*, Invent. Math. **47** (1978), no. 1, 29–39. ↑1.1, 2.2

[Cha97]   Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180. ↑1.4.2, iii, 6.3, 6.4

[Coj05]   Alina Carmen Cojocaru, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. **119** (2005), no. 3, 265–289. ↑1.3

[CD08]   Alina Carmen Cojocaru and Chantal David, *Frobenius fields for elliptic curves*, Amer. J. Math. **130** (2008), no. 6, 1535–1560. ↑1.7

[Elk87]   Noam D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* **Q**, Invent. Math. **89** (1987), no. 3, 561–567. ↑1.5

[Gal70]   Patrick X. Gallagher, *The number of conjugacy classes in a finite group*, Math. Z. **118** (1970), 175–179. ↑B.1

[Hal08]   Chris Hall, *An open image theorem for a general class of abelian varieties* (2008). With an appendix by Emmanuel Kowalski, arXiv:0803.1682v1. ↑ii

[IK04]   Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. ↑iii

[Kac59]   Mark Kac, *Statistical independence in probability, analysis and number theory.*, The Carus Mathematical Monographs, No. 12, Published by the Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, 1959. ↑

[Kob88]   Neal Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165. ↑1.2

[Kow06]   E. Kowalski, *The large sieve, monodromy and zeta functions of curves*, J. Reine Angew. Math. **601** (2006), 29–69. ↑iii

[Kow08]   _____, *The large sieve and its applications: arithmetic geometry, random walks, discrete groups*, Cambridge University Press, 2008. ↑1.1, iii, iv

[LO77]   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, Durham, 1975), Academic Press, London, 1977, pp. 409–464. ↑A.4

[Lan94]   Serge Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. ↑4.2

[Lan02]   _____, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. ↑4.2, B.2

[LT76]   Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers; Lecture Notes in Mathematics, Vol. 504. ↑1.7

[LW54]   Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827. ↑5.1

[LP97]   Martin W. Liebeck and László Pyber, *Upper bounds for the number of conjugacy classes of a finite group*, J. Algebra **198** (1997), no. 2, 538–562. ↑B.2

[MW71]   J. S. Milne and W. C. Waterhouse, *Abelian varieties over finite fields*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64. ↑i

[Mon78]   Hugh L. Montgomery, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. **84** (1978), no. 4, 547–567. ↑1.1, 2.4

[Mur01]   M. Ram Murty, *Problems in analytic number theory*, Graduate Texts in Mathematics, vol. 206, Springer-Verlag, New York, 2001. Readings in Mathematics. ↑4.2

[MMS88]   M. Ram Murty, V. Kumar Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), no. 2, 253–281. ↑A.2, A.2

[Rib75]   Kenneth A. Ribet, *On l-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245–275. ↑3.3

[Ser72]   Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑3.3

[Ser77]   _____, *Linear representations of finite groups*, Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott; Graduate Texts in Mathematics, Vol. 42. ↑1.6

[Ser81]   _____, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. ↑ii, A.1, A.2, A.2, A.4

[Ser92]   _____, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Darmon; With a foreword by Darmon and the author. ↑1.3.1, ii

[Ser94]   _____, *Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 377–400. ↑ii

[Ser97]   _____, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre. ↑1.3.1, 5.1

[Ser00]   _____, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000. 1985–1998. ↑3.3, i

[Sta74]   H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152. ↑A.3

[Zyw11]   David Zywina, *A refinement of Koblitz's conjecture*, Int. J. Number Theory **7** (2011), no. 3, 739–769. ↑1.2, 4

[Zyw10]   _____, *The Lang-Trotter conjecture and mixed representations*, preprint (2010). ↑1.7

[Zyw11]   _____, *The splitting of reductions of an abelian variety*, preprint (2011). ↑1.4.2

DEPARTMENT OF MATHEMATICS AND STATISTICS, QUEEN'S UNIVERSITY, KINGSTON, ON K7L 3N6, CANADA

E-mail address: zywina@mast.queensu.ca

URL: http://www.mast.queensu.ca/~zywina