THE LANG-TROTTER CONJECTURE AND MIXED REPRESENTATIONS

DAVID ZYWINA

ABSTRACT. For a fixed elliptic curve E over $\mathbb{Q}$ and imaginary quadratic field k, let $P_{E,k}(x)$ be the number of primes $p \leq x$ for which the reduction of E modulo p has complex multiplication by k. We shall show that $P_{E,k}(x) \ll_{E,k} x(\log\log x)^2/(\log x)^2$, and $P_{E,k}(x) \ll_E x^{4/5}/(\log x)^{1/5}$ assuming the Generalized Riemann Hypothesis. These are the best known bounds on $P_{E,k}(x)$, and represent progress towards the *Lang-Trotter conjecture* which predicts that $P_{E,k}(x) \sim C_{E,k} \cdot x^{1/2}/\log x$ as $x \to \infty$, for an explicit constant $C_{E,k} > 0$.

The argument uses the Galois representations occurring in the original heuristics of Lang and Trotter, which mix the Galois representations coming from the action on the torsion points of E with those from the class field theory of k. With these representations, our bounds for $P_{E,k}(x)$ will be deduced using effective versions of the Chebotarev density theorem.

1. INTRODUCTION

1.1. **The Lang-Trotter conjecture.**

Let E be an elliptic curve defined over $\mathbb{Q}$, and let N_E be the product of the primes for which E has bad reduction. For each prime $p \nmid N_E$, let E_p be the elliptic curve over $\mathbb{F}_p$ obtained by reduction modulo p. The ring $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_p)$ is either an order of an imaginary quadratic extension of $\mathbb{Q}$ (when E has ordinary reduction at p), or an order of a quaternion algebra (when E has supersingular reduction at p). It is natural to ask how frequently these different fields occur as the prime p varies.

Fix an imaginary quadratic extension $k/\mathbb{Q}$, and define the counting function

$$P_{E,k}(x) := \#\{p \leq x : p \nmid N_E,\ \operatorname{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong k\}.$$

In the rest of this paper, we will assume that $x \geq 3$ in order to ensure that all our bounds are defined and uniform.

First consider the case where E has complex multiplication by an imaginary quadratic field K. Since $\operatorname{End}_{\overline{\mathbb{Q}}}(E)$ injects into $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_p)$, we have $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$ for all ordinary primes p of E. Thus if $K \cong k$,

$$P_{E,k}(x) \sim \frac{1}{2}\pi(x)$$

as $x \to \infty$, where $\pi(x)$ is the number of rational primes less than x (i.e., k shows up half the time as the endomorphism field of the E_p's). If $K \ncong k$, then $P_{E,k}(x) = 0$.

If E does not have complex multiplication things are much more complicated. In this case, there is the following conjecture of Lang and Trotter [LT76].

Date: April 7, 2009.

2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 11N05, 11R45.

Key words and phrases. Elliptic curves modulo p, Lang-Trotter conjecture, Chebotarev density theorem.

This research was supported by an NSERC postgraduate scholarship.

Conjecture 1.1 (Lang-Trotter, 1976)**.** Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication, and let k be an imaginary quadratic extension of $\mathbb{Q}$. There is an explicit constant $C_{E,k} > 0$ such that

$$P_{E,k}(x) \sim C_{E,k} \frac{x^{1/2}}{\log x}$$

as $x \to \infty$.

Remark 1.2. Heuristics for Conjecture 1.1 and a description of the constant $C_{E,k}$ will be given in Appendix A.

Conjecture 1.1 is formulated in a slightly different way than in [LT76]. For each prime $p \nmid N_E$, let $\pi_p(E)$ be the Frobenius endomorphism in $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_p)$. The endomorphism $\pi_p(E)$ is a root of an integral polynomial

$$x^2 - a_p(E)x + p.$$

Hasse showed that $|a_p(E)| < 2\sqrt{p}$, so the field $\mathbb{Q}(\pi_p(E))$ is an imaginary quadratic extension of $\mathbb{Q}$. Thus for ordinary primes p, $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\pi_p(E))$. Our counting function becomes

$$P_{E,k}(x) = \#\{p \leq x : E \text{ has ordinary reduction at } p,\ \mathbb{Q}(\pi_p(E)) \cong k\}.$$

If $p > 3$ is a prime of supersingular reduction, then $\mathbb{Q}(\pi_p(E)) \cong \mathbb{Q}(\sqrt{-p})$. Thus

$$\#\{p \leq x : p \nmid N_E, \mathbb{Q}(\pi_p(E)) \cong k\} = P_{E,k}(x) + O(1),$$

which is the quantity studied by Lang and Trotter and of course has the same conjectural asymptotics.

We now justify our restriction to imaginary quadratic fields. Suppose that $p \nmid N_E$ is a prime where E has supersingular reduction, then $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q}$ is the unique quaternion algebra over $\mathbb{Q}$ ramified precisely at p and ∞. Thus if K is not an imaginary quadratic field, then we have $P_{E,K}(x) \leq 1$.

1.2. **Known bounds.** Conjecture 1.1 seems to be extremely difficult, and in lieu of a proof it is interesting to find non-trivial bounds on $P_{E,k}(x)$. No lower bounds are known, if fact $\lim_{x\to\infty} P_{E,k}(x) = \infty$ is not known for a single non-CM $E/\mathbb{Q}$ and field k. We shall now focus on upper bounds.

In [Ser81, p.191], J.-P. Serre asserts (but does not prove) that using Selberg sieve techniques one can show

$$P_{E,k}(x) \ll_{E,k} \frac{x}{(\log x)^\gamma} \qquad \text{for some } \gamma > 1,$$

and under the Generalized Riemann Hypothesis (GRH)

$$P_{E,k}(x) \ll_{E,k} x^\delta \qquad \text{for some } \delta < 1.$$

The first proof to appear in the literature occurs much later, and is due to Cojocaru, Fouvry, and Murty [CFM05]. They use a sieving technique called the *square sieve* to show

$$P_{E,k}(x) \ll_{N_E} \frac{x(\log\log x)^{13/12}}{(\log x)^{25/24}}(1 + \#\{p : p \text{ ramifies in } k\}),$$

and $P_{E,k}(x) \ll_{N_E} x^{17/18} \log x$ under GRH. Cojocaru and David [CD08] have since used the square sieve to prove $P_{E,k}(x) \ll_{N_E} x^{13/14} \log x$ under GRH.

In his collected papers, Serre [Ser86, p.715] remarks that instead of a sieve, one could use a mixed ℓ-adic representation to deduce a bound $P_{E,k}(x) \ll_{E,k} x^\delta$ (assuming GRH). The technique involves constructing a certain ℓ-adic Galois representation $r\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathrm{GL}_2(\mathbb{Z}_\ell)$, and then applying an effective version of the Chebotarev density theorem. The first factor of r comes from the Galois action on the ℓ-adic Tate module of E, while the second factor come from a Hecke character of k. A sketch of this method can be found in §6 of [CFM05].

Following Serre's ideas, Cojocaru and David [CD08] have proven assuming GRH that

$$P_{E,k}(x) \ll_{N_E,h_k} \frac{x^{4/5}}{(\log x)^{1/5}},$$

where h_k is the class number of k. Though they do not state the dependence on h_k explicitly, the proof shows that the implicit constant grows like $h_k^{3/5}$ in terms of the class number.

1.3. **Statement of results.** In this paper we present an upper bound on $P_{E,k}(x)$ that has better asymptotics and dependence on k than earlier bounds. Our technique is similar to the approach of Serre, but is really motivated by the Galois representations occuring in Lang and Trotter's original heuristics for Conjecture 1.1. The needed representations will be defined in §2. The key difference with the method of Serre is that it is turns out to be more convenient (and simpler) to work over the Hilbert class field of k rather than over $\mathbb{Q}$. Our main result is the following upper bounds on $P_{E,k}(x)$.

Theorem 1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. Let k be an imaginary quadratic extension of $\mathbb{Q}$, and let h_k be the class number of k.*

(i) *Assuming the Generalized Riemann Hypothesis,*

$$P_{E,k}(x) \ll_E \frac{1}{h_k^{3/5}} \frac{x^{4/5}}{(\log x)^{1/5}} + x^{1/2}(\log x)^4(\log\log x)^3.$$

(ii) *There is a constant $c > 0$ depending on E such that for $\log\log x \geq c d_k^{1/2}$,*

$$P_{E,k}(x) \ll_E \frac{x(\log\log x)^2}{(\log x)^2}.$$

Remark 1.4.

(i) If one is not interested in the dependence of the bounds on the field k, then we have simply $P_{E,k}(x) \ll_E x^{4/5}/(\log x)^{1/5}$ under GRH, and $P_{E,k}(x) \ll_{E,k} x(\log\log x)^2/(\log x)^2$ unconditionally. However, the dependence of the constant on k is important for applications like Corollary 1.5 below.

(ii) The heuristics in [LT76] for Conjecture 1.1 use only properties of E that can be expressed in terms of the Galois action on its Tate modules and the Sato-Tate law. Lang and Trotter axiomatized their heuristics beyond non-CM elliptic curves $E/\mathbb{Q}$ to "GL_2-distributions of elliptic type" (see [LT76, Part I §1] for definitions). Though we make no further mention of it, the proof of the above theorem also works in this more general setting.

(iii) There is another major conjecture in the book [LT76]. Let $E/\mathbb{Q}$ be a non-CM elliptic curve and fix an integer $t \in \mathbb{Z}$. Define the counting function

$$P_{E,t}(x) = \#\{p \leq x : p \nmid N_E,\, a_p(E) = t\}.$$

Lang and Trotter conjecture that there is a constant $C_{E,t} \geq 0$ such that

$$P_{E,t}(x) \sim C_{E,t} \frac{x^{1/2}}{\log x}$$

as $x \to \infty$ (if $C_{E,t} = 0$, then this is defined to mean that there only finitely many p such that $a_p(E) = t$). The best known general upper bounds are

$$P_{E,t}(x) \ll_E \frac{x^{4/5}}{(\log x)^{1/5}}$$

under GRH, and

$$P_{E,t}(x) \ll_E \frac{x(\log\log x)^2}{(\log x)^2}$$

unconditionally (analogous results are proven in [MMS88, Mur97] for modular forms, and the proofs carry over immediately to elliptic curves). Theorem 1.3 thus gives the analogue of these bounds for Conjecture 1.1 and its proof uses many of the same techniques.

(iv) We do not work out the dependency on E in our bounds, but it can be verified that it depends only on the integer N_E.

Let $D_E(x)$ be the set of imaginary quadratic extensions $k/\mathbb{Q}$ (in some fixed algebraic closure of $\mathbb{Q}$) for which there exists a prime $p \le x$ with $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong k$.

Corollary 1.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. Assuming the Generalized Riemann Hypothesis,*

$$|D_E(x)| \gg_E \frac{x^{2/7}}{(\log x)^2}.$$

Remark 1.6. This improves on the bound $|D_E(x)| \gg_E x^{1/14}/(\log x)^2$ from [CD08, Corollary 5].

1.4. Acknowledgements.

I would like to thank Bjorn Poonen for his encouragement and helpful remarks.

Notation

Let f and g be 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 $x \ge C_1$, $|f(x)| \le C_2|g(x)|$. We shall use $O(f)$ to represent an unspecified function g with $g \ll f$. The dependencies of the constants C_1 and C_2 will be always be indicated by subscripts on the symbols $\ll$, $\gg$ and O; in particular, no subscripts implies that the constants are absolute.

Define the logarithmic integral, $\operatorname{Li}(x) = \int_2^x \frac{dt}{\log t}$. The function $\operatorname{Li}(x)$ is asymptotic to $x/\log x$ as $x \to \infty$.

Let F be a number field. Let $\overline{F}$ be a fixed algebraic closure of F, and let F^{ab} be the maximal abelian extension of F in $\overline{F}$. We denote the ring of integers of F by $\mathcal{O}_F$. For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, let $N(\mathfrak{p})$ be the cardinality of the field $\mathcal{O}_F/\mathfrak{p}$. Let Σ_F be the set of nonzero prime ideals of $\mathcal{O}_F$, and let $\Sigma_F(x)$ be the set of $\mathfrak{p} \in \Sigma_F$ with $N(\mathfrak{p}) \le x$. Let d_F be the absolute discriminant of F.

Consider a Galois extension L/F of number fields with Galois group $\operatorname{Gal}(L/F)$. Fix a $\mathfrak{p} \in \Sigma_F$ that is unramified in L and choose a $\mathfrak{P} \in \Sigma_L$ dividing $\mathfrak{p}$; we will denote by $(\mathfrak{P}, L/F) \in \operatorname{Gal}(L/F)$ the corresponding Frobenius automorphism. The conjugacy class of $(\mathfrak{P}, L/F)$ in $\operatorname{Gal}(L/F)$ does not depend on which prime $\mathfrak{P} \in \Sigma_L$ we chose, and will be denoted by $(\mathfrak{p}, L/F)$ or simply $\operatorname{Frob}_{\mathfrak{p}}$ if the field extension is clear from context.

The symbol k will always denote a imaginary quadratic extension of $\mathbb{Q}$. Let h_k be the class number of $\mathcal{O}_k$, and w_k the number of roots of unity in k. Whenever k is being used, we will denote the Hilbert class field of k by H. For an integer $m \ge 1$, let $\nu(m)$ be the number of distinct prime divisors of m. Finally, the symbols ℓ and p will only be used to denote rational primes.

2. Galois representations

In this section, we describe the Galois representations that will be needed for our proof of Theorem 1.3. These are amongst the representations used by Serge Lang and Hale Trotter in their heuristics for Conjecture 1.1 (cf. Appendix A).

2.1. **Torsion fields of elliptic curves.** For the basics on elliptic curves see [Sil92]. Fix an elliptic curve E defined over a number field F. For each integer $m \geq 1$, let $E[m]$ be the group of m-torsion in $E(\overline{F})$. The natural $\operatorname{Gal}(\overline{F}/F)$-action on $E[m]$ gives a representation, $\rho\colon \operatorname{Gal}(\overline{F}/F) \to \operatorname{Aut}(E[m])$. We denote by $F(E[m])$ the fixed field in $\overline{F}$ of $\ker\rho$, thus ρ induces an injective homomorphism

$$\rho_{E/F,m}\colon \operatorname{Gal}(F(E[m])/F) \hookrightarrow \operatorname{Aut}(E[m]).$$

The group $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2, so there are well-defined trace and determinant maps, $\operatorname{tr}\colon \operatorname{Aut}(E[m]) \to \mathbb{Z}/m\mathbb{Z}$ and $\det\colon \operatorname{Aut}(E[m]) \to (\mathbb{Z}/m\mathbb{Z})^\times$.

Let μ_m be the group of m-th roots of unity in $\overline{F}$. Let $\chi\colon \operatorname{Gal}(\overline{F}/F) \to (\mathbb{Z}/m\mathbb{Z})^\times$ be the character such that $\sigma(\zeta) = \zeta^{\chi(\sigma)}$, for all $\zeta \in \mu_m$, $\sigma \in \operatorname{Gal}(\overline{F}/F)$. This character induces an injective homomorphism

$$\chi_{F,m}\colon \operatorname{Gal}(F(\mu_m)/F) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times .$$

If $\mathbb{Q}(\mu_m) \cap F = \mathbb{Q}$, then $\chi_{F,m}$ is an isomorphism. The next lemma is a direct consequence of the compatibility of the Weil pairing of E with the Galois action.

Lemma 2.1. *With notation as above, $F(\mu_m) \subseteq F(E[m])$, and for all $\sigma \in \operatorname{Gal}(F(E[m])/F)$*

$$\det \rho_{E/F,m}(\sigma) = \chi_{F,m}(\sigma|_{F(\mu_m)}).$$

For a finite group G, let G' be the derived subgroup of G; i.e., G' is the smallest normal subgroup of G such that G/G' is abelian.

Lemma 2.2. *If m is a positive integer relatively prime to 6, then $\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})' = \operatorname{SL}_2(\mathbb{Z}/m\mathbb{Z})$.*

Proof. See Corollary 8 of the appendix to [Coj05]. □

Lemma 2.3. *Let E be a non-CM elliptic curve defined over a number field F, and let m be a positive integer relatively prime to 6 such that $\rho_{E/F,m}$ is an isomorphism. Then*

$$F(E[m]) \cap F^{\mathrm{ab}} = F(\mu_m).$$

Proof. By assumption $\rho_{E/F,m}\colon \operatorname{Gal}(F(E[m])/F) \to \operatorname{Aut}(E[m])$ is an isomorphism, so by Lemma 2.2

$$\operatorname{Gal}(F(E[m])/F)' = \{\sigma \in \operatorname{Gal}(F(E[m])/F) : \det \rho_{E/F,m}(\sigma) = 1\}.$$

From Lemma 2.1, we deduce that $\operatorname{Gal}(F(E[m])/F)' = \operatorname{Gal}(F(E[m])/F(\mu_m))$. Therefore,

$$\operatorname{Gal}(F(E[m]) \cap F^{\mathrm{ab}}/F) = \operatorname{Gal}(F(E[m])/F)/\operatorname{Gal}(F(E[m])/F)' = \operatorname{Gal}(F(\mu_m)/F)$$

and the lemma follows. □

The following deep theorem, which is vital for this paper, is due to Serre.

Theorem 2.4. *Let E be a non-CM elliptic curve defined over a number field F. There is a positive integer $A_{E,F}$ such that the Galois representation*

$$\rho_{E/F,m}\colon \operatorname{Gal}(F(E[m])/F) \to \operatorname{Aut}(E[m])$$

is an isomorphism for all m relatively prime to $A_{E,F}$.

Proof. This follows from [Ser72, p.299 Théorème 3′], which says that the index

$$[\operatorname{Aut}(E[m]) : \rho_{E/F,m}(\operatorname{Gal}(F(E[m])/F))]$$

is bounded independent of m. □

We now specialize to the case that will be of interest to us.

Lemma 2.5. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. There is a constant $c_E > 0$ such that for any imaginary quadratic extension k of $\mathbb{Q}$ with Hilbert class field H,*

$$\rho_{E/H,\ell}\colon \operatorname{Gal}(H(E[\ell])/H) \hookrightarrow \operatorname{Aut}(E[\ell])$$

is an isomorphism for all primes $\ell \geq c_E$ that are unramified in k.

Proof. By Theorem 2.4, there is a constant $c_E \geq 5$ such that $\rho_{E/\mathbb{Q},\ell}$ is an isomorphism for all primes $\ell \geq c_E$. Take any $\ell \geq c_E$ which is unramified in k.

In order to show that $\rho_{E/H,\ell}\colon \operatorname{Gal}(H(E[\ell])/H) \hookrightarrow \operatorname{Aut}(E[\ell])$ is an isomorphism it suffices to show that $\mathbb{Q}(E[\ell]) \cap H = \mathbb{Q}$, since in this situation we have a canonical isomorphism $\operatorname{Gal}(H(E[\ell])/H) \cong \operatorname{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ and $\rho_{E/\mathbb{Q},\ell}$ is an isomorphism.

Suppose that $\mathbb{Q}(E[\ell]) \cap H \neq \mathbb{Q}$. The field $\mathbb{Q}(E[\ell]) \cap H$ is a solvable extension of $\mathbb{Q}$, so there is a field $L \subseteq \mathbb{Q}(E[\ell]) \cap H$ with $L/\mathbb{Q}$ a non-trivial abelian extension. By Lemma 2.3, L is a subfield of $\mathbb{Q}(\mu_\ell) \cap H$ ($\ell \neq 2$ or 3, since we have chosen $c_E \geq 5$). We deduce that L is unramified over $\mathbb{Q}$ at all prime numbers except possibly ℓ. However, L is a subfield of H which is unramified at ℓ (since k is). Therefore, L is unramifed over $\mathbb{Q}$ at all finite places and thus $L = \mathbb{Q}$, contradicting that $L/\mathbb{Q}$ is a non-trivial extension. □

Remark 2.6.

(i) The constant c_E of Lemma 2.5 is independent of the field k.

(ii) The constant c_E can be bounded explicitly in terms of N_E (for example, see [Coj05, Theorem 2]). Serre has asked whether one can take $c_E = 41$ [Ser81, p.399 Question 2].

Given an elliptic curve E over a number field F and a prime $\mathfrak{p} \in \Sigma_F$ of good reduction, define

$$a_{\mathfrak{p}}(E) = N(\mathfrak{p}) + 1 - |E_{\mathfrak{p}}(\mathcal{O}_F/\mathfrak{p})|.$$

Fix a positive integer m. If $\mathfrak{p} \in \Sigma_F$ is a prime of good reduction for E which does not divide m, then $\mathfrak{p}$ is unramified in the extension $F(E[m])/F$. By Lemma 2.1,

$$\det\left(\rho_{E/F,m}(\operatorname{Frob}_{\mathfrak{p}})\right) = \chi_{F,m}(\operatorname{Frob}_{\mathfrak{p}}) \equiv N(\mathfrak{p}) \pmod{m},$$

and one can show that

$$\operatorname{tr}\left(\rho_{E/F,m}(\operatorname{Frob}_{\mathfrak{p}})\right) \equiv a_{\mathfrak{p}}(E) \pmod{m}.$$

2.2. **Class field theory of k.** Let k be an imaginary quadratic extension of $\mathbb{Q}$. We now review some class field theory concerning k; this will be especially simple since k has no real places and the group $\mathcal{O}_k^\times$ is finite.

Fix a $\mathfrak{p} \in \Sigma_k$. Given a fractional ideal $\mathfrak{a}$ of k, let $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$ be the power of $\mathfrak{p}$ occuring in the factorization of $\mathfrak{a}$. For $a \in k^\times$, define $v_{\mathfrak{p}}(a) := v_{\mathfrak{p}}(a\mathcal{O}_k)$ (and extend this definition by setting $v_{\mathfrak{p}}(0) = +\infty$).

Fix a nonzero integral ideal $\mathfrak{m}$ of k. Let $S(\mathfrak{m})$ be the set of maximal ideals of $\mathcal{O}_k$ dividing $\mathfrak{m}$ and let $I_k^{S(\mathfrak{m})}$ be the group of fractional ideals of k generated by $\Sigma_k - S(\mathfrak{m})$. Define the following subgroups of $k^\times$:

$$k_{\mathfrak{m}} = \{a \in k^\times : v_{\mathfrak{p}}(a) = 0 \text{ for all } \mathfrak{p}|\mathfrak{m}\}$$

and

$$k_{\mathfrak{m},1} = \{a \in k_{\mathfrak{m}} : v_{\mathfrak{p}}(a-1) \geq v_{\mathfrak{p}}(\mathfrak{m}) \text{ for all } \mathfrak{p}|\mathfrak{m}\}.$$

Now consider the group homomorphism $\iota\colon k_{\mathfrak{m}} \to I_k^{S(\mathfrak{m})}$, which takes an element of $k_{\mathfrak{m}}$ to the fractional ideal of k it generates. The *ray class group modulo* $\mathfrak{m}$ is then defined as

$$\operatorname{Cl}_{\mathfrak{m}} = I_k^{S(\mathfrak{m})}/\iota(k_{m,1}).$$

Note that for $\mathfrak{m} = \mathcal{O}_k$, $\mathrm{Cl}_{\mathcal{O}_k}$ is just the usual class group of k, which we will also denote by Cl_k.

Lemma 2.7. *Let $\mathfrak{m}$ be a nonzero proper ideal of $\mathcal{O}_k$. Define a group homomorphism*

$$\beta_{\mathfrak{m}} \colon (\mathcal{O}_k/\mathfrak{m})^\times \to \mathrm{Cl}_{\mathfrak{m}}, \quad a + \mathfrak{m} \mapsto a\mathcal{O}_k \cdot i(k_{\mathfrak{m},1}).$$

There is an exact sequence of groups

$$1 \to \mathcal{O}_k^\times/\mathcal{O}_k^\times \cap (1+\mathfrak{m}) \xrightarrow{\alpha} (\mathcal{O}_k/\mathfrak{m})^\times \xrightarrow{\beta_{\mathfrak{m}}} \mathrm{Cl}_{\mathfrak{m}} \xrightarrow{\gamma} \mathrm{Cl}_k \to 1,$$

where α is reduction modulo $\mathfrak{m}$ and γ is induced by the natural map $I_k^{S(\mathfrak{m})} \to \mathrm{Cl}_k$.

Proof. It is straightforward to show that

$$1 \to \mathcal{O}_k^\times \cap (1+\mathfrak{m}) = \mathcal{O}_k^\times \cap k_{\mathfrak{m},1} \to \mathcal{O}_k^\times \to k_{\mathfrak{m}}/k_{\mathfrak{m},1} \xrightarrow{\iota} \mathrm{Cl}_{\mathfrak{m}} \xrightarrow{\gamma} \mathrm{Cl}_k \to 1 \tag{2.1}$$

is an exact sequence. We have a natural inclusion, $k_{\mathfrak{m}} \hookrightarrow \mathcal{O}_{k,\mathfrak{m}}^\times$, where $\mathcal{O}_{k,\mathfrak{m}}$ is the $\mathfrak{m}$-adic completion of $\mathcal{O}_k$. Composing with the reduction modulo $\mathfrak{m}$ map gives a group homomorphism, $f\colon k_{\mathfrak{m}} \to (\mathcal{O}_{k,\mathfrak{m}}/\mathfrak{m}\mathcal{O}_{k,\mathfrak{m}})^\times = (\mathcal{O}_k/\mathfrak{m})^\times$. This induces an isomorphism, $\overline{f}\colon k_{\mathfrak{m}}/k_{\mathfrak{m},1} \xrightarrow{\sim} (\mathcal{O}_k/\mathfrak{m})^\times$. Identifying $k_{\mathfrak{m}}/k_{\mathfrak{m},1}$ in (2.1) by $(\mathcal{O}_k/\mathfrak{m})^\times$ via the isomorphism $\overline{f}$, gives the desired exact sequence. □

There is a unique abelian extension $k(\mathfrak{m})$ of k (in a fixed algebraic closure $\overline{k}$ of k) that is unramified outside $S(\mathfrak{m})$ and for which the Artin map

$$I_k^{S(\mathfrak{m})} \to \mathrm{Gal}(k(\mathfrak{m})/k), \; \mathfrak{a} \mapsto \prod_{\mathfrak{p} \in \Sigma_k - S(\mathfrak{m})} (\mathfrak{p}, k(\mathfrak{m})/k)^{v_{\mathfrak{p}}(\mathfrak{a})}$$

has kernel $i(k_{\mathfrak{m},1})$ (note that we can view $(\mathfrak{p}, k(\mathfrak{m})/k)$ as an element of $\mathrm{Gal}(k(m)/k)$ since the group is abelian). This induces a group isomorphism

$$\varphi_{k(\mathfrak{m})/k} \colon \mathrm{Cl}_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(k(\mathfrak{m})/k). \tag{2.2}$$

The field $k(\mathfrak{m})$ is the *ray class field* for $\mathfrak{m}$. The field $k(\mathcal{O}_k)$ is the Hilbert class field of k, which we will always denoted by H. For a nonzero integer m, we will write $k(m)$ instead of $k(m\mathcal{O}_k)$.

Fix an integer $m \geq 5$. We now apply the above class field theory with $\mathfrak{m} = \mathcal{O}_k$ and $m\mathcal{O}_k$. The following diagram commutes,

$$\begin{tikzcd}
\mathrm{Cl}_{m\mathcal{O}_k} \arrow[r, "\varphi_{k(m)/k}", "\sim"'] \arrow[d] & \mathrm{Gal}(k(m)/k) \arrow[d] \\
\mathrm{Cl}_k \arrow[r, "\varphi_{H/k}", "\sim"'] & \mathrm{Gal}(H/k),
\end{tikzcd}$$

where the left and right maps are quotient and restriction maps respectively. The commutative diagram induces an isomorphism

$$\varphi_{k(m)/k} \colon \ker\left(\mathrm{Cl}_{m\mathcal{O}_k} \to \mathrm{Cl}_k\right) \xrightarrow{\sim} \mathrm{Gal}(k(m)/H). \tag{2.3}$$

Since $m \geq 5$, one can check that $\mathcal{O}_k^\times \cap (1 + m\mathcal{O}_k) = \{1\}$. By Lemma 2.7, there is an isomorphism

$$\beta_{m\mathcal{O}_k} \colon \left(\mathcal{O}_k/m\mathcal{O}_k\right)^\times/\mathcal{O}_k^\times \xrightarrow{\sim} \ker\left(\mathrm{Cl}_{m\mathcal{O}_k} \to \mathrm{Cl}_k\right), \tag{2.4}$$

where we have identified $\mathcal{O}_k^\times$ with its image in $(\mathcal{O}_k/m\mathcal{O}_k)^\times$. Composing the inverses of (2.3) and (2.4) defines an isomorphism

$$\psi_{k,m} \colon \mathrm{Gal}(k(m)/H) \xrightarrow{\sim} \left(\mathcal{O}_k/m\mathcal{O}_k\right)^\times/\mathcal{O}_k^\times. \tag{2.5}$$

We now give an explicit description of how the map $\psi_{k,m}$ acts on Frobenius elements.

Lemma 2.8. *Let $m \geq 5$ be an integer and $p \nmid m$ a rational prime. Suppose that p splits completely in H, and let $\mathfrak{P} \in \Sigma_H$ be a prime ideal dividing p. The prime ideal $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_k$ is principal. For any generator $\pi \in \mathcal{O}_K$ of $\mathfrak{p}$, we have*

$$\psi_{k,m}(\mathrm{Frob}_{\mathfrak{P}}) = (\pi + m\mathcal{O}_k)\mathcal{O}_k^\times \in (\mathcal{O}_k/m\mathcal{O}_k)^\times / \mathcal{O}_k^\times.$$

Proof. Since $\mathfrak{p}$ splits completely in H, it must be principal; so there is indeed an element $\pi \in \mathcal{O}_k$ generating $\mathfrak{p}$. The map (2.4) sends $(\pi + m\mathcal{O}_k)\mathcal{O}_k^\times$ to the ideal class in $\mathrm{Cl}_{m\mathcal{O}_k}$ of $\pi\mathcal{O}_k = \mathfrak{p}$. The map $\varphi_{k(m)/k}$ sends the ideal class containing $\mathfrak{p}$ to the Frobenius element $(\mathfrak{p}, k(m)/k) \in \mathrm{Gal}(k(m)/k)$. Since $\mathfrak{p}$ splits completely in H, $(\mathfrak{p}, k(m)/k) = (\mathfrak{P}, k(m)/H)$. The lemma is now immediate from our definition of $\psi_{k,m}$. □

Remark 2.9. Lemma 2.8 actually gives a full description of $\psi_{k,m}$ since every element in $\mathrm{Gal}(k(m)/H)$ is of the form $\mathrm{Frob}_{\mathfrak{P}}$ with $\mathfrak{P}$ as in the lemma (this is an easy consequence of the Chebotarev density theorem).

Let $N\colon (\mathcal{O}_k/m\mathcal{O}_k)^\times / \mathcal{O}_k^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ be the norm map, which is well defined since the norm map takes value 1 on $\mathcal{O}_k^\times$.

Lemma 2.10. *Fix an integer $m \geq 5$. Then $H(\mu_m) \subseteq k(m)$, and for all $\sigma \in \mathrm{Gal}(k(m)/H)$*

$$N(\psi_{k,m}(\sigma)) = \chi_{H,m}(\sigma|_{H(\mu_m)}).$$

Proof. Let $p \nmid m$ be a prime that splits completely in H and let $\mathfrak{P} \in \Sigma_H$ be any prime dividing p (such $\mathfrak{P}$ have density 1 in the prime ideals of H). Fix a generator π of $\mathfrak{P} \cap \mathcal{O}_k$. By Lemma 2.8,

$$N(\psi_{k,m}((\mathfrak{P}, k(m)/H))) \equiv N(\pi) = N(\mathfrak{P}) \pmod{m}.$$

Since $\chi_{H,m}((\mathfrak{P}, H(\mu_m)/H)) \equiv N(\mathfrak{P}) \pmod{m}$, we have

$$N(\psi_{k,m}((\mathfrak{P}, k(m)/H))) = \chi_{H,m}((\mathfrak{P}, H(\mu_m)/H)). \tag{2.6}$$

If any such $\mathfrak{P}$ splits completely in $k(m)$, then by (2.6) it also splits completely in $H(\mu_m)$. Class field theory then tells us that $H(\mu_m) \subseteq k(m)$. For any $\sigma \in \mathrm{Gal}(k(m)/H)$, there exists a $\mathfrak{P} \in \Sigma_H$ dividing a rational prime $p \nmid m$ such that p splits completely in H and $\sigma = (\mathfrak{P}, k(m)/H)$. Then (2.6) becomes $N(\psi_{k,m}(\sigma)) = \chi_{H,m}(\sigma|_{H(\mu_m)})$. □

We now consider the trace map

$$\mathrm{Tr}\colon \mathcal{O}_k/m\mathcal{O}_k \to \mathbb{Z}/m\mathbb{Z}.$$

Lemma 2.11. *Let $m \geq 5$ be an integer and $p \nmid m$ a prime. Suppose that p splits completely in H, and let $\mathfrak{P} \in \Sigma_H$ be a prime ideal dividing p. Then*

$$\mathrm{Tr}(\psi_{k,m}(\mathrm{Frob}_{\mathfrak{P}})) = \{\mathrm{Tr}_{k/\mathbb{Q}}(\pi) \pmod{m} : \pi \in \mathcal{O}_k \textit{ generates } \mathfrak{P} \cap \mathcal{O}_k\}.$$

Proof. Let ϖ be a generator of $\mathfrak{P} \cap \mathcal{O}_k$. By Lemma 2.8, $\psi_{k,m}(\mathrm{Frob}_{\mathfrak{P}}) = (\varpi + m\mathcal{O}_k)\mathcal{O}_k^\times$.

$$\begin{aligned} \mathrm{Tr}(\psi_{k,m}(\mathrm{Frob}_{\mathfrak{P}})) &= \mathrm{Tr}\left(\{\varpi\zeta + m\mathcal{O}_k : \zeta \in \mathcal{O}_k^\times\}\right) \\ &= \{\mathrm{Tr}_{k/\mathbb{Q}}(\varpi\zeta) \pmod{m} : \zeta \in \mathcal{O}_k^\times\} \\ &= \{\mathrm{Tr}_{k/\mathbb{Q}}(\pi) \pmod{m} : \pi \in \mathcal{O}_k \text{ that generate } \mathfrak{P} \cap \mathcal{O}_k\} \end{aligned}$$ □

2.3. **Mixed representations.** Let E be a non-CM elliptic curve over $\mathbb{Q}$, and let k be an imaginary quadratic field. In this section, we combine the Galois representations $\rho_{E/H,m}$ and $\psi_{k,m}$. Fix any integer $m \geq 5$. Define the number field

$$L(m) = H(E[m])k(m),$$

the Galois group

$$G(m) = \mathrm{Gal}(L(m)/H),$$

and the group

$$\mathscr{G}(m) = \{(A, u) \in \mathrm{Aut}(E[m]) \times \left((\mathcal{O}_k/m\mathcal{O}_k)^\times/\mathcal{O}_k^\times\right) : \det(A) = N(u)\}.$$

We then have an important homomorphism

$$\Psi_m \colon G(m) \to \mathscr{G}(m), \quad \sigma \mapsto \left(\rho_{E/H,m}(\sigma|_{H(E[m])}), \psi_{k,m}(\sigma|_{k(m)})\right).$$

The map Ψ_m is well-defined, since by Lemmas 2.1 and 2.10

$$\det(\rho_{E/H,m}(\sigma|_{H(E[m])})) = \chi_{H,m}(\sigma|_{H(\mu_m)}) = N(\psi_{k,m}(\sigma|_{k(m)})).$$

The map Ψ_m is injective since both $\rho_{E/H,m}$ and $\psi_{k,m}$ are injective.

Remark 2.12. The notation just introduced does not indicate the dependence on E or k, which will always be fixed whenever these concepts appear.

Lemma 2.13. *Let $m \geq 5$ be an integer relatively prime to 6 such that $\rho_{E/H,m}$ is an isomorphism. Then $H(E[m]) \cap k(m) = H(\mu_m)$.*

Proof. We have already seen that $H(E[m]) \supseteq H(\mu_m)$ and $k(m) \supseteq H(\mu_m)$, so $H(E[m]) \cap k(m) \supseteq H(\mu_m)$. Since $k(m)$ is an abelian extension of H, we deduce from Lemma 2.3 that $H(E[m]) \cap k(m) \subseteq H(\mu_m)$. □

Lemma 2.14. *Suppose $m \geq 5$ is relatively prime to 6 and $\rho_{E/H,m}$ is an isomorphism. Then Ψ_m is an isomorphism.*

Proof. We already know that Ψ_m is injective, so all that remains to prove is surjectivity. Take any $(A, u) \in \mathscr{G}(m)$. Since $\rho_{E/H,m}$ and $\psi_{k,m}$ are isomorphisms, there exist $\sigma' \in \mathrm{Gal}(H(E[m])/H)$ and $\sigma'' \in \mathrm{Gal}(k(m)/H)$ such that $\rho_{E/H,m}(\sigma') = A$ and $\psi_{k,m}(\sigma'') = u$. By Lemmas 2.1 and 2.10, we have

$$\chi_{H,m}(\sigma'|_{H(\mu_m)}) = \det \rho_{E/H,m}(\sigma') = \det A = N(u) = N(\psi_{k,m}(\sigma'')) = \chi_{H,m}(\sigma''|_{H(\mu_m)}),$$

and thus $\sigma'|_{H(\mu_m)} = \sigma''|_{H(\mu_m)}$. By Lemma 2.13, $H(E[m]) \cap k(m) = H(\mu_m)$, so there exists a unique $\sigma \in \mathrm{Gal}(H(E[m])k(m)/H) = G(m)$ such that $\sigma|_{H(E[m])} = \sigma'$ and $\sigma|_{k(m)} = \sigma''$.

$$\Psi_m(\sigma) = \left(\rho_{E/H,m}(\sigma|_{H(E[m])}), \psi_{k,m}(\sigma|_{k(m)})\right) = \left(\rho_{E/H,m}(\sigma'), \psi_{k,m}(\sigma'')\right) = (A, u)$$ □

3. Frobenius conditions on $P_{E,k}$

3.1. **An upper bound.** Consider the following subset of $G(m)$, which is stable under conjugation:

$$C(m) := \left\{\sigma \in G(m) : \mathrm{tr}(\rho_{E/H,m}(\sigma|_{H(E[m])})) \in \mathrm{Tr}(\psi_{k,m}(\sigma|_{k(m)}))\right\}. \tag{3.1}$$

Lemma 3.1. *Let p be a prime where E has good ordinary reduction and $\mathbb{Q}(\pi_p(E)) \cong k$; then p splits completely in H. If $m \geq 5$ is an integer with $p \nmid m$, then $(\mathfrak{P}, L(m)/H) \subseteq C(m)$ for all $\mathfrak{P} \in \Sigma_H$ dividing p.*

Proof. To ease notation, let $k = \mathbb{Q}(\pi_p(E))$. Since $\pi_p(E)$ is a root of $x^2 - a_p(E)x + p$, we have $a_p(E) = \mathrm{Tr}_{k/\mathbb{Q}}(\pi_p(E))$ and $p = N_{k/\mathbb{Q}}(\pi_p(E))$. The equality $p = N_{k/\mathbb{Q}}(\pi_p(E))$ implies that p is either split or ramified in k, so

$$p\mathcal{O}_k = \mathfrak{p} \cdot \mathfrak{p}^\tau,$$

where $\mathfrak{p} = \pi_p(E)\mathcal{O}_k$ and τ is the non-trivial automorphism of k. If p is ramified in k, then

$$a_p(E) = \mathrm{Tr}_{k/\mathbb{Q}}(\pi_p(E)) = \pi_p(E) + \pi_p(E)^\tau \in \mathfrak{p} + \mathfrak{p}^\tau = \mathfrak{p}.$$

Hence $a_p(E) \equiv 0 \pmod{p}$, contradicting our assumption that E had ordinary reduction at p. Therefore, p splits in k. Since $\mathfrak{p}$ and $\mathfrak{p}^\tau$ are principal ideals in $\mathcal{O}_k$, the prime p splits completely in H.

Fix an $m \geq 5$ relatively prime to p. Take any $\mathfrak{P} \in \Sigma_H$ dividing p. From above, there is a $\pi \in \{\pi_p(E), \pi_p(E)^\tau\}$ which generates $\mathfrak{P} \cap \mathcal{O}_k$. Since p splits completely in H we have $\mathcal{O}_H/\mathfrak{P} = \mathbb{Z}/p\mathbb{Z}$. Thus $N(\mathfrak{P}) = p$ and

$$a_{\mathfrak{P}}(E) = |E_{\mathfrak{P}}(\mathcal{O}_H/\mathfrak{P})| - (N(\mathfrak{P}) + 1) = |E_p(\mathbb{Z}/p\mathbb{Z})| - (p+1) = a_p(E).$$

By Lemma 2.11,

$$\mathrm{Tr}_{k/\mathbb{Q}}(\pi) \pmod{m} \in \mathrm{Tr}(\psi_{k,m}(\mathrm{Frob}_{\mathfrak{P}})).$$

Since $\mathrm{tr}(\rho_{E/H,m}(\mathrm{Frob}_{\mathfrak{P}})) \equiv a_{\mathfrak{P}}(E) = a_p(E) = \mathrm{Tr}_{k/\mathbb{Q}}(\pi) \pmod{m}$,

$$\mathrm{tr}(\rho_{E/H,m}(\mathrm{Frob}_{\mathfrak{P}})) \in \mathrm{Tr}(\psi_{k,m}(\mathrm{Frob}_{\mathfrak{P}})).$$

Therefore, $(\mathfrak{P}, L(m)/H) \subseteq C(m)$ as desired. □

Definition 3.2. 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

$$\pi_C(x, L/K) = \#\{\mathfrak{p} \in \Sigma_K(x) : \mathfrak{p} \text{ unramified in } L, \text{ and } (\mathfrak{p}, L/K) \subseteq C\}.$$

Proposition 3.3. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let k be an imaginary quadratic extension of $\mathbb{Q}$. Fix an integer $m \geq 5$. Then*

$$P_{E,k}(x) \leq \frac{1}{2h_k}\pi_{C(m)}(x, L(m)/H) + \nu(m),$$

where $C(m) \subseteq G(m)$ is defined as in (3.1), and $L(m)$ is defined as in §2.3.

Proof. Let $p \leq x$ be a prime relatively prime to m such that E has good ordinary reduction at p and $\mathbb{Q}(\pi_p(E)) \cong k$ (equivalently $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong k$).

Lemma 3.1 shows that p splits completely in H and hence $p\mathcal{O}_H$ factors into $[H : \mathbb{Q}] = 2h_k$ distinct prime ideals $\mathfrak{P} \in \Sigma_H$ all of norm p. Given any such $\mathfrak{P} \in \Sigma_H$, we have $(\mathfrak{P}, L(m)/H) \subseteq C(m)$. Therefore

$$\#\{p \leq x : p \nmid mN_E, \mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong k\} \leq \frac{1}{2h_k}\pi_{C(m)}(x, L(m)/H),$$

and hence $P_{E,k}(x) \leq \frac{1}{2h_k}\pi_{C(m)}(x, L(m)/H) + \nu(m)$ by including the primes which divide m. □

3.2. **Cardinality of conjugacy classes.** In order to use the Chebotarev density theorem to estimate $P_{E,k}(x)$ (via Proposition 3.3), we need estimates on $|C(m)|$ and $|C(m)|/|G(m)|$. We limit ourselves to the case where m is prime. Though one could compute these values exactly, we will be satisfied with upper bounds. Let χ be the Kronecker character of the field k.

Lemma 3.4. *Let $\ell \geq 5$ be a prime that is unramified in k, then*

$$|\mathscr{G}(\ell)| = \ell(\ell-1)^2(\ell+1)(\ell-\chi(\ell))/w_k,$$

where $\mathscr{G}(\ell)$ is defined as in §2.3.

Proof. Since ℓ is unramified in k (and hence also in H), the character $\chi_{H,\ell}\colon \operatorname{Gal}(H(\mu_\ell)/H) \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ is surjective. Therefore by Lemma 2.10, the homomorphism $N\colon (\mathcal{O}_k/\ell\mathcal{O}_k)^\times/\mathcal{O}_k^\times \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ is surjective. The homomorphism $\det\colon \operatorname{Aut}(E[\ell]) \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ is also surjective.

$$|\mathscr{G}(\ell)| = \frac{|\operatorname{Aut}(E[\ell])| \cdot |(\mathcal{O}_k/\ell\mathcal{O}_k)^\times/\mathcal{O}_k^\times|}{|(\mathbb{Z}/\ell\mathbb{Z})^\times|} = \ell(\ell^2-1)|(\mathcal{O}_k/\ell\mathcal{O}_k)^\times|/w_k$$

The lemma follows by noting that $|(\mathcal{O}_k/\ell\mathcal{O}_k)^\times| = (\ell-1)(\ell-\chi(\ell))$. □

Lemma 3.5. *Suppose ℓ is a rational prime unramified in k. For any $t \in \mathbb{Z}/\ell\mathbb{Z}$ and $d \in (\mathbb{Z}/\ell\mathbb{Z})^\times$,*

$$\#\{u \in (\mathcal{O}_k/\ell\mathcal{O}_k)^\times : N(u) = d, \operatorname{Tr}(u) = t\} \leq 4.$$

Proof. Suppose that $u \in (\mathcal{O}_k/\ell\mathcal{O}_k)^\times$ satisfies $N(u) = d$ and $\operatorname{Tr}(u) = t$. Then u is a root of the polynomial $f(x) = x^2 - tx + d \in \mathbb{Z}/\ell\mathbb{Z}[x]$.

- If ℓ is inert in k, then $\mathcal{O}_k/\ell\mathcal{O}_k$ is a field. Therefore $f(x) = 0$ has at most two roots in $\mathcal{O}_k/\ell\mathcal{O}_k$.
- If ℓ splits in k, then there is a ring isomorphism $\mathcal{O}_k/\ell\mathcal{O}_k \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. So $f(x) = 0$ has at most four roots in $\mathcal{O}_k/\ell\mathcal{O}_k$. □

Lemma 3.6. *Let $\ell \geq 5$ be a prime that is unramified in k.*

(i) *Then*

$$[L(\ell) : H] = |G(\ell)| \leq \ell(\ell-1)^2(\ell+1)(\ell-\chi(\ell))/w_k,$$

with equality holding if $\rho_{E/H,\ell}$ is an isomorphism.

(ii) *If $\rho_{E/H,\ell}$ is an isomorphism, then*

$$|C(\ell)| \ll \ell^4 \quad \text{and} \quad \frac{|C(\ell)|}{|G(\ell)|} \ll \frac{1}{\ell}.$$

Proof.

(i) The map Ψ_ℓ is always injective, so $[L(\ell) : H] = |G(\ell)| \leq |\mathscr{G}(\ell)|$. If $\rho_{E/H,\ell}$ is an isomorphism then Ψ_ℓ is an isomorphism by Lemma 2.14, so $[L(\ell) : H] = |G(\ell)| = |\mathscr{G}(\ell)|$. Part (i) now follows from Lemma 3.4.

(ii) By Lemma 2.14, $\Psi_\ell\colon G(\ell) \to \mathscr{G}(\ell)$ is an isomorphism and hence

$$\Psi_\ell(C(\ell)) = \{(A,u) \in \mathscr{G}(\ell) : \operatorname{tr}(A) \in \operatorname{Tr}(u)\}.$$

$$\begin{aligned}|C(\ell)| &= \#\{(A,u) \in \mathscr{G}(\ell) : \operatorname{tr}(A) \in \operatorname{Tr}(u)\}\\ &= \#\{(A,u) \in \operatorname{Aut}(E[\ell]) \times \left((\mathcal{O}_k/\ell\mathcal{O}_k)^\times/\mathcal{O}_k^\times\right) : \det(A) = N(u), \operatorname{tr}(A) \in \operatorname{Tr}(u)\}\\ &\leq \#\{(A,u) \in \operatorname{Aut}(E[\ell]) \times (\mathcal{O}_k/\ell\mathcal{O}_k)^\times : \det(A) = N(u), \operatorname{tr}(A) = \operatorname{Tr}(u)\}\end{aligned}$$

By Lemma 3.5,

$$|C(\ell)| \leq 4 \cdot |\operatorname{Aut}(E[\ell])| \leq 4\ell^4.$$

Using $w_k \leq 6$ and our formula for $|G(\ell)|$ from part (i), we have $1/|G(\ell)| \ll 1/\ell^5$. Therefore, $|C(\ell)|/|G(\ell)| \ll \ell^4/\ell^5 = 1/\ell$. □

3.3. **A zero density result.**

We now give a simple consequence of the work done so far.

Proposition 3.7. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$, and let k be an imaginary quadratic extension of $\mathbb{Q}$. Then*

$$\lim_{x\to\infty} \frac{P_{E,k}(x)}{\pi(x)} = 0.$$

In other words, the set of primes p such that $\operatorname{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong k$ has natural density zero.

Proof. Consider any prime $\ell \geq 5$ such that ℓ is unramified in k and $\rho_{E/H,\ell}$ is an isomorphism. By Lemma 2.5, these conditions will be true for all ℓ sufficiently large. By Proposition 3.3 and the Chebotarev density theorem, $\limsup_{x\to\infty} P_{E,k}(x)/\pi(x) \leq \frac{1}{2h_k}|C(\ell)|/|G(\ell)|$. By Lemma 3.6, $\limsup_{x\to\infty} P_{E,k}(x)/\pi(x) \ll \frac{1}{2h_k\ell}$. Since this holds for all sufficiently large primes ℓ, we deduce that $\limsup_{x\to\infty} P_{E,k}(x)/\pi(x) = 0$. □

Theorem 1.3 gives an effective version of Proposition 3.7. In order to prove the theorem we will need effective versions of the Chebotarev density theorem.

4. Effective Chebotarev density theorems

Let L/K be a Galois extension of number fields with Galois group G. Let C be a subset of G stable under conjugation. Recall from Definition 3.2 that

$$\pi_C(x, L/K) = \#\{\mathfrak{p} \in \Sigma_K(x) : \mathfrak{p} \text{ unramified in } L, \text{ and } (\mathfrak{p}, L/K) \subseteq C\}.$$

The Chebotarev density theorem says that as $x \to \infty$,

$$\pi_C(x, L/K) = \frac{|C|}{|G|}\operatorname{Li} x + o\Big(\frac{x}{\log x}\Big).$$

An effective version would give an explicit error term.

The extension L/K is said to satisfy *Artin's Holomorphy Conjecture* (AHC) if for each non-trivial irreducible representation ρ of G, the Artin L-series $L(s,\rho)$ has analytic continuation to the whole complex plane. The *Generalized Riemann Hypothesis* (GRH) asserts that the Dedekind zeta function of any number field has no zeros with real part $> 1/2$.

4.1. The constant $M(L/K)$.

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

$$P(L/K) := \{p : \text{there exists a } \mathfrak{p} \in \Sigma_K \text{ such that } \mathfrak{p}|p \text{ and } \mathfrak{p} \text{ is ramified in } L\}.$$

Lemma 4.1. *Let $K \subseteq F \subseteq L$ be number fields, then $M(F/K) \leq M(L/K)$.*

Proof. This is immediate from $[F:K] \leq [L:K]$ and $P(F/K) \subseteq P(L/K)$. □

4.2. Conditional versions of the Chebotarev density theorem.

Proposition 4.2. *Let L/K be a Galois extension of number fields with Galois group G. Let C be a subset of G stable under conjugation, and let H be a normal subgroup of G such that $HC \subseteq C$.*

(i) *Suppose that GRH holds. Then*

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

(ii) *Suppose that GRH holds and that AHC is true for the extension L^H/K. Then*

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

Proof.

(i) The $H = 1$ case is a consequence of Remark 3 following [Ser81, Théorème 4].

Now suppose $H \neq 1$, and let $\overline{C}$ be the image of C in $G/H = \operatorname{Gal}(L^H/K)$. The inclusion $HC \subseteq C$ (which is equivalent to $HC = C$) implies that $|\overline{C}| = |C|/|H|$.

Let $\mathfrak{p} \in \Sigma_K$ be a prime ideal unramified in L. Choose any $\mathfrak{P} \in \Sigma_L$ dividing $\mathfrak{p}$. The equality $HC = C$ implies that $(\mathfrak{P}, L/K) \in C$ if and only if $(\mathfrak{P} \cap \mathcal{O}_{L^H}, L^H/K) = (\mathfrak{P}, L/K) \cdot H \in \overline{C}$. Therefore $(\mathfrak{p}, L/K) \subseteq C$ if and only if $(\mathfrak{p}, L^H/K) \subseteq \overline{C}$. We deduce that

$$\pi_{\overline{C}}(x, L^H/K) = \pi_C(x, L/K) + O([K:\mathbb{Q}]|P(L/K)|),$$

where the error term bounds the number of prime ideals in Σ_K which are ramified in L and unramified in L^H. By the case already done and Lemma 4.1,

$$\begin{aligned}\pi_{\overline{C}}(x, L^H/K) &= \frac{|\overline{C}|}{|G/H|}\operatorname{Li} x + O\Big(|\overline{C}| x^{1/2}[K:\mathbb{Q}]\log\Big(M(L^H/K)x\Big)\Big)\\ &= \frac{|C|}{|G|}\operatorname{Li} x + O\Big(\frac{|C|}{|H|} x^{1/2}[K:\mathbb{Q}]\log\Big(M(L/K)x\Big)\Big)\end{aligned}$$

and hence

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

The desired error term follows by noting that $|C|/|H| \geq 1$ (unless $C = \emptyset$, in which case the proposition is trivial), and $|P(L/K)| \leq 2\log(\prod_{p \in P(L/K)} p) \leq 2\log M(L/K)$.

(ii) See [MMS88, Proposition 3.12]. □

Remark 4.3. Artin's Holomorphy Conjecture is known for abelian extensions, because in that case Artin L-functions are also Hecke L-functions which are known to have the desired analytic continuation. We will later apply Proposition 4.2(ii) in the case where G/H is an abelian group, and hence the resulting estimate will be conditional only upon GRH.

4.3. Unconditional versions of the Chebotarev density theorem.

Lemma 4.4. *Let L be a number field. If $L = \mathbb{Q}$, then $\zeta(s) = \zeta_{\mathbb{Q}}(s)$ has no zeros in the real interval $1/2 \leq \sigma \leq 1$. If $L \neq \mathbb{Q}$, then the Dedekind zeta function $\zeta_L(s)$ has at most one zero in the real interval, $1 - (4\log d_L)^{-1} \leq \sigma \leq 1$.*

Proof. See [Sta74, Lemma 3]. □

Definition 4.5. If the exceptional zero of Lemma 4.4 exists, then we will denote in by β_L.

Proposition 4.6. *Let L/K be a Galois extension of number fields with Galois group G. Let C be a subset of G stable under conjugation, and let $||C||$ be the number of conjugacy classes of G contained in C.*

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

$$\Big|\pi_C(x, L/K) - \frac{|C|}{|G|}\operatorname{Li} x\Big| \leq \frac{|C|}{|G|}\operatorname{Li}(x^{\beta_L}) + O\Big(||C||\, x\exp\Big(-c\sqrt{\frac{\log x}{[L:\mathbb{Q}]}}\Big)\Big),$$

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

Proof. See [LO77, Theorem 1.3]. □

Proposition 4.7. *Let L/K be a Galois extension of number fields with Galois group G. Let C be a subset of G stable under conjugation, and suppose H is a normal subgroup of G such that*

G/H is abelian and $HC \subseteq C$. There are absolute constants $b, c > 0$ such that if $\log x \geq b[K : \mathbb{Q}](\log M(L/K))^2$, then

$$\Big|\pi_C(x, L/K) - \frac{|C|}{|G|}\operatorname{Li} x\Big| \leq \frac{|C|}{|G|}\operatorname{Li}(x^{\beta_L}) + O\Big(\Big(\frac{|C|}{|H|}\Big)^{1/2}[K:\mathbb{Q}]x\exp\Big(-c\sqrt{\frac{\log x}{[K:\mathbb{Q}]}}\Big)(\log(M(L/K)x))^2\Big),$$

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

Proof. This follows from [Mur97, Theorem 4.6], though see Remark 4.8. We have assumed that G/H is abelian, so one can show (in the notation of [Mur97]) that $d_{G/H} = 1$ and $|\chi_{G/H}(\overline{C})| \leq |\overline{C}| = |C|/|H|$. □

Remark 4.8. Proposition 4.7 is a special case of [Mur97, Theorem 4.6], which treats the case where AHC holds for all characters of the Galois group G/H (which need not be abelian). It also gives a more precise dependence on the exception zero than we have (we will make use of only the trivial bound $\beta_L \leq 1$ in our application). Unfortunately, due to some printing problems a few typos were introduced into the published version of [Mur97]; in particular $|D|^{1/2}/|H|$ should be replaced by $(|D|/|H|)^{1/2}$ in [Mur97, Theorem 4.6].

4.4. **The function $\widetilde{\pi}_C(x, L/K)$.** Let L/K be a Galois extension of number fields with Galois group G. For each prime ideal $\mathfrak{p} \in \Sigma_K$, choose any $\mathfrak{P} \in \Sigma_L$ dividing $\mathfrak{p}$. We then have a distinguished Frobenius element $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}/I_{\mathfrak{P}}$, where $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ are the decomposition and inertia subgroups of G at $\mathfrak{P}$. Let φ be a class function on G. For $m \geq 1$, define

$$\varphi(\operatorname{Frob}_{\mathfrak{p}}^m) := \frac{1}{|I_{\mathfrak{P}}|}\sum_{\substack{g \in D_{\mathfrak{P}} \\ gI_{\mathfrak{P}} = \sigma_{\mathfrak{P}}^m \in D_{\mathfrak{P}}/I_{\mathfrak{P}}}} \varphi(g).$$

As the notation suggests, the value of $\varphi(\operatorname{Frob}_{\mathfrak{p}}^m)$ is independent of the choice of $\mathfrak{P} \in \Sigma_L$. For $\mathfrak{p}$ unramified in L, this definition agrees with the value of φ on the conjugacy class $\operatorname{Frob}_{\mathfrak{p}}^m$ of G. Define

$$\pi_\varphi(x) := \sum_{\substack{\mathfrak{p} \in \Sigma_K \text{ unramified in } L \\ N(\mathfrak{p}) \leq x}} \varphi(\operatorname{Frob}_{\mathfrak{p}}) \quad \text{and} \quad \widetilde{\pi}_\varphi(x) := \sum_{\substack{\mathfrak{p} \in \Sigma_K, m \geq 1 \\ N(\mathfrak{p}^m) \leq x}} \frac{1}{m}\varphi(\operatorname{Frob}_{\mathfrak{p}}^m).$$

Definition 4.9. Let L/K be a Galois extension of number fields with Galois group G. Let C be a subset of G stable under conjugation, and let $\delta_C \colon G \to \{0, 1\}$ be the characteristic function of C. Define $\widetilde{\pi}_C(x, L/K) := \widetilde{\pi}_{\delta_C}(x)$.

Fix a finite group G and an element $s \in G$. Let $C_G(s)$ be the conjugacy class of G containing s, and let $\operatorname{Cent}_G(s)$ be the centralizer (i.e., the group of $g \in G$ such that $gsg^{-1} = s$). The orbit-stabilizer formula gives $|C_G(s)| = |G|/|\operatorname{Cent}_G(s)|$.

Let H be a subgroup of G, and suppose that φ is a class function of H. The *induced* class function on G is defined by $(\operatorname{Ind}_H^G \varphi)(g) = \frac{1}{|H|}\sum_{t \in G,\, t^{-1}gt \in H} \varphi(t^{-1}gt)$.

Proposition 4.10. *Let L/K be a Galois extension of number fields with Galois group G, and let H be a subgroup of G.*

(i) *For any class function φ of H,*

$$\widetilde{\pi}_{\operatorname{Ind}_H^G \varphi}(x) = \widetilde{\pi}_\varphi(x).$$

(ii) *For any $s \in H$,*

$$\widetilde{\pi}_{C_H(s)}(x, L/L^H) = [\operatorname{Cent}_G(s) : \operatorname{Cent}_H(s)] \cdot \widetilde{\pi}_{C_G(s)}(x, L/K).$$

Proof.

(i) See [Ser81, Proposition 8(a)].

(ii) Let $\delta_{C_H(s)}\colon H \to \{0,1\}$ and $\delta_{C_G(s)}\colon G \to \{0,1\}$ be the characteristic functions of $C_H(s)$ and $C_G(s)$ respectively. One can check that $\operatorname{Ind}_H^G \delta_{C_H(s)} = \lambda \cdot \delta_{C_G(s)}$ for some λ. Thus using part (i),

$$\widetilde{\pi}_{C_H(s)}(x, L/L^H) = \widetilde{\pi}_{\delta_{C_H(s)}}(x) = \widetilde{\pi}_{\operatorname{Ind}_H^G \delta_{C_H(s)}}(x) = \lambda \cdot \widetilde{\pi}_{\delta_{C_G(s)}}(x) = \lambda \cdot \widetilde{\pi}_{C_G(s)}(x, L/K).$$

To compute λ, we use Frobenius reciprocity (see [Ser77, Theorem 13]).

$$\begin{aligned} \frac{\lambda}{|\operatorname{Cent}_G(s)|} &= \lambda \frac{|C_G(s)|}{|G|} \\ &= \left\langle \lambda \cdot \delta_{C_G(s)}, 1_G \right\rangle_G \\ &= \left\langle \operatorname{Ind}_H^G \delta_{C_H(s)}, 1_G \right\rangle_G \\ &= \left\langle \delta_{C_H(s)}, 1_H \right\rangle_H = \frac{|C_H(s)|}{|H|} = \frac{1}{|\operatorname{Cent}_H(s)|} \end{aligned}$$ □

The next proposition bounds the difference between $\widetilde{\pi}_C(x, L/K)$ and $\pi_C(x, L/K)$.

Proposition 4.11. *Let L/K be a Galois extension of number fields with Galois group G.*

(i) *Let φ be a class function of G, and define $||\varphi|| = \sup_{s\in G} |\varphi(s)|$. Then*

$$\widetilde{\pi}_\varphi(x) - \pi_\varphi(x) \ll ||\varphi|| \left(\frac{1}{[L:K]} \log d_L + [K:\mathbb{Q}] x^{1/2} \right).$$

(ii) *If C is a subset of G stable under conjugation, then*

$$\widetilde{\pi}_C(x, L/K) - \pi_C(x, L/K) \ll [K:\mathbb{Q}] \Big(\frac{1}{[L:\mathbb{Q}]} \log d_L + x^{1/2} \Big).$$

Proof. Part (i) is [Ser81, Proposition 7]. Part (ii) follows from (i) by letting φ be the characteristic function of C. □

5. Preliminary bounds

Throughout this section we fix a non-CM elliptic curve E defined over $\mathbb{Q}$ and an imaginary quadratic extension $k/\mathbb{Q}$.

In §5.1 and §5.2, we give some bounds that will show up in our proofs. In §5.3, which is not needed for the rest of the paper, we use an effective Chebotarev density theorem to prove (under GRH) that

$$P_{E,k}(x) \ll_E \frac{1}{h_k^{3/4}} \frac{x^{7/8}}{(\log x)^{1/2}} + x^{1/2} (\log x)^4.$$

The reason for proving this bound (which is usually weaker than Theorem 1.3) is to illustrate the basic principle of the proof without the extra group theory calculations of §6.

5.1. Trivial $P_{E,k}(x)$ bound.

The following easy lemma shows that for a fixed k, the function $P_{E,k}(x)$ vanishes for small x.

Lemma 5.1. *If $d_k > 4x$, then $P_{E,k}(x) = 0$.*

Proof. Suppose $p \le x$ is a prime such that $\mathbb{Q}(\pi_p(E)) \cong k$. Thus $\mathbb{Q}(\sqrt{a_p(E)^2 - 4p}) = \mathbb{Q}(\sqrt{-d_k})$, and one shows that $-d_k$ divides $a_p(E)^2 - 4p$ (the divisibility with respect to the prime 2 follows from $a_p(E)^2 - 4p$ being congruent to 0 or 1 modulo 4). Therefore, $d_k \le 4p - a_p(E)^2 \le 4x$. □

5.2. A bound on $\log M(L/K)$.

Lemma 5.2. *For a finite extension L/K of number fields,*

$$\frac{1}{[L:\mathbb{Q}]}\log d_L \leq \frac{1}{[K:\mathbb{Q}]}\log d_K + \Big(1-\frac{1}{[L:K]}\Big)\sum_{p\in P(L/K)}\log p + |P(L/K)|\log[L:K].$$

Proof. See [Ser81, Proposition 4´]. □

Lemma 5.3. *Let $\ell \geq 5$ be a prime that is unramified in k, and let K be a field such that $H \subseteq K \subseteq L(\ell)$. Then $\frac{1}{[K:\mathbb{Q}]}\log d_K \ll_E \log(\ell d_k^{1/2})$.*

Proof. We first use Lemma 5.2 and the inclusions $P(K/H) \subseteq P(L(\ell)/H) \subseteq \{\ell\}\cup\{p : p|N_E\}$.

$$\begin{aligned}\frac{1}{[K:\mathbb{Q}]}\log d_K &\leq \frac{1}{[H:\mathbb{Q}]}\log d_H + \sum_{p\in P(K/H)}\log p + |P(K/H)|\log[K:H]\\ &\leq \frac{1}{[H:\mathbb{Q}]}\log d_H + \log(\ell N_E) + (\nu(N_E)+1)\log[L(\ell):H]\end{aligned}$$

From Lemma 5.2 and $P(H/k)=\emptyset$, we have $\frac{1}{[H:\mathbb{Q}]}\log d_H \leq \frac{1}{[k:\mathbb{Q}]}\log d_k = \frac{1}{2}\log d_k$. By Lemma 3.6, $[L(\ell):H] \leq \ell^5$. We now combine these facts with the previous inequality to obtain

$$\begin{aligned}\frac{1}{[K:\mathbb{Q}]}\log d_K &\leq \frac{1}{2}\log d_k + \log(\ell N_E) + (\nu(N_E)+1)\log(\ell^5)\\ &\ll_E \frac{1}{2}\log d_k + \log(\ell) = \log(\ell d_k^{1/2}).\end{aligned}$$ □

Lemma 5.4. *Let $\ell \geq 5$ be a prime that is unramified in k. Let K and L be Galois extensions of H such that $H \subseteq K \subseteq L \subseteq L(\ell)$. Then $\log M(L/K) \ll_E \log(\ell d_k^{1/2})$.*

Proof. By the definition of $M(L/K)$, $\log M(L/K) = \log[L:K] + \frac{1}{[K:\mathbb{Q}]}\log d_K + \sum_{p\in P(L/K)}\log p$. By Lemma 3.6 we have $[L(\ell):H] \leq \ell^5$, by Lemma 5.3 we have $\frac{1}{[K:\mathbb{Q}]}\log d_K \ll_E \log(\ell d_k^{1/2})$, and since $P(L/K) \subseteq P(L(\ell)/H)$ we have $\sum_{p\in P(L/K)}\log p \leq \log(\ell N_E)$. Therefore, $\log M(L/K) \ll_E \log(\ell d_k^{1/2})$ as desired. □

5.3. A quick bound on $P_{E,k}(x)$.

We may assume that $d_k \leq 4x$ (otherwise by Lemma 5.1, $P_{E,k}(x)=0$, and our final bounds will be vacuously true).

Fix a prime $\ell \geq 5$ such that ℓ is unramified in k and $\rho_{E/H,\ell}$ is an isomorphism; we will make a specific choice of ℓ later. There is an injective homomorphism

$$i\colon (\mathbb{Z}/\ell\mathbb{Z})^\times \hookrightarrow \mathscr{G}(\ell), \quad a \mapsto \big(a\cdot I, a\big).$$

The image $i((\mathbb{Z}/\ell\mathbb{Z})^\times)$ lies in the center of $\mathscr{G}(\ell)$ and hence is a normal subgroup of $\mathscr{G}(\ell)$. Let $\mathscr{H}(\ell)$ be the corresponding normal subgroup of $G(\ell)$ under the isomorphism $\Psi_\ell\colon G(\ell) \xrightarrow{\sim} \mathscr{G}(\ell)$. We find that

$$\mathscr{H}(\ell)C(\ell) \subseteq C(\ell),$$

since the trace maps $\mathrm{tr}\colon \mathrm{Aut}(E[\ell]) \to \mathbb{Z}/\ell\mathbb{Z}$ and $\mathrm{Tr}\colon \big(\mathcal{O}_k/\ell\mathcal{O}_k\big)^\times \to \mathbb{Z}/\ell\mathbb{Z}$ commute with multiplication by elements of $(\mathbb{Z}/\ell\mathbb{Z})^\times$. By Proposition 3.3, $P_{E,k}(x) \leq \frac{1}{2h_k}\pi_{C(\ell)}(x, L(\ell)/H) + 1$. Assuming GRH, by the Chebotarev density theorem (Proposition 4.2(i)),

$$P_{E,k}(x) \leq \frac{1}{2h_k}\Big(\frac{|C(\ell)|}{|G(\ell)|}\operatorname{Li}x + O\Big(\frac{|C(\ell)|}{|\mathscr{H}(\ell)|}x^{1/2}[H:\mathbb{Q}]\log\Big(M(L(\ell)/H)x\Big)\Big)\Big) + 1.$$

Using Lemma 3.6 and Lemma 5.4,

$$P_{E,k}(x) \ll_E \frac{1}{2h_k}\frac{1}{\ell}\frac{x}{\log x} + \ell^3 x^{1/2} \log\Big(\ell d_k^{1/2} x\Big). \tag{5.1}$$

Since $d_k \leq 4x$,

$$P_{E,k}(x) \ll_E \frac{1}{h_k}\frac{1}{\ell}\frac{x}{\log x} + \ell^3 x^{1/2} \log(\ell x). \tag{5.2}$$

We now need to choose a specific prime ℓ to minimize our bound. The expression $\frac{1}{h_k}\frac{1}{\ell}\frac{x}{\log x}$ (resp. $\ell^3 x^{1/2}\log(\ell x)$) is a decreasing (resp. increasing) function of ℓ. In order to achieve an optimal bound in (5.2), we want both terms to be of roughly the same magnitude. Thus we certainly want $\ell \ll x$, and hence hope to find ℓ with $\ell^4 \approx \frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}$.

Lemma 5.5. *There exists an absolute constant $\gamma \geq 5$ such that for any $y \geq \gamma$, if $y \geq 2\log d_k$ then the interval $[y, 2y]$ contains a prime not dividing d_k.*

Proof. By the prime number theorem, there is an absolute constant $\gamma \geq 5$ such that for $y \geq \gamma$, $\sum_{y \leq p \leq 2y} \log p > y/2$. Suppose $y \geq \gamma$ and all of the primes in the interval $[y, 2y]$ divide d_k. Then $\log d_k \geq \sum_{y\leq p\leq 2y} \log p > y/2$. Therefore, if $y \geq \gamma$ and $\log d_k \leq y/2$, then there exists a prime not dividing d_k in the interval $[y, 2y]$. □

We now break up our bound of $P_{E,k}(x)$ into two cases.

Case 1: Suppose $\left(\frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}\right)^{1/4} \geq \log(4x)$.

Let $y = 2\Big(\frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}\Big)^{1/4} + c_E + \gamma$, where c_E is the constant from Lemma 2.5 and γ is the constant from Lemma 5.5. Using our assumption $d_k \leq 4x$, we have $y \geq 2\log(4x) \geq 2\log d_k$. Therefore by Lemma 5.5, there exists a prime $\ell \nmid d_k$ in the interval $[y, 2y]$. Note that ℓ is unramified in k, $\ell \geq 5$, and $\rho_{E/H,\ell}$ is an isomorphism (since $\ell \geq c_E$). With this choice of ℓ, (5.2) becomes

$$\begin{aligned}
P_{E,k}(x) &\ll_E \frac{1}{h_k}\frac{1}{y}\frac{x}{\log x} + y^3 x^{1/2}\log x \\
&\ll_E \frac{1}{h_k}\Big(h_k\frac{(\log x)^2}{x^{1/2}}\Big)^{1/4}\frac{x}{\log x} + \Big(\frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}\Big)^{3/4} x^{1/2}\log x \\
&\ll \frac{1}{h_k^{3/4}}\frac{x^{7/8}}{(\log x)^{1/2}}.
\end{aligned}$$

Case 2: Suppose $\left(\frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}\right)^{1/4} \leq \log(4x)$.

Let $y = 2\log(4x) + c_E + \gamma$. Since $y \geq 2\log(4x) \geq 2\log d_k$, Lemma 5.5 tells us that there is a prime ℓ in the interval $[y, 2y]$. Note that ℓ is unramified in k, $\ell \geq 5$, and $\rho_{E/H,\ell}$ is an isomorphism (since $\ell \geq c_E$). With this choice of ℓ, (5.2) becomes

$$\begin{aligned}
P_{E,k}(x) &\ll_E \frac{1}{h_k}\frac{1}{y}\frac{x}{\log x} + y^3 x^{1/2}\log x \\
&\ll_E \frac{1}{h_k}\frac{x}{(\log x)^2} + x^{1/2}(\log x)^4 \\
&= x^{1/2}\Big(\frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}\Big) + x^{1/2}(\log x)^4 \\
&\ll x^{1/2}(\log x)^4 + x^{1/2}(\log x)^4 = 2x^{1/2}(\log x)^4.
\end{aligned}$$

We record the result obtained by combining the two cases.

Proposition 5.6. *Assuming GRH,* $P_{E,k}(x) \ll_E \frac{1}{h_k^{3/4}} \frac{x^{7/8}}{(\log x)^{1/2}} + x^{1/2}(\log x)^4$. □

Remark 5.7. Assume GRH and AHC. Proceeding as above, except using part (ii) of Proposition 4.2, we obtain

$$P_{E,k}(x) \ll_E \frac{1}{h_k}\frac{1}{\ell}\frac{x}{\log x} + \ell^{3/2}x^{1/2}\log(\ell d_k^{1/2}x).$$

This is precisely the statement of Lemma 6.3(i), except with the additional assumption that ℓ is split in k and *without* the AHC assumption. The main idea in §6 is to reduce the bounds to abelian extensions where AHC is known to hold.

6. The proof of Theorem 1.3

Fix a non-CM elliptic curve E defined over $\mathbb{Q}$ and an imaginary quadratic extension k of $\mathbb{Q}$. The following proof has clearly been motivated by the work of Murty, Murty, and Saradha [MMS88].

Let $\ell \geq 5$ be a prime such that ℓ *splits* in k and $\rho_{E/H,\ell}$ is an isomorphism. We will later make a more specific choice of ℓ.

6.1. Setup and a Frobenius condition.

Define the set

$$\mathscr{C}(\ell) = \{\sigma \in C(\ell) : \det(xI - \rho_{E/H,\ell}(\sigma|_{H(E[\ell])})) \text{ has a root in } \mathbb{Z}/\ell\mathbb{Z}\}, \tag{6.1}$$

where $C(\ell)$ was defined by (3.1). The set $\mathscr{C}(\ell)$ is stable under conjugation in $G(\ell)$. The next lemma gives a refinement of Proposition 3.3 in the case where $m = \ell$ is a prime that splits in k.

Lemma 6.1. *Fix a prime* $\ell \geq 5$ *that splits in* k *such that* $\rho_{E/H,\ell}$ *is an isomorphism. Then*

$$P_{E,k}(x) \leq \frac{1}{2h_k}\pi_{\mathscr{C}(\ell)}(x, L(\ell)/H) + 1.$$

Proof. Let $p \leq x$ be a prime such that E has good ordinary reduction at p and $\mathbb{Q}(\pi_p(E)) \cong k$. Suppose that $p \neq \ell$. Then Lemma 3.1 shows that p splits completely in H and for each $\mathfrak{P} \in \Sigma_H$ dividing p, $(\mathfrak{P}, L(\ell)/H) \subseteq C(\ell)$. For $\mathfrak{P} \in \Sigma_H$ dividing p, the polynomial

$$\det(xI - \rho_{E/H,\ell}(\mathrm{Frob}_{\mathfrak{P}})) \equiv x^2 - a_{\mathfrak{P}}(E)x + N(\mathfrak{P}) = x^2 - a_p(E)x + p \pmod{\ell}$$

has a root in $\mathbb{Z}/\ell\mathbb{Z}$, since by assumption ℓ splits in $k \cong \mathbb{Q}(\pi_p(E))$. Therefore, $(\mathfrak{P}, L(\ell)/H) \subseteq \mathscr{C}(\ell)$. So

$$\#\{p \leq x : p \nmid \ell N_E, \mathrm{End}_{\overline{\mathbb{F}}_p}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q} \cong k\} \leq \frac{1}{2h_k}\pi_{\mathscr{C}(\ell)}(x, L(\ell)/H)$$

and the lemma follows by including the prime ℓ. □

Choose a Borel subgroup B of $\mathrm{Aut}(E[\ell])$ (i.e., there is an isomorphism $\mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ under which B corresponds to the group of invertible upper triangular matrices). The following subgroup of $G(\ell)$ will play an important role in the proof:

$$\mathscr{B}(\ell) = \{\sigma \in G(\ell) : \rho_{E/H,\ell}(\sigma|_{H(E[\ell])}) \in B\}.$$

The inverse image of B under the map

$$G(\ell) \twoheadrightarrow \mathrm{Aut}(E[\ell]), \quad \sigma \mapsto \rho_{E/H,\ell}(\sigma|_{H(E[\ell])}),$$

is $\mathscr{B}(\ell)$. Thus $[G(\ell) : \mathscr{B}(\ell)] = [\mathrm{Aut}(E[\ell]) : B] = \ell + 1$, so

$$[L(\ell)^{\mathscr{B}(\ell)} : \mathbb{Q}] = 2h_k[L(\ell)^{\mathscr{B}(\ell)} : H] = 2h_k[G(\ell) : \mathscr{B}(\ell)] = 2h_k(\ell + 1). \tag{6.2}$$

Define the set

$$D := \mathscr{C}(\ell) \cap \mathscr{B}(\ell) = C(\ell) \cap \mathscr{B}(\ell).$$

Lemma 6.2. *Fix a prime $\ell \geq 5$ such that ℓ splits in k and $\rho_{E/H,\ell}$ is an isomorphism. Then*

$$P_{E,k}(x) \leq \frac{1}{2h_k}\pi_D(x, L(\ell)/L(\ell)^{\mathscr{B}(\ell)}) + O_E\Big(\ell \log(\ell d_k^{1/2}) + \ell x^{1/2}\Big).$$

Proof. Any element of $\mathscr{C}(\ell)$ is conjugate in $G(\ell)$ to an element of $\mathscr{B}(\ell)$. Choose a subset $\Gamma \subseteq \mathscr{B}(\ell)$ such that there is a *disjoint* union

$$\mathscr{C}(\ell) = \bigcup_{\gamma\in\Gamma} C_{G(\ell)}(\gamma)$$

(recall that for a group G and an element $s \in G$, $C_G(s)$ is the conjugacy class of s in G). Thus

$$\pi_{\mathscr{C}(\ell)}(x, L(\ell)/H) \leq \widetilde{\pi}_{\mathscr{C}(\ell)}(x, L(\ell)/H) = \sum_{\gamma\in\Gamma} \widetilde{\pi}_{C_{G(\ell)}(\gamma)}(x, L(\ell)/H),$$

and by Proposition 4.10 (with $G = G(\ell)$, $H = \mathscr{B}(\ell)$, $L = L(\ell)$),

$$\begin{aligned}\pi_{\mathscr{C}(\ell)}(x, L(\ell)/H) &\leq \sum_{\gamma\in\Gamma} [\mathrm{Cent}_{G(\ell)}(\gamma) : \mathrm{Cent}_{\mathscr{B}(\ell)}(\gamma)]^{-1} \cdot \widetilde{\pi}_{C_{\mathscr{B}(\ell)}(\gamma)}(x, L(\ell)/L(\ell)^{\mathscr{B}(\ell)}) \\ &\leq \sum_{\gamma\in\Gamma} \widetilde{\pi}_{C_{\mathscr{B}(\ell)}(\gamma)}(x, L(\ell)/L(\ell)^{\mathscr{B}(\ell)}) \leq \widetilde{\pi}_D(x, L(\ell)/L(\ell)^{\mathscr{B}(\ell)}).\end{aligned}$$

So by Proposition 4.11(ii),

$$\pi_{\mathscr{C}(\ell)}(x, L(\ell)/H) \leq \pi_D(x, L(\ell)/L(\ell)^{\mathscr{B}(\ell)}) + O\Big([L(\ell)^{\mathscr{B}(\ell)} : \mathbb{Q}]\Big(\frac{1}{[L(\ell) : \mathbb{Q}]}\log d_{L(\ell)} + x^{1/2}\Big)\Big).$$

Lemma 5.3 gives $\frac{1}{[L(\ell):\mathbb{Q}]}\log d_{L(\ell)} \ll_E \log(\ell d_k^{1/2})$. This and (6.2) gives

$$\pi_{\mathscr{C}(\ell)}(x, L(\ell)/H) \leq \pi_D(x, L(\ell)/L(\ell)^{\mathscr{B}(\ell)}) + O_E(2h_k(\ell+1)(\log(\ell d_k^{1/2}) + x^{1/2})).$$

The lemma then follows from Lemma 6.1. □

We now apply our effective versions of the Chebotarev density theorem.

Lemma 6.3. *Fix a prime $\ell \geq 5$ such that ℓ splits in k and $\rho_{E/H,\ell}$ is an isomorphism.*

(i) *Assuming GRH,*

$$P_{E,k}(x) \ll_E \frac{1}{h_k\ell}\frac{x}{\log x} + \ell^{3/2}x^{1/2}\log(\ell d_k^{1/2}x).$$

(ii) *Unconditionally, there is an absolute constant $c_1 > 0$ and a constant $c_2 > 0$ depending on E such that if $\log x \geq c_2 h_k \ell \Big(\log(h_k\ell)\Big)^2$, then*

$$P_{E,k}(x) \ll_E \frac{1}{h_k\ell}\frac{x}{\log x} + \ell^{3/2}x\exp\Big(-c_1\sqrt{\frac{\log x}{h_k\ell}}\Big)(\log(h_k\ell x))^2.$$

Proof. Let us make things a little more explicit. Fix a group isomorphism $\alpha\colon \mathrm{Aut}(E[\ell]) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that B maps onto the group of invertible upper triangular matrices. This induces an isomorphism

$$\begin{aligned}\Psi_{\alpha,\ell}\colon G(\ell) &\xrightarrow{\sim} \{(A, u) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \big((\mathcal{O}_k/\ell\mathcal{O}_k)^\times/\mathcal{O}_k^\times\big) : \det(A) = N(u)\} \\ \sigma &\mapsto \Big(\alpha\big(\rho_{E/H,\ell}(\sigma|_{H(E[\ell])})\big)), \psi_{k,\ell}(\sigma|_{k(\ell)})\Big).\end{aligned}$$

That $\Psi_{\alpha,\ell}$ is a well-defined isomorphism is a consequence of Ψ_ℓ being an isomorphism (Lemma 2.14). Therefore,

$$\Psi_{\alpha,\ell}(\mathscr{B}(\ell)) = \{(A, u) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \big((\mathcal{O}_k/\ell\mathcal{O}_k)^\times/\mathcal{O}_k^\times\big) : \det(A) = N(u),\ A \text{ upper triangular}\}.$$

Consider the following subgroup of $\mathscr{B}(\ell)$,

$$\mathscr{H} = \Psi_{\alpha,\ell}^{-1}\Big\{\Big(\big(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\big), (a+\ell\mathcal{O}_k)\mathcal{O}_k^\times\Big) : a \in (\mathbb{Z}/\ell\mathbb{Z})^\times, b \in \mathbb{Z}/\ell\mathbb{Z}\Big\}.$$

The homomorphism

$$\Psi_{\alpha,\ell}(\mathscr{B}(\ell)) \to (\mathbb{Z}/\ell\mathbb{Z})^\times \times \big((\mathcal{O}_k/\ell\mathcal{O}_k)^\times/\mathcal{O}_k^\times\big), \qquad \Big(\big(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\big), u\Big) \mapsto (a^{-1}c, a^{-1}u)$$

has kernel $\Psi_{\alpha,\ell}(\mathscr{H})$. Therefore $\mathscr{H}$ is a normal subgroup of $\mathscr{B}(\ell)$, and the quotient $\mathscr{B}(\ell)/\mathscr{H}$ is abelian. Since the group $\mathrm{Gal}(L(\ell)^{\mathscr{H}}/L(\ell)^{\mathscr{B}(\ell)}) = \mathscr{B}(\ell)/\mathscr{H}$ is abelian, Artin's Holomorphy Conjecture is known to hold for the extension $L(\ell)^{\mathscr{H}}/L(\ell)^{\mathscr{B}(\ell)}$. One readily verifies that $\mathscr{H}D \subseteq D$.

Before applying the Chebotarev density theorem, we first need to bound some of the values that will occur.

$$\begin{aligned} |D| &= \#\{(A,u) \in \mathscr{G}(\ell) : A \in B, \mathrm{tr}(A) \in \mathrm{Tr}(u)\} \\ &= \#\{(A,u) \in B \times \big((\mathcal{O}_k/\ell\mathcal{O}_k)^\times/\mathcal{O}_k^\times\big) : \det(A) = N(u), \mathrm{tr}(A) \in \mathrm{Tr}(u)\} \\ &\leq \#\{(A,u) \in B \times (\mathcal{O}_k/\ell\mathcal{O}_k)^\times : \det(A) = N(u), \mathrm{tr}(A) = \mathrm{Tr}(u)\} \end{aligned}$$

Using Lemma 3.5, we find that $|D| \leq 4|B| \leq 4\ell^3$. By Lemma 3.6, $1/|\mathscr{B}(\ell)| = [G(\ell) : \mathscr{B}(\ell)]/|G(\ell)| = (\ell+1)/|G(\ell)| \ll 1/\ell^4$. It is clear that $|\mathscr{H}| = \ell(\ell-1)$. Therefore,

$$\frac{|D|}{|\mathscr{B}(\ell)|} \ll \frac{1}{\ell} \quad \text{and} \quad \frac{|D|}{|\mathscr{H}|} \ll \ell.$$

From (6.2), $[L(\ell)^{\mathscr{B}(\ell)} : \mathbb{Q}] = 2h_k(\ell+1)$. By Lemma 5.4,

$$\log M(L(\ell)/L(\ell)^{\mathscr{B}(\ell)}) \ll_E \log(\ell d_k^{1/2}).$$

(i) Assume GRH. We now apply Proposition 4.2(ii) (without any extra AHC assumption!).

$$\begin{aligned} &\pi_D(x, L(\ell)/L(\ell)^{\mathscr{B}(\ell)}) \\ &= \frac{|D|}{|\mathscr{B}(\ell)|}\,\mathrm{Li}\,x + O\Big(\Big(\frac{|D|}{|\mathscr{H}|}\Big)^{1/2} x^{1/2} [L(\ell)^{\mathscr{B}(\ell)} : \mathbb{Q}] \log\Big(M(L(\ell)/L(\ell)^{\mathscr{B}(\ell)})x\Big)\Big) \\ &\ll_E \frac{1}{\ell}\frac{x}{\log x} + h_k \ell^{3/2} x^{1/2} \log(\ell d_k^{1/2} x) \end{aligned}$$

(ii) We now apply Proposition 4.7 with the trivial bound $\beta_L \leq 1$. For $\log x \gg [L(\ell)^{\mathscr{B}(\ell)} : \mathbb{Q}](\log M(L(\ell)/L(\ell)^{\mathscr{B}(\ell)}))^2$ (and hence also if $\log x \gg_E h_k\ell(\log(\ell d_k^{1/2}))^2$),

$$\begin{aligned} &\pi_D(x, L(\ell)/L(\ell)^{\mathscr{B}(\ell)}) \\ &\ll \frac{|D|}{|\mathscr{B}(\ell)|}\,\mathrm{Li}\,x + \Big(\frac{|D|}{|\mathscr{H}|}\Big)^{1/2} [L(\ell)^{\mathscr{B}(\ell)} : \mathbb{Q}] x \exp\Big(-c\sqrt{\frac{\log x}{[L(\ell)^{\mathscr{B}(\ell)} : \mathbb{Q}]}}\Big) \log\Big(M(L(\ell)/L(\ell)^{\mathscr{B}(\ell)})x\Big)^2 \\ &\ll_E \frac{1}{\ell}\frac{x}{\log x} + h_k\ell^{3/2} x \exp\Big(-c\sqrt{\frac{\log x}{2h_k(\ell+1)}}\Big)(\log(\ell d_k^{1/2} x))^2 \\ &\ll \frac{1}{\ell}\frac{x}{\log x} + h_k\ell^{3/2} x \exp\Big(-c_1\sqrt{\frac{\log x}{h_k\ell}}\Big)(\log(\ell d_k^{1/2} x))^2, \end{aligned}$$

where $c_1 > 0$ is an absolute constant. We can replace $d_k^{1/2}$ by h_k since $\log(d_k^{1/2}) \ll \log h_k + 1$ by the Brauer-Siegel theorem.

In both cases, combining the upper bound of $\pi_D(x, L(\ell)/L(\ell)^{\mathscr{B}(\ell)})$ with Lemma 6.2 concludes the proof. □

6.2. **A conditional choice of ℓ.** It remains to choose a specific prime ℓ in Proposition 6.3. Assume that GRH holds (the next section will give the unconditional argument).

Lemma 6.4. *Assume GRH. There is an absolute constant $\gamma > 0$ such if $\frac{y^{1/2}}{\log y} \geq \gamma \log d_k$, then there exists a prime ℓ that splits in k and lies in the interval $[y, 2y]$.*

Proof. By Proposition 4.2(i),

$$\begin{aligned}\#\{\ell : \ell \text{ splits in } k,\ y \leq \ell \leq 2y\} &= \frac{1}{2}\int_y^{2y} \frac{dt}{\log t} + O(y^{1/2}\log(d_k y)) \\ &\geq \frac{1}{2}\frac{y}{\log(2y)} + O(y^{1/2}\log y + y^{1/2}\log d_k).\end{aligned}$$

There exist absolute constants $c_1 > 0$ and $c_2 > 0$ such that for $y \geq c_1$,

$$\begin{aligned}\#\{\ell : \ell \text{ splits in } k,\ \text{and } y \leq \ell \leq 2y\} &> \frac{1}{4}\frac{y}{\log y} - c_2 y^{1/2}\log d_k \\ &= \frac{1}{4}y^{1/2}\Big(\frac{y^{1/2}}{\log y} - 4c_2\log d_k\Big).\end{aligned}$$

Let $\gamma = \sup\{4c_2, c_1^{1/2}\}$. If $\frac{y^{1/2}}{\log y} \geq \gamma \log d_k$, then $y \geq \gamma^2 \geq c_1$. So,

$$\begin{aligned}\#\{p : p \text{ splits in } k,\ y \leq p \leq 2y\} &> \frac{1}{4}y^{1/2}\Big(\frac{y^{1/2}}{\log y} - 4c_2\log d_k\Big) \\ &\geq \frac{1}{4}y^{1/2}\Big(\frac{y^{1/2}}{\log y} - \gamma\log d_k\Big) \geq 0.\end{aligned}$$

□

By Lemma 5.1, we may assume that $d_k \leq 4x$. We now break up our proof of Theorem 1.3(i) into two cases.

Case 1: Suppose that $\Big(\frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}\Big)^{2/5} \geq (\log x \cdot \log\log x)^2$.

The idea is to chose a prime ℓ such that both terms in the right hand side of the inequality in Lemma 6.3(i) have roughly the same magnitude.

Let $y = C\Big(\frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}\Big)^{2/5} + c_E + 5$, where c_E is the constant from Lemma 2.5 and $C \geq 2$ is an absolute constant still to be chosen. By our hypothesis, $y \geq C(\log x \cdot \log\log x)^2$. Since $y^{1/2}/\log y$ is increasing for large y,

$$\begin{aligned}y^{1/2}/\log y &\gg C^{1/2}(\log x \cdot \log\log x)/(\log C + 2\log\log x) \\ &\gg \frac{C^{1/2}}{\log C}\log x \gg \frac{C^{1/2}}{\log C}\log d_k\end{aligned}$$

By choosing C sufficiently large and using Lemma 6.4, we may assume that there exists a prime ℓ that splits in k and lies in the interval $[y, 2y]$. Note that ℓ splits in k, $\ell \geq 5$, and $\rho_{E/H,\ell}$ is an isomorphism (since $\ell \geq c_E$). We now use our choice of ℓ in the interval $[y, 2y]$, in the bound of Lemma 6.3(i).

$$\begin{aligned} P_{E,k}(x) &\ll_E \frac{1}{h_k}\frac{1}{\ell}\frac{x}{\log x} + \ell^{3/2}x^{1/2}\log(\ell d_k^{1/2}x) \\ &\ll \frac{1}{h_k}\frac{1}{y}\frac{x}{\log x} + y^{3/2}x^{1/2}\log(yx) \\ &\ll_E \frac{1}{h_k}\Big(h_k^{2/5}\frac{(\log x)^{4/5}}{x^{1/5}}\Big)\frac{x}{\log x} + \Big(\frac{1}{h_k^{2/5}}\frac{x^{1/5}}{(\log x)^{4/5}}\Big)^{3/2}x^{1/2}\log x \\ &\ll \frac{1}{h_k^{3/5}}\frac{x^{4/5}}{(\log x)^{1/5}} \end{aligned}$$

Case 2: Suppose that $\Big(\frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}\Big)^{2/5} \le (\log x \cdot \log\log x)^2$.

$$\frac{1}{h_k}\frac{x}{\log x} = \Big(\frac{1}{h_k}\frac{x^{1/2}}{(\log x)^2}\Big)x^{1/2}\log x \le (\log x\cdot\log\log x)^5x^{1/2}\log x = x^{1/2}(\log x)^6(\log\log x)^5 \tag{6.3}$$

Let $y = C(\log x\cdot\log\log x)^2 + c_E + 5$, where c_E is the constant from Lemma 2.5 and $C > 0$ is an absolute constant which we will be chosen sufficiently large.

$$\frac{y^{1/2}}{\log y} \gg_E \frac{C^{1/2}\log x\cdot\log\log x}{\log C + \log\log x} \gg \frac{C^{1/2}}{\log C}\log x$$

Since $d_k \le 4x$, we see by Lemma 6.4 that C can be chosen such that there is a prime ℓ that splits in k and lies in the interval $[y, 2y]$. Then

$$\begin{aligned} P_{E,k}(x) &\ll_E \frac{1}{h_k}\frac{1}{\ell}\frac{x}{\log x} + \ell^{3/2}x^{1/2}\log(\ell d_k^{1/2}x) \\ &\ll \frac{1}{h_k}\frac{1}{y}\frac{x}{\log x} + y^{3/2}x^{1/2}\log x \\ &\ll \frac{1}{y}x^{1/2}(\log x)^6(\log\log x)^5 + y^{3/2}x^{1/2}\log x \qquad \text{(by (6.3))} \\ &\ll_E x^{1/2}(\log x)^4(\log\log x)^3. \end{aligned}$$

Combining both cases, we have as desired

$$P_{E,k}(x) \ll_E \frac{1}{h_k^{3/5}}\frac{x^{4/5}}{(\log x)^{1/5}} + x^{1/2}(\log x)^4(\log\log x)^3.$$

6.3. **An unconditional choice of ℓ.** Define $y := C\frac{1}{h_k}\frac{\log x}{(\log\log x)^2}$, where $0 < C < 1$ is a constant which depends only on E and will be chosen sufficiently small.

Suppose there is a prime ℓ that splits in k, $\rho_{E/H,\ell}$ is an isomorphism, and ℓ lies in the interval $[y, 2y]$.

$$\begin{aligned} h_k\ell(\log(h_k\ell))^2 &\ll h_ky(\log(h_ky))^2 \\ &\ll C\frac{\log x}{(\log\log x)^2}(\log\log x)^2 = C\log x \end{aligned}$$

So for $C > 0$ sufficiently small, the condition

$$c_2h_k\ell(\log(h_k\ell))^2 \le \log x \tag{6.4}$$

holds where c_2 is the constant from Lemma 6.3(ii). By Lemma 6.3(ii),

$$\begin{aligned}
P_{E,k}(x) &\ll_E \frac{1}{h_k \ell}\frac{x}{\log x} + \ell^{3/2} x \exp\Big(-c_1\sqrt{\frac{\log x}{h_k \ell}}\Big)(\log(h_k \ell x))^2 \\
&\ll \frac{1}{h_k y}\frac{x}{\log x} + y^{3/2} x \exp\Big(-c_1\sqrt{\frac{\log x}{2 h_k y}}\Big)(\log(h_k y x))^2 \\
&\ll C^{-1}\frac{x(\log\log x)^2}{(\log x)^2} + \frac{C^{3/2}}{h_k^{3/2}}\frac{(\log x)^{3/2}}{(\log\log x)^3} x \exp\Big(-\frac{c_1}{\sqrt{2C}}\log\log x\Big)(\log x)^2 \\
&\ll C^{-1}\frac{x(\log\log x)^2}{(\log x)^2} + C^{3/2}\frac{x}{(\log x)^{\frac{c_1}{\sqrt{2C}}-7/2}}
\end{aligned}$$

Choose $C > 0$ sufficiently small such that (6.4) holds and $c_1/\sqrt{2C} - 7/2 \geq 2$, then

$$P_{E,k}(x) \ll_E \frac{x(\log\log x)^2}{(\log x)^2}.$$

It still remains to impose suitable conditions to ensure that such a prime ℓ exists.

Lemma 6.5. *There is an absolute constant $c > 0$ such that if $\log y \geq c d_k^{1/2}$, then there exists a rational prime ℓ in the interval $[y, 2y]$ that splits in k.*

Proof. By taking $c > 0$ sufficiently large, we will have $\log(2y) \geq 20(\log d_k)^2$. Then by the Chebotarev density theorem (Proposition 4.6), there is an absolute constant $c' > 0$ such that

$$\begin{aligned}
N_y &:= \#\{\ell : y \leq \ell \leq 2y,\ \ell \text{ splits in } k\} \\
&= \frac{1}{2}\int_y^{2y}\frac{dt}{\log t} + O(y^{\beta_k}/\log y) + O(y\exp(-c'\sqrt{\log y})),
\end{aligned}$$

where β_k is the possible exception zero of $\zeta_k(s)$ from Lemma 4.4. So

$$N_y \geq \frac{y}{\log(2y)}\Big(1 + O\Big(\frac{1}{y^{1-\beta_k}}\Big) + O\Big(\log(2y)\exp(-c'\sqrt{\log y})\Big)\Big).$$

By taking $c > 0$ sufficiently large, there is an absolute constant $c'' > 0$ such that

$$N_y \geq \frac{y}{\log(2y)}\Big(1/2 - \frac{c''}{y^{1-\beta_k}}\Big).$$

By [Sta74, Lemma 11], $1 - \beta_k \gg (d_k^{1/2})^{-1}$, so $\log(y^{1-\beta_k}) = (1-\beta_k)\log y \gg \frac{\log y}{d_k^{1/2}} \geq c$. By taking $c > 0$ sufficiently large, we will ensure that $1/2 - c''/y^{1-\beta_k} > 0$ and hence $N_y > 0$. □

In the present case,

$$\log y = \log\log x - 2\log\log\log x - \log h_k + \log C = \log\log x - 2\log\log\log x + O(\log d_k).$$

So for $\log\log x \gg d_k^{1/2}$ we have $\log y \geq c d_k^{1/2}$, with $c > 0$ as in Lemma 6.5. Therefore, if $\log\log x \gg d_k^{1/2}$ then there is a prime ℓ in the interval $[y, 2y]$ that splits in k. Finally, if we take $c \geq \log c_E$, where c_E is the constant from Lemma 2.5, then $\rho_{E/H,\ell}$ is an isomorphism.

7. The proof of Corollary 1.5

We start with the identity

$$\pi(x) = \#\{p : p|N_E\} + \#\{p \leq x : E \text{ has supersingular reduction at } p\} + \sum_{k \in D_E(x)} P_{E,k}(x).$$

By [Ser81, Théorème 20], $\#\{p \leq x : E \text{ is supersingular at } p\} = o_E(x/\log x)$, so

$$\pi(x) = o_E(x/\log x) + \sum_{k \in D_E(x)} P_{E,k}(x).$$

We now use the bounds from Theorem 1.3(i).

$$\begin{aligned} x/\log x &\ll_E \sum_{k \in D_E(x)} P_{E,k}(x) \\ &\ll_E \sum_{k \in D_E(x)} \Big(\frac{1}{h_k^{3/5}} \frac{x^{4/5}}{(\log x)^{1/5}} + x^{1/2}(\log x)^4(\log\log x)^3 \Big) \\ &= \Big(\sum_{k \in D_E(x)} \frac{1}{h_k^{3/5}} \Big) \frac{x^{4/5}}{(\log x)^{1/5}} + |D_E(x)| x^{1/2}(\log x)^4(\log\log x)^3 \end{aligned}$$

Using GRH, one can show that, $h_k \gg d_k^{1/2}/\log d_k$. We now use this lower bound for h_k, and Lemma 5.1 which says that $d_k \leq 4x$ for all $k \in D_E(k)$.

$$\begin{aligned} \sum_{k \in D_E(x)} \frac{1}{h_k^{3/5}} &\ll \sum_{k \in D_E(x)} \frac{(\log d_k)^{3/5}}{d_k^{3/10}} \\ &\ll \sum_{k \in D_E(x)} \frac{1}{d_k^{3/10}} (\log x)^{3/5} \\ &\leq \sum_{d=1}^{|D_E(x)|} \frac{1}{d^{3/10}} (\log x)^{3/5} \ll |D_E(x)|^{7/10} (\log x)^{3/5} \end{aligned}$$

Combining with our previous inequality gives:

$$\begin{aligned} x/\log x &\ll_E |D_E(x)|^{7/10} x^{4/5} (\log x)^{2/5} + |D_E(x)| x^{1/2} (\log x)^4 (\log\log x)^3 \\ &\ll \sup\Big\{ |D_E(x)|^{7/10} x^{4/5} (\log x)^{2/5}, |D_E(x)| x^{1/2} (\log x)^4 (\log\log x)^3 \Big\}. \end{aligned}$$

- If $|D_E(x)|^{7/10} x^{4/5} (\log x)^{2/5} < |D_E(x)| x^{1/2} (\log x)^4 (\log\log x)^3$, then
$$|D_E(x)| \gg_E (x/\log x)/(x^{1/2}(\log x)^4(\log\log x)^3) = x^{1/2}/((\log x)^5(\log\log x)^3).$$
- If $|D_E(x)|^{7/10} x^{4/5} (\log x)^{2/5} \geq |D_E(x)| x^{1/2} (\log x)^7$, then
$$|D_E(x)|^{7/10} \gg_E \frac{x^{1/5}}{(\log x)^{7/5}} \quad \text{and hence} \quad |D_E(x)| \gg_E \frac{x^{2/7}}{(\log x)^2}.$$

We conclude that $|D_E(x)| \gg_E x^{2/7}/(\log x)^2$, since it is the weaker of the two bounds.

Remark 7.1. If we had used the bound $P_{E,k}(x) \ll_E \frac{x^{4/5}}{(\log x)^{1/5}}$, then we would have concluded that $|D_E(x)| \gg_E \frac{x^{1/5}}{(\log x)^{4/5}}$. Thus the factor $\frac{1}{h_k^{3/5}}$ occuring in our bound of $P_{E,k}(x)$ gives us a significant improvement.

Appendix A. Heuristics for the Lang-Trotter conjecture

In this appendix, we will give heuristics for Conjecture 1.1 so one msy see how the representations studied in this paper first occurred. In their heuristics, Lang and Trotter construct the simplest probabilistic model that is compatible with known equidistribution laws. We will not be as systematic here, for a more careful (and hence more convincing) heuristic see [LT76, Part II]. Fix a non-CM elliptic curve $E/\mathbb{Q}$ and an imaginary quadratic field k.

Let $\mathcal{P}_k$ be the set of rational primes $p \nmid N_E$ that split completely in H, and let $\mathcal{P}_k(x)$ be the set of primes in $\mathcal{P}_k$ that are of size at most x. By Lemma 3.1, if E has good ordinary reduction at a prime p and $\mathbb{Q}(\pi_p(E)) \cong k$, then $p \in \mathcal{P}_k$. Given $p \in \mathcal{P}_k$, we will give heuristics for the "probability" that $\mathbb{Q}(\pi_p(E)) \cong k$. This heuristic probability will be asymptotic to $\frac{4w_k}{\pi^2} C^{\mathrm{fin}}_{E,k} \frac{1}{2\sqrt{p}}$ for an explicit constant $C^{\mathrm{fin}}_{E,k} > 0$ which will be described. Then as $x \to \infty$, we conjecture that

$$P_{E,k}(x) \sim \sum_{p \in \mathcal{P}_k(x)} \frac{4w_k}{\pi^2} C^{\mathrm{fin}}_{E,k} \frac{1}{2\sqrt{p}}.$$

By the Chebotarev density theorem,

$$\sum_{p \in \mathcal{P}_k(x)} \frac{1}{2\sqrt{p}} \sim \frac{1}{2h_k} \sum_{p \leq x} \frac{1}{2\sqrt{p}} \sim \frac{1}{2h_k} \frac{x^{1/2}}{\log x}.$$

Thus we recover the Lang-Trotter conjecture

$$P_{E,k}(x) \sim C_{E,k} \frac{x^{1/2}}{\log x},$$

with $C_{E,k} := \dfrac{1}{2h_k} \dfrac{4w_k}{\pi^2} C^{\mathrm{fin}}_{E,k}$.

A.1. **Equidistribution laws.** We briefly recall the equidistribution laws that play a role in the heuristics. The bounds in this paper used only the Chebotarev density theorem; it would be interesting to find upper bounds for $P_{E,k}(x)$ using the archimedean laws (see [Mur85] for results in this direction concerning the *other* Lang-Trotter conjecture).

A.1.1. *Sato-Tate.* Define the function $g_1 \colon [-1,1] \to [0,\infty)$ by $g_1(\xi) = \frac{2}{\pi}\sqrt{1-\xi^2}$. For any interval $I \subseteq [-1,1]$, the *Sato-Tate conjecture* predicts that the set

$$\left\{\mathfrak{P} \in \Sigma_H : a_{\mathfrak{P}}(E)/(2\sqrt{N(\mathfrak{P})}) \in I\right\}$$

has natural density $\int_I g_1(\xi) d\xi$ in Σ_H.

A.1.2. *Hecke.* Define the function $g_2 \colon (-1,1) \to [0,\infty)$ by $g_2(\xi) = \frac{w_k}{\pi}\frac{1}{\sqrt{1-\xi^2}}$. For any interval $I \subseteq [-1,1]$, from Hecke we know that

$$\lim_{x\to\infty} \frac{1}{|\Sigma_H(x)|} \sum_{\mathfrak{P} \in \Sigma_H(x)} \#\left\{\pi \in \mathcal{O}_k : \mathfrak{P} \cap \mathcal{O}_k = \pi\mathcal{O}_k,\ \mathrm{Tr}_{k/\mathbb{Q}}(\pi)/(2\sqrt{N(\mathfrak{P})}) \in I\right\} \sim \int_I g_2(\xi) d\xi.$$

If we assume the interval I has sufficiently small length, then the set

$$\{\mathfrak{P} \in \Sigma_H : \text{there exists a } \pi \in \mathcal{O}_k \text{ such that } \mathfrak{P} \cap \mathcal{O}_k = \pi\mathcal{O}_k \text{ and } \mathrm{Tr}_{k/\mathbb{Q}}(\pi)/(2\sqrt{N(\mathfrak{P})}) \in I\}$$

has natural density $\int_I g_2(\xi) d\xi$ in Σ_H.

A.1.3. *Chebotarev.* This section uses the Galois groups described in §2.3. Fix an integer $m \geq 5$, and take any $t \in \mathbb{Z}/m\mathbb{Z}$. Define the set

$$G(m)_t = \{\sigma \in G(m) : \operatorname{tr}(\rho_{E/H,m}(\sigma|_{H(E[m])})) = t,\ \operatorname{Tr}(\psi_{k,m}(\sigma|_{k(m)}) \ni t\}.$$

The Chebotarev density theorem shows that the set

$$\{\mathfrak{P} \in \Sigma_H : a_{\mathfrak{P}}(E) \equiv t \pmod{m},\ \exists \pi \in \mathcal{O}_k \text{ such that } \mathfrak{P} \cap \mathcal{O}_k = \pi\mathcal{O}_k \text{ and } \operatorname{Tr}_{k/\mathbb{Q}}(\pi) \equiv t \pmod{m}\}$$

has natural density $|G(m)_t|/|G(m)|$. We will need a more refined version.

Given a random $\mathfrak{P} \in \Sigma_H$ of degree 1 *and* a random generator π of $\mathfrak{P} \cap \mathcal{O}_k$, we want to know the probability that

$$a_{\mathfrak{P}}(E) \equiv t \pmod{m} \text{ and } \operatorname{Tr}_{k/\mathbb{Q}}(\pi) \equiv t \pmod{m}. \tag{A.1}$$

Define the group

$$\widetilde{\mathscr{G}}(m) = \{(A, u) \in \operatorname{Aut}(E[m]) \times (\mathcal{O}_k/m\mathcal{O}_k)^\times : \det(A) = N(u)\},$$

which has a natural projection $\varphi \colon \widetilde{\mathscr{G}}(m) \to \mathscr{G}(m)$. Let $\widetilde{G}(m)$ be the group $\varphi^{-1}(\Psi_m(G(m)))$ and define $\widetilde{G}(m)_t = \{(A, u) \in \widetilde{G}(m) : \operatorname{tr}(A) = t,\ \operatorname{Tr}(u) = t\}$. By the Chebotarev density theorem (applied to the Galois group $G(m)$, and weighting each conjugacy classes appropriately),

$$\sum_{\substack{\mathfrak{P} \in \Sigma_H(x) \\ a_{\mathfrak{P}}(E) \equiv t \ (\mathrm{mod}\ m)}} \frac{\#\{\pi \in \mathcal{O}_k : \mathfrak{P} \cap \mathcal{O}_k = \pi\mathcal{O}_k, \operatorname{Tr}_{k/\mathbb{Q}}(\pi) \equiv t \pmod{m}\}}{w_k}$$

$$\sim \frac{1}{w_k}\frac{|\widetilde{G}(m)_t|}{|G(m)|}|\Sigma_H(x)| = \frac{|\widetilde{G}(m)_t|}{|\widetilde{G}(m)|}|\Sigma_H(x)|.$$

Thus the probability that random $\mathfrak{P} \in \Sigma_H$ of degree 1 and generator π of $\mathfrak{P} \cap \mathcal{O}_k$ satisfy (A.1) is equal to $|\widetilde{G}(m)_t|/|\widetilde{G}(m)|$. For latter use, define

$$\widetilde{C}(m) = \{(A, u) \in \widetilde{G}(m) : \operatorname{tr}(A) = \operatorname{Tr}(u)\}.$$

A.2. **Heuristics.** Given $p \in \mathcal{P}_k$, we now give heuristics for the "probability" that $\mathbb{Q}(\pi_p(E)) \cong k$, or equivalently that there is a $\pi \in \mathcal{O}_k$ such that $N_{k/\mathbb{Q}}(\pi) = p$ and $\operatorname{Tr}_{k/\mathbb{Q}}(\pi) = a_p(E)$.

Fix any $\mathfrak{P} \in \Sigma_H$ dividing p. Then $\mathbb{Q}(\pi_p(E)) \cong k$ is equivalent to the existence of a $\pi \in \mathcal{O}_k$ such that $\mathfrak{P} \cap \mathcal{O}_k = \pi\mathcal{O}_k$ and $\operatorname{Tr}_{k/\mathbb{Q}}(\pi) = a_{\mathfrak{P}}(E)$.

There is a finite set $S \subseteq [-1, 1]$ such that if $z_0 \in \{z \in \mathbb{C} : |z| = 1\}$ satisfies $\operatorname{Re}(z_0) = t$, then $\operatorname{Re}(\zeta z_0) \neq t$, for all w_k-th roots of unity $\zeta \neq 1$ in $\mathbb{C}$.

Fix an integer $t \in \mathbb{Z}$ with $|t| \leq 2\sqrt{p}$. By considering the Hecke and Sato-Tate distributions only (and assuming they are independent of each other), we would expect the probability that there is a $\pi \in \mathcal{O}_k$ such that $\mathfrak{P} \cap \mathcal{O}_k = \pi\mathcal{O}_k$, $a_{\mathfrak{P}}(E) = t$, and $\operatorname{Tr}_{k/\mathbb{Q}}(\pi) = t$ to be

$$\frac{g_1(\frac{t}{2\sqrt{p}})}{2\sqrt{p}}\frac{g_2(\frac{t}{2\sqrt{p}})}{2\sqrt{p}} = \frac{2\omega_k}{\pi^2}\frac{1}{4p}.$$

If $t/(2\sqrt{p}) \notin S$, then the corresponding generator π is uniquely determined.

However, these purely archimedean heuristics ignore the Chebotarev contribution. Fix an integer $m \geq 5$. Suppose that $t/(2\sqrt{p}) \notin S$. From §A.1.3, $|\widetilde{G}(m)_t|/|\widetilde{G}(m)|$ is the probability that $a_{\mathfrak{P}}(E) \equiv t$ and $\operatorname{Tr}_{k/\mathbb{Q}}(\pi) \equiv t \pmod{m}$, while the naive probability that such congruences hold is $1/m^2$. So to take into account the congruences modulo m, we should multiply our probability by a correction term of $\dfrac{|\widetilde{G}(m)_t|}{|\widetilde{G}(m)|}/\dfrac{1}{m^2}$.

We thus expect the probability that $\mathbb{Q}(\pi_p(E))$ is isomorphic to k is approximately:

$$\sum_{\substack{t\in\mathbb{Z}\\|t|\le 2\sqrt{p}}} m^2\frac{|\widetilde{G}(m)_t|}{|\widetilde{G}(m)|}\frac{2\omega_k}{\pi^2} = m^2\sum_{t_0\in\mathbb{Z}/m\mathbb{Z}}\frac{|\widetilde{G}(m)_{t_0}|}{|\widetilde{G}(m)|}\sum_{\substack{|t|\le 2\sqrt{p}\\ t\equiv t_0 \pmod m}}\frac{2w_k}{\pi^2}\frac{1}{4p}$$
$$\approx \frac{4w_k}{\pi^2}\left(m\sum_{t_0\in\mathbb{Z}/m\mathbb{Z}}\frac{|\widetilde{G}(m)_{t_0}|}{|\widetilde{G}(m)|}\right)\frac{1}{2\sqrt{p}} = \frac{4w_k}{\pi^2}\cdot m\frac{|\widetilde{C}(m)|}{|\widetilde{G}(m)|}\cdot\frac{1}{2\sqrt{p}}.$$

The above heuristic dealt only with congruences modulo a fixed integer m. Define

$$C_{E,k}^{\mathrm{fin}} := \lim_m m\frac{|\widetilde{C}(m)|}{|\widetilde{G}(m)|},$$

where the limit is over natural numbers m ordered by divisibility. The convergence of this limit is proven in [LT76], where a product expression is also given that is useful for numerical computations. Thus for $p\in\mathcal{P}_k$, we expect that the "probability" that $\mathbb{Q}(\pi_p(E))\cong k$ to be asymptotic to

$$\frac{4w_k}{\pi^2}C_{E,k}^{\mathrm{fin}}\frac{1}{2\sqrt{p}}.$$

References

[Coj05] Alina Carmen Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canad. Math. Bull. **48** (2005), no. 1, 16–31. With an appendix by Ernst Kani. ↑2.1, ii

[CD08] Alina Carmen Cojocaru and Chantal David, *Frobenius fields for elliptic curves*, Amer. J. Math. **130** (2008), no. 6, 1535–1560. ↑1.2, 1.6

[CFM05] Alina Carmen Cojocaru, Etienne Fouvry, and M. Ram Murty, *The square sieve and the Lang-Trotter conjecture*, Canad. J. Math. **57** (2005), no. 6, 1155–1177. ↑1.2

[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. ↑4.3

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

[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. ↑1.1, 1.1, ii, iii, A, A.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. ↑iii, ii, 6

[Mur85] V. Kumar Murty, *Explicit formulae and the Lang-Trotter conjecture*, Rocky Mountain J. Math. **15** (1985), no. 2, 535–551. Number theory (Winnipeg, Man., 1983). ↑A.1

[Mur97] ———, *Modular forms and the Chebotarev density theorem. II*, Analytic number theory (Kyoto, 1996), London Math. Soc. Lecture Note Ser., vol. 247, Cambridge Univ. Press, Cambridge, 1997, pp. 287–308. ↑iii, 4.3, 4.8

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑2.1

[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. ↑ii

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. ↑1.2, ii, i, i, 4.4, 5.2, 7

[Ser86] ———, *Œuvres. Vol. III*, Springer-Verlag, Berlin, 1986. 1972–1984. ↑1.2

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original. ↑2.1

[Sta74] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152. ↑4.3, 6.3

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, USA
E-mail address: zywina@math.upenn.edu
URL: http://www.math.upenn.edu/~zywina