BOUNDS FOR THE LANG-TROTTER CONJECTURES

DAVID ZYWINA

ABSTRACT. For a non-CM elliptic curve $E/\mathbb{Q}$, Lang and Trotter made very deep conjectures concerning the number of primes $p \le x$ for which $a_p(E)$ is a fixed integer (and for which the Frobenius field at p is a fixed imaginary quadratic field). Under GRH, we use a smoothed version of the Chebotarev density theorem to improve the best known Lang-Trotter upper bounds of Murty, Murty and Saradha, and Cojocaru and David.

1. INTRODUCTION

1.1. **The Lang-Trotter conjectures.** Fix a non-CM elliptic curve E defined over $\mathbb{Q}$ and let N_E be its conductor. Take any prime $p \nmid N_E$. Let E_p be the reduction of E modulo p; it is an elliptic curve over $\mathbb{F}_p$. Let π_p be the Frobenius endomorphism of E_p. We have $\pi_p^2 - a_p(E)\pi_p + p = 0$ for a unique integer $a_p(E)$. We can also define $a_p(E)$ by the formula $a_p(E) = |E_p(\mathbb{F}_p)| - (p+1)$. From Hasse, we know that $|a_p(E)| < 2\sqrt{p}$ and hence $\mathbb{Q}(\pi_p)$ in $\mathrm{End}(E_p) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic field.

Fix an integer a and an imaginary quadratic field k. We define the following functions of $x \ge 2$:

$$P_{E,a}(x) := \#\{p \le x : p \nmid N_E,\ a_p(E) = a\},$$
$$P_{E,k}(x) := \#\{p \le x : p \nmid N_E,\ \mathbb{Q}(\pi_p) \cong k\}.$$

Lang and Trotter made the following two conjectures concerning the asymptotics of $P_{E,a}(x)$ and $P_{E,k}(x)$, cf. [LT76].

Conjecture 1.1 (Lang-Trotter)**.**

(a) There is an explicit constant $C_{E,a} \ge 0$ such that

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

as $x \to \infty$. When $C_{E,a} = 0$, we interpret this asymptotic as meaning that $P_{E,a}(x)$ is a bounded function of x.

(b) There is an explicit constant $C_{E,k} > 0$ such that

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

as $x \to \infty$.

1.2. **Upper bounds.** In this paper, we are interested in improving the best known upper bounds on $P_{E,a}(x)$ and $P_{E,k}(x)$ as functions of x; we will summarize previous results in §1.3. Some bounds are conditional on the Generalized Riemann Hypothesis (GRH) for number fields.

Theorem 1.2. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ and let a be an integer. Assuming GRH, we have*

$$P_{E,a}(x) \ll_E \frac{x^{4/5}}{(\log x)^{3/5}} \quad \text{and} \quad P_{E,0}(x) \ll_E \frac{x^{3/4}}{(\log x)^{1/2}}.$$

The best known unconditional bounds for $P_{E,a}(x)$ can be found in §1.3. We now give bounds for $P_{E,k}(x)$.

Theorem 1.3. *Let E be a non-CM elliptic curve over $\mathbb{Q}$ and let k be an imaginary quadratic field.*

(i) Assume GRH. Then

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

where h_k is the class number of k. In particular, $P_{E,k}(x) \ll_E x^{4/5}/(\log x)^{3/5}$.

(ii) There is a constant $c > 0$, depending only on E and k, such that

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

whenever $x \geq c$. In particular, $P_{E,k}(x) \ll_{E,k} x(\log\log x)^2/(\log x)^2$.

Let $D_E(x)$ be the set of imaginary quadratic extensions k of $\mathbb{Q}$, in some fixed algebraic closure of $\mathbb{Q}$, for which there exists a prime $p \leq x$ with $\mathbb{Q}(\pi_p) \cong k$. The following, which will be proved in §6, is an easy consequence of Theorem 1.3(i).

Corollary 1.4. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. Assuming GRH, we have*

$$|D_E(x)| \gg_E \frac{x^{2/7}}{(\log x)^{10/7}}.$$

This improves on the bound $|D_E(x)| \gg_E x^{1/14}/(\log x)^2$ from [CD08]. The explicit dependence of k in Theorem 1.3(i) is very important here.

1.3. **Some earlier results.** We first describe bounds for $P_{E,a}(x)$. Under GRH, Serre proved that $P_{E,a}(x) \ll_E x^{7/8}(\log x)^{1/2}$ and $P_{E,0}(x) \ll_E x^{3/4}$, cf. [Ser81]. Under GRH, Murty, Murty and Saradha obtained the improved bound

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

cf. [MMS88]. In [Ser81], Serre proved (unconditionally) that $P_{E,a}(x) \ll_{E,\varepsilon} x/(\log x)^{5/4-\varepsilon}$ for any $\varepsilon > 0$. The exponent $5/4$ was improved to 2 by D. Wan [Wan90]. The best general unconditional bound for $P_{E,a}(x)$ is the bound

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

of V. K. Murty [Mur97]. For $a = 0$, there is also the superior bound $P_{E,0}(x) \ll_E x^{3/4}$ of Elkies, Kaneko and Murty, cf. [Elk91].

We now describe bounds for $P_{E,k}(x)$. In [Ser81, p. 191], Serre claimed without proof that $P_{E,k}(x) \ll_{E,k} x^\theta$ (under GRH) and $P_{E,k}(x) \ll_{E,k} x/(\log x)^{\gamma+1}$ for some positive constants θ and γ. Under GRH, Cojocaru, Fouvry and Murty [CFM05] showed that one could take $\theta = 7/8$ and any $\gamma > 1/24$. Under GRH, Cojocaru and David [CD08] obtained the bound

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

Upper bounds for $P_{E,a}(x)$ and $P_{E,k}(x)$ are in general hard to improve. The function of x obtained indicates the strength of the methods used and often different methods will give the exact same bound. For example, assume E is semistable and that the L-function for E and its symmetric powers has analytic continuation and satisfies the appropriate analogue of the Riemann hypothesis, then Rouse and Thorner proved that $P_{E,0}(x) \ll_E x^{3/4}/(\log x)^{1/2}$, cf. [RT13]. This is the same bound as Theorem 1.2 under GRH!

The goal of this paper is to push the upper bounds obtained using Chebotarev to the limit. It is not clear to the author how to improve them without completely new ideas.

1.4. **Overview.** In §2, we recall several effective versions of the Chebotarev density theorem. Under GRH and Artin's holomorphy conjecture, we also give some improved Chebotarev upper bounds; they key point being that we can obtain superior error terms if we count primes using a smoothed weighting.

In §3, we review some of the Galois representations associated to E and k. These representations play a role in the heuristics of Lang and Trotter in [LT76]. To understand their images we will need Serre's open image theorem and some class field theory.

We prove Theorem 1.2 in §4. We follow the proof of Murty, Murty and Saradha in [MMS88] and use our stronger Chebotarev bound. We prove Theorem 1.3 in §5. We again follow the general strategy of [MMS88] though the groups are more complicated.

Notation. For two functions $f(x)$ and $g(x)$ of a real variable $x \geq 2$, we say that $f \ll g$ (or $g \gg f$) if there is a positive constants C such $|f(x)| \leq C|g(x)|$ for all $x \geq 2$. We shall use $O(f)$ to denote an unspecified function g with $g \ll f$. We will always indicate the dependence of the implied constant C with subscripts on $\ll$ or O (in particular, no subscripts indicates that the constant is absolute). The logarithm integral is $\mathrm{Li}(x) := \int_2^x (\log t)^{-1}\, dt$; it satisfies $\mathrm{Li}(x) \ll x/\log x$.

For a number field K, let $\mathcal{O}_K$ be its ring of integers. Let Σ_K be the set of non-zero prime ideals of $\mathcal{O}_K$. For each $\mathfrak{p} \in \Sigma_K$, let $N(\mathfrak{p})$ be the cardinality of the residue field $\mathcal{O}_K/\mathfrak{p}$.

For a number field K, let $\overline{K}$ be a fixed algebraic closure of K. Define the absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$. For each $\mathfrak{p} \in \Sigma_K$, let $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}_K$ be a Frobenius automorphism for the prime $\mathfrak{p}$. If $\rho\colon \mathrm{Gal}_K \to G$ is a representation unramified at $\mathfrak{p}$, then $\rho(\mathrm{Frob}_\mathfrak{p})$ is a well-defined conjugacy class.

Acknowledgements. This paper uses parts of an unpublished preprint that benefited from helpful comments from Bjorn Poonen.

2. Chebotarev bounds

Fix a Galois extension of number fields L/K with Galois group G. Define

$$M(L/K) := 2[L:K] \cdot d_K^{1/[K:\mathbb{Q}]} \cdot \prod_{p \in \mathcal{P}(L/K)} p,$$

where d_K is the absolute discriminant of K and $\mathcal{P}(L/K)$ is the set of rational primes p that are divisible by some $\mathfrak{p} \in \Sigma_K$ that ramifies in L.

We say that L/K satisfies Artin's Holomorphy Conjecture (AHC) if for each irreducible character $\chi\colon G \to \mathbb{C}$, the Artin L-function $L(s,\chi)$ extends to a function analytic on the whole complex plane except at $s = 1$ when $\chi = 1$. If $G = \mathrm{Gal}(L/K)$ is abelian, then AHC is known to hold for L/K; the Artin L-function then agrees with a Hecke L-function that has the required properties. The Generalized Riemann Hypothesis (GRH) for the field L asserts that any zero ρ of the Dedekind L-function of the field L with $0 \leq \mathrm{Re}(s) \leq 1$ satisfies $\mathrm{Re}(s) = 1/2$. We say that GRH holds if it holds for all number fields.

2.1. **Chebotarev density theorem.** Let $\varphi\colon G \to \mathbb{C}$ be a class function. For each prime $\mathfrak{p} \in \Sigma_K$, choose any $\mathfrak{P} \in \Sigma_L$ dividing $\mathfrak{p}$. We then have a distinguished (arithmetic) 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, respectively, at $\mathfrak{P}$. For each integer $m \geq 1$, we define

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

As the notation suggests, $\varphi(\mathrm{Frob}_{\mathfrak{p}}^m)$ is independent of the choice of $\mathfrak{P}$. For $\mathfrak{p}$ unramified in L, this definition agrees with the value of φ on the conjugacy class $\mathrm{Frob}_{\mathfrak{p}}^m$ of G. For $x \geq 2$, define

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

Now let C be a subset of G that is stable under conjugation and let $\delta_C\colon G \to \{0,1\}$ be the class function such that $\delta_C(g) = 1$ if and only if $g \in C$. We define

$$\pi_C(x, L/K) := \pi_{\delta_C}(x) \quad \text{and} \quad \widetilde{\pi}_C(x, L/K) := \widetilde{\pi}_{\delta_C}(x).$$

It is often more convenient to use $\widetilde{\pi}_C(x, L/K)$ since it has better functorial properties, cf. §2.3.

The Chebotarev density theorem says that

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|}\operatorname{Li}(x) \tag{2.1}$$

as $x \to +\infty$. An effective form of Chebotarev is a version with an explicit error term. The following theorems of Murty, Murty and Saradha give effective versions.

Theorem 2.1.

(i) Suppose that AHC holds for L/K and that GRH holds for L. Then

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

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

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

where β_L is the possible exceptional zero of the Dedekind L-function of the field L (it would be real and satisfy $1/2 < \beta_L < 1$). The term $\frac{|C|}{|G|}\operatorname{Li}(x^{\beta_L})$ is present only when β_L exists.

Proof. Part (i) is Corollary 3.7 of [MMS88]. Part (ii) is a special case of Theorem 4.6 of [Mur97] where the group is abelian. In the notation of [Mur97], we have have $H = 1$ and G/H abelian, so $d_{G/H} = 1$ and $|\chi_{G/H}(\overline{C})| \leq |C|$. □

2.2. **Smoothed Chebotarev.** We will prove the following smoothed analogue of Chebotarev in §7.

Theorem 2.2. *Let L/K be a finite Galois extension of number fields with Galois group G. Assume that AHC holds for the extension L/K and that GRH holds for L. Let C be a subset of G stable under conjugation.*

Take any smooth function $f\colon (0,\infty) \to \mathbb{R}$ with compact support. Then for $x \geq 2$, we have

$$\sum_{\mathfrak{p}} \delta_C(\mathrm{Frob}_{\mathfrak{p}})\log N(\mathfrak{p})\cdot f(N(\mathfrak{p})/x) = \frac{|C|}{|G|}\int_0^\infty f(t)dt\ \cdot x + O_f\Big(|C|^{1/2}[K:\mathbb{Q}]x^{1/2}\log M(L/K)\Big),$$

where the sum is over all the primes $\mathfrak{p} \in \Sigma_K$ that are unramified in L.

In our application, we are only interested in asymptotic upper bounds for $\pi_C(x, L/K)$, so there is no harm in counting using a smoothed weight. Under GRH, the following gives an upper bound that cannot be deduced from Theorem 2.1(i).

Theorem 2.3. *Let L/K be a Galois extension of number fields with Galois group G. Assume that AHC holds for L/K and that GRH holds for L. Let C be a subset of G that is stable under conjugation. Then*

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

Proof. First fix a smooth function $f\colon (0,\infty)\to\mathbb{R}$ with compact support that is non-negative and satisfies $f(t)\geq 1$ for all $1/2\leq t\leq 1$. For every $x\geq 2$, define

$$A(x) := \sum_{\substack{\mathfrak{p}\in\Sigma_K,\ \sqrt{x}\leq N(\mathfrak{p})\leq x\\ \mathfrak{p}\text{ unramified in }L}} \delta_C(\mathrm{Frob}_\mathfrak{p})\log N(\mathfrak{p}) \quad\text{and}\quad \Pi(x) := \sum_{\mathfrak{p}\in\Sigma_K,\, x/2\leq N(\mathfrak{p})\leq x} \delta_C(\mathrm{Frob}_\mathfrak{p})\log N(\mathfrak{p}).$$

By our choice of f, we have $\Pi(x)\leq \sum_{\mathfrak{p}\in\Sigma_K}\delta_C(\mathrm{Frob}_\mathfrak{p})\log N(\mathfrak{p})\cdot f(N(\mathfrak{p})/x)$. By Theorem 2.3, we have $\Pi(x)\ll_f \frac{|C|}{|G|}x + |C|^{1/2}[K:\mathbb{Q}]x^{1/2}\log M(L/K)$.

Let $m\geq 1$ be the smallest integer for which $x/2^m\geq\sqrt{x}$. We have $A(x)\leq\sum_{i=0}^m\Pi(x/2^i)$, so our bound for $\Pi(x)$ gives

$$\begin{aligned} A(x) &\ll_f \frac{|C|}{|G|}x\sum_{i=0}^m\frac{1}{2^i} + |C|^{1/2}[K:\mathbb{Q}]x^{1/2}\log M(L/K)\sum_{i=0}^m\frac{1}{2^{i/2}}\\ &\ll \frac{|C|}{|G|}x + |C|^{1/2}[K:\mathbb{Q}]x^{1/2}\log M(L/K).\end{aligned}$$

There at most $[K:\mathbb{Q}]$ primes $\mathfrak{p}$ dividing any rational prime p, so

$$|\{\mathfrak{p}\in\Sigma_K : N(\mathfrak{p})\leq\sqrt{x}\}|\leq[K:\mathbb{Q}]\cdot|\{p : p\leq\sqrt{x}\}|\ll[K:\mathbb{Q}]\tfrac{\sqrt{x}}{\log\sqrt{x}}.$$

Therefore,

$$\begin{aligned}\pi_C(x,L/K) &\leq A(x)/\log(\sqrt{x}) + [K:\mathbb{Q}]x^{1/2}/\log(\sqrt{x})\\ &\ll_f \frac{|C|}{|G|}\frac{x}{\log x} + |C|^{1/2}[K:\mathbb{Q}]\frac{x^{1/2}}{\log x}\log M(L/K) + [K:\mathbb{Q}]\frac{x^{1/2}}{\log x}.\end{aligned}$$

The theorem now follows if $|C|\neq 0$. If $|C|=0$, then the theorem is trivial. □

For future use, we also give the following consequence of Theorem 2.2.

Corollary 2.4. *Fix notation and assumptions as in Theorem 2.2. Assume that $C\neq\emptyset$. There is an absolute constant $c>0$ such that if*

$$x\geq c\frac{|G|^2}{|C|}[K:\mathbb{Q}]^2\log^2 M(L/K),$$

then there is a prime $\mathfrak{p}\in\Sigma_K$ unramified in L with $x/2\leq N(\mathfrak{p})\leq x$ such that $\delta_C(\mathrm{Frob}_\mathfrak{p})=1$.

Proof. Let $f\colon(0,\infty)\to\mathbb{R}$ be a non-negative smooth function with compact support whose support is in the interval $[1/2,1]$ and is non-zero. Suppose that there are no primes $\mathfrak{p}\in\Sigma_K$ with $x/2\leq N(\mathfrak{p})\leq x$ such that $\mathfrak{p}$ is unramified in L and $\delta_C(\mathrm{Frob}_\mathfrak{p})=1$. The sum in Theorem 2.2 is then zero, so

$$\frac{|C|}{|G|}x\ll_f |C|^{1/2}[K:\mathbb{Q}]x^{1/2}\log M(L/K);$$

note that the integral $\int_0^\infty f(t)dt$ is positive by our choice of f. Rearranging, we deduce that $x\ll_f |G|^2/|C|\cdot[K:\mathbb{Q}]^2\log^2 M(L/K)$. We obtain the desired contradiction by choosing the constant c in the statement of the corollary sufficiently large. □

2.3. **Functorial properties.** Let H be a subgroup of G. Take any class function $\varphi\colon H \to \mathbb{C}$. As above, we can define $\widetilde{\pi}_\varphi(x)$; note that H is the Galois group of the extension L/L^H. Define the induced function

$$\operatorname{Ind}_H^G \varphi\colon G \to \mathbb{C}, \quad g \mapsto \frac{1}{|H|} \sum_{t\in G,\, t^{-1}gt\in H} \varphi(t^{-1}gt);$$

it is a class function of G.

Lemma 2.5.

(i) Let H be a subgroup of G and let φ be a class function of H. Then $\widetilde{\pi}_{\operatorname{Ind}_H^G \varphi}(x) = \widetilde{\pi}_\varphi(x)$.

(ii) Let N be a normal subgroup of G and let φ' be a class function of G/N. Then $\widetilde{\pi}_{\varphi'}(x) = \widetilde{\pi}_\varphi(x)$, where φ is the function obtained by composing the projection $G \to G/N$ with φ'.

Proof. See Proposition 8 of [Ser81]. □

Lemma 2.6.

(i) Let H be a subgroup of G and let C be a subset of G stable under conjugation. Suppose that every element of C is conjugate to some element of H. Then

$$\widetilde{\pi}_C(x, L/K) \le \widetilde{\pi}_{C\cap H}(x, L/L^H).$$

(ii) Let N be a normal subgroup of G and let C be a subset of G stable under conjugation that satisfies $NC \subseteq C$. Then

$$\widetilde{\pi}_C(x, L/K) = \widetilde{\pi}_{C'}(x, L^N/K),$$

where C' is the image of C in $G/N = \operatorname{Gal}(L^N/K)$.

Proof. Part (ii) is an immediate consequence of Lemma 2.5(ii); note that δ_C is equal to the projection $G \to G/N$ composed with $\delta_{C'}$.

We now prove (i). By assumption on C, there is a set $S \subseteq H$ for which we have a disjoint union $C = \cup_{s\in S} C_G(s)$, where $C_G(s)$ is the conjugacy class of s in G. For each $s \in S$, let $C_H(s)$ be the conjugacy class of s in H. We have $(\operatorname{Ind}_H^G \delta_{C_H(s)})(g) = 0$ for $g \in G - C_G(s)$, so

$$\operatorname{Ind}_H^G \delta_{C_H(s)} = \lambda_s \cdot \delta_{C_G(s)}$$

for some λ_s. Therefore, $\widetilde{\pi}_{C_H(s)}(x, L/L^H) = \lambda_s \widetilde{\pi}_{C_G(s)}(x, L/K)$ by Lemma 2.5(i). We have

$$\widetilde{\pi}_C(x, L/K) = \sum_{s\in S} \widetilde{\pi}_{C_G(s)}(x, L/K) = \sum_{s\in S} \lambda_s^{-1} \widetilde{\pi}_{C_H(s)}(x, L/L^H).$$

Using Frobenius reciprocity, cf. [Ser77, Theorem 13], we have

$$\lambda_s \cdot |C_G(s)|/|G| = \big\langle \lambda_s \cdot \delta_{C_G(s)}, 1_G \big\rangle_G = \big\langle \operatorname{Ind}_H^G \delta_{C_H(s)}, 1_G \big\rangle_G = \big\langle \delta_{C_H(s)}, 1_H \big\rangle_H = |C_H(s)|/|H|.$$

We have $|C_G(s)| = |G|/|\operatorname{Cent}_G(s)|$ and $|C_H(s)| = |H|/|\operatorname{Cent}_H(s)|$, where $\operatorname{Cent}_H(s)$ and $\operatorname{Cent}_G(s)$ are the centralizers of s in G and H, respectively. Therefore, $\lambda_s^{-1} = [\operatorname{Cent}_G(s) : \operatorname{Cent}_H(s)]^{-1} \le 1$ and hence

$$\widetilde{\pi}_C(x, L/K) \le \sum_{s\in S} \widetilde{\pi}_{C_H(s)}(x, L/L^H) \le \widetilde{\pi}_{C\cap H}(x, L/L^H).$$ □

In our applications, we will use Lemma 2.6 to reduce our computations of $\pi_C(x, L/K)$ to the case where G is abelian. The following says that $\widetilde{\pi}_C(x, L/K)$ is a good approximation of $\pi_C(x, L/K)$.

Lemma 2.7. *For any subset C of G stable under conjugation, we have*

$$\widetilde{\pi}_C(x, L/K) = \pi_C(x, L/K) + O\big([K:\mathbb{Q}]\big(\tfrac{x^{1/2}}{\log x} + \log M(L/K)\big)\big).$$

Proof. Let $\pi_K(x)$ be the number of $\mathfrak{p} \in \Sigma_K$ for which $N(\mathfrak{p}) \le x$. Since there are at most $[K:\mathbb{Q}]$ primes $\mathfrak{p} \in \Sigma_K$ dividing any p, we have $\pi_K(x) \ll [K:\mathbb{Q}] \cdot x/\log x$. For each $\mathfrak{p} \in \Sigma_K$, let $\deg \mathfrak{p}$ be the integer for which $N(\mathfrak{p}) = p^{\deg \mathfrak{p}}$, where p is the prime divisible by $\mathfrak{p}$. Define the sums

$$B_1 := \sum_{m \ge 2} \sum_{\substack{\mathfrak{p} \in \Sigma_K \\ N(\mathfrak{p})^m \le x}} \frac{1}{m}, \quad B_2 := \sum_{\substack{\mathfrak{p} \in \Sigma_K, \deg \mathfrak{p} > 1 \\ N(\mathfrak{p}) \le x}} 1 \quad \text{and} \quad B_3 := \sum_{\substack{\mathfrak{p} \in \Sigma_K \text{ ramified in } L \\ \deg \mathfrak{p} = 1,\, N(\mathfrak{p}) \le x}} 1.$$

We have $0 \le \widetilde{\pi}_C(x, L/K) - \pi_C(x, L/K) \le B_1 + B_2 + B_3$, so it suffices to bound the B_1, B_2 and B_3.

Let $M \ge 1$ be the largest integer for which $x^{1/M} \ge 2$. We have

$$B_1 \le \sum_{m=2}^{M} \frac{1}{m} \pi_K(x^{1/m}) \le [K:\mathbb{Q}] \sum_{m=2}^{M} \frac{1}{m} \frac{x^{1/m}}{\log(x^{1/m})} \le [K:\mathbb{Q}] \frac{x^{1/2}}{\log x} \sum_{m=2}^{M} \frac{1}{m^2} \ll [K:\mathbb{Q}] \frac{x^{1/2}}{\log x}.$$

We have $B_2 \le \sum_{p \le \sqrt{x}} [K:\mathbb{Q}] \ll [K:\mathbb{Q}] \cdot x^{1/2}/\log x$. If $\mathfrak{p} \in \Sigma_K$ is a prime with $\deg \mathfrak{p} = 1$ that ramifies in L, then $N(\mathfrak{p}) \in \mathcal{P}(L/K)$, where $\mathcal{P}(L/K)$ is the set from the definition of $M(L/K)$. Since there are at most $[K:\mathbb{Q}]$ primes $\mathfrak{p} \in \Sigma_K$ dividing any p, we have $B_3 \le [K:\mathbb{Q}] \sum_{p \in \mathcal{P}(L/K)} \log p \le [K:\mathbb{Q}] \log M(L/K)$. □

3. Galois representations

3.1. **Elliptic curves.** Fix a non-CM elliptic curve E defined over $\mathbb{Q}$. For each prime ℓ, let $E[\ell]$ be the ℓ-torsion subgroup of $E(\overline{\mathbb{Q}})$; it is a free $\mathbb{F}_\ell$-module of rank 2. There is a natural action of $\mathrm{Gal}_\mathbb{Q}$ on $E[\ell]$ that respects the group structure and can be expressed in terms of a Galois representation

$$\rho_{E,\ell} \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{F}_\ell}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell).$$

The representation $\rho_{E,\ell}$ is unramified at all primes $p \nmid N_E \ell$ and we have

$$\det(xI - \rho_{E,\ell}(\mathrm{Frob}_p)) \equiv x^2 - a_p(E)x + p \pmod{\ell}.$$

We have $\det \circ \rho_{E,\ell} = \chi_\ell$, where $\chi_\ell \colon \mathrm{Gal}_\mathbb{Q} \to \mathbb{F}_\ell^\times$ is the representation for which $\sigma(\zeta) = \zeta^{\chi_\ell(\sigma)}$ for all ℓ-th roots of unity $\zeta \in \overline{\mathbb{Q}}$. The following is an important theorem of Serre, cf. [Ser72].

Theorem 3.1 (Serre)**.** *The representation $\rho_{E,\ell}$ is surjective for all but finitely many primes ℓ.*

3.2. **Some class field theory.** Fix an imaginary quadratic field k and let $\mathcal{H}$ be its Hilbert class field. Denote the ring of integers of k by $\mathcal{O}$. Take any non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$. Let $v_\mathfrak{p} \colon k^\times \twoheadrightarrow \mathbb{Z}$ be the surjective discrete valuation corresponding to $\mathfrak{p}$ which we extend by setting $v_\mathfrak{p}(0) = +\infty$.

Fix an integer $m \ge 1$. Let I_k^m be the group of fractional ideals of k generated by prime ideals $\mathfrak{p} \nmid m$ of $\mathcal{O}$. Let

$$\iota \colon k_m := \{a \in k^\times : v_\mathfrak{p}(a) = 0 \text{ for all } \mathfrak{p} | m\} \to I_k^m$$

be the homomorphism that takes an element of k_m to the fractional ideal of k it generates. The ray class group modulo m is the group

$$\mathrm{Cl}_m := I_k^m / \iota(k_{m,1}),$$

where $k_{m,1} := \{a \in k_m : v_\mathfrak{p}(a-1) \ge v_\mathfrak{p}(m) \text{ for all } \mathfrak{p} | m\}$. Note that Cl_1 is the usual class group of $\mathcal{O}$ which we will also denote by Cl_k.

By class field theory, there is a continuous homomorphism

$$\widetilde{\psi}_{k,m} \colon \mathrm{Gal}_k \to \mathrm{Cl}_m$$

such that for each prime $\mathfrak{p} \nmid m$ of $\mathcal{O}$, $\widetilde{\psi}_{k,m}$ is unramified at $\mathfrak{p}$ and $\widetilde{\psi}_{k,m}(\mathrm{Frob}_\mathfrak{p})$ is the class of Cl_m represented by $\mathfrak{p}$. The map $\widetilde{\psi}_{k,m}$ is clearly surjective.

The homomorphism $\widetilde{\psi}_{k,1}$ is unramified at all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}$ and has image Cl_k. By class field theory, we deduce that the fixed field in $\bar{k}$ of $\ker(\widetilde{\psi}_{k,1})$ is $\mathcal{H}$, i.e., the Hilbert class field of k.

Lemma 3.2. *If $m \geq 5$, then there is an exact sequence of groups*

$$1 \to \mathcal{O}^\times \xrightarrow{\alpha_m} (\mathcal{O}/m\mathcal{O})^\times \xrightarrow{\beta_m} \mathrm{Cl}_m \xrightarrow{\gamma_m} \mathrm{Cl}_k \to 1,$$

where α_m is reduction modulo m, β_m maps a coset $a + m\mathcal{O}$ to the class of $\mathrm{Cl}_\mathfrak{m}$ containing $a\mathcal{O}$, and γ_m is induced by the natural map $I_k^m \to \mathrm{Cl}_k$.

Proof. Let $\bar{\iota}\colon k_m/k_{m,1} \to \mathrm{Cl}_m$ be the group homomorphism induced from $\iota\colon k_m \xrightarrow{\iota} I_k^m$. Since $\ker(\iota) = \mathcal{O}^\times$, we have an exact sequence

$$\mathcal{O}^\times \to k_m/k_{m,1} \xrightarrow{\bar{\iota}} \mathrm{Cl}_m\,.$$

We have $\mathcal{O}^\times \cap k_{m,1} = 1$ since $m \geq 5$. The group $I_k^m/\iota(k_m)$ is naturally isomorphic to Cl_k. We thus have an exact sequence

$$1 \to \mathcal{O}^\times \to k_m/k_{m,1} \xrightarrow{\bar{\iota}} \mathrm{Cl}_m \to \mathrm{Cl}_k \to 1. \tag{3.1}$$

Finally, we explain why $(\mathcal{O}/m\mathcal{O})^\times$ is isomorphic to $k_m/k_{m,1}$. We have a natural inclusion $k_m \hookrightarrow \mathcal{O}_m^\times$, where $\mathcal{O}_m$ is the m-adic completion of $\mathcal{O}$. Composing with the reduction modulo m map gives a group homomorphism, $f\colon k_\mathfrak{m} \to (\mathcal{O}_m/m\mathcal{O}_m)^\times = (\mathcal{O}/m\mathcal{O})^\times$. The kernel of f is $k_{m,1}$ and it is surjective by weak approximation. We thus an induced isomorphism $\overline{f}\colon k_m/k_{m,1} \xrightarrow{\sim} (\mathcal{O}/m\mathcal{O})^\times$. Identifying $k_m/k_{m,1}$ in (3.1) by $(\mathcal{O}/m\mathcal{O})^\times$ via the isomorphism $\overline{f}$, gives an exact sequence that agrees with the one in the statement of the lemma. □

We now focus on the case where m is a prime $\ell \geq 5$. By Lemma 3.2, we may view $\mathcal{O}^\times$ as a subgroup of $(\mathcal{O}/\ell\mathcal{O})^\times$. With γ_ℓ as in Lemma 3.2, we have $\widetilde{\psi}_{k,\ell} = \gamma_\ell \circ \widetilde{\psi}_{k,1}$. So by restricting $\widetilde{\psi}_{k,\ell}$ to $\mathrm{Gal}_\mathcal{H}$ and using Lemma 3.2, we obtain a surjective homomorphism

$$\psi_{k,\ell}\colon \mathrm{Gal}_\mathcal{H} \to (\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times.$$

Lemma 3.3. *Fix a prime $p \nmid \ell$ that splits completely in $\mathcal{H}$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_\mathcal{H}$ that divides p. The representation $\psi_{k,\ell}$ is unramified at $\mathfrak{P}$ and satisfies*

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

where π is a generator of the prime ideal $\mathfrak{P} \cap \mathcal{O}$ of $\mathcal{O}$.

Proof. Set $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}$; it is a prime that splits completely in $\mathcal{H}$. Since $\mathfrak{p} \nmid \ell$, $\widetilde{\psi}_{k,\ell}$ is unramified at $\mathfrak{p}$ and $\widetilde{\psi}_{k,\ell}(\mathrm{Frob}_\mathfrak{p}) = [\mathfrak{p}] \in \mathrm{Cl}_\ell$. That $\mathfrak{p}$ splits completely in $\mathcal{H}$ implies that $\gamma_\ell([\mathfrak{p}]) = 1$ and hence that $\mathfrak{p}$ is indeed principal, say $\mathfrak{p} = \pi\mathcal{O}$. We have $\gamma_\ell([\mathfrak{p}])$, so we may identify $\widetilde{\psi}_{k,\ell}(\mathrm{Frob}_\mathfrak{p}) = [\mathfrak{p}]$ with an element of $(\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times$ as viewed above as a subgroup of Cl_ℓ; in particular, we identify $\widetilde{\psi}_{k,\ell}(\mathrm{Frob}_\mathfrak{p})$ with the coset represented by π. Finally, since $\mathfrak{p}$ splits completely in $\mathcal{H}$ we find that $\widetilde{\psi}_{k,\ell}(\mathrm{Frob}_\mathfrak{P}) = \widetilde{\psi}_{k,\ell}(\mathrm{Frob}_\mathfrak{p})$. Therefore, $\psi_{k,\ell}(\mathrm{Frob}_\mathfrak{p})$ is represented by π as desired. □

Let $N_{k/\mathbb{Q}}\colon (\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times \to \mathbb{F}_\ell^\times$ be the homomorphism induces by the usual norm map $N_{k/\mathbb{Q}}\colon k \to \mathbb{Q}$; it is well defined since the norm map takes value 1 on $\mathcal{O}^\times$.

Lemma 3.4. *The homomorphism $N_{k/\mathbb{Q}} \circ \psi_{k,\ell}\colon \mathrm{Gal}_\mathcal{H} \to \mathbb{F}_\ell^\times$ agrees with $\chi_\ell|_{\mathrm{Gal}_\mathcal{H}}$.*

Proof. Take any prime $\mathfrak{P}|p$ as in the statement of Lemma 3.3. It suffices to show that $N_{k/\mathbb{Q}}(\psi_{k,\ell}(\mathrm{Frob}_{\mathfrak{P}})) = \chi_\ell(\mathrm{Frob}_{\mathfrak{P}})$ since such primes $\mathfrak{P}$ of $\mathcal{O}_{\mathcal{H}}$ have density 1. Since p splits completely in $\mathcal{H}$, we have $\chi_\ell(\mathrm{Frob}_{\mathfrak{P}}) \equiv N(\mathfrak{p}) = p \pmod{\ell}$.

By Lemma 3.3, we have $N_{k/\mathbb{Q}}(\psi_{k,\ell}(\mathrm{Frob}_{\mathfrak{P}})) \equiv N_{k/\mathbb{Q}}(\pi) \pmod{\ell}$, where $\pi \in \mathcal{O}$ is a generator of the ideal $\mathfrak{P} \cap \mathcal{O}$. Since p splits completely in $\mathcal{H}$, and hence also k, we have $N_{k/\mathbb{Q}}(\pi) = p$. Therefore, $N_{k/\mathbb{Q}}(\psi_{K,\ell}(\mathrm{Frob}_{\mathfrak{P}})) \equiv p \equiv \chi_\ell(\mathrm{Frob}_{\mathfrak{P}}) \pmod{\ell}$. □

3.3. **Mixed representations.** Let E be a non-CM elliptic curve over $\mathbb{Q}$. Let k be an imaginary quadratic field, let $\mathcal{O}$ be its ring of integers, and let $\mathcal{H}$ be its Hilbert class field.

Fix a prime $\ell \geq 5$. We have Galois representations $\rho_{E,\ell}$ and $\psi_{k,\ell}$ from the previous sections. By Lemma 3.4, we have $\det \circ \rho_{E,\ell}|_{\mathrm{Gal}_{\mathcal{H}}} = N_{k/\mathbb{Q}} \circ \psi_{k,\ell}$. We thus have a well-defined Galois representation

$$\Psi_\ell \colon \mathrm{Gal}_{\mathcal{H}} \to \mathcal{G}, \quad \sigma \mapsto (\rho_{E,\ell}(\sigma), \psi_{k,\ell}(\sigma)),$$

where $\mathcal{G} := \{(A, u) \in \mathrm{GL}_2(\mathbb{F}_\ell) \times ((\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times) : \det(A) = N_{k/\mathbb{Q}}(u)\}$.

The trace map $\mathrm{Tr}_{k/\mathbb{Q}} \colon k \to \mathbb{Q}$ induces a linear map $\mathrm{Tr}_{k/\mathbb{Q}} \colon \mathcal{O}/\ell\mathcal{O} \to \mathbb{F}_\ell$. For $u \in (\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times$, $\mathrm{Tr}_{k/\mathbb{Q}}(u)$ is a subset of $\mathbb{F}_\ell$ of cardinality at most $|\mathcal{O}^\times|$.

Lemma 3.5. *Let $p \nmid N_E$ be a prime for which E has ordinary reduction at p and for which $\mathbb{Q}(\pi_p)$ is isomorphic to k.*

(i) The prime p splits completely in $\mathcal{H}$.

(ii) Take any prime $\mathfrak{P} \in \Sigma_{\mathcal{H}}$ dividing $\pi_p\mathcal{O}$. Then for any prime $\ell \geq 5$ not equal to p, the representations $\rho_{E,\ell}$ and $\psi_{k,\ell}$ are unramified at $\mathfrak{P}$ and

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

Proof. To ease notation, set $k = \mathbb{Q}(\pi_p)$. Since π_p is a root of $x^2 - a_p(E)x + p$, we have $a_p(E) = \mathrm{Tr}_{k/\mathbb{Q}}(\pi_p)$ and $p = N_{k/\mathbb{Q}}(\pi_p)$. The equality $p = N_{k/\mathbb{Q}}(\pi_p)$ implies that p is either split or ramified in k, so $p\mathcal{O} = \mathfrak{p} \cdot \mathfrak{p}^\tau$, where $\mathfrak{p} := \pi_p\mathcal{O}$ and τ is the non-trivial automorphism of k.

We claim that p splits in k. Suppose otherwise that p is ramified in k. We then have

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

and hence $a_p(E) \equiv 0 \pmod{p}$ which contradicts our assumption that E has ordinary reduction at p.

Since $\mathfrak{p}$ and $\mathfrak{p}^\tau$ are principal ideals in $\mathcal{O}$, the prime p splits completely in $\mathcal{H}$. This completes the proof of (i).

Now take any prime $\ell \nmid 6p$ and any $\mathfrak{P} \in \Sigma_{\mathcal{H}}$ that divides $\mathfrak{p} = \pi_p\mathcal{O}$. Since p splits completely in $\mathcal{H}$, we have $\mathcal{O}_{\mathcal{H}}/\mathfrak{P} = \mathbb{F}_p$. Therefore, $\rho_{E,\ell}$ is unramified at $\mathfrak{P}$ and we have

$$\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}})) = \mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p)) \equiv a_p(E) \pmod{\ell}$$

By Lemma 3.3, we have $\psi_{k,\ell}(\mathrm{Frob}_{\mathfrak{P}}) = (\pi_p + \ell\mathcal{O}) \cdot \mathcal{O}^\times$. The image of $a_p(E) = \mathrm{Tr}_{k/\mathbb{Q}}(\pi_p)$ in $\mathbb{F}_\ell$ thus belongs to $\mathrm{Tr}_{k/\mathbb{Q}}(\psi_{k,\ell}(\mathrm{Frob}_{\mathfrak{P}}))$. Therefore, $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}})) \in \mathrm{Tr}_{k/\mathbb{Q}}(\psi_{k,\ell}(\mathrm{Frob}_{\mathfrak{P}}))$ as claimed. □

The representation Ψ_ℓ is surjective for all sufficiently large ℓ.

Lemma 3.6. *If $\rho_{E,\ell}$ is surjective, then the representation Ψ_ℓ is surjective.*

Proof. Let $p_1 \colon \mathcal{G} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ and $p_2 \colon \mathcal{G} \to (\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times$ be the projection maps. Let H be a subgroup of $\mathcal{G}$ with $p_1(H) \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$ and $p_2(H) = (\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times$.

We claim that $H = \mathcal{G}$. For a finite group G, let G' be the commutator subgroups of G. Since $p_1(H)$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$, we have

$$\mathrm{SL}_2(\mathbb{F}_\ell)' \subseteq p_1(H)' \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)' = \mathrm{SL}_2(\mathbb{F}_\ell).$$

The group $\mathrm{SL}_2(\mathbb{F}_\ell)$ is perfect since $\ell \geq 5$, so $p_1(H') = p_1(H)' = \mathrm{SL}_2(\mathbb{F}_\ell)$. We have $p_1(H') = \mathrm{SL}_2(\mathbb{F}_\ell)$ and $p_2(H') = ((\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times)' = \{1\}$, so $H' = \mathrm{SL}_2(\mathbb{F}_\ell) \times \{1\}$. The group H' is normal in $\mathcal{G}$ and p_2 induces an isomorphism $\mathcal{G}/H' \xrightarrow{\sim} (\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times$. Since $p_2|_H$ is surjective, we deduce that the natural map $H/H' \hookrightarrow \mathcal{G}/H'$ is surjective and hence $H = \mathcal{G}$.

Set $H := \Psi_\ell(\mathrm{Gal}_\mathcal{H})$. We have $p_2(H) = (\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times$ since $\psi_{k,\ell}$ is surjective. We have $p_1(H) = \rho_{E,\ell}(\mathrm{Gal}_\mathcal{H})$. Since $\rho_{E,\ell}$ is surjective, $\mathcal{H}/\mathbb{Q}$ is solvable, and $\mathrm{SL}_2(\mathbb{F}_\ell)$ is perfect, we have $\rho_{E,\ell}(\mathrm{Gal}_\mathcal{H}) \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$. From our claim, we deduce that $\Psi_\ell(\mathrm{Gal}_\mathcal{H}) = H = \mathcal{G}$. □

4. Proof of Theorem 1.2

Assume that GRH holds. Fix a non-CM elliptic curve $E/\mathbb{Q}$ and an integer a.

For each prime ℓ, we have constructed a representation $\rho_{E,\ell}\colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_\ell)$. Let I be the set of primes in the interval $[y, 2y]$, where y is a fixed real number that satisfies $c \leq y \leq x$ for some constant c depending on E. We will make a more specific choice of y later on. After increasing c, we may assume that I is non-empty and that $\rho_{E,\ell}$ is surjective for all primes $\ell \in I$.

For each prime ℓ, define

$$P_{E,a}(x,\ell) := \#\{p \leq x : p \nmid N_E,\ a_p(E) = a \text{ and } \ell \text{ splits in } \mathbb{Q}(\pi_p)\}.$$

Using our GRH assumption, Lemma 4.4 of [MMS88] shows that

$$P_{E,a}(x) \ll_E \max_{\ell \in I} P_{E,a}(x,\ell). \tag{4.1}$$

Now take any prime $\ell \in I$. Set $L := \mathbb{Q}(E[\ell])$; it is the fixed field in $\overline{\mathbb{Q}}$ of $\ker \rho_{E,\ell}$. Using $\rho_{E,\ell}$, we may identify the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ with $G := \mathrm{GL}_2(\mathbb{F}_\ell)$. Define

$$C := \{A \in G : \mathrm{tr}(A) \equiv a \bmod \ell \text{ and } \mathrm{tr}(A)^2 - 4\det(A) \in \mathbb{F}_\ell \text{ is a square}\};$$

it is a subset of G that is stable under conjugation.

Lemma 4.1. *We have $P_{E,k}(x,\ell) \leq \pi_C(x, L/\mathbb{Q}) + 1$.*

Proof. Take any prime $p \nmid N_E\ell$ such that $a_p(E) = a$ and ℓ splits in $\mathbb{Q}(\pi_p)$. The representation $\rho_{E,\ell}$ is unramified at p and we have $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p)) \equiv a_p(E) = a$ and $\det(\rho_{E,\ell}(\mathrm{Frob}_p)) \equiv p$ modulo ℓ.

Since ℓ splits in $\mathbb{Q}(\pi_p) \cong \mathbb{Q}((a_p(E)^2 - 4p)^{1/2})$, we find that the image of $a_p(E)^2 - 4p$ in $\mathbb{F}_\ell$ is a square. Therefore, $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p))^2 - 4\det(\rho_{E,\ell}(\mathrm{Frob}_p)) \in \mathbb{F}_\ell$ is a square.

We have thus shown that $\rho_{E,\ell}(\mathrm{Frob}_p) \subseteq C$. The bound $P_{E,k}(x,\ell) \leq \pi_C(x, L/\mathbb{Q}) + 1$ is now clear; we have added 1 to take into account the excluded prime $p = \ell$. □

Let B be the group of upper triangular matrices in G.

Lemma 4.2. *We have $P_{E,a}(x,\ell) \leq \widetilde{\pi}_{C\cap B}(x, L/L^B) + 1$.*

Proof. Observe that every conjugacy class of G in C contains an element from B. Lemma 2.6(i) implies that $P_{E,a}(x,\ell) \leq \widetilde{\pi}_C(x, L/\mathbb{Q}) + 1 \leq \widetilde{\pi}_{C\cap B}(x, L/L^B) + 1$. □

Let U be the subgroup of B consisting of the upper triangular matrices whose diagonal entries are both 1. The group U is normal in B and B/U is abelian. Let C' be the image of $C \cap B$ in $B/U = \mathrm{Gal}(L^U/L^B)$.

Lemma 4.3. *We have $P_{E,a}(x,\ell) \leq \widetilde{\pi}_{C'}(x, L^U/L^B) + 1$.*

Proof. We have $U \cdot (C \cap B) = C \cap B$. Lemma 2.6(ii) implies that $\widetilde{\pi}_{C\cap B}(x, L/L^B) = \widetilde{\pi}_{C'}(x, L^U/L^B)$. Therefore, $P_{E,a}(x,\ell) \leq \widetilde{\pi}_{C'}(x, L^U/L^B) + 1$ by Lemma 4.2. □

Before applying our Chebotarev bound to $\widetilde{\pi}_{C'}(x, L^U/L^B)$, we first bound some of the terms that will occur.

Lemma 4.4. *We have* $|C'| \ll \ell$, $|C'|/|B/U| \ll 1/\ell$, $[L^B : \mathbb{Q}] \ll \ell$ *and* $\log M(L^U/L^B) \ll_E \log \ell$.

Proof. We have $|G| = (\ell-1)^2(\ell+1)\ell \asymp \ell^4$, $|B| = (\ell-1)^2\ell \asymp \ell^3$, $|U| = \ell$ and $|B/U| = (\ell-1)\ell \asymp \ell^2$. We have $[L^B : \mathbb{Q}] = [G : B] \asymp \ell$. The map $(\mathbb{F}_\ell^\times)^2 \to B$, $(b_1, b_2) \mapsto \left(\begin{smallmatrix} b_1 & 0 \\ 0 & b_2 \end{smallmatrix}\right)$ induces an isomorphism $(\mathbb{F}_\ell^\times)^2 \xrightarrow{\sim} B/U$. Therefore,

$$|C'| = |\{(b_1, b_2) \in \mathbb{F}_\ell^2 : b_1 b_2 \neq 0,\ b_1 + b_2 \equiv a \bmod \ell\}| \leq \ell.$$

We thus have $|C'|/|B/U| \ll \ell/\ell^2 = \ell$. If a prime p ramifies in L, then $p | N_E \ell$. By Proposition 4′ of [Ser81], we have $\log(d_{L^B}^{1/[L^B:\mathbb{Q}]}) \ll_E \log(\ell \cdot [L^B : \mathbb{Q}]) \ll \log \ell$. □

The AHC conjecture holds for the extension L^U/L^B since its Galois group B/U is abelian. By Theorem 2.3 and our GRH assumption, we have

$$\begin{aligned}\widetilde{\pi}_{C'}(x, L^U/L^B) &\ll \frac{|C'|}{|B/U|}\frac{x}{\log x} + |C'|^{1/2}[L^B : \mathbb{Q}]\frac{x^{1/2}}{\log x}\log M(L^U/L^B) \\ &\ll_E \frac{1}{\ell}\frac{x}{\log x} + \ell^{1/2} \cdot \ell \cdot \frac{x^{1/2}}{\log x}\log \ell,\end{aligned}$$

where the last line uses Lemma 4.4. Lemma 4.3 and $\ell \in [y, 2y]$ implies that

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

Since this holds for all $\ell \in I$, the inequality (4.1) gives

$$P_{E,a}(x) \ll_E \frac{1}{y}\frac{x}{\log x} + y^{3/2}\frac{x^{1/2}}{\log x}\log y.$$

Take $y := c' \cdot x^{1/5}/(\log x)^{2/5}$, where c' is a constant chosen large enough to ensure that $y \geq c$ for all $x \geq 2$. With this choice of y, we obtain the bound $P_{E,a}(x) \ll_E x^{4/5}/(\log x)^{3/5}$.

Finally consider the case where $a = 0$. Take any $\ell \in I$ and keep notation as above. Let H be the subgroup of B consisting of the matrices whose eigenvalues are both equal; it is a normal subgroup of B and we have $H \cdot (C \cap B) = C \cap B$ (multiplying a trace 0 matrix by a scalar does not change the trace). Lemma 2.6(ii) implies that $\widetilde{\pi}_{C\cap B}(x, L/L^B) = \widetilde{\pi}_{C''}(x, L^H/L^B)$, where C'' is the image of $C \cap H$ in B/H. Therefore, $P_{E,a}(x, \ell) \leq \widetilde{\pi}_{C''}(x, L^H/L^B) + 1$ by Lemma 4.2. Arguing as above, and using $|B/H| = \ell - 1$ and $|C''| = 1$, we have

$$P_{E,0}(x) \ll \max_{\ell \in I} P_{E,0}(x, \ell) \ll \max_{\ell \in I}\left(\frac{1}{\ell}\frac{x}{\log x} + 1^{1/2} \cdot \ell \cdot \frac{x^{1/2}}{\log x}\log \ell\right).$$

Choosing $y \asymp x^{1/4}/(\log x)^{1/2}$, we deduce that $P_{E,0}(x) \ll x^{3/4}/(\log x)^{1/2}$.

5. Proof of Theorem 1.3

Fix a non-CM elliptic curve E over $\mathbb{Q}$ and an imaginary quadratic field k. Let $\mathcal{O}$ be the ring of integers of k. Let $\mathcal{H}$ be the Hilbert class field of k and let h_k be the class number of k. Fix a prime $\ell \geq 5$ such that $\rho_{E,\ell}$ is surjective and ℓ *splits* in k; we will make a more specific choice later.

In §3.3, we constructed a Galois representation

$$\Psi_\ell \colon \mathrm{Gal}_{\mathcal{H}} \to \mathcal{G},$$

where $\mathcal{G} := \{(A,u) \in \mathrm{GL}_2(\mathbb{F}_\ell) \times ((\mathcal{O}/\ell\mathcal{O})^\times/\mathcal{O}^\times) : \det(A) = N_{k/\mathbb{Q}}(u)\}$. The representation Ψ_ℓ is surjective by Lemma 3.6. Let L be the fixed field in $\overline{\mathcal{H}}$ of $\ker \Psi_\ell$. Using Ψ_ℓ, we will identify the Galois group $\mathrm{Gal}(L/\mathcal{H})$ with $\mathcal{G}$.

Recall that the trace map $\mathrm{Tr}_{k/\mathbb{Q}}\colon k \to \mathbb{Q}$ induces a linear map $\mathrm{Tr}_{k/\mathbb{Q}}\colon \mathcal{O}/\ell\mathcal{O} \to \mathbb{F}_\ell$. Define the set

$$\mathcal{C} := \{(A,u) \in \mathcal{G} : \mathrm{tr}(A) \in \mathrm{Tr}_{k/\mathbb{Q}}(u),\ \mathrm{tr}(A)^2 - 4\det(A) \in \mathbb{F}_\ell \text{ is a square}\};$$

it is a subset of $\mathcal{G}$ stable under conjugacy. We now give a useful bound for $P_{E,k}(x)$.

Lemma 5.1. *We have* $P_{E,k}(x) \le \frac{1}{h_k}\pi_{\mathcal{C}}(x, L/\mathcal{H}) + 4$.

Proof. Take any prime $p \nmid N_E\ell$ for which E has ordinary reduction at p and for which $k \cong \mathbb{Q}(\pi_p)$. By Lemma 3.5, the prime p splits completely in $\mathcal{H}$. Let $\mathfrak{P} \in \Sigma_{\mathcal{H}}$ be any of the h_k primes that divide $\pi_{\mathfrak{p}}\mathcal{O}$. By Lemma 3.5, we have $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}})) \in \mathrm{Tr}_{k/\mathbb{Q}}(\psi_{k,\ell}(\mathrm{Frob}_{\mathfrak{P}}))$.

Since $k \cong \mathbb{Q}(\pi_p)$ and ℓ splits in k, the polynomial $x^2 - a_p(E)x + p$ will factor modulo ℓ. Therefore, the image of $a_p(E)^2 - 4p$ in $\mathbb{F}_\ell$ is a square. Since p splits completely in $\mathcal{H}$, we have $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}})) = \mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p))$ and $\det(\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}})) = \det(\rho_{E,\ell}(\mathrm{Frob}_p))$. Therefore, $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}}))^2 - 4\det(\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}})) \equiv a_p(E)^2 - 4p \pmod{\ell}$ is a square.

We have verified that $\Psi_\ell(\mathrm{Frob}_{\mathfrak{P}}) \subseteq \mathcal{C}$ for each of the h_k primes $\mathfrak{P}$ dividing $\pi_p\mathcal{O}$. So the set

$$\{p \le x : p \nmid N_E,\ \mathbb{Q}(\pi_p) \cong k\} - (S \cup \{\ell\})$$

has cardinality at most $\frac{1}{h_k}\pi_C(x, L/\mathcal{H})$, where S is the set of primes $p \nmid N_E$ for which E has supersingular reduction at p and $\mathbb{Q}(\pi_p) \cong k$. It thus suffices to show that $|S| \le 3$.

Take any prime $p \in S$ with $p \ge 5$. Since E has supersingular reduction at $p \ge 5$, we have $a_p(E) = 0$. Therefore, k is isomorphic to $\mathbb{Q}(\pi_p) \cong \mathbb{Q}(\sqrt{-p})$. So if $p \in S$, then p is 2, 3 or the unique prime (if it exists) such that $k \cong \mathbb{Q}(\sqrt{-p})$. Therefore, $|S| \le 3$. □

Let B be the group of upper triangular matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Define

$$\mathcal{B} := \{(A,u) \in \mathcal{G} : A \in B\};$$

it is a subgroup of $\mathcal{G}$. We can identify $\mathcal{B}$ with the Galois group $\mathrm{Gal}(L/L^{\mathcal{B}})$.

Lemma 5.2. *We have* $P_{E,k}(x) \le \frac{1}{h_k}\widetilde{\pi}_{\mathcal{C}\cap\mathcal{B}}(x, L/L^{\mathcal{B}}) + 4$.

Proof. Any matrix $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ with $\mathrm{tr}(A)^2 - 4\det(A) \in \mathbb{F}_\ell$ a square is conjugate to a matrix in B. Therefore, every element of $\mathcal{C}$ is conjugate in $\mathcal{G}$ to some element of $\mathcal{B}$. By Lemma 2.6(i), we have $\widetilde{\pi}_{\mathcal{C}}(x, L/\mathcal{H}) \le \widetilde{\pi}_{C\cap\mathcal{B}}(x, L/L^{\mathcal{B}})$. The lemma now follows from Lemma 5.1 and the easy bound $\pi_{\mathcal{C}}(x, L/\mathcal{H}) \le \widetilde{\pi}_{\mathcal{C}}(x, L/\mathcal{H})$. □

Let $\mathcal{U}$ be the image of the group

$$\{(A,a) \in \mathrm{GL}_2(\mathbb{F}_\ell) \times \mathbb{F}_\ell^\times : \text{the eigenvalues of } A \text{ are both } a\}$$

in $\mathcal{G}$ (we can identify $\mathbb{F}_\ell^\times$ with a subgroup of $(\mathcal{O}/\ell\mathcal{O})^\times$ since $\mathbb{F}_\ell$ is a subalgebra of $\mathcal{O}/\ell\mathcal{O}$). The group $\mathcal{U}$ is normal in $\mathcal{B}$ and $\mathcal{B}/\mathcal{U}$ is an abelian group. We can identify $\mathcal{B}/\mathcal{U}$ with the Galois group $\mathrm{Gal}(L^{\mathcal{U}}/L^{\mathcal{B}})$. Let $\mathcal{C}'$ be the image of $\mathcal{C} \cap \mathcal{B}$ under the homomorphism $\mathcal{B} \to \mathcal{B}/\mathcal{U}$; it is stable under conjugacy in $\mathcal{B}/\mathcal{U}$.

Lemma 5.3. *We have* $P_{E,k}(x) \le \frac{1}{h_k}\widetilde{\pi}_{\mathcal{C}'}(x, L^{\mathcal{U}}/L^{\mathcal{B}}) + 4$.

Proof. Observe that $\mathcal{U} \cdot (\mathcal{C} \cap \mathcal{B}) = \mathcal{C} \cap \mathcal{B}$; whether an element $(A,u) \in \mathcal{B}$ belongs to $\mathcal{C}$ depends only on u and the eigenvalues of A, and that $\mathrm{tr}(A) \in \mathrm{Tr}_{k/\mathbb{Q}}(u)$ remains true if A and u are multiplied by a common scalar in $\mathbb{F}_\ell^\times$. Lemma 2.6(ii) implies that $\widetilde{\pi}_{\mathcal{C}\cap\mathcal{B}}(x, L/L^{\mathcal{B}}) = \widetilde{\pi}_{C'}(x, L^{\mathcal{U}}/L^{\mathcal{B}})$. The lemma then follows from Lemma 5.2. □

Since $L^{\mathcal{U}}/L^{\mathcal{B}}$ is an abelian extension, we can now apply our Chebotarev bounds to obtain bounds for $P_{E,k}(x)$. We first bound some terms that will show up.

Lemma 5.4.

(i) We have $|\mathcal{G}| \asymp \ell^5$, $|\mathcal{B}| \asymp \ell^4$ and $|\mathcal{U}| \asymp \ell^2$.
(ii) We have $|\mathcal{C}'| \ll \ell$ and $|\mathcal{C}'|/|\mathcal{B}/\mathcal{U}| \ll 1/\ell$.
(iii) We have $[L^{\mathcal{B}} : \mathbb{Q}] \ll h_k \ell$.
(iv) We have $\log M(L^{\mathcal{U}}/L^{\mathcal{B}}) \ll_E \log(d_k \ell)$.

Proof. Since ℓ splits in k, we have $(\mathcal{O}/\ell\mathcal{O})^\times \cong \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$. Therefore,

$$|\mathcal{C} \cap \mathcal{B}| \le |\{(A, b, c) \in B \times \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times : \det(A) = bc \text{ and } \operatorname{tr}(A) = b + c\}| \le 2|B|,$$

where the last inequality uses that $x^2 - \operatorname{tr}(A)x + \det(A)$ has at most two roots $b, c \in \mathbb{F}_\ell$. We thus have $|\mathcal{C} \cap \mathcal{B}| \le 2\ell^3$. Since $\mathcal{U} \cdot (\mathcal{C} \cap \mathcal{B}) = \mathcal{C} \cap \mathcal{B}$, we have $|\mathcal{C}'| = |\mathcal{C} \cap \mathcal{B}|/|\mathcal{U}| \le 2\ell^3/|\mathcal{U}| \ll \ell$. We have $|\mathcal{C}'|/|\mathcal{B}/\mathcal{U}| \ll 1/\ell$ since $|\mathcal{B}/\mathcal{U}| \asymp \ell^2$. We have $[L^{\mathcal{B}} : \mathbb{Q}] = [\mathcal{H} : \mathbb{Q}][L^{\mathcal{B}} : \mathcal{H}] = 2h_k \cdot [\mathcal{G} : \mathcal{B}]$, so $[L^{\mathcal{B}} : \mathbb{Q}] \ll h_k \ell$.

Let $\mathcal{P}$ be the set of rational primes p divisible by some $\mathfrak{P} \in \Sigma_{\mathcal{H}}$ that ramifies in L. Each prime in $\mathcal{P}$ divides $N_E \ell$. We have $[\mathcal{B} : \mathcal{U}] \ll \ell^2$, so

$$\log M(L^{\mathcal{U}}/L^{\mathcal{B}}) \le \log\left([\mathcal{B} : \mathcal{U}] d_{L^{\mathcal{B}}}^{1/[L^{\mathcal{B}}:\mathbb{Q}]} \cdot N_E \ell\right) \ll_E [L^{\mathcal{B}} : \mathbb{Q}]^{-1} \log(d_{L^{\mathcal{B}}}) + \log \ell.$$

It thus suffices to prove that $[L^{\mathcal{B}} : \mathbb{Q}]^{-1} \log(d_{L^{\mathcal{B}}}) \ll_E \log(d_k \ell)$. By Proposition 4 of [Ser81], we have

$$[L^{\mathcal{B}} : \mathbb{Q}]^{-1} \log(d_{L^{\mathcal{B}}}) \le [\mathcal{H} : \mathbb{Q}]^{-1} \log(d_{\mathcal{H}}) + \sum\nolimits_{p \in \mathcal{P}} \log p + |\mathcal{P}| \log([L^{\mathcal{B}} : \mathcal{H}]).$$

We have $[L^{\mathcal{B}} : \mathcal{H}] \ll \ell$, so $[L^{\mathcal{B}} : \mathbb{Q}]^{-1} \log(d_{L^{\mathcal{B}}}) \ll_E [\mathcal{H} : \mathbb{Q}]^{-1} \log(d_{\mathcal{H}}) + \log \ell$. Since $\mathcal{H}/k$ is unramified, Proposition 4 of [Ser81] implies that $[\mathcal{H} : \mathbb{Q}]^{-1} \log(d_{\mathcal{H}}) = 2^{-1} \log d_k$ and hence $[L^{\mathcal{B}} : \mathbb{Q}]^{-1} \log(d_{L^{\mathcal{B}}}) \ll_E \log(d_k \ell)$. □

Lemma 5.5. *If $d_k > 4x$, then $P_{E,k}(x) = 0$.*

Proof. Suppose that $d_k > 4x$ and $P_{E,k}(x) > 0$. There is thus a prime $p \nmid N_E$ satisfying $p \le x$ and $k \cong \mathbb{Q}(\pi_p)$. We have $\mathbb{Q}(\sqrt{a_p(E)^2 - 4p}) \cong \mathbb{Q}(\sqrt{-d_k})$, and hence d_k divides $a_p(E)^2 - 4p$ (the divisibility with respect to the prime 2 uses that $a_p(E)^2 - 4p$ is congruent to 0 or 1 modulo 4). Therefore, $d_k \le 4p - a_p(E)^2 \le 4x$ which contradicts our assumption. □

By Lemma 5.5, we may assume that $d_k \le 4x$; the desired bounds are trivial otherwise.

5.1. **Conditional bounds.** Assume that GRH holds.

By Lemma 5.3, Theorem 2.3 and Lemma 2.7, we have

$$\begin{aligned} P_{E,k}(x) &\le \frac{1}{h_k} \widetilde{\pi}_{\mathcal{C}'}(x, L^{\mathcal{U}}/L^{\mathcal{B}}) + 4 \\ &\ll \frac{1}{h_k}\Big(\frac{|\mathcal{C}'|}{|\mathcal{B}/\mathcal{U}|}\frac{x}{\log x} + |\mathcal{C}'|^{1/2}\,[L^{\mathcal{B}} : \mathbb{Q}]\frac{x^{1/2}}{\log x}\,\log M(L^{\mathcal{U}}/L^{\mathcal{B}})\Big) + 4 \\ &\ll_E \frac{1}{h_k}\frac{1}{\ell}\frac{x}{\log x} + \ell^{3/2}\,\frac{x^{1/2}}{\log x}\log(d_k \ell). \end{aligned}$$

Using Lemma 5.4 and $d_k \le 4x$, we find that

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

We still need to choose our prime ℓ.

Lemma 5.6. *Assuming GRH, there is an absolute constant $\gamma > 0$ such that if $y \geq \gamma(\log d_k)^2$, then there exists a prime ℓ in the interval $[y, 2y]$ that splits completely in k.*

Proof. This follows from Corollary 2.4 with the extension $k/\mathbb{Q}$. □

Define

$$y := \begin{cases} C \cdot h_k^{-2/5} \cdot x^{1/5}/(\log x)^{2/5} & \text{if } h_k \leq x^{1/2}/(\log x)^6, \\ C \cdot (\log x)^2 & \text{otherwise,} \end{cases}$$

where $C > 0$ is some constant depending only on E. In both cases, we have $y \geq C(\log x)^2$.

Since $d_k \leq 4x$, we have, after possibly increasing C, that $y \geq \gamma(\log d_k)^2$ with γ as in Lemma 5.6. By Lemma 5.6, there is a prime $\ell \in [y, 2y]$ that splits completely in k. After possibly increasing the constant C first, we may assume by Theorem 3.1 that $\rho_{E,\ell}$ is surjective and that $\ell \geq 5$. With this prime ℓ, we obtain the bound

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

Since $y \ll_E x$, we have

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

If $h_k \leq x^{1/2}/(\log x)^6$, then substituting y gives the bound

$$P_{E,k}(x) \ll_E h_k^{-3/5}x^{4/5}/(\log x)^{3/5};$$

our y was chosen so that both terms in (5.1) have the same magnitude. In the case $h_k > x^{1/2}/(\log x)^6$, we obtain

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

The bound of Theorem 1.3(i) follows by adding our two possible bounds for $P_{E,k}(x)$.

5.2. **Unconditional bounds.** Define

$$y := C\frac{1}{h_k}\frac{\log x}{(\log\log x)^2},$$

where $C > 0$ is a constant depending only on E to be chosen later. Suppose that there is a prime ℓ in the interval $[y, 2y]$ such that ℓ splits in k, $\ell \geq 5$, and $\rho_{E,\ell}$ is surjective.

The group $\mathcal{B}/\mathcal{U} = \mathrm{Gal}(L^{\mathcal{U}}/L^{\mathcal{B}})$ is abelian. By Theorem 2.1(ii), there are absolute constants $b, c > 0$ such that if $\log x \geq b[L^{\mathcal{B}} : \mathbb{Q}]\log^2 M(L^{\mathcal{U}}/L^{\mathcal{B}})$, then

$$\pi_{\mathcal{C}'}(x, L^{\mathcal{U}}/L^{\mathcal{B}}) \ll \frac{|\mathcal{C}'|}{|\mathcal{B}/\mathcal{U}|}\,\frac{x}{\log x} + |\mathcal{C}'|^{1/2}\,[L^{\mathcal{B}} : \mathbb{Q}]x\exp\left(-\frac{c(\log x)^{1/2}}{[L^{\mathcal{B}} : \mathbb{Q}]^{1/2}}\right)\log^2(M(L^{\mathcal{U}}/L^{\mathcal{B}})x),$$

where we have used that $\beta_{L^{\mathcal{U}}} \leq 1$ if it exists.

By Lemma 5.4, we have

$$[L^{\mathcal{B}} : \mathbb{Q}]\log^2 M(L^{\mathcal{U}}/L^{\mathcal{B}}) \ll h_k\ell\log^2(d_k\ell) \ll h_k\ell\log^2(h_k\ell),$$

where the last inequality use the Brauer-Seigel theorem. Using Lemma 5.4, we deduce that there are positive absolute constants b' and c' such that if $\log x \geq b' \cdot h_k\ell \cdot \log^2(h_k\ell)$, then

$$\pi_{\mathcal{C}'}(x, L^{\mathcal{U}}/L^{\mathcal{B}}) \ll_E \frac{1}{\ell}\,\frac{x}{\log x} + h_k\ell^{3/2}x\exp\left(-c'\sqrt{\frac{\log x}{h_k\ell}}\right)\log^2(h_k\ell \cdot x).$$

Using that $\ell \in [y, 2y]$, we have

$$\pi_{\mathcal{C}'}(x, L^{\mathcal{U}}/L^{\mathcal{B}}) \ll_E h_k \frac{x(\log\log x)^2}{(\log x)^2} + \frac{1}{\sqrt{h_k}} \cdot \frac{(\log x)^{3/2}}{(\log\log x)^3} \cdot x \exp\left(- \frac{c'}{2\sqrt{C}} \log\log x \right) (\log x)^2.$$

By taking our constant $C > 0$ sufficiently small, we find that $\pi_{\mathcal{C}'}(x, L^{\mathcal{U}}/L^{\mathcal{B}}) \ll_E h_k \cdot \frac{x(\log\log x)^2}{(\log x)^2}$. By Lemmas 2.7 and 5.4, we find that $\tilde{\pi}_{\mathcal{C}'}(x, L^{\mathcal{U}}/L^{\mathcal{B}}) \ll_E h_k \cdot x(\log\log x)^2/(\log x)^2$. Therefore,

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

by Lemma 5.3.

Finally, we now need to know that such a prime ℓ exists; at least if x is sufficiently large. By the Chebotarev density theorem and Theorem 3.1, there is a constant $\gamma \geq 1$, depending on E and k, such that if $y \geq \gamma$, then there is a prime $\ell \in [y, 2y]$ for which ℓ splits in k and $\rho_{E,\ell}$ is surjective. So for x sufficiently large, we will have $y \geq \gamma$ and the desired prime ℓ exists. (One could make this explicit by using an effective version of the Chebotarev density theorem.) This completes the proof of Theorem 1.3(ii).

6. Proof of Corollary 1.4

We start with the identity

$$\pi(x) = |\{p \leq x : p | N_E\}| + \sum\nolimits_{k \in D_E(x)} P_{E,k}(x).$$

Theorem 1.3(i) then implies that

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

Using GRH, one can show that, $h_k \gg d_k^{1/2}/\log d_k$. By Lemma 5.5, we have $d_k \leq 4x$ for all $k \in D_E(x)$. Using these bounds, we have:

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

Therefore, $\sum_{k \in D_E(x)} h_k^{-3/5} \ll |D_E(x)|^{7/10} (\log x)^{3/5}$. Combining with our previous inequality, we have

$$x/\log x \ll_E |D_E(x)|^{7/10} x^{4/5} + |D_E(x)| x^{1/2} (\log x)^3.$$

Therefore, we have $x/\log x \ll_E |D_E(x)|^{7/10} x^{4/5}$ or $x/\log x \ll_E |D_E(x)| x^{1/2} (\log x)^3$. Equivalently, we have $|D_E(x)| \gg_E x^{2/7}/(\log x)^{10/7}$ or $|D_E(x)| \gg_E x^{1/2}/(\log x)^4$. We conclude that $|D_E(x)| \gg_E x^{2/7}/(\log x)^{10/7}$ since this is the weaker of the two possible bounds.

Remark 6.1. If we had instead used the bound $P_{E,k}(x) \ll_E x^{4/5}/(\log x)^{3/5}$, then we would have deduced that $|D_E(x)| \gg_E x^{1/5}/(\log x)^{2/5}$. Thus the factor $h_k^{-3/5}$ occuring in our bound of $P_{E,k}(x)$ gives a significant improvement.

7. Proof of Theorem 2.2

Fix a real number $x \geq 2$. For each class function $\varphi\colon G \to \mathbb{C}$, we define

$$\Theta_\varphi(x) := \sum_{\mathfrak{p}\in\Sigma_K, m\geq 1} \varphi(\mathrm{Frob}_\mathfrak{p}^m) \log N(\mathfrak{p}) \cdot f(N(\mathfrak{p})^m/x).$$

We first estimate $\Theta_\chi(x)$ for irreducible characters $\chi\colon G \to \mathbb{C}$.

Lemma 7.1. *For any irreducible character χ of G, we have*

$$\Theta_\chi(x) = \delta_\chi \cdot x \int_0^\infty f(t)\,dt + O_f\Big(\chi(1)[K:\mathbb{Q}]x^{1/2}\log M(L/K)\Big),$$

where $\delta_\chi = 1$ if $\chi = 1$ and $\delta_\chi = 0$ otherwise.

Proof. Let $L(s,\chi)$ be the Artin L-function arising from χ; for background on Artin L-functions see [Mar77]. By our AHC assumption, the series $L(s,\chi)$ extends to a function analytic everywhere except at $s = 1$ when $\chi = 1$. We have $\mathrm{ord}_{s=1} L(s,\chi) = -\delta_\chi$.

Define $A_\chi := d_K^{\chi(1)} \cdot N(\mathcal{F}_\chi)$, where $\mathcal{F}_\chi \subseteq \mathcal{O}_K$ is the Artin conductor corresponding to χ. We define the completed L-function $\Lambda(s,\chi) := A_\chi^{s/2}\gamma_\chi(s)L(s,\chi)$, where $\gamma_\chi(s)$ is a certain product of Γ-factors. See [Mar77, p.12] for the precise definition of γ_χ; we simply note that there are explicit positive integers a and b with $a + b = \chi(1)[K:\mathbb{Q}]$ such that

$$\gamma_\chi(s) = (\pi^{-s/2}\Gamma(\tfrac{s}{2}))^a \cdot (\pi^{-(s+1)/2}\Gamma(\tfrac{s+1}{2}))^b.$$

The functional equation for $\Lambda(s,\chi)$ says that

$$\Lambda(s,\chi) = W_\chi \cdot \Lambda(1-s,\overline{\chi})$$

for some $W_\chi \in \mathbb{C}^\times$ with absolute value 1. The logarithmic derivative of the Artin L-series of $L(s,\chi)$ is

$$\frac{L'}{L}(s,\chi) = -\sum_{\mathfrak{p}\in\Sigma_K} \log N(\mathfrak{p}) \sum_{m\geq 1} \chi(\mathrm{Frob}_\mathfrak{p}^m) N(\mathfrak{p})^{-ms}.$$

In particular, $-\frac{L'}{L}(s,\chi) = \sum_{n\geq 1} \Lambda_\chi(n) n^{-s}$, where

$$\Lambda_\chi(n) := \log n \sum_{\substack{\mathfrak{p}\in\Sigma_K, m\geq 1\\ N(\mathfrak{p})^m = n}} \frac{1}{m}\chi(\mathrm{Frob}_\mathfrak{p}^m).$$

Let $\varphi\colon (0,+\infty) \to \mathbb{C}$ be a smooth function with compact support. The Mellin transform of φ is

$$\widehat{\varphi}(s) := \int_0^\infty \varphi(t) t^s \frac{dt}{t}.$$

Define the function $\psi\colon (0,+\infty) \to \mathbb{C}$ by $\psi(t) := t^{-1}\varphi(t^{-1})$. The explicit formula, as given by Iwaniec and Kowalski in Theorem 5.11 of [IK04], says that

$$\sum_{n\geq 1}\Big(\Lambda_\chi(n)\varphi(n) + \overline{\Lambda_\chi(n)}\psi(n)\Big) = \varphi(1)\log A_\chi + \delta_\chi\int_0^\infty \varphi(t)\,dt + \frac{1}{2\pi i}\int_{(1/2)}\Big(\frac{\gamma_\chi'}{\gamma_\chi}(s) + \frac{\gamma_{\overline{\chi}}'}{\gamma_{\overline{\chi}}}(1-s)\Big)\widehat{\varphi}(s)\,ds - \sum_\rho \widehat{\varphi}(\rho), \tag{7.1}$$

where the sum is over the zeros ρ of $L(s,\chi)$, with multiplicity, for which $0 \leq \mathrm{Re}(\rho) \leq 1$. The explicit formula in [IK04] is given for a general L-function that satisfies certain properties; they are all known to hold for Artin L-function except for the analytic continuation which holds by our

ongoing AHC assumption.

We now take $\varphi\colon (0,+\infty)\to\mathbb{C}$ to be the function $\varphi(t)=f(t/x)$. Observe that

$$\Theta_\chi(x)=\sum_{n\geq 1}\Lambda_\chi(n)\varphi(n)$$

and that $\delta_\chi\int_0^\infty \varphi(t)\,dt=\delta_\chi x\int_0^\infty f(t)\,dt$; it thus remains to bound the other terms occurring in (7.1).

We first bound $\sum_{n\geq 1}\overline{\Lambda_\chi(n)}\psi(n)$. If $\Lambda_\chi(n)$ is non-zero, then n is a prime power. Since there are at most $[K:\mathbb{Q}]$ primes $\mathfrak{p}\in\Sigma_K$ dividing a fixed rational prime, we have $|\Lambda_\chi(n)|\leq \log n\cdot\chi(1)[K:\mathbb{Q}]$. There is a number $c>0$, depending only on f, such that $f(t)=0$ for $t\leq c$. If $n\geq c^{-1}$, then $1/(xn)\leq c$ and hence $\psi(n)=n^{-1}f(1/(xn))=0$. Therefore,

$$\sum_{n\geq 1}\overline{\Lambda_\chi(n)}\psi(n)\ll\sum_{n\leq c^{-1}}|\Lambda_\chi(n)|\,|\psi(n)|\leq\chi(1)[K:\mathbb{Q}]\sum_{n\leq c^{-1}}\log n\cdot\sup_{t\in\mathbb{R}}|f(t)|\ll_f\chi(1)[K:\mathbb{Q}].$$

We have $\log A_\chi\ll\chi(1)[K:\mathbb{Q}]\log M(L/K)$ by Proposition 2.5 of [MMS88]. Therefore, $\varphi(1)\log A_\chi\ll_f\chi(1)[K:\mathbb{Q}]\log M(L/K)$.

For $y\in\mathbb{R}$, we have

$$\widehat{\varphi}(1/2+iy)=\int_0^\infty f(t/x)t^{1/2+iy}\,\frac{dt}{t}=x^{1/2}\cdot x^{iy}\int_{-\infty}^\infty f(e^u)e^{u/2}e^{i\cdot uy}\,du,$$

where we have made the substitution $t=xe^u$. We have $\int_{-\infty}^\infty f(e^u)e^{u/2}e^{i\cdot uy}\,du\ll_f 1/(|y|+1)^2$ since $f(e^u)e^{u/2}$, and hence also its Fourier transform, is a Schwartz function. Therefore,

$$\widehat{\varphi}(1/2+iy)\ll_f x^{1/2}/(|y|+1)^2.$$

Using that $\frac{\Gamma'}{\Gamma}(1/2+iy)\ll\log(|y|+2)$ for all real y (cf. Lemma 6.1 of [LO77]), we have

$$\tfrac{\gamma_\chi'}{\gamma_\chi}(1/2+iy)\ll\chi(1)[K:\mathbb{Q}]x^{1/2}/(|y|+1)^2.$$

Therefore,

$$\int_{(1/2)}\Big(\tfrac{\gamma_\chi'}{\gamma_\chi}(s)+\tfrac{\gamma_{\overline{\chi}}'}{\gamma_{\overline{\chi}}}(1-s)\Big)\widehat{\varphi}(s)\,ds\ll_f\chi(1)[K:\mathbb{Q}]x^{1/2}\int_{-\infty}^\infty\tfrac{\log(|y|+2)}{(|y|+1)^2}\,dy\ll\chi(1)[K:\mathbb{Q}]x^{1/2}.$$

We now bound the sum $\sum_\rho\widehat{\varphi}(\rho)$. We have $\zeta_L(s)=\prod_\chi L(s,\chi)^{\chi(1)}$, where the product is over irreducible characters χ of G and ζ_L is the Dedekind zeta function of L. By assumption, AHC holds for L/K and GRH holds for L, so we deduce that any zero ρ of $L(s,\chi)$ with $0\leq\mathrm{Re}(s)\leq 1$ satisfies $\mathrm{Re}(s)=1/2$. Therefore,

$$\sum_\rho\widehat{\varphi}(\rho)\ll_f x^{1/2}\sum_{\rho=1/2+iy}1/(|y|+1)^2.$$

For each real number t, let $N(t,\chi)$ be the number of zeros $\rho=1/2+iy$ of $L(s,\chi)$, counted with multiplicity, such that $|t-y|\leq 1$. From equation (3.5.5) and Proposition 2.5 of [MMS88], we have

$$N(t,\chi)\ll\chi(1)[K:\mathbb{Q}]\log M(L/K)+\chi(1)[K:\mathbb{Q}]\log(|t|+2).$$

Therefore,

$$\begin{aligned}\sum_\rho\widehat{\varphi}(\rho)\ll_f x^{1/2}\sum_{n\in\mathbb{Z}}\frac{N(n,\chi)}{(|n|+1)^2}&\ll x^{1/2}\chi(1)[K:\mathbb{Q}]\log M(L/K)\sum_{n\in\mathbb{Z}}\frac{\log(|n|+2)}{(|n|+1)^2}\\&\ll x^{1/2}\chi(1)[K:\mathbb{Q}]\log M(L/K).\end{aligned}$$

Using the above bounds with (7.1), we obtain the desired estimate for $\Theta_\chi(x)=\sum_{n\geq 1}\Lambda_\chi(n)\varphi(n)$. □

Lemma 7.2. *Let D be any subset of G that is stable under conjugation. Then*

$$\Big|\Theta_{\delta_D}(x) - \frac{|D|}{|G|}\Theta_1(x)\Big| \le |D|^{1/2}\cdot\Big(\frac{1}{|G|}\sum_{\chi\neq 1}|\Theta_\chi(x)|^2\Big)^{1/2},$$

where the sum is over the non-trivial irreducible characters χ of G.

Proof. We have $\Theta_{\delta_D}(x) - \frac{|D|}{|G|}\Theta_1(x) = \sum_{C\subseteq D}(\Theta_{\delta_C}(x) - \frac{|C|}{|G|}\Theta_1(x))$, where the sum is over the conjugacy classes C of G. Using the triangle inequality and the Cauchy-Schwartz inequality, we find that $|\Theta_{\delta_D}(x) - \frac{|D|}{|G|}\Theta_1(x)|$ is less than or equal to

$$\sum_{C\subseteq D}\Big|\Theta_{\delta_C}(x) - \frac{|C|}{|G|}\Theta_1(x)\Big| \le \Big(\sum_{C\subseteq D}|C|\Big)^{1/2}\Big(\sum_C\frac{1}{|C|}\Big|\Theta_{\delta_C}(x) - \frac{|C|}{|G|}\Theta_1(x)\Big|^2\Big)^{1/2}.$$

Since $\sum_{C\subseteq D}|C| = |D|$, it suffices to prove that

$$\sum_C\frac{1}{|C|}\Big|\Theta_{\delta_C}(x) - \frac{|C|}{|G|}\Theta_1(x)\Big|^2 = \frac{1}{|G|}\sum_{\chi\neq 1}|\Theta_\chi(x)|^2, \tag{7.2}$$

where the first sum is over the conjugacy classes C of G and the second sum is over the non-trivial irreducible characters of G.

For C and χ as above, let $\chi(C)$ be the common value of $\chi(g)$ with $g\in C$. We have $\delta_C = \frac{|C|}{|G|}\sum_\chi\overline{\chi(C)}\cdot\chi$, so by linearity $\Theta_{\delta_C}(x) = \frac{|C|}{|G|}\sum_\chi\overline{\chi(C)}\,\Theta_\chi(x)$. Therefore,

$$\begin{aligned}\sum_C\frac{1}{|C|}\Big|\Theta_{\delta_C}(x) - \frac{|C|}{|G|}\Theta_1(x)\Big|^2 &= \sum_C\frac{1}{|C|}\Big|\frac{|C|}{|G|}\sum_{\chi\neq 1}\overline{\chi(C)}\Theta_\chi(x)\Big|^2\\ &= \frac{1}{|G|}\sum_C\frac{|C|}{|G|}\sum_{\chi\neq 1,\chi'\neq 1}\chi(C)\overline{\chi'(C)}\Theta_\chi(x)\overline{\Theta_{\chi'}(x)}\end{aligned}$$

Since $\sum_C\frac{|C|}{|G|}\chi(C)\overline{\chi'(C)} = \frac{1}{|G|}\sum_{g\in G}\chi(g)\chi'(g)$ is equal to 1 if $\chi=\chi'$ and 0 otherwise, we have

$$\sum_C\frac{1}{|C|}\Big|\Theta_{\delta_C}(x) - \frac{|C|}{|G|}\Theta_1(x)\Big|^2 = \frac{1}{|G|}\sum_{\chi\neq 1}\Theta_\chi(x)\overline{\Theta_\chi(x)} = \frac{1}{|G|}\sum_{\chi\neq 1}|\Theta_\chi(x)|^2.$$

This proves (7.2). □

Lemma 7.3. *Let C be any subset of G stable under conjugation. Then*

$$\Theta_{\delta_C}(x) = \frac{|C|}{|G|}\,x\int_0^\infty f(t)\,dt + O_f\Big(|C|^{1/2}[K:\mathbb{Q}]x^{1/2}\log M(L/K)\Big).$$

Proof. The lemma is trivial if $C=\emptyset$, so assume that $C\neq\emptyset$. By Lemma 7.2 and Lemma 7.1, we have

$$\begin{aligned}\Big|\Theta_{\delta_C}(x) - \frac{|C|}{|G|}\Theta_1(x)\Big| &\le |C|^{1/2}\cdot\Big(\frac{1}{|G|}\sum_{\chi\neq 1}\big(\chi(1)[K:\mathbb{Q}]x^{1/2}\log M(L/K)\big)^2\Big)^{1/2}\\ &\ll_f |C|^{1/2}[K:\mathbb{Q}]x^{1/2}\log M(L/K)\cdot\Big(\frac{1}{|G|}\sum\nolimits_{\chi\neq 1}\chi(1)^2\Big)^{1/2}.\end{aligned}$$

Since $\sum_\chi\chi(1)^2 = |G|$, we have

$$\Theta_{\delta_C}(x) = \frac{|C|}{|G|}\Theta_1(x) + O_f\Big(|C|^{1/2}[K:\mathbb{Q}]x^{1/2}\log M(L/K)\Big).$$

The lemma follows by using Lemma 7.1 with $\chi=1$ to estimate $\Theta_1(x)$. □

There is a constant $c > 0$, depending only on f, such that $f(t) = 0$ for all $t \geq c$. In particular, we have $f(N(\mathfrak{p})^m/x) = 0$ if $N(\mathfrak{p})^m \geq cx$. Let $S(x)$ be the sum in the statement of Theorem 2.2. One can readily check that

$$0 \leq \Theta_{\delta_C}(x) - S(x) \leq (\tilde{\pi}_C(cx, L/K) - \pi_C(cx, L/K)) \cdot \log(cx) \cdot \max_{t \in \mathbb{R}} |f(t)|.$$

By Lemma 2.7, we have $S(x) = \Theta_{\delta_C}(x) + O_f([K : \mathbb{Q}]x^{1/2} \log M(L/K))$. Theorem 2.2 now follows directly from Lemma 7.3.

REFERENCES

[CD08] Alina Carmen Cojocaru and Chantal David, *Frobenius fields for elliptic curves*, Amer. J. Math. **130** (2008), no. 6, 1535–1560. MR2464027 (2009k:11092) ↑1.2, 1.3

[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. MR2178556 (2006e:11074) ↑1.3

[Elk91] Noam D. Elkies, *Distribution of supersingular primes*, Astérisque **198-200** (1991), 127–132 (1992). Journées Arithmétiques, 1989 (Luminy, 1989). MR1144318 (93b:11070) ↑1.3

[IK04] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR2061214 (2005h:11005) ↑7, 7

[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), 1977, pp. 409–464. MR0447191 (56 #5506) ↑7

[LT76] Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers. MR0568299 (58 #27900) ↑1.1, 1.4

[Mar77] J. Martinet, *Character theory and Artin L-functions*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), 1977, pp. 1–87. MR0447187 (56 #5502) ↑7

[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. MR935007 (89d:11036) ↑1.3, 1.4, 2.1, 4, 7

[Mur97] V. Kumar Murty, *Modular forms and the Chebotarev density theorem. II*, Analytic number theory (Kyoto, 1996), 1997, pp. 287–308. MR1694997 (2000g:11094) ↑1.3, 2.1

[RT13] Jeremy Rouse and Jesse Thorner, *The explicit Sato-Tate conjecture and densities pertaining to Lehmer-type questions*, arXiv:1305.5283 [math.NT] (2013). ↑1.3

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR0387283 (52 #8126) ↑3.1

[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. MR0450380 (56 #8675) ↑2.3

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. MR644559 (83k:12011) ↑1.3, 2.3, 4, 5

[Wan90] Da Qing Wan, *On the Lang-Trotter conjecture*, J. Number Theory **35** (1990), no. 3, 247–268. MR1062334 (91f:11079) ↑1.3

DEPARTMENT OF MATHEMATICS, CORNELL UNIVERSITY, ITHACA, NY 14853, USA
E-mail address: zywina@math.cornell.edu
URL: http://www.math.cornell.edu/~zywina