Frobenius fields for elliptic curves

Alina Carmen Cojocaru
University of Illinois at Chicago
Department of Mathematics, Statistics and Computer Science
322 Science and Engineering Office (M/C 249)
851 S. Morgan Street
Chicago, IL, 60607-7045, USA
cojocaru@math.uic.edu

Chantal David
Concordia University
Department of Mathematics and Statistics
1455 de Maisonneuve West
Montréal, Québec, H3G 1M8, Canada
cdavid@mathstat.concordia.ca

July 2, 2007

Abstract

Let $E/\mathbb{Q}$ be an elliptic curve over the field of rational numbers, with $\mathrm{End}_{\bar{\mathbb{Q}}}(E) = \mathbb{Z}$. Let K be a fixed imaginary quadratic field over $\mathbb{Q}$, and x a positive real number. For each prime p of good reduction for E, let $\pi_p(E)$ be a root of the characteristic polynomial of the Frobenius endomorphism of E over the finite field $\mathbb{F}_p$. Let $\Pi_E(K;x)$ be the number of primes $p \leq x$ such that the field extension $\mathbb{Q}(\pi_p(E))$ is the fixed imaginary quadratic field K. We present upper bounds for $\Pi_E(K;x)$ obtained using two different approaches. The first one, inspired from work of Serre, is to consider the image of Frobenius in a mixed Galois representation associated to K and to the elliptic curve E. The second one, inspired from work of Cojocaru, Fouvry and Murty, is based on an application of the square sieve. The bounds obtained using the first approach are better, $\Pi_E(K;x) \ll x^{4/5}/(\log x)^{1/5}$, and are the best known so far. The bounds obtained using the second approach are weaker, but are independent of the number field K, a property which is essential for other applications. All results are conditional upon GRH.

Contents

1 Introduction

Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$, of conductor N. For a prime $p \nmid N$, let $E_p/\mathbb{F}_p$ be the reduction of E modulo p and write $|E_p(\mathbb{F}_p)| = p + 1 - a_p(E)$ for the number of $\mathbb{F}_p$-rational points of E_p, where $a_p(E) \in \mathbb{Z}$. By using Hasse's bound that $|a_p(E)| < 2\sqrt{p}$, we see that the polynomial $P_{E,p}(X) := X^2 - a_p(E)X + p$ has two complex conjugate roots $\pi_p(E), \overline{\pi_p(E)}$ satisfying $|\pi_p(E)| = \sqrt{p}$. Even more is true: $P_{E,p}(X)$ is the characteristic polynomial of the Frobenius of the reduction E_p, after we identify the Frobenius with one of the roots $\pi_p(E)$ or $\overline{\pi_p(E)}$. Our goal in this paper is to study the Frobenius fields $\mathbb{Q}(\pi_p(E))$, as the prime p varies.

If $E/\mathbb{Q}$ is with complex multiplication, then for all primes $p \nmid N$ of ordinary reduction for E we have $\mathbb{Q}(\pi_p(E)) = \mathrm{End}_{\bar{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$, where $\mathrm{End}_{\bar{\mathbb{Q}}}(E)$ denotes the endomorphism ring of E. By contrast, if $E/\mathbb{Q}$ is without complex multiplication, then there are infinitely many distinct fields $\mathbb{Q}(\pi_p(E))$ as p runs over primes of ordinary reduction for E (see [CoFoMu] for quantitative results). An open question due to Lang and Trotter is that of estimating the number of primes $p \leq x$ for which the field $\mathbb{Q}(\pi_p(E))$ is isomorphic to a fixed imaginary quadratic extension of $\mathbb{Q}$. More precisely, we have:

Conjecture 1 *(Lang-Trotter, 1976)*
Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, without complex multiplication. Let K be an imaginary quadratic field. Let

$$\Pi_E(K; x) := \#\{p \leq x : p \nmid N, \mathbb{Q}(\pi_p(E)) = K\}.$$

Then there exists a positive constant $c(E, K)$, depending on E and K, such that

$$\Pi_E(K; x) \sim c(E, K)\frac{\sqrt{x}}{\log x}$$

as $x \to \infty$.

This conjecture was first investigated by Serre in 1981, as an application of the effective versions of the Chebotarev Density Theorem due to Lagarias and Odlyzko. Indeed, in [Se81,

p.191] Serre stated (without proof) that, under the assumption of a Generalized Riemann Hypothesis (GRH) and using the Selberg sieve, one has

$$\Pi_E(K;x) \ll_{E,K} x^{\theta} \tag{1}$$

for some (unspecified) $1/2 \leq \theta < 1$. Here, the notation $\ll_{E,K}$ means that the implied constant depends on E and K. In [Se85, p.715], Serre added the remark that instead of the Selberg sieve, one could use a mixed Galois representation

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathrm{GL}_2(\mathbb{Z}_\ell)$$

associated to both E and K, and apply an effective version of the Chebotarev Density Theorem directly to obtain (1). Here, ℓ is a rational prime suitably chosen in terms of x, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$, and $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is the group of invertible matrices with entries in the ring of ℓ-adic integers. Again, no proof was given, but when worked out, the method would give $\theta = 9/10$. The first proof to appear in literature occurs only later and is due to Cojocaru, Fouvry and Murty [CoFoMu], who used the square sieve to show that, under GRH, one has

$$\Pi_E(K;x) \ll_N x^{17/18} \log x, \tag{2}$$

where the implied $\ll_N$ constant depends only on the conductor N of E and is uniform in K. From this uniformity they deduce that the number $|\mathcal{D}_E(x)|$ of distinct squarefree parts of $4p - a_p(E)^2$, for primes $p \leq x$ of good reduction for E, is, under GRH,

$$|\mathcal{D}_E(x)| \gg_N \frac{x^{1/18}}{(\log x)^2}.$$

In [CoFoMu] the authors also include new remarks made by Serre concerning his comment in [Se85, p.715], namely that the mixed Galois representation method together with a PGL_2-reduction would give, under GRH, that

$$\Pi_E(K;x) \ll_{E,K} x^{7/8}, \tag{3}$$

with an unspecified implicit constant.

The purpose of this paper is two-fold. Firstly, we improve upon Serre's mixed Galois representation method and show that, under GRH, $\Pi_E(K;x) \ll_{E,K} x^{4/5}/(\log x)^{1/5}$. The key ingredient in the proof of this bound is a technique due to Murty, Murty and Saradha [MuMuSa] of applying the effective version of the Chebotarev Density Theorem in an abelian extension, hence in an extension where Artin's Holomorphy Conjecture (AHC) holds true. Secondly, we present a new way of estimating a character sum associated to E which occurs in the application of the square sieve to the question of estimating $\Pi_E(K;x)$. This improves the results of [CoFoMu]. Though the improvement to the character sum estimate does not lead to results as good as the one obtained using the mixed Galois representation method, the results obtained by the square sieve have the advantage of being independent of the number field K, a property which is essential for some applications (see Corollary 4); they may also be applied in different other contexts, such as [Co], [CoDu].

A result similar to Theorem 2 was obtained independently by Zywina [Zy] by using a mixed Galois representation approach. The mixed Galois representation of [Zy] is closer to the one considered in [LaTr] than the one considered by Serre.

Here are the precise statements of our results.

Theorem 2 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and without complex multiplication. Let K be a quadratic imaginary extension of $\mathbb{Q}$ of class number h.*

1. *Assume that GRH holds. Then*

$$\Pi_E(K;x) \ll_{N,h} \frac{x^{4/5}}{(\log x)^{1/5}}.$$

2. *Assume that GRH and a Pair Correlation Conjecture (PCC) hold. Then*

$$\Pi_E(K;x) \ll_{N,h} x^{3/4}.$$

The implicit $\ll_{N,h}$-constants depend on N and h.

Theorem 3 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and without complex multiplication. Let ℓ_1, ℓ_2 be distinct rational primes such that the mod $\ell_1\ell_2$ Galois representation associated to E is surjective. Let*

$$S_{\ell_1,\ell_2}(E) := \sum_{\substack{p \le x \\ p \nmid \ell_1\ell_2 N}} \left(\frac{4p - a_p(E)^2}{\ell_1\ell_2} \right).$$

Then

$$S_{\ell_1,\ell_2}(E) = \kappa_{\ell_1\ell_2}\pi(x) + \ell_1^{\theta}\ell_2^{\theta}x^{1/2}\log(\ell_1\ell_2 N x),$$

where

$$\kappa_{\ell_1\ell_2} = \begin{cases} \dfrac{1}{(\ell_1^2-1)(\ell_2^2-1)} & \text{if } \ell_1 \equiv \ell_2 (\mathrm{mod}\, 4), \\ -\dfrac{1}{(\ell_1^2-1)(\ell_2^2-1)} & \text{if } \ell_1 \not\equiv \ell_2 (\mathrm{mod}\, 4), \end{cases}$$

and

1. *$\theta = 3$ if we assume GRH;*
2. *$\theta = 3/2$ if we assume GRH and AHC;*
3. *$\theta = 1/2$ if we assume GRH, AHC and PCC.*

Note that this result improves the error terms in the sharper version of the results of [CoFoMu, Section 3] obtained in [CoDu, Prop. 4.3] (where the character sum is in term of the function $a_p(E)^2 - 4p$ which changes slightly the corresponding constant $\kappa_{\ell_1\ell_2}$).

Corollary 4 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and without complex multiplication. Let K be a quadratic imaginary extension of $\mathbb{Q}$.*

1. *Assume GRH. Then*
$$\Pi_E(K;x) \ll_N x^{13/14}\log x.$$
2. *Assume GRH and AHC. Then*
$$\Pi_E(K;x) \ll_N x^{7/8}\log x.$$
3. *Assume GRH, AHC and PCC. Then*
$$\Pi_E(K;x) \ll_N x^{3/4}\log x.$$

The implicit $\ll_N$-constants depend on N and are independent of K.

Corollary 5 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and without complex multiplication.*

1. *Assume GRH. Then*
$$|\mathcal{D}_E(x)| \gg_N \frac{x^{1/14}}{(\log x)^2}.$$
2. *Assume GRH and AHC. Then*
$$|\mathcal{D}_E(x)| \gg_N \frac{x^{1/8}}{(\log x)^2}.$$
3. *Assume GRH, AHC and PCC. Then*
$$|\mathcal{D}_E(x)| \gg_N \frac{x^{1/4}}{(\log x)^2}.$$

The implicit $\ll_N$-constants depend on N.

Notation: In what follows, p and ℓ, ℓ_1, ℓ_2 will denote rational primes, and x will denote a positive real number, tending to ∞. For two functions $f, g : D \longrightarrow \mathbb{R}$ (with $D \subseteq \mathbb{R}$ infinite) we write $f(x) = \mathrm{O}(g(x))$, or $f(x) \ll g(x)$, or $g(x) \gg f(x)$ if there exists a positive constant M such that $|f(x)| \leq Mg(x)$ for all $x \in D$. More precisely, we write $f(x) = \mathrm{O}_C(g(x))$, or $f(x) \ll_C g(x)$, or $g(x) \gg_C f(x)$ if the constant M is a function of some quantity C. We also write $f(x) \asymp g(x)$ if $f(x) \ll g(x) \ll f(x)$; we write $f(x) = \mathrm{o}(g(x))$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$; and we write $f(x) \sim g(x)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

2 Galois representations

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and without complex multiplication. Let K be an imaginary quadratic field, of class number h and number of units w. In this section we construct a mixed Galois representation associated to both E and K; this representation will be essential in the proof of Theorem 2.

Let ℓ be a rational prime which splits completely in K, say as

$$\ell\mathcal{O}_K = \mathfrak{L} \cdot \bar{\mathfrak{L}}$$

for complex conjugate distinct prime ideals $\mathfrak{L}, \bar{\mathfrak{L}}$ of the ring of integers $\mathcal{O}_K$ of K.

On one hand, we consider the mod ℓ representation associated to E and obtained by the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the group $E[\ell]$ of ℓ-division points of E:

$$\rho_{\ell,E} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

We assume that ℓ is sufficiently large to ensure that the representation $\rho_{\ell,E}$ is surjective, and that $\mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$, where $\mathbb{Q}(E[\ell])$ denotes the field of ℓ-division points of E. This property is guaranteed by Serre's Theorem on the image of the absolute Galois group acting on the subgroup of torsion of $E(\overline{\mathbb{Q}})$ [Se72]. Further, we consider the projection of $\rho_{\ell,E}$ in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and obtain a bijective representation

$$\hat{\rho}_{\ell,E} : \mathrm{Gal}(F_{\ell,E}/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

where $F_{\ell,E}$ is the extension of $\mathbb{Q}$ that makes the representation injective. We recall that the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is ramified only at the prime divisors of ℓN, and for primes $p \nmid \ell N$ we have

$$\mathrm{tr}\, \rho_{\ell,E}(\mathrm{Fr}_p) \equiv a_p(E) (\mathrm{mod}\, \ell), \tag{4}$$

$$\det \rho_{\ell,E}(\mathrm{Fr}_p) \equiv p (\mathrm{mod}\, \ell), \tag{5}$$

where Fr_p denotes the Frobenius at p in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Now we consider a representation associated to K, as follows. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$ and write $\mathfrak{p}^h = \alpha\mathcal{O}_K$ and

$$\pi_{\mathfrak{p}}(K) := \alpha^w.$$

Define

$$\chi_\ell = (\chi_{\mathfrak{L}}, \chi_{\bar{\mathfrak{L}}}) : \mathrm{Gal}(\bar{K}/K) \longrightarrow (\mathcal{O}_K/\mathfrak{L})^* \times (\mathcal{O}_K/\bar{\mathfrak{L}})^* \simeq (\mathbb{Z}/\ell\mathbb{Z})^* \times (\mathbb{Z}/\ell\mathbb{Z})^*$$

by

$$\mathrm{Fr}_{\mathfrak{p}} \mapsto (\pi_{\mathfrak{p}}(K) (\mathrm{mod}\, \mathfrak{L}), \pi_{\mathfrak{p}}(K) (\mathrm{mod}\, \bar{\mathfrak{L}})),$$

where $\mathrm{Fr}_{\mathfrak{p}}$ denotes the Frobenius at $\mathfrak{p}$ in $\mathrm{Gal}(\bar{K}/K)$. Then the product of the two components of χ_ℓ is the hw-th power of the ℓ-th cyclotomic character of K. We are interested in the representation induced from $G_K := \mathrm{Gal}(\bar{K}/K)$ to $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by the first component.

Since G_K is a subgroup of index 2 of $G_{\mathbb{Q}}$, we may write $G_{\mathbb{Q}} = G_K \oplus G_K\mathfrak{c}$, where $\mathfrak{c}$ is the non-trivial automorphism of K. Then the induced representation is

$$\begin{aligned}
\rho_{\ell,K} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) &\longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \\
\sigma &\mapsto \begin{pmatrix} \chi_{\mathfrak{L}}(\sigma) & 0 \\ 0 & \chi_{\mathfrak{L}}(\mathfrak{c}\sigma\mathfrak{c}) \end{pmatrix} \qquad \text{if } \sigma \in G_K; \\
\sigma &\mapsto \begin{pmatrix} 0 & \chi_{\mathfrak{L}}(\sigma\mathfrak{c}) \\ \chi_{\mathfrak{L}}(\mathfrak{c}\sigma) & 0 \end{pmatrix} \qquad \text{if } \sigma \notin G_K.
\end{aligned}$$

As with $\rho_{\ell,E}$, we consider the projection of $\rho_{\ell,K}$ in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and obtain a representation

$$\hat{\rho}_{\ell,K} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Lemma 6 *Let $N_\ell \leq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be the image of the representation $\rho_{\ell,K}$, and let PN_ℓ be the image of the projective representation $\hat{\rho}_{\ell,K}$. Then*

$$\begin{aligned}
N_\ell &= \left\{ \begin{pmatrix} a^{hw} & 0 \\ 0 & b^{hw} \end{pmatrix}, \begin{pmatrix} 0 & a^{hw} \\ b^{hw} & 0 \end{pmatrix} \ : \ a, b \in (\mathbb{Z}/\ell\mathbb{Z})^* \right\}, \\
PN_\ell &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b^{hw} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ b^{hw} & 0 \end{pmatrix} \ : \ b \in (\mathbb{Z}/\ell\mathbb{Z})^* \right\}.
\end{aligned}$$

In particular,

$$|N_\ell| = 2\left(\frac{\ell-1}{\gcd(\ell-1, hw)}\right)^2 \quad \textit{and} \quad |PN_\ell| = \frac{2(\ell-1)}{\gcd(\ell-1, hw)}.$$

Proof. Let $\mathrm{Cl}(\ell)$ be the ray class group modulo $\ell\mathcal{O}_K$ of K. For any $C \in \mathrm{Cl}(\ell)$, there exist infinitely many primes $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathfrak{p} \sim C$ in the class group. In particular, for any $\gamma \in (\mathcal{O}_K/\ell\mathcal{O}_K)^*$, there are infinitely many primes $\mathfrak{p}$ of $\mathcal{O}_K$ such that

$$\begin{aligned}
\mathfrak{p} \sim (\gamma) \quad &\Longrightarrow \quad \pi_{\mathfrak{p}}(K) \equiv \gamma^{hw} (\mathrm{mod}\, \ell\mathcal{O}_K) \\
&\Longleftrightarrow \quad \pi_{\mathfrak{p}}(K) \equiv \alpha^{hw} (\mathrm{mod}\, \mathfrak{L}) \ \text{ and } \ \overline{\pi_{\mathfrak{p}}(K)} \equiv \overline{\beta}^{hw} (\mathrm{mod}\, \mathfrak{L}),
\end{aligned}$$

where $\gamma (\mathrm{mod}\, \ell)$ corresponds to $(\alpha (\mathrm{mod}\, \mathfrak{L}), \beta (\mathrm{mod}\, \overline{\mathfrak{L}}))$ under the Chinese Remainder Theorem.

Now let p be a rational prime which splits in K, say as $p\mathcal{O}_K = \mathfrak{p} \cdot \bar{\mathfrak{p}}$. By the definition of the induced representation and the properties of Frobenius endomorphisms, we have that

$$\rho_{\ell,K}(\mathrm{Fr}_p) = \begin{pmatrix} \pi_{\mathfrak{p}}(K) (\mathrm{mod}\, \mathfrak{L}) & 0 (\mathrm{mod}\, \mathfrak{L}) \\ 0 (\mathrm{mod}\, \mathfrak{L}) & \overline{\pi_{\mathfrak{p}}(K)} (\mathrm{mod}\, \mathfrak{L}) \end{pmatrix}.$$

Then for split primes p, $\rho_{\ell,K}(\mathrm{Fr}_p)$ consist of all diagonal matrices whose diagonal entries are hw-th powers in $(\mathbb{Z}/\ell\mathbb{Z})^*$.

To determine the image of the inert primes, it suffices to notice that $\mathfrak{c}$, the non-trivial automorphism of K, corresponds to the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and that for any $a, b \in (\mathbb{Z}/\ell\mathbb{Z})^*$,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & b \\ a & 0 \end{pmatrix}.$$

This proves the result for N_ℓ; the result for PN_ℓ follows immediately. The orders of the groups follow by counting hw-th powers in $(\mathbb{Z}/\ell\mathbb{Z})^*$. $\square$

As above, after taking the quotient of the projective representation $\hat{\rho}_{\ell,K}$ by its kernel we obtain an isomorphism

$$\hat{\rho}_{\ell,K} : \mathrm{Gal}(F_{\ell,K}/\mathbb{Q}) \longrightarrow PN_\ell,$$

where $F_{\ell,K}$ is the extension of $\mathbb{Q}$ that makes the representation injective. We then consider the product representation

$$\begin{array}{rcl} \hat{\rho}_\ell : \mathrm{Gal}(F_{\ell,E}F_{\ell,K}/\mathbb{Q}) & \longrightarrow & \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times PN_\ell \\ \sigma & \mapsto & (\hat{\rho}_{\ell,E}(\sigma), \hat{\rho}_{\ell,K}(\sigma)). \end{array}$$

Let

$$G_\ell := \mathrm{Im}\,\hat{\rho}_\ell = \mathrm{Gal}(F_{\ell,E}F_{\ell,K}/\mathbb{Q}).$$

Note that if ℓ is a rational prime which splits in K, sufficiently large as in the beginning of the section, and such that $F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}$, then

$$G_\ell \simeq \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times PN_\ell.$$

The next proposition guarantees the existence of infinitely many such ℓ given by arithmetic progressions of modulus related to the quadratic imaginary field K.

As usual, let ζ_ℓ be a primitive ℓ-th root of unity, and let $\mathbb{Q}(\sqrt{\ell^*})$ be the quadratic extension contained in the cyclotomic extension $\mathbb{Q}(\zeta_\ell)$.

Lemma 7 *Let $F_{\ell,E}$ and $F_{\ell,K}$ be the fields defined above. Then*

$$\begin{array}{rcl} F_{\ell,E} \cap F_{\ell,K} & \subseteq & \mathbb{Q}(\sqrt{\ell^*}), \\ F_{\ell,E} \cap \mathbb{Q}(\zeta_\ell) & = & \mathbb{Q}(\sqrt{\ell^*}). \end{array}$$

Proof. By the choice of ℓ we have that $K \cap F_{\ell,E} = \mathbb{Q}$ and the extension $KF_{\ell,E}/K$ has Galois group $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. As $F_{\ell,K}/K$ is abelian, $KF_{\ell,E} \cap F_{\ell,K}$ is an abelian extension of K. But $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ has only two abelian quotients, of order 1 or 2. Then

$$[KF_{\ell,E} \cap F_{\ell,K} : K] \leq 2 \Rightarrow [KF_{\ell,E} \cap F_{\ell,K} : \mathbb{Q}] \leq 4 \Rightarrow [F_{\ell,E} \cap F_{\ell,K} : \mathbb{Q}] \leq 2.$$

As $F_{\ell,E} \cap F_{\ell,K}/\mathbb{Q}$ ramifies only at ℓ (thanks to our assumption that $\mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$), this implies that $F_{\ell,E} \cap F_{\ell,K} \subseteq \mathbb{Q}(\sqrt{\ell^*})$. To prove the second assertion, we remark that by definition $F_{\ell,E}$ is the subfield of $\mathbb{Q}(E[\ell])$ fixed by the scalar matrices. As each scalar matrix acts on ζ_ℓ by

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \zeta_\ell = \zeta_\ell^{a^2},$$

we have that $F_{\ell,E} \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\sqrt{\ell^*})$. $\square$

Proposition 8 *1. Let $K = \mathbb{Q}(i)$. If $\ell \equiv 5 (\mathrm{mod}\, 8)$, then ℓ splits in K and $F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}$.*

2. Let $K = \mathbb{Q}(\sqrt{-D})$, where $D > 1$ is squarefree, i.e. $D = 2^k D'$ with D' odd and $k \in \{0, 1\}$.

(a) If $D' \equiv 1 (\mathrm{mod}\, 4)$, then for any prime ℓ such that

$$\ell \equiv 7 (\mathrm{mod}\, 8) \ \text{ and } \ \left(\frac{\ell}{D'}\right) = -1 \tag{6}$$

we have that ℓ splits in K and $F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}$.

(b) If $D' \equiv 3 (\mathrm{mod}\, 4)$, then for any prime ℓ such that

$$\ell \equiv 7 (\mathrm{mod}\, 8) \ \text{ and } \ \left(\frac{\ell}{D'}\right) = 1 \tag{7}$$

we have that ℓ splits in K and $F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}$.

Proof. *1.* If $K = \mathbb{Q}(i)$, then $hw = 4$ and then by Lemma 6 we obtain that $[F_{\ell,K} : K] = |PN_\ell|/2 = (\ell - 1)/4$ if $\ell \equiv 5 (\mathrm{mod}\, 8)$, and $(\ell - 1)/4$ is an odd integer. Thus $F_{\ell,K}/K$ has no subfield of order 2, and so $\mathbb{Q}(\sqrt{\ell^*}) \not\subseteq F_{\ell,K}$. The result then follows by Lemma 7.
2. For any quadratic imaginary field K we have $2 \mid hw$. Then, using Lemma 6, we obtain that

$$[F_{\ell,K} : K] = \frac{|PN_\ell|}{2} = \left(\frac{\ell - 1}{\gcd(hw, \ell - 1)}\right)^2 \ \text{ divides } \ \left(\frac{\ell - 1}{2}\right)^2.$$

When $\ell \equiv 7 (\mathrm{mod}\, 8)$, this is an odd integer and so $F_{\ell,K}/K$ has no subfield of order 2. This implies that $\mathbb{Q}(\sqrt{\ell^*}) \not\subseteq F_{\ell,K}$, and so $F_{\ell,E} \cap F_{\ell,K} = \mathbb{Q}$, by Lemma 7.

We now want ℓ to split in $K = \mathbb{Q}(\sqrt{-D})$, which is equivalent to $-D$ being a square modulo ℓ, i.e.

$$\left(\frac{-D}{\ell}\right) = (-1) \left(\frac{2}{\ell}\right)^k \left(\frac{\ell}{D'}\right) (-1)^{(D'-1)/2} = 1. \tag{8}$$

Then, by choosing $\ell \equiv 7 (\mathrm{mod}\, 8)$ such that

$$\left(\frac{\ell}{D'}\right) = -1 \qquad \text{if } D' \equiv 1 (\mathrm{mod}\, 4),$$
$$\left(\frac{\ell}{D'}\right) = 1 \qquad \text{if } D' \equiv 3 (\mathrm{mod}\, 4),$$

we have that the Legendre symbol of (8) is 1, which means that ℓ splits completely in K. We also remark that the primes ℓ satisfying (6) or (7) are given by 1/8 of the arithmetic progressions modulo $8D'$. $\square$

For the rest of the paper, ℓ will be a prime satisfying the hypotheses of Proposition 8. Then, ℓ splits in K and

$$G_\ell = \mathrm{Gal}(F_{\ell,E}F_{\ell,K}/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times PN_\ell.$$

In particular,

$$|G_\ell| = |\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})| \cdot |PN_\ell| = \frac{2\ell(\ell-1)^2(\ell+1)}{\gcd(\ell-1, hw)} \asymp_K \ell^4, \tag{9}$$

where the constant in $\asymp_K$ depends on K.

3 The Chebotarev Density Theorem

The main tool in our proofs of Theorems 2 and 3 is the Chebotarev Density Theorem in various effective forms due to Lagarias-Odlyzko, Murty-Murty-Saradha, and Murty-Murty, which we record in what follows.

Let L/k be a finite Galois extension of number fields with Galois group G. Let d_L and d_k be the absolute values of the discriminants of $L/\mathbb{Q}$ and $k/\mathbb{Q}$, respectively. Let $n_L := [L : \mathbb{Q}]$ and $n_k := [k : \mathbb{Q}]$. We denote by p rational primes, by $\mathfrak{p}$ nonzero prime ideals of k, and by $\wp$ nonzero prime ideals of L. Furthermore, we denote by $\mathcal{P}(L/k)$ the set of rational primes p for which there exists a prime $\mathfrak{p}$ of k with $\mathfrak{p}|p$ and with $\mathfrak{p}$ ramified in L/k, and we set

$$M(L/k) := |G| d_k^{1/n_k} \prod_{p \in \mathcal{P}(L/k)} p.$$

Let $C \subseteq G$ be a subset of G stable under conjugation, and let

$$\pi_C(x, L/k) := \#\{\mathfrak{p} : N_{k/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathrm{Fr}_\mathfrak{p} \subseteq C\}.$$

The Chebotarev Density Theorem asserts that, as $x \to \infty$,

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

where $\operatorname{li} x := \displaystyle\int_2^x \frac{1}{\log t}\, dt$ is the logarithmic integral. We are interested in effective versions of this result. The first such was obtained by Lagarias and Odlyzko, under the assumption of GRH, and is stated below in a form due to Serre.

Theorem 9 *Assume GRH for the Dedekind zeta function of L. Then, as $x \to \infty$,*

$$\pi_C(x, L/k) = \frac{|C|}{|G|} \operatorname{li} x + \mathrm{O}\left(|C| x^{1/2} \left(\frac{\log |d_L|}{n_L} + \log x \right) \right).$$

The implicit O*-constant is absolute.*

For a proof, see [Se81, p.133].

Improvements of the above result were obtained by Murty, Murty and Saradha in 1988 and by Murty and Murty in 2002, under the additional assumptions of Artin's Holomorphy Conjecture (AHC) and a Pair Correlation Conjecture (PCC).

Theorem 10 *1. Assume GRH and AHC for the Artin L-functions associated to the irreducible characters of G. Then, as $x \to \infty$,*

$$\pi_C(x, L/k) = \frac{|C|}{|G|} \operatorname{li} x + \mathrm{O}\left(|C|^{1/2} x^{1/2} n_k \log(M(L/k)x) \right).$$

2. Assume GRH, AHC and PCC for the Artin L-functions attached to the irreducible characters of G. Then, as $x \to \infty$,

$$\pi_C(x, L/k) = \frac{|C|}{|G|} \operatorname{li} x + \mathrm{O}\left(|C|^{1/2} x^{1/2} \left(\frac{|\tilde{G}|}{|G|} \right)^{1/4} n_k \log(M(L/k)x) \right),$$

where $|\tilde{G}|$ denotes the number of conjugacy classes in G.

The implicit O*-constants are absolute.*

Part 1 of this result is Corollary 3.7 in [MuMuSa, p.265], and part 2 is the main result in [MuMu].

As shown in [MuMuSa], sometimes one can apply Theorem 10 in an abelian extension, hence in an extension for which AHC is known to be true. The precise version of the Chebotarev Density Theorem which we will be using in such a context is:

Theorem 11 *Assume GRH for Artin L-functions. Let D be a nonempty union of conjugacy classes in G and let H be a normal subgroup of G such that $HD \subseteq D$.*

1. Assume AHC for the Artin L-functions associated to the irreducible characters of G/H. Then

$$\pi_D(x, L/k) = \frac{|D|}{|G|} \operatorname{li} x + \mathrm{O}\left(\left(\frac{|D|}{|H|} \right)^{1/2} x^{1/2} n_k \log(M(L/k)x) \right).$$

2. *Assume AHC and PCC for the Artin L-functions associated to the irreducible characters of G/H. Then*

$$\pi_D(x, L/k) = \frac{|D|}{|G|} \operatorname{li} x + \mathrm{O}\left(\left(\frac{|D|}{|H|} \right)^{1/2} x^{1/2} \left(\frac{|\tilde{G}|}{|G|} \right)^{1/4} n_k \log(M(L/k)x) \right),$$

where $|\tilde{G}|$ denotes the number of conjugacy classes in G.

The implicit O*-constants are absolute.*

The first part of this result is Proposition 3.12 in [MuMuSa, p.267]. The second part is an immediate consequence of the first part combined with the second part of Theorem 10.

The quantity $M(L/k)$ in the above theorems can be estimated using the following result from [Se81, Prop.6, p.130].

Lemma 12 *Let L be a number field of degree n_L over $\mathbb{Q}$ such that $L/\mathbb{Q}$ is Galois. Let d_L be the absolute value of the discriminant of L, and $\mathcal{P}(L/\mathbb{Q})$ the set of rational primes which ramify in $L/\mathbb{Q}$. Then*

$$\log d_L \leq (n_L - 1) \sum_{p \in \mathcal{P}(L/\mathbb{Q})} \log p + n_L \log n_L.$$

We conclude this section by recording some group theoretical results which are used to reduce the study of $\pi_C(x, L/\mathbb{Q})$ to the study of $\pi_D(x, L/k)$ for some $\mathbb{Q} \subseteq k \subseteq L$ such that L/k is abelian. We first need to recall a few definitions from [MuMuSa].

For a prime $\wp$ of L, let $D_\wp$ and $I_\wp$ be its decomposition and inertia groups, respectively. Let $\mathfrak{p}$ be a prime of k with $\wp | \mathfrak{p}$. Let ϕ be a class function of G, and for an integer $m \geq 1$ define

$$\phi(\mathrm{Fr}_\mathfrak{p}^m) := \frac{1}{|I_\mathfrak{p}|} \sum_{\substack{g \in D_\wp \\ g \equiv \mathrm{Fr}_\mathfrak{p}^m \pmod{I_\wp}}} \phi(g),$$

$$\tilde{\pi}_\phi(x) := \sum_{N_{k/\mathbb{Q}}(\mathfrak{p}^m) \leq x} \frac{1}{m} \phi(\mathrm{Fr}_\mathfrak{p}^m),$$

$$\pi_\phi(x) := \sum_{N_{k/\mathbb{Q}}(\mathfrak{p}) \leq x} \phi(\mathrm{Fr}_\mathfrak{p}).$$

Now for $C \subseteq G$ a conjugacy class of G (as before), denote by δ_C its characteristic function. For an element $s \in G$ denote by $C_G(s)$ its conjugacy class in G, and by $C_H(s)$ its conjugacy class in a subgroup $H \leq G$ of G, if $s \in H$.

Lemma 13 *We keep the above setting and notation.*

1. *If ϕ is a class function of G, then*

$$\tilde{\pi}_\phi(x) = \pi_\phi(x) + \mathrm{O}\left(||\phi|| \left\{ \frac{1}{|G|} \log d_L + [k:\mathbb{Q}]\, x^{1/2} \right\}\right),$$

where $||\phi|| := \sup_{s\in G} |\phi(s)|$. The implicit O*-constant is absolute.*

2. *If $s \in H$, let*

$$\tilde{\pi}_{C_H(s)}(x, L/L^H) := \tilde{\pi}_{\delta_{C_H(s)}}(x),$$
$$\tilde{\pi}_{C_G(s)}(x, L/k) := \tilde{\pi}_{\delta_{C_G(s)}}(x).$$

Then

$$\tilde{\pi}_{C_H(s)}(x, L/L^H) = \lambda \cdot \tilde{\pi}_{C_G(s)}(x, L/k),$$

where

$$\lambda := \frac{|C_H(s)|/|H|}{|C_G(s)|/|G|}.$$

For more on this lemma, see [MuMuSa, pp.256–258].

4 Proof of Theorem 2

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, without complex multiplication. Let $K = \mathbb{Q}(\sqrt{-D})$ $(D > 0)$ be an imaginary quadratic field of class number h and number of units w. We want to find an upper estimate for $\Pi_E(K; x)$.

We start by remarking that to estimate $\Pi_E(K; x)$ it is enough to consider only the primes $p \nmid N$ for which $a_p(E) \neq 0$, for otherwise $\mathbb{Q}(\pi_p(E)) = \mathbb{Q}(\sqrt{-p})$, hence the contribution from the primes with $a_p(E) = 0$ is at most one.

Let us fix a rational prime ℓ which satisfies the hypotheses of Proposition 8, and large enough to ensure that the representation $\rho_{E,\ell}$ is surjective and that $\mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$, as in the beginning of Section 2. This prime will play the role of a parameter and will be chosen optimally as a function of x. In what follows, we will use the notation introduced in Section 2.

The following elementary lemma will be used to define a union of conjugacy classes in G_ℓ:

Lemma 14 *Let a, b be independent variables and n a positive integer. Then there exists a polynomial $P_n(X) \in \mathbb{Z}[X]$ such that*

$$\frac{(a^n + b^n)^2}{(ab)^n} = P_n\left(\frac{(a+b)^2}{ab}\right).$$

Proof. For a proof, see [CoDa, Lemma 27]. □

We define a union of conjugacy classes $C_\ell \subseteq G_\ell$ by

$$C_\ell := \left\{ (\hat{g}_1, \hat{g}_2) \in G_\ell : t(g_2) = P_{hw}(t(g_1)),\ g_2 = \begin{pmatrix} 1 & 0 \\ 0 & b^{hw} \end{pmatrix} \text{ and } \left(\frac{(\operatorname{tr} g_1)^2 - 4 \det g_1}{\ell} \right) = 1 \right\},$$

where for any matrix $g \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,

$$t(g) := \frac{(\operatorname{tr} g)^2}{\det g}.$$

We remark that $t(g)$ and the Legendre symbol condition in the definition of C_ℓ are well-defined on matrices of $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

We now show that C_ℓ characterizes the primes p such that $\mathbb{Q}(\pi_p(E)) = K$.

Lemma 15 *Let ℓ be a prime splitting completely in the quadratic extension K, and let $C_\ell \subset G_\ell$ be as defined above. Then*

$$\Pi_E(K; x) \leq \Pi_{C_\ell}(x, F_\ell/\mathbb{Q}).$$

Proof. Let p be a prime which is unramified in $F_\ell/\mathbb{Q}$ and such that $a_p(E) \neq 0$ and $\mathbb{Q}(\pi_p(E)) = K$. On one hand, p splits completely in $\mathbb{Q}(\pi_p(E)) = K$ as

$$p\mathcal{O}_K = (\pi_p(E))(\overline{\pi_p(E)}) =: \mathfrak{p} \cdot \bar{\mathfrak{p}}.$$

On the other hand, let $\pi_p(K)$ be one of $\pi_{\mathfrak{p}}(K)$ or $\pi_{\bar{\mathfrak{p}}}(K)$. From the definition of $\pi_p(K)$ we have that

$$p^{hw}\mathcal{O}_K = (\pi_p(K))(\overline{\pi_p(K)})$$

and

$$\hat{\rho}_{\ell,K}(\mathrm{Fr}_p) = \begin{pmatrix} \pi_p(K) (\mathrm{mod}\, \mathcal{L}) & 0 (\mathrm{mod}\, \mathcal{L}) \\ 0 (\mathrm{mod}\, \mathcal{L}) & \overline{\pi_p(K)} (\mathrm{mod}\, \mathcal{L}) \end{pmatrix}.$$

By combining these three observations we obtain that

$$\pi_p(E)^{hw} = \pi_p(K),$$

after possibly renaming the roots. We use this in Lemma 14 and deduce that

$$\frac{\left(\pi_p(K) + \overline{\pi_p(K)}\right)^2}{\pi_p(K)\overline{\pi_p(K)}} = \frac{\left(\pi_p(E)^{hw} + \overline{\pi_p(E)}^{hw}\right)^2}{\pi_p(E)^{hw}\overline{\pi_p(E)}^{hw}} = P_{hw}\left(\frac{(\pi_p(E) + \overline{\pi_p(E)})^2}{\pi_p(E)\overline{\pi_p(E)}} \right).$$

Next, we reduce both sides (which are elements of $\mathbb{Q}$ with denominator co-prime to ℓ) modulo ℓ and we recall the definition of $\hat{\rho}_{\ell,K}(\mathrm{Fr}_p)$ for primes p which split in K to deduce that

$$t\left(\hat{\rho}_{\ell,K}(\mathrm{Fr}_p)\right) \equiv P_{hw}\left(t\left(\hat{\rho}_{\ell,E}(\mathrm{Fr}_p)\right)\right) (\mathrm{mod}\, \ell).$$

Finally, we remark that the assumption that ℓ splits completely in $K = \mathbb{Q}(\pi_p(E))$ implies that the characteristic polynomial $P_{E,p}(X) = X^2 - a_p(E)X + p$ of $\pi_p(E)$ splits completely in $\mathbb{F}_\ell[X]$, which implies that

$$\left(\frac{(\operatorname{tr}\hat{\rho}_{\ell,K}(\mathrm{Fr}_p))^2 - 4\det\hat{\rho}_{\ell,K}(\mathrm{Fr}_p)}{\ell}\right) = 1.$$

This completes the proof of the lemma. $\square$

Let us define

$$B_\ell := \left\{(\hat{g}_1, \hat{g}_2) \in G_\ell : g_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \text{ and } g_2 = \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix}\right\}.$$

We choose $\Gamma \subseteq B_\ell \cap C_\ell$ a maximal set of elements $\gamma = (\hat{\gamma}_1, \hat{\gamma}_2)$ which are non-conjugate in G_ℓ. Let $g = (\hat{g}_1, \hat{g}_2) \in C_\ell$. As

$$\left(\frac{(\operatorname{tr} g_1)^2 - 4\det g_1}{\ell}\right) = 1,$$

g is conjugate to an element of B_ℓ, and we have

$$C_\ell = \cup_{\gamma\in\Gamma} C_{G_\ell}(\gamma).$$

We also define

$$D_\ell := \cup_{\gamma\in\Gamma} C_{B_\ell}(\gamma).$$

We now record a few properties of the sets introduced above:

Lemma 16 *1.* $|B_\ell| = \dfrac{\ell(\ell-1)^2}{\gcd(\ell-1, hw)} \asymp_K \ell^3$.

2. $|\Gamma| \asymp \ell$.

3. Let $\gamma \in \Gamma$. Then

$$|C_{G_\ell}(\gamma)| \asymp \ell^2$$

and

$$|C_{B_\ell}(\gamma)| \asymp \ell.$$

4. We have

$$|C_\ell| \asymp \ell^3$$

and

$$|D_\ell| \asymp \ell^2.$$

5. Let $\gamma \in \Gamma$. Then

$$\frac{|C_{B_\ell}(\gamma)|/|B_\ell|}{|C_{G_\ell}(\gamma)|/|G_\ell|} = 1 + \underline{o}(1).$$

Proof. *1.* The proof of the first part is direct by counting the matrices of B_ℓ.
2. Let $(\hat{g}_1, \hat{g}_2) \in C_\ell$. Because of the Legendre symbol condition, g_1 is conjugate in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ to a diagonal matrix

$$\gamma_1 = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \text{ with } \alpha \neq \beta. \tag{10}$$

Also, any two diagonal matrices are conjugate in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ if and only if they have the same diagonal entries. This gives $\asymp \ell$ conjugacy classes for $\hat{g}_1$. By the definition of C_ℓ, g_2 is a diagonal matrix, and $\hat{g}_2$ is completely determined by $\hat{g}_1$, and then $|\Gamma| \asymp \ell$.
3. To compute the size of $|C_{G_\ell}(\gamma)|$, we first remark that for a diagonal matrix as in (10), its conjugacy class in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ consists of all matrices with trace $\alpha+\beta$ and determinant $\alpha\beta$; there are $\asymp \ell^2$ of these matrices, and none of these matrices are equivalent in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. As $\gamma = (\gamma_1, \gamma_2)$, where γ_1 a diagonal matrix as in (10), and the size of the conjugacy class of γ_2 in PN_ℓ has 1 or 2 elements, this completes the computation.

Similarly, the size of $|C_{B_\ell}(\gamma)|$ follows from the computation

$$\frac{1}{d}\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix}\begin{pmatrix} d & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b(\beta-1)/d \\ 0 & \beta \end{pmatrix}.$$

4. This follows from parts *2* and *3*.
5. This follows from (9) and parts *1* and *3*. □

We are ready to start estimating $\pi_{C_\ell}(x, F_\ell/\mathbb{Q})$. For this, we will use a reduction method introduced in [MuMuSa] which enables us to apply the effective version of the Chebotarev Density Theorem (Theorem 11) in an abelian extension, hence in an extension where AHC holds true. This is where we improve upon the method described in [CoFoMu, Section 6].

We first reduce the Galois group from G_ℓ to B_ℓ. Using the second part of Lemma 13 and the fifth part of Lemma 16, we deduce that

$$\tilde{\pi}_{C_{G_\ell}(\gamma)}(x, F_\ell/\mathbb{Q}) = (1+\underline{o}(1))\,\tilde{\pi}_{C_{B_\ell}(\gamma)}(x, F_\ell/F_\ell^{B_\ell})$$

for all $\gamma \in \Gamma$. This implies that

$$\begin{aligned} \pi_{C_\ell}(x, F_\ell/\mathbb{Q}) = \sum_{\gamma\in\Gamma} \pi_{C_{G_\ell}(\gamma)}(x, F_\ell/\mathbb{Q}) &\leq \sum_{\gamma\in\Gamma} \tilde{\pi}_{C_{G_\ell}(\gamma)}(x, F_\ell/\mathbb{Q}) \\ &\ll \sum_{\gamma\in\Gamma} \tilde{\pi}_{C_{B_\ell}(\gamma)}(x, F_\ell/F_\ell^{B_\ell}) = \tilde{\pi}_\phi(x), \end{aligned} \tag{11}$$

where $\phi : B_\ell \longrightarrow \{0,1\}$ denotes the characteristic function of $D_\ell = \cup_{\gamma\in\Gamma} C_{B_\ell}(\gamma)$.

Using the first part of Lemma 13 with $L := F_\ell$, $k := F_\ell^{B_\ell}$, $G := \mathrm{Gal}(F_\ell/F_\ell^{B_\ell})$, as well as Lemma 12, we see that

$$\tilde{\pi}_\phi(x) = \pi_\phi(x) + \mathrm{O}\left(\ell \log(\ell d_K N) + \ell x^{1/2}\right). \tag{12}$$

The implicit O-constant is absolute. Hence, in order to estimate $\pi_{C_\ell}(x, F_\ell/\mathbb{Q})$ it remains to estimate $\pi_\phi(x)$, where ϕ is the characteristic function of D_ℓ. To do so, we define

$$H_\ell := \left\{ (\hat{g}_1, \hat{g}_2) \in B_\ell : g_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}, \ \ g_2 = \begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix} \right\}.$$

Then H_ℓ is a subgroup of B_ℓ with the following properties:

Lemma 17 *1. H_ℓ is a normal subgroup of B_ℓ and B_ℓ/H_ℓ is abelian.*

2. $H_\ell D_\ell \subseteq D_\ell$.

3. $|H_\ell| \asymp \ell$.

Proof. *1.* This part follows easily after observing that H_ℓ is the kernel of the group homomorphism

$$B_\ell \longrightarrow (\mathbb{Z}/\ell\mathbb{Z})^* \times (\mathbb{Z}/\ell\mathbb{Z})^*$$
$$\left(\widehat{\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}}, \widehat{\begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix}} \right) \mapsto (a_1^{-1} d_1, a_2^{-1} d_2),$$

where $a_1, b_1, d_1, a_2, d_2 \in \mathbb{Z}/\ell\mathbb{Z}$.
2. Let $(\hat{g}_1, \hat{g}_2) \in H_\ell$. As $\hat{g}_2$ is the identity, it suffices to look at the effect of multiplying the first component of elements of D_ℓ by g_1, i.e.

$$\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & b \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} \alpha & b + \beta b_1 \\ 0 & \beta \end{pmatrix},$$

which is still an element of the same conjugacy class in D_ℓ.
3. The proof of this part consists of a trivial counting argument. □

Since B_ℓ/H_ℓ is abelian, AHC is true for the Artin L-functions associated to the irreducible characters of B_ℓ/H_ℓ. Then the first part of Theorem 11 implies that, under GRH,

$$\begin{aligned} \pi_\phi(x) = \pi_{D_\ell}(x; F_\ell/F_\ell^{B_\ell}) &\ll \frac{|D_\ell|}{|B_\ell|} \operatorname{li} x + \left(\frac{|D_\ell|}{|H_\ell|} \right)^{1/2} \left[F_\ell^{B_\ell} : \mathbb{Q} \right] x^{1/2} \log M(F_\ell/F_\ell^{B_\ell}) \\ &\ll \frac{\gcd(\ell - 1, hw)}{\ell} \cdot \frac{x}{\log x} + \ell^{3/2} x^{1/2} \log(\ell d_K N x) \\ &\ll \frac{hwx}{\ell \log x} + \ell^{3/2} x^{1/2} \log(\ell d_K N x), \end{aligned} \tag{13}$$

where we have used (9), Lemma 16 and Lemma 17 to evaluate the size of the various groups, and Lemma 12 to evaluate $\log M\left(F_\ell/F_\ell^{B_\ell}\right)$. Finally, by putting together (11), (12) and (13), we obtain that, under GRH,

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{hwx}{\ell \log x} + \ell^{3/2} x^{1/2} \log(\ell d_K N x) + \ell \log(\ell d_K N). \tag{14}$$

The implicit $\ll$-constant is absolute. Let us also remark that $w \leq 4$ and that we may assume that $d_K \leq 4x$, for otherwise $\Pi_E(K;x) = 0$. Therefore (14) becomes

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{hx}{\ell \log x} + \ell^{3/2} x^{1/2} \log(\ell N x) + \ell \log(\ell N) \tag{15}$$

with an absolute implicit $\ll$-constant.

By choosing ℓ such that

$$\ell \asymp \frac{h^{2/5} x^{1/5}}{(\log x)^{4/5}} \tag{16}$$

in (15), we obtain

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{h^{3/5} x^{4/5}}{(\log x)^{1/5}} + \frac{h^{3/5} x^{4/5} \log(hNx)}{(\log x)^{6/5}},$$

and so

$$\Pi_E(K;x) \ll_{N,h} \frac{x^{4/5}}{(\log x)^{1/5}},$$

where the implicit constant depends on N and h.

The existence of a prime ℓ which satisfies the conditions of Proposition 8 and has size (16) is ensured by the Prime Number Theorem for primes in arithmetic progressions, under GRH. Indeed, if

$$y := \frac{h^{2/5} x^{1/5}}{(\log x)^{4/5}},$$

then GRH ensures that there is a prime ℓ satisfying the hypotheses of Proposition 8 and lying in the interval $[y, y+u]$ for any $y^{1/2}(\log y)^{2+\varepsilon} \leq u \leq y$. We then choose x sufficiently large such that the representation $\rho_{E,\ell}$ is surjective and $\mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$, as required in the beginning of Section 2. With this, the proof of the first part of Theorem 2 is complete.

If in addition to GRH we assume PCC, then we can apply the second part of Theorem 11 to estimate $\pi_\phi(x)$. This introduces an extra factor of $1/\sqrt{\ell}$ in the error term, and leads to

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll \frac{hx}{\ell \log x} + \ell x^{1/2} \log(\ell N x) + \ell \log(\ell N),$$

where the implicit $\ll$-constant is absolute. By choosing ℓ such that

$$\ell \asymp \frac{h^{1/2} x^{1/4}}{\log x}$$

we obtain that

$$\pi_{C_\ell}(x, F_\ell/\mathbb{Q}) \ll h^{1/2} x^{3/4} + h^{1/2} x^{3/4} \frac{\log(hNx)}{\log x},$$

and so

$$\Pi_E(K;x) \ll_{N,h} x^{3/4},$$

where the implicit constant depends on N and h. The existence of such a prime ℓ is justified as for part one.

5 Proof of Theorem 3 and Corollaries 4, 5

In this section, we will prove Theorem 3. As before, let $E/\mathbb{Q}$ be an elliptic curve of conductor N and without complex multiplication. Let $\ell_1 \neq \ell_2$ be rational primes such that the mod $\ell_1\ell_2$ Galois representation associated to E is surjective. We want to obtain upper estimates for the character sum

$$S_{\ell_1,\ell_2}(E) := \sum_{\substack{p\leq x\\ p\nmid \ell_1\ell_2 N}} \left(\frac{4p-a_p(E)^2}{\ell_1\ell_2}\right).$$

This was already done in [CoFoMu] as an application of the effective versions of the Chebotarev Density Theorem due to Lagarias-Odlyzko (under GRH) and to Murty-Murty-Saradha and Murty-Murty (under GRH, AHC and PCC). Our improvement to the results of [CoFoMu] is a new way of estimating this sum by making use of a PGL_2-reduction. First, let us recall the way the sum was estimated in [CoFoMu]: for $t \in \mathbb{Z}/\ell_1\ell_2\mathbb{Z}, d \in (\mathbb{Z}/\ell_1\ell_2\mathbb{Z})^*$, let

$$C_{\ell_1\ell_2}(t,d) := \{g \in \mathrm{GL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z}) : \operatorname{tr} g = t, \det g = d\};$$

under GRH, one has

$$\begin{aligned}
S_{\ell_1,\ell_2}(E) &= \sum_{\substack{t\in\mathbb{Z}/\ell_1\ell_2\mathbb{Z}\\ d\in(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})^*}} \sum_{\substack{p\leq x\\ p\nmid\ell_1\ell_2 N\\ a_p(E)\equiv t(\mathrm{mod}\,\ell_1\ell_2)\\ p\equiv d(\mathrm{mod}\,\ell_1\ell_2)}} \left(\frac{4p-a_p(E)^2}{\ell_1\ell_2}\right)\\
&= \sum_{\substack{t\in\mathbb{Z}/\ell_1\ell_2\mathbb{Z}\\ d\in(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})^*}} \left(\frac{4d-t^2}{\ell_1\ell_2}\right) \pi_{C_{\ell_1\ell_2}(t,d)}(x, \mathbb{Q}(E[\ell_1\ell_2])/\mathbb{Q})\\
&= \sum_{\substack{t\in\mathbb{Z}/\ell_1\ell_2\mathbb{Z}\\ d\in(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})^*}} \left(\frac{4d-t^2}{\ell_1\ell_2}\right) \left[\frac{\ell_1^2\ell_2^2+\mathrm{O}\left(\ell_1^2\ell_2+\ell_1\ell_2^2\right)}{\ell_1\ell_2(\ell_1-1)^2(\ell_2-1)^2(\ell_1+1)(\ell_2+1)}\pi(x)\right.\\
&\qquad\qquad \left. +\,\mathrm{O}\left(\ell_1^2\ell_2^2 x^{1/2}\log(\ell_1\ell_2 N x)\right)\right]\\
&\ll \left(\frac{1}{\ell_1}+\frac{1}{\ell_2}\right)\frac{x}{\log x} + \ell_1^4\ell_2^4 x^{1/2}\log(\ell_1\ell_2 N x),
\end{aligned}$$

where the third line is an application of Theorem 9 applied to the division fields of $E/\mathbb{Q}$, after making use of properties (4) and (5).

By carefully estimating the size of $C_{\ell_1\ell_2}(t,d)$, in [CoDu, Prop. 4.3] the authors obtained the sharper estimate

$$S_{\ell_1,\ell_2}(E) = \kappa_{\ell_1\ell_2}\pi(x) + \mathrm{O}\left(\ell_1^4\ell_2^4 x^{1/2}\log(\ell_1\ell_2 N x)\right).$$

To improve upon the above we proceed as follows. First, we write

$$\sum_{\substack{p\le x\\ p\nmid \ell_1\ell_2 N}}\left(\frac{4p-a_p(E)^2}{\ell_1\ell_2}\right) = \sum_{\substack{p\le x\\ p\nmid \ell_1\ell_2 N\\ \left(\frac{4p-a_p(E)^2}{\ell_1}\right)\left(\frac{4p-a_p(E)^2}{\ell_2}\right)=1}} 1 - \sum_{\substack{p\le x\\ p\nmid \ell_1\ell_2 N\\ \left(\frac{4p-a_p(E)^2}{\ell_1}\right)\left(\frac{4p-a_p(E)^2}{\ell_2}\right)=-1}} 1 \quad (17)$$

$$= \pi_{C_1\cup C_2}(x, F_{\ell_1\ell_2,E}/\mathbb{Q}) - \pi_{C_3\cup C_4}(x, F_{\ell_1\ell_2,E}/\mathbb{Q}), \quad (18)$$

where

$$C_1 := \left\{(\hat{g}_1,\hat{g}_2)\in \mathrm{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z}) : \left(\frac{4\det g_1-(\mathrm{tr}\, g_1)^2}{\ell_1}\right)=\left(\frac{4\det g_2-(\mathrm{tr}\, g_2)^2}{\ell_2}\right)=1\right\},$$

$$C_2 := \left\{(\hat{g}_1,\hat{g}_2)\in \mathrm{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z}) : \left(\frac{4\det g_1-(\mathrm{tr}\, g_1)^2}{\ell_1}\right)=\left(\frac{4\det g_2-(\mathrm{tr}\, g_2)^2}{\ell_2}\right)=-1\right\},$$

$$C_3 := \left\{(\hat{g}_1,\hat{g}_2)\in \mathrm{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z}) : \left(\frac{4\det g_1-(\mathrm{tr}\, g_1)^2}{\ell_1}\right)=-\left(\frac{4\det g_2-(\mathrm{tr}\, g_2)^2}{\ell_2}\right)=1\right\},$$

$$C_4 := \left\{(\hat{g}_1,\hat{g}_2)\in \mathrm{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z}) : \left(\frac{4\det g_1-(\mathrm{tr}\, g_1)^2}{\ell_1}\right)=-\left(\frac{4\det g_2-(\mathrm{tr}\, g_2)^2}{\ell_2}\right)=-1\right\},$$

and where $F_{\ell_1\ell_2,E}$ is the extension $F_{\ell_1,E}F_{\ell_2,E}$ introduced in Section 2.

Then we use Theorem 9 under GRH, and we do this for PGL_2-extensions instead of GL_2. Note that this is possible because the conditions defining the conjugacy classes C_1, C_2, C_3, C_4 are well-defined in $\mathrm{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})$. This is not true, however, for the conjugacy classes $C_{\ell_1\ell_2}(t,d)$ considered in [CoFoMu].

For a prime ℓ, let

$$C_\ell(1) := \#\left\{g\in \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \left(\frac{4\det g-(\mathrm{tr}\, g)^2}{\ell}\right)=1\right\},$$

$$C_\ell(-1) := \#\left\{g\in \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \left(\frac{4\det g-(\mathrm{tr}\, g)^2}{\ell}\right)=-1\right\}.$$

It is a straightforward counting argument to show that

$$|C_\ell(1)| = \begin{cases} \dfrac{\ell^3-\ell^2}{2}-\ell & \text{if } \ell\equiv 1 (\mathrm{mod}\, 4),\\ \dfrac{\ell^3-\ell^2}{2} & \text{if } \ell\equiv 3 (\mathrm{mod}\, 4),\end{cases}$$

and

$$|C_\ell(-1)| = \begin{cases} \dfrac{\ell^3-\ell^2}{2} & \text{if } \ell\equiv 1 (\mathrm{mod}\, 4),\\ \dfrac{\ell^3-\ell^2}{2}-\ell & \text{if } \ell\equiv 3 (\mathrm{mod}\, 4).\end{cases}$$

Thus,

$$\begin{aligned}|C_1 \cup C_2| &= |C_{\ell_1}(1)| \cdot |C_{\ell_2}(1)| + |C_{\ell_1}(-1)| \cdot |C_{\ell_2}(-1)| \\ &= \begin{cases} \dfrac{(\ell_1^3-\ell_1^2)(\ell_2^3-\ell_2^2)}{2} - \dfrac{\ell_1(\ell_2^3-\ell_2^2)}{2} - \dfrac{\ell_2(\ell_1^3-\ell_1^2)}{2} + \ell_1\ell_2 & \text{if } \ell_1 \equiv \ell_2 (\mathrm{mod}\, 4), \\ \dfrac{(\ell_1^3-\ell_1^2)(\ell_2^3-\ell_2^2)}{2} - \dfrac{\ell_1(\ell_2^3-\ell_2^2)}{2} - \dfrac{\ell_2(\ell_1^3-\ell_1^2)}{2} & \text{if } \ell_1 \not\equiv \ell_2 (\mathrm{mod}\, 4), \end{cases}\end{aligned}$$

and

$$\begin{aligned}|C_3 \cup C_4| &= |C_{\ell_1}(1)| \cdot |C_{\ell_2}(-1)| + |C_{\ell_1}(-1)| \cdot |C_{\ell_2}(1)| \\ &= \begin{cases} \dfrac{(\ell_1^3-\ell_1^2)(\ell_2^3-\ell_2^2)}{2} - \dfrac{\ell_1(\ell_2^3-\ell_2^2)}{2} - \dfrac{\ell_2(\ell_1^3-\ell_1^2)}{2} & \text{if } \ell_1 \equiv \ell_2 (\mathrm{mod}\, 4), \\ \dfrac{(\ell_1^3-\ell_1^2)(\ell_2^3-\ell_2^2)}{2} - \dfrac{\ell_1(\ell_2^3-\ell_2^2)}{2} - \dfrac{\ell_2(\ell_1^3-\ell_1^2)}{2} + \ell_1\ell_2 & \text{if } \ell_1 \not\equiv \ell_2 (\mathrm{mod}\, 4). \end{cases}\end{aligned}$$

Now let us recall that we are choosing ℓ_1, ℓ_2 such that the mod $\ell_1\ell_2$ Galois representation associated to E is surjective, and so the image of this representation has size equal to $|\mathrm{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})| = (\ell_1^3-\ell_1)(\ell_2^3-\ell_2)$. Then, by making use of the above estimates and by applying Theorem 9 under GRH to (18), we obtain that

$$S_{\ell_1,\ell_2}(E) = \sum_{\substack{p \le x \\ p \nmid \ell_1\ell_2 N}} \left(\frac{4p - a_p(E)^2}{\ell_1\ell_2} \right) = \kappa_{\ell_1\ell_2}\pi(x) + \mathrm{O}\left(\ell_1^3\ell_2^3 x^{1/2}\log(\ell_1\ell_2 N x)\right),$$

where $\kappa_{\ell_1\ell_2}$ is the constant defined in the statement of Theorem 3.

To prove the second and third parts of Theorem 3, we use the effective versions of the Chebotarev Density Theorem due to Murty-Murty-Saradha, and to Murty-Murty (Theorem 10). Under GRH and AHC we obtain

$$S_{\ell_1,\ell_2}(E) = \kappa_{\ell_1\ell_2}\pi(x) + \mathrm{O}\left(\ell_1^{3/2}\ell_2^{3/2} x^{1/2}\log(\ell_1\ell_2 N x)\right),$$

and under GRH, AHC and PCC we obtain

$$S_{\ell_1,\ell_2}(E) = \kappa_{\ell_1\ell_2}\pi(x) + \mathrm{O}\left(\ell_1^{1/2}\ell_2^{1/2} x^{1/2}\log(\ell_1\ell_2 N x)\right).$$

All the implicit $\ll$-constants are absolute. This completes the proof of Theorem 3.

To prove Corollary 4, we use the square sieve and the above estimates. Let us first recall the square sieve from [HB]:

Theorem 18 *Let $\mathcal{A}$ be a finite set of (not necessarily distinct) non-zero integers, and let $\mathcal{P}$ be a set of (distinct) odd rational primes. Set*

$$S(\mathcal{A}) := \#\{\alpha \in \mathcal{A} : \alpha \text{ is a square}\}.$$

Then

$$S(\mathcal{A}) \le \frac{|\mathcal{A}|}{|\mathcal{P}|} + \max_{\substack{\ell_1,\ell_2\in\mathcal{P}\\ \ell_1\neq\ell_2}} \left|\sum_{\alpha\in\mathcal{A}} \left(\frac{\alpha}{\ell_1\ell_2}\right)\right| + \frac{2}{|\mathcal{P}|}\sum_{\alpha\in\mathcal{A}}\sum_{\substack{\ell\in\mathcal{P}\\ \gcd(\alpha,\ell)\neq 1}} 1 + \frac{1}{|\mathcal{P}|^2}\sum_{\alpha\in\mathcal{A}}\left(\sum_{\substack{\ell\in\mathcal{P}\\ \gcd(\alpha,\ell)\neq 1}} 1\right)^2.$$

For a proof of this result, see [HB] or [CoFoMu].

For our application we take

$$\mathcal{A} := \left\{D(4p - a_p(E)^2) : p \nmid N, p \le x\right\},$$

$$\mathcal{P} := \{\ell : z \le \ell \le 2z\},$$

where $K = \mathbb{Q}(\sqrt{-D})$ and where $z = z(x)$ is a positive real number, depending on x, and to be chosen later. By following the first part of the proof of Theorem 1.2 of [CoFoMu], we obtain

$$\begin{aligned}
\Pi_E(K,x) &\le S(\mathcal{A})\\
&\ll \frac{x\log z}{z\log x} + \max_{\substack{\ell_1,\ell_2\in\mathcal{P}\\ \ell_1\neq\ell_2}} |S_{\ell_1,\ell_2}(E)|\\
&+ \frac{x\log z}{z\log x}\log D + \frac{x\log z}{z}\\
&+ \frac{x(\log z)^2}{z^2\log x}(\log D)^2 + \frac{x(\log z)^2}{z^2}\log D + \frac{x(\log x)(\log z)^2}{z^2},
\end{aligned}$$

where the implicit $\ll$-constants are absolute. The character sum $|S_{\ell_1,\ell_2}(E)|$ is now estimated using Theorem 3. We obtain

$$\begin{aligned}
\Pi_E(K,x) &\ll \frac{x\log z}{z\log x} + z^{2\theta}x^{1/2}\log(zNx)\\
&+ \frac{x\log z}{z\log x}\log D + \frac{x\log z}{z}\\
&+ \frac{x(\log z)^2}{z^2\log x}(\log D)^2 + \frac{x(\log z)^2}{z^2}\log D + \frac{x(\log x)(\log z)^2}{z^2},
\end{aligned}$$

where $\theta = 3$ under GRH, $\theta = 3/2$ under GRH and AHC, and $\theta = 1/2$ under GRH, AHC and PCC.

Then by taking

$$z := x^{1/14},$$

we obtain

$$\Pi_E(K;x) \ll_N x^{13/14} \log x,$$

under GRH; by taking

$$z := x^{1/8},$$

we obtain

$$\Pi_E(K;x) \ll_N x^{7/8} \log x,$$

under GRH and AHC; finally, by taking

$$z := x^{1/4},$$

we obtain

$$\Pi_E(K;x) \ll_N x^{3/4} \log x,$$

under GRH, AHC and PCC. This completes the proof of Corollary 4. Corollary 5 is now a simple consequence of these estimates (thanks to their uniformity in K), together with the Prime Number Theorem and the fact that E has at most $\mathrm{O}(x^{3/4})$ supersingular primes.

Remark 19 *1.* We remind the reader that the square sieve does not lead to the best exponent of x in the estimate of $\Pi_E(K;x)$. Nevertheless, the character sum estimates (uniform in K) can play a significant role in other asymptotic problems such as the one considered by [CoDu]. Using our new method of estimating $S_{\ell_1,\ell_2}(E)$, the error term in the main result Proposition 5.3 of [CoDu] can be improved from $\mathrm{O}_N(x^{53/54+\varepsilon})$ to $\mathrm{O}_N(x^{41/42+\varepsilon})$ under GRH (and $\mathrm{O}_N(x^{13/14+\varepsilon})$ under GRH and AHC, $\mathrm{O}_N(x^{11/12+\varepsilon})$ under GRH, AHC and PCC). Using additional methods, one can improve these error terms even further [Sh].

2. Other character sums associated to E, such as

$$S_{\ell_1,\ell_2}(E) := \sum_{\substack{p \le x \\ p \nmid \ell_1 \ell_2 N}} \left(\frac{p+1-a_p(E)}{\ell_1 \ell_2} \right),$$

are also of interest and can be estimated similarly. This one, in particular, may be used when considering the question of estimating the number of primes $p \le x$ for which $|E_p(\mathbb{F}_p)|$ is squarefree (see [Co]). In estimating this character sum, however, we cannot make use of the PGL_2-reduction, but we can still make use of observation (17) and the applications of the effective versions of the Chebotarev Density Theorem.

Acknowledgements: The authors are indebted to Hershy Kisilevsky for useful discussions during the preparation of this paper. They are also indebted to Igor Shparlinski for pointing out an improvement to an earlier version of Theorem 3. Part of the work on this paper was done at the Fields Institute for Research in Mathematical Sciences and Concordia University. The authors are grateful to both institutions for providing them with excellent working environments.

References

[Co] A.C. Cojocaru, *Cyclicity of elliptic curves modulo p*, PhD thesis, Queen's University, Canada, 2002.

[CoDa] A.C. Cojocaru, C. David, *Frobenius fields for Drinfeld modules of rank 2*, 31 pages, submitted, 2006.

[CoDu] A.C. Cojocaru, W. Duke, *Reductions of an elliptic curve and their Tate-Shafarevich groups,* Mathematische Annalen 329, 2004, pp. 513–534.

[CoFoMu] A.C. Cojocaru, E. Fouvry, M.R. Murty, *The square sieve and the Lang-Trotter conjecture,* Canadian Journal of Mathematics, vol. 57, no. 6, 2005, pp. 1155–1177.

[HB] D.R. Heath-Brown, *The square sieve and consecutive squarefree numbers*, Mathematische Annalen 266, 1984, pp. 251–259.

[LaTr] S. Lang, H. Trotter, *Frobenius distributions in* GL_2*-extensions,* Lecture Notes in Mathematics 504, Springer Verlag, 1976.

[MuMuSa] M.R. Murty, V.K. Murty, N. Saradha, *Modular forms and the Chebotarev density theorem*, American Journal of Mathematics, vol. 110, no. 2, 1998, pp. 253–281.

[MuMu] M.R. Murty, V.K. Murty, *The Chebotarev density theorem and pair correlation of zeros of Artin L-functions*, preprint.

[Se72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae 15, 1972, pp. 259–331.

[Se81] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publications Mathématiques I.H.E.S., no. 54, 1981, pp. 123–201.

[Se85] J.-P. Serre, *Collected papers*, volume III, Springer Verlag, 1985.

[Sh] I.E. Shparlinski, private communication.

[Zy] D. Zywina, *The Lang-Trotter conjecture and mixed representations*, preprint 2006.