IMRN International Mathematics Research Notices
2005, No. 50

Uniform Results for Serre's Theorem for Elliptic Curves

Alina Carmen Cojocaru and Chris Hall

1 Introduction

Let E/K be an elliptic curve defined over a number field K and without complex multiplication (CM). For a rational prime ℓ, let $K(E[\ell])$ be the ℓth division field of E, which we know is a finite Galois extension of K. By a celebrated result of Serre [18], there exists a positive constant $c(E, K)$, depending on E and K, such that $\mathrm{Gal}(K(E[\ell])/K) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell \geq c(E, K)$. In [18, 19], Serre asked whether there exists a positive constant $c(K)$, depending at most on K, such that $\mathrm{Gal}(K(E[\ell])/K) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell \geq c(K)$. An affirmative answer to this question would have important diophantine applications, as illustrated in [14].

Currently, there exist few results related to Serre's question. In [13], Mazur showed that for $K = \mathbb{Q}$ and for semistable elliptic curves $E/\mathbb{Q}$ without CM, one has $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for any prime $\ell \geq 11$. In [2, 9, 12, 19], upper bounds in terms of invariants of E (height and conductor) were given for the *exceptional* primes ℓ of an elliptic curve $E/\mathbb{Q}$, that is, for those primes ℓ for which $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. More ideas are still needed, however, to completely answer Serre's question.

Naturally, one can ask if Serre's question is true "on average" or "over function fields." The goal of our paper is to study these two questions. In [4], Duke gave an affirmative answer to the first question for a natural two-parameter family of elliptic curves $E/\mathbb{Q}$ which contains every elliptic curve over $\mathbb{Q}$. One of our aims is to obtain a more refined average result; that is, to answer Serre's question for "most" elements of a one-parameter family of elliptic curves. This is the content of Theorem 1.3 below. We will also

Received 8 July 2005. Revision received 19 September 2005.

answer the second question. In particular, in Theorem 1.1 we show that the function-field analogue of Serre's question has an affirmative answer. As we will see, Theorems 1.1 and 1.3 are intimately connected via Theorem 1.2. We will also give an immediate application of Theorem 1.2 to one of the classical Lang-Trotter conjectures on Frobenius traces.

Now let us state our main results rigorously. Let $C/\mathbb{F}_q$ be a proper, smooth, geometrically connected curve over the finite field $\mathbb{F}_q$ with q elements. Let $K := \mathbb{F}_q(C)$ be the function field of $C/\mathbb{F}_q$, and let E/K be an elliptic curve with nonconstant j-invariant (i.e., $j(E) \in K\backslash\mathbb{F}_q$). For a rational prime ℓ invertible in K, let $G_\ell := \mathrm{Gal}(K(E[\ell])/K)$ be the Galois group of the ℓth division field of E/K. Choosing a basis of $E[\ell]$ gives an embedding $G_\ell \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and induces the following commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & H_\ell \arrow[r] \arrow[d] & G_\ell \arrow[r] \arrow[d] & \langle q\rangle \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \arrow[r] & \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \arrow[r, "\det"] & (\mathbb{Z}/\ell\mathbb{Z})^\times \arrow[r] & 1
\end{tikzcd} \tag{1.1}$$

where det is the determinant map. Let $\overline{\mathbb{F}}_q$ denote an algebraic closure of $\mathbb{F}_q$. The fixed field of H_ℓ corresponds to the scalar extension $(K(E[\ell])\cap\overline{\mathbb{F}}_q)K/K$ given by adjoining a primitive ℓth root of unity, so we call H_ℓ the *geometric Galois group* of $K(E[\ell])/K$.

In [7], Igusa showed that for rational primes $\ell_1 \neq \ell_2$, distinct from $\mathrm{char}\,\mathbb{F}_q$, the (geometric) extensions $\overline{\mathbb{F}}_q(j(E), E[\ell_i])/\overline{\mathbb{F}}_q(j(E))$, $i = 1, 2$, are disjoint with respective (geometric) Galois group $\mathrm{SL}_2(\mathbb{Z}/\ell_i\mathbb{Z})$. In particular, the (geometric) extension $K/\mathbb{F}_q(j(E))$ is disjoint from $\mathbb{F}_q(j(E), E[\ell])/\mathbb{F}_q(j(E))$ for almost all primes ℓ; that is, there exists a positive constant $c(E, K)$, depending on E and K, such that the geometric Galois group of $K(E[\ell])/K$ is $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell \geq c(E, K)$, $\ell \neq \mathrm{char}\,\mathbb{F}_q$. The function-field analogue of Serre's question can thus be formulated as whether $c(E, K)$ can be chosen to depend only on K. We prove that this is indeed so.

Theorem 1.1. Let $C/\mathbb{F}_q$ be a proper, smooth, geometrically connected curve, and let $K := \mathbb{F}_q(C)$ be its function field. Then there exists a positive constant $c(K)$, depending at most on the genus of K, such that for any elliptic curve E/K with nonconstant j-invariant and any rational prime $\ell \geq c(K)$, $\ell \neq \mathrm{char}\,\mathbb{F}_q$, the geometric Galois group of $K(E[\ell])/K$ is $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. More precisely,

$$c(K) := 2 + \max\left\{\ell : \ell \text{ prime},\ \frac{1}{12}\left[\ell - \left(6 + 3\,e_2 + 4\,e_3\right)\right] \leq \mathrm{genus}(K)\right\}, \tag{1.2}$$

where $e_2 = +1$ if $\ell \equiv 1 (\mathrm{mod}\, 4)$ and -1 otherwise, and $e_3 = +1$ if $\ell \equiv 1 (\mathrm{mod}\, 3)$ and -1 otherwise. □

The proof applies to any perfect field of characteristic 0 or equal to $p = \operatorname{char} \mathbb{F}_q$ in place of $\mathbb{F}_q$. For example, we can apply it to an elliptic curve $E/\mathbb{Q}(t)$ with nonconstant j-invariant (i.e., $j(E) \in \mathbb{Q}(t)\backslash\mathbb{Q}$). For almost all $t_0 \in \mathbb{Q}$ the special fiber E_{t_0} of E is an elliptic curve over $\mathbb{Q}$. The average analogue of Serre's question that we consider is whether there is a universal constant $c(\mathbb{Q})$ which depends at most on $\mathbb{Q}$ and works for "most" curves E_{t_0} in the one-parameter family $E/\mathbb{Q}(t)$. We pass from the function field to the average analogue of Serre's question via the following application of Theorem 1.1 and of a function-field version of the Chebotarev density theorem due to [17].

Theorem 1.2. Let $A(t), B(t) \in \mathbb{Z}[t]$ be fixed polynomials such that the j-invariant $j(E)$ of the curve

$$E/\mathbb{Q}(t) : y^2 = x^3 + A(t)x + B(t) \tag{1.3}$$

is nonconstant. Let $\Delta_{A,B}(t) := -16[4A(t)^3 + 27B(t)^2]$ be the discriminant of the curve E. Let $p \neq \ell$ be fixed rational primes such that the specialization of $j(E)$ to $\mathbb{F}_p(t)$ is nonconstant and $\ell \geq 17$. Let τ be a fixed integer. Then

$$\#\{t_0 \in \mathbb{F}_p : \Delta_{A,B}(t_0) \not\equiv 0 (\operatorname{mod} p),\ a_p(t_0) \equiv \tau (\operatorname{mod} \ell)\} = \frac{1}{\ell} p + O_{A,B}\left(\ell p^{1/2}\right), \tag{1.4}$$

where $a_p(t_0) := p + 1 - |E_{t_0}(\mathbb{F}_p)|$, and the implied $O_{A,B}$-constant depends at most on the polynomials A, B. □

We note that for almost all primes p, the specialization $E/\mathbb{F}_p(t)$ will also be an elliptic curve with nonconstant j-invariant.

The average result is as follows.

Theorem 1.3. Let $A(t), B(t) \in \mathbb{Z}[t]$ be fixed polynomials such that the j-invariant of the curve

$$E/\mathbb{Q}(t) : y^2 = x^3 + A(t)x + B(t) \tag{1.5}$$

is nonconstant. Let $\Delta_{A,B}$ be as in Theorem 1.2, and let S be the set of rational solutions to $\Delta_{A,B}(t) = 0$. Let $T > 0$ be fixed and set

$$\mathcal{F}(T) := \left\{ \frac{m}{n} \in \mathbb{Q}\backslash S : m, n \in \mathbb{Z},\ n \neq 0,\ (m,n) = 1,\ \max\left\{|m|, |n|\right\} \leq T \right\}. \tag{1.6}$$

For rational primes $\ell \geq 17$, set

$$\begin{aligned} \mathcal{E}_\ell(T) &:= \left\{t_0 \in \mathcal{F}(T) : \mathrm{Gal}\left(\mathbb{Q}\left(E_{t_0}[\ell]\right)/\mathbb{Q}\right) \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})\right\}, \\ \mathcal{E}(T) &:= \bigcup_{\ell \geq 17} \mathcal{E}_\ell(T). \end{aligned} \tag{1.7}$$

Then

$$\lim_{T \to \infty} \frac{\left|\mathcal{E}(T)\right|}{\left|\mathcal{F}(T)\right|} = 0. \tag{1.8}$$

□

We remark that the restriction to primes $\ell \geq 17$ in the above result is imposed by the hypothesis of Theorem 1.2, which, in turn, is imposed by Theorem 1.1. In particular, for $\ell = 13$ one finds that the modular curve $X_0(13)/\mathbb{Q}$, which corresponds to a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, has genus zero and that the universal elliptic curve $E \to X_0(13)$ (cf. [8]) satisfies $\mathcal{E}_{13}(T) = \mathcal{F}(T)$. One could certainly try to estimate the union of $\mathcal{E}_\ell(T)$ for all primes ℓ, but the techniques involved will be completely different from the ones presented in this paper.

Finally, Theorem 1.2 can also be used to give unconditional estimates regarding the Lang-Trotter conjecture on Frobenius traces.

Theorem 1.4. Let $A(t), B(t) \in \mathbb{Z}[t]$ be fixed polynomials such that the j-invariant of the curve

$$E/\mathbb{Q}(t) : y^2 = x^3 + A(t)x + B(t) \tag{1.9}$$

is nonconstant. Let $\Delta_{A,B}$ be as in Theorem 1.2. Let $0 \neq \tau \in \mathbb{Z}$ and let $T = T(x)$, $x \in (0, \infty)$. Let $\mathcal{F}(T)$ be as in Theorem 1.3 and for $t_0 \in \mathcal{F}(T)$ set

$$P_{t_0}^{\tau}(x) := \#\left\{p \leq x : p \nmid N_{t_0},\ a_p(t_0) = \tau\right\}, \tag{1.10}$$

where N_{t_0} is the conductor of $E_{t_0}/\mathbb{Q}$ and, as in Theorem 1.2, $a_p(t_0) := p + 1 - |E_{t_0}(\mathbb{F}_p)|$. Then, as $x \to \infty$,

$$\frac{1}{\left|\mathcal{F}(T)\right|} \sum_{t_0 \in \mathcal{C}(T)} P_{t_0}^{\tau}(x) \ll \frac{x^{3/4}}{\log x}, \tag{1.11}$$

provided that $T \asymp x$. □

A brief account of the history of the problem of estimating $P_{t_0}^{\tau}(x)$ will be given in Section 5.

Notation 1.5. If not otherwise stated, p, ℓ denote rational primes and q a prime power. As usual, $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ denotes the ring of 2×2 invertible matrices with entries in $\mathbb{Z}/\ell\mathbb{Z}$, $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ denotes the subring of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ consisting of matrices of determinant 1, $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ denotes the quotient $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/(\mathbb{Z}/\ell Z)^{\times}$, and $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ denotes the quotient $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})/(\pm 1)$. For a matrix m, $\det m$ and $\operatorname{tr} m$ denote its determinant and trace. For a finite set S, $\#S$ and $|S|$ are notations for its cardinality. For two real-valued functions f, g with g positive we write $f = O(g)$ or $f \ll g$ if there exists a constant $M > 0$ such that $|f(x)| \leq Mg(x)$ for all x. Often we specify the implied constant M by writing $f = O_M(g)$ or $f \ll_M g$. If f and g are positive and $f \ll g$, $g \ll f$, then we write $f \asymp g$. If $g \neq 0$ and the domain of f is infinite, we write $f \sim g$ to denote $\lim_{x\to\infty} f(x)/g(x) = 1$.

2 Proof of Theorem 1.1

Let $p := \operatorname{char} \mathbb{F}_q$ and let $\ell \neq 2, 3, p$ be a fixed rational prime. The statement of Theorem 1.1 is geometric in that it suffices to prove the theorem after a finite extension of scalars. Therefore we may assume that K contains a primitive ℓth root of unity (i.e., $q \equiv 1 (\mathrm{mod}\, \ell)$) and so $H_\ell = G_\ell$. Let us fix an embedding $G_\ell = \mathrm{Gal}(K(E[\ell])/K) \to \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

We write $X(1)/\mathbb{F}_q$ for the j-line of elliptic curves and $X(\ell)/\mathbb{F}_q$ for the modular curve parameterizing elliptic curves with level-ℓ structure. Then there exists a natural dominant morphism $X(\ell) \to X(1)$. There exist also dominant morphisms $C \xrightarrow{j} X(1)$ and $C_\ell \to C$ corresponding to the finite extensions of function fields $\mathbb{F}_q(j) \to K$, given by $j \mapsto j(E)$, and $K \to K(E[\ell])$, respectively (recall that $j(E)$ is nonconstant). Moreover, there is a natural action of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ on $X(\ell)$ and a G_ℓ-equivariant dominant morphism $C_\ell \to X(\ell)$ such that the following diagram commutes:

$$\begin{tikzcd} C_\ell \arrow[r] \arrow[d] & X(\ell) \arrow[d] \\ C \arrow[r] & X(1) \end{tikzcd} \tag{2.1}$$

The composite morphism $C_\ell \to X(\ell)/G_\ell$ factors through $C_\ell \to C$. In particular, the genus of the quotient $X(\ell)/G_\ell$ is at most the genus of C. To prove Theorem 1.1, we show that the quantity

$$\mathcal{N}(\ell) := \min\left\{\mathrm{genus}\left(X(\ell)/G\right) : G \subsetneq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})\right\} \tag{2.2}$$

tends to infinity as ℓ does. This implies that $G_\ell = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for $\ell \geq \ell_0$, where

$$\ell_0 := 2 + \max\left\{\ell' : \mathcal{N}(\ell') \leq \mathrm{genus}(C)\right\}, \tag{2.3}$$

which is precisely what we want to prove. We note that in [11] Levin uses a similar argument to bound the prime-to-p part of the torsion subgroup of $E(K)$ in terms of the genus of C.

The action of $SL_2(\mathbb{Z}/\ell\mathbb{Z})$ on $X(\ell)$ factors through the quotient group $\Gamma := PSL_2(\mathbb{Z}/\ell\mathbb{Z})$. Since $SL_2(\mathbb{Z}/\ell\mathbb{Z})$ has no subgroups of index 2, it suffices to show that the image of G_ℓ is all of Γ. For every subgroup $G \subseteq \Gamma$ we write π_G for the projection $X(\ell) \to X(\ell)/G$. We observe that if H is a subgroup of G, then $\pi_G : X(\ell) \to X(\ell)/G$ factors through $\pi_H : X(\ell) \to X(\ell)/H$, hence the genus of $X(\ell)/G$ is at most the genus of $X(\ell)/H$. Consequently,

$$\mathcal{N}(\ell) = \min\left\{\text{genus}\left(X(\ell)/G\right) : G \subsetneq \Gamma,\ G \text{ maximal}\right\}. \tag{2.4}$$

There are three cases of subgroups $G \subsetneq \Gamma$ that we must consider:

(1) $G = \Gamma \cap \mathbf{B}$, where $\mathbf{B} \subseteq PGL_2(\mathbb{Z}/\ell\mathbb{Z})$ is the image of a Borel subgroup;

(2) $G = \Gamma \cap N(\mathbf{C})$, where $N(\mathbf{C}) \subseteq PGL_2(\mathbb{Z}/\ell\mathbb{Z})$ is the image of the normalizer of a Cartan subgroup $\mathbf{C}$;

(3) G is isomorphic to the permutation groups $\boldsymbol{A}_4$, $\boldsymbol{S}_4$, or $\boldsymbol{A}_5$.

Let us also note that every maximal subgroup of Γ is $\Gamma \cap H$ for some maximal subgroup $H \subset PGL_2(\mathbb{Z}/\ell\mathbb{Z})$, hence a priori $[H : \Gamma \cap H] \leq 2$. Moreover, the determinant of any Borel subgroup or the normalizer of any Cartan subgroup of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$ is all of $(\mathbb{Z}/\ell\mathbb{Z})^\times$, thus $[\mathbf{B} : \Gamma \cap \mathbf{B}] = [N(\mathbf{C}) : \Gamma \cap N(\mathbf{C})] = 2$. In both cases this follows from the stronger fact that the determinant of a Cartan subgroup of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$ is all of $(\mathbb{Z}/\ell\mathbb{Z})^\times$, hence $[\mathbf{C} : \Gamma \cap \mathbf{C}] = 2$. In the last case above, $\boldsymbol{A}_4$ and $\boldsymbol{A}_5$ have no subgroups of index 2, and $\boldsymbol{A}_4 \subset \boldsymbol{S}_4$ is the unique subgroup of index 2.

Now let us see how we can calculate the genus of $X(\ell)/G$ for maximal subgroups $G \subseteq \Gamma$. The morphism $X(\ell) \to X(\ell)/\Gamma = X(1)$ is separable and tamely ramified, hence the same holds for the morphism $X(\ell) \to X(\ell)/G$ for every subgroup $G \subseteq \Gamma$. In particular, for every $G \subseteq \Gamma$ we may use the Riemann-Hurwitz formula to relate the genus of $X(\ell)$ and the genus of $X(\ell)/G$. For $G = \Gamma$ this allows us to deduce the genus of $X(\ell)$ because $X(\ell)/\Gamma$ has genus 0, and for other G it allows us to deduce the genus of $X(\ell)/G$. In all cases the genus of $X(\ell)/G$ is a geometric invariant, so it suffices to work over $\overline{\mathbb{F}}_q$.

For every geometric point $x \in X(\ell)$ we write $I(x) \subseteq \Gamma$ for the stabilizer of x. Then the Riemann-Hurwitz formula gives

$$2 \cdot \text{genus}\left(X(\ell)\right) - 2 = |G| \cdot \left(2 \cdot \text{genus}\left(X(\ell)/G\right) - 2\right) + \sum_{x \in X(\ell)} \left(\left|I(x) \cap G\right| - 1\right). \tag{2.5}$$

Table 2.1

G	$g_{(2)}$	$g_{(3)}$	$g_{(\ell)}$	$\text{genus}(X(\ell)/G)$
(1)	0	0	0	$\frac{1}{24}(\ell-3)(\ell-5)(\ell+2)$
$\Gamma\cap\mathbf{C}$	$\frac{1+e_{sp}\,e_2}{2}$	$\frac{1+e_{sp}\,e_3}{2}$	0	$\frac{1}{12}[\ell^2-(6-e_{sp})\ell+5-e_{sp}(3e_2+4e_3)]$
$\Gamma\cap N(\mathbf{C})$	$\frac{\ell+1+e_2-e_{sp}}{2}$	$\frac{1+e_{sp}\,e_3}{2}$	0	$\frac{1}{24}[\ell^2-(9-e_{sp})\ell+17+3e_2$ $-e_{sp}(6+3e_2+4e_3)]$
$\Gamma\cap\mathbf{B}$	$\frac{\ell(1+e_2)}{2}$	$\frac{\ell(1+e_3)}{2}$	1	$\frac{1}{12}[\ell-(6+3e_2+4e_3)]$
$\mathbf{A}_4$	3	4	0	$\frac{1}{288}[\ell^3-6\ell^2-51\ell+(294+18e_2+32e_3)]$
$\mathbf{S}_4$	9	4	0	$\frac{1}{576}[\ell^3-6\ell^2-87\ell+(582+54e_2+32e_3)]$
$\mathbf{A}_5$	15	10	0	$\frac{1}{1440}[\ell^3-6\ell^2-171\ell+(1446+90e_2+80e_3)]$
Γ	$\frac{\ell(\ell+e_2)}{2}$	$\frac{\ell(\ell+e_3)}{2}$	$\ell+1$	0

From Igusa we know that for $\pi_\Gamma(x)$ away from $j = 0, 1728, \infty$, the inertia subgroup $I(x)$ is trivial, and in the remaining three cases it is cyclic of order $n = 3, 2, \ell$, respectively. Moreover, there are $|\Gamma|/n$ points in the respective fiber, and Γ permutes them transitively. In particular, for a fixed cyclic subgroup $I \subseteq \Gamma$, the number of x such that $I(x) = I$ depends only on $|I|$. If $I \subset G$, then every x such that $I(x) = I$ will be ramified in $X(\ell) \to X(\ell)/G$.

We let $\gamma_{(n)}$ denote the number of $I \subseteq \Gamma$ such that $I \simeq \mathbb{Z}/n\mathbb{Z}$. Similarly, we write $g_{(n)}$ for the number of $I \subseteq G$ such that $I \simeq \mathbb{Z}/n\mathbb{Z}$. This allows us to rewrite the ramification part of (2.5) as follows:

$$\sum_{x\in X(\ell)} \left(\left|I(x)\cap G\right|-1\right) = \sum_{n=2,3,\ell} g_{(n)}\frac{|\Gamma|}{n\gamma_{(n)}}(n-1) = |\Gamma|\left(\frac{g_{(2)}}{2\gamma_{(2)}}+\frac{2g_{(3)}}{3\gamma_{(3)}}+\frac{(\ell-1)g_{(\ell)}}{\ell\gamma_{(\ell)}}\right). \tag{2.6}$$

(We gratefully acknowledge D. Allcock for pointing out this way of looking at the ramification part.)

We need to compute the numbers $|G|$, $g_{(n)}$, $\text{genus}(X(\ell)/G)$, and $\gamma_{(n)}$ as $G \subsetneq \Gamma$ varies over the maximal subgroups of Γ. Except for the orders, whose computation we leave as an exercise for the reader, the results are summarized in Table 2.1, where $e_{sp} = +1$ if $\mathbf{C}$ is split and -1 otherwise; $e_2 = +1$ if $\ell \equiv 1 (\text{mod}\, 4)$ and -1 otherwise; and $e_3 = +1$ if $\ell \equiv 1 (\text{mod}\, 3)$ and -1 otherwise. We will explain shortly how to calculate the $g_{(n)}$'s (and $\gamma_{(n)}$'s).

From Table 2.1 it is clear that $\mathcal{N}(5) = \mathcal{N}(7) = \mathcal{N}(11) = \mathcal{N}(13) = 0$, $\mathcal{N}(17) = 1$, and that

$$\mathcal{N}(\ell) = \frac{1}{12}\big[\ell - \big(6 + 3\,e_2 + 4\,e_3\,\big)\big] > 0 \tag{2.7}$$

for $\ell \geq 17$. Thus $\mathcal{N}(\ell)$ tends to infinity as ℓ does, which is what we wanted to show.

To complete the proof of the theorem, it remains to explain how to calculate the $g_{(n)}$'s. Computing $g_{(n)}$ for the three exceptional groups $\mathbf{A}_4, \mathbf{S}_4, \mathbf{A}_5$ is a relatively simple exercise which, again, we leave for the reader. We note that the exceptional cases occur only for certain values of ℓ (see [18, Section 2.5]), and the formulas in Table 2.1 for the genus of $X(\ell)/G$ will not be integral for general values of ℓ.

Now we observe that every subgroup $I \subseteq \Gamma$ of order ℓ is contained in a unique Borel subgroup $\mathbf{B} \subseteq \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$, hence $\gamma_{(\ell)}$ is equal to the number of Borel subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Sending a Borel subgroup to the unique line in $(\mathbb{Z}/\ell\mathbb{Z})^2$ stabilized by it gives a bijection between Borel subgroups and lines, so there are $\gamma_{(\ell)} = \ell + 1$ Borel subgroups. If $G \subsetneq \Gamma$ is a maximal subgroup of order divisible by ℓ, then taking $I \subseteq G$ we see that $G = \Gamma \cap \mathbf{B}$ and $g_{(\ell)} = 1$.

Finally, suppose $I \subseteq \Gamma$ is a subgroup of order $n = 2$ or 3. It lies in a unique Cartan subgroup $\Gamma \cap \mathbf{C}$, and whether or not $\mathbf{C}$ is split depends only on ℓ and n. We recall that $[\mathbf{C} : \Gamma \cap \mathbf{C}] = 2$, so $|\Gamma \cap \mathbf{C}| = (\ell - e_{\mathrm{sp}})/2$, and in particular, exactly one of the orders $(\ell \pm 1)/2$ is divisible by n. Combining this with the fact that $\mathbf{C}$ is cyclic, we deduce that $g_{(n)}(\Gamma \cap \mathbf{C}) = (1 + e_{\mathrm{sp}}\, e_n)/2$. Every Cartan subgroup $\mathbf{C} \subset \Gamma$ is conjugate to every other subgroup of the same type, so there are $|\Gamma|/|N(\mathbf{C})| = \ell(\ell + e_{\mathrm{sp}})/2$ Cartan subgroups of the same type. Then

$$\gamma_{(n)} = \frac{\ell(\ell+1)}{2} \cdot \frac{1+e_n}{2} + \frac{\ell(\ell-1)}{2} \cdot \frac{1-e_n}{2} = \frac{\ell\big(\ell + e_n\,\big)}{2}. \tag{2.8}$$

Every Borel subgroup $\mathbf{B}$ contains exactly ℓ split Cartan subgroups and no nonsplit Cartan subgroups, so $g_{(n)}(\Gamma \cap \mathbf{B}) = \ell(1+e_n)/2$. Finally, $\Gamma \cap (N(\mathbf{C}) \setminus \mathbf{C})$ consists of $|\Gamma \cap \mathbf{C}|$ involutions, hence $g_{(2)}(N(\mathbf{C})) = g_{(2)}(\mathbf{C}) + (\ell - e_{\mathrm{sp}})/2$ and $g_{(3)}(N(\mathbf{C})) = g_{(3)}(\mathbf{C})$.

3 Proof of Theorem 1.2

The proof of Theorem 1.2 is an application of an effective version of the Chebotarev density theorem over function fields, due to Murty and Scherk [17, Theorem 2].

Let p and ℓ be rational primes as in the statement of the theorem. Let $K := \mathbb{F}_p(t)$ be the specialization of $\mathbb{Q}(t)$ and let $|K|$ be its set of places. We observe that there is a finite set of places $S \subseteq |K|$ such that $K(E[\ell])/K$ is unramified away from S. We may take S

to be the set of places of bad reduction of E/K, in which case $\deg(S)$ will be bounded by a constant which is independent of p. For every $v \in |K| \backslash S$ there is a well-defined conjugacy class $\mathrm{Fr}_v \subseteq \mathrm{Gal}(K(E[\ell])/K)$ associated to v, the so-called *Frobenius class*, satisfying $\deg(\mathrm{Fr}_v) = p^{\deg(v)}$.

Since K has genus zero, then the constant $c(K)$ given by Theorem 1.1 is 15. By the hypothesis of Theorem 1.2, we have $\ell \geq 17$, thus Theorem 1.1 implies that the geometric Galois group of $K(E[\ell])/K$ is $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. In other words, $G_\ell := \mathrm{Gal}(K(E[\ell])/K)$ is the unique subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ containing $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and satisfying $\det(G_\ell) = \langle p \rangle$. We set

$$\begin{aligned} G_\ell^p &:= \{g \in G_\ell : \det(g) = p\}, \\ \mathcal{C}_\tau &:= \{g \in G_\ell : \mathrm{tr}(g) = \tau\}, \\ \mathcal{C}_\tau^p &:= \mathcal{C}_\tau \cap G_\ell^p. \end{aligned} \tag{3.1}$$

We notice that each of G_ℓ^p and $\mathcal{C}_\tau$ is a union of conjugacy classes, hence $\mathcal{C}_\tau^p$ is as well. Once we show that $|\mathcal{C}_\tau^p| \asymp \ell^2$, Theorem 1.2 is a specific instance of the effective Chebotarev theorem due to Murty-Scherk that we mentioned above. We give a specialization of their result taking advantage of our assumptions.

Proposition 3.1 (Murty-Scherk [17]). With $K = \mathbb{F}_p(t)$ as before, let F/K be a tamely ramified, finite Galois extension and let $U \subset |K|$ be the open complement of its ramification locus $Z \subset |K|$. Let $G := \mathrm{Gal}(F/K)$ and suppose that $\mathcal{C} \subseteq G$ is a union of conjugacy classes. Let $G^p := \{g \in G : \det(g) = p\}$ and $\mathcal{C}^p := \mathcal{C} \cap G^p$. Then

$$\#\{v \in U(\mathbb{F}_p) : \mathrm{Fr}_v \subseteq \mathcal{C}^p\} = \frac{|\mathcal{C}^p|}{|G^p|}|U(\mathbb{F}_p)| + O_{K,Z}\left(|\mathcal{C}^p|^{1/2} p^{1/2}\right), \tag{3.2}$$

where the implied $O_{K,Z}$-constant depends only on the genus of K and the degree of Z. □

We apply this proposition to the extension $K(E[\ell])/K$, of Galois group G_ℓ, and to the conjugacy set $\mathcal{C}_\tau$. As we noted in the proof of Theorem 1.1, $K(E[\ell])/K$ is tamely ramified. Let us also note that $\deg(Z) \leq \deg(S)$, hence the implicit $O_{K,Z}$-constant may be taken to be independent of ℓ and p. In our application, $|G_\ell^p| = |\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})| = \ell(\ell^2 - 1)$ and $|\mathcal{C}_\tau^p| = \ell(\ell + e \cdot \ell)$, where $e \in \{-1, 0, 1\}$, depending only on the quantity $\delta := \tau^2 - 4p$. It remains to show how to calculate $|\mathcal{C}_\tau^p|$.

When $\delta = 0$, every $g \in \mathcal{C}_\tau^p$ has one eigenvalue $b \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ of multiplicity two, and g/b is an element of order ℓ. Either $g/b = 1$, in which case g lies in the center of

G_ℓ, or g lies in a unique Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. For each Borel subgroup there are $\ell - 1$ such g, all of which are conjugate. Moreover, every Borel is conjugate, so there are $(\ell+1)(\ell-1) = \ell^2 - 1$ elements in the conjugacy class of g. Combining these we see that

$$\left|\mathcal{C}_\tau^p\right| = \left(\ell^2 - 1\right) + 1 = \ell^2. \tag{3.3}$$

When $\delta \neq 0$, every $g \in \mathcal{C}_\tau^p$ has distinct eigenvalues and $g \in \mathbf{C}$ for some Cartan subgroup $\mathbf{C} \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. We know that $\mathbf{C}$ is split if δ is a square and nonsplit otherwise. The conjugacy class of g contains exactly one other element of $\mathbf{C}$ which is given by $\omega\gamma\omega^{-1}$ for any $\omega \in N(\mathbf{C})\backslash\mathbf{C}$ (as before, $N(\mathbf{C})$ is the normalizer of $\mathbf{C}$ in G_ℓ). Finally, by assumption, g is nonscalar, thus it does not lie in the intersection of two different Cartan subgroups. Hence

$$\left|\mathcal{C}_\tau^p\right| = \ell(\ell+1), \tag{3.4}$$

the number of split Cartans, if δ is a square, and

$$\left|\mathcal{C}_\tau^p\right| = \ell(\ell-1), \tag{3.5}$$

the number of nonsplit Cartans, otherwise.

4 Proof of Theorem 1.3

Similarly to the proof of [4, Theorem 1], the proof of Theorem 1.3 is an application of Gallagher's 2-dimensional large sieve [5, Lemma A], which we recall below.

Lemma 4.1 (Gallagher [5]). Let $\mathcal{A}$ be a subset of $\mathbb{Z}^2$, and $\mathcal{P}$ a set of rational primes. For each prime $p \in \mathcal{P}$, let $\Omega(p)$ be a subset of $(\mathbb{Z}/p\mathbb{Z})^2$ with $\omega(p)$ elements. For $x > 0$, $\alpha = (\alpha_1, \alpha_2) \in \mathcal{A}$, set

$$\begin{aligned} P(x) &:= \sum_{\substack{p\in\mathcal{P}\\ p\le x}} \frac{\omega(p)}{p^2}, \\ P(\alpha, x) &:= \#\left\{p \le x : p \in \mathcal{P},\ \alpha(\operatorname{mod} p) \in \Omega(p)\right\}. \end{aligned} \tag{4.1}$$

Then for any $z \ge x^2$,

$$\sum_{\substack{\alpha\in\mathcal{A}\\ |\alpha|\le z}} \left[P(\alpha, x) - P(x)\right]^2 \ll z^2 P(x), \tag{4.2}$$

where $|\alpha| \le z$ means that $\max\{\alpha_1, \alpha_2\} \le z$. □

Let $\ell \geq 17$ be a fixed rational prime, and let $\delta, \tau \in \mathbb{Z}/\ell\mathbb{Z}$ be fixed residue classes with $\delta \not\equiv 0 (\mathrm{mod}\, \ell)$. We keep the notation introduced in the statement of Theorem 1.3. Our first aim is to find an upper estimate for the cardinality of

$$\mathcal{E}_{\ell,\delta,\tau}(T) := \left\{t_0 \in \mathcal{F}(T) : \pi_{t_0}(x, \ell, \delta, \tau) = 0 \; \forall x > 0\right\}, \tag{4.3}$$

where

$$\pi_{t_0}(x, \ell, \delta, \tau) := \#\left\{p \leq x : p \nmid \ell \cdot N_{t_0},\ p \equiv \delta (\mathrm{mod}\, \ell),\ a_p\left(E_{t_0}\right) \equiv \tau (\mathrm{mod}\, \ell)\right\} \tag{4.4}$$

and where N_{t_0} is the conductor of $E_{t_0}/\mathbb{Q}$. We apply Lemma 4.1 to

$$\begin{aligned}
&\mathcal{A} := \left\{(m, n) \in \mathbb{Z}^2 : n \neq 0,\ (m, n) = 1,\ \frac{m}{n} \notin S\right\},\\
&\mathcal{P} := \left\{p : p \neq \ell,\ p \equiv \delta (\mathrm{mod}\, \ell)\right\},\\
&\Omega(p) := \left\{(m, n) \in \mathcal{A} : (n, p) = 1,\ p \nmid N_{m/n},\ a_p\left(E_{m/n}\right) \equiv \tau (\mathrm{mod}\, \ell)\right\},\\
&z := T, \qquad x := \sqrt{T}.
\end{aligned} \tag{4.5}$$

We obtain

$$\begin{aligned}
P\left(\sqrt{T}\right)^2 \left|\mathcal{E}_{\ell,\delta,\tau}(T)\right| &= \sum_{\substack{(m,n)\in\mathcal{A} \\ \max\{|m|,|n|\}\leq T \\ (m/n)\in\mathcal{E}_{\ell,\delta,\tau}(T)}} \left[\pi_{m/n}\left(\sqrt{T}; \ell, \delta, \tau\right) - P\left(\sqrt{T}\right)\right]^2 \\
&\leq \sum_{\substack{(m,n)\in\mathcal{A} \\ \max\{|m|,|n|\}\leq T}} \left[\pi_{m/n}\left(\sqrt{T}; \ell, \delta, \tau\right) - P\left(\sqrt{T}\right)\right]^2 \\
&\ll T^2 \cdot P\left(\sqrt{T}\right),
\end{aligned} \tag{4.6}$$

which implies that

$$\left|\mathcal{E}_{\ell,\delta,\tau}(T)\right| \ll \frac{T^2}{P\left(\sqrt{T}\right)}. \tag{4.7}$$

Now we need to estimate $P(\sqrt{T})$; here is where the crucial difference lies between our proof and the proof of the two-parameter average obtained in [4]. Since $\ell \geq 17$, we can apply Theorem 1.2 and obtain

$$\begin{aligned} P(\sqrt{T}) &= \sum_{\substack{p \le \sqrt{T} \\ p \ne \ell \\ p \equiv \delta (\operatorname{mod} \ell)}} \frac{1}{p^2}\left[\frac{1}{\ell}p(p-1) + O_{A,B}\left(\ell p^{3/2}\right)\right] \\ &= \frac{1}{\ell}\pi(\sqrt{T}; \ell, \delta) + O_{A,B}\left(\frac{T^{1/4}}{\log T}\right), \end{aligned} \tag{4.8}$$

where, for $x > 0$,

$$\pi(x; \ell, \delta) := \#\{p \le x : p \equiv \delta (\operatorname{mod} \ell)\}. \tag{4.9}$$

We recall that by the Siegel-Walfisz theorem, if $\ell \ll (\log x)^B$ for some $B > 0$, then $\pi(x; \ell, \delta) \gg x/\ell \log x$. Thus in order to obtain an upper bound for $\#\mathcal{E}_{\ell,\delta,\tau}(T)$ it suffices that we verify that the hypothesis of the Siegel-Walfisz theorem holds for our particular ℓ.

Let us note that $\mathcal{E}_{\ell,\delta,\tau}(T)$ is a subset of rational numbers $t_0 \in \mathcal{F}(T)$ such that ℓ is an exceptional prime for $E_{t_0}/\mathbb{Q}$ (in the sense defined in Section 1). By [12], there exist positive absolute constants c_1, γ_1 such that

$$\ell \le c_1 \left(\log H(E_{t_0})\right)^{\gamma_1} \tag{4.10}$$

for any $t_0 \in \mathcal{E}_{\ell,\delta,\tau}(T)$, where $H(E_{t_0})$ is the naive height of $E_{t_0}/\mathbb{Q}$. Consequently, there exists a positive constant $c_2(A, B)$, depending on the polynomials A, B, such that

$$\ell \le c_2(A, B)(\log T)^{\gamma_1}. \tag{4.11}$$

Thus the hypothesis of Siegel-Walfisz is satisfied, and we get the lower bound

$$P(\sqrt{T}) \gg_{A,B} \frac{\sqrt{T}}{(\log T)^{\gamma_2}} \tag{4.12}$$

for some absolute constant $\gamma_2 > 0$. By plugging this estimate into (4.7) and by invoking once again (4.11), we obtain

$$\left|\mathcal{E}_{\ell,\delta,\tau}(T)\right| \ll_{A,B} T^{3/2}(\log T)^{\gamma_3} \tag{4.13}$$

for some absolute constant $\gamma_3 > 0$.

Combining all these "ℓ, δ, τ-estimates" leads to

$$\left|\mathcal{E}(T)\right| \leq \sum_{\ell \geq 17} \sum_{\substack{\delta,\tau \in \mathbb{Z}/\ell\mathbb{Z} \\ \delta \not\equiv 0 (\mathrm{mod}\, \ell)}} \left|\mathcal{E}_{\ell,\delta,\tau}(T)\right| \ll_{A,B} T^{3/2}(\log T)^{\gamma_4} \tag{4.14}$$

for some absolute constant $\gamma_4 > 0$, where, again, we made use of (4.11). It is now clear that

$$\lim_{T \to \infty} \frac{\left|\mathcal{E}(T)\right|}{\left|\mathcal{F}(T)\right|} = 0, \tag{4.15}$$

and so the proof of Theorem 1.3 is complete.

5 Proof of Theorem 1.4

A well-known conjecture formulated by Lang and Trotter in 1976 [10] predicts that for an elliptic curve $E/\mathbb{Q}$, of conductor N_E, and for an integer $\tau \in \mathbb{Z}$, there exists a positive constant $c(E, \tau)$, depending on E and τ, such that

$$P_E^\tau(x) := \#\{p \leq x : p \nmid N_E,\ a_p(E) = \tau\} \sim c(E, \tau)\frac{\sqrt{x}}{\log x}, \tag{5.1}$$

provided that E is without complex multiplication, or is with complex multiplication but $\tau \neq 0$. Here, $a_p(E) := p + 1 - |E(\mathbb{F}_p)|$.

From [15, 16, 19] we know nontrivial upper bounds for $P_E^\tau(x)$ under the assumption of a generalized Riemann hypothesis (GRH). More specifically, the current best bound is $P_E^\tau(x) \ll_E (x^{4/5}/\log x)$, obtained under GRH in [16]. It is also known that the conjecture is true on average over two-parameter families of elliptic curves [3].

A straightforward application of Theorem 1.2 leads to an upper bound for the one-parameter average $(1/|\mathcal{F}(T)|) \sum_{t_0 \in \mathcal{F}(T)} P_{t_0}^\tau(x)$, as follows.

Let $\ell \geq 17$ be an arbitrary rational prime to be chosen optimally later. Clearly we have

$$\begin{aligned} \sum_{t_0 \in \mathcal{F}(T)} P_{t_0}^\tau(x) &\leq \sum_{t_0 \in \mathcal{F}(T)} \#\{p \leq x : p \nmid N_t,\ a_p(E_{t_0}) \equiv \tau (\mathrm{mod}\, \ell)\} \\ &= \sum_{p \leq x} \sum_{\substack{t_0 \in \mathcal{F}(T) \\ p \nmid N_{t_0} \\ a_p(E_{t_0}) \equiv \tau (\mathrm{mod}\, \ell)}} 1. \end{aligned} \tag{5.2}$$

By Theorem 1.2, the most inner sum is

$$\ll \left(\frac{T^2}{p^2} + 1\right)\left(\frac{p^2}{\ell} + \ell p^{3/2}\right). \tag{5.3}$$

Thus

$$\begin{aligned}\sum_{t_0 \in \mathcal{F}(T)} P^{\tau}_{t_0}(x) &\ll_{A,B} \sum_{p \leq x} \left(\frac{T^2}{\ell} + \frac{T^2 \ell}{p^{1/2}} + \frac{p^2}{\ell} + \ell p^{3/2} \right) \\ &\ll \frac{T^2 x}{\ell \log x} + \frac{T^2 \ell x^{1/2}}{\log x} + \frac{x^3}{\ell \log x} + \frac{\ell x^{5/2}}{\log x}.\end{aligned} \tag{5.4}$$

We choose the prime ℓ so that $\ell \asymp x^{1/4}$. Since the parameter T is such that $T \asymp x$, (5.4) becomes

$$\frac{1}{\#\mathcal{F}(T)} \sum_{t_0 \in \mathcal{F}(T)} P^{\tau}_{t_0}(x) \ll \frac{x^{3/4}}{\log x}, \tag{5.5}$$

which completes the proof.

6 Conclusions

It is natural to ask whether the constant $c(K)$ given in Theorem 1.1 depends at most on the so-called *gonality* of K. Recall that the gonality of K is defined to be the degree of the smallest nonconstant map $C \to \mathbb{P}^1$, an analogue of the degree of a number field over $\mathbb{Q}$. For example, if we consider an infinite sequence of hyperelliptic curves of strictly increasing genus, then Theorem 1.1 will fail to yield a bound which works for all curves in the sequence. On the other hand, a bound in terms of the gonality of every curve of the sequence—two—would suffice.

In [1], it is shown that the gonality of $(X(\ell)/G)/\mathbb{C}$ (we keep the notation introduced in Section 2) is asymptotic to a constant times the genus of $X(\ell)/G$; however, Abramovich's proof does not generalize to char p. We note that for any nonconstant map of curves $C_1 \to C_2$, the gonality of C_1 is at least the gonality of C_2. The analogous fact, that $\text{genus}(C_1) \geq \text{genus}(C_2)$, is all we used in the first part of our proof of Theorem 1.1. In particular, the problem reduces to asking whether the gonality of $X(\ell)/G$ tends to infinity as $G \subsetneq \mathrm{PSL}_2(\mathbb{Z}/\ell/\mathbb{Z})$ varies over the maximal subgroups and ℓ tends to infinity.

As pointed out in the introduction regarding Theorem 1.3, it is of interest to estimate the size of $\bigcup_{\ell \geq 2} \mathcal{E}_\ell(T)$, and not only the size of the union over primes $\ell \geq 17$. For example, in [4], the sieve argument together with a result of Deuring in place of Theorem 1.2 imposes $\ell \geq 5$. The remaining estimates for the primes $\ell = 2, 3$ are based on lattice point arguments. Moreover, in [6], estimates for each individual $\ell \geq 2$ are given for a two-parameter family of elliptic curves. Grant's arguments, however, do not seem to work for one-parameter families of elliptic curves. It is reasonable to expect that, for small primes, a different type of sieve arguments should actually work (this is already clear for $\ell = 2$), and we will address this problem in a different paper.

It is also natural to ask whether Theorem 1.3 holds for a one-parameter family of elliptic curves defined over a fixed number field that is not necessarily $\mathbb{Q}$, and whether we could take $A(t), B(t)$ to be fixed elements of the function field of any given curve. To answer the first question, we would need to work out an n-dimensional large sieve for number fields. To answer the second question, we would need to find an optimal way of ordering the parameters t. We plan to undertake these additional questions in a future project.

Acknowledgments

We are grateful to Peter Sarnak for suggesting that we treat the one-parameter average of Serre's question and for useful conversations on this topic. We are also grateful to Daniel Allcock, Jordan Ellenberg, Nick Katz, and Felipe Voloch for helpful discussions.

References

[1] D. Abramovich, *A linear lower bound on the gonality of modular curves*, Int. Math. Res. Not. **1996** (1996), no. 20, 1005–1011.

[2] A. C. Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canad. Math. Bull. **48** (2005), no. 1, 16–31.

[3] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Int. Math. Res. Not. **1999** (1999), no. 4, 165–183.

[4] W. Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818.

[5] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic Number Theory (Proc. Sympos. Pure Math., Vol. 24, St. Louis Univ., St. Louis, Mo, 1972), American Mathematical Society, Rhode Island, 1973, pp. 91–101.

[6] D. Grant, *A formula for the number of elliptic curves with exceptional primes*, Compositio Math. **122** (2000), no. 2, 151–164.

[7] J.-I. Igusa, *Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves*, Amer. J. Math. **81** (1959), 453–476.

[8] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, New Jersey, 1985.

[9] A. Kraus, *Une remarque sur les points de torsion des courbes elliptiques* [*A remark about the torsion points of elliptic curves*], C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 9, 1143–1146 (French).

[10] S. Lang and H. Trotter, *Frobenius Distributions in* GL_2*-Extensions. Distribution of Frobenius Automorphisms in* GL_2*-Extensions of the Rational Numbers*, Lecture Notes in Mathematics, vol. 504, Springer, Berlin, 1976.

[11] M. Levin, *On the group of rational points on elliptic curves over function fields*, Amer. J. Math. **90** (1968), 456–462.

[12] D. W. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. **25** (1993), no. 3, 247–254.

[13] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), no. 2, 129–162.

[14] L. Merel, *Arithmetic of elliptic curves and Diophantine equations*, J. Théor. Nombres Bordeaux **11** (1999), no. 1, 173–200.

[15] V. K. Murty, *Explicit formulae and the Lang-Trotter conjecture*, Rocky Mountain J. Math. **15** (1985), no. 2, 535–551.

[16] M. R. Murty, V. K. Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), no. 2, 253–281.

[17] V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 6, 523–528.

[18] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331 (French).

[19] ———, *Quelques applications du théorème de densité de Chebotarev* [*Some applications of the Chebotarev density theorem*], Inst. Hautes Études Sci. Publ. Math. **54** (1981), 123–201 (French).

Alina Carmen Cojocaru: Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08540, USA
E-mail address: cojocaru@math.princeton.edu

Chris Hall: Department of Mathematics, University of Texas at Austin, 1 University Station c1200, Austin, TX 78712-0257, USA
E-mail address: cjh@math.utexas.edu