Canad. J. Math. Vol. **57** (6), 2005 pp. 1155–1177

The Square Sieve and the Lang–Trotter Conjecture

Alina Carmen Cojocaru, Etienne Fouvry and M. Ram Murty

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ and without complex multiplication. Let K be a fixed imaginary quadratic field. We find nontrivial upper bounds for the number of ordinary primes $p \leq x$ for which $\mathbb{Q}(\pi_p) = K$, where π_p denotes the Frobenius endomorphism of E at p. More precisely, under a generalized Riemann hypothesis we show that this number is $O_E(x^{17/18}\log x)$, and unconditionally we show that this number is $O_{E,K}\big(\frac{x(\log\log x)^{13/12}}{(\log x)^{25/24}}\big)$. We also prove that the number of imaginary quadratic fields K, with $-\operatorname{disc} K \leq x$ and of the form $K = \mathbb{Q}(\pi_p)$, is $\gg_E \log\log\log x$ for $x \geq x_0(E)$. These results represent progress towards a 1976 Lang–Trotter conjecture.

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N, and let S_E be the set of primes of bad reduction for E (that is, the prime divisors of N). For a prime p of good reduction for E (*i.e.* $p \notin S_E$) we introduce the usual notation: $\bar{E}$ is the reduction of E modulo p; $a_p := p + 1 - \#\bar{E}(\mathbb{F}_p)$ (here, $\#S$ denotes the cardinality of a set S); π_p is a (complex) root of the polynomial $X^2 - a_pX + p \in \mathbb{Z}[X]$. We recall that p is said to be of *ordinary* reduction for E if $a_p \neq 0$, and of *supersingular* reduction for E otherwise. Also, let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ and $\operatorname{End}_{\overline{\mathbb{Q}}}(E)$ denote the ring of endomorphisms of E over $\overline{\mathbb{Q}}$.

If E is a curve with complex multiplication (denoted CM), then we know that, for primes p of ordinary reduction for E,

$$\mathbb{Q}(\pi_p) = \operatorname{End}_{\overline{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

By contrast, if E is a curve without complex multiplication (denoted non-CM), then we will prove that, when p runs over primes of ordinary reduction for E, there are infinitely many distinct fields $\mathbb{Q}(\pi_p)$ (see Corollary 1.5 below). More generally, we have the following conjecture of Lang and Trotter [LT]:

Conjecture 1.1 (Lang–Trotter, 1976) *Let E be a non-*CM *elliptic curve defined over $\mathbb{Q}$. Let K be a fixed imaginary quadratic field. We denote by*

$$P_E(K, x) := \#\{p \leq x : p \notin S_E, \mathbb{Q}(\pi_p) = K\}.$$

Received by the editors November 17, 2003.

The first author was supported in part by an Ontario Graduate Scholarship and by an NSERC post-doctoral fellowship. Research of the third author was supported in part by an NSERC grant.

AMS subject classification: Primary: 11G05; secondary: 11N36, 11R45.

Keywords: Elliptic curves modulo p; Lang–Trotter conjecture; applications of sieve methods.

Then there exists a positive constant $C(K,E)$, depending on K and E, such that, as $x \to \infty$,

$$P_E(K,x) \sim C(K,E)\frac{x^{1/2}}{\log x}.$$

In 1981 [Se3, p. 191], J-P. Serre asserted that one could show, under the assumption of a Generalized Riemann Hypothesis (denoted GRH) and using Selberg's sieve, that

$$P_E(K,x) = O_{E,K}(x^{\theta}) \tag{1}$$

for some $\theta < 1$. This result does not appear anywhere in the literature and, moreover, we do not know of any progress concerning the conjecture of Lang and Trotter to have been made yet. Serre had a proof for (1) which he did not publish. In [Se4, p. 715], Serre made a brief remark indicating that in order to obtain (1), one could use the context of l-adic Lie groups, namely apply [Se3, Theorem 10] directly to a Galois representation $r\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_l) \times \mathrm{GL}_2(\mathbb{Z}_l)$, where $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denotes the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$ and $\mathrm{GL}_2(\mathbb{Z}_l)$ denotes the group of 2×2 invertible matrices with entries in the l-adic integers $\mathbb{Z}_l$, and where the first factor of r is given by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the l-adic Tate module and the second factor is a Hecke character of K. In private communication, he has indicated to us that this gives an estimate of $O_K(x^{\frac{9}{10}}/(\log x)^{\frac{3}{5}})$, without specifying the dependence on K. Based on his remark, this dependence seems to be at least as large as the class number of K, which grows like $\sqrt{D}$ if we write $K = \mathbb{Q}(\sqrt{-D})$ for some positive square-free integer D. Kumar Murty has observed that one can dispense with the context of l-adic Lie groups and apply the Chebotarev density theorem directly, with the same result. The existence of the extra factor (roughly similar to $\sqrt{D}$, as mentioned above) in the upper bound for $P_E(K,x)$ annihilates the interest in this upper bound as $\log D/\log x$ increases, and apparently prevents us from deducing a result as good as Corollary 1.5 below.

Our goal in this paper is to indicate how a simple device, that we call *the square sieve*, can be used to get non-trivial upper bounds for $P_E(K,x)$. It will be noticed that even though the exponent 17/18 (see Theorem 1.2 below) can be improved upon, our bound is uniform in K. Thus, the 'raison d'être' of this paper is two-fold. First to derive a non-trivial and independent of K estimate for $P_E(K,x)$ in a simple way (since no such estimate has ever appeared in print) and second to give a novel application of the square sieve. No doubt, the technique will have wider applications.

In the last section, we record remarks made by Serre to us in several e-mail communications. These remarks may be useful in future research.

Precise formulations of our results are as follows.

Theorem 1.2 *Let E be a non-*CM *elliptic curve defined over $\mathbb{Q}$ and of conductor N. Let $\mathbb{Q}(\sqrt{-D})$ be a fixed imaginary quadratic field. Let $x \geq 3$ be a positive real number.*

With the notation introduced before we have that:

(a) *if we assume* GRH *for the Dedekind zeta functions of the division fields of E, then*

$$P_E\big(\mathbb{Q}(\sqrt{-D}),x\big) \ll_N x^{17/18}\log x;$$

(b) *if we assume* GRH *and Artin's Holomorphy Conjecture (denoted* AHC*) for the L-functions of the irreducible characters of the Galois groups of the division fields of E, then*

$$P_E\big(\mathbb{Q}(\sqrt{-D}), x\big) \ll_N x^{13/14}\log x;$$

(c) *if we assume* GRH*, as well as* AHC *and a Pair Correlation Conjecture (denoted* PCC*) for the L-functions of the irreducible characters of the Galois groups of the division fields of E, then*

$$P_E\big(\mathbb{Q}(\sqrt{-D}), x\big) \ll_N x^{11/12}\log x.$$

The implied $\ll$-constants above depend at most on N.

Theorem 1.3 *There exists an absolute constant c such that, for any non-*CM *elliptic curve E defined over $\mathbb{Q}$ and of conductor N, for every real number $x \geq 3$, and for every positive square-free integer $D \geq 1$, we have*

$$P_E\big(\mathbb{Q}(\sqrt{-D}), x\big) \ll_N \frac{x(\log\log x)^{13/12}}{(\log x)^{25/24}}\big(1 + \nu(x, D, c)\big),$$

where

$$\nu(x, D, c) := \#\left\{ p \text{ a prime} : p|D, c\frac{(\log x)^{1/24}}{(\log\log x)^{1/12}} \leq p \leq 2c\frac{(\log x)^{1/24}}{(\log\log x)^{1/12}} \right\}.$$

In particular, under the same conditions, we have

$$P_E\big(\mathbb{Q}(\sqrt{-D}), x\big) \ll_N \frac{x(\log\log x)^{13/12}}{(\log x)^{25/24}}\big(1 + \nu(D)\big),$$

where $\nu(D)$ denotes the number of (distinct) prime divisors of D. The implied $\ll$-constants above depend on N, at most.

Remark 1.4 Since the number of primes between $c\frac{(\log x)^{1/24}}{(\log\log x)^{1/12}}$ and $2c\frac{(\log x)^{1/24}}{(\log\log x)^{1/12}}$ is

$$\sim 24c\frac{(\log x)^{1/24}}{(\log\log x)^{13/12}},$$

we see that the above upper bound is, in the worst case (*i.e.,* when any prime p of the above interval divides D) just as weak as the trivial bound $P_E\big(\mathbb{Q}(\sqrt{-D}), x\big) \ll \frac{x}{\log x}$. Notice that for almost all square-free positive integers $D \leq 4x$, the above upper-bounds are valuable and that the effect of the term $\nu(x, D, c)$ could be diminished by averaging over D belonging to an interval.

We are also concerned with the values of the fields $\mathbb{Q}(\pi_p)$ as p runs over primes. We denote by $\mathcal{D}_E(x)$ the set of (distinct) square-free parts of $4p-a_p^2$ for primes $p \leq x$ of ordinary reduction for E. So $\mathcal{D}_E(\infty)$ is the sequence $(1 \leq)D_1 < D_2 < D_3 < \cdots$ of square-free positive integers D such that $\mathbb{Q}(\sqrt{-D}) = \mathbb{Q}(\pi_p)$ for some prime p of ordinary reduction for E (note the trivial inclusion $\mathcal{D}_E(x) \subset \mathcal{D}_E(\infty) \cap [1, 4x]$). Using Theorems 1.2 and 1.3 we obtain conditional and unconditional lower bounds for $\#\big(\mathcal{D}_E(\infty) \cap [1, x]\big)$.

Corollary 1.5 *Let E be a non-*CM *elliptic curve defined over $\mathbb{Q}$ and of conductor N. For $x \geq 3$, we have that:*

(a) *if we assume* GRH *for the Dedekind zeta functions of the division fields of E, then*

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

(b) *if we assume* GRH *and* AHC *for the L-functions of the irreducible characters of the Galois groups of the division fields of E, then*

$$\#\mathcal{D}_E(x) \gg_N \frac{x^{1/14}}{(\log x)^2};$$

(c) *if we assume* GRH, AHC *and* PCC *for the L-functions of the irreducible characters of the Galois groups of the division fields of E, then*

$$\#\mathcal{D}_E(x) \gg_N \frac{x^{1/12}}{(\log x)^2};$$

(d) *without any unproven hypothesis,*

$$\#\mathcal{D}_E(\infty) = \infty.$$

More precisely, there exists $x_0 = x_0(N)$ such that, for any $x > x_0$, at least one of the following two events (2), (3) *is true:*

$$\#\big(\mathcal{D}_E(\infty) \cap [1, 4x]\big) \geq (\log x)^{1/24}, \tag{2}$$

$$\min\big\{\big(\mathcal{D}_E(\infty) \cap (4x, \infty)\big)\big\} \leq \exp\big((\log x)^{26}\big). \tag{3}$$

In any case we have, for $x \geq x_0(N)$,

$$\#\big(\mathcal{D}_E(\infty) \cap [1, x]\big) \gg_N \log\log\log x.$$

The implied constants in these estimates depend on N, at most.

Remark 1.6 Note that in the statement $\#\mathcal{D}_E(\infty) = \infty$ of Corollary 1.5, the condition for a prime p to be of ordinary reduction is essential, for otherwise $D = p$, and the result is a trivial consequence of a theorem of Elkies [El] telling us that there are infinitely many supersingular primes p for E.

Remark 1.7 The pair of exponents $(\frac{1}{24}, 26)$ appearing in (2) and (3) can be replaced by others (to be more precise, by any pair of real numbers (θ_0, θ_1) satisfying $\theta_0 > 0$ and $\theta_1 > 24(1 + \theta_0)$; see the proof in Section 5). They illustrate our poor knowledge of the set $\mathcal{D}_E(\infty)$, which is mainly due to the effect of the term $\nu(x, D, c)$, which may be quite large.

In what follows, p, q, l will denote rational primes, k positive integers, and x, z positive real numbers. Given an elliptic curve E defined over $\mathbb{Q}$ and of conductor N, the prime p will be such that $p \nmid N$. Whenever we write $\ll_c$, $\gg_c$ or O_c for some c, we indicate that the implicit constant depends on c, at most; whenever we write $\ll$, $\gg$ or O, it indicates that the implicit constant is absolute.

2 Preliminaries

2.1 The Square Sieve

The principal tool in the proofs of our main results is the square sieve, which originates in [H-B] and which can be stated as follows:

Theorem 2.1 (The square sieve) *Let $\mathcal{A}$ be a finite set of not necessarily distinct, nonzero integers, and let $\mathcal{P}$ be a set of (distinct) odd primes. Set*

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

Then

$$S(\mathcal{A}) \le \frac{\#\mathcal{A}}{\#\mathcal{P}} + \max_{\substack{l,q\in\mathcal{P}\\ l\neq q}} \Big| \sum_{\alpha\in\mathcal{A}} \Big(\frac{\alpha}{lq}\Big) \Big| + \frac{2}{\#\mathcal{P}} \sum_{\alpha\in\mathcal{A}} \sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)\neq 1}} 1 + \frac{1}{(\#\mathcal{P})^2} \sum_{\alpha\in\mathcal{A}} \Big(\sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)\neq 1}} 1\Big)^2,$$

where $(\frac{\cdot}{lq})$ denotes the Jacobi symbol, (α, l) denotes the greatest common divisor of α and l, and max *denotes the maximum element of the above set of numbers.*

Proof We observe that if $\alpha \in \mathcal{A}$ is a square, then

$$\sum_{l\in\mathcal{P}} \Big(\frac{\alpha}{l}\Big) = \sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)=1}} \Big(\frac{\alpha}{l}\Big) + \sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)\neq 1}} \Big(\frac{\alpha}{l}\Big) = \sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)=1}} 1 = \#\mathcal{P} - \sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)\neq 1}} 1,$$

that is,

$$\sum_{l\in\mathcal{P}} \Big(\frac{\alpha}{l}\Big) + \sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)\neq 1}} 1 = \#\mathcal{P}.$$

Thus

$$\begin{aligned}
S(\mathcal{A}) &\le \sum_{\alpha\in\mathcal{A}} \frac{1}{(\#\mathcal{P})^2}\Big(\sum_{l\in\mathcal{P}}\Big(\frac{\alpha}{l}\Big) + \sum_{\substack{l\in\mathcal{P}\\(\alpha,l)\neq 1}} 1\Big)^2 \\
&= \sum_{\alpha\in\mathcal{A}} \frac{1}{(\#\mathcal{P})^2}\Big(\sum_{l,q\in\mathcal{P}}\Big(\frac{\alpha}{lq}\Big) + 2\Big(\sum_{l\in\mathcal{P}}\Big(\frac{\alpha}{l}\Big)\Big)\Big(\sum_{\substack{l\in\mathcal{P}\\(\alpha,l)\neq 1}} 1\Big) + \Big(\sum_{\substack{l\in\mathcal{P}\\(\alpha,l)\neq 1}} 1\Big)^2\Big) \\
&= \sum_{\alpha\in\mathcal{A}} \frac{1}{(\#\mathcal{P})^2}\sum_{l\in\mathcal{P}}\Big(\frac{\alpha}{l^2}\Big) + \sum_{\alpha\in\mathcal{A}} \frac{1}{(\#\mathcal{P})^2}\sum_{\substack{l,q\in\mathcal{P}\\l\neq q}}\Big(\frac{\alpha}{lq}\Big) \\
&\qquad + \sum_{\alpha\in\mathcal{A}} \frac{1}{(\#\mathcal{P})^2}\Big(2\Big(\sum_{l\in\mathcal{P}}\Big(\frac{\alpha}{l}\Big)\Big)\sum_{\substack{l\in\mathcal{P}\\(\alpha,l)\neq 1}} 1 + \Big(\sum_{\substack{l\in\mathcal{P}\\(\alpha,l)\neq 1}} 1\Big)^2\Big) \\
&\le \frac{\#\mathcal{A}}{\#\mathcal{P}} + \max_{\substack{l,q\in\mathcal{P}\\l\neq q}}\Big|\sum_{\alpha\in\mathcal{A}}\Big(\frac{\alpha}{lq}\Big)\Big| + \frac{2}{\#\mathcal{P}}\sum_{\alpha\in\mathcal{A}}\sum_{\substack{l\in\mathcal{P}\\(\alpha,l)\neq 1}} 1 + \frac{1}{(\#\mathcal{P})^2}\sum_{\alpha\in\mathcal{A}}\Big(\sum_{\substack{l\in\mathcal{P}\\(\alpha,l)\neq 1}} 1\Big)^2.
\end{aligned}$$

This completes the proof of the lemma. ∎

Remark 2.2 In the above proof, the fact that $\mathcal{P}$ was a set of primes did not play a crucial role. Thus, the main idea of the proof has the potential for wider applications.

2.2 The Chebotarev Density Theorem

Another important tool for the proofs of our main results is the Chebotarev density theorem, which we recall below.

We let $L/\mathbb{Q}$ be a finite Galois extension with group G, of degree n_L and discriminant d_L, and we denote by ζ_L the Dedekind zeta function of L. We let C be a conjugacy set in G, that is, C is a union of conjugacy classes of G. The set of conjugacy classes contained in C is denoted by $\tilde{C}$, and the set of conjugacy classes contained in G is denoted by $\tilde{G}$. We denote by $\mathcal{P}(L/\mathbb{Q})$ the set of rational primes p which ramify in $L/\mathbb{Q}$ and set

$$M(L/\mathbb{Q}) := (\#G)\prod_{p\in\mathcal{P}(L/\mathbb{Q})} p.$$

We define

$$\pi_C(x, L/\mathbb{Q}) := \#\{p \le x : p \text{ unramified in } L/\mathbb{Q}, \sigma_p \subseteq C\},$$

where σ_p is the Artin symbol of p in the extension $L/\mathbb{Q}$.

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

$$\pi_C(x, L/\mathbb{Q}) \sim \frac{\#C}{\#G}\operatorname{li} x,$$

where $\operatorname{li} x = \int_2^x \frac{1}{\log t}\,dt$ is the logarithmic integral.

Effective versions of this theorem (that is, versions with explicit error terms) are what we actually need in our calculations. They were first derived by J. Lagarias and A. Odlyzko in 1976 (see [LO]), refined by J.-P. Serre (see [Se3]), and subsequently improved by Kumar Murty, Ram Murty and N. Saradha (see [MMS] and [MM]). We state them below.

Theorem 2.3 *Assuming* GRH *for the Dedekind zeta function of L, we have that, for all $x \geq 3$,*

$$\pi_C(x, L/\mathbb{Q}) = \frac{\#C}{\#G} \operatorname{li} x + O\Big((\#C) x^{1/2} \Big(\frac{\log |d_L|}{n_L} + \log x \Big) \Big).$$

The implied O-constant is absolute.

This version of the effective Chebotarev density theorem is slightly more refined than a statement given in [LO] and is due to Serre (see [Se3, p. 133]).

Unconditional versions of the effective Chebotarev density theorem are also very useful, however the error terms obtained are not as good as the conditional ones:

Theorem 2.4 *There exist positive constants A, b and b', with A effective and b, b' absolute, such that, if*

$$\log x \geq b n_L (\log |d_L|)^2,$$

then

$$\pi_C(x, L/\mathbb{Q}) = \frac{\#C}{\#G} \operatorname{li} x + O\Big(\frac{\#C}{\#G} \operatorname{li} \Big(x \exp\Big(-b' \frac{\log x}{\max\{|d_L|^{1/n_L}, \log |d_L|\}} \Big) \Big) \Big)$$
$$+ O\Big((\#\tilde{C}) x \exp\Big(-A \sqrt{\frac{\log x}{n_L}} \Big) \Big).$$

The implied O-constants are absolute.

This is a consequence of the unconditional Chebotarev density theorem in [LO, formulae (1.6), (1.7), (1.8)] and of Stark's bound given in [St] for the exceptional zero of ζ_L as defined in [LO, pp. 455–456]. Of course, the first O-term can be dropped if there does not exist such an exceptional zero.

By assuming, in addition to GRH, conjectures AHC and PCC, one can improve the error term in the asymptotic formula for $\pi_C(x, L/\mathbb{Q})$. For formulations of conjectures AHC and PCC we refer the reader to [RM3].

Theorem 2.5

1. *Assuming* GRH *and* AHC *for the Artin L-functions attached to the irreducible characters of G, we have that, for all $x \geq 3$,*

$$\pi_C(x, L/\mathbb{Q}) = \frac{\#C}{\#G} \operatorname{li} x + O\Big((\#C)^{1/2} x^{1/2} \log\big(M(L/\mathbb{Q}) x \big) \Big).$$

2. *Assuming* GRH, AHC *and* PCC *for the Artin L-functions attached to the irreducible characters of G, we have that, for all* $x \geq 3$,

$$\pi_C(x, L/\mathbb{Q}) = \frac{\#C}{\#G} \operatorname{li} x + O\Big((\#C)^{1/2} x^{1/2} \Big(\frac{\#\tilde{G}}{\#G} \Big)^{1/4} \log(M(L/\mathbb{Q})x) \Big).$$

The implied O-constants are absolute.

These results were obtained by Kumar Murty, Ram Murty and N. Saradha, and Kumar Murty and Ram Murty, respectively (see [MMS, MM]).

The following result is often very helpful in estimating the error terms in the effective Chebotarev density theorem. Its proof is given in [Se3, p. 130] and is based on a result of Hensel (see [Se3, pp. 126–127]).

Lemma 2.6 *Let* $L/\mathbb{Q}$ *be a finite Galois extension of degree* n_L *and discriminant* d_L. *Using the notation introduced above, we have that*

$$\frac{n_L}{2} \sum_{p \in \mathcal{P}(L/\mathbb{Q})} \log p \leq \log |d_L| \leq (n_L - 1) \sum_{p \in \mathcal{P}(L/\mathbb{Q})} \log p + n_L \log n_L.$$

2.3 Some Group Theory

For a positive integer k, let us denote by $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$ the group of 2×2 invertible matrices with entries in the coset residues modulo k, and by det and tr the determinant and trace, respectively, of any matrix in this group.

Lemma 2.7 *Let* $q > 2$ *be a prime and* $d, t \in \mathbb{Z}/q\mathbb{Z}$ *be fixed. Then, for* $d \neq 0$,

$$\#\{g \in \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) : \det g = d, \operatorname{tr} g = t\} = q\Big(q + \Big(\frac{t^2 - 4d}{q} \Big) \Big),$$

where $(\frac{\cdot}{q})$ *denotes the Legendre symbol modulo q.*

Proof The cardinality in question is the number of solutions $\alpha, \beta, \gamma, \delta \pmod q$ of the system of equations

$$\alpha\delta - \beta\gamma = d, \tag{4}$$

$$\alpha + \delta = t. \tag{5}$$

Since the last equation determines δ in terms of α, the number of solutions $\alpha, \beta, \gamma, \delta \pmod q$ of (4) and (5) is also the number of solutions $\alpha, \beta, \gamma \pmod q$ of the equation

$$\alpha^2 - \alpha t + \beta\gamma + d = 0. \tag{6}$$

We see that equation (6) has degree 2 in α, and so the total number of solutions is

$$\sum_{\beta \pmod q} \sum_{\gamma \pmod q} \Big(1 + \Big(\frac{t^2 - 4\beta\gamma - 4d}{q}\Big)\Big)$$
$$= q^2 + \sum_{\substack{\beta \pmod q \\ \beta \neq 0}} \sum_{\gamma \pmod q} \Big(\frac{t^2 - 4\beta\gamma - 4d}{q}\Big) + q\Big(\frac{t^2 - 4d}{q}\Big).$$

Since the inner sum over γ is zero, we obtain the result. ∎

Corollary 2.8 *Let l and q be two distinct odd primes, and $d, t \in \mathbb{Z}/lq\mathbb{Z}$ be fixed with $(d, lq) = 1$. Then*

$$\#\{g \in \mathrm{GL}_2(\mathbb{Z}/lq\mathbb{Z}) : \det g = d, \operatorname{tr} g = t\} = lq\Big(l + \Big(\frac{t^2 - 4d}{l}\Big)\Big)\Big(q + \Big(\frac{t^2 - 4d}{q}\Big)\Big),$$

where $(\frac{\cdot}{l})$ and $(\frac{\cdot}{q})$ denote the Legendre symbols modulo l and q, respectively.

Proof This is an immediate consequence of Lemma 2.7 and the ring isomorphism $\mathrm{GL}_2(\mathbb{Z}/lq\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. ∎

Corollary 2.9 *Let l and q be two distinct odd primes. Then*

$$\#\{g \in \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) : 4\det g = (\operatorname{tr} g)^2\} = q^2(q-1),$$
$$\#\{g \in \mathrm{GL}_2(\mathbb{Z}/lq\mathbb{Z}) : 4\det g = (\operatorname{tr} g)^2\} = l^2q^2(l-1)(q-1).$$

Proof We sum the formula of Lemma 2.7 over d and t modulo q satisfying $t^2 = 4d$, $t \not\equiv 0 \pmod q$, and apply the ring isomorphism $\mathrm{GL}_2(\mathbb{Z}/lq\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. ∎

3 Proof of Theorem 1.2

We want to find an upper bound for the number of primes $p \le x$, $p \notin S_E$, for which $\mathbb{Q}(\pi_p) = \mathbb{Q}(\sqrt{-D})$, that is, for which

$$4p - a_p^2 = Dm^2$$

for some nonzero integer m. For this, it is enough to find an upper bound for the number of squares in the multi-set

$$\mathcal{A} := \{D(4p - a_p^2) : p \le x\}.$$

We use the square sieve (Theorem 2.1) with $\mathcal{A}$ as above and with the set $\mathcal{P}$ of primes defined by

$$\mathcal{P} := \{q \text{ a prime} : z < q \le 2z\},$$

where

$$z = z(x) > aN(\log\log N)^{\frac{1}{2}} \tag{7}$$

is a positive real number depending on x and to be chosen later, with a denoting a positive absolute constant also to be specified later. For a nonzero integer α let

$$\nu_z(\alpha) := \#\{l \in \mathcal{P} : l|\alpha\}. \tag{8}$$

Then, from Theorem 2.1 and the inequality $\nu_z(\alpha) \ll \log\alpha$, we obtain

$$\begin{aligned} S(\mathcal{A}) &= \#\{\alpha \in \mathcal{A} : \alpha \text{ is a square}\} \\ &\leq \frac{\#\mathcal{A}}{\#\mathcal{P}} + \max_{\substack{l,q\in\mathcal{P}\\ l\neq q}} \Big| \sum_{\alpha\in\mathcal{A}} \Big(\frac{\alpha}{lq}\Big) \Big| + O\bigg(\frac{1}{\#\mathcal{P}} \sum_{\alpha\in\mathcal{A}} \log\alpha + \frac{1}{(\#\mathcal{P})^2} \sum_{\alpha\in\mathcal{A}} (\log\alpha)^2 \bigg). \end{aligned} \tag{9}$$

We easily observe that, by elementary estimates, we have

$$\#\mathcal{A} \ll \frac{x}{\log x}, \quad \#\mathcal{P} \asymp \frac{z}{\log z}, \tag{10}$$

$$\begin{aligned} \sum_{\alpha\in\mathcal{A}} \log\alpha &= \sum_{p\leq x} \log\big(D(4p - a_p^2)\big) \\ &= \pi(x)\log D + \sum_{p\leq x} \log(4p - a_p^2) \\ &\leq \pi(x)\log D + \sum_{p\leq x} \log(4p) \\ &\ll \frac{x\log D}{\log x} + x, \end{aligned} \tag{11}$$

and

$$\begin{aligned} \sum_{\alpha\in\mathcal{A}} (\log\alpha)^2 &= \sum_{p\leq x} (\log D)^2 + 2(\log D) \sum_{p\leq x} \log(4p - a_p^2) + \sum_{p\leq x} \big(\log(4p - a_p^2)\big)^2 \\ &\ll \frac{x(\log D)^2}{\log x} + x\log D + x\log x. \end{aligned} \tag{12}$$

Thus, in order to obtain an upper estimate for $S(\mathcal{A})$, it suffices to find an upper bound for $\max_{\substack{l,q\in\mathcal{P}\\ l\neq q}} |\sum_{\alpha\in\mathcal{A}} (\frac{\alpha}{lq})|$.

Let $l, q \in \mathcal{P}$, $l \neq q$ be fixed. We write

$$\begin{aligned}\sum_{\alpha\in\mathcal{A}}\Big(\frac{\alpha}{lq}\Big) &= \sum_{\substack{p\le x\\ p\nmid lqN}}\left(\frac{D(4p-a_p^2)}{lq}\right)+O(\log N)\\ &= \Big(\frac{D}{lq}\Big)\sum_{t(\mathrm{mod}\ lq)}\sum_{d(\mathrm{mod}\ lq)}\sum_{\substack{p\le x,\,p\nmid lqN\\ a_p\equiv t(\mathrm{mod}\ lq)\\ p\equiv d(\mathrm{mod}\ lq)}}\Big(\frac{4p-a_p^2}{lq}\Big)+O(\log N)\\ &= \Big(\frac{D}{lq}\Big)\sum_{t(\mathrm{mod}\ lq)}\sum_{\substack{d(\mathrm{mod}\ lq)\\ (d,lq)=1}}\Big(\frac{4d-t^2}{lq}\Big)\pi_E(x,lq,t,d)+O(\log N), \qquad (13)\end{aligned}$$

where

$$\pi_E(x,lq,t,d) := \#\{p\le x : p\nmid lqN, a_p\equiv t(\mathrm{mod}\ lq), p\equiv d(\mathrm{mod}\ lq)\}. \qquad (14)$$

We shall use effective versions of the Chebotarev density theorem to estimate $\pi_E(x, lq, t, d)$ for $(d, lq) = 1$. Before giving the details, we need to recall a few properties of E.

For any positive integer k we denote by $E[k]$ the group of k-division points of E, and by $\mathbb{Q}(E[k])$ the field obtained by adjoining to $\mathbb{Q}$ the x- and y-coordinates of the k-division points of E. We know that $\mathbb{Q}(E[k])/\mathbb{Q}$ is a finite Galois extension, whose ramified primes lie among the prime divisors of k and of the conductor N of E. We denote by $n(k), d(k)$ and G_k the degree, discriminant and Galois group, respectively, of $\mathbb{Q}(E[k])/\mathbb{Q}$. One can define a natural Galois representation

$$\phi_k\colon G_k \to \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}),$$

which is easily seen to be injective. Thus, using Lemma 2.6 and recalling that

$$\#\,\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}) = k^4\prod_{\substack{p\mid k\\ p\ \mathrm{prime}}}\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{p^2}\Big),$$

we deduce that

$$\frac{\log|d(k)|}{n(k)} \le \log n(k)+\log(kN) \le 5\log k+\log N,$$

and, consequently, that

$$d(k)^{\frac{1}{n(k)}} \le k^5N,\ \log|d(k)| \le k^4\log(k^5N) \text{ and } n(k)\big(\log|d(k)|\big)^2 \le k^{12}\big(\log(k^5N)\big)^2. \qquad (15)$$

If E is a non-CM elliptic curve (as in our situation), then, by deep results of Serre, there exists a positive integer $A(E)$, depending on E, such that ϕ_k is surjective for

any $\big(k, A(E)\big) = 1$ (see [Se1] and [acC2, Appendix]). Therefore for such k we have $G_k = \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$. We also know that there exists a positive absolute constant a such that if $p > aN(\log\log N)^{\frac{1}{2}}$, then $p \nmid A(E)$ (see [acC2, Theorem 2]). Therefore, with this choice of a in (7) we have that $\big(lq, A(E)\big) = 1$ for our fixed primes l, q, and so the representation ϕ_{lq} is bijective. Another important property of ϕ_k is that

$$\operatorname{tr} \phi_k(\sigma_p) \equiv a_p (\operatorname{mod} k)$$

and

$$\det \phi_k(\sigma_p) \equiv p (\operatorname{mod} k)$$

for any prime $p \nmid N$ and any integer k such that $(p, kN) = 1$, where σ_p denotes the Artin symbol of p in $\mathbb{Q}(E[k])/\mathbb{Q}$.

Now let us look at ϕ_{lq} for our fixed distinct primes $l, q \in \mathcal{P}$ and let us set

$$C_{lq}(t,d) := \{g \in G_{lq} : p \nmid lqN, \det \phi_{lq}(g) = d, \operatorname{tr} \phi_{lq}(g) = t\}.$$

Since, from the above, $G_{lq} \simeq \mathrm{GL}_2(\mathbb{Z}/lq\mathbb{Z})$, Corollary 2.8 provides us with precise information about $\#C_{lq}(t,d)$. We also observe that

$$\pi_E(x, lq, t, d) = \#\{p \le x : p \nmid lqN, \phi_{lq}(\sigma_p) \subseteq C_{lq}(t,d)\}, \tag{16}$$

hence we can now use the Chebotarev density theorem to estimate $\pi_E(x, lq, t, d)$ for $(d, lq) = 1$.

(a) Assuming GRH for the Dedekind zeta function of $\mathbb{Q}(E[lq])$ and using Theorem 2.3 and Corollary 2.8, we obtain that, for $(d, lq) = 1$,

$$\begin{aligned}\pi_E(x, lq, t, d) &= \frac{\#C_{lq}(t,d)}{\#G_{lq}} \operatorname{li} x + O\big((\#C_{lq}(t,d) x^{\frac{1}{2}} \log(lqNx)\big) \\ &= \frac{\big(l + (\frac{t^2-4d}{l})\big)\big(q + (\frac{t^2-4d}{q})\big)}{(l-1)(l^2-1)(q-1)(q^2-1)} \operatorname{li} x + O\big(l^2 q^2 x^{\frac{1}{2}} \log(lqNx)\big).\end{aligned}$$

Then (13) becomes

$$\begin{aligned}\sum_{\alpha \in \mathcal{A}} \Big(\frac{\alpha}{lq}\Big) = \Big(\frac{D}{lq}\Big) &\frac{lq}{(l^2-1)(l-1)(q^2-1)(q-1)} \operatorname{li} x \sum_{t (\operatorname{mod} lq)} \sum_{\substack{d (\operatorname{mod} lq) \\ (d, lq) = 1}} \Big(\frac{4d - t^2}{lq}\Big) \\ &+ O\Big(\sum_{t (\operatorname{mod} lq)} \sum_{d (\operatorname{mod} lq)} \frac{l+q}{(l^2-1)(l-1)(q^2-1)(q-1)} \operatorname{li} x\Big) \\ &+ O\Big(\sum_{t (\operatorname{mod} lq)} \sum_{d (\operatorname{mod} lq)} l^2 q^2 x^{\frac{1}{2}} \log(lqNx)\Big).\end{aligned}$$

We observe that $\sum_{(d,q)\neq 1}(\frac{4d-t^2}{q}) = (\frac{-t^2}{q})$, so, by the Chinese remainder theorem, we have that, for any integer t,

$$\Big|\sum_{\substack{d \pmod{lq}\\(d,lq)=1}} \Big(\frac{4d-t^2}{lq}\Big)\Big| \leq 1.$$

Therefore

$$\sum_{\alpha\in\mathcal{A}} \Big(\frac{\alpha}{lq}\Big) = O\bigg(\Big(\frac{1}{l}+\frac{1}{q}\Big)\frac{x}{\log x}\bigg) + O\big(l^4q^4x^{\frac{1}{2}}\log(lqNx)\big). \tag{17}$$

By plugging (10)–(12) and (17) into (9) we get

$$\begin{aligned} S(\mathcal{A}) \ll{}& \frac{x\log z}{z\log x} + \frac{x}{z\log x} + z^8x^{\frac{1}{2}}\log(zNx)\\ &+ \frac{x\log z}{z\log x}\log D + \frac{x\log z}{z}\\ &+ \frac{x(\log z)^2}{z^2\log x}(\log D)^2 + \frac{x(\log z)^2}{z^2}\log D + \frac{x(\log x)(\log z)^2}{z^2}. \end{aligned}$$

Now we choose

$$z := x^{\frac{1}{18}}$$

and notice that $P_E\big(\mathbb{Q}(\sqrt{-D}),x\big) = 0$ for (square-free) $D > 4x$, which allows us to assume $\log D \ll \log x$. This gives us that $P_E\big(\mathbb{Q}(\sqrt{-D}),x\big) \leq S(\mathcal{A}) \ll_N x^{17/18}\log x$, completing the proof of the first part of the theorem.

(b) We assume GRH and AHC and use part 1 of Theorem 2.5 to improve the error term in the asymptotic formula for $\pi_E(x,lq,t,d)$ for $(d,lq)=1$. We obtain

$$\pi_E(x,lq,t,d) = \frac{\big(l+(\frac{t^2-4d}{l})\big)\big(q+(\frac{t^2-4d}{q})\big)}{(l-1)(l^2-1)(q-1)(q^2-1)}\operatorname{li} x + O\big(lqx^{\frac{1}{2}}\log(lqNx)\big).$$

Proceeding as in part (a), we see that (13) becomes

$$\sum_{\alpha\in\mathcal{A}} \Big(\frac{\alpha}{lq}\Big) = O\bigg(\Big(\frac{1}{l}+\frac{1}{q}\Big)\frac{x}{\log x}\bigg) + O\big(l^3q^3x^{\frac{1}{2}}\log(lqNx)\big). \tag{18}$$

We plug (10)–(12) and (18) into (9) and get

$$\begin{aligned} S(\mathcal{A}) \ll{}& \frac{x\log z}{z\log x} + \frac{x}{z\log x} + z^6x^{\frac{1}{2}}\log(zNx)\\ &+ \frac{x\log z}{z\log x}\log D + \frac{x\log z}{z}\\ &+ \frac{x(\log z)^2}{z^2\log x}(\log D)^2 + \frac{x(\log z)^2}{z^2}\log D + \frac{x(\log x)(\log z)^2}{z^2}. \end{aligned}$$

Now we choose

$$z := x^{\frac{1}{14}}.$$

Arguing as in part (a), this gives us $P_E\big(\mathbb{Q}(\sqrt{-D}), x\big) \leq S(\mathcal{A}) \ll_N x^{\frac{13}{14}} \log x$, which completes the proof of the second part of the theorem.

(c) Let us assume GRH, AHC and PCC and use part 2 of Theorem 2.5 to obtain even better error terms for $\pi_E(x, lq, t, d)$ for $(d, lq) = 1$. We remark that for the primes l and q under consideration we have $\frac{\#\widetilde{G_{lq}}}{\#G_{lq}} = \frac{\#\widetilde{\mathrm{GL}_2(\mathbb{Z}/lq\mathbb{Z})}}{\#\,\mathrm{GL}_2(\mathbb{Z}/lq\mathbb{Z})} = \frac{1}{(l^2-l)(q^2-q)}$.Then

$$\begin{aligned}\pi_E(x, lq, t, d) &= \frac{\#C_{lq}}{\#G_{lq}} \operatorname{li} x + O\left((\#C_{lq})^{\frac{1}{2}} \left(\frac{\#(\widetilde{G_{lq}})}{\#G_{lq}} \right)^{\frac{1}{4}} x^{\frac{1}{2}} \log(lqNx) \right) \\ &= \frac{\big(l + (\frac{t^2-4d}{l})\big)\big(q + (\frac{t^2-4d}{q})\big)}{(l-1)(l^2-1)(q-1)(q^2-1)} \operatorname{li} x + O\big(l^{\frac{1}{2}} q^{\frac{1}{2}} x^{\frac{1}{2}} \log(lqNx)\big).\end{aligned}$$

Proceeding again as in part (a), we see that (13) becomes

$$\sum_{\alpha \in \mathcal{A}} \left(\frac{\alpha}{lq} \right) = O\left(\left(\frac{1}{l} + \frac{1}{q} \right) \frac{x}{\log x} \right) + O\big(l^{\frac{5}{2}} q^{\frac{5}{2}} x^{\frac{1}{2}} \log(lqNx)\big). \tag{19}$$

Then, from (9)–(12) and (19), we get

$$\begin{aligned}S(\mathcal{A}) \ll{}& \frac{x \log z}{z \log x} + \frac{x}{z \log x} + z^5 x^{\frac{1}{2}} \log(zNx) \\ &+ \frac{x \log z}{z \log x} \log D + \frac{x \log z}{z} \\ &+ \frac{x (\log z)^2}{z^2 \log x} (\log D)^2 + \frac{x (\log z)^2}{z^2} \log D + \frac{x (\log x)(\log z)^2}{z^2}.\end{aligned}$$

Now we choose

$$z := x^{\frac{1}{12}}.$$

As in part (a), this gives us $P_E\big(\mathbb{Q}(\sqrt{-D}), x\big) \leq S(\mathcal{A}) \ll_N x^{\frac{11}{12}} \log x$, which completes the proof of Theorem 1.2.

4 Proof of Theorem 1.3

We use the notation introduced in the proof of Theorem 1.2 and we proceed similarly, however this time we are not assuming GRH or any other hypotheses. More precisely,

we apply the square sieve (Theorem 2.1) to the multi-set of integers $\mathcal{A} := \{D(4p - a_p^2) : p \le x\}$ and the set of primes $\mathcal{P} := \{q : z \le q \le 2z\}$, where

$$z := c\frac{(\log x)^{\frac{1}{24}}}{(\log\log x)^{\frac{1}{12}}} \tag{20}$$

for some positive constant c to be fixed later. We obtain

$$\begin{aligned} P_E\big(\mathbb{Q}(\sqrt{-D}), x\big) &\le S(\mathcal{A}) \\ &\ll \frac{x\log z}{z\log x} \\ &\quad + \max_{\substack{l,q\in\mathcal{P}\\ l\neq q}}\Big|\Big(\frac{D}{lq}\Big)\sum_{t(\mathrm{mod}\ lq)}\sum_{\substack{d(\mathrm{mod}\ lq)\\(d,lq)=1}}\Big(\frac{4d-t^2}{lq}\Big)\pi_E(x,lq,t,d)\Big| \\ &\quad + \frac{\log z}{z}\sum_{p\le x}\sum_{\substack{z\le q\le 2z\\ q\mid D(4p-a_p^2)}} 1 + \Big(\frac{\log z}{z}\Big)^2\sum_{p\le x}\Big(\sum_{\substack{z\le q\le 2z\\ q\mid D(4p-a_p^2)}} 1\Big)^2. \end{aligned} \tag{21}$$

Here $\pi_E(x, lq, t, d)$ is defined as in (14) and can be estimated by using the unconditional effective Chebotarev density theorem. Indeed, we first observe that $\pi_E(x, lq, t, d)$ is also given by (16) and that if x is large enough so that $z \gg N(\log\log N)^{\frac{1}{2}}$, then the Galois representation ϕ_{lq} is surjective for any distinct primes $l, q \in \mathcal{P}$. Thus the sizes of the conjugacy sets $C_{lq}(t, d)$ appearing in (16) can be estimated once again using Corollary 2.8. Then we observe that, from (15) with $k = lq$ and from (20),

$$n(lq)\big(\log|d(lq)|\big)^2 \le 25(lq)^{12}\big(\log(lqN)\big)^2 \le 25\cdot 4^{12}z^{24}\big(\log(4z^2N)\big)^2 \le \frac{\log x}{c'}$$

for some positive absolute constant c', depending on c. If c is chosen sufficiently small, then the hypothesis of Theorem 2.4 is satisfied. Thus from Theorem 2.4, Corollary 2.8 and again (15) we obtain that, for $(d, lq) = 1$, there exists a positive absolute constant A' such that

$$\begin{aligned} \pi_E(x,lq,t,d) &= \#\{p\le x : p\nmid lqN, \phi_{lq}(\sigma_p)\subseteq C_{lq}(t,d)\} \\ &= \frac{\big(l+(\frac{t^2-4d}{l})\big)\big(q+(\frac{t^2-4d}{q})\big)}{(l-1)(l^2-1)(q-1)(q^2-1)}\operatorname{li} x \\ &\quad + O\Big(\frac{x}{l^2q^2\log x}\exp\Big(-\frac{A'\log x}{(lq)^5N}\Big)\Big) \\ &\quad + O\Big(x\exp\Big(-A'\sqrt{\frac{\log x}{l^4q^4}}\Big)\Big). \end{aligned}$$

Arguing as in the proof of Theorem 1.2 and keeping in mind our choice of z we further get

$$\begin{aligned}\max_{\substack{l,q\in\mathcal{P}\\ l\neq q}}\Big|\Big(\frac{D}{lq}\Big)\sum_{t(\mathrm{mod}\ lq)}\sum_{\substack{d(\mathrm{mod}\ lq)\\(d,lq)=1}}\Big(\frac{4d-t^2}{lq}\Big)\pi_E(x,lq,t,d)\Big|&\\ \ll \frac{x}{z\log x}+\frac{x}{\log x}\exp\Big(-\frac{A'\log x}{z^{10}N}\Big)+xz^4\exp\Big(-A'\sqrt{\frac{\log x}{z^8}}\Big)&\\ \ll \frac{x}{z\log x}.&\qquad(22)\end{aligned}$$

It remains to estimate the last two terms of (21). Using notation (8) we write

$$\begin{aligned}\sum_{p\leq x}\sum_{\substack{z\leq q\leq 2z\\ q|D(4p-a_p^2)}}1&\leq\sum_{p\leq x}\sum_{\substack{z\leq q\leq 2z\\ q|D}}1+\sum_{p\leq x}\sum_{\substack{z\leq q\leq 2z\\ q|(4p-a_p^2)}}1\\ &\ll\frac{x}{\log x}\nu_z(D)+\frac{z}{\log z}\log N\\ &\quad+\sum_{z\leq q\leq 2z}\#\{p\leq x: p\nmid qN, 4p-a_p^2\equiv 0(\mathrm{mod}\ q)\},\qquad(23)\end{aligned}$$

and

$$\begin{aligned}\sum_{p\leq x}\Big(\sum_{\substack{z\leq q\leq 2z\\ q|D(4p-a_p^2)}}1\Big)^2&\leq\sum_{p\leq x}\Big(\sum_{\substack{z\leq q\leq 2z\\ q|D(4p-a_p^2)}}1+\sum_{\substack{z\leq l,q\leq 2z\\ l\neq q\\ lq|D(4p-a_p^2)}}1\Big)\\ &\ll\frac{x}{\log x}\big(\nu_z(D)+\nu_z(D)^2\big)+\frac{z^2}{(\log z)^2}\log N\\ &\quad+\sum_{z\leq q\leq 2z}\#\{p\leq x: p\nmid qN, 4p-a_p^2\equiv 0(\mathrm{mod}\ q)\}\\ &\quad+\sum_{\substack{z\leq l,q\leq 2z\\ l\neq q}}\#\{p\leq x: p\nmid lqN, 4p-a_p^2\equiv 0(\mathrm{mod}\ lq)\}.\qquad(24)\end{aligned}$$

We use the properties of the Galois representations ϕ_l and ϕ_{lq} recalled in Section 3 to write

$$\#\{p\leq x: p\nmid qN, 4p-a_p^2\equiv 0(\mathrm{mod}\ q)\}=\#\{p\leq x: p\nmid qN, \phi_q(\sigma_p)\subseteq D_q\}$$

and

$$\#\{p\leq x: p\nmid lqN, 4p-a_p^2\equiv 0(\mathrm{mod}\ lq)\}=\#\{p\leq x: p\nmid lqN, \phi_{lq}(\sigma_p)\subseteq D_{lq}\},$$

where

$$D_q = \{g \in \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) : 4\det g = (\operatorname{tr} g)^2\}$$

and

$$D_{lq} = \{g \in \mathrm{GL}_2(\mathbb{Z}/lq\mathbb{Z}) : 4\det g = (\operatorname{tr} g)^2\}.$$

We emphasize that x is large enough so that the representations ϕ_l and ϕ_{lq} are surjective. From Corollary 2.9 we know that

$$\#D_q = q^2(q-1) \quad \text{and} \quad \#D_{lq} = l^2q^2(l-1)(q-1),$$

and so, by applying the unconditional effective Chebotarev density theorem to $\mathbb{Q}(E[q])/\mathbb{Q}$ and $\mathbb{Q}(E[lq])/\mathbb{Q}$, respectively, we find that for some positive absolute constant A'' we have

$$\begin{aligned}\#\{p \le x : p \nmid qN, \phi_q(\sigma_p) \subseteq D_q\} &= \frac{q}{q^2-1}\operatorname{li} x + O\Big(\frac{x}{q\log x}\exp\Big(-\frac{A''\log x}{q^5N}\Big)\Big)\\ &\quad + O\Big(qx\exp\Big(-A''\sqrt{\frac{\log x}{q^4}}\Big)\Big),\\ \#\{p \le x : p \nmid lqN, \phi_{lq}(\sigma_p) \subseteq D_{lq}\} &= \frac{lq}{(l^2-1)(q^2-1)}\operatorname{li} x\\ &\quad + O\Big(\frac{x}{lq\log x}\exp\Big(-\frac{A''\log x}{l^5q^5N}\Big)\Big)\\ &\quad + O\Big(lqx\exp\Big(-A''\sqrt{\frac{\log x}{l^4q^4}}\Big)\Big).\end{aligned}$$

We plug these estimates into (23) and (24) and obtain

$$\sum_{p\le x}\sum_{\substack{z\le q\le 2z\\ q\mid D(4p-a_p^2)}} 1 \ll_N \frac{x}{\log x}\nu_z(D) + \frac{x}{(\log x)(\log z)} + \frac{z}{\log z} \tag{25}$$

and

$$\sum_{p\le x}\Big(\sum_{\substack{z\le q\le 2z\\ q\mid D(4p-a_p^2)}} 1\Big)^2 \ll_N \frac{x}{\log x}\nu_z(D)^2 + \frac{x}{(\log x)(\log z)} + \frac{z^2}{(\log z)^2}. \tag{26}$$

Combining (20), (21), (22), (25) and (26) and using the trivial bounds $\nu_z(D) \ll \frac{z}{\log z}$

and $1+\nu_z(D)\le 1+\nu(D)$ we deduce that

$$\begin{aligned} P_E\big(\mathbb{Q}(\sqrt{-D}),x\big) &\ll_N \frac{x\log z}{z\log x}\big(1+\nu_z(D)\big)\Big(1+\frac{\log z}{z}\nu_z(D)\Big)\\ &\ll_N \frac{x\log z}{z\log x}\big(1+\nu_z(D)\big),\\ &\ll_N \frac{x(\log\log x)^{\frac{13}{12}}}{(\log x)^{\frac{25}{24}}}\big(1+\nu_z(D)\big)\\ &\ll_N \frac{x(\log\log x)^{\frac{13}{12}}}{(\log x)^{\frac{25}{24}}}\big(1+\nu(D)\big). \end{aligned}$$

This completes the proof of Theorem 1.3.

5 Proof of Corollary 1.5

Now we want to give a lower bound for $\#\mathcal{D}_E(x)$. We recall that there are $o(\frac{x}{\log x})$ supersingular primes $p\le x$ of E (see [Se3, p. 174]), thus we have

$$\pi(x)=o\Big(\frac{x}{\log x}\Big)+\sum_{D\in\mathcal{D}_E(x)}P_E\big(\mathbb{Q}(\sqrt{-D}),x\big),$$

where $\pi(x)$ denotes the number of primes $\le x$. This implies that

$$\#\mathcal{D}_E(x)\ge\big(1-o(1)\big)\frac{x/\log x}{\max_{D\le 4x}P_E\big(\mathbb{Q}(\sqrt{-D}),x\big)}. \tag{27}$$

By inserting the different upper bounds provided by Theorem 1.2 into (27), we obtain parts (a)–(c) of Corollary 1.5.

Inequality (27) is, however, too weak to allow us to deduce something interesting by simply using Theorem 1.3. We proceed differently, as follows. Suppose that x is a sufficiently large number so that we have

$$\#\big(\mathcal{D}_E(\infty)\cap[1,4x]\big)<(\log x)^{\frac{1}{24}}. \tag{28}$$

As in (20), we define, for any real y,

$$Z(y):=c\frac{(\log y)^{1/24}}{(\log\log y)^{1/12}}.$$

By Theorem 1.3 we have that, for any $y>x$ and for some $c_0>0$,

$$\begin{aligned} \pi(y)&=o\Big(\frac{y}{\log y}\Big)+\sum_{D\in\mathcal{D}_E(y)}P_E\big(\mathbb{Q}(\sqrt{-D}),y\big)\\ &\le c_0\frac{y(\log\log y)^{13/12}}{(\log y)^{25/24}}\sum_{D\in\mathcal{D}_E(y)}\big(1+\nu_{Z(y)}(D)\big)+o\Big(\frac{y}{\log y}\Big). \end{aligned}$$

After division and after using (28), we get

$$\begin{aligned}\frac{1}{2c_0}\cdot\frac{(\log y)^{1/24}}{(\log\log y)^{13/12}} &\le \sum_{D\in\mathcal{D}_E(y)}\big(1+\nu_{Z(y)}(D)\big)\\ &= \sum_{\substack{D\in\mathcal{D}_E(y)\\ D\le 4x}}\big(1+\nu_{Z(y)}(D)\big)+\sum_{\substack{D\in\mathcal{D}_E(y)\\ 4x<D\le 4y}}\big(1+\nu_{Z(y)}(D)\big)\\ &\le \sum_{\substack{D\in\mathcal{D}_E(\infty)\\ D\le 4x}}\big(1+\nu_{Z(y)}(D)\big)+\sum_{\substack{D\in\mathcal{D}_E(y)\\ 4x<D\le 4y}}\big(1+\nu_{Z(y)}(D)\big)\\ &\le 2(\log x)^{\frac{1}{24}}\cdot\frac{\log x}{\log Z(y)}+\sum_{\substack{D\in\mathcal{D}_E(y)\\ 4x<D\le 4y}}\big(1+\nu_{Z(y)}(D)\big),\end{aligned}$$

under the assumption $y\le e^x$. Thus, if we have the strict inequality

$$\frac{1}{2c_0}\cdot\frac{(\log y)^{1/24}}{(\log\log y)^{13/12}} > 2\frac{(\log x)^{25/24}}{\log Z(y)}, \tag{29}$$

we can deduce that $\mathcal{D}_E(\infty)$ contains at least an element between $4x$ and $4y$. It is now easy to check that (29) is satisfied with the choice

$$y=\exp\big((\log x)^{26}\big).$$

The last point of Corollary 1.5 is an easy consequence of the fact that, if $(\nu_n)_n$ is a sequence of positive numbers satisfying $\nu_{n+1}\le\exp\big((\log\nu_n)^{26}\big)$ for sufficiently large n, then for $x\ge x_0$ we have $\#\{n\le x:\nu_n\le x\}\gg\log\log\log x$. The proof of Corollary 1.5 is now completed.

Remark 5.1 We recall that [Se3, Theorem 20] proves that for any integer h we have

$$\#\{p\le x: p\notin S_E, a_p=h\}=o\Big(\frac{x}{\log x}\Big).$$

Thus in the last statement of Corollary 1.5 we can modify the definition of $\mathcal{D}_E(x)$ by inserting the extra conditions "a_p does not belong to a fixed finite set of values" without changing the rate of growth of the sequence $(D_n)_{n\ge1}$. We also recall that the case $a_p=1$ corresponds to what is known as *anomalous* primes.

6 Concluding Remarks

There is a cognate set of Lang–Trotter conjectures concerning the frequency of values of the a_p's. A special case of these conjectures concerns the distribution of supersingular primes, which was studied by E. Fouvry and Ram Murty in [FM1, FM2]. It was

clear to the authors that the methods used to study these questions could not be employed in the study of the frequency of the "Frobenius fields" $\mathbb{Q}(\pi_p)$, even though the conjectures seem to be of the same species. Perhaps this was also noticed by Serre (see especially the note on [Se3, p. 191]). In fact, it was this remark of Serre that prompted the second and third authors of the present paper to consider the square sieve as a tool to attack this question (more than 10 years ago). Unfortunately, nothing was published. Thanks to the first author, our memories were revived, and the technique has been streamlined with effect, not only to the questions considered here, but to others as well (see [acC1]). Certainly, it can be used to study the Frobenius fields for non-CM elliptic curves defined over a number field, and not only over $\mathbb{Q}$. The square sieve can also be applied to other questions of arithmetic-geometric interest, as described in the forthcoming book [CM].

We emphasize that the square sieve is a simpler technique than the more conventional sieve methods and that our results are uniform in D, whereas in [Se4, Remark 631, p. 715] no such uniformity was claimed. We are grateful to J-P. Serre for his extensive comments comparing his methods alluded to in [Se3] and [Se4] with ours, developed in this paper. As these remarks may be of value in future research, we record here their quintessence.

First, if in our application of the square sieve we use PGL_2 instead of GL_2, as in [Se3], we can improve the 17/18 exponent in Theorem 1.2 to 13/14. Similar improvements can be obtained for parts (b) and (c) of Theorem 1.2 (11/12 and 9/10, respectively). A minor improvement can also be achieved in Theorem 1.3. Under GRH, Serre's application of Selberg's sieve (referred to in [Se3, p. 191]) will lead to the same exponents.

Secondly, with regard to the brief remark in [Se4, p. 715], the following elaboration was given by Serre: Theorem 10 of [Se3] is applicable in a wider context, which will be illustrated through three examples.

Let L be a number field and let E, E' be two non-CM elliptic curves defined over L which are not isogenous over $\overline{\mathbb{Q}}$. Let $C(x)$ be the number of prime ideals v of L with $N_{L/\mathbb{Q}}(v) \leq x$ and for which E and E' have the same Frobenius trace. Then, under GRH, $C(x) = O_{E,E',L}(x^{\frac{11}{12}})$ (here, the O-constant depends in an unspecified way on E, E' and L). To see this, consider the Lie group $\mathrm{PGL}_2 \times \mathrm{PGL}_2$, which is of dimension 6 in the setting of Theorem 10 of [Se3]. There is a natural class function t on PGL_2 given by $t(g) := \mathrm{tr}(g)^2/\det g$. The equation $t(g) = t(g')$ defines a divisor $\mathcal{D}$ in $\mathrm{PGL}_2 \times \mathrm{PGL}_2$, which is invariant under conjugation. Now let us look at the l-adic representations attached to E and E'. They give a homomorphism

$$\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to \mathrm{PGL}_2(\mathbb{Q}_l) \times \mathrm{PGL}_2(\mathbb{Q}_l),$$

where $\mathbb{Q}_l$ denotes the field of l-adic rational numbers. For a prime v coprime to l, where E and E' have the same Frobenius trace, the Frobenius element of v in $\mathrm{PGL}_2(\mathbb{Q}_l) \times \mathrm{PGL}_2(\mathbb{Q}_l)$ is a $\mathbb{Q}_l$-point of $\mathcal{D}$. Applying Theorem 10 of [Se3] gives the result stated above.

Keeping the above setting, another application concerns the problem of counting the number of primes v which give rise to the same Frobenius fields. That is, we want to count the number of primes v with $N_{L/\mathbb{Q}}(v) \leq x$ such that the field generated

by the eigenvalue of the Frobenius Frob_v at v of E is the same as the field generated by the eigenvalue of Frob_v of E'. If we confine our attention to first degree primes v and and if the field generated is neither $\mathbb{Q}(i)$, nor $\mathbb{Q}(e^{2\pi i/3})$, then the equality of the Frobenius fields implies that $\mathrm{tr}\big(\mathrm{Frob}_v(E)\big) = \pm\,\mathrm{tr}\big(\mathrm{Frob}_v(E')\big)$. Thus, the class function defined in the previous paragraph takes the same values and, as before, we can take the same divisor $\mathcal{D}$ and apply Theorem 10 of [Se3]. The case $\mathbb{Q}(i)$ leads to $t(g)^2 = t(g')^2$, and the case $\mathbb{Q}(e^{2\pi i/3})$ leads to $t(g)^3 - 3t(g) = t(g')^3 - 3t(g')$ (note that the precise form of the equation does not matter). In any case, we are led to an estimate of $O_{E,E',L}(x^{\frac{11}{12}})$. Again, the O-constant depends in an unspecified way on E, E' and L.

Finally, we can apply Theorem 10 of [Se3] to the Lang–Trotter conjecture discussed in this paper and improve the exponent $9/10$ mentioned in Section 1 to $7/8$. To be precise, let E be an elliptic curve defined over a number field L and let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field. Let $G = \mathrm{PGL}_2 \times \mathcal{N}$, where $\mathcal{N}$ is the normalizer of the maximal torus of PGL_2, be the Lie group required by Theorem 10 of [Se3]. We define a representation

$$\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to \mathrm{PGL}_2(\mathbb{Q}_l) \times \mathcal{N}(\mathbb{Q}_l)$$

as follows. The first component is given by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ on the l-adic Tate module composed with the natural map

$$\mathrm{Gal}(\overline{\mathbb{Q}}/L) \to \mathrm{GL}_2(\mathbb{Q}_l) \to \mathrm{PGL}_2(\mathbb{Q}_l).$$

To describe the second component, let h, w be the class number and the number of roots of unity of K. For every non-zero ideal $\mathfrak{a}$ of K define $f(\mathfrak{a})$ as the w-th power of a generator of the principal ideal $\mathfrak{a}^h$. This is a well-defined Hecke character of K. It is associated with an l-adic representation

$$\mathrm{Gal}(\overline{K}/K) \to K_l^* := \mathbb{Q}_l^* \times \mathbb{Q}_l^*,$$

whose two components we denote by f_1 and f_2. The product $f_1 f_2$ is the hw-th power of the cyclotomic character. As f_1 is a 1-dimensional representation of $\mathrm{Gal}(\overline{K}/K)$, the induced representation of f_1 is a 2-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. That is, we have a map

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_l).$$

By restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$, we get a representation

$$r\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Q}_l),$$

and hence

$$r\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/L) \to \mathrm{PGL}_2(\mathbb{Q}_l).$$

The image of r is contained in the normalizer $\mathcal{N}$ of the diagonal torus PGL_2. Confining our attention to primes v of degree one (as primes of degree 2 or higher give a contribution of $O(x^{\frac{1}{2}})$ to our estimate), we seek to construct a divisor $\mathcal{D}$ as in the

previous two examples. This means that we must find an algebraic relation between $t(g)$ and $t(g')$, where g and g' are the Frobenius elements defined by v. We consider first the case when K is neither $\mathbb{Q}(i)$, nor $\mathbb{Q}(e^{2\pi i/3})$, so that $w = 2$. In this case we are interested in those v whose Frobenius automorphism has eigenvalues a and b in K with $ab = N_{K/\mathbb{Q}}(v)$ and whose t-invariant is $t(g) = (a+b)^2/ab$. On the other hand, the eigenvalues $r(\mathrm{Frob}_v)$ are a^{2h}, b^{2h}, so that $t(g') = (a^{2h} + b^{2h})^2/(ab)^{2h}$. For each $m > 0$ there is a well-defined polynomial $P(m, z)$ such that

$$P\left(m, \frac{(a+b)^2}{ab}\right) = \frac{(a^m + b^m)^2}{(ab)^m}$$

for all a, b, as it is easily checked. We therefore have

$$t(g') = P\big(2h, t(g)\big),$$

which is the required algebraic relation. The cases $w = 4$ and $w = 6$ are analogous. Now, by applying Theorem 10 of [Se3], we get an estimate of $O_{E,K}(x^{\frac{7}{8}})$ for our problem. Here, as in the previous examples, the error term depends on E and K in an unspecified way.

Acknowledgements We are grateful to Professors Kumar Murty and Jean-Pierre Serre for their detailed useful comments on a previous version of the paper.

References

[acC1] A. C. Cojocaru, *Cyclicity of elliptic curves modulo p*. PhD thesis, Queen's University, Kingston, Canada, 2002.

[acC2] ———, *On the surjectivity of the Galois representations associated to non-*CM *elliptic curves*. With an Appendix by E. Kani, Canad. Math. Bull.**48**(2005), 16–31.

[CM] A. C. Cojocaru and M. Ram Murty, *Introduction to Sieve Methods and Their Applications*. London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 2005.

[El] N. D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$. Invent. Math. (3) **89**(1987), 561–567.

[FM1] E. Fouvry and M. Ram Murty, *Supersingular primes common to two elliptic curves*. London Math. Soc. Lecture Notes Series 215, Number Theory, Paris 1992–93 (ed., Sinnou David), 1995, 91–102.

[FM2] ———, *On the distribution of supersingular primes*. Canad. J. Math. (1) **48**(1996), 81–104.

[H-B] D. R. Heath-Brown, *The square sieve and consecutive square-free numbers*. Math. Ann. **266**(1984), 251–259.

[LO] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem*. In: Algebraic Number Fields, (ed., A. Fröhlich), New York, Academic Press, 1977, 409–464.

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

[RM1] M. Ram Murty, *An analogue of Artin's conjecture for abelian extensions*. J. Number Theory (3) **18**(1984), 241–248.

[RM3] M. Ram Murty, *An introduction to Artin L-functions*. J. Ramanujan Math. Soc. (3) **16**(2001), 261–307.

[MM] M. Ram Murty and V. Kumar Murty, *The Chebotarev density theorem and pair correlation of zeros of Artin L-functions*, to be submitted.

[MMS] M. Ram Murty, V. Kumar Murty and N. Saradha, *Modular forms and the Chebotarev density theorem*. Amer. J. Math. **110**(1988), 253–281.

[Se1] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**(1972), 259–331.

[Se2] ———, *A course in arithmetic*. Graduate Texts in Math. **7**, Springer Verlag, 1996.
[Se3] ———, *Quelques applications du théorème de densité de Chebotarev*. Inst. Hautes Études Sci. Publ. Math. **54**(1981), 123–201.
[Se4] ———, *Collected papers*. Volume III, Springer Verlag, 1985.
[Si1] J. H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Math. **106**, Springer Verlag, New York, 1986.
[Si2] ———, *Advanced topics in the arithmetic of elliptic curves*. Graduate Texts in Math. **151**, Springer Verlag, New York, 1994.
[St] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*. Invent. Math. **23**(1974), 135–152.

Department of Mathematics
Princeton University
Fine Hall, Washington Road
Princeton, New Jersey
USA 08544
email: cojocaru@math.princeton.edu

Department of Mathematics and Statistics
Queen's University
Jeffery Hall
Kingston, Ontario
K7L 3N6
email: murty@mast.queensu.ca

Laboratoire de mathématiques
Université Paris-Sud Bât. 425
9140 Orsay Cedex
France, CNRS UMR 8628
email Etienne.Fouvry@math.u-psud.fr