Canad. J. Math. 2021, pp. 1–33
http://dx.doi.org/10.4153/S0008414X21000237
© Canadian Mathematical Society 2021

Cyclicity of elliptic curves modulo primes in arithmetic progressions

Yıldırım Akbal and Ahmet M. Güloğlu

Abstract. We consider the reduction of an elliptic curve defined over the rational numbers modulo primes in a given arithmetic progression and investigate how often the subgroup of rational points of this reduced curve is cyclic.

1 Introduction

1.1 History of the cyclicity conjecture

Let $E/\mathbb{Q}$ be an elliptic curve given by a global minimal (see [33, Corollary VIII.8.3]) Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, \dots, a_6 \in \mathbb{Z}$. Primes that do not divide the discriminant Δ_E of this equation, or equivalently, its conductor N_E, are called the primes of good reduction. For such primes p, the reduction $\widetilde{E}_p$ of E modulo p is a nonsingular elliptic curve. In particular, let $\widetilde{E}(\mathbb{F}_p)$ denote the subgroup of $\mathbb{F}_p$-rational points of the reduced curve $\widetilde{E}_p$.

In 1976, Lang and Trotter formulated (cf. [21]) the following elliptic curve analogue of Artin's primitive root conjecture:

Conjecture 1 (Lang–Trotter Conjecture) *Let $E/\mathbb{Q}$ be an elliptic curve of rank at least 1. Let $P \in E(\mathbb{Q})$ be a fixed point on E of infinite order. Then, the density of primes p such that $\widetilde{E}(\mathbb{F}_p) = \langle P \bmod p \rangle$ exists.*

As the first step toward this conjecture, the same year, following Hooley's conditional proof of Artin's conjecture (cf. [16]), Jean Pierre Serre proved (cf. [32]) assuming Generalized Riemann Hypothesis (GRH) that

$$\left|\{p \leqslant x : p \nmid N_E, \widetilde{E}(\mathbb{F}_p) \text{ is cyclic}\}\right| = \delta_E \operatorname{Li}(x) + o(x/\log x), \tag{1}$$

Received by the editors May 28, 2020; revised February 18, 2021; accepted April 26, 2021.
Published online on Cambridge Core May 3, 2021.
AMS subject classification: **11G05**, 11N13, 11N36, 11N45, 11R45.
Keywords: Cyclicity conjecture, reduction of elliptic curves modulo primes, primes in arithmetic progressions, Chebotarev density theorem.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

with the density δ_E given by

$$\delta_E = \sum_{n\geqslant 1} \frac{\mu(n)}{[K_n : \mathbb{Q}]}. \tag{2}$$

Here, $\mathrm{Li}(x) = \int_2^x dt/\log t$, and $K_n = \mathbb{Q}(E[n])$ is the *n-division field* obtained by adjoining to $\mathbb{Q}$ the affine coordinates of the group $E[n](\overline{\mathbb{Q}})$ of n-torsion points of E, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$.

Murty and Cojocaru have shown in [7, pp. 621–2] that $\delta_E > 0$ for both Complex Multiplication (CM) and non-CM curves (curves with and without complex multiplication), *provided* $K_2 \neq \mathbb{Q}$. This result also follows as a byproduct of Theorem 4 by taking $f = 1$ for non-CM curves. Furthermore, the proof of Theorem 4 provides an important modification needed in their argument for the non-CM case (see Remark 2). All of these results assume that GRH holds.

In general, an explicit Euler product for δ_E is known only for the so-called Serre curves (see, for example, [2, Section 2.4.1], both for the definition and the explicit formula for δ_E).

In 1975, Borosh et al. (cf. [3]) conjectured that for many elliptic curves E defined over $\mathbb{Q}$, there are infinitely many primes p for which $\widetilde{E}(\mathbb{F}_p)$ is cyclic. Combining the claim of [3] with the results of [7], we state the following.

Conjecture 2 *$\widetilde{E}(\mathbb{F}_p)$ is cyclic for infinitely many primes p if and only if E contains a nonrational two-torsion point.*

In 1990, Gupta and Murty showed in [12] that for any elliptic curve E, $\widetilde{E}(\mathbb{F}_p)$ is cyclic for at least $c_E x/(\log x)^2$ primes for some positive constant c_E, provided $K_2 \neq \mathbb{Q}$. When $K_2 = \mathbb{Q}$, then the torsion group $E(\mathbb{Q})_{\mathrm{tors}}$ of rational points on E contains a subgroup of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since for all primes p, except for a finite number of them, the torsion group embeds into $\widetilde{E}(\mathbb{F}_p)$, we deduce that there can be at most a finite number of primes p for which $\widetilde{E}(\mathbb{F}_p)$ is cyclic, thereby settling Conjecture 2.

The asymptotic formula (1), however, has been proven *unconditionally* only for CM curves. In 1979, Ram Murty showed (cf. [28]) that (1) holds without GRH for all CM elliptic curves. In 2010, Akbary and Murty [1, Theorem 1.1] improved the error term of [28] to $O(x/(\log x)^A)$ for any sufficiently large positive constant A. They, however, assume that the curve has multiplication by the full ring of integers $\mathfrak{O}_K$ of an imaginary quadratic field K.

For non-CM curves, Cojocaru showed (cf. [4]) in 2002 that if E is a non-CM elliptic curve, then (1) holds with an error $\ll_{N_E} x \log\log x/(\log^2 x)$ under the assumption that the Dedekind zeta functions of the division fields of E have no zeros to the right of $x = \frac{3}{4}$.

Upon combining the results of [1, 12, 28], it follows that $\delta_E > 0$ for curves with complex multiplication by $\mathfrak{O}_K$, provided that $K_2 \neq \mathbb{Q}$, which gives a second proof of Conjecture 2 for these curves via the asymptotic formula in [1].

In 2004, assuming GRH, Cojocaru and Murty (cf. [7, Theorems 1.1, 1.2]) improved the error terms in (1) to $O_{N_E}(x^{5/6}(\log x)^{2/3})$ for non-CM curves, and to $O(x^{3/4}(\log N_E x)^{1/2})$ for CM curves with explicit dependence on the conductor N_E.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

This way, they were able to deduce estimates for the smallest prime p_E for which $\widetilde{E}(\mathbb{F}_p)$ is cyclic.

1.2 The goal of this paper

For the rest of the paper, $f \geqslant 1$ is an integer, and a represents a residue class modulo f and $\gcd(a, f) = 1$.

As a natural variation, we consider Conjecture 2 for primes $p \equiv a \bmod f$. More precisely, for a given elliptic curve E, we try to determine all moduli f, and the corresponding residue classes a for each modulus f such that $\widetilde{E}(\mathbb{F}_p)$ is cyclic for infinitely many primes $p \equiv a \bmod f$. This is in analogy with Artin's Primitive Root Conjecture considered for primes in arithmetic progressions, which was studied in [23, 24, 26, 27].

We give unconditional lower bound estimates similar to the one given by Gupta and Murty in [12]. Unfortunately, we obtain only partial results which impose certain restrictions on f and a related to the use of the sieve method (see Section 1.3).

We also find asymptotic formulas obtained under GRH with error terms similar to the ones given by Cojocaru and Murty in [7] mentioned above, and with explicit dependence on the modulus f and certain constants related to the curve E. For Serre curves, an explicit Euler product for the corresponding density, which we shall denote by $\delta_E(f, a)$, is given in [2, Corollary 2.5.9]. To find an explicit product or to show at least that the density is positive in *all* the cases that we predict (see Question 1) seems out of reach, since one needs to know the nontrivial intersections of the division fields K_n for an arbitrary elliptic curve, but these are not completely understood. This is exactly the same reason why there is no explicit product in general for δ_E in (1). What is known about them is given in the Appendix. Furthermore, in our problem, one needs precise information about the intersections $K_n \cap \mathbb{Q}(\zeta_f)$ for any $n \geqslant 1$. What we know about these are given in Lemmas 7 and 8, which are obtained by the results in Appendix. The corresponding density in the case of Artin's Conjecture with primes in progressions is given explicitly in [27, Theorem 1.2] since in this case the corresponding intersections are known and given in [27, Lemma 2.4].

Before we state our prediction on what the analogue of Conjecture 2 should be in our case, we first introduce some notation. We denote by ζ_n any fixed primitive nth root of unity, and by $\mathbb{Q}(\zeta_n)$ the corresponding cyclotomic extension. The letter σ when used with a subscript is reserved for automorphisms of cyclotomic fields and the one which takes ζ_n to ζ_n^a, for each a coprime to the modulus in question, will be denoted by σ_a. Also, the letters p and q always denote primes.

Question 1 Let E be an elliptic curve defined over $\mathbb{Q}$ and let f and a be relatively prime positive integers. Is it true that there are infinitely many primes $p \equiv a \bmod f$ for which $\widetilde{E}(\mathbb{F}_p)$ is cyclic unless $K_d \subseteq \mathbb{Q}(\zeta_f)$ for some $d \geqslant 2$ and $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_f)/K_d)$, in which case there are at most a finite number of such primes?

One direction follows easily. To see this, we first need to quote two key facts from [7, Lemma 2.1, Proposition 3.5.3]:

1. For *odd* $p \nmid N_E$, $\widetilde{E}(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in K_q for any prime $q \neq p$.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

2. $\mathbb{Q}(\zeta_n) \subseteq K_n$ for each integer $n \geqslant 2$.

Now, if $K_d \subseteq \mathbb{Q}(\zeta_f)$ for some $d \geqslant 2$, and σ_a fixes K_d, then any $p \nmid N_E$ with $p \equiv a \bmod f$ will split completely in K_d, thereby in any K_q with $q \mid d$. Thus, $\widetilde{E}(\mathbb{F}_p)$ cannot be cyclic for odd $p \neq q$ with $p \nmid N_E$. We record this result below. But, first note that $K_d \subseteq \mathbb{Q}(\zeta_f)$ implies K_d is abelian over $\mathbb{Q}$, and González-Jiménez and Lozano-Robledo show (cf. [9]) that K_d is abelian only if $d \in \{2, 3, 4, 5, 6, 8\}$ for non-CM curves, and if $d \in \{2, 3, 4\}$ for CM curves. Thus, we deduce the following result.

Proposition 1 *Assume that $(a, f) = 1$, $K_d \subseteq \mathbb{Q}(\zeta_f)$ for some $d \geqslant 2$, and σ_a fixes K_d. Then, $\widetilde{E}(\mathbb{F}_p)$ is cyclic for at most finitely many primes $p \equiv a \bmod f$.*

We also note that for $f = 1$, our claim reduces to Conjecture 2 since in this case, $\mathbb{Q}(\zeta_d) \subseteq K_d \subseteq \mathbb{Q}(\zeta_f) = \mathbb{Q}$ is possible only for $d = 1, 2$.

As for the opposite direction of our claim, we have partial results which imposes certain restrictions on f and a. For the remaining cases, other than the numerical calculations we have done, we cannot provide a heuristic argument as evidence to support our claim. In what follows, we list the partial results we were able to prove that strongly support our prediction.

1.3 Unconditional results

Let K_n^{ab} be the maximal abelian extension of $\mathbb{Q}$ in K_n. By the Kronecker-Weber Theorem, $K_n^{ab} \subseteq \mathbb{Q}(\zeta_{\mathfrak{f}_n})$ for some positive integer $\mathfrak{f}_n$, minimal with respect to this inclusion, that is divisible exactly by the primes that ramify in K_n^{ab}. This number $\mathfrak{f}_n$ is called the conductor of K_n^{ab}.

Theorem 1 *Let E be an elliptic curve over $\mathbb{Q}$ satisfying $[K_2 : \mathbb{Q}] = 3$ and let a and f be any positive integers such that $(a, f) = 1$ and $(a - 1, f)$ has no odd prime divisors. Let $A \geqslant 0$ be given. Then, for x sufficiently large and assuming $f \ll (\log x)^A$, the group $\widetilde{E}(\mathbb{F}_p)$ is cyclic for $\gg x/(\log x)^{2+A}$ primes $p \equiv a \bmod f$, unless $K_2 \subseteq \mathbb{Q}(\zeta_f)$ and σ_a fixes K_2.*

To see why this Theorem is consistent with and provides an affirmative answer to Question 1, note that the Artin map $\langle p, \mathbb{Q}(\zeta_f)/\mathbb{Q}\rangle = \sigma_a$ for any prime $p \nmid N_E$ with $p \equiv a \bmod f$. Thus, if $K_q \subseteq \mathbb{Q}(\zeta_f)$ for some *odd* prime q, and σ_a fixes K_q, then it also fixes $\mathbb{Q}(\zeta_q)$, and this means $q \mid (a - 1, f)$, contradicting our assumption in Theorem 1. Therefore, it is enough to check whether $K_q \subseteq \mathbb{Q}(\zeta_f)$ and σ_a fixes K_q only for $q = 2$.

Theorem 1 works for any elliptic curve, CM or non-CM and is also practical in the sense that one can determine the moduli f, and whether $K_2 \subseteq \mathbb{Q}(\zeta_f)$ or not, and the residue classes a for which $\widetilde{E}(\mathbb{F}_p)$ is cyclic for infinitely many primes $p \equiv a \bmod f$. To see this, note that if E is given by

$$y^2 = x^3 + a_1x^2 + a_2x + a_3,$$

with an irreducible cubic, then K_2 is a cubic extension exactly when the discriminant Δ_E is a square in $\mathbb{Q}$. In this case, Häberle describes in [13, Corollary 12] how to determine the conductor $\mathfrak{f}_2$ of a cubic extension of $\mathbb{Q}$. In particular, $\mathfrak{f}_2$ is of the form

$$q_1q_2\cdots q_r \qquad (r \geqslant 1),$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

where each $q_i \equiv 1 \bmod 3$ is a prime, with *at most* one exception, which then must be 9. Therefore, any number f not divisible by $\mathfrak{f}_2$ will be an admissible modulus, and we may then choose the residue class a coprime to f such that $(a-1, f)$ has no odd prime divisors. Furthermore, in case $K_2 \subseteq \mathbb{Q}(\zeta_f)$, for any a whose order modulo f does not divide $\varphi(f)/3 = |\operatorname{Gal}(\mathbb{Q}(\zeta_f)/K_2)|$, σ_a cannot fix K_2.

In general, there are $2\varphi(f)/3$ possible choices for a. In particular, when f is a prime power divisible by $\mathfrak{f}_2$, one can take any residue class a which is not a cubic residue modulo f.

The proof of Theorem 1 uses linear sieve of Iwaniec (cf. [18]). The idea is to count the primes $p \leqslant x$ with $p \equiv a \bmod f$ such that $p-1$ is free of odd primes not exceeding x^α for some $\alpha > \frac{1}{4}$. Having the exponent $\alpha > \frac{1}{4}$ is essential for the rest of the proof to work, and one way to achieve this is to combine the linear sieve of Iwaniec [18, Theorem 1] with a follow up paper by Fouvry and Iwaniec [8] with a necessary modification provided later by Heath–Brown (see [15, Lemma 2]). Using sieve theory also necessitates the restriction on residue classes in Theorem 1. Indeed, if some odd prime $q \leqslant x^\alpha$ were to divide $(a-1, f)$, then p would split completely in $\mathbb{Q}(\zeta_q)$; that is, $q \mid p-1$, and one could not guarantee then that p does not split in K_q, which is the only way the sieve can be used to prove Theorem 1.

Since it is desirable to remove the restriction on residue classes a, we also investigated ways to deal with the case when $(a-1, f)$ is divisible by odd primes. To understand the obstacles in this situation, we consider an example. Say, $f > 5$ is a prime, and we want to count primes $p \equiv 1 \bmod f$ for which $\widetilde{E}(\mathbb{F}_p)$ is cyclic. Note that these primes split completely in $\mathbb{Q}(\zeta_f)$. Fortunately, there is hope for these primes not to split completely in K_f since it follows from [9] that K_f is nonabelian when $f > 5$. One has to make sure p does not split completely in K_q for primes $q \neq p$. To get an unconditional result using sieve methods, one has to count primes $p \leqslant x$, $p \nmid N_E$, $p-1$ not divisible by primes $q \leqslant x^\alpha$ with some $\alpha > \frac{1}{4}$ except for 2 and f, and the Artin map $\langle p, K_{2f}/\mathbb{Q}\rangle \subseteq C$, where C is a conjugacy class that consists of automorphisms in $\operatorname{Gal}(K_{2f}/\mathbb{Q}(\zeta_f))\backslash\{1_{K_{2f}}\}$. This may be done using a result of Murty and Petersen (cf. [29, Theorem 0.2]), but only, in the best scenario, with an exponent $\alpha = 1/2(\varphi(f)-2) - \varepsilon < \frac{1}{4}$ (note $\varphi(f) = f-1 > 4$). Thus, unless [29, Theorem 0.2] can be improved, getting an unconditional result seems to be out of reach with current methods.

One last note relevant also to the next result is that when applying the sieve one has to work with two congruences; namely, that $p \equiv a \bmod f$ and $p \equiv b \bmod \mathfrak{f}_2$. The latter is needed to make sure that p does not split completely in K_2 (see Lemma 2 and Remark 4). When K_2 is cubic, these two congruences are shown to be compatible in Lemma 3, and this leads to Theorem 1 above. However, in what follows, we shall see that this is not always the case when K_2 is nonabelian, or a quadratic field. Thus, the next result is slightly weaker than but is similar to the cubic case.

The character χ_D that appears in the statement of Theorem 2 is the real primitive character of conductor $|D|$ associated with the quadratic field $\mathbb{Q}(\sqrt{D})$ given by the Kronecker symbol $\chi_D(\cdot) = \left(\frac{D}{\cdot}\right)$, and $\mathfrak{d}_2$ stands for the discriminant of the quadratic extension K_2^{ab} of conductor $\mathfrak{f}_2 = |\mathfrak{d}_2|$.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Theorem 2 *Let E be an elliptic curve over $\mathbb{Q}$ satisfying $[K_2^{ab} : \mathbb{Q}] = 2$ and let a and f be any positive integers such that $(a, f) = 1$ and $(a-1, f)$ has no odd prime divisors. Let $A \geqslant 0$ be given. Then, for x sufficiently large and assuming $f \ll (\log x)^A$, the group $\widetilde{E}(\mathbb{F}_p)$ is cyclic for $\gg x/(\log x)^{2+A}$ primes $p \equiv a \bmod f$ if $\mathfrak{f}_2 \nmid f$, unless $\mathfrak{f}_2 = 3(f, \mathfrak{f}_2)$ and $\chi_{-\mathfrak{d}_2/3}(a) = -1$. The same lower bound holds if $\mathfrak{f}_2 \mid f$ and σ_a does not fix K_2^{ab}.*

In case one uses a Weierstrass model given by

$$y^2 = g(x) = x^3 + Ax^2 + Bx + C,$$

K_2^{ab} is generated by the square root of the square-free part of Δ_E. So, in practice, conditions given above can easily be checked to determine which moduli f and the corresponding residue classes a are admissible.

Note that Theorem 2 comes close to, but falls short of providing the converse of Proposition 1 due to the exceptional case when $\mathfrak{f}_2 \nmid f$. To see what the problem is, we consider an example:

Assume that $K_2^{ab} = \mathbb{Q}(\sqrt{21})$, $f = 7$, and $a = 5$ so that

$$\mathfrak{f}_2 = \mathfrak{d}_2 = 21, \quad \left(\frac{-\mathfrak{d}_2/3}{5}\right) = \left(\frac{-7}{5}\right) = -1, \quad 21 = 3\gcd(7, 21).$$

Since $\mathfrak{f}_2 \nmid f$, $K_2^{ab} \notin \mathbb{Q}(\zeta_f) = \mathbb{Q}(\zeta_7)$. We require primes $p \equiv 5 \bmod 7$ not split completely in K_2^{ab} so that they do not split completely in K_2. The latter is achieved by imposing a condition that $p \equiv b \bmod 21$ for some b. We want to see why the sieve cannot be applied. Note that the second congruence should guarantee that $\sigma_b \in \mathrm{Gal}(\mathbb{Q}(\zeta_{21})/\mathbb{Q})$, but σ_b does not fix K_2^{ab}; that is, $\sigma_b(\sqrt{21}) = -\sqrt{21}$. Here, b should be chosen in such a way that $(b-1, 21) = 1$. At the same time, we need $7 \mid b - 5$ so that the congruences $p \equiv 5 \bmod 7$ and $p \equiv b \bmod 21$ are compatible. This implies then that σ_b restricted to $\mathbb{Q}(\zeta_7)$ sends $\sqrt{-7}$ to $-\sqrt{-7}$ because $\sigma_a = \sigma_5$ does. This can be seen as follows:

The Artin map $\langle 5, \mathbb{Q}(\zeta_7)/\mathbb{Q}\rangle = \sigma_5$ when restricted to $K = \mathbb{Q}(\sqrt{-7})$ equals $\langle 5, K/\mathbb{Q}\rangle$, and thus, is not identity on K since $5\mathfrak{O}_K$ is a prime ideal in K. This follows from Kummer's Theorem (cf. [19, Section 1, Theorem 7.4]) as $x^2 + 7$ is irreducible modulo 5; in other words, -7 is a quadratic non-residue modulo 5 and this is captured by $\chi_{-7}(5) = -1$.

Hence, in order to get $\sigma_b(\sqrt{21}) = -\sqrt{21}$, we need $\sigma_b(\sqrt{-3}) = \sqrt{-3}$. This implies that $b \equiv 1 \bmod 3$, hence $p \equiv 1 \bmod 3$, and p splits completely in $\mathbb{Q}(\zeta_3)$. As a result, the sieve cannot be used since we could not choose b so that $(b-1, 21) = 1$. Therefore, we have to exclude cases where $\mathfrak{f}_2 = 3(f, \mathfrak{f}_2)$ and $\chi_{-\mathfrak{d}_2/3}(a) = -1$ when $\mathfrak{f}_2 \nmid f$ (see Lemma 4).

1.4 Conditional results

Next, we move onto the asymptotic results similar to Serre's Theorem in (1). We first introduce a few facts and give some definitions.

For each integer $m \geqslant 1$, there exists a representation

$$\rho_m = \rho_{E/\mathbb{Q},m} : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

determined by the action of the absolute Galois group $G_{\mathbb{Q}}$ on the torsion group $E[m]$. The fixed field of its kernel is the m-division field K_m, so

$$\mathrm{Gal}(K_m/\mathbb{Q}) \simeq \rho_m(G_{\mathbb{Q}}). \tag{3}$$

In 1972, Serre proved (cf. [31]) that

$$S_E = \{p \text{ prime} : \rho_p(G_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})\}$$

is finite if and only if E is non-CM. When E is non-CM, the *Serre constant* of $E/\mathbb{Q}$ is defined as the number

$$A(E) = 30 \prod_{\substack{p>5 \\ p\in S_E}} p. \tag{4}$$

Furthermore, we define the constant

$$M_E = \prod_{p|A(E)N_E} p.$$

We shall denote our prime counting function by

$$\pi_E(x; f, a) = \#\{p \leqslant x : p \nmid 2N_E, p \equiv a \bmod f, \text{ and } \widetilde{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

Arithmetic functions ω, τ, σ, and H that appear below are

$$\omega(n) = \sum_{p|n} 1, \quad \tau(n) = \sum_{d>0, d|n} 1, \quad \sigma(n) = \sum_{d>0, d|n} d, \quad H(n) = \sum_{d|n} \sum_{\substack{1\leqslant k\leqslant d \\ d|k^2}} 1, \tag{5}$$

and, as usual, φ is Euler's totient function.

Theorem 3 *Let $E/\mathbb{Q}$ be a non-CM curve. Assuming GRH holds for all Dedekind zeta functions of the fields $K_d\mathbb{Q}(\zeta_f)$ for all square-free $d \geqslant 1$, we have*

$$\pi_E(x; f, a) = \delta_E(f, a)\,\mathrm{Li}(x) + E(x),$$

where

$$\delta_E(f, a) := \sum_{d=1}^{\infty} \frac{\mu(d)\gamma_{a,f}(K_d)}{[K_d\mathbb{Q}(\zeta_f) : \mathbb{Q}]}, \tag{6}$$

where μ denotes the Möbius function, and $\gamma_{a,f}(K_d) = 1$ if σ_a fixes $K_d \cap \mathbb{Q}(\zeta_f)$, and is 0 otherwise, and the error term $E(x)$ satisfies

$$\begin{aligned} E(x) \ll{}& x^{1/2} f \log(fxN_E) + x^{5/6} \left(\frac{H(f)\log^2(fxN_E)}{f}\right)^{1/3} \\ &+ x^{5/8} \left(\frac{\tau(f_2)M_E^3 \log^3(fxN_E)}{\varphi(f)\log x}\right)^{1/4} + \frac{\tau(f_2)M_E^3}{x^{1/2}\varphi(f)\log x}. \end{aligned} \tag{7}$$

Here, f_2 denotes the largest divisor of f that is coprime to M_E.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Remark 1 It follows from (19) that $H(n)$ satisfies

$$2^k\sigma\left(\prod_{i\leqslant k} p_i^{[\alpha_i/2]-1}\right) \leqslant H\left(\prod_{i\leqslant k} p_i^{\alpha_i}\right) \leqslant 2^k\sigma\left(\prod_{i\leqslant k} p_i^{\lfloor\alpha_i/2\rfloor}\right). \tag{8}$$

In particular, for $f=\prod_{i\leqslant k} p_i^{\alpha_i}$, it follows from [17] that

$$H(f) < 2.59\cdot 2^k\sqrt{f}\log\log\sqrt{f},$$

whenever $\prod_i p^{\lfloor\alpha_i/2\rfloor}\geqslant 7$, and $H(f)<2^{k+1}\sqrt{f}$ otherwise. The last inequality, of course, gives only a crude estimate since the behavior of H is not very regular. For example, if f is a large prime, then $H(f)=2$ while $H(f^2)=2+f>f$.

In this paper, we did not try to see if a weaker quasi-GRH would work as in [4], but rather wanted to get explicit and smaller error terms that can be obtained under GRH.

As for the positivity of the density, we have the following.

Theorem 4 *Let $E/\mathbb{Q}$ be a non-CM curve. If $(f, M_E)=1$, and $K_2\neq\mathbb{Q}$, then the quantity $\delta_E(f,a)$ given by (6) satisfies*

$$\begin{aligned}\delta_E(f,a) \geqslant \frac{1}{\varphi(f)}\prod_{\substack{p\nmid M_E\\(p,f)\mid a-1}}\left(1-\frac{\varphi(p,f)}{[K_p:\mathbb{Q}]}\right)\prod_{2<p\mid M_E}\left(1-\frac{1}{p-1}\right)\\ \cdot\frac{1}{[K_2:\mathbb{Q}]}\left([K_2:\mathbb{Q}]-1-\frac{\mu(\mathfrak{f}_2)([K_2^{ab}:\mathbb{Q}]-1)}{\prod_{2<p\mid\mathfrak{f}_2}(p-2)}\right)>0,\end{aligned} \tag{9}$$

where $\varphi(p,f)$ stands for $\varphi(\gcd(p,f))$.

Remark 2 Note that when $f=1$, (9) would imply δ_E in (2) is at least

$$\frac{1}{2}\left(1-\frac{\mu(\mathfrak{f}_2)}{\prod_{2<p\mid\mathfrak{f}_2}(p-2)}\right)\prod_{2<p\mid M_E}\left(1-\frac{1}{p-1}\right)\prod_{p\nmid M_E}\left(1-\frac{1}{[K_p:\mathbb{Q}]}\right).$$

This is obtained in the same way as Cojocaru and Murty had their result in [7], yet the two results are different. The reason is that when $\mathfrak{f}_2$ is not a prime, then K_2^{ab} may have nontrivial intersections with $\mathbb{Q}(\zeta_d)$ with square-free $d\mid M_E$, even though $K_2^{ab}\cap\mathbb{Q}(\zeta_q)=\mathbb{Q}$ for each prime $q\mid d$. They seem to have overlooked this point in their work.

By the definition of M_E, we have $[K_p:\mathbb{Q}]=(p^2-p)(p^2-1)\asymp p^4$ for $p\nmid M_E$. Thus, we obtain from (9) that

$$\delta_E(f,a)\gg\frac{1}{\varphi(f)}\prod_{2<p\mid M_E}\left(1-\frac{1}{p-1}\right)=\frac{2\varphi(M_E)}{\varphi(f)M_E}\gg\frac{1}{\varphi(f)\log\log M_E}.$$

The restrictions on the modulus f in Theorem 9 can be discarded for Serre Curves. Indeed, Julio Brau Avila showed in his thesis (cf. [2, Corollary 2.5.9]) that $\delta_E(f,a)$ is positive for Serre curves for any co-prime a and f. Although an asymptotic formula is not given in Brau's work, the density $\delta_E(f,a)$ is given explicitly as a product using

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

a different approach. Since Nathan Jones proved (cf. [20]) that almost all non-CM curves are Serre curves, Brau's result strongly supports our prediction.

Brau also considers the non-CM and non-Serre curve

$$y^2 = x^3 + x^2 + 4x + 4,$$

as an example, with $K_2 = \mathbb{Q}(\zeta_4)$ (so $\mathfrak{f}_2 = 4$), $N_E = 20$, and $A(E) = 30$ (yielding $M_E = 30$). Proposition 2.5.12 in [2] then states that $\delta_E(f, a) = 0$ for this curve if and only if $4 \mid f$ and $a \equiv 1 \bmod 4$. Proposition 1 and Theorem 2 in this paper show that there are infinitely many primes $p \equiv a \bmod f$ for which $\widetilde{E}(\mathbb{F}_p)$ is cyclic unless $4 \mid f$ and $a \equiv 1 \bmod 4$, in which case there are at most finitely many such primes, which agrees with Brau's result.

Next, we turn to CM curves. We assume as in [1] and [7] that the endomorphism ring is isomorphic to the full ring of integers. The exact definition of the arithmetic function $G_D(a, f)$ that appears inside the error term below is given in the proof.

Theorem 5 *Let $E/\mathbb{Q}$ be an elliptic curve with $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathfrak{O}_K$, where $\mathfrak{O}_K$ is the ring of algebraic integers of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. If GRH holds for all Dedekind zeta functions of the fields $K_d\mathbb{Q}(\zeta_f)$ for all square-free $d \geqslant 1$, then*

$$\pi_E(x; f, a) = \delta_E(f, a)\,\mathrm{Li}(x) + E(x),$$

where $\delta_E(f, a)$ is given by (6) and the error term $E(x)$ satisfies

$$E(x) \ll x^{3/4}\left(\frac{\log(fxN_E)}{\log x}\right)^{1/2} + x^{3/4}\left(\frac{\log(fxN_E)G_D(a,f)}{f^3}\right)^{1/2} + x^{1/2} f \log(fxN_E) + x^{1/2}\left(\frac{1}{f} + \frac{\log x}{f^2}\right) G_D(a, f). \tag{10}$$

Here, $G_D(a, f)$ is the cardinality of the set given by (23), is multiplicative in the second variable and satisfies

$$G_D(a, f) < c \cdot 4^{\omega(f)}\tau(f)f^2, \tag{11}$$

where $c = 2$ if $D \equiv 1, 2 \bmod 4$, or $D \equiv 3 \bmod 4$ and f is odd, and $c = 49$ otherwise.

As for the density, we have the following result.

Theorem 6 *The density $\delta_E(f, a)$ in Theorem 5 is positive if one of the following holds:*

(1) *$K_2 \cap K = \mathbb{Q}$, $\gamma_{a,f}(K_2K) = \gamma_{a,f}(K_2)\gamma_{a,f}(K)$, and both (a) and (b) hold, where*
   (a) *$K_2 \subsetneq \mathbb{Q}(\zeta_f)$ or σ_a does not fix $K_2 \cap \mathbb{Q}(\zeta_f)$,*
   (b) *$K \subsetneq \mathbb{Q}(\zeta_f)$ or σ_a does not fix $K \cap \mathbb{Q}(\zeta_f)$.*

(2) *$K_2^{ab} = K$, and either $K_2 \subsetneq \mathbb{Q}(\zeta_f)$ or σ_a does not fix $K_2 \cap \mathbb{Q}(\zeta_f)$.*

Remark 3 We did not attempt to handle the CM case without GRH in this paper even though division fields are better understood for these curves, and one may be able to improve Theorems 5 and 6. We leave this task to a separate paper.

As we mentioned above, the Appendix provided by Ernst Kani at the end of the paper provides detailed exposition on the intersection of division fields, which play a fundamental role in the proofs of all the results on the density $\delta_E(a, f)$.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

2 Proofs of unconditional results

2.1 The linear sieve

Assume that $F \geqslant 1$ is an integer satisfying

$$F \ll (\log x)^A \quad \text{for some } A \geqslant 0, \tag{12}$$

c is an integer coprime to F such that $(c-1, F)$ has no odd prime divisors. Put

$$\mathcal{A} = \{p - 1 : p \leqslant x, p \equiv c \bmod F\}$$

and, as usual, define

$$\mathcal{P}(z) = \prod_{q<z, q\in\mathcal{P}} q,$$

where $\mathcal{P}$ is the set of *odd primes coprime to F*. We seek a lower bound for

$$S(\mathcal{A}, \mathcal{P}, z) = |\{n \in \mathcal{A} : (n, \mathcal{P}(z)) = 1\}|.$$

For $d \mid \mathcal{P}(z)$, we have

$$\mathcal{A}_d := \sum_{\substack{n\in\mathcal{A}\\ d\mid n}} 1 = \pi(x; dF, c_d) = \frac{\omega(d)}{d}\frac{\mathrm{Li}(x)}{\varphi(F)} - r(\mathcal{A}, d),$$

say. Here, $\pi(x; dF, c_d)$ denotes the number of primes $p \leqslant x$ that are congruent to c_d modulo dF, c_d is the unique integer (by Chinese Remainder Theorem) modulo dF satisfying $c_d \equiv 1 \bmod d$ and $c_d \equiv c \bmod F$, and $\omega(d) = d/\varphi(d)$ satisfies $0 < \omega(q) < q$ for all odd primes q. Furthermore, the inequalities

$$\prod_{\substack{w\leqslant p<z\\ p\nmid 2F}} \left(1 - \frac{\omega(p)}{p}\right)^{-1} < \exp\left(\sum_{\substack{p\geqslant w\\ p>2}} \frac{1}{p^2 - 2p}\right) \prod_{w\leqslant p\leqslant z} \left(1 - \frac{1}{p}\right)^{-1} \leqslant \frac{\log z}{\log w}\left(1 + \frac{K}{\log w}\right)$$

and

$$\sum_{\substack{w\leqslant p<z\\ p\in\mathcal{P}}} \sum_{k\geqslant 2} \frac{\omega(p^k)}{p^k} = \sum_{\substack{w\leqslant p<z\\ p\in\mathcal{P}}} \frac{1}{(p-1)^2} \leqslant \frac{L}{\log(3w)}$$

hold for all $z > w \geqslant 2$ for some constants $K, L > 1$, where in the second inequality of the first equation we use Merten's estimate [25, Theorem 2.7]

$$\prod_{p\leqslant x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma} \log x + O(1).$$

We have verified so far that the necessary conditions given in [18] by equations (1) and (2) are satisfied. Hence, we are now ready to use the lower bound sieve of Iwaniec in

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

[18]. Thus, assume that $\varepsilon_1 \in (0, 1/3)$, and $2 \leqslant y^{1/4} \leqslant z < y^{1/2}$. Then, it follows from [18, Theorem 1] that

$$S(\mathcal{A}, \mathcal{P}, z) \geqslant \frac{\mathrm{Li}(x)}{\varphi(F)} \prod_{\substack{2<p<z \\ p \nmid F}} \left(1 - \frac{1}{p-1}\right) \{f(s) - E(\varepsilon_1, y, K, L)\} - R(\mathcal{A}, y),$$

where $s = \log y / \log z$, $E(\varepsilon_1, y, K, L) \ll \varepsilon_1 + \varepsilon_1^{-8} e^{K+L} (\log y)^{-1/3}$ and

$$R(\mathcal{A}, y) = \sum_{l < \exp(8/\varepsilon_1^3)} \sum_{\substack{d<y \\ d \mid \mathcal{P}(z)}} \lambda_l(d) \left(\frac{\mathrm{Li}(x)}{\varphi(dF)} - \pi(x; dF, c_d) \right)$$

for some well factorable functions λ_l (see the paragraph before [15, Lemma 2] for the definition). Here, the implied constant is absolute. The function $f(s)$ that appears above is a continuous solution of a system of differential-difference equations given in [18], and in the interval $2 \leqslant s \leqslant 4$ that we are interested in $f(s)$ is given by (cf. [11, p. 126])

$$f(s) = \frac{2e^{\gamma}}{s} \log(s-1),$$

where $\gamma = 0.5772156649\ldots$ is the Euler–Mascheroni constant.

Now, we choose $y = x^{4/7-\varepsilon_2}$ and $z = y^{1/(2+\varepsilon_2)}$ with a fixed $\varepsilon_2 \in (0,1)$ so that $s = 2 + \varepsilon_2$, and

$$f(s) > \frac{\varepsilon_2 e^{\gamma}}{2+\varepsilon_2} > \varepsilon_2/2.$$

For ε_1 sufficiently small in terms of ε_2 and x sufficiently large, we get

$$f(s) - E(\varepsilon_1, y, K, L) > \varepsilon_2/3.$$

Furthermore, it follows from [15, Lemma 2] that for a given ε_2 and any $B > 0$,

$$R(\mathcal{A}, y) \ll x F^k (\log x)^{-B},$$

for some fixed positive integer k, where the implied constant may depend on c, ε_2, and B. Then, choosing $B = (k+1)A + 3$, it follows from (12) that

$$S(\mathcal{A}, \mathcal{P}, z) \geqslant c(\varepsilon_2, A) \frac{x}{(\log x)^{2+A}}$$

for sufficiently large x. For $\varepsilon_2 \in (0, 2/35)$, we see that $z = x^{\alpha}$ with

$$\alpha = \alpha(\varepsilon_2) = \frac{4/7 - \varepsilon_2}{2+\varepsilon_2} = \frac{1}{4} + \frac{2/7 - 5\varepsilon_2}{8 + 4\varepsilon_2} > \frac{1}{4}.$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Furthermore, since

$$\sum_{q\geqslant x^{\alpha}}\sum_{\substack{p\leqslant x\\ q^2\mid p-1}} 1 < \sum_{x^{\alpha}\leqslant q<\sqrt{x}}\left(\frac{x}{q^2}+1\right) \ll x^{1-\alpha} = o\left(\frac{x}{\log^{2+A}x}\right),$$

we can also assume that each $p-1$ counted in $S(\mathcal{A},\mathcal{P},x^{\alpha})$ has *distinct* odd prime divisors $q\geqslant x^{\alpha}$ coprime to F. Finally, since there are only finitely many divisors of N_E, we obtain the following result:

Lemma 1 *Let $A\geqslant 0$ and $\varepsilon\in(0,2/35)$ be given. Assume that c and F are positive coprime integers such that $F\ll(\log x)^A$ and no odd prime divides $(c-1,F)$. Then, there is some $\alpha=\alpha(\varepsilon)>1/4$ and a positive constant $c(\alpha,A)$ such that for x sufficiently large, there are at least $c(\alpha,A)x/(\log x)^{2+A}$ primes $p\leqslant x$ with $p\equiv c \bmod F$ and $p\nmid N_E$ such that odd prime divisors q of $p-1$ are distinct, coprime to F and satisfy $q\geqslant x^{\alpha}$.*

2.2 Proofs of Theorems 1 and 2

As mentioned in the introduction, Murty and Gupta showed in [12] unconditionally that for any elliptic curve $E/\mathbb{Q}$ for which $K_2\neq\mathbb{Q}$, there are infinitely many primes p for which $\widetilde{E}(\mathbb{F}_p)$ is cyclic. The first step in their proof is to make sure p does not split completely in K_2, which is established by imposing a congruence condition on p as mentioned in [12, Lemma 3]. Since this result plays a fundamental role in this paper and since they do not give any details, we show below that there is in fact an appropriate arithmetic progression that serves this purpose.

Lemma 2 *If $K_2\neq\mathbb{Q}$, there exists some $b\in(\mathbb{Z}/\mathfrak{f}_2\mathbb{Z})^{\times}$ such that $\gamma_{b,\mathfrak{f}_2}(K_2)=0$ and the odd part of $\mathfrak{f}_2$ is coprime to $b-1$.*

Remark 4 As mentioned in the introduction, to be able to apply the linear sieve, it is of fundamental importance to make sure that no odd prime divides $(\mathfrak{f}_2,b-1)$, and that is exactly why we need to prove that there is at least one such b. Otherwise, only finding some $b\in(\mathbb{Z}/\mathfrak{f}_2\mathbb{Z})^{\times}$ such that $\gamma_{b,\mathfrak{f}_2}(K_2)=0$ can easily be accomplished by choosing an automorphism σ in $\mathrm{Gal}(\mathbb{Q}(\zeta_{\mathfrak{f}_2})/\mathbb{Q})$ which does not fix $K_2\cap\mathbb{Q}(\zeta_{\mathfrak{f}_2})$.

Proof Note that $K_2\cap\mathbb{Q}(\zeta_{\mathfrak{f}_2})=K_2^{ab}$.

Assume first that $[K_2^{ab}:\mathbb{Q}]=2$. Then, $K_2^{ab}=\mathbb{Q}(\sqrt{D})$ for some square-free integer D, and

$$\mathfrak{f}_2=\begin{cases} 4|D| & \text{if } D\equiv 2,3 \bmod 4,\\ |D| & \text{if } D\equiv 1 \bmod 4\end{cases} \tag{13}$$

is the absolute value of the discriminant $\mathfrak{d}_2$ of K_2^{ab} over $\mathbb{Q}$ (cf. [19, Corollary VI.1.3]). We choose $b=3$ if $D=-1,2$; $b=7$ if $D=-2$. For $|D|>2$, let p be the smallest *odd*

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

prime divisor of D, and choose b as the unique solution modulo $\mathfrak{f}_2$ of the system of congruences

$$\begin{cases} b \equiv g_p & \bmod p \\ b \equiv g_q^2 & \bmod q \\ b \equiv 1 & \bmod 4 \end{cases} \quad (\forall q \mid D/p) \qquad \text{if } D \equiv 3 \bmod 4$$

$$\begin{cases} b \equiv g_p & \bmod p \\ b \equiv g_q^2 & \bmod q \end{cases} \quad (\forall q \mid D/p) \qquad \text{if } D \equiv 1 \bmod 4$$

$$\begin{cases} b \equiv g_p & \bmod p \\ b \equiv g_q^2 & \bmod q \\ b \equiv 1 & \bmod 8 \end{cases} \quad (\forall q \mid D/(2p)) \qquad \text{if } D \equiv 2 \bmod 4$$

Here, g_p denotes a primitive root modulo p for each odd prime divisor of D. Since $q > 3$ for any $q \neq p$, $g_q^2 \not\equiv 1 \bmod q$. Furthermore, $\sigma_b(\sqrt{D}) = -\sqrt{D}$. Thus, we have the desired b.

Next, assume that $[K_2 : \mathbb{Q}] = 3$ (note $K_2 = K_2^{ab}$). Hasse proved (cf. [14]) that

$$\mathfrak{f}_2 = p_1 p_2 \cdots p_r, \tag{14}$$

where $p_1, \ldots, p_r$ are either all distinct primes with $p_i \equiv 1 \bmod 3$, or all except one, say p_r, are such primes, and $p_r = 9$.

If $r = 1$, any b which is not a cube modulo p_1 works. In particular, there are $2\varphi(p_1)/3$ choices for b. If $r > 1$, write $\mathfrak{f}_2 = p_1 m$. Since $K_2 \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ for any $n \mid m$ (otherwise, $K_2 \subset \mathbb{Q}(\zeta_m)$), we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)K_2/\mathbb{Q}) \simeq \mathrm{Gal}(K_2/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_2})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_r})/\mathbb{Q}).$$

Thus, there are $2\prod_{i=2}^{r}(\varphi(p_i) - 1)$ choices for an automorphism $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)K_2/\mathbb{Q})$, which is not identity on K_2 and on any $\mathbb{Q}(\zeta_{p_i})$ for $i = 2, \ldots, r$. Furthermore,

$$[\mathbb{Q}(\zeta_{\mathfrak{f}_2}) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_m)K_2 : \mathbb{Q}][\mathbb{Q}(\zeta_{p_1}) : \mathbb{Q}]}{[L : \mathbb{Q}]} = \frac{3\varphi(\mathfrak{f}_2)}{[L : \mathbb{Q}]},$$

where $L = \mathbb{Q}(\zeta_m)K_2 \cap \mathbb{Q}(\zeta_{p_1})$, implies $[L : \mathbb{Q}] = 3$. Since $[\mathbb{Q}(\zeta_{p_1}) : \mathbb{Q}] > 3$, we can extend $\tau_{|L}$ to a nonidentity automorphism β of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_1})/\mathbb{Q})$. Since τ and β agree on L, it follows from Galois theory that there is a $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{\mathfrak{f}_2})/\mathbb{Q})$ which extends τ and β. Then, σ uniquely determines some $b \in (\mathbb{Z}/\mathfrak{f}_2\mathbb{Z})^\times$ such that $(b-1, \mathfrak{f}_2) = 1$ and $\gamma_{b,\mathfrak{f}_2}(K_2) = 0$ as desired. ∎

Remark 5 Let $\chi_{\mathfrak{d}_2}$ be the real primitive character of conductor $\mathfrak{f}_2$ given by the Kronecker symbol $(\frac{\mathfrak{d}_2}{\cdot})$. Then, $\gamma_{b,\mathfrak{f}_2}(K_2) = 1$ if and only if $b \in \ker \chi_{\mathfrak{d}_2}$ (to see how this character plays a role, see for example, [19, I.7.4 and pp. 250–1]). So, when $[K_2^{ab} : \mathbb{Q}] = 2$, we choose b in such a way that $b \notin \ker \chi_{\mathfrak{d}_2}$ and that $b \not\equiv 1 \bmod q$ for odd $q \mid D$.

The next result is needed in the proof of Theorem 1.

Lemma 3 *Assume that* $[K_2 : \mathbb{Q}] = 3$. *Let* $m > 1$ *be a proper divisor of* $\mathfrak{f}_2$ *and a an integer such that* $(m, a(a-1)) = 1$. *Then, there is some b satisfying conditions of Lemma 2 such that* $b \equiv a \bmod m$.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Proof Write $\mathfrak{f}_2 = pdm = pn$, where p is a prime, $d \geqslant 1$ and $(d, m) = 1$. Since $K_2 \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$, there is some $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)K_2/\mathbb{Q})$ which is not identity on K_2 and on $\mathbb{Q}(\zeta_q)$ for each prime (if any) $q \mid d$, while it equals σ_a on $\mathbb{Q}(\zeta_m)$. If $p = 3$, then $\mathbb{Q}(\zeta_n)K_2 = \mathbb{Q}(\zeta_{\mathfrak{f}_2})$. Thus, $\tau = \sigma_b$ for some b. If $3 \mid m$, then $b \equiv a \bmod m$ implies $b \equiv 2 \bmod 3$ since $(m, a(a-1)) = 1$. Otherwise, $3 \mid d$ and $\sigma_b \neq 1_{\mathbb{Q}(\zeta_3)}$ implies $b \equiv 2 \bmod 3$. In either case, we obtain the desired result. If $p \neq 3$, we put $L = \mathbb{Q}(\zeta_n)K_2 \cap \mathbb{Q}(\zeta_p)$. Then,

$$[L : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_n) : \mathbb{Q}][K_2 : \mathbb{Q}][\mathbb{Q}(\zeta_p) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{\mathfrak{f}_2}) : \mathbb{Q}]} = \frac{3\varphi(\mathfrak{f}_2/p)\varphi(p)}{\varphi(\mathfrak{f}_2)} = 3 < \varphi(p).$$

Thus, we can extend $\tau_{|L}$ to a nonidentity automorphism β of $\mathbb{Q}(\zeta_p)$. Since τ and β agree on L, it follows from Galois theory that there is a $\sigma_b \in \mathrm{Gal}(\mathbb{Q}(\zeta_{\mathfrak{f}_2})/\mathbb{Q})$ which extends τ and β for some b with the desired property. ∎

Proof of Theorem 1 If $\mathfrak{f}_2 \nmid f$, then we can write $f = mg$ with $m = (\mathfrak{f}_2, f) < \mathfrak{f}_2$. Applying Lemma 2 if $m = 1$, and Lemma 3 for $m > 1$ yields some b with which the system $p \equiv b \bmod \mathfrak{f}_2$ and $p \equiv a \bmod f$ is solvable since $m \mid a - b$, and there is a unique solution, say, c modulo $F = [f, \mathfrak{f}_2]$. Applying Lemma 1 to primes $p \equiv c \bmod F$, we find some $\alpha > 1/4$ and a set of primes $S_\alpha(x)$ having properties stated in Lemma 1. We would like to show that the number of $p \in S_\alpha(x)$ for which $\widetilde{E}(\mathbb{F}_p)$ is not cyclic is negligible. The rest of the proof follows the proof of [12, Theorem 1], but we shall include it here.

Recall that $|\widetilde{E}(\mathbb{F}_p)| = p + 1 - a_p$, where a_p denotes the trace of the Frobenius associated to E and p. Put

$$S(b, x) = \{p \in S_\alpha(x) : a_p = b\}.$$

By Hasse's inequality, $S_\alpha(x)$ is the union of $S(b, x)$ with $|b| \leqslant 2\sqrt{x}$. Take a prime $p \in S(b, x)$ for which $\widetilde{E}(\mathbb{F}_p)$ is not cyclic. Then, p splits completely in K_q, for some odd prime q. Since $\mathbb{Q}(\zeta_q) \subset K_q$, $q \mid p - 1$ and the fact that $p \in S_\alpha(x)$ implies $q \geqslant x^\alpha$ and is coprime to $[f, \mathfrak{f}_2]$. Moreover, $q^2 \mid |\widetilde{E}(\mathbb{F}_p)| = p + 1 - a_p = p - 1 + (2 - b)$, thus $q \mid b - 2$. Notice that $b \neq 2$ since odd prime divisors of $p - 1$ are distinct. Since $q \geqslant x^\alpha$ with $\alpha > 1/4$ and $|a_p - 2| \ll x^{1/2}$, there is only one such prime q for a given b, for x sufficiently large. Therefore, any $p \in S(b, x)$ for which $\widetilde{E}(\mathbb{F}_p)$ is not cyclic satisfies

$$p \equiv b - 1 \bmod q^2$$

and the number of such p is $< x/q^2 + O(1) \ll x^{1-2\alpha}$. The total number of $p \in S_\alpha(x)$ for which $\widetilde{E}(\mathbb{F}_p)$ is not cyclic is, therefore, $\ll x^{3/2-2\alpha} = o(x/(\log x)^{2+A})$.

If $\mathfrak{f}_2 \mid f$ and $\gamma_{a,f}(K_2^{ab}) = 0$, we can apply Lemma 1 with the pair (a, f), and repeat the same arguments above. ∎

Lemma 4 *Assume that* $[K_2^{ab} : \mathbb{Q}] = 2$, $m > 1$ *is a proper divisor of* $\mathfrak{f}_2$, $(a, m) = 1$ *and the odd part of m is coprime to* $a - 1$. *Then, there is some b satisfying conditions of Lemma 2 such that* $b \equiv a \bmod m$ *unless* $\mathfrak{f}_2 = 3m$ *and* $\chi_{-\mathfrak{d}_2/3}(a) = -1$.

Proof By remark 5, we need to find some b with $(b, \mathfrak{f}_2) = 1$ such that $\chi_{\mathfrak{d}_2}(b) = -1$ and that $b \not\equiv 1 \bmod q$ for odd $q \mid D$. Write $\mathfrak{f}_2 = pdm = pn$ with $d \geqslant 1$. Whenever $p = 3$, we need to choose $b \equiv 2 \bmod 3$ so that $3 \nmid b - 1$, and $b \equiv a \bmod m$. This gives $\chi_{\mathfrak{d}_2}(b) = (\frac{b}{3})\chi_{-\mathfrak{d}_2/3}(b) = -\chi_{-\mathfrak{d}_2/3}(b)$. If $d = 1$, this implies $\chi_{-\mathfrak{d}_2/3}(a)$ should be 1 since otherwise

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

$\gamma_{b,\mathfrak{f}_2}(K_2^{ab}) = 1$. If $d \neq 1$ and $(d, m) = 1$, we choose b modulo d in such a way that $q \nmid b - 1$ for each odd $q \mid d$ and that $\chi_{\mathfrak{d}_2}(b) = -1$. This can be done since odd prime divisors of d are larger than 3. If $(d, m) \neq 1$, it equals 4 or 8. In this case, we choose b similarly for odd prime divisors of d, and congruent to a modulo the odd part of m. We finally choose b modulo (d, m) so that $\chi_{\mathfrak{d}_2}(b) = -1$. If $3 \nmid \mathfrak{f}_2$, then we choose b similarly. ■

Proof of Theorem 2 If $\mathfrak{f}_2 \nmid f$, then we can write $f = mg$ with $m = (\mathfrak{f}_2, f) < \mathfrak{f}_2$. Applying Lemma 2 if $m = 1$, and Lemma 4 for $m > 1$ yields some b with which the system $p \equiv b \bmod \mathfrak{f}_2$ and $p \equiv a \bmod f$ is solvable since $m \mid a - b$, and there is a unique solution modulo $[f, \mathfrak{f}_2]$. Applying Lemma 1 and proceeding as in the proof of Theorem 1, we get the result. If $\mathfrak{f}_2 \mid f$ and $\gamma_{a,f}(K_2^{ab}) = 0$, we can apply Lemma 1 with the pair (a, f). ■

3 Proofs of Theorems 3 and 4

Throughout this section, we assume that E is an elliptic curve over $\mathbb{Q}$ that has no complex multiplication.

3.1 Preliminaries

Recall that $\mathfrak{f}_n$ is the conductor of K_n^{ab}. It follows from [30, V Theorem 1.10, p.324] that $\mathfrak{f}_n$ is divisible exactly by those primes that ramify in K_n^{ab}. Also, primes that ramify in K_n are among the divisors of nN_E (see, for example, [33, p. 179]). Since these primes also ramify in K_n, $\mathfrak{f}_n \mid (nN_E)^\infty$. In particular, $\mathfrak{f}_2 \mid M_E^\infty$ and we use this implicitly in the proof of Theorem 4.

Lemma 5 ([7, Lemma 2.1]) *Let E be an elliptic curve defined over $\mathbb{Q}$, and p a prime with $p \nmid N_E$. Then, for any prime $q \neq p$, $\widetilde{E}(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ if and only if p splits completely in K_q. Therefore, for odd p, $\widetilde{E}(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in K_q for any prime $q \neq p$.*

Lemma 6 *If $(d, e) = 1$, then $K_{de} = K_d K_e$.*

Proof Since $K_d, K_e \subseteq K_{de}$, $K_d K_e \subseteq K_{de}$. Now, take any de-torsion point (x, y) of E, and note that since $(d, e) = 1$, $(x, y) = ad(x, y) \oplus be(x, y)$ for some integers a and b, where $\oplus$ denotes the group operation on E; that is, (x, y) is the sum of a d-torsion and an e-torsion point. Thus, the claim follows. ■

Lemma 7 *If $(e, A(E)) = 1$, then $K_e \cap \mathbb{Q}(\zeta_g) = \mathbb{Q}(\zeta_{(e,g)})$, where $A(E)$ is Serre's constant defined in (4).*

Proof By [6, Appendix Corollary 13], $\mathbb{Q}(\zeta_e)$ is the maximal abelian extension of $\mathbb{Q}$ in K_e. Thus, $K_e \cap \mathbb{Q}(\zeta_g)$, being abelian, lies in both $\mathbb{Q}(\zeta_e)$ and $\mathbb{Q}(\zeta_g)$, and also contains their intersection since $\mathbb{Q}(\zeta_e) \subseteq K_e$. ■

Lemma 8 (Theorem 1 in Appendix) *If $(m, nM_E) = 1$, then $K_n \cap K_m = \mathbb{Q}$.*

Below we give an effective version of Chebotarev's Density Theorem.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Lemma 9 ([7, Theorem 3.1, Lemma 3.4]) *Let $L/\mathbb{Q}$ be a Galois extension of discriminant Δ_L, $G = \mathrm{Gal}(L/\mathbb{Q})$, $C \subseteq G$ a conjugacy class, and $\mathcal{P}(L)$ the set of primes p that ramify in L. Then, assuming GRH for the Dedekind zeta function of L,*

$$\pi_C(x, L/\mathbb{Q}) = \frac{|C|}{|G|}\mathrm{Li}(x) + O\left(x^{1/2}\log\left(x[L:\mathbb{Q}]\prod_{p\in\mathcal{P}(L)} p\right)\right),$$

where

$$\pi_C(x, L/\mathbb{Q}) = |\{p \leqslant x : p \nmid \Delta_L, \mathrm{Frob}_p(L/\mathbb{Q}) \subseteq C\}|.$$

Lemma 10 *For real $Y \geqslant 1$ and integer $k \geqslant 1$,*

$$\sum_{n>Y} \frac{1}{n^k\varphi(n)} \ll Y^{-k}.$$

Proof We have

$$\begin{aligned}\sum_{Y<e\leqslant Z} \frac{1}{e^k\varphi(e)} &= \sum_{Y<e\leqslant Z} \frac{1}{e^{k+1}} \prod_{p|e} \frac{p}{p-1} \\ &< \prod_p \left(1 + \frac{1}{p^2-1}\right) \sum_{Y<e\leqslant Z} \frac{1}{e^{k+1}} \sum_{d|e} \frac{\mu(d)^2}{d} \\ &< e^{\pi^2/6} \sum_{Y<ed\leqslant Z} \frac{1}{e^{k+1}d^{k+2}} \\ &\ll \sum_{d\leqslant Z} \frac{1}{d^{k+2}} \sum_{e>Y/d} \frac{1}{e^{k+1}} \ll Y^{-k} \sum_{d\leqslant Z} \frac{1}{d^2},\end{aligned}$$

and taking limit as $Z \to \infty$, the result follows. ∎

Lemma 11 *For $Y > 1$,*

$$\sum_{n>Y} \frac{1}{\varphi(n)^2} \ll \frac{1}{Y}.$$

Proof Note that for any $x \geqslant 1$,

$$\lfloor x \rfloor \leqslant \sum_{n\leqslant x} \frac{n}{\varphi(n)} = \sum_{d\leqslant x} \frac{\mu(d)^2}{\varphi(d)} \sum_{n\leqslant x/d} 1 < x \sum_d \frac{\mu(d)^2}{d\varphi(d)} = cx$$

where $c > 1$ and the last inequality holds by Lemma 10. Thus,

$$\begin{aligned}\sum_{n\leqslant x} \frac{n^2}{\varphi(n)^2} &= \sum_{n\leqslant x} \frac{n}{\varphi(n)} \sum_{d|n} \frac{\mu(d)^2}{\varphi(d)} \leqslant \sum_{d\leqslant x} \frac{\mu(d)^2 d}{\varphi(d)^2} \sum_{n\leqslant x/d} \frac{n}{\varphi(n)} \\ &< cx \sum_{d\geqslant 1} \frac{\mu(d)^2}{\varphi(d)^2} = c_1 x,\end{aligned}$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

where the first inequality follows by using $\varphi(dn) \geqslant \varphi(d)\varphi(n)$ and the second by $\varphi(d) \gg d/\log\log d$ (cf. [25, Theorem 2.9]). We conclude that for $z > y > 1$,

$$\sum_{y<n\leqslant z} \frac{1}{\varphi(n)^2} = \int_y^z \frac{1}{x^2} d \sum_{n\leqslant x} \frac{n^2}{\varphi(n)^2} = \frac{1}{z^2} \sum_{n\leqslant z} \frac{n^2}{\varphi(n)^2} - \frac{1}{y^2} \sum_{n\leqslant y} \frac{n^2}{\varphi(n)^2} + 2\int_y^z x^{-3} \sum_{n\leqslant x} \frac{n^2}{\varphi(n)^2} dx < \frac{2c_1 - 1}{y} + \frac{1}{y^2} - \frac{c_1}{z}.$$

Taking limit as $z \to \infty$, we get the result. ∎

3.2 Proof of Theorem 3

We shall assume $f < \frac{1}{2}\sqrt{x}$ since otherwise the theorem trivially holds. For a square-free integer $d \geqslant 1$, put

$$\pi_{E,d}(x; f, a) = \#\{p \leqslant x : p \nmid 2N_E, p \equiv a \bmod f, p \text{ splits completely in } K_d\}.$$

If a prime $p \leqslant x$ splits completely in K_d for some $d > 1$, then p splits completely in K_q for each prime $q \mid d$. Since p ramifies in $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_p) \subseteq K_p$ by [7, Proposition 3.5#3], $p \nmid d$. Consequently, it follows from Lemmas 5 and 6 that d^2 divides $|\widetilde{E}(\mathbb{F}_p)|$. Then, by Hasse's inequality $d^2 \leqslant (\sqrt{p}+1)^2$, yielding $d \leqslant \sqrt{x}+1$. Hence, using inclusion–exclusion principle we can write

$$\pi_E(x; f, a) = \sum_{d\leqslant \sqrt{x}+1} \mu(d)\pi_{E,d}(x; f, a).$$

Put

$$\Sigma_1 = \sum_{d\leqslant y} \mu(d)\pi_{E,d}(x; f, a), \qquad \Sigma_2 = \sum_{y<d\leqslant \sqrt{x}+1} \mu(d)\pi_{E,d}(x; f, a), \tag{15}$$

where y is a parameter satisfying $2f \leqslant y \leqslant \sqrt{x}$.

3.2.1 Main term Σ_1

For each square-free $d \leqslant y$, there is a unique automorphism in $\mathrm{Gal}(K_d\mathbb{Q}(\zeta_f)/\mathbb{Q})$ whose restrictions to K_d and $\mathbb{Q}(\zeta_f)$ are identity and σ_a, respectively, provided that $\gamma_{a,f}(K_d) = 1$. Thus, $\pi_{E,d}(x; f, a)$ counts primes $p \leqslant x$ of good reduction whose Frobenius automorphism coincides with this automorphism whenever $\gamma_{a,f}(K_d) = 1$. Therefore, it follows from Lemma 9 that for each square-free $d \leqslant y$,

$$\pi_{E,d}(x; f, a) = \frac{\mathrm{Li}(x)}{[K_d\mathbb{Q}(\zeta_f) : \mathbb{Q}]} + O\left(x^{1/2} \log\left(x[K_d\mathbb{Q}(\zeta_f) : \mathbb{Q}] \prod_{p\in\mathcal{P}(K_d\mathbb{Q}(\zeta_f))} p\right)\right)$$

if $\gamma_{a,f}(K_d) = 1$, and is 0 otherwise. Here, the product is taken over primes $p \in \mathcal{P}(K_d\mathbb{Q}(\zeta_f))$, where $\mathcal{P}(L)$, for any number field L, is defined in Lemma 9.

Note that $[K_d\mathbb{Q}(\zeta_f) : \mathbb{Q}] \leqslant [K_d : \mathbb{Q}]\varphi(f) < d^4 f$, the second inequality holds by (3). By [7, Proposition 3.5#3], $\mathbb{Q}(\zeta_f) \subseteq K_f$. Thus, $K_d\mathbb{Q}(\zeta_f) \subset K_{[d,f]}$, and this implies $\mathcal{P}(K_d\mathbb{Q}(\zeta_f)/\mathbb{Q}) \subseteq \mathcal{P}(K_{[d,f]}/\mathbb{Q})$. By [33, p. 179], we conclude that $\mathcal{P}(K_d\mathbb{Q}(\zeta_f)/\mathbb{Q})$ is a

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

subset of the primes dividing dfN_E. Therefore, the above error is $\ll x^{1/2}\log(dfxN_E)$, and we conclude

$$\Sigma_1 = \mathrm{Li}(x)\sum_{d\leqslant y}\frac{\mu(d)\gamma_{a,f}(K_d)}{[K_d\mathbb{Q}(\zeta_f):\mathbb{Q}]} + O(yx^{1/2}\log(fxN_E)). \tag{16}$$

Replacing the sum over $d \leqslant y$ by $\delta_E(a,f)$ in (6) produces an error

$$\ll \mathrm{Li}(x)\sum_{d>y}\frac{\mu^2(d)}{[K_d\mathbb{Q}(\zeta_f):\mathbb{Q}]}.$$

To estimate the sum over $d > y$, we write $f = f_1f_2$, where $f_1 \mid M_E^\infty$ and $(f_2, M_E) = 1$. Then,

$$\begin{aligned}\sum_{d>y}\frac{\mu^2(d)}{[K_d\mathbb{Q}(\zeta_f):\mathbb{Q}]} &= \sum_{\substack{de>y\\ d\mid M_E,(e,M_E)=1}}\frac{\mu^2(de)}{[K_{de}\mathbb{Q}(\zeta_f):\mathbb{Q}]}\\ &= \sum_{d\mid M_E}\frac{\mu^2(d)}{[K_d\mathbb{Q}(\zeta_{f_1}):\mathbb{Q}]}\sum_{\substack{e>y/d\\ (e,M_E)=1}}\frac{\mu^2(e)}{[K_e\mathbb{Q}(\zeta_{f_2}):\mathbb{Q}]}\\ &\leqslant \sum_{d\mid M_E}\frac{\mu^2(d)}{\varphi(f_1)}\sum_{\substack{e>y/d\\ (e,M_E)=1}}\frac{\mu^2(e)[K_e\cap\mathbb{Q}(\zeta_{f_2}):\mathbb{Q}]}{[K_e:\mathbb{Q}][\mathbb{Q}(\zeta_{f_2}):\mathbb{Q}]}.\end{aligned}$$

Here, the second equality follows by Lemma 8 (see the proof of Lemma 12 for details). By [7, Proposition 3.6.2] and Lemma 7, we get

$$[K_e:\mathbb{Q}] \gg e^3\varphi(e), \qquad [K_e\cap\mathbb{Q}(\zeta_{f_2}):\mathbb{Q}] = \varphi(e,f_2).$$

Thus, the last sum over e is

$$\begin{aligned}&\ll \frac{1}{\varphi(f_2)}\sum_{e>y/d}\frac{\mu^2(e)\varphi(e,f_2)}{\varphi(e)e^3} = \frac{1}{\varphi(f_2)}\sum_{k\mid f_2}\varphi(k)\sum_{\substack{e>y/d\\ (e,f_2)=k}}\frac{\mu^2(e)}{\varphi(e)e^3}\\ &\leqslant \frac{1}{\varphi(f_2)}\sum_{k\mid f_2}\frac{1}{k^3}\sum_{e>y/(kd)}\frac{1}{\varphi(e)e^3},\end{aligned}$$

where, in the last inequality, we used $\varphi(ek) \geqslant \varphi(e)\varphi(k)$. By Lemma 10, we derive that

$$\sum_{d>y}\frac{\mu^2(d)}{[K_d\mathbb{Q}(\zeta_f):\mathbb{Q}]} \ll \frac{\tau(f_2)}{y^3\varphi(f)}\sum_{d\mid M_E}\mu^2(d)d^3 \ll \frac{\tau(f_2)}{y^3\varphi(f)}M_E^3. \tag{17}$$

We will use (17) once we estimate Σ_2.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

3.2.2 Estimate of the error Σ_2

By Lemma 5, and the fact that p splits completely in $\mathbb{Q}(\zeta_d)$, we obtain

$$\Sigma_2 \leqslant \sum_{y<d\leqslant\sqrt{x}+1} \sum_{\substack{p\leqslant x, p\nmid 2N_E \\ p\equiv a \bmod f \\ p\equiv 1 \bmod d \\ d^2\mid \#\widetilde{E}(\mathbb{F}_p)}} 1.$$

Writing $|\widetilde{E}(\mathbb{F}_p)| = p+1-a_p$, we have by Hasse's inequality, $|a_p| < 2\sqrt{p} \leqslant 2\sqrt{x}$. Thus, Σ_2 is

$$\begin{aligned}
&\leqslant \sum_{y<d\leqslant\sqrt{x}+1} \sum_{|b|\leqslant 2\sqrt{x}} \sum_{\substack{p\leqslant x, p\nmid 2N_E \\ p\equiv a \bmod f \\ p\equiv 1 \bmod d \\ d^2\mid p+1-b \\ a_p=b}} 1 \leqslant \sum_{y<d\leqslant\sqrt{x}+1} \sum_{\substack{|b|\leqslant 2\sqrt{x} \\ d\mid b-2}} \sum_{\substack{n\leqslant x \\ n\equiv a \bmod f \\ n\equiv b-1 \bmod d^2}} 1 \\
&\ll \sum_{y<d\leqslant\sqrt{x}+1} \sum_{\substack{|b|\leqslant 2\sqrt{x} \\ d\mid b-2 \\ (d^2,f)\mid a+1-b}} \left(1+\frac{x}{[f,d^2]}\right) \ll \sum_{y<d\leqslant\sqrt{x}+1} \left(1+\frac{\sqrt{x}}{d}\right)\left(1+\frac{x}{[f,d^2]}\right) \\
&\ll \sqrt{x}\log x + \frac{x}{f} \sum_{y<d\leqslant\sqrt{x}+1} \frac{(f,d^2)}{d^2}\left(1+\frac{\sqrt{x}}{d}\right).
\end{aligned}$$

The last sum over d is

$$\begin{aligned}
&= \sum_{n\mid f} n \sum_{\substack{y<d\leqslant\sqrt{x}+1 \\ (f,d^2)=n}} \frac{1}{d^2}\left(1+\frac{\sqrt{x}}{d}\right) = \sum_{n\mid f} n \sum_{1\leqslant k\leqslant n} \sum_{\substack{y<d\leqslant\sqrt{x}+1 \\ d\equiv k \bmod n \\ (f,d^2)=n}} \frac{1}{d^2}\left(1+\frac{\sqrt{x}}{d}\right) \\
&\leqslant \sum_{n\mid f} n \sum_{\substack{1\leqslant k\leqslant n \\ n\mid k^2}} \sum_{\substack{y<d\leqslant\sqrt{x}+1 \\ d\equiv k \bmod n}} \frac{1}{d^2}\left(1+\frac{\sqrt{x}}{d}\right).
\end{aligned}$$

Using the estimate

$$\sum_{\substack{d>y \\ d\equiv k \bmod n}} \frac{1}{d^\ell} < \frac{1}{n^\ell} \sum_{m>(y-k)/n} \frac{1}{m^\ell} \ll \frac{1}{n(y-n)^{\ell-1}} \qquad (\ell>1),$$

and recalling that $2f \leqslant y \leqslant \sqrt{x}$, we obtain

$$\begin{aligned}
\Sigma_2 &\leqslant \sqrt{x}\log x + \frac{x}{f}\sum_{n\mid f} n \sum_{\substack{1\leqslant k\leqslant n \\ n\mid k^2}} \sum_{\substack{y<d\leqslant\sqrt{x}+1 \\ d\equiv k \bmod n}} \frac{1}{d^2}\left(1+\frac{\sqrt{x}}{d}\right) \\
&\ll \sqrt{x}\log x + \frac{x^{3/2}}{fy^2} H(f),
\end{aligned} \tag{18}$$

where $H(f)$ is given by (5).

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

3.2.3 Finale

Combining (16)–(18), we obtain

$$\pi_E(x;f,a)-\delta_E(a,f)\operatorname{Li}(x)\ll\frac{x\tau(f_2)M_E^3}{y^3\varphi(f)\log x}+x^{1/2}y\log(fxN_E)+\frac{x^{3/2}}{fy^2}H(f).$$

Recall, we assumed that $2f\leqslant y\leqslant\sqrt{x}$. To balance the terms on the right side, we use [10, Lemma 2.4] which states that there is some y in the interval $[2f,\sqrt{x}]$ for which the right hand side above is bounded by

$$\begin{aligned}\ll&\frac{\tau(f_2)M_E^3}{x^{1/2}\varphi(f)\log x}+x^{1/2}\frac{H(f)}{f}+x^{1/2}f\log(fxN_E)\\&+x^{5/8}\left(\frac{\tau(f_2)M_E^3\log^3(fxN_E)}{\varphi(f)\log x}\right)^{1/4}+x^{5/6}\left(\frac{H(f)\log^2(fxN_E)}{f}\right)^{1/3}.\end{aligned}$$

Note that writing $n=b^2c$, where b^2 is the largest square dividing n, yields

$$\sum_{\substack{1\leqslant k\leqslant n\\ n|k^2}}1=\sum_{1\leqslant k\leqslant b}1=b, \tag{19}$$

and it follows that $H(f)$ is multiplicative. For $k\geqslant 1$, we have

$$H(p^{2k})=2\sigma(p^{k-1})+p^k,\quad H(p^{2k-1})=2\sigma(p^{k-1}).$$

This gives the inequality in (8). In particular, $H(f)<f^2$ holds. Thus, the second term can be eliminated in the error term above, and we end up with (7). This completes the proof.

3.3 Positivity of density $\delta_E(f,a)$

Given a family

$$\mathcal{F}=\{L_p:\forall p,\mathbb{Q}\subseteq L_p\subseteq K_p,L_p/\mathbb{Q}\text{ is Galois}\},$$

we define the density associated with $\mathcal{F}$ by

$$\delta_{\mathcal{F}}(f,a):=\sum_{d\geqslant 1}\frac{\mu(d)\gamma_{a,f}(L_d)}{[L_d\mathbb{Q}(\zeta_f):\mathbb{Q}]},\qquad\text{with } L_d=\prod_{p|d}L_p,$$

where, for any number field L,

$$\gamma_{a,f}(L)=\begin{cases}1 & \text{if } \sigma_a\in\operatorname{Gal}\big(\mathbb{Q}(\zeta_f)/L\cap\mathbb{Q}(\zeta_f)\big),\\ 0 & \text{otherwise.}\end{cases}$$

In particular, $\delta_E(f,a)=\delta_{\mathcal{F}}(f,a)$ when $L_p=K_p$ for each p.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Lemma 12 *Let $\mathcal{F} = \{L_p\}_p$ be a family where $\mathbb{Q} \subsetneq L_p \subseteq K_p$ for each prime p. Then, $\delta_E(f,a) \geqslant \delta_{\mathcal{F}}(f,a)$. Furthermore, if $L_p = K_p$ for each $p \nmid M_E$, then*

$$\delta_{\mathcal{F}}(fg,a) = \frac{1}{\varphi(fg)} \prod_{\substack{p \nmid M_E \\ (p,f)\mid a-1}} \left(1 - \frac{\varphi(p,f)}{[K_p:\mathbb{Q}]}\right) \sum_{d \mid M_E} \frac{\mu(d)\gamma_{a,g}(L_d)}{[L_d : L_d \cap \mathbb{Q}(\zeta_g)]},$$

where $(f, M_E) = 1$, $g \mid M_E^{\infty}$, and $(a, fg) = 1$.

Remark 6 For any prime $p \nmid A(E)$, $[K_p:\mathbb{Q}] = (p^2-p)(p^2-1)$, so the product is absolutely convergent.

Proof For any finite subset $\mathcal{P}$ of primes, the set

$$\{p \leqslant x : p \nmid 2N_E, p \equiv a \bmod f, \forall q \in \mathcal{P}, p \text{ does not split completely in } K_q\}$$

contains

$$\{p \leqslant x : p \nmid 2N_E, p \equiv a \bmod f, \forall q \in \mathcal{P}, p \text{ does not split completely in } L_q\}.$$

Thus, proceeding as in the proof of [7, Lemma 6.1], the first assertion follows.

As for the latter, we write

$$\delta_{\mathcal{F}}(fg,a) = \sum_{d \mid M_E} \sum_{\substack{e \\ (e,M_E)=1}} \frac{\mu(de)\gamma_{a,fg}(L_{de})}{[L_d K_e \mathbb{Q}(\zeta_{fg}) : \mathbb{Q}]}.$$

First note that

$$\begin{aligned}[L_d K_e \mathbb{Q}(\zeta_{fg}) : \mathbb{Q}] &= \frac{[L_{de}:\mathbb{Q}][\mathbb{Q}(\zeta_{fg}):\mathbb{Q}]}{[L_{de} \cap \mathbb{Q}(\zeta_{fg}):\mathbb{Q}]} \\ &= \frac{[L_d:\mathbb{Q}][K_e:\mathbb{Q}][\mathbb{Q}(\zeta_{fg}):\mathbb{Q}]}{[L_d\mathbb{Q}(\zeta_g) \cap K_e\mathbb{Q}(\zeta_f):\mathbb{Q}][K_e \cap \mathbb{Q}(\zeta_f):\mathbb{Q}][L_d \cap \mathbb{Q}(\zeta_g):\mathbb{Q}]},\end{aligned}$$

and since numerators are the same, so are the denominators. Furthermore, since $(ef, dgM_E) = 1$, Lemma 8 gives

$$L_d\mathbb{Q}(\zeta_g) \cap K_e\mathbb{Q}(\zeta_f) \subseteq K_{[d,g]} \cap K_{[e,f]} = \mathbb{Q}.$$

Thus, we have

$$[L_{de} \cap \mathbb{Q}(\zeta_{fg}):\mathbb{Q}] = [K_e \cap \mathbb{Q}(\zeta_f):\mathbb{Q}][L_d \cap \mathbb{Q}(\zeta_g):\mathbb{Q}].$$

Since $K_e \cap \mathbb{Q}(\zeta_f)$ and $L_d \cap \mathbb{Q}(\zeta_g)$ are disjoint by Lemma 8, we see that

$$\gamma_{a,fg}(L_{de}) = 1 \Longleftrightarrow \gamma_{a,f}(K_e) = \gamma_{a,g}(L_d) = 1.$$

Finally, since $K_e \cap \mathbb{Q}(\zeta_f) = \mathbb{Q}(\zeta_{(e,f)})$ by Lemma 7, $\delta_{\mathcal{F}}(fg,a)$ is given by

$$\frac{1}{\varphi(fg)} \sum_{d \mid M_E} \frac{\mu(d)\gamma_{a,g}(L_d)[L_d \cap \mathbb{Q}(\zeta_g):\mathbb{Q}]}{[L_d:\mathbb{Q}]} \sum_{\substack{e \\ (e,M_E)=1 \\ (e,f)\mid a-1}} \frac{\mu(e)\varphi(e,f)}{[K_e:\mathbb{Q}]},$$

and the result follows by writing the last sum as a product. ∎

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Proof of Theorem 4 We choose $L_2 = K_2$, $L_p = \mathbb{Q}(\zeta_p)$ for $p \mid M_E/2$, $L_p = K_p$ for $(p, M_E) = 1$. By Lemma 12,

$$\delta_E(f,a) \geqslant \delta_{\mathcal{F}}(f,a) = \frac{1}{\varphi(f)} \prod_{\substack{p \nmid M_E \\ (p,f)\mid a-1}} \left(1 - \frac{\varphi(p,f)}{[K_p:\mathbb{Q}]}\right) \sum_{d \mid M_E} \frac{\mu(d)}{[L_d:\mathbb{Q}]}. \tag{20}$$

Splitting the sum over d, we obtain

$$\begin{aligned}
\sum_{d\mid M_E} \frac{\mu(d)}{[L_d:\mathbb{Q}]} &= \sum_{\substack{d\mid M_E \\ 2\nmid d}} \frac{\mu(d)}{[\mathbb{Q}(\zeta_d):\mathbb{Q}]} - \sum_{\substack{d\mid M_E/2 \\ 2\nmid d}} \frac{\mu(d)}{[K_2\mathbb{Q}(\zeta_d):\mathbb{Q}]} \\
&= \sum_{\substack{d\mid M_E \\ 2\nmid d}} \frac{\mu(d)}{\varphi(d)} \left(1 - \frac{[K_2 \cap \mathbb{Q}(\zeta_d):\mathbb{Q}]}{[K_2:\mathbb{Q}]}\right) \\
&= \left(1 - \frac{[K_2^{ab}:\mathbb{Q}]}{[K_2:\mathbb{Q}]}\right) \sum_{\substack{\mathfrak{f}_2 \mid d \mid M_E \\ 2\nmid d}} \frac{\mu(d)}{\varphi(d)} + \left(1 - \frac{1}{[K_2:\mathbb{Q}]}\right) \sum_{\substack{\mathfrak{f}_2 \nmid d \mid M_E \\ 2\nmid d}} \frac{\mu(d)}{\varphi(d)}.
\end{aligned}$$

Here, we have used the fact that $K_2 \cap \mathbb{Q}(\zeta_d) = K_2^{ab} \cap \mathbb{Q}(\zeta_d)$ is either $\mathbb{Q}$ or K_2^{ab}. The latter implies $K_2^{ab} \subseteq \mathbb{Q}(\zeta_{(\mathfrak{f}_2,d)})$, which holds if $\mathfrak{f}_2 = (\mathfrak{f}_2, d)$; that is, if $\mathfrak{f}_2 \mid d$. The converse trivially holds. If $\mathfrak{f}_2$ is not square-free, then

$$\sum_{d\mid M_E} \frac{\mu(d)}{[L_d:\mathbb{Q}]} = \left(1 - \frac{1}{[K_2:\mathbb{Q}]}\right) \prod_{2<p\mid M_E} \left(1 - \frac{1}{p-1}\right).$$

If $\mathfrak{f}_2$ is square-free, then by (13) and (14), it must be odd. Then, writing

$$\sum_{\substack{\mathfrak{f}_2 \nmid d \mid M_E \\ 2\nmid d}} \frac{\mu(d)}{\varphi(d)} = \sum_{\substack{d\mid M_E \\ 2\nmid d}} \frac{\mu(d)}{\varphi(d)} - \sum_{\substack{\mathfrak{f}_2 d \mid M_E \\ 2\nmid d \\ (d,\mathfrak{f}_2)=1}} \frac{\mu(d\mathfrak{f}_2)}{\varphi(d\mathfrak{f}_2)}$$

we derive

$$\sum_{d\mid M_E} \frac{\mu(d)}{[L_d:\mathbb{Q}]} = \left(1 - \frac{1}{[K_2:\mathbb{Q}]}\right) \sum_{\substack{d\mid M_E \\ 2\nmid d}} \frac{\mu(d)}{\varphi(d)} - \frac{[K_2^{ab}:\mathbb{Q}]-1}{[K_2:\mathbb{Q}]} \sum_{\substack{\mathfrak{f}_2 d \mid M_E \\ 2\nmid d \\ (d,\mathfrak{f}_2)=1}} \frac{\mu(d\mathfrak{f}_2)}{\varphi(d\mathfrak{f}_2)}.$$

The second sum on the right side can be written as

$$\begin{aligned}
\sum_{\substack{\mathfrak{f}_2 d \mid M_E \\ 2\nmid d \\ (d,\mathfrak{f}_2)=1}} \frac{\mu(d\mathfrak{f}_2)}{\varphi(d\mathfrak{f}_2)} &= \frac{\mu(\mathfrak{f}_2)}{\varphi(\mathfrak{f}_2)} \sum_{\substack{d\mid M_E/\mathfrak{f}_2 \\ 2\nmid d}} \frac{\mu(d)}{\varphi(d)} = \frac{\mu(\mathfrak{f}_2)}{\varphi(\mathfrak{f}_2)} \prod_{2<p\mid M_E/\mathfrak{f}_2} \left(1 - \frac{1}{p-1}\right) \\
&= \mu(\mathfrak{f}_2) \frac{\prod_{2<p\mid M_E} \left(1 - \frac{1}{p-1}\right)}{\varphi(\mathfrak{f}_2) \prod_{p\mid \mathfrak{f}_2} \left(1 - \frac{1}{p-1}\right)} = \frac{\mu(\mathfrak{f}_2)}{\prod_{2<p\mid \mathfrak{f}_2}(p-2)} \sum_{\substack{d\mid M_E \\ 2\nmid d}} \frac{\mu(d)}{\varphi(d)},
\end{aligned}$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

where we have used the fact that M_E and $\mathfrak{f}_2$ are square-free (and, $\mathfrak{f}_2$ is odd). Inserting this expression back into the previous equation, we obtain

$$\sum_{d\mid M_E}\frac{\mu(d)}{[L_d:\mathbb{Q}]}=\frac{1}{[K_2:\mathbb{Q}]}\left([K_2:\mathbb{Q}]-1-\frac{\mu(\mathfrak{f}_2)([K_2^{ab}:\mathbb{Q}]-1)}{\prod_{2<p\mid\mathfrak{f}_2}(p-2)}\right)\sum_{\substack{d\mid M_E\\ 2\nmid d}}\frac{\mu(d)}{\varphi(d)}.$$

Combining this identity with (20), we conclude that

$$\delta_{\mathcal{F}}(f,a)=\frac{1}{\varphi(f)}\prod_{\substack{p\nmid M_E\\ (p,f)\mid a-1}}\left(1-\frac{\varphi(p,f)}{[K_p:\mathbb{Q}]}\right)\prod_{2<p\mid M_E}\left(1-\frac{1}{p-1}\right)$$
$$\cdot\frac{1}{[K_2:\mathbb{Q}]}\left([K_2:\mathbb{Q}]-1-\frac{\mu(\mathfrak{f}_2)([K_2^{ab}:\mathbb{Q}]-1)}{\prod_{2<p\mid\mathfrak{f}_2}(p-2)}\right)>0,$$

and this gives (9). ∎

4 Proofs of Theorems 5 and 6

Throughout this section, we assume that E is an elliptic curve over $\mathbb{Q}$ with complex multiplication.

4.1 Proof of Theorem 5

We proceed as in the proof of Theorem 3. Everything up to equation (16) applies to the CM case. We start with the estimate of Σ_1 given by (15). By [7, Proposition 3.8], $[K_d:\mathbb{Q}]\gg\varphi(d)^2$. Thus, using Lemma 11, we obtain

$$\sum_{d>y}\frac{\mu^2(d)}{[K_d\mathbb{Q}(\zeta_f):\mathbb{Q}]}\ll\sum_{d>y}\frac{1}{\varphi(d)^2}\ll y^{-1},$$

which yields

$$\Sigma_1=\mathrm{Li}(x)\delta_E(f,a)+O\left(\frac{x}{y\log x}+yx^{1/2}\log(fxN_E)\right). \tag{21}$$

Next, we deal with

$$\Sigma_2=\sum_{y<d\leqslant\sqrt{x}+1}\mu(d)\pi_{E,d}(x;f,a).$$

If p is a prime counted in $\pi_{E,d}(x;f,a)$, then p splits completely in K_d and thus in $\mathbb{Q}(\zeta_d)$ since $\mathbb{Q}(\zeta_d)\subseteq K_d$. Thus, by Lemma 5, d^2 divides $|\widetilde{E}(\mathbb{F}_p)|$ and also $d\mid p-1$. Hence, we note that $|\widetilde{E}(\mathbb{F}_p)|\neq p+1$, since otherwise, $d\mid p+1-(p-1)=2$, which is impossible since $d>y>2$. This means no prime except possibly $p=3$ that splits completely in K_d can have supersingular reduction. Therefore, it follows from [5, Lemma 2.2] that $p\neq 3$ splits completely in K_d if and only if $\pi_p-1\in d\mathfrak{O}_K$. Here, π_p is one of the complex roots of the polynomial $X^2-(p+1-|\widetilde{E}(\mathbb{F}_p)|)X+p$. Note that $N_{K/\mathbb{Q}}(\pi_p)=\pi_p\overline{\pi_p}=p$. Thus, we deduce that

$$\pi_{E,d}(x;f,a)\leqslant 1+\left|\{3\neq p\leqslant x: p\nmid N_E, p\equiv a \bmod f, \pi_p\equiv 1 \bmod d\mathfrak{O}_K\}\right|.$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Since K is an imaginary quadratic extension of $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{-D})$ for some square-free positive integer D, and $\mathfrak{O}_K = \mathbb{Z}[\omega_D]$, where

$$\omega_D = \begin{cases} \sqrt{-D} & \text{if } D \equiv 1, 2 \bmod 4 \\ \frac{1}{2}(1+\sqrt{-D}) & \text{if } D \equiv 3 \bmod 4. \end{cases}$$

Thus, any $\alpha \in \mathfrak{O}_K$ with $\alpha \equiv 1 \bmod d\mathfrak{O}_K$ can be written as

$$\alpha = \begin{cases} bd + 1 + cd\sqrt{-D} & \text{if } D \equiv 1, 2 \bmod 4 \\ \frac{1}{2}\left(bd + 2 + cd\sqrt{-D}\right),\ b \equiv c \bmod 2 & \text{if } D \equiv 3 \bmod 4, \end{cases}$$

for some integers b and c, and therefore has its norm equal to

$$N_{K/\mathbb{Q}}(\alpha) = \begin{cases} (bd+1)^2 + D(cd)^2 & \text{if } D \equiv 1, 2 \bmod 4 \\ \frac{1}{4}\left((bd+2)^2 + D(cd)^2\right) & \text{if } D \equiv 3 \bmod 4. \end{cases}$$

Note that

$$N_{K/\mathbb{Q}}(\pi_p) \equiv a \bmod f \iff 4N_{K/\mathbb{Q}}(\pi_p) \equiv 4a \bmod (\gcd(f,2)^2 f).$$

We shall use this equivalent form only when $D \equiv 3 \bmod 4$ since, in this case, $4N_{K/\mathbb{Q}}(\alpha)$ becomes a quadratic form in b, c, d with *integer* coefficients. Using this observation we deduce that $\pi_{E,d}(x; f, a)$ is at most

$$|\{(b,c) \in \mathbb{Z}^2 : F(b,d,c) \equiv a' \bmod f', F(b,d,c) \leqslant 4x, 2 \mid b - c \text{ if } D \equiv 3 \bmod 4\}|,$$

where

$$F(b,d,c) = (bd+1)^2 + D(cd)^2, a' = a, f' = f \qquad \text{if } D \equiv 1, 2 \bmod 4$$
$$F(b,d,c) = (bd+2)^2 + D(cd)^2, a' = 4a, f' = (f,2)^2 f \qquad \text{if } D \equiv 3 \bmod 4.$$

Now, summing over $d \in (y, \sqrt{x}+1]$ leads to the bound

$$\Sigma_2 \leqslant \sum_{\alpha,\beta,\gamma \bmod f'} \sum_{\substack{y<d\leqslant\sqrt{x}+1 \\ d\equiv\beta \bmod f'}} \sum_{\substack{b\equiv\alpha, c\equiv\gamma \bmod f' \\ F(b,d,c)\leqslant 4x \\ F(b,d,c)\equiv a' \bmod f' \\ (b\equiv c \bmod 2)}} 1$$
$$\leqslant \sum_{\substack{\alpha,\beta,\gamma \bmod f' \\ F(\alpha,\beta,\gamma)\equiv a' \bmod f' \\ (\alpha\equiv\gamma \bmod 2)}} \sum_{\substack{y<d\leqslant\sqrt{x}+1 \\ d\equiv\beta \bmod f'}} \sum_{\substack{|b|\leqslant\frac{2\sqrt{x}+2}{d} \\ b\equiv\alpha \bmod f'}} \sum_{\substack{|c|\leqslant\frac{2\sqrt{x}}{d\sqrt{D}} \\ c\equiv\gamma \bmod f'}} 1,$$

with the parity condition required only when $D \equiv 3 \bmod 4$. Note that the second inequality follows from the fact that

$$F(b,d,c) \equiv F(b \bmod f', d \bmod f', c \bmod f') \bmod f'$$

since $F(b,d,c)$ has integer coefficients.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

For $y \in [2f, \sqrt{x}]$, and *uniformly* for any α, β, γ modulo f,

$$\sum_{\substack{y<d\leqslant\sqrt{x}+1\\ d\equiv\beta \bmod f'}} \sum_{\substack{|b|\leqslant\frac{2\sqrt{x}+2}{d}\\ b\equiv\alpha \bmod f'}} \sum_{\substack{|c|\leqslant\frac{2\sqrt{x}}{d\sqrt{D}}\\ c\equiv\gamma \bmod f'}} 1 \ll \sum_{\substack{y<d\leqslant\sqrt{x}+1\\ d\equiv\beta \bmod f'}} \left(1+\frac{\sqrt{x}}{df}\right)\left(1+\frac{\sqrt{x}}{df\sqrt{D}}\right)$$
$$\ll \sum_{\substack{y<d\leqslant\sqrt{x}+1\\ d\equiv\beta \bmod f'}} \left(1+\frac{\sqrt{x}}{df}+\frac{\sqrt{x}}{df\sqrt{D}}+\frac{x}{d^2f^2\sqrt{D}}\right)$$
$$\ll_D \frac{\sqrt{x}}{f}+\frac{\sqrt{x}\log x}{f^2}+\frac{x}{yf^3}.$$

Note that the implied constant depends on K. Since $E/\mathbb{Q}$ has CM by $\mathfrak{O}_K$, then K is one of the nine imaginary quadratic fields of class number one, and so the implied constant above can be replaced by an absolute constant. Inserting this estimate into the previous estimate of Σ_2, we deduce that

$$\Sigma_2 \ll \left(\frac{\sqrt{x}}{f}+\frac{\sqrt{x}\log x}{f^2}+\frac{x}{yf^3}\right) G_D(a,f), \tag{22}$$

where $G_D(a,f)$ is the cardinality of the set

$$\{(\alpha,\beta,\gamma) \in (\mathbb{Z}/f'\mathbb{Z})^3 : F(\alpha,\beta,\gamma) \equiv a' \bmod f', 2 \mid \alpha-\gamma \text{ if } D \equiv 3 \bmod 4\}. \tag{23}$$

Combining (21) and (22), we obtain the bound

$$\pi_E(x;f,a) - \delta_E(a,f)\,\mathrm{Li}(x) \ll x^{1/2}y\log(fxN_E) + \frac{x}{y\log x} + \frac{x}{yf^3}G_D(a,f)$$
$$+ x^{1/2}\left(\frac{1}{f}+\frac{\log x}{f^2}\right) G_D(a,f).$$

Recalling that $2f \leqslant y \leqslant \sqrt{x}$ and using [10, Lemma 2.4] yields the error

$$E(x) \ll x^{1/2} f\log(fxN_E) + x^{1/2}\frac{G_D(a,f)}{f^3} + x^{3/4}\left(\frac{\log(fxN_E)}{\log x}\right)^{1/2}$$
$$+ x^{3/4}\left(\frac{\log(fxN_E)G_D(a,f)}{f^3}\right)^{1/2} + x^{1/2}\left(\frac{1}{f}+\frac{\log x}{f^2}\right) G_D(a,f).$$

Note that the second term can be eliminated since it is already smaller than the fifth term, and this gives the error in (10).

To complete the proof of Theorem 5, we need to estimate $G_D(a,f)$. Since G_D is multiplicative in the second variable, it is enough to estimate $G_D(a,p^k)$ for primes p with $p^k \| f'$. Note that $p \nmid a$ since $(a,f)=1$.

Assume first that $D \equiv 1, 2 \bmod 4$. Recall, in this case, $f' = f$ and $a' = a$. Put

$$A_i = \{(\alpha,\beta,\gamma) : p^i \| a - D(\beta\gamma)^2, F(\alpha,\beta,\gamma) \equiv a \bmod p^k\}.$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Note that for any triple in A_i with $i \geqslant 1$, $p \nmid D\beta\gamma$. Also, if $i \geqslant k$, then for $\varphi(p^k)$ possible choices of $1 \leqslant \gamma \leqslant p^k$, there are at most $\eta(p^k)$ choices for β satisfying

$$D(\beta\gamma)^2 \equiv a \bmod p^k,$$

where $\eta(p^n) = 2$ if p is odd, or $p = 2$ and $n = 1, 2$, and it equals 4 otherwise. Furthermore,

$$(\alpha\beta + 1)^2 \equiv a - D(\beta\gamma)^2 \equiv 0 \bmod p^k$$

implies

$$\alpha\beta \equiv -1 \bmod p^{\lceil k/2 \rceil},$$

and there is unique α modulo $p^{\lceil k/2 \rceil}$ satisfying this congruence, which gives $p^{k-\lceil k/2 \rceil}$ choices for α modulo p^k. Hence,

$$\sum_{i \geqslant k} |A_i| \leqslant \eta(p^k) p^{k-\lceil k/2 \rceil} \varphi(p^k). \tag{24}$$

Next, assume that $p \nmid a - D(\beta\gamma)^2$. Then,

$$X^2 \equiv a - D(\beta\gamma)^2 \bmod p^k$$

has at most $\eta(p^k)$ solutions. If $X_0 = X_0(\beta, \gamma)$ is one of these solutions, and $p^i \| \beta$ with $0 \leqslant i \leqslant k$, then there are $\gcd(\beta, p^k) = p^i$ values of $\alpha \in [1, p^k]$ satisfying

$$\alpha\beta \equiv X_0 - 1 \bmod p^k,$$

provided $p^i \mid X_0 - 1$. Since there are $\varphi(p^{k-i})$ values of β modulo p^k with $p^i \| \beta$, and at most p^k values of γ, we get

$$|A_0| \leqslant \eta(p^k) p^{2k} + \sum_{0 \leqslant i \leqslant k-1} \eta(p^k) p^k \varphi(p^{k-i}) p^i = \eta(p^k) p^{2k} \left(k(1 - 1/p) + 1\right). \tag{25}$$

Finally, assume $1 \leqslant i \leqslant k - 1$ and $k > 2$ (note for $k \leqslant 2$, this part will not contribute as will be seen below). In this case, we have

$$D(\beta\gamma)^2 \equiv a \bmod p^i.$$

For $\varphi(p^k)$ choices of γ, there are at most $\eta(p^i) p^{k-i}$ choices for β modulo p^k. For these values of γ and β,

$$X^2 \equiv a - D(\beta\gamma)^2 \bmod p^k \tag{26}$$

implies $p^{\lceil i/2 \rceil} \mid X$, which then yields $p^{i+1} \mid a - D(\beta\gamma)^2$ if i is odd. Thus, (26) has no solutions for odd $i < k$. Otherwise, writing $X = p^{i/2} Y$ with $1 \leqslant Y \leqslant p^{k-i/2}$ gives

$$Y^2 \equiv \frac{a - D(\beta\gamma)^2}{p^i} \bmod p^{k-i}.$$

Since the right side is now coprime to p, there are at most $\eta(p^{k-i})$ solutions for Y modulo p^{k-i}, which gives $\eta(p^{k-i}) p^{i/2}$ choices for X. If X_0 is one of these possible solutions, then

$$\alpha\beta + 1 \equiv X_0 \bmod p^k$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

has exactly one solution for α. Hence,

$$\begin{aligned}\sum_{1\leqslant i\leqslant k-1}|A_i| &\leqslant \sum_{\substack{1\leqslant i\leqslant k-1\\ 2|i}}\varphi(p^k)\eta(p^i)\eta(p^{k-i})p^{k-i}p^{i/2}\\ &< \eta(p^k)^2\varphi(p^k)\sum_{1\leqslant i\leqslant\lfloor(k-1)/2\rfloor}p^{k-i} < \eta(p^k)^2p^{2k-1}.\end{aligned}\tag{27}$$

Combining (24), (25), and (27), we conclude that

$$\begin{aligned}G_D(a,p^k) &\leqslant \eta(p^k)p^{2k}\Big(\min\{1,(k-2)(k-1)\}\eta(p^k)p^{-1}\\ &\quad + p^{-\lceil k/2\rceil}(1-1/p)+k(1-1/p)+1\Big) < 2k\eta(p^k)p^{2k}.\end{aligned}\tag{28}$$

Next, assume $D\equiv 3 \bmod 4$. We shall count the solutions to

$$F(\alpha,\beta,\gamma) = (\alpha\beta+2)^2 + D(\beta\gamma)^2 \equiv 4a \bmod p^k.$$

Assume first that p is odd. Since $p\nmid 4a$ in this case, the proof in the previous case goes through and gives the same upper bound in (28) for $G_D(a,p^k)$.

Next, assume $2^k\| f$. Then, we consider $F\equiv 4a \bmod 2^{k+2}$ with $\alpha\equiv\gamma \bmod 2$. If γ is even, then so is α and we have to count the solutions to

$$(\alpha\beta+1)^2 + D(\beta\gamma)^2 \equiv a \bmod 2^k,$$

where $\alpha,\gamma\in[1,2^{k+1}]$ and $\beta\in[1,2^{k+2}]$. When all variables lie in $[1,2^k]$, there are at most $2k\eta(2^k)2^{2k}$ triples by (28). Lifting variables, we get at most $32k\eta(2^k)2^{2k}$ solutions.

When α and γ are odd and β is even, we end up with the congruence

$$(\alpha\beta+1)^2 + D(\beta\gamma)^2 \equiv a \bmod 2^k,$$

where $\alpha,\gamma\in[1,2^{k+2}]$ are odd, while $\beta\in[1,2^{k+1}]$. If β is odd,

$$\gamma^2 \equiv D^{-1}\beta^{-2}\left(a-(\alpha\beta+1)^2\right) \bmod 2^k$$

has at most $\eta(2^k)$ solutions for γ since right hand is odd, and these can be lifted to $4\eta(2^k)$ solutions mod 2^{k+2}. Hence, there are at most $4\eta(2^k)2^{2k+1}$ triples modulo 2^{k+2}.

If $2^i\|\beta$ for $1\leqslant i\leqslant k$, then

$$X^2 \equiv a - D(\beta\gamma)^2 \bmod 2^k$$

has at most $\eta(2^k)$ solutions. If X_0 is one of the possible solutions, then

$$\alpha\beta \equiv X_0 - 1 \bmod 2^k$$

has at most 2^{i+2} solutions for α modulo 2^{k+2}. There are 2^{k+1-i} values of β modulo 2^{k+2} with $2^i\mid\beta$, and 2^{k+1} odd values of $\gamma\in[1,2^{k+2}]$. Hence, we get at most

$$4\eta(2^k)2^{2k+1} + \sum_{1\leqslant i\leqslant k}\eta(2^k)2^{i+2+k+1-i+k+1} = (8+16k)\eta(2^k)2^{2k}$$

solutions.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Finally, if all the variables are odd, then we have

$$y^2 \equiv D^{-1}\beta^{-2}\left(4a-(\alpha\beta+2)^2\right) \bmod 2^{k+2}.$$

Given odd $\alpha,\beta \in [1,2^{k+2}]$, there are at most $\eta(2^{k+2})$ solutions for $y \in [1,2^{k+2}]$ since the right hand side is odd. Hence, we obtain at most $\eta(2^{k+2})2^{2k+2}$ triples. Combining all the estimates, we deduce that

$$G_D(a,2^k) \leqslant \eta(2^k)2^{2k}(48k+16) < \frac{49}{2}\cdot 2k\eta(2^k)2^{2k}.$$

Multiplying the bounds for $G_D(a,p^k)$ over the prime powers dividing f, we obtain the bound in (11). This completes the proof.

4.2 Proof of Theorem 6

Recall that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathfrak{O}_K$, where $K=\mathbb{Q}(\sqrt{-D})$. By [28, Lemma 6], for all $p \geqslant 3$, $K \subset K_p$. Suppose first that $K_2 \cap K = K_2^{ab} \cap K = \mathbb{Q}$ and that

$$\gamma_{a,f}(K_2K) = \gamma_{a,f}(K_2)\gamma_{a,f}(K). \tag{29}$$

Note that

$$\begin{aligned}[K_2\cap\mathbb{Q}(\zeta_f):\mathbb{Q}][K\cap\mathbb{Q}(\zeta_f):\mathbb{Q}] &= [(K_2\cap\mathbb{Q}(\zeta_f))(K\cap\mathbb{Q}(\zeta_f)):\mathbb{Q}]\\ &\leqslant [K_2K\cap\mathbb{Q}(\zeta_f):\mathbb{Q}]\end{aligned}$$

since

$$(K_2\cap\mathbb{Q}(\zeta_f))(K\cap\mathbb{Q}(\zeta_f)) \subseteq K_2K\cap\mathbb{Q}(\zeta_f).$$

Then, taking $\mathcal{F}=\{K_2,K\}$ and using [7, Lemma 6.1] yields

$$\begin{aligned}\delta_{\mathcal{F}}(a,f) &= \frac{1}{\varphi(f)} - \frac{\gamma_{a,f}(K_2)}{[K_2\mathbb{Q}(\zeta_f):\mathbb{Q}]} - \frac{\gamma_{a,f}(K)}{[K\mathbb{Q}(\zeta_f):\mathbb{Q}]} + \frac{\gamma_{a,f}(K_2)\gamma_{a,f}(K)}{[K_2K\mathbb{Q}(\zeta_f):\mathbb{Q}]}\\ &\geqslant \frac{1}{\varphi(f)}\left(1-\frac{\gamma_{a,f}(K_2)[K_2\cap\mathbb{Q}(\zeta_f):\mathbb{Q}]}{[K_2:\mathbb{Q}]}\right)\left(1-\frac{\gamma_{a,f}(K)[K\cap\mathbb{Q}(\zeta_f):\mathbb{Q}]}{2}\right).\end{aligned}$$

Thus, $\delta_{\mathcal{F}}(a,f)>0$ if $K_2 \subsetneq \mathbb{Q}(\zeta_f)$ or $\gamma_{a,f}(K_2)=0$, and $K \subsetneq \mathbb{Q}(\zeta_f)$ or $\gamma_{a,f}(K)=0$, provided (29) holds and $K_2\cap K=\mathbb{Q}$.

If $K_2^{ab}=K$, then taking $\mathcal{F}=\{K_2\}$ yields

$$\delta_{\mathcal{F}}(a,f) = \frac{1}{\varphi(f)}\left(1-\frac{\gamma_{a,f}(K_2)[K_2\cap\mathbb{Q}(\zeta_f):\mathbb{Q}]}{[K_2:\mathbb{Q}]}\right).$$

We conclude again that $\delta_{\mathcal{F}}>0$ if $K_2 \subsetneq \mathbb{Q}(\zeta_f)$ or $\gamma_{a,f}(K_2)=0$.

Appendix A Intersections of division fields

By Ernst Kani

Let E/K be an elliptic curve defined over a number field K. Recall that for each integer $m \geqslant 1$, we have a natural representation

$$\rho_m = \rho_{E/K,m} : G_K = \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(m) := \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

The fixed field of its kernel is the m-division field $K(E[m]) = \overline{K}^{\ker(\rho_m)}$, so

$$\mathrm{Gal}(K(E[m])/K) \simeq G_m := \mathrm{Im}(\rho_m).$$

Put

$$S_{E/K} = \{p \text{ prime} : G_p \neq \mathrm{GL}(p)\}.$$

By Serre [31], $S_{E/K}$ is finite if (and only if) E is non-CM, which we assume henceforth. In this case, the *Serre constant* of E/K is defined as the number

$$A_{E/K} = 30 \prod_{\substack{p>5 \\ p\in S_{E/K}}} p.$$

The main aim of this appendix is to prove the following result.

Theorem 1 *Let $E/\mathbb{Q}$ be a non-CM elliptic curve, and let $m, n \geqslant 1$ be integers with $(m, nN_E A_{E/\mathbb{Q}}) = 1$, where N_E denotes the conductor of $E/\mathbb{Q}$. Then,*

$$\mathbb{Q}(E[m]) \cap \mathbb{Q}(E[n]) = \mathbb{Q}.$$

Note that we cannot drop the condition of Theorem 1 that $(m, N_E) = 1$, even if m is a prime; cf. Proposition 2 and Example 1 below.

As we shall see presently, Theorem 1 follows from the following result which is valid for elliptic curves over an arbitrary number field K. This, in turn, follows easily from the results of the Appendix of [6].

Theorem 2 *Let E/K be a non-CM elliptic curve, and let $m, n \geqslant 1$ be integers with $(m, nA_{E/K}) = 1$. Then, $K(E[m]) \cap K(E[n])$ is an abelian extension of K.*

Proof of Theorem 1 (using Theorem 2) Put $L = \mathbb{Q}(E[n]) \cap \mathbb{Q}(E[m])$. By Theorem 2, we know that $L/\mathbb{Q}$ is an abelian extension with $L \subset \mathbb{Q}(E[m])$. Since m is coprime to $A_{E/\mathbb{Q}}$, we know that $\mathbb{Q}(\zeta_m)$ is the maximal abelian extension of $\mathbb{Q}$ in $\mathbb{Q}(E[m])$; cf. [6]. Thus, $L \subset \mathbb{Q}(\zeta_m)$, and so $L/\mathbb{Q}$ is ramified only at the primes $p \mid m$. On the other hand, since $L \subset \mathbb{Q}(E[n])$, we see by the criterion of Néron–Ogg–Shafarevič that $L/\mathbb{Q}$ is ramified only at primes $p \mid nN_E$; cf. Silverman [33, Theorem VII.7.1]. Thus, since $(m, nN_E) = 1$, it follows that $L/\mathbb{Q}$ is everywhere unramified and so $L = \mathbb{Q}$, as claimed. ∎

To prove Theorem 2, we will use some basic facts about the nonabelian composition factors of a subgroup G of $\mathrm{GL}(m)$ which were presented in the Appendix of [6]. For this, let $\mathcal{N}(G)$ denote the set of (isomorphism classes) of nonabelian composition factors of a group G, and put

$$\mathrm{Occ}(G) = \bigcup_{H\leqslant G} \mathcal{N}(H).$$

Proposition 1 *(a) For any integer $m > 1$, we have that*

$$\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) = \bigcup_{p\mid m} \mathrm{Occ}(\mathrm{PSL}_2(p)),$$

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

where $\mathrm{PSL}_2(p) = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\{\pm 1\}$, *if* p *is prime. Moreover,* $\mathrm{Occ}(\mathrm{PSL}_2(p)) = \varnothing$ *when* $p = 2$ *or* 3, *whereas for* $p \geqslant 5$, *we have*

$$\{\mathrm{PSL}_2(p)\} \subseteq \mathrm{Occ}(\mathrm{PSL}_2(p)) \subseteq \{A_5, \mathrm{PSL}_2(p)\}.$$

(b) If $G \leqslant \mathrm{GL}(m)$, *where* $(m, 30) = 1$, *then*

$$G \geqslant \mathrm{SL}(m) := \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \iff \forall\, p \mid m, \mathrm{PSL}_2(p) \in \mathrm{Occ}(G).$$

If this is the case, then $G/\mathrm{SL}(m)$ *is abelian and* $\mathcal{N}(G) = \{\mathrm{PSL}_2(p) : p|m\}$.

Proof (a) This is Lemma 10 of the Appendix of [6].

(b) The first assertion is Theorem 2(b) of the same Appendix. To prove the others, note that $G/\mathrm{SL}(m) \leqslant \mathrm{GL}(m)/\mathrm{SL}(m) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ is abelian, so

$$\mathcal{N}(G) = \mathcal{N}(\mathrm{SL}(m)) = \bigcup_{p|m} \mathcal{N}\left(\mathrm{SL}(p^{v_p(m)})\right),$$

the latter because $\mathrm{SL}(m) = \prod_{p|m} \mathrm{SL}(p^{v_p(m)})$. Since the kernel of the homomorphism $\mathrm{SL}(p^r) \to \mathrm{SL}(p)$ is a p-group, we have that

$$\mathcal{N}(\mathrm{SL}(p^r)) = \mathcal{N}(\mathrm{SL}(p)) = \{\mathrm{PSL}_2(p)\},$$

and so the last assertion follows. ∎

Corollary 1 *If* $(m, A_{E/K}) = 1$, *then* $\mathrm{SL}(m) \leqslant G_m$. *Thus, if* L/K *is a solvable extension with* $L \subset K(E[m])$, *then* L/K *is abelian.*

Proof Since $(m, A_{E/K}) = 1$, we have that $G_p = \mathrm{GL}(p)$ for all $p \mid m$, and so $\mathrm{PSL}_2(p) \in \mathrm{Occ}(\mathrm{GL}(p)) \subset \mathrm{Occ}(G_m)$, the latter because G_p is a quotient of G_m, $\forall\, p \mid m$. Thus, $\mathrm{SL}(m) \leqslant G_m$ by Proposition 1 because $(m, 30) = 1$.

To prove the second assertion, let

$$H := \mathrm{Gal}(K(E[m])/L) \trianglelefteq G := \mathrm{Gal}(K(E[m])/K).$$

Since $G/H \simeq \mathrm{Gal}(L/K)$ is solvable and $G \simeq G_m$, we have that $\mathrm{Occ}(H) = \mathrm{Occ}(G_m)$. Thus, by Proposition 1(b), there exists $H_1 \leqslant H$ with $H_1 \simeq \mathrm{SL}(m)$, and then G/H_1 is abelian. Thus, the quotient G/H of G/H_1 is also abelian. ∎

Proof of Theorem 2 Put $L = K(E[n]) \cap K(E[m])$ and $H = \mathrm{Gal}(L/K)$. Then H is a quotient of $\mathrm{Gal}(K([E[n])/K) \simeq G_n \leqslant \mathrm{GL}(n)$ and also of $\mathrm{Gal}(K(E[m])/K) \simeq G_m$, so

$$\begin{aligned}\mathcal{N}(H) &\subset \mathrm{Occ}(\mathrm{GL}(n)) \cap \mathcal{N}(G_m)\\ &\subset (\{A_5\} \cup \{\mathrm{PSL}_2(p) : p \mid n, p \geqslant 5\}) \cap \{\mathrm{PSL}_2(p) : p \mid m\},\end{aligned}$$

where the last inclusion follows from both parts of Proposition 1 together with Corollary 1. Since $(n, m) = 1$ and $5 \nmid m$, we see that this intersection is empty because $\mathrm{PSL}(p) \simeq A_5 \Leftrightarrow p = 5$ and $\mathrm{PSL}(p) \simeq \mathrm{PSL}(q) \Leftrightarrow p = q$; cf. [6]. Thus, $\mathcal{N}(H) = \varnothing$, which means that H is solvable. Since $L \subset K(E[m])$, we have by Corollary 1 that L/K is abelian. ∎

We now show that the condition $(m, N_E) = 1$ in Theorem 1 cannot be dropped. This follows from the following result together with Example 1 which shows that there exist elliptic curves $E/\mathbb{Q}$ satisfying the hypotheses of Proposition 2.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

Proposition 2 *Let $E/\mathbb{Q}$ be an elliptic curve with prime conductor $N_E = p$ with $p \equiv 3 \bmod 4$. Suppose that the discriminant of some integral model of $E/\mathbb{Q}$ satisfies $\Delta_E < 0$ and $v_p(\Delta_E) \equiv 1 \bmod 2$. Then, $(p, A_{E/\mathbb{Q}}) = 1$, but*

$$\mathbb{Q}(E[p]) \cap \mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-p}).$$

Proof Since there are no elliptic curves of conductor $N_E < 11$, the hypothesis implies that $p \geqslant 11$. Moreover, since N_E is squarefree, $E/\mathbb{Q}$ is semi-stable (and non-CM), so by Corollary 1 of Section 5.4 of Serre [31], we know that $p \notin S_{E/\mathbb{Q}}$ because $p > (\sqrt{2}+1)^2 \approx 5.8$. Thus $p \nmid A_{E/\mathbb{Q}}$.

For any integral model of $E/\mathbb{Q}$, there exists an integer $d \geqslant 1$ such that

$$\Delta_E = d^{12}\Delta_{E/\mathbb{Q}}^{min},$$

where $\Delta_{E/\mathbb{Q}}^{min}$ denotes the minimal discriminant of $E/\mathbb{Q}$. Thus, the given conditions on Δ_E do not depend on the choice of the model.

Since N_E and $\Delta_{E/\mathbb{Q}}^{min}$ have the same prime divisors, we see that $\Delta_{E/\mathbb{Q}}^{min} = -p^k$, with k odd, so $\Delta_E = -d^{12}p^k$. By taking an integral model of the form $Y^2 = f(X)$, where $f(X)$ is a cubic, we see that $\mathbb{Q}(E[2])$ is the splitting field of $f(X)$. Since $\Delta_E = 16\,\mathrm{disc}(f)$, it follows from field theory that $\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(E[2])$. Moreover, $\mathbb{Q}(\sqrt{-p})$ is the maximal abelian extension of $\mathbb{Q}$ in $\mathbb{Q}(E[2])$. Indeed, if $f(X)$ is irreducible, then this is clear by field theory, and otherwise we have that $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-p})$ is abelian.

On the other hand, the condition $p \equiv 3 \bmod 4$ implies (cf. [22, Theorem V1.3.3]) that

$$\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(E[p]).$$

This proves the inclusion $\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(E[p]) \cap \mathbb{Q}(E[2])$. Since the latter intersection is abelian by Theorem 2 and is contained in $\mathbb{Q}(E[2])$, it follows from what was said above that it is contained in $\mathbb{Q}(\sqrt{-p})$, and so the assertion follows. ∎

Example 1 Consider the following elliptic curves $E_i/\mathbb{Q}$ defined by the equations

$$E_1 : Y^2 = X^3 - 432X + 8208,$$
$$E_2 : Y^2 = X^3 - 432X + 15120$$
$$E_3 : Y^2 = X^3 - 997056X - 383201712.$$

The discriminant of E_i is $\Delta_{E_i} = -6^{12}p_i$, for $i = 1, 2, 3$, where $p_1 = 11$, $p_2 = 43$ and $p_3 = 19$. Furthermore, $N_{E_i} = p_i \equiv 3 \bmod 4$, and so $E_i/\mathbb{Q}$ satisfies the hypotheses of Proposition 2 with $p = p_i$, for $i = 1, 2, 3$.

Acknowledgment We would like to thank Ram Murty for helpful discussions, and suggesting the use of linear sieve that plays a significant role and makes an important contribution to the results we obtained. We thank Ernst Kani for sharing his notes given in appendix that are used in several parts of the paper and play an essential role in the proof of some of the theorems. We also thank the referees for carefully reading the paper and their helpful suggestions that we believe improved the organization of this paper.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

References

[1] A. Akbary and V. K. Murty, *An analogue of the Siegel-Walfisz theorem for the cyclicity of CM elliptic curves mod p*. Indian J. Pure Appl. Math. **41**(2010), no. 1, 25–37.
[2] J. B. Avila, *Galois representations of elliptic curves and abelian entanglements*, Doctoral thesis, Leiden University, 2015.
[3] I. Borosh, C. J. Moreno, and H. Porta, *Elliptic curves over finite fields. II*. Math. Comput. **29**(1975), 951–964.
[4] A. C. Cojocaru, *On the cyclicity of the group of F_p-rational points of non-CM elliptic curves*. J. Number Theory **96**(2002), 335–350.
[5] A. C. Cojocaru, *Cyclicity of CM elliptic curves modulo p*. Trans. Amer. Math. Soc. **355**(2003), no. 7, 2651–2662.
[6] A. C. Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*. With an appendix by E. Kani. Canad. Math. Bull. **48**(2005), no. 1, 16–31.
[7] A. C. Cojocaru and M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*. Math. Ann. **330**(2004), no. 3, 601–625.
[8] E. Fouvry and H. Iwaniec, *Primes in arithmetic progressions*. Acta Arith. **42**(1983), no. 2, 197–218.
[9] E. González-Jiménez and Á. Lozano-Robledo, *Elliptic curves with Abelian division fields*. Math. Z. **283**(2016), 835–859.
[10] S. W. Graham and G. Van der Kolesnik, *Corput's method of exponential sums*. London Mathematical Society Lecture Note Series, 126, Cambridge University Press, Cambridge, MA, 1991.
[11] G. Greaves, *Sieves in number theory*. In: 2001 Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Vol. 43, Springer-Verlag, Berlin, Germany, 2001.
[12] R. Gupta and M. R. Murty, *Cyclicity and generation of points mod p on elliptic curves*. Invent. Math. **101**(1990), 225–235.
[13] L. Häberle, *On cubic Galois field extensions*. J. Number Theory **130**(2010), 307–317.
[14] H. Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*. Abh. Deutsche Akad. Wiss. **2**(1950), 3–95.
[15] D. R. Heath-Brown, *Artin's conjecture for primitive roots*. Quart. J. Math. Oxford Ser. (2) **37**(1986), no. 145, 27–38.
[16] C. Hooley, *On Artin's conjecture*. J. Reine Angew. Math. **225**(1967), 209–220.
[17] A. Ivić, *Two inequalities for the sum of divisor function*. Univ. u Novom Sadu Zb. Rad. Prirod.-Mat. Fak. **7**(1977), 17–22.
[18] H. Iwaniec, *A new form of the error term in linear sieve*. Acta Arith. **37**(1980), 307–320.
[19] G. J. Janusz, *Algebraic number fields*. 2nd ed., Graduate Studies in Mathematics, 7, American Mathematical Society, Providence, RI, 1996. x+276 pp.
[20] N. Jones, *Almost all elliptic curves are serre curves*. Trans. Amer. Math. Soc. **362**(2010), no. 3, 1547–1570.
[21] S. Lang and H. Trotter, *Primitive points on elliptic curves*. Bull. Amer. Math. Soc. **83**(1977), no. 2, 289–292.
[22] S. A. Lang, *Graduate texts in mathematics. Vol. 211*. Revised 3rd ed., Springer-Verlag, New York, NY, 2002.
[23] H. W. Lenstra, *On Artin's conjecture and Euclid's algorithm in global fields*. Invent. Math. **42**(1977), 201–224.
[24] H. W. Lenstra, P. Stevenhagen, and P. Moree, *Character sums for primitive root densities*. Math. Proc. Cambridge Philos. Soc. **157**(2014), 489–511.
[25] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*. Cambridge Studies in Advanced Mathematics, 97, Cambridge University Press, Cambridge, MA, 2007. xviii+552 pp.
[26] P. Moree, *On primes in arithmetic progression having a prescribed primitive root*. J. Number Theory **78**(1999), 85–98.
[27] P. Moree, *On primes in arithmetic progression having a prescribed primitive root. II*. Functiones et Approximatio **39**(2008), 133–144.
[28] M. R. Murty, *On Artin's conjecture*. J. Number Theory **16**(1983), 147–168.
[29] M. R. Murty and K. L. Petersen, *A Bombieri-Vinogradov theorem for all number fields*. Trans. Amer. Math. Soc. **365**(2013), no. 9, 4987–5032.
[30] J. Neukirch, *Algebraic number theory*. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322, Springer-Verlag, Berlin, Germany, 1999.

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.

[31] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**(1972), 259–331.
[32] J. P. Serre, *Résumé des cours de 1977-1978, Annuaire du Collège de France (1978), 67–70 in Oeuvres. Vol. III (French)* [Collected papers. Vol. III] 1972–1984, Springer-Verlag, Berlin, Germany, 1986.
[33] J. H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106, Springer Verlag, NewYork, NY, 1986.

Department of Mathematics, Atılım University, 06830 Gölbaşı, Ankara, Turkey
e-mail: yildirim.akbal@atilim.edu.tr

Department of Mathematics, Bilkent University, 06800 Bilkent, Ankara, Turkey
e-mail: guloglua@fen.bilkent.edu.tr

Downloaded from https://www.cambridge.org/core. 27 Apr 2022 at 05:44:39, subject to the Cambridge Core terms of use.