CYCLICITY OF CM ELLIPTIC CURVES MODULO p

ALINA CARMEN COJOCARU

ABSTRACT. Let E be an elliptic curve defined over $\mathbb{Q}$ and with complex multiplication. For a prime p of good reduction, let $\overline{E}$ be the reduction of E modulo p. We find the density of the primes $p \leq x$ for which $\overline{E}(\mathbb{F}_p)$ is a cyclic group. An asymptotic formula for these primes had been obtained conditionally by J.-P. Serre in 1976, and unconditionally by Ram Murty in 1979. The aim of this paper is to give a new simpler unconditional proof of this asymptotic formula and also to provide explicit error terms in the formula.

1. INTRODUCTION

Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. By a famous result of Mordell, the set $E(\mathbb{Q})$ of $\mathbb{Q}$-rational points of E is a finitely generated abelian group. The study of the free part of $E(\mathbb{Q})$ is still one of the major problems in arithmetic geometry.

Now, for a prime p of good reduction for E (that is, $p \nmid N$), we denote by $\overline{E}$ the reduction of E modulo p. This is an elliptic curve defined over $\mathbb{F}_p$, the finite field with p elements. Naturally, as in the rational case, one is interested in the study of the structure of the group $\overline{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of $\overline{E}$. From classical theory, $\overline{E}(\mathbb{F}_p)$ can be written as the product of two cyclic finite groups. Indeed, $\overline{E}(\mathbb{F}_p) \subseteq \overline{E}(\overline{\mathbb{F}_p})[k] \subseteq \mathbb{Z}/k\mathbb{Z} \oplus \mathbb{Z}/k\mathbb{Z}$, where $\overline{\mathbb{F}_p}$ denotes the algebraic closure of $\mathbb{F}_p$, k is a positive integer such that the order $\#\overline{E}(\mathbb{F}_p)$ of $\overline{E}(\mathbb{F}_p)$ divides k, and $\overline{E}(\overline{\mathbb{F}_p})[k]$ denotes the group of $\overline{\mathbb{F}_p}$-rational points of $\overline{E}$ annihilated by k. Early computations of Borosh, Moreno and Porta ([BMP]) showed that, in fact, for "many" primes p, the group $\overline{E}(\mathbb{F}_p)$ is cyclic. One expects this to be true for infinitely many primes p, as suggested by the elliptic curve analogue of Artin's primitive root conjecture formulated by Lang and Trotter in 1977 (see [LT2]).

Our goal in this paper is to provide an asymptotic formula, with explicit error terms, for the function

$$f(x, \mathbb{Q}) := \#\{p \leq x : p \nmid N, \overline{E}(\mathbb{F}_p) \text{ cyclic}\},$$

in the case of an elliptic curve E defined over $\mathbb{Q}$ and with complex multiplication.

In 1976 (see [Se1]), J.-P. Serre showed that C. Hooley's *conditional* method of proving Artin's conjecture on primitive roots (see [Ho, ch. 3]) can be adapted to estimate $f(x, \mathbb{Q})$. More precisely, let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ and

let $\mathbb{Q}(E[k])$ denote the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the $\overline{\mathbb{Q}}$-rational points of E annihilated by k. Then, under the Generalized Riemann Hypothesis (denoted GRH) for the Dedekind zeta functions of the division fields $\mathbb{Q}(E[k])$ of E, Serre proves that, as $x \to \infty$,

$$(1) \qquad\qquad f(x, \mathbb{Q}) = \mathfrak{f}_E \operatorname{li} x + \operatorname{o}\left(\frac{x}{\log x}\right),$$

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

$$\mathfrak{f}_E := \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]},$$

with $\mu(\cdot)$ denoting the Möbius function.

We recall that for real-valued functions f and $g \neq 0$ we write $f(x) = \operatorname{o}(g(x))$ to mean that $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0$. Also, if g has positive values, we write $f(x) = \operatorname{O}(g(x))$ or $f \ll g$ to mean that there exists a positive constant A such that $|f(x)| \leq Ag(x)\ \forall x$. If the constant A depends on some quantity B, then we may write $f(x) = \operatorname{O}_B(g(x))$ or $f \ll_B g$. In this paper, whenever we write $f(x) = \operatorname{O}(g(x))$ or $f \ll g$, we mean that the implied O-constants are absolute. If $f \ll g \ll f$, then we write $f \asymp g$.

In 1979[1] (see [Mu1, pp. 161-167]), Ram Murty removed GRH in formula (1) for elliptic curves with complex multiplication (denoted CM). His proof uses class field theoretical properties of the division fields of CM elliptic curves, as well as a number field version of the Bombieri-Vinogradov theorem (whose proof is based on the large sieve for number fields). In 2000 (see [acC1]), the author proved formula (1) for elliptic curves without complex multiplication (denoted non-CM) under the assumption of a quasi-GRH (more precisely, a zero-free region of real part $> 3/4$ for the Dedekind zeta functions of $\mathbb{Q}(E[k])$). For more history about $f(x, \mathbb{Q})$ in both the CM and non-CM cases we refer the reader to [acC1], [acC2] and [Mu3].

In this paper we give a new simpler *unconditional* proof for the asymptotic formula for $f(x, \mathbb{Q})$ in the complex multiplication case, and provide explicit error terms in this formula. We are proving the following:

Theorem 1.1. *Let E be a CM elliptic curve defined over $\mathbb{Q}$, of conductor N and with complex multiplication by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field $K = \mathbb{Q}\left(\sqrt{-D}\right)$, where D is a positive square-free integer. Then, as $x \to \infty$,*

$$(2) \qquad\qquad f(x, \mathbb{Q}) = \mathfrak{f}_E \operatorname{li} x + \operatorname{O}_N\left(\frac{x}{(\log x)(\log \log \log x)}\right),$$

or, more precisely,

$$(3) \qquad f(x, \mathbb{Q}) = \mathfrak{f}_E \operatorname{li} x + \operatorname{O}\left(\frac{x}{(\log x)(\log \log \frac{\log x}{N^2})} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}}\right),$$

where the O-constant in (2) depends on N and the one in (3) is absolute.

Corollary 1.2. *Let E be a CM elliptic curve defined over $\mathbb{Q}$, of conductor N and such that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Then the smallest prime $p \nmid N$ for which $\overline{E}(\mathbb{F}_p)$ is cyclic has size $\operatorname{O}\left(\exp\left(N^2\right)\right)$. The implied O-constant is absolute.*

---

[1]It was communicated to the author by Ram Murty that this result was obtained in 1979; however, it appeared in print only in 1983.

It is possible that the error terms in Theorem 1.1 can be improved, but this involves more sophisticated methods than the ones used in our paper. We relegate this to future research.

2. Preliminaries

2.1. **Notation.** Given an elliptic curve E defined over $\mathbb{Q}$, p will always denote a prime of good reduction for E. We set $a_p := p + 1 - \#\overline{E}(\mathbb{F}_p)$ and say that p is of ordinary reduction if $a_p \neq 0$, and of supersingular reduction if $a_p = 0$. We denote by π_p and $\overline{\pi_p}$ the roots of the polynomial $X^2 - a_p X + p \in \mathbb{Z}[X]$.

If not otherwise stated, q will denote a rational prime and k a positive integer; $\pi(x)$ will denote the number of rational primes $\leq x$; $\#\mathcal{S}$ will denote the cardinality of a set $\mathcal{S}$; $\mathrm{Ker}\,\phi$ will denote the kernel of a morphism ϕ.

2.2. **Algebraic preliminaries.** The following preliminary lemmas are well known, but, for the sake of completeness, we include them here.

Lemma 2.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. Let $E[k]$ be the group of k-division points of E. Then*

(1) *the ramified primes of $\mathbb{Q}(E[k])/\mathbb{Q}$ are divisors of kN;*
(2) *assuming that E has complex multiplication and $k > 2$, we have*

$$\phi(k)^2 \ll [\mathbb{Q}(E[k]) : \mathbb{Q}] \ll k^2,$$

where $\phi(k)$ denotes the Euler function.

For proofs of this lemma the reader is referred to [Silv1, p. 179] and [Silv2, p. 135].

Lemma 2.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. Using the notation introduced in Section 2.1 we have that, for a positive integer k and a prime $p \nmid k$ of good reduction for E, p splits completely in $\mathbb{Q}(E[k])/\mathbb{Q}$ if and only if $\frac{\pi_p - 1}{k}$ is an algebraic integer.*

Proof. We recall that π_p is the algebraic quadratic integer corresponding to the Frobenius endomorphism

$$\overline{E}\left(\overline{\mathbb{F}_p}\right) \longrightarrow \overline{E}\left(\overline{\mathbb{F}_p}\right)$$
$$(x, y) \mapsto (x^p, y^p),$$

which we also denote by π_p.

Since $(p, kN) = 1$, we have that p is unramified in $\mathbb{Q}(E[k])/\mathbb{Q}$ (see part 1 of Lemma 2.1). By classical results in algebraic number theory, p splits completely in $\mathbb{Q}(E[k])/\mathbb{Q}$ if and only if $\pi_p|_{\overline{E}[k]} = 1$, where 1 denotes the identity map. This last condition is equivalent to saying that $\mathrm{Ker}([k]) \subseteq \mathrm{Ker}(\pi_p - 1)$ as maps $\overline{E}\left(\overline{\mathbb{F}_p}\right) \longrightarrow \overline{E}\left(\overline{\mathbb{F}_p}\right)$, where $[k]$ is the multiplication by k map. Hence there exists an elliptic curve endomorphism $\phi : \overline{E}\left(\overline{\mathbb{F}_p}\right) \longrightarrow \overline{E}\left(\overline{\mathbb{F}_p}\right)$ such that $\phi \circ [k] = \pi_p - 1$ (see [Silv1, Corollary 4.11, p. 77]). This is equivalent to saying that $\frac{\pi_p - 1}{k}$ is an algebraic integer. $\square$

Lemma 2.3. *Let E be a CM elliptic curve defined over $\mathbb{Q}$ and with complex multiplication by an imaginary quadratic field K. Then, for every prime p of ordinary good reduction for E, we have $\mathbb{Q}(\pi_p) = K$.*

Proof. First we observe that

$$\mathbb{Q}(\pi_p) \subseteq \mathrm{End}_{\mathbb{F}_p}(\overline{E}) \otimes_{\mathbb{Z}} \mathbb{Q} \subseteq \mathrm{End}_{\overline{\mathbb{F}_p}}(\overline{E}) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Then we note that, since E has complex multiplication by K, we have an embedding $K \subseteq \mathrm{End}_{\overline{\mathbb{F}_p}}(\overline{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$, and, moreover, since p is a prime of ordinary reduction, we actually have $K = \mathrm{End}_{\overline{\mathbb{F}_p}}(\overline{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$. Thus $\mathbb{Q}(\pi_p) \subseteq K$ for any prime p of ordinary reduction for E. But K is a degree 2 extension of $\mathbb{Q}$, and so is $\mathbb{Q}(\pi_p)$. This gives us the desired equality. $\qquad\square$

Lemma 2.3 describes a feature of CM elliptic curves that will play a very important role in our unconditional estimates of $f(x, \mathbb{Q})$. It actually describes one of the main differences between CM and non-CM elliptic curves (see [LT1]).

2.3. **Analytic preliminaries.** The next preliminary lemma is an application of the sieve of Eratosthenes, which we recall below.

Theorem 2.4 (The sieve of Eratosthenes)**.** *Let $\mathcal{A}$ be a set of natural numbers $\leq x$, and let $\mathcal{P}$ be a set of rational primes. To each prime $p \in \mathcal{P}$ we associate $\omega(p)$ distinguished residue classes modulo p. For any square-free integer d composed of primes of $\mathcal{P}$ we set*

$$\mathcal{A}(d) := \{a \in \mathcal{A} : a \text{ belongs to at least one of the } \omega(p) \text{ residue classes}$$
$$\text{modulo } p \text{ for all } p | d\},$$

and

$$\omega(d) := \prod_{p|d} \omega(p).$$

For a fixed real number z, we let $S(\mathcal{A}, \mathcal{P}, z)$ be the number of elements $a \in \mathcal{A}$ that do not belong to any of the distinguished residue classes modulo p for all $p \in \mathcal{P}, p \leq z$, and we set

$$W(z) := \prod_{\substack{p \in \mathcal{P} \\ p \leq z}} \left(1 - \frac{\omega(p)}{p}\right).$$

We assume that

(1) *there exists a real number X such that, for all square-free integers d composed of primes of $\mathcal{P}$,*

$$\#\mathcal{A}(d) = X \frac{\omega(d)}{d} + R_d$$

for some $R_d = \mathrm{O}(\omega(d))$;

(2) $\displaystyle \sum_{\substack{p \in \mathcal{P} \\ p \leq z}} \frac{\omega(p) \log p}{p} \leq c \log z + \mathrm{O}(1)$ *for some positive constant c.*

Then

$$S(\mathcal{A}, \mathcal{P}, z) = XW(z) + \mathrm{O}\left(x(\log z)^{c+1} \exp\left(-\frac{\log x}{\log z}\right)\right),$$

where the implied O-constant is absolute.

For a proof of this result, see [Mu4, p. 141].

Lemma 2.5. *Let $x \in \mathbb{R}$ and let D, k be fixed positive integers with $k < \sqrt{x} - 1$. Then*

$$
\begin{aligned}
S_k^1 \quad &:= \quad \#\left\{ p \le x : p = (\alpha k + 1)^2 + D\beta^2 k^2 \text{ for some } \alpha, \beta \in \mathbb{Z} \right\} \\
&= \quad O\left(\left(\frac{\sqrt{x}}{k} + 1 \right) \frac{\sqrt{x} \log \log x}{k\sqrt{D} \log \frac{\sqrt{x}-1}{k}} \right);
\end{aligned}
$$

$$
\begin{aligned}
S_k^2 \quad &:= \quad \#\left\{ p \le x : p = \left(\frac{\alpha}{2} k + 1 \right)^2 + D\frac{\beta^2}{4} k^2 \text{ for some } \alpha, \beta \in \mathbb{Z} \right\} \\
&= \quad O\left(\left(\frac{\sqrt{x}}{k} + 1 \right) \frac{\sqrt{x} \log \log x}{k\sqrt{D} \log \frac{\sqrt{x}-1}{k}} \right).
\end{aligned}
$$

The implied O*-constants are absolute.*

Proof. 1. Let us observe that the conditions $p \le x$ and $p = (\alpha k + 1)^2 + D\beta^2 k^2$ for some $\alpha, \beta \in \mathbb{Z}$ imply

$$
\alpha \in \left[\frac{-1 - \sqrt{x}}{k}, \frac{-1 + \sqrt{x}}{k} \right] \cap \mathbb{Z},
$$

$$
\beta \in \left[-\frac{\sqrt{x}}{k\sqrt{D}}, \frac{\sqrt{x}}{k\sqrt{D}} \right] \cap \mathbb{Z}, \quad \beta \ne 0.
$$

Thus

$$
\text{(4)} \quad S_k^1 \le \sideset{}{'}\sum_{\beta} \#\left\{ \alpha \in \left[\frac{-1 - \sqrt{x}}{k}, \frac{-1 + \sqrt{x}}{k} \right] \cap \mathbb{Z} : (\alpha k + 1)^2 + D\beta^2 k^2 \text{ a prime} \right\},
$$

where the sum $\sideset{}{'}\sum_{\beta}$ is over nonzero numbers $\beta \in \left[-\frac{\sqrt{x}}{k\sqrt{D}}, \frac{\sqrt{x}}{k\sqrt{D}} \right] \cap \mathbb{Z}$. We set

$$
\mathcal{A} := \left\{ \alpha \in \left[\frac{-1 - \sqrt{x}}{k}, \frac{-1 + \sqrt{x}}{k} \right] \cap \mathbb{Z} \right\},
$$

$$
\mathcal{P} := \left\{ p \text{ a rational prime} : (p, k) = 1, \left(\frac{-D}{p} \right) = 1 \right\},
$$

with $\left(\frac{\cdot}{p} \right)$ denoting the Legendre symbol modulo p. To each prime $p \in \mathcal{P}$ we associate the residue classes

$$
(-1 \pm \beta k \mathcal{D}) k^{-1} \pmod{p},
$$

where $\mathcal{D}$ is an integer such that $\mathcal{D}^2 \equiv -D \pmod{p}$ (let us observe that $(\alpha k + 1)^2 + D\beta^2 q^2 = p$ imposes the conditions $\left(\frac{-D}{p} \right) = 1$ and $(p, k) = 1$, and hence $\mathcal{D}$ and $k^{-1} \pmod{p}$ are well defined).

For a fixed real number z we have

$$
\text{(5)} \quad
\begin{aligned}
&\#\left\{ \alpha \in \left[\frac{-1 - \sqrt{x}}{k}, \frac{-1 + \sqrt{x}}{k} \right] \cap \mathbb{Z} : (\alpha k + 1)^2 + D\beta^2 k^2 \text{ a prime} \right\} \\
&\quad \le S(\mathcal{A}, \mathcal{P}, z) + \pi(z) \\
&\quad \le S(\mathcal{A}, \mathcal{P}, z) + z,
\end{aligned}
$$

with $S(\mathcal{A}, \mathcal{P}, z)$ defined as in the sieve of Eratosthenes.

Now we want to verify that the hypotheses of Theorem 2.4 are satisfied. Elementary estimates give us

$$\#\mathcal{A}(d) := \# \left\{ \alpha \in \mathcal{A} : (\alpha k + 1)^2 + D\beta^2 k^2 \equiv 0 (\operatorname{mod} d) \right\} = 2 \left(\frac{2\sqrt{x}}{k} + 1 \right) \frac{1}{d} + \mathrm{O}(1)$$

for all square-free integers d composed of primes of $\mathcal{P}$. Thus the first hypothesis of the sieve of Eratosthenes is satisfied with $\omega(d) = 2$ and $X = \frac{2\sqrt{x}}{k} + 1$. Using Mertens' theorem and recalling that $\left(\frac{-D}{p} \right) = 1$, hence that p splits completely in $\mathbb{Q}(\sqrt{-D})$, we obtain

$$\sum_{\substack{p \in \mathcal{P} \\ p \leq z}} \frac{\omega(p) \log p}{p} = 2 \sum_{\substack{p \in \mathcal{P} \\ p \leq z}} \frac{\log p}{p} = \log z + \mathrm{O}(1).$$

Thus the second hypothesis of the sieve of Eratosthenes is satisfied with $c = 1$. Therefore,

$$S(\mathcal{A}, \mathcal{P}, z) = \left(\frac{2\sqrt{x}}{k} + 1 \right) W(z) + \mathrm{O} \left(\frac{\sqrt{x} + 1}{k} (\log z)^2 \exp \left(-\frac{\log \frac{\sqrt{x}-1}{k}}{\log z} \right) \right),$$

where

$$W(z) = \prod_{\substack{p \in \mathcal{P} \\ p \leq z}} \left(1 - \frac{2}{p} \right) \leq \exp \left(-2 \sum_{\substack{p \in \mathcal{P} \\ p \leq z}} \frac{1}{p} \right) \ll \exp(-\log\log z) = \frac{1}{\log z},$$

by using the elementary inequality $1 + t \leq \exp(t)$ and, again, Mertens' theorem.

Let us choose z such that

$$\log z = \frac{\log \frac{\sqrt{x}-1}{k}}{3 \log\log x}.$$

Then

$$\mathrm{O} \left(\frac{\sqrt{x} + 1}{k} (\log z)^2 \exp \left(-\frac{\log \frac{\sqrt{x}-1}{k}}{\log z} \right) \right) = \mathrm{O} \left(\frac{\sqrt{x} + 1}{k} \frac{1}{\log x (\log\log x)^2} \right),$$

and so

$$S(\mathcal{A}, \mathcal{P}, z) = \left(\frac{2\sqrt{x}}{k} + 1 \right) \mathrm{O} \left(\frac{\log\log x}{\log \frac{\sqrt{x}-1}{k}} \right) + \mathrm{O} \left(\frac{\sqrt{x}}{k \log x (\log\log x)^2} \right)$$

$$= \left(\frac{2\sqrt{x}}{k} + 1 \right) \mathrm{O} \left(\frac{\log\log x}{\log \frac{\sqrt{x}-1}{k}} \right).$$

From (5) we obtain

$$\# \left\{ \alpha \in \left[\frac{-1 - \sqrt{x}}{k}, \frac{-1 + \sqrt{x}}{k} \right] \cap \mathbb{Z} : (\alpha k + 1)^2 + D\beta^2 k^2 \text{ a prime} \right\}$$

$$= \left(\frac{2\sqrt{x}}{k} + 1 \right) \mathrm{O} \left(\frac{\log\log x}{\log \frac{\sqrt{x}-1}{k}} \right),$$

which, used in (4), completes the proof of the first part of the lemma.

2. Similar to the proof above. $\qquad\square$

We remark that for S_k^1 and S_k^2 of the above lemma we actually have elementary estimates that are weaker than the ones given by Lemma 2.5 only by a $\frac{\log \log x}{\log x}$ factor. The sieve has been invoked precisely for obtaining this saving.

Lemma 2.6. *Keeping the notation of Lemma* 2.5, *we have that, for any k and x,*

$$S_k^i \ll \frac{\sqrt{x}}{k\sqrt{D}} \left(\frac{2\sqrt{x}}{k} + 1 \right),$$

where $1 \leq i \leq 2$.

Proof. We justify this estimate for $i = 1$. The case $i = 2$ is resolved similarly. We observe that the conditions $p \leq x$ and $p = (\alpha k + 1)^2 + D\beta^2 k^2$ for some $\alpha, \beta \in \mathbb{Z}$ give us $\frac{2\sqrt{x}}{k} + 1$ choices for α and $\frac{2\sqrt{x}}{k\sqrt{D}}$ choices for β. The lemma follows. $\qquad\square$

3. THE PROOF OF THE THEOREM AND COROLLARY

As explained in [Mu1, pp. 153-154], we have that $\overline{E}(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in $\mathbb{Q}(E[q])$ for any prime $q \neq p$. Also, we have that if $p \leq x$ and p splits completely in $\mathbb{Q}(E[k])$ for some k, then $k^2 | (p + 1 - a_p)$, and so, using Hasse's bound $a_p \leq 2\sqrt{p}$, we obtain $k \leq 2\sqrt{x}$. Therefore, using the simple asymptotic sieve, we can write

$$f(x, \mathbb{Q}) = N(x, y) + \mathrm{O}\left(M\left(x, y, 2\sqrt{x}\right) \right),$$

where

$$N(x, y) := \# \left\{ p \leq x : p \text{ does not split completely in any } \mathbb{Q}(E[q])/\mathbb{Q}, q \leq y \right\},$$

$$M\left(x, y, 2\sqrt{x}\right) := \# \{ p \leq x : p \text{ splits completely in some } \mathbb{Q}(E[q])/\mathbb{Q}$$
$$\text{with } y \leq q \leq 2\sqrt{x} \},$$

and where y is a real number to be chosen later. In order to estimate $f(x, \mathbb{Q})$ we need to estimate each of $N(x, y)$ and $M(x, y, 2\sqrt{x})$ and to choose the parameter y appropriately.

3.1. Estimate for $N(x, y)$. By the inclusion-exclusion principle we have

$$N(x, y) = \sideset{}{'}\sum_{k} \mu(k) \pi_1(x, \mathbb{Q}(E[k])/\mathbb{Q}),$$

where the sum is over all square-free positive integers $k \leq 2\sqrt{x}$ whose prime divisors are $\leq y$, and where

$$\pi_1(x, \mathbb{Q}(E[k])/\mathbb{Q}) := \#\{ p \leq x : p \text{ splits completely in } \mathbb{Q}(E[k])/\mathbb{Q} \}.$$

We estimate this sum by using the unconditional effective version of the Chebotarev density theorem as stated in [Mu2, p. 243] or [acC1, p. 337]. To do so, let us recall from [Se2, p. 130] that if $L/\mathbb{Q}$ is a finite normal field extension that is ramified only at the primes $p_1, p_2, \ldots, p_m$, then

$$\frac{1}{[L:\mathbb{Q}]} \log |\operatorname{disc}(L/\mathbb{Q})| \leq \log[L:\mathbb{Q}] + \sum_{j=1}^{m} \log p_j,$$

where $[L : \mathbb{Q}]$ and $\text{disc}(L/\mathbb{Q})$ denote the degree and the discriminant, respectively, of $L/\mathbb{Q}$. We apply this result, together with Lemma 2.1, to the fields $\mathbb{Q}(E[k])$, whose degree and discriminant over $\mathbb{Q}$ we denote by $n(k)$ and d_k, respectively. We get

$$n(k)|d_k|^{\frac{2}{n(k)}} \ll k^8 N^2$$

and

$$n(k) \left(\log |d_k|\right)^2 \ll k^6 \left(\log \left(k^2 N\right)\right)^2,$$

and so the maximum of the two quantities above is $\ll k^8 N^2$. In order to apply the unconditional effective Chebotarev density theorem mentioned before we need to have $k^8 N^2 \ll \log x$. Since $k \leq \exp(2y)$, it is enough to choose

$$(6) \qquad y = \frac{1}{8}(\log\log x - 2\log N).$$

Then, by the unconditional effective Chebotarev density theorem, we obtain

$$N(x, y) = \left(\sum_k{}' \frac{\mu(k)}{n(k)}\right) \text{li}\, x + O\left(\sum_k{}' x \exp\left(-A\sqrt{\frac{\log x}{n(k)}}\right)\right)$$

for some effective positive constant A. To handle the error term we use that $n(k) \ll k^2$ and that there are at most 2^y square-free numbers composed of primes $\leq y$. Then

$$(7) \qquad N(x, y) = \left(\sum_k{}' \frac{\mu(k)}{n(k)}\right) \text{li}\, x + O\left(\frac{x}{N^{1/4}(\log x)^B}\right)$$

for any positive constant B.

3.2. Estimate for $M\left(x, y, 2\sqrt{x}\right)$.

For real numbers ξ_1, ξ_2, we denote by

$$M^o\left(x, \xi_1, \xi_2\right)$$

the number of primes $p \leq x$ such that p has ordinary reduction and splits completely in some $\mathbb{Q}(E[q])$ with $\xi_1 \leq q \leq \xi_2$, and by

$$M^s(x, \xi_1, \xi_2)$$

the number of primes $p \leq x$ such that p has supersingular reduction and splits completely in some $\mathbb{Q}(E[q])$ with $\xi_1 \leq q \leq \xi_2$. We write

$$(8) \qquad M\left(x, y, 2\sqrt{x}\right) = M^o\left(x, y, 2\sqrt{x}\right) + M^s\left(x, y, 2\sqrt{x}\right)$$

and estimate each of the two terms. For the first one we observe that

$$(9) \qquad M^o\left(x, y, 2\sqrt{x}\right) \leq \sum_{y < q \leq 2\sqrt{x}} \pi_1^o(x, \mathbb{Q}(E[q])/\mathbb{Q}),$$

where

$$\pi_1^o(x, \mathbb{Q}(E[q])/\mathbb{Q}) := \#\{p \leq x : a_p \neq 0 \text{ and } p \text{ splits completely in } \mathbb{Q}(E[q])/\mathbb{Q}\}.$$

By Lemmas 2.2 and 2.3 we obtain

$$\pi_1^o(x, \mathbb{Q}(E[q])/\mathbb{Q}) \leq \#\left\{p \leq x : \frac{\pi_p - 1}{q} \in \mathcal{O}_K\right\}.$$

Since the norm of π_p in $K/\mathbb{Q}$ is p, we get

$$\#\left\{p \leq x : \frac{\pi_p - 1}{q} \in \mathcal{O}_K\right\} \leq S_q,$$

where S_q is S_q^1 if $-D \equiv 2, 3 \pmod 4$, and S_q^2 if $-D \equiv 1 \pmod 4$, with S_q^1, S_q^2 as in Lemma 2.5.

Let us fix a real number $u < \sqrt{x} - 1$. Using the elementary estimate for S_q given in Lemma 2.6, we obtain

$$
\begin{aligned}
\sum_{u < q \leq 2\sqrt{x}} \pi_1^o(x, \mathbb{Q}(E[q])/\mathbb{Q}) \ &\leq \ \sum_{u < q \leq 2\sqrt{x}} S_q \\
&\ll \ \sum_{u < q \leq 2\sqrt{x}} \frac{\sqrt{x}}{q\sqrt{D}} \left(\frac{2\sqrt{x}}{q} + 1 \right) \\
&= \ \frac{2x}{\sqrt{D}} \sum_{u < q \leq 2\sqrt{x}} \frac{1}{q^2} + \frac{\sqrt{x}}{\sqrt{D}} \sum_{u < q \leq 2\sqrt{x}} \frac{1}{q} \\
&\ll \ \frac{x}{\sqrt{D} u \log u} + \frac{\sqrt{x} \log \log x}{\sqrt{D}}.
\end{aligned}
$$
(10)

On the other hand, using the estimates for S_q given in Lemma 2.5, we obtain

$$
\begin{aligned}
\sum_{y < q \leq u} \pi_1^o(x, \mathbb{Q}(E[q])/\mathbb{Q}) \ &\leq \ \sum_{y < q \leq u} S_q \\
&\ll \ \sum_{y \leq q \leq u} \left(\frac{x}{q^2 \sqrt{D}} + \frac{\sqrt{x}}{q\sqrt{D}} \right) \frac{\log \log x}{\log \frac{\sqrt{x}-1}{q}} \\
&\ll \ \frac{x \log \log x}{\sqrt{D} \log \frac{\sqrt{x}-1}{u}} \sum_{y < q \leq u} \frac{1}{q^2} + \frac{\sqrt{x} \log \log x}{\sqrt{D} \log \frac{\sqrt{x}-1}{u}} \sum_{y < q \leq u} \frac{1}{q} \\
&\ll \ \frac{x \log \log x}{\sqrt{D} (\log \frac{\sqrt{x}-1}{u}) y \log y} + \frac{\sqrt{x} (\log \log x)(\log \log u)}{\sqrt{D} \log \frac{\sqrt{x}-1}{u}}.
\end{aligned}
$$
(11)

We choose
$$ u = \log x $$

and recall that $y = \frac{1}{8}(\log \log x - 2 \log N)$ (see (6)) and that D is bounded, since E has CM. Then, from (9), (10) and (11) we get

(12) $$ M^o(x, y, 2\sqrt{x}) = O\left(\frac{x \log \log x}{(\log x)(\log \frac{\log x}{N^2})(\log \log \frac{\log x}{N^2})} \right). $$

For the second term in (8) we have

(13) $$ M^s\left(x, y, 2\sqrt{x}\right) \leq \sum_{y < q \leq 2\sqrt{x}} \pi_1^s(x, \mathbb{Q}(E[q])/\mathbb{Q}), $$

where

$$ \pi_1^s(x, \mathbb{Q}(E[q])/\mathbb{Q}) := \#\{p \leq x : a_p = 0 \text{ and } p \text{ splits completely in } \mathbb{Q}(E[q])/\mathbb{Q}\}. $$

We observe that if p is a prime of supersingular reduction that splits completely in some $\mathbb{Q}(E[q])/\mathbb{Q}$, then $q = 2$. Indeed, for such primes p and q we have, on the one hand, that $q^2 | (p + 1 - a_p) = (p+1)$, and, on the other hand, that $q | (p-1)$; thus $q | 2$. Now we note that in the sum of (13) we run over $q > y$; thus, by our choice of y (see (6)), $q \neq 2$. This implies that

(14) $$ M^s\left(x, y, 2\sqrt{x}\right) = 0. $$

3.3. **The final formula.** Putting together (7), (8), (12) and (14) we get

$$f(x, \mathbb{Q}) = \left(\sideset{}{'}\sum_k \frac{\mu(k)}{n(k)} \right) \operatorname{li} x \quad + \quad \mathrm{O}\left(\frac{x}{N^{1/4}(\log x)^B} \right)$$

$$+ \quad \mathrm{O}\left(\frac{x}{(\log x)(\log \log x)} \right)$$

$$+ \quad \mathrm{O}\left(\frac{x}{(\log x)(\log \log \frac{\log x}{N^2})} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}} \right),$$

where the implied O-constants are absolute. It remains to analyze $\left(\sideset{}{'}\sum_k \frac{\mu(k)}{n(k)} \right) \operatorname{li} x$.

We write

$$\sideset{}{'}\sum_k \frac{\mu(k)}{n(k)} = \sum_k \frac{\mu(k)}{n(k)} - \sideset{}{''}\sum_k \frac{\mu(k)}{n(k)},$$

where $\sum_k{}''$ means that the sum is over those positive square-free integers k for which there exists a prime divisor $q > y$. Using part 2 of Lemma 2.1 we get that

$$\sideset{}{''}\sum_k \frac{\mu(k)}{n(k)} \operatorname{li} x \quad \ll \quad \frac{x}{\log x} \sum_{q>y} \sum_{t=1}^{\infty} \frac{1}{q^2 t^{3/2}}$$

$$\ll \quad \frac{x}{(\log x) y \log y}$$

$$= \quad \mathrm{O}\left(\frac{x}{(\log x)(\log \frac{\log x}{N^2})(\log \log \frac{\log x}{N^2})} \right).$$

Thus

(15) $$f(x, \mathbb{Q}) = \mathfrak{f}_E \operatorname{li} x + \mathrm{O}\left(\frac{x}{(\log x)(\log \log \frac{\log x}{N^2})} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}} \right).$$

This completes the proof of Theorem 1.1.

3.4. **The proof of Corollary 1.2.** First, let us recall that it was pointed out by Serre (see [Mu3, p. 327]) that the density $\mathfrak{f}_E$ is positive if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Now, we note that a necessary condition for formula (15) to hold is that $x \geq \exp(N^2)$. Then, if $x \asymp \exp(N^2)$, the main term of (15) will be bigger than the error term. This proves the assertion of the corollary.

4. Concluding remarks

As mentioned in the proof of Corollary 1.2, the density $\mathfrak{f}_E$ is positive if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. For the sake of clarity, we explain this in what follows in the case of a CM elliptic curve E defined over $\mathbb{Q}$. Naturally, in order to have $\mathfrak{f}_E \neq 0$ we need to assume $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, for otherwise the torsion part of $E(\mathbb{Q})$ contains the Klein four group and so $\overline{E}(\mathbb{F}_p)$ cannot be cyclic. The condition is also sufficient. To see this, let us first note that if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, then $[\mathbb{Q}(E[2]) : \mathbb{Q}]$ is 2, 3 or 6. We let K_2 be the unique abelian subextension contained in $\mathbb{Q}(E[2])$. Also, we let K be the CM field of E. We recall that $K(E[q]) = \mathbb{Q}(E[q])$ for any prime $q \geq 3$ (see [Mu1, p. 165, Lemma 6]), and we observe that since K is a quadratic field and K_2 is a cubic or a quadratic field, we have either $K_2 \cap K = \mathbb{Q}$ or $K_2 = K$. If $K_2 \cap K = \mathbb{Q}$,

then using that $K_2 \subseteq \mathbb{Q}(E[2])$ and $K \subseteq \mathbb{Q}(E[q])$ for any $q \geq 3$, we deduce that the density of the primes p that do not split completely in any of the fields $\mathbb{Q}(E[q])$ is greater than or equal to the density of the primes p that do not split completely in K_2 and K. In other words,

$$\mathfrak{f}_E \geq \left(1 - \frac{1}{[K_2 : \mathbb{Q}]}\right)\left(1 - \frac{1}{[K : \mathbb{Q}]}\right) \geq \frac{1}{4}.$$

If $K_2 = K$, then $K \subseteq \mathbb{Q}(E[q])$ for any prime q, and so the density of the primes p that do not split completely in any of the fields $\mathbb{Q}(E[q])$ is greater than or equal to the density of the primes p that do not split completely in K. In other words,

$$\mathfrak{f}_E \geq \left(1 - \frac{1}{[K : \mathbb{Q}]}\right) \geq \frac{1}{2}.$$

This completes the proof of the positivity of $\mathfrak{f}_E$.

The main significance of our unconditional proof of the asymptotic formula for $f(x, \mathbb{Q})$ in the case of a CM elliptic curve lies in the simplicity of the tools that are used. Ram Murty's initial proof avoided the GRH by using a difficult application of the large sieve for number fields, namely a Bombieri-Vinogradov type result for number fields. In our new proof we use instead an application of the sieve of Eratosthenes, one of the simplest sieves in number theory. We point out that this application of the sieve of Eratosthenes (Lemma 2.5) could be viewed as a Brun-Titchmarsh theorem for quadratic number fields, since it gives nontrivial upper bounds for the number of (principal) prime ideals whose generator satisfies congruence conditions. A result of this kind had been obtained in [Sch], but as an application of the large sieve for number fields, and could have been used in our treatment of $M(x, y, 2\sqrt{x})$.

Another significance of our new proof is that it provides explicit error terms, with absolute O-constants. As noted in Corollary 1.2, we can then deduce an unconditional upper bound for the smallest prime p for which $\overline{E}(\mathbb{F}_p)$ is cyclic. Considerable improvements of this bound, under GRH, will be discussed in an upcoming paper.

Naturally, one can ask if our ideas can be explored further and used in other related situations. For example, one could consider the question of determining the number of prime ideals for which the reduction of a CM elliptic curve defined over a number field gives a cyclic group. It seems that our tools can be used in this situation. Another question is that of using the ideas of this paper in the case of a non-CM elliptic curve. At present, no unconditional proof for the asymptotic formula for $f(x, \mathbb{Q})$ is known in this situation, but, as mentioned in Section 1, only a proof based on a quasi-GRH assumption (see [acC1]). If we assume a variation of a conjecture of Lang and Trotter on the number of distinct fields $\mathbb{Q}(\pi_p)$ obtained when p runs over primes of ordinary reduction for a non-CM elliptic curve (see [LT1]), then it turns out that we can follow the current CM approach even in the non-CM case. The dependence $\frac{1}{\sqrt{D}}$ on the discriminant D of the estimates provided by Lemma 2.5 will be more advantageous than the dependence on D provided by Schaal's result mentioned above. This is, again, an asset of our new proof. Yet another related question is that of determining an asymptotic formula for the number of primes p for which the order of $\overline{E}(\mathbb{F}_p)$ is square-free. The ideas of our paper can be successfully used to answer this question if E is a CM elliptic curve. The details of our last two claims will be given in different upcoming papers.

Acknowledgements

References

[acC1] A. C. Cojocaru, "On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves", Journal of Number Theory, vol. 96, no. 2, October 2002, pp. 335-350.

[acC2] A. C. Cojocaru, "Cyclicity of elliptic curves modulo p", Ph.D. thesis, Queen's University, Kingston, Canada, 2002.

[BMP] I. Borosh, C. J. Moreno, and H. Porta, "Elliptic curves over finite fields II", Mathematics of Computation, vol. 29, July 1975, pp. 951-964. MR **53:**8067

[Ho] C. Hooley, "Applications of sieve methods to the theory of numbers", Cambridge University Press, 1976. MR **53:**7976

[LT1] S. Lang and H. Trotter, "Frobenius distributions in GL_2-extensions", Lecture Notes in Mathematics 504, Springer-Verlag, 1976. MR **58:**27900

[LT2] S. Lang and H. Trotter, "Primitive points on elliptic curves", Bulletin of the American Mathematical Society, vol. 83, no. 2, March 1977, pp. 289-292. MR **55:**308

[Mu1] M. Ram Murty, "On Artin's conjecture", Journal of Number Theory, vol. 16, no. 2, April 1983, pp. 147-168. MR **86f:**11087

[Mu2] M. Ram Murty, "An analogue of Artin's conjecture for abelian extensions", Journal of Number Theory, vol. 18, no. 3, June 1984, pp. 241-248. MR **85j:**11161

[Mu3] M. Ram Murty, "Artin's conjecture and elliptic analogues", Sieve Methods, Exponential Sums and their Applications in Number Theory (eds. G. R. H. Greaves, G. Harman, M. N. Huxley), Cambridge University Press, 1996, pp. 326-344. MR **2000a:**11098

[Mu4] M. Ram Murty, "Problems in analytic number theory", Graduate Texts in Mathematics 206, Springer-Verlag, 2001. MR **2001k:**11002

[Sch] W. Schaal, "On the large sieve method in algebraic number fields", Journal of Number Theory 2, 1970, pp. 249-270. MR **42:**7626

[Se1] J. -P. Serre, "Résumé des cours de 1977-1978", Annuaire du Collège de France 1978, pp. 67-70.

[Se2] J. -P. Serre, "Quelques applications du théorème de densité de Chebotarev", Inst. Hautes Etudes Sci. Publ. Math., no. 54, 1981, pp. 123-201. MR **83k:**12011

[Silv1] J. H. Silverman, "The arithmetic of elliptic curves", Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986. MR **87g:**11070

[Silv2] J. H. Silverman, "Advanced topics in the arithmetic of elliptic curves", Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994. MR **96b:**11074

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada, K7L 3N6

E-mail address: `alina@mast.queensu.ca`

Current address: The Fields Institute for Research in Mathematical Sciences, 222 College Street, Toronto, Ontario, M5T 3J1, Canada

E-mail address: `alina@fields.utoronto.ca`