Indian J. Pure Appl. Math., **41**(1): 25-37, February 2010

AN ANALOGUE OF THE SIEGEL-WALFISZ THEOREM FOR THE CYCLICITY OF CM ELLIPTIC CURVES MOD p

Amir Akbary* and V. Kumar Murty**

*Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, T1K 3M4, Canada
e-mail: amir.akbary@uleth.ca
**Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, Ontario, M5S 2E4, Canada
e-mail: murty@math.toronto.edu

Abstract Let E be a CM elliptic curve defined over $\mathbb{Q}$ and of conductor N. We establish an asymptotic formula, uniform in N and with improved error term, for the counting function of primes p for which the reduction mod p of E is cyclic. Our result resembles the classical Siegel-Walfisz theorem regarding the distribution of primes in arithmetic progressions.

Key words Reduction mod p of elliptic curves, cyclicity of CM elliptic curves mod p, Siegel-Walfisz Theorem.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. For a prime of good reduction p, let $\bar{E}$ be the reduction of E mod p. Let $\bar{E}(\mathbb{F}_p)$ be the group of rational points of $\bar{E}$ with coordinates in $\mathbb{F}_p$. Let

$$C(x,E) := \#\{p \leq x : \ p \nmid N, \ \bar{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

The GRH in this paper stands for the assumption of the Generalized Riemann Hypothesis for the Dedekind zeta functions of the extensions $\mathbb{Q}(E[m])/\mathbb{Q}$, where $E[m]$ is the group of m-torsion points of E and $m = 1$ or m is square free.

Since $E[2]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and prime to p-torsions have trivial intersection with the kernel of reduction mod p map, it is clear that if $\mathbb{Q}(E[2]) = \mathbb{Q}$ then $C(x,E) = 0$ or 1. Serre [12] proved that, under the assumption of the GRH, if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$ then

$$C(x,E) = \mathfrak{c}_E \, \mathrm{li}(x) + o\left(\frac{x}{\log x}\right),$$

where the density $\mathfrak{c}_E > 0$. Here $\mathrm{li}(x) = \int_2^x dt/\log t$, and we recall that $f(x) = o(g(x))$ means $\lim_{x\to\infty} f(x)/g(x) = 0$; similarly $f(x) = O_A(g(x))$ (or equivalently $f(x) \ll_A g(x)$) means that the function $|f(x)/g(x)|$ is bounded by a constant depending on A as $x \to \infty$.

In fact the proof of Theorem 2 of Murty [10] shows that, under GRH,

$$C(x, E) = \mathfrak{c}_E \,\mathrm{li}(x) + O_E\left(\frac{x \log\log x}{(\log x)^2}\right),$$

where

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

Here $\mu(.)$ is the Möbius function.

One can show that the above series representing $\mathfrak{c}_E$ is absolutely convergent (see [10, Proof of Theorem 2]). Moreover, for odd k, we have $E[2k] = E[2] \oplus E[k]$. If the elements of $E[2]$ are defined over $\mathbb{Q}$, then it follows that $\mathbb{Q}(E[2k]) = \mathbb{Q}(E[k])$. So for odd squarefree k, the terms corresponding to k and $2k$ in the series add to zero. Thus, the series defining $\mathfrak{c}_E$ is seen to be equal to zero in this case.

The error term in the above formula has been improved significantly by Cojocaru and Murty in [3] under various assumptions on the Artin L- functions associated to the extensions $\mathbb{Q}(E[m])/\mathbb{Q}$. Moreover the dependence of the error term on the conductor of E has been made explicit.

There are also several unconditional results on this problem. Firstly, one can show that the constant $\mathfrak{c}_E$ (defined by the above series) is positive if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$ (see [3, Section 6] for a proof). More precisely, if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, in the CM case $\mathfrak{c}_E \geq 1/4$, and in the non-CM case $\mathfrak{c}_E \gg 1/\log\log N$.

Secondly Gupta and Murty [5] proved that the number of primes $p \leq x$ for which $\bar{E}(\mathbb{F}_p)$ is cyclic is $\gg x/(\log x)^2$.

Stronger unconditional results are known for elliptic curves with complex multiplication. In [10], Murty removed the dependence on GRH in Serre's theorem for CM elliptic curves though he did not provide an error term. Cojocaru [2] established an unconditional asymptotic formula for cyclicity of CM curves with an error term

$$O_N\left(\frac{x}{(\log x)\log\log\log x}\right).$$

More precisely, she proved

$$C(x, E) = \mathfrak{c}_E \,\mathrm{li}(x) + O\left(\frac{x}{(\log x)\log\log \frac{\log x}{N^2}} \frac{\log\log x}{\log \frac{\log x}{N^2}}\right), \tag{1.1}$$

where the implied constant is absolute.

In this paper we improve the error term in the above asymptotic formula. Our result is uniform in N, so it is applicable to all CM elliptic curves of conductor N

in a certain range. To show the dependence on the conductor N we use the notation $C(x, N, E)$ for our counting function.

We prove the following:

Theorem 1.1. *Let E denote a CM elliptic curve defined over $\mathbb{Q}$ of conductor N and with complex multiplication by the full ring of integers $\mathfrak{O}_K$ of an imaginary quadratic field K. Let $A, B > 0$ and $N \leq (\log x)^A$, then we have*

$$C(x, N, E) = \mathfrak{c}_E \operatorname{li}(x) + O_{A,B}\left(\frac{x}{(\log x)^B}\right),$$

uniformly in N, where

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

and the implied constant depends only on A and B.

We view this theorem as an elliptic analogue of the classical Siegel-Walfisz theorem for distribution of prime numbers in an arithmetic progression. Indeed, let us denote by $\pi(x, q, a)$ the number of primes $\leq x$ that are congruent to $a \pmod q$. The Siegel-Walfisz theorem implies that for any $A, B > 0$, uniformly for $q \leq (\log x)^A$ we have

$$\pi(x, q, a) = \frac{1}{\varphi(q)}\operatorname{li}(x) + O_{A,B}\left(\frac{x}{(\log x)^B}\right).$$

In fact, the Siegel-Walfisz theorem gives a stronger result. Given any $A > 0$ there exists a constant $C = C(A)$ so that uniformly for $q \leq (\log x)^A$, we have

$$\pi(x, q, a) = \frac{1}{\varphi(q)}\operatorname{li}(x) + O(x \exp(-C(\log x)^{1/2})).$$

We do not know how to obtain this stronger version in our setting.

As an application of our theorem, we have a new proof of positivity of $\mathfrak{c}_E$ in the case that the CM curve E has an irrational 2-torsion point.

Corollary 1.2. $\mathfrak{c}_E \neq 0 \iff \mathbb{Q}(E[2]) \neq \mathbb{Q}$.

Proof : As we said above if $\mathbb{Q}(E[2]) = \mathbb{Q}$ then $C(x, N, E) = 0$ or 1, and so $\mathfrak{c}_E = 0$.

On the other hand if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$ and $\mathfrak{c}_E = 0$, our theorem states that

$$C(x, N, E) \ll \frac{x}{(\log x)^3},$$

however from [5, Theorem 1], we know that

$$C(x, N, E) \gg \frac{x}{(\log x)^2}.$$

This is a contradiction. So $\mathfrak{c}_E \neq 0$. □

Let $P(N,E)$ denote the smallest prime p for which $\bar{E}(\mathbb{F}_p)$ is cyclic. In [3], Cojocaru and Murty, as an elliptic curve analogue of Linnik's problem, considered the problem of finding upper bounds for $P(N,E)$. They proved, under GRH, that if E has an irrational 2-torsion point then

$$P(N,E) = O_\epsilon\left((\log N)^{4+\epsilon}\right)$$

for non-CM elliptic curves, and

$$P(N,E) = O_\epsilon\left((\log N)^{2+\epsilon}\right)$$

for CM elliptic curves.

As a direct corollary of our theorem we have the following unconditional result for CM elliptic curves.

Corollary 1.3. *Let $\epsilon > 0$ and Suppose that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Then*

$$P(N,E) = O_\epsilon(\exp(N^\epsilon)).$$

Proof : We assume that $0 < \epsilon < 1$ and in Theorem 1.1 let $A = 1/\epsilon$. Then for $x \geq \exp(N^\epsilon)$ we have

$$C(x,N,E) = \mathfrak{c}_E \,\mathrm{li}(x) + O_\epsilon\left(\frac{x}{(\log x)^{1/\epsilon}}\right).$$

Now since $\mathfrak{c}_E \geq 1/4$ (see [3, Section 6]) we have that $C(x,N,E) > 0$ for large values of x (depending only on ϵ). So $\bar{E}(\mathbb{F}_p)$ is cyclic for primes of size $O_\epsilon(\exp(N^\epsilon))$. □

Observe that (1.1) gives the weaker unconditional result

$$P(N,E) = O\left(\exp\left(N^2\right)\right),$$

for CM curves.

The main tools used in Cojocaru's proof of (1.1) are an unconditional version of the Chebotarev density theorem and the sieve of Eratosthenes. The method of our proof is a simplified version of the method used in [10] which employs the results that are consequence of the large sieve inequality in algebraic number fields. The improvement in the range of N, in Theorem 1.1, is a consequence of applying a sharp upper bound for the possible exceptional zero of the Dedekind zeta function of the extension $\mathbb{Q}(E[2])/\mathbb{Q}$ (see the proof of Lemma 2.3). The improvement of the error term in Theorem 1.1 is achieved by employing a version of the Bombieri-Vinogradov theorem in number fields due to Huxley (see Lemma 2.9).

In the next section we prove some lemmas that will be needed in the proof of our main result. Section 3 gives a proof of Theorem 1.1.

Notation 1.4. Unless otherwise stated, p and q are rational primes, and m is a squarefree integer. K is an imaginary quadratic field with the ring of integers $\mathfrak{O}_K$,

$N(\mathfrak{a})$ denote the norm of an ideal $\mathfrak{a}$ of $\mathfrak{O}_K$, $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$, and $\mathfrak{m} = m\mathfrak{O}_K$. E is an elliptic curve defined over $\mathbb{Q}$ and of conductor N, and $E[m]$ denotes the group of m-torsion points of E. Moreover for a prime of good reduction p, $\bar{E}$ denotes the reduction of E mod p, and $\bar{E}(\mathbb{F}_p)$ is the group of rational points of $\bar{E}$ with cooordinates in $\mathbb{F}_p$. Finally d_m denotes the discriminant of $\mathbb{Q}(E[m])/\mathbb{Q}$ and $n_m = [\mathbb{Q}(E[m]) : \mathbb{Q}]$ denotes the degree of the extension $\mathbb{Q}(E[m])/\mathbb{Q}$.

2. Preliminaries

Lemma 2.1 *Let $p \neq q$ be primes, and $p \nmid N$. Then $\bar{E}(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z} \iff$ p splits completely in $\mathbb{Q}(E[q])$.*

Proof : See [10, Lemma 2]. □

Our next lemma provides a criterion for the cyclicity of $\bar{E}(\mathbb{F}_p)$.

Lemma 2.2 *Suppose that $p \nmid N$. Then $\bar{E}(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in $\mathbb{Q}(E[q])$ for any prime q.*

Proof : If $\bar{E}(\mathbb{F}_p)$ is cyclic then $\bar{E}(\mathbb{F}_p)$ does not contain a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ for any prime q. So by Lemma 2.1, p does not split completely in $\mathbb{Q}(E[q])$ for any $q \neq p$. Moreover, since $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(E[p])$, p ramifies in $\mathbb{Q}(E[p])$ as it ramifies in $\mathbb{Q}(\zeta_p)$. This shows that p does not split completely in $\mathbb{Q}(E[p])$.

Conversely, if p does not split completely in $\mathbb{Q}(E[q])$ for any prime q. Then, by Lemma 2.1, $\bar{E}(\mathbb{F}_p)$ does not contain a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ for any prime $q \neq p$. Moreover the p-primary part of $\bar{E}(\mathbb{F}_p)$ is a subgroup of $\bar{E}[p]$ (the group of p-torsion points of $\bar{E}$) which itself is isomorphic to a subgroup of $\mathbb{Z}/p\mathbb{Z}$. So $\bar{E}(\mathbb{F}_p)$ does not contain a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ for any prime q, and thus it is cyclic. □

Since $\mathbb{Q}(E[q_1q_2]) = \mathbb{Q}(E[q_1])\mathbb{Q}(E[q_2])$ for primes $q_1 \neq q_2$, it is plain to deduce from the above lemma that for a prime of good reduction p, $\bar{E}(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in $\mathbb{Q}(E[m])$ for any square free m.

For square free m, let

$$P(x, m) = \#\{p \leq x;\ p \nmid N,\ p \text{ split completely in } \mathbb{Q}(E[m])\}.$$

We also define

$$P(x, 1) = \#\{p \leq x;\ p \nmid N\}.$$

From Lemma 2.1, we deduce that if a prime of good reduction p splits completely in $\mathbb{Q}(E[m])$ then $m^2 \mid \#\bar{E}(\mathbb{F}_p)$ (Note that if p splits completely in $\mathbb{Q}(E[m])$ then $(p, m) = 1$ as $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(E[m])$). From Hasse's bound we know that $\#\bar{E}(\mathbb{F}_p) \leq (\sqrt{p} + 1)^2$, so if $m^2 \mid \#\bar{E}(\mathbb{F}_p)$ we have $m \leq \sqrt{p} + 1 \leq 2\sqrt{p}$. This shows that

$$m > 2\sqrt{x} \Longrightarrow P(x, m) = 0.$$

Let $n_m = [\mathbb{Q}(E[m]) : \mathbb{Q}]$ and d_m be the discriminant of $\mathbb{Q}(E[m])/\mathbb{Q}$. In the next lemma we employ an unconditional version of the Chebotarev density theorem to give an asymptotic formula for $P(x, 2)$.

Lemma 2.3. *Let E denote an elliptic curve defined over $\mathbb{Q}$ of conductor N. Let $A, B > 0$ and suppose that x satisfies $N \leq (\log x)^A$. Then*

$$P(x,2) = \frac{1}{n_2}\mathrm{li}(x) + O_{A,B}\left(\frac{x}{(\log x)^B}\right) + O\left(\log N\right),$$

uniformly in N.

Proof : First of all note that since $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, we have $n_2 = 1,\ 2,\ 3$, or 6. So by [8, Theorem 1.3], for $|d_2| \leq \exp((\log x)^{1/2}/\sqrt{60})$ we have

$$P(x,2) = \frac{1}{n_2}\mathrm{li}(x) - \frac{1}{n_2}\mathrm{li}(x^\beta) + O\left(x\exp(-c_1\sqrt{\log x/n_2})\right) + O(\log N), \quad (2.1)$$

where β is the possible exceptional zero of the Dedekind zeta function of $\mathbb{Q}(E[2])/\mathbb{Q}$ and c_1 and the implied constants are absolute. We know that for any $\epsilon > 0$ there is an absolute positive constant $c(\epsilon)$ such that

$$\beta \leq 1 - \frac{c(\epsilon)}{|d_2|^\epsilon},$$

(see [4, Page 426] for a proof). Taking $\epsilon = 1/12A$ in the above bound for β, and applying it in (2.1) will imply the result as long as $|d_2| \ll (\log x)^{6A}$. Observing that $|d_2| \leq (12N)^6$ (see [2, Section 3.1]) will establish the result for $N \leq (\log x)^A$. □

Lemma 2.4. *If $m \geq 3$ is square free and $p \nmid 6N$ is a prime that splits completely in $\mathbb{Q}(E[m])$, then p is an ordinary prime.*

Proof : We prove this by contradiction. Suppose $p \nmid 6N$ is a supersingular prime. So $\#\bar{E}(\mathbb{F}_p) = p + 1$ since $p \neq 2, 3$ (see [13, Page 145, Exercise 5.10.(b)]). Now since p splits completely in $\mathbb{Q}(E[m])$ and $m \geq 3$ is square free, there is a prime $q \neq 2$ such that p splits completely in $\mathbb{Q}(E[q])$. So by Lemma 2.1, $q^2 \mid \#\bar{E}(\mathbb{F}_p) = p + 1$. On the other hand since the cyclotomic field $\mathbb{Q}(\zeta_q) \subseteq \mathbb{Q}(E[q])$ then p also splits completely in $\mathbb{Q}(\zeta_q)$, and so $q \mid p - 1$. Thus $q \mid (p+1) - (p-1) = 2$ which is a contradiction, since $q \neq 2$. So p is not supersingular. □

From now on we assume that $E/\mathbb{Q}$ has CM by $\mathfrak{O}_K$. In this case it is known that K has class number 1, and moreover we know that if p is an ordinary prime then p splits in $\mathfrak{O}_K$ ([9, Page 182, Theorem 12]). So Lemma 2.4 establishes a close connection between the primes that split completely in $\mathbb{Q}(E[m])$ and the primes that split completely in K.

For an ordinary prime p, let π_p and $\bar{\pi}_p$ be the roots of the polynomial $X^2 - a_pX + p \in \mathbb{Z}[X]$, where $a_p = p + 1 - \#\bar{E}(\mathbb{F}_p)$. From the theory of complex multiplication we know that $\pi_p \in \mathfrak{O}_K$ and moreover we may assume that it represents the Frobenius endomorphism of $\bar{E}$. Note that $N(\pi_p) = \pi_p\bar{\pi}_p = p$ and $\pi_p + \bar{\pi}_p = p + 1 - \#\bar{E}(\mathbb{F}_p)$.

Next observe that if $p \nmid N$ is an ordinary prime then

$$p \text{ splits completely in } \mathbb{Q}(E[m]) \iff \pi_p \equiv 1 \mod m\mathfrak{O}_K.$$

(See Lemma 2.2 of [2] for a proof.)

The next lemma establishes a trivial upper bound for $P(x,m)$.

Lemma 2.5. *For square free m, $3 \le m \le 2\sqrt{x}$, we have*

$$P(x,m) \ll \frac{x}{m^2},$$

where the implied constant is absolute.

Proof : For square free $m \ge 3$, we have

$$\begin{aligned} P(x,m) &\le \#\{\pi_p \in \mathfrak{O}_K :\ N(\pi_p) = p \le x,\ p \nmid N,\ \pi_p \equiv 1 \bmod m\mathfrak{O}_K\} + 2 \\ &\le \#\{\alpha \in \mathfrak{O}_K :\ N(\alpha) \le x,\ \alpha \equiv 1 \bmod m\mathfrak{O}_K\} + 2 \end{aligned}$$

By [10, Lemma 5] the last expression

$$\ll \frac{x}{m^2} + 2 \ll \frac{x}{m^2},$$

where 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 1, and so the implied constant above can be replaced by an absolute constant. □

The following lemma plays a crucial role in the proof of Theorem 1.1.

Lemma 2.6. *If $m \ge 3$ then $\mathbb{Q}(E[m]) = K(E[m])$.*

Proof : See [10, Lemma 6]. □

Using the above lemma we can relate the rational primes that split completely in $\mathbb{Q}(E[m])$ to the prime ideals of $\mathfrak{O}_K$ that splits completely in $K(E[m])$. To do this, we first recall some basic facts from algebraic number theory.

For a totally imaginary field K, we define an equivalence relation on the set of ideals of $\mathfrak{O}_K$ as follows. We say two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent, written $\mathfrak{a} \sim \mathfrak{b}$, if there exists α, $\beta \in \mathfrak{O}_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, where (α) (resp. (β)) denotes the ideal generated by α (resp. β). This relation gives us h equivalence classes, where h is called the class number of K (or $\mathfrak{O}_K$). We also say that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent $\bmod \mathfrak{q}$, denoted $\mathfrak{a} \sim \mathfrak{b} \bmod \mathfrak{q}$, if they are relatively prime to $\mathfrak{q}$ and there exists α, $\beta \in \mathfrak{O}_K$, such that $\alpha \equiv \beta \equiv 1 \bmod \mathfrak{q}$, and $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. Again this is an equivalence relation and we have $h(\mathfrak{q})$ classes where

$$h(\mathfrak{q}) = \frac{h\varphi(\mathfrak{q})}{T(\mathfrak{q})}.$$

Here $T(\mathfrak{q})$ is the number of residue classes of elements of $\mathfrak{O}_K \bmod \mathfrak{q}$ that contain a unit, and $\varphi(\mathfrak{q})$ is the number field analogue of the Euler function. If K is an imaginary quadratic field then $T(\mathfrak{q}) \le 6$. In the sequel, $N(\mathfrak{a})$ denotes the norm of an ideal $\mathfrak{a} \in \mathfrak{O}_K$.

For $(\mathfrak{a}, \mathfrak{q}) = 1$, let

$$\pi_K(x; \mathfrak{q}, \mathfrak{a}) = \#\{\mathfrak{p} :\ \text{prime ideal};\ N(\mathfrak{p}) \le x,\ \text{and } \mathfrak{p} \sim \mathfrak{a} \bmod \mathfrak{q}\}.$$

From now on we denote $m\mathfrak{O}_K$ by $\mathfrak{m}$, and $\mathfrak{f}$ denotes an ideal of $\mathfrak{O}_K$ whose prime divisors are exactly primes of bad reduction of E over K.

The following lemma gives a description, in terms of ideal classes mod $\mathfrak{fm}$, of prime ideals of $\mathfrak{O}_K$ that split completely in $K(E[m])$.

Lemma 2.7. *Let $E/\mathbb{Q}$ have CM by $\mathfrak{O}_K$ and $m \geq 1$ be an integer. Then there is an ideal $\mathfrak{f}$ of $\mathfrak{O}_K$ and $t(m)$ ideal classes mod $\mathfrak{fm}$ with the following property:*

If $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$ with $\mathfrak{p} \nmid \mathfrak{fm}$, then, $\mathfrak{p}$ $splits\ completely\ in\ K(E[m])$ $if\ and\ only\ if$ $\mathfrak{p} \sim \mathfrak{m}_1$, or $\mathfrak{m}_2$, $or \cdots$, or $\mathfrak{m}_{t(m)} \bmod \mathfrak{fm}$.

Moreover, $t(m)\ [K(E[m]) : K] = h(\mathfrak{fm})$, where $t(m) \leq c\ \varphi(\mathfrak{f}) \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 + \frac{1}{N(\mathfrak{p})-1}\right)$. Here c is an absolute constant and $\varphi(\mathfrak{f})$ is the number field analogue of the Euler function.

Proof : For the first assertion see [10, Lemma 4], or [1, Lemma 3.3]. Next let $\left(\frac{K(E[m])/K}{\mathfrak{p}}\right)$ be the Artin symbol (see [14, Page 116] for the definition) of $\mathfrak{p}$ in the extension $K(E[m])/K$. We know that $\mathfrak{p}$ splits completely in $K(E[m])$ if and only if $\left(\frac{K(E[m])/K}{\mathfrak{p}}\right) = 1$.

Set

$$\begin{aligned}\phi(x; K(E[\mathfrak{m}])/K) &= \#\{\mathfrak{p} : \text{ prime ideal of } K; \\ &\qquad N(\mathfrak{p}) \leq x,\ \mathfrak{p} \nmid \mathfrak{fm}, \text{ and } \left(\frac{K(E[m])/K}{\mathfrak{p}}\right) = 1\}.\end{aligned}$$

Then from the first assertion we have

$$\phi(x; K(E[m])/K) = \sum_{i=1}^{t(m)} \pi_K(x; \mathfrak{fm}, \mathfrak{m}_i).$$

Now the second statement follows by employing the Chebotarev density theorem, the prime ideal theorem, and comparing the main terms of the two sides of the above identity.

Finally we have

$$\begin{aligned}t(m) &= \frac{h(\mathfrak{fm})}{[K(E[m]) : K]} \\ &= \frac{h\varphi(\mathfrak{fm})}{T(\mathfrak{fm})[K(E[m]) : K]} \\ &= \frac{h\varphi(\mathfrak{f})}{T(\mathfrak{fm}) \prod_{\mathfrak{p}|(\mathfrak{f},\mathfrak{m})} \left(1 - \frac{1}{N(\mathfrak{p})}\right)} \frac{\varphi(\mathfrak{m})}{[K(E[m]) : K]}.\end{aligned}$$

Since $T(\mathfrak{fm}) \geq 1$ and $h = 1$, the result follows if we can show that $\varphi(\mathfrak{m})/[K(E[m]) : K]$ is absolutely bounded (i.e. independent of K, E, and m). To show this let E_0 be a fixed elliptic curve defined over $\mathbb{Q}$ with CM by $\mathfrak{O}_K$. Then for any other elliptic

curve E defined over $\mathbb{Q}$ and with CM by $\mathfrak{O}_K$, there is an extension L of K such that $[L : K] \leq 6$ and E is isomorphic to E_0 over L. Thus $L(E[m]) = L(E_0[m])$ and

$$\begin{aligned}[K(E_0[m]) : K] &\leq [L(E_0[m]) : K] = [L(E[m]) : K] \\ &= [L(E[m]) : K(E[m])][K(E[m]) : K] \\ &\leq 6[K(E[m]) : K].\end{aligned}$$

So we have

$$\frac{\varphi(\mathfrak{m})}{[K(E[m]) : K]} = \frac{\varphi(\mathfrak{m})}{[K(E_0[m]) : K]} \frac{[K(E_0[m]) : K]}{[K(E[m]) : K]} \leq 6 \frac{\varphi(\mathfrak{m})}{[K(E_0[m]) : K]}.$$

By a theorem of Deuring (see [11, Section 4.5]) we know that $\varphi(\mathfrak{m})/[K(E_0[m]) : K]$ is bounded by a constant which depends only on E_0. Since E_0 is fixed for given K, and K is one of the nine imaginary quadratic field of class number 1, we conclude that $\varphi(\mathfrak{m})/[K(E[m]) : K]$ is absolutely bounded. This completes the proof of the assertion regarding $t(m)$. □

Remark 2.8. In the previous lemma $\mathfrak{f}$ can be taken as the conductor of the Grössencharacter associated to E (see [10, Page 163]). Then we have $N = N(\mathfrak{f})|d_K|$ where d_K is the discriminant of the quadratic imaginary field K.

The following extension of the Bombieri-Vinogradov theorem to K is due to Huxley.

Lemma 2.9. *For each positive constant B, there is a positive constant $C = C(B)$ such that*

$$\sum_{N(\mathfrak{q}) \leq Q} \max_{(\mathfrak{a},\mathfrak{q})=1} \frac{1}{T(\mathfrak{q})} \left| \pi_K(x; \mathfrak{q}, \mathfrak{a}) - \frac{\mathrm{li}(x)}{h(\mathfrak{q})} \right| \ll \frac{x}{(\log x)^B},$$

where $Q = x^{\frac{1}{2}}(\log x)^{-C}$. The implied constant depends only on B and on the field K.

Proof : See [7], Theorem 1. □

We are ready to prove the main result of this paper.

3. Proof of Theorem 1.1.

Proof : First of all note that in light of Lemma 2.2, we have

$$\begin{aligned}C(x, N, E) &= \#\{p \leq x;\ p \nmid N,\ p \text{ does not split completely in} \\ &\quad \mathbb{Q}(E[q]) \text{ for any prime } q\}.\end{aligned}$$

Recall that for square free m, we set

$$P(x, m) = \#\{p \leq x;\ p \nmid N,\ p \text{ splits completely in } \mathbb{Q}(E[m])\}.$$

So by an application of the inclusion-exclusion argument described in [10, Section 3] we have

$$C(x,N,E)=\sum_{m=1}^{2\sqrt{x}}\mu(m)P(x,m).$$

The upper index can be chosen as $2\sqrt{x}$ since $P(x,m)=0$ for $m>2\sqrt{x}$ (see the discussion after Lemma 2.2).

In the following computation $\mathfrak{f}$ is the ideal given in Lemma 2.7, $A,B>0$ are arbitrary positive numbers, and $C=C(A,B)$ is the corresponding number to $A+B+1$ in Lemma 2.9. Also we denote $\log x$ by $\mathcal{L}$.

Next by employing Lemma 2.5, we have

$$\begin{aligned}C(x,N,E) &= \sum_{1\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}}\mu(m)P(x,m)+O\left(\sum_{m>\frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}}^{2\sqrt{x}}\frac{x}{m^2}\right)\\ &= \sum_{1\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}}\mu(m)P(x,m)+O\left(N(\mathfrak{f})x^{3/4}(\log x)^{C/2}\right).\end{aligned}$$

Now we apply the prime number theorem and Lemma 2.3 to evaluate the terms $P(x,1)$ and $P(x,2)$. We have, uniformly for $N\leq(\log x)^A$,

$$\begin{aligned}C(x,N,E) &= P(x,1)-P(x,2)\\ &+ \sum_{3\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}}\mu(m)P(x,m)+O\left(N(\mathfrak{f})x^{3/4}(\log x)^{C/2}\right)\\ &= \left(1-\frac{1}{[\mathbb{Q}(E[2]):\mathbb{Q}]}\right)\mathrm{li}(x)+O_{A,B}\left(\frac{x}{(\log x)^B}\right)+O(\log N)\\ &+ \sum_{3\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}}\mu(m)P(x,m). \qquad (3.1)\end{aligned}$$

Here we used the fact that $N(\mathfrak{f})\leq N$ (see Remark 2.8).

For square free $m\geq 3$, we note that the primes that split completely in $\mathbb{Q}(E[m])$ are closely related to the prime ideals of $\mathfrak{O}_K$ that split completely in $K(E[m])$. Observe that by Lemma 2.6, for $m\geq 3$ we have $\mathbb{Q}(E[m])=K(E[m])$, and by Lemma 2.4 a prime that splits completely in $\mathbb{Q}(E[m])$ it will split completely in $\mathfrak{O}_K$ also. Thus, if we let

$$\tilde{P}(x,\mathfrak{m})=\#\{\mathfrak{p}:\ N(\mathfrak{p})\leq x,\ \mathfrak{p}\nmid\mathfrak{f}\mathfrak{m},\ \mathfrak{p}\text{ splits completely in }K(E[m])\},$$

we have

$$P(x,m)=\frac{1}{2}\tilde{P}(x,m)+O\left(\frac{x^{1/2}}{\log x}\right)+O(\log N). \qquad (3.2)$$

Justification for this identity is the following. Since $m \geq 3$, then any prime p ($\neq 2, 3$) in the set that $P(x,m)$ counts is an ordinary prime and so $p\mathfrak{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathfrak{O}_K$. So such a prime p splits completely in $\mathbb{Q}(E[m]) = K(E[m])$ if and only if both $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ split completely in $K(E[m])$. However $\mathfrak{p}$ splits completely in $K(E[m])$ if and only if $\bar{\mathfrak{p}}$ splits completely in $K(E[m])$, this explains the coefficient $1/2$ of $\tilde{P}(x,m)$ in the above identity. Also we use the fact that the number of prime ideals $\mathfrak{p}$ of $\mathfrak{O}_K$ with degree 2 over $\mathbb{Q}$ and $N(\mathfrak{p}) \leq x$ is $O(x^{1/2}/\log x)$.

Now an application of (3.2) yields

$$\begin{aligned}\sum_{3\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}} \mu(m)P(x,m) &= \frac{1}{2}\sum_{3\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}} \mu(m)\frac{\mathrm{li}(x)}{[K(E[m]):K]} \\ &\quad +\frac{1}{2}\sum_{3\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}} \mu(m)\left(\tilde{P}(x,\mathfrak{m})- \right. \\ &\quad \left.\frac{\mathrm{li}(x)}{[K(E[m]):K]}\right) + O\left(\frac{x^{3/4}}{(\log x)^{1+C/2}}\right) \\ &\quad +O\left(\log N\frac{x^{1/4}}{(\log x)^{C/2}}\right). \qquad (3.3)\end{aligned}$$

Observe that by Lemma 2.7, we have

$$\tilde{P}(x,\mathfrak{m}) - \frac{\mathrm{li}(x)}{[K(E[m]):K]} = \sum_{i=1}^{t(m)}\left(\pi_K(x,\mathfrak{fm},\mathfrak{m}_i) - \frac{\mathrm{li}(x)}{h(\mathfrak{fm})}\right).$$

So

$$\begin{aligned}&\sum_{3\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}} \left|\tilde{P}(x,\mathfrak{m}) - \frac{\mathrm{li}(x)}{[K(E[m]):K]}\right| \\ &\qquad \leq \sum_{N(\mathfrak{fm})\leq \frac{x^{1/2}}{\mathcal{L}^C}}\sum_{i=1}^{t(m)}\left|\pi_K(x,\mathfrak{fm},\mathfrak{m}_i) - \frac{\mathrm{li}(x)}{h(\mathfrak{fm})}\right|,\end{aligned}$$

which is

$$\leq \quad c\,\varphi(\mathfrak{f})\prod_{\mathfrak{p}|\mathfrak{f}}\left(1+\frac{1}{N(\mathfrak{p})-1}\right)\sum_{N(\mathfrak{q})\leq \frac{x^{1/2}}{\mathcal{L}^C}}\max_{(\mathfrak{a},\mathfrak{q})=1}\left|\pi_K(x;\mathfrak{q},\mathfrak{a}) - \frac{\mathrm{li}(x)}{h(\mathfrak{q})}\right|, \qquad (3.4)$$

by Lemma 2.7. We know that $N = N(\mathfrak{f})|d_K|$ (see Remark 2.8). So $\varphi(\mathfrak{f}) \leq N(\mathfrak{f}) \leq N$ and

$$\prod_{\mathfrak{p}|\mathfrak{f}}\left(1+\frac{1}{N(\mathfrak{p})-1}\right) \quad \leq 2 \quad \prod_{\mathfrak{p}|\mathfrak{f}}\left(1+\frac{1}{N(\mathfrak{p})}\right)$$

$$\leq 2 \sum_{N(\mathfrak{a})\leq N(\mathfrak{f})} \frac{1}{N(\mathfrak{a})} \ll_K \log N(\mathfrak{f}) \ll_K \log N.$$

Putting these together, and applying Lemma 2.9 in (3.4) yields

$$\sum_{3\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}} \left|\tilde{P}(x,\mathfrak{m}) - \frac{\mathrm{li}(x)}{[K(E[m]):K]}\right|$$
$$\ll_{K,A,B} N\log N \frac{x}{(\log x)^{A+B+1}}. \tag{3.5}$$

Note that $T(\mathfrak{q}) \leq 6$. Again since there are only nine imaginary quadratic fields K of class number 1, we can assume that the implied constant does not depend on K.

Now from (3.1), (3.3), and (3.5), and for $N \leq (\log x)^A$, we have

$$\begin{aligned} C(x,N,E) &= \sum_{1\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}} \frac{\mu(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\mathrm{li}(x) + O_{A,B}\left(N\log N\frac{x}{(\log x)^{A+B+1}}\right) \\ &= \sum_{1\leq m\leq \frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}} \frac{\mu(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\mathrm{li}(x) + O_{A,B}\left(\frac{x}{(\log x)^{B}}\right). \end{aligned}$$

Since by [3, Proposition 3.8], we have $n_m \gg \varphi(m)^2 \gg m^2/(\log\log m)^2$, we can write

$$\sum_{m>\frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}} \frac{\mu(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]} \ll \sum_{m>\frac{x^{1/4}}{N(\mathfrak{f})\mathcal{L}^{C/2}}} \frac{(\log\log m)^2}{m^2} \ll \frac{(\log x)^{\frac{A}{2}+\frac{C}{4}}}{x^{1/8}}.$$

Here we used the inequality $m/\varphi(m) \ll \log\log m$ (see [6, Theorem 328]). So we have

$$C(x,N,E) = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]}\mathrm{li}(x) + O_{A,B}\left(\frac{x}{(\log x)^{B}}\right),$$

for $N \leq (\log x)^A$. □

Acknowledgement

The first author would like to thank Dragos Ghioca for several helpful discussions related to this work. Also the authors would like to thank the referee for helpful comments and suggestions. The research of both authors is partially supported by NSERC.

References

1. A. Akbary, On the greatest prime divisor of N_p, *J. Ramanujan Math. Soc*., **23** (2008), 259-282.

2. A. C. Cojocaru, Cyclicity of CM elliptic curves mod p, *Trans. Amer. Math. Soc*., **355** (2003), 2651-2662.

3. 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), 601-625.

4. L. J. Goldstein, A generalization of the Siegel-Walfisz theorem, *Trans. Amer. Math. Soc*., **149** (1970), 417-429.

5. R. Gupta and M. R. Murty, Cyclicity and generation of points mod p on elliptic curves, *Invent. Math*., **101** (1990), 225-235.

6. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, 1979.

7. M. N. Huxley, The large sieve inequality for algebraic number fields III, *J. London Math. Soc*., **3** (1971), 233-240.

8. J. Lagarias and A. Odlyzko, Effective versions of the Chebotarev density theorem, in *Algebraic Number Fields*, ed. A. Fröhlich, pp. 409-464, Academic Press, London, 1977.

9. S. Lang, *Elliptic Functions*, Graduate Text in Mathematics, **112**, Springer-Verlag, New York, 1987.

10. M. R. Murty, On Artin's conjecture, *J. Number Theory*, **16** (1983), 147-168.

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

12. J. -P. Serre, Résumé des cours de l'année scolaire 1977-1978, Annuaire du Collège de France, 1978, 67-70, in *Collected Papers, vol. III*, Springer, 1985.

13. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Text in Mathematics, **106**, Springer, New York, 1986.

14. J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, **151**, Springer, New York, 1994.