Journal of Number Theory, October 2002, 335–350

On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves

Alina Carmen Cojocaru

ABSTRACT: Let E be an elliptic curve defined over $\mathbb{Q}$ and without complex multiplication. For a prime p of good reduction, let $\overline{E}$ be the reduction of E modulo p. Assuming that certain Dedekind zeta functions have no zeros in $\mathrm{Re}(s) > 3/4$, we determine how often $\overline{E}(\mathbb{F}_p)$ is a cyclic group. This result was previously obtained by J. -P. Serre using the full Generalized Riemann Hypothesis for the same Dedekind zeta functions considered by us.

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$. For a prime p of good reduction we denote by $\overline{E}$ the reduction of E modulo p. If the Mordell-Weil group of rational points $E(\mathbb{Q})$ of E has rank at least 1, and if we are given a rational point a on E, of infinite order, then we can formulate an elliptic curve analogue of Artin's problem on primitive roots, as proposed by S. Lang and H. Trotter in [LT]. The analogue is as follows: fix a rational point a on E of infinite order and determine the density of those primes p for which E has good reduction and $\overline{E}(\mathbb{F}_p)$ is cyclic and generated by a modulo p. In considering this problem, we see that the implicit question of whether $\overline{E}(\mathbb{F}_p)$ is cyclic is being asked. In [Se2], J. -P. Serre showed that C. Hooley's conditional method [Ho, ch. 3] of proving Artin's conjecture on primitive roots can be adapted to prove that the set of primes p for which $\overline{E}(\mathbb{F}_p)$ is cyclic has a density. Serre's proof assumes the Generalized Riemann Hypothesis (denoted GRH) for certain Dedekind zeta functions. More precisely, we have:

Theorem 1.1 *(J. -P. Serre, 1976)*

Let E be an elliptic curve defined over $\mathbb{Q}$. For each prime q, let $L_q := \mathbb{Q}(E[q])$, where $E[q]$ is the set of $q-$division points of E over $\overline{\mathbb{Q}}$. Let $L_1 := \mathbb{Q}$, and for each square-free integer k, let $L_k := \prod_{q|k} L_q$. Denote by $f(x, \mathbb{Q})$ the number of primes $p \leq x$ such that E has good reduction at p and $\overline{E}(\mathbb{F}_p)$ is cyclic. Assuming GRH for the Dedekind zeta functions of L_k, we have

$$f(x, \mathbb{Q}) = C_E \operatorname{li} x + \mathrm{O}\left(\frac{x \log\log x}{(\log x)^2}\right),$$

where $C_E := \sum_{k=1}^{\infty} \frac{\mu(k)}{[L_k : \mathbb{Q}]}$ *and* $\operatorname{li} x = \int_2^x \frac{1}{\log t}\, dt$.

As shown in [Mu4, p. 327], $C_E \neq 0$ whenever E has an irrational point of order 2. If all the 2-division points are rational, then clearly $\overline{E}(\mathbb{F}_p)$ is not cyclic for all primes p, for, in this case, $\overline{E}(\mathbb{F}_p)$ contains the Klein four group for p sufficiently large.

In 1980 [Mu1, p.161-167], Ram Murty removed GRH in the result above for elliptic curves defined over $\mathbb{Q}$ and with complex multiplication. In 1987 [Mu3], he also demonstrated unconditionally the existence of infinitely many primes p for which $\overline{E}(\mathbb{F}_p)$ is cyclic for certain elliptic curves defined over $\mathbb{Q}$ and without complex multiplication. In 1990 [GM1], Rajiv Gupta and Ram Murty proved unconditionally that for an elliptic curve E defined over $\mathbb{Q}$, the group $\overline{E}(\mathbb{F}_p)$ is cyclic for infinitely many primes p if and only if E has an irrational 2-division point. In the case E has an irrational 2-division point, they obtained

$$\#\{p \leq x, E \text{ has good reduction at } p, \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \gg \frac{x}{\log^2 x}.$$

In this paper we will prove the following theorem:

Theorem 1.2 *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ and without complex multiplication. Using the same notation as in Theorem 1.1 and assuming that the Dedekind zeta functions of all L_k do not vanish on* $\mathrm{Re}(s) > 3/4$, *we have*

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

In proving Theorem 1.2, we will be careful to isolate the precise steps where we need to invoke the "quasi-Riemann Hypothesis" assumption. It turns out, as it will be seen below, that if our goal is the assertion

$$f(x, \mathbb{Q}) \sim C_E \operatorname{li} x,$$

then the "quasi-Riemann Hypothesis" need only be invoked at one step, the other steps being handled unconditionally.

The main tool used in the proofs of Theorems 1.1 and 1.2 is the Chebotarev density theorem, which we recall now. Let $L/\mathbb{Q}$ be a finite Galois extension of degree n_L and with discriminant d_L. For a positive real number x, let

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

The Chebotarev density theorem asserts that

$$\pi_1(x, L/\mathbb{Q}) \sim \frac{1}{n_L} \operatorname{li} x.$$

Effective versions of this theorem were given by J. Lagarias and A. Odlyzko [LO] and are as follows:

(a) there is an effective positive constant A and there is an absolute positive constant c, such that if

$$\sqrt{\frac{\log x}{n_L}} \geq c \max\left(\log |d_L|, |d_L|^{1/n_L}\right),$$

then

$$\pi_1(x, L/\mathbb{Q}) = \frac{1}{n_L} \operatorname{li} x + \mathrm{O}\left(x \exp\left(-A\sqrt{\frac{\log x}{n_L}}\right)\right),$$

where the implied constant is absolute (see [Mu2, p. 243]);

(b) if we assume GRH for the Dedekind zeta function of L, then

$$\pi_1(x, L/\mathbb{Q}) = \frac{1}{n_L} \operatorname{li} x + \mathrm{O}\left(\frac{x^{1/2}}{n_L} \log\left(|d_L| x^{n_L}\right)\right)$$

(see [Se3, p. 133]);

(c) if we assume that for the Dedekind zeta function of L we have a zero-free region of $\mathrm{Re}(s) > \delta$, then

$$\pi_1(x, L/\mathbb{Q}) = \frac{1}{n_L} \operatorname{li} x + \mathrm{O}\left(\frac{x^{\delta}}{n_L} \log\left(|d_L| x^{n_L}\right)\right)$$

(this result is not in the literature, however it is clear that the methods of [LO] and [Se3] can be used to deduce it).

In addition to the Chebotarev density theorem, we will use the Brun-Titchmarsh theorem, which asserts that, given any integer $q \geq 1$, any integer a coprime to q, and any real number x with $x > q$, we have

$$\pi(x, q, a) \leq \frac{2x}{\phi(q) \log(x/q)},$$

where $\pi(x, q, a)$ denotes the number of primes $p \leq x$ which are congruent to $a (\mathrm{mod}\, q)$ and $\phi(\cdot)$ is the classical Euler function (see, for example, [Mu5, p.147]). We will also use the elementary estimate

$$\sum_{q > y} \frac{1}{q^{r+1}} \ll \frac{1}{y^r \log y},$$

where y and r are fixed and the sum is over primes q.

Here, for two functions f and g with positive real values, we use the notation $f(x) \ll g(x)$ and $f(x) \asymp g(x)$ if we have positive constants c and c_1, c_2 such that, for all x, $f(x) \leq c g(x)$ and $c_1 g(x) \leq f(x) \leq c_2 g(x)$, respectively.

Acknowledgements: The results of this paper are contained in my doctoral thesis [acC]. I am very grateful to my doctoral thesis supervisor, Professor M. Ram Murty, for his many valuable suggestions and comments on previous versions of this paper.

2 Proof of Theorem 1.2

Let us observe that for a prime $p \geq 3$ of good reduction for E, the p-primary part of $\overline{E}(\mathbb{F}_p)$ is either trivial or of order p, for otherwise $p^2 | \#\overline{E}(\mathbb{F}_p)$, so that $p^2 \leq p + 1 + 2\sqrt{p}$ by Hasse's bound [Si, p. 131]. Since this is not possible for $p \geq 3$, we deduce that for such primes p, the $p-$primary part of $\overline{E}(\mathbb{F}_p)$ is always cyclic. Hence, to enumerate the primes p for which $\overline{E}(\mathbb{F}_p)$ is cyclic, it suffices to consider the q-primary components of the group for $q \neq p$.

From [Mu1, p.159] we know that

Lemma 2.1 *For an elliptic curve E defined over $\mathbb{Q}$ and for a prime p of good reduction and a prime $q \neq p$, we have that p splits completely in L_q if and only if $\overline{E}(\mathbb{F}_p)$ contains a $(q,q)-$ type subgroup (that is, a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$). Consequently, $\overline{E}(\mathbb{F}_p)$ is a cyclic group if and only if p does not split completely in the field extension $L_q = \mathbb{Q}(E[q])$ for any prime $q \neq p$.*

From now on p will be used to denote primes of good reduction for E and we shall omit to specify it. Also q will be used to denote rational primes. Using the lemma above, we obtain that

$$f(x,\mathbb{Q}) = \#\{p \leq x, p \text{ does not split completely in any } L_q \text{ for all primes } q \neq p\}.$$

Let us observe that if p splits completely in L_q for some q, then $q^2 | \#\overline{E}(\mathbb{F}_p)$. Therefore, $q^2 \leq p+1+2\sqrt{p}$ by Hasse's bound, and so $p \leq x$ gives $q \leq 2\sqrt{x}$.

We recall that the field extension $L_q/\mathbb{Q}$ has the following properties: it is normal, its ramified primes are divisors of qN, where N is the conductor of E, and $L_q \supseteq \mathbb{Q}(\zeta_q)$, where ζ_q denotes a primitive q-th root of unity (see [Si, p. 90, 98]). From classical results in the theory of elliptic curves, we know that the degree $n(q) := [L_q : \mathbb{Q}]$ is $\ll q^4$ for all q, and from results of Serre [Se1, p. 294], we have that, for elliptic curves without complex multiplication, the degree $n(q)$ is $\asymp q^4$ for q sufficiently large.

To estimate $f(x,\mathbb{Q})$ we start by using the simple asymptotic sieve as in [Mu1, p. 153-154]. For real numbers y and z (which will be optimally chosen later), let

$$N(x,y) := \#\{p \leq x, p \text{ does not split completely in any } L_q \text{ for } q \leq y\},$$

$$M(x,y,z) := \#\{p \leq x, p \text{ splits completely in some } L_q \text{ with } y \leq q \leq z\}.$$

Then

$$N(x,y) - M\left(x,y,2\sqrt{x}\right) \leq f(x,\mathbb{Q}) \leq N(x,y),$$

so that

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

We shall estimate each of $N(x,y)$ and $M\left(x,y,2\sqrt{x}\right)$, and then obtain an estimate for $f(x,\mathbb{Q})$.

2.1 Estimate for $N(x,y)$

By the inclusion-exclusion principle we have

$$N(x,y) = \sum_k{}' \mu(k)\pi_1(x, L_k/\mathbb{Q}),$$

where the sum is over all square-free positive integers k whose prime divisors are $\leq y$.

We want to estimate this sum by using the effective Chebotarev density theorem (a) stated in section 1. Let us recall the following result of Hensel [Se3, p. 130]: if $K/\mathbb{Q}$ is a finite normal field extension which is ramified only at the primes $p_1, p_2, \ldots, p_m$, then

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

where $\mathrm{disc}(K/\mathbb{Q})$ is the discriminant of $K/\mathbb{Q}$. Applying this result to the field extensions $L_k/\mathbb{Q}$, we obtain

$$n(k)|d_k|^{2/n(k)} \ll k^6$$

and

$$n(k)\left(\log|d_k|\right)^2 \ll k^{12}\log^2 k \ll k^{14},$$

where $n(k) = [L_k : \mathbb{Q}]$ and $d_k = \mathrm{disc}(L_k/\mathbb{Q})$, and where we used that $n(k) \ll k^4$. We want to choose y such that for all square-free integers k whose prime divisors are $\leq y$, we have

$$k^{14} \ll \log x.$$

Let us observe that

$$k \leq \prod_{p\leq y} p = \exp\left(\sum_{p\leq y}\log p\right) \leq \exp(2y).$$

We choose

$$y = d\log\log x$$

for some positive constant d such that $\exp(2y) \ll (\log x)^{1/14}$. Then the hypothesis of the unconditional Chebotarev density theorem (a) is satisfied and we obtain:

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

for some positive effective constant A. To handle the error term we observe that $n(k) \ll k^4 \ll (\log x)^{2/7}$, and that there are at most 2^y, hence at most $(\log x)^d$, square-free numbers composed of primes $\leq y$. Hence the error term becomes

$$\mathrm{O}\left((\log x)^d x\exp\left(-A(\log x)^{5/14}\right)\right),$$

which is $\mathrm{O}\left(x(\log x)^{-B}\right)$ for any positive constant B sufficiently large.

Thus we showed that

$$N(x,y) = \left(\sum_k{}' \frac{\mu(k)}{n(k)}\right)\mathrm{li}\, x + \mathrm{O}\left(x(\log x)^{-B}\right).$$

Let us note that this estimate is unconditional. In his proof, J. -P. Serre used the conditional version of Chebotarev density theorem (b) (see [Mu1, p. 155]) to treat $N(x,y)$.

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

Let us write

$$M\left(x,y,2\sqrt{x}\right) \leq M\left(x,y,\frac{x^{1/4}}{(\log x)^3}\right) + M\left(x,\frac{x^{1/4}}{(\log x)^3},x^{1/4}(\log x)^3\right) + M\left(x,x^{1/4}(\log x)^3,2\sqrt{x}\right)$$

and estimate each of the three terms.

1. To estimate the first term, we write

$$\begin{aligned} M\left(x, y, \frac{x^{1/4}}{(\log x)^3}\right) &\leq \sum_{y \leq q \leq \frac{x^{1/4}}{(\log x)^3}} \pi_1(x, L_q/\mathbb{Q}) \\ &= \sum_{y \leq q \leq (\log x)^{1/14}} \pi_1(x, L_q/\mathbb{Q}) + \sum_{(\log x)^{1/14} < q \leq \frac{x^{1/4}}{(\log x)^3}} \pi_1(x, L_q/\mathbb{Q}). \end{aligned}$$

For the first sum above we proceed as with $N(x, y)$ and obtain

$$\begin{aligned} \sum_{y \leq q \leq (\log x)^{1/14}} \pi_1(x, L_q/\mathbb{Q}) &= \sum_{y \leq q \leq (\log x)^{1/14}} \frac{\operatorname{li} x}{n(q)} + \sum_{y \leq q \leq (\log x)^{1/14}} \mathrm{O}\left(x \exp\left(-A\sqrt{\frac{\log x}{n(q)}}\right)\right) \\ &= \sum_{y \leq q \leq (\log x)^{1/14}} \frac{\operatorname{li} x}{n(q)} + \mathrm{O}\left(x(\log x)^{-C}\right) \end{aligned}$$

for any positive constant C sufficiently large.

To estimate the second sum, we use the conditional version of the Chebotarev density theorem (c) with $\delta = 3/4$, and Hensel's result. We note that this is the only place where we use a "quasi-Riemann Hypothesis".

$$\begin{aligned} \sum_{(\log x)^{1/14} < q \leq \frac{x^{1/4}}{(\log x)^3}} \pi_1(x, L_q/\mathbb{Q}) &\ll \sum_{(\log x)^{1/14} < q \leq \frac{x^{1/4}}{(\log x)^3}} \frac{\operatorname{li} x}{n(q)} + \sum_{(\log x)^{1/14} < q \leq \frac{x^{1/4}}{(\log x)^3}} \frac{x^{3/4}}{n(q)} \log\left(|d_q| x^{n(q)}\right) \\ &\ll \sum_{(\log x)^{1/14} < q \leq \frac{x^{1/4}}{(\log x)^3}} \frac{\operatorname{li} x}{n(q)} + \sum_{(\log x)^{1/14} < q \leq \frac{x^{1/4}}{(\log x)^3}} x^{3/4} \log(qx). \end{aligned}$$

For the error term $\displaystyle\sum_{(\log x)^{1/14} < q \leq \frac{x^{1/4}}{(\log x)^3}} x^{3/4} \log(qx)$ we have:

$$\begin{aligned} \sum_{(\log x)^{1/14} < q \leq \frac{x^{1/4}}{(\log x)^3}} x^{3/4} \log(qx) &\leq x^{3/4} \sum_{q \leq \frac{x^{1/4}}{(\log x)^3}} \log q + x^{3/4} (\log x) \sum_{q \leq \frac{x^{1/4}}{(\log x)^3}} 1 \\ &\ll \frac{x}{(\log x)^2}. \end{aligned}$$

Thus

$$M\left(x, y, \frac{x^{1/4}}{(\log x)^3}\right) \ll \operatorname{li} x \sum_{y \leq q \leq \frac{x^{1/4}}{(\log x)^3}} \frac{1}{n(q)} + \mathrm{O}\left(x(\log x)^{-C}\right) + \mathrm{O}\left(\frac{x}{(\log x)^2}\right).$$

Let us remark that, in estimating $M\left(x, y, \frac{x^{1/4}}{(\log x)^3}\right)$, we have split the sum over q such that $y \leq q \leq (\log x)^{1/14}$ and $(\log x)^{1/14} < q \leq \frac{x^{1/4}}{(\log x)^3}$, in order to isolate the range where we need to invoke the 3/4-quasi-Riemann Hypothesis.

2. To estimate the second term, let us observe that $L_q \supseteq \mathbb{Q}(\zeta_q)$ implies that any prime p which splits completely in L_q is congruent to $1 (\mathrm{mod}\, q)$. By using the Brun-Titchmarsh theorem and elementary number theory estimates such as Mertens' theorem, we obtain:

$$\begin{aligned} M\left(x, \frac{x^{1/4}}{(\log x)^3}, x^{1/4}(\log x)^3\right) &\ll \sum_{\frac{x^{1/4}}{(\log x)^3} < q \leq x^{1/4}(\log x)^3} \frac{x}{q \log \frac{x}{q}} \\ &\ll \frac{x}{\log x} \sum_{\frac{x^{1/4}}{(\log x)^3} < q \leq x^{1/4}(\log x)^3} \frac{1}{q} \\ &\ll \frac{x}{(\log x)^2} \sum_{\frac{x^{1/4}}{(\log x)^3} < q \leq x^{1/4}(\log x)^3} \frac{\log q}{q} \\ &\ll \frac{x}{(\log x)^2} \left(\log\left(x^{1/4}(\log x)^3\right) - \log \frac{x^{1/4}}{(\log x)^3}\right) \\ &\ll \frac{x \log\log x}{(\log x)^2}. \end{aligned}$$

Thus

$$M\left(x, \frac{x^{1/4}}{(\log x)^3}, x^{1/4}(\log x)^3\right) = \mathrm{O}\left(\frac{x \log\log x}{(\log x)^2}\right).$$

3. Now we shall estimate the third term $M\left(x, x^{1/4}(\log x)^3, 2\sqrt{x}\right)$. This is where we improve Serre's method of proving Theorem 1.1.

For each integer a with $|a| \leq 2\sqrt{x}$, we consider the set

$$S_a(q) := \{p \leq x, a_p = a \text{ and } p \text{ splits completely in } L_q\},$$

where $a_p := p + 1 - \#\overline{E}(\mathbb{F}_p)$. Then

$$M\left(x, x^{1/4}(\log x)^3, 2\sqrt{x}\right) \leq \sum_{x^{1/4}(\log x)^3 < q \leq 2\sqrt{x}} \sum_{\substack{a \in \mathbb{Z}, \\ |a| \leq 2\sqrt{x}}} \#S_a(q).$$

We observe that $p \in S_a(q)$ implies $p \equiv 1 (\mathrm{mod}\, q)$ and $p + 1 - a \equiv 0 (\mathrm{mod}\, q^2)$, hence $q | a - 2$. Then, for $u = x^{1/4}(\log x)^3$,

$$\sum_{u < q \leq 2\sqrt{x}} \sum_{\substack{a \in \mathbb{Z}, \\ |a| \leq 2\sqrt{x}}} \#S_a(q) \leq \sum_{u < q \leq 2\sqrt{x}} \sum_{\substack{a \in \mathbb{Z}, \\ |a| \leq 2\sqrt{x} \\ a \neq 2, q | a-2}} \sum_{\substack{p \leq x, \\ q^2 | p+1-a}} 1 + \sum_{u < q \leq 2\sqrt{x}} \sum_{\substack{p \leq x, \\ q^2 | p-1}} 1 =: \sum\nolimits^{*} + \sum\nolimits^{**},$$

where the second sum arises from the case $a = 2$, for which we have $q^2 | p - 1$.

We estimate $\sum^{*}$ and $\sum^{**}$. Let us note that for fixed integers α and β, we have the elementary estimate

$$\#\{n \leq x, n \equiv \alpha (\mathrm{mod}\, \beta)\} \leq \frac{x}{\beta} + 1,$$

where n denotes a positive integer. Hence we obtain:

$$\begin{aligned}\sum^{*} &\leq \sum_{u<q\leq 2\sqrt{x}} \sum_{\substack{a\in\mathbb{Z},\\ |a|\leq 2\sqrt{x}\\ a\neq 2, q|a-2}} \left(\frac{x}{q^2}+1\right)\\ &\ll \sum_{u<q\leq 2\sqrt{x}} \left(\frac{x}{q^2}+1\right)\left(\frac{\sqrt{x}}{q}+1\right)\\ &\ll \frac{x^{3/2}}{u^2\log u}+\frac{x}{u\log u}+\sqrt{x}\log x+\sqrt{x};\end{aligned}$$

$$\sum^{**} \leq \sum_{u<q\leq 2\sqrt{x}} \left(\frac{x}{q^2}+1\right) \ll \frac{x}{u\log u}+\sqrt{x}.$$

We plug in $u = x^{1/4}(\log x)^3$ and obtain

$$M\left(x, x^{1/4}(\log x)^3, 2\sqrt{x}\right) = \mathrm{O}\left(\frac{x}{(\log x)^7}\right).$$

2.3 Putting everything together

Using the estimates obtained in the previous sections we get that, for any sufficiently large B,

$$\begin{aligned}f(x,\mathbb{Q}) &= \operatorname{li} x \sum_k{}' \frac{\mu(k)}{n(k)}\\ &+ \mathrm{O}\left(\operatorname{li} x \sum_{y<q\leq \frac{x^{1/4}}{(\log x)^3}} \frac{1}{n(q)}\right) + \mathrm{O}\left(x(\log x)^{-B}\right) + \mathrm{O}\left(\frac{x}{(\log x)^2}\right)\\ &+ \mathrm{O}\left(\frac{x\log\log x}{(\log x)^2}\right) + \mathrm{O}\left(\frac{x}{(\log x)^7}\right).\end{aligned}$$

Let us analyze $\operatorname{li} x \sum_k{}' \frac{\mu(k)}{n(k)}$ and $\operatorname{li} x \sum_{y<q\leq \frac{x^{1/4}}{(\log x)^3}} \frac{1}{n(q)}$. For the first sum we write

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

where $\sum_k{}''$ means that the sum is over those square-free positive integers k for which there exists a prime divisor $q > y$.

We recall that $n(q) = (q^2-1)(q^2-q)$ for q sufficiently large (see [Se1, p. 294]), and, we note that, more precisely, this equality holds for any prime $q \geq aN(\log\log N)^{1/2}$,

where a is a positive absolute constant and N is the conductor of the elliptic curve (see, for example, [acC] or [Kr]). We write the square-free integer k as

$$k = k_1 k_2,$$

where k_1 is composed of primes $< aN(\log\log N)^{1/2}$, and k_2 is composed of primes $\geq aN(\log\log N)^{1/2}$. As explained in [acC], we have

$$n(k) = n(k_1)n(k_2) \geq \phi(k_1)n(k_2) = \phi(k_1)\prod_{q|k_2}\left(q^2-1\right)\left(q^2-q\right) \gg \phi(k_1)(k_2)^4,$$

where we used that $L_{k_1} \supseteq \mathbb{Q}(\zeta_{k_1})$.

We denote by $\sum_{k_1}$ the sum running over square-free positive integers k_1 composed of primes $< aN(\log\log N)^{1/2}$, and by $\sum_{k_2}''$ the sum running over square-free positive integers k_2 composed of primes $\geq aN(\log\log N)^{1/2}$ and having a prime divisor $> y$ (here we also use that $y = y(x) \geq aN(\log\log N)^{1/2}$). Then we have (remembering that we are summing over square-free numbers):

$$\sum_k{}'' \frac{\mu(k)}{n(k)} \leq \sum_{k=k_1k_2}{}'' \frac{1}{\phi(k_1)n(k_2)} \ll \sum_{k_1}\frac{1}{\phi(k_1)}\sum_{k_2}{}''\frac{1}{(k_2)^4} \ll \sum_{q>y}\frac{1}{q^4} \ll \frac{1}{y^3\log y}.$$

Since in fact $y = d\log\log x$, we obtain

$$\operatorname{li} x \sum_k{}' \frac{\mu(k)}{n(k)} = \operatorname{li} x \sum_k \frac{\mu(k)}{n(k)} + \mathrm{O}\left(\frac{x}{(\log x)(\log\log x)^3\log\log\log x}\right).$$

For the second sum $\operatorname{li} x \sum_{y<q\leq\frac{x^{1/4}}{(\log x)^3}} \frac{1}{n(q)}$ we note again that

$$\sum_{y<q\leq\frac{x^{1/4}}{(\log x)^3}} \frac{1}{n(q)} \ll \sum_{q\geq y}\frac{1}{q^4} \ll \frac{1}{y^3\log y}.$$

Hence

$$\operatorname{li} x \sum_{y<q\leq\frac{x^{1/4}}{(\log x)^3}} \frac{1}{n(q)} = \mathrm{O}\left(\frac{x}{(\log x)(\log\log x)^3\log\log\log x}\right).$$

These estimates give us

$$f(x,\mathbb{Q}) = C_E \operatorname{li} x + \mathrm{O}\left(\frac{x}{(\log x)(\log\log x)^3\log\log\log x}\right).$$

If we use the conditional effective Chebotarev density theorem (c) for estimating $N(x,y)$ and $M\left(x,y,\frac{x^{1/4}}{(\log x)^3}\right)$, with y chosen such that

$$2^y y = \frac{x^{1/4}}{(\log x)^3},$$

then we obtain

$$f(x,\mathbb{Q}) = C_E \operatorname{li} x + \mathrm{O}\left(\frac{x\log\log x}{(\log x)^2}\right),$$

that is, the error term is the same as the one obtained by Serre by assuming the (full) Generalized Riemann Hypothesis for the Dedekind zeta functions of L_k.

Indeed, using version (c) of the Chebotarev density theorem with $\delta = \frac{3}{4}$, we obtain

$$N(x,y) = \left(\sum_k{}' \frac{\mu(k)}{n(k)}\right) \operatorname{li} x + \sum_k{}' \mathrm{O}\left(x^{3/4}\left(\frac{\log|d_k|}{n(k)} + \log x\right)\right).$$

We use Hensel's result as before and obtain that the error term above is

$$\sum_k{}' \mathrm{O}\left(x^{3/4}\left(\log k + \log x\right)\right).$$

Since the number of square-free positive integers k whose prime divisors are $\leq y$ is at most 2^y, and since such a k is $\leq \exp(2y)$, we have that the error term is in fact

$$\mathrm{O}\left(2^y x^{3/4}(y + \log x)\right).$$

Our new choice of y makes this error term be $\mathrm{O}\left(\frac{x}{(\log x)^2}\right)$. For $M\left(x, y, \frac{x^{1/4}}{(\log x)^3}\right)$ we proceed in a similar way and obtain

$$M\left(x, y, \frac{x^{1/4}}{(\log x)^3}\right) \leq \operatorname{li} x \sum_{y \leq q < \frac{x^{1/4}}{(\log x)^3}} \frac{1}{n(q)} + \mathrm{O}\left(\frac{x}{(\log x)^3}\right).$$

The terms $M\left(x, \frac{x^{1/4}}{(\log x)^3}, x^{1/4}(\log x)^3\right)$ and $M\left(x, x^{1/4}(\log x)^3, 2\sqrt{x}\right)$ are estimated exactly as before. It remains to analyze the sums $\operatorname{li} x \sum_k{}'' \frac{\mu(k)}{n(k)}$ and $\operatorname{li} x \sum_{y < q \leq \frac{x^{1/4}}{(\log x)^3}} \frac{1}{n(q)}$. Both are $\mathrm{O}\left(\frac{x}{y^3(\log x)(\log y)}\right)$, which, with the new choice of y, is $\mathrm{O}\left(\frac{x}{(\log x)^4}\right)$. Hence the biggest error term we get is $\mathrm{O}\left(\frac{x(\log\log x)}{(\log x)^2}\right)$ and this gives us the asymptotic formula we claimed above.

The proof we presented in detail points out that in order to have an unconditional estimate for $f(x,\mathbb{Q})$ in the non-CM case, we need to find good unconditional estimates for $M\left(x, (\log x)^{1/14}, \frac{x^{1/4}}{(\log x)^3}\right)$.

2.4 Final remarks

Our new contribution to this problem is the unconditional treatment of $M\left(x, x^{1/4}(\log x)^3, 2\sqrt{x}\right)$. It may be useful in later research to know that this term can be treated in other ways as follows.

For a fixed integer $a \neq 2, |a| \leq 2\sqrt{x}$, we first show that if we have $p \leq x$ such that $a_p = a$ and p splits completely in some L_q with $x^{1/4}(\log x)^3 < q \leq 2\sqrt{x}$, then q is uniquely determined by a. We have seen that such a q satisfies

$$q | (a-2).$$

If we have two such primes $q_1 \neq q_2$, with $x^{1/4}(\log x)^3 < q_1, q_2 \leq 2\sqrt{x}$, then the above divisibility relation and Hasse's inequality give us

$$\sqrt{x}(\log x)^6 < 2\sqrt{x} - 2,$$

which is a contradiction.

Thus for each $a \neq 2$ we have at most one prime q_a such that $q_a|(a-2)$ and $x^{1/4}(\log x)^3 < q_a \leq 2\sqrt{x}$. Then, with notation as in section 2.2,

$$\begin{aligned}
\sum_{x^{1/4}(\log x)^3 < q \leq 2\sqrt{x}} \sum_{\substack{a\in\mathbb{Z},\\ a\neq 2,\\ |a|\leq 2\sqrt{x}}} \#S_a(q) &\leq \sum_{\substack{a\in\mathbb{Z},\\ a\neq 2,\\ |a|\leq 2\sqrt{x}}} \#\left\{p \leq x, p \equiv a-1 (\mathrm{mod}\, q_a^2)\right\} \\
&\leq \sum_{\substack{a\in\mathbb{Z},\\ a\neq 2,\\ |a|\leq 2\sqrt{x}}} \left(\frac{x}{q_a^2}+1\right) \\
&< \left(\frac{x^{1/2}}{(\log x)^6}+1\right) 4\sqrt{x} \\
&= \mathrm{O}\left(\frac{x}{(\log x)^6}\right).
\end{aligned}$$

This argument is in the style of [GM1, th. 1, p. 227-228].

We can also use the following argument (see again the notation in section 2.2).

$$\begin{aligned}
\sum\nolimits^* &= \sum_{\substack{a\in\mathbb{Z},\\ |a|\leq 2\sqrt{x}\\ a\neq 2}} \sum_{\substack{x^{1/4}(\log x)^3 < q \leq 2\sqrt{x},\\ q|a-2}} \sum_{\substack{p\leq x,\\ q^2|p+1-a}} 1 \\
&\ll \sum_{\substack{a\in\mathbb{Z},\\ |a|\leq 2\sqrt{x}\\ a\neq 2}} \sum_{\substack{x^{1/4}(\log x)^3 < q \leq 2\sqrt{x},\\ q|a-2}} \left(\frac{x}{q^2}+1\right) \\
&\ll \sum_{\substack{a\in\mathbb{Z},\\ |a|\leq 2\sqrt{x}\\ a\neq 2}} \sum_{\substack{x^{1/4}(\log x)^3 < q \leq 2\sqrt{x},\\ q|a-2}} \left(\frac{x^{1/2}}{(\log x)^6}+1\right) \\
&\ll \sum_{\substack{a\in\mathbb{Z},\\ a\neq 2,\\ |a|\leq 2\sqrt{x}}} \frac{x^{1/2}}{(\log x)^6}\nu(a-2),
\end{aligned}$$

with $\nu(t)$ denoting the number of distinct prime divisors of t. Since the average order of $\nu(t)$ is $\log\log t$, we obtain that the sum is

$$\ll \frac{x \log\log x}{(\log x)^6}.$$

This estimate is slightly weaker than the one we had in section 2.2, but good enough for our purpose.

Let us note that for $\sum^{**}$ we can use the estimate

$$\sum^{**} \ll \#\{p \leq x, a_p = 2\} = \mathrm{O}\left(\frac{x(\log\log x)^2}{(\log x)^2}\right)$$

(see [KMu, Theorem 5.1, p. 302]). This, again, is a slightly weaker bound than the one we obtained in section 2.2 , and will make the final error term in the asymptotic formula for $f(x, \mathbb{Q})$ be equal to $\mathrm{O}\left(\frac{x(\log\log x)^2}{(\log x)^2}\right)$.

REFERENCES

[acC] A. C. Cojocaru -"Cyclicity of elliptic curves modulo p", PhD thesis, Queen's University at Kingston, Canada, 2002

[GM1] R. Gupta, M. R. Murty -"Cyclicity and generation of points modulo p on elliptic curves", Inventiones mathematicae 101, 1990, p. 225-235

[Ho] C. Hooley -"Applications of sieve methods to the theory of numbers", Cambridge University Press 1976

[Kr] A. Kraus -"Une remarque sur les points de torsion des courbes elliptiques", C. R. Acad. Sci. Paris, t. 321, Série I, 1995, p. 1143-1146

[KMu] V. K. Murty -"Modular forms and Chebotarev density theorem II", in Analytic Number Theory, Y.Motohashi (ed.), Cambridge University Press 1997, p. 287-308

[LO] J. Lagarias, A. Odlyzko -"Effective versions of the Chebotarev density theorem", in Algebraic Number Fields, A. Fröhlich (ed.) New York: Academic Press 1977, p. 409-464

[LT] S. Lang, H. Trotter -"Primitive points on elliptic curves", Bulletin of the American Mathematical Society vol. 83, no. 2, March 1977, p.289-292

[Mu1] M. R. Murty -"On Artin's conjecture", Journal of Number Theory vol. 16, no. 2, April 1983, p. 147-168

[Mu2] M. R. Murty -"An analogue of Artin's conjecture for abelian extensions", Journal of Number Theory vol. 18, no. 3, June 1984, p. 241-248

[Mu3] M. R. Murty -"On the supersingular reduction of elliptic curves", Proc. Indian Acad. Sci. (Math. Sci.) vol. 97, no. 1-3, December 1987, p. 247-250

[Mu4] M. R. Murty -"Artin's conjecture and elliptic analogues", Sieve Methods, Exponential Sums and their Applications in Number Theory, Cambridge University Press 1996, p. 325-344

[Mu5] M. R. Murty -"Problems in analytic number theory", Graduate Texts in Mathematics, Vol. 206, Springer Verlag, 2001

[Se1] J. -P. Serre -"Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques", Invent. Math. 15, 1972, p. 259-331

[Se2] J. -P. Serre -"Résumé des cours de 1977-1978", Annuaire du Collège de France 1978, p. 67-70, in Collected Papers, volume III, Springer Verlag, 1986, p. 465-468

[Se3] J. -P. Serre -"Quelques applications du théorème de densité de Chebotarev", Publ. Math. I. H. E. S., no. 54, 1981, p. 123-201

[Si] J. H. Silverman -"The arithmetic of elliptic curves", Graduate Texts in Mathematics, Vol. 106, Springer Verlag, 1986

Alina Carmen Cojocaru

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