Mathematische Annalen

Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem

Alina Carmen Cojocaru · M. Ram Murty

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. For a prime $p \nmid N$ we denote by $\overline{E}$ the reduction of E modulo p. We obtain an asymptotic formula for the number of primes $p \le x$ for which $\overline{E}(\mathbb{F}_p)$ is cyclic, assuming a certain generalized Riemann hypothesis. The error terms that we get are substantial improvements of earlier work of J-P. Serre and M. Ram Murty. We also consider the problem of finding the size of the smallest prime $p = p_E$ for which the group $\overline{E}(\mathbb{F}_p)$ is cyclic and we show that, under the generalized Riemann hypothesis, $p_E = \mathbb{O}\left((\log N)^{4+\varepsilon}\right)$ if E is without complex multiplication, and $p_E = \mathbb{O}\left((\log N)^{2+\varepsilon}\right)$ if E is with complex multiplication, for any $0 < \varepsilon < 1$.

Mathematics Subject Classification (2000): 11G05, 11N36, 11R45

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. For a prime $p \nmid N$ let $\overline{E}$ be the reduction of E modulo p. This is again an elliptic curve, defined over the finite field $\mathbb{F}_p$ with p elements. Many natural and interesting questions arise regarding the group $\overline{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of $\overline{E}$. The most basic ones are to estimate the size and to find the structure of the group $\overline{E}(\mathbb{F}_p)$. Other questions arise as elliptic curve analogues of classical problems and conjectures in number theory. We will discuss a few such examples in what follows.

First we recall that we have information about the size of $\overline{E}(\mathbb{F}_p)$. Indeed, if we write

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

A. C. Cojocaru[*]
Pinceton University, Mathematics Department, 810 Fine Hall, Washington Road, Princeton, NJ 08540, USA (e-mail: cojocaru@math.princeton.edu)

M. R. Murty[**]
Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, K7L 3N6 Canada (e-mail: murty@mast.queensu.ca)

for some integer a_p, where $\#S$ denotes the cardinality of a set S, then the famous Riemann Hypothesis for $\overline{E}$, proven by Hasse in 1933, asserts that

$$|a_p| \leq 2\sqrt{p}.$$

We also have information about the structure of $\overline{E}(\mathbb{F}_p)$. Let $\overline{\mathbb{F}}_p$ denote an algebraic closure of $\mathbb{F}_p$ and for a positive integer k let $\overline{E}(\overline{\mathbb{F}}_p)[k]$ and $\overline{E}(\mathbb{F}_p)[k]$ denote the groups of $\overline{\mathbb{F}}_p$- and $\mathbb{F}_p$-rational points of $\overline{E}$, respectively, which are annihilated by k. We see that $\overline{E}(\mathbb{F}_p)$ is a subgroup of $\overline{E}(\overline{\mathbb{F}}_p)[k]$ for some positive integer k such that $\#\overline{E}(\mathbb{F}_p)|k$, and we recall from classical theory that $\overline{E}(\overline{\mathbb{F}}_p)[k]$ is isomorphic to a subgroup of $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ (see [Si1, p.89]). We deduce that $\overline{E}(\mathbb{F}_p)$ can be written as the product of two finite cyclic groups $\mathbb{Z}/d_p\mathbb{Z} \times \mathbb{Z}/d_pe_p\mathbb{Z}$ for uniquely determined positive integers d_p, e_p, depending on p.

There is some interest in determining when the group $\overline{E}(\mathbb{F}_p)$ is actually *cyclic*. In 1975, I. Borosh, C.J. Moreno and H. Porta calculated the structure of $\overline{E}(\mathbb{F}_p)$ for various primes p and various elliptic curves E defined over $\mathbb{Q}$. They conjectured that for 'many' elliptic curves E defined over $\mathbb{Q}$, there are infinitely many primes p for which $\overline{E}(\mathbb{F}_p)$ is cyclic (see [BoMoPo, pp. 963–964]). As we will see (statement (5) below), this prediction is indeed true. In 1976, S. Lang and H. Trotter formulated an elliptic curve analogue of Artin's conjecture on primitive roots (see [LaTr]): let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N and having arithmetic rank ≥ 1; let $a \in E(\mathbb{Q})$ be a fixed rational point on E of infinite order; then the density of the primes $p \nmid N$ for which $\overline{E}(\mathbb{F}_p) = \langle a(\bmod p)\rangle$ exists. Clearly, showing that the density of the primes $p \nmid N$ for which $\overline{E}(\mathbb{F}_p)$ is cyclic exists is a natural subproblem of Lang and Trotter's conjecture.

With the increasing development of elliptic curve public-key cryptography initiated by N. Koblitz and V. Miller in the late 1980's, the problem of determining how often the group $\overline{E}(\mathbb{F}_p)$ is cyclic acquired yet a new significance. More precisely, certain public-key cryptosystems based on the presumed intractability of the discrete logarithm problem can be implemented using the group of points of an elliptic curve $\overline{E}$ defined over a finite field (see [Ko1]). Then one wants the cyclic group generated by a certain point $\overline{a}$ on $\overline{E}$ to have order divisible by a large prime. One way to accomplish this is to choose the elliptic curve $\overline{E}$ and the finite field so that the group of points of $\overline{E}$ has prime order; then the desired condition holds for any nontrivial point $\overline{a}$ on $\overline{E}$. To find such an elliptic curve, we can start by fixing an elliptic curve E defined over $\mathbb{Q}$ (possibly of rank at least 1), then we reduce E modulo primes p of good reduction and choose a prime p such that $\#\overline{E}(\mathbb{F}_p)$ is prime, or such that the group $\overline{E}(\mathbb{F}_p)$ is cyclic and generated by $a(\bmod p)$ for some fixed global point $a \in E(\mathbb{Q})$ of infinite order (if such a point exists). We are naturally led to the above 1976 question of Lang and Trotter on primitive points, or to the 1988 question of Koblitz of determining the proportion of the primes p for which $\#\overline{E}(\mathbb{F}_p)$ is prime (see [Ko2]). The cyclicity of $\overline{E}(\mathbb{F}_p)$ is a common subproblem of both these questions.

The precise goal in this paper is to determine an *explicit* asymptotic formula for

$$f(x, \mathbb{Q}) := \# \left\{ p \leq x : p \nmid N, \overline{E}(\mathbb{F}_p) \text{ cyclic} \right\} \tag{1}$$

and to obtain upper bounds in terms of the conductor N for the smallest prime $p = p_E$ for which $\overline{E}(\mathbb{F}_p)$ is cyclic. This latter problem can be viewed as an elliptic curve analogue of Linnik's question about the size of the least prime in an arithmetic progression (see [Li1] and [Li2]).

In 1976, J-P. Serre adapted Hooley's conditional proof of Artin's conjecture [Ho, chapter 3] to obtain an asymptotic formula for the number of primes $p \leq x$ for which the group of points modulo p of an elliptic curve is cyclic (see [Se3] or [Mu1, pp. 159–161]). Before stating Serre's result, let us introduce some more notation. For any positive integer k let $E[k]$ denote the group of points of E which are annihilated by k (called *the k-division group of E*) and let $\mathbb{Q}(E[k])$ be the field obtained by adjoining to $\mathbb{Q}$ the x- and y-coordinates of the points of $E[k]$ (called *the k-division field of E*). Serre showed that if we assume the generalized Riemann hypothesis (denoted GRH) for the Dedekind zeta functions of the division fields of E, then, as $x \to \infty$,

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \operatorname{li} x + \operatorname{error}(E, x), \tag{2}$$

where

$$\mathfrak{f}_E = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(E[k]) : \mathbb{Q}]} \tag{3}$$

with $\mu(\cdot)$ denoting the Möbius function and $\operatorname{li} x = \int_2^x \frac{dt}{\log t}$ denoting the logarithmic integral, and where

$$\operatorname{error}(E, x) = \operatorname{o}\left(\frac{x}{\log x}\right). \tag{4}$$

It is not difficult to see that $\mathfrak{f}_E$ is finite and that it is positive if and only if E has an irrational 2-division point. For clarity and completeness, we will explain this in detail in Section 6 of the paper.

In 1979 [Mu1, pp. 161–167], R. Murty eliminated the use of GRH in Serre's argument for elliptic curves with complex multiplication (denoted CM). His proof uses class field theoretical properties of CM elliptic curves and the large sieve for number fields in the form of a number field version of the Bombieri-Vinogradov Theorem. In 1987 [Mu2], R. Murty also demonstrated unconditionally the existence of infinitely many primes p for which $\overline{E}(\mathbb{F}_p)$ is cyclic for certain elliptic curves E without complex multiplication (denoted non-CM). More precisely, he showed that for elliptic curves $E_a : y^2 = (x^2 + 1)(x + a)$ with $a \in \mathbb{Q}$ and such that its j-invariant j_{E_a} satisfies $j_{E_a} \notin \mathbb{Z}$, the group of points of E_a modulo p is cyclic for any supersingular prime p of E_a. By 1987 results of N. Elkies, there are infinitely many supersingular primes, hence there are infinitely many primes p for which $\overline{E_a}(\mathbb{F}_p)$ is cyclic. In 1990 [GuMu2], R. Gupta and R. Murty showed

unconditionally that for any elliptic curve E which has an irrational 2-division point, we have

$$f(x, \mathbb{Q}) \gg_E \frac{x}{(\log x)^2}. \tag{5}$$

The implied $\gg_E$-constant depends on E. In 2000 [Co1], A.C. Cojocaru showed that if E is a non-CM elliptic curve, then Serre's result holds under the assumption of a quasi-GRH, namely a zero-free region of Re $s > 3/4$ for the Dedekind zeta functions of the division fields of E, and with

$$\text{error}(E, x) = O_N \left(\frac{x \log \log x}{(\log x)^2} \right). \tag{6}$$

In 2001 [Co2], she also gave a new simpler unconditional proof for formula (2) in the case of a CM elliptic curve, and obtained

$$\text{error}(E, x) = O_N \left(\frac{x}{(\log x)(\log \log \log x)} \right) = O \left(\frac{x}{(\log x)(\log \log \log x)} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}} \right). \tag{7}$$

The implied O_N-constants above depend on N, while the O-constant is absolute.

In this paper we will obtain asymptotic formulae for $f(x, \mathbb{Q})$ with error terms of type $O_N \left(x^\delta \right)$ for some $0 < \delta < 1$. It will be the first time such error terms are obtained in such questions. Moreover, we will obtain an explicit dependence of the error terms on the conductor N. This feature will allow us to deduce estimates for the smallest prime p for which $\overline{E}(\mathbb{F}_p)$ is cyclic.

Before stating the principal results of the paper, let us recall that associated to an elliptic curve E defined over $\mathbb{Q}$ one can define a natural representation $\phi_k : \text{Gal}(\mathbb{Q}(E[k])/\mathbb{Q}) \longrightarrow \text{GL}_2(\mathbb{Z}/k\mathbb{Z})$, which is easily seen to be injective. A famous result of Serre (see [Se2]) asserts that if the curve E is non-CM, then there exists a finite set of primes S_E such that ϕ_l is surjective for any prime $l \notin S_E$. Moreover, if we set $A(E) := 2 \cdot 3 \cdot 5 \cdot \prod_{l \in S_E} l$, where the product is over primes l, then ϕ_k is surjective for any positive integer k coprime to $A(E)$ (see Appendix of [Co4]). We will refer to $A(E)$ as *Serre's constant associated to E*.

The main results of the paper are as follows.

Theorem 1.1. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor N. Let $A(E)$ be Serre's constant associated to E. Let $x \geq 9$.*

1. *Assuming GRH for the Dedekind zeta functions of the division fields of E, we have that*

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \operatorname{li} x + O_N \left(x^{5/6} (\log x)^{2/3} \right),$$

or, more precisely,

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \operatorname{li} x + O \left(x^{5/6} (\log(Nx))^{2/3} \right) + O \left(\frac{(\log \log x)(\log(Nx))}{\log x} A(E)^3 \right).$$

2. *Assuming GRH, Artin's Holomorphy Conjecture (denoted AHC) and a Pair Correlation Conjecture (denoted PCC) for the L-functions associated to the irreducible characters of the Galois groups of the division fields of E, we have that*

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \, \mathrm{li} \, x + \mathrm{O}_N \left(x^{7/10} (\log x)^{4/5} \right),$$

or, more precisely,

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \, \mathrm{li} \, x + \mathrm{O} \left(x^{7/10} (\log(Nx))^{4/5} A(E) \right)$$
$$+ \mathrm{O} \left(\frac{(\log \log x)(\log(Nx))^{6/5}}{x^{1/5} \log x} A(E)^3 \right).$$

The O_N-constants above depend on N, and the O-constants are absolute.

For formulations of AHC and PCC we refer the reader to [Mu5].

Theorem 1.2. *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N, and with complex multiplication by the full ring of integers of an imaginary quadratic field. Let $x \geq 9$. Assuming GRH for the Dedekind zeta functions of the division fields of E, we have that*

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \, \mathrm{li} \, x + \mathrm{O} \left(x^{3/4} (\log(Nx))^{1/2} \right).$$

The implied O-constant is absolute.

Theorem 1.3. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$, of conductor N and such that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Assuming GRH for the Dedekind zeta functions of the division fields of E, we have that the smallest prime $p = p_E$ for which $\overline{E}(\mathbb{F}_p)$ is cyclic has size*

$$p_E = \mathrm{O}_\varepsilon \left((\log N)^{4+\varepsilon} \right),$$

where $\varepsilon > 0$ is any small real number. The implied O_ε-constant depends only on ε.

Theorem 1.4. *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N, with complex multiplication by the full ring of integers of an imaginary quadratic field, and such that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Assuming GRH for the Dedekind zeta functions of the division fields of E, we have that the smallest prime $p = p_E$ for which $\overline{E}(\mathbb{F}_p)$ is cyclic has size*

$$p_E = \mathrm{O}_\varepsilon \left((\log N)^{2+\varepsilon} \right),$$

where $\varepsilon > 0$ is any small real number. The implied O_ε-constant depends only on ε.

In what follows, p, q, l will denote rational primes, k a positive integer, and x, y positive real numbers tending to infinity. Given an elliptic curve E defined over

$\mathbb{Q}$ and of conductor N, the prime p will be such that $p \nmid N$. Given k, $\phi(k)$ will denote the Euler function of k, that is, the number of positive integers $\leq k$ and coprime to k, and $\nu(k)$ will denote the number of distinct prime factors of k. We recall that for functions $f, g : D \subseteq \mathbb{C} \longrightarrow \mathbb{R}$ with g taking positive values, we write $f(x) = O(g(x))$, $f(x) \ll g(x)$, or $g(x) \gg f(x)$ if there exists a positive constant M such that $|f(x)| \leq Mg(x)$ for any $x \in D$. In case f takes positive values and $f(x) \ll g(x) \ll f(x)$, we write $f(x) \asymp g(x)$. If D is infinite and g is non-zero on D, we write $f(x) \sim g(x)$ if $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$, and $f(x) = o(g(x))$ if $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0$. We also make the following convention about the implicit $\ll, \gg, \asymp$ and O-constants: whenever we write $\ll_c, \gg_c, \asymp_c$ or O_c for some c, we indicate that the implicit constant M depends on c; whenever we write $\ll, \gg, \asymp$ or O, we indicate that the implicit constant M is absolute.

2. Outline of the proofs

In order to estimate $f(x, \mathbb{Q})$ we use the following important result.

Lemma 2.1. *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N, and let p be a prime with $p \nmid N$. If $q \neq p$, then $\overline{E}(\mathbb{F}_p)$ contains a (q, q)-type subgroup (that is, a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$) if and only if p splits completely in $\mathbb{Q}(E[q])$. Consequently, $\overline{E}(\mathbb{F}_p)$ is a cyclic group if and only if p does not split completely in the q-division field $\mathbb{Q}(E[q])$ of E for any prime $q \neq p$.*

Proof. First we remark that p is an unramified prime of $\mathbb{Q}(E[q])$, since it is coprime to qN (see Proposition 3.5 below). Then we let

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

be the Frobenius endomorphism and we observe that

$$\operatorname{Ker}(\pi_p - 1) = \overline{E}(\mathbb{F}_p). \tag{8}$$

Now, $\overline{E}(\mathbb{F}_p)$ contains a (q, q)-type subgroup if and only if $\overline{E}(\mathbb{F}_p)[q] \subseteq \overline{E}(\mathbb{F}_p)$, and, from (8), if and only if $\overline{E}(\mathbb{F}_p)[q] \subseteq \operatorname{Ker}(\pi_p - 1)$. But from classical algebraic number theory this is equivalent to p splitting completely in $\mathbb{Q}(E[q])/\mathbb{Q}$. This concludes the proof of the lemma. □

We also observe that if $p \leq x$ splits completely in $\mathbb{Q}(E[k])$ for some k, then $k \leq 2\sqrt{x}$. Indeed, on the one hand from Lemma 2.1 we get that $k^2 | \#\overline{E}(\mathbb{F}_p)$. On the other hand, from Hasse's inequality we know that $\#\overline{E}(\mathbb{F}_p) \leq \left(\sqrt{p} + 1\right)^2$. Therefore $k \leq \sqrt{x} + 1 \leq 2\sqrt{x}$.

By using the above and the inclusion-exclusion principle, we can write

$$f(x, \mathbb{Q}) = \sum_{k \leq 2\sqrt{x}} \mu(k)\pi_1(x, \mathbb{Q}(E[k])/\mathbb{Q}), \tag{9}$$

where for a number field $L/\mathbb{Q}$ we use the notation

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

From (9) we see that explicit formulae for $\pi_1(x, \mathbb{Q}(E[k])/\mathbb{Q})$ shall give us an explicit formula for $f(x, \mathbb{Q})$. As will be recalled in Section 3, an explicit formula for $\pi_1(x, \mathbb{Q}(E[k])/\mathbb{Q})$ is provided by effective versions of the Chebotarev Density Theorem. However, the best error term in each of these formulae is $O\left(x^{1/2}\log(kNx)\right)$, and it is clear that by summing over $k \leq 2\sqrt{x}$ we obtain something bigger than the expected main term $\mathfrak{f}_E \operatorname{li} x \sim \mathfrak{f}_E \frac{x}{\log x}$. The usual technique in analytic number theory for overcoming this difficulty is to split the sum (9) describing $f(x, \mathbb{Q})$ into subsums, some of which are to be handled as suggested above, the others differently.

In his 1976 treatment of $f(x, \mathbb{Q})$, Serre considered the splitting

$$f(x, \mathbb{Q}) = \sideset{}{'}\sum_k \mu(k)\pi_1(x, \mathbb{Q}(E[k])/\mathbb{Q}) + O\left(\sum_{y<q\leq 2\sqrt{x}} \pi_1(x, \mathbb{Q}(E[q])/\mathbb{Q})\right),$$

where the sum $\sideset{}{'}\sum_k$ is over square-free positive integers k whose prime divisors are $\leq y$, the sum $\sum_{y<q\leq 2\sqrt{x}}$ is over rational primes q, and $y = y(x)$ is some real parameter which is optimally chosen in each case. This approach emulates the one used by Hooley in his conditional treatment of Artin's primitive root conjecture (see chapter 3 of [Ho]). It was also used by the authors for obtaining their earlier respective results mentioned in Section 1.

A more natural splitting, however, is

$$f(x, \mathbb{Q}) = \sum_{k\leq y} \mu(k)\pi_1(x, \mathbb{Q}(E[k])/\mathbb{Q}) + \sum_{y<k\leq 2\sqrt{x}} \mu(k)\pi_1(x, \mathbb{Q}(E[k])/\mathbb{Q})$$

$$=: \sum\nolimits_{\text{main}} + \sum\nolimits_{\text{error}} \tag{10}$$

for some parameter $y = y(x)$, to be chosen later. The first sum will provide the main term in the asymptotic formula for $f(x, \mathbb{Q})$ and will be estimated using effective versions of the Chebotarev Density Theorem. The second sum will provide the error term for $f(x, \mathbb{Q})$ and will be estimated using various sieve methods. We emphasize that the novelty in our treatment of $f(x, \mathbb{Q})$ consists not only in the new splitting (10), but also in the new ways of estimating $\sum_{\text{error}}$. As will be seen, our approach leads to much better error terms than the ones obtained following Serre's (or Hooley's) approach.

In our estimates we will also be careful in keeping track of the dependence of the error terms on the conductor N of E. This feature will allow us to determine

the size of the smallest prime p for which $\overline{E}(\mathbb{F}_p)$ is cyclic, by comparing the main term with the error term in the formula for $f(x, \mathbb{Q})$.

3. Preliminaries

3.1. The Chebotarev Density Theorem

The Chebotarev Density Theorem is one of the principal tools needed for proving the main theorems of this paper. We recall it in what follows.

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

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

The Chebotarev Density Theorem asserts that, as $x \to \infty$,

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

In our calculations we need effective versions of this theorem (that is, versions with explicit error terms). They were first derived by J. Lagarias and A. Odlyzko in 1976 (see [LaOd]), refined by J-P. Serre (see [Se4]), and subsequently improved by K. Murty, R. Murty and N. Saradha (see [MuMuSa] and [MuMu]).

Theorem 3.1. *Assuming GRH for the Dedekind zeta function of L, we have that*

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

The implied O-*constant is absolute.*

This version of the effective Chebotarev Density Theorem is slightly more refined than a statement given in [LaOd] and is due to Serre (see [Se4, p. 133]).

By assuming, in addition to GRH, Artin's Holomorphy Conjecture (denoted AHC) and a Pair Correlation Conjecture (denoted PCC), one can improve the error term in the above asymptotic formula for $\pi_1(x, L/\mathbb{Q})$.

Theorem 3.2. *Assuming GRH, AHC and PCC for the Artin L-functions attached to the irreducible characters of G, we have that*

$$\pi_1(x, L/\mathbb{Q}) = \frac{1}{\#G} \operatorname{li} x + \mathrm{O}\left(x^{1/2} \left(\frac{\#\tilde{G}}{\#G} \right)^{1/4} \log(M(L/\mathbb{Q})x) \right),$$

where $\tilde{G}$ denotes the set of conjugacy classes of G. The implied O-*constant is absolute.*

This result is due to K. Murty and R. Murty (see [MuMu]).

Remark 3.3. If $L/\mathbb{Q}$ is an abelian extension, then all the conjugacy classes of $G = \mathrm{Gal}(L/\mathbb{Q})$ are singleton sets; consequently, the quotient $\frac{\#\tilde{G}}{\#G}$ becomes 1 and the error terms given in Theorems 3.1 and 3.2 have the same size. Similarly, if the quotient $\frac{\#\tilde{G}}{\#G}$ is not 'very small', then the error term given in Theorem 3.2 is not significantly different from the one given in Theorem 3.1. In such a situation we say that the group G is 'almost abelian'. The improvement made in Theorem 3.2 is most significant in the case of a non-abelian extension $L/\mathbb{Q}$ whose Galois group G has few conjugacy classes. This will be apparent in our applications of the Chebotarev Density Theorem in Section 4.

The following result is very helpful in estimating the error terms in the effective Chebotarev Density Theorem.

Lemma 3.4. *Let $L/\mathbb{Q}$ be a finite Galois extension of degree n_L and discriminant d_L. Using the same notation as before, we have that*

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

For a proof of this lemma we refer the reader to [Se4, p. 130].

3.2. Division fields of elliptic curves

In this section we gather some properties of the division fields $\mathbb{Q}(E[k])$ of an elliptic curve E defined over $\mathbb{Q}$. We write

$$n(k) = [\mathbb{Q}(E[k]) : \mathbb{Q}] \qquad (11)$$

for the degree of $\mathbb{Q}(E[k])$ over $\mathbb{Q}$.

Proposition 3.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. Let k be a positive integer.*

1. $\mathbb{Q}(E[k])/\mathbb{Q}$ is a finite Galois extension for which $\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q}) \leq \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$. Consequently,

$$n(k) \leq k^4 \prod_{q|k} \left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right) \leq k^4.$$

2. The ramified primes of $\mathbb{Q}(E[k])/\mathbb{Q}$ are divisors of kN.
3. The cyclotomic field $\mathbb{Q}(\zeta_k)$ is contained in $\mathbb{Q}(E[k])$. Therefore

$$\phi(k)|n(k),$$

and a rational prime p which splits completely in $\mathbb{Q}(E[k])$ satisfies $p \equiv 1 \pmod{k}$.

Part 1 of this proposition is a direct consequence of the injectivity of the Galois representation $\phi_k : \mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$ associated to E; for parts 2 and 3 we refer the reader to [Si1, p. 179 and p. 98].

Proposition 3.5 gives us lower and upper bounds for $n(k)$. We are interested in determining even more precise estimates for $n(k)$. As will be recalled below, the size of $n(k)$ differs drastically according to whether E is a CM or a non-CM curve.

From the celebrated theorem of Serre on the surjectivity of ϕ_k we deduce the following (see, for example, Appendix of [Co4]).

Proposition 3.6. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ and let $A(E)$ be Serre's constant associated to E.*

1. *For any integer k coprime to $A(E)$ we have that*

$$n(k) = k^4 \prod_{q|k} \left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right)$$

   and that $\mathbb{Q}(\zeta_k)$ is the maximal abelian extension of $\mathbb{Q}$ which is contained in $\mathbb{Q}(E[k])$.
2. *Let k be a positive integer. We write it uniquely as $k = k_1 k_2$ with k_1 composed of primes which are divisors of $A(E)$ and k_2 composed of primes which are coprime to $A(E)$. Then*

$$n(k) \geq \phi(k_1)n(k_2) \gg \phi(k)k_2^3.$$

Proof. 1. For the first statement of part 1 we refer the reader to [Se1] or [Co4, Appendix]. Now for k coprime to $A(E)$ let us show that $\mathbb{Q}(\zeta_k)$ is the maximal abelian extension contained in $\mathbb{Q}(E[k])$. We have $\mathrm{Gal}(L_k/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$ and

$$\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q}) \simeq (\mathbb{Z}/k\mathbb{Z})^*, \qquad \frac{\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})}{\mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z})} \simeq (\mathbb{Z}/k\mathbb{Z})^*.$$

Thus, to prove the desired assertion it suffices to show that the commutator $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})'$ of $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$ is $\mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z})$. This can be deduced easily by using the Chinese Remainder Theorem to write $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}) \simeq \prod_{q^r||k} \mathrm{GL}_2(\mathbb{Z}/q^r\mathbb{Z})$ and by using [Br, Theorem 1.4 a, p. 474] that for odd primes q, $\mathrm{GL}_2(\mathbb{Z}/q^r\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/q^r\mathbb{Z})$. Since k is coprime to $A(E)$, all its prime factors are odd, and so we are done.

2. Let k_1 be a positive integer composed of primes dividing $A(E)$, and k_2 a positive integer composed of primes coprime to $A(E)$. Then $(k_1, k_2) = 1$. Using parts 2 and 3 of Proposition 3.5 and part 1 of our proposition, we obtain that $\mathbb{Q}(\zeta_{k_1}) \cap \mathbb{Q}(E[k_2]) = \mathbb{Q}$. Since $\mathbb{Q}(E[k_1 k_2]) = \mathbb{Q}(E[k_1])\mathbb{Q}(E[k_2])$, we obtain

$$n(k_1 k_2) \geq [\mathbb{Q}(\zeta_{k_1}) : \mathbb{Q}][\mathbb{Q}(E[k_2]) : \mathbb{Q}] = \phi(k_1)n(k_2).$$

Now we note that part 1 tells us that

$$n(k_2) = \# \mathrm{GL}_2(\mathbb{Z}/k_2\mathbb{Z}) = k_2^4 \prod_{l \mid k_2} \left(1 - \frac{1}{l}\right)\left(1 - \frac{1}{l^2}\right) = \phi(k_2)k_2^3 \prod_{l \mid k_2}\left(1 - \frac{1}{l^2}\right),$$

where the products are over primes l. Thus

$$n(k) = n(k_1 k_2) \geq \phi(k)k_2^3 \prod_l \left(1 - \frac{1}{l^2}\right) \gg \phi(k)k_2^3.$$

$\square$

As explained in [Co3, p. 27] or [Co4], one can refine the proof of [Se4, Lemma 19, p. 198] to deduce upper bounds for $A(E)$.

Proposition 3.7. *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor N. Let $A(E)$ be Serre's constant associated to E. We assume GRH for the Dedekind zeta functions of the division fields of E. Then there exists a positive constant a, not depending on E, such that*

$$A(E) \leq a(\log N)(\log\log 2N)^3.$$

We also recall that, unconditionally, $A(E) \ll_\varepsilon N^{1+\varepsilon}$ for any $\varepsilon > 0$ (see [Co4]) and, moreover, if E is semistable (that is, N is square-free), then $A(E)$ is an absolute constant (see [Ma]).

Good estimates for the size of $n(k)$ in the case of a CM elliptic curve can be obtained as a consequence of deep results in the theory of complex multiplication. Before stating the result, we recall that if $\mathcal{O}_K$ is the ring of integers of a number field K and if $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_K$, then the generalized Euler function of $\mathfrak{p}^a$ for some positive integer a is

$$\Phi(\mathfrak{p}^a) = N_{K/\mathbb{Q}}(\mathfrak{p}^a)\left(1 - \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})}\right),$$

where $N_{K/\mathbb{Q}}(\cdot)$ denotes the norm of K over $\mathbb{Q}$; by multiplicativity, one extends the definition of $\Phi(\cdot)$ to all non-zero ideals of $\mathcal{O}_K$.

Proposition 3.8. *Let E be a CM elliptic curve defined over $\mathbb{Q}$ and with complex multiplication by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Then for any positive integer $k \geq 3$ we have*

$$n(k) \asymp \Phi(k\mathcal{O}_K),$$

where $\Phi(\cdot)$ denotes the generalized Euler function corresponding to the ring of integers $\mathcal{O}_K$. In particular,

$$\phi(k)^2 \ll n(k) \ll k^2.$$

Proof. The very first estimate is obtained as a consequence of deep results in the theory of complex multiplication, as follows. We let $h(\cdot)$ denote the Weber function of E. Then we know that $K(j_E, h(E[k]))$ is the ray class field of K modulo k (see [Si2, Theorem 5.6, p. 135]), where j_E denotes the j-invariant of E. We obtain that

$$[K(j_E, h(E[k])) : K] = \frac{h_K \Phi(k\mathcal{O}_K)}{W_K},$$

where h_K denotes the class number of K and W_K the number of roots of unity in K.

Since E is a CM elliptic curve defined over $\mathbb{Q}$, we have that its CM field K is an imaginary quadratic field of class number 1. This implies that $K(j_E, h(E[k])) = K(h(E[k]))$, that W_K is bounded absolutely, and, moreover, that

$$[K(h(E[k])) : K] \asymp \Phi(k\mathcal{O}_K).$$

Now let us recall that $E[k] \simeq \mathbb{Z}/k\mathbb{Z} \oplus \mathbb{Z}/k\mathbb{Z}$, and so, by choosing two fixed generators for $E[k]$, we get that $[K(E[k]) : K(h(E[k]))]$ is bounded absolutely.

Putting all these observations together we obtain

$$[\mathbb{Q}(E[k]) : \mathbb{Q}] \asymp [K(E[k]) : K] \asymp [K(h(E[k])) : K] \asymp \Phi(k\mathcal{O}_K).$$

$\square$

4. Proof of Theorem 1.1

1. We estimate $\sum_{\text{main}}$ by using the effective Chebotarev Density Theorem 3.1, together with the estimates given in Lemma 3.4 and with parts 1 and 2 of Proposition 3.5. We obtain that

$$
\begin{aligned}
\sum\nolimits_{\text{main}} &= \sum_{k \leq y} \mu(k)\pi_1(x, \mathbb{Q}(E[k])/\mathbb{Q}) \\
&= \left(\sum_{k \leq y} \frac{\mu(k)}{n(k)} \right) \operatorname{li} x + \sum_{k \leq y} \mathrm{O}\left(x^{1/2} \log(kNx)\right) \\
&= \left(\sum_{k \leq y} \frac{\mu(k)}{n(k)} \right) \operatorname{li} x + \mathrm{O}\left(yx^{1/2} \log(Nx)\right), \quad (12)
\end{aligned}
$$

where $n(k)$ is defined in (11).

It remains to estimate $\sum_{\text{error}}$. For each integer a with $|a| \leq 2\sqrt{x}$ and for each positive square-free integer k we let

$$S_a(k) := \left\{ p \leq x : a_p = a, \, p \text{ splits completely in } \mathbb{Q}(E[k])/\mathbb{Q} \right\}.$$

Then, using Hasse's inequality,

$$\left|\sum_{\text{error}}\right| \leq \sum_{\substack{y<k\leq 2\sqrt{x} \\ k \text{ square-free}}} \sum_{\substack{a\in\mathbb{Z} \\ |a|\leq 2\sqrt{x}}} \#S_a(k). \tag{13}$$

We see that by using part 3 of Proposition 3.5 and Lemma 2.1 we have that $p \in S_a(k)$ implies $p \equiv 1 \,(\mathrm{mod}\, k)$ and $p+1-a \equiv 0\,(\mathrm{mod}\, k^2)$; hence $k|(a-2)$. We then obtain

$$\sum_{\substack{y<k\leq 2\sqrt{x} \\ k \text{ square-free}}} \sum_{\substack{a\in\mathbb{Z} \\ |a|\leq 2\sqrt{x}}} \#S_a(k) \leq \sum_{\substack{y<k\leq 2\sqrt{x} \\ k \text{ square-free}}} \sum_{\substack{a\in\mathbb{Z} \\ |a|\leq 2\sqrt{x} \\ a\neq 2, k|a-2}} \sum_{\substack{p\leq x \\ a_p=a \\ k^2|p+1-a}} 1$$

$$+ \sum_{\substack{y<k\leq 2\sqrt{x} \\ k \text{ square-free}}} \sum_{\substack{p\leq x \\ a_p=2 \\ k^2|p-1}} 1$$

$$=: \sum\nolimits^{*} + \sum\nolimits^{**}. \tag{14}$$

We use elementary estimates to handle $\sum^{*}$ and $\sum^{**}$:

$$\sum\nolimits^{*} \leq \sum_{\substack{y<k\leq 2\sqrt{x} \\ k \text{ square-free}}} \sum_{\substack{a\in\mathbb{Z} \\ |a|\leq 2\sqrt{x} \\ a\neq 2, k|a-2}} \left(\frac{x}{k^2}+1\right)$$

$$\ll \sum_{\substack{y<k\leq 2\sqrt{x} \\ k \text{ square-free}}} \left(\frac{x}{k^2}+1\right)\left(\frac{\sqrt{x}}{k}+1\right)$$

$$\ll \frac{x^{3/2}}{y^2} + \frac{x}{y} + \sqrt{x}\log\frac{x}{y} + \sqrt{x}; \tag{15}$$

$$\sum\nolimits^{**} \leq \sum_{\substack{y<k\leq 2\sqrt{x} \\ k \text{ square-free}}} \left(\frac{x}{k^2}+1\right) \ll \frac{x}{y} + \sqrt{x}. \tag{16}$$

Plugging (12)–(16) into (10) gives

$$f(x,\mathbb{Q}) = \left(\sum_{k\leq y}\frac{\mu(k)}{n(k)}\right)\mathrm{li}\,x + O\left(x^{1/2}y\log(Nx)\right)$$

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

Now we choose y such that $x^{1/2} y \log(Nx) = \frac{x^{3/2}}{y^2}$, that is, we choose

$$y := \left(\frac{x}{\log(Nx)} \right)^{1/3}.$$

Then

$$f(x, \mathbb{Q}) = \left(\sum_{k \le y} \frac{\mu(k)}{n(k)} \right) \operatorname{li} x + O\left(x^{5/6} (\log(Nx))^{2/3} \right). \tag{17}$$

It remains to analyze the tail

$$\left(\sum_{k > y} \frac{\mu(k)}{n(k)} \right) \operatorname{li} x = \mathfrak{f}_E \operatorname{li} x - \left(\sum_{k \le y} \frac{\mu(k)}{n(k)} \right) \operatorname{li} x.$$

In what follows, k, k_1, and k_2 will denote positive square-free integers. We write each $k > y$ as $k = k_1 k_2$ with k_1, k_2 uniquely determined such that k_1 is composed of primes dividing $A(E)$ and k_2 is composed of primes coprime to $A(E)$. Using part 2 of Proposition 3.6 we get

$$\sum_{\substack{k > y \\ k \text{ square-free} \\ k = k_1 k_2}} \frac{1}{n(k)} \le \sum_{k_1} \frac{1}{\phi(k_1)} \sum_{k_2 > \frac{y}{k_1}} \frac{1}{\phi(k_2) k_2^3} \ll \sum_{k_1} \frac{1}{\phi(k_1)} \sum_{k_2 > \frac{y}{k_1}} \frac{\log \log k_2}{k_2^4}$$

$$\ll \sum_{k_1} \frac{1}{\phi(k_1)} \int_{\frac{y}{k_1}}^{\infty} \frac{\log \log t}{t^4} \, dt \ll \frac{\log \log y}{y^3} \sum_{k_1} \frac{k_1^3}{\phi(k_1)}$$

$$= \frac{\log \log y}{y^3} \prod_{q | A(E)} \left(1 + \frac{q^3}{q - 1} \right)$$

$$\le \frac{\log \log y}{y^3} A(E)^2 \exp(\nu(A(E)))$$

$$\le \frac{\log \log y}{y^3} A(E)^3, \tag{18}$$

where we have also used that $\phi(t) \gg \frac{t}{\log \log t}$ and $\nu(t) \le \frac{\log t}{\log 2}$. Plugging (18) into (17) finally gives

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \operatorname{li} x + O\left(x^{5/6} (\log(Nx))^{2/3} \right) + O\left(\frac{(\log \log x)(\log(Nx))}{\log x} A(E)^3 \right).$$

This completes the proof of part 1 of Theorem 1.1.

2. Now we assume that GRH, AHC and PCC hold for the Artin L-functions attached to the irreducible characters of the Galois groups of the division fields of E. Therefore, in estimating $\sum_{\text{main}}$ we can use the improved Chebotarev Density

Theorem given by Theorem 3.2. To use this result, we first need to estimate the factor $\frac{\#\widetilde{G_k}}{\#G_k}$ for all positive square-free integers $k \leq y$, where G_k is the image of $\mathrm{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})$ under the Galois representation ϕ_k associated to E and $\widetilde{G_k}$ is the set of conjugacy classes of G_k. As before, we write $k \leq y$ as $k = k_1 k_2$ with k_1 composed of primes dividing $A(E)$ and k_2 composed of primes coprime to $A(E)$. Since

$$\#\widetilde{G_k} \leq \left(\#\widetilde{G_{k_1}}\right)\left(\#\widetilde{G_{k_2}}\right),$$

it suffices to estimate $\#\widetilde{G_{k_1}}$ and $\#\widetilde{G_{k_2}}$. Using the description of the possible groups G_q for primes $q|A(E)$ given in [Se2] and [Se4, p. 197], we obtain that

$$\#\widetilde{G_{k_1}} \leq \prod_{q|k_1} \#\widetilde{G_q} \leq \prod_{q|k_1} \#G_q \ll k_1^2 \phi(k_1),$$

and using the surjectivity of ϕ_{k_2}, we obtain that

$$\#\widetilde{G_{k_2}} = \#\widetilde{\mathrm{GL}_2(\mathbb{Z}/k_2\mathbb{Z})} = k_2 \phi(k_2).$$

These estimates and the lower bound for $\#G_k$ given by part 2 of Proposition 3.6 give us

$$\frac{\#\widetilde{G_k}}{\#G_k} \ll \frac{k_1^2 k_2 \phi(k)}{\phi(k) k_2^3} = \frac{k_1^2}{k_2^2}.$$

Then, with $M(L_k/\mathbb{Q})$ defined as in Section 3.1 and estimated using Lemma 3.4 and parts 1 and 2 of Proposition 3.5, we obtain that the error term in $\sum_{\mathrm{main}}$ becomes

$$\sum_{\substack{k \leq y \\ k \text{ square-free} \\ k = k_1 k_2}} \mathrm{O}\left(x^{1/2} \left(\frac{\#\widetilde{G_k}}{\#G_k}\right)^{1/4} \log(M(L_k/\mathbb{Q})x)\right)$$

$$= \mathrm{O}\left(x^{1/2} \log(Nx) \sum_{k_1} k_1^{1/2} \sum_{k_2 \leq \frac{y}{k_1}} \frac{1}{k_2^{1/2}}\right)$$

$$= \mathrm{O}\left(x^{1/2} \log(Nx) \sum_{k_1} k_1^{1/2} \left(\frac{y}{k_1}\right)^{1/2}\right)$$

$$= \mathrm{O}\left(x^{1/2} y^{1/2} 2^{\nu(A(E))} \log(Nx)\right)$$

$$= \mathrm{O}\left(x^{1/2} y^{1/2} A(E) \log(Nx)\right),$$

where we have also used that $\nu(t) \leq \frac{\log t}{\log 2}$. Therefore

$$\sum_{\mathrm{main}} = \left(\sum_{k \leq y} \frac{\mu(k)}{n(k)}\right) \mathrm{li}\, x + \mathrm{O}\left(x^{1/2} y^{1/2} A(E) \log(Nx)\right).$$

We point out that the additional conjectures AHC and PCC allowed us to obtain $y^{1/2}$ instead of y in the above error terms (compare with (12)). For $\sum_{\text{error}}$ and the tail $\sum_{k>y} \dfrac{\mu(k)}{n(k)}$ li x we proceed exactly as in part 1. We now choose y such that $x^{1/2} y^{1/2} \log(Nx) = \frac{x^{3/2}}{y^2}$, that is, we choose

$$y := \left(\frac{x}{\log(Nx)} \right)^{2/5}.$$

Plugging this into our estimates leads to

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \, \text{li} \, x + \text{O}\left(x^{7/10} (\log(Nx))^{4/5} A(E) \right)$$
$$+ \text{O}\left(\frac{(\log \log x)(\log(Nx))^{6/5}}{x^{1/5} \log x} A(E)^3 \right).$$

This completes the proof of part 2 of Theorem 1.1.

Remark 4.1. If we use the estimate $\nu(t) \ll \frac{\log t}{\log \log t}$ instead of the more elementary one $\nu(t) \leq \frac{\log t}{\log 2}$, then we can slightly improve our error terms above to obtain

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \, \text{li} \, x + \text{O}\left(x^{5/6} (\log(Nx))^{2/3} \right) + \text{O}_\varepsilon \left(\frac{(\log \log x)(\log(Nx))}{\log x} A(E)^{2+\varepsilon} \right)$$

under GRH, and

$$f(x, \mathbb{Q}) = \mathfrak{f}_E \, \text{li} \, x + \text{O}_\varepsilon \left(x^{7/10} (\log(Nx))^{4/5} A(E)^\varepsilon \right)$$
$$+ \text{O}_\varepsilon \left(\frac{(\log \log x)(\log(Nx))^{6/5}}{x^{1/5} \log x} A(E)^{2+\varepsilon} \right)$$

under GRH, AHC and PCC, for any $0 < \varepsilon < 1$.

5. Proof of Theorem 1.2

The sum $\sum_{\text{main}}$ is estimated exactly as in the proof of part 1 of Theorem 1.1. For the sum $\sum_{\text{error}}$ we make two separate analyses according to whether $a_p \neq 0$ or $a_p = 0$. We recall that a prime p is said to have *ordinary* reduction if $a_p \neq 0$, and *supersingular* reduction otherwise. We write

$$\sum_{\text{error}} \leq \sum_{\substack{y < k \leq 2\sqrt{x} \\ k \text{ square-free}}} \pi_1^o(x, \mathbb{Q}(E[k])/\mathbb{Q}) + \sum_{\substack{y < k \leq 2\sqrt{x} \\ k \text{ square-free}}} \pi_1^s(x, \mathbb{Q}(E[k])/\mathbb{Q}), \quad (19)$$

where

$$\pi_1^o(x, \mathbb{Q}(E[k])/\mathbb{Q})$$
$$:= \#\{p \leq x : p \text{ has ordinary reduction and splits completely in } \mathbb{Q}(E[k])/\mathbb{Q}\},$$

$\pi_1^s(x, \mathbb{Q}(E[k])/\mathbb{Q})$
$:= \#\{p \leq x : p$ has supersingular reduction and splits completely in $\mathbb{Q}(E[k])/\mathbb{Q}\}$.

Let us estimate

$$\sum_{\substack{y < k \leq 2\sqrt{x} \\ k \text{ square-free}}} \pi_1^o(x, \mathbb{Q}(E[k])/\mathbb{Q}).$$

As explained for example in [Co2] we have that p splits completely in $\mathbb{Q}(E[k])/\mathbb{Q}$ if and only if $\frac{\pi_p - 1}{k}$ is an algebraic integer, where π_p denotes a complex root of the polynomial $X^2 - a_p X + p$. Since E has complex multiplication by $\mathbb{Q}(\sqrt{-D})$ for some square-free $D < 0$, we obtain that, for primes p of ordinary good reduction, $\mathbb{Q}(\pi_p) = \mathbb{Q}(\sqrt{-D})$. Therefore

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

where $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ denotes the ring of algebraic integers of $\mathbb{Q}(\sqrt{-D})$. We observe that the norm of π_p in $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ is p, hence

$$\# \left\{ p \leq x : \frac{\pi_p - 1}{k} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-D})} \right\} \leq S_k,$$

where S_k is S_k^1 if $-D \equiv 2, 3 \pmod 4$, and S_k^2 if $-D \equiv 1 \pmod 4$, and

$$S_k^1 := \# \left\{ p \leq x : p = (\alpha k + 1)^2 + D\beta^2 k^2 \text{ for some } \alpha, \beta \in \mathbb{Z} \right\},$$

$$S_k^2 := \# \left\{ p \leq x : p = \left(\frac{\alpha}{2} k + 1 \right)^2 + D\frac{\beta^2}{4} k^2 \text{ for some } \alpha, \beta \in \mathbb{Z} \right\}.$$

For any k, x and $1 \leq i \leq 2$ we have the elementary estimate

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

Therefore

$$\sum_{\substack{y < k \leq 2\sqrt{x} \\ k \text{ square-free}}} \pi_1^o(x, \mathbb{Q}(E[k])/\mathbb{Q}) \ll \sum_{\substack{y < k \leq 2\sqrt{x} \\ k \text{ square-free}}} \left(\frac{x}{k^2\sqrt{D}} + \frac{\sqrt{x}}{k\sqrt{D}} \right)$$

$$\ll \frac{x}{y\sqrt{D}} + \frac{\sqrt{x} \log x}{\sqrt{D}}. \tag{20}$$

The summation

$$\sum_{\substack{y < k \leq 2\sqrt{x} \\ k \text{ square-free}}} \pi_1^s(x, \mathbb{Q}(E[k])/\mathbb{Q})$$

counts primes p for which $k^2|(p+1-a_p)$ and $k|(p-1)$. Hence $k|2$, which is a contradiction with $k > y = y(x)$. This implies that

$$\sum_{\substack{y < k \le 2\sqrt{x} \\ k \text{ square-free}}} \pi_1^s(x, \mathbb{Q}(E[k])/\mathbb{Q}) = 0. \tag{21}$$

Plugging (12) and (19)–(21) into (10) gives

$$f(x, \mathbb{Q}) = \left(\sum_{k \le y} \frac{\mu(k)}{n(k)} \right) \operatorname{li} x + O\left(x^{1/2} y \log(Nx)\right) + O\left(\frac{x}{y\sqrt{D}}\right) + O\left(\frac{\sqrt{x} \log x}{\sqrt{D}}\right).$$

We note that the discriminant D is fixed and, moreover, bounded, as we are in the CM case. Thus it will play no role in our error terms above.

We now choose y such that $x^{1/2} y \log(Nx) = \frac{x}{y}$, that is, we choose

$$y := \frac{x^{1/4}}{(\log(Nx))^{1/2}}.$$

This implies that

$$f(x, \mathbb{Q}) = \left(\sum_{k \le y} \frac{\mu(k)}{n(k)} \right) \operatorname{li} x + O\left(x^{3/4}(\log(Nx))^{1/2}\right).$$

It remains to analyze the tail $\left(\displaystyle\sum_{k > y} \frac{\mu(k)}{n(k)} \right) \operatorname{li} x$. From Proposition 3.8 we know that for any positive square-free integer $k \ge 3$, $n(k) \gg \phi(k)^2$. Also, we recall that as $k \to \infty$, $\phi(k) \gg \frac{k}{\log \log k}$. Then, by partial summation, we get that

$$\sum_{k > y} \frac{\mu(k)}{n(k)} \ll \sum_{\substack{k > y \\ k \text{ square-free}}} \frac{(\log \log k)^2}{k^2} \ll \frac{(\log \log y)^2}{y}. \tag{22}$$

Using our previous estimates and our choice of y we finally obtain

$$f(x, \mathbb{Q}) = f_E \operatorname{li} x + O\left(x^{3/4}(\log(Nx))^{1/2}\right).$$

This completes the proof of Theorem 1.2.

Remark 5.1. We observe that in the CM case the Galois group $\operatorname{Gal}(\mathbb{Q}(E[k])/\mathbb{Q})$ is 'almost abelian' (in the sense explained in Remark 3.3 of Section 3). Therefore Theorem 3.2 will not give us better error terms than the ones already obtained by using Theorem 3.1.

6. Finiteness and positivity of the density $\mathfrak{f}_E$

Let E be an elliptic curve defined over $\mathbb{Q}$ and let $\mathfrak{f}_E$ be its cyclicity constant defined by (3). We want to justify that $\mathfrak{f}_E$ is finite and that it is positive if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$.

If E is a non-CM curve, then let $A(E)$ be Serre's constant associated to E and write each positive square-free integer k as $k = k_1 k_2$ for some positive square-free integers uniquely determined such that k_1 is composed of prime divisors of $A(E)$ and k_2 is coprime to $A(E)$. Then, as in the discussion for (18), we have

$$\mathfrak{f}_E \ll \prod_{q \mid A(E)} \left(1 + \frac{1}{q-1}\right) \sum_{k_2 \geq 9} \frac{\log \log k_2}{k_2^4},$$

which is certainly finite.

If E is a CM curve, then, as in the discussion for (22), we have

$$\mathfrak{f}_E \ll \sum_{k \geq 9} \frac{(\log \log k)^2}{k^2},$$

which, again, is finite.

Let us justify that if $\mathfrak{f}_E \neq 0$, then $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. We observe that if $\mathbb{Q}(E[2]) = \mathbb{Q}$, then the torsion group $E(\mathbb{Q})_{\text{tors}}$ of rational points on E contains a subgroup of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since for all primes p, except for a finite number of them, the group $E(\mathbb{Q})_{\text{tors}}$ embeds into $\overline{E}(\mathbb{F}_p)$, we deduce that $\mathfrak{f}_E = 0$. This observation also shows the stronger fact that if $\mathbb{Q}(E[2]) = \mathbb{Q}$, then there are only finitely many primes p for which $\overline{E}(\mathbb{F}_p)$ is cyclic.

The converse of the above statement can be proven immediately by combining (5) with part 1 of Theorem 1.1 and with Theorem 1.2. Indeed, if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, then

$$\mathfrak{f}_E \operatorname{li} x + O_E\left(x^\theta (\log x)^\delta\right) \gg_E \frac{x}{(\log x)^2}, \tag{23}$$

where $\theta = \frac{5}{6}$, $\delta = \frac{2}{3}$ in the non-CM case, and $\theta = \frac{3}{4}$, $\delta = \frac{1}{2}$ in the CM case. By multiplying (23) by $\log x / x$ and by taking $x \to \infty$, we obtain $\mathfrak{f}_E > 0$.

Now let us give unconditional arguments for why $\mathfrak{f}_E > 0$ if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$ (recall that Theorems 1.1 and 1.2 assume GRH). We will consider the non-CM and CM cases separately. First we will prove a lemma of a more general interest.

Lemma 6.1. *Let $\mathcal{F} = (L_q)_{q \in \mathcal{P}}$, $\mathcal{F}' = (L'_q)_{q \in \mathcal{P}'}$ be two families of finite Galois extensions of a number field L, indexed over sets of rational primes $\mathcal{P} \supseteq \mathcal{P}'$. For any square-free integer k composed of primes of $\mathcal{P}$ or $\mathcal{P}'$, let $L_k := \prod_{q \mid k, q \in \mathcal{P}} L_q$ and $L'_k := \prod_{q \mid k, q \in \mathcal{P}'} L'_q$, respectively. Also let $n(k) := [L_k : L]$, $n'(k) := [L'_k : L]$, and*

$$\delta(\mathcal{F}) := \sum_{\substack{k \\ q \mid k \Rightarrow q \in \mathcal{P}}} \frac{\mu(k)}{n(k)}, \quad \delta(\mathcal{F}') := \sum_{\substack{k \\ q \mid k \Rightarrow q \in \mathcal{P}'}} \frac{\mu(k)}{n'(k)},$$

where $n(1) = n'(1) = 1$. We assume that:

1. *$\mathcal{F}$ covers $\mathcal{F}'$, that is, for any $q' \in \mathcal{P}'$ there exists $q \in \mathcal{P}$ such that $L'_{q'} \subseteq L_q$ and for any $q \in \mathcal{P}$ there exists $q' \in \mathcal{P}'$ such that $L'_{q'} \subseteq L_q$;*

2. $\displaystyle\sum_{\substack{k \\ q|k \Rightarrow q \in \mathcal{P}}} \frac{1}{n(k)} < \infty, \quad \sum_{\substack{k \\ q|k \Rightarrow q \in \mathcal{P}'}} \frac{1}{n'(k)} < \infty.$

Then $\delta(\mathcal{F}) \geq \delta(\mathcal{F}')$.

Proof. Let us consider an arbitrary finite subset $\mathcal{P}_f$ of $\mathcal{P}$ and take $\mathcal{P}'_f$ to be the finite subset of $\mathcal{P}'$ such that $(L_q)_{q \in \mathcal{P}_f}$ covers $(L'_q)_{q \in \mathcal{P}'_f}$ (in the sense of assumption 1). Also, set

$$\delta_{\mathcal{P}_f}(\mathcal{F}) := \sum_{\substack{k \\ q|k \Rightarrow q \in \mathcal{P}_f}} \frac{\mu(k)}{n(k)}, \quad \delta_{\mathcal{P}'_f}(\mathcal{F}') := \sum_{\substack{k \\ q|k \Rightarrow q \in \mathcal{P}'_f}} \frac{\mu(k)}{n'(k)},$$

$$P(x, \mathcal{F}, \mathcal{P}_f) := \#\{\mathfrak{p} : N_{L/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathfrak{p} \text{ does not split completely in } L_q \ \forall q \in \mathcal{P}_f\},$$

$$P(x, \mathcal{F}', \mathcal{P}'_f) := \#\{\mathfrak{p} : N_{L/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathfrak{p} \text{ does not split completely in } L'_q \ \forall q \in \mathcal{P}'_f\},$$

where x is any positive real number, $\mathfrak{p}$ are prime ideals of the ring of integers of L, and $N_{L/\mathbb{Q}}$ is the norm of $L/\mathbb{Q}$.

Since $\mathcal{P}_f$ covers $\mathcal{P}'_f$, we clearly have

$$P(x, \mathcal{F}, \mathcal{P}_f) \geq P(x, \mathcal{F}', \mathcal{P}'_f) \tag{24}$$

for any x. On the other hand, by the inclusion-exclusion principle and the Chebotarev Density Theorem we have

$$P(x, \mathcal{F}, \mathcal{P}_f) = \sum_{\substack{k \\ q|k \Rightarrow q \in \mathcal{P}_f}} \frac{\mu(k)}{n(k)} \operatorname{li} x + \operatorname{o}\left(\frac{x}{\log x}\right), \tag{25}$$

$$P(x, \mathcal{F}', \mathcal{P}'_f) = \sum_{\substack{k \\ q|k \Rightarrow q \in \mathcal{P}'_f}} \frac{\mu(k)}{n'(k)} \operatorname{li} x + \operatorname{o}\left(\frac{x}{\log x}\right), \tag{26}$$

since the sums over k are finite. Combining (24) with (25) and (26), and taking $x \to \infty$, leads us to

$$\delta_{\mathcal{P}_f}(\mathcal{F}) \geq \delta_{\mathcal{P}'_f}(\mathcal{F}').$$

This inequality holds for any finite subset $\mathcal{P}_f$ of $\mathcal{P}$ and its corresponding finite subset $\mathcal{P}'_f$ of $\mathcal{P}'$. By taking the limit as $\mathcal{P}_f$ approaches $\mathcal{P}$ we obtain the desired inequality. $\qquad\square$

Corollary 6.2. *We keep the setting and the hypotheses of Lemma 6.1. If the fields in $\mathcal{F}'$ are mutually independent, then*

$$\delta(\mathcal{F}) \geq \prod_{q \in \mathcal{P}'} \left(1 - \frac{1}{n'(q)}\right).$$

We will use Corollary 6.2 to show that if E is a non-CM elliptic curve defined over $\mathbb{Q}$ and such that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, then $\mathfrak{f}_E > 0$. As usual, let N be the conductor of E and $A(E)$ be Serre's constant associated to E. We define $\mathcal{F} = (L_q = \mathbb{Q}(E[q]))_{q \geq 2}$. To define $\mathcal{F}' = (L_q')_q$, let us first note that $[\mathbb{Q}(E[2]) : \mathbb{Q}]$ is either 2, 3 or 6, and let K_2 be the unique abelian subextension contained in $\mathbb{Q}(E[2])$ (note that we may have $\mathbb{Q}(E[2]) = K_2$). Then we define

$$L_q' := \begin{cases} L_q & \text{if } q \nmid NA(E), \\ \mathbb{Q}(\zeta_q) & \text{if } q|NA(E), q \neq 2, \mathbb{Q}(\zeta_q) \cap K_2 = \mathbb{Q}, \\ K_2 & \text{if } q = 2 \text{ or } q|NA(E), q \neq 2, \mathbb{Q}(\zeta_q) \cap K_2 = \mathbb{Q}. \end{cases}$$

We see that the families $\mathcal{F}$, $\mathcal{F}'$ satisfy the hypotheses of Lemma 6.1.

Moreover, from part 2 of Proposition 3.5 and part 1 of Proposition 3.6 we see that $\mathcal{F}'$ consists of mutually independent fields. Therefore

$$\mathfrak{f}_E \geq \frac{1}{2} \prod_{\substack{q|NA(E) \\ q \neq 2 \\ \mathbb{Q}(\zeta_q) \cap K_2 = \mathbb{Q}}} \left(1 - \frac{1}{\phi(q)}\right) \prod_{q \nmid NA(E)} \left(1 - \frac{1}{n(q)}\right) > 0.$$

The above analysis also shows that

$$\mathfrak{f}_E \gg \prod_{q|NA(E)} \left(1 - \frac{1}{q-1}\right),$$

since for $q \nmid NA(E)$ we have that $n(q) \asymp q^4$, by Serre's theorem. We can invoke now Mertens' theorem [HaWr, p. 351] (or elementary estimates for the Euler function) to deduce that

$$\prod_{\substack{q|NA(E) \\ q \neq 2}} \left(1 - \frac{1}{q-1}\right) \gg \frac{1}{\log \log(NA(E))}.$$

Then, by Proposition 3.7 we obtain that, under GRH,

$$\mathfrak{f}_E \gg \frac{1}{\log \log \log N}. \tag{27}$$

Similarly, by the unconditional upper bound $A(E) \ll_\varepsilon N^{1+\varepsilon}$ for any ε we obtain that, under no hypothesis,

$$\mathfrak{f}_E \gg \frac{1}{\log \log N}.$$

Now let us consider the case of a CM elliptic curve E defined over $\mathbb{Q}$ and such that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, and let us use again Corollary 6.2 to show that $\mathfrak{f}_E > 0$. We let $\mathcal{F} = (L_q = \mathbb{Q}(E[q]))_{q \geq 2}$, and, as before, we let K_2 be the unique abelian subextension of $\mathbb{Q}(E[2])$. Also let K be the complex multiplication field of E. We recall that $K(E[q]) = \mathbb{Q}(E[q])$ for any prime $q \geq 3$ (see [Mu1, Lemma 6]) and we observe that since K is a quadratic field and K_2 is a cubic or quadratic field, we have either $K_2 = K$ or $K_2 \cap K = \mathbb{Q}$. If $K_2 = K$ we take $\mathcal{F}' = (K_2)$ and so

$$\mathfrak{f}_E \geq \frac{1}{2},$$

and if $K_2 \cap K = \mathbb{Q}$ we take $\mathcal{F}' = (K_2, K)$ and so

$$\mathfrak{f}_E \geq \frac{1}{4}.$$

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

Remark 6.3. A careful study of the arguments in [Mu1, pp.161–167] for an unconditional proof of the asymptotic formula (2) in the case of a CM elliptic curve E defined over $\mathbb{Q}$ and of conductor N will lead to error$(E, x) = O_N \left(\frac{x}{(\log x)^B} \right)$ for any sufficiently large positive constant B. By combining this with (5) we can deduce again, unconditionally, that if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, then $\mathfrak{f}_E > 0$.

7. Proof of Theorem 1.3

We use the asymptotic formula for $f(x, \mathbb{Q})$ given by part 1 of Theorem 1.1 more precisely, we compare the main term $\mathfrak{f}_E \operatorname{li} x \sim \mathfrak{f}_E \frac{x}{\log x}$ with the error terms

$$O \left(x^{5/6} (\log(Nx))^{2/3} \right) \quad \text{and} \quad O \left(\frac{(\log \log x)(\log(Nx))}{\log x} A(E)^3 \right).$$

In doing so, we recall that under the current hypothesis we have $A(E) = O \left((\log N) (\log \log 2N)^3 \right)$ (see Proposition 3.7). Thus the second error term above is

$$O \left(\frac{(\log \log x)(\log(Nx))}{\log x} (\log N)^3 (\log \log 2N)^6 \right).$$

To find an upper estimate for the smallest x for which the main term is bigger than the error terms we can take $x = (\log N)^\alpha$ for some α, chosen such that

$$\frac{(\log N)^\alpha}{\alpha (\log \log N)(\log \log \log N)} \gg (\log N)^{\frac{5}{6}\alpha} (\log N + \alpha \log \log N)^{\frac{2}{3}} \qquad (28)$$

and

$$\frac{(\log N)^{\alpha}}{\alpha(\log\log N)(\log\log\log N)} \gg \frac{(\log\alpha + \log\log\log N)(\log N + \alpha\log\log N)}{\alpha\log\log N}$$
$$\times (\log N)^3(\log\log 2N)^6, \qquad (29)$$

where we have also used the lower bound (27) for the density $\mathfrak{f}_E$. Inequality (28) gives us $\alpha \geq \frac{5}{6}\alpha + \frac{2}{3} + \varepsilon$, or, equivalently, $\alpha \geq 4 + \varepsilon$ for any $\varepsilon > 0$, and inequality (29) gives us $\alpha \geq \varepsilon + 1 + 3$, or, equivalently, $\alpha \geq 4 + \varepsilon$ for any $\varepsilon > 0$. Thus the smallest x for which the main term is bigger than the error terms is

$$O_\varepsilon\left((\log N)^{4+\varepsilon}\right),$$

as claimed in the statement of the theorem.

Remark 7.1. The additional hypotheses AHC and PCC do not seem to lead to better estimates for p_E following this approach. Also, the slight improvements given in Remark 4.1 do not lead to better estimates for p_E, either.

8. Proof of Theorem 1.4

Similarly to the non-CM case, this result follows easily from Theorem 1.2 by comparing the main term with the error term. Note that in this case we can use the absolute lower bound $\mathfrak{f}_E \geq 1/4$ in the main term.

9. Final remarks

The high quality of the error terms in Theorems 1.1 and 1.2 leads us to suspect that the question about the cyclicity of $\overline{E}(\mathbb{F}_p)$ has a sharp divergence with the classical primitive root conjecture of Artin. Under GRH, it seems that we can do no better than obtain an error term of the form

$$O\left(\frac{x\log\log x}{(\log x)^2}\right)$$

in the primitive root problem.

It is possible that a delicate application of the lower bound sieve may lead to unconditional versions of Theorems 1.3 and 1.4. We reserve these investigations for a future paper. It will suffice for the moment to say that, in the CM case, the availability of a Bombieri-Vinogradov type theorem should make this hope feasible. As a first step, this would mean re-working the lower bound sieve technique and keeping track of the dependence of the error terms on the conductor of the elliptic curve.

References

[BoMoPo] Borosh, I., Moreno, C.J., Porta, H.: Elliptic curves over finite fields II. Math. Comput. **29**, 951–964 (1975)

[Br] Brenner, J.: The linear homogeneous group. Ann. Math. **39**, 472–493 (1938)

[Co1] Cojocaru, A.C.: On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves. J. Number Theory **96**, 335–350 (2002)

[Co2] Cojocaru, A.C.: Cyclicity of CM elliptic curves modulo p. Trans. AMS **355**, 2651–2662 (2003)

[Co3] Cojocaru, A.C.: Cyclicity of elliptic curves modulo p. PhD thesis, Queen's University, Canada, 2002

[Co4] Cojocaru, A.C.: On the surjectivity of the Galois representations associated to non-CM elliptic curves. With an Appendix by E. Kani, to appear in Canadian Math. Bulletin

[GuMu1] Gupta, R., Murty, M.R.: Primitive points on elliptic curves. Compositio Math. **58**, 13–44 (1986)

[GuMu2] Gupta, R., Murty, M.R.: Cyclicity and generation of points modulo p on elliptic curves. Invent. Math. **101**, 225–235 (1990)

[HaWr] Hardy, G.H., Wright, E.M.: An introduction to the theory of numbers. 5th ed., Oxford University Press, 1979

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

[Ko1] Koblitz, N.: Elliptic curve cryptosystems. Math. Comput. **48**, 203–209 (1987)

[Ko2] Koblitz, N.: Primality of the number of points on an elliptic curve over a finite field. Pacific J. Math. **131**, 157–165 (1988)

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

[LaTr] Lang, S., Trotter, H.: Primitive points on elliptic curves. Bull. Am. Math. Soc. **83**(2), 289–292 (1977)

[Li1] Linnik, Y.V.: On the least prime in an arithmetic progression. I. The basic theorem. Rec. Math. (Mat. Sbornik) N. S. **15**(57), 139–178 (1944)

[Li2] Linnik, Y.V.: On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon. Rec. Math. (Mat. Sbornik) N. S. **15**(57), 347–368 (1944)

[Ma] Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)

[Mu1] Murty, M.R.: On Artin's conjecture. J. Number Theory **16**, 147–168 (1983)

[Mu2] Murty, M.R.: On the supersingular reduction of elliptic curves. Proc. Indian Acad. Sci. (Math. Sci.) **97**(1–3), 247–250 (1987)

[Mu3] Murty, M.R.: Artin's conjecture for primitive roots. Math. Intelligencer **10**, 59–67 (1988)

[Mu4] Murty, M.R.: Artin's conjecture and elliptic analogues. In: Sieve Methods, Exponential Sums and their Applications in Number Theory, G.R.H. Greaves, G. Harman, M.N. Huxley (eds.), Cambridge University Press, 1996, pp. 326–344

[Mu5] Murty, M.R.: An introduction to Artin L-functions, J. Ramanujan Math. Soc. **16**, 261–307 (2001)

[MuMu] Murty, M.R., Murty, V.K.: The Chebotarev density theorem and pair correlation of zeros of Artin L-functions. To appear

[MuMuSa] Murty, M.R., Murty, V.K., Saradha, N.: Modular forms and the Chebotarev density theorem. Am. J. Math. **110**, 253–281 (1988)

[Se1] Serre, J-P.: Abelian l-adic representations and elliptic curves. W.A. Benjamin, Inc., New York, 1968

[Se2]   Serre, J-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972)

[Se3]   Serre, J-P.: Résumé des cours de 1977-1978. Annuaire du Collège de France, 67–70 (1978)

[Se4]   Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. Publ. Math. I.H.E.S., 123–201 (1981)

[Se5]   Serre, J-P.: Collected papers. volume III, Springer Verlag, 1985

[Si1]   Silverman, J.H.: The arithmetic of elliptic curves. Graduate Texts in Mathematics 106, Springer Verlag, New York, 1986

[Si2]   Silverman, J.H.: Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics 151, Springer Verlag, New York, 1994