J. Ramanujan Math. Soc. **28,** No.3 (2013) 271–298

On the asymptotics for invariants of elliptic curves modulo p

Adam Tyler Felix[1,*] and M. Ram Murty[2,**]

[1]*Department of Mathematics & Computer Science, University of Lethbridge, Lethbridge, Alberta, Canada*
e-mail: adam.felix@uleth.ca

[2]*Department of Mathematics & Statistics, Queen's University, Kingston, Ontario, Canada*
e-mail: murty@mast.queensu.ca

Communicated by: Dipendra Prasad

Received: July 12, 2012

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$. Let $\overline{E}(\mathbb{F}_p)$ denote the elliptic curve modulo p. It is known that there exist integers i_p and f_p such that $\overline{E}(\mathbb{F}_p) \cong \mathbb{Z}/i_p\mathbb{Z} \times \mathbb{Z}/i_p f_p\mathbb{Z}$. We study questions related to i_p and f_p. In particular, for any $\alpha > 0$ and $k \in \mathbb{N}$, we prove there exist positive constants c_α and c_k such that for any $A > 0$

$$\sum_{p \le x} (\log i_p)^\alpha = c_\alpha \mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right)$$

and

$$\sum_{p \le x} \tau_k(i_p) = c_k \mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right)$$

unconditionally for CM elliptic curves, where $\tau_k(n)$ is the number of ways of writing n as a product of k positive integers. For a CM curve E and $0 < \alpha < 1$, we prove that there exists a constant $c'_\alpha > 0$ such that

$$\sum_{p \le x} i_p^\alpha = c'_\alpha \mathrm{li}(x) + O\left(x^{\frac{3+\alpha}{4}} (\log x)^{\frac{1-\alpha}{2}}\right)$$

*Research of the first author supported by an NSERC PGS-D and a Max-Planck-Institut Stipend

**Research of the second author supported by an NSERC Discovery Grant

if GRH holds. For a non-CM curve E and $0 < \alpha < 1/2$, we prove that there exists $c''_\alpha > 0$ such that

$$\sum_{p \leq x} i_p^\alpha = c''_\alpha \mathrm{li}(x) + O\left(x^{\frac{5+2\alpha}{6}} (\log x)^{\frac{4-2\alpha}{3}}\right)$$

if GRH holds.

1991 *Mathematics Subject Classification.* 11N37, 11N36, 11R45, 11G05

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. For a prime $p \nmid N$, let $\overline{E}$ be the reduction of E modulo p. This is an elliptic curve defined over $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Hasse's Theorem [20, Theorem V.1.1] states $|a_p| \leq 2\sqrt{p}$ where

$$a_p := p + 1 - \#\overline{E}(\mathbb{F}_p) \tag{1.1}$$

We also have that there exist unique positive integers i_p and f_p such that $\overline{E}(\mathbb{F}_p) \cong \mathbb{Z}/i_p\mathbb{Z} \times \mathbb{Z}/i_p f_p\mathbb{Z}$. To see this let $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$. Then, $\overline{E}(\mathbb{F}_p)$ is a finite group since it is the set of solutions to a non-singular cubic curve with components in $\mathbb{F}_p$. For any elliptic curve $\widetilde{E}$ defined over a field $\Bbbk$, let $\widetilde{E}[k]$ denote the set of $\Bbbk$-rational points which are annihilated by the mapping $P \mapsto kP$. We have $\overline{E}(\mathbb{F}_p) \subset \overline{E}(\overline{\mathbb{F}_p})[k]$ for some k with $\#\overline{E}(\mathbb{F}_p) | k$ since $\overline{E}(\mathbb{F}_p)$ is finite. By [20, Corollary III.6.4], we have $\overline{E}(\overline{\mathbb{F}_p})[k] = \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$. So, $\overline{E}(\mathbb{F}_p) \cong \mathbb{Z}/i_p\mathbb{Z} \times \mathbb{Z}/i_p f_p\mathbb{Z}$ by the Fundamental theorem of finitely generated Abelian groups. As such, we have $\#\overline{E}(\mathbb{F}_p) = i_p^2 f_p$. Our main interest is in the sequence i_p as p ranges over all primes p.

We note that $\overline{E}(\mathbb{F}_p)$ is cyclic if and only if $i_p = 1$. The question of how often $\overline{E}(\mathbb{F}_p)$ is cyclic has been studied before by many authors. Borosh, Moreno, and Porta [4] computationally showed that we expect this to occur often. Serre [18] showed that on the generalized Riemann hypothesis (GRH) for the Dedekind zeta functions of the division fields $\mathbb{Q}(E[k])$ we have

$$N_E(x) := \#\{p \leq x : p \nmid N, \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \sim c_E \mathrm{li}(x) \tag{1.2}$$

where c_E is a positive constant if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, where $\mathbb{Q}(E[k])$ is smallest field containing the coordinates x, y for all $(x, y) \in E[k]$, and where $\mathrm{li}(x) := \int_2^x \frac{dt}{\log t}$. Murty [16] removed the dependence of GRH in (1.2) in the case E has complex multiplication (hereafter denoted by CM):

$$N_E(x) = c_E \mathrm{li}(x) + O_N\left(\frac{x \log\log x}{(\log x)^2}\right). \tag{1.3}$$

In [17], he showed for certain non-CM elliptic curves, there exist infinitely many primes p such that $\overline{E}(\mathbb{F}_p)$ is cyclic. Gupta and Murty [12] showed that for any elliptic curve E such that $\mathbb{Q}(E[2]) \neq \mathbb{Q}$, the following relation holds

$$\#\{p \leq x : p \nmid N, \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \gg_N \frac{x}{(\log x)^2}.$$

In [5], Cojocaru proved that (1.2) only needs a 3/4-GRH. That is, there are no zeroes of the Dedekind zeta functions of $\mathbb{Q}(E[k])$ in the region $\Re(s) > 3/4$ as k ranges over squarefree integers. In [6], she also simplified the unconditional proof of when E has CM, and in [8], she and M. Ram Murty proved that if the GRH is assumed, then the relation becomes

$$N_E(x) = c_E \mathrm{li}(x) + O_N(x^{5/6}(\log x)^{2/3})$$

if E does not have CM and

$$N_E(x) = c_E \mathrm{li}(x) + O_N(x^{3/4}(\log x)^{1/2})$$

if E has CM. Here the dependence on the conductor N in the error terms can be made explicit. Similar results exist for $N_E(x; w) := \#\{p \leq x : p \nmid N, i_p = w\}$ where $w \in \mathbb{N}$ is fixed (see [7, Theorem 2]).

1.1 Generalizing Serre's result

Note that

$$N_E(x) = \sum_{\substack{p \leq x \\ p \nmid N}} \chi_{\{1\}}(i_p),$$

where for $S \subset \mathbb{N}$, we define $\chi_S(n) = 1$ if $n \in S$ and $\chi_S(n) = 0$ otherwise. We would like to know when can $\chi_{\{1\}}$ be replaced by a function $f : \mathbb{N} \to \mathbb{C}$ and the relation

$$\sum_{p \leq x} f(i_p) \sim c_{E,f} \mathrm{li}(x)$$

holds where $c_{E,f}$ is a constant depending on E and f?

Kowalski [15, Proposition 3.8] has shown the following unconditional result:

$$\sum_{p \leq x} i_p \gg \begin{cases} \frac{x \log\log x}{\log x} & \text{if } E \text{ has CM} \\ \frac{x}{\log x} & \text{otherwise} \end{cases}.$$

In fact, this result is true for any elliptic curve E defined over a number field K, where the above implied constant is now dependent on K. Define $\tau(n) = \sum_{d|n} 1$. Akbary and Ghioca [2] have shown

$$\sum_{p \leq x} \tau(i_p) = c_E \mathrm{li}(x) + O(x^{5/6}(\log x)^{2/3}) \tag{1.4}$$

if GRH holds, and

$$\sum_{p \leq x} \tau(i_p) = c_E \mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right)$$

unconditionally for any $A > 1$ if E has CM with endomorphism ring isomorphic to the ring of algebraic integers of some imaginary quadratic field. They have also shown that (1.4) can be generalized to Abelian varieties defined over $\mathbb{Q}$ which have a one-dimensional subvariety which is also defined over $\mathbb{Q}$.

1.2 Definitions and notation

Throughout, the letter E will denote an elliptic curve defined over $\mathbb{Q}$ of conductor N. In particular, $E(\mathbb{Q})$ is an Abelian group with additive identity 0. For $k \in \mathbb{Z}$, we define

$$E[k] := \{(x, y) \in \overline{\mathbb{Q}}^2 : k(x, y) = 0\}.$$

We similarly define $E(K)[k]$ for any field K with $\mathbb{Q} \subset K$. We denote by $\mathbb{Q}(E[k])$ the smallest field containing $\mathbb{Q}$ and the set $\{x, y : (x, y) \in E[k]\}$. We say that E has CM if the endomorphism ring of E is larger than $\mathbb{Z}$. See [20, §III.4] for more information about the endomorphism ring of elliptic curves. See [20, Appendix C], [21, Chapter II], or [25, Chapter 10] for more information about complex multiplication.

The letters p and q will denote prime numbers with $p \nmid N$. We note that this will not affect the proofs as there are only finitely many primes which divide N. Also, d, k, m, n, and w will denote positive integers, and x, y, and z will denote positive real numbers.

By the notation $f(x) = O\big(g(x)\big)$ or $f(x) \ll g(x)$, we mean that there exists a constant C such that for all x in the domain of f and g we have $|f(x)| \leq Cg(x)$. By $f(x) = O_E\big(g(x)\big)$ or $f(x) \ll_E g(x)$ we mean that the above constant is dependent on E. We may be more explicit with this notation. For example, we may write $f(x) \ll_N g(x)$ if the constant C is dependent on the conductor N. By $f(x) \sim g(x)$ we mean

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$$

where x in the above limit is restricted to the domain of f and g.

For $x \geq 2$, define the logarithmic integral by the following function

$$\mathrm{li}(x) := \int_2^x \frac{dt}{\log t}.$$

For $b, k \in \mathbb{N}$, define $\pi(x; k, b) = \#\{p \leq x : p \equiv b \bmod k\}$. For $m \in \mathbb{N}$, define

$$\pi_m(x) := \#\{p \leq x : m | i_p\}.$$

We also define the following arithmetic functions: for all $n \in \mathbb{N}$, we have

$$\Lambda(n) := \begin{cases} \log p & \text{if } n = p^\alpha \text{ for some } \alpha \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

$$\omega(n) := \#\{p|n\},$$

$$\Omega(n) := \#\{p^\alpha | n : \alpha \in \mathbb{N}\},$$

$$\varphi(n) := \#\{1 \leq a \leq n : \gcd(a, n) = 1\},$$

$$\mu(n) := \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is squarefree} \\ 0 & \text{otherwise} \end{cases},$$

$$\tau(n) := \#\{d|n\},$$

for $k \in \mathbb{N}$,

$$\tau_k(n) := \#\{(a_1, a_2, \ldots, a_k) \in \mathbb{N}^k : n = a_1 a_2 \cdots a_k\},$$

and for $\alpha \in \mathbb{R}$,

$$\sigma_\alpha(n) := \sum_{m|n} m^\alpha.$$

The functions Λ, φ, and μ are known as the von Mangoldt function, the Euler totient function, and Möbius function, respectively.

For K an algebraic number field, we define $\mathcal{O}_K$ to be the ring of algebraic integers of K. The letter $\mathfrak{p}$ will always denote a prime ideal of $\mathcal{O}_K$. For a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, define $N(\mathfrak{a})$ to be the index of $\mathfrak{a}$ inside $\mathcal{O}_K$. We define the number field analogue of φ, the Euler totient function, as follows: let $\mathfrak{a}$ be a non-zero ideal $\mathfrak{a}$ in $\mathcal{O}_K$. The number of residue classes relatively prime to $\mathfrak{a}$ in $\mathcal{O}_K$ is $\Phi(\mathfrak{a})$. As when $K = \mathbb{Q}$, we have the following multiplicative formula for Φ

$$\Phi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right). \tag{1.5}$$

1.3 Statement of results

We first introduce two hypotheses: let α and β be real numbers with α non-negative. Let $g : \mathbb{N} \to \mathbb{C}$. We say that Hypothesis $H(g; \alpha, \beta)$ holds if

$$\sum_{m \leq x} |g(m)| \ll x^{1+\alpha} (\log x)^\beta.$$

We say that Hypothesis $H'(g;\alpha,\beta)$ holds if

$$\sum_{m\leq x}|g(m)|^2 \ll x^{1+\alpha}(\log x)^{\beta}.$$

In §4, §5, and §6, we will prove the following result:

Theorem 1.1. *Let E be an elliptic curve. Let $f:\mathbb{N}\to\mathbb{C}$ and $g:\mathbb{N}\to\mathbb{C}$ be such that*

$$f(n)=\sum_{d|n}g(d)$$

for all $n\in\mathbb{N}$.

(a) *Suppose E has CM, and suppose $H(g;0,\beta)$ and $H'(g;0,\gamma)$ hold for some real numbers β and γ. Then, there exists a constant $c_{E,f}$ such that*

$$\sum_{p\leq x}f(i_p)=c_{E,f}\mathrm{li}(x)+O_E\left(\frac{x}{(\log x)^A}\right)$$

for all $A>1$.

(b) *Suppose E has CM and $H(g;\alpha,\beta)$ holds for some $\alpha<1$ and for some $\beta\in\mathbb{R}$. Suppose further that GRH holds for E. Then, there exists a constant $c_{E,f}$ such that*

$$\sum_{p\leq x}f(i_p)=c_{E,f}\mathrm{li}(x)+O_E\left(x^{\frac{3+\alpha}{4}}(\log x)^{\frac{2\beta-\alpha-1}{2}}\right).$$

(c) *Suppose E does not have CM and $H(g;\alpha,\beta)$ holds for some $\alpha<1/2$ and for some $\beta\in\mathbb{R}$. Suppose further that GRH holds for E. Then, there exists a constant $c_{E,f}$ such that*

$$\sum_{p\leq x}f(i_p)=c_{E,f}\mathrm{li}(x)+O_E\left(x^{\frac{5+2\alpha}{6}}(\log x)^{\frac{(1+\beta)(2-\alpha)}{3}}\right).$$

(d) *Suppose E has CM and $H(g;2,-\beta)$ holds for some $\beta>2$. Suppose further that GRH holds for E. Then, there exists a constant $c_{E,f}$ such that*

$$\sum_{p\leq x}f(i_p)=c_{E,f}\mathrm{li}(x)+O_E\left(\frac{x}{(\log x)^{\beta-1}}\right).$$

In §7, we will give some applications of this result. In particular, we will show that the functions $(\log n)^{\alpha}$, $\omega(n)^k$, $\Omega(n)^k$, $2^{\omega(n)k}$, and $\tau_k(n)^r$ where k and r are fixed non-negative integers and α is a fixed non-negative real number which all satisfy the hypotheses of Theorem 1.1 (a), (b), and (c). We will also

show that the functions n^α and $\sigma_\alpha(n)$ satisfy the hypotheses of Theorem 1.1 (b) and (c) where α must be in the ranges given in (b) or (c) of this theorem. Theorem 1.1 (d) and the results for functions n^α and σ_α nearly answer a problem posed by Kowalski ([15, Problem 3.1]).

We are able to apply Theorem 1.1 to $e_p := i_p f_p$, which is the exponent of $\overline{E}(\mathbb{F}_p)$, and to f_p to obtain the following result.

Theorem 1.2. *Let k be a fixed positive integer. Then, there exist constants $c_{E,k}$ and $c_{E,2k}$ such that*

$$\sum_{p\le x} e_p^k = c_{E,k}\mathrm{li}(x^{k+1}) + O(x^k E(x))$$

and

$$\sum_{p\le x} f_p^k = c_{E,2k}\mathrm{li}(x^{k+1}) + O(x^k E(x)),$$

where

$$E(x) = \begin{cases} O_E(x^{3/4}(\log x)^2) & \text{if } E \text{ has CM and GRH holds for } E \\ O_E(x^{5/6}(\log x)^2) & \text{if } E \text{ does not have CM and GRH holds for } E \\ O_{A,E}\left(\frac{x}{(\log x)^A}\right) & \text{if } E \text{ has CM} \end{cases}.$$

This result improves and generalizes the result of Freiberg and Kurlberg [10]. See also [14,26].

In §7, we also prove the following result:

Theorem 1.3. *Let E be an elliptic curve. Suppose E has CM. Then, for every $C > 0$, there exists $x_0 := x_0(C)$ such that for $x \ge x_0$, we have*

$$\sum_{p\le x} i_p \ge C\frac{x\log\log x}{\log x}$$

unconditionally. That is,

$$\lim_{x\to\infty} \frac{\left(\sum_{p\le x} i_p\right)\log x}{x\log\log x} = +\infty.$$

2. Outline of proofs

In order to evaluate the summations in question and $\pi_m(x) = \#\{p \le x : m | i_p\}$ in particular, we need the following classical result:

Lemma 2.1. *Let $m \in \mathbb{N}$ be fixed. Let $p \nmid N$. Then, $m | i_p$ if and only if p splits completely in the field $\mathbb{Q}(E[m])$.*

Proof. See [16, Lemma 2], [8, Lemma 2.1], or [2, Lemma 3.2]. □

We also need the following bound on i_p.

Lemma 2.2. *For any $p \nmid N$, $i_p \leq \sqrt{p} + 1$.*

Proof. By Hasse's theorem (1.1), we have

$$i_p^2 | \#\overline{E}(\mathbb{F}_p) = p + 1 - a_p \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \leq (\sqrt{x} + 1)^2.$$

Thus, $i_p \leq \sqrt{x} + 1$. □

Let $f : \mathbb{N} \to \mathbb{C}$. We now ask when does the following relation hold for f

$$\sum_{p \leq x} f(i_p) \sim c_{E,f} \pi(x)$$

where $c_{E,f}$ is a constant depending on E and f?

Note that if we write

$$f(n) = \sum_{m|n} g(m)$$

where $g : \mathbb{N} \to \mathbb{C}$, then

$$\sum_{p \leq x} f(i_p) = \sum_{p \leq x} \sum_{m | i_p} g(m) = \sum_{m \leq \sqrt{x}+1} g(m) \sum_{\substack{p \leq x \\ m | i_p}} 1 = \sum_{m \leq \sqrt{x}+1} g(m) \pi_m(x) \tag{2.1}$$

by Lemma 2.2.

We note that it is always possible to write

$$f(n) = \sum_{m|n} g(m)$$

by the Möbius inversion formula (see [9, Theorem 1.2.2]).

Break the final summation in (2.1) as follows:

$$\sum_{p \leq x} f(i_p) = \sum_{m \leq y} g(m) \pi_m(x) + \sum_{y < m \leq \sqrt{x}+1} g(m) \pi_m(x).$$

Now, GRH, the effective Chebotarev density theorem, and Lemma 2.1 or class field theory and a generalization of the Bombieri-Vinogradov theorem allow us to handle the first summation. Techniques of [8] or [16] allow us to handle the last summation. See also [3].

3. Preliminaries

3.1 The Chebotarev density theorem for the division fields

We will need the following corollary of the effective Chebotarev density theorem [19], Lemma 2.1, and [20, Theorem VII.7.1].

Theorem 3.1. *Let $m \in \mathbb{N}$. Suppose GRH holds for the Dedekind zeta function of $\mathbb{Q}(E[m])$. Then,*

$$\pi_m(x) = \frac{\mathrm{li}(x)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} + O(\sqrt{x}\log(mNx)).$$

Proof. See [8, Section 3] or [2, Corollary 3.4]. □

For the size of $[\mathbb{Q}(E[m]) : \mathbb{Q}]$, we have the following result.

Lemma 3.2. *Let E be an elliptic curve defined over $\mathbb{Q}$.*

(a) *Then,*

$$m^{2-\varepsilon} \ll_{E,\varepsilon} [\mathbb{Q}(E[m]) : \mathbb{Q}] \leq m^4$$

for any $\varepsilon > 0$.

(b) *Suppose E has complex multiplication by the full ring of integers $\mathcal{O}_K$ of a quadratic imaginary field K. Then, for any positive integer $m \geq 3$, we have*

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

In particular,

$$\varphi(m)^2 \ll [\mathbb{Q}(E[m]) : \mathbb{Q}] \ll m^2.$$

Proof. (a) For the lower bound see [2, Equation (3.1)]. The upper bound is a consequence of injectivity of the Galois representation $\phi_m : \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(E[m])) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ associated to E (see [22, Galois Representation Theorem on p. 196]).

(b) This is [8, Proposition 3.8]. We note this proof restricts to E with CM by the full ring of integers of an imaginary quadratic field. However, the proof extends to E with CM by an order of such a field (see [10, Proposition 3.2.d]). □

These bounds on $[\mathbb{Q}(E[m]) : \mathbb{Q}]$ and the previous asymptotic will allow us to obtain an asymptotic formula for small m. For large m, we need the following result.

Lemma 3.3. *For $3 \leq m \leq \sqrt{x} + 1$, we have $\pi_m(x) \ll \frac{x}{m^2}$.*

Proof. For squarefree m, this is [3, Lemma 2.5]. The same proof works for generic m by [6, Lemma 2.2] or [16, Lemma 5]. □

3.2 Complex multiplication and class field theory

Let E be an elliptic curve with complex multiplication by an order in the ring of algebraic integers $\mathcal{O}_K$ of an imaginary quadratic field K. Then, by [20, Appendix C, Example 11.3.1], we have that K has class number 1. We say $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent (and write $\mathfrak{a} \sim \mathfrak{b}$) if there exist $\alpha, \beta \in \mathcal{O}_K$ such that $\langle\alpha\rangle\mathfrak{a} = \langle\beta\rangle\mathfrak{b}$. We say that $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent modulo $\mathfrak{q}$ if both $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime to $\mathfrak{q}$, there exist $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha \equiv \beta \equiv 1 \bmod \mathfrak{q}$, and $\langle\alpha\rangle\mathfrak{a} = \langle\beta\rangle\mathfrak{b}$. This is an equivalence relation with $h(\mathfrak{q}) = \Phi(\mathfrak{q})/T(\mathfrak{q})$ equivalence classes, where Φ is the number field analogue of the Euler totient function and $T(\mathfrak{q})$ is the number of residue classes modulo $\mathfrak{q}$ that contain a unit.

Let $N(\mathfrak{a})$ denote the norm of an ideal $\mathfrak{a} \subset \mathcal{O}_K$. For $\mathfrak{a}$ and $\mathfrak{q}$ with $\gcd(\mathfrak{a}, \mathfrak{q}) = 1$, define

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

Denote by $\mathfrak{m}$ the ideal $m\mathcal{O}_K$ where $m \in \mathbb{N}$. The ideal $\mathfrak{f}$ will denote an ideal of $\mathcal{O}_K$ which has prime ideal divisors in $\mathcal{O}_K$ which are prime ideals of bad reduction of E over K. We will need the following lemma:

Lemma 3.4. *Let E be an elliptic curve defined over $\mathbb{Q}$ which has CM by $\mathcal{O}_K$ for some imaginary quadratic field K. Let $m \geq 1$ be an integer. Then, there is an ideal $\mathfrak{f}$ of $\mathcal{O}_K$ and $t(m)$ ideal classes modulo $\mathfrak{fm}$ represented by $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_{t(m)}$ with the following property: if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ with $\mathfrak{p} \nmid \mathfrak{fm}$, then $\mathfrak{p}$ splits completely in $K(E[m])$ if and only if $\mathfrak{p} \sim \mathfrak{m}_i \bmod \mathfrak{fm}$ for some $i \in \{1, 2, \ldots, t(m)\}$. Moreover, $t(m)[K(E[m]) : K] = h(\mathfrak{fm})$ and*

$$t(m) \ll \Phi(\mathfrak{f}) \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 + \frac{1}{N(\mathfrak{p}) - 1}\right).$$

Proof. This is [3, Lemma 2.7]. Also, see [16, Lemma 4] or [1, Lemma 3.3]. □

We will need the following extension of the Bombieri–Vinogradov theorem (see [13, Theorem 1]):

Lemma 3.5. *For any $A > 0$, there exists $B = B(A)$ such that*

$$\sum_{N(\mathfrak{q}) \leq \frac{\sqrt{x}}{(\log x)^B}} \max_{\gcd(\mathfrak{a}, \mathfrak{q}) = 1} \frac{1}{T(\mathfrak{q})} \left| \pi_K(x; \mathfrak{q}, \mathfrak{a}) - \frac{\mathrm{li}(x)}{h(\mathfrak{q})} \right| \ll_{B,K} \frac{x}{(\log x)^A}.$$

Define

$$\widetilde{\pi}_{\mathfrak{m}}(x) := \#\{\mathfrak{p} \subset \mathcal{O}_K : N(\mathfrak{p}) \leq x, \mathfrak{p} \nmid \mathfrak{fm}, \mathfrak{p} \text{ splits completely in } K(E[m])\}.$$

Then, we have the following result:

Lemma 3.6. *For $m \in \mathbb{N}$ with $m \geq 3$,*

$$\pi_m(x) = \frac{\widetilde{\pi}_{\mathfrak{m}}(x)}{2} + O\left(\frac{\sqrt{x}}{\log x}\right) + O(\log N)$$

and

$$\pi_m(x) \leq \frac{1}{2}\widetilde{\pi}_{\mathfrak{m}}(x).$$

Proof. The first relation is [3, Eq. (3.2)] and its justification on page 35.

For the second relation, we have that if p is a prime of good reduction for E over $\mathbb{Q}$ which splits completely in $\mathbb{Q}(E[m])$, then $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are prime ideals of good reduction for E over K and so $\mathfrak{p} \nmid \mathfrak{f}$ where $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. Hence, $2\pi_m(x) \leq \widetilde{\pi}_m(x)$. □

4. Proof of Theorem 1.1(a)

Recall the hypotheses of Theorem 1.1: we have functions $f : \mathbb{N} \to \mathbb{C}$ and $g : \mathbb{N} \to \mathbb{C}$ such that

$$f(n) = \sum_{m|n} g(m)$$

for all $n \in \mathbb{N}$. We also have

$$\sum_{n \leq y} |g(n)| \ll y^{1+\alpha}(\log y)^{\beta}.$$

By (2.1),

$$\sum_{p \leq x} f(i_p) = \sum_{m \leq \sqrt{x}+1} g(m)\pi_m(x)$$

Thus,

$$\sum_{p \leq x} f(i_p) = \sum_{m \leq y} g(m)\pi_m(x) + \sum_{y < m \leq \sqrt{x}+1} g(m)\pi_m(x)$$

where y with $y \leq \sqrt{x} + 1$ will be chosen later.

Then,

$$\sum_{y < m \leq \sqrt{x}+1} g(m)\pi_m(x) \ll x \sum_{y < m \leq \sqrt{x}+1} \frac{|g(m)|}{m^2}$$

by Lemma 3.3. By $H(g; 0, \beta)$, we have

$$\sum_{m > y} \frac{|g(m)|}{m^2} \ll \frac{(\log y)^{\beta}}{y}.$$

Hence,

$$\sum_{y < m \leq \sqrt{x}+1} g(m)\pi_m(x) \ll \frac{x(\log y)^{\beta}}{y}. \tag{4.1}$$

For the main term, we will use Lemma 3.5. We have

$$\sum_{m\leq y} g(m)\pi_m(x) = g(1)\pi_1(x) + g(2)\pi_2(x) + \sum_{3\leq m\leq y} g(m)\pi_m(x).$$

The prime number theorem and [3, Lemma 2.3] give us

$$g(1)\pi_1(x) + g(2)\pi_2(x) = \left(g(1) + \frac{g(2)}{[\mathbb{Q}(E[2]) : \mathbb{Q}]}\right)\mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right).$$

So, we may now consider

$$\sum_{3\leq m\leq y} g(m)\pi_m(x).$$

Let $G_m = \mathrm{Gal}(K(E[m])/K)$. By Lemma 3.6, we have

$$\begin{aligned}
&\sum_{3\leq m\leq y} g(m)\pi_m(x)\\
&\quad= \sum_{3\leq m\leq y} g(m)\left(\frac{\widetilde{\pi}_{\mathfrak{m}}(x)}{2} + O\left(\frac{\sqrt{x}}{\log x}\right) + O(\log N)\right)\\
&\quad= \frac{1}{2}\mathrm{li}(x)\sum_{3\leq m\leq y}\frac{g(m)}{|G_m|} + O\left(\sum_{3\leq m\leq y}\left|g(m)\left(\widetilde{\pi}_{\mathfrak{m}}(x) - \frac{\mathrm{li}(x)}{|G_m|}\right)\right|\right)\\
&\qquad+ O\left(\frac{\sqrt{x}}{\log x}\sum_{m\leq y}|g(m)|\right) + O\left(\log N\sum_{m\leq y}|g(m)|\right)\\
&\quad= \frac{1}{2}\mathrm{li}(x)\sum_{m\geq 3}\frac{g(m)}{|G_m|} + O\left(\mathrm{li}(x)\sum_{m>y}\frac{|g(m)|}{|G_m|}\right) + O_N\left(\frac{y\sqrt{x}(\log y)^\beta}{\log x}\right)\\
&\qquad+ O\left(\sum_{3\leq m\leq y}\left|g(m)\left(\widetilde{\pi}_{\mathfrak{m}}(x) - \frac{\mathrm{li}(x)}{|G_m|}\right)\right|\right). \qquad (4.2)
\end{aligned}$$

We have $|G_m| \gg \varphi(m)^2$ by Lemma 3.2 (b) since E has CM. Thus,

$$\sum_{m\geq 3}\frac{|g(m)|}{|G_m|} \ll \sum_{m\geq 3}\frac{|g(m)|}{\varphi(m)^2} < \infty \qquad (4.3)$$

and

$$\sum_{m>y}\frac{|g(m)|}{|G_m|} \ll \frac{(\log y)^\beta(\log\log y)^2}{y^{1-\alpha}} \qquad (4.4)$$

by $H(g;0,\beta)$. So we must bound

$$\sum_{3\le m\le y}\left|g(m)\left(\widetilde{\pi}_{\mathfrak{m}}(x)-\frac{\mathrm{li}(x)}{|G_m|}\right)\right|.$$

Let us first evaluate the summation

$$\sum_{3\le m\le y}\left|\widetilde{\pi}_{\mathfrak{m}}(x)-\frac{\mathrm{li}(x)}{|G_m|}\right|.$$

By Lemma 3.4, we have $t(m)|G_m| = h(\mathfrak{fm})$ and

$$\widetilde{\pi}_{\mathfrak{m}}(x)=\sum_{i=1}^{t(m)}\pi_K(x;\mathfrak{fm},\mathfrak{m}_i).$$

Thus,

$$\widetilde{\pi}_{\mathfrak{m}}(x)-\frac{\mathrm{li}(x)}{|G_m|}=\sum_{i=1}^{t(m)}\left(\pi_K(x;\mathfrak{fm},\mathfrak{m}_i)-\frac{\mathrm{li}(x)}{h(\mathfrak{fm})}\right). \tag{4.5}$$

Recall that $t(m)\ll_{\mathfrak{f}} 1$ by Lemma 3.4. We may also take $\mathfrak{f}$ to be the conductor of the Größencharacter associated to E by [16, Proof of Lemma 4] or [3, Remark 2.8]. Let $t(m)\le C(\mathfrak{f})$, where $C(\mathfrak{f})$ is this constant depending on $\mathfrak{f}$. By Lemma 3.5, we have

$$\sum_{N(\mathfrak{q})\le\frac{\sqrt{x}}{(\log x)^B}}\max_{\gcd(\mathfrak{a},\mathfrak{q})=1}\frac{1}{T(\mathfrak{q})}\left|\pi_K(x;\mathfrak{q},\mathfrak{a})-\frac{\mathrm{li}(x)}{h(\mathfrak{q})}\right|\ll\frac{x}{(\log x)^A}. \tag{4.6}$$

However, we know that $T(\mathfrak{q})\le 6$. Thus, (4.6) becomes

$$\sum_{N(\mathfrak{q})\le\frac{\sqrt{x}}{(\log x)^B}}\max_{\gcd(\mathfrak{a},\mathfrak{q})=1}\left|\pi_K(x;\mathfrak{q},\mathfrak{a})-\frac{\mathrm{li}(x)}{h(\mathfrak{q})}\right|\ll\frac{x}{(\log x)^A}.$$

Suppose $y\le x^{1/4}/\sqrt{N(\mathfrak{f})}(\log x)^B$. By (4.5), we have

$$\begin{aligned}\sum_{3\le m\le y}\left|\widetilde{\pi}_{\mathfrak{m}}(x)-\frac{\mathrm{li}(x)}{|G_m|}\right| &= \sum_{3\le m\le y}\left|\sum_{i=1}^{t(m)}\left(\pi_K(x;\mathfrak{fm},\mathfrak{m}_i)-\frac{\mathrm{li}(x)}{h(\mathfrak{fm})}\right)\right|\\ &\le \sum_{3\le m\le\frac{x^{1/4}}{\sqrt{N(\mathfrak{f})}(\log x)^B}}\left|\sum_{i=1}^{t(m)}\left(\pi_K(x;\mathfrak{fm},\mathfrak{m}_i)-\frac{\mathrm{li}(x)}{h(\mathfrak{fm})}\right)\right|\\ &\ll \sum_{i=1}^{C(\mathfrak{f})}\sum_{N(\mathfrak{m})=m^2\le\frac{\sqrt{x}}{N(\mathfrak{f})(\log x)^{2B}}}\left|\pi_K(x;\mathfrak{fm},\mathfrak{m}_i)-\frac{\mathrm{li}(x)}{h(\mathfrak{fm})}\right|\end{aligned}$$

$$\ll \sum_{i=1}^{C(\mathfrak{f})} \sum_{N(\mathfrak{fm}) \leq \frac{\sqrt{x}}{(\log x)^{2B}}} \left| \pi_K(x; \mathfrak{fm}, \mathfrak{m}_i) - \frac{\mathrm{li}(x)}{h(\mathfrak{fm})} \right|$$

$$\ll \sum_{i=1}^{C(\mathfrak{f})} \sum_{N(\mathfrak{q}) \leq \frac{\sqrt{x}}{(\log x)^{2B}}} \left| \pi_K(x; \mathfrak{q}, \mathfrak{m}_i) - \frac{\mathrm{li}(x)}{h(\mathfrak{q})} \right|$$

$$\ll \sum_{i=1}^{C(\mathfrak{f})} \frac{x}{(\log x)^A} \ll \frac{x}{(\log x)^A}.$$

We are now ready to evaluate

$$\sum_{3 \leq m \leq y} \left| g(m) \left(\widetilde{\pi}_{\mathfrak{m}}(x) - \frac{\mathrm{li}(x)}{|G_m|} \right) \right|.$$

We have $\widetilde{\pi}_{\mathfrak{m}}(x) = 2\pi_m(x) + O(\sqrt{x}/\log x)$ by Lemma 3.6. However, we have p splits completely in $\mathbb{Q}(E[m])$ with $m \geq 3$ implies $p \equiv 1 \bmod m$ by [20, Corollary III.8.1.1]. Thus,

$$\begin{aligned} \left| \widetilde{\pi}_{\mathfrak{m}}(x) - \frac{\mathrm{li}(x)}{|G_m|} \right| &\leq 2\pi_m(x) + O\left(\frac{\sqrt{x}}{\log x} \right) + \frac{\mathrm{li}(x)}{|G_m|} \\ &\ll \pi(x; m, 1) + \frac{\sqrt{x}}{\log x} + \frac{\mathrm{li}(x)}{\varphi(m)^2} \\ &\ll \frac{x}{m} + \frac{\sqrt{x}}{\log x} + \frac{x(\log\log m)^2}{m^2} \\ &\ll \frac{x}{m} \end{aligned} \tag{4.7}$$

for $m \leq \sqrt{x}\log x$. By the Cauchy-Schwarz inequality, $H'(g; 0, \gamma)$, and (4.7), we have

$$\begin{aligned} &\sum_{3 \leq m \leq y} \left| g(m) \left(\widetilde{\pi}_{\mathfrak{m}}(x) - \frac{\mathrm{li}(x)}{|G_m|} \right) \right| \\ &\quad = \sum_{3 \leq m \leq y} \left| g(m) \left(\widetilde{\pi}_{\mathfrak{m}}(x) - \frac{\mathrm{li}(x)}{|G_m|} \right)^{1/2} \left(\widetilde{\pi}_{\mathfrak{m}}(x) - \frac{\mathrm{li}(x)}{|G_m|} \right)^{1/2} \right| \\ &\quad \leq \left(\sum_{m \leq y} |g(m)|^2 \left| \widetilde{\pi}_{\mathfrak{m}}(x) - \frac{\mathrm{li}(x)}{|G_m|} \right| \right)^{1/2} \left(\sum_{m \leq y} \left| \widetilde{\pi}_{\mathfrak{m}}(x) - \frac{\mathrm{li}(x)}{|G_m|} \right| \right)^{1/2} \end{aligned}$$

$$\ll \left(x \sum_{m \le y} \frac{|g(m)|^2}{m} \right)^{1/2} \frac{\sqrt{x}}{(\log x)^{A/2}}$$
$$\ll \frac{x (\log y)^{\frac{\gamma+1}{2}}}{(\log x)^{\frac{A}{2}}}.$$

Choosing A sufficiently large and $y = x^{1/4}/\sqrt{N(\mathfrak{f})}(\log x)^B$ finishes the proof of Theorem 1.1 (a) by (4.1), (4.2), (4.4).

5. Proof of Theorem 1.1 (b) and (c)

Let $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$. By GRH and Theorem 3.1, we have

$$\sum_{m \le y} g(m)\pi_m(x) = \sum_{m \le y} g(m) \left(\frac{\mathrm{li}(x)}{|G_m|} + O\left(\sqrt{x}\log(mNx)\right) \right)$$
$$= \mathrm{li}(x) \sum_{m \ge 1} \frac{g(m)}{|G_m|} + O\left(\mathrm{li}(x) \sum_{m > y} \frac{|g(m)|}{|G_m|} \right)$$
$$+ O_N\left(\sqrt{x}\log x \sum_{m \le y} |g(m)| \right).$$

If E has CM, by $H(g; \alpha, \beta)$ (see (4.3) and (4.4)), we have

$$\sum_{m \ge 1} \frac{g(m)}{|G_m|} < \infty$$

and

$$\sum_{m > y} \frac{|g(m)|}{|G_m|} \ll \frac{(\log y)^{\beta} (\log\log y)^2}{y^{1-\alpha}}. \tag{5.1}$$

If E does not have CM, then we have $|G_m| \gg m^{2-\varepsilon}$ for all $\varepsilon > 0$ by Lemma 3.2 (a). Thus,

$$\sum_{m \ge 1} \frac{|g(m)|}{|G_m|} < \infty$$

and

$$\sum_{m > y} \frac{|g(m)|}{|G_m|} \ll \frac{1}{y^{1-\alpha-\varepsilon}} \tag{5.2}$$

by $H(g; \alpha, \beta)$.

Thus,

$$\sum_{m\leq y} g(m)\pi_m(x) = c_E \mathrm{li}(x) + O\left(\frac{x(\log y)^{\beta}(\log\log y)^2}{y^{1-\alpha}\log x}\right) + O(y^{1+\alpha}\sqrt{x}(\log x)(\log y)^{\beta})$$

if E has CM, and

$$\sum_{m\leq y} g(m)\pi_m(x) = c_E \mathrm{li}(x) + O\left(\frac{x}{y^{1-\alpha-\varepsilon}\log x}\right) + O(y^{1+\alpha}\sqrt{x}(\log x)(\log y)^{\beta})$$

if E does not have CM, where

$$c_E = \sum_{m\geq 1} \frac{g(m)}{|G_m|}$$

is a constant by Lemma 3.2 (a).

Now we must bound the error term

$$\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m(x).$$

We will break this determination up into the CM and non-CM cases:

5.1 CM Case

Let $a_p := p + 1 - \#\overline{E}(\mathbb{F}_p)$. We define p to an ordinary prime if $a_p \neq 0$, and we define p to be supersingular if $a_p = 0$. We also define

$$\pi_m^{\mathrm{o}}(x) := \#\{p \leq x : p \text{ is ordinary and } m|i_p\}$$

and

$$\pi_m^{\mathrm{s}}(x) := \#\{p \leq x : p \text{ is supersingular and } m|i_p\}.$$

We note that $\pi_m(x) = \pi_m^{\mathrm{o}}(x) + \pi_m^{\mathrm{s}}(x)$. Thus,

$$\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m(x) = \sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m^{\mathrm{o}}(x) + \sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m^{\mathrm{s}}(x).$$

Observe that $a_p = 0$ implies $\#\overline{E}(\mathbb{F}_p) = p + 1$. We also have $m|i_p|i_p^2 f_p = \#\overline{E}(\mathbb{F}_p) = p + 1$. Hence, $p \equiv -1 \bmod m$. By [20, Corollary III.8.1.1],

$p \equiv 1 \bmod m$, which is a contradiction to $p \equiv -1 \bmod m$ unless $m = 2$. Our (future) choice of y says $\pi_m^{\mathrm{s}}(x) = 0$ for $m > y$. Therefore, we have

$$\sum_{y < m \le \sqrt{x}+1} g(m)\pi_m^{\mathrm{s}}(x) = 0.$$

For ordinary primes, we have the following reasoning of [8, Page 617]: a prime p splits completely in $\mathbb{Q}(E[m])$ if and only if $(\theta_p - 1)/m$ is an algebraic integer where θ_p is a complex root of the polynomial $X^2 - a_p X + p$. Let K be the imaginary quadratic field with which E has CM by $\mathcal{O}_K$. Let $D > 0$ be a squarefree integer such that $K = \mathbb{Q}(\sqrt{-D})$.

We need the following result of [6, Lemma 2.3]:

Lemma 5.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by an order of the ring of algebraic integers of an imaginary quadratic field K. We have $\mathbb{Q}(\theta_p) = K$ for every ordinary prime p of good reduction for E.*

Hence,

$$\pi_m^{\mathrm{o}}(x) \le \#\left\{ p \le x : \frac{\theta_p - 1}{m} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-D})} \right\}.$$

Since θ_p is a complex root of $X^2 - a_p X + p \in \mathbb{Z}[X]$, its norm is p. Therefore,

$$\#\left\{ p \le x : \frac{\theta_p - 1}{m} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-D})} \right\} \le S_m$$

where

$$S_m := \#\{p \le x : p = (\alpha m + 1)^2 + \beta^2 m^2 D \text{ for some } \alpha, \beta \in \mathbb{Z}\}$$

if $-D \equiv 2, 3 \bmod 4$, and

$$S_m := \#\left\{ p \le x : p = \frac{(\alpha m + 2)^2 + \beta^2 m^2 D}{4} \text{ for some } \alpha, \beta \in \mathbb{Z} \right\}$$

if $-D \equiv 1 \bmod 4$. This implies $\alpha \ll 1 + 2\sqrt{x}/m$ and $\beta \le \sqrt{x}/m\sqrt{D}$. Hence,

$$S_m \ll \frac{\sqrt{x}}{m\sqrt{D}} \left(1 + \frac{2\sqrt{x}}{m}\right) \ll_D \frac{x}{m^2} + \frac{\sqrt{x}}{m}. \tag{5.3}$$

By the above equation and $H(g; \alpha, \beta)$, we have

$$\begin{aligned} \sum_{y < m \le \sqrt{x}+1} g(m)\pi_m^{\mathrm{o}}(x) &\ll x \sum_{y < m\sqrt{x}+1} \frac{|g(m)|}{m^2} + \sqrt{x} \sum_{y < m \le \sqrt{x}+1} \frac{|g(m)|}{m} \\ &\ll \frac{x(\log y)^\beta}{y^{1-\alpha}} + x^{\frac{1+\alpha}{2}} (\log x)^\beta. \end{aligned}$$

Collecting all terms, we obtain

$$\sum_{p\leq x} f(i_p) = c_E \mathrm{li}(x) + O\left(\frac{x(\log y)^{\beta}(\log\log y)^2}{y^{1-\alpha}\log x}\right) + O(y^{1+\alpha}\sqrt{x}(\log x)(\log y)^{\beta}) + O\left(\frac{x(\log x)^{\beta}}{y^{1-\alpha}}\right) + O\left(x^{\frac{1+\alpha}{2}}(\log x)^{\beta}\right)$$

for any $y \to \infty$ as $x \to \infty$. Let $y = x^{1/4}/(\log x)^{1/2}$. Thus, we have

$$\sum_{p\leq x} f(i_p) = c_E \mathrm{li}(x) + O\left(x^{\frac{3+\alpha}{4}}(\log x)^{\frac{2\beta-\alpha-1}{2}}\right)$$

as claimed.

5.2 Non-CM case

We need to obtain a bound for $\pi_m(x) := \#\{p \leq x : p \nmid N, m|i_p\}$. By Lemma 2.1 and [20, Corollary III.8.1.1], we have $m|i_p$ implies $p \equiv 1 \bmod m$. We also have $m|i_p$ implies $m^2|i_p^2 f_p = \#\overline{E}(\mathbb{F}_p) = p + 1 - a_p$, which implies $p \equiv a_p - 1 \bmod m^2$. Hence, $a_p \equiv p + 1 \equiv 2 \bmod m$.

For $\pi(x; m^2, a)$, we have the trivial bound

$$\pi(x; m^2, a) \ll \frac{x}{m^2} + 1.$$

We also have $x/m^2 \geq x/(x + 2\sqrt{x} + 1) \gg 1$ since $m \leq \sqrt{x} + 1$. Hence, $\pi(x; m^2, a) \ll x/m^2$. Thus, we have

$$\pi_m(x) \ll \sum_{\substack{|a|\leq 2\sqrt{x} \\ a\equiv 2 \bmod m}} \pi(x; m^2, a) \ll \sum_{\substack{|a|\leq 2\sqrt{x} \\ a\equiv 2 \bmod m}} \frac{x}{m^2} \ll \frac{x^{3/2}}{m^3}.$$

By $H(g; \alpha, \beta)$,

$$\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m(x) \ll x^{3/2} \sum_{y<m\leq\sqrt{x}+1} \frac{|g(m)|}{m^3} \ll \frac{x^{3/2}(\log y)^{\beta}}{y^{2-\alpha}}.$$

Collecting the error terms gives us

$$\sum_{p\leq x} f(i_p) = c_E \mathrm{li}(x) + O\left(\frac{x}{y^{1-\alpha-\varepsilon}\log x}\right) + O(y^{1+\alpha}\sqrt{x}(\log x)(\log y)^{\beta}) + O\left(\frac{x^{3/2}(\log y)^{\beta}}{y^{2-\alpha}}\right)$$

where

$$c_E := \sum_{m\geq 1} \frac{g(m)}{|G_m|}$$

is a constant by Lemma 3.2 (a).

Choosing $y = x^{1/3}/(\log x)^{1/3}$ gives us

$$\sum_{p\leq x} f(i_p) = c_E \mathrm{li}(x) + O\left(x^{\frac{5+2\alpha}{6}} (\log x)^{\frac{3\beta+2-\alpha}{3}}\right).$$

This completes the proof of Parts (b) and (c) of Theorem 1.1.

6. The case $\alpha = 2$

6.1 The proof of Theorem 1.1 (d)

We have

$$\begin{aligned}\sum_{p\leq x} f(i_p) &= \sum_{m\leq \sqrt{x}+1} g(m)\pi_m(x) \\ &= \sum_{m\leq y} g(m)\pi_m(x) + \sum_{y<m\leq \sqrt{x}+1} g(m)\pi_m(x).\end{aligned}$$

By Theorem 3.1,

$$\begin{aligned}\sum_{m\leq y} g(m)\pi_m(x) &= \sum_{m\leq y} g(m)\left(\frac{\mathrm{li}(x)}{|G_m|} + O(\sqrt{x}\log(mx))\right) \\ &= \mathrm{li}(x)\sum_{m\leq y}\frac{g(m)}{|G_m|} + O\left(\sqrt{x}\log x \sum_{m\leq y}|g(m)|\right) \\ &= \mathrm{li}(x)\sum_{m\leq y}\frac{g(m)}{|G_m|} + O\left(\frac{y^2\sqrt{x}(\log x)}{(\log y)^{\beta}}\right)\end{aligned}$$

By partial summation and the classical bound $m/\varphi(m) \ll \log\log m$, we also have

$$\sum_{m>y}\frac{|g(m)|}{|G_m|} \ll \frac{(\log\log y)^2}{(\log y)^{\beta-1}}.$$

Hence,

$$\sum_{m\leq y} g(m)\pi_m(x) = C_E\mathrm{li}(x) + O\left(\frac{x(\log\log y)^2}{(\log x)(\log y)^{\beta-1}}\right) + O\left(\frac{y^2\sqrt{x}(\log x)}{(\log y)^{\beta}}\right).$$

Using the notation of §5 and $H(g; 1, -\beta)$, we have

$$\begin{aligned}\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m(x) &\ll \sum_{y<m\leq\sqrt{x}+1} |g(m)|\pi_m^{\mathrm{o}}(x)\\ &\ll \sum_{y<m\leq\sqrt{x}+1} |g(m)|\left(\frac{x}{m^2}+\frac{\sqrt{x}}{m}\right)\\ &\ll \frac{x}{(\log x)^{\beta}}\end{aligned}$$

Choosing $y = x^{1/4}$ gives the result.

Remarks. We note that this technique works for $\beta = 2$ assuming we divide by a sufficiently large power of $\log\log x$. This method can be extended indefinitely in this manner.

By [2, Lemma 3.2], we may extend all the results which relied upon GRH to Abelian varieties which contain a one-dimensional Abelian subvariety that is also defined over $\mathbb{Q}$.

We also note that given the sharpness of the error terms in Theorem 1.1 we only need to assume that there are no zeros in the region $\Re(s) > \theta$ where θ is determined by E having CM or not. For non-CM curves, if we assume the Pair Correlation Conjecture and Artin's Holomorphy Conjecture for L-functions associated to the irreducible characters of the Galois groups of $\mathbb{Q}(E[m])$ as m ranges over all $m \in \mathbb{N}$, then the error terms in our result would be improved. See [8] for more details.

6.2 Proof of Theorem 1.3

Let $G'_m = \mathrm{Gal}(K(E[m])/K)$ where K is the CM field. Then,

$$\begin{aligned}|G'_m| = [K(E[m]) : K] &= \frac{[K(E[m]) : \mathbb{Q}]}{[K : \mathbb{Q}]} = \frac{[\mathbb{Q}(E[m]) : \mathbb{Q}]}{[K : \mathbb{Q}]}\\ &= \frac{1}{2}[\mathbb{Q}(E[m]) : \mathbb{Q}] \ll m^2\end{aligned}$$

for $m \geq 3$ by Lemma 3.2 (b) and [16, Lemma 6], which states that $K(E[m]) = \mathbb{Q}(E[m])$ when $m \geq 3$. For $y \leq \sqrt{x}+1$, we have

$$\begin{aligned}\sum_{p\leq x} i_p = \sum_{m\leq\sqrt{x}+1} \varphi(m)\pi_m(x) &\geq \sum_{3\leq m\leq y} \varphi(m)\pi_m(x)\\ &\gg \sum_{3\leq m\leq y} \varphi(m)\left(\widetilde{\pi}_m(x) + O\left(\frac{\sqrt{x}}{\log x}\right)\right)\\ &\gg \sum_{3\leq m\leq y} \varphi(m)\widetilde{\pi}_m(x) + O\left(\frac{y^2\sqrt{x}}{\log x}\right)\end{aligned}$$

$$= \sum_{3\le m\le y} \varphi(m)\left(\widetilde{\pi}_m(x) - \frac{\mathrm{li}(x)}{|G'_m|} + \frac{\mathrm{li}(x)}{|G'_m|}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right)$$

$$= \mathrm{li}(x)\sum_{3\le m\le y}\frac{\varphi(m)}{|G'_m|} + O\left(\left|\sum_{3\le m\le y}\varphi(m)\left(\widetilde{\pi}_m(x) - \frac{\mathrm{li}(x)}{|G'_m|}\right)\right|\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right)$$

$$= \mathrm{li}(x)\sum_{3\le m\le y}\frac{\varphi(m)}{|G'_m|} + O\left(y\sum_{3\le m\le y}\left|\widetilde{\pi}_m(x) - \frac{\mathrm{li}(x)}{|G'_m|}\right|\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right)$$

$$= \mathrm{li}(x)\sum_{3\le m\le y}\frac{\varphi(m)}{|G'_m|} + O_A\left(\frac{yx}{(\log x)^A}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right).$$

We note that all of the above constants are absolute except for $O_A(yx/(\log x)^A)$. Choose $A > 3$ and $y = (\log x)^{A-2}$. For sufficiently large x, which is dependent on A, we then obtain

$$\sum_{p\le x} i_p = \mathrm{li}(x)\sum_{3\le m\le y}\frac{\varphi(m)}{|G'_m|} + O_A\left(\frac{x}{(\log x)^2}\right) + O\left(\sqrt{x}(\log x)^{2A-5}\right)$$

$$\gg \frac{x}{\log x}\sum_{3\le m\le y}\frac{\varphi(m)}{m^2} + O_A\left(\frac{x}{(\log x)^2}\right)$$

$$\gg \frac{x\log y}{\log x} + O_A\left(\frac{x}{(\log x)^2}\right)$$

$$\gg (A-2)\frac{x\log\log x}{\log x} + O_A\left(\frac{x}{(\log x)^2}\right)$$

$$\gg (A-2)\frac{x\log\log x}{\log x},$$

as required.

7. Applications

We break this section up into three subsections: one for arithmetic functions, which will tell us about some statistics of invariants of the sequence i_p as p ranges over primes $\le x$, a second on differentiable functions on $\mathbb{R}_{>0}$, and a third for other invariants of the elliptic curve. Throughout this section, c, with or without subscripts, will denote a constant.

7.1 Arithmetic functions

Let us first consider the function $\chi_{\{1\}}(n)$ and $\tau(n)$ that have been previously studied. We note that

$$\chi_{\{1\}}(n) = \sum_{d|n} \mu(d),$$

and

$$\tau(n) = \sum_{d|n} 1.$$

We have

$$\sum_{n \le x} |\mu(n)| \le \sum_{n \le x} 1 = [x] \ll x.$$

Hence $H(\mu; 0, 0)$, $H'(\mu; 0, 0)$, $H(1; 0, 0)$, and $H'(1; 0, 0)$ are satisfied. Thus, we obtain

$$N_E(x) := \#\{p \le x : \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} = c_{\chi_{\{1\}},E}\mathrm{li}(x) + O_{A,E}\left(\frac{x}{(\log x)^A}\right)$$

if E has CM,

$$N_E(x) = c_{\chi_{\{1\}},E}\mathrm{li}(x) + O_E\left(\frac{x^{3/4}}{(\log x)^{1/2}}\right)$$

if E has CM and GRH holds for E, and

$$N_E(x) = c_{\chi_{\{1\}},E}\mathrm{li}(x) + O_E(x^{5/6}(\log x)^{2/3})$$

if E does not have CM and GRH holds for E.

Similarly, we have

$$\sum_{p \le x} \tau(i_p) = c_{\tau,E}\mathrm{li}(x) + O_{A,E}\left(\frac{x}{(\log x)^A}\right)$$

if E has CM,

$$\sum_{p \le x} \tau(i_p) = c_{\tau,E}\mathrm{li}(x) + O_E\left(\frac{x^{3/4}}{(\log x)^{1/2}}\right)$$

if E has CM and GRH holds for E, and

$$\sum_{p \le x} \tau(i_p) = c_{\tau,E}\mathrm{li}(x) + O_E(x^{5/6}(\log x)^{2/3})$$

if E does not have CM and GRH holds for E.

These results recover the work in [2,3,8]. For generalizations, we need the following lemma.

Lemma 7.1.

(a) *For any $k \in \mathbb{N}$, we have*

$$\sum_{m \le x} \frac{\tau(m)^k}{m} \ll (\log x)^{2^k}.$$

In addition,

$$\sum_{n \le x} \frac{\tau(n)^2}{n} \ll (\log x)^3.$$

(b) *Let $k \in \mathbb{N}$. Then*

$$\sum_{n \le x} \tau_k(n) = x P_{k-1}(\log x) + O\left(x^{\frac{k-1}{k}} (\log x)^{k-2}\right),$$

where P_{k-1} is a polynomial of degree $k-1$.

(c) *Let k be a positive integer, and let r be a non-negative integer. Then $\tau_k(n)^r \ll_{r,k} \tau(n)^{2(k-1)r}$.*

Proof. The first statement of Part (a) is [9, Lemma 10.2.7] and the second statement is established from [23, Théorème II.7.15] and the fact

$$\sum_{n=1}^{\infty} \frac{\tau(n)^2}{n^s} = \frac{\zeta(s)^4}{\zeta(2s)}.$$

Part (b) is given at [24, p. 313]. Part (c) follows from [11, Proposition 22.10] with $t = 2$. □

We consider the functions $\omega(n)^r$, $\Omega(n)^r$, $2^{\omega(n)r}$, and $\tau_k(n)^r$. We first assume $r = 1$. Let $f : \mathbb{N} \to \mathbb{C}$ be one of these functions. Then, by the Möbius inversion formula [9, Theorem 1.2.2], we have that there exists $g : \mathbb{N} \to \mathbb{C}$ such that

$$f(n) = \sum_{m|n} g(m)$$

for all $n \in \mathbb{N}$. In fact,

$$\omega(n) = \sum_{p|n} 1$$

$$\Omega(n) = \sum_{p^\alpha | n} 1$$

$$2^{\omega(n)} = \sum_{\substack{m|n \\ m \text{ is squarefree}}} 1$$

$$\tau_k(n) = \sum_{d|n} \tau_{k-1}(d)$$

Hence, $\omega(n)$, $\Omega(n)$, and $2^{\omega(n)}$ satisfy $H(g;0,0)$ and $H'(g;0,0)$, and $\tau_k(n)$ satisfies $H(g;0,k-1)$ and $H'(g;0,2^{4k-8})$ by Lemma 7.1 (a) and (b). Thus, for $f(n)=\omega(n)$, $\Omega(n)$, or $2^{\omega(n)}$, we have

$$\sum_{p\leq x} f(i_p) = c_{E,f}\mathrm{li}(x) + O_E\left(\frac{x}{(\log x)^A}\right)$$

if E has CM,

$$\sum_{p\leq x} f(i_p) = c_{E,f}\mathrm{li}(x) + O_E\left(\frac{x^{3/4}}{(\log x)^{1/2}}\right)$$

if GRH holds and E has CM, and

$$\sum_{p\leq x} f(i_p) = c_{E,f}\mathrm{li}(x) + O_E(x^{5/6}(\log x)^{2/3})$$

if GRH holds and E does not have CM. For $f(n)=\tau_k(n)$, the error term in the first equation does not change, the error term in the second equation becomes $x^{3/4}(\log x)^{k+\frac{1}{2}}$, and the error term in the third equation becomes $x^{5/6}(\log x)^{2k/3}$. Similar asymptotic equations hold for $r>1$. The error term in the first equation remains unchanged. The error term in the second equation changes to $x^{3/4}(\log x)^{2^{(k-1)(r+1)}}$ by Lemma 7.1 (a) and (c), and the error term in the third equation changes to $x^{5/6}(\log x)^{2^{(k-1)(r+1)}}$. We note that all of the above constants of the form $c_{E,f}$ for some function f are positive.

We also note that Theorem 1.1 (a), (b), (c) can be applied to any characteristic function χ_S where S is a subset of $\mathbb{N}$.

Let $\alpha\in\mathbb{R}$ with $\alpha>0$ (the case $\alpha=0$ is $\sigma_\alpha(n)=\tau(n)$). Recall

$$\sigma_\alpha(n) := \sum_{m|n} m^\alpha,$$

and let

$$g_\alpha(n) := \sum_{m|n} \mu\left(\frac{n}{m}\right)\sigma_\alpha(m).$$

By the Möbius Inversion Formula [9, Theorem 1.2.2], we have

$$\sigma_\alpha(n) = \sum_{m|n} g_\alpha(m).$$

We also have

$$|g_\alpha(n)| \leq \sum_{m|n}\sigma_\alpha(m) \leq \tau(n)\sigma_\alpha(n) \leq \tau(n)^2 n^\alpha.$$

Thus, by Lemma 7.1 (a), $\sigma_\alpha(n)$ satisfies $H(g_\alpha, \alpha, 3)$. Therefore, we have

$$\sum_{p \le x} \sigma_\alpha(i_p) = c_E \mathrm{li}(x) + O\left(x^{\frac{3+\alpha}{4}} (\log x)^{\frac{5-\alpha}{2}}\right)$$

if E has CM, $\alpha < 1$, and GRH holds, and

$$\sum_{p \le x} \sigma_\alpha(i_p) = c_E \mathrm{li}(x) + O\left(x^{\frac{5+2\alpha}{6}} (\log x)^{\frac{4}{3}(2-\alpha)}\right)$$

if E does not have CM, $\alpha < 1/2$, and GRH holds.

7.2 Analytic functions

Let $f(n) = (\log n)^\beta$ for some fixed positive real number β. Then, we have

$$g(m) = \sum_{m|n} \mu(m) \left(\log \frac{n}{m}\right)^\beta \ll \tau(n)(\log n)^\beta$$

where $g : \mathbb{N} \to \mathbb{C}$ with $f(n) = \sum_{m|n} g(m)$. Thus, $f(n)$ satisfies $H(g; 0, \beta + 1)$ and $H'(g; 0, 2\beta + 1)$. Hence, we have

$$\sum_{p \le x} (\log i_p)^\beta = c_{E,\beta} \mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right)$$

if E has CM,

$$\sum_{p \le x} (\log i_p)^\beta = c_{E,\beta} \mathrm{li}(x) + O\left(x^{3/4} (\log x)^{\beta + \frac{1}{2}}\right)$$

if GRH holds and E has CM, and

$$\sum_{p \le x} (\log i_p)^\beta = c_{E,\beta} \mathrm{li}(x) + O\left(x^{5/6} (\log x)^{\frac{4+2\beta}{3}}\right)$$

if GRH holds and E does not have CM.

Let $f(n) = n^\alpha$ for some fixed real positive α. By the Möbius inversion formula [9, Theorem 1.2.2], we have there exists $g : \mathbb{N} \to \mathbb{C}$ such that

$$n^\alpha = \sum_{m|n} g(m),$$

and hence, $g(n) \le \tau(n) n^\alpha$. Thus, $f(n) = n^\alpha$ satisfies $H(g; \alpha, 1)$. Hence,

$$\sum_{p \le x} i_p^\alpha = c'_{E,\alpha} \mathrm{li}(x) + O\left(x^{\frac{3+\alpha}{4}} (\log x)^{\frac{1-\alpha}{2}}\right)$$

if $\alpha < 1$, GRH holds, and E has CM, and

$$\sum_{p \leq x} i_p^{\alpha} = c'_{E,\alpha} \mathrm{li}(x) + O\left(x^{\frac{5+2\alpha}{6}} (\log x)^{\frac{4-2\alpha}{3}}\right)$$

if $\alpha < 1/2$, GRH holds, and E does not have CM. In the CM case, this nearly resolves a problem posed by Kowalski [15, Problem 3.1] of determining the asymptotic behaviour of

$$\sum_{p \leq x} i_p.$$

Let $f : \mathbb{N} \to \mathbb{C}$ be such that $f(n) \ll n/(\log n)^{\beta}$ where $\beta > 3$. Writing $f(n) = \sum_{d|n} g(d)$ and using the Möbius inversion formula [9, Theorem 1.2.2], we see that $g(n) \ll \tau(n) n/(\log n)^{\beta}$. Hence, $H(g; 2, -\beta + 1)$ holds and $\beta - 1 > 2$. By Theorem 1.1 (d), we have

$$\sum_{p \leq x} f(i_p) = c_{E,f} \mathrm{li}(x) + O\left(\frac{x}{(\log x)^{\beta-1}}\right).$$

Let us consider the function $f(n) = n$ and a CM curve E. We note GRH for E on $\mathbb{N}$ implies

$$\sum_{p \leq x} i_p \gg x.$$

This result is [15, Proposition 3.8].

7.3 Applications to invariants of $\overline{E}(\mathbb{F}_p)$

Note that, for a given prime p, $\overline{E}(\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/i_p\mathbb{Z} \times \mathbb{Z}/i_p f_p \mathbb{Z}$. We will consider the following two invariants of $\#\overline{E}(\mathbb{F}_p)$: the index f_p of the maximal subgroup of the group $\overline{E}(\mathbb{F}_p)$ which has the form $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ and the exponent $e_p := i_p f_p$ of $\overline{E}(\mathbb{F}_p)$. In [10], the following is result is established

$$\sum_{p \leq x} e_p = c_E \mathrm{li}(x^2) + O_E(x^{19/10} (\log x)^{11/5})$$

if GRH holds for E, and

$$\sum_{p \leq x} e_p = c_E \mathrm{li}(x^2) + O\left(\frac{x^2 \log\log x}{(\log x)^{1/8}}\right).$$

(See also [14,26].) Following the same technique (Equations (4.1)–(4.3) of [10]), we have

$$\sum_{p \leq x} e_p = \sum_{p \leq x} \frac{p + 1 - a_p}{i_p} = \sum_{p \leq x} \frac{p}{i_p} + \sum_{p \leq x} \frac{1 - a_p}{i_p}.$$

By Hasse's inequality (1.1), the second summation becomes

$$\sum_{p\le x}\frac{1-a_p}{i_p}\ll\sum_{p\le x}\sqrt{p}\ll\frac{x^{3/2}}{\log x}.$$

We note that $f(n)=1/n=\sum_{d|n}g(d)$ satisfies $H(g;0,1)$ and $H'(g;0,3)$. By Theorem 1.1 (a), (b), and (c), we have

$$\sum_{p\le x}\frac{1}{i_p}=c_E\mathrm{li}(x)+O(E(x))$$

where

$$E(x)=\begin{cases}O_E(x^{3/4}(\log x)^2) & \text{if } E \text{ has CM and GRH holds for } E\\ O_E(x^{5/6}(\log x)^2) & \text{if } E \text{ does not have CM and GRH holds for } E\\ O_{A,E}\left(\frac{x}{(\log x)^A}\right) & \text{if } E \text{ has CM}\end{cases}.$$

for any $A>0$. By partial summation, we have

$$\sum_{p\le x}e_p=c_E\mathrm{li}(x^2)+O(xE(x)),$$

where $E(x)$ is as above.

Noting that $f_k(n)=1/n^k=\sum_{d|n}g_k(n)$ satisfies $H(g_k;0,1)$ and $H'(g_k;0,3)$, and using induction and partial summation give us the first part of Theorem 1.2. Note that $c_E=c_{E,1}$. Also note that our error term is of the form

$$xE(x)=\begin{cases}O_E(x^{7/4}(\log x)^2) & \text{if } E \text{ has CM and GRH holds for } E\\ O_E(x^{11/6}(\log x)^2) & \text{if } E \text{ does not have CM and}\\ & \quad\text{GRH holds for } E\\ O_{A,E}\left(\frac{x^2}{(\log x)^A}\right) & \text{if } E \text{ has CM}\end{cases}.$$

Since

$$\sum_{p\le x}f_p^k=\sum_{p\le x}\frac{(p+1-a_p)^k}{i_p^{2k}},$$

we similarly have the second part of Theorem 1.2.

Acknowledgements

We thank Amir Akbary for his helpful comments on some results in this paper. We would also like to thank the reviewer for a careful reading of a previous draft of this paper.

References

[1] A. Akbary, On the greatest prime divisor of N_p, *J. Ramanujan Math. Soc.*, **23(3)** (2008) 259–282.

[2] A. Akbary and D. Ghioca, A geometric variant of Titchmarsh divisor problem, *Int. J. Number Theory*, **8(1)** (2012) 53–69.

[3] A. Akbary and V. K. Murty, An analogue of the Siegel-Walfisz theorem for the cyclicity of CM elliptic curves mod p, *Indian J. Pure Appl. Math.*, **41(1)** (2010) 25–37.

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

[5] A. C. Cojocaru, On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves, *J. Number Theory*, **96(2)** (2002) 335–350.

[6] A. C. Cojocaru, Cyclicity of CM elliptic curves modulo p, *Trans. Amer. Math. Soc.*, **355(7)** (2003) 265–2662.

[7] A. C. Cojocaru, Questions about the reductions modulo primes of an elliptic curve, In *Number theory, CRM Proc. Lecture Notes*, Providence, Rhode Island, *Amer. Math. Soc.*, **36** (2004) 61–79.

[8] 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.

[9] A. C. Cojocaru and M. R. Murty, An Introduction to Sieve Methods and their Applications, Cambridge University Press, New York (2006).

[10] T. Freiberg and P. Kurlberg, On the Average Exponent of Elliptic Curves Modulo p, to appear in *Int. Math. Res. Notices*, 22pp. (2013), doi: 10.1093/imrn/rns280.

[11] J. B. Friedlander and H. Iwaniec, Opera de Cribro, *American Mathematical Society Colloquium Publications, 57. American Mathematical Society*, Providence, Rhode Island (2010).

[12] R. Gupta and M. R. Murty, Cyclicity and generation of points mod$p$ on elliptic curves, *Invent. Math.*, **101(1)** (1990) 225–235.

[13] M. N. Huxley, The large sieve inequality for algebraic number fields III, Zero density results, *J. London Math. Soc. (2)*, **3** (1971) 233–240.

[14] S. Kim, The average exponent of cm elliptic curves modulo p, *arXiv 1207.6652* (2012) 1–8.

[15] E. Kowalski, Analytic problems for elliptic curves, *J. Ramanujan Math. Soc.*, **21(1)** (2006) 19–114.

[16] M. R. Murty, On Artin's conjecture, *J. Number Theory*, **16(2)** (1983) 147–168.

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

[18] J.-P. Serre, Résumé des cours de 1977–1978, *Ann. Collège France, Collège de France* (1978) 67–70.

[19] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math I. H. E. S.*, **54** (1981) 323–401.

[20] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York (1986).

[21] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, New York (1994).

[22] J. H. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer-Verlag, New York (1992).

[23] G. Tenenbaum, Introduction à la théorie analytique et probabiliste des nombres, *Société Mathématique de* France, Paris (1990).

[24] E. C. Titchmarsh, The theory of the Riemann zeta function, Oxford Science Publications, second edition edition, 1986, (revised by D. R. Heath-Brown).

[25] L. C. Washington, Elliptic Curves: Number Theory and Cryptology, Chapman & Hall/CRC, Boca Raton, Florida (2003).

[26] J. Wu, The average exponent of elliptic curves modulo p, *arXiv 1206.5929* (2012) 1–7.