ON THE ASYMPTOTIC NATURE OF ELLIPTIC CURVES MODULO p

ADAM TYLER FELIX AND M. RAM MURTY

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$. In 1976, Serre proved, on GRH, that for a positive proportion of primes $p \leq x$, the elliptic curve modulo p is cyclic. This was later to be shown to be true unconditionally for E with complex multiplication by M. Ram Murty. Let $\overline{E}(\mathbb{F}_p)$ denote the elliptic curve modulo p. Then, there exist integers $i(p), f(p)$ such that $\overline{E}(\mathbb{F}_p) \cong \mathbb{Z}/i(p)\mathbb{Z} \times \mathbb{Z}/i(p)f(p)\mathbb{Z}$. Hence, $\overline{E}(\mathbb{F}_p)$ is cyclic if and only if $i(p) = 1$. We study questions related to $i(p)$. In particular, for any $\alpha > 0$, we prove there exists a constant $c_\alpha > 0$ such that for any $A > 0$ we have

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

unconditionally for E a CM curve. For E a CM curve with $0 < \alpha < 1$, assuming GRH we prove that there exists a constant $c'_\alpha > 0$ such that

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

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

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

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 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, a field. Hasse's Theorem [20, Theorem V.1.1] says

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

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

We also have $\overline{E}(\mathbb{F}_p) \cong \mathbb{Z}/i(p)\mathbb{Z} \times \mathbb{Z}/i(p)f(p)\mathbb{Z}$ where $i(p)$ and $f(p)$ are integers. To see this let $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$. Since $\overline{E}(\mathbb{F}_p)$ is the set of solutions to a non-singular cubic curve with components in $\mathbb{F}_p$, it is a finite group. 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 $P \mapsto kP$. Then, since $\overline{E}(\mathbb{F}_p)$ is finite, we have $\overline{E}(\mathbb{F}_p) \subset \overline{E}(\overline{\mathbb{F}_p})[k]$ for some k with $\overline{E}(\mathbb{F}_p)|k$. 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

Key words and phrases. Cyclicity, Elliptic curves, primes.

Research of the first author supported by an NSERC PGS-D.

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

the Fundamental theorem of finitely generated Abelian groups. As such, we have $\#\overline{E}(\mathbb{F}_p) = i(p)^2 f(p)$. Our 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] showed, computationally, that we expect this 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

$$N_E(x) := \#\{p \leq x : p \nmid N, \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \sim c_E \text{li}(x) \tag{1.1}$$

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 $\text{li}(x) := \int_2^x \frac{dt}{\log t}$. Murty [16] removed the dependence of GRH in (1.1) assuming E has complex multiplication (CM) and the error term in (1.1) can be made explicit:

$$N_E(x) = c_E \text{li}(x) + O_N\left(\frac{x \log\log x}{(\log x)^2}\right). \tag{1.2}$$

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 [10] 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 Equation (1.1) 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 $\Re(s) > 3/4$. In [6], she also simplified the unconditional proof of when E has CM, and in [7], she and M. Ram Murty proved that if the GRH is assumed, then the relation becomes

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

if E is non-CM and

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

if E is 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.**

We can reformulate Serre's result in the following way:

$$\begin{aligned} N_E(x) &= \#\{p \leq x : p \nmid N, \overline{E}(\mathbb{F}_p) \text{ is cyclic}\} \\ &= \#\{p \leq x : p \nmid N, i(p) = 1\} \\ &= \sum_{\substack{p \leq x \\ p \nmid N}} \chi_{\{1\}}(i(p)) \end{aligned}$$

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

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

holds where $c_{E,f}$ is a constant dependent on E and f? Kowalski [13, Proposition 3.8] has shown the following unconditional result:

$$\sum_{p \le x} i(p) \gg \begin{cases} \dfrac{x \log\log x}{\log x} & \text{if } E \text{ is a CM curve} \\ \dfrac{x}{\log x} & \text{otherwise} \end{cases}.$$

In fact, this result is true for any elliptic curve E defined over some field K. The above implied constant is now dependent on K. Akbary and Ghioca [2] have shown

$$\sum_{p \le x} \tau(i(p)) = c_E \mathrm{li}(x) + O(x^{5/6}(\log x)^{2/3}) \tag{1.3}$$

if GRH holds, and unconditionally

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

for any $A > 1$ if E is a CM curve with endomorphism ring isomorphic to the ring of algebraic integers of some imaginary quadratic field. In fact, (1.3) can be generalized to Abelian varieties defined over $\mathbb{Q}$ which have a dimension one subvariety also defined over $\mathbb{Q}$.

1.2. **Definitions and Notation.** Throughout p and q will denote prime number unless otherwise stated. Also, d, k, m, n, and w will denote positive integers, and x, y, and z will denote positive real numbers.

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

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

We similarly define $E(K)[k]$ for any field K with $\mathbb{Q} \subset K$. Also, by $\mathbb{Q}(E[k])$ we will denote as the smallest field containing $\mathbb{Q}$ and the set $\{x, y : (x, y) \in E[k]\}$. We will say that E has complex multiplication (CM) if the endomorphism ring of E is larger than $\mathbb{Z}$. See [20, §III.4] for more information about the endomorphism ring. See [20, Appendix C], [21, Chapter II], or [22, Chapter 10], for more information about CM.

The condition that GRH holds for E is the following statement: GRH holds for all Dedekind zeta functions of the fields $K_m := \mathbb{Q}(E[m])$ as m ranges over $\mathbb{N}$. We should note that in some cases n will not range over all $\mathbb{N}$.

Let $\tau(n), \omega(n)$, and $\Omega(n)$ denote the number of positive divisors, prime divisors counted without multiplicity, prime divisors counted with multiplicity of n, respectively. Let

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

By the notation $f(x) = O(g(x))$ 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 $f(x) = O_E(g(x))$ or $f(x) \ll_a g(x)$ 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.

1.3. **Statement of Results.** In §3, we will prove the following result:

Theorem 1.1. *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 $n \in \mathbb{N}$. Let $\alpha \in \mathbb{R}$ with $\alpha \geq 0$, and let $k, r \in \mathbb{Z}$ with $k \geq 1$ and $r \geq 0$ such that $|g(n)| \ll \tau_k(n)^r (\log n)^\alpha$ for all $n \in \mathbb{N}$ where the implied constant may depend on r, k and α. Let E be an elliptic curve with CM. Then, there exists a positive constant $c_{E,f}$ such that

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

In §4, we will prove the following result:

Theorem 1.2. *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 $n \in \mathbb{N}$. Let $\alpha, \beta \in \mathbb{R}$ be fixed with $\beta \geq 0$, and let $k, r \in \mathbb{Z}$ with $k \geq 1$ and $r \geq 0$ such that $|g(n)| \ll \tau_k(n)^r n^\alpha (\log n)^\beta$ for all $n \in \mathbb{N}$. Then, there exists a positive constant $c_{E,f}$ such that

(a) *if $\alpha < 1$, GRH holds for E, and E is a CM curve, then*

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

(b) *if $\alpha < 1/2$, GRH holds for E, and E is a non-CM curve, then*

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

In §5, we will give some applications of these results.

2. Preliminary Lemmata

2.1. **Upper bound for $i(p)$.** From Hasse's Theorem, we have $\#\overline{E}(\mathbb{F}_p) = p + 1 - a_p$ where $|a_p| \leq 2\sqrt{p}$. We also have $i(p)^2 \leq i(p)^2 f(p) = \#\overline{E}(\mathbb{F}_p) \leq p+1+|a_p| \leq p+1+2\sqrt{p} = (1+\sqrt{p})^2$. Hence,

$$i(p) \leq \sqrt{p} + 1. \tag{2.1}$$

2.2. **Conjugacy condition and Chebotarev density theorem.** We also have the following condition:

$$d|i(p) \iff p \text{ splits completely in } \mathbb{Q}(E[d]). \tag{2.2}$$

For a proof of this see [16, Lemma 2 in §5], [7, Lemma 2.1], or [2, Lemma 3.2]. Condition (2.2) is important because it allows us to use the Chebotarev density theorem:

Theorem 2.1. *Let K be a finite Galois extension over $\mathbb{Q}$ with Galois group $\mathrm{Gal}(K/\mathbb{Q}) = G$. Let $C \subset G$ be closed under conjugation, and assume the GRH holds for the Dedekind zeta function for K. Define*

$$\pi(x; K/\mathbb{Q}, C) := \#\{p \leq x : p \text{ is unramified in } K \text{ such that } \sigma_p \subset C\}$$

where σ_p is the Frobenius conjugacy class corresponding to p in $\mathrm{Gal}(K/\mathbb{Q})$. Then,

$$\pi(x; K/\mathbb{Q}, C) = \frac{|C|}{|G|}\mathrm{li}(x) + O\left(|C|\sqrt{x}\log\left(|G|\left(\prod_{p\in\mathcal{P}(K/\mathbb{Q})} p\right)x\right)\right),$$

where $\mathcal{P}(K/\mathbb{Q})$ is the set of rational primes which ramify in K, and the implied constant in s absolute.

This is [14, Theorem 1] and [19, Théorème 4]. There are unconditional versions of the Chebotarev density theorem.

Let $\pi_m(x) := \#\{p \leq x : p \nmid N, m|i(p)\}$. Then, by condition (2.2) and classical algebraic number theory [12, Property III.2.5], we have $d|i(p)$ if and only if $\sigma_p = 1$. Therefore, in the Chebotarev density theorem, we can replace C with $\{1\}$. We note that p ramifies in $\mathbb{Q}(E[d])$ implies $p|N$ or $p|d$ by the criterion of Néron-Ogg-Shafarevich [20, Theorem VII.7.1]. So now we just need to estimate $|G|$. We have $|\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})| \leq m^4$ by the injectivity of the Galois representation $\phi_m : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Thus, by the Chebotarev density theorem, we have

$$\pi_m(x) = \frac{\mathrm{li}(x)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} + O(\sqrt{x}\log(mNx)) \tag{2.3}$$

where the implied constant is absolute.

2.3. **Complex Multiplication.** Let E be an elliptic curve with complex multiplication by 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. By [16, Lemma 6], $\mathbb{Q}(E[m]) = K(E[m])$ for $m \geq 3$.

Define the following equivalence relation on the set of ideals of $\mathcal{O}_K$. We say $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if there exist $\alpha, \beta \in \mathcal{O}_K$ such that $\langle \alpha \rangle \mathfrak{a} = \langle \beta \rangle \mathfrak{b}$. Here $\langle \gamma \rangle$ for $\gamma \in \mathcal{O}_K$, is the ideal of $\mathcal{O}_K$ generated by γ. If this is the case, we write $\mathfrak{a} \sim \mathfrak{b}$. This gives us h equivalence classes. We call h the class number of K or $\mathcal{O}_K$. 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 gives another equivalence relation with $h(\mathfrak{q})$ equivalence classes with $h(\mathfrak{q}) = h\varphi(\mathfrak{q})/T(\mathfrak{q})$ where φ is the number field analogue of the Euler totient function, and $T(\mathfrak{q})$ is the number of residue classes of elements of $\mathcal{O}_K$ modulo $\mathfrak{q}$ that contain a unit. If K is an imaginary quadratic field, then $T(\mathfrak{q}) \leq 6$. Let $N(\mathfrak{a})$ denote the norm of an ideal $\mathfrak{a} \in \mathcal{O}_K$.

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 $\mathfrak{f}$ of $\mathcal{O}_K$ whose prime ideal divisors of $\mathcal{O}_K$ are prime ideals of bad reduction of E over K. We need the following lemma:

Lemma 2.1. *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 $\mathfrak{fm}$ 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, $t(m)[K(E[m]) : K] = h(\mathfrak{fm})$ where

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

Here the implied constant is absolute and $\varphi(\mathfrak{f})$ is the number field analogue of Euler's totient function.

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

Finally, we need the following extension of the Bombieri-Vinogradov theorem due to Huxley [11, Theorem 1]:

Lemma 2.2. *For any $A > 0$, there exists $B = B(A)$ such that*

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

where the implied constant is dependent only on B and K.

We also define

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

Then, we have the following equality for $m \geq 3$:

$$\pi_m(x) = \frac{\widetilde{\pi}_{\mathfrak{m}}(x)}{2} + O\left(\frac{\sqrt{x}}{\log x}\right) + O(\log N). \tag{2.4}$$

This is due to Akbary and V. K. Murty [3, Eq. (3.2)]. In fact, we have

$$\pi_m(x) \leq \frac{1}{2}\widetilde{\pi}_{\mathfrak{m}}(x). \tag{2.5}$$

To see this we review the justification of (2.4). By (2.2), we have that $\pi_m(x)$ counts the number of primes which split completely in $\mathbb{Q}(E[m])$. Since, $m \geq 3$, we have $\mathbb{Q}(E[m]) = K(E[m])$. Thus, if p splits completely in $\mathbb{Q}(E[m])$, then p splits completely in $K(E[m])$ and hence in K, an imaginary quadratic field. Thus, $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. However, $\mathfrak{p}$ splits completely in $K(E[m])$ if and only if $\overline{\mathfrak{p}}$ splits completely in $K(E[m])$. Thus, every prime $p \in \mathbb{N}$ gives two prime ideals to $\widetilde{\pi}_{\mathfrak{m}}(x)$, and vice versa. The $O(\sqrt{x}/\log x)$ term comes from the number of prime ideals of $\mathcal{O}_K$ which are inert or ramified in $\mathbb{Q}$ with norm $\leq x$. This gives us (2.4).

For (2.5), we have that 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 $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$.

For $m = 1$ or $m = 2$, we have

$$\pi_1(x) = \#\{p \leq x : p \nmid N, 1|i(p)\} = \pi(x) - \omega(N) = \mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right) + O(\log N) \tag{2.6}$$

by the prime number theorem, and

$$\pi_2(x) = \#\{p \leq x : p \nmid N, 2|i(p)\} = \frac{\mathrm{li}(x)}{[\mathbb{Q}(E[2]) : \mathbb{Q}]} + O\left(\frac{x}{(\log x)^A}\right) \tag{2.7}$$

for any $A > 1$ and x sufficiently large by [3, Lemma 2.3].

3. Proof of Theorem 1.1

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 $n \in \mathbb{N}$. Suppose $|g(n)| \ll \tau_k(n)^r (\log n)^\alpha$ for all n where the implied constant may depend on k, r, and α. Then, by (2.1), we have

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

where $\pi_m(x) := \#\{p \leq x : m|i(p)\}$. Let y be chosen later such that $y \leq \sqrt{x} + 1$. We have

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

We have that E is an elliptic curve with complex multiplication by the ring of algebraic integers $\mathcal{O}_K$ of an imaginary quadratic field K. Then, we have

$$\begin{aligned}\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m(x) &\leq \frac{1}{2}\sum_{y<m\leq\sqrt{x}+1} g(m)\widetilde{\pi}_{\mathfrak{m}}(x) && \text{(by (2.5))}\\ &\ll \sum_{y<m\leq\sqrt{x}+1} \tau_k(m)^r(\log m)^\alpha\widetilde{\pi}_{\mathfrak{m}}(x) && \text{(by hypothesis)}\\ &\ll (\log x)^\alpha \sum_{y<m\leq\sqrt{x}+1} \tau_k(m)^r \sum_{i=1}^{t(m)} \pi_K(x;\mathfrak{fm},\mathfrak{m}_i)\end{aligned}$$

by Lemma 2.1. Also, by [15, Page 132, Theorem 3] and Lemma 2.1, we have

$$\begin{aligned}\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m(x) &\ll x(\log x)^\alpha \sum_{y<m\leq\sqrt{x}+1} \frac{t(m)\tau_k(m)^r}{N(\mathfrak{fm})}\\ &\ll x(\log x)^\alpha \frac{\varphi(\mathfrak{f})}{N(\mathfrak{f})}\prod_{\mathfrak{p}|\mathfrak{f}}\left(1-\frac{1}{N(\mathfrak{p})-1}\right)\sum_{y<m\leq\sqrt{x}+1}\frac{\tau_k(m)^r}{N(\mathfrak{m})}\\ &\ll_{\mathfrak{f}} x(\log x)^\alpha \sum_{y<m\leq\sqrt{x}+1}\frac{\tau_k(m)^r}{N(\mathfrak{m})}.\end{aligned}$$

Recall $\mathfrak{m} = m\mathcal{O}_K$. So $N(\mathfrak{m}) = m^2$. Thus,

$$\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m(x) \ll x(\log x)^\alpha \sum_{m>y}\frac{\tau_k(m)^r}{m^2}.$$

By [9, Proposition 22.10], for all $n\in\mathbb{N}$, there exists $d\leq\sqrt{n}$ with $d|n$ such that

$$\tau_k(n)^r \leq (2\tau(d))^{2(k-1)r} \leq (2\tau(n))^{2(k-1)r} \ll_{r,k} \tau(n)^{2(k-1)r}. \tag{3.1}$$

Thus,

$$\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m(x) \ll x(\log x)^\alpha \sum_{m>y}\frac{\tau(m)^{2(r-1)k}}{m^2}.$$

Using [8, Lemma 10.2.7], we have

$$\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m(x) \ll \frac{x(\log x)^{\beta+2^{2(k-1)r}}}{y} \tag{3.2}$$

for any $\varepsilon>0$.

For the main term, we will use the Huxley version of the Bombieri-Vinogradov Theorem. We have

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

Now, (2.6) and (2.7) give us

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

Thus, we may consider

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

Let $G_m=\mathrm{Gal}(K(E[m])/K)$. By (2.4), we have

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

By [7, Proposition 3.8 and its proof], we have $|G_m|\gg\varphi(m)^2$. Thus,

$$\sum_{m\ge 3}\frac{|g(m)|}{|G_m|}\ll\sum_{m\ge 3}\frac{|g(m)|}{\varphi(m)^2}\ll\sum_{m\ge 3}\frac{\tau_k(m)^r(\log m)^\beta(\log\log m)^2}{m^{2-\alpha}}<\infty \tag{3.3}$$

since $\tau_k(m)\ll m^\varepsilon$, $(\log m)\ll m^\varepsilon$, and $\log\log m\ll m^\varepsilon$ for any $\varepsilon>0$. We also have

$$\sum_{m>y}\frac{|g(m)|}{|G_m|}\ll\frac{(\log y)^{\beta+2^{2(k-1)r}}(\log\log y)^2}{y^{1-\alpha}} \tag{3.4}$$

for all $\varepsilon>0$ since $\tau_k(m)\ll m^\varepsilon$, $(\log m)\ll m^\varepsilon$, and $\log\log m\ll m^\varepsilon$ for any $\varepsilon>0$. So we must deal with

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

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 2.1, 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,

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

Recall that $t(m) \ll_{\mathfrak{f}} 1$, and by [16, Proof of Lemma 4] or [3, Remark 2.8], we may take $\mathfrak{f}$ to be the the Großencharacter associated to E. By Lemma 2.2, we have

$$\sum_{N(\mathfrak{q}) \leq \frac{\sqrt{x}}{(\log x)^B}} \max_{\gcd(\mathfrak{a},\mathfrak{q})=1} \frac{1}{T(\mathfrak{q})} \left| \pi_K(x; \mathfrak{q}, \mathfrak{a}) - \frac{\mathrm{li}(x)}{h(\mathfrak{q})} \right| \ll \frac{x}{(\log x)^A}. \tag{3.5}$$

However, we know that $T(\mathfrak{q}) \leq 6$ when $T(\mathfrak{q})$ is an imaginary quadratic field. Thus, (3.5) becomes

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

Hence, assuming $y \leq x^{1/4}/N(\mathfrak{f})(\log x)^B$, we have

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

We are now ready to evaluate

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

By (2.4), we have $\widetilde{\pi}_{\mathfrak{m}}(x) = 2\pi_m(x) + O(\sqrt{x}/\log x)$. However, by [7, Proposition 3.5], we have p splits completely in $\mathbb{Q}(E[m])$ with $m \geq 3$ implies $p \equiv 1 \bmod m$. Thus,

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

for $m \leq \sqrt{x}\log x$. By the Cauchy-Schwarz inequality, we have

$$\begin{aligned}
\left|\sum_{3\leq m\leq y}\left(g(m)\left(\widetilde{\pi}_{\mathfrak{m}}(x)-\frac{\mathrm{li}(x)}{|G_m|}\right)\right)\right| &= \left|\sum_{3\leq m\leq y}\left(g(m)\left(\widetilde{\pi}_{\mathfrak{m}}(x)-\frac{\mathrm{li}(x)}{|G_m|}\right)^{1/2}\left(\widetilde{\pi}_{\mathfrak{m}}(x)-\frac{\mathrm{li}(x)}{|G_m|}\right)^{1/2}\right)\right| \\
&\leq \left(\sum_{m\leq y}|g(m)|^2\left|\widetilde{\pi}_{\mathfrak{m}}(x)-\frac{\mathrm{li}(x)}{|G_m|}\right|\right)^{\frac{1}{2}}\left(\sum_{m\leq y}\left|\widetilde{\pi}_{\mathfrak{m}}(x)-\frac{\mathrm{li}(x)}{|G_m|}\right|\right)^{1/2} \\
&\ll \left(x\sum_{m\leq y}\frac{\tau_k(m)^{2r}(\log m)^{2\alpha}}{m}\right)\frac{\sqrt{x}}{(\log x)^{A/2}} \\
&\ll \frac{x}{(\log x)^{\frac{A}{2}-2\alpha}}\sum_{m\leq y}\frac{\tau_k(m)^{2r}}{m} \\
&\ll \frac{x}{(\log x)^{\frac{A}{2}-2\alpha}}\sum_{m\leq y}\frac{\tau(m)^{4(k-1)r}}{m} \\
&\ll \frac{x}{(\log x)^{\frac{A}{2}-2\alpha-2^{4(k-1)r}}}
\end{aligned}$$

by (3.1) and [8, Lemma 10.2.7]. Choosing A sufficiently large and $y = x^{1/4}/N(\mathfrak{f})(\log x)^B$ finishes the proof of Theorem 1.1(a) by (3.2), (3.4), (3.5), and since r, k, and α are fixed. This completes the proof of Theorem 1.1

4. Proof of Theorem 1.2

Let $G_m = \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$. By the Chebotarev density theorem and GRH (that is, (2.3), we have

$$\begin{aligned}
\sum_{m\leq y}g(m)\pi_m(x) &= \sum_{m\leq y}g(m)\left(\frac{\mathrm{li}(x)}{|G_m|}+O\left(\sqrt{x}\log(mNx)\right)\right) \\
&= \mathrm{li}(x)\sum_{m\geq 1}\frac{g(m)}{|G_m|}+O\left(\mathrm{li}(x)\sum_{m>y}\frac{|g(m)|}{|G_m|}\right)+O_N\left(\sqrt{x}\log x\sum_{m\leq y}|g(m)|\right).
\end{aligned}$$

By (3.3) and (3.4), if E is CM, then

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

and

$$\sum_{m>y}\frac{|g(m)|}{|G_m|}\ll\frac{(\log y)^{\beta+2^{2(k-1)r}}(\log\log y)^2}{y} \tag{4.1}$$

for any $\varepsilon > 0$. If E in non-CM, then we have $|G_m| \gg m^{2-\varepsilon}$ for all $\varepsilon > 0$ by [2, Equation (3.1)]. Thus, as in (3.3), we have

$$\sum_{m\geq 1} \frac{|g(m)|}{|G_m|} \ll \sum_{m\geq 1} \frac{\tau_k(m)^r m^\alpha (\log m)^\beta}{m^{2-\varepsilon}} \ll \sum_{m\geq 1} \frac{1}{m^{2-\alpha-\varepsilon}} < \infty$$

since $|g(m)| \ll \tau_k(m)^r m^\beta (\log m)^\beta \ll m^{\beta+\varepsilon}$ for any $\varepsilon > 0$, and

$$\sum_{m> y} \frac{|g(m)|}{|G_m|} \ll \sum_{m> y} \frac{\tau_k(m)^r m^\alpha (\log m)^\beta}{m^{2-\varepsilon}} \ll \sum_{m\geq 1} \frac{1}{m^{2-\alpha-\varepsilon}} \ll \frac{1}{y^{1-\alpha-\varepsilon}} \tag{4.2}$$

for any $\varepsilon > 0$.

For the remaining error term, we have $|g(m)| \ll \tau_k(m)^r m^\alpha (\log m)^\beta$ by hypothesis. Thus, by (3.1), we have

$$\begin{aligned}\sum_{m\leq y} |g(m)| &\ll \sum_{m\leq y} \tau_k(m)^r m^\alpha (\log m)^\beta \ll y^\alpha (\log y)^\beta \sum_{m\leq y} \tau_k(m)^r \\ &\ll y^{1+\alpha} (\log y)^\beta \sum_{m\leq y} \frac{\tau_k(m)^r}{m} \ll y^{1+\alpha} (\log y)^\beta \sum_{m\leq y} \frac{\tau(m)^{2(k-1)r}}{m} \\ &\ll y^{1+\alpha} (\log y)^{\beta+2^{2(k-1)r}}.\end{aligned}$$

Thus,

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

if E is non-CM,

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

if E is CM where

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

is a constant.

Now we must deal with 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:

4.1. **Complex Multiplication.** 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 $a_p = 0$. 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,

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

We note that $a_p = 0$ implies $\#\overline{E}(\mathbb{F}_p) = p+1$. We also have $m|i(p)|i(p)^2 f(p) = \#\overline{E}(\mathbb{F}_p) = p+1$. Also, since p splits completely in $\mathbb{Q}(E[m])$ implies p splits completely in $\mathbb{Q}(\zeta_m)$. Thus, $p \equiv 1 \bmod m$ and $p \equiv -1 \bmod m$ which is a contradiction unless $m = 2$, by our (future) choice of y, this says $\pi_m^{\mathrm{s}}(x) = 0$ for $m > y$. Therefore, we have

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

For ordinary primes we have the following logic of [7, 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 $K = \mathbb{Q}(\sqrt{-D})$ where D is a squarefree positive integer and K is the field with which E has complex multiplication by the ring of algebraic integers $\mathcal{O}_K$ of K. By [6, Lemma 2.3], if p is a prime of good reduction that is also ordinary, then $\mathbb{Q}(\theta_p) = \mathbb{Q}(\sqrt{-D})$. Hence,

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

Note that the norm of θ_p in $\mathbb{Q}(\sqrt{-D}) = \mathbb{Q}(\theta_p)$ is p since it is complex and the root of the integer monic polynomial $X^2 - a_p X + p$. Hence,

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

where

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

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

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

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

$$S_m \ll \frac{\sqrt{x}}{m\sqrt{D}}\left(1 + \frac{2\sqrt{x}}{m}\right) \ll \frac{x}{m^2} + \frac{\sqrt{x}}{m}. \tag{4.3}$$

Therefore, by (3.1), (4.3), [8, Lemma 10.2.7] and the hypothesis of the theorem, we have

$$\begin{aligned}\sum_{y<m\leq\sqrt{x}+1} g(m)\pi_m^{\circ}(x) &\ll x\sum_{y<m\sqrt{x}+1}\frac{|g(m)|}{m^2}+\sqrt{x}\sum_{y<m\leq\sqrt{x}+1}\frac{|g(m)|}{m}\\ &\ll x(\log x)^{\beta}\sum_{m>y}\frac{\tau_k(m)^r}{m^{2-\alpha}}+x^{\frac{1+\alpha}{2}}(\log x)^{\beta}\sum_{m\leq\sqrt{x}+1}\frac{\tau_k(m)^r}{m}\\ &\ll \frac{x(\log x)^{\beta}}{y^{1-\alpha}}\sum_{m>y}\frac{\tau(m)^{2(k-1)r}}{m}+x^{\frac{1+\alpha}{2}}(\log x)^{\beta}\sum_{m\leq\sqrt{x}+1}\frac{\tau(m)^{2(k-1)r}}{m}\\ &\ll \frac{x(\log x)^{\beta+2^{2(k-1)r}}}{y^{1-\alpha}}+x^{\frac{1+\alpha}{2}}(\log x)^{\beta+2^{2(k-1)r}}.\end{aligned}$$

Collecting all error terms we obtain

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

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

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

4.2. **Non-Complex Multiplication.** We need to obtain a bound for $\pi_m(x):=\#\{p\leq x : p\nmid N, m|i(p)\}$. We note that by (2.2) $m|i(p)$ implies p splits completely in $\mathbb{Q}(E[m])$. This last condition implies p splits completely in $\mathbb{Q}(\zeta_m)$ which is equivalent to $p\equiv 1 \bmod m$. Also, $m|i(p)$ implies $m^2|i(p)^2f(p)=\#\overline{E}(\mathbb{F}_p)=p+1-a_p$. Hence, $a_p\equiv p+1\equiv 2 \bmod m$. Also, $p\equiv a_p-1 \bmod m^2$. Let $\pi(x;m^2,a):=\#\{p\leq x : p\equiv a \bmod m^2\}$. We have the trivial bound

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

Since $m\leq\sqrt{x}+1$, we have $x/m^2\geq x/(x+2\sqrt{x}+1)\gg 1$. Thus, $\pi(x;m^2,a)\ll x/m^2$. Thus, by the above discussion, we have

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

Thus, by (3.1) and [8, Lemma 10.2.7], we have

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

Collecting the error terms and noticing gives us

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

Choosing $y = x^{1/3}$ gives us

$$\sum_{p\leq x} f(i(p)) = c_E \mathrm{li}(x) + O\left(x^{\frac{5+2\alpha}{6}}(\log x)^{\beta+2^{2(k-1)r}}\right).$$

This completes the proof of Theorem 1.2.

5. Applications

We break this section up into two subsections: one for arithmetic functions which will tell us about some statistics of the sequence $i(p)$ as p ranges over primes $\leq x$, and the other for analytic functions which will come to mean well-behaved functions that tend to ∞ as $i(p) \to \infty$.

5.1. **Arithmetic Functions.** We consider the functions $\omega(n)^r$, $\Omega(n)^r$, $2^{\omega(n)r}$, and $\tau_k(n)^r$. Let $f : \mathbb{N} \to \mathbb{C}$ be one of these functions. Then, by the Möbius inversion formula [8, Chapter 1, §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, we have

$$g(n) = \sum_{m|n} \mu(d) f\left(\frac{n}{m}\right)$$

for all $n \in \mathbb{N}$ where μ is the Möbius function. Hence,

$$|g(n)| \leq \sum_{m|n} f\left(\frac{n}{m}\right) \leq \tau(n) f(n) \ll \tau_k(n)^{r+1}$$

since $\omega(n) \leq \max(\Omega(n), 2^{\omega(n)}) \leq \tau(n) \leq \tau_k(n)$ for all n and k in $\mathbb{N}$. Thus, $f(n)$ satisfies the criteria of Theorem 1.1 with $\alpha = 0$. Hence, we have

$$\sum_{p\leq x} \omega(i(p))^r = c_{E,\omega^r}\mathrm{li}(x) + O_E\left(\frac{x}{(\log x)^A}\right)$$
$$\sum_{p\leq x} \Omega(i(p))^r = c_{E,\Omega^r}\mathrm{li}(x) + O_E\left(\frac{x}{(\log x)^A}\right)$$
$$\sum_{p\leq x} 2^{i(p)r} = c_{E,2^\omega}\mathrm{li}(x) + O_E\left(\frac{x}{(\log x)^A}\right)$$
$$\sum_{p\leq x} \tau_k(i(p))^r = c_{E,\tau_k^r}\mathrm{li}(x) + O_E\left(\frac{x}{(\log x)^A}\right)$$

if E is a CM curve,

$$\sum_{p\leq x} \omega(i(p))^r = c_{E,\omega^r}\mathrm{li}(x) + O_E\left(x^{3/4}(\log x)^{2^{2(k-1)(r+1)}}\right)$$
$$\sum_{p\leq x} \Omega(i(p))^r = c_{E,\Omega^r}\mathrm{li}(x) + O_E\left(x^{3/4}(\log x)^{2^{2(k-1)(r+1)}}\right)$$
$$\sum_{p\leq x} 2^{i(p)r} = c_{E,2^\omega}\mathrm{li}(x) + O_E\left(x^{3/4}(\log x)^{2^{2(k-1)(r+1)}}\right)$$
$$\sum_{p\leq x} \tau_k(i(p))^r = c_{E,\tau_k^r}\mathrm{li}(x) + O_E\left(x^{3/4}(\log x)^{2^{2(k-1)(r+1)}}\right)$$

if GRH holds and E is a CM curve

$$\sum_{p\leq x} \omega(i(p))^r = c_{E,\omega^r}\mathrm{li}(x) + O_E\left(x^{5/6}(\log x)^{2^{2(k-1)(r+1)}}\right)$$
$$\sum_{p\leq x} \Omega(i(p))^r = c_{E,\Omega^r}\mathrm{li}(x) + O_E\left(x^{5/6}(\log x)^{2^{2(k-1)(r+1)}}\right)$$
$$\sum_{p\leq x} 2^{i(p)r} = c_{E,2^\omega}\mathrm{li}(x) + O_E\left(x^{5/6}(\log x)^{2^{2(k-1)(r+1)}}\right)$$
$$\sum_{p\leq x} \tau_k(i(p))^r = c_{E,\tau_k^r}\mathrm{li}(x) + O_E\left(x^{5/6}(\log x)^{2^{2(k-1)(r+1)}}\right)$$

if GRH holds and E is a non-CM curve. Since $\omega(n) = \sum_{p|n} 1$, we note that all of the above constant are positive. To see this we note that

$$c_{E,\omega} = \sum_{m\geq 1} \frac{g(m)}{|G_m|} = \sum_{p\geq 1} \frac{1}{|G_p|} > 0$$

and we have

$$\sum_{p\leq x}\omega(i(p))\leq\sum_{p\leq x}f(i(p))$$

for any f defined above. We leave the analysis of the coefficients $c_{E,f}$ to future research. We also note that these theorems can be applied to the functions χ_S where S is a singleton set to obtain results about when $i(p)=1$ or some other fixed integer w.

Remark. We also note that the exponent of $\log x$ in these examples is not optimal. For example, let $f(n)=\chi_{\{1\}}(n)=1$ if and only if $n=1$ and 0 otherwise. Then, Cojocaru and Murty [7] showed that the GRH gives us

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

if E has CM, and

$$\sum_{p\leq x}\chi_{\{1\}}(i(p))=N_E(x)=c_E\mathrm{li}(x)+O_N(x^{5/6}(\log x)^{2/3})$$

if E does not have CM. Also, Akbary and Ghioca [2] showed that

$$\sum_{p\leq x}\tau(i(p))=c'_E\mathrm{li}(x)+O(x^{5/6}(\log x)^{1/3}).$$

The reason we do not obtain these optimal bounds that this technique is generic. If we were to focus on specific f, we could obtain better results. For $\chi_{\{1\}}$, we have

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

Thus, $|g(n)|\leq 1\ll\tau_2(n)^0n^0(\log n)^0$. Thus, Theorem 1.2 gives us that on GRH, we have

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

if E has CM,

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

if E does not have CM, and

$$\sum_{p\leq x}\tau(i(p))=c'_E\mathrm{li}(x)+O(x^{5/6}(\log x)^4).$$

However, we used (3.1) in the determination of the exponent of $\log x$, which says

$$\tau(n)=\tau_2(n)^1\leq\tau(n)^{2(2-1)1}=\tau(n)^2.$$

This bound contributes to the some of the non-optimal error terms. We should note that if $r=1$ in Theorem 1.2, then we could use the following result to improve the technique:

$$\sum_{m\leq x}\tau_k(m)=xP_{k-1}(\log x)+O(x^{\frac{k-1}{k}}(\log x)^{k-2})$$

where P_{k-1} is polynomial of degree $k-1$. Hence, this gives

$$\sum_{m\leq x}\frac{\tau_k(m)}{m}\ll(\log x)^k$$

instead of

$$\sum_{m\leq x}\frac{\tau_k(m)}{m}\ll(\log x)^{2^{2(k-1)}}.$$

Hence, we have the following theorem:

Theorem 5.1. *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 $n\in\mathbb{N}$. Let $\alpha,\beta\in\mathbb{R}$ be fixed with $\beta\geq 0$, and let $k\in\mathbb{N}$ such that $|g(n)|\ll\tau_k(n)n^{\alpha}(\log n)^{\beta}$ for all $n\in\mathbb{N}$. Then, there exists a positive constant $c_{E,f}$ such that
(a) *if $\alpha<1$, GRH holds for E, and E is a CM curve, then*

$$\sum_{p\leq x}f(i(p))=c_{E,f}\mathrm{li}(x)+O\left(x^{\frac{3+\alpha}{4}}(\log x)^{\beta+k}\right).$$

(b) *if $\alpha<1/2$, GRH holds for E, and E is a non-CM curve, then*

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

We note that if $k=1$ in the above theorem, then we may assume $r=0$ since $\tau_k(n)=\tau_1(n)=1$ for all $n\in\mathbb{N}$. So the above theorem also yields an improvement for $r=0$. This gives us (assuming GRH)

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

if E is CM, and

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

if E is non-CM. Also, assuming GRH, we obtain

$$\sum_{p\leq x}\tau(i(p))=c'_E\mathrm{li}(x)+O(x^{3/4}\log x)$$

if E is CM, and

$$\sum_{p\leq x}\tau(i(p))=c'_E\mathrm{li}(x)+O(x^{5/6}\log x)$$

if E is non-CM since $\tau(n)=\sum_{d|n}g(d)$ implies $g(d)=1$. These error terms are not optimal, but near optimal. The reasons for the discrepancy are the additional intricacies of the functions involved. We could similarly improve the above equations for $\omega(n),\Omega(n),2^{\omega(n)}$, and $\tau_k(n)$. This generalizes the work of Cojocaru and Murty [7] and Akbary and Ghioca [2].

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

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

and

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

Thus, by the Möbius Inversion Formula, we have

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

We also have

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

Hence, $\sigma_\alpha(n)$ satisfies the criteria of Theorem 1.2 with $r = k = 2$ and $\beta = 0$ as long as α satisfies the corresponding criterion. Thus, we have

$$\sum_{p \leq x} \sigma_\alpha(i(p)) = c_E \mathrm{li}(x) + O(x^{\frac{3+\alpha}{4}} (\log x)^8)$$

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

$$\sum_{p \leq x} \sigma_\alpha(i(p)) = c_E \mathrm{li}(x) + O(x^{\frac{5+2\alpha}{6}} (\log x)^8)$$

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

5.2. **Analytic Functions.** Let $f(n) = (\log n)^\alpha$ for some fixed positive real number α. Then, for $g : \mathbb{N} \to \mathbb{C}$ with $f(n) = \sum_{m|n} g(m)$, we have

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

Thus, $f(n)$ satisfies the criteria of Theorems 1.1 and 5.1. Hence, we have

$$\sum_{p \leq x} (\log i(p))^\alpha = c_{E,\alpha} \mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right)$$

if E is a CM curve,

$$\sum_{p \leq x} (\log i(p))^\alpha = c_{E,\alpha} \mathrm{li}(x) + O\left(x^{3/4} (\log x)^{1+\alpha}\right)$$

if GRH holds for E and E is a CM curve, and

$$\sum_{p \leq x} (\log i(p))^\alpha = c_{E,\alpha} \mathrm{li}(x) + O\left(x^{5/6} (\log x)^{1+\alpha}\right)$$

if GRH holds for E and E is a non-CM curve. We note the constant $c_{E,\alpha}$ are positive. This is true since

$$\pi(x) \leq \frac{1}{(\log 2)^\alpha} \sum_{p \leq x} (\log i(p))^\alpha = c_{E,\alpha} \mathrm{li}(x) + o(\mathrm{li}(x)).$$

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

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

and hence $g(n) \leq \tau(n) n^\alpha$. Thus, $f(n) = n^\alpha$ satisfies the criteria of Theorem 5.1. Hence,

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

if $\alpha < 1$, GRH holds for E and E is a CM curve, and

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

if $\alpha < 1/2$, GRH holds for E, and E is a non-CM curve. This nearly resolves a problem posed by Kowalski [13, Problem 3.1].

5.3. **The case $\alpha = 1$ and $\beta > 3$.** In this subsection, we are concerned with the function $f(1) = 1$ and, for $n \geq 2$, $f(n) = n/(\log n)^\beta$ where $\beta > 3$ is fixed. We will show the following theorem:

Theorem 5.2. *Let E be an elliptic curve with CM. Suppose GRH holds for E. Then, there exists a constant C_E such that*

$$\sum_{p \leq x} f(i(p)) = C_E \mathrm{li}(x) + O\left(\frac{x}{(\log x)^{\beta-2}}\right)$$

where the implied constant is dependent on E.

As always, let $g : \mathbb{N} \to \mathbb{C}$ be the function defined by

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

Hence,

$$|g(n)| \ll \frac{n}{(\log n)^\beta} \sum_{d|n} 1 = \frac{\tau(n) n}{(\log n)^\beta}.$$

Therefore,

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

By (2.3), we have

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

Now,

$$\begin{aligned}\left|\sum_{m\ge 1}\frac{g(m)}{|G_m|}\right| &\le \frac{1}{|G_1|} + \sum_{m\ge 1}\frac{|g(m)|}{|G_m|} \ll \sum_{m\ge 2}\frac{\tau(m)m}{\varphi(m)^2(\log m)^\beta}\\ &\ll \sum_{m\ge 2}\frac{\tau(m)(\log\log m)^2}{m(\log m)^\beta}\\ &\ll \sum_{m\ge 2}\frac{\tau(m)}{m(\log m)^{\beta-\varepsilon}}\end{aligned}$$

and this last summation converges by partial summation since $\beta > 3$. Also, by partial summation, we have

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

Hence,

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

Also, as before, we have

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

by [8, Lemma 10.2.7 and §9.3]. Choosing $y = x^{1/4}$ gives the result.

Remark. By [2, Lemma 3.2], we may extend all the result which relied upon GRH to Abelian varieties which contains a dimension one Abelian subvariety also defined over $\mathbb{Q}$.

We also note that given the sharpness of the error terms in Theorem 1.2 we only need to assume that there are no zero in the region $\Re(s) > \theta$ where θ is determined by E having CM

or not.

We also note the GRH implies

$$\sum_{p\leq x} i(p) \gg x.$$

To see we note that for any $0 < \theta < 1/2$, we have

$$\begin{aligned}\sum_{p\leq x} i(p) &= \sum_{m\leq \sqrt{x}+1} \varphi(m)\pi_m(x) \geq \sum_{m\leq x^\theta} \varphi(m)\pi(x)\\ &= \sum_{m\leq x^\theta} \varphi(m)\left(\frac{\mathrm{li}(x)}{|G_m|} + O(\sqrt{x}\log(mx))\right)\\ &\gg \mathrm{li}(x)\sum_{m\leq x^\theta}\frac{\varphi(m)}{m^2} + O\left(\sqrt{x}\log x\sum_{m\leq x^\theta}\varphi(m)\right)\\ &\gg \theta x + O(y^2\sqrt{x}\log x).\end{aligned}$$

Choose $\theta < 1/4$ will suffice.

We also note that if E has CM, then

$$\frac{x\log\log x}{\log x} = o\left(\sum_{p\leq x} i(p)\right).$$

That is, for every $C > 0$, there exists x_0 such that for a $x \geq x_0$, we have

$$\sum_{p\leq x} i(p) \gg C\frac{x\log\log x}{\log x}.$$

To see this let $G'_m = \mathrm{Gal}(K(E[m])/K)$ where K is the field by which E has complex multiplication. Then, $|G'_m| = |\mathrm{Gal}(\mathbb{Q}(E[m])/K)| = \frac{1}{2}[\mathbb{Q}(E[m]) : \mathbb{Q}] \ll m^2$ for $m \geq 3$ by [7,

Proposition 3.8]. Note that, for $y \leq \sqrt{x}+1$, we have

$$\begin{aligned}
\sum_{p\leq x} i(p) &= \sum_{m\leq \sqrt{x}+1} \varphi(m)\pi_m(x) \geq \sum_{3\leq m\leq y} \varphi(m)\pi_m(x) \gg \sum_{3\leq m\leq y} \varphi(m)\left(\widetilde{\pi}_m(x) + O\left(\frac{\sqrt{x}}{\log x}\right)\right) \\
&\gg \sum_{3\leq m\leq y} \varphi(m)\widetilde{\pi}_m(x) + O\left(\frac{y^2\sqrt{x}}{\log x}\right) \\
&= \sum_{3\leq m\leq y} \varphi(m)\left(\widetilde{\pi}_m(x) - \frac{\mathrm{li}(x)}{|G'_m|} + \frac{\mathrm{li}(x)}{|G'_m|}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right) \\
&\gg \mathrm{li}(x) \sum_{3\leq m\leq y} \frac{\varphi(m)}{|G'_m|} + O\left(y \sum_{3\leq m\leq y} \left|\widetilde{\pi}_m(x) - \frac{\mathrm{li}(x)}{|G'_m|}\right|\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right) \\
&\gg \frac{x}{\log x} \sum_{3\leq m\leq y} \frac{\varphi(m)}{m^2} + O_A\left(\frac{yx}{(\log x)^A}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right) \\
&\gg \frac{x\log y}{\log x} + O_A\left(\frac{yx}{(\log x)^A}\right) + O\left(\frac{y^2\sqrt{x}}{\log x}\right).
\end{aligned}$$

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

$$\begin{aligned}
\sum_{p\leq x} i(p) &\gg (A-2)\frac{x\log\log x}{\log x} + O_A\left(\frac{x}{(\log x)^2}\right) + O(\sqrt{x}(\log x)^{A-3}) \\
&\gg (A-2)\frac{x\log\log x}{\log x}
\end{aligned}$$

as required.

We note that the coefficients c_E may be of interest when f is an arithmetic function: $\omega(n), \Omega(n), 2^{\omega(n)}$ or $\tau_k(n)$. We relegate the study of the these coefficients to a future paper.

References

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

[2] A. Akbary and D. Ghioca. A geometric variant of the Titchmarsh divisor problem. *to appear in Int. J. Number Theory*, to appear.

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

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

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

[6] A. C. Cojocaru. Cyclicity CM elliptic curves modulo p. *Trans. Amer. Math. Soc.*, 355(7):2651–2662, 2003.

[7] Alina Carmen Cojocaru and M. Ram Murty. Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem. *Math. Ann.*, 330:601–625, 2004.

[8] Alina Carmen Cojocaru and M. Ram Murty. *An Introduction to Sieve Methods and their Applications*. Cambridge University Press, New York, 2006.

[9] John B. Friedlander and Henryk Iwaniec. *Opera de Cribro*. American Mathematical Society Colloquium Publications, 57. American Mathematical Society, Providence, Rhode Island, 2010.
[10] Rajiv Gupta and M. Ram Murty. Primitive points on elliptic curves. *Comp. Math.*, 58(1):13–44, 1986.
[11] M. N. Huxley. The large sieve inequality for algebraic number fields III. zero density results. *J. London Math. Soc. (2)*, 3:233–240, 1971.
[12] Gerald J. Janusz. *Algebraic Number Fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, Rhode Island, second edition edition, 1996.
[13] E. Kowalski. Analytic problems for elliptic curves. *J. Ramanujan Math. Soc.*, 21(1):19–114, 2006.
[14] Jeffrey Lagarias and Andrew Odlyzko. Effective versions of the Chebotarev density theorem. In Albrecht Frohlich, editor, *Algebraic Number Fields*, pages 409–464, New York, 1977. Academic Press Inc.
[15] Serge Lang. *Algebraic Number Theory*. Addison-Wesley Publishing Company, Inc., Reading, Massachusetts-London-Don Mills, Ontario, 1970.
[16] M. Ram Murty. On Artin's conjecture. *J. Number Theory*, 16(2):147–168, 1983.
[17] M. Ram Murty. On the supersingular reduction of elliptic curves. *Proc. Indian Acad. Sci. Math. Sci.*, 97(1-3):247–250, 1987.
[18] Jean-Pierre Serre. Résumé des cours de 1977-1978. *Ann. Collège France, Collège de France*, pages 67–70, 1978.
[19] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Publ. Math I. H. E. S.*, 54:323–401, 1981.
[20] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.
[21] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.
[22] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptology*. Chapman & Hall/CRC, Boca Raton, Florida, 2003.

Department of Mathematics & Statistics, Queen's University, Kingston, Ontario
E-mail address: felix@mast.queensu.ca

Department of Mathematics & Statistics, Queen's University, Kingston, Ontario
E-mail address: murty@mast.queensu.ca