Check for
updates

Square-free orders for CM elliptic curves modulo p in short intervals

Peng-Jie Wong[1]

Abstract

Let E be a CM elliptic curve over $\mathbb{Q}$. We refine the work of Cojocaru on the asymptotic formulae for the number of primes $p \leq x$ for which the reduction modulo p of E is of square-free order. Also, we derive an unconditional short interval variant for the asymptotics. Compared to the estimate derived from the generalised Riemann hypothesis, the presented result is valid for even shorter intervals. Furthermore, we improve the short interval variant of the cyclicity problem for CM elliptic curves previously obtained by the author.

Keywords CM elliptic curves · Square-free orders · The cyclicity problem

Mathematics Subject Classification 11N45 · 11G05 · 11N36

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, and let N_E be its conductor. For a prime p of good reduction, we let $\bar{E}$ be the reduction of E modulo p and $\bar{E}(\mathbb{F}_p)$ be the group of rational points of $\bar{E}$ over $\mathbb{F}_p$. By Hasse's bound, there is an integer a_p such that $|a_p| \leq 2\sqrt{p}$ and $|\bar{E}(\mathbb{F}_p)| = p + 1 - a_p$. For $p \geq 5$, p is called supersingular if $a_p = 0$; otherwise, p is ordinary.

Since Lang and Trotter [14] formulated an elliptic curve analogue of Artin's primitive root conjecture, the study of the structure of $\bar{E}(\mathbb{F}_p)$, as p varies, has attracted many mathematicians. For instance, Cojocaru [5] determined an asymptotic formula for

$$h_E(x, \mathbb{Q}) = \#\{p \leq x \mid p \nmid N_E, a_p \neq 0, \text{ and } |\bar{E}(\mathbb{F}_p)| \text{ is square-free}\} \quad (1)$$

when E has complex multiplication (CM) by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. More precisely, she showed that

$$h_E(x, \mathbb{Q}) = \delta_E \operatorname{Li}(x) + O\left(\frac{x}{(\log x)(\log\log((\log x)/N_E^2))} \frac{\log\log x}{\log((\log x)/N_E^2)}\right), \quad (2)$$

In memory of my friend, Richard

✉ Peng-Jie Wong
pjwong@math.nsysu.edu.tw

[1] Department of Applied Mathematics, National Sun Yat-Sen University, Kaohsiung City, Taiwan

where $\text{Li}(x) = \int_2^x \frac{dt}{\log t}$ is the logarithmic integral function,

$$\delta_E = \frac{1}{2} \sum_{\mathfrak{a},m} \frac{\mu(\mathfrak{a})\mu(m)}{[K(E[\mathfrak{a}^2])K(E[m]) : K]}, \tag{3}$$

the sum is over square-free integral ideals $\mathfrak{a}$ of $\mathcal{O}_K$ composed of degree-one unramified prime ideals and over square-free $m \in \mathbb{N}$, and $\mu(\mathfrak{a})$ is the number field analogue of the Möbius function for K. Here, as later, $E[m]$ (resp., $E[\mathfrak{a}]$) denotes the group of m-torsion points (resp., the group of $\mathfrak{a}$-torsion points) of E. Moreover, under the generalised Riemann hypothesis (GRH) for the Dedekind zeta functions of the division fields of E, Cojocaru established

$$h_E(x, \mathbb{Q}) = \delta_E \text{Li}(x) + O(x^{5/6}(\log x)^2(\log(N_E x))^{1/3}). \tag{4}$$

Recall that as E is defined over $\mathbb{Q}$, the field K is one of the nine imaginary quadratic fields of class number 1. It worth remarking that by [5, Theorem 1.3], one knows $\delta_E > 0$ whenever K is $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, or $\mathbb{Q}(\sqrt{-163})$.

One of the objectives of this article is to prove the following improved estimates for $h_E(x, \mathbb{Q})$.

Theorem 1 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E and with complex multiplication by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Then for any $A > 0$, we have*

$$h_E(x, \mathbb{Q}) = \delta_E \text{Li}(x) + O_A\left(N_E \frac{x}{(\log x)^A}\right), \tag{5}$$

where δ_E is defined as in (3).

Moreover, assuming GRH, for any $\eta \in (0, \frac{1}{3})$, we have

$$h_E(x, \mathbb{Q}) = \delta_E \text{Li}(x) + O_\eta\left(x^{5/6} \frac{(\log(N_E x))^{1/3}}{(\log x)^{2/3}}\right) \tag{6}$$

uniformly in $N_E \leq x^\eta$.

Remark For general elliptic curves $E/\mathbb{Q}$, one may instead consider

$$\pi_E^{\text{SF}}(x) = \#\{p \leq x \mid p \nmid N_E \text{ and } |\bar{E}(\mathbb{F}_p)| \text{ is square-free}\}.$$

For E with CM, the methods used in [5] and this article can be adapted to study $\pi_E^{\text{SF}}(x)$. When E is non-CM, Cojocaru [4] showed how to derive an asymptotic formula for $\pi_E^{\text{SF}}(x)$ under the generalized Riemann hypothesis, Artin's holomorphy conjecture, and the pair correlation conjecture. However, the precise asymptotic of $\pi_E^{\text{SF}}(x)$ is still not known unconditionally for this case. Nonetheless, in [8], Gekeler proved that the conjectural asymptotic for $\pi_E^{\text{SF}}(x)$ holds on average over elliptic curves E. Moreover, in [2], Akhtari, David, Hahn, and Thompson unconditionally established the predicted upper bound for $\pi_E^{\text{SF}}(x)$ and showed that the average results are compatible with the conjectural asymptotics at the level of the constants.

It is worth mentioning that in [5], after establishing (2) and (4), Cojocaru studied an elliptic curve analogue of Linnik's problem as follows. Denoting p_E the smallest ordinary prime p for which $|\bar{E}(\mathbb{F}_p)|$ is square-free, she showed that if $\delta_E \neq 0$, then $p_E = O(\exp(eN_E^3))$, unconditionally, and $p_E = O_\epsilon((\log N_E)^{2+\epsilon})$ under GRH. In light of her work, we prove the following refined unconditional bound for p_E.

Corollary 1.1 *Let $\epsilon \in (0, 1)$. If $\delta_E \neq 0$, then*

$$p_E = O_\epsilon(\exp(N_E^\epsilon)).$$

Proof For $\epsilon \in (0, 1)$, we apply Theorem 1 with $A = 2/\epsilon$ to obtain

$$h_E(x, \mathbb{Q}) = \delta_E \operatorname{Li}(x) + O_\epsilon \left(N_E \frac{x}{(\log x)^{2/\epsilon}} \right).$$

As $\delta_E \gg \frac{1}{\log \log N_E}$ (see [5, Sec. 7]), if we choose $x = \exp(N_E^\epsilon)$, then $h_E(x, \mathbb{Q}) > 0$ for N_E sufficiently large with respect to ϵ. Thus, there is an ordinary prime $p_E = p = O_\epsilon(\exp(N_E^\epsilon))$ such that $|\bar{E}(\mathbb{F}_p)|$ is square-free. □

Furthermore, as may be noticed, the estimates (2), (4), (5), and (6) present an "elliptic" analogue of the prime number theorem. Indeed, a strong form of the prime number theorem states that for any $A > 0$, one has

$$\pi(x) = \operatorname{Li}(x) + O \left(\frac{x}{(\log x)^A} \right); \tag{7}$$

under the Riemann hypothesis, one has

$$\pi(x) = \operatorname{Li}(x) + O(x^{1/2} \log x). \tag{8}$$

In a slightly different vein, as (7) gives

$$\pi(2x) - \pi(x) = \operatorname{Li}(2x) - \operatorname{Li}(x) + O \left(\frac{x}{(\log x)^A} \right),$$

one may ask for an asymptotic formula of the distribution of primes in short intervals when $(x, 2x]$ is replaced by $(x, x+h]$ for some $x^{1-\delta} \le h \le x$ with $\delta \in [0, 1)$. Under the Riemann hypothesis, (8) implies that for any $A > 0$,

$$\pi(x + h) - \pi(x) = \operatorname{Li}(x + h) - \operatorname{Li}(x) + O \left(\frac{h}{(\log x)^A} \right) \tag{9}$$

whenever $x^{1-\delta} \le h \le x$ with $\delta \in [0, \frac{1}{2})$. Although the Riemann hypothesis is still out of reach, there are some progresses towards (9). For example, Huxley [11] showed that (9) is valid for $x^{1-\delta} \le h \le x$ with $\delta \in [0, \frac{5}{12})$. From the above discussion, one may further consider

$$h_E(x, h, \mathbb{Q}) = \#\{x < p \le x + h \mid p \nmid N_E, a_p \ne 0, \text{ and } |\bar{E}(\mathbb{F}_p)| \text{ is square-free}\}. \tag{10}$$

By the virtue of (5), for any $A > 0$, we have

$$h_E(x, x, \mathbb{Q}) = \delta_E(\operatorname{Li}(2x) - \operatorname{Li}(x)) + O_A \left(N_E \frac{x}{(\log x)^A} \right).$$

Furthermore, by (4), under GRH, for any $x^{1-\delta} \le h \le x$ with $\delta \in [0, \frac{1}{6})$, one has

$$h_E(x, h, \mathbb{Q}) = \delta_E(\operatorname{Li}(x + h) - \operatorname{Li}(x)) + O \left((\log N_E)^{1/3} \frac{h}{(\log x)^A} \right) \tag{11}$$

for any $A > 0$. However, it is apparent that we are far from reaching GRH, which leads one to ask whether an unconditional version of (11) can be obtained. In this article, we shall prove the following estimate for $h_E(x, h, \mathbb{Q})$, which is not only unconditional but also valid for shorter intervals compared to (11).

Theorem 2 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E and with complex multiplication by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Let $A > 0$ and $0 \leq \delta < \frac{1}{5}$. Then for any $x^{1-\delta} \leq h \leq x$, we have*

$$h_E(x, h, \mathbb{Q}) = \delta_E(\mathrm{Li}(x + h) - \mathrm{Li}(x)) + O_A\left(N_E \frac{h}{(\log x)^A}\right),$$

where δ_E is defined as in (3).

Remark The proofs of (2) and (4) in [5] respectively rely on the effective versions of the Chebotarev density theorem established by Lagarias and Odlyzko [13] and Murty et al. [16]. In contrast, our proofs of (5) and Theorem 2 make a use of the Bombieri–Vinogradov theorem for number fields due to Huxley [10] (see also Theorem 4 below) and its short interval variant (Theorem 5). This is inspired by the works of Akbary and Murty [1] and Murty [15] on the cyclicity problem discussed below. The key observation is that the Chebotarev conditions involved in the proofs can be translated into congruence conditions over certain ray class groups via Artin reciprocity. Nonetheless, to establish (6), we still require the effective result of Murty et al. [16]. The new input in our argument is to consider a finer splitting (17) below and invoke the Brun–Titchmarsh inequality (for K) due to Hinz and Lodemann [9] to control the "middle range" $\mathcal{N}_0(x, y, x^\theta)$.

Last but not least, we recall that rooted in the Lang–Trotter conjecture, there is a problem of finding an asymptotic formula for the number of primes $p \leq x$ for which the reduction modulo p of E is cyclic.[1] More precisely, one may consider

$$\pi_c(x, E) = \#\{p \leq x \mid p \nmid N_E \text{ and } \bar{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

This has been studied by Akbary, Cojocaru, Gupta, M.R. Murty, V.K. Murty, and Serre (see [18] for a more detailed discussion and references therein). Similar to the above-discussed problem concerning square-free orders for CM elliptic curves in short intervals, one can also consider

$$\pi_c(x + h, E) - \pi_c(x, E) = \#\{x < p \leq x + h \mid p \nmid N_E \text{ and } \bar{E}(\mathbb{F}_p) \text{ is cyclic}\}.$$

By the work of Akbary and Murty [1], one has

$$\pi_c(2x, E) - \pi_c(x, E) = \mathfrak{c}_E(\mathrm{Li}(2x) - \mathrm{Li}(x)) + O_{A,D}\left(\frac{x}{(\log x)^A}\right)$$

uniformly in $N_E \leq (\log x)^D$, where

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

and the implied constant depends on A and D. Moreover, under GRH, the work of Cojocaru and Murty [6] yields

$$\pi_c(x + h, E) - \pi_c(x, E) = \mathfrak{c}_E(\mathrm{Li}(x + h) - \mathrm{Li}(x)) + O_E\left(\frac{h}{(\log x)^A}\right) \qquad (12)$$

for any $x^{1-\delta} \leq h \leq x$ with $0 \leq \delta < \frac{1}{4}$. Unconditionally, in [18], the present author showed that the estimate (12) is valid whenever $x^{1-\delta} \leq h \leq x$, with $0 \leq \delta < \frac{1}{25}$. In this article, we shall further sharpen such an unconditional result as follows.

---

[1] Note that if $|\bar{E}(\mathbb{F}_p)|$ is square-free, then $\bar{E}(\mathbb{F}_p)$ is cyclic. So, the study of the square-freeness of $|\bar{E}(\mathbb{F}_p)|$ may be seen as an intermediate problem between such a cyclicity problem and Koblitz's conjecture [12] on the primality of $|\bar{E}(\mathbb{F}_p)|$.

Theorem 3 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E and with complex multiplication by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Let $A > 0$ and $0 \leq \delta < \frac{1}{5}$. Then for any $x^{1-\delta} \leq h \leq x$, we have*

$$\pi_c(x + h, E) - \pi_c(x, E) = \mathfrak{c}_E(\mathrm{Li}(x + h) - \mathrm{Li}(x)) + O\left(N_E(\log N_E)\frac{h}{(\log x)^A}\right),$$

where the implied constant depends on $\mathbb{Q}(E[2])$ and A.

Remark The key idea for the improvement is to use a number field analogue of the Brun-Titchmarsh inequality, the estimate (35). A similar estimate of such an analogue also plays a crucial role in proving Theorem 2, especially bounding the first inner sum in (31). By these estimates, we then *only* require the Bombieri–Vinogradov theorem for number fields and its short interval variant to control small suitable initial ranges through the sieving procedures.

The rest of this article is arranged as follows. In the next section, we will discuss the strategy of proving Theorems 1 and 2. We will prove Theorems 1, 2, and 3 in Sects. 3, 4, 5, respectively. We also note that throughout our proofs of (5) and Theorems 2 and 3, we will implicitly assume $N_E \leq \exp(\sqrt{\log x})$ as the claimed estimates hold trivially otherwise.

2 Overview of the proofs of Theorems 1 and 2

In this section, we shall collect some necessary facts and review the strategy of Cojocaru [5]. Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Let N_E, $E[m]$, and $E[\mathfrak{a}]$ be defined as in the introduction. We recall that for any $m \in \mathbb{N}$, there is an injective Galois representation

$$\rho_m : \mathrm{Gal}(K(E[m])/K) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

such that

$$\mathrm{tr}\,\rho_m(\sigma_\mathfrak{p}) \equiv a_\mathfrak{p} \pmod{m} \tag{13}$$

and

$$\det \rho_m(\sigma_\mathfrak{p}) \equiv \mathrm{N}(\mathfrak{p}) \pmod{m}, \tag{14}$$

for any prime $\mathfrak{p} \nmid mN_E$ of K, where $\sigma_\mathfrak{p}$ denotes the Artin symbol at $\mathfrak{p}$, $\mathrm{N}(\mathfrak{p})$ is the norm of $\mathfrak{p}$, and $a_\mathfrak{p} = \mathrm{N}(\mathfrak{p}) + 1 - |\bar{E}(\mathbb{F}_\mathfrak{p})|$. Following Cojocaru [5], we set

$$D_m = \{g \in \mathrm{Gal}(K(E[m])/K) \mid \det \rho_m(g) + 1 - \mathrm{tr}\,\rho_m(g) \equiv 0 \pmod{m}\}.$$

By a criterion of Deuring [7], for any prime $p \geq 5$ that is of good reduction for E, p is ordinary (i.e. $a_p \neq 0$) if and only if p splits in K. Moreover, if p splits in K and $\mathfrak{p}$ is a prime of K above p, then we have $\mathrm{N}(\mathfrak{p}) = p$ and $a_\mathfrak{p} = a_p$. Thus, from (13) and (14), it follows that the condition $|\bar{E}(\mathbb{F}_p)| \equiv 0 \pmod{m^2}$ is equivalent to $\sigma_\mathfrak{p} \subseteq D_{m^2}$. Hence, we obtain

$$\#\{p \leq x \mid p \nmid mN_E, a_p \neq 0, |\bar{E}(\mathbb{F}_p)| \equiv 0 \pmod{m^2}\}$$
$$= \frac{1}{2}\#\{\mathfrak{p} \subset \mathcal{O}_K \mid \mathrm{N}(\mathfrak{p}) \leq x, \mathfrak{p} \nmid mN_E, \sigma_\mathfrak{p} \subseteq D_{m^2}\} + O\left(\frac{\sqrt{x}}{\log x} + \log(mN_E)\right),$$

where the error comes from the degree-two primes $\mathfrak{p}$ of K such that $\mathrm{N}(\mathfrak{p}) \leq x$ (there are at most $O(\sqrt{x}/\log x)$ such primes) and ramified primes (cf. [1, Eq. (3.2)]).

For the sake of convenience, we shall set

$$\pi_{D_{m^2}}(x) = \#\{\mathfrak{p} \subset \mathcal{O}_K \mid N(\mathfrak{p}) \le x, \mathfrak{p} \nmid mN_E, \sigma_{\mathfrak{p}} \subseteq D_{m^2}\}. \tag{15}$$

Similar to [5, Sec. 2], by the inclusion–exclusion principle, Hasse's bound, and the above discussion, we can express $h_E(x, \mathbb{Q})$ as

$$h_E(x, \mathbb{Q}) = \sum_{m \le 2\sqrt{x}} \mu(m)\#\{p \le x \mid p \nmid mN_E, a_p \ne 0, m^2 \mid |\bar{E}(\mathbb{F}_p)|\}$$

$$= \mathcal{N}(x, y) + \mathcal{M}(x, y, 2\sqrt{x}) + O\left(\frac{\sqrt{x}y}{\log x} + y \log(yN_E)\right), \tag{16}$$

where $h_E(x, \mathbb{Q})$ is as introduced in (1),

$$\mathcal{N}(x, y) = \frac{1}{2} \sum_{m \le y} \mu(m)\pi_{D_{m^2}}(x),$$

and

$$\mathcal{M}(x, y, 2\sqrt{x}) = O\left(\sum_{y < m \le 2\sqrt{x}} \#\{p \le x \mid p \nmid mN_E, a_p \ne 0, m^2 \mid |\bar{E}(\mathbb{F}_p)|\}\right).$$

In addition, we can consider a finer splitting

$$h_E(x, \mathbb{Q}) = \mathcal{N}(x, y) + \mathcal{N}_0(x, y, x^\theta) + \mathcal{M}(x, x^\theta, 2\sqrt{x}) + O\left(\frac{x^{\frac{1}{2}+\theta}}{\log x} + x^\theta \log(N_E x)\right), \tag{17}$$

for $\theta \in (0, \frac{1}{4})$, where

$$\mathcal{N}_0(x, y, x^\theta) = O\left(\sum_{y < m \le x^\theta} \mu(m)^2 \pi_{D_{m^2}}(x)\right). \tag{18}$$

On the other hand, reasoning similarly, we also have

$$h_E(x, h, \mathbb{Q}) = \mathcal{N}(x, h, y) + \mathcal{M}(x, h, y, 2\sqrt{x}) + O\left(\frac{\sqrt{x}y}{\log x} + y \log(yN_E)\right),$$

where $h_E(x, h, \mathbb{Q})$ is defined in (10),

$$\mathcal{N}(x, h, y) = \frac{1}{2} \sum_{m \le y} \mu(m)\#\{\mathfrak{p} \subset \mathcal{O}_K \mid x < N(\mathfrak{p}) \le x + h, \mathfrak{p} \nmid mN_E, \sigma_{\mathfrak{p}} \subseteq D_{m^2}\},$$

and

$$\mathcal{M}(x, h, y, 2\sqrt{x+h})$$
$$= O\left(\sum_{y < m \le 2\sqrt{x+h}} \#\{x < p \le x + h \mid p \nmid mN_E, a_p \ne 0, m^2 \mid |\bar{E}(\mathbb{F}_p)|\}\right).$$

To establish asymptotic formulae for $h_E(x, \mathbb{Q})$ and $h_E(x, h, \mathbb{Q})$, it is crucial to analyse $\mathcal{N}(x, y)$ and $\mathcal{N}(x, h, y)$, respectively. In [5], Cojocaru applied effective versions of the Chebotarev density theorem established in [13, 16] to handle $h_E(x, \mathbb{Q})$. Under GRH, the effective version due to Murty et al. [16] provides a satisfactory error term. In contrast, the unconditional result obtained by Lagarias and Odlyzko gives a much weaker estimate, which led Cojocaru to use a more delicate sieve argument. In light of the works of Akbary

and Murty [1] and Murty [15], we observe that the Chebotarev conditions involved (i.e., $\sigma_{\mathfrak{p}} \subseteq D_{m^2}$) can be further translated into congruence conditions over certain ray class groups via Artin reciprocity (see Sect. 3 for more details). This observation hints at using the following Bombieri–Vinogradov theorem for number fields and its short interval variant. As shall be seen, such a Bombieri–Vinogradov theorem for number fields will play a crucial role in improving Cojocaru's estimate (2).

Let F be a number field, and let $\mathfrak{a}$ and $\mathfrak{q}$ be integral ideals of F. For any $(\mathfrak{a}, \mathfrak{q}) = 1$, we set

$$\pi(x, \mathfrak{q}, \mathfrak{a}) = \#\{\mathfrak{p} \subset \mathcal{O}_F \mid N(\mathfrak{p}) \le x \text{ and } \mathfrak{p} \sim \mathfrak{a}(\text{mod } \mathfrak{q})\},$$

where $\mathfrak{p} \sim \mathfrak{a}$ (mod $\mathfrak{q}$) means that $\mathfrak{p}$ and $\mathfrak{a}$ belong to the same ray class of the ray class group modulo $\mathfrak{q}$. (For the background on ray class groups, we refer the reader to [3, Ch. 3].) In [10], Huxley proved the following Bombieri–Vinogradov theorem for number fields, which improves the previous result of Wilson [17].

Theorem 4 (Huxley) *Let F be a number field. Then for any $A > 0$, there is $B = B(A) > 0$ such that for $Q \le x^{1/2}/(\log x)^B$, one has*

$$\sum_{N(\mathfrak{q}) \le Q} \frac{h(\mathfrak{q})}{\phi(\mathfrak{q})} \max_{(\mathfrak{a}, \mathfrak{q})=1} \max_{y \le x} \left| \pi(y, \mathfrak{q}, \mathfrak{a}) - \frac{1}{h(\mathfrak{q})} \text{Li}(y) \right| \ll_{F,A} \frac{x}{(\log x)^A},$$

where $h(\mathfrak{q})$ is the cardinality of the ray class group modulo $\mathfrak{q}$, and $\phi(\mathfrak{q})$ is the number field analogue of Euler's totient function for F.

Also, we recall the following short interval variant established by the present author in [18].

Theorem 5 *Let F be a number field of degree n_F. For $0 \le \delta < \frac{2}{5n_F}$, fix $0 \le \theta < \frac{1}{5n_F + 10}(2 - 5n_F \delta)$. Then for any $x^{1-\delta} \le h \le x$ and $A > 0$, we have*

$$\sum_{N(\mathfrak{q}) \le x^\theta} \frac{h(\mathfrak{q})}{\phi(\mathfrak{q})} \max_{(\mathfrak{a}, \mathfrak{q})=1} \left| \pi(x+h, \mathfrak{q}, \mathfrak{a}) - \pi(x, \mathfrak{q}, \mathfrak{a}) - \frac{\text{Li}(x+h) - \text{Li}(x)}{h(\mathfrak{q})} \right| \ll \frac{h}{(\log x)^A},$$

where the implied constant depends on F and A.

In our consideration, we will take $F = K$, an imaginary quadratic field of class number one associated to a CM elliptic curve E as discussed in the introduction. For such an instance, the factor $\frac{h(\mathfrak{q})}{\phi(\mathfrak{q})}$ can be dropped from the estimates in Theorems 4 and 5 as follows. Let h_F denote the class number of F and r_1 be the number of real embeddings of F. It is known that

$$h(\mathfrak{q}) = \frac{h_F 2^{r_1} \phi(\mathfrak{q})}{T(\mathfrak{q})},$$

where $T(\mathfrak{q})$ is the number of residue classes (mod $\mathfrak{q}$) that contain a unit (see [17, Eq. (7)]). Now, for imaginary quadratic fields of class number one, it is known that $T(\mathfrak{q}) \le 6$, and hence $\frac{h(\mathfrak{q})}{\phi(\mathfrak{q})} \ge \frac{1}{6}$. Thus, the factor $\frac{h(\mathfrak{q})}{\phi(\mathfrak{q})}$ can be removed.

Secondly, we shall control $\mathcal{M}(x, y, 2\sqrt{x})$ and $\mathcal{M}(x, h, y, 2\sqrt{x+h})$ by the sieve methods used by Cojocaru [5]. As remarked by Cojocaru, the difficulties of the proofs lie in analysing $\mathcal{M}(x, y, 2\sqrt{x})$ and $\mathcal{M}(x, h, y, 2\sqrt{x+h})$ since the classical Brun-Titchmarsh inequality is not strong enough. Consequently, similar to the argument in [5, Sec. 5], we will require a Brun-Titchmarsh type estimate for short intervals in Sect. 4.

Last but not least, we remark that instead of directly following Cojocaru's argument to control $\mathcal{N}_0(x, y, x^\theta)$, one can derive a refined estimate for this range by applying the following

number field analogue of the Brun–Titchmarsh inequality established by Hinz and Lodemann [9, Theorem 4].

Theorem 6 (Hinz–Lodemann) *In the above notation, for any* $(\mathfrak{a}, \mathfrak{q}) = 1$, *if* $N(\mathfrak{q}) < x$, *then*

$$\pi(x, \mathfrak{q}, \mathfrak{a}) \leq \frac{2x}{h(\mathfrak{q}) \log(x/N(\mathfrak{q}))} \cdot \left(1 + O\left(\frac{\log \log(3x/N(\mathfrak{q}))}{\log(x/N(\mathfrak{q}))}\right)\right).$$

3 Proof of Theorem 1

3.1 Proof of the first part of Theorem 1

Recall that by the theory of complex multiplication, Murty [15, Lemma 4] showed that there exists an integral ideal $\mathfrak{f} = \mathfrak{f}_E$ of $\mathcal{O}_K$ such that

$$K_{\mathfrak{m}} \subseteq K(E[m]) \subseteq K_{\mathfrak{f}\mathfrak{m}},$$

where $K_{\mathfrak{m}}$ (resp., $K_{\mathfrak{f}\mathfrak{m}}$) is the ray class field of K of level $\mathfrak{m} = m\mathcal{O}_K$ (resp., $\mathfrak{f}\mathfrak{m}$). Moreover, as remarked in [1] (see also [15, p, 163]), $\mathfrak{f}$ above can be taken as the conductor of the Hecke character associated with E, and thus $N_E = N(\mathfrak{f})d_K$, where d_K is the absolute discriminant of K. In particular, we have $\phi(\mathfrak{f}) \leq N(\mathfrak{f}) \leq N_E$.

Now, we let $\tilde{D}_{m^2}$ stand for the preimage of D_{m^2} under the quotient map from $\mathrm{Gal}(K_{\mathfrak{f}\mathfrak{m}^2}/K)$ to $\mathrm{Gal}(K(E[m^2])/K)$. As $\tilde{D}_{m^2}$ is a conjugacy set in $\mathrm{Gal}(K_{\mathfrak{f}\mathfrak{m}^2}/K)$, we can let $\pi_{\tilde{D}_{m^2}}(x)$ denote the number of unramified primes $\mathfrak{p}$ in $K_{\mathfrak{f}\mathfrak{m}^2}/K$ such that $N(\mathfrak{p}) \leq x$ and the Artin symbol $\tilde{\sigma}_{\mathfrak{p}}$ at $\mathfrak{p}$ is contained in $\tilde{D}_{m^2}$. It is known that

$$\pi_{D_{m^2}}(x) = \pi_{\tilde{D}_{m^2}}(x) + O\left(\frac{\log d_{K_{\mathfrak{f}\mathfrak{m}^2}}}{[K_{\mathfrak{f}\mathfrak{m}^2} : K]}\right), \tag{19}$$

where $\pi_{D_{m^2}}(x)$ is defined as in (15) (see, e.g., [16, p. 268]). Recall that by Hensel's bound (see, e.g., [5, Lemma 3.4]), for any Galois extension L/K of number fields, one has

$$\log d_L \leq [L : K] \log d_K + n_L \sum_p \log p + n_L \log[L : K],$$

where for a number field F, d_F and n_F denote its absolute discriminant and degree, respectively, and the sum is over the primes p lying below primes of K that ramify in L/K. Thus, applying the above inequality with $L = K_{\mathfrak{f}\mathfrak{m}^2}$, we have

$$\frac{\log d_{K_{\mathfrak{f}\mathfrak{m}^2}}}{[K_{\mathfrak{f}\mathfrak{m}^2} : K]} \leq \log d_K + n_K \log N(\mathfrak{f}\mathfrak{m}^2) + n_K \log[K_{\mathfrak{f}\mathfrak{m}^2} : K] \leq \log d_K + 4 \log N(\mathfrak{f}\mathfrak{m}^2)$$

as $n_K = 2$ and $[K_{\mathfrak{f}\mathfrak{m}^2} : K] \leq h(\mathfrak{f}\mathfrak{m}^2) \leq 1 \cdot 2^0 \cdot \phi(\mathfrak{f}\mathfrak{m}^2) \leq N(\mathfrak{f}\mathfrak{m}^2)$. Hence, we arrive at

$$\frac{\log d_{K_{\mathfrak{f}\mathfrak{m}^2}}}{[K_{\mathfrak{f}\mathfrak{m}^2} : K]} \ll_K \log N(\mathfrak{f}\mathfrak{m}^2). \tag{20}$$

Moreover, by Artin reciprocity (see, e.g., [3, Ch. 3 and 5]), there are $u(m^2)$ ray classes $\mathfrak{m}_i$ modulo $\mathfrak{f}\mathfrak{m}^2$ so that

$$\pi_{\tilde{D}_{m^2}}(x) = \sum_{i=1}^{u(m^2)} \pi(x, \mathfrak{f}\mathfrak{m}^2, \mathfrak{m}_i), \tag{21}$$

where $u(m^2) \leq h(\mathfrak{f}m^2) \leq N(\mathfrak{f}m^2)$. It then follows from the Chebotarev density theorem and the prime ideal theorem for ray classes that

$$\frac{|D_{m^2}|}{[K(E[m^2]):K]} = \frac{|\tilde{D}_{m^2}|}{[K_{\mathfrak{f}m^2}:K]} = \frac{u(m^2)}{h(\mathfrak{f}m^2)}. \tag{22}$$

We are now in a position to estimate $\mathcal{N}(x, y)$. Choosing $y = z/N(\mathfrak{f})^{1/4}$, we write

$$
\begin{aligned}
\mathcal{N}(x, y) &= \frac{1}{2} \sum_{m \leq z/N(\mathfrak{f})^{1/4}} \mu(m) \pi_{D_{m^2}}(x) \\
&= \frac{1}{2} \sum_{m \leq z/N(\mathfrak{f})^{1/4}} \mu(m) \frac{|D_{m^2}| \operatorname{Li}(x)}{[K(E[m^2]):K]} + \frac{1}{2} \sum_{m \leq z/N(\mathfrak{f})^{1/4}} \mu(m) \mathcal{E}(x, m^2),
\end{aligned}
\tag{23}
$$

where

$$\mathcal{E}(x, m^2) = \pi_{D_{m^2}}(x) - \frac{|D_{m^2}| \operatorname{Li}(x)}{[K(E[m^2]):K]}.$$

By (19), (20), (21), and (22), we have

$$
\begin{aligned}
\mathcal{E}(x, m^2) &= \pi_{\tilde{D}_{m^2}}(x) - \frac{|\tilde{D}_{m^2}| \operatorname{Li}(x)}{[K_{\mathfrak{f}m^2}:K]} + O(\log N(\mathfrak{f}m^2)) \\
&= \sum_{i=1}^{u(m^2)} \left(\pi(x, \mathfrak{f}m^2, \mathfrak{m}_i) - \frac{\operatorname{Li}(x)}{h(\mathfrak{f}m^2)} \right) + O(\log N(\mathfrak{f}m^2)).
\end{aligned}
$$

Therefore, by Theorem 4, together with the discussion beneath Theorem 5, for $z^4 \leq x^{1/2-\epsilon}$ and $A > 0$, we have

$$
\begin{aligned}
\sum_{m \leq z/N(\mathfrak{f})^{1/4}} &\left| \mathcal{E}(x, m^2) \right| \\
&\ll \sum_{N(\mathfrak{f}m^2) \leq z^4} \left(\sum_{i=1}^{u(m^2)} \left| \pi(x, \mathfrak{f}m^2, \mathfrak{m}_i) - \frac{\operatorname{Li}(x)}{h(\mathfrak{f}m^2)} \right| + \log N(\mathfrak{f}m^2) \right) \\
&\ll \sum_{N(\mathfrak{f}m^2) \leq z^4} u(m^2) \max_{1 \leq i \leq u(m^2)} \left| \pi(x, \mathfrak{f}m^2, \mathfrak{m}_i) - \frac{\operatorname{Li}(x)}{h(\mathfrak{f}m^2)} \right| + z^4 \log x \\
&\ll z^4 \sum_{N(\mathfrak{q}) \leq z^4} \max_{(\mathfrak{a}, \mathfrak{q})=1} \left| \pi(x, \mathfrak{q}, \mathfrak{a}) - \frac{\operatorname{Li}(x)}{h(\mathfrak{q})} \right| + z^4 \log x \\
&\ll_A \frac{x z^4}{(\log x)^{5A+12}}
\end{aligned}
\tag{24}
$$

as $u(m^2) \leq N(\mathfrak{f}m^2)$. Since there are only nine imaginary quadratic fields K of class number one, we can make the implied constant independent of K.

By [5, Eq. (36)], one has

$$\mathcal{M}(x, y, 2\sqrt{x}) \ll \frac{x}{y}(\log x)^3 + \sqrt{x}(\log x)^4. \tag{25}$$

Also, by [5, Eq. (39)], one knows

$$\sum_{m > y} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]):K]} \operatorname{Li}(x) \ll \frac{x \log y}{y \log x}.$$

As $y = z/\mathrm{N}(\mathfrak{f})^{1/4}$ and $\mathrm{N}(\mathfrak{f}) \leq N_E$, the above two estimates, together with (16), (23), and (24), then give

$$h_E(x, \mathbb{Q}) = \frac{1}{2} \sum_{m=1}^{\infty} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]) : K]} \mathrm{Li}(x) + O_A\left(N_E \frac{xy^4}{(\log x)^{5A+12}}\right)$$
$$+ O\left(\frac{x}{y}(\log x)^3 + \sqrt{x}(\log x)^4 + \frac{x \log y}{y \log x} + \frac{\sqrt{x}y}{\log x} + y \log(yN_E)\right).$$

Finally, choosing $y = (\log x)^{A+3}$, we conclude that for any $A > 0$,

$$h_E(x, \mathbb{Q}) = \frac{1}{2} \sum_{m=1}^{\infty} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]) : K]} \mathrm{Li}(x) + O_A\left(N_E \frac{x}{(\log x)^A}\right),$$

which, together with the identity

$$\frac{1}{2} \sum_{m=1}^{\infty} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]) : K]} = \frac{1}{2} \sum_{\mathfrak{a}, m} \frac{\mu(\mathfrak{a})\mu(m)}{[K(E[\mathfrak{a}^2])K(E[m]) : K]} \tag{26}$$

(see [5, Eq. (11) and (40)]), yields the claimed asymptotic formula (5).

3.2 Proof of the second part of Theorem 1

The proof of (6) follows closely Cojocaru's argument. The main difference lies in bounding $\mathcal{N}_0(x, y, x^\theta)$ by Theorem 6, the Brun-Titchmarsh inequality for number fields due to Hinz and Lodemann.

We begin by recalling that as $K(E[m^2])/K$ is an abelian Galois extension, Artin's (holomorphy) conjecture is proven for this case. Applying the effective Chebotarev density theorem established by Murty et al. [16], Cojocaru [5, Eq. (34)] derived that

$$\mathcal{N}(x, y) = \frac{1}{2} \sum_{m \leq y} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]) : K]} \mathrm{Li}(x) + O(y^2 x^{1/2} \log(N_E x)),$$

for $y \leq 2\sqrt{x}$, under GRH. Hence, by (26), one knows

$$\mathcal{N}(x, y) = \delta_E \mathrm{Li}(x) + O(y^2 x^{1/2} \log(N_E x)) - \frac{1}{2} \sum_{m > y} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]) : K]} \mathrm{Li}(x). \tag{27}$$

In [5, Lemma 3.12], Cojocaru showed that $|D_{q^2}| \leq q^2$ for any odd prime q that is unramified in K. From this, she deduced in [5, Corollary 3.13] that $|D_{m^2}| \leq m^2$ for any odd positive square-free integer m composed of primes which are unramified in K. We remark that this bound can be extended to all square-free integers $m > 1$ so that $|D_{m^2}| \ll m^2$ as follows.[2] Observe that for any prime ℓ that is even or ramifies in K, we always have

$$|D_{\ell^2}| \leq |\mathrm{Gal}(K(E[\ell^2])/K)| \ll \ell^4.$$

As only finitely many primes ramify in K, we can write this bound as $|D_{\ell^2}| \ll_K 1$. In addition, since K must be one of nine imaginary quadratic fields of class number one, we deduce that $|D_{\ell^2}|$ is absolutely bounded (i.e. $|D_{\ell^2}| \ll 1$) for any prime ℓ that is even or ramifies in K.

---

[2] In fact, such an extension has been used implicitly in [5, Eq. (34) and (39)].

This, combined with the above-mentioned result of Cojocaru, yields $|D_{m^2}| \ll m^2$ for any square-free integer $m > 1$. As a direct consequence, we have

$$\sum_{m>y} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]):K]} \ll \sum_{m>y} \frac{\mu(m)^2|D_{m^2}|}{[K(E[m^2]):K]} \ll \sum_{m>y} \frac{m^2}{\phi(m^2)^2} = \sum_{m>y} \frac{1}{\phi(m)^2} \ll \frac{1}{y},$$

(28)

where we used the bound $[K(E[k]):K] \gg \phi(k)^2$ for any integer $k \geq 3$ (see, e.g., [5, Eq. (19)]). Hence, the last sum in (27) is $\ll \frac{x}{y \log x}$ (cf. [5, Eq. (39)]).

Now, we shall estimate $\mathcal{N}_0(x, y, x^\theta)$ introduced as in (18) with $y \leq x^\theta$ and $\theta \in (0, \frac{1}{4})$. To do so, it suffices to bound

$$\sum_{y<m\leq x^\theta} \mu(m)^2 \pi_{D_{m^2}}(x).$$

It follows from (19), (20), and (21), this sum is

$$\sum_{y<m\leq x^\theta} \mu(m)^2 \sum_{i=1}^{u(m^2)} \pi(x, \mathfrak{f}\mathfrak{m}^2, \mathfrak{m}_i) + O(x^\theta \log(N_E x)).$$

Moreover, applying Theorem 6, when $N_E \leq x^{1-4\theta-\epsilon}$ (so that $\mathrm{N}(\mathfrak{f}\mathfrak{m}^2) \leq N_E m^4 \leq x^{1-\epsilon}$ for $m \leq x^\theta$), we can bound the double sum above by

$$\ll_\epsilon \sum_{y<m\leq x^\theta} \mu(m)^2 \sum_{i=1}^{u(m^2)} \frac{x}{h(\mathfrak{f}\mathfrak{m}^2) \log x} = \sum_{y<m\leq x^\theta} \frac{\mu(m)^2|D_{m^2}|}{[K(E[m^2]):K]} \frac{x}{\log x},$$

where the equality is due to (22). Therefore, by (28), we deduce that

$$\mathcal{N}_0(x, y, x^\theta) \ll_\epsilon \frac{x}{y \log x} + x^{\frac{1}{4}} \ll \frac{x}{y \log x}$$

upon recalling the assumption that $y < x^\theta$ with $\theta \in (0, \frac{1}{4})$. As (25) gives

$$\mathcal{M}(x, x^\theta, 2\sqrt{x}) = \frac{x}{x^\theta}(\log x)^3 + \sqrt{x}(\log x)^4,$$

we then arrive at

$$h_E(x, \mathbb{Q}) = \delta_E \, \mathrm{Li}(x) + O_\epsilon\left(y^2 x^{1/2} \log(N_E x) + \frac{x}{y \log x} + \frac{x}{x^\theta}(\log x)^3 + \sqrt{x}(\log x)^4\right).$$

Therefore, choosing $\theta = \frac{1}{6} + \epsilon$ and

$$y = \frac{x^{1/6}}{(\log x)^{1/3}(\log(N_E x))^{1/3}},$$

we obtain

$$h_E(x, \mathbb{Q}) = \delta_E \, \mathrm{Li}(x) + O_\epsilon\left(x^{5/6}\frac{(\log(N_E x))^{1/3}}{(\log x)^{2/3}}\right)$$

whenever $N_E \leq x^{1-\frac{4}{6}-5\epsilon}$, as desired.

4 Proof of Theorem 2

We start by setting $y = z/N(\mathfrak{f})^{1/4}$ and writing

$$\mathcal{N}(x, h, y) = \frac{1}{2} \sum_{m \leq z/N(\mathfrak{f})^{1/4}} \mu(m)(\pi_{D_{m^2}}(x + h) - \pi_{D_{m^2}}(x))$$

$$= \frac{1}{2} \sum_{m \leq z/N(\mathfrak{f})^{1/4}} \mu(m) \frac{|D_{m^2}|(\mathrm{Li}(x + h) - \mathrm{Li}(x))}{[K(E[m^2]) : K]} + \frac{1}{2} \sum_{m \leq z/N(\mathfrak{f})^{1/4}} \mu(m)\tilde{\mathcal{E}}(x, m^2),$$

where

$$\tilde{\mathcal{E}}(x, m^2) = \pi_{D_{m^2}}(x + h) - \pi_{D_{m^2}}(x) - \frac{|D_{m^2}|(\mathrm{Li}(x + h) - \mathrm{Li}(x))}{[K(E[m^2]) : K]}.$$

As argued in Sect. 3, $\tilde{\mathcal{E}}(x, m^2)$ is equal to

$$\pi_{\tilde{D}_{m^2}}(x + h) - \pi_{\tilde{D}_{m^2}}(x) - \frac{|\tilde{D}_{m^2}|(\mathrm{Li}(x + h) - \mathrm{Li}(x))}{[K_{\mathfrak{f}m^2} : K]} + O(\log N(\mathfrak{f}m^2))$$

$$= \sum_{i=1}^{u(m^2)} \left(\pi(x + h, \mathfrak{f}m^2, \mathfrak{m}_i) - \pi(x, \mathfrak{f}m^2, \mathfrak{m}_i) - \frac{\mathrm{Li}(x + h) - \mathrm{Li}(x)}{h(\mathfrak{f}m^2)}\right) + O(\log N(\mathfrak{f}m^2)).$$

Now, for $\delta \in [0, \frac{1}{5})$, $\theta \in (0, \frac{1-5\delta}{10})$, and $z^4 \leq x^\theta$, applying Theorem 5, for any $A > 0$, we derive

$$\sum_{N(\mathfrak{f}m^2) \leq z^4} \sum_{i=1}^{u(m^2)} \left|\pi(x + h, \mathfrak{f}m^2, \mathfrak{m}_i) - \pi(x, \mathfrak{f}m^2, \mathfrak{m}_i) - \frac{\mathrm{Li}(x + h) - \mathrm{Li}(x)}{h(\mathfrak{f}m^2)}\right|$$

$$\ll z^4 \sum_{N(\mathfrak{q}) \leq z^4} \max_{(\mathfrak{a}, \mathfrak{q})=1} \left|\pi(x + h, \mathfrak{q}, \mathfrak{a}) - \pi(x, \mathfrak{q}, \mathfrak{a}) - \frac{\mathrm{Li}(x + h) - \mathrm{Li}(x)}{h(\mathfrak{q})}\right|$$

$$\ll_A N_E \frac{hy^4}{(\log x)^{5A+13}},$$

whenever $x^{1-\delta} \leq h \leq x$. Thus, we arrive at

$$\sum_{m \leq z/N(\mathfrak{f})^{1/4}} |\tilde{\mathcal{E}}(x, m^2)| \ll_A N_E \frac{hy^4}{(\log x)^{5A+12}}.$$

As remarked previously, in order to adapt the sieve method developed by Cojocaru in [5, Sect. 5] (to control $\mathcal{M}(x, y, 2\sqrt{x})$), we shall require a number field analogue of the Brun-Titchmarsh inequality as follows. Assume $K = \mathbb{Q}(\sqrt{-D})$. For an ordinary prime $p \nmid 6N_E$, we write $p\mathcal{O}_K = (\pi_p)(\bar{\pi}_p)$ and note that $N(\pi_p) = p$. Observe that

$$(\sqrt{x} - 1)^2 < (\sqrt{p} - 1)^2 \leq N(\pi_p - 1) \leq (\sqrt{p} + 1)^2 \leq (\sqrt{x + h} + 1)^2 \qquad (29)$$

for $x < p \leq x + h$. Following Cojocaru [5], we shall use the decomposition $m = m_i m_r m_s$, where m_i is composed of primes inert in K, m_r is composed of primes ramifying in K, and m_s is composed of primes splitting completely in K. It follows from [5, Lemma 3.17] that for any square-free $m \in \mathbb{N}$ such that m^2 divides $|\bar{E}(\mathbb{F}_p)|$ for some ordinary prime p, one knows

$$(\pi_p - 1) = m_i m_r I(m_s) \cdot (\alpha) \qquad (30)$$

for some $\alpha \in \mathcal{O}_K$. Here, $I(k_s)$ is an ideal in $\mathcal{O}_K$ obtained from the product of the ideals $\mathfrak{q}\bar{\mathfrak{q}}$, $\mathfrak{q}^2$, or $\bar{\mathfrak{q}}^2$ in accordance to whether π_p splits completely in $K(E[\mathfrak{q}\bar{\mathfrak{q}}])$, $K(E[\mathfrak{q}^2])$, or $K(E[\bar{\mathfrak{q}}^2])$, respectively, while $\mathfrak{q}$ runs over the primes of K above prime divisors q of m_s. (As remarked in [5, p. 610], there are $3^{\nu(m_s)}$ possibilities of such ideals $I(k_s)$.) Hence, for $x < p \leq x + h$, by (29) and (30), we have

$$\frac{(\sqrt{x} - 1)^2}{m^2} \leq \mathrm{N}(\alpha) = \frac{\mathrm{N}(\pi_p - 1)}{\mathrm{N}(m_i m_r I(m_s))} \leq \frac{(\sqrt{x+h} + 1)^2}{m^2}.$$

The number of such α is

$$\ll \left(\frac{\sqrt{x+h} - \sqrt{x} + 2}{m} + 1 \right) \left(\frac{\sqrt{x+h} - \sqrt{x} + 2}{m\sqrt{D}} + 1 \right) \ll \left(\frac{\sqrt{x+h} - \sqrt{x}}{m} + 1 \right)^2,$$

which is

$$\ll \frac{h}{m^2} + \frac{\sqrt{x+h}}{m}$$

for $m \leq 2\sqrt{x+h}$. (Here, we used $(\sqrt{x+h} - \sqrt{x})^2 = h + 2(x - \sqrt{x+h}\sqrt{x}) \ll h$. Note that if x/h tends to ∞ as $x \to \infty$, we have

$$\lim_{x \to \infty} \frac{x - \sqrt{x+h}\sqrt{x}}{h} = \lim_{v \to \infty} v\left(1 - \sqrt{1 + \frac{1}{v}}\right) = \lim_{w \to 0} \frac{1 - \sqrt{1+w}}{w} = -\frac{1}{2},$$

where the last equality is due to l'Hôpital's rule.)

Processing an argument similar to [5, Eq. (36)], we have

$$\mathcal{M}(x, h, y, 2\sqrt{x+h}) \leq \sum_{\substack{y < m \leq 2\sqrt{x+h} \\ m \text{ square-free} \\ m = m_i m_r m_s}} \sum_{\substack{x < p \leq x + h \\ a_p \neq 0 \\ (\pi_p - 1) = m_i m_r I(m_s) \cdot (\alpha)}} 1$$

$$\ll \sum_{\substack{y < m \leq 2\sqrt{x+h} \\ m \text{ square-free} \\ m = m_i m_r m_s}} 3^{\nu(m_s)} \left(\frac{h}{m_i^2 m_r^2 m_s^2} + \frac{\sqrt{x}}{m_i m_r m_s} \right) \tag{31}$$

$$\ll \sum_{m_s \leq 2\sqrt{x+h}} \sum_{\frac{y}{m_s} < \tilde{m} \leq 2\sqrt{x+h}} 3^{\nu(m_s)} \left(\frac{h}{\tilde{m}^2 m_s^2} + \frac{\sqrt{x}}{\tilde{m} m_s} \right)$$

$$\ll \sum_{m_s \leq 2\sqrt{x+h}} 3^{\nu(m_s)} \left(\frac{h}{y m_s} + \frac{\sqrt{x}}{m_s} \log x \right)$$

$$\ll \frac{h}{y}(\log x)^3 + \sqrt{x}(\log x)^4,$$

where the last bound follows from the elementary estimates $\sum_{m \leq x} \frac{1}{m} = \log x + O(1)$ and

$$\sum_{m \leq x} 3^{\nu(m)} \ll x(\log x)^2.$$

Also, as in [5, Eq. (39)], it can be checked that

$$\sum_{m > y} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]) : K]}(\mathrm{Li}(x + h) - \mathrm{Li}(x)) \ll \frac{h \log y}{y \log x}.$$

Now, gathering everything together, we deduce

$$h_E(x, h, \mathbb{Q}) = \frac{1}{2} \sum_{m=1}^{\infty} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]) : K]} (\mathrm{Li}(x + h) - \mathrm{Li}(x)) + O_A\left(N_E \frac{hy^4}{(\log x)^{5A+12}}\right)$$
$$+ O\left(\frac{h}{y}(\log x)^3 + \sqrt{x}(\log x)^4 + \frac{h \log y}{y \log x} + \frac{\sqrt{x}y}{\log x} + y \log(yN_E)\right).$$

Finally, choosing $y = (\log x)^{A+3}$, we conclude that for any $A > 0$,

$$h_E(x, h, \mathbb{Q}) = \frac{1}{2} \sum_{m=1}^{\infty} \frac{\mu(m)|D_{m^2}|}{[K(E[m^2]) : K]} (\mathrm{Li}(x + h) - \mathrm{Li}(x)) + O_A\left(N_E \frac{h}{(\log x)^A}\right)$$

whenever $x^{1-\delta} \le h \le x$ with $\delta < \frac{1}{5}$. Recalling the identity (26), we conclude the proof.

5 Proof of Theorem 3

Following [15, Sec. 3], by an application of the inclusion–exclusion principle, one has

$$\pi_c(x, E) = \#\{p \le x \mid p \nmid N_E \text{ and } \bar{E}(\mathbb{F}_p) \text{ is cyclic}\} = \sum_{m=1}^{2\sqrt{x}} \mu(m)\pi_E(x, m),$$

where $\pi_E(x, m)$ denotes the number of primes $p \le x$ such that $p \nmid N_E$ splits completely in $\mathbb{Q}(E[m])$.

In [18, Sec. 4], the present author used the estimate

$$\pi_E(x, m) \ll \frac{x}{m^2} \tag{32}$$

(for square-free $3 \le m \le 2\sqrt{x}$) to obtain

$$\sum_{z/\mathrm{N}(\mathfrak{f})^{1/2} \le m \le 2\sqrt{x+h}} \pi_E(x + h, m) - \pi_E(x, m) \ll \sum_{z/\mathrm{N}(\mathfrak{f})^{1/2} \le m \le 2\sqrt{x+h}} \frac{x}{m^2} \ll N_E^{1/2}\frac{x}{z}. \tag{33}$$

The key to proving Theorem 3 is to improve (32) (and thus (33)) as follows. Observe

$$\pi_E(x + h, m) - \pi_E(x, m)$$
$$\le \#\{\pi_p \in \mathcal{O}_K \mid p \nmid N_E, x < \mathrm{N}(\pi_p) = p \le x + h, \pi_p \equiv 1 (\mathrm{mod}\, m\mathcal{O}_K)\} + 2. \tag{34}$$

(Here, we use the fact that for square-free $m \ge 3$, if $p \nmid 6N_E$ splits completely in $\mathbb{Q}(E[m])$, then $p\mathcal{O}_K = (\pi_p)(\bar{\pi}_p)$ and $\pi_p \equiv 1 (\mathrm{mod}\, m\mathcal{O}_K)$. See [1, Lemmata 2.4 and 2.5].) Now, for $3 \le m \le \sqrt{x + h}$, if $x < \mathrm{N}(\pi_p) = p \le x + h$ and

$$(\pi_p - 1) = m \cdot (\alpha)$$

for some $\alpha \in \mathcal{O}_K$, then it follows from (29) that

$$\frac{(\sqrt{x} - 1)^2}{m^2} \le \mathrm{N}(\alpha) = \frac{\mathrm{N}(\pi_p - 1)}{\mathrm{N}(m)} \le \frac{(\sqrt{x + h} + 1)^2}{m^2}.$$

As shown in the previous section, the number of such α is $\ll \frac{h}{m^2} + \frac{\sqrt{x+h}}{m}$. Hence, by (34), for $3 \le m \le 2\sqrt{x + h}$, we deduce

$$\pi_E(x + h, m) - \pi_E(x, m) \ll \frac{h}{m^2} + \frac{\sqrt{x + h}}{m}. \tag{35}$$

This leads us to

$$\pi_c(x + h, E) - \pi_c(x, E) = \sum_{1 \le m \le z/\mathrm{N}(\mathfrak{f})^{1/2}} \mu(m)(\pi_E(x + h, m) - \pi_E(x, m))$$
$$+ O(N_E^{1/2} h z^{-1} + \sqrt{x} \log x).$$

Now, controlling the range $1 \le m \le z/\mathrm{N}(\mathfrak{f})^{1/2}$ as in [18, Eq. (4.2)-(4.4)], we see that $\pi_c(x + h, E) - \pi_c(x, E)$ equals

$$\sum_{1 \le m \le z/\mathrm{N}(\mathfrak{f})^{1/2}} \frac{\mu(m)}{n(m)}(\mathrm{Li}(x + h) - \mathrm{Li}(x))$$
$$+ O\left(N_E^{1/2} h z^{-1} + \sqrt{x} \log x + N_E(\log N_E)\frac{h}{(\log x)^A} + \frac{\sqrt{x}z}{\log x} + (\log N_E)z\right),$$

where $n(m)$ denotes the degree of $\mathbb{Q}(E[m])$, and the implied constant depends on $\mathbb{Q}(E[2])$ and A, whenever $z^2 \le x^\theta$ and $x^{1-\delta} \le h \le x$ with $0 \le \theta < \frac{1}{10}(1 - 5\delta)$ and $0 \le \delta < \frac{1}{5}$.

Finally, from the last paragraph of [18, Sec. 4], we know

$$\sum_{m > z/\mathrm{N}(\mathfrak{f})^{1/2}} \frac{\mu(m)}{n(m)}(\mathrm{Li}(x + h) - \mathrm{Li}(x)) \ll \frac{N_E^{1/2} h}{z}.$$

Hence, for any $0 \le \delta < \frac{1}{5}$ and $x^{1-\delta} \le h \le x$, balancing the errors, we obtain

$$\pi_c(x + h, E) - \pi_c(x, E) = \mathfrak{c}_E(\mathrm{Li}(x + h) - \mathrm{Li}(x)) + O\left(N_E(\log N_E)\frac{h}{(\log x)^A}\right),$$

which completes the proof.

Data availability The author does not analyse or generate any datasets, as the present article proceeds on purely mathematical grounds.

References

1. Akbary, A., Murty, V.K.: An analogue of the Siegel–Walfisz theorem for the cyclicity of CM elliptic curves mod p. Indian J. Pure Appl. Math. **41**, 25–37 (2010)
2. Akhtari, S., David, C., Hahn, H., Thompson, L.: Distribution of squarefree values of sequences associated with elliptic curves, Women in numbers 2: research directions in number theory. In: Contemp. Math., 606, Centre Rech. Math. Proc., pp. 171–188. Amer. Math. Soc., Providence (2013)
3. Childress, N.: Class Field Theory. Universitext, Springer, New York (2009)
4. Cojocaru, A.C.: Cyclicity of elliptic curves modulo p. Ph.D. thesis, Queen's University, Canada (2002)
5. Cojocaru, A.C.: Square-free orders for CM elliptic curves modulo p. Math. Ann. **342**, 587–615 (2008)
6. Cojocaru, A.C., Murty, M.R.: Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem. Math. Ann. **330**, 601–625 (2004)
7. Deuring, M.: Die typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hansischen Univ. **14**, 197–272 (1941)
8. Gekeler, E.-U.: Statistics about elliptic curves over finite prime fields. Manuscripta Math. **127**, 55–67 (2008)

9. Hinz, J., Lodemann, M.: On Siegel zeros of Hecke–Landau zeta-functions. Mh. Math. **118**, 231–248 (1994)
10. Huxley, M.N.: The large sieve inequality for algebraic number fields III. Zero-density results. J. Lond. Math. Soc. **3**, 233–240 (1971)
11. Huxley, M.N.: On the difference between consecutive primes. Invent. Math. **15**, 164–170 (1972)
12. Koblitz, N.: Primality of the number of points on an elliptic curve over a finite field. Pac. J. Math. **131**, 157–165 (1988)
13. Lagarias, J.C., Odlyzko, A.M.: Effective versions of the Chebotarev density theorem. In: Algebraic Number Fields: L-functions and Galois Properties (Durham, 1975), pp. 409–464. Academic Press, London (1977)
14. Lang, S., Trotter, H.: Primitive points on elliptic curves. Bull. Am. Math. Soc. **83**, 289–292 (1977)
15. Murty, M.R.: On Artin's conjecture. J. Number Theory **16**, 147–168 (1983)
16. Murty, M.R., Murty, V.K., Saradha, N.: Modular forms and the Chebotarev density theorem. Am. J. Math. **110**, 253–281 (1988)
17. Wilson, R.J.: The large sieve in algebraic number fields. Mathematika **16**, 189–204 (1969)
18. Wong, P.-J.: Cyclicity and exponents of CM elliptic curves modulo p in short intervals. Trans. Am. Math. Soc. **373**, 8725–8749 (2020)