ON THE AVERAGE EXPONENT OF ELLIPTIC CURVES MODULO p

TRISTAN FREIBERG AND PÄR KURLBERG

Abstract. Given an elliptic curve E defined over $\mathbb{Q}$ and a prime p of good reduction, let $\tilde{E}(\mathbb{F}_p)$ denote the group of $\mathbb{F}_p$-points of the reduction of E modulo p, and let e_p denote the exponent of said group. Assuming a certain form of the Generalized Riemann Hypothesis (GRH), we study the average of e_p as $p \leqslant X$ ranges over primes of good reduction, and find that the average exponent essentially equals $p \cdot c_E$, where the constant $c_E > 0$ depends on E. For E without complex multiplication (CM), c_E can be written as a rational number (depending on E) times a universal constant, $c := \prod_q \left(1 - \frac{q^3}{(q^2-1)(q^5-1)}\right)$, the product being over all primes q. Without assuming GRH, we can determine the average exponent when E has CM, as well as give an upper bound on the average in the non-CM case.

1. Introduction

Given an elliptic curve E defined over $\mathbb{Q}$, and a prime p for which E has good reduction, let $\tilde{E}(\mathbb{F}_p)$ denote the group of $\mathbb{F}_p$-points of the reduction of E modulo p. The behavior of $\tilde{E}(\mathbb{F}_p)$ as p varies over the primes has received considerable attention — the oscillations of the cardinalities $|\tilde{E}(\mathbb{F}_p)|$ is a central question in modern number theory, and the structure of $\tilde{E}(\mathbb{F}_p)$ as a group, for example, the existence of large cyclic subgroups, especially of prime order, is of interest because of applications to elliptic curve cryptography [**10**, **12**].

If p is a prime of good reduction then $\tilde{E}(\mathbb{F}_p) \cong \mathbb{Z}/d_p\mathbb{Z} \times \mathbb{Z}/e_p\mathbb{Z}$ for uniquely determined integers d_p, e_p, with $d_p \mid e_p$. The size of the maximal cyclic subgroup, that is the exponent, of $\tilde{E}(\mathbb{F}_p)$ is therefore e_p. For primes p of bad reduction we set $e_p = 0$. The purpose of this paper, motivated by a question of Joseph Silverman (personal communication), is to investigate the average of e_p as p varies. Conditional on a certain form of the Generalized Riemann Hypothesis (GRH), we will show that there exists $c_E \in (0,1)$ such that

$$\sum_{p \leqslant X} e_p \sim c_E \cdot \mathrm{Li}\left(X^2\right) \quad \text{as} \quad X \to \infty,$$

where $\mathrm{Li}\left(X^2\right) := \int_2^{X^2} \mathrm{d}t/(\log t)$ is the logarithmic integral of X^2. Since $\sum_{p \leqslant X} p \sim \mathrm{Li}\left(X^2\right)$ (by partial summation and the prime number theorem), we may interpret this as the average value of e_p being $p \cdot c_E$.

Before stating our main theorem we explain what we mean by GRH. Given a positive integer k, let L_k denote the k-division field of E, that is, the number field obtained by adjoining to $\mathbb{Q}$ the coordinates of all points in $E[k]$, the subgroup of k-torsion of points of E. Let $\zeta_{L_k}(s)$ denote the Dedekind zeta function associated with L_k. We say that $\zeta_{L_k}(s)$ satisfies

Date: November 27, 2012.

The first author is supported by the Göran Gustafsson Foundation (KVA). The second author is supported by grants from the Göran Gustafsson Foundation (KVA) and the Swedish Research Council.

the Riemann Hypothesis (RH) if all zeros with positive real part lie on the line $\mathrm{Re}(s) = 1/2$. By GRH we will here, and in what follows, mean that the Riemann Hypothesis holds for ζ_{L_k} for all positive integers k.

Theorem 1.1. *Given an elliptic curve E defined over $\mathbb{Q}$, there exists a number $c_E \in (0, 1)$ such that on GRH we have*

$$\sum_{p \leqslant X} e_p = c_E \cdot \mathrm{Li}\left(X^2\right) + O_E\left(X^{19/10}(\log X)^{6/5}\right)$$

for $X \geqslant 2$. The implied constant depends on E at most.

Settling for a weaker error term, we can remove the GRH assumption for CM-curves.

Theorem 1.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication, and let c_E be as in Theorem 1.1. For $X \geqslant 3$, we have*

$$\sum_{p \leqslant X} e_p = c_E \cdot \mathrm{Li}\left(X^2\right) \cdot \left\{1 + O_E\left(\frac{\log\log X}{(\log X)^{1/8}}\right)\right\}.$$

The implied constant depends on E at most.

(*Note added in proof:* The error terms in Theorems 1.1 and 1.2 have recently been improved by Wu [**22**] and Kim [**9**]. See Section 8 for details.)

For non-CM curves we can give an unconditional upper bound of the correct order of magnitude. In the following theorem, we use the notation $F(X) \lesssim G(X)$, which means that $\limsup_{X\to\infty} F(X)/G(X) \leqslant 1$.

Theorem 1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$, and let c_E as in Theorem 1.1. As X tends to infinity, we have*

$$\sum_{p \leqslant X} e_p \lesssim c_E \cdot \mathrm{Li}\left(X^2\right).$$

We will now describe c_E in more detail. With $n_{L_k} := [L_k : \mathbb{Q}]$ denoting the degree of the extension $L_k/\mathbb{Q}$, $\omega(k)$ the number of distinct prime factors of k, $\phi(k)$ the Euler totient function of k, and $\mathrm{rad}(k)$ the largest squarefree divisor of k, we have (whether or not E has CM)

$$c_E := \sum_{k=1}^{\infty} \frac{(-1)^{\omega(k)}\phi(\mathrm{rad}(k))}{k n_{L_k}}. \tag{1.1}$$

In Lemma 3.5 below, we will show that this sum is absolutely convergent, and that $c_E \in (0, 1)$. If E does not have CM, there exists a universal constant

$$c := \prod_q \left(1 - \frac{q^3}{(q^2-1)(q^5-1)}\right) = 0.8992282528\ldots, \tag{1.2}$$

such that c_E/c is a rational number depending only on E. If E has CM by an order $\mathfrak{O}$ in a imaginary quadratic number field K, c_E can similarly be written as a rational number (depending on E) times an Euler product, depending only on K, of the form

$$\prod_{q \text{ splits in } K} \left(1 - \frac{1}{q^2(1-1/q)(1-1/q^3)}\right) \cdot \prod_{q \text{ inert in } K} \left(1 - \frac{1}{q^2(1+1/q)(1-1/q^3)}\right).$$

We will indicate how to prove the last two statements in Section 7.

1.1. **Background and discussion.** *The multiplicative order of a number modulo p.* Given a rational number $g \neq 0, \pm 1$ and a prime p, let $l_g(p)$ denote the multiplicative order of g modulo p (unless p divides ab, where $g = a/b$, a, b coprime, in which case set $l_g(p) = 0$). In [**11**], the second author and Pomerance, on assuming the Riemann hypothesis for Dedekind zeta functions associated with certain Kummer extensions, determined the average of $l_g(p)$ as $p \leqslant X$ ranges over primes by showing that

$$\sum_{p \leqslant X} l_g(p) = C_g \cdot \mathrm{Li}\left(X^2\right) + O\left(\frac{X^2}{(\log X)^{3/2 - 2/\log\log\log X}}\right),$$

where C_g can be expressed in terms of the degrees of certain Kummer extensions, namely

$$C_g := \sum_{k=1}^{\infty} \frac{(-1)^{\omega(k)}\phi(k)\mathrm{rad}(k)}{k^2 \cdot [\mathbb{Q}(g^{1/k}, e^{2\pi i/k}) : \mathbb{Q}]} = \sum_{k=1}^{\infty} \frac{(-1)^{\omega(k)}\phi(\mathrm{rad}(k))}{k \cdot [\mathbb{Q}(g^{1/k}, e^{2\pi i/k}) : \mathbb{Q}]}.$$

Thus, even though we consider two rather different quantities associated with groups modulo p, namely the multiplicative *order* of a fixed element modulo p and the *exponent* of an elliptic curve modulo p, the sums defining C_g and c_E are very similar; the only difference is that degrees of Kummer fields replace degrees of k-divison fields. (Note that the exponent fluctuations for $(\mathbb{Z}/p\mathbb{Z})^\times$ are essentially trivial since the group is cyclic.) Further, C_g can also be written as the product of a rational number (depending on g) times a universal constant, namely $C := \prod_q (1 - q/(q^3-1)) = 0.5759599689\ldots$ (the product being over all primes q).

Upper and lower bounds on e_p. As $p \to \infty$, Hasse's bound implies that $|\tilde{E}(\mathbb{F}_p)|/p \sim 1$ which, together with the rank of $\tilde{E}(\mathbb{F}_p)$ being at most two, implies that $\sqrt{p} \ll e_p \ll p$. For E any non-CM curve, Schoof [**15**] improved the lower bound to $e_p \gg \sqrt{p} \cdot \log p / \log\log p$, and noted that this is unlikely to hold for CM curves since the curve E defined by $y^2 = x^3 - x$ has exponent $e_p = \sqrt{p-1}$ for any prime of the form $p = (4n)^2 + 1$.

If one removes zero density subsets of the primes, Duke [**5**] has significantly improved the lower bound. Namely, if $f : \mathbb{R}^+ \to \mathbb{R}^+$ is any increasing function tending to infinity, $e_p > p/f(p)$ holds for 'almost all' primes, in the sense that it holds for all but $o(\pi(X))$ primes $p \leqslant X$. (As usual, $\pi(X)$ denotes the number of primes up to X.) For CM curves the result is unconditional, whereas for non-CM curves GRH is assumed. (For the latter he also shows that the weaker bound $e_p > p^{3/4}/\log p$ holds unconditionally for almost all primes.)

Finally we mention that Shparlinski [**20**] has shown that for any $\epsilon > 0$ and p large, $e_p \geqslant p^{1-\epsilon}$ holds for almost all elliptic curves E in the family $\{E_{a,b}\}_{a,b}$, where $E_{a,b}$ denotes the curve $y^2 = x^3 + ax + b$.

The proportion of primes for which $\tilde{E}(\mathbb{F}_p)$ is cyclic. A question closely related to the size of the exponent is cyclicity — how often does the equality $|\tilde{E}(\mathbb{F}_p)| = e_p$ hold? Borosh, Moreno and Porta [**1**] conjectured that $\tilde{E}(\mathbb{F}_p)$ is cyclic for infinitely many primes p, except in certain cases where this cannot be so for 'trivial reasons'. Serre later proved [**19**], on GRH, that

$$\frac{1}{\pi(X)} \sideset{}{^*}\sum_{\substack{p\leqslant X \\ \tilde{E}(\mathbb{F}_p) \text{ is cyclic}}} 1 \sim c_E^* \quad \text{as} \quad X \to \infty, \tag{1.3}$$

where $\sum^*$ denotes a sum restricted to p at which E has good reduction, and, with $\mu(k)$ denoting the Möbius function of k, $c_E^* = \sum_{k=1}^{\infty} \mu(k)/n_{L_k}$. Furthermore, $c_E^* > 0$ *unless* all 2-torsion points on E are defined over $\mathbb{Q}$, an obvious obstruction[1] to $\tilde{E}(\mathbb{F}_p)$ being cyclic.

Cojocaru and Murty [**4**] obtained versions of (1.3) with effective error terms, and in the special case in which E has CM, Murty [**13**] was quite remarkably able to establish (1.3) *unconditionally* (the proofs were later significantly simplified by Cojocaru [**2**]).

For more background on this and related topics, we recommend the nice survey article [**3**] by Cojocaru.

2. Outline of the proof of Theorem 1.1

We begin by noting that our approach is in spirit a synthesis of the ideas in [**11, 19**], together with refinements by Murty [**13**] and Cojacaru [**2**].

As for notation, in this outline we shall use '$\approx$' to indicate equality with an implied error term, and p shall always denote a prime of good reduction. Recall that $e_p = |\tilde{E}(\mathbb{F}_p)|/d_p$, so if $|\tilde{E}(\mathbb{F}_p)| =: p + 1 - a_p$, then, since $|a_p| \leqslant 2\sqrt{p}$ by Hasse's inequality, we have

$$\sum_{p\leqslant X} e_p \approx \sum_{p\leqslant X} \frac{p}{d_p}. \tag{2.1}$$

We can treat the sum $\sum_{p\leqslant X} p/d_p$ by using partial summation and the prime number theorem, once we have evaluated the sum $\sum_{p\leqslant X} \frac{1}{d_p}$.

Since $d_p \mid e_p$ we have $d_p^2 \leqslant |\tilde{E}(\mathbb{F}_p)| \leqslant (\sqrt{p}+1)^2$ by Hasse's inequality, hence $d_p < 2\sqrt{X}$ for $p \leqslant X$. As in [**11**], we use the elementary identity $\frac{1}{k} = \sum_{hj|k} \frac{\mu(h)}{j}$ to write

$$\sum_{p\leqslant X} \frac{1}{d_p} = \sum_{p\leqslant X} \sum_{hj|d_p} \frac{\mu(h)}{j} = \sum_{hj\leqslant 2\sqrt{X}} \frac{\mu(h)}{j} \sum_{\substack{p\leqslant X \\ hj|d_p}} 1. \tag{2.2}$$

Now, by Lemma 3.1, a positive integer k divides d_p if and only if p splits completely in L_k, and the Chebotarev density theorem (cf. Lemma 3.3) then gives

$$\sum_{\substack{p\leqslant X \\ k|d_p}} 1 \approx \sum_{\substack{p\leqslant X \\ p \text{ splits completely} \\ \text{in } L_k/\mathbb{Q}}} 1 \approx \frac{\mathrm{Li}\,(X)}{n_{L_k}}.$$

[1] The only way for $E(\mathbb{Q})$ to have a rationally defined subgroup isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ is if $\ell = 2$; this easily follows from the fact that $E(\mathbb{R})$ is isomorphic to either $\mathbb{R}/\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$.

Thus,

$$\sum_{hj\leqslant 2\sqrt{X}} \frac{\mu(h)}{j} \sum_{\substack{p\leqslant X\\ hj\mid d_p}} 1 \approx \mathrm{Li}\,(X) \sum_{hj\leqslant 2\sqrt{X}} \frac{\mu(h)}{j}\cdot\frac{1}{n_{L_{hj}}} \approx \mathrm{Li}\,(X) \sum_{k=1}^{\infty} \frac{(-1)^{\omega(k)}\phi(\mathrm{rad}(k))}{kn_{L_k}}. \tag{2.3}$$

The last error term in (2.3), and indeed showing that the last sum is absolutely convergent, involves bounding a sum of the type $\sum_{k>Y}\frac{1}{n_{L_k}}$. We do this in Lemma 3.4, but here lower bounds for n_{L_k} are crucial.

To give lower bounds on n_{L_k}, we use Serre's open image theorem [**16**,**17**]. If E is a non-CM curve, compactness together with the image being open gives that the image of the absolute Galois group has finite index inside $\mathrm{GL}_2(\hat{\mathbb{Z}})$, hence $n_{L_k} \gg_E \phi(k)k^3$. If E is a CM curve, a similar open image result of Serre gives that $n_{L_k} \gg \phi(k)^2$. (For more details, see Proposition 3.2.)

Now, combining (2.1), (2.2), and (2.3), we obtain, via partial summation and the prime number theorem, that

$$\sum_{p\leqslant X} e_p \approx \mathrm{Li}\left(X^2\right)\cdot\sum_{k=1}^{\infty}\frac{(-1)^{\omega(k)}\phi(\mathrm{rad}(k))}{kn_{L_k}},$$

which is the claimed main term.

As for estimating the error terms, a slight complication arises — even assuming GRH, we cannot directly bound the sum of the error terms in the Chebotarev density theorem for 'large' k, that is, $k\in(\sqrt{X}/(\log X)^2, 2\sqrt{X}]$. To deal with this range Serre used the fact that the cyclotomic field $\mathbb{Q}(e^{2\pi i/q})$ is contained in L_q; the sum can thus be restricted to primes $p\equiv 1 \bmod q$, and Brun's sieve is then enough to bound the errors arising from the large k. However, to make an exponent saving in the error term we use a refinement of Serre's approach due to Cojacaru and Murty [**4**] (see Lemma 3.6 for further details.)

3. Preliminaries

In this section we collect some needed results on elliptic curves.

Notation. Throughout, p, q, and ℓ denote (rational) primes; h, j, k, and m denote positive integers. The arithmetic functions ω, ϕ, rad, and μ have already been introduced; also, $\tau(k)$ is the number of divisors of k, and $\sigma(k)$ is the sum of the divisors of k.

Whenever we write $F=O\left(G\right)$, $F\ll G$, or $G\gg F$, we mean that $|F|\leqslant c\cdot G$ where c is an absolute positive constant. By $F\asymp G$ we mean that $F\ll G\ll F$.

The logarithmic integral is defined for numbers $t\geqslant 2$ by $\mathrm{Li}\,(t) := \int_2^t \frac{\mathrm{d}u}{\log u}$.

We fix an elliptic curve E, defined over $\mathbb{Q}$, of conductor N. The results in this section relate to E. For primes p of good reduction (that is, $p\nmid N$), d_p and e_p are the unique positive integers such that we have $\tilde{E}(\mathbb{F}_p)\cong\mathbb{Z}/d_p\mathbb{Z}\times\mathbb{Z}/e_p\mathbb{Z}$ with $d_p\mid e_p$. Thus e_p is the exponent of $\tilde{E}(\mathbb{F}_p)$ if $p\nmid N$, and we set $e_p=0$ if $p\mid N$. Also, if $p\nmid N$, $a_p := p+1-|\tilde{E}(\mathbb{F}_p)|$, and π_p denotes a root of the polynomial $X^2-a_pX+p\in\mathbb{Z}[X]$.

The k-division field of E is denoted L_k; n_{L_k} denotes the degree of the extension $L_k/\mathbb{Q}$, and Δ_{L_k} denotes its discriminant.

Lemma 3.1. *If $p \nmid kN$ then the following statements are equivalent.*

1. *$\tilde{E}(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$.*
2. *p splits completely in L_k.*
3. *$\frac{\pi_p - 1}{k}$ is an algebraic integer.*

Proof. For the equivalence of (1) and (2), see [**13**, Lemma 2]. For the equivalence of (2) and (3), see [**2**, Lemma 2.2]. □

We now give some estimates on the degree of the k-division field of E.

Proposition 3.2. *(a) L_k contains $\mathbb{Q}(e^{2\pi i/k})$ (the k-th cyclotomic field), hence p splits completely in L_k only if $p \equiv 1 \bmod k$. Also, $\phi(k)$ divides n_{L_k}.*
(b) n_{L_k} divides $|\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})| = k^4 \prod_{q|k} (1 - 1/q)(1 - 1/q^2)$.
(c) If E is a non-CM curve, then there exists a constant $B_E \geqslant 1$, depending only on E, such that $|\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})| \leqslant B_E \cdot n_{L_k}$ for every k.
(d) If E has CM, then $\phi(k)^2 \ll n_{L_k} \leqslant k^2$.

Proof. (a) See [**21**, Corollary 8.1.1, Chapter III].

(b) First of all note that $n_{L_k} = |\mathrm{Gal}(L_k/\mathbb{Q})|$ as $L_k/\mathbb{Q}$ is a Galois extension. The action of the absolute Galois group $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ on the k-torsion subgroup $E[k]$ of E induces a representation $\rho_{E,k} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Aut}(E[k]) \cong \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$, which is injective.

(c) With $T_\ell(E)$ denoting the ℓ-adic Tate module of E, the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ on $\prod_\ell \mathrm{Aut}(T_\ell(E)) \cong \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$ induces a representation $\rho_E : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$. By Serre's open image theorem [**17**, Theorem 3], the image of ρ_E is open, and since $\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$ is compact, the image is of finite index. Since $\mathrm{Gal}(L_k/\mathbb{Q})$ is isomorphic to the projection of $\mathrm{Im}(\rho_E)$, by the map $\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$, the result follows.

(d) If E has CM, Serre's open image result for the CM case [**17**, Corollaire, Théorème 5, p.302] gives that $n_{L_k} \gg \phi(k)^2$. (If E has CM by an order $\mathfrak{O}$, the image is open in $\prod_\ell \mathfrak{O}_\ell^\times$, where $\mathfrak{O}_\ell = \mathfrak{O} \otimes \mathbb{Z}_\ell$.) The upper bound follows from $|(\mathfrak{O}/k\mathfrak{O})^\times| \leqslant k^2$. □

Lemma 3.3. *(a) There exist absolute constants $c_1, B > 0$, such that the following statements hold. (i) If $c_1 k^{14} N^2 \leqslant \log X$, then, whether or not E has CM,*

$$|\{p \leqslant X \,:\, p \nmid N \text{ and } k \mid d_p\}| = \frac{\mathrm{Li}(X)}{n_{L_k}} + O\left(X \exp\left(-B(\log X)^{5/14}\right)\right). \tag{3.1}$$

(ii) If $c_1 k^8 N^2 \leqslant \log X$ and E has CM, then

$$|\{p \leqslant X \,:\, p \nmid N \text{ and } k \mid d_p\}| = \frac{\mathrm{Li}(X)}{n_{L_k}} + O\left(X \exp\left(-B(\log X)^{3/8}\right)\right). \tag{3.2}$$

(b) For $X \geqslant 2$ we have, on GRH, that

$$|\{p \leqslant X \,:\, p \nmid N \text{ and } k \mid d_p\}| = \frac{\mathrm{Li}(X)}{n_{L_k}} + O\left(X^{1/2} \log(XN)\right). \tag{3.3}$$

Proof. Note that if $p \leqslant X$ and $p \nmid N$, then *a priori* we have $k \leqslant 2\sqrt{X}$ for $k \mid d_p$, because $d_p \mid e_p$ and so $d_p^2 \leqslant |\tilde{E}(\mathbb{F}_p)| \leqslant (\sqrt{p} + 1)^2$ by Hasse's inequality. Since $p \nmid d_p$ (cf. [**21**, Exercise 5.6(a), p.145]), the conditions $p \nmid N$ and $k \mid d_p$ are equivalent to $p \nmid kN$ and $k \mid d_p$, that is

$p \nmid kN$ and $\tilde{E}(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$. Therefore, by Lemma 3.1,

$$\sum_{\substack{p \leqslant X \\ p \text{ splits completely} \\ \text{in } L_k/\mathbb{Q}}} 1 = |\{p \leqslant X \,:\, p \nmid N \text{ and } k \mid d_p\}| + O\left(\log(XN)\right), \tag{3.4}$$

where the $O\left(\log(XN)\right)$ term is the negligible contribution from the primes p dividing kN: $\omega(kN) \ll \log(kN) \ll \log(XN)$.

(a) (i) As $L_k/\mathbb{Q}$ is a Galois extension, an effective form of the Chebotarev density theorem (for example, see [**14**, Lemma 2]) gives

$$\sum_{\substack{p \leqslant X \\ p \text{ splits completely} \\ \text{in } L_k/\mathbb{Q}}} 1 = \frac{\mathrm{Li}\,(X)}{n_{L_k}} + O\left(X \exp\left(-B\sqrt{\tfrac{\log X}{n_{L_k}}}\right)\right), \tag{3.5}$$

where B is an absolute positive constant, provided

$$c \cdot \max\left\{n_{L_k}|\Delta_{L_k}|^{2/n_{L_k}}, n_{L_k}\left(\log|\Delta_{L_k}|\right)^2\right\} \leqslant \log X, \tag{3.6}$$

for a certain absolute positive constant c. We claim that there is an absolute positive constant c_1 such that if $c_1 k^{14} N^2 \leqslant \log X$, then (3.6) does indeed hold. In that case, Proposition 3.2(b) gives $\sqrt{n_{L_k}} \leqslant k^2 \leqslant (\log X)^{1/7}$ (we may suppose that $c_1 \geqslant 1$), so applying this to the error term in (3.5) and combining with (3.4) gives (3.1).

We now prove our claim. The first of the following sequence of inequalities holds with any Galois extension $L/\mathbb{Q}$ in place of $L_k/\mathbb{Q}$ [**18**, Proposition 6, p.130]; the second holds because the ramified primes of $L_k/\mathbb{Q}$ are divisors of kN [**21**, Proposition 4.1(a), Chapter VII]:

$$\frac{\log|\Delta_{L_k}|}{n_{L_k}} \leqslant \log n_{L_k} + \sum_{\substack{p \text{ ramifies in} \\ L_k/\mathbb{Q}}} \log p \leqslant \log n_{L_k} + \sum_{p \mid kN} \log p \leqslant \log n_{L_k} + \log(kN). \tag{3.7}$$

Our claim follows straightforwardly using this and the inequality $n_{L_k} \leqslant k^4$.

(ii) Similar, but in the CM case we use the fact that $n_{L_k} \leqslant k^2$, by Proposition 3.2(d).

(b) By [**18**, Théorème 4, p.133], on GRH we have

$$\sum_{\substack{p \leqslant X \\ p \text{ splits completely} \\ \text{in } L_k/\mathbb{Q}}} 1 = \frac{\mathrm{Li}\,(X)}{n_{L_k}} + O\left(X^{1/2}\left(\frac{\log|\Delta_{L_k}|}{n_{L_k}} + \log X\right)\right).$$

Applying (3.7) and the inequality $n_{L_k} \leqslant k^4 \ll X^2$, we obtain (3.3) by putting this into (3.4). □

Lemma 3.4. *With B_E as in Proposition 3.2(c), we have*

$$\sum_{k > Y} \frac{1}{n_{L_k}} \ll \begin{cases} 1/Y & \text{if } E \text{ has CM,} \\ B_E/Y^3 & \text{if } E \text{ is a non-CM curve,} \end{cases} \tag{3.8}$$

and

$$\sum_{k>Y}\frac{\sigma(k)\tau(k)}{kn_{L_k}} \ll \begin{cases}(\log Y)/Y & \text{if } E \text{ has CM,}\\ B_E(\log Y)/Y^3 & \text{if } E \text{ is a non-CM curve.}\end{cases} \tag{3.9}$$

Proof. In the CM case we have, by Proposition 3.2(d), that

$$\sum_{k>Y}\frac{1}{n_{L_k}} \ll \sum_{k>Y}\frac{1}{\phi(k)^2} \ll \frac{1}{Y}. \tag{3.10}$$

The last bound holds because $\phi(k) \approx k$ 'on average'. It can be proved by entirely elementary means, the key being the identity $\frac{k}{\phi(k)} = \sum_{j|k}\frac{|\mu(j)|}{\phi(j)}$. We spare the reader the details. Similarly, since $|\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})| = k^4\prod_{q|k}(1-1/q)(1-1/q^2) \gg k^3\phi(k)$, Proposition 3.2(c) gives

$$\sum_{k>Y}\frac{1}{n_{L_k}} \ll B_E\sum_{k>Y}\frac{1}{k^3\phi(k)} \ll \frac{B_E}{Y^3}$$

in the non-CM case.

Again if E has CM, we have

$$\sum_{k>Y}\frac{\sigma(k)\tau(k)}{kn_{L_k}} \ll \sum_{k>Y}\frac{\sigma(k)\tau(k)}{k\phi(k)^2} \ll \frac{\log Y}{Y}.$$

One way to obtain the last bound is to establish that $\sum_{k\leqslant Y}\sigma(k)\tau(k) \ll Y^2\log Y$, then apply partial summation to show that $\sum_{k>Y}\sigma(k)\tau(k)/k^3 \ll (\log Y)/Y$, and use the identity $\frac{k}{\phi(k)} = \sum_{j|k}\frac{|\mu(j)|}{\phi(j)}$ two more times. Similarly, if E is a non-CM curve, then

$$\sum_{k>Y}\frac{\sigma(k)\tau(k)}{kn_{L_k}} \ll B_E\sum_{k>Y}\frac{\sigma(k)\tau(k)}{k^4\phi(k)} \ll \frac{B_E\log Y}{Y^3}.$$

□

Lemma 3.5. *The sum in* (1.1) *defining* c_E *is absolutely convergent, and* $c_E \in (0,1)$.

Proof. Absolute convergence of the sum in (1.1) follows at once from (3.8). To show that $c_E \in (0,1)$, first note that for every $j \geqslant 1$, $\sum_{h\geqslant 1}\frac{\mu(h)}{n_{L_{hj}}} \ll_E 1$ by (3.8), because $n_{L_{hj}} \leqslant n_{L_h}$. Next, we claim that

$$\sum_{h\geqslant 1}\frac{\mu(h)}{n_{L_{hj}}} \geqslant 0 \qquad (j \geqslant 1). \tag{3.11}$$

To see this, fix any $j \geqslant 1$ and any $Y \geqslant j$. Let $Q = \prod_{q\leqslant Y} q$ and let X be large enough in terms of Y and N so that $\log X \geqslant c_1(QY)^{14}N^2$, where c_1 is the constant of Lemma 3.3(a). Also assume that $\sum_{h|Q}|\mu(h)| = 2^Y \ll \log X$. An inclusion-exclusion argument gives

$$\sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p=j}} 1 \leqslant \sum_{h|Q}\mu(h)\sum_{\substack{p\leqslant X\\ p\nmid N,\ hj\mid d_p}} 1.$$

Applying Lemma 3.3(a)(i), we obtain

$$\sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p=j}} 1 \leqslant \mathrm{Li}\,(X)\sum_{h\mid Q}\frac{\mu(h)}{n_{L_{hj}}} + O\left(2^Y X\exp\left(-B(\log X)^{5/14}\right)\right).$$

Dividing by $\mathrm{Li}\,(X)$ and letting X tend to infinity, we find that

$$0 \leqslant \limsup_{X\to\infty}\frac{1}{\mathrm{Li}\,(X)}\sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p=j}} 1 \leqslant \sum_{h\mid Q}\frac{\mu(h)}{n_{L_{hj}}}.$$

Letting Y tend to infinity (cf. (3.8)), we obtain (3.11).

Now, for any $Y\geqslant 1$,

$$\sum_{j\leqslant Y}\sum_{h\geqslant 1}\frac{\mu(h)}{n_{L_{hj}}} = \sum_{k\geqslant 1}\frac{1}{n_{L_k}}\sum_{\substack{hj=k\\ j\leqslant Y}}\mu(h) = \sum_{k\leqslant Y}\frac{1}{n_{L_k}}\sum_{hj=k}\mu(h) + O\left(\sum_{k>Y}\frac{1}{n_{L_k}}\sum_{hj=k}1\right).$$

Since $\sum_{hj=k}\mu(h)$ vanishes unless $k=1$, the main term here is just $1/n_{L_1}=1$. Applying (3.9) to the O-term (note that $\sum_{hj=k}1=\tau(k)\leqslant\sigma(k)\tau(k)/k$), then letting Y tend to infinity, we obtain

$$\sum_{j\geqslant 1}\sum_{h\geqslant 1}\frac{\mu(h)}{n_{L_{hj}}} = 1. \tag{3.12}$$

Now since $\sum_{h\mid k}\mu(h)\cdot h = (-1)^{\omega(k)}\phi(\mathrm{rad}(k))$, we have

$$c_E = \sum_{k\geqslant 1}\frac{1}{n_{L_k}}\sum_{hj=k}\frac{\mu(h)}{j} = \sum_{j\geqslant 1}\frac{1}{j}\sum_{h\geqslant 1}\frac{\mu(h)}{n_{L_{hj}}}, \tag{3.13}$$

convergence being assured by (3.8), (3.11) and (3.12). In view of (3.11), (3.12) and (3.13), we see that $0<c_E\leqslant 1$. In fact recalling that $c_E^*=\sum_{h\geqslant 1}\frac{\mu(h)}{n_{L_h}}$ is the cyclicity constant, we can deduce from (3.11) — (3.13) that $c_E\in(0,1]\cap[c_E^*,\frac{1}{2}(c_E^*+1)]$, with $c_E=1$ if and only if $c_E^*=1$. However, that $c_E^*<1$ can be seen by considering $\{p\leqslant X : p\nmid N \text{ and } q>t\}$. By the Chebotarev density theorem (cf. Lemma 3.3(a)(i)) we have, for $t\geqslant 2$ and sufficiently large X,

$$\frac{1}{\pi(X)}\cdot|\{p\leqslant X : p\nmid N, q\mid d_p\Rightarrow q>t\}| \leqslant 1-\frac{1}{\pi(X)}\cdot|\{p\leqslant X\ :\ p\nmid N \text{ and } 2\mid d_p\}| < 1-\frac{1}{2n_{L_2}}.$$

On the other hand, using inclusion-exclusion, followed by Lemma 3.3(a)(i) and (3.8), one can show that

$$\frac{1}{\pi(X)}\cdot|\{p\leqslant X : p\nmid N, q\mid d_p\Rightarrow q>t\}| = c_E^* + O_E\left(\frac{1}{t}\right) + O_E\left(2^t\exp\left(-B(\log X)^{5/14}\right)\right).$$

For suitable $t=t(X)$ and sufficiently large X, comparing gives $c_E^*<1$. □

Lemma 3.6. *(a) For $X,Y\geqslant 2$ we have*

$$|\{p\leqslant X\ :\ p\nmid N \textit{ and } d_p>Y\}| \ll \frac{X^{3/2}}{Y^2}+X^{1/2}\log X. \tag{3.14}$$

(b) If E has CM and $2 < Y \leqslant \log X$, then

$$|\{p \leqslant X \,:\, p \nmid N \text{ and } d_p > Y\}| \ll \frac{X \log\log X}{Y \log X}. \tag{3.15}$$

Proof. (a) First of all note that since $d_p \mid e_p$, we have $d_p^2 \leqslant |\tilde{E}(\mathbb{F}_p)| \leqslant (\sqrt{p}+1)^2$ by Hasse's inequality. Thus, if $p \nmid N$ and $d_p > Y$ then $d_p = k$ for some $Y < k \leqslant 2\sqrt{X}$. But $d_p = k$ implies $k^2 \mid (p+1-a_p)$, and also $k \mid p-1$ by Lemma 3.1 and Proposition 3.2(a); hence $k \mid a_p - 2$. Since $a_p \leqslant 2\sqrt{p}$ by Hasse's inequality, we therefore have

$$\begin{aligned}
\sum_{\substack{p \leqslant X \\ p \nmid N,\, d_p > Y}} 1 &\leqslant \sum_{Y < k \leqslant 2\sqrt{X}} \sum_{\substack{|a| \leqslant 2\sqrt{X} \\ a \neq 2 \\ a \equiv 2 \bmod k}} \sum_{\substack{p \leqslant X \\ a_p = a \\ k^2 | p+1-a}} 1 + \sum_{Y < k \leqslant 2\sqrt{X}} \sum_{\substack{p \leqslant X \\ a_p = 2 \\ k^2 | p-1}} 1 \\
&\ll \sum_{Y < k \leqslant 2\sqrt{X}} \frac{\sqrt{X}}{k} \left(\frac{X}{k^2} + 1 \right) + \sum_{Y < k \leqslant 2\sqrt{X}} \left(\frac{X}{k^2} + 1 \right) \\
&\ll \frac{X^{3/2}}{Y^2} + \sqrt{X} \log X + \frac{X}{Y} + \sqrt{X} \ll \frac{X^{3/2}}{Y^2} + \sqrt{X} \log X.
\end{aligned}$$

(Here we have used the elementary bound $\sum_{k>Y} k^{-m} \ll Y^{1-m}$, $m \geqslant 2$.)

(b) Suppose E has complex multiplication by an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, D a squarefree positive integer. We begin with the following observation. Since $p \nmid d_p$, the statement '$p \nmid N$ and $k \mid d_p$' is equivalent to the statement '$p \nmid kN$ and p splits completely in L_k' (Lemma 3.1). In that case $p \equiv 1 \bmod k$ by Proposition 3.2(a). If $a_p = 0$, then we also have $p \equiv -1 \bmod k$, because $k^2 \mid d_p e_p = (p+1-a_p)$. But we can only have both $p \equiv -1 \bmod k$ and $p \equiv 1 \bmod k$ if $k = 1$ or 2. Therefore, we necessarily have $a_p \neq 0$ when $k \mid d_p$ and $k \geqslant 3$. Moreover, $\frac{\pi_p - 1}{k}$ is an algebraic integer (Lemma 3.1), and since $\mathbb{Q}(\pi_p) = K$ when $a_p \neq 0$ (see [**2**, Lemma 2.3]), we have that $\frac{\pi_p - 1}{k} \in \mathfrak{O}_K$.

Now,

$$\{p \leqslant X \,:\, p \nmid N \text{ and } d_p > Y\} \subseteq \mathscr{P}_1(X) \cup \mathscr{P}_2(X, Y) \cup \mathscr{P}_3(Y), \tag{3.16}$$

where

$$\begin{aligned}
\mathscr{P}_1(X) &:= \{p \leqslant X \,:\, p \nmid N \text{ and } q \mid d_p \text{ for some } q \in (\log X, 2\sqrt{X}]\}, \\
\mathscr{P}_2(X, Y) &:= \{p \leqslant X \,:\, p \nmid N \text{ and } q \mid d_p \text{ for some } q \in (Y, \log X]\}, \\
\mathscr{P}_3(Y) &:= \{p \leqslant X \,:\, p \nmid N,\ d_p > Y, \text{ and } q \mid d_p \Rightarrow q \leqslant Y\} \\
&\subseteq \{p \leqslant X \,:\, p \nmid N,\ k \mid d_p \text{ for some } k \in [Y, Y^2]\}.
\end{aligned}$$

Since $2 < Y \leqslant \log X$ we have, by our initial observation, that

$$|\mathscr{P}_1(X)| = \sum_{\log X < q \leqslant 2\sqrt{X}} \sum_{\substack{p \leqslant X \\ p \nmid N,\, q \mid d_p \\ a_p \neq 0}} 1 \leqslant \sum_{\log X < q \leqslant 2\sqrt{X}} \sum_{\substack{p \leqslant X \\ \frac{\pi_p - 1}{k} \in \mathfrak{O}_K}} 1. \tag{3.17}$$

Since π_p has norm p in $K/\mathbb{Q}$, it follows that

$$|\mathscr{P}_1(X)| \leqslant \sum_{\log X < q \leqslant 2\sqrt{X}} |S_j(X; D, q)|, \tag{3.18}$$

with

$$S_j(X; D, k) := \left\{ p \leqslant X : p = \left(\tfrac{u}{j}k + 1\right)^2 + D\left(\tfrac{v}{j}\right)^2 k^2 \text{ for some } u, v \in \mathbb{Z} \right\},$$

and $j = 1$ if $-D \equiv 2, 3 \bmod 4$; $j = 2$ if $-D \equiv 1 \bmod 4$. A trivial bound for $|S_i(X; D, q)|$ will suffice here:

$$\begin{aligned} \sum_{\log X < q \leqslant 2\sqrt{X}} |S_j(X; D, q)| &\ll \sum_{\log X < q \leqslant 2\sqrt{X}} \frac{\sqrt{X}}{q\sqrt{D}} \left(\frac{\sqrt{X}}{q} + 1 \right) \\ &\ll X \sum_{q > \log X} \frac{1}{q^2} + \sqrt{X} \sum_{q \leqslant 2\sqrt{X}} \frac{1}{q} \\ &\ll \frac{X}{(\log X)(\log\log X)} + \sqrt{X} \log\log X. \end{aligned} \tag{3.19}$$

(To obtain the last bound, apply partial summation and the prime number theorem to each sum.)

We bound $|\mathscr{P}_2(X, Y)|$ and $|\mathscr{P}_3(Y)|$ similarly, but we need the following non-trivial bound [**2**, Lemma 2.5]:

$$|S_j(X; D, k)| \ll \left(\frac{\sqrt{X}}{k} + 1 \right) \frac{\sqrt{X} \log\log X}{k\sqrt{D} \log\left(\frac{\sqrt{X} - 1}{k} \right)},$$

provided $k < \sqrt{X} - 1$. Thus,

$$\begin{aligned} |\mathscr{P}_2(X, Y)| &\leqslant \sum_{Y < q \leqslant \log X} |S_j(X; D, q)| \\ &\ll \sum_{Y < q \leqslant \log X} \left(\frac{\sqrt{X}}{q} + 1 \right) \frac{\sqrt{X} \log\log X}{q\sqrt{D} \log\left(\frac{\sqrt{X} - 1}{q} \right)} \\ &\ll \frac{X \log\log X}{\log\left(\frac{\sqrt{X} - 1}{\log X} \right)} \sum_{q > Y} \frac{1}{q^2} + \frac{\sqrt{X} \log\log X}{\log\left(\frac{\sqrt{X} - 1}{\log X} \right)} \sum_{q \leqslant \log X} \frac{1}{q} \\ &\ll \frac{X \log\log X}{(\log X) Y \log Y}, \end{aligned} \tag{3.20}$$

and

$$\begin{aligned} |\mathscr{P}_3(Y)| &\leqslant \sum_{Y<k\leqslant Y^2} |S_i(X;D,k)| \\ &\ll \sum_{Y\leqslant k\leqslant Y^2} \left(\frac{\sqrt{X}}{k}+1\right) \frac{\sqrt{X}\log\log X}{k\sqrt{D}\log\left(\frac{\sqrt{X}-1}{k}\right)} \\ &\ll \frac{X\log\log X}{\log\left(\frac{\sqrt{X}-1}{Y}\right)} \sum_{Y\leqslant k\leqslant Y^2}\frac{1}{k^2} + \frac{\sqrt{X}\log\log X}{\log\left(\frac{\sqrt{X}-1}{Y}\right)} \sum_{Y\leqslant k\leqslant Y^2}\frac{1}{k} \\ &\ll \frac{X\log\log X}{(\log X)Y} + \frac{\sqrt{X}(\log\log X)(\log Y)}{\log X}. \end{aligned} \tag{3.21}$$

Since $Y \leqslant \log X$, putting (3.17) — (3.21) into (3.16), we obtain (3.15). □

4. Proof of Theorem 1.1

Let $X \geqslant 2$ and set

$$Y = Y(X) := \frac{X^{1/5}}{(\log X)^{2/5}}.$$

We proceed on GRH, so that partial summation applied to (3.3) gives

$$\begin{aligned} \sum_{\substack{p\leqslant X \\ p\nmid N,\ k\mid d_p}} p &= X \sum_{\substack{p\leqslant X \\ p\nmid N,\ k\mid d_p}} 1 - \int_2^X \left(\textstyle\sum_{\substack{p\leqslant t \\ p\nmid N, k\mid d_p}} 1\right) \mathrm{d}t \\ &= \frac{X\mathrm{Li}\,(X)}{n_{L_k}} - \frac{1}{n_{L_k}}\int_2^X \mathrm{Li}\,(t)\ \mathrm{d}t + O\left(X^{3/2}\log(XN)\right) \\ &= \frac{\mathrm{Li}\,(X^2)}{n_{L_k}} + O\left(X^{3/2}\log(XN)\right). \end{aligned} \tag{4.1}$$

Here we have used that $\int_2^X \mathrm{Li}\,(t)\ \mathrm{d}t = X\mathrm{Li}\,(X) - \mathrm{Li}\,(X^2) + O\,(1)$.

Now, $e_p = |\tilde{E}(\mathbb{F}_p)|/d_p = (p+1-a_p)/d_p$ if $p \nmid N$, and by definition $e_p = 0$ otherwise, hence

$$\sum_{p\leqslant X} e_p = \sum_{\substack{p\leqslant X \\ p\nmid N}} \frac{p}{d_p} + \sum_{\substack{p\leqslant X \\ p\nmid N}} \frac{1-a_p}{d_p} =: \mathcal{T}_0 + \mathcal{E}_0. \tag{4.2}$$

Since $|a_p| \leqslant 2\sqrt{p}$ by Hasse's inequality, we have

$$\mathcal{E}_0 := \sum_{\substack{p\leqslant X \\ p\nmid N}} \frac{1-a_p}{d_p} \ll \sum_{p\leqslant X}\sqrt{p} \leqslant X^{1/2}\sum_{p\leqslant X} 1 \leqslant X^{3/2}. \tag{4.3}$$

We write

$$\mathcal{T}_0 := \sum_{\substack{p\leqslant X \\ p\nmid N}} \frac{p}{d_p} = \sum_{\substack{p\leqslant X \\ p\nmid N,\ d_p\leqslant Y}} \frac{p}{d_p} + \sum_{\substack{p\leqslant X \\ p\nmid N,\ d_p > Y}} \frac{p}{d_p} =: \mathcal{T}_1 + \mathcal{E}_1.$$

To bound $\mathcal{E}_1$, we apply (3.14), and then use the definition of Y:

$$\mathcal{E}_1 := \sum_{\substack{p\leqslant X\\ p\nmid N,\, d_p>Y}} \frac{p}{d_p} \leqslant \frac{X}{Y} \sum_{\substack{p\leqslant X\\ p\nmid N,\, d_p>Y}} 1 \ll \frac{X^{5/2}}{Y^3} + \frac{X^{3/2}\log X}{Y} \ll X^{19/10}(\log X)^{6/5}. \tag{4.4}$$

We partition $\mathcal{T}_1$, using the identity $\frac{1}{k} = \sum_{hj|k} \frac{\mu(h)}{j}$, as follows:

$$\mathcal{T}_1 := \sum_{\substack{p\leqslant X\\ p\nmid N,\, d_p\leqslant Y}} p \sum_{hj|d_p} \frac{\mu(h)}{j} = \sum_{\substack{p\leqslant X\\ p\nmid N}} p \sum_{\substack{hj|d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} - \sum_{\substack{p\leqslant X\\ p\nmid N,\, d_p>Y}} p \sum_{\substack{hj|d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} =: \mathcal{T}_{11} - \mathcal{E}_{11}.$$

We now consider $\mathcal{E}_{11}$, making yet another partition:

$$\mathcal{E}_{11} := \sum_{\substack{p\leqslant X\\ p\nmid N\\ d_p>Y^2}} p \sum_{\substack{hj|d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} + \sum_{\substack{p\leqslant X\\ p\nmid N\\ Y<d_p\leqslant Y^2}} p \sum_{\substack{hj|d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} =: \mathcal{E}_{12} + \mathcal{E}_{13}.$$

Next, we note that

$$\sum_{\substack{hj|d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} \ll \sum_{j\leqslant Y} \frac{1}{j} \sum_{h\leqslant Y/j} 1 \leqslant Y \sum_{j\leqslant Y} \frac{1}{j^2} \ll Y.$$

Thus, by (3.14) (with Y^2 in place of Y), and by the definition of Y, we have

$$\begin{aligned}\mathcal{E}_{12} := \sum_{\substack{p\leqslant X\\ p\nmid N\\ d_p>Y^2}} p \sum_{\substack{hj|d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} &\ll XY \sum_{\substack{p\leqslant X\\ p\nmid N\\ d_p>Y^2}} 1 \\ &\ll \frac{X^{5/2}}{Y^3} + X^{3/2} Y \log X \ll X^{19/10}(\log X)^{6/5}.\end{aligned} \tag{4.5}$$

For $\mathcal{E}_{13}$, we use

$$\sum_{\substack{hj|d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} \ll \sum_{h|d_p} 1 \sum_{j|d_p} \frac{1}{j} = \frac{\tau(d_p)}{d_p} \sum_{j|d_p} \frac{d_p}{j} = \frac{\tau(d_p)\sigma(d_p)}{d_p}.$$

Thus,

$$\begin{aligned}\mathcal{E}_{13} :=& \sum_{\substack{p\leqslant X\\ p\nmid N\\ Y<d_p\leqslant Y^2}} p \sum_{\substack{hj|d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} \\ &\ll \sum_{\substack{p\leqslant X\\ p\nmid N\\ Y<d_p\leqslant Y^2}} p \cdot \frac{\tau(d_p)\sigma(d_p)}{d_p} \leqslant \sum_{Y<k\leqslant Y^2} \frac{\tau(k)\sigma(k)}{k} \sum_{\substack{p\leqslant X\\ p\nmid N,\, k\mid d_p}} p.\end{aligned}$$

We apply (4.1) to the last sum, noting that $\mathrm{Li}\,(X^2) \ll X^2/\log X$. Then we use (3.9), as well as the bound $\sum_{k\leqslant Y^2}\frac{\tau(k)\sigma(k)}{k} \ll \int_2^{Y^2}\log t\,\mathrm{d}t \ll Y^2\log Y$. (Apply partial summation to $\sum_{k\leqslant t}\tau(k)\sigma(k) \ll t^2\log t$.) Thus,

$$\begin{aligned}\sum_{Y<k\leqslant Y^2}\frac{\tau(k)\sigma(k)}{k}&\sum_{\substack{p\leqslant X\\ p\nmid N,\ k\mid d_p}} p\\ &\ll \frac{X^2}{\log X}\sum_{k>Y}\frac{\tau(k)\sigma(k)}{kn_{L_k}} + X^{3/2}\log(XN)\sum_{k\leqslant Y^2}\frac{\tau(k)\sigma(k)}{k}\\ &\ll \begin{cases}\frac{X^2\log Y}{Y\log X} + X^{3/2}(\log(XN))Y^2\log Y & \text{if } E \text{ has CM,}\\ \frac{X^2}{\log X}\cdot\frac{B_E\log Y}{Y^3} + X^{3/2}(\log(XN))Y^2\log Y. & \text{if } E \text{ is a non-CM curve.}\end{cases}\end{aligned}$$

Combining and using the definition of Y, we obtain

$$\mathcal{E}_{13} \ll \begin{cases}X^{19/10}(\log(XN))^{6/5} & \text{if } E \text{ has CM,}\\ B_EX^{7/5}(\log X)^{6/5} + X^{19/10}(\log(XN))^{6/5} & \text{if } E \text{ is a non-CM curve.}\end{cases} \tag{4.6}$$

Finally we consider $\mathcal{T}_{11}$. By (4.1), and since

$$\left|\sum_{hj\leqslant Y}\frac{\mu(h)}{j}\right| = \left|\sum_{k\leqslant Y}\sum_{hj=k}\frac{\mu(h)}{j}\right| \leqslant \sum_{k\leqslant Y}\left|\sum_{hj=k}\frac{\mu(h)}{j}\right| \leqslant \sum_{k\leqslant Y}\frac{\phi(k)}{k} \leqslant Y,$$

we have

$$\begin{aligned}\mathcal{T}_{11} := \sum_{\substack{p\leqslant X\\ p\nmid N}} p\sum_{\substack{hj\mid d_p\\ hj\leqslant Y}}\frac{\mu(h)}{j} &= \sum_{hj\leqslant Y}\frac{\mu(h)}{j}\sum_{\substack{p\leqslant X\\ p\nmid N,\ hj\mid d_p}} p\\ &= \mathrm{Li}\left(X^2\right)\sum_{hj\leqslant Y}\frac{\mu(h)}{j}\cdot\frac{1}{n_{L_{hj}}} + O\left(X^{3/2}Y\log(XN)\right).\end{aligned} \tag{4.7}$$

Now, for prime powers q^m we have

$$\sum_{hj=q^m}\frac{\mu(h)}{j} = \frac{1}{q^m} - \frac{1}{q^{m-1}} = \frac{1-q}{q^m},$$

and so by multiplicativity we have

$$\sum_{hj=k}\frac{\mu(h)}{j} = \prod_{q^m\|k}\frac{1-q}{q^m} = \frac{(-1)^{\omega(k)}}{k}\prod_{q\mid k}(q-1) = \frac{(-1)^{\omega(k)}\phi(\mathrm{rad}(k))}{k}.$$

(Here, $q^m\|k$ means that $q^m \mid k$ but $q^{m+1}\nmid k$.) Therefore, setting c_E as in (1.1), and using (3.8), we obtain

$$\sum_{hj\leqslant Y}\frac{\mu(h)}{j}\cdot\frac{1}{n_{L_{hj}}} = \sum_{k=1}^{\infty}\frac{(-1)^{\omega(k)}\phi(\mathrm{rad}(k))}{kn_{L_k}} + O\left(\sum_{k>Y}\frac{1}{n_{L_k}}\right)$$

$$= c_E + \begin{cases} O\left(1/Y\right) & \text{if } E \text{ has CM,} \\ O\left(B_E/Y^3\right) & \text{if } E \text{ is a non-CM curve.} \end{cases}$$

Putting this into (4.7), then using the definition of Y, we obtain

$$\begin{aligned} \mathcal{T}_{11} &= c_E \cdot \mathrm{Li}\left(X^2\right) \\ &\quad + \begin{cases} O\left(\frac{X^{9/5}}{(\log X)^{3/5}}\right) + O\left(X^{17/10}(\log(XN))^{3/5}\right) & \text{if } E \text{ has CM,} \\ O\left(B_E X^{7/5}(\log X)^{1/5}\right) + O\left(X^{17/10}(\log(XN))^{3/5}\right) & \text{if } E \text{ is a non-CM curve.} \end{cases} \end{aligned} \tag{4.8}$$

Gathering the estimates (4.8), (4.6), (4.5), (4.4), (4.3), and (4.2), the largest error term being of size $O\left(X^{19/10}(\log(XN))^{6/5}\right)$, we obtain

$$\sum_{p \leqslant X} e_p = \mathcal{T}_{11} - (\mathcal{E}_{12} + \mathcal{E}_{13}) + \mathcal{E}_1 + \mathcal{E}_0 = c_E \cdot \mathrm{Li}\left(X^2\right) + O\left(X^{19/10}(\log(XN))^{6/5}\right),$$

plus $O\left(B_E X^{7/5}(\log X)^{6/5}\right)$ if E is a non-CM curve, this term being dominated by the other O-term once $X \geqslant B_E^2$. □

5. Proof of Theorem 1.2

We now fix an elliptic curve E defined over $\mathbb{Q}$, of conductor N. We suppose that E has complex multiplication by an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. We know that there are only nine possibilities for D, namely $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. (See [**21**, Appendix C, §11].)

Let c_1 be the absolute positive constant of Lemma 3.3(a), and let c_0, c_2 be positive constants to be specified presently. Suppose $X \geqslant \exp\left(c_0 N^2\right)$ and set

$$Y = Y(X, N) := c_2 \left(\frac{\log X}{N^2}\right)^{\frac{1}{24}}.$$

We choose c_0 and c_2 so that $2 < Y \leqslant (\log X)^{1/3}$ and $2c_1 Y^{24} N^2 \leqslant \log X$.

Similarly to (4.1), partial summation and Lemma 3.3(a)(ii) give

$$\sum_{\substack{p \leqslant X \\ p \nmid N,\ k \mid d_p}} p = \frac{\mathrm{Li}\left(X^2\right)}{n_{L_k}} + O\left(X^2 \exp\left(-B(\log X)^{3/8}\right)\right), \tag{5.1}$$

provided $c_1 k^8 N^2 \leqslant \log X$. One of the error terms involved is

$$\int_2^X \left(\sum_{\substack{p \leqslant t \\ p \nmid N,\ k \mid d_p}} 1 - \tfrac{\mathrm{Li}(t)}{n_{L_k}}\right) \mathrm{d}t.$$

We can apply (5.1) to $\int_{\exp(c_1 k^8 N^2)}^X (\cdots)\,\mathrm{d}t$, but we can only apply a trivial bound to the rest of the integral:

$$\int_2^{\exp(c_1 k^8 N^2)} \left(\sum_{\substack{p \leqslant t \\ p \nmid N,\ k \mid d_p}} 1 - \tfrac{\mathrm{Li}(t)}{n_{L_k}}\right) \mathrm{d}t \ll \int_2^{\exp(c_1 k^8 N^2)} t\,\mathrm{d}t \ll \exp\left(2c_1 k^8 N^2\right).$$

This is $O\left(X\right)$ if $k \leqslant Y^3$, because $2c_1 Y^8 N^2 \leqslant \log X$.

We now proceed as in the proof of Theorem 1.1. The differences are as follows. Analogous with (4.4) and (4.5) we have, by (3.15), that

$$\mathcal{E}_1 := \sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p>Y}} \frac{p}{d_p} \leqslant \frac{X}{Y} \sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p>Y}} 1 \ll \frac{X^2}{\log X}\cdot\frac{\log\log X}{Y^2}, \tag{5.2}$$

and

$$\mathcal{E}_{12} := \sum_{\substack{p\leqslant X\\ p\nmid N\\ d_p>Y^3}} p \sum_{\substack{hj\mid d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} \ll XY \sum_{\substack{p\leqslant X\\ p\nmid N\\ d_p>Y^3}} 1 \ll \frac{X^2}{\log X}\cdot\frac{\log\log X}{Y^2}. \tag{5.3}$$

Analogous with (4.6) we have

$$\mathcal{E}_{13} := \sum_{\substack{p\leqslant X\\ p\nmid N\\ Y<d_p\leqslant Y^3}} p \sum_{\substack{hj\mid d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} \leqslant \sum_{Y<k\leqslant Y^3} \frac{\tau(k)\sigma(k)}{k} \sum_{\substack{p\leqslant X\\ p\nmid N,\ k\mid d_p}} p.$$

Since (5.1) holds uniformly for $k \leqslant Y^3$, we may apply it to the last sum to obtain

$$\mathcal{E}_{13} \ll \frac{X^2}{\log X}\sum_{k>Y}\frac{\tau(k)\sigma(k)}{kn_{L_k}} + X^2\exp\left(-B(\log X)^{3/8}\right)\sum_{k\leqslant Y^3}\frac{\tau(k)\sigma(k)}{k}.$$

We use (3.9) to bound the second last sum and an elementary bound for the last sum. Thus, we have

$$\mathcal{E}_{13} \ll \frac{X^2}{\log X}\cdot\frac{\log Y}{Y} + X^2\exp\left(-B(\log X)^{3/8}\right)\cdot Y^3\log Y \ll \frac{X^2}{\log X}\cdot\frac{\log Y}{Y}. \tag{5.4}$$

Analogous with (4.8), we have, by (5.1),

$$\begin{aligned}\mathcal{T}_{11} &:= \sum_{\substack{p\leqslant X\\ p\nmid N}} p \sum_{\substack{hj\mid d_p\\ hj\leqslant Y}} \frac{\mu(h)}{j} = \operatorname{Li}\left(X^2\right)\left(c_E + O\left(\frac{1}{Y}\right)\right) + YX^2\exp\left(-B(\log X)^{3/8}\right)\\ &= c_E\cdot\operatorname{Li}\left(X^2\right) + O\left(\frac{X^2}{Y\log X}\right).\end{aligned} \tag{5.5}$$

Gathering the estimates (5.5), (5.4), (5.3), (5.2), and (4.2), we obtain

$$\begin{aligned}\sum_{p\leqslant X} e_p &= \mathcal{T}_{11} - (\mathcal{E}_{12}+\mathcal{E}_{13}) + \mathcal{E}_1 + \mathcal{E}_0\\ &= c_E\cdot\operatorname{Li}\left(X^2\right) + O\left(\frac{X^2}{\log X}\left(\frac{\log\log X}{Y^2}+\frac{\log Y}{Y}\right)\right).\end{aligned}$$

Since $Y = (N^{-2}\log X)^{1/24}$, the theorem follows. □

6. Proof of Theorem 1.3

Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N. We make no assumptions as to whether or not E has CM. Let c_1 be the absolute positive constant of Lemma 3.3(a), and let c_0, c_2 be positive constants to be specified presently. Suppose $X \geqslant \exp\left(c_0 N^2\right)$ and set

$$Y = Y(X,N) := c_2 \log\left[\frac{\log X}{N^2}\right]^{\frac{1}{42}}.$$

We choose c_0 and c_2 so that $2c_1 \exp\left(42Y\right) N^2 \leqslant \log X$.

As in the proofs of the first two theorems, we have

$$\sum_{p\leqslant X} e_p = \sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p\leqslant Y}} \frac{p}{d_p} + \sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p>Y}} \frac{p}{d_p} + \sum_{\substack{p\leqslant X\\ p\nmid N}} \frac{1-a_p}{d_p} =: \mathcal{T}_1 + \mathcal{E}_1 + O\left(X^{3/2}\right). \tag{6.1}$$

Since $d_p \leqslant 2\sqrt{p}$, and since $p \equiv 1 \bmod j$ if $d_p = j$ by Proposition 3.2(a), we have

$$\sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p>Y}} \frac{1}{d_p} = \sum_{Y<j\leqslant 2\sqrt{X}} \frac{1}{k} \sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p=j}} 1 \leqslant \sum_{Y<j\leqslant 2\sqrt{X}} \frac{1}{j} \sum_{\substack{p\leqslant X\\ p\equiv 1 \bmod j}} 1.$$

By the Brun-Titchmarsh inequality [**6**, Theorem 3.7],

$$\sum_{Y<j\leqslant 2\sqrt{X}} \frac{1}{j} \sum_{\substack{p\leqslant X\\ p\equiv 1 \bmod j}} 1 \ll \sum_{Y<j\leqslant 2\sqrt{X}} \frac{1}{j}\cdot\frac{X}{\phi(j)\log(X/j)} \ll \frac{X}{\log X}\sum_{j>Y}\frac{1}{j\phi(j)} \ll \frac{X}{Y\log X}$$

(cf. (3.10) for the last bound). Hence

$$\mathcal{E}_1 := \sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p>Y}} \frac{p}{d_p} \leqslant X \sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p>Y}} \frac{1}{d_p} \ll \frac{X^2}{Y\log X}. \tag{6.2}$$

We claim that, with c_E as in (1.1) and B_E as in Proposition 3.2(c), we have

$$\mathcal{T}_1 \leqslant \begin{cases} c_E \cdot \mathrm{Li}\left(X^2\right) + O\left(\frac{X^2}{Y\log X}\right) & \text{if } E \text{ has CM,}\\ c_E \cdot \mathrm{Li}\left(X^2\right) + O\left(\frac{X^2}{Y\log X} + \frac{B_E X^2}{Y^3 \log X}\right) & \text{if } E \text{ is a non-CM curve.}\end{cases} \tag{6.3}$$

Here and in the next two instances, by $F \leqslant G + O\left(H\right)$, we mean that either $F - G < 0$ or $0 \leqslant F - G \ll H$. The theorem follows by combining (6.3) and (6.2) with (6.1).

Let us prove our claim. By an inclusion-exclusion argument, the following inequality holds for any number $X \geqslant 2$ and any integer Q:

$$\sum_{\substack{p\leqslant X\\ p\nmid N,\ d_p=j}} p \leqslant \sum_{h\mid Q} \mu(h) \sum_{\substack{p\leqslant X\\ p\nmid N,\ hj\mid d_p}} p.$$

Thus, applying partial summation and (3.1) to the last sum (as we did to obtain (5.1)), and noting that $\sum_{h|Q} |\mu(h)| = 2^{\omega(Q)}$, we obtain

$$\sum_{\substack{p\leqslant X\\ p\nmid N,\, d_p = j}} p \leqslant \mathrm{Li}\left(X^2\right)\sum_{h|Q}\frac{\mu(h)}{n_{L_{hj}}} + O\left(2^{\omega(Q)}X^2\exp\left(-B(\log X)^{5/14}\right)\right),$$

provided $2c_1(hj)^{14}N^2 \leqslant \log X$ for every $h \mid Q$.

We set $Q = Q(Y) := \prod_{q\leqslant Y} q$. Then $\log Q \sim Y$ as $Y \to \infty$ by the prime number theorem, and we may suppose that X and Y are large enough so that $QY \leqslant \exp(3Y)$, that is $2c_1(QY)^{14}N^2 \leqslant 2c_1\exp(42Y)\,N^2 \leqslant \log X$ (by definition of Y and our choice of constants).

Thus, since $2^{\omega(Q)} = 2^Y \ll (\log X)^{1/42}$, and since $\sum_{j\leqslant Y}\frac{1}{j} \ll \log Y \ll \log\log\log X$, we have

$$\begin{aligned}\mathcal{T}_1 := \sum_{\substack{p\leqslant X\\ p\nmid N,\, d_p\leqslant Y}}\frac{p}{d_p} &= \sum_{j\leqslant Y}\frac{1}{j}\sum_{\substack{p\leqslant X\\ p\nmid N,\, d_p = j}} p\\ &\leqslant \mathrm{Li}\left(X^2\right)\sum_{j\leqslant Y}\sum_{h|Q}\frac{\mu(h)}{jn_{L_{hj}}} + O\left(X^2\exp\left(-\tfrac{1}{2}B(\log X)^{5/14}\right)\right).\end{aligned} \tag{6.4}$$

Letting $S = \{hj : h \mid Q \text{ and } j \leqslant Y\}$, we have

$$\sum_{j\leqslant Y}\sum_{h|Q}\frac{\mu(h)}{jn_{L_{hj}}} = \sum_{k\in S}\frac{1}{n_{L_k}}\sum_{hj=k}\frac{\mu(h)}{j} = \sum_{k\in S}\frac{1}{kn_{L_k}}\sum_{h|k}\mu(h)\cdot h.$$

We complete the sum over k, noting that $k \notin S$ implies either $k > Y$ or $k = hj$ with $\mu(h) = 0$, and that $\sum_{h|k}\mu(h)\cdot h = (-1)^{\omega(k)}\phi(\mathrm{rad}(k))$, obtaining

$$\begin{aligned}\sum_{j\leqslant Y}\sum_{h|Q}\frac{\mu(h)}{jn_{L_{hj}}} &= \sum_{k=1}^{\infty}\frac{(-1)^{\omega(k)}\phi(\mathrm{rad}(k))}{kn_{L_k}} + O\left(\sum_{k>Y}\frac{1}{n_{L_k}}\right)\\ &= c_E + \begin{cases} O(1/Y) & \text{if } E \text{ has CM},\\ O\left(B_E/Y^3\right) & \text{if } E \text{ is a non-CM curve.}\end{cases}\end{aligned}$$

by (3.8). Combining this with (6.4) gives (6.3). □

7. Further remarks on the constant c_E

Notation in this section is as in the proof of Proposition 3.2. Let us first assume that E is a non-CM curve. Let $G = \varprojlim \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$, the product being over all primes ℓ, and let H denote the image of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ in G under ρ_E. For $n \geqslant 1$ an integer, there is a natural projection map from G to $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$; let

$$\Gamma_n := \ker\left(G \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})\right).$$

By Serre's open image theorem, the index $(G : H)$ is finite, hence there exist n such that $\Gamma_n < H$; let m denote the smallest such n. (In order to show that the growth of n_{L_k} is "regular", it is convenient to work with a large subgroup $\prod_\ell K_\ell \subset H$, with each K_ℓ having simple structure.) Now, the image of Gal $\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ in $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$ can be obtained by composing the maps

$$H \hookrightarrow G \twoheadrightarrow G/\Gamma_k \cong \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}),$$

and hence

$$n_{L_k} = [L_k : \mathbb{Q}] = |H/H \cap \Gamma_k|.$$

Write $m = \prod_{p|m} p^{m_p}$ and let $k = \prod_{p|k} p^{k_p}$ be given.
Claim: If $k_p \geqslant m_p$ for some p and $a \geqslant 1$, then

$$|H/H \cap \Gamma_{p^a \cdot k}| = |H/H \cap \Gamma_k| \cdot |\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}}|.$$

Moreover, if $k_p = 0$, we have $\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}} = \Gamma_1/\Gamma_{p^a} \cong \mathrm{GL}_2(\mathbb{Z}/p^a\mathbb{Z})$, and if $k_p > 0$ then

$$|\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}}| = p^{4a}.$$

Proof of claim: We note that

$$|H/H \cap \Gamma_{p^a \cdot k}| = |H/H \cap \Gamma_k| \cdot |(H \cap \Gamma_k)/(H \cap \Gamma_{p^a \cdot k})|$$

and

$$|(H \cap \Gamma_k)/(H \cap \Gamma_{p^a \cdot k})| = \frac{|(H \cap \Gamma_k)/(\Gamma_m \cap \Gamma_k)| \cdot |(\Gamma_m \cap \Gamma_k)/(\Gamma_m \cap \Gamma_{p^a k})|}{|(H \cap \Gamma_{p^a k})/(\Gamma_m \cap \Gamma_{p^a k})|}. \tag{7.1}$$

Let $N = \Gamma_m \cap \Gamma_k$ and $S = H \cap \Gamma_{p^a k}$. Since $\Gamma_m < H$ and (trivially) $\Gamma_{p^a k} < \Gamma_k$, we find that

$$S \cap N = (H \cap \Gamma_{p^a k}) \cap (\Gamma_m \cap \Gamma_k) = \Gamma_m \cap \Gamma_{p^a k}.$$

Moreover, since $k_p \geqslant m_p$, given any $h_1 \in H \cap \Gamma_k$ we can find $h_2 \in H \cap \Gamma_{p^a k}$ such that $h_1 = h_2 \cdot (1, 1, \ldots, 1, \gamma_p, 1, 1, \ldots)$, where $\gamma_p = I + p^{k_p} M$ and $M \in \mathrm{Mat}_2(\mathbb{Z}_p)$, and consequently

$$S \cdot N = (H \cap \Gamma_{p^a k}) \cdot (\Gamma_m \cap \Gamma_k) = H \cap \Gamma_k.$$

Now, by the second isomorphism theorem of group theory, $SN/N \cong S/S \cap N$, hence

$$(H \cap \Gamma_k)/(\Gamma_m \cap \Gamma_k) = SN/N \cong S/S \cap N = (H \cap \Gamma_{p^a k})/(\Gamma_m \cap \Gamma_{p^a k}),$$

which, together with (7.1), implies that

$$|(H \cap \Gamma_k)/(H \cap \Gamma_{p^a \cdot k})| = |(\Gamma_m \cap \Gamma_k)/(\Gamma_m \cap \Gamma_{p^a k})|.$$

With $[a, b]$ denoting the least common multiple of two integers a, b, we have $\Gamma_a \cap \Gamma_b = \Gamma_{[a,b]}$. Further, if $a \mid b$ and $(ab, c) = 1$, then $\Gamma_{ac}/\Gamma_{bc} \cong \Gamma_a/\Gamma_b$. Thus, again using that $k_p \geqslant m_p$, we find that

$$(\Gamma_m \cap \Gamma_k)/(\Gamma_m \cap \Gamma_{p^a k}) = \Gamma_{[m,k]}/\Gamma_{[m,p^a k]} \cong \Gamma_{p^{k_p}}/\Gamma_{p^{k_p+a}}.$$

Hence

$$|H/H \cap \Gamma_{p^a \cdot k}| = |H/H \cap \Gamma_k| \cdot |(H \cap \Gamma_k)/(H \cap \Gamma_{p^a \cdot k})| = |H/H \cap \Gamma_k| \cdot |\Gamma_{p^{k_p}}/\Gamma_{p^{k_p+a}}|,$$

and the first part of the claim is proved. The latter part of the claim follows from

$$|\Gamma_{p^{k_p}}/\Gamma_{p^{a+k_p}}| = \prod_{j=k_p}^{a+k_p-1} |\Gamma_{p^j}/\Gamma_{p^{j+1}}|$$

together with $\Gamma_{p^j}/\Gamma_{p^{j+1}} \cong \Gamma_p/\Gamma_{p^2}$, and $|\Gamma_p/\Gamma_{p^2}| = p^4$.

Now, let $\langle m\rangle$ be the set containing 1 and the positive integers composed only of primes dividing m. For any k we have $k = hj$ with $h \in \langle m\rangle$ and $(j, m) = 1$. We can further write $h = h_1h_2$ in a unique way with $h_1 \mid m$, $(h_1, h_2) = 1$, and $\nu_p > m_p$ for every $p \mid h_2$, where $p^{\nu_p}\| h_2$ and $p^{m_p}\| m$. From the above claim it follows that $n_{L_k} = n_{L_h} \cdot n_{L_j}$, that $n_{L_j} = |\mathrm{GL}_2(\mathbb{Z}/j\mathbb{Z})|$, and that

$$n_{L_h} = r_E(h_1)\prod_{p\mid h_2} p^{4(\nu_p-m_p)},$$

where $r_E(h_1)$ is a rational number depending only on E and h_1, $p^{\nu_p}\| h_2$, and $p^{m_p}\| m$.

We therefore have

$$\begin{aligned} c_E &= \sum_{h\in\langle m\rangle} \frac{(-1)^{\omega(h)}\phi(\mathrm{rad}(h))}{hn_{L_h}} \prod_{q\nmid m}\left(1-\sum_{k\geqslant 1}\frac{q-1}{q^k n_{L_{q^k}}}\right) \\ &= c\cdot\prod_{q\mid m}\left(1-\frac{q^3}{(q^2-1)(q^5-1)}\right)^{-1}\cdot\sum_{h\in\langle m\rangle}\frac{(-1)^{\omega(h)}\phi(\mathrm{rad}(h))}{hn_{L_h}}, \end{aligned}$$

with c as defined in (1.2). Using the fact that $n_{L_h} = r_E(h_1)\prod_{p\mid h_2} p^{4(\nu_p-m_p)}$, it is a straightforward matter to show that the sum over $h \in \langle m\rangle$ is equal to the rational number

$$\prod_{q\mid m}\left(1-\frac{q-1}{q^{m_q}(q^5-1)}\right)\sum_{h_1\mid m}\frac{(-1)^{\omega(h_1)}\phi(\mathrm{rad}(h_1))}{h_1 r_E(h_1)}\prod_{q\mid h_1}\left(1-\frac{q-1}{q^{m_q}(q^5-1)}\right)^{-1}.$$

The CM case is similar, except that $n_{L_{q^k}}$ (for all but finitely many q and $k \geqslant 1$) equals $(q-1)^2 \cdot q^{2(k-1)}$ if q splits in K, and is equal to $(q^2-1)\cdot q^{2(k-1)}$ if q is inert in K. (Recall that K denotes the quadratic imaginary field that contains the order by which E has CM.)

8. Further remarks on the error terms

Wu [**22**] has simplified the calculations involved in the proofs of Theorems 1.1 and 1.2, and improved on the error terms given by us. In the unconditional CM case, Kim [**9**] has made further improvements by using a different approach, namely using class field theory and a Bombieri-Vinogradov type theorem for number fields due to Huxley [**8**]. More precisely, in the case where E has CM, Wu obtained an error term of size $O_E((\log X)^{-1/14}))$, improving on our original error term $O_E(\log\log\log X/\log\log X)$; in fact his method, on noting that $n_{L_k} \leqslant k^2$ holds in the CM case (cf. (3.2)), gives an error term of size $O_E((\log X)^{-1/8})$. In [**9**] Kim greatly improved on the error term in the CM case, by showing that for any $A > 0$ we have, unconditionally, $\sum_{p\leqslant X} e_p = c_E \cdot \mathrm{Li}\left(X^2\right)\cdot\left\{1+O_{E,A}\left(\frac{1}{(\log X)^A}\right)\right\}$. Regarding conditional results, Wu [**22**] has shown that on GRH,

$$\sum_{p\leqslant X} e_p = c_E\cdot\mathrm{Li}\left(X^2\right)+O_E\left(X^{11/6}(\log X)^{1/3}\right),$$

whether or not E has CM. It is worth noting that on GRH, Wu's treatment, together with separating out supersingular primes, gives an improved error term in the case where E has CM, namely $\sum_{p\leqslant X} e_p = c_E\cdot\mathrm{Li}\left(X^2\right)+O_E\left(X^{7/4}(\log X)^{1/2}\right)$.

We will now outline Wu's argument by sketching a proof of this GRH-conditional CM result. As in the proofs of Theorems 1.1 and 1.2, the problem reduces, via partial summation and the Hasse bound, to showing that

$$\sum_{\substack{p\leqslant X\\ p\nmid N}} \frac{1}{d_p} = c_E \cdot \mathrm{Li}\,(X) \cdot \left\{1 + O_E\left(X^{-\frac{1}{4}}(\log X)^{\frac{3}{2}}\right)\right\}. \tag{8.1}$$

Briefly, we set $Y = Y(X) := X^{\frac{1}{4}}(\log X)^{-\frac{1}{2}}$. As in the proofs of Theorems 1.1 and 1.2, we use the fact that $\frac{1}{d_p} = \sum_{hj\mid d_p} \frac{\mu(h)}{j}$ to obtain

$$\sum_{\substack{p\leqslant X\\ p\nmid N}} \frac{1}{d_p} = \left\{\sum_{k\leqslant Y} + \sum_{Y<k\leqslant 2\sqrt{X}}\right\} \sum_{hj=k} \frac{\mu(h)}{j} \sum_{\substack{p\leqslant X\\ p\nmid N,\, k\mid d_p}} 1.$$

In considering the sum over $Y < k \leqslant 2\sqrt{X}$, we note, as we did in the proof of Lemma 3.6(b), that only the primes of ordinary reduction contribute. Then, again as in the proof of Lemma 3.6(b), we use the trivial estimate $|S_j(X; D, k)| \ll \frac{X}{k^2} + \frac{\sqrt{X}}{k}$. Thus,

$$\sum_{Y<k\leqslant 2\sqrt{X}} \sum_{hj=k} \frac{\mu(h)}{j} \sum_{\substack{p\leqslant X\\ p\nmid N,\, k\mid d_p}} 1 \ll \sum_{y<k\leqslant 2\sqrt{X}} \sum_{\substack{p\leqslant X\\ p\nmid N,\, k\mid d_p\\ a_p\neq 0}} 1 \ll \frac{X}{Y} + \sqrt{X}\log X.$$

We use Lemma 3.3(b) to handle the sum over $k \leqslant Y$, obtaining

$$\sum_{k\leqslant Y} \sum_{hj=k} \frac{\mu(h)}{j} \sum_{\substack{p\leqslant X\\ p\nmid N,\, k\mid d_p}} 1 = \mathrm{Li}\,(X) \sum_{k\leqslant y} \frac{1}{n_{L_k}} \sum_{hj=k} \frac{\mu(h)}{j} + O\left(Y\sqrt{X}\log(XN)\right).$$

We complete the sum, applying Lemma 3.4 to bound the error that arises. Combining everything, we obtain $\sum_{\substack{p\leqslant X\\ p\nmid N}} \frac{1}{d_p} = c_E{\cdot}\mathrm{Li}\,(X)\left(1 + O_E\left(\frac{Y(\log X)^2}{\sqrt{X}} + \frac{\log X}{Y}\right)\right)$. Since $Y = X^{\frac{1}{4}}(\log X)^{-\frac{1}{2}}$, this gives (8.1).

Acknowledgements

For providing corrections and useful comments, we are grateful to the anonymous referee, Valentin Blomer, Adam Felix, Nathan Jones, Sungjin Kim, and Jie Wu.

References

[1] I. Borosh, C. J. Moreno, and H. Porta, 'Elliptic curves over finite fields. II', Math. Comput., **29** (1975), 951–964. MR 0404264

[2] A. C. Cojocaru, 'Cyclicity of CM elliptic curves modulo p', *Trans. Amer. Math. Soc.*, **355** (2003), 2651–2662. MR 1975393

[3] A. C. Cojocaru, 'Questions about the reductions modulo primes of an elliptic curve', *Number Theory*, 61–79, CRM Proc. Lecture Notes **36**, Amer. Math. Soc., Providence, RI, 2011. MR 2076566

[4] A. C. Cojocaru and M. R. Murty, 'Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem', *Math. Ann.*, **330** (2004), 601–625. MR 2099195

[5] W. Duke, 'Almost all reductions modulo p of an elliptic curve have a large exponent', C. R. Math. Acad. Sci. Paris, **337** (2003), 689–692. MR 2030403

[6] H. Halberstam and H. E. Richert, *Sieve methods*, London Mathematical Society Monographs, No. 4, Academic Press, New York-London, 1974. MR 0424730

[7] C. Hooley, 'On Artin's conjecture', *J. Reine Angew. Math.*, **225** (1967), 209–220. MR 0207630

[8] M. N. Huxley, 'The large sieve inequality for algebraic number fields. III. Zero-density results', *J. London Math. Soc. (2)*, **3** (1971), 233–240. MR 0276196

[9] S. Kim, 'On the average exponent of CM elliptic curves modulo p', preprint (2012), arXiv:1207.6652.

[10] N. Koblitz, 'Elliptic curve cryptosystems', *Math. Comp.*, **48** (1987), 203–209. MR 866109

[11] P. Kurlberg and C. Pomerance, 'On a problem of Arnold: the average multiplicative order of a given integer', preprint (2011), arXiv:1108.5209.

[12] V. S. Miller, 'Use of elliptic curves in cryptography', *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, Lecture Notes in Comput. Sci., **218**, Springer, Berlin, 1986, 417–426. MR 851432

[13] M. R. Murty, 'On Artin's conjecture', J. Number Theory, **16** (1983), 147–168. MR 698163

[14] M. R. Murty, 'An analogue of Artin's conjecture for abelian extensions', *J. Number Theory*, **18** (1984), 241–248. MR 746861

[15] R. Schoof, 'The exponents of the groups of points on the reductions of an elliptic curve', *Arithmetic algebraic geometry (Texel, 1989)*, *Progr. Math.*, **89**, Birkhäuser, Boston MA, 1991, 325–335. MR 1085266

[16] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR 0263823

[17] J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.*, **15** (1972), 259–331. MR 0387283

[18] J.-P. Serre, 'Quelques applications du théorème de densité de Chebotarev', *Inst. Hautes Études Sci. Publ. Math.*, **54** (1981), 323–401. MR 644559

[19] J.-P. Serre, 'Résumé des cours de 1977–1978', *Annuaire du Collège de France 1978*, 67–70, *Œuvres, Collected papers Volume III, 1972–1984*, Springer-Verlag, Berlin, 1986, 465–468. MR 926691

[20] I. E. Shparlinski, 'Exponents of modular reductions of families of elliptic curves', *Rev. Un. Mat. Argentina*, **50** (2009), 69–74. MR 2643518

[21] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, **106**, Springer-Verlag, New York, 1986. MR 817210

[22] J. Wu, 'The average exponent of elliptic curves modulo p', preprint (2012), arXiv:1206.5929.

Department of Mathematics, KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden

E-mail address: tristanf@kth.se

Department of Mathematics, KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden

E-mail address: kurlberg@kth.se