

# Square-free orders for CM elliptic curves modulo $p$

Alina Carmen Cojocaru

Received: 5 July 2007 / Revised: 9 April 2008 / Published online: 27 June 2008  
© Springer-Verlag 2008

**Abstract** Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ , of conductor  $N$ , and with complex multiplication. We prove unconditional and conditional asymptotic formulae for the number of ordinary primes  $p \nmid N$ ,  $p \leq x$ , for which the group of points of the reduction of  $E$  modulo  $p$  has square-free order. These results are related to the problem of finding an asymptotic formula for the number of primes  $p$  for which the group of points of  $E$  modulo  $p$  is cyclic, first studied by Serre (1977). They are also related to the stronger problem about primitive points on  $E$  modulo  $p$ , formulated by Lang and Trotter (Bull Am Math Soc 83:289–292, 1977), and the one about the primality of the order of  $E$  modulo  $p$ , formulated by Koblitz [Pacific J. Math. 131(1):157–165, 1988].

**Mathematics Subject Classification (2000)** Primary 11G05; Secondary 11N36 · 11R45

## Contents

1	Introduction	588
2	Overview of the proofs	591
3	Preliminaries	594
3.1	The Chebotarev Density Theorem	594
3.2	The Brun–Titchmarsh Theorem	596
3.3	Division fields of CM elliptic curves	597

---

A. C. Cojocaru (✉)  
Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago,  
851 S. Morgan Str., 322 SEO, Chicago, IL 60607, USA  
e-mail: cojocaru@math.uic.edu

A. C. Cojocaru  
The Institute of Mathematics of the Romanian Academy, Bucharest, Romania

3.3.1 Generalities . . . . . 597  
 3.3.2 Estimates for the sizes of the conjugacy sets  $D_{k^2}$  . . . . . 598  
 3.4 Characterization of the square-freeness of  $\#E_p(\mathbb{F}_p)$  . . . . . 602  
 4 Proof of Theorem 1.1 . . . . . 604  
 4.1 Estimate for  $N(x, y)$  . . . . . 604  
 4.2 Estimate for  $M(x, y, 2\sqrt{x})$  . . . . . 605  
 4.3 Putting things together . . . . . 608  
 5 Proof of Theorem 1.2 . . . . . 609  
 6 The positivity of the density  $\delta_E$  . . . . . 611  
 7 Proof of Theorem 1.4 . . . . . 614

**1 Introduction**

Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and of conductor  $N$ . For a prime  $p$  of good reduction for  $E$  (that is,  $p \nmid N$ ), let  $E_p$  be the reduction of  $E$  modulo  $p$ . This is an elliptic curve defined over the finite field  $\mathbb{F}_p$  with  $p$  elements, whose  $\mathbb{F}_p$ -rational points  $E_p(\mathbb{F}_p)$  form a finite abelian group isomorphic to  $\mathbb{Z}/d_p\mathbb{Z} \times \mathbb{Z}/d_p e_p\mathbb{Z}$  for some uniquely determined integers  $d_p, e_p$ , depending on  $p$  and  $E$ . Moreover, the order of this group can be written as  $\#E_p(\mathbb{F}_p) = p + 1 - a_p$  for some integer  $a_p$  satisfying Hasse’s inequality  $|a_p| \leq 2\sqrt{p}$ . If  $p \geq 5$  and  $a_p = 0$ , we say that  $p$  is a *supersingular* prime for  $E$ ; if  $p \geq 5$  and  $a_p \neq 0$ , we say that  $p$  is an *ordinary* prime for  $E$ .

Over the past three decades there has been an increasing interest in studying the properties of the group  $E_p(\mathbb{F}_p)$  as  $p$  varies over rational primes  $\nmid N$ . Our purpose in this paper is to determine an asymptotic formula for the function

$$h_E(x, \mathbb{Q}) := \#\{p \leq x : p \nmid N, a_p \neq 0, \#E_p(\mathbb{F}_p) \text{ is square-free}\} \tag{1}$$

in the case of an elliptic curve with complex multiplication (CM).

Before stating the main result, let us recall what CM means. If  $\overline{\mathbb{Q}}$  denotes an algebraic closure of  $\mathbb{Q}$ , and  $\text{End}_{\overline{\mathbb{Q}}}(E)$  denotes the ring of endomorphisms of  $E$  over  $\overline{\mathbb{Q}}$ , then we have a natural embedding  $\mathbb{Z} \leq \text{End}_{\overline{\mathbb{Q}}}(E)$ . If this embedding is an isomorphism, we say that  $E$  is *without complex multiplication* (or *non-CM*). If it is a strict embedding, then  $\text{End}_{\overline{\mathbb{Q}}}(E)$  is an order  $\mathcal{O}$  in an imaginary quadratic field  $K$  of class number 1. In this case we say that  $E$  has *complex multiplication* by  $\mathcal{O}$ , and that  $K$  is its *CM field*.

The main results of the paper are as follows.

**Theorem 1.1** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and of conductor  $N$ . Assume that  $E$  has complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . Let  $x \in \mathbb{R}$  be such that  $\log x > 3N^2$ . Then there exists a constant  $\delta_E$ , depending on  $E$ , such that*

$$h_E(x, \mathbb{Q}) = \delta_E \text{li } x + O_N \left( \frac{x}{(\log x)(\log \log \log x)} \right), \tag{2}$$

or, more precisely,

$$h_E(x, \mathbb{Q}) = \delta_E \text{li } x + O \left( \frac{x}{(\log x)(\log \log \frac{\log x}{N^2})} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}} \right). \tag{3}$$

Here,  $\operatorname{li} x = \int_2^\infty \frac{dt}{\log t}$  is the logarithmic integral, the constant implied in the  $O_N$ -notation depends on  $N$ , and the constant implied in the  $O$ -notation is absolute. The density  $\delta_E$  will be given explicitly in formula (40) of Sect. 6.

In our investigations towards the asymptotic formula for  $h_E(x, \mathbb{Q})$  we will be interested not only in the main term of the formula, but also in the error terms, as already apparent in our statement of Theorem 1.1. A natural problem is then to look for the best error term which we can obtain. Under the assumption of a generalized Riemann hypothesis (GRH), we will obtain an error term significantly smaller than the one in (3):

**Theorem 1.2** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and of conductor  $N$ . Assume that  $E$  has complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . Assume the validity of GRH for the Dedekind zeta functions of the division fields of  $E$ . Then there exists a constant  $\delta_E$ , depending on  $E$ , such that*

$$h_E(x, \mathbb{Q}) = \delta_E \operatorname{li} x + O\left(x^{5/6}(\log x)^2(\log Nx)^{1/3}\right). \tag{4}$$

The implied  $O$ -constant is absolute.

Certainly, it is of interest to also know when the density  $\delta_E$  is positive. We can show:

**Theorem 1.3** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and of conductor  $N$ . Assume that  $E$  has complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . Let  $\delta_E$  be the density of the ordinary primes  $p$  for which  $\#E_p(\mathbb{F}_p)$  is square-free.*

1. If  $K = \mathbb{Q}(\sqrt{-7})$ , then  $\delta_E = 0$ .
2. If  $K$  is one of  $\mathbb{Q}(\sqrt{-11})$ ,  $\mathbb{Q}(\sqrt{-19})$ ,  $\mathbb{Q}(\sqrt{-43})$ ,  $\mathbb{Q}(\sqrt{-67})$ , or  $\mathbb{Q}(\sqrt{-163})$ , then  $\delta_E > 0$ .

Let us remark that a thorough study of densities such as  $\delta_E$  uses methods of a different nature than the ones developed in this paper and shall be relegated to future investigations.

Having explicit error terms in the asymptotic formula for  $h_E(x, \mathbb{Q})$  enables us to find estimates (in terms of  $N$ ) for the smallest (ordinary) prime  $p = p_E$  for which  $\#E_p(\mathbb{F}_p)$  is square-free:

**Theorem 1.4** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and of conductor  $N$ . Assume that  $E$  has complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . Let  $p_E$  be the smallest ordinary prime  $p$  for which  $\#E_p(\mathbb{F}_p)$  is square-free. If  $\delta_E > 0$ , then:*

1. Unconditionally, we have

$$p_E = O\left(\exp\left(eN^3\right)\right);$$

2. Under GRH for the Dedekind zeta functions of the division fields of  $E$ , we have

$$p_E = O_\varepsilon \left( (\log N)^{2+\varepsilon} \right)$$

for any  $0 < \varepsilon < 1$ .

The implied  $O$ -constant is absolute, and the implied  $O_\varepsilon$ -constant depends only on  $\varepsilon$ .

In studying the function  $h_E(x, \mathbb{Q})$  we have been motivated by long-standing conjectures about the structure of  $E_p(\mathbb{F}_p)$ , as explained in the following paragraphs.

In 1977 [12], S. Lang and H. Trotter formulated an elliptic curve analogue of Artin's primitive root conjecture, which asserts that if  $E$  is an elliptic curve defined over  $\mathbb{Q}$ , of conductor  $N$ , and of arithmetic rank  $\geq 1$ , and if  $a$  is a rational point on  $E$  of infinite order, then the density of the primes  $p \nmid N$  for which  $a \pmod{p}$  generates  $E_p(\mathbb{F}_p)$  exists. This conjecture was investigated by R. Gupta and R. Murty [9], who obtained an asymptotic formula for the number of ordinary primes  $p$  for which  $\langle a \pmod{p} \rangle = E_p(\mathbb{F}_p)$  in the case of a CM elliptic curve  $E$  and under the assumption of GRH.

We remark that in Lang and Trotter's conjectural statement, two requirements on  $E_p(\mathbb{F}_p)$  are being made: it must be a cyclic group *and* it must be generated by  $a \pmod{p}$ . Therefore, a natural subproblem to consider is to show that, given an elliptic curve  $E$  over  $\mathbb{Q}$ , the density of the primes  $p$  for which  $E_p(\mathbb{F}_p)$  is cyclic exists. This latter problem has been studied extensively by several people (J-P Serre, R Murty, R Gupta, the author etc; see [4] and the references therein). Moreover, we remark that if the order of  $E_p(\mathbb{F}_p)$  is prime, then the two requirements of the Lang-Trotter conjecture are satisfied for any point  $a$ . This observation was first made by N. Koblitz in 1988 [10], who also formulated a conjectural asymptotic formula for the number of primes  $p$  for which  $\#E_p(\mathbb{F}_p)$  is prime. For investigations on this conjecture, see [1, 5, 13, 24].

The study of the square-freeness of  $\#E_p(\mathbb{F}_p)$  might be viewed as an intermediate problem between the study of the cyclicity of  $E_p(\mathbb{F}_p)$  and that of the primality of  $\#E_p(\mathbb{F}_p)$ . Since the very different properties of elliptic curves with and without CM lead to different analyzes in this type of problems, in the present paper we focus our attention only on the case of elliptic curves with CM. The more general situation of CM elliptic curves over number fields other than  $\mathbb{Q}$  and/or with CM by an order in an imaginary quadratic field follows the same main steps as the current work, however involves additional technical features that will be addressed in a separate paper. The case of elliptic curves without CM is based on different ideas and is also relegated to a separate paper.

**Notation** Throughout the paper, in addition to the notation introduced above, the following standard notation will be used.  $p$  denotes a prime of good reduction for  $E$ ;  $q, \ell$  denote rational primes;  $k$  denotes a positive integer;  $x, y$  denote positive real numbers (approaching  $\infty$ ). For a complex number  $z \in \mathbb{C}$ ,  $\bar{z}$  denotes its complex conjugate. For a positive integer  $n$ ,  $\phi(n)$  denotes the Euler function of  $n$  (i.e. the number of positive integers  $\leq n$  and coprime to  $n$ ), and  $\nu(n)$  denotes the number of distinct prime divisors of  $n$ .  $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$  denotes the group of 2 by 2 invertible matrices with entries in  $\mathbb{Z}/n\mathbb{Z}$ , whose trace and determinant we call  $\mathrm{tr}$  and  $\mathrm{det}$ . For

an algebraic number field  $K$ ,  $\mathcal{O}_K$  denotes its ring of algebraic integers,  $N_{K/\mathbb{Q}}(\cdot)$  its norm map over  $\mathbb{Q}$ ,  $d_K$  its absolute discriminant over  $\mathbb{Q}$ , and  $\Phi(\cdot)$  its generalized Euler function. We recall that if  $\mathfrak{q}$  is a nonzero prime ideal of  $\mathcal{O}_K$  and  $n \geq 1$ , then

$$\Phi(\mathfrak{q}^n) := N_{K/\mathbb{Q}}(\mathfrak{q}^n) \left( 1 - \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{q})} \right);$$

this definition is extended to all the nonzero ideals of  $\mathcal{O}_K$  by multiplicativity. We denote by  $\mathfrak{q}$  and  $\mathfrak{p}$  nonzero prime ideals of  $\mathcal{O}_K$ , and by  $\mathbb{F}_{\mathfrak{p}}$  and  $E_{\mathfrak{p}}$  the residue field and the reduction of  $E$  at  $\mathfrak{p}$ , respectively. We denote by  $\gcd$  and  $\text{lcm}$  the greatest common divisor and the least common multiple of two integers or two integral ideals of a number field. For two functions  $f, g : D \subseteq \mathbb{C} \rightarrow \mathbb{R}$ , with  $g$  taking positive values, we write  $f(x) = O(g(x))$ ,  $f(x) \ll g(x)$ , or  $g(x) \gg f(x)$  if there exists a positive constant  $M$  such that  $|f(x)| \leq Mg(x)$  for any  $x \in D$ . In case  $f$  takes positive values and  $f(x) \ll g(x) \ll f(x)$ , we write  $f(x) \asymp g(x)$ . If  $D$  is infinite and  $g$  is nonzero on  $D$ , we write  $f(x) \sim g(x)$  if  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$ , and  $f(x) = o(g(x))$  if  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 0$ . We make the following convention about the implicit  $\ll, \gg, \asymp$  and  $O$ -constants: whenever we write  $\ll_c, \gg_c, \asymp_c$  or  $O_c$  for some  $c$ , we indicate that the implicit constant  $M$  depends on  $c$ ; whenever we write  $\ll, \gg, \asymp$  or  $O$ , we indicate that the implicit constant  $M$  is absolute.

## 2 Overview of the proofs

In Sect. 1 we remarked that the main problem of this paper might be viewed as a variant of the elliptic curve analogue of Artin’s primitive root conjecture. In 1965 [7], C. Hooley obtained a conditional (that is, under a certain GRH) proof of Artin’s primitive root conjecture by first observing that an integer  $a$  is a primitive root modulo a prime  $p$  if and only if  $p$  does not split completely in certain finite Galois extensions of the cyclotomic fields  $\mathbb{Q}(\zeta_q)$  for any prime  $q \neq p$ ; then he used the simple asymptotic sieve to sift out these primes  $p$ . Here,  $\zeta_q$  denotes a primitive  $q$ th root of unity. The arguments in Hooley’s proof involve the use of conditional effective versions of the Chebotarev Density Theorem and, more significantly, sieve estimates, among which the classical Brun–Titchmarsh Theorem. In 1977 [14, 18], Serre used an elliptic curve adaptation of Hooley’s analysis to prove, under a certain GRH, an asymptotic formula for the number of primes  $p$  for which the reduction  $E_p$  of a fixed elliptic curve  $E$  gives a cyclic group. More precisely, he observed that  $E_p(\mathbb{F}_p)$  is cyclic if and only if  $p$  does not split completely in the division fields  $\mathbb{Q}(E[q])$  (to be introduced below) for any prime  $q \neq p$ ; then he used the simple asymptotic sieve to sift out these primes  $p$ . Serre’s arguments involved again the use of the conditional effective versions of the Chebotarev Density Theorem and the Brun–Titchmarsh Theorem.

It is natural to suspect that the problem considered in this paper could be approached similarly, namely it could be translated into “Chebotarev conditions” and then treated via the simple asymptotic sieve. Indeed, as a *starting point* we proceed along these lines, as follows.

We fix  $E$  an elliptic curve defined over  $\mathbb{Q}$ , of conductor  $N$ , with complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . With the notation introduced in Sect. 1, we note that

$$h_E(x, \mathbb{Q}) = \sum_k \mu(k) \#\left\{p \leq x : p \nmid N, a_p \neq 0, \#E_p(\mathbb{F}_p) \equiv 0 \pmod{k^2}\right\}, \tag{5}$$

where the sum  $\sum_k$  is over positive integers  $k$  such that  $k^2 | (p + 1 - a_p)$  for some  $p \leq x$ , hence, from Hasse’s inequality, such that  $k \leq 2\sqrt{x}$ .

Now we need to recall a few classical facts about elliptic curves. For precise references, see [22]. For a positive integer  $k$ , let  $E[k]$  denote the group of  $k$ -division points of  $E$  (i.e. the complex points of  $E$  of order dividing  $k$ ). Let  $L_k := K(E[k])$  be the  $k$ -division field of  $E$  over  $K$  (i.e. the field obtained by adjoining to  $K$  the  $x$  and  $y$  coordinates of the  $k$ -division points of  $E$ ). We know that  $L_k$  is a finite, Galois extension of  $K$ , whose ramified primes are divisors of  $kN$ , and which contains the cyclotomic field  $\mathbb{Q}(\zeta_k)$  (here,  $\zeta_k$  denotes a primitive  $k$ th root of unity). We denote by  $n(k) = [L_k : K]$  the degree of  $L_k/K$ , by  $d(k)$  the absolute discriminant of  $L_k/\mathbb{Q}$ , and by  $G_k = \text{Gal}(L_k/K)$  the Galois group of  $L_k/K$ . We recall that we can define a natural Galois representation

$$\phi_k : G_k \longrightarrow \text{GL}_2(\mathbb{Z}/k\mathbb{Z})$$

associated to  $E/K$ , which has the important properties that it is injective and

$$\text{tr } \phi_k(\sigma_{\mathfrak{p}}) \equiv a_{\mathfrak{p}} \pmod{k}, \tag{6}$$

$$\det \phi_k(\sigma_{\mathfrak{p}}) \equiv N_{K/\mathbb{Q}}(\mathfrak{p}) \pmod{k} \tag{7}$$

for any integer  $k$  and prime  $\mathfrak{p}$  such that  $\mathfrak{p} \nmid kN$ , where  $\sigma_{\mathfrak{p}}$  denotes the Artin symbol of  $\mathfrak{p}$  in  $L_k/K$  and  $a_{\mathfrak{p}} := N_{K/\mathbb{Q}}(\mathfrak{p}) + 1 - \#E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ . We set

$$D_k := \{g \in \phi_k(G_k) : \det g + 1 - \text{tr } g \equiv 0 \pmod{k}\}. \tag{8}$$

Now let  $p \nmid kN$  be an ordinary prime for  $E/\mathbb{Q}$ . This means that  $p$  splits completely in  $K$ , say as  $p\mathcal{O}_K = \mathfrak{p} \cdot \bar{\mathfrak{p}}$ . Then  $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$  and  $a_{\mathfrak{p}} = a_p$ , and so, using (6) and (7), we see that the condition  $\#E_p(\mathbb{F}_p) \equiv 0 \pmod{k^2}$  is equivalent to

$$\det \phi_{k^2}(\sigma_{\mathfrak{p}}) + 1 - \text{tr } \phi_{k^2}(\sigma_{\mathfrak{p}}) \equiv 0 \pmod{k^2}, \tag{9}$$

where  $\sigma_{\mathfrak{p}}$  is the Artin symbol of  $\mathfrak{p}$  in  $L_{k^2}/K$ . Using notation (8), we obtain that

$$\begin{aligned} \#\left\{p \leq x : p \nmid kN, a_p \neq 0, \#E_p(\mathbb{F}_p) \equiv 0 \pmod{k^2}\right\} &\sim \frac{1}{2} \#\left\{\mathfrak{p} \leq \mathcal{O}_K : N_{K/\mathbb{Q}}(\mathfrak{p}) \right. \\ &\leq x, \mathfrak{p} \nmid kN, \phi_{k^2}(\sigma_{\mathfrak{p}}) \subseteq D_{k^2}\left.\right\}; \end{aligned} \tag{10}$$

thus our problem has been translated into general Chebotarev conditions.

As usual, let us note that by using the strongest effective Chebotarev Density Theorem (to be discussed in the following section) to estimate the cardinality of the right hand side of (10), we obtain error terms of the form  $O_{k,N}(x^{\frac{1}{2}} \log x)$  for each  $k \leq 2\sqrt{x}$ . However, from (5) and (10) we see that the expected main term for  $h_E(x, \mathbb{Q})$  is  $\delta_E \operatorname{li} x \sim \delta_E \frac{x}{\log x}$ , with

$$\delta_E = \frac{1}{2} \sum_{k \geq 1} \frac{\mu(k) \# D_{k^2}}{[K(E[k^2]) : K]}. \tag{11}$$

Thus we will be able to use the Chebotarev Density Theorem *only* in a *suitably small* range of  $k$ . This suggests that we write, instead,

$$h_E(x, \mathbb{Q}) = N(x, y) + M(x, y, 2\sqrt{x}) + O\left(\frac{x}{(\log x)^B}\right) \tag{12}$$

for any  $B > 0$ , where

$$N(x, y) := \frac{1}{2} \sum_{\substack{k \leq 2\sqrt{x} \\ q|k \Rightarrow q \leq y}} \mu(k) \# \{ \mathfrak{p} \leq \mathcal{O}_K : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathfrak{p} \nmid kN, \phi_{k^2}(\sigma_{\mathfrak{p}}) \subseteq D_{k^2} \}, \tag{13}$$

$$M(x, y, 2\sqrt{x}) := O\left( \sum_{y < q \leq 2\sqrt{x}} \# \{ p \leq x : p \nmid qN, a_p \neq 0, \#E_p(\mathbb{F}_p) \equiv 0 \pmod{q^2} \} \right), \tag{14}$$

and where  $y = y(x)$  is a positive real number, depending on  $x$ , to be chosen optimally.<sup>1</sup> The third term comes from an effective version of (10).

Another way of splitting the summation describing  $h_E(x, \mathbb{Q})$  (inspired by the methods developed in [6]) is

$$h_E(x, \mathbb{Q}) = \mathcal{N}(x, y) + \mathcal{M}(x, y, 2\sqrt{x}) + O\left(x^{1/2} \log x\right), \tag{15}$$

where

$$\mathcal{N}(x, y) := \frac{1}{2} \sum_{k \leq y} \mu(k) \# \{ \mathfrak{p} \leq \mathcal{O}_K : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathfrak{p} \nmid kN, \phi_{k^2}(\sigma_{\mathfrak{p}}) \subseteq D_{k^2} \} \tag{16}$$

<sup>1</sup> We recall that, throughout the paper,  $q$  denotes a rational prime.

and

$$\mathcal{M}(x, y, 2\sqrt{x}) := O \left( \sum_{y < k \leq 2\sqrt{x}} \# \left\{ p \leq x : p \nmid kN, a_p \neq 0, \#E_p(\mathbb{F}_p) \equiv 0 \pmod{k^2} \right\} \right). \tag{17}$$

Again,  $y = y(x)$  is some parameter depending on  $x$ , to be chosen optimally. The third term comes from an effective version of (10), under GRH.

The sums  $N(x, y)$  and  $\mathcal{N}(x, y)$ , respectively, will give the main term in our final formula for  $h_E(x, \mathbb{Q})$  and will be estimated using effective versions of the Chebotarev Density Theorem. The terms  $M(x, y, 2\sqrt{x})$  and  $\mathcal{M}(x, y, 2\sqrt{x})$ , respectively, will provide the error terms in our final formula and will be estimated using various sieve methods.

We emphasize that the difficulties lie in estimating  $M(x, y, 2\sqrt{x})$  and  $\mathcal{M}(x, y, 2\sqrt{x})$ . For example, the classical Brun–Titchmarsh Theorem is not powerful enough for our problem and thus new ideas are needed now.

We also remark that Hooley and Serre used splittings of type (12) in their treatments of the Artin primitive root conjecture and of the cyclicity of  $E_p(\mathbb{F}_p)$ . In our treatment of  $h_E(x, \mathbb{Q})$  we will use (12) to obtain an unconditional asymptotic formula, and (15) to obtain a conditional (upon GRH) asymptotic formula, with improved error terms.<sup>2</sup>

In our analysis of  $h_E(x, \mathbb{Q})$  we will be careful to keep track of the dependence of all the occurring error terms on the conductor  $N$  of  $E$ . This feature will enable us to find upper bounds in terms of  $N$  for the smallest prime  $p$  for which  $\#E_p(\mathbb{F}_p)$  is square-free, by comparing the main term with the final error terms.

### 3 Preliminaries

#### 3.1 The Chebotarev Density Theorem

Let  $L/K$  be a finite Galois extension of number fields, of Galois group  $G$ . Let  $n_L$  be the degree and  $d_L$  the absolute discriminant of  $L/\mathbb{Q}$ ; let  $n_K$  be the degree and  $d_K$  the absolute discriminant of  $K/\mathbb{Q}$ . We denote by  $\zeta_L$  the Dedekind zeta function of  $L$ . Let  $C$  be a conjugacy set in  $G$ , that is,  $C$  is a finite union of conjugacy classes of  $G$ . The set of conjugacy classes contained in  $C$  is denoted by  $\tilde{C}$ , and the set of conjugacy classes contained in  $G$  is denoted by  $\tilde{G}$ . We denote by  $\mathcal{P}(L/K)$  the set of rational primes  $p$  which lie below primes of  $K$  which ramify in  $L/K$ . Then we set

$$M(L/K) := (\#G)d_K^{1/n_K} \prod_{p \in \mathcal{P}(L/K)} p.$$

<sup>2</sup> A natural splitting like (15) does not seem to work in the classical case of Artin’s primitive root conjecture.

We define

$$\pi_C(x, L/K) := \#\{\mathfrak{p} \leq \overline{\mathcal{O}_K} : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathfrak{p} \text{ unramified in } L/K, \sigma_{\mathfrak{p}} \subseteq C\},$$

where  $\sigma_{\mathfrak{p}}$  is the Artin symbol of  $\mathfrak{p}$  in the extension  $L/K$ .

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

$$\pi_C(x, L/K) \sim \frac{\#C}{\#G} \operatorname{li} x.$$

Effective versions of this theorem were first derived by J Lagarias and A Odlyzko (see [11]). It is their versions, as refined by J-P Serre (see [19]), that we shall be using in our proofs. We state them below.

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

$$\pi_C(x, L/K) = \frac{\#C}{\#G} \operatorname{li} x + O\left((\#C)x^{1/2}n_K \log M(L/K)x\right).$$

*The implied O-constant is absolute.*

If, in addition to GRH, we assume Artin’s Holomorphy Conjecture (denoted AHC), then the error term above has a better dependence on  $C$ . Indeed, we have the following result of [15, Cor. 3.7, p. 265]:

**Theorem 3.2** *Assuming GRH for the Dedekind zeta function of  $L$ , together with AHC for the Artin  $L$ -functions of  $L/K$ , we have that*

$$\pi_C(x, L/K) = \frac{\#C}{\#G} \operatorname{li} x + O\left((\#C)^{1/2}x^{1/2}n_K \log M(L/K)x\right).$$

*The implied O-constant is absolute.*

Finally, we have the following unconditional version:

**Theorem 3.3** *There exist positive constants  $A$  and  $c$ , with  $A$  effective and  $c$  absolute, such that, if*

$$\sqrt{\frac{\log x}{n_L}} \geq c \max \left\{ \log d_L, d_L^{1/n_L} \right\},$$

*then*

$$\pi_C(x, L/K) = \frac{\#C}{\#G} \operatorname{li} x + O\left(\left(\#\tilde{C}\right)x \exp\left(-A\sqrt{\frac{\log x}{n_L}}\right)\right),$$

*where, we recall,  $\tilde{C}$  denotes the set of conjugacy classes contained in  $C$ . The implied O-constant is absolute.*

The following result is often very helpful in estimating the error terms in the effective Chebotarev Density Theorem. Its proof is given in [19, p. 130] and is based on a result of Hensel.

**Lemma 3.4** *Let  $L/K$  be a finite Galois extension of number fields. Using the notation introduced above, we have that*

$$\log d_L \leq \#G \log d_K + n_L \left(1 - \frac{1}{\#G}\right) \sum_{p \in \mathcal{P}(L/K)} \log p + n_L \log \#G.$$

### 3.2 The Brun–Titchmarsh Theorem

In our analysis of  $h_E(x, \mathbb{Q})$  we will need information about primes in arithmetic progressions, such as the upper bounds provided by the Brun–Titchmarsh Theorem and its generalizations. We recall them below.

**Theorem 3.5** (The Brun–Titchmarsh Theorem) *Let  $k \geq 1$  and  $a$  be fixed coprime integers. For any real number  $x$  with  $x > k$  we have*

$$\pi(x, k, a) \ll \frac{x}{\phi(k) \log \frac{x}{k}},$$

where

$$\pi(x, k, a) := \#\{p \leq x : p \equiv a \pmod{k}\}.$$

By using the sieve of Eratosthenes, we obtain the following weak analogue of Theorem 3.5 for imaginary quadratic fields (for a proof, see [3, pp. 2655–2657]).

**Lemma 3.6** *Let  $x > 0$  and let  $D, k$  be fixed positive integers with  $k < \sqrt{x} - 1$ . Then*

$$\begin{aligned} S_k^1 &:= \#\left\{p \leq x : p = (\alpha k + 1)^2 + D\beta^2 k^2 \text{ for some } \alpha, \beta \in \mathbb{Z}\right\} \\ &= O\left(\left(\frac{\sqrt{x}}{k} + 1\right) \frac{\sqrt{x} \log \log x}{k\sqrt{D} \log \frac{\sqrt{x}-1}{k}}\right); \end{aligned}$$

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

*Remark 3.7* With notation as in Lemma 3.6, we see that for any  $k, x$ , and for each  $1 \leq i \leq 2$ ,

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

The sieve argument is invoked for obtaining a saving of  $\frac{\log \log x}{\log x}$  in these estimates.

A general number field analogue of Theorem 3.5 was obtained by Schaal [17] as an application of the large sieve for number fields, which generalizes a large sieve inequality of Bombieri and Davenport and improves a prior number field version due to Huxley.

**Theorem 3.8** *Let  $K$  be a number field of degree  $n_K$  and absolute discriminant  $d_K$ , having  $r_1$  real embeddings into  $\mathbb{C}$  and  $2r_2$  complex conjugate embeddings into  $\mathbb{C}$ . Let  $\alpha_K$  be the residue of the Dedekind zeta function of  $K$  at  $s = 1$ . Let  $I$  be an integral ideal of  $K$  and let  $\beta \in \mathcal{O}_K$  be such that  $\gcd\{\beta, I\} = 1$ . We take  $M_1, \dots, M_{r_1} \in [0, \infty)$  and  $P_1, \dots, P_{n_K} \in (0, \infty)$  with  $P_l = P_{l+r_2}$  for  $l = r_1 + 1, \dots, r_1 + r_2$ . For  $\omega \in \mathcal{O}_K$  we denote by  $\omega^{(l)}$  its  $l$ th conjugate. We consider the set*

$$S := \{\omega \in \mathcal{O}_K : \omega \equiv \beta \pmod{I}, (\omega) \text{ a prime ideal, and } \omega \text{ satisfies (C)}\},$$

where conditions (C) are as follows:

$$M_l \leq \omega^{(l)} \leq M_l + P_l, \quad \forall 1 \leq l \leq r_1,$$

$$|\omega^{(l)}| \leq P_l, \quad \forall r_1 + 1 \leq l \leq n_K.$$

If  $P := P_1 \dots P_{n_K} \geq 2$  and  $N_{K/\mathbb{Q}}(I) \leq \frac{P}{(\log P)^{2r+2/n_K}}$ , with  $r := r_1 + r_2 - 1$ , then

$$\#S \leq \frac{2^{3r_2+1}}{\alpha_K \sqrt{d_K}} \cdot \frac{P}{\Phi(I) \log \frac{P}{N_{K/\mathbb{Q}}(I)}} \left\{ 1 + O_K \left( \left( \log \frac{P}{N_{K/\mathbb{Q}}(I)} \right)^{-1/n_K} \right) \right\},$$

where the  $O_K$ -constant above depends on  $K$  and is independent of  $I$ .

### 3.3 Division fields of CM elliptic curves

Our proofs of Theorems 1.1 and 1.2 will also rely heavily on the properties of the division fields of CM elliptic curves. We recall them below.

#### 3.3.1 Generalities

**Proposition 3.9** *Let  $E$  be an elliptic curve defined over a field  $K$  and of conductor  $N$ . We keep the notation introduced in Sects. 1 and 2. Then for any positive integer  $k$ , we have the following:*

1.  $L_k/K$  is a finite Galois extension for which  $\text{Gal}(L_k/K) \leq \text{GL}_2(\mathbb{Z}/k\mathbb{Z})$ . Consequently,

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

2. the ramified primes of  $L_k/\mathbb{Q}$  are divisors of  $kN$ ;
3. the cyclotomic field  $\mathbb{Q}(\zeta_k)$  is contained in  $L_k$ ; therefore

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

and a rational prime  $p$  which splits completely in  $L_k$  satisfies  $p \equiv 1 \pmod{k}$ .

For a proof, we refer the reader to [22, pp. 90, 98, 179].

Proposition 3.9 provides us with upper and lower bounds for the degree  $n(k)$  of the extension  $L_k/K$ . In the case of a CM elliptic curve we have the following more precise estimates:

**Proposition 3.10** *Let  $E$  be a CM elliptic curve defined over  $\mathbb{Q}$ , with complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ .*

1. For any positive integer  $k \geq 3$ , we have

$$n(k) \asymp \Phi(k\mathcal{O}_K). \tag{18}$$

In particular, from (18) we deduce that

$$\phi(k)^2 \ll n(k) \ll k^2. \tag{19}$$

2. Let  $I$  be a nonzero ideal of  $\mathcal{O}_K$  such that  $\gcd\{I, 6N\} = 1$ , and let  $E[I]$  denote the group of  $I$ -division points of  $E/K$ . Then, by adjoining to  $K$  the  $x$  and  $y$  coordinates of the points of  $E[I]$ , we obtain a finite Galois extension of  $K$  which is unramified outside  $6NI$ , totally ramified at the primes dividing  $I$ , and has Galois group equal to the unit group  $(\mathcal{O}_K/I)^\times$ . For an arbitrary nonzero ideal  $I$ , we have that  $\text{Gal}(K(E[I])/K)$  embeds into  $(\mathcal{O}_K/I)^\times$ , hence is abelian.

This proposition is a consequence of the theory of complex multiplication; the reader may consult [23, Sect. 5 of Chap. II], [8] or [16, Sect. 5] for a proof.

### 3.3.2 Estimates for the sizes of the conjugacy sets $D_{k^2}$

In order to find an asymptotic formula for  $h_E(x, \mathbb{Q})$ , we will need estimates for the sizes of the conjugacy sets  $D_{k^2}$  defined in Sect. 2. To obtain such estimates, it is useful to have an explicit realization of the Galois groups  $G_{k^2} = \text{Gal}(K(E[k^2])/K)$  as matrix groups.

**Lemma 3.11** *Let  $E$  be a CM elliptic curve defined over  $\mathbb{Q}$ , with complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K = \mathbb{Q}(\sqrt{-D})$ , where  $D$  is positive and square-free. Let  $q$  be an odd rational prime and  $n$  a positive integer.*

1. If  $q$  splits completely in  $K/\mathbb{Q}$ , then

$$\text{Gal}(K(E[q^n])/K) \leq \left\{ \begin{pmatrix} a + b\sqrt{-D} & 0 \\ 0 & a + b\sqrt{-D} \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/q^n\mathbb{Z}) \right\}. \tag{20}$$

2. If  $q$  is inert in  $K/\mathbb{Q}$ , then

$$\text{Gal}(K(E[q^n])/K) \leq \left\{ \begin{pmatrix} a & -bD \\ b & a \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/q^n\mathbb{Z}) \right\} \tag{21}$$

in the case  $-D \equiv 2, 3 \pmod{4}$ , and

$$\text{Gal}(K(E[q^n])/K) \leq \left\{ \begin{pmatrix} a & -b\frac{D+1}{4} \\ b & a+b \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/q^n\mathbb{Z}) \right\} \tag{22}$$

in the case  $-D \equiv 1 \pmod{4}$ .

*Proof* First we recall that, since  $E$  has complex multiplication by  $\mathcal{O}_K$ , we have an isomorphism

$$\begin{aligned} \frac{\mathbb{C}}{\mathcal{O}_K} &\longrightarrow E(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)) \end{aligned}$$

and a commutative diagram

$$\begin{array}{ccc} \frac{\mathbb{C}}{\mathcal{O}_K} & \xrightarrow{\phi_\alpha} & \frac{\mathbb{C}}{\mathcal{O}_K} \\ \downarrow & & \downarrow \\ E(\mathbb{C}) & \xrightarrow{[\alpha]} & E(\mathbb{C}) \end{array}$$

(see [21, p. 105, Proposition 4.11] and [23, p. 97]), where, for any  $\alpha \in \mathcal{O}_K$  and  $z \in \mathbb{C}$ ,

$$\phi_\alpha(z) = \alpha z,$$

and  $\wp$  is the Weierstrass function defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \mathcal{O}_K \\ \omega \neq 0}} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Moreover, all the endomorphisms of  $E(\mathbb{C})$  are of the form  $[\alpha]$  defined above, for some  $\alpha \in \mathcal{O}_K$ .

Let us briefly observe that

$$\overline{\wp(z)} = \wp(\bar{z}) \quad \text{and} \quad \overline{\wp'(z)} = \wp'(\bar{z})$$

and that  $\wp(z)$  is an even function, while its derivative  $\wp'(z)$  is an odd function.

In what follows, we assume that  $-D \equiv 2, 3 \pmod{4}$ , thus  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-D}]$ . The proofs in the case  $-D \equiv 1 \pmod{4}$  are similar.

1. If  $q$  splits completely in  $K$ , then, on one hand, the Legendre symbol  $\left(\frac{-D}{q}\right)$  of  $-D$  modulo  $q$  is 1; on the other hand,  $q\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$  for some distinct nonzero prime ideals  $\mathfrak{q}_1, \mathfrak{q}_2$  of  $\mathcal{O}_K$  with  $N_{K/\mathbb{Q}}(\mathfrak{q}_1) = N_{K/\mathbb{Q}}(\mathfrak{q}_2) = q$ , which we write as

$$\mathfrak{q}_1 = \beta\mathcal{O}_K, \quad \mathfrak{q}_2 = \bar{\beta}\mathcal{O}_K$$

for some  $0 \neq \beta \in \mathcal{O}_K$ . We also observe that

$$E[q^n] = E[\mathfrak{q}_1^n] \oplus E[\mathfrak{q}_2^n],$$

where

$$E[\mathfrak{q}_1^n] := \left\{ P \in E(\overline{\mathbb{Q}}) : [\beta^n]P = O \right\},$$

$$E[\mathfrak{q}_2^n] := \left\{ P \in E(\overline{\mathbb{Q}}) : [\bar{\beta}^n]P = O \right\}.$$

But  $E[q^n] \simeq \mathbb{Z}/q^n\mathbb{Z} \oplus \mathbb{Z}/q^n\mathbb{Z}$ , hence  $E[\mathfrak{q}_1^n]$  and  $E[\mathfrak{q}_2^n]$  must be cyclic  $\mathbb{Z}/q^n\mathbb{Z}$ -modules. We choose

$$P_1 := \left( \wp \left( \frac{1}{\beta^n} \right), \wp' \left( \frac{1}{\beta^n} \right) \right)$$

as a  $\mathbb{Z}/q^n\mathbb{Z}$ -basis for  $E[\mathfrak{q}_1^n]$  and

$$P_2 := \left( \wp \left( \frac{1}{\bar{\beta}^n} \right), \wp' \left( \frac{1}{\bar{\beta}^n} \right) \right)$$

as a  $\mathbb{Z}/q^n\mathbb{Z}$ -basis for  $E[\mathfrak{q}_2^n]$ ; thus  $\{P_1, P_2\}$  is a  $\mathbb{Z}/q^n\mathbb{Z}$ -basis for  $E[q^n]$ .

With respect to this basis, the automorphisms of  $E[q^n]$  can be embedded into

$$\left\{ \begin{pmatrix} a + b\sqrt{-D} & 0 \\ 0 & a + b\sqrt{-D} \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/q^n\mathbb{Z}) \right\},$$

where we are using that  $\left(\frac{-D}{q}\right) = 1$ . Part 1 of the lemma follows.

2. Now let us assume that  $q$  is inert in  $K = \mathbb{Q}(\sqrt{-D})$ , that is,  $(q)$  is a prime ideal of  $\mathcal{O}_K$  and  $\left(\frac{-D}{q}\right) = -1$ .

We choose

$$P_1 := \left( \wp \left( \frac{1}{q^n} \right), \wp' \left( \frac{1}{q^n} \right) \right),$$

$$P_2 := \left( \wp \left( \frac{\sqrt{-D}}{q^n} \right), \wp' \left( \frac{\sqrt{-D}}{q^n} \right) \right)$$

as a  $\mathbb{Z}/q^n\mathbb{Z}$ -basis for  $E [q^n]$ . With respect to this basis, the automorphisms of  $E [q^n]$  can be embedded into

$$\left\{ \begin{pmatrix} a & -bD \\ b & a \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/q^n\mathbb{Z}) \right\}.$$

Indeed, for  $\alpha = a + b\sqrt{-D} \in \mathcal{O}_K$  we have

$$[\alpha]P_1 = \left( \wp \left( \frac{\alpha}{q^n} \right), \wp' \left( \frac{\alpha}{q^n} \right) \right) = aP_1 + bP_2,$$

$$[\alpha]P_2 = \left( \wp \left( \frac{\alpha\sqrt{-D}}{q^n} \right), \wp' \left( \frac{\alpha\sqrt{-D}}{q^n} \right) \right) = -bDP_1 + aP_2.$$

Part 2 of the lemma follows. □

**Lemma 3.12** *Let  $E$  be a CM elliptic curve defined over  $\mathbb{Q}$ , with complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K = \mathbb{Q}(\sqrt{-D})$ , where  $D$  is positive and square-free. Let  $q$  be an odd rational prime, unramified in  $K$ . Let*

$$D_{q^2} = \left\{ g \in \text{Gal}(K(E[q^2])/K) : \det g + 1 - \text{tr } g \equiv 0 \pmod{q^2} \right\},$$

where we view  $\text{Gal}(K(E[q^2])/K)$  as a subgroup of  $\text{GL}_2(\mathbb{Z}/q^2\mathbb{Z})$  via the representation  $\phi_{q^2}$ , as described in Sect. 2. Then  $\#D_{q^2} \leq q^2$ .

*Proof* First let us assume that  $q$  splits completely in  $K/\mathbb{Q}$ . Then if  $g \in D_{q^2}$ , we have

$$g = \begin{pmatrix} a + qa' & 0 \\ 0 & a + qa' \end{pmatrix}$$

for some  $1 \leq a \leq q - 1, 0 \leq a' \leq q - 1$ , chosen such that

$$\det g + 1 - \text{tr } g \equiv 0 \pmod{q^2}. \tag{23}$$

This implies that  $a - 1 \equiv 0 \pmod{q}$ , a contradiction.

Now let us assume that  $q$  is inert in  $K = \mathbb{Q}(\sqrt{-D})$ , hence we have  $\left(\frac{-D}{q}\right) = -1$ . If  $g \in D_{q^2}$  and  $-D \equiv 2, 3 \pmod{4}$ , then

$$g = \begin{pmatrix} a + qa' & -(b + qb')D \\ b + qb' & a + qa' \end{pmatrix}$$

for some  $0 \leq a, b \leq q - 1, 0 \leq a', b' \leq q - 1$ , chosen such that

$$\det g + 1 - \text{tr } g \equiv 0 \pmod{q^2}. \tag{24}$$

Condition (24) implies that

$$(a - 1)^2 + b^2 D \equiv 0 \pmod{q}, \tag{25}$$

and so, if  $b \not\equiv 0 \pmod{q}$ ,  $-D$  is a square modulo  $q$ , a contradiction. If  $b \equiv 0 \pmod{q}$ , then condition (25) implies that  $a \equiv 1 \pmod{q}$ , thus

$$g = \begin{pmatrix} 1 + qa' & -qb'D \\ q' & 1 + qa' \end{pmatrix}$$

for some  $0 \leq a', b' \leq q - 1$ . Since condition (24) is satisfied for any  $0 \leq a', b' \leq q - 1$ , we deduce that there are  $q^2$  such matrices  $g$ .

We proceed similarly if  $-D \equiv 1 \pmod{4}$  and obtain at most  $q^2$  matrices  $g \in D_{q^2}$ . This completes the proof of the lemma. □

We obtain the following immediate consequence:

**Corollary 3.13** *Under the hypotheses of Lemma 3.12 and for any odd positive square-free integer  $k$  composed of primes which are unramified in  $K$ , we have  $\#D_{k^2} \leq k^2$ .*

### 3.4 Characterization of the square-freeness of $\#E_p(\mathbb{F}_p)$

In this section we describe an important characterization of the primes  $p$  for which  $\#E_p(\mathbb{F}_p)$  is square-free in the case that the elliptic curve  $E$  is with CM. We start with two standard results:

**Lemma 3.14** *Let  $E$  be a CM elliptic curve defined over  $\mathbb{Q}$  and with complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . Let  $p$  be a prime of good ordinary reduction for  $E$ , and let  $p\mathcal{O}_K = (\pi_p)(\bar{\pi}_p)$  be its prime factorization in  $K$ . Then  $\mathbb{Q}(\pi_p) = K$ .*

**Lemma 3.15** *Let  $E$  be a CM elliptic curve defined over  $\mathbb{Q}$  and with complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . Let  $p$  be a prime of good ordinary reduction for  $E$ , and let  $p\mathcal{O}_K = (\pi_p)(\bar{\pi}_p)$  be its prime factorization in  $K$ . Let  $I$  be a nonzero ideal of  $\mathcal{O}_K$  such that  $\pi_p \nmid I$ . Then  $\pi_p$  splits completely in  $K(E[I])/K$  if and only if  $\pi_p \equiv 1 \pmod{I}$ .*

For proofs of these lemmas, the reader is referred to Sect. 2.2 of [3].

As an immediate consequence of Lemma 3.15 and Theorem 3.8, we have:

**Lemma 3.16** *Let  $E$  be a CM elliptic curve defined over  $\mathbb{Q}$  and with complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . Let  $x > 2$  and let  $I$  be a nonzero ideal of  $\mathcal{O}_K$  with  $N_{K/\mathbb{Q}}(I) \leq \frac{x}{\log x}$ . Then*

$$\begin{aligned} & \#\{p \leq x : a_p \neq 0, \pi_p \text{ splits completely in } K(E[I])/K\} \\ & \ll \frac{x}{\Phi(I) \log \frac{x}{N_{K/\mathbb{Q}}(I)}} \left( 1 + \frac{1}{\sqrt{\log \frac{x}{N_{K/\mathbb{Q}}(I)}}} \right). \end{aligned}$$

The main result of this section is:

**Lemma 3.17** *Let  $E$  be a CM elliptic curve defined over  $\mathbb{Q}$ , of conductor  $N$  and with complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . Let  $p, q$  be primes such that  $p \nmid qN$  with  $p \geq 5$ . We assume that  $p$  has ordinary reduction for  $E$ , and we let  $p\mathcal{O}_K = (\pi_p)(\bar{\pi}_p)$  be its prime factorization in  $K$ .*

1. *If  $q$  is inert in  $K$ , then  $q^2 \mid \#E_p(\mathbb{F}_p)$  if and only if  $p$  splits completely in  $K(E[q])$ .*
2. *If  $q$  ramifies in  $K$ , then  $q^2 \mid \#E_p(\mathbb{F}_p)$  if and only if  $p$  splits completely in  $K(E[q])$ .*
3. *If  $q$  splits in  $K$ , say as  $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$  for distinct complex conjugate prime ideals  $\mathfrak{q}, \bar{\mathfrak{q}}$  of  $\mathcal{O}_K$ , then  $q^2 \mid \#E_p(\mathbb{F}_p)$  if and only if  $\pi_p$  splits completely in one of  $K(E[q])$ ,  $K(E[q^2])$ , or  $K(E[\bar{q}^2])$ .*

*Proof* Throughout the proof, we will be using the two lemmas recalled above. Let us consider each of the three situations for  $q$ .

1. If  $q$  is inert in  $K$ , we write  $(q) = \mathfrak{q}$  for some prime ideal  $\mathfrak{q}$  of  $K$  with  $N_{K/\mathbb{Q}}(\mathfrak{q}) = q^2$ .

“ $\Leftarrow$ ” We assume that  $p$  splits completely in  $K(E[q])$ . This means that  $(\pi_p)$  splits completely in  $K(E[q])$ , hence  $q \mid (\pi_p - 1)$  in  $\mathbb{Q}(\pi_p) = K$ . By taking the norm  $N_{K/\mathbb{Q}}(\cdot)$ , we obtain that  $q^2 \mid p + 1 - a_p = \#E_p(\mathbb{F}_p)$ .

“ $\Rightarrow$ ” We assume that  $q^2 \mid \#E_p(\mathbb{F}_p)$ , which is equivalent to  $q^2 \mid (\pi_p - 1)(\bar{\pi}_p - 1)$  in  $K$ . Thus

$$(\pi_p - 1)(\bar{\pi}_p - 1) = q^2(\alpha)$$

for some  $\alpha \in \mathcal{O}_K$  (where we are also using that  $K$  has class number 1). It is easy to see now that  $q \mid (\pi_p - 1)$ , hence that  $\pi_p$  splits completely in  $K(E[q])$ . This also implies that  $\bar{\pi}_p$  splits completely in  $K(E[\bar{q}]) = K(E[q])$ . Thus, recalling that  $p$  splits in  $K$  as  $(p) = (\pi_p)(\bar{\pi}_p)$ , we obtain that  $p$  splits completely in  $K(E[q]) = K(E[\bar{q}])$ .

2. If  $q$  ramifies in  $K$ , we write  $(q) = \mathfrak{q}^2$  for some prime ideal  $\mathfrak{q}$  of  $\mathcal{O}_K$  with  $N_{K/\mathbb{Q}}(\mathfrak{q}) = q$ .

“ $\Leftarrow$ ” We assume that  $p$  splits completely in  $K(E[q])$ . As before, this means that  $\pi_p \equiv 1 \pmod{q}$ , hence that  $q^2 \mid \#E_p(\mathbb{F}_p)$ .

“ $\Rightarrow$ ” We assume that  $q^2 \mid \#E_p(\mathbb{F}_p)$ , hence that

$$(\pi_p - 1)(\bar{\pi}_p - 1) = q^4(\alpha)$$

for some  $\alpha \in \mathcal{O}_K$ . This tells us that  $q^2 \mid (\pi_p - 1)$ , hence that  $\pi_p$  splits completely in  $K(E[q^2])$ . Consequently,  $\bar{\pi}_p$  splits completely in  $K(E[\bar{q}^2]) = K(E[q^2])$ , and so  $p$  must split completely in  $K(E[q^2]) = K(E[q])$ .

3. If  $q$  splits completely in  $K$ , we write  $(q) = \mathfrak{q}\bar{\mathfrak{q}}$  for distinct complex conjugate prime ideals  $\mathfrak{q}, \bar{\mathfrak{q}}$  of  $\mathcal{O}_K$  with  $N_{K/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}(\bar{\mathfrak{q}}) = q$ .

“ $\Leftarrow$ ” As in parts 1 and 2, if  $\pi_p$  splits completely in one of  $K(E[q])$ ,  $K(E[q^2])$ , or  $K(E[\bar{q}^2])$ , then  $\pi_p \equiv 1 \pmod{q}$ , or  $\pi_p \equiv 1 \pmod{q^2}$ , or  $\pi_p \equiv 1 \pmod{\bar{q}^2}$ , respectively. By taking  $N_{K/\mathbb{Q}}(\cdot)$ , we obtain that  $q^2 \mid \#E_p(\mathbb{F}_p)$ .

“ $\Rightarrow$ ” Finally, we assume that  $q^2 \mid \#E_p(\mathbb{F}_p)$ , which implies that

$$(\pi_p - 1)(\bar{\pi}_p - 1) = q^2 \bar{q}^2 (\alpha)$$

for some  $\alpha \in \mathcal{O}_K$ . Then we must have  $q\bar{q} \mid (\pi_p - 1)$ , or  $q^2 \mid (\pi_p - 1)$ , or  $\bar{q}^2 \mid (\pi_p - 1)$ , which tells us that  $\pi_p$  splits completely in  $K(E[q\bar{q}]) = K(E[q])$ , or  $K(E[q^2])$ , or  $K(E[\bar{q}^2])$ , respectively. This completes the proof of the lemma.  $\square$

As an immediate consequence of Lemma 3.17, we have:

**Corollary 3.18** *Let  $E$  be a CM elliptic curve defined over  $\mathbb{Q}$ , of conductor  $N$  and with complex multiplication by the full ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$ . Let  $p \geq 5$  be a prime of ordinary good reduction for  $E$ . Write  $p\mathcal{O}_K = (\pi_p)(\bar{\pi}_p)$  as before. Then  $\#E_p(\mathbb{F}_p)$  is square-free if and only if  $\pi_p$  does not split completely in any of:  $K(E[q])$  for any prime ideal  $\mathfrak{q}$  of  $K$  lying over a rational prime which is inert in  $K$ ;  $K(E[q^2])$  for any prime ideal  $\mathfrak{q}$  of  $K$  lying over a rational prime which ramifies in  $K$ ;  $K(E[q\bar{q}])$ ,  $K(E[q^2])$  and  $K(E[\bar{q}^2])$  for any prime ideal  $\mathfrak{q}$  of  $K$  lying over a rational prime which splits completely in  $K$ .*

### 4 Proof of Theorem 1.1

To prove Theorem 1.1, we follow the strategy discussed in Sect. 2. More precisely, we use (12) and analyze each of the terms  $N(x, y)$  and  $M(x, y, 2\sqrt{x})$ .

#### 4.1 Estimate for $N(x, y)$

Following (13), we write

$$N(x, y) = \frac{1}{2} \sum'_k \mu(k) \# \{ \mathfrak{p} \leq \mathcal{O}_K : N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x, \mathfrak{p} \nmid kN, \phi_{k^2}(\sigma_{\mathfrak{p}}) \subseteq D_{k^2} \},$$

where the dash on the summation indicates that we sum over positive integers  $k \leq 2\sqrt{x}$  whose prime divisors are  $\leq y$ . We will use the unconditional effective Chebotarev Density Theorem 3.3 to estimate this sum.

By Lemma 3.4 and part 2 of Proposition 3.9 we obtain that

$$n(k^2) (\log d(k^2))^2 \ll n(k^2)^3 (\log(n(k^2)kN))^2$$

and

$$n(k^2) d(k^2)^{2/n(k^2)} \ll n(k^2)^3 k^2 N^2,$$

thus

$$\max \left\{ n(k^2) (\log d(k^2))^2, n(k^2) d(k^2)^{2/n(k^2)} \right\} \ll k^{14} N^2.$$

In order to apply Theorem 3.3 we need  $k^{14} N^2 \leq \log x$ , and since  $k \leq \exp(2y)$ , this condition is ensured if we choose

$$y := \frac{1}{28} (\log \log x - 2 \log N). \tag{26}$$

We obtain

$$N(x, y) = \frac{1}{2} \sum'_k \frac{\mu(k) \# D_{k^2}}{n(k^2)} \operatorname{li} x + O \left( \sum'_k \# (\widetilde{D_{k^2}}) x \exp \left( -A \sqrt{\frac{\log x}{n(k^2)}} \right) \right) \tag{27}$$

for some positive effective constant  $A$ , where  $\widetilde{D_{k^2}}$  denotes the set of conjugacy classes contained in  $D_{k^2}$ . We note that, by using Proposition 3.10,

$$\# (\widetilde{D_{k^2}}) \leq \# D_{k^2} \leq n(k^2) \leq k^4$$

for any  $k \geq 3$ . Also, since there are at most  $2^y \ll \frac{(\log x)^{1/28}}{N^{1/28}}$  positive square-free integers  $k$  with prime divisors  $< y$ , and since  $k \leq \exp(2y)$ , the error term in the above estimates becomes

$$\begin{aligned} O \left( \sum'_k k^4 x \exp \left( -A \sqrt{\frac{\log x}{n(k^2)}} \right) \right) &= O \left( \exp(9y) \frac{x}{(\log x)^{B'}} \right) \\ &= O \left( \frac{x}{N^{9/28} (\log x)^B} \right) \end{aligned} \tag{28}$$

for any positive constants  $B'$  and  $B$ .

#### 4.2 Estimate for $M(x, y, 2\sqrt{x})$

To estimate  $M(x, y, 2\sqrt{x})$ , we make use of Lemma 3.17.<sup>3</sup>

More precisely, we write

$$M(x, y, 2\sqrt{x}) = M_i(x, y, 2\sqrt{x}) + M_r(x, y, 2\sqrt{x}) + M_s(x, y, 2\sqrt{x}), \tag{29}$$

<sup>3</sup> We emphasize that our unconditional treatment of  $M(x, y, 2\sqrt{x})$  is possible thanks to Lemmas 3.14 and 3.17, which are results specific to elliptic curves with CM. An unconditional treatment for the same quantity in the case of an elliptic curve  $E/\mathbb{Q}$  without CM would require a Bombieri–Vinogradov type result for  $\pi_{D, q^2}(x, \mathbb{Q}(E[q^2])/\mathbb{Q})$ , where  $q$  lies in a suitably large range depending on  $x$ , and such a result is not yet known.

where

$$\begin{aligned}
 M_i(x, y, 2\sqrt{x}) &:= \sum_{\substack{y < q \leq 2\sqrt{x} \\ q \text{ inert in } K}} \#\{p \leq x : a_p \neq 0, q^2 \mid \#E_p(\mathbb{F}_p)\}, \\
 M_r(x, y, 2\sqrt{x}) &:= \sum_{\substack{y < q \leq 2\sqrt{x} \\ q \text{ ramified in } K}} \#\{p \leq x : a_p \neq 0, q^2 \mid \#E_p(\mathbb{F}_p)\}, \\
 M_s(x, y, 2\sqrt{x}) &:= \sum_{\substack{y < q \leq 2\sqrt{x} \\ q \text{ split in } K}} \#\{p \leq x : a_p \neq 0, q^2 \mid \#E_p(\mathbb{F}_p)\}.
 \end{aligned}$$

We estimate each of these three sums separately.

**Estimate for  $M_i(x, y, 2\sqrt{x})$ .** By part 1 of Lemma 3.17 we have

$$M_i(x, y, 2\sqrt{x}) = \sum_{\substack{y < q \leq 2\sqrt{x} \\ q \text{ inert in } K}} \#\{p \leq x : p \text{ splits completely in } K(E[q])\}.$$

The condition that  $p$  splits completely in  $K(E[q])$  is equivalent to  $\pi_p \equiv 1 \pmod{q}$  in  $\mathcal{O}_K$ , where  $p\mathcal{O}_K = (\pi_p)(\bar{\pi}_p)$ , as before. This implies that

$$M_i(x, y, 2\sqrt{x}) \leq \sum_{\substack{y < q \leq 2\sqrt{x} \\ q \text{ inert in } K}} S_q,$$

where  $S_q = S_q^1$  if  $-D \equiv 2, 3 \pmod{4}$  and  $S_q = S_q^2$  if  $-D \equiv 1 \pmod{4}$ , and where  $S_q^1, S_q^2$  have been defined in Lemma 3.6. We split the above sum into two parts, according to whether  $y < q \leq \log x$  or  $\log x < q \leq 2\sqrt{x}$ , and use the ‘‘Eratosthenes estimate’’ given by Lemma 3.6 for the first range, and the elementary estimate given by Remark 3.7 for the latter range. We obtain

$$\begin{aligned}
 M_i(x, y, 2\sqrt{x}) &\ll \frac{x \log \log x}{\sqrt{D}} \sum_{y < q \leq \log x} \frac{1}{q^2 \log \frac{\sqrt{x}-1}{q}} \\
 &\quad + \frac{\sqrt{x} \log \log x}{\sqrt{D}} \sum_{y < q \leq \log x} \frac{1}{q \log \frac{\sqrt{x}-1}{q}} \\
 &\quad + \frac{x}{\sqrt{D}} \sum_{\log x < q \leq 2\sqrt{x}} \frac{1}{q^2} + \frac{\sqrt{x}}{\sqrt{D}} \sum_{\log x < q \leq 2\sqrt{x}} \frac{1}{q} \\
 &\ll \frac{x \log \log x}{y(\log x)(\log y)} + \frac{\sqrt{x}(\log \log x)(\log \log \log x)}{\log x} \\
 &\quad + \frac{x}{(\log x)(\log \log x)} + \sqrt{x} \log \log \log x.
 \end{aligned}$$

With our choice of  $y$  given in (26), this becomes

$$M_i(x, y, 2\sqrt{x}) = O\left(\frac{x}{(\log x)(\log \log \frac{\log x}{N^2})} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}}\right). \tag{30}$$

Note that  $D$  belongs to a finite number of integers, thus the  $O$ -constant above is absolute.

**Estimate for  $M_r(x, y, 2\sqrt{x})$ .** We count ordinary primes  $p \leq x$  with  $q^2 | (p+1-a_p)$  for some prime  $y < q \leq 2\sqrt{x}$  which ramifies in  $\mathbb{Q}(\pi_p) = K = \mathbb{Q}(\sqrt{-D})$ , hence which divides the discriminant of  $K$ . Since  $y \asymp \log \log x$ , we obtain that, for  $x \gg \exp \exp D$ ,

$$M_r(x, y, 2\sqrt{x}) = 0. \tag{31}$$

**Estimate for  $M_s(x, y, 2\sqrt{x})$ .** To estimate  $M_s(x, y, 2\sqrt{x})$  we have, by part 3 of Lemma 3.17, that

$$M_s(x, y, 2\sqrt{x}) \leq \sum_{y < q \leq 2\sqrt{x}} S_q + \sum_{\substack{y < q \leq 2\sqrt{x} \\ (q) = \mathfrak{q}\bar{\mathfrak{q}}, \mathfrak{q} \neq \bar{\mathfrak{q}}}} \# \left\{ p \leq x : p \text{ splits in } K \text{ and } \pi_p \text{ splits in } K(E[q^2]) \right\},$$

where by ‘‘splits’’ we mean that it splits completely. The first sum is estimated in the same way as  $M_i(x, y, 2\sqrt{x})$ . We obtain

$$\sum_{y < q \leq 2\sqrt{x}} S_q = O\left(\frac{x}{(\log x) \left(\log \log \frac{\log x}{N^2}\right)} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}}\right).$$

For the second sum we observe that the condition that  $\pi_p$  splits completely in  $K(E[q^2])$  implies that

$$(\pi_p - 1) = \mathfrak{q}^2(\alpha)$$

for some  $\alpha \in \mathcal{O}_K$ . We also observe that

$$\begin{aligned} & \# \left\{ (\alpha) : N_{K/\mathbb{Q}}(\pi_p - 1) = \frac{N_{K/\mathbb{Q}}(\pi_p - 1)}{N_{K/\mathbb{Q}}(\mathfrak{q}^2)} \leq \left(\frac{\sqrt{x} + 1}{q}\right)^2 \right\} \\ &= O\left(\left(\frac{\sqrt{x} + 1}{q} + 1\right) \frac{\sqrt{x} + 1}{q\sqrt{D}}\right) \\ &= O\left(\left(\frac{\sqrt{x}}{q} + 1\right) \frac{\sqrt{x}}{q}\right). \end{aligned} \tag{32}$$

Now, similarly to our estimates for  $M_i(x, y, 2\sqrt{x})$ , we write

$$\begin{aligned} & \sum_{\substack{y < q \leq 2\sqrt{x} \\ (q) = q\bar{q}, q \neq \bar{q}}} \# \left\{ p \leq x : p \text{ splits in } K \text{ and } \pi_p \text{ splits in } K \left( E \left[ q^2 \right] \right) \right\} \\ & \ll \sum_{\substack{y < q \leq \log x \\ (q) = q\bar{q}, q \neq \bar{q}}} \sum_{\substack{p \leq x \\ \pi_p \equiv 1 \pmod{q^2}}} 1 + \sum_{\substack{\log x < q \leq 2\sqrt{x} \\ (q) = q\bar{q}, q \neq \bar{q}}} \sum_{\substack{p \leq x \\ \pi_p \equiv 1 \pmod{q^2}}} 1, \end{aligned}$$

and we use the ‘‘Schaal estimate’’ given by Theorem 3.8 (or Lemma 3.16) for the first sum, and the elementary estimate given by (32) for the second sum. We obtain:

$$\begin{aligned} \sum_{\substack{y < q \leq \log x \\ (q) = q\bar{q}, q \neq \bar{q}}} \sum_{\substack{p \leq x \\ \pi_p \equiv 1 \pmod{q^2}}} 1 & \ll \sum_{y < q \leq \log x} \frac{x}{q^2 \log \frac{x}{q^2}} \left( 1 + \frac{1}{\sqrt{\log \frac{x}{q^2}}} \right) \\ & \ll \frac{x}{y(\log x)(\log y)}; \\ \sum_{\substack{\log x < q \leq 2\sqrt{x} \\ (q) = q\bar{q}, q \neq \bar{q}}} \sum_{\substack{p \leq x \\ \pi_p \equiv 1 \pmod{q^2}}} 1 & \ll \sum_{\log x < q \leq 2\sqrt{x}} \left( \left( \frac{\sqrt{x} + 1}{q} \right)^2 + \frac{\sqrt{x} + 1}{q} \right) \\ & \ll \frac{x}{(\log x)(\log \log x)} + \sqrt{x} \log \log x. \end{aligned}$$

These estimates and our choice of  $y$  given in (26) lead to

$$M_x(x, y, 2\sqrt{x}) = O\left( \frac{x}{(\log x)(\log \log \frac{\log x}{N^2})} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}} \right). \tag{33}$$

### 4.3 Putting things together

Using (12), (27)–(31), and (33), we obtain that

$$\begin{aligned} h_E(x, \mathbb{Q}) &= \frac{1}{2} \sum_k \frac{\mu(k) \#D_{k^2}}{n(k^2)} \text{li } x + O\left( \frac{x}{N^{9/28}(\log x)^B} \right) \\ &+ O\left( \frac{x}{(\log x)(\log \log \frac{\log x}{N^2})} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}} \right) \end{aligned}$$

for any positive constant  $B$ .

It remains to analyze the term  $\frac{1}{2} \sum_k \frac{\mu(k) \#D_{k^2}}{n(k^2)} \text{li } x$ . We recall that for odd square-free positive integers  $k$  composed of primes which are unramified in  $K$  we have  $\#D_{k^2} = O(k^2)$  (see Corollary 3.13). For  $k$  equal to 2 or composed of ramified primes

of  $K$  we obtain that  $\#D_{k^2}$  is bounded absolutely. Hence

$$\begin{aligned} \frac{1}{2} \left( \sum_{k \geq 1} \frac{\mu(k)\#D_{k^2}}{n(k^2)} - \sum_k' \frac{\mu(k)\#D_{k^2}}{n(k^2)} \right) \text{li } x &\ll \frac{x}{\log x} \sum_{q>y} \sum_{t \geq 1} \frac{q^2 t^2}{q^4 (t^2)^{7/2}} \\ &\ll \frac{x}{y(\log y)(\log x)}. \end{aligned}$$

Using (26) in this estimate, we obtain that

$$\begin{aligned} h_E(x, \mathbb{Q}) &= \frac{1}{2} \sum_{k \geq 1} \frac{\mu(k)\#D_{k^2}}{n(k^2)} \text{li } x + O\left(\frac{x}{N^{9/28}(\log x)^B}\right) \\ &\quad + O\left(\frac{x}{(\log x)(\log \log \frac{\log x}{N^2})} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}}\right). \end{aligned}$$

This completes the proof of Theorem 1.1.

### 5 Proof of Theorem 1.2

We consider the problem of improving the error terms in the asymptotic formula for  $h_E(x, \mathbb{Q})$  obtained in Theorem 1.1. This time we shall use splitting (15) introduced in Sect. 2 and assume GRH.

We estimate  $\mathcal{N}(x, y)$  similarly to how we estimated  $N(x, y)$  in Theorem 1.1; now, however, we use the conditional Chebotarev Density Theorem 3.2. Note that since the extensions  $L_{k^2}/K$  are abelian, AHC holds and we do not have it as an extra assumption. We obtain that

$$\begin{aligned} \mathcal{N}(x, y) &= \frac{1}{2} \sum_{k \leq y} \frac{\mu(k)\#D_{k^2}}{n(k^2)} \text{li } x + \sum_{k \leq y} O\left(kx^{1/2}(\log(kNx))\right) \\ &= \frac{1}{2} \sum_{k \leq y} \frac{\mu(k)\#D_{k^2}}{n(k^2)} \text{li } x + O\left(y^2 x^{1/2}(\log(Nx))\right), \end{aligned} \tag{34}$$

where we have also used Lemma 3.4, Proposition 3.9 and Corollary 3.13.

The sum  $\mathcal{M}(x, y, 2\sqrt{x})$  is estimated along similar lines as the sum  $M(x, y, 2\sqrt{x})$ . The details follow.

We write each index  $k$  as

$$k = k_i k_r k_s,$$

where  $k_i$  is composed of inert primes of  $K$ ,  $k_r$  is composed of ramified primes of  $K$ , and  $k_s$  is composed of primes which split completely in  $K$ . By using Lemma 3.17 we obtain that, for any square-free integer  $k$  such that  $k^2 \mid \#E_p(\mathbb{F}_p)$  for some ordinary

prime  $p$ , we have that  $p$  splits completely in  $K$  and

$$(\pi_p - 1) = k_i k_r I(k_s) \cdot (\alpha) \tag{35}$$

for some  $\alpha \in \mathcal{O}_K$ , where  $I(k_s)$  is an ideal of  $\mathcal{O}_K$  obtained by taking the product of the ideals  $q\bar{q}$ ,  $q^2$ , or  $\bar{q}^2$  according to whether  $\pi_p$  splits completely in  $K(E[q\bar{q}])$ ,  $K(E[q^2])$ , or  $K(E[\bar{q}^2])$ , respectively, with  $q$  running over the prime ideals of  $K$  lying above prime divisors  $q$  of  $k_s$ . We note that there are  $3^{v(k_s)}$  possible such ideals  $I(k_s)$ . We also remark that for  $\alpha$  as in (35) we have

$$N_{K/\mathbb{Q}}(\alpha) = \frac{N_{K/\mathbb{Q}}(\pi_p - 1)}{N_{K/\mathbb{Q}}(k_i k_r I(k_s))} \leq \frac{(\sqrt{p} + 1)^2}{k^2} \leq \frac{(\sqrt{x} + 1)^2}{k^2},$$

so that the number of possible  $\alpha$  is

$$O\left(\left(\frac{\sqrt{x} + 1}{k} + 1\right) \frac{\sqrt{x} + 1}{k\sqrt{D}}\right) O\left(\left(\frac{\sqrt{x}}{k} + 1\right) \frac{\sqrt{x}}{k}\right).$$

The above remarks imply that

$$\begin{aligned} \mathcal{M}(x, y, 2\sqrt{x}) &\leq \sum_{\substack{y < k \leq 2\sqrt{x} \\ k \text{ square-free} \\ k = k_i k_r k_s}} \sum_{\substack{p \leq x \\ a_p \neq 0 \\ (\pi_p - 1) = k_i k_r I(k_s)(\alpha)}} 1 \\ &\ll \sum_{\substack{y < k \leq 2\sqrt{x} \\ k \text{ square-free} \\ k = k_i k_r k_s}} 3^{v(k_s)} \left( \frac{x}{k_i^2 k_r^2 k_s^2} + \frac{\sqrt{x}}{k_i k_r k_s} \right) \\ &\ll \sum_{k_s \leq 2\sqrt{x}} \sum_{\substack{y \\ \frac{y}{k_s} < k_i \leq 2\sqrt{x}}} 3^{v(k_s)} \left( \frac{x}{k_i^2 k_s^2} + \frac{\sqrt{x}}{k_i k_s} \right) \\ &\ll \sum_{k_s \leq 2\sqrt{x}} 3^{v(k_s)} \left( \frac{x}{y k_s} + \frac{\sqrt{x}}{k_s} \log x \right) \\ &\ll \frac{x}{y} (\log x)^3 + \sqrt{x} (\log x)^4, \end{aligned} \tag{36}$$

where we have also used that  $\sum_{n \leq x} \frac{1}{n} = \log x + O(1)$  and

$$\sum_{k \leq x} c^{v(k)} \ll x (\log x)^{c-1}. \tag{37}$$

Putting (15), (34), and (36) together gives

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

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

$$y := \frac{x^{1/6} \log x}{(\log(Nx))^{1/3}}.$$

Then

$$h_E(x, \mathbb{Q}) = \sum_{k \leq y} \frac{\mu(k) \#D_{k^2}}{n(k^2)} \operatorname{li} x + O\left(x^{5/6} (\log x)^2 (\log(Nx))^{1/3}\right). \tag{38}$$

To handle the tail  $\frac{1}{2} \sum_{k > y} \frac{\mu(k) \#D_{k^2}}{n(k^2)} \operatorname{li} x$ , we use again our estimates for  $\#D_{k^2}$  and  $n(k^2)$ , as well as (37). We obtain, by partial summation, that

$$\begin{aligned} \sum_{k > y} \frac{\mu(k) \#D_{k^2}}{n(k^2)} \operatorname{li} x &\ll \frac{x}{\log x} \sum_{k > y} \frac{k^2 2^{v(k)}}{k^4} \\ &\ll \frac{x \log y}{y \log x} \\ &\ll x^{5/6} (\log x)^{-1} (\log(Nx))^{1/3}. \end{aligned} \tag{39}$$

From (38) and (39) we now deduce the asymptotic formula claimed in the statement of Theorem 1.2.

### 6 The positivity of the density $\delta_E$

In this section we prove Theorem 1.3 about the positivity of the density  $\delta_E$ . Before proceeding any further, let us remark that since we are in the CM case, the order of the torsion subgroup  $E(\mathbb{Q})_{\text{tors}}$  of  $E(\mathbb{Q})$  can be 1, 2, 3, 4, or 6. Hence if  $\#E(\mathbb{Q})_{\text{tors}} = 4$ , then  $4 \mid \#E_p(\mathbb{F}_p)$  for all but finitely many primes  $p$ , and so  $\delta_E = 0$ . This clearly happens if  $\mathbb{Q}(E[2]) = \mathbb{Q}$ . Thus a necessary condition for the positivity of  $\delta_E$  is that  $\mathbb{Q}(E[2]) \neq \mathbb{Q}$ . Now let us also find a sufficient condition. Our arguments will be similar to the ones used in [9, pp. 28–32].

From Corollary 3.18 we see that

$$\delta_E = \frac{1}{2} \sum_{\mathfrak{a}, k} \frac{\mu(\mathfrak{a}) \mu(k)}{[K(E[\mathfrak{a}^2])K(E[k]) : K]}, \tag{40}$$

where the sum is over square-free ideals  $\mathfrak{a}$  of  $\mathcal{O}_K$  composed of first degree unramified prime ideals, and over square-free positive integers  $k$ .

We write each  $\mathfrak{a}$  and  $k$  as above in the form

$$\mathfrak{a} = \mathfrak{a}_1 \mathfrak{b}, \quad k = k_1 b,$$

where  $\mathfrak{a}_1, \mathfrak{b}$  are square-free ideals of  $\mathcal{O}_K$  such that  $\gcd\{\mathfrak{a}_1, (6N)\} = 1$  and  $\mathfrak{b} | (6N)$ , and  $k_1, b$  are positive square-free integers such that  $\gcd\{k_1, 6N\} = 1$  and  $b | 6N$ .

With this notation, we make the following important remarks:

$$[K(E[\mathfrak{a}^2])K(E[k]) : K] = [K(E[\mathfrak{a}_1^2])K(E[k_1]) : K] \cdot [K(E[\mathfrak{b}^2])K(E[b]) : K], \tag{41}$$

$$[K(E[\mathfrak{a}_1^2])K(E[k_1]) : K] = \frac{[K(E[\mathfrak{a}_1^2]) : K] \cdot [K(E[k_1]) : K]}{\Phi(\gcd\{\mathfrak{a}_1, (k_1)\})}, \tag{42}$$

where, we recall,  $\Phi(\cdot)$  denotes the generalized Euler function of  $K$ . Equation (41) is derived from the relation

$$[K(E[\mathfrak{a}^2])K(E[k]) : K(E[\mathfrak{b}^2])K(E[b])] = [K(E[\mathfrak{a}_1^2])K(E[k_1]) : K],$$

which is a straightforward consequence of the fact that for prime ideals  $\mathfrak{q}$  of  $\mathcal{O}_K$  dividing  $\text{lcm}\{\mathfrak{a}_1^2, (k_1)\}$  we have that  $K(E[\mathfrak{q}^2])$  is an extension of  $K$  in which  $\mathfrak{q}$  ramifies totally, and in which primes not dividing  $6N\mathfrak{q}$  do not ramify (see Proposition 3.10). The proof of (42) is also based on Proposition 3.10, as follows. Since  $\mathfrak{a}_1$  and  $k_1$  are coprime to  $(6N)$  and  $6N$ , respectively, so is  $\text{lcm}\{\mathfrak{a}_1^2, (k_1)\}$ . Thus the corresponding Galois groups of  $K(E[\mathfrak{a}_1^2])/K$ ,  $K(E[k_1])/K$ , and  $K(E[\text{lcm}\{\mathfrak{a}_1^2, (k_1)\}])/K$  are isomorphic to the unit groups  $(\mathcal{O}_K/\mathfrak{a}_1^2)^\times$ ,  $(\mathcal{O}_K/k_1\mathcal{O}_K)^\times$ , and  $(\mathcal{O}_K/\text{lcm}\{\mathfrak{a}_1^2, (k_1)\})^\times$ , respectively. Moreover,  $\Phi(\cdot)$  is multiplicative, hence we can write

$$\begin{aligned} [K(E[\mathfrak{a}_1^2])K(E[k_1]) : K] &= [K(E[\text{lcm}\{\mathfrak{a}_1^2, (k_1)\}]) : K] \\ &= \Phi(\text{lcm}\{\mathfrak{a}_1^2, (k_1)\}) \\ &= \frac{\Phi(\mathfrak{a}_1^2)\Phi((k_1))}{\Phi(\gcd\{\mathfrak{a}_1^2, (k_1)\})} \\ &= \frac{[K(E[\mathfrak{a}_1^2]) : K][K(E[k_1]) : K]}{\Phi(\gcd\{\mathfrak{a}_1, k_1\})}. \end{aligned}$$

Using (41) we can now write

$$\delta_E = \frac{1}{2} \sum_{\mathfrak{a}_1, k_1} \frac{\mu(\mathfrak{a}_1)\mu(k_1)}{[K(E[\mathfrak{a}_1^2])K(E[k_1]) : K]} \sum_{b, b} \frac{\mu(\mathfrak{b})\mu(b)}{[K(E[\mathfrak{b}^2])K(E[b]) : K]} =: \frac{1}{2} \delta_1 \delta_2. \tag{43}$$

It remains to analyze the positivity of each of  $\delta_1$  and  $\delta_2$ .

By using (42), we write

$$\delta_1 = \sum_{a_1, k_1} \frac{\mu(a_1)\mu(k_1)\Phi(\gcd\{a_1, (k_1)\})}{[K(E[a_1^2]) : K][K(E[k_1]) : K]}.$$

Since  $\gcd\{a_1, (6N)\} = \gcd\{k_1, 6N\} = 1$ , by Proposition 3.10 all the functions involved in the expression of  $\delta_1$  are multiplicative. Therefore we can rewrite the sum as an Euler product, and show that each of the factors involved is positive.

First we write

$$\delta_1 = \sum_{k_1} \frac{\mu(k_1)}{[K(E[k_1]) : K]} \prod_{\mathfrak{q}} \left(1 - \frac{\Phi(\gcd\{\mathfrak{q}, (k_1)\})}{[K(E[\mathfrak{q}^2]) : K]}\right),$$

where the inner product is over first degree unramified prime ideals  $\mathfrak{q}$  of  $\mathcal{O}_K$ , coprime to  $(6N)$ . In the following discussion on  $\delta_1$ , the meaning of  $\mathfrak{q}$  will remain the same. By using once again that for  $\mathfrak{q} \nmid (6N)$  we have  $[K(E[\mathfrak{q}^2]) : K] = \Phi(\mathfrak{q}^2)$ , and by rearranging the factors, we obtain

$$\begin{aligned} \delta_1 &= \prod_{\mathfrak{q}} \left(1 - \frac{1}{\Phi(\mathfrak{q}^2)}\right) \sum_{k_1} \frac{\mu(k_1)}{[K(E[k_1]) : K]} \prod_{\mathfrak{q}|k_1} \left(1 - \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{q})}\right) \left(1 - \frac{1}{\Phi(\mathfrak{q}^2)}\right)^{-1} \\ &= \prod_{\substack{\mathfrak{q} \nmid 6N \\ \mathfrak{q} \text{ inert in } K}} \left(1 - \frac{1}{q^2(q^2 - 1)}\right) \left(1 - \frac{1}{q^2 - 1}\right) \\ &\quad \times \prod_{\substack{\mathfrak{q} \nmid 6N \\ \mathfrak{q} \text{ splits in } K}} \left(1 - \frac{1}{q(q - 1)}\right) \left(1 - \frac{q - 1}{q^2 - q - 1}\right). \end{aligned}$$

From here it is clear that  $\delta_1 > 0$ .

Now we analyze  $\delta_2$ . Let  $\theta$  be the density of the primes  $\mathfrak{p}$  of  $K$  not splitting completely in any of  $K(E[q])$ , where  $q$  is a rational prime of second degree in  $K$  and dividing  $6N$ , and in any of  $K(E[\mathfrak{q}])$ , where  $\mathfrak{q}$  is a prime ideal of  $\mathcal{O}_K$ , dividing  $(6N)$ , and of first degree. Since  $\delta_2$  is the density of primes  $\mathfrak{p}$  of  $K$  not splitting completely in any of  $K(E[\mathfrak{q}^2])$ , where  $\mathfrak{q}$  is a prime ideal of  $K$  of first degree and dividing  $(6N)$ , and in any of  $K(E[q])$ , where  $q$  is a rational prime dividing  $6N$ , we have

$$\delta_2 \geq \theta. \tag{44}$$

It was shown in [9, pp. 30] that

$$\theta \geq \prod_{\mathfrak{q}|(6N)} \left(1 - \frac{w(\mathfrak{q})}{\Phi(\mathfrak{q})}\right), \tag{45}$$

where the product is over prime ideal divisors  $\mathfrak{q}$  of  $(6N)$  and  $w(\mathfrak{q})$  denotes the number of inequivalent units modulo  $\mathfrak{q}$ . Thus, as in [9, p. 30],  $\theta > 0$  if 2 and 3 are inert in  $K$ , which happens if  $K \neq \mathbb{Q}(\sqrt{-1})$  or  $K \neq \mathbb{Q}(\sqrt{-3})$ .

Along the same lines as in [9, p. 30–31] we also have that  $\delta_2 > 0$  if  $K = \mathbb{Q}(\sqrt{-11})$ , and  $\delta_E = 0$  if  $K = \mathbb{Q}(\sqrt{-7})$ . This completes the proof of Theorem 1.3.

## 7 Proof of Theorem 1.4

We prove Theorem 1.4 by comparing the main term  $\delta_E \operatorname{li} x \sim \delta_E \frac{x}{\log x}$  with the error terms

$$O\left(\frac{x}{(\log x)(\log \log \frac{x}{N^2})} \cdot \frac{\log \log x}{\log \frac{\log x}{N^2}}\right), \quad (46)$$

$$O\left(x^{5/6}(\log x)^2(\log(Nx))^{1/3}\right) \quad (47)$$

obtained in Theorems 1.1 and 1.2, respectively. We recall that the latter assumes GRH.

From (44), (45) and Mertens' Theorem we deduce that

$$\delta_E \gg \frac{1}{\log \log N}.$$

Then we see that if we choose  $x := c \exp(eN^3)$  for some suitable absolute constant  $c$ , we have that the main term is bigger than the error term (46), while if we choose  $x := c(\varepsilon)(\log N)^{2+\varepsilon}$  for some suitable constant  $c(\varepsilon)$  depending on a fixed  $\varepsilon > 0$ , we have that the main term is bigger than the error term (47). This completes the proof of Theorem 1.4.

**Acknowledgments** The core of this paper is based on Chaps. 8 and 9 of [2]. I thank Professor Ram Murty for his guidance and enthusiasm during my work on this problem.

## References

1. Balog, A., Cojocaru, A.C., David, C.: Average twin prime conjecture for elliptic curves, preprint (2007). <http://www.mathstat.concordia.ca/faculty/cdavid/PAPERS/Balog-Cojocaru-David-2007.pdf>
2. Cojocaru, A.C.: Cyclicity of elliptic curves modulo  $p$ . Ph.D. Thesis, Queen's University at Kingston, Canada (2002)
3. Cojocaru, A.C.: Cyclicity of CM elliptic curves modulo  $p$ . *Trans. Am. Math. Soc.* **355**(7), 2651–2662 (2003)
4. Cojocaru, A.C.: Questions about the reductions modulo primes of an elliptic curve. In: Goren, E., Kisilevsky, H. (eds.) *The Proceedings of the 7th Canadian Number Theory Association Meeting, Montréal, 2002. CRM Proceedings and Lecture Notes*, vol. 36, 2004
5. Cojocaru, A.C.: Reductions of an elliptic curve with almost prime orders. *Acta Arith.* **119**, 265–289 (2005)
6. Cojocaru, A.C., Ram Murty, M.: Cyclicity of elliptic curves modulo  $p$  and elliptic curve analogues of Linnik's problem. *Math. Ann.* **330**, 601–625 (2004)
7. Hooley, C.: *Applications of Sieve Methods to the Theory of Numbers*. Cambridge University Press, London (1976)

8. Gupta, R.: Fields of division points of elliptic curves related to Coates–Wiles. Ph.D. Thesis, MIT (1983)
9. Gupta, R., Murty, M.R.: Primitive points on elliptic curves. *Compos. Math.* **58**, 13–44 (1986)
10. Koblitz, N.: Primality of the number of points on an elliptic curve over a finite field. *Pacific J. Math.* **131**(1), 157–165 (1988)
11. Lagarias, J., Odlyzko, A.: Effective versions of the Chebotarev density theorem. In: Fröhlich, A. (ed.) *Algebraic Number Fields*, pp. 409–464. Academic Press, New York (1977)
12. Lang, S., Trotter, H.: Primitive points on elliptic curves. *Bull. Am. Math. Soc.* **83**, 289–292 (1977)
13. Miri, S.A., Murty, V.K.: An application of sieve methods to elliptic curves. *Indocrypt 2001*. Springer Lecture Notes, vol. 2247, pp. 91–98 (2001)
14. Murty, M.R.: On Artin’s conjecture. *J. Number Theory* **16**(2), 147–168 (1983)
15. Murty, M.R., Murty, V.K., Saradha, N.: Modular forms and the Chebotarev density theorem. *Am. J. Math.* **110**, 253–281 (1988)
16. Rubin, K.: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton–Dyer. In: *Arithmetic Theory of Elliptic Curves* (Cetraro, 1997). Lecture Notes in Math., vol. 1716, pp. 167–234. Springer, Berlin (1999)
17. Schaal, W.: On the large sieve method in algebraic number fields. *J. Number Theory* **2**, 249–270 (1970)
18. Serre, J.-P.: Résumé des cours de 1977–1978. *Annuaire du Collège de France*, pp. 67–70 (1978)
19. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. *Publ. Math. I. H. E. S.* **54**, 123–201 (1981)
20. Serre, J.-P.: *Collected papers*, vol. III. Springer, Heidelberg (1985)
21. Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, Princeton (1994)
22. Silverman, J.H.: *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, vol. 106. Springer, New York (1986)
23. Silverman, J.H.: *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, vol. 151. Springer, New York (1994)
24. Steuding, J., Weng, A.: On the number of prime divisors of the order of elliptic curves modulo  $p$ . *Acta Arith.* **117**(4), 341–352 (2005)