ACTA ARITHMETICA
119.3 (2005)

Reductions of an elliptic curve with almost prime orders

by

Alina Carmen Cojocaru (Princeton, NJ)

1. Introduction. Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. If $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$, then we can define a group structure on $E(\overline{\mathbb{Q}})$. Let $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ be the endomorphism ring of E over $\overline{\mathbb{Q}}$. We know that $\mathbb{Z}$ embeds into this ring, and that most of the time this embedding is actually an isomorphism. If so, i.e. if $\mathbb{Z} \simeq \mathrm{End}_{\overline{\mathbb{Q}}}(E)$, then we say that E is *without complex multiplication* (or *non-CM*). If $\mathbb{Z}$ is strictly contained in $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$, then $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ 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* $\mathcal{O}$ (or *has CM by* $\mathcal{O}$) and that K is the *CM field* of E. Throughout this paper we make the convention that a CM curve E has $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ isomorphic to the full ring of integers $\mathcal{O}_K$ of its CM field K.

If we restrict our attention to the group $E(\mathbb{Q})$ of $\mathbb{Q}$-rational points of E, then we know by Mordell's Theorem that this is a finitely generated abelian group, hence we have a group isomorphism $E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{\mathrm{tors}}$ for some non-negative integer r, called the *rank of* E *over* $\mathbb{Q}$, and with $E(\mathbb{Q})_{\mathrm{tors}}$ denoting the torsion subgroup of $E(\mathbb{Q})$. It is well known that a good understanding of both r and $E(\mathbb{Q})_{\mathrm{tors}}$ could be achieved by studying the reductions of E modulo rational primes.

More precisely, for a prime $p > 3$ with $p \nmid N$, let E_p be the *reduction of* E *modulo* p. This is an elliptic curve over $\mathbb{F}_p$, the finite field with p elements, whose group $E_p(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points is finite, of cardinality

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

for an integer a_p satisfying Hasse's inequality

$$|a_p| < 2\sqrt{p}. \tag{2}$$

2000 *Mathematics Subject Classification*: 11N05, 11N13, 11N36, 11R45, 14H52.
Research supported in part by an NSERC postdoctoral fellowship.

The integers a_p can be used to define an L-function associated to E, which, by a famous conjecture of Birch and Swinnerton-Dyer, provides information about the rank r of E. The groups $E_p(\mathbb{F}_p)$ can also be used to obtain a precise description of $E(\mathbb{Q})_{\text{tors}}$ by combining a classical result of Nagell and Lutz with the fact that $E(\mathbb{Q})_{\text{tors}}$ embeds into $E_p(\mathbb{F}_p)$ for almost all p.

More motivation for studying the groups $E_p(\mathbb{F}_p)$, *as p varies*, arises from interesting analogies between natural questions about these groups and classical questions in number theory. For example, by noting that $E_p(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \times \mathbb{Z}/d_pe_p\mathbb{Z}$ for some integers d_p, e_p uniquely determined by p and E, one may ask: given a fixed integer $d \neq 0$, for how many primes $p \leq x$ do we have $d_p = d$? The particular case that $d_p = d = 1$ (i.e. $E_p(\mathbb{F}_p)$ is cyclic) has been studied extensively over the past 30 years (see [Co1] and the references therein; also see [Co1] for general d). The question about the cyclicity of $E_p(\mathbb{F}_p)$ may be viewed as a subproblem of an elliptic curve version of Artin's problem about primitive roots, formulated by Lang and Trotter [LaTr] in 1977, and investigated in [GuMu]: given an elliptic curve E over $\mathbb{Q}$ with rank ≥ 1, and given $\alpha \in E(\mathbb{Q})$ a point of infinite order, for how many primes $p \leq x$ do we have $E_p(\mathbb{F}_p) = \langle \alpha \pmod p \rangle$? Clearly, if $\#E_p(\mathbb{F}_p)$ is prime, then $E_p(\mathbb{F}_p) = \langle \alpha \pmod p \rangle$ is satisfied for any α. Based on this observation, N. Koblitz [Ko] formulated the stronger question: for how many primes p is $\#E_p(\mathbb{F}_p)$ prime? More precisely, with the convention (kept throughout the paper) that p denotes a rational prime, we have:

Conjecture 1 (Koblitz, 1988 [Ko]). *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N, and such that the finitely many elliptic curves which are $\mathbb{Q}$-isogenous to E have a trivial $\mathbb{Q}$-torsion group. Then there exists a positive constant $C(E)$, depending on E, such that, as $x \to \infty$,*

$$\#\{p \leq x : p \nmid N, \#E_p(\mathbb{F}_p) = p + 1 - a_p \text{ is a prime}\} \sim C(E) \frac{x}{(\log x)^2}.$$

The motivation for this conjecture comes from elliptic curve cryptography, for which one needs elliptic curves over finite fields such that the groups of points of these curves have (large) prime orders. Heuristics similar to the ones of Hardy and Littlewood on the twin prime conjecture led Koblitz to the above formula.

No progress was made on Koblitz's Conjecture until recently, when S. Ali Miri and V. Kumar Murty [MiMu] exploited the similarity between the primality of $\#E_p(\mathbb{F}_p) = p + 1 - a_p$ and that of $p + 2$. More precisely, they carried out an elliptic curve version of the classical result that there are infinitely many primes p such that $p+2$ has at most 4 distinct prime divisors, described in [Bo, pp. 71–75] as an application of Selberg's sieve. Their proof deals only with non-CM elliptic curves, but could be easily modified to handle CM elliptic curves as well. It makes use of an effective version of the

Chebotarev Density Theorem, due to Lagarias and Odlyzko [LaOd], which requires the assumption of GRH.

THEOREM 2 (S. Ali Miri and V. Kumar Murty, 2001 [MiMu]). *Let E be a non-CM elliptic curve defined over $\mathbb{Q}$, of conductor N, and such that the finitely many elliptic curves which are $\mathbb{Q}$-isogenous to E have a trivial torsion group. Assume the Generalized Riemann Hypothesis (GRH) for Dedekind zeta functions. Then there exists a positive constant $C(E)$, depending on E, such that, as $x \to \infty$,*

$$\#\{p \le x : p \nmid N, \#E_p(\mathbb{F}_p) \text{ has at most } 16 \text{ distinct prime factors}\} \ge C(E)\,\frac{x}{(\log x)^2}.$$

Currently, the best result about the number of primes p for which $p+2$ is almost a prime is that there are infinitely many primes p for which $p+2$ has at most 2 prime divisors (counted with multiplicities) and was obtained by J. Chen using sieves with weights (see [Ch] or [HaRi, pp. 320–338]). Chen's method does not seem to be amenable to generalizations to treat the situation of elliptic curves. The method of proof of the slightly weaker result that there are infinitely many primes p for which $p+2$ has at most 3 prime divisors (counted with multiplicities) [HaRi, pp. 247–252], based on the weighted sieve of Richert [Ri], can, however, be generalized. Elaborating on the ideas introduced in [MiMu], and using Richert's sieve, an improved Chebotarev Density Theorem due to Murty, Murty and Saradha [MuMuSa], and a reduction method due to Serre [Se2], J. Steuding and A. Weng [StWe] showed:

THEOREM 3 (J. Steuding and A. Weng, 2005 [StWe]). *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N, and such that the finitely many elliptic curves which are $\mathbb{Q}$-isogenous to E have a trivial $\mathbb{Q}$-torsion group. Assume GRH for Dedekind zeta functions.*

(i) *If E is non-CM, then there exists a positive constant $C(E)$, depending on E, such that, as $x \to \infty$,*

$$\#\{p \le x : p \nmid N, \#E_p(\mathbb{F}_p) \text{ has at most } 8 \text{ prime factors}\} \ge C(E)\,\frac{x}{(\log x)^2}.$$

(ii) *If E has CM by the full ring of integers of an imaginary quadratic field, then there exists a positive constant $C(E)$, depending on E, such that, as $x \to \infty$,*

$$\#\{p \le x : p \nmid N, \#E_p(\mathbb{F}_p) \text{ has at most } 3 \text{ prime factors}\} \ge C(E)\,\frac{x}{(\log x)^2}.$$

We emphasize that in Theorem 3, the prime factors of $\#E_p(\mathbb{F}_p)$ are counted with multiplicities.

Certainly one would like to have unconditional results, which we succeed in proving if E is a curve with CM. This is the content of our main theorem below:

THEOREM 4. *Let E be a CM elliptic curve defined over $\mathbb{Q}$, of conductor N, and such that the finitely many elliptic curves which are $\mathbb{Q}$-isogenous to E have a trivial $\mathbb{Q}$-torsion group. Then, without any unproven hypotheses, there exists a positive constant $C(E)$, depending on E, such that, as $x \to \infty$,*

$$\#\{p \le x : p \nmid N,\ \#E_p(\mathbb{F}_p) \text{ has at most } 5 \text{ prime factors}\} \ge C(E)\,\frac{x}{(\log x)^2}.$$

In [MiMu], Miri and Murty showed in addition to Theorem 2 that, if GRH holds and if E is non-CM, then for almost all primes p the group $E_p(\mathbb{F}_p)$ has $\log\log p$ distinct prime factors. The ideas used in the proof of Theorem 4 can be used to prove the aforementioned result in the case that E is with CM and without assuming GRH. Moreover, a careful look at the proof given by Miri and Murty reveals that in the non-CM case we do not need to assume the full strength of GRH, but a quasi-GRH, defined as follows. Let K be a number field and let $1/2 \le \theta < 1$; we say that the Dedekind zeta function $\zeta_K(s)$ of K satisfies the *θ-quasi-GRH* if $\zeta_K(s)$ has a zero-free region of $s \in \mathbb{C}$, $\mathrm{Re}(s) > \theta$. We show:

THEOREM 5. *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N. If E is non-CM, we assume that the Dedekind zeta functions satisfy the θ-quasi-GRH for some arbitrary $1/2 \le \theta < 1$. Let $\nu(n)$ denote the number of distinct prime factors of an integer n. Then, as $x \to \infty$,*

$$\sum_{\substack{p \le x \\ p \nmid N}} (\nu(p+1-a_p) - \log\log p)^2 = \mathrm{O}_N\left(\frac{x \log\log x}{\log x}\right).$$

The implied O_N-constant depends on the conductor N of E.

Here is an immediate consequence of this result:

COROLLARY 6. *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N. If E is non-CM, assume the θ-quasi-GRH for Dedekind zeta functions for some arbitrary $1/2 \le \theta < 1$. Let $\varepsilon > 0$. Then, except possibly for*

$$\mathrm{O}_{N,\varepsilon}\left(\frac{x}{(\log x)(\log\log x)^{2\varepsilon}}\right)$$

of the primes $p \le x$, the number $\nu(\#E_p(\mathbb{F}_p))$ of distinct prime factors of $\#E_p(\mathbb{F}_p)$ satisfies

$$\log\log p - (\log\log p)^{1/2+\varepsilon} < \nu(\#E_p(\mathbb{F}_p)) < \log\log p + (\log\log p)^{1/2+\varepsilon}.$$

Another immediate consequence is as follows. Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N. If E is non-CM, assume the θ-quasi-GRH for Dedekind zeta functions for some arbitrary $1/2 \le \theta < 1$. Then

$$\#\{p \le x : p \nmid N,\ \#E_p(\mathbb{F}_p) \text{ is prime}\} \ll_N \frac{x}{(\log x)(\log\log x)}.$$

The implied $\ll_N$-constant depends on the conductor N of E.

One could ask if it is possible to obtain an upper bound of the right order of magnitude for the number of primes $p \le x$ for which $\#E_p(\mathbb{F}_p)$ is prime. We can do so by using Selberg's sieve and the ideas employed in the proofs of the previous theorems. We obtain:

PROPOSITION 7. *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N. If E is non-CM, assume the θ-quasi-GRH for Dedekind zeta functions for some arbitrary $1/2 \le \theta < 1$. Then*

$$\#\{p \le x : p \nmid N,\ \#E_p(\mathbb{F}_p) \textit{ is prime}\} \ll_N \frac{x}{(\log x)^2}.$$

Also, if E is non-CM we have, unconditionally,

$$\#\{p \le x : p \nmid N,\ \#E_p(\mathbb{F}_p) \textit{ is prime}\} \ll_N \frac{x}{(\log x)(\log\log\log x)}.$$

The implied $\ll_N$-constants depend on the conductor N of E.

As a corollary, we obtain an elliptic curve analogue of Brun's Theorem about the convergence of the sum of reciprocals of twin primes:

COROLLARY 8. *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N. If E is non-CM, assume the θ-quasi-GRH for Dedekind zeta functions for some arbitrary $1/2 \le \theta < 1$. Then*

$$B(E) := \sum_{\substack{p \nmid N \\ \#E_p(\mathbb{F}_p) \textit{ prime}}} \frac{1}{p} < \infty.$$

The constant $B(E)$ has been computed for a few particular elliptic curves E in [La].

2. Divisors of $\#E_p(\mathbb{F}_p)$

2.1. *A general sieve problem.* Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. We keep the notation introduced in Section 1, and we recall that our principal goal in this paper is to count rational primes $p \nmid N$ for which $\#E_p(\mathbb{F}_p) = p + 1 - a_p$ is a prime or an "almost" prime (that is, it has a bounded number of prime factors). Our general strategy is to formulate this as a sieve problem, and then to use appropriate sieve methods to tackle it.

More precisely, we set

$$\begin{aligned}\mathcal{A} &:= \{p \le x : p \nmid N\},\\ \mathcal{P} &:= \{l : l \text{ a rational prime}\},\\ \mathcal{A}_{l^n} &:= \{p \in \mathcal{A} : p \neq l,\ l^n \mid p+1-a_p\} \quad \text{for each } l \in \mathcal{P},\ n \in \mathbb{N},\end{aligned}$$

and the sieve problem consists of estimating, from above and below, the cardinality

$$S(\mathcal{A}, \mathcal{P}, z) := \#\Big(\mathcal{A} \setminus \bigcup_{\substack{l \in \mathcal{P}\\ l<z}} \mathcal{A}_l\Big),$$

or the cardinality of a variant of the above set, where $z = z(x)$ is a parameter to be chosen in each case. As in any sieve problem, the main necessary ingredient is a good estimate for the cardinalities of the condition sets $\mathcal{A}_{l^n}$.

Before continuing, let us note that for *supersingular* primes p of E (that is, primes for which $a_p = 0$), the problem of investigating the primality of $\#E_p(\mathbb{F}_p)$ (or of $\#E_p(\mathbb{F}_p)/2$) is the same as the classical twin prime problem. Therefore, to remain in a genuine elliptic curve setting, our investigations should be restricted to primes p of *ordinary* reduction for E (that is, primes for which $a_p \neq 0$). In the case of an elliptic curve E without CM, most of the primes are of ordinary reduction, that is, there are only $\mathrm{O}_N(x^{3/4})$ supersingular primes $\le x$ (see [El, pp. 25–26]). Hence in this case it is unnecessary to distinguish between supersingular and ordinary primes in our sievings. If E is with CM, then by results of Deuring [De], half of the primes are supersingular, half are ordinary. To be more precise, the supersingular primes of E are the primes inert in the CM field K of E, and the ordinary primes of E are the primes splitting completely in K. Therefore in the CM case the data for the sieve problem that we should actually investigate is:

$$\begin{aligned}\mathcal{A}^{\mathrm{o}} &:= \{p \le x : p \nmid N,\ a_p \neq 0\},\\ \mathcal{P} &:= \{l : l \text{ a rational prime}\},\\ \mathcal{A}^{\mathrm{o}}_{l^n} &:= \{p \in \mathcal{A}^{\mathrm{o}} : p \neq l,\ l^n \mid p+1-a_p\} \quad \text{for each } l \in \mathcal{P},\ n \in \mathbb{N}.\end{aligned}$$

2.2. *Chebotarev conditions.* Now let us see what estimates we can obtain for the cardinalities of the condition sets $\mathcal{A}_{l^n}$ and $\mathcal{A}^{\mathrm{o}}_{l^n}$. As explained in [Ko, pp. 159–163], for primes $l \neq p$ the congruence $l^n \mid p+1-a_p$ translates into a Chebotarev condition for p. Then one could use the Chebotarev Density Theorem to estimate $\#\mathcal{A}_{l^n}$ and $\#\mathcal{A}^{\mathrm{o}}_{l^n}$. We shall elaborate on this remark in what follows.

Let l be a rational prime and n a positive integer. Let $E[l^n]$ be the group of l^n-division points of E. We recall that we have a group isomorphism $E[l^n] \simeq \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$, and that, by adjoining to $\mathbb{Q}$ the x- and y-coordinates of the points in $E[l^n]$, we obtain a finite Galois extension $\mathbb{Q}(E[l^n])$ of $\mathbb{Q}$.

Moreover, we can define a natural representation

$$\phi_{l^n} : \mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z}),$$

which has the important properties that it is injective and that

$$\det \mathrm{Frob}_p(\mathbb{Q}(E[l^n])/\mathbb{Q}) \equiv p \pmod{l^n},$$
$$\mathrm{tr}\, \mathrm{Frob}_p(\mathbb{Q}(E[l^n])/\mathbb{Q}) \equiv a_p \pmod{l^n}$$

for any prime $p \nmid lN$, where $\mathrm{Frob}_p(\mathbb{Q}(E[l^n])/\mathbb{Q})$ denotes the Artin symbol of p in $\mathbb{Q}(E[l^n])/\mathbb{Q}$, and where we view $\mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q})$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$ (here det and tr denote the determinant and trace of a matrix). Consequently, the primes $p \nmid lN$ for which $p + 1 - a_p \equiv 0 \pmod{l^n}$ are the ones for which $\mathrm{Frob}_p(\mathbb{Q}(E[l^n])/\mathbb{Q})$ is contained in the conjugacy set (i.e. a finite union of conjugacy classes) of $\mathrm{Gal}(\mathbb{Q}(E[l^n])/\mathbb{Q})$ consisting of elements with at least one eigenvalue equal to 1.

The Chebotarev Density Theorem allows us to count primes $p \le x$ whose Artin symbol in a finite Galois extension L of $\mathbb{Q}$ lies in a given conjugacy set C of the Galois group G of $L/\mathbb{Q}$. Stated rigorously, it says that, as $x \to \infty$,

$$\#\{p \le x : \mathrm{Frob}_p(L/\mathbb{Q}) \subseteq C\} \sim \frac{\#C}{\#G} \operatorname{li} x,$$

where $\operatorname{li} x$ denotes the logarithmic integral $\int_2^x \frac{1}{\log t}\, dt$. (Here, for two functions $f, g : D \subseteq \mathbb{R} \to \mathbb{R}$ with D infinite and $g \neq 0$ we say that $f \sim g$ if $\lim_{x\to\infty} f(x)/g(x) = 1$.)

Combining the Chebotarev Density Theorem with the previous remark we see that

$$\#\mathcal{A}_{l^n} = \delta(l^n) \operatorname{li} x + R_{l^n} \quad \text{and} \quad \#\mathcal{A}^{\mathrm{o}}_{l^n} = \delta^{\mathrm{o}}(l^n) \operatorname{li} x + R^{\mathrm{o}}_{l^n}$$

for some "densities" $\delta(l^n), \delta^{\mathrm{o}}(l^n)$, and some "error terms" $R_{l^n}, R^{\mathrm{o}}_{l^n}$.

Since from classical theory we have information about the image of the representation ϕ_{l^n}, the precise sizes of the densities $\delta(l^n), \delta^{\mathrm{o}}(l^n)$ can be easily calculated by counting 2×2 matrices with one eigenvalue equal to 1. Indeed, we recall:

PROPOSITION 9. *Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N.*

(i) *If E is non-CM, then there exists a positive constant $A(E)$, depending on E, such that for any integer d coprime to $A(E)$ we have*

$$\mathrm{Gal}(\mathbb{Q}(E[d])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}).$$

(ii) *If E has CM by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K, then for any integer d coprime to $6N$ we have*

$$\mathrm{Gal}(\mathbb{Q}(E[d])/K) \simeq (\mathcal{O}_K/d\mathcal{O}_K)^*.$$

For proofs of (or more details on) these results, we refer the reader to [Co2], [Ru, p. 187], and [Se1].

From here we deduce that for integers d composed of sufficiently large primes, the densities $\delta(d)$ and $\delta^{\mathrm{o}}(d)$ are multiplicative in d. Moreover, we can calculate the following explicit formulae:

PROPOSITION 10. *Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. Let l be a rational prime and n a positive integer.*

(i) *If E is non-CM, then*

$$\delta(l^n) = 1/l^n + \mathrm{O}(1/l^{n+1}).$$

(ii) *If E has CM by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K, then*

$$\delta^{\mathrm{o}}(l^n) = \begin{cases} 1/2l^{n+1} + \mathrm{O}(1/l^{n+2}) & \text{if } l \text{ is inert in } K \text{ and } n \text{ odd}, \\ 1/2l^n + \mathrm{O}(1/l^{n+1}) & \text{if } l \text{ is inert in } K \text{ and } n \text{ even}, \\ (n+1)/2l^n + \mathrm{O}(1/l^{n+1}) & \text{if } l \text{ splits completely in } K, \\ 1/2l^n + \mathrm{O}(1/l^{n+1}) & \text{if } l \text{ ramifies in } K. \end{cases}$$

For explanations on how to obtain these estimates we refer the reader to [MiMu] and [StWe]. As we will see in Section 2.4, part (ii) of this proposition is actually an immediate consequence of Lemma 14.

More effort is required to find satisfactory estimates for the error terms. We shall discuss this in more detail in the next section.

2.3. *Conditional estimates for R_d, R_d^{o}.* In [StWe, pp. 345–347], Steuding and Weng obtained estimates for R_l, R_l^{o} and $R_{l^2}, R_{l^2}^{\mathrm{o}}$ by using effective versions of the Chebotarev Density Theorem due to R. Murty, K. Murty and N. Saradha [MuMuSa, p. 265, p. 268], together with a "reduction method" of Serre [Se2, Section 2.6]. Implicit in their analyzes are also estimates for $R_{l^n}, R_{l^n}^{\mathrm{o}}$ for any $n \geq 1$. We record their estimates for general R_d, R_d^{o} below.

PROPOSITION 11. *Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. Let d be a positive integer. Assume GRH for Artin L-functions.*

(i) *If E is without CM, then*

$$R_d = \mathrm{O}(d^{3/2} x^{1/2} \log(dNx)).$$

(ii) *If E has CM by the full ring of integers of an imaginary quadratic field, then*

$$R_d^{\mathrm{o}} = \mathrm{O}(d^{1/2} x^{1/2} \log(dNx)).$$

The implied O*-constants are absolute.*

REMARK 12. Using the effective versions of the Chebotarev Density Theorem given by Lagarias and Odlyzko [LaOd], we can easily obtain estimates for the error terms R_d, R_d^{o} under the assumption of more relaxed

formulations of GRH, as follows. Let $1/2 \le \theta < 1$. Under the θ-quasi-GRH for the Dedekind zeta functions of the division fields of an elliptic curve E defined over $\mathbb{Q}$ and of conductor N, we obtain:

(i) if E is without CM, then
$$R_d = \mathrm{O}(d^3 x^\theta \log(dNx));$$

(ii) if E has CM, then
$$R_d^{\mathrm{o}} = \mathrm{O}(dx^\theta \log(dNx)).$$

The implied O-constants are absolute.

Remark 13. Using the results in [LaOd], we can also obtain *unconditional* estimates for the error terms R_d, R_d^{o}, as long as d is *very small* compared to x. More precisely, if $d \ll \log\log x$ and if $A > 0$ is an arbitrary real number, then:

(i) if E is without CM, we have
$$R_d = \mathrm{O}_A\left(d^3 \frac{x}{(\log x)^A}\right);$$

(ii) if E has CM, we have
$$R_d^{\mathrm{o}} = \mathrm{O}_A\left(d \frac{x}{(\log x)^A}\right).$$

The implied O_A-constants depend only on A.

2.4. *Unconditional estimates for R_d^{o} in the CM case.* We emphasize that Proposition 11 assumes the validity of GRH. An important question to ask is whether we can eliminate this assumption. As will be explained below, we are able to do so in the case of an elliptic curve with CM. The key lemma that we rely on is:

Lemma 14. *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N, and with CM by the full ring of integers $\mathcal{O}_K$ of K. Let $N_{K/\mathbb{Q}}(\cdot)$ denote the norm of K over $\mathbb{Q}$. Let $p \nmid N$ be a prime of ordinary reduction for E. Write $(p) = (\pi_p)(\overline{\pi}_p)$ for the prime factorization of p in K, where $\pi_p, \overline{\pi}_p$ are complex conjugate prime elements of $\mathcal{O}_K$ of norm $N_{K/\mathbb{Q}}(\pi_p) = p$. Let $l \ne p$ be another prime and n a positive integer.*

(i) *Assume that l is inert in K, that is, $(l) = L$ for some prime ideal L of $\mathcal{O}_K$ with $N_{K/\mathbb{Q}}(L) = l^2$. If n is odd, then the following assertions are equivalent*:

(a) $l^n \mid \#E_p(\mathbb{F}_p)$;
(b) $l^{n+1} \mid \#E_p(\mathbb{F}_p)$;
(c) $\pi_p \equiv 1 \pmod{L^{(n+1)/2}}$.

If n is even, then $l^n \mid \#E_p(\mathbb{F}_p)$ if and only if $\pi_p \equiv 1 \pmod{L^{n/2}}$.

(ii) *Assume that l splits completely in K, that is, $(l) = L\overline{L}$ for a prime ideal L of $\mathcal{O}_K$ with $N_{K/\mathbb{Q}}(L) = l$. Here $\overline{L} \neq L$ is the complex conjugate of L. Then $l^n \,|\, \#E_p(\mathbb{F}_p)$ if and only if $\pi_p \equiv 1 \pmod{L^i\overline{L}^{n-i}}$ for some $0 \leq i \leq n$.*

(iii) *Assume that l ramifies in K, that is, $(l) = L^2$ for some prime ideal L of $\mathcal{O}_K$ with $N_{K/\mathbb{Q}}(L) = l$. Then $l^n \,|\, \#E_p(\mathbb{F}_p)$ if and only if $\pi_p \equiv 1 \pmod{L^n}$.*

Proof. First let us recall that for ordinary primes p of an elliptic curve E we have $p + 1 - a_p = (\pi_p - 1)(\overline{\pi}_p - 1)$; if, in addition, E has CM by K, then $\mathbb{Q}(\pi_p) = K$. Hence with p, E and K as in our lemma, $N_{K/\mathbb{Q}}(\pi_p - 1) = p + 1 - a_p$. The proof of the lemma is a straightforward consequence of this observation.

(i) We are in the case that l is inert in K. First, consider the case when n is odd. Assume that $\pi_p \equiv 1 \pmod{L^{(n+1)/2}}$. By taking $N_{K/\mathbb{Q}}(\cdot)$, we obtain $l^{n+1} \,|\, p + 1 - a_p$, and so $l^n \,|\, p + 1 - a_p$. Now assume that $l^n \,|\, p + 1 - a_p$. This implies that $L^n \,|\, (\pi_p - 1)(\overline{\pi}_p - 1)$ in $\mathbb{Q}(\pi_p) = K$, or, in other words, that

$$(\pi_p - 1)(\overline{\pi}_p - 1) = L^n(\alpha)$$

for some $\alpha \in \mathcal{O}_K$. Since $L = \overline{L}$ and $\overline{(\pi_p - 1)} = (\overline{\pi}_p - 1)$, and since $\mathcal{O}_K$ is a Dedekind domain, we obtain

$$(\pi_p - 1)(\overline{\pi}_p - 1) = L^{n+1}(\beta)$$

for some $\beta \in \mathcal{O}_K$, and moreover,

$$L^{(n+1)/2} \,|\, (\pi_p - 1),$$

i.e. $\pi_p \equiv 1 \pmod{L^{(n+1)/2}}$.

For n even, the proof proceeds along similar lines.

(ii) We are in the case that l splits completely in K. Assume that $\pi_p \equiv 1 \pmod{L^i\overline{L}^{n-i}}$ for some $0 \leq i \leq n$. By taking $N_{K/\mathbb{Q}}(\cdot)$, we deduce that $l^n \,|\, p + 1 - a_p$. Now assume that $l^n \,|\, p + 1 - a_p$. This implies that $L^n\overline{L}^n \,|\, (\pi_p - 1)(\overline{\pi}_p - 1)$ in $\mathbb{Q}(\pi_p) = K$, or that

$$(\pi_p - 1)(\overline{\pi}_p - 1) = L^n\overline{L}^n(\alpha)$$

for some $\alpha \in \mathcal{O}_K$. As in part (i), by using that $\overline{(\pi_p - 1)} = (\overline{\pi}_p - 1)$ and that $\mathcal{O}_K$ is a Dedekind domain, we obtain

$$L^i\overline{L}^{n-i} \,|\, (\pi_p - 1)$$

for some $0 \leq i \leq n$, hence $\pi_p \equiv 1 \pmod{L^i\overline{L}^{n-i}}$.

(iii) Finally, we are in the case that l ramifies in K. Assume that $\pi_p \equiv 1 \pmod{L^n}$. By taking $N_{K/\mathbb{Q}}(\cdot)$, this gives us $l^n \,|\, p + 1 - a_p$. Now assume that

$l^n \mid p+1-a_p$. This implies that $L^{2n} \mid (\pi_p - 1)(\overline{\pi}_p - 1)$ in $\mathbb{Q}(\pi_p) = K$, or that

$$(\pi_p - 1)(\overline{\pi}_p - 1) = L^{2n}(\alpha)$$

for some $\alpha \in \mathcal{O}_K$. Again, by keeping in mind that $\overline{L} = L$, $\overline{(\pi_p - 1)} = (\overline{\pi}_p - 1)$ and that $\mathcal{O}_K$ is a Dedekind domain, we obtain

$$L^n \mid (\pi_p - 1),$$

hence $\pi_p \equiv 1 \pmod{L^n}$. ∎

Using this lemma and appealing to number field versions of the Siegel–Walfisz Theorem, we could obtain unconditional estimates for R_d° for positive integers d lying in a short range relative to x (roughly this means that d should be smaller than a power of $\log x$). However, for our purposes it is not necessary to estimate each error term individually, but as a sum of the form $\sum_{d \le y} |R_d^{\circ}|$ for some parameter $y = y(x)$. It is desirable that y be as close to x as possible. We will be able to estimate sums of this form, unconditionally, by combining Lemma 14 with a number field version of the Bombieri–Vinogradov Theorem, due to Huxley, which we record below. Before, let us recall some standard notation. If $\wp$ is a prime ideal of the ring of integers $\mathcal{O}_K$ of a number field K, and $k \ge 1$, we define the *generalized Euler function* of $\wp^k$ by

$$\Phi_K(\wp^k) = N_{K/\mathbb{Q}}(\wp)^k \left(1 - \frac{1}{N_{K/\mathbb{Q}}(\wp)}\right).$$

This definition is extended by multiplicativity to all non-zero ideals of $\mathcal{O}_K$. Also, if I is an ideal of $\mathcal{O}_K$, we define the *generalized von Mangoldt function* of I by $\Lambda_K(I) = \log N_{K/\mathbb{Q}}(\wp)$ if $I = \wp^k$ for some prime ideal $\wp$ of $\mathcal{O}_K$ and some $k \ge 1$, and 0 otherwise.

Proposition 15 (Huxley [Hu, Thm. 1, p. 233]). *Let K be a number field of degree n. For each ideal I of $\mathcal{O}_K$, let $h(I)$ denote the number of reduced narrow ideal classes modulo I, and let $\Phi_K(I)$ denote the generalized Euler function of I. For a positive integer y and a narrow ideal class H modulo I, let*

$$\Psi(y, H) := \sum_{\substack{\wp^n \in H \\ N_{K/\mathbb{Q}}(\wp^n) \le y}} \Lambda_K(\wp^n),$$

where the sum is over prime ideal powers $\wp^n$ which lie in H and satisfy $N_{K/\mathbb{Q}}(\wp^n) \le y$, and $\Lambda_K(\wp^n)$ is the generalized von Mangoldt function of $\wp^n$. Then for any $A > 0$ there exists $B = B(A) > 0$ such that

$$\sum_{N_{K/\mathbb{Q}}(I) \le x^{1/2}/(\log x)^B} \frac{h(I)}{\Phi_K(I)} \max_H \max_{y \le x} \left| \Psi(y, H) - \frac{y}{h(I)} \right| \ll_{A,K} \frac{x}{(\log x)^A}, \tag{3}$$

where the first maximum is over reduced narrow ideal classes modulo I. The implied $\ll_{A,K}$-constant depends only on A and K.

REMARK 16. We will use Huxley's result, together with partial summation, in the case that K is the CM field of a CM elliptic curve E defined over $\mathbb{Q}$. We recall that such a field is imaginary quadratic, of class number 1. In this context (3) becomes

$$\sum_{N_{K/\mathbb{Q}}(I)\le x^{1/2}/(\log x)^B} \max_H \max_{y\le x} \left| \Pi(y,H) - \frac{\operatorname{li} y}{\Phi(I)} \right| \ll_{A,K} \frac{x}{(\log x)^A}, \tag{4}$$

where

$$\Pi(y,H) := \#\{(\pi) \in H : \pi \text{ a prime element in } \mathcal{O}_K,\ N_{K/\mathbb{Q}}(\pi) \le y\}.$$

We are ready to give unconditional estimates for $\sum_d |R_d^\circ|$ in the case of a CM elliptic curve.

PROPOSITION 17. *Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. Assume that E has CM by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Then for any $A > 0$ there exists $B = B(A) > 0$ such that, as $x \to \infty$,*

$$\sum_{d\le x^{1/4}/(\log x)^B} |R_d^\circ| \ll_{A,K} \frac{x}{(\log x)^A}.$$

The implied $\ll_{A,K}$-constant depends only on A and K.

Proof. First, let us set some notation. In what follows (as is the case throughout the paper), l denotes a rational prime. We write a positive integer d as

$$d = d_i d_r d_s,$$

where

$$d_i := \prod_{\substack{l^n \| d \\ l \text{ inert in } K}} l^n, \qquad d_r := \prod_{\substack{l^n \| d \\ l \text{ ramified in } K}} l^n, \qquad d_s := \prod_{\substack{l^n \| d \\ l \text{ splits in } K}} l^n,$$

and where by "splits" we mean "splits completely". Also, $l^n \| d$ means that $l^n \mid d$, but $l^{n+1} \nmid d$.

For each rational prime $l \mid d$, we will use the notation:

1. if $l \mid d_i$,
$$(l) = L$$
for a prime ideal L of $\mathcal{O}_K$ with $N_{K/\mathbb{Q}}(L) = l^2$;

2. if $l \mid d_r$,
$$(l) = L^2$$
for a prime ideal L of $\mathcal{O}_K$ with $N_{K/\mathbb{Q}}(L) = l$;

3. if $l \mid d_s$,
$$(l) = L\overline{L}$$
for complex conjugate distinct prime ideals $L, \overline{L}$ of $\mathcal{O}_K$ with $N_{K/\mathbb{Q}}(L) = N_{K/\mathbb{Q}}(\overline{L}) = l$.

Moreover, we denote by
$$d_s = l_1^{n_1} \cdots l_{\nu(d_s)}^{n_{\nu(d_s)}}$$
the prime factorization of d_s, and we set
$$I(d_i) := \prod_{\substack{l^n \| d_i \\ n \text{ odd}}} L^{(n+1)/2} \prod_{\substack{l^n \| d_i \\ n \text{ even}}} L^{n/2};$$
$$I(d_r) := \prod_{l^n \| d_r} L^n;$$
$$I^{i_1,\dots,i_{\nu(d_s)}}(d_s) := \prod_{1 \le j \le \nu(d_s)} L_j^{i_j} \overline{L}_j^{n_j - i_j}$$
for $0 \le i_1 \le n_1, \dots, 0 \le i_{\nu(d_s)} \le n_{\nu(d_s)}$.

Using Lemma 14, we see that
$$|R_d^{\circ}| \le \sum_{\substack{0 \le i_1 \le n_1 \\ \dots \\ 0 \le i_{\nu(d_s)} \le n_{\nu(d_s)}}} \left| \Pi^s(x; I(d_i)I(d_r)I^{i_1,\dots,i_{\nu(d_s)}}(d_s), 1) - \frac{1}{2\Phi(I(d_i)I(d_r)I^{i_1,\dots,i_{\nu(d_s)}}(d_s))} \operatorname{li} x \right|,$$
where for an ideal J of $\mathcal{O}_K$,
$$\Pi^s(x; J, 1) := \#\{(\pi) : \pi \text{ prime in } \mathcal{O}_K, \; N_{K/\mathbb{Q}}(\pi) = p \le x \text{ for some rational prime } p, \; \pi \equiv 1 \pmod{J}\}.$$
Therefore, if $y = y(x)$ is some positive real number, we have
$$\sum_{d \le y} |R_d^{\circ}| \le {\sum_{I(d)}}' \left| \Pi^s(x; I(d_i)I(d_r)I^{i_1,\dots,i_{\nu(d_s)}}(d_s), 1) - \frac{1}{2\Phi(I(d_i)I(d_r)I^{i_1,\dots,i_{\nu(d_s)}}(d_s))} \operatorname{li} x \right|, \tag{5}$$
where the summation ${\sum}'_{I(d)}$ is over ideals $I(d)$ of the form
$$I(d_i)I(d_r)I^{i_1,\dots,i_{\nu(d_s)}}(d_s)$$
of $\mathcal{O}_K$ with d such that
$$N_{K/\mathbb{Q}}(I(d)) = d_i d_r d_s \prod_{\substack{l^n \| d_i \\ n \text{ odd}}} l \le y.$$

For simplicity of notation, let $|\mathcal{R}_d|$ be the dth term in the sum on the right-hand side of (5).

By (4), for any $A > 0$ there exists $B = B(A) > 0$ such that

$$\sum_{\substack{d \\ N_{K/\mathbb{Q}}(I(d)) < x^{1/2}/(\log x)^B}} |\mathcal{R}_d| \ll_{A,K} \frac{x}{(\log x)^A}. \tag{6}$$

Now we choose

$$y := \frac{x^{1/4}}{(\log x)^{B/2}}$$

and observe that all ideals of the form $I(d)$ with $d \le y$ have $N_{K/\mathbb{Q}}(I(d)) \le x^{1/2}/(\log x)^B$. Combining this with (5) and (6) finishes the proof of the proposition. ∎

2.5. *Unconditional upper bounds for $\#\mathcal{A}_d^{\circ}$ in the CM case.* We recall the following result of Schaal:

Proposition 18 (Schaal, [Sc, Thm. 6, pp. 251–252]). *Let K be a number field of degree n_K and discriminant d_K, having r_1 real embeddings into $\mathbb{C}$ and $2r_2$ complex conjugate embeddings into $\mathbb{C}$. Let $r := r_1 + r_2 - 1$. Let α_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 $(\beta, I) = 1$. Take $M_1, \dots, M_{r_1} \in [0, \infty)$ and $P_1, \dots, P_{n_K} \in (0, \infty)$ with $P_j = P_{j+r_2}$ for $j = r_1 + 1, \dots, r_1 + r_2$. For $\omega \in \mathcal{O}_K$ denote by $\omega^{(j)}$ its jth conjugate. Consider the set*

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

where conditions (C) *are as follows*:

$$\text{(C)} \qquad \begin{aligned} &M_j \le \omega^{(j)} \le M_j + P_j, \quad \forall 1 \le j \le r_1, \\ &|\omega^{(j)}| \le P_j, \quad \forall r_1 + 1 \le j \le n_K. \end{aligned}$$

If $P := P_1 \cdots P_{n_K} \ge 2$ and $N_{K/\mathbb{Q}}(I) \le P/(\log P)^{2r+2/n_K}$, then

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

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

Combining this with Lemma 14 we obtain immediately:

Proposition 19. *Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N, and with CM by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K (recall that it has class number 1). Let $d \le (x/\log x)^{1/2}$*

and write $d = d_i d_r d_s$ *as in the proof of Proposition* 17. *Then*

$$\#\mathcal{A}_d^{\circ} \ll \frac{\nu(d_s)}{\prod_{l|d_i}(l^2-1)\cdot\prod_{l|d_r} l(l-1)\cdot\prod_{l|d_s}(l-1)}\cdot\frac{x}{\log x},$$

where l *denotes a rational prime.*

3. Proof of Theorem 4

3.1. *Richert's sieve with weights.* The proof of Theorem 4 is an application of the weighted sieve of Richert [HaRi, Thm. 9.1, p. 243, Lemma 9.1, pp. 246–247], which we recall below:

PROPOSITION 20 (Richert's weighted sieve). *Let* $\mathcal{A}$ *be a finite set of* (*not necessarily positive and not necessarily distinct*) *integers. Let* $\mathcal{P}$ *be an infinite set of rational primes. For each prime* $l \in \mathcal{P}$, *let* $\mathcal{A}_l := \{a \in \mathcal{A} : a \equiv 0 \pmod l\}$. *Write*

$$\#\mathcal{A} = X + R_1 \quad \textit{and} \quad \#\mathcal{A}_l = \delta(l)X + R_l$$

for each $l \in \mathcal{P}$, *where* X *is some approximation to* $\#\mathcal{A}$, $\delta(l)X$ *is some approximation to* $\#\mathcal{A}_l$, *and* R_1, R_l *are the remainders in these approximations. Let* d *denote squarefree positive integers composed of primes of* $\mathcal{P}$ *and let*

$$\delta(d) := \prod_{l|d}\delta(l), \qquad \mathcal{A}_d := \bigcap_{l|d}\mathcal{A}_l, \qquad R_d := \#\mathcal{A}_d - \delta(d)X.$$

For $z > 0$, *let*

$$P(z) := \prod_{\substack{l\in\mathcal{P}\\ l<z}} l, \qquad W(z) := \prod_{l|P(z)}(1-\delta(l)).$$

Assume that:

(Ω_1) *there exists* $A_1 \geq 0$ *such that* $0 \leq \delta(l) \leq 1 - 1/A_1$ *for all* $l \in \mathcal{P}$;

($\Omega_2(1, L)$) *there exist* $L \geq 1$ *and* $A_2 \geq 1$ *such that, if* $2 \leq w \leq z$, *then*

$$-L \leq \sum_{w\leq p\leq z}\delta(p)\log p - \log\frac{z}{w} \leq A_2;$$

(R$(1, \alpha)$) *there exist* $0 < \alpha < 1$ *and* $A_3, A_4 \geq 1$ *such that, if* $X \geq 2$, *then*

$$\sum_{d<X^{\alpha}/(\log X)^{A_4}} 3^{\nu(d)}|R_d| \leq A_3\frac{X}{(\log X)^2}.$$

Assume also that there exist $u, v, \lambda \in \mathbb{R}$ *and* $A_5 \geq 1$ *such that*

$$\frac{1}{\alpha} < u < v, \qquad \frac{2}{\alpha} \leq v \leq \frac{4}{\alpha}, \qquad 0 < \lambda < A_5.$$

Set

$$\mathcal{W}(\mathcal{A},\mathcal{P},v,u,\lambda) := \sum_{\substack{a\in\mathcal{A}\\(a,P(X^{1/v}))=1}} \left(1-\lambda \sum_{\substack{X^{1/v}\le l<X^{1/u}\\ l|a,\, l\in\mathcal{P}}} \left(1-u\,\frac{\log l}{\log X}\right)\right).$$

Then there exists a constant $c=c(A_1,\dots,A_5,u,v,\alpha)>0$ such that

$$\mathcal{W}(\mathcal{A},\mathcal{P},v,u,\lambda) \ge X\cdot W(X^{1/v})\cdot\left(f(\alpha,v,u,\lambda)-\frac{cL}{(\log X)^{1/14}}\right),$$

where

$$f(\alpha,v,u,\lambda) := \frac{2e^{\gamma}}{\alpha v}\left(\log(\alpha v-1)-\lambda\alpha u\log\frac{v}{u}+\lambda(\alpha u-1)\log\frac{\alpha v-1}{\alpha u-1}\right)$$

and γ is Euler's constant.

3.2. *An infinitude of primes p with $\nu(\#E_p(\mathbb{F}_p))$ absolutely bounded.* Let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N, such that the finitely many elliptic curves $\mathbb{Q}$-isogenous to E have a trivial torsion group. We assume that E has CM by the full ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. With notation as in Section 1, we want to count the primes $p\nmid N$ with $a_p\ne 0$ for which $\#E_p(\mathbb{F}_p)=p+1-a_p$ has a bounded (and small) number of prime divisors. We do so by applying Proposition 20 to the sieve problem $(\mathcal{A}^{\mathrm{o}},\mathcal{P},\mathcal{A}^{\mathrm{o}}_{l^n})$ introduced in Section 2.

To apply the sieve we need to verify assumptions (Ω_1), $(\Omega_2(1,L))$ and $(\mathrm{R}(1,\alpha))$. As in [StWe, pp. 347, 350], it is straightforward to verify (Ω_1) and $(\Omega_2(1,L))$. The difficulty lies in verifying $(\mathrm{R}(1,\alpha))$, for which estimates for R^{o}_l are needed. In [StWe], the authors used GRH. If α is chosen appropriately, we are able to verify $(\mathrm{R}(1,\alpha))$ without any unproven hypotheses, by using Proposition 17.

Let

$$\alpha := \frac{1}{4.05}$$

and let $B=B(2)$ be given by Proposition 17. The Cauchy–Buniakowski–Schwarz inequality gives us

$$\sum_{d\le x^{1/4}/(\log x)^B} 3^{\nu(d)}|R^{\mathrm{o}}_d| \le \left(\sum_{d\le x^{1/4}/(\log x)^B}\frac{3^{2\nu(d)}}{d}\right)^{1/2}\left(\sum_{d\le x^{1/4}/(\log x)^B} d|R^{\mathrm{o}}_d|^2\right)^{1/2}. \tag{7}$$

By elementary methods,

$$\sum_{d\le x^{1/4}/(\log x)^B}\frac{3^{2\nu(d)}}{d} \le \sum_{d\le x^{1/4}/(\log x)^B}\frac{\tau(d)^{2\log 3/\log 2}}{d} \ll (\log x)^{\beta}$$

for some $\beta > 0$, where $\tau(\cdot)$ is the divisor function (i.e. $\tau(d) = \sum_{\delta|d} \delta$). Now note that, by Proposition 19, $d|R_d^{\circ}| \ll x$. Hence

$$\sum_{d \le x^{1/4}/(\log x)^B} 3^{\nu(d)} |R_d^{\circ}| \ll x^{1/2} (\log x)^{\beta} \Big(\sum_{d \le x^{1/4}/(\log x)^B} |R_d^{\circ}| \Big)^{1/2}.$$

Proposition 17 can now be invoked for the last sum, leading to

$$\sum_{d \le x^{1/4}/(\log x)^B} 3^{\nu(d)} |R_d^{\circ}| \ll \frac{x}{(\log x)^2}.$$

This verifies $(\mathrm{R}(1, \alpha))$.

To apply the sieve, let $u, v, \lambda, A_5 \in \mathbb{R}$ be such that

$$\frac{1}{\alpha} < u < v, \quad \frac{2}{\alpha} \le v \le \frac{4}{\alpha}, \quad 0 < \lambda \le A_5. \tag{8}$$

Later on we will specify precise values of these parameters. Richert's weighted sieve gives

$$\mathcal{W}(\mathcal{A}, \mathcal{P}, v, u, \lambda) \ge X \cdot W(X^{1/v}) \Big(f(\alpha, v, u, \lambda) - \frac{C}{(\log X)^{1/14}} \Big)$$

for some constant $C > 0$, where

$$X := \frac{1}{2} \operatorname{li} x.$$

As explained in [StWe, pp. 348, 350], we have

$$W(X^{1/v}) \gg_E \frac{1}{\log X} \prod_{\substack{l \text{ prime} \\ \chi(l)=0}} \Big(1 - \frac{1}{(l-1)^2} \Big) \times \prod_{\substack{l \text{ prime} \\ \chi(l) \ne 0}} \Big(1 - \chi(l) \frac{l^2 - l - 1}{(l - \chi(l))(l-1)^2} \Big), \tag{9}$$

where $\chi(\cdot)$ is the quadratic character associated to the CM field of E. Thus

$$\mathcal{W}(\mathcal{A}, \mathcal{P}, v, u, \lambda) \gg_E \frac{x}{(\log x)^2} \Big(f(\alpha, v, u, \lambda) - \frac{C}{(\log x)^{1/15}} \Big). \tag{10}$$

Now we proceed along the lines of the proof of [HaRi, Thm. 9.2, pp. 247–252]. Let p be a prime counted in $\mathcal{W}(\mathcal{A}, \mathcal{P}, v, u, \lambda)$ and whose weight

$$\mathrm{wt}(p) := 1 - \lambda \sum_{\substack{X^{1/v} \le l < X^{1/u} \\ l | \# E_p(\mathbb{F}_p)}} \Big(1 - u \frac{\log l}{\log X} \Big)$$

is positive. By the definition of $\mathcal{W}(\mathcal{A}, \mathcal{P}, v, u, \lambda)$, for such p we deduce that $\# E_p(\mathbb{F}_p)$ has no prime divisors $l < X^{1/v}$. However, $\# E_p(\mathbb{F}_p)$ may have prime

divisors $l \geq X^{1/u}$. It is easy to see that

$$\mathrm{wt}(p) \leq 1 - \lambda\nu(\#E_p(\mathbb{F}_p)) + \frac{\lambda u}{\log X} \sum_{l \mid \#E_p(\mathbb{F}_p)} \log l.$$

By using Hasse's bound, we see that the quantity on the right is

$$\leq 1 - \lambda\nu(\#E_p(\mathbb{F}_p)) + \frac{\lambda u(2\log 2 + \log x)}{\log x}.$$

Since $\mathrm{wt}(p)$ is positive, we must have

$$\nu(\#E_p(\mathbb{F}_p)) \leq \frac{1}{\lambda} + u.$$

Now we choose u, v, λ such that (8) is satisfied, the integral part $[1/\lambda + u]$ is minimal, and $f(\alpha, v, u, \lambda) > 0$ (note that there is no unique choice of these parameters). For example choose

$$u := 4.1, \quad \lambda := 0.53, \quad v := 16. \tag{11}$$

We deduce that the primes p of positive weight $\mathrm{wt}(p)$ which are counted in $\mathcal{W}(\mathcal{A}, \mathcal{P}, v, u, \lambda)$ satisfy the constraint $\nu(\#E_p(\mathbb{F}_p)) \leq 5$. Since $\mathrm{wt}(p) \leq 1$, we conclude from (9) and (10) that, as $x \to \infty$,

$$\#\{p \leq x : p \nmid N, a_p \neq 0, \nu(\#E_p(\mathbb{F}_p)) \leq 5\}$$
$$\gg_E \prod_{\substack{l \text{ prime} \\ \chi(l)=0}} \left(1 - \frac{1}{(l-1)^2}\right) \cdot \prod_{\substack{l \text{ prime} \\ \chi(l)\neq 0}} \left(1 - \chi(l)\,\frac{l^2 - l - 1}{(l - \chi(l))(l-1)^2}\right) \frac{x}{(\log x)^2}.$$

3.3. *A refined argument.* In what follows we refine the above argument to obtain infinitely many ordinary primes p such that $\Omega(\#E_p(\mathbb{F}_p)) \leq 5$, where for a natural number n we denote by $\Omega(n)$ the number of all prime factors of n (counted with multiplicities). We need to show that the number of ordinary primes $p \leq x$ with $(\#E_p(\mathbb{F}_p), P(X^{1/v})) = 1$, having positive weight in $\mathcal{W}(\mathcal{A}, \mathcal{P}, v, u, \lambda)$ and for which there exists a prime $X^{1/v} \leq l < X^{1/u}$ such that $l^2 \mid \#E_p(\mathbb{F}_p)$, is small, i.e. is $o(x/(\log x)^2)$. Again we want to prove this unconditionally, and for this we rely on Lemma 14.

Let $\sum_p'$ be the sum over primes $p \leq x$, $p \nmid N$, $a_p \neq 0$, with

$$(\#E_p(\mathbb{F}_p), P(X^{1/v})) = 1$$

and for which there exists a prime $X^{1/v} \leq l < X^{1/u}$ such that $l^2 \mid \#E_p(\mathbb{F}_p)$.

By interchanging summations and using Lemma 14 with $n = 2$ we obtain:

$$(12)\quad \sum_p{}' \sum_{\substack{X^{1/v}\le l<X^{1/u}\\ l^2\mid \#E_p(\mathbb{F}_p)}} 1 \ll \sum_{X^{1/v}\le l<X^{1/u}} \sum_{\substack{p\neq l\\ l^2\mid \#E_p(\mathbb{F}_p)}}{}' 1 + \mathrm{O}\Big(\frac{x^{1/u}}{\log x}\Big)$$

$$\ll \sum_{X^{1/v}\le l<X^{1/u}} \#\{p\le x : p\nmid lN,\ a_p\neq 0,\ \pi_p\equiv 1 \pmod l\}$$

$$+ \sum_{\substack{X^{1/v}\le l<X^{1/u}\\ (l)=L\overline{L},\ L\neq\overline{L}}} \#\{p\le x : p\nmid lN,\ a_p\neq 0,\ \pi_p\equiv 1 \pmod{L^2}\}$$

$$+ \sum_{\substack{X^{1/v}\le l<X^{1/u}\\ (l)=L\overline{L},\ L\neq\overline{L}}} \#\{p\le x : p\nmid lN,\ a_p\neq 0,\ \pi_p\equiv 1 \pmod{\overline{L}^2}\} + \mathrm{O}\Big(\frac{x^{1/u}}{\log x}\Big).$$

Proposition 18 of Schaal and elementary estimates can be invoked now to estimate the number of ordinary primes p having π_p congruent to $1 \pmod l$, $1 \pmod{L^2}$ and $1 \pmod{\overline{L}^2}$. Since $N_{K/\mathbb{Q}}(l) = N_{K/\mathbb{Q}}(L^2) = N_{K/\mathbb{Q}}(\overline{L}^2) = l^2 \le X^{2/u}$, we deduce that (12) is

$$\ll_K \frac{x}{\log x} \sum_{X^{1/v}\le l<X^{1/u}} \frac{1}{l^2} + \mathrm{O}\Big(\frac{x^{1/u}}{\log x}\Big) \ll_K \frac{x^{1-1/v}}{(\log x)^2} + \frac{x^{1/u}}{\log x} = \mathrm{o}\left(\frac{x}{(\log x)^2}\right),$$

where we have also made use of our choice of u and v. Thus the primes p in question do not contribute to our final lower bound for $\mathcal{W}(\mathcal{A},\mathcal{P},v,u,\lambda)$. This shows that

$$\#\{p\le x : p\nmid N,\ a_p\neq 0,\ \Omega(\#E_p(\mathbb{F}_p))\le 5\}$$
$$\gg_E \prod_{\substack{l \text{ prime}\\ \chi(l)=0}} \Big(1-\frac{1}{(l-1)^2}\Big)\cdot \prod_{\substack{l \text{ prime}\\ \chi(l)\neq 0}} \Big(1-\chi(l)\,\frac{l^2-l-1}{(l-\chi(l))(l-1)^2}\Big)\frac{x}{(\log x)^2},$$

which completes the proof of Theorem 4.

4. Proof of Theorem 5. In this section we prove Theorem 5 by using Turán's normal order method. These investigations actually go back to a general formalism of the normal order method due to K. Murty and R. Murty [MuMu1]. We keep the convention that p and l denote rational primes. We proceed along classical lines and show that

$$\sum_{p\le x} (\nu(p+1-a_p) - \log\log x)^2 = \mathrm{O}\Big(\frac{x\log\log x}{\log x}\Big),$$

under a quasi-GRH if E is non-CM. A standard argument can be used to show that the above implies

$$\sum_{\substack{p\le x\\ p\nmid N\\ a_p\neq 0}} (\nu(p+1-a_p)-\log\log p)^2 = \mathrm{O}\bigg(\frac{x\log\log x}{\log x}\bigg),$$

which is exactly what is claimed in the statement of Theorem 5.

We recall that a classical theorem of Erdős [Er] asserts that

$$\sum_{p\le x}(\nu(p+1)-\log\log p)^2 = \mathrm{O}\bigg(\frac{x\log\log x}{\log x}\bigg). \tag{13}$$

Therefore, in view of Deuring's formula for the number of supersingular primes of a CM elliptic curve E, for such E it remains to treat only ordinary primes p.

The classical starting observation is that for positive integers $n\le x$ and for $y=x^\delta$ with $0<\delta<1/2$ we have

$$\nu(n)=\nu_y(n)+\mathrm{O}(1),$$

where $\nu_y(n)$ denotes the number of distinct prime divisors of n which are $\le y$. Therefore

$$\begin{aligned}
\sum_{\substack{p\le x\\ p\nmid N}}{}'\nu(p+1-a_p) &= \sum_{\substack{p\le x\\ p\nmid N}}{}'\nu_y(p+1-a_p)+\mathrm{O}\bigg(\frac{x}{\log x}\bigg),\\
\sum_{\substack{p\le x\\ p\nmid N}}{}'\nu^2(p+1-a_p) &= \sum_{\substack{p\le x\\ p\nmid N}}{}'\nu_y^2(p+1-a_p)\\
&\quad+\sum_{\substack{p\le x\\ p\nmid N}}{}'\mathrm{O}(\nu_y(p+1-a_p))+\mathrm{O}\bigg(\frac{x}{\log x}\bigg),
\end{aligned}$$

where $\sum'$ means that we run over all primes $p\nmid N$ if E is non-CM, and only over primes $p\nmid N$ with $a_p\neq 0$ if E has CM.

By interchanging summations and by using the notation introduced in Section 2, we obtain

$$\begin{aligned}
\sum_{\substack{p\le x\\ p\nmid N}}{}'\nu_y(p+1-a_p) &= \operatorname{li} x\sum_{l\le y}\delta'(l)+\sum_{l\le y}R'_l+\mathrm{O}\bigg(\frac{y}{\log y}\bigg),\\
\sum_{\substack{p\le x\\ p\nmid N}}{}'\nu_y^2(p+1-a_p) &= \operatorname{li} x\sum_{\substack{l_1,l_2\le y\\ l_1\neq l_2}}\delta'(l_1l_2)+\sum_{\substack{l_1,l_2\le y\\ l_1\neq l_2}}R'_{l_1l_2}+\sum_{\substack{p\le x\\ p\nmid N}}{}'\nu_y(p+1-a_p),
\end{aligned}$$

where, for an integer d, $\delta'(d) = \delta(d)$ and $R'_d = R_d$ if E is non-CM, and $\delta'(d) = \delta^{\mathrm{o}}(d)$ and $R'_d = R^{\mathrm{o}}_d$ if E has CM.

First let us consider the case of an elliptic curve E without CM. In this case we assume that there exists some $1/2 \le \theta < 1$ such that the Dedekind zeta functions of the division fields of E satisfy a θ-quasi-GRH. We choose

$$y := \frac{x^{(1-\theta)/8}}{(\log x)^{1/4}}$$

and then the sums $\sum_{l_1 \ne l_2 < y} R_{l_1 l_2}$ can be estimated under the θ-quasi-GRH by using Remark 12. More precisely,

$$\sum_{l \le y} R_l = \sum_{l \le y} \mathrm{O}(l^3 x^\theta \log(lNx)) = \mathrm{O}(y^4 x^\theta \log(Nx)) = \mathrm{O}_N\left(\frac{x}{\log x}\right),$$

and similarly,

$$\begin{aligned}\sum_{\substack{l_1, l_2 \le y \\ l_1 \ne l_2}} R_{l_1 l_2} &= \sum_{\substack{l_1, l_2 \le y \\ l_1 \ne l_2}} \mathrm{O}(l_1^3 l_2^3 x^\theta \log(l_1 l_2 Nx)) \\ &= \mathrm{O}(y^8 x^\theta \log(Nx)) = \mathrm{O}_N\left(\frac{x}{\log x}\right).\end{aligned}$$

For the sums $\sum_{l \le y} \delta(l)$ and $\sum_{l_1 \ne l_2 \le y} \delta(l_1 l_2)$ we use the formulae given in Proposition 10. Also, we recall that for sufficiently large l_1, l_2, the density $\delta(l_1 l_2)$ is multiplicative. We obtain

$$\begin{aligned}\sum_{\substack{p \le x \\ p \nmid N}} \nu_y(p + 1 - a_p) &= (\mathrm{li}\, x)(\log\log y) + \mathrm{O}_N\left(\frac{x}{\log x}\right) \\ &= (\mathrm{li}\, x)(\log\log x) + \mathrm{O}_N\left(\frac{x}{\log x}\right); \\ \sum_{\substack{p \le x \\ p \nmid N}} \nu_y^2(p + 1 - a_p) &= (\mathrm{li}\, x)(\log\log y)^2 + (\mathrm{li}\, x)(\log\log x) + \mathrm{O}\left(\frac{x}{\log x}\right) \\ &= (\mathrm{li}\, x)(\log\log x)^2 + \mathrm{O}_N\left(\frac{x \log\log x}{\log x}\right).\end{aligned}$$

By putting these estimates together we deduce that

$$\sum_{\substack{p \le x \\ p \nmid N}} (\nu(p + 1 - a_p) - \log\log x)^2 = \mathrm{O}_N\left(\frac{x \log\log x}{\log x}\right).$$

Now let us assume that we are in the case of an elliptic curve with CM by the full ring of integers of an imaginary quadratic field K. This time we assume no unproven hypotheses. Let $A > 0$ and let $B = B(A)$ be as given

by Proposition 17. We choose

$$y := \frac{x^{1/4}}{(\log x)^B}$$

so that the sums $\sum_{l\le y} R_l^{\mathrm{o}}$ and $\sum_{l_1\ne l_2<y} R_{l_1l_2}^{\mathrm{o}}$ can be estimated unconditionally. For the sums $\sum_{l\le y}\delta^{\mathrm{o}}(l)$ and $\sum_{l_1\ne l_2\le y}\delta^{\mathrm{o}}(l_1l_2)$ we use the formulae given in Proposition 10, also recalling the multiplicativity property of $\delta^{\mathrm{o}}(\cdot)$. More precisely, by splitting the sums according to whether l, l_1, and l_2 are inert, split completely or ramify in K, and by invoking elementary estimates such as Mertens' Theorem, we obtain

$$\begin{aligned}\sum_{\substack{p\le x\\ p\nmid N\\ a_p\ne 0}} \nu_y(p+1-a_p) &= \frac{\operatorname{li} x}{2}\sum_{\substack{l\le y\\ l \text{ inert in } K}}\frac{1}{l^2-1}+\frac{\operatorname{li} x}{2}\sum_{\substack{l\le y\\ l \text{ splits in } K}}\frac{2l-3}{(l-1)^2}\\ &\quad+\mathrm{O}_{A,K}\left(\frac{x}{(\log x)^A}\right)\\ &= \frac{(\operatorname{li} x)(\log\log x)}{2}+\mathrm{O}_{K,N}\left(\frac{x}{\log x}\right).\end{aligned}$$

Similarly, and also relying on the above estimate, we obtain

$$\begin{aligned}\sum_{\substack{p\le x\\ p\nmid N\\ a_p\ne 0}} \nu_y^2(p+1-a_p) &= \operatorname{li} x\sum_{\substack{l_1,l_2\le y\\ l_1\ne l_2}}\delta^{\mathrm{o}}(l_1l_2)+\frac{(\operatorname{li} x)(\log\log x)}{2}+\mathrm{O}_{K,N}\left(\frac{x}{\log x}\right)\\ &= \frac{(\operatorname{li} x)(\log\log x)^2}{2}+\mathrm{O}_{K,N}\left(\frac{x\log\log x}{\log x}\right).\end{aligned}$$

We put everything together and deduce that

$$\sum_{\substack{p\le x\\ p\nmid N\\ a_p\ne 0}} (\nu(p+1-a_p)-\log\log x)^2 = \mathrm{O}_{K,N}\left(\frac{x\log\log x}{\log x}\right).$$

The dependence of the $\mathrm{O}_{K,N}$-constant on K can be absorbed into a constant depending only on N, since there are only nine possibilities for the fields K (recall that K is an imaginary quadratic field of class number 1).

From here and (13) it is an easy exercise to deduce Corollary 6.

5. Proof of Proposition 7. Let l denote rational primes and n positive integers. We consider the sieve problems $(\mathcal{A},\mathcal{P},\mathcal{A}_{l^n})$ if E is non-CM, and $(\mathcal{A}^{\mathrm{o}},\mathcal{P},\mathcal{A}_{l^n}^{\mathrm{o}})$ if E has CM, and apply Selberg's sieve (see [CoMu, Thm. 7.2.1 and Lemma 7.2.3]). Let $\widetilde{\delta}(\cdot)$ be the completely multiplicative function defined by $\widetilde{\delta}(l)=\delta(l)$ for all $l\in\mathcal{P}$. Let $z=z(x)$ be a parameter to be chosen

in each case. We observe that

$$\#\{p \le x : p \nmid N,\ \#E_p(\mathbb{F}_p) \text{ a prime}\} \le z + S(\mathcal{A}, \mathcal{P}, z),$$
$$\#\{p \le x : p \nmid N,\ a_p \ne 0,\ \#E_p(\mathbb{F}_p) \text{ a prime}\} \le z + S(\mathcal{A}^{\mathrm{o}}, \mathcal{P}, z),$$

where $S(\mathcal{A}, \mathcal{P}, z) = \#(\mathcal{A} \setminus \bigcup_{l|P(z)} \mathcal{A}_l)$ and $S(\mathcal{A}^{\mathrm{o}}, \mathcal{P}, z) = \#(\mathcal{A}^{\mathrm{o}} \setminus \bigcup_{l|P(z)} \mathcal{A}_l^{\mathrm{o}})$.

First let us consider the case when E is without CM. We assume that for some $1/2 \le \theta < 1$, the Dedekind zeta functions of the division fields of E satisfy the θ-quasi-GRH. Then, by using part (i) of Remark 12 in Selberg's sieve we obtain

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, z) &\le \frac{X}{\sum\limits_{\substack{d \le z \\ d|P(z)}} \widetilde{\delta}(d)} + \mathrm{O}\Big(\sum_{\substack{d_1, d_2 \le z \\ d_1, d_2 | P(z)}} |R_{[d_1,d_2]}| \Big) \\ &\ll \frac{x}{(\log z)(\log x)} + z^8 x^{\theta} \log(Nx). \end{aligned}$$

We choose

$$z := \frac{x^{(1-\theta)/8}}{(\log x)^{3/8}}$$

and derive the desired upper bound

$$\#\{p \le x : p \nmid N,\ \#E_p(\mathbb{F}_p) \text{ a prime}\} \ll_N \frac{x}{(\log x)^2}.$$

To obtain an unconditional result, we rely on part (i) of Remark 13 to deduce

$$S(\mathcal{A}, \mathcal{P}, z) \ll \frac{x}{(\log z)(\log x)} + z^8 \frac{x}{(\log x)^A}$$

for any $A > 0$, and with $z := c \log\log x$ for a suitable absolute constant c. This implies that

$$\#\{p \le x : p \nmid N,\ \#E_p(\mathbb{F}_p) \text{ a prime}\} \ll \frac{x}{(\log x)(\log\log\log x)}.$$

Now let us assume that E has CM by the full ring of integers of an imaginary quadratic field K. Let $B = B(2)$ be given by Proposition 17, and choose

$$z := \frac{x^{1/8}}{(\log x)^{B/2}}.$$

By using Proposition 17 to estimate the sums $\sum_{d_1,d_2 \le z} |R^{\mathrm{o}}_{[d_1,d_2]}|$ we obtain

$$S(\mathcal{A}^{\mathrm{o}}, \mathcal{P}, z) \ll \frac{x}{(\log z)(\log x)} + \frac{x}{(\log x)^2} \ll \frac{x}{(\log x)^2},$$

which leads to the desired upper bound

$$\#\{p \le x : p \nmid N,\ a_p \ne 0,\ \#E_p(\mathbb{F}_p) \text{ a prime}\} \ll \frac{x}{(\log x)^2}.$$

Corollary 8 is obtained by the partial summation technique combined with the above upper bounds.

6. Concluding remarks. By assuming, in addition to GRH, a Pair Correlation Conjecture (PCC) on the zeroes of Artin L-functions, we could actually prove that in the non-CM case we have

$$\#\{p \le x : p \nmid N,\ \#E_p(\mathbb{F}_p) \text{ has at most 3 prime factors}\} \ge C(E)\,\frac{x}{(\log x)^2}. \tag{14}$$

This is a consequence of the improved effective versions of the Chebotarev Density Theorem due to K. Murty and R. Murty [MuMu2]. Namely, under GRH and PCC one would obtain, in the non-CM case,

$$R_d = \mathrm{O}_N(d^{1/2}x^{1/2}\log(dx)).$$

Then, using this estimate in the Richert's sieve, one gets (14). In the CM case the assumption of PCC does not seem to lead to any further improvements, because of the "almost abelian" nature of the division fields involved.

Acknowledgements. I wish to thank Kumar Murty and Ram Murty for their careful reading of preliminary versions of this paper, and for helpful suggestions.

References

[Bo] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, 1st ed., Astérisque 18 (1974).

[Ch] J. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica 16 (1973), 157–176.

[Co1] A. C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curves*, in: Number Theory, CRM Proc. Lecture Notes 36, Amer. Math. Soc., Providence, RI, 2004, 61–79.

[Co2] —, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, with an appendix by E. Kani, Canad. Math. Bull. 48 (2005), 16–31.

[CoMu] A. C. Cojocaru and M. R. Murty, *An Introduction to Sieve Methods and Their Applications*, to be published by Cambridge Univ. Press.

[De] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941), 197–272.

[El] N. D. Elkies, *Supersingular primes of a given elliptic curve over a number field*, PhD thesis, Harvard Univ., Cambridge, MA, 1987.

[Er] P. Erdős, *On the normal number of prime factors of $p-1$ and some related questions concerning Euler's ϕ function*, Quart. J. Math. Oxford Ser. 6 (1935), 205–213.

[GuMu] R. Gupta and M. R. Murty, *Primitive points on elliptic curves*, Compositio Math. 58 (1986), 13–44.

[HaRi] H. Halberstam and H. E. Richert, *Sieve Methods*, Academic Press, London, 1974.

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

[Ko] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. 131 (1988), 157–165.

[LaOd] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in: Algebraic Number Fields, A. Fröhlich (ed.), Academic Press, New York, 1977, 409–464.

[La] M. Lane, *Elliptic curve analogues of the twin prime conjecture*, senior thesis, Princeton Univ., Princeton, NJ, 2005.

[LaTr] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. 83 (1977), 289–292.

[MiMu] S. A. Miri and V. K. Murty, *An application of sieve methods to elliptic curves*, in: Progress in Cryptology—Indocrypt 2001 (Chennai), Lecture Notes in Comput. Sci. 2247, Springer, Berlin, 2001, 91–98.

[MuMu1] M. R. Murty and V. K. Murty, *Prime divisors of Fourier coefficients of modular forms*, Duke Math. J. 51 (1984), 57–76.

[MuMu2] —, —, *The Chebotarev density theorem and pair correlation of zeroes of Artin L-functions*, to appear.

[MuMuSa] M. R. Murty, V. K. Murty and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. 110 (1988), 253–281.

[Ri] H. E. Richert, *Selberg's sieve with weights*, Mathematika 16 (1969), 1–22.

[Ru] K. Rubin, *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. 1716, Springer, Berlin, 1999, 167–234.

[Sc] W. Schaal, *On the large sieve method in algebraic number fields*, J. Number Theory 2 (1970), 249–270.

[Se1] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.

[Se2] —, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 123–201.

[StWe] J. Steuding and A. Weng, *On the number of prime divisors of the order of elliptic curves modulo p*, Acta Arith. 117 (2005), 341–352.

Department of Mathematics
Princeton University
810 Fine Hall
Washington Road
Princeton, NJ, 08544-1000, U.S.A.
E-mail: cojocaru@math.princeton.edu

Received on 13.8.2004
and in revised form on 13.4.2005 (4824)