Reduction mod p of Subgroups of the Mordell-Weil Group of an Elliptic Curve

Amir Akbary and V. Kumar Murty*

Abstract

Let E be an elliptic curve defined over $\mathbb{Q}$. Let Γ be a free subgroup of rank r of $E(\mathbb{Q})$. For any prime p of good reduction, let Γ_p be the reduction of Γ modulo p and E_p be the reduction of E modulo p. We prove that if E has CM then for all but $o(x/\log x)$ of primes $p \leq x$,

$$|\Gamma_p| \geq p^{\frac{r}{r+2}+\epsilon(p)},$$

where $\epsilon(p)$ is any function of p such that $\epsilon(p) \to 0$ as $p \to \infty$. This is a consequence of two other results. Denote by N_p the cardinality of $E_p(\mathbb{F}_p)$, where $\mathbb{F}_p$ is a finite field of p elements. Then for any $\delta > 0$, the set of primes p for which N_p has a divisor in the range $(p^{\delta-\epsilon(p)}, p^{\delta+\epsilon(p)})$ has density zero. Moreover, the set of primes p for which $|\Gamma_p| < p^{\frac{r}{r+2}-\epsilon(p)}$ has density zero.

Keywords: Reduction mod p of elliptic curves, Elliptic curves over finite fields, Brun-Titchmarsh inequality, Large sieve in number fields.

2000 *Mathematics Subject Classification.* Primary 11G20, Secondary 11N36.

1 Introduction

Artin's primitive root conjecture asserts that if $a \in \mathbb{Z}$ and $a \neq \pm 1$ or a square, then the set of primes p for which $a \pmod p$ is a primitive root has positive density.

*Research of both authors is partially supported by NSERC.

More generally, we may consider an algebraic group G defined over $\mathbb{Q}$ and Γ a finitely generated subgroup of $G(\mathbb{Q})$. For all but a finite number of primes p, there is a natural reduction map

$$\Gamma \to \bar{G}(\mathbb{F}_p) \tag{1}$$

where $\bar{G}$ denote the reduction of G mod p, and we may ask for the distribution of primes p for which this map is surjective. Thus, in the classical Artin primitive root conjecture, $G = \mathbb{G}_m$ and Γ is the subgroup generated by a.

Lang and Trotter [LT] considered the case where G is an elliptic curve E and Γ is a free subgroup of the group of rational points $E(\mathbb{Q})$. Significant results on this question were obtained by Gupta and R. Murty [GM]. In particular, they showed assuming the Generalized Riemann Hypothesis that if the rank of Γ is sufficiently large, then the set of primes for which (1) is surjective has a density.

It is also of interest to consider lower bounds on the size of the image in (1). Let Γ be a subgroup of $\mathbb{Q}^*$ generated by r non-zero multiplicatively independent rationals $a_1, \cdots, a_r$. For all primes p not dividing the numerators and the denominators of $a_1, \cdots, a_r$, we let Γ_p be the reduction of Γ mod p. Erdös and R. Murty [EM] proved the following theorem regarding the size of Γ_p as p varies.

Theorem 1.1 (**Erdös and R. Murty**) *Let $\epsilon(x)$ be any function tending to zero as $x \to \infty$. Then for all but $o(x/\log x)$ primes $p \leq x$,*

$$|\Gamma_p| \geq p^{\frac{r}{r+1}+\epsilon(p)}.$$

In this paper we prove an elliptic analogue of this result. More precisely, Let E be an elliptic curve defined over $\mathbb{Q}$. For any prime p of good reduction, let E_p be the elliptic curve over $\mathbb{F}_p$ obtained by reducing E modulo p. By the Mordell theorem we know that $E(\mathbb{Q})$ is finitely generated. Let Γ be a free subgroup of rank r of $E(\mathbb{Q})$ and let Γ_p be the reduction of Γ mod p. One can ask how the size of Γ_p grows as $p \to \infty$. For arbitrary r one can prove the following result which is implicit in the work of Matthews [M] and Gupta and R. Murty [GM].

Proposition 1.2 *Let E be an elliptic curve over $\mathbb{Q}$ and Γ be a free subgroup of rank r of $E(\mathbb{Q})$. Let $\epsilon(p)$ be a function of p such that increases monotonically to ∞ as $p \to \infty$. Then for all but $o(x/\log x)$ of primes $p \leq x$, we have*

$$|\Gamma_p| \geq p^{\frac{r}{r+2}-\epsilon(p)}.$$

In this paper we improve the above bound for the case that E is a CM elliptic curve. From now on let E have CM by the entire ring of integers of an imaginary quadratic field K, and for a prime of good reduction let $N_p = \#E_p(\mathbb{F}_p)$.

Theorem 1.3 *Let E be a CM elliptic curve. Let Γ be a free subgroup of rank r of $E(\mathbb{Q})$. Let Γ_p be the reduction of Γ mod p. Let $\epsilon(p)$ be a function of p such that $\epsilon(p) \to 0$ as $p \to \infty$. Then for all but $o(x/\log x)$ of primes $p \leq x$, we have*

$$|\Gamma_p| \geq p^{\frac{r}{r+2}+\epsilon(p)}.$$

Next let

$$\mathcal{P}_\Gamma(\theta) = \{\text{primes } p \text{ such that } |\Gamma_p| \leq p^\theta\}.$$

R. Murty, Rosen and Silverman proved that

$$\tilde{\delta}(\mathcal{P}_\Gamma(\theta)) \leq \left(1 + \frac{2}{r}\right)\theta,$$

where $\tilde{\delta}(\ )$ denotes the upper logarithmic Dirichlet density of a set. We observe that this result is non-trivial only if $\theta \leq \frac{r}{r+2}$. The following is a direct consequence of Theorem 1.3.

Corollary 1.4 *Let $\theta \leq \frac{r}{r+2}$. Then under the assumptions of Theorem 1.3, $\mathcal{P}_\Gamma(\theta)$ has density zero and so $\tilde{\delta}(\mathcal{P}_\Gamma(\theta)) = 0$.*

To prove our results, several tools are necessary. Firstly, we need to establish a Brun-Titchmarsh type inequality for N_p and we do this in Section 2. Also, we need information about the normal order of the number of divisors of N_p which discuss in Section 3. Another important tool that we need is a version of the large sieve inequality for integers in an imaginary quadratic field. All of these tools are used to prove a key technical theorem (Theorem 4.1). This is stated in Section 4 along with a strategy to prove it. The proof itself is given in Sections 5, 6, and 7. Finally, in Sections 8 and 9 the proofs of Proposition 1.2 and Theorem 1.4 are given.

We make some remarks regarding the analogue of Theorem 1.3 for elliptic curves without complex multiplication. A key tool that we use is the Brun-Titchmarsh inequality for N_p. In the non-CM case, this has not yet been proved. Moreover, even assuming the Generalized Riemann Hypothesis, the error term in the Chebotarev density theorem grows too rapidly for an argument to work. Thus, at present, without additional hypothesis, we are not able to prove the analogue of Theorem 1.3 in the non complex multiplication case. However this difficulty can be overcome if we assume that Γ has sufficiently large rank.

2 Brun-Titchmarsh inequality for N_p

From now on p denote a rational prime and l denote an integer that may or may not be prime. Let $(a,l)=1$ and define

$$\pi(x;l,a)=\sum_{\substack{p\leq x\\ l|p-a}}1.$$

The classical Brun-Titchmarsh inequality in its sharpest known form (due to Montgomery and Vaughan [MV]) states that

$$\pi(x;l,a)\leq\frac{2x}{\phi(l)\log(x/l)}$$

for $1\leq l<x$. Here we are interested in an analogue of this inequality for divisors of N_p of an elliptic curve.

Let E be an elliptic curve defined over $\mathbb{Q}$ which has complex multiplication by the entire ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. We want to obtain an upper bound for

$$\pi_E(x;l)=\sum_{\substack{p\leq x\\ l|N_p}}{}'1.$$

In the above sum $'$ means that the sum is taken over primes p of good reduction and moreover $p\neq 2,3$.

To establish such a bound, we closely follow the arguments given in Lemma 14 of [C]. For simplicity, we first consider the case that l is prime, and then we study the general case.

prime l

We break the sum into the following sums.

$$\pi_E(x;l)=\sum_{\substack{p\leq x\\ l|N_p}}{}'1=\sum_{\substack{p\leq x,\mathrm{ss}\\ l|N_p}}{}'1+\sum_{\substack{p\leq x,\mathrm{ord}\\ l|N_p}}{}'1=(\mathrm{I})+(\mathrm{II}).$$

Here ss stands for supersingular and ord stands for ordinary. Now we estimate each of the above sums.

(I) In this case we have $N_p=p+1$ for $p\geq 5$, and so by the Brun-Titchmarsh inequality

$$\sum_{\substack{p\leq x,\mathrm{ss}\\ l|N_p}}{}'1\leq\pi(x;l,-1)\leq\frac{2x}{\phi(l)\log(x/l)}$$

for $l < x$.

(II) To study the other sum, we need the following lemma which is a simple corollary of Theorem 6 of [S].

Lemma 2.1 *Let $\mathfrak{l}$ be an integral ideal of an imaginary quadratic field K. For $x \geq 2$, let*

$$\pi_K(x; \mathfrak{l}, 1) = \#\{\omega \in \mathcal{O}_K;\ N(\omega) \leq x,\ (\omega) \text{ a prime ideal},\ \ \omega \equiv 1 \pmod{\mathfrak{l}}\}.$$

Then we have

$$\pi_K(x; \mathfrak{l}, 1) \ll_K \frac{x}{\phi(\mathfrak{l}) \log(x/N(\mathfrak{l}))}$$

as long as $N(\mathfrak{l}) \leq \frac{x}{\log x}$. Here $N(\omega) = \omega\bar{\omega}$, $\phi(\mathfrak{l}) = |(\mathcal{O}_K/\mathfrak{l})^*|$ is the number of invertible residue classes mod $\mathfrak{l}$, and $N(\mathfrak{l})$ is the norm of the ideal $\mathfrak{l}$ in the extension $K/\mathbb{Q}$. The implied constant in the inequality depends only on K.

From the theory of complex multiplication we know that for an ordinary prime p there is a unique choice of an element $\pi_p \in \mathcal{O}_K$ such that π_p represents the p-power Frobenius morphism, $p = \pi_p\bar{\pi}_p$, (π_p) is a prime ideal of $\mathcal{O}_K$, and $K = \mathbb{Q}(\pi_p)$. Moreover, in this case

$$N_p = (\pi_p - 1)(\bar{\pi}_p - 1)$$

and K has class number 1. (For more information regarding these facts see Chapter 5 and Appendix C of [Si].)

Now (l) can be an inert prime, a split prime or a ramified prime in K. We consider each of these cases in turn.

(II-in) Since (l) is inert, so (l) is a prime in $\mathcal{O}_K$, and so

$$l \mid N_p \iff \pi_p \equiv 1 \pmod{(l)}.$$

Now from here and Lemma 2.1 we have

$$\sum_{\substack{p \leq x, \text{ord} \\ l \mid N_p, \text{in}}}{}' 1 \leq \pi_K(x; (l), 1) \ll \frac{x}{(l^2 - 1)\log(x/l^2)},$$

for $l \leq \left(\frac{x}{\log x}\right)^{1/2}$.

(II-sp) In this case $(l) = \mathfrak{l}_1\mathfrak{l}_2$. So

$$l \mid N_p \iff \pi_p \equiv 1 \pmod{\mathfrak{l}_1} \ \text{ or } \ \pi_p \equiv 1 \pmod{\mathfrak{l}_2}.$$

So from here and Lemma 2.1 we have

$$\sum_{\substack{p\le x,\text{ord}\\ l|N_p,\text{sp}}}{}' 1 \le \pi_K(x;\mathfrak{l}_1,1)+\pi_K(x;\mathfrak{l}_2,1) \ll \frac{x}{\phi(l)\log(x/l)},$$

for $l \le \frac{x}{\log x}$.

(II-ram) In this case $(l)=\mathfrak{l}^2$. So

$$l \mid N_p \iff \pi_p \equiv 1 \pmod{\mathfrak{l}}.$$

So from here and Lemma 2.1 we have

$$\sum_{\substack{p\le x,\text{ord}\\ l|N_p,\text{ram}}}{}' 1 \le \pi_K(x;\mathfrak{l},1) \ll \frac{x}{\phi(l)\log(x/l)},$$

for $l \le \frac{x}{\log x}$.

Putting everything together, for l prime, we have

$$\pi_E(x;l) \ll_K \frac{x}{\phi(l)\log\left(x/l^2\right)},$$

for $l \le \left(\frac{x}{\log x}\right)^{1/2}$.

General l

Now we drop the restriction that l is prime. The analysis of the first sum (I) is the same, so we assume that p is ordinary. We first decompose l as $l = l_{\text{in}}\ l_{\text{sp}}\ l_{\text{ram}} = (\prod_i p_i^{\alpha_i})(\prod_j q_j^{\beta_j})(\prod_k r_k^{\gamma_k})$, where (p_i)'s are inert, (q_j)'s are split and (r_k)'s are ramified in K. We have

$$l|N_p \iff p_i^{\alpha_i}|N_p,\ q_j^{\beta_j}|N_p,\ r_k^{\gamma_k}|N_p, \text{ for all } i,\ j,\ k.$$

Now note that

$$p_i^{\alpha_i}|N_p \Rightarrow \pi_p \equiv 1 \pmod{(p_i)^{\delta_i}},$$

where

$$\delta_i = \begin{cases} \left[\frac{\alpha_i}{2}\right]+1 & \text{if} \quad \alpha_i \text{ is odd} \\ \frac{\alpha_i}{2} & \text{if} \quad \alpha_i \text{ is even} \end{cases}.$$

Next let η_j be the highest power of q_j in the factorization of N_p. Since K is a principal ideal domain, there is a unique integer α in $\mathcal{O}_K$ such that

$$e\frac{N_p}{q_j^{\eta_j-\beta_j}} = \alpha\bar{\alpha},$$

where $\alpha \mid \pi_p - 1$, $\bar{\alpha} \mid \bar{\pi}_p - 1$, and e is a unit of K. Since (q_i) splits we have $(q_j) = \mathfrak{q}_{j1}\mathfrak{q}_{j2}$. Let μ_{j1} be the highest power of $\mathfrak{q}_{j1}$ in the prime factorization of (α) and μ_{j2} the highest power of $\mathfrak{q}_{j2}$ in the prime factorization of (α). We have

$$q_j^{\beta_j} | N_p \Rightarrow \pi_p \equiv 1 \pmod{\mathfrak{q}_{j1}^{\mu_{j1}}\mathfrak{q}_{j2}^{\mu_{j2}}},$$

where

$$\mu_{j1} + \mu_{j2} = \beta_j.$$

Finally

$$r_k^{\gamma_k} | N_p \Rightarrow \pi_p \equiv 1 \pmod{\mathfrak{r}_k^{\gamma_k}},$$

where $(r_k) = \mathfrak{r}_k^2$. Let J denote the set of indices j. For each function

$$f : J \longrightarrow \mathbb{Z}$$

given by

$$f(j) \;=\; \mu_{j,1}$$

where $0 \leq \mu_{j,1} \leq \beta_j$, set

$$\mu_{j,2} \;=\; \beta_j \;-\; f(j)$$

and consider the ideal

$$\mathfrak{a}_f = \prod_i (p_i)^{\delta_i} \prod_j \mathfrak{q}_{j1}^{\mu_{j1}} \mathfrak{q}_{j2}^{\mu_{j2}} \prod_k \mathfrak{r}_k^{\gamma_k}.$$

Note that the number of such maps f is

$$\prod_j (\beta_j + 1) \;=\; d(l_{\mathrm{sp}}).$$

It is clear that

$$l | N_p \Rightarrow \pi_p \equiv 1 \pmod{\mathfrak{a}_f},$$

for some $\mathfrak{a}_f$. From here and Lemma 2.1, we have

$$\begin{aligned} \sum_{\substack{p \leq x, \mathrm{ord} \\ l | N_p}}{}' 1 \quad &\leq \quad \sum_f \pi_K(x; \mathfrak{a}_f, 1) \\ &\ll_K \quad \frac{\prod_j \displaystyle\sum_{\mu_{j1}+\mu_{j2}=\beta_j} \frac{1}{\phi(q_j^{\mu_{j1}})\phi(q_j^{\mu_{j2}})}}{\prod_i (p_i^{2\delta_i} - p_i^{2\delta_i - 2}) \prod_k \phi(r_k^{\gamma_k})} \frac{x}{\log\left(\frac{x}{\prod_i p_i^{2\delta_i} l_{\mathrm{sp}} l_{\mathrm{ram}}}\right)}, \end{aligned}$$

for $\prod_i p_i^{2\delta_i} l_{\mathrm{sp}} l_{\mathrm{ram}} \leq \frac{x}{\log x}$. So we have the following proposition.

Proposition 2.2 *Let E be an elliptic curve over $\mathbb{Q}$ which has complex multiplication by the ring of integers of an imaginary quadratic number field K. Let $l = l_{\text{in}} l_{\text{sp}} l_{\text{ram}}$. Then*

$$\pi_E(x; l) \ll_K \frac{2^{\omega(l_{\text{sp}})} d(l_{\text{sp}})}{\phi(l)} \frac{x}{\log(x/l^2)},$$

for $l \leq \left(\frac{x}{\log x}\right)^{1/2}$. Here, $\omega(l_{\text{sp}})$ is the number of distinct prime divisors of l_{sp}, $d(l_{\text{sp}})$ is the number of divisors of l_{sp}, and $\phi(l)$ is the Euler function.

Proposition 2.3 *Under the conditions of the Proposition 2.2 we have*

$$\pi_E(x; l) \ll_K \frac{d(l_{\text{sp}})}{l} x,$$

where the implied constant depends only on K.

Proof Following the arguments before Proposition 2.2, we have

$$\pi_E(x; l) \leq \pi(x; l, -1) + \sum_f \pi(x; \mathfrak{a}_f, 1).$$

Note that since K is an imaginary quadratic field of class number 1, we have

$$\begin{aligned} \pi_K(x; \mathfrak{a}, 1) &\leq \#\{\omega \in \mathcal{O}_K;\ N(\omega) \leq x,\ \ \omega \equiv 1 \pmod{\mathfrak{a}}\} \\ &\leq \#\{\gamma \in \mathcal{O}_K;\ N(\gamma) \ll \frac{x}{N(\mathfrak{a})}\} \\ &\ll_K \frac{x}{N(\mathfrak{a})}. \end{aligned}$$

Therefore

$$\begin{aligned} \pi_E(x; l) &\ll_K \frac{x}{l} + \frac{d(l_{\text{sp}}) x}{\prod_i p_i^{2\delta_i} l_{\text{sp}} l_{\text{ram}}} \\ &\ll_K \frac{d(l_{\text{sp}})}{l} x. \end{aligned}$$

3 Normal order of $\omega(N_p)$

In [C] and [L], Cojocaru and Liu independently proved that for a CM elliptic curve over $\mathbb{Q}$, the normal order of $\omega(N_p)$ is $\log\log p$, where $\omega(n)$ denotes the number of distinct prime divisors of n. This means that given $\epsilon > 0$,

$$\#\{p \leq x, |\omega(N_p) - \log\log p| > \epsilon \log\log p\} = o(\pi(x)),$$

where $\pi(x)$ denotes the number of primes not exceeding x. Cojocaru and Liu's result is a consequence of the following theorem.

Theorem 3.1 (**Cojocaru and Liu**) *For $y < x^{\frac{1}{6}}$, we have*

$$\sum_{\substack{l \le y \\ l \text{ prime}}} \pi_E(x; l) = \pi(x) \log\log y + O(\pi(x)),$$

and for $y < x^{\frac{1}{12}}$ we have

$$\sum_{\substack{l_1, l_2 \le y \\ l_1 \ne l_2 \text{ prime}}} \pi_E(x; l_1 l_2) = \pi(x)(\log\log y)^2 + O(\pi(x) \log\log y).$$

Proof See the proof of Theorem 1 in [L] or the proof of Theorem 5 in [C]. □

To explain our next statement we need to introduce some notations. Let $\epsilon(x)$ be a function such $\epsilon(x) \to 0$ as $x \to \infty$. For simplicity we write $\epsilon(x)$ as ϵ. We call a number a C if it is only composed of primes in the interval $(x^{\epsilon}, x^{\delta}]$, where $0 < \delta < 1$ is a fixed number. We denote by $C(N_p)$ the largest C that divides N_p. We claim that the normal order of $C(N_p)$ is $\xi(p)$, where $\xi = \log(1/\epsilon)$. More precisely we have

Proposition 3.2 $\sum_{p \le x}{}' (\omega(C(N_p)) - \xi)^2 = O(\pi(x)\xi)$. *Here $'$ means that the sum is taken over primes of good reduction.*

Proof We have

$$\begin{aligned} & \sum_{p \le x}{}' (\omega(C(N_p)) - \xi)^2 \\ = & \sum_{p \le x}{}' \omega^2(C(N_p)) - 2\xi \sum_{p \le x}{}' \omega(C(N_p)) + \pi(x)\xi^2. \end{aligned} \tag{2}$$

If $\delta < \frac{1}{6}$, we get from Theorem 3.1 that

$$\begin{aligned} \sum_{p \le x}{}' \omega(C(N_p)) &= \sum_{p \le x}{}' \sum_{\substack{l \mid N_p \\ x^{\epsilon} < l \le x^{\delta}}} 1 \\ &= \sum_{x^{\epsilon} < l \le x^{\delta}} \pi_E(x; l) \\ &= \pi(x)\xi + O(\pi(x)). \end{aligned} \tag{3}$$

If $\delta \geq \frac{1}{6}$, the same result is again true, since

$$\sum_{p\leq x}{}' \sum_{\substack{l|N_p \\ x^\epsilon < l \leq x^\delta}} 1 = \sum_{p\leq x}{}' \sum_{\substack{l|N_p \\ x^\epsilon < l \leq x^{\frac{1}{7}}}} 1 + O(\pi(x)).$$

Another application of Theorem 3.1 yields

$$\sum_{p\leq x}{}' \omega^2(C(N_p)) = \pi(x)\xi^2 + O(\pi(x)\xi). \tag{4}$$

Now applying (3) and (4) in (2) imply the result. □

The following is a direct corollary of the previous theorem.

Corollary 3.3 $\#\{p \leq x;\ \omega(C(N_p)) > \frac{4}{3}\xi\} \ll \frac{\pi(x)}{\xi}$.

Remark. We remark that arguments similar to the above were used in [MM].

4 The Key Technical Theorem

Our improvement upon Proposition 1.2 is a corollary of the following theorem regarding the divisors of N_p in a short interval.

Theorem 4.1 *Let E be a CM elliptic curve. Let $0 < \delta < 1$ and let $\epsilon_1(x)$ and $\epsilon_2(x)$ be such that*

$$\lim_{x\to\infty} \epsilon_1(x) = \lim_{x\to\infty} \epsilon_2(x) = 0.$$

Let

$$H(x, x^{\delta-\epsilon_1(x)}, x^{\delta+\epsilon_2(x)}) = \#\{p \leq x;\ \ \exists u \mid N_p \ \text{ such that } x^{\delta-\epsilon_1(x)} < u < x^{\delta+\epsilon_2(x)}\}.$$

Then we have

$$H(x, x^{\delta-\epsilon_1(x)}, x^{\delta+\epsilon_2(x)}) = o\left(\frac{x}{\log x}\right)$$

as $x \to \infty$.

Remark. Note that this is false for $\delta = 0$. For example, if $t = |E(\mathbb{Q})_{\text{tors}}| > 1$ then N_p has a divisor that is $O(1)$, namely t itself.

We will prove Theorem 4.1 in the case $\epsilon_1(x) = \epsilon(x)$ and $\epsilon_2(x) = 0$. The proof for the remaining case $\epsilon_1(x) = 0$ and $\epsilon_2(x) = \epsilon(x)$ is exactly similar. For simplicity we write $\epsilon(x)$ as ϵ. Also without loss of generality we assume that $x^\epsilon \to \infty$, since otherwise we can replace ϵ with a bigger function ϵ' such that $\epsilon' \to 0$ and $x^{\epsilon'} \to \infty$ as $x \to \infty$. Then the theorem for ϵ follows from the theorem for ϵ'.

The strategy of our proof is inspired by a proof of a theorem of Erdös [E], regarding the set of multiples of a special sequence, given in [HR], Chapter V, Theorem 16. To prove the theorem we need to introduce some notations. Let

$$\xi = \log\left(\frac{1}{\epsilon}\right), \quad I = [1, x^\epsilon], \quad \text{and} \quad J = (x^\epsilon, x^\delta].$$

We use the letter A for an integer that is entirely composed of primes in I and denote the greatest A that divides N_p by $A(N_p)$.

Recall that the letter C represents an integer that is entirely composed of primes in the interval J and the greatest C that divides N_p is denoted by $C(N_p)$.

We denote by B those square-free C's that are in the interval $(x^{\delta-(\epsilon+\epsilon\xi)}, x^\delta]$.

Finally we call a square-free C a C^* if it satisfies the following two conditions:

(i) $\omega(C^*) \le \frac{4}{3}\xi$.

(ii) C^* has a representation in the form $C^* = BC$.

The proof of Theorem 4.1 proceeds as follows.

Let

$$\mathcal{D} = \{p \le x; \ \ \exists d \mid N_p \ \text{ such that } x^{\delta-\epsilon} < d \le x^\delta\}.$$

Let $A(n)$ (respectively $C(n)$) be the largest A (respectively C) that divides n. We consider the following four subsets of $\mathcal{D}$.

$$\begin{aligned}
\mathcal{D}_1 &= \{p \in \mathcal{D};\ C(N_p) \text{ is divisible by the square of a prime}\},\\
\mathcal{D}_2 &= \{p \in \mathcal{D};\ \omega(C(N_p)) > \frac{4}{3}\xi\},\\
\mathcal{D}_3 &= \{p \in \mathcal{D};\ A(d) > x^{\epsilon\xi}\},\\
\mathcal{D}_4 &= \{p \in \mathcal{D};\ C(N_p) \text{ is a } C^*\}.
\end{aligned}$$

We observe that

$$\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3 \cup \mathcal{D}_4.$$

We claim that the density of each of these 4 sets in the set of primes is zero, which proves the theorem. Corollary 3.3 shows this assertion for $\mathcal{D}_2$. In the next section we prove the claim for $\mathcal{D}_1$ and $\mathcal{D}_4$. Finally in section 6 we prove the claim for $\mathcal{D}_3$.

Note. If p is supersingular then $N_p = p + 1$ for $p \geq 5$, thus the estimations for supersingular primes in $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{D}_3$, and $\mathcal{D}_4$ are exactly similar to the $p - 1$ estimates of [EM]. So without loss of generality, in the next section, we do our computations only for ordinary primes. Also note that δ is a fixed constant, however ϵ and ξ are functions of x.

5 Lemmas on C's, B's, and A's

Lemma 5.1 *The number of primes $p \leq x$ such that $C(N_p)$ is divisible by the square of a prime $(> x^\epsilon)$ is bounded by*

$$\frac{\pi(x)}{x^\epsilon} + x^{\frac{4}{5}}.$$

Proof The number in question is bounded by

$$\sum_{\substack{l > x^\epsilon \\ l \text{ prime}}} \pi_E(x; l^2).$$

Using Propositions 2.2 and 2.3, one can deduce that

$$\sum_{\substack{l > x^\epsilon \\ l \text{ prime}}} \pi_E(x; l^2) = \sum_{\substack{x^\epsilon < l < x^{\frac{1}{5}} \\ l \text{ prime}}} \pi_E(x; l^2) + \sum_{\substack{l \geq x^{\frac{1}{5}} \\ l \text{ prime}}} \pi_E(x; l^2) \ll \frac{\pi(x)}{x^\epsilon} + x^{\frac{4}{5}}.$$

□

In the sequel we need to apply a version of the large sieve in an imaginary quadratic field K. Let

$$\mathcal{A} = \{\tau \in \mathcal{O}_K;\ N(\tau) \leq u\}.$$

Let $\mathcal{P}$ be a set of prime ideals $\mathfrak{p} \in \mathcal{P}$ in $\mathcal{O}_K$ with the ideal norm $N(\mathfrak{p}) \leq z$. Let $\Lambda(\mathfrak{p})$ be a map which associates to any $\mathfrak{p}$ a subset $\Lambda(\mathfrak{p})$ of $\mathcal{O}/\mathfrak{p}$. Let $\lambda(\mathfrak{p}) = |\Lambda(\mathfrak{p})|$. We set

$$\mathcal{S}(\mathcal{A}, \mathcal{P}) = \{\tau \in \mathcal{O}_K;\ N(\tau) \leq u \ \text{ and } \ \tau (\text{mod } \mathfrak{p}) \notin \Lambda(\mathfrak{p}) \text{ for all } \mathfrak{p} \in \mathcal{P}\}.$$

Lemma 5.2 *We have*

$$|\mathcal{S}(\mathcal{A},\mathcal{P})| \ll \frac{u+z^2}{L(z)}$$

with an absolute implied constant where

$$L(z) = \sum_{N(\mathfrak{d})\le z} \mu^2(\mathfrak{d}) \prod_{\mathfrak{p}\mid\mathfrak{d}} \frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})-\lambda(\mathfrak{p})}.$$

Here $\mu(\mathfrak{d})$ is the analogue of the classical Möbius function.

Proof See [H] and Corollary 5.18 of [K]. □

We also need the following lemma in the proof of Propositions 5.4 and 5.5.

Lemma 5.3 *Let $\mathcal{P}$ be the set of prime ideals in $\mathcal{O}_K$ with norm less than or equal to z. Let $\mathcal{P}_1$ be a subset of $\mathcal{P}$ and $\mathcal{P}_2$ be the complement of $\mathcal{P}_1$ in $\mathcal{P}$. Let $\mathfrak{P}_1$ (respectively $\mathfrak{P}_2$) be the product of the elements of $\mathcal{P}_1$ (respectively $\mathcal{P}_2$). Set*

$$\lambda(\mathfrak{p}) = \begin{cases} 1 & \text{if} \quad \mathfrak{p} \mid \mathfrak{P}_1, \\ 2 & \text{if} \quad \mathfrak{p} \mid \mathfrak{P}_2. \end{cases}$$

Then

$$L(z) = \sum_{N(\mathfrak{d})\le z} \mu^2(\mathfrak{d}) \prod_{\mathfrak{p}\mid\mathfrak{d}} \frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})-\lambda(\mathfrak{p})} \gg \prod_{\mathfrak{p}\mid\mathfrak{P}_1} \left(1-\frac{1}{N(\mathfrak{p})}\right) (\log z)^2,$$

where the implied constant depends only on K.

Proof We have

$$\begin{aligned} L(z) &= \sum_{N(\mathfrak{d})\le z} \frac{\mu^2(\mathfrak{d})\lambda(\mathfrak{d})}{N(\mathfrak{d})} \prod_{\mathfrak{p}\mid\mathfrak{d}} \left(1-\frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}\right)^{-1} \\ &= \sum_{N(\mathfrak{d})\le z} \frac{\mu^2(\mathfrak{d})\lambda(\mathfrak{d})}{N(\mathfrak{d})} \prod_{\mathfrak{p}\mid\mathfrak{d}} \left(1+\frac{\lambda(\mathfrak{p})}{N(\mathfrak{p})}+\frac{\lambda^2(\mathfrak{p})}{N(\mathfrak{p})}+\cdots\right) \\ &= \sum_{N(s(\mathfrak{m}))\le z} \frac{\lambda(\mathfrak{m})}{N(\mathfrak{m})} \\ &\ge \sum_{N(\mathfrak{m})\le z} \frac{\lambda(\mathfrak{m})}{N(\mathfrak{m})}, \end{aligned}$$

where $s(\mathfrak{m})$ denotes the square-free part of the ideal $\mathfrak{m}$ and $\lambda(\mathfrak{m})$ is the completely multiplicative function defined by $\lambda(\mathfrak{p})$. Let $\mathfrak{m}_2$ be the largest divisor of $\mathfrak{m}$ whose prime divisors composed entirely of primes of $\mathcal{P}_2$. Then we have

$$\begin{aligned}\sum_{N(\mathfrak{m})\le z}\frac{\lambda(\mathfrak{m})}{N(\mathfrak{m})} &\ge \sum_{N(\mathfrak{m})\le z}\frac{d(\mathfrak{m}_2)}{N(\mathfrak{m})}\\ &= \sum_{N(\mathfrak{m})\le z}\frac{1}{N(\mathfrak{m})}\sum_{\mathfrak{e}|\mathfrak{m},(\mathfrak{e},\mathfrak{P}_1)=1}1\\ &\ge \sum_{N(\mathfrak{m})\le z}\frac{1}{N(\mathfrak{m})}\sum_{\substack{\mathfrak{e}|\mathfrak{m},(\mathfrak{e},\mathfrak{P}_1)=1\\ N(\mathfrak{e})\le\sqrt{z}}}1\\ &\ge \sum_{N(\mathfrak{f})\le\sqrt{z}}\sum_{\substack{N(\mathfrak{e})\le\sqrt{z}\\ (\mathfrak{e},\mathfrak{P}_1)=1}}\frac{1}{N(\mathfrak{f})N(\mathfrak{e})}.\end{aligned}$$

Now the result follows since

$$\sum_{\substack{N(\mathfrak{e})\le\sqrt{z}\\ (\mathfrak{e},\mathfrak{P}_1)=1}}\frac{1}{N(\mathfrak{e})}\ge\prod_{\mathfrak{p}|\mathfrak{P}_1}\left(1-\frac{1}{N(\mathfrak{p})}\right)\sum_{N(\mathfrak{e})\le\sqrt{z}}\frac{1}{N(\mathfrak{e})},$$

and

$$\sum_{N(\mathfrak{a})\le Q}\frac{1}{N(\mathfrak{a})}=\alpha_K\log Q+O(1),$$

where α_K is the residue of Dedekind's zeta function belonging to the field K (see Lemma 5 of [S] for details). □

Proposition 5.4 *Consider a fixed number of type C that is square-free. Denote it by C. Let*

$$M(u;C)=\#\{t\le u;\quad tC=N_p \text{ for some ordinary } p \text{ and } \omega_J(t)=0\},$$

where $\omega_J(t)$ is the number of distinct prime divisors of t which belong to $J=(x^\epsilon,x^\delta]$. If C is divisible by an inert prime, then $M(u,C)=0$. Otherwise, we have

$$M(u;C)\ll\epsilon 2^{\omega(C)}\prod_{p|C}\left(1+\frac{1}{p-1}\right)\frac{u\log x}{(\log u)^2},$$

as long as $3\le x^\epsilon<u^\alpha\le x^\delta$, where $\alpha=\min\{\delta,\frac{1}{2}\}$. The implied constant depends only on K and δ.

Proof Since p is ordinary then $N_p = (\pi_p - 1)(\bar{\pi}_p - 1)$. Moreover, $K = \mathbb{Q}(\pi_p)$ is a quadratic imaginary field of class number one and so $\mathcal{O}_K$ is a unique factorization domain. If $M(u, C) \neq 0$, then none of the prime divisors of C can be inert in $\mathcal{O}_K$ as C is square-free and $(t, C) = 1$. This shows that there is a $\gamma \in \mathcal{O}_K$ such that $C = N(\gamma)$. We note that such γ is not unique, and up to units there are at most $2^{\omega(C)}$ possibilities for γ. On the other hand since $N_p = N(\pi_p - 1)$, we can conclude that there is a $\tau \in \mathcal{O}_K$ such that $t = N(\tau)$. So if $tC = N_p$, there are τ, and $\gamma \in \mathcal{O}_K$ and a unit e such that $e\tau\gamma + 1 = \pi_p$. We have

$$M(u, C) \leq \sum_{\gamma} \sum_{e \in \mathcal{O}_K^\times} |\mathcal{S}_{e,\gamma}|,$$

where $\mathcal{S}_{e,\gamma}$ is

$$\{\tau \in \mathcal{O}_K;\ N(\tau) \leq u,\ \ (e\tau\gamma + 1) = \mathfrak{q},\ \text{for some prime } \mathfrak{q},\ \ \text{and } \omega_J(\tau\bar{\tau}) = 0\}.$$

Now by employing the large sieve we estimate the size of $\mathcal{S}_{e,\gamma}$.

Let $\mathcal{A}$ be elements of $\mathcal{O}_K$ with norm $\leq u$, and $\mathcal{P}$ be prime ideals of $\mathcal{O}_K$ with norm $\leq z$. Here $z \leq x^\delta$ and will be chosen later as a power of u. Let $\mathfrak{C} = (\gamma)$. Then we have

$$|\mathcal{S}_{e,\gamma}| \ll |\mathcal{P}| + |\mathcal{S}(\mathcal{A}, \mathcal{P})|,$$

where

$$\lambda(\mathfrak{p}) = \begin{cases} 1 & \text{if} \quad N(\mathfrak{p}) \leq x^\epsilon, \\ 2 & \text{if} \quad x^\epsilon < N(\mathfrak{p}) \leq z,\ (\mathfrak{p}, \mathfrak{C}) = 1, \\ 1 & \text{if} \quad x^\epsilon < N(\mathfrak{p}) \leq z,\ \mathfrak{p} \mid \mathfrak{C}. \end{cases}$$

Now from Lemma 5.2 we have

$$|\mathcal{S}_{e,\gamma}| \ll |\mathcal{P}| + \frac{u + z^2}{L(z)}. \tag{5}$$

By Lemma 5.3 and the number field analogue of Mertens' theorem, we have

$$\begin{aligned} L(z) &\gg \prod_{N(\mathfrak{p}) \leq x^\epsilon} \left(1 - \frac{1}{N(\mathfrak{p})}\right) \prod_{p \mid C} \left(1 - \frac{1}{p}\right) (\log z)^2 \\ &\gg \prod_{p \mid C} \left(1 - \frac{1}{p}\right) \frac{(\log z)^2}{\log x^\epsilon}. \end{aligned}$$

Finally by applying the lower bound for $L(z)$ and choosing $z = u^\alpha$ ($\alpha = \min\{\delta, \frac{1}{2}\}$) in (5) we have the result. □

The following proposition is also a consequence of the large sieve.

Proposition 5.5 *Let C be a fixed number of type C which is square-free and A be a fixed number of type A. Let*

$$\tilde{M}(u; AC) = \#\{t \leq u; \quad t \text{ is prime, } tAC = N_p \text{ for some ordinary } p \text{ and } (t, AC) = 1\}.$$

If C is divisible by an inert prime or A is exactly divisible by an inert prime to an odd exponent, then $\tilde{M}(u, AC) = 0$. Otherwise, we have

$$\tilde{M}(u; AC) \ll d(A_{\text{nin}})2^{\omega(C)} \prod_{p|A_{\text{nin}}} \left(1 + \frac{1}{p-1}\right)^2 \prod_{p|C} \left(1 + \frac{1}{p-1}\right) \frac{u}{(\log u)^2},$$

where A_{nin} denotes the largest divisor of A whose prime divisors are not inert in K. The implied constant depends only on K.

Proof The proof is very similar to the previous proposition. If C is not divisible by an inert prime and inert primes of A have even multiplicity, then there are γ and $\alpha \in \mathcal{O}_K$ such that $C = N(\gamma)$, and $A = N(\alpha)$. We note that up to units there are at most $d(A_{\text{nin}})2^{\omega(C)}$ possibilities for $\alpha\gamma$. So as in the previous proposition, we have

$$\tilde{M}(u, C) \leq \sum_{\alpha\gamma} \sum_{e \in \mathcal{O}_K^\times} |\tilde{\mathcal{S}}_{e,\alpha\gamma}|,$$

where $\tilde{\mathcal{S}}_{e,\alpha\gamma}$ is

$$\{\tau \in \mathcal{O}_K;\ N(\tau) \leq u, \quad (\tau) \text{ is prime and } (e\tau\alpha\gamma + 1) = \mathfrak{q}, \text{ for some prime } \mathfrak{q}\}.$$

Next let $\mathcal{A}$ be elements of $\mathcal{O}_K$ with norm $\leq u$, and $\mathcal{P}$ be prime ideals of $\mathcal{O}_K$ with norm $\leq z$. Let $\mathfrak{AC} = (\alpha)(\gamma) = (\alpha\gamma)$. Then we have

$$|\tilde{\mathcal{S}}_{e,\alpha\gamma}| \ll |\mathcal{P}| + |\tilde{\mathcal{S}}(\mathcal{A}, \mathcal{P})|,$$

where

$$\tilde{\lambda}(\mathfrak{p}) = \begin{cases} 2 & \text{if} \quad N(\mathfrak{p}) \leq z,\ (\mathfrak{p}, \mathfrak{AC}) = 1, \text{ and } N(\mathfrak{p}) \neq 2, \\ 1 & \text{if} \quad N(\mathfrak{p}) \leq z,\ \mathfrak{p} \mid \mathfrak{AC}, \text{ or } N(\mathfrak{p}) = 2. \end{cases}$$

Now from Lemma 5.2 we have

$$|\tilde{\mathcal{S}}_{e,\alpha\gamma}| \ll |\mathcal{P}| + \frac{u + z^2}{\tilde{L}(z)}. \tag{6}$$

By Lemma 5.3 we have

$$\begin{aligned}\tilde{L}(z) &\gg \prod_{\mathfrak{p}|\mathfrak{A}}\left(1-\frac{1}{N(\mathfrak{p})}\right)\prod_{\mathfrak{p}|\mathfrak{C}}\left(1-\frac{1}{N(\mathfrak{p})}\right)(\log z)^2\\ &\gg \prod_{p|A_{\mathrm{nin}}}\left(1-\frac{1}{p}\right)^2\prod_{p|C}\left(1-\frac{1}{p}\right)(\log z)^2.\end{aligned}$$

Finally by applying the lower bound for $\tilde{L}(z)$ and choosing $z = u^{1/2}$ in (6) we have the result. □

From now on, without loss of generality, we assume that $x^\epsilon \geq 3$ and each C does not have any inert prime divisor. For square-free C we define

$$\psi(C) = \prod_{p|C}\left(\frac{1}{p}+\frac{1}{p(p-1)}\right).$$

Note that $\psi(C) = 1/\phi(C)$. Also for an A we assume that any inert prime divisor has even multiplicity. Let p denote non-inert prime divisors of A and q denote inert prime divisors of A. We define

$$\psi(A) = \psi(\prod_{p|A}p^b\prod_{q|A}q^{2c}) = \prod_{p|A}\left(\frac{1}{p^b}+\frac{2}{p^b(p-1)}+\frac{1}{p^b(p-1)^2}\right)\prod_{q|A}\frac{1}{q^{2c}},$$

where b or $c \geq 1$. Note that if $b = 0$, we define the product over $p \mid A$ as 1.

The following is a consequence of Propositions 5.4 and 5.5.

Corollary 5.6 *With the notations of Section* 4

$$|\mathcal{D}_4| \ll \epsilon^{\frac{\kappa+1}{2}}\xi^{\frac{5}{2}}\frac{x}{\log x},$$

where $\kappa > -1$. *More precisely,* $\kappa + 1 = \frac{2}{3} - \frac{4}{3}\log\frac{3}{2} \simeq 0.126$.

Proof We have

$$\begin{aligned}\mathcal{D}_4 &= \{p \in \mathcal{D};\ C(N_p) = C^* \leq 3x^{1-\epsilon^{\frac{\kappa+1}{4}}}\}\\ &\quad \cup \{p \in \mathcal{D};\ C(N_p) = C^* > 3x^{1-\epsilon^{\frac{\kappa+1}{4}}}\}\\ &= \mathcal{D}_{41} \cup \mathcal{D}_{42}.\end{aligned}$$

From Proposition 5.4 we have

$$\begin{aligned}|\mathcal{D}_{41}| \ll \sum_{C^*} M(\frac{3x}{C^*}; C^*) &\ll \epsilon x \log x \sum_{C^*} \frac{2^{\omega(C^*)}\psi(C^*)}{\left(\log(3x/C^*)\right)^2} \\ &\ll \frac{\epsilon x}{\epsilon^{\frac{\kappa+1}{2}} \log x} \sum_{C^*} 2^{\omega(C^*)}\psi(C^*).\end{aligned}$$

In Lemma 5.9 we prove that

$$\sum_{C^*} 2^{\omega(C^*)}\psi(C^*) \ll \epsilon^{\kappa}\xi^{\frac{5}{2}},$$

which shows that

$$|\mathcal{D}_{41}| \ll \epsilon^{\frac{\kappa+1}{2}}\xi^{\frac{5}{2}} \frac{x}{\log x}. \tag{7}$$

Next note that if $p \in \mathcal{D}_{42}$, then $N_p = A(N_p)C(N_p) = AC^* = ABC$, where $C > 3x^{1-\delta-\epsilon^{\frac{\kappa+1}{4}}}$. Now since $\delta < 1$, $\omega(C) \leq \frac{4}{3}\xi$, and $\xi\epsilon^{\frac{\kappa+1}{4}} \to 0$ as $x \to \infty$, we can assume that $C = C_1 q$ for a prime $q > x^{\epsilon^{\frac{\kappa+1}{4}}}$. So by employing Proposition 5.5, we have

$$\begin{aligned}|\mathcal{D}_{42}| &\ll \sum_{ABC_1 \leq 3x^{1-\epsilon^{\frac{\kappa+1}{4}}}} \tilde{M}(\frac{3x}{ABC_1}; ABC_1) \\ &\ll \sum_{ABC_1 \leq 3x^{1-\epsilon^{\frac{\kappa+1}{4}}}} \frac{d(A_{\text{nin}})2^{\omega(BC_1)}\psi(A)\psi(BC_1)}{\left(\log(3x/ABC_1)\right)^2} \\ &\ll \frac{x}{\epsilon^{\frac{\kappa+1}{2}}(\log x)^2} \left(\sum_{A}^{\sharp} d(A_{\text{nin}})\psi(A)\right)\left(\sum_{C^*} 2^{\omega(C^*)}\psi(C^*)\right),\end{aligned}$$

where $\sharp$ denotes that the sum ranges over A with $\omega(A) \leq \frac{4}{3}\zeta$. Here $\zeta = \log\log x^{\epsilon}$ is the normal order of $\omega(A(N_p))$, so the number of primes with $\omega(A(N_p)) > \frac{4}{3}\zeta$ has density zero in the set of primes. Applying Lemmas 5.10 and 5.9 in the last inequality results in

$$|\mathcal{D}_{42}| \ll \epsilon^{\frac{\kappa+1}{2}}\xi^{\frac{5}{2}} \frac{x}{\log x}. \tag{8}$$

Now (7) and (8) yield the result. □

The next four lemmas establish the results needed in the previous corollary.

Lemma 5.7 *Let $C^{(s)}$ be a number of type C with exactly s distinct prime factors. Suppose that $s \leq \frac{4}{3}\xi$. Then*

$$\sum_i^{\mu} \psi(C_i^{(s)}) \ll \frac{\xi^s}{2^s s!},$$

where μ means that $C_i^{(s)}$ runs through square-free values.

Proof We have

$$\begin{aligned} \sum_{\substack{p\in J \\ \text{p non}-\text{inert}}} \psi(p) &= \sum_{\substack{p\in J \\ \text{p non}-\text{inert}}} \left(\frac{1}{p} + \frac{1}{p(p-1)}\right) \\ &= \frac{\log\log x^{\delta}}{2} - \frac{\log\log x^{\epsilon}}{2} + O\left(\frac{1}{\log x^{\epsilon}}\right) \leq \frac{\xi}{2} + c. \end{aligned}$$

So

$$\begin{aligned} \sum_i^{\mu} \psi(C_i^{(s)}) \ll \frac{1}{s!}\left(\sum_{p\in J} \psi(p)\right)^s &\ll \frac{(\frac{\xi}{2}+c)^s}{s!} \\ &\ll \frac{\xi^s(1+2c\xi^{-1})^{\frac{4}{3}\xi}}{2^s s!} \\ &\ll \frac{\xi^s}{2^s s!}. \end{aligned}$$

□

Lemma 5.8 *If $r \leq \frac{4}{3}\xi$, then $\sum_{i=1}^{\infty} \psi(B_i^{(r)}) \ll \epsilon\xi^2 \frac{\xi^r}{2^r r!}$, where $B_i^{(r)}$ denote a number of type B with exactly r distinct prime factors.*

Proof With the notation as previous lemma, let

$$B_i^{(r)} = p_1 p_2 \cdots p_r, \quad p_1 < p_2 < \cdots < p_r.$$

It is clear that p_r belongs to the interval

$$\left(\frac{x^{\delta-(\epsilon+\epsilon\xi)}}{p_1\cdots p_{r-1}}, \frac{x^{\delta}}{p_1\cdots p_{r-1}}\right).$$

We note that since $p_r^r > B_i^{(r)}$, we have

$$p_1 p_2 \cdots p_{r-1} < (x^{\delta})^{(r-1)/r}.$$

Taking

$$U = \frac{x^{\delta-(\epsilon+\epsilon\xi)}}{p_1 \cdots p_{r-1}}, \qquad V = x^{\epsilon+\epsilon\xi}$$

in the inequality

$$\sum_{U<p\le UV} \frac{1}{p} \ll \frac{\log V}{\log U} + O\left(\frac{1}{\log U}\right)$$

yields

$$\sum_{U<p_r\le UV} \psi(p_r) \ll \frac{r\epsilon(1+\xi)}{\delta - r(\epsilon+\epsilon\xi)} \ll \epsilon\xi^2.$$

(Note that $r \le \frac{4}{3}\xi$.) Now similar to the previous lemma we have

$$\begin{aligned}
\sum_{i=1}^{\infty} \psi(B_i^{(r)}) &\ll \frac{\epsilon\xi^2}{(r-1)!} \left(\sum_{\substack{p\in J \\ \text{p non-inert}}} \psi(p) \right)^{r-1} \\
&\ll \epsilon\xi^2 \frac{\xi^{r-1}}{2^{r-1}(r-1)!} \\
&\ll \epsilon\xi^2 \frac{\xi^r}{2^r r!}.
\end{aligned}$$

□

Lemma 5.9 $\sum_{i=1}^{\infty} 2^{\omega(C_i^*)}\psi(C_i^*) \ll \epsilon^{\kappa}\xi^{\frac{5}{2}}$, *where* $\kappa > -1$.

Proof By definition of C^* and Lemmas 5.7 and 5.8 we have

$$\begin{aligned}
\sum_{i=1}^{\infty} 2^{\omega(C_i^*)}\psi(C_i^*) &\ll \sum_{0\le r+s\le\frac{4}{3}\xi} \sum_{i=1}^{\infty} 2^r \psi(B_i^{(r)}) \sum_{i}^{\mu} 2^s \psi(C_i^{(s)}) \\
&\ll \epsilon\xi^2 \sum_{0\le r+s\le\frac{4}{3}\xi} \frac{\xi^{r+s}}{r!s!} = \epsilon\xi^2 \sum_{l=0}^{[\frac{4}{3}\xi]} \frac{(2\xi)^l}{l!}.
\end{aligned}$$

We note that for $l \le 2\xi$, $\frac{(2\xi)^l}{l!}$ increases with l, so

$$\sum_{i=1}^{\infty} 2^{\omega(C_i^*)}\psi(C_i^*) \ll \epsilon\xi^2 \frac{(2\xi)^{\frac{4}{3}\xi}}{\Gamma(\frac{4}{3}\xi)}.$$

By Stirling's formula we have

$$\frac{1}{\Gamma(\frac{4}{3}\xi)} \ll \xi^{\frac{1}{2}} \left(\frac{e}{\frac{4}{3}\xi}\right)^{\frac{4}{3}\xi},$$

and so

$$\sum_{i=1}^{\infty} 2^{\omega(C_i^*)}\psi(C_i^*) \ll \epsilon\xi^{\frac{5}{2}}(\frac{3e}{2})^{\frac{4}{3}\xi}.$$

The result follows since $(\frac{3e}{2})^{\frac{4}{3}} = e^c$ for some $c < 2$. More precisely, $\kappa = 1 - c = -\frac{1}{3} - \frac{4}{3}\log\frac{3}{2} \simeq -0.874$. □

Lemma 5.10 *We have*

$$\sum_{A}^{\sharp} d(A_{\text{nin}})\psi(A) \ll \epsilon \log x,$$

where $\sharp$ *denotes that the sum ranges over* A *with* $\omega(A) \leq \frac{4}{3}\zeta = \frac{4}{3}\log\log x^{\epsilon}$.

Proof Let $I = [1, x^{\epsilon}]$. We have

$$\begin{aligned}
\sum_{\substack{l\in I\\ \text{prime}}} \sum_{i=1}^{\infty} d(l^i_{\text{nin}})\psi(l^i) &= \sum_{\substack{p\in I\\ \text{p non-inert}}} \sum_{b=1}^{\infty} \left(\frac{b+1}{p^b} + \frac{2(b+1)}{p^b(p-1)} + \frac{b+1}{p^b(p-1)^2}\right) \\
&+ \sum_{\substack{q\in I\\ q \text{ inert}}} \sum_{c=1}^{\infty} \frac{1}{q^{2c}} \\
&= \sum_{\substack{p\in I\\ p \text{ non-inert}}} \frac{2}{p} + O(1) \leq \zeta + c.
\end{aligned}$$

Now let $A^{(s)}$ be an A with exactly s distinct prime factors. So

$$\begin{aligned}
\sum_{A^{(s)}} d(A^{(s)}_{\text{nin}})\psi(A^{(s)}) \ll \frac{1}{s!}\left(\sum_{\substack{l\in I\\ \text{prime}}} \sum_{i=1}^{\infty} d(l^i_{\text{nin}})\psi(l^i)\right)^s &\ll \frac{(\zeta+c)^s}{s!} \\
&\ll \frac{\zeta^s(1+c\zeta^{-1})^{\frac{4}{3}\zeta}}{s!} \\
&\ll \frac{\zeta^s}{s!}.
\end{aligned}$$

Finally we have

$$\begin{aligned}\sum_A^{\sharp} d(A_{\text{nin}})\psi(A) &\ll \sum_{s=0}^{\frac{4}{3}\zeta}\sum_{A^{(s)}} d(A^{(s)}_{\text{nin}})\psi(A^{(s)}) \\ &\ll \sum_{s=0}^{\frac{4}{3}\zeta}\frac{\zeta^s}{s!} \ll \exp(\zeta) = \epsilon\log x.\end{aligned}$$

□

6 Another Lemma on A's

Lemma 6.1 *Let*

$$N(x) = \#\{p \le x; \quad A(N_p) > x^{\epsilon\xi}\}.$$

Then

$$N(x) \ll \frac{\pi(x)}{\xi}.$$

Proof Let $N(x)$ be the number of primes in question. We have

$$\begin{aligned}N(x)\epsilon\xi\log x &\le \sum_{p\le x}\log A(N_p) \\ &= \sum_{p\le x}\sum_{d|A(N_p)}\Lambda(d) = \sum_{\substack{l\le x^{\epsilon}\\ l \text{ prime}}}\log l \sum_{\substack{p\le x\\ A(N_p)\equiv 0 \pmod{l^i}}} 1 \\ &\le \sum_{\substack{l\le x^{\epsilon}\\ l \text{ prime}}}(\log l)\{\pi_E(x;l) + \pi_E(x;l^2) + \cdots\}. \qquad (9)\end{aligned}$$

By Proposition 2.2, for prime l, we have

$$\pi_E(x;l^i) \ll \frac{(i+1)}{\phi(l^i)}\frac{x}{\log(x/l^{2i})} \qquad \text{for} \qquad l^i \le \left(\frac{x}{\log x}\right)^{\frac{1}{2}}. \qquad (10)$$

Now the right hand side of (9) can be written as

$$\sum_{l\le x^{\epsilon}}\sum_{l^i<x^{\frac{1}{3}}}(\log l)\pi_E(x;l^i) + \sum_{l\le x^{\epsilon}}\sum_{l^i\ge x^{\frac{1}{3}}}(\log l)\pi_E(x;l^i) = \Sigma_I + \Sigma_{II}. \qquad (11)$$

An application of (10) in Σ_I yields

$$\begin{aligned}\Sigma_I &\ll \pi(x)\sum_{l\le x^\epsilon}\frac{\log l}{l-1}+\pi(x)\sum_{l\le x^\epsilon}\sum_{i=2}^{\infty}\frac{(i+1)\log l}{l^i}\\ &\ll \pi(x)\epsilon\log x+\pi(x)\sum_{l=1}^{\infty}\frac{\log l}{l^2}\\ &\ll \pi(x)\epsilon\log x+\pi(x). \qquad (12)\end{aligned}$$

We have

$$\begin{aligned}\Sigma_{II} &\ll x\sum_{l\le x^\epsilon}\sum_{i=\frac{1}{3\epsilon}}^{\infty}\frac{(i+1)\log l}{l^i}\\ &\ll \frac{x}{\epsilon}\sum_{l=2}^{\infty}\frac{\log l}{l^{\frac{1}{3\epsilon}}}\\ &\ll \frac{x}{\epsilon}\left(-\zeta'\left(\frac{1}{3\epsilon}\right)\right). \qquad (13)\end{aligned}$$

Now applying (12) and (13) in (11) together with (9) imply

$$N(x)\ll\frac{\pi(x)}{\xi}\left(1+\frac{1}{\log x^\epsilon}+\left(\frac{1}{\epsilon}\right)^2\left(-\zeta'\left(\frac{1}{3\epsilon}\right)\right)\right).$$

This implies the result since $x^\epsilon\to\infty$ and

$$\left(\frac{1}{\epsilon}\right)^2\left(-\zeta'\left(\frac{1}{3\epsilon}\right)\right)\to 0$$

as $x\to\infty$ (see [T], page 43). □

7 Proof of Theorem 1.3

Proof By employing Lemmas 5.1 and 6.1 and Corollaries 3.3 and 5.6, we have

$$\begin{aligned}H(x,x^{\delta-\epsilon},x^\delta)=|\mathcal{D}| &\le |\mathcal{D}_1|+|\mathcal{D}_2|+|\mathcal{D}_3|+|\mathcal{D}_4|\\ &\ll \pi(x)\left(x^{-\epsilon}+x^{-\frac{1}{5}}\log x+\xi^{-1}+\epsilon^{\frac{\kappa+1}{2}}\xi^{\frac{5}{2}}\right),\end{aligned}$$

where $\kappa > -1$. This completes the proof of the theorem since

$$\lim_{x\to\infty}\left(x^{-\epsilon} + x^{-\frac{1}{5}}\log x + \xi^{-1} + \epsilon^{\kappa+1}\xi^{\frac{5}{2}}\right) = 0.$$

□

8 Proof of Proposition 1.2

Proof We first prove that

$$\#\{p;\ \ |\Gamma_p| < z\} = O\left(\frac{z^{1+\frac{2}{r}}}{\log z}\right).$$

Let $\{Q_1, Q_2, \cdots, Q_r\}$ be a basis of Γ. We consider the set

$$S = \{n_1Q_1 + n_2Q_2 + \cdots + n_rQ_r;\ \ 0 \le n_i \le z^{\frac{1}{r}}\}.$$

Since Q_1, Q_2, $\cdots$, Q_r are linearly independent, then the number of elements of S exceeds

$$([z^{\frac{1}{r}}] + 1)^r > z.$$

Now if p is a prime such that $|\Gamma_p| < z$, then there are two distinct elements of S, say P and Q such that $P = Q$ in $E_p(\mathbb{F}_p)$. In other words there are integers $|m_i| \le z^{\frac{1}{r}}$ such that

$$m_1Q_1 + \cdots + m_rQ_r \neq \mathcal{O} \quad \text{in} \quad E(\mathbb{Q}),$$

however

$$m_1Q_1 + \cdots + m_rQ_r = \mathcal{O} \quad \text{in} \quad E_p(\mathbb{F}_p),$$

where $\mathcal{O}$ denotes the identity element. (Note that here we used the same notation for a point in $E(\mathbb{Q})$ and its reduction in $E_p(\mathbb{F}_p)$.) Let $R = m_1Q_1 + \cdots + m_rQ_r$ in $E(\mathbb{Q})$. Then R is a rational point in $E(\mathbb{Q})$, and so has a representation in the form

$$R = \left(\frac{m}{e^2}, \frac{n}{e^3}\right),$$

where m, n, and e are integers with $e > 0$ and $(m, e) = (n, e) = 1$ (See [ST], page 68). Now since under reduction mod p, R maps to $\mathcal{O}$, we conclude that $p \mid e$. So for fixed m_i the number of primes satisfying $|\Gamma_p| < z$ is bounded by

$$\omega(e) \ll \frac{\log e}{\log\log e} \ll \frac{h_x(R)}{\log h_x(R)},$$

where $\omega(e)$ is the number of distinct prime divisors of e and

$$h_x(R) = h_x\left(\left(\frac{m}{e^2}, \frac{n}{e^3}\right)\right) = \log \max\{|m|, |e^2|\},$$

is the x-height of R. Recall that the canonical height

$$\hat{h}(R) = \lim_{n\to\infty} \frac{h_x(2^n R)}{2^{2n}}$$

is a quadratic form on E, and it gives a bilinear pairing $\langle\ ,\ \rangle$ with $\hat{h}(R) = \langle R, R\rangle$ (see [Si], page 229, Theorem 9.3). Moreover we know that $\hat{h} = h_x + O(1)$, where $O(1)$ depends on E only. So we have

$$\omega(e) \ll \frac{\log e}{\log\log e} \ll \frac{h_x(R)}{\log h_x(R)} = \frac{\hat{h}(R) + O(1)}{\log\left(\hat{h}(R) + O(1)\right)} \ll \frac{\langle R, R\rangle}{\log\langle R, R\rangle}.$$

So for fixed $|m_i| \le z^{\frac{1}{r}}$, we have $\omega(e) \ll z^{\frac{2}{r}}/\log z$. The number of possible values for e is bounded by the number of possible R. Noting the range of the m_i (i.e. $|m_i| \le z^{\frac{1}{r}}$) , we conclude that the number in question is $O\left(z^{1+\frac{2}{r}}/\log z\right)$.

To deduce the result, note that

$$\begin{aligned} \#\left\{p \le x;\ |\Gamma_p| < p^{\frac{r}{r+2}-\epsilon(p)}\right\} \ &\le\ o\left(\frac{x}{\log x}\right) \\ &+\ \#\left\{\frac{x}{\log x} < p \le x;\ |\Gamma_p| < x^{\frac{r}{r+2}}\left(\frac{x}{\log x}\right)^{-\epsilon\left(\frac{x}{\log x}\right)}\right\}, \end{aligned}$$

which is $o(x/\log x)$ upon choosing

$$z = x^{\frac{r}{r+2}}\left(\frac{x}{\log x}\right)^{-\epsilon\left(\frac{x}{\log x}\right)}$$

in the above estimate. □

9 Proof of Theorem 1.4

Proof First of all note that without loss of generality we can assume that $p^{\epsilon(p)} \to \infty$, since otherwise we can always find an $\epsilon_1(p)$ such that $\epsilon(p) \le \epsilon_1(p)$, $\epsilon_1(p) \to 0$, $p^{\epsilon_1(p)} \to \infty$,

and then the result for $\epsilon(p)$ follows from the result for $\epsilon_1(p)$. In fact, we can assume that $p^{\epsilon(p)}$ is a monotone increasing function. Next let

$$\mathcal{A} = \#\{p \le x; \quad p^{\frac{r}{r+2}-\epsilon(p)} < |\Gamma_p| < p^{\frac{r}{r+2}+\epsilon(p)}\}.$$

We have

$$\begin{aligned}
\mathcal{A} &= o\left(\frac{x}{\log x}\right) + \#\{\frac{x}{\log x} < p \le x; \quad p^{\frac{r}{r+2}-\epsilon(p)} < |\Gamma_p| < p^{\frac{r}{r+2}+\epsilon(p)}\} \\
&\le o\left(\frac{x}{\log x}\right) + \#\{\frac{x}{\log x} < p \le x; \quad \left(\frac{x}{\log x}\right)^{\frac{r}{r+2}} x^{-\epsilon(x)} < |\Gamma_p| < x^{\frac{r}{r+2}+\epsilon(x)}\} \\
&\le o\left(\frac{x}{\log x}\right) + \#\{\frac{x}{\log x} < p \le x; \quad x^{\frac{r}{r+2}-\left(\epsilon(x)+\frac{r}{r+2}\frac{\log\log x}{\log x}\right)} < |\Gamma_p| < x^{\frac{r}{r+2}+\epsilon(x)}\}.
\end{aligned}$$

Now since $|\Gamma_p|$ is a divisor of N_p, by Theorem 4.1, $\mathcal{A} = o(x/\log x)$. Combining this with Proposition 1.2 implies the result. □

ACKNOWLEDGMENTS

The authors would like to thank Professor Ram Murty for his suggestions and several helpful discussions related to this work. This paper was completed while the first author was spending a sabbatical year at Queen's University. He would like to thank Queen's University for providing an excellent working environment.

References

[C] A. C. Cojocaru, Reduction of an elliptic curve with almost prime orders, *Acta Arith.* **119** (2005), 265–289.

[E] P. Erdös, A generalization of a theorem of Besicovitch, *J. London Math. Soc.* **11** (1936), 92–98.

[EM] P. Erdös and M. R. Murty, On the order of a (mod p), *CRM Proceedings and Lecture Notes*, Volume **19**, 1999, 87–97.

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

[H] M. N. Huxley, The large sieve inequality for algebraic number fields, *Mathematika* **15** (1968), 178–187.

[HR] H. Halberstam and K. F. Roth, *Sequences*, Springer-Verlag, 1982.

[K] E. Kowalski, Analytic problems for elliptic curves, *J. Ramanujan Math. Soc.* **21** (2006), 19–114.

[L] Y.-R. Liu, Prime divisors of the number of rational points on elliptic curves with complex multiplication, *Bull. London Math. Soc.* **37** (2005), 658–664.

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

[M] C. R. Matthews, Counting points modulo p for some finitely generated subgroups of algebraic groups, *Bull. London Math. Soc.* **14** (1982), 149–154.

[MV] H. L. Montgomery and R. C. Vaughan, The large sieve, *Mathematika* **20** (1973), 119–134.

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

[MMR] M. R. Murty, M. Rosen, and J. H. Silverman, Variations on a theme of Romanoff, *Int. J. Math.* **7** (1996), 373–391.

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

[Si] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[ST] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

[T] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford University Press, 1951.

Department of Mathematics and Computer Science, University of Lethbridge, 4401 University Drive West, Lethbridge, Alberta, T1K 3M4, CANADA
E–mail address: amir.akbary@uleth.ca

Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, Ontario, M5S 2E4, CANADA
E–mail address: murty@math.toronto.edu