Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5)
Vol. IX (2010), 815-832

Orders of CM elliptic curves modulo p with at most two primes

HENRYK IWANIEC AND JORGE JIMÉNEZ URROZ

Abstract. In this paper of 1988 N. Koblitz conjectured that given an elliptic curve E over the rationals, the order of the group of $\mathbb{F}_p$ points of its reduction modulo p, $|E(\mathbb{F}_p)|$, is a prime number for infinitely many primes p. Since then a wide number of research articles has been dedicated to understand and solve this conjecture. In this paper we give the best result known nowadays. We can prove quantitatively that for infinitely many primes p the reduction of the curve $y^2 = x^3 - x$ modulo p has order which is eight times an almost prime number. The problem turns out to be the equivalent to the twin prime conjecture in the Gaussian domain. The result could be extended to any CM curve with certain considerations. We also point out the relation of the result with certain considerations. We also point out the relation of the result with the cyclicity of $E(\mathbb{F}_p)$, and the Lang Trotter conjecture.

Mathematics Subject Classification (2010): 11N36 (primary); 11G07, 14G50 (secondary).

1. Introduction and statement of results

Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. There is a huge variety of papers dedicated to the study of this object, and we can safely say that the main interest to do so is that, in fact, apart from an algebraic curve, it can be equiped with a compatible structure as a finitely generated Abelian group. For example, we know that $E(\mathbb{Q})$, the set of $\mathbb{Q}$-rational points of E, can be seen as the direct product $E(\mathbb{Q}) \simeq E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r$. Let us mention here that, while the torsion is very well understood, the mathematical community is making a great effort in trying to understand the rank r of this group with certain generality.

Since the operations of the group are algebraic functions defined over the same field as the curve, we can also consider the structure of the set of points, not over $\mathbb{Q}$, but over different fields of interest. In this sense, let N be the conductor of the curve and p be a prime of good reduction for E (that is, $p \nmid N$). We denote by E_p the reduction of E modulo p. This is an elliptic curve defined over $\mathbb{F}_p$ and, as in

The first author was supported in part by NSF grant DMS-03-01168. The second by DGICYT Grants MTM2006-15038-C02-02, MTM2009-11068 and TSI2006-02731.

Received June 23, 2009; accepted in revised form November 19, 2009.

the rational case, we are interested in the study of the structure of the group $E(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of E_p. Again it is well known that in this case it is the product of two cyclic finite groups

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus Z/e_p\mathbb{Z}$$

with $d_p|e_p$. However, the behaviour of the invariants d_p and e_p, when varying the prime p, or the elliptic curve $E/\mathbb{Q}$, are highly mysterious and its study comes from very many different perspectives.

Computations of Borosh, Moreno and Porta in 1975 [1] showed that for many primes p one has, $d_p = 1$, *i.e.* the group $E(\mathbb{F}_p)$ is cyclic. This fact, still open, was proved by Serre [19] under GRH three years later. But even more is expected to be true. In their 1977 paper [16] Lang and Trotter conjectured that the elliptic curve analogue of Artin's primitive root conjecture should be true: given an elliptic curve $E/\mathbb{Q}$ and a nontorsion point $a \in E(\mathbb{Q})$, the density of primes for which a generates $E(\mathbb{F}_p)$ exists. In particular, if this density is nonzero, for a positive proportion of primes the group $E(\mathbb{F}_p)$ is cyclic. Since then, there has been an extensive study, both of the conjecture itself, and of the cyclicity of the group of $\mathbb{F}_p$-points. A few examples can be found in [1, 3, 7, 16] and [19].

In 1988 N. Koblitz [15] was also considering the structure of the group of $\mathbb{F}_p$-points of the reduced curve, but this time for its cryptographical implications. Nowadays the security of cryptosystems is based in certain difficult mathematical assumptions, and the Diffie-Hellman assumption regarding the computation of logarithms in finite fields is one of the most famous ones. It is also well known that elliptic curves provide good examples of representations of Abelian groups reducing the size of keys needed to guarantee the same level of security as in the finite-field case. However, to perform elliptic logarithms which are considered to be computationally secure one needs to find a finite field, $\mathbb{F}_p$, and one curve $E/\mathbb{F}_p$, defined over the field, such that the size of the group of $\mathbb{F}_p$-points, $|E(\mathbb{F}_p)|$, has a prime factor as large as possible. One problem arises naturally from above:

Problem 1.1. Let x be a positive number, $E/\mathbb{Q}$ be an elliptic curve over the rationals, and consider the sequence $\widehat{\mathcal{A}}(x) = \{|E(\mathbb{F}_p)| \ : \ p \leq x\}$. How many elements $a \in \mathcal{A}(x)$ have a large prime factor?

Before we start, an observation is needed. Since the reduction modulo p injects $E(\mathbb{Q})_{\text{tors}}$ into $E(\mathbb{F}_p)$ for almost all primes p (in what follows we will always be considering only primes of good reduction), if the curve has rational torsion, then all the elements in $\widehat{\mathcal{A}} = \widehat{\mathcal{A}}(\infty)$ have a non-trivial common factor. In this sense, if d_E is the greatest common divisor of all the elements in $\widehat{\mathcal{A}}$, it is more convenient to consider the sequence $\mathcal{A} = \{\frac{1}{d_E}|E(\mathbb{F}_p)| \ : \ p \text{ prime}\}$.

In his paper [15] Koblitz conjectured that for any elliptic curve over the rationals, the elements in $\mathcal{A}$ not only have a big prime factor very frequently, but in fact are infinitely often primes themselves. Concretely if we denote by $\Pi_E(x)$ the function which counts the number of $a \in \mathcal{A}$, $a \leq x$, that are primes, then he claims that for curves without rational torsion there exist a constant c, depending on the curve, such that $\Pi_E(x) \sim cx/(\log x)^2$ as $x \to \infty$.

Observe that both problems, to find lower bounds for the prime factors of $|E(\mathbb{F}_p)|$, either for cryptographical purposes or towards Koblitz's conjecture, and to ensure cyclicity of the group, can be studied at the same time. In particular if we are able to prove that many elements in $\mathcal{A}$ are squarefree, then automatically, at least when $d_E = 1$, the corresponding group will be cyclic. But if we are able to also say that the number of its prime factors is small, then one of them has to be big in comparison with the size of the element. Hence, to attack both problems, we want to find squarefree elements in $\mathcal{A}$ with few prime factors. We are in a good position to understand our question as part of a general framework, namely inside sieve theory. Let us say that an integer n is P_r if it is squarefree with at most r prime factors. If $r = 2$ we say our number is almost prime. In these terms we are interested in locating many P_r among the elements of $\mathcal{A}$ with as small r as possible. In particular Koblitz' conjecture deals with the case $r = 1$.

Although the most efficient techniques known at present to attack this kind of problems are sieve methods, it is however important to note that, unfortunately, at least considered in its classical way, the sieve can not provide us with lower bounds for the number of primes in certain sequences due to the parity problem. In fact when $r = 1$ there is not a single example of a curve for which the asymptotics predicted by Koblitz have been proved.

For $r > 1$ the situation is not much more promising although now, with sieve methods, one can accomplish something. Miri and Murty in [17] proved, assuming the Grand Riemann Hipothesis, GRH, that for curves without complex multiplication $|\{P_{16} \in \mathcal{A}(x)\}| \gg x/(\log x)^2$. In [20, 21] Steuding and Weng improved the previous result giving $|\{P_6 \in \mathcal{A}(x)\}| \gg x/(\log x)^2$ for non-CM curves. They also proved $|\{P_4 \in \mathcal{A}(x)\}| \gg x/(\log x)^2$ in the CM case, but always under GRH. Very recently, Cojocaru in [4] proved unconditionally that for CM elliptic curves $|\{P_5 \in \mathcal{A}(x)\}| \gg x/(\log x)^2$.

In this paper we will also be considering curves with complex multiplication, focusing on the non-supersingular case. We shall improve the previous works unconditionally. For simplicity, we will restrict our arguments to the curve $E := y^2 = x^3 - x$, although the general CM case could be treated in a similar way. Note that any elliptic curve over $\mathbb{Q}$ can only have complex multiplication by an order of an imaginary quadratic field of class number one. In our case the ordinary primes are $p \equiv 1 \pmod 4$ and, for these, $|E(\mathbb{F}_p)| = p + 1 - 2a$ where $p = a^2 + b^2$, and $a + ib \equiv 1 \pmod{2(1+i)}$ and so we deduce that 8 always divides $|E(\mathbb{F}_p)| = (a-1)^2 + b^2$.

Theorem 1.2. *For $x \geq 5$ we have*

$$\left|\left\{p \leq x\,,\ p \equiv 1 (\mathrm{mod}\ 4)\ :\ \frac{1}{8}|E(\mathbb{F}_p)| = P_2\right\}\right| \gg x/(\log x)^2.$$

It is important to note that for these primes p in Theorem 1.2 of size about x one of the prime divisors of the P_2 has to be of order at least $\sqrt{x}$.

Several remarks are needed. First of all, as we have mentioned, although this theorem is stated for the particular case of the curve $y^2 = x^3 - x$, a completely analogous result holds for any curve $E/\mathbb{Q}$ with complex multiplication. However, just to understand the sequence $\mathcal{A}(x)$ in full generality, one must control the integer d_E, *i.e.* the common factor of the elements $|E(\mathbb{F}_p)|$, attached to the curve. In general this integer will not be trivial. Indeed, we have already mentioned that the torsion of the curve will be part of d_E and recall for example that curves with CM by $\mathbb{Q}(\sqrt{-7})$ always have nontrivial rational 2-torsion. But, in general, it could appear something else and, in this way, a quite interesting study of the corresponding integers d_E appears. The nature of this study is, on one hand more algorithmic and, in any case, far apart from the main lines of discussion for the proof of Theorem 1.2. These reasons lead us to restrict ourselves to the case under discussion. A general statement about CM curves, with a sketch of the proof following the proof of Theorem 1.2, along with the complete study of the integers d_E that appear in each case, and some applications, can be found in [13].

More remarks should be given concerning the particular statement of Theorem 1.2. First we see that we have supersingular reduction for any prime $p \equiv 3 \pmod 4$. Although this case might be of less interest for cryptographic purposes, it is interesting to see what happens. Now $|E(\mathbb{F}_p)| = p + 1$ is always divisible by $d = 4$ and, if we ask whether or not those elements of $\mathcal{A}$ can be prime, we will be asking for primes q such that $p + 1 = 4q$ for some prime q, and this is well known to be essentially equivalent to the Twin Prime Conjecture, so the best one can hope for is a result analogous to Chen's [2] for this problem.

We have already mentioned that, when $p \equiv 1 \pmod 4$, $p = a^2 + b^2$ for some integers a, b which, looking at the problem in the Gaussian domain, is just saying that p splits in $\mathbb{Z}[i]$ as $p = \pi\overline{\pi}$ for $\pi = a + bi$. If we take π to be primary, *i.e.* $\pi \equiv 1 \pmod{2(1+i)}$, then $|E(\mathbb{F}_p)| = N(\pi - 1) \equiv 0 \pmod 8$, and so those elements of the sequence $\mathcal{A}$ will be prime if and only if there exists a prime $\widehat{\pi}$ such that $\pi - 1 = 2(1 + i)\epsilon\widehat{\pi}$, for some unit $\epsilon = \pm 1, \pm i$. In other words, the problem for $p \equiv 1 \pmod 4$ is also equivalent to the Twin Prime Conjecture, but now in the Gaussian domain.

For the proof of Theorem 1.2 we will apply techniques similar to those of Chen, but in the domain of Gaussian integers. First we will need two different extensions of the Bombieri-Vinogradov theorem. The first generalization needed is the analogous result for the field $\mathbb{Q}(i)$. Among many generalizations that occur in the literature in this direction, we appeal to [14], which is suitable to our particular case. The second generalization is a Bombieri-Vinogradov type theorem, not for primes, but rather for Gaussian P_3 type numbers.

To improve the previous results in [17, 20], and [4], apart from the Bombieri-Vinogradov theorem, which in this context is even more efficient than any version of the Riemann Hypothesis, one has to apply the switching principle (see Section 5). In order to make it effective one first needs to increase the level of distribution in the sequence by discarding the inert primes, which contribute as squares (see formulas (3.8) and (3.9) below).

Finally, a question that naturally arises from the previous study is what happens for CM elliptic curves over number fields. Let us note that, first of all, the proof of Theorem 1.2 (or [13, Theorem 1]), heavily relies on a very precise formula for the number of points over $\mathbb{F}_p$ of a curve $E/\mathbb{Q}$ with CM. This type of formulas for a general CM curve over a number field is presented in [18], however it remains to be seen what are the consequences of their formulation for this problem. Moreover, another key fact to carry out the rational case is that any CM elliptic curve with rational coefficients has a quadratic imaginary field of class number one as the CM field. Hence, the present method would not apply directly to CM curves defined over number fields and higher class numbers.

ACKNOWLEDGEMENTS. We would like to thank Nathan Jones for a careful reading of a previous version and for many helpful comments and suggestions for the final presentation of the paper.

2. A weighted sum for the sieve problem

Let us introduce the notation we will need afterwards. The functions $\tau(\cdot)$, $\mu(\cdot)$ and $\phi(\cdot)$, will denote the divisor, Möbius and Euler's phi function respectively, and γ will be the Euler-Mascheroni constant. As usual for any sequence of rational integers, C, and positive number x, we will denote $C(x) = \{c \in C \,:\, c \leq x\}$, and $|C(x)|$ the number of elements in the set. Given an integer d, the set $C_d = \{c \in C \,:\, d|c\}$ consists of the elements of C which are multiples of d and $S(C, d) = |\{c \in C \,:\, (c, d) = 1\}|$ counts the number of elements in C coprime with d. Analogously we define $\mathfrak{C}_\delta$ and $S(\mathfrak{C}, \delta)$ for $\mathfrak{C} \subset \mathbb{Z}[i]$ and $\delta \in \mathbb{Z}[i]$. We will also make several useful conventions. From now on $\lambda, \lambda_1, \lambda_2, \ldots,$ denote primes in $\mathbb{Z}[i]$ and $l, l_1, l_2, \ldots$ the rational primes below them. Furthermore p, p_0, p_1, p_2, p_3 will be rational primes splitting in $\mathbb{Z}[i]$, and $\pi, \pi_0, \pi_1, \pi_2, \pi_3$ will denote primary Gaussian primes above them. On the other hand q will be a rational prime inert in the domain. We put

$$\mathcal{P}(z) = \{p \equiv 1 \pmod 4 \,:\, p \leq z\}, \qquad \text{and} \qquad P(z) = \prod_{p \in \mathcal{P}(z)} p,$$

and on the other hand,

$$\mathcal{Q}(z) = \{q \equiv 3 \pmod 4 \,:\, q \leq z\}, \qquad \text{and} \qquad Q(z) = \prod_{q \in \mathcal{Q}(z)} q.$$

In order to prove Theorem 1.2 we first translate the problem in terms of Gaussian integers. Let

$$\mathcal{A}(x) = \left\{a = N\left(\tfrac{\pi-1}{2(1+i)}\right),\ |\pi|^2 \leq x\right\},$$

and

$$S(x) = \sum_{P_2 \in \mathcal{A}(x)} 1.$$

It is clear that $S(x)$ is twice the left hand side of the inequality in Theorem 1.2 and, therefore, it suffices to prove

$$S(x) \gg x/(\log x)^2. \tag{2.1}$$

A weighted sum will be considered to achieve this goal. In particular let

$$\begin{aligned} W(x) &= \sum_{\substack{a\in\mathcal{A}(x)\\(a,2P(z)Q(z))=1}} \left\{ 1 - \sum_{\substack{p_0|a\\ z<p_0\le y}} \frac{1}{2} - \sum_{\substack{a=p_1p_2p_3\\ z<p_3\le y<p_2<p_1}} \frac{1}{2} \right\} \\ &= \sum_{\substack{a\in\mathcal{A}(x)\\(a,2P(z)Q(z))=1}} 1 - \frac{1}{2}\sum_{z<p_0\le y}\ \sum_{\substack{ap_0\in\mathcal{A}(x)\\(a,2P(z)Q(z))=1}} 1 - \frac{1}{2}\sum_{\substack{z<p_3\le y<p_2<p_1\\ p_3p_2p_1\in\mathcal{A}(x)}} 1 \qquad (2.2) \\ &= W_1(x) - \frac{1}{2}W_2(x) - \frac{1}{2}W_3(x), \end{aligned}$$

where

$$z = x^{1/8} \quad\text{and}\quad y = x^{1/3}. \qquad (2.3)$$

A similar sum was also used by Chen in his original article, [2], and is precisely designed to detect P_2 numbers. Indeed, since any integer less than x cannot have more than three prime divisors bigger than y, any squarefree term of $\mathcal{A}(x)$ with at least four prime divisors will be counted at least twice in the second sum of $W(x)$, meanwhile those with exactly three prime divisors will be counted, in the worst case, at least once on each inner sum of $W(x)$. Hence, any term with positive weight in $W(x)$ has to be either P_2 or divisible by some nontrivial square. However, the contribution to $W(x)$ of non-squarefree elements is easily bounded by

$$\sum_{p>z}\ \sum_{\substack{n\le x\\ n\equiv 0\left(\operatorname{mod} p^2\right)}} \tau(n) \ll \frac{x\log x}{z\log z}.$$

Hence

$$S(x) \ge \sum_{\substack{P_2\in\mathcal{A}(x)\\(P_2,2P(z)Q(z))=1}} 1 \ge W(x) + O\left(\frac{x\log x}{z\log z}\right),$$

and so, in order to prove the theorem we need the estimation

$$W(x) \gg x/(\log x)^2.$$

We will estimate $W_1(x)$, $W_2(x)$, $W_3(x)$ separately.

3. Lower bound for $W_1(x)$

Let us first note that $W_1(x) = S(\mathcal{A}(x), 2P(z)Q(z))$ is the usual sum in sieve theory which counts the elemets in the sequence $\mathcal{A}(x)$ coprime with a product of certain primes, in this case $2P(z)Q(z)$. In order to estimate this sum we need to have some control on $\mathcal{A}_d(x) = \{a \in \mathcal{A}(x) : d|a\}$ for any $d|2P(z)Q(z)$. We will write d as $d = 2^e d_1 d_2$ such that $d_1|P(z)$ and $d_2|Q(z)$. For that purpose we will use the following:

Lemma 3.1. *Let C be a sequence of integers. For $x > 0$ and d squarefree we have*

$$|C_d(x)| = \sum_{k|d} \mu(k) S(C(x), k).$$

Proof. It follows by the Möbius inversion formula. □

Now it is clear that for any squarefree integer k, and $\alpha \in \mathbb{Z}[i]$ we have $(N(\alpha), k) = 1$ if and only if $(\alpha, \kappa) = 1$ where

$$\kappa = \begin{cases} k \text{ if } 2 \nmid k \\ (1+i)\frac{k}{2} \text{ if } 2|k. \end{cases} \tag{3.1}$$

Hence, $S(\mathcal{A}(x), k) = S(\mathfrak{A}(x), \kappa)$, where

$$\mathfrak{A}(x) = \left\{ \frac{\pi - 1}{2(1+i)} \ : \ |\pi|^2 \leq x \right\},$$

and so, by Lemma 3.1,

$$|\mathcal{A}_d(x)| = \sum_{k|d} \mu(k) S(\mathfrak{A}(x), \kappa). \tag{3.2}$$

In order to estimate $S(\mathfrak{A}(x), \kappa)$ we will use the inclusion-exclusion principle over the ideals in $\mathbb{Z}[i]$. In particular let us define the Möbius function

$$\widehat{\mu}(\mathfrak{d}) = \begin{cases} 1 & \text{if } \mathfrak{d} =<1> \\ (-1)^r & \text{if } \mathfrak{d} = \lambda_1 \cdots \lambda_r, \lambda_i \text{ distinct,} \\ 0 & \text{if } \lambda^2 | \mathfrak{d}. \end{cases}$$

It is easy to see that $\widehat{\mu}(\cdot)$ is a multiplicative function over the ideals in $\mathbb{Z}[i]$ which satisfies

$$\sum_{\mathfrak{d}|\alpha} \widehat{\mu}(\mathfrak{d}) = \begin{cases} 1 & \alpha =<1> \\ 0 & \text{otherwise,} \end{cases}$$

and so for any $\kappa \in \mathbb{Z}[i]$ we have

$$S(\mathfrak{A}(x), \kappa) = \sum_{\alpha \in \mathfrak{A}(x)} \sum_{\mathfrak{d}|(\alpha,\kappa)} \widehat{\mu}(\mathfrak{d}) = \sum_{\mathfrak{d}|\kappa} \widehat{\mu}(\mathfrak{d}) |\mathfrak{A}_{\mathfrak{d}}(x)|. \tag{3.3}$$

Hence, the problem reduces to computing $|\mathfrak{A}_{\mathfrak{d}}(x)|$ for ideals $\mathfrak{d}|(1+i)P(z)Q(z)$. By definition we have

$$|\mathfrak{A}_{\mathfrak{d}}(x)| = \Pi(x; 2(1+i)\mathfrak{d}, 1) = \begin{cases} \Pi(x; \mathfrak{d}, 1) & \text{if } (1+i) \nmid \mathfrak{d}, \\ \frac{1}{2}\Pi\left(x; \frac{\mathfrak{d}}{(1+i)}, 1\right) + R_{\mathfrak{d}}(x) & \text{if } (1+i)|\mathfrak{d} \end{cases}$$

where, for a general ideal $\mathfrak{a} \in \mathbb{Z}[i]$, and Gaussian integer α, we write

$$\Pi(x; \mathfrak{a}, \alpha) = \sum_{\substack{\pi \equiv \alpha (\mathrm{mod}\ \mathfrak{a}) \\ |\pi|^2 \le x}} 1,$$

and

$$R_{\mathfrak{d}}(x) = \Pi(x; 2(1+i)\mathfrak{d}, 1) - \frac{1}{2}\Pi(x; 2\mathfrak{d}, 1),$$

because $\Pi(x; 2(1+i)\mathfrak{d}, 1) = \Pi(x; \mathfrak{d}, 1)$ for any $\mathfrak{d}$ odd. Hence, to deduce our bounds for $W_1(x)$, we can use Johnson's generalization of the Bombieri-Vinogradov theorem, Corollary in [14, page 203], to imaginary quadratic fields. In particular, if we let $\Pi(x)$ be the number of splitting primary primes in $\mathbb{Z}[i]$ with norm up to x, we have:

Proposition 3.2. *Let $\mathfrak{a}$ run over the ideals of $\mathbb{Z}[i]$, and α run over the Gaussian integers. We have*

$$\sum_{N(\mathfrak{a}) \le Q} \max_{(\alpha, \mathfrak{a})=1} \left| \Pi(x; \mathfrak{a}, \alpha) - \frac{1}{\Phi(\mathfrak{a})}\Pi(x) \right| \ll \frac{x}{(\log x)^A} \tag{3.4}$$

where $Q = \sqrt{x}/(\log x)^B$ and $\Phi(\mathfrak{a}) = |(\mathbb{Z}[i]/\mathfrak{a})^*|$. Here A is any positive number and B and the implied constant depends only on A.

Proof. Immediate from the mentioned Corollary in [14]. □

In our case, $\mathfrak{a} = \delta/(1+i)^e$, for $e = 1$ or 0 depending on wether $(1+i)|\mathfrak{d}$ or not, hence

$$\Phi(\mathfrak{a}) = \prod_{\pi|\mathfrak{d}} (|\pi|^2 - 1) \prod_{q|\mathfrak{d}} (q^2 - 1),$$

and so

$$|\mathfrak{A}_{\mathfrak{d}}(x)| = \Pi(x)\widehat{g}(\mathfrak{d}) + \widehat{r}_{\mathfrak{d}}(x), \tag{3.5}$$

where $\widehat{g}(\cdot)$ is the multiplicative function over the ideals in $\mathbb{Z}[i]$ such that

$$\widehat{g}(1+i) = \frac{1}{2}, \quad \widehat{g}(\pi) = \frac{1}{|\pi|^2 - 1}, \quad \widehat{g}(q) = \frac{1}{q^2 - 1}.$$

By Proposition 3.2 the error terms satisfy

$$\sum_{N(\mathfrak{d}) \le \sqrt{x}/(\log x)^B} |\widehat{r}_{\mathfrak{d}}(x)| \ll \frac{x}{(\log x)^A}. \tag{3.6}$$

Hence, by (3.2), (3.3) and (3.5) we get for $d = 2^e d_1 d_2$, $d_1|P(z)$, $d_2|Q(z)$ as above

$$\begin{aligned} |\mathcal{A}_d(x)| &= \sum_{k|d} \mu(k)(\Pi(x) \sum_{\mathfrak{d}|\kappa} \widehat{\mu}(\mathfrak{d})\widehat{g}(\mathfrak{d}) + \sum_{\mathfrak{d}|\kappa} \widehat{\mu}(\mathfrak{d})\widehat{r}_{\mathfrak{d}}(x)) \\ &= \Pi(x) \sum_{k|d} \mu(k)H(k) + \sum_{k|d} \mu(k) \sum_{\mathfrak{d}|\kappa} \widehat{\mu}(\mathfrak{d})\widehat{r}_{\mathfrak{d}}(x)) \end{aligned}$$

where $H(\cdot)$ is the multiplicative function such that $H(2) = \frac{1}{2}$, $H(p) = (1-\widehat{g}(\pi))^2$ for splitting primes and $H(q) = 1 - \widehat{g}(q)$ for primes inert in $\mathbb{Z}[i]$. Moreover, by switching the order of summation, we easily get

$$\sum_{k|d}\mu(k)\sum_{\mathfrak{d}|\kappa}\widehat{\mu}(\mathfrak{d})\widehat{r}_{\mathfrak{d}}(x)) = \sum_{a_{\mathfrak{d}}=d}\widehat{\mu}(\mathfrak{d})\widehat{r}_{\mathfrak{d}}(x)\mu(a_{\mathfrak{d}}),$$

where $a_{\mathfrak{d}} = 2^e a_1 b_2$ whenever $\mathfrak{d} = (1+i)^e \alpha_1 b_2$ for $N(\alpha_1) = a_1, a_1|d_1$ and $b_2|d_2$. Hence we can use the approximation

$$|\mathcal{A}_d(x)| = \Pi(x)g(d) + r_d(x), \tag{3.7}$$

where $g(\cdot)$ is the multiplicative function such that $g(l) = 1 - H(l)$ for any prime l, and the error satisfies $|r_d(x)| \le \sum_{a_{\mathfrak{d}}=d}|\widehat{r}_{\mathfrak{d}}(x)|$ which gives us, by Proposition 3.2,

$$\sum_{\substack{d=2^e d_1 d_2\\ 2^e d_1 d_2^2 \le \sqrt{x}/(\log x)^B}} |r_d(x)| \ll \frac{x}{(\log x)^A}. \tag{3.8}$$

In order to make the level of distribution in the error term as large as possible, we should control the contribution to the sum from moduli d with d_2 large. These terms can be easily estimated as follows. First, ignoring that the elements in $\mathcal{A}(x)$ are parametrized by primes, we have

$$|\mathcal{A}_d(x)| \le \sum_{\substack{u^2+v^2\le x/8\\ d|u^2+v^2}} 1 \le \sum_{\substack{u^2+v^2\le x/8d_2^2\\ d_1|u^2+v^2}} 1 \ll \tau(d_1)\frac{x}{d_1 d_2^2}.$$

On the other hand, since d is squarefree, we have

$$\Pi(x)g(d) \ll \frac{\tau(d_1)}{\phi(d_1)d_2^2}\frac{x}{\log x},$$

and so the total contribution to (3.8) from every d with $d_2 \gg (\log x)^{A+1}$ is absorbed by the right hand side. Hence, by changing B to $B + A + 1$, we can write (3.8) as

$$\sum_{d\le\sqrt{x}/(\log x)^B} |r_d(x)| \ll \frac{x}{(\log x)^A}. \tag{3.9}$$

Now, a straightforward application of the prime number theorem for the arithmetic progression $p \equiv 1 \pmod 4$ allows us to see that the density function $g(\cdot)$ verifies the linear sieve assumption

$$\left(\frac{\log z}{\log w}\right)\left(1-\frac{L_1}{\log w}\right) \le \prod_{w\le p<z}(1-g(p))^{-1} \le \left(\frac{\log z}{\log w}\right)\left(1+\frac{L_2}{\log w}\right), \tag{3.10}$$

for some constants L_1, L_2, and so by (3.9) and (3.10) we can apply a linear sieve to $\mathcal{A}(x)$ with level of distribution $D(x) = \sqrt{x}/(\log x)^B$ to deduce, by the Jurkat-Richert theorem (see [9, Theorem 8.4, page 236]) that

$$W_1(x) \geq \Pi(x)V(z)f(s)\{1 + o(1)\}, \tag{3.11}$$

where

$$V(z) = \prod_{p \leq z}(1 - g(p)), \tag{3.12}$$

$s = \frac{\log D(x)}{\log z}$, and $f(s) = 2e^\gamma \frac{\log(s-1)}{s}$ for $2 \leq s \leq 4$, by (2.8) and (2.9) of [9, pages 226 and 227]. (See also [11, Chapter 5]). In particular, with our selection in (2.3) of $z = x^{1/8}$ and $D(x)$ above we get $s = 4 - 8B\frac{\log\log x}{\log x}$, $f(s) = \frac{e^\gamma}{2}\log 3 + o(1)$, and we get the lower bound

$$W_1(x) \geq \left(\tfrac{1}{2}e^\gamma \log 3 + \varepsilon\right)\Pi(x)V(z), \tag{3.13}$$

valid for any $\varepsilon > 0$ and for x sufficiently large in terms of ε.

4. Upper bound for $W_2(x)$

We now proceed to bound $W_2(x)$ from above. Here instead of $\mathcal{A}(x)$, the sets to consider in the sieve process are

$$\mathcal{A}_{p_0}(x) = \{a \in \mathcal{A}(x) \ : \ p_0 | a\},$$

for each prime p_0 in the interval $(z, y]$. In this case the number of elements in $\mathcal{A}_{p_0}$ divisible by d is precisely

$$\left|\mathcal{A}_{dp_0}(x)\right| = \Pi(x)g(dp_0) + r_{dp_0}(x)$$

for $g(\cdot)$ and $r(\cdot)$ as in (3.7), and so we can apply the upper-bound linear sieve of Jurkat and Richert, now with level of distribution $D(x)/p_0$, to find

$$\sum_{\substack{a \in \mathcal{A}_{p_0}(x) \\ (a, 2P(z)Q(z))=1}} 1 \leq \Pi(x)V(z)g(p_0)\left\{F\left(s_{p_0}\right) + o(1)\right\} + \sum_{\substack{d \leq D(x)/p_0 \\ d | 2P(z)Q(z)}} \left|r_{dp_0}(x)\right|, \tag{4.1}$$

where $V(z)$ is given in (3.12), $s_{p_0} = \log(D(x)/p_0)/\log z$, and $F(s) = 2e^\gamma s^{-1}$ for any $1 \leq s \leq 3$ by [9, equation (2.8)] (also [11, equation (3.76)]). In our case, $z < p_0 \leq y$, and so $F(s_{p_0}) = \frac{e^\gamma}{2}\frac{\log x}{\log(x/p_0^2)} + o(1)$. Hence, summing over all the primes p_0 in the interval we get

$$W_2(x) \leq \Pi(x)V(z)\left\{\sum_{z < p_0 \leq y} F(s_{p_0})g(p_0) + o(1)\right\}, \tag{4.2}$$

since $\sum_{z<p_0\le y} g(p_0) = 2\sum_{z<p_0\le y}\frac{1}{p_0-1} = O(1)$, and the absolute error terms satisfy

$$\sum_{z<p_0\le y}\ \sum_{\substack{d\le D(x)/p_0\\ d|2P(z)Q(z)}} \left|r_{dp_0}(x)\right| \ll x/(\log x)^A,$$

by (3.9). Partial summation and (3.10) allow us to obtain

$$W_2(x) \le \Pi(x)V(z)\frac{e^\gamma}{2}\int_z^y \frac{\log x}{\log(x/t^2)t\log t}\mathrm{d}t + o(1).$$

By changing variables $t = x^u$ we get

$$W_2(x) \le \left(\tfrac{1}{2}e^\gamma \log 6 + \varepsilon\right)\Pi(x)V(z), \tag{4.3}$$

for any $\varepsilon > 0$, and x sufficiently large depending on ε.

5. Upper bound for $W_3(x)$

Finally we have to control $W_3(x)$ which counts the number of elements a in $\mathcal{A}(x)$ such that $a = p_1p_2p_3$ for splitting primes in a certain range. More precisely $W_3(x)$ counts the total number of solutions to any of the four equations
$\pi = 1 + (1+i)^3\epsilon\pi_1\pi_2\pi_3$ with $\epsilon \in \{\pm 1, \pm i\}$, in primary primes such that

$$|\pi|^2 \le x \quad \text{and } z \le |\pi_3|^2 < y \le |\pi_2|^2 \le |\pi_1|^2.$$

For this purpose we will also use a linear sieve and the Jurkat-Richert theorem, not directly, but using a switching device and changing the roles of primes π with the triples π_1, π_2, π_3. With this in mind let us again note that the condition $|\pi|^2 \le x$ can be replaced by $|\pi_1\pi_2\pi_3|^2 \le x/8$ with a negligible error of $O(\sqrt{x})$. Let us now consider the sequence

$$\mathcal{B}(x) = \{N(1+\omega) \,:\, \omega \in \Omega(x)\},$$

where

$$\begin{aligned}\Omega(x) = \{\omega = (1+i)^3\epsilon\pi_1\pi_2\pi_3 : \epsilon \in \mathbb{Z}[i]^*,\\ |\omega|^2 \le x, z \le |\pi_3|^2 < y < |\pi_2|^2 < |\pi_1|^2\}.\end{aligned}$$

Then, $W_3(x)$ counts essentially the number of primes in $\mathcal{B}(x)$. In particular

$$W_3(x) \le \sum_{\substack{b\in\mathcal{B}(x)\\ (b,2P(\sqrt{x})Q(\sqrt{x}))=1}} 1 + O(\sqrt{x}),$$

and the problem is ready to apply sieve theory to the sequence $\mathcal{B}(x)$, in this case with new sieve parameter $z_0 = \sqrt{x}$. Again we need to estimate $|\mathcal{B}_d(x)|$, the number of elements in $\mathcal{B}(x)$ divisible by $d|P(\sqrt{x})Q(\sqrt{x})$. Observe that now, if $2|d$, then the set $\mathcal{B}_d(x)$ is trivially empty. As before, we will write $d = d_1 d_2$ where $d_1|P(\sqrt{x})$ and $d_2|Q(\sqrt{x})$. Again using Lemma 3.1 we get

$$|\mathcal{B}_d(x)| = \sum_{k|d} \mu(k) S(B(x), k)$$

for κ given in (3.1) and

$$\mathfrak{B}(x) = \{1 + \omega \,:\, \omega \in \Omega(x)\},$$

and in the same way we will obtain our estimates by aproximating $S(\mathfrak{B}(x), \kappa)$ for any $\kappa|P(\sqrt{x})Q(\sqrt{x})$. For this purpose we note that, just as in Section 3,

$$|\mathfrak{B}_{\mathfrak{d}}(x)| = \sum_{\substack{\omega\in\Omega(x)\\ \omega\equiv-1(\text{mod } \mathfrak{d})}} 1, \tag{5.1}$$

and so, as in the previous cases, the key point to evaluate $|\mathfrak{B}_{\mathfrak{d}}(x)|$, and then $|\mathcal{B}_d(x)|$, relies on the existence of an analogous Bombieri-Vinogradov theorem for the numbers in the set $\Omega(x)$, which we now state. To ease notation we will denote the error term in the approximation as

$$E(x;\alpha,\mathfrak{a}) = \sum_{\substack{\omega\in\Omega(x)\\ \omega\equiv\alpha(\text{mod } \mathfrak{a})}} 1 - \frac{1}{\Phi(\mathfrak{a})} \sum_{\substack{\omega\in\Omega(x)\\ (\omega,\mathfrak{a})=1}} 1.$$

Proposition 5.1. *Let the notation be as above, and $x > 0$. We have*

$$\sum_{N(\mathfrak{a})\leq Q} \max_{(\alpha,\mathfrak{a})=1} |E(x;\alpha,\mathfrak{a})| \ll \frac{x}{(\log x)^A}, \tag{5.2}$$

with $Q = \sqrt{x}/(\log x)^B$. Here A is any positive number and B and the implied constant depend only on A.

In order to prove the proposition we need some lemmata. The first is a generalization of Lemma 17.3 of [12], which will be crucial in the proof of the proposition. Then, a large sieve inequality in the Gaussian domain will allow us to end the proof. As usual $||\widehat{a}|| = \left(\sum_{N(\alpha)\leq N} |\widehat{a}(\alpha)|^2\right)^{1/2}$.

Lemma 5.2. *Let $\mathfrak{d}$ be an ideal in $\mathbb{Z}[i]$, $\xi \in \mathbb{Z}[i]$, $(\xi,\mathfrak{d}) = 1$ and $\widehat{a}(\alpha) \in \mathbb{C}$ a sequence of complex numbers, indexed over Gaussian integers α, such that for any N*

$$\left| \sum_{\substack{N(\alpha)\leq N\\ \alpha\equiv\xi(\mathit{mod}\ \mathfrak{d})}} \widehat{a}(\alpha) - \frac{1}{\Phi(\mathfrak{d})} \sum_{\substack{N(\alpha)\leq N\\ (\alpha,\mathfrak{d})=1}} \widehat{a}(\alpha) \right| \leq ||\widehat{a}||N^{1/2}\Delta^9, \tag{5.3}$$

for some $0 < \Delta < 1$. *Let* $\mathfrak{M}$ *be an ideal in* $\mathbb{Z}[i]$ *and* χ *a non-principal character modulo* $\mathfrak{M}$. *Then*

$$\left|\sum_{(\alpha,\mathfrak{d})=1} \widehat{a}(\alpha)\chi(\alpha)\right| \le ||\widehat{a}||\Delta^3\widehat{\tau}(\mathfrak{d})N(\mathfrak{M})(N\log N)^{1/2},$$

where $\widehat{\tau}(\mathfrak{d})$ *counts the number of ideal divisors of* $\mathfrak{d}$.

Proof. The proof will go along the lines of [12, Lemma 17.3]. In particular it is easy to see that

$$\begin{aligned}&\sum_{(\alpha,\mathfrak{d})=1} \widehat{a}(\alpha)\chi(\alpha)\\ &= \sum_{\substack{\mathfrak{c}|\mathfrak{d}\\ N(\mathfrak{c})\le K}} \widehat{\mu}(\mathfrak{c})\sum_{\mathfrak{e}|\mathfrak{c}}\widehat{\mu}(\mathfrak{e})\sum_{(\alpha,\mathfrak{e})=1}\widehat{a}(\alpha)\chi(\alpha) + \sum_{\substack{\mathfrak{c}|\mathfrak{d}\\ N(\mathfrak{c})>K}}\widehat{\mu}(\mathfrak{c})\sum_{\substack{(\alpha,\mathfrak{d})=1\\ \alpha\equiv 0 (\mathrm{mod}\ \mathfrak{c})}}\widehat{a}(\alpha)\chi(\alpha)\\ &= S_1 + S_2,\end{aligned}$$

where K will be chosen later. By splitting into classes modulo $\mathfrak{e}\mathfrak{M}$, and applying (5.3) for each class we get

$$S_1 \ll ||\widehat{a}||N^{1/2}\Delta^9\sum_{\substack{\mathfrak{c}|\mathfrak{d}\\ N(\mathfrak{c})\le K}}\sum_{\mathfrak{e}|\mathfrak{c}}|\widehat{\mu}(\mathfrak{e})|\Phi(\mathfrak{e}\mathfrak{M}) \le K||\widehat{a}||N^{1/2}\Delta^9 N(\mathfrak{M})\widehat{\tau}(\mathfrak{d}).$$

For the last inequality we have used that if $\mathfrak{e}$ is a squarefree ideal, then $\Phi(\mathfrak{e}\mathfrak{M}) \le \Phi(\mathfrak{e})N(\mathfrak{M})$ for any ideal $\mathfrak{M}$ in $\mathbb{Z}[i]$, and that for any squarefree ideal $\mathfrak{c}$, $\sum_{\mathfrak{e}|\mathfrak{c}}\Phi(\mathfrak{e}) = N(\mathfrak{c})$. In order to get an upper bound for S_2 we use the Cauchy-Schwarz inequality twice to get

$$S_2 \le \widehat{\tau}(\mathfrak{d})^{1/2}||\widehat{a}||\left(\sum_{\substack{\mathfrak{c}|\mathfrak{d}\\ N(\mathfrak{c})>K}}\sum_{\substack{N(\alpha)\le N\\ \alpha\equiv 0(\mathrm{mod}\ \mathfrak{c})}} 1\right)^{1/2} \le \widehat{\tau}(\mathfrak{d})||\widehat{a}||(N\log N)^{1/2}K^{-1/2},$$

since

$$\sum_{\substack{N(\alpha)\le N\\ \alpha\equiv 0(\mathrm{mod}\ \mathfrak{c})}} 1 \le \sum_{n\le N/K}\sum_{N(\xi)=n} 1 \le \sum_{n\le N/K}\tau(n) \ll \frac{1}{K}N\log N. \tag{5.4}$$

The lemma follows by choosing $K = \Delta^{-6}$. □

Lemma 5.3. *For any arithmetic function* $f(n)$ *such that* $f(nm) \le f(n)f(m)$ *for every pair of integers* n, m *we have*

$$\sum_{n\le x}\tau(n)f(n) \le \left(\sum_{n\le x} f(n)\right)^2$$

for any $x > 0$.

Proof. Immediate by switching the order of summation. □

Lemma 5.4. *Let k be a positive integer, and $x > 0$. Then*

$$\sum_{n\leq x}\frac{\tau(n)^k}{\phi(n)} \ll (\log x)^{2^{k+1}}.$$

Proof. Apply the previous lemma to $\tau(n)^{k-1}/\phi(n)$, induction, and the fact that $\sum_{n\leq x}\frac{1}{\phi(n)} \ll (\log x)^2$, the last inequality being consequence of the trivial one $\phi(n) \gg n/\log x$ for any $n \leq x$. □

Proof of Proposition 5.1. We first want to separate the variable π_3 from the variables π_1, π_2 in the definition of the set $\Omega(x)$. To this end we split $\Omega(x)$ into subsets $\Omega_k(x)$ in which $z(1+\delta)^k \leq |\pi_3|^2 < z(1+\delta)^{k+1}$, where δ is a small number and $0 \leq k \leq K$ with $K = [\log(y/z)/\log(1+\delta)]$. Note that the number of such subsets $\Omega_k(x)$ which cover $\Omega(x)$ is $O(\delta^{-1}\log x)$. In each $\Omega_k(x)$ we replace the condition $|\omega|^2 = 8|\pi_1\pi_2\pi_3|^2 \leq x$ by the condition $8|\pi_1\pi_2|^2 z(1+\delta)^k \leq x$ and we denote the resulting set by $\Omega'_k(x)$. The above modified partition covers the set $\Omega(x)$ in a one-to-one fashion, except for the numbers $\omega = (1+i)^3\varepsilon\pi_1\pi_2\pi_3$ with $x/(1+\delta) < 8|\pi_1\pi_2\pi_3|^2 < x(1+\delta)$ or $y < |\pi_3|^2 \leq (1+\delta)y$, $8|\pi_1\pi_2\pi_3|^2 < x$. However these boundary terms contribute to (5.2) trivially $O(\delta x(\log x)^C)$, for some constant C, so they can be ignored by choosing $\delta = (\log x)^{-A-C}$. Therefore, it suffices to show (5.2) for the restricted sets $\Omega'_k(x)$ separately with A replaced by $2A+C+1$. Put $z_k = z(1+\delta)^k$ and let $E_k(x;\alpha,\mathfrak{a})$ be the corresponding error term for the set $\Omega'_k(x)$.

Summing over the non-principal characters of $(\mathbb{Z}[i]/\mathfrak{a})^*$ we get, by orthogonality,

$$\begin{aligned}|E_k(x;\alpha,\mathfrak{a})| &\leq \frac{1}{\Phi(\mathfrak{a})}\sum_{\chi\neq\chi_0}\left|\sum_{\omega\in\Omega'_k(x)}\chi(\omega)\right| \\ &\leq \frac{4}{\Phi(\mathfrak{a})}\sum_{\chi\neq\chi_0}\left|\sum_{z_k\leq|\pi_3|^2<z_k(1+\delta)}\chi(\pi_3)\sum_{\substack{y\leq|\pi_2|^2<|\pi_1|^2\\ |\pi_1\pi_2|^2\leq x/8z_k}}\chi(\pi_1\pi_2)\right|.\end{aligned}$$

Summing over all ideals of norm up to Q, and splitting into primitive characters we get,

$$\begin{aligned}&\sum_{N(\mathfrak{a})\leq Q}\max_{(\alpha,\mathfrak{a})=1}|E_k(x;\alpha,\mathfrak{a})| \\ &\quad\ll \sum_{N(\mathfrak{a}_1)\leq Q}\frac{1}{\Phi(\mathfrak{a}_1)}\sum_{N(\mathfrak{a}_2)\leq Q}\frac{1}{\Phi(\mathfrak{a}_2)}\sideset{}{^*}\sum_{\substack{\chi\,(\mathrm{mod}\ \mathfrak{a}_2)\\ \chi\neq\chi_0}}|A_{k,\mathfrak{a}_1}(\chi)B_{k,\mathfrak{a}_1}(\chi)|. \qquad (5.5)\end{aligned}$$

where

$$A_{k,\mathfrak{a}_1}(\chi) = \sum_{(\alpha,\mathfrak{a}_1)=1} \widehat{a}(\alpha)\chi(\alpha), \qquad B_{k,\mathfrak{a}_1}(\chi) = \sum_{(\beta,\mathfrak{a}_1)=1} \widehat{b}(\beta)\chi(\beta),$$

for

$$\widehat{a}(\alpha) = \begin{cases} 1 & \text{if } \alpha = \pi_3,\, z_k \le |\pi_3|^2 < z_k(1+\delta) \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\widehat{b}(\beta) = \begin{cases} 1 & \text{if } \beta = \pi_1\pi_2,\, y \le |\pi_2|^2 < |\pi_1|^2,\, |\beta|^2 < x/8z_k \\ 0 & \text{otherwise.} \end{cases}$$

Observe that, in particular, $\widehat{b}(\beta) = 0$ if $|\beta|^2 > x/8z_k$.

We now want to use Lemma 5.2 in (5.5). For this purpose we split the sum in (5.5) into two, depending on whether $N(\mathfrak{a}_2) \le R$ or $N(\mathfrak{a}_2) > R$. Let us call D_1 and D_2 each of these two sums respectively. Since $||\widehat{a}|| \le (2z_k)^{1/2}$, and $||\widehat{b}|| \le (x/(8z_k))^{1/2}$, we just have to use Lemma 5.2 and Cauchy-Schwarz to get

$$D_1 \le (x \log x)\Delta^3 \sum_{N(\mathfrak{a}_1)\le Q} \frac{\widehat{\tau}(\mathfrak{a}_1)}{\Phi(\mathfrak{a}_1)} \sum_{N(\mathfrak{a}_2)\le R} N(\mathfrak{a}_2),$$

where Δ will be chosen so that $\widehat{a}$ satisfies (5.3) (which is possible by Proposition 3.2). It is now immediate, from Lemmas 5.3 and 5.4 that

$$D_1 \ll x \log x \Delta^3 R^2 (\log R)(\log Q)^8, \tag{5.6}$$

since (see (5.4))

$$\sum_{N(\mathfrak{a}_2)\le R} N(\mathfrak{a}_2) \le R \sum_{N(\mathfrak{a}_2)\le R} 1 \ll R^2 \log R,$$

and, if $N(\mathfrak{c}) = n$, then $\Phi(\mathfrak{c}) \ge \phi(n)$, and so

$$\sum_{N(\mathfrak{a}_1)\le Q} \frac{\widehat{\tau}(\mathfrak{a}_1)}{\Phi(\mathfrak{a}_1)} = \sum_{n\le Q} \sum_{N(\mathfrak{a}_1)=n} \frac{\widehat{\tau}(\mathfrak{a}_1)}{\Phi(\mathfrak{a}_1)} \le \sum_{n\le Q} \tau(n) \sum_{N(\mathfrak{a}_1)=n} \frac{1}{\Phi(\mathfrak{a}_1)} \le \sum_{n\le Q} \frac{\tau(n)^2}{\phi(n)}. \tag{5.7}$$

Finally we need to estimate D_2. A direct application of Cauchy-Schwarz gives us

$$D_2 \le \sum_{j=0}^{[\log(Q/R)]-1} \sum_{N(\mathfrak{a}_1)\le Q} \frac{1}{\Phi(\mathfrak{a}_1)} (A_j B_j)^{1/2}$$

where

$$A_j = \sum_{e^j R \le N(\mathfrak{a}_2) \le e^{j+1} R} \frac{1}{\Phi(\mathfrak{a}_2)} \sideset{}{^*}\sum_{\substack{\chi \,(\mathrm{mod}\ \mathfrak{a}_2) \\ \chi\ne\chi_0}} A_{k,\mathfrak{a}_1}(\chi)^2,$$

$$B_j = \sum_{e^j R \le N(\mathfrak{a}_2) \le e^{j+1} R} \frac{1}{\Phi(\mathfrak{a}_2)} \sideset{}{^*}\sum_{\substack{\chi \,(\mathrm{mod}\ \mathfrak{a}_2) \\ \chi\ne\chi_0}} B_{k,\mathfrak{a}_1}(\chi)^2.$$

The estimate of A_j, B_j is straightforward from the following large sieve inequality in the Gaussian domain:

Lemma 5.5. *Let $\mathfrak{d}$ be an ideal in $\mathbb{Z}[i]$, $\widehat{a}(\alpha)$ a sequence of complex numbers supported on Gaussian integers with $N(\alpha) \le N$, and $Q \ge 1$. Then*

$$\sum_{N(\mathfrak{a})\le Q} \frac{N(\mathfrak{a})}{\Phi(\mathfrak{a})} \sideset{}{^*}\sum_{\substack{\chi\,(mod\ \mathfrak{a})\\ \chi\ne\chi_0}} \Big|\sum_{(\alpha,\mathfrak{d})=1} \widehat{a}(\alpha)\chi(\alpha)\Big|^2 \ll (Q^2+N)||\widehat{a}||^2.$$

Proof. This is a consequence of [10, equation (3.1), page 180]. □

We can use the previous lemma to bound A_j, B_j and, in this way, deduce that

$$\begin{aligned} D_2 &\ll x^{1/2} \sum_{N(\mathfrak{a}_1)\le Q} \frac{1}{\Phi(\mathfrak{a}_1)} \\ &\times \sum_{j=0}^{[\log(Q/R)]} \frac{1}{e^j R}(e^{j+1}R + (z_k)^{1/2})(e^{j+1}R + (x/8z_k)^{1/2}) \\ &\ll x^{1/2}(\log x)^6(Q + (x/z)^{1/2} + y^{1/2} + x^{1/2}/R), \end{aligned} \tag{5.8}$$

since

$$\sum_{N(\mathfrak{a}_1)\le Q} \frac{1}{\Phi(\mathfrak{a}_1)} \le (\log Q)^4,$$

by Lemma 5.4, as in (5.7). Now Proposition 5.1 follows choosing $Q = x^{1/2}/(\log x)^B$ for B given by Proposition 3.2, $\Delta = (\log x)^{-2A-2013}$, and $R = \Delta^{-1}$. □

It is straightforward to go from the previous proposition to the estimate

$$\sum_{\substack{d\le\sqrt{x}/(\log x)^B\\ d \text{ odd}}} |\,|\mathcal{B}_d(x)| - |\Omega(x)|g(d)| \ll \frac{x}{(\log x)^A}. \tag{5.9}$$

Indeed, first note that in our case we have, by (5.1), $\mathfrak{a} = \mathfrak{d}_1 d_2$ with d_1, d_2 as mentioned above. Then, to get (5.9) first remove the condition $(\omega, \mathfrak{a}) = 1$ by noting that the elements in $\Omega(x)$ only have divisors $|\pi|^2 > x^{1/8}$ and so if one of them is fixed (dividing certain ideal $\mathfrak{a}$), then we will trivially have less than $x^{7/8}\log x$ elements left, which will be absorbed by the error term. Second, change the summation over ideals by the more convenient over integers. The argument to do so is the same as the one done to go from (3.8) to (3.9). Observe that, in this case, we have the extra condition d odd since all the elements in $\Omega(x)$ are divisible by 2. Equation (5.9) allows us to apply a linear sieve to the sequence $\mathcal{B}(x)$ with level of distribution $D(x)$, and again Jurkat-Richert theorem to obtain

$$W_3(x) \le \prod_{2<p<\sqrt{x}} (1-g(p))|\Omega(x)|\{F(1)+o(1)\} = e^\gamma V(z)|\Omega(x)|\{1+o(1)\},$$

since $F(s) = 2e^{\gamma}s^{-1}$ as in (4.1), and $\prod_{2<p<\sqrt{x}}(1-g(p)) = \frac{1}{2}V(z)(1+o(1))$ by (3.10). To finish the proof we just have to compare $|\Omega(x)|$ with $\Pi(x)$ appearing in (3.13) and (4.3). By definition we have

$$\begin{aligned}|\Omega(x)| &\le 4 \sum_{z\le|\pi_3|^2<y}\ \sum_{<|\pi_2|^2<\sqrt{x}/|\pi_3|} \Pi(x/(8|\pi_3\pi_2|^2)\\ &\sim \tfrac{1}{2}\Pi(x) \sum_{z\le|\pi_3|^2<y}\ \sum_{<|\pi_2|^2<\sqrt{x}/|\pi_3|} \frac{\log x}{\log(x/(|\pi_3\pi_2|^2)}.\end{aligned}$$

A new application of partial summation, together with a change of variables, as in the deduction of (4.3), gives

$$|\Omega(x)| \le \tfrac{1}{2}\Pi(x)\int_{\frac{1}{8}}^{\frac{1}{3}}\int_{\frac{1}{3}}^{\frac{1-v}{2}} \frac{1}{1-u-v}\,\frac{\mathrm{d}u\mathrm{d}v}{uv} = \frac{1}{2}c\Pi(x),$$

for some $c < 0.36308373$. We just have to combine the previous results to get

$$W_3(x) \le \left(\frac{1}{2}e^{\gamma}c + \varepsilon\right)\Pi(x)V(z). \tag{5.10}$$

Theorem 1.2 follows by plugging (3.13), (4.3), and (5.10) into (2.2).

References

[1] I. BOROSH, C. J. MORENO and H. PORTA, *Elliptic curves over finite fields. II*, Math. Comp. **29** (1975), 951–964.

[2] J. R. 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.

[3] A. C. COJOCARU,*Questions about the reductions modulo primes of an elliptic curve*, In: “Number Theory”, CRM Proc. Lecture Notes, 36, Amer. Math. Soc., Providence, RI, 2004, 61–79.

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

[5] G. GREAVES, *Sieves in number theory*, In: “A Series of Modern Surveys in Mathematics”, Vol. 43, Springer-Berlin, 2001.

[6] J. FRIEDLANDER and H. IWANIEC, *The sieve*, preprint.

[7] R. GUPTA and M. R. MURTY, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), 13–44.

[8] R. GUPTA and M. R. MURTY, *Cyclicity and generation of points modulo p on elliptic curves*, Invent. Math. **101** (1990), 225–235.

[9] H. HALBERSTAM and H. E. RICHERT, “Sieve Methods”, London Mathematical Society Monographs, No. 4. Academic Press, London-New York, 1974.

[10] J. G. HINZ, *A generalization of Bombieri’s prime number theorem to algebraic number fields*, Acta Arith. **51** (1988), 173–193.

[11] H. IWANIEC, “Sieve Methods”, notes for a graduate course at Rutgers University, 1996.

[12] H. IWANIEC and E. KOWALSKI, "Analytic Number Theory", Colloquium publications, Vol. 53, AMS, 2004.

[13] J. JIMÉNEZ URROZ, *Almost prime orders of CM elliptic curves modulo p*, ANTS-VIII, 2008, In: Lecture Notes in Comput. Sci., Vol. 5011, Springer, 2008, 74–87.

[14] D. JOHNSON, *Mean values of Hecke L-functions*, J. Reine Angew. Math. **305** (1979), 195–205.

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

[16] S. LANG and H. TROTTER, "Frobenius Distributions in GL2-extensions", Lecture Notes in Math., Vol. 504, Springer-Verlag, Berlin-New York, 1976.

[17] S. A. MIRI and V. K. MURTY, *An application of sieve methods to elliptic curves*, In: Lecture Notes in Comput. Sci., Vol. 2247, 2001, 91–98.

[18] K. RUBIN and A. SILVERBERGER, *Point counting on reductions of CM elliptic curves*, http://arxiv.org/abs/0706.3711v1.

[19] J.-P. SERRE, Résumé des cours de 1977–1978, Ann. Collège France, Paris, 1978, 67–70.

[20] 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.

[21] J. STEUDING and A. WENG, Erratum: "On the number of prime divisors of the order of elliptic curves modulo p", Acta Arith. **117** (2005), 341–352; Acta Arith. **119** (2005), 407–408.

Department of Mathematics
Rutgers University
Hill Center-Busch Campus
110 Frelinghuysen Road
Piscataway, NJ 08854-8019, USA
iwaniec@math.rutgers.edu

Dept. Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Campus Nord, c/Jordi Girona 1-3
08034 Barcelona, Spain
jjimenez@ma4.upc.edu