ORDERS OF REDUCTIONS OF ELLIPTIC CURVES WITH MANY AND FEW PRIME FACTORS

LEE TROUPE

Abstract. In this paper, we investigate extreme values of $\omega(\#E(\mathbb{F}_p))$, where $E/\mathbb{Q}$ is an elliptic curve with complex multiplication and ω is the number-of-distinct-prime-divisors function. For fixed $\gamma > 1$, we prove that

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log\log x\} = \frac{x}{(\log x)^{2+\gamma\log\gamma-\gamma+o(1)}}.$$

The same result holds for the quantity $\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) < \gamma \log\log x\}$ when $0 < \gamma < 1$. The argument is worked out in detail for the curve $E : y^2 = x^3 - x$, and we discuss how the method can be adapted for other CM elliptic curves.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. For primes p of good reduction, one has

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

where d_p and e_p are uniquely determined natural numbers such that d_p divides e_p. Thus, $\#E(\mathbb{F}_p) = d_pe_p$. We concern ourselves with the behavior $\omega(\#E(\mathbb{F}_p))$, where $\omega(n)$ denotes the number of distinct prime factors of the number n, as p varies over primes of good reduction. Work has been done already in this arena: If the curve E has CM, Cojocaru [Coj05, Corollary 6] showed that the normal order of $\omega(\#E(\mathbb{F}_p))$ is $\log\log p$, and a year later, Liu [Liu06] established an elliptic curve analogue of the celebrated Erdős - Kac theorem: For any elliptic curve $E/\mathbb{Q}$ with CM, the quantity

$$\frac{\omega(\#E(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}}$$

has a Gaussian normal distribution. In particular, $\omega(\#E(\mathbb{F}_p))$ has normal order $\log\log p$ and standard deviation $\sqrt{\log\log p}$. (These results hold for elliptic curves without CM, if one assumes GRH.)

In light of the Erdős - Kac theorem, one may ask how often $\omega(n)$ takes on extreme values, e.g. values greater than $\gamma\log\log n$, for some fixed $\gamma > 1$. A more precise version of the following result appears in [EN79]; its proof is due to Delange.

Theorem 1.1. *Fix $\gamma > 1$. As $x \to \infty$,*

$$\#\{n \leq x : \omega(n) > \gamma\log\log x\} = \frac{x}{(\log x)^{1+\gamma\log\gamma-\gamma+o(1)}}.$$

Presently, we establish an analogous theorem for the quantity $\omega(\#E(\mathbb{F}_p))$, where $E/\mathbb{Q}$ is an elliptic curve with CM.

Theorem 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve with CM. For $\gamma > 1$ fixed,*

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma\log\log x\} = \frac{x}{(\log x)^{2+\gamma\log\gamma-\gamma+o(1)}}.$$

The same statement is true for the quantity $\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) < \gamma\log\log x\}$ when $0 < \gamma < 1$.

The author was partially supported by NSF RTG Grant DMS-1344994.

In what follows, the above theorem will be proved for $E/\mathbb{Q}$ with $E: y^2 = x^3 - x$. Essentially the same method can be used for any elliptic curve with CM; refer to the discussion in §4 of [Polar]. To establish the theorem, we prove corresponding upper and lower bounds in sections §3 and §4, respectively.

Remark. One can ask similar questions about other arithmetic functions applied to $\#E(\mathbb{F}_p)$. For example, Pollack has shown [Polar] that, if E has CM, then

$$\sum_{p\leq x}{}' \tau(\#E(\mathbb{F}_p)) \sim c_E \cdot x,$$

where the sum is restricted to primes p of good ordinary reduction for E. Several elements of Pollack's method of proof will appear later in this manuscript.

Notation. K will denote an extension of $\mathbb{Q}$ with ring of integers $\mathbb{Z}_K$. For each ideal $\mathfrak{a} \subset \mathbb{Z}_K$, we write $\|\mathfrak{a}\|$ for the norm of $\mathfrak{a}$ (that is, $\|\mathfrak{a}\| = \#\mathbb{Z}_K/\mathfrak{a}$) and $\Phi(\mathfrak{a}) = \#(\mathbb{Z}_K/\mathfrak{a})^\times$. The function ω applied to an ideal $\mathfrak{a} \subset \mathbb{Z}_K$ will denote the number of distinct prime ideals appearing in the factorization of $\mathfrak{a}$ into a product of prime ideals. For $\alpha \in \mathbb{Z}_K$, $\|\alpha\|$ and $\Phi(\alpha)$ denote those functions evaluated at the ideal (α). If α is invertible modulo an ideal $\mathfrak{u} \subset \mathbb{Z}_K$, we write $\gcd(\alpha, \mathfrak{u}) = 1$. The notation $\log_k x$ will be used to denote the kth iterate of the natural logarithm; this is not to be confused with the base-k logarithm. The letters p and q will be reserved for rational prime numbers. We make frequent use of the notation $\ll, \gg$ and O-notation, which has its usual meaning. Other notation may be defined as necessary.

Acknowledgements. The author thanks Paul Pollack for a careful reading of this manuscript and many helpful suggestions.

2. Useful propositions

One of our primary tools will be a version of Brun's sieve in number fields. The following theorem can be proved in much the same way that one obtains Brun's pure sieve in the rational integers, cf. [Pol09, §6.4].

Theorem 2.1. *Let K be a number field with ring of integers $\mathbb{Z}_K$. Let $\mathcal{A}$ be a finite sequence of elements of $\mathbb{Z}_K$, and let $\mathcal{P}$ be a finite set of prime ideals. Define*

$$S(\mathcal{A}, \mathcal{P}) := \#\{a \in \mathcal{A} : \gcd(a, \mathfrak{P}) = 1\}, \text{ where } \mathfrak{P} := \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}.$$

For an ideal $\mathfrak{u} \subset \mathbb{Z}_K$, write $A_\mathfrak{u} := \#\{a \in \mathcal{A} : a \equiv 0 \pmod{\mathfrak{u}}\}$. Let X denote an approximation to the size of $\mathcal{A}$. Suppose δ is a multiplicative function taking values in $[0, 1]$, and define a function $r(\mathfrak{u})$ such that

$$A_\mathfrak{u} = X\delta(\mathfrak{u}) + r(\mathfrak{u})$$

for each $\mathfrak{u}$ dividing $\mathfrak{P}$. Then, for every even $m \in \mathbb{Z}^+$,

$$S(\mathcal{A}, \mathcal{P}) = X \prod_{\mathfrak{p}\in\mathcal{P}} (1 - \delta(\mathfrak{p})) + O\Bigg(\sum_{\mathfrak{u}|\mathfrak{P},\, \omega(\mathfrak{u})\leq m} |r(\mathfrak{u})|\Bigg) + O\Bigg(X \sum_{\mathfrak{u}|\mathfrak{P},\, \omega(\mathfrak{u})\geq m} \delta(\mathfrak{u})\Bigg).$$

All implied constants are absolute.

In our estimation of O-terms arising from the use of Proposition 2.1, we will make frequent use of the following analogue of the Bombieri-Vinogradov theorem, which we state for an arbitrary imaginary quadratic field $K/\mathbb{Q}$ with class number 1. For $\alpha \in \mathbb{Z}_K$ and an ideal $\mathfrak{q} \subset \mathbb{Z}_K$, write

$$\pi(x; \mathfrak{q}, \alpha) = \#\{\mu \in \mathbb{Z}_K : \|\mu\| \leq x, \mu \equiv \alpha \pmod{\mathfrak{q}}\}.$$

Proposition 2.2. *For every $A > 0$, there is a $B > 0$ so that*

$$\sum_{\|\mathfrak{q}\| \leq x^{1/2}(\log x)^{-B}} \max_{\alpha : \gcd(\alpha, \mathfrak{u}) = 1} \max_{y \leq x} |\pi(y; \mathfrak{q}, \alpha) - w_K \cdot \frac{\mathrm{Li}(y)}{\Phi(\mathfrak{q})}| \ll \frac{x}{(\log x)^A},$$

where the above sum and maximum are taken over $\mathfrak{q} \subset \mathbb{Z}_K$ and $\alpha \in \mathbb{Z}_K$. Here w_K denotes the size of the group of units of $\mathbb{Z}_K$

The above follows from Huxley's analogue of the Bombieri-Vinogradov theorem for number fields [Hux71]; see the discussion in [Polar, Lemma 2.3].

The following proposition is an analogue of Mertens' theorem for imaginary quadratic fields. It follows immediately from Theorem 2 of [Ros99].

Proposition 2.3. *Let $K/\mathbb{Q}$ be an imaginary quadratic field and let α_K denote the residue of the associated Dedekind zeta function, $\zeta_K(s)$, at $s = 1$. Then*

$$\prod_{\|\mathfrak{p}\| \leq x} \left(1 - \frac{1}{\|\mathfrak{p}\|}\right)^{-1} \sim e^{\gamma} \alpha_K \log x,$$

where the product is over all prime ideals $\mathfrak{p}$ in $\mathbb{Z}_K$. Here (and only here), γ is the Euler-Mascheroni constant.

Note also that the "additive version" of Mertens' theorem, i.e.,

$$\sum_{\|\mathfrak{p}\| \leq x} \frac{1}{\|\mathfrak{p}\|} = \log_2 x + B_K + O_K\left(\frac{1}{\log x}\right)$$

for some constant B_K, holds in this case as well; it appears as Lemma 2.4 in [Rosen].

Finally, we will make use of the following estimate for elementary symmetric functions [HR83, p. 147, Lemma 13].

Lemma 2.4. *Let $y_1, y_2, \ldots, y_M$ be M non-negative real numbers. For each positive integer d not exceeding M, let*

$$\sigma_d = \sum_{1 \leq k_1 < k_2 < \cdots < k_d \leq M} y_{k_1} y_{k_2} \cdots y_{k_d},$$

so that σ_d is the dth elementary symmetric function of the y_k's. Then, for each d, we have

$$\sigma_d \geq \frac{1}{d!} \sigma_1^d \left(1 - \binom{d}{2} \frac{1}{\sigma_1^2} \sum_{k=1}^{M} y_k^2\right).$$

3. An upper bound

Theorem 3.1. *Let E be the elliptic curve $E : y^2 = x^3 - x$ and fix $\gamma > 1$. Then*

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log_2 x\} \ll_\gamma \frac{x(\log_2 x)^5}{(\log x)^{2 + \gamma \log \gamma - \gamma}}.$$

The same statement is true if instead $0 < \gamma < 1$ and the strict inequality is reversed on the left-hand side.

Before proving Theorem 3.1, we refer to [JU08, Table 2] for the following useful fact concerning the numbers $\#E(\mathbb{F}_p)$: For primes $p \leq x$ with $p \equiv 1 \pmod 4$, we have

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi}) = (\pi - 1)\overline{(\pi - 1)}, \tag{1}$$

where $\pi \in \mathbb{Z}[i]$ is chosen so that $p = \pi\overline{\pi}$ and $\pi \equiv 1 \pmod{(1+i)^3}$. (Such π are sometimes called *primary.*) This determines π completely up to conjugation.

We begin the proof of Theorem 3.1 with the following lemma, which will allow us to disregard certain problematic primes p.

Lemma 3.2. *Let $x \geq 3$ and let $P(n)$ denote the largest prime factor of n. Let $\mathcal{X}$ denote the set of $n \leq x$ for which either of the following properties fail:*
(i) $P(n) > x^{1/6\log_2 x}$
(ii) $P(n)^2 \nmid n$.
Then, for any $A > 0$, the size of $\mathcal{X}$ is $O(x/(\log x)^A)$.

The following upper bound estimate of de Bruijn [dB66, Theorem 2] will be useful in proving the above lemma.

Proposition 3.3. *Let $x \geq y \geq 2$ satisfy $(\log x)^2 \leq y \leq x$. Whenever $u := \frac{\log x}{\log y} \to \infty$, we have*
$$\Psi(x,y) \leq x/u^{u+o(u)}.$$

Proof of Lemma 3.2. If $n \in \mathcal{X}$, then either (a) $P(n) \leq x^{1/6\log_2 x}$ or (b) $P(n) > x^{1/6\log_2 x}$ and $P(n)^2 \mid n$. By Proposition 3.3, the number of $n \leq x$ for which (a) holds is $O(x/(\log x)^A)$ for any $A > 0$, noting that $(\log x)^A \ll (\log x)^{\log_3 x} = (\log_2 x)^{\log_2 x}$. The number of $n \leq x$ for which (b) holds is
$$\ll x \sum_{p > x^{1/6\log_2 x}} p^{-2} \ll x \exp(-\log x/6\log_2 x),$$
and this is also $O(x/(\log x)^A)$. □

We would like to use Lemma 3.2 to say that a negligible amount of the numbers $\#E(\mathbb{F}_p)$, for $p \leq x$, belong to $\mathcal{X}$. The following lemma allows us to do so.

Lemma 3.4. *The number of $p \leq x$ with $\#E(\mathbb{F}_p) \in \mathcal{X}$ is $O(x/(\log x)^B)$, for any $B > 0$.*

Proof. Suppose $\#E(\mathbb{F}_p) = b \in \mathcal{X}$. Then, by (1), $b = \|\pi - 1\|$, where $\pi \in \mathbb{Z}[i]$ is a Gaussian prime lying above p. Thus, the number of $p \leq x$ with $\#E(\mathbb{F}_p) = b$ is bounded from above by the number of Gaussian integers with norm b, which, by [HW00, Theorem 278], is $4\sum_{d|b}\chi(d)$, where χ is the nontrivial character modulo 4. Now, using the Cauchy-Schwarz inequality and Lemma 3.2,
$$4\sum_{b\in\mathcal{X}}\sum_{d|b}\chi(d) \leq 4\sum_{b\in\mathcal{X}}\tau(b) \leq 4\Big(\sum_{b\in\mathcal{X}}1\Big)^{1/2}\Big(\sum_{b\in\mathcal{X}}\tau(b)^2\Big)^{1/2}$$
$$\ll \Big(\frac{x}{(\log x)^A}\Big)^{1/2}\Big(x\log^3 x\Big)^{1/2} = \frac{x}{(\log x)^{A/2-3/2}}.$$
Since $A > 0$ can be chosen arbitrarily, this completes the proof. □

For k a nonnegative integer, define N_k to be the number of primes $p \leq x$ of good ordinary reduction for E such that $\#E(\mathbb{F}_p)$ possesses properties (i) and (ii) from the above lemma and such that $\omega(\#E(\mathbb{F}_p)) = k$. Then, in the case when $\gamma > 1$,
$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma\log\log x\} = \sum_{k > \gamma\log_2 x} N_k + O\Big(\frac{x}{(\log x)^A}\Big)$$
for any $A > 0$. Our task is now to bound N_k from above in terms of k. Evaluating the sum on k then produces the desired upper bound.

It is clear that
$$N_k \leq \sum_{\substack{a \leq x^{1-1/6\log_2 x} \\ \omega(a)=k-1}} \sum_{\substack{p\leq x \\ p\equiv 1 \ (\mathrm{mod}\ 4) \\ a|\#E(\mathbb{F}_p) \\ \#E(\mathbb{F}_p)/a \text{ prime}}} 1. \tag{2}$$

To handle the inner sum, we need information on the integer divisors of $\#E(\mathbb{F}_p)$, where $p \le x$ and $p \equiv 1 \pmod 4$. We employ the analysis of Pollack in his proof of [Polar, Theorem 1.1], which we restate here for completeness.

By (1), we have $a \mid \#E(\mathbb{F}_p)$ if and only if $a \mid (\pi-1)\overline{(\pi-1)} = \|\pi - 1\|$. With this in mind, we have

$$\sum_{\substack{a \le x^{1-1/6\log\log x} \\ \omega(a)=k-1}} \sum_{\substack{p\le x \\ p\equiv 1 \pmod 4 \\ a \mid \#E(\mathbb{F}_p) \\ \#E(\mathbb{F}_p)/a \text{ prime}}} 1 = \frac{1}{2} \sum_{\substack{a \le x^{1-1/6\log\log x} \\ \omega(a)=k-1}} {\sum_{\substack{\pi\,:\,\|\pi\|\le x \\ \pi\equiv 1 \pmod{(1+i)^3} \\ a \mid \|\pi-1\| \\ \|\pi-1\|/a \text{ prime}}}}' 1,$$

where the $'$ on the sum indicates a restriction to primes π lying over rational primes $p \equiv 1 \pmod 4$.

3.1. **Divisors of shifted Gaussian primes.** The conditions on the primed sum above can be reformulated purely in terms of Gaussian integers.

Definition 3.5. For a given integer $a \in \mathbb{N}$, write $a = \prod_q q^{v_q}$, with each q prime. For each $q \mid a$ with $q \equiv 1 \pmod 4$, write $q = \pi_q \overline{\pi}_q$. Define a set S_a which consists of all products α of the form

$$\alpha = (1+i)^{v_2} \prod_{\substack{q\mid a \\ q\equiv 3 \pmod 4}} q^{\lceil v_q/2 \rceil} \prod_{\substack{q\mid a \\ q\equiv 1 \pmod 4}} \alpha_q,$$

where $\alpha_q \in \{\pi_q^i \overline{\pi}_q^{v_q - i} : i = 0, 1, \ldots, v_q\}$.

Notice that the condition $a \mid \|\pi - 1\|$ is equivalent to $\pi - 1$ being divisible by some element of the set S_a. We can therefore write

$$\sum_{\substack{a \le x^{1-1/6\log\log x} \\ \omega(a)=k-1}} \sum_{\substack{p\le x \\ p\equiv 1 \pmod 4 \\ a \mid \#E(\mathbb{F}_p) \\ \#E(\mathbb{F}_p)/a \text{ prime}}} 1 \le \frac{1}{2} \sum_{\substack{a \le x^{1-1/6\log\log x} \\ \omega(a)=k-1}} \sum_{\alpha\in S_a} {\sum_{\substack{\pi\,:\,\|\pi\|\le x \\ \pi\equiv 1 \pmod{(1+i)^3} \\ \alpha \mid \pi-1 \\ \|\pi-1\|/a \text{ prime}}}}' 1. \tag{3}$$

Now, for any $\alpha \in S_a$, we have

$$\alpha\overline{\alpha} = a \prod_{q\equiv 3 \pmod 4} q^{2\lceil v_q/2\rceil - v_q}.$$

Observe that

$$\frac{\|\pi-1\|}{a} = \frac{(\pi-1)\overline{(\pi-1)}}{\alpha\overline{\alpha}} \prod_{q\equiv 3 \pmod 4} q^{2\lceil v_q/2\rceil - v_q}.$$

Therefore, if $\frac{\|\pi-1\|}{a}$ is to be prime, the number a must satisfy exactly one of the following properties:

1. The number a is divisible by exactly one prime $q \equiv 3 \pmod 4$ with v_q an odd number, and $\alpha = u(\pi - 1)$ where $u \in \mathbb{Z}[i]$ is a unit; or
2. All primes $q \equiv 3 \pmod 4$ which divide a have v_q even, and $(\pi-1)/\alpha$ is a prime in $\mathbb{Z}[i]$.

This splits the outer sum in (3) into two components.

Lemma 3.6. *We have*

$$\sideset{}{^\flat}\sum_{\substack{a \le x^{1-1/6\log\log x} \\ \omega(a)=k-1}} \sum_{\alpha\in S_a} {\sum_{\substack{\pi\,:\,\|\pi\|\le x \\ \pi\equiv 1 \pmod{(1+i)^3} \\ (\pi-1)/\alpha\in U}}}' 1 = O\left(\frac{x}{\log^A x}\right),$$

where U is the set of units in $\mathbb{Z}[i]$ and the $\flat$ on the outer sum indicates a restriction to integers a such that there is a unique prime power $q^{v_q}\|a$ with $q \equiv 3 \pmod 4$ and v_q odd.

Proof. If $\alpha = u(\pi - 1)$ for $u \in U$, then there are at most four choices for π, given α. Thus

$$\sideset{}{^\flat}\sum_{\substack{a \le x^{1-1/6\log\log x} \\ \omega(a)=k-1}} \sum_{\alpha \in S_a} \sideset{}{'}\sum_{\substack{\pi\,:\,\|\pi\| \le x \\ \pi \equiv 1 \pmod{(1+i)^3} \\ \alpha = u(\pi-1)}} 1 \le 4 \sideset{}{^\flat}\sum_{\substack{a \le x^{1-1/6\log\log x} \\ \omega(a)=k-1}} |S_a|.$$

We have $|S_a| = \prod_{q \equiv 1 \pmod 4}(v_q + 1)$; this is bounded from above by the divisor function on a, which we denote $\tau(a)$. Therefore, the above is

$$\ll \sum_{a \le x^{1-1/6\log\log x}} \tau(a) \ll x^{1-1/6\log_2 x}(\log x),$$

which is $O(x/\log^A x)$ for any $A > 0$. $\square$

The second case provides the main contribution to the sum.

Lemma 3.7. *Let $a \le x^{1-1/6\log\log x}$ with $\omega(a) = k - 1$ such that all primes $q \equiv 3 \pmod 4$ dividing a have v_q even. Let $\alpha \in S_a$. Then*

$$\sideset{}{'}\sum_{\substack{\pi\,:\,\|\pi\| \le x \\ \pi \equiv 1 \pmod{(1+i)^3} \\ \alpha \mid \pi - 1 \\ (\pi-1)/\alpha \text{ prime}}} 1 \ll \frac{x(\log_2 x)^5}{\|\alpha\|(\log x)^2}$$

uniformly over all a as above and $\alpha \in S_a$.

Proof. If $\pi \equiv 1 \pmod \alpha$, then $\pi = 1 + \alpha\beta$ for some $\beta \subset \mathbb{Z}[i]$. Thus $\beta = \frac{\pi-1}{\alpha}$, and so $\|\beta\| \le \frac{2x}{\|\alpha\|}$. Let $\mathcal{A}$ denote the sequence of elements in $\mathbb{Z}[i]$ given by

$$\Big\{\beta(1 + \alpha\beta) : \|\beta\| \le \frac{2x}{\|\alpha\|}\Big\}.$$

Define $\mathcal{P} = \{\mathfrak{p} \subset \mathbb{Z}[i] : \|\mathfrak{p}\| \le z\}$ where z is a parameter to be chosen later. Then, in the notation of Theorem 2.1,

$$\sideset{}{'}\sum_{\substack{\pi\,:\,\|\pi\| \le x \\ \pi \equiv 1 \pmod{(1+i)^3} \\ \alpha \mid \pi - 1 \\ (\pi-1)/\alpha \text{ prime}}} 1 \le S(\mathcal{A}, \mathcal{P}) + O(z).$$

Here, the $O(z)$ term comes from those $\pi \in \mathbb{Z}[i]$ such that both π and $(\pi - 1)/\alpha$ are primes of norm less than z.

For $\mathfrak{u} \subset \mathbb{Z}[i]$, write $A_{\mathfrak{u}} = \#\{a \in \mathcal{A} : a \equiv 0 \pmod{\mathfrak{u}}\}$. An element $\mathfrak{a} \in \mathcal{A}$ is counted by $A_{\mathfrak{u}}$ if and only if a generator of $\mathfrak{u}$ divides a. Thus, by familiar estimates on the number of integer lattice points contained in a circle, $A_{\mathfrak{u}}$ satisfies the equation

$$A_{\mathfrak{u}} = \frac{2\pi x}{\|\alpha\|}\frac{\nu(\mathfrak{u})}{\|\mathfrak{u}\|} + O\Big(\nu(\mathfrak{u})\frac{\sqrt{x}}{(\|\alpha\|\|\mathfrak{u}\|)^{1/2}}\Big),$$

where

$$\nu(\mathfrak{u}) = \#\{\beta \pmod{\mathfrak{u}} : \beta(1 + \alpha\beta) \equiv 0 \pmod{\mathfrak{u}}\}.$$

We apply Theorem 2.1 with

$$X = \frac{2\pi x}{\|\alpha\|} \quad \text{and} \quad \delta(\mathfrak{u}) = \frac{\nu(\mathfrak{u})}{\|\mathfrak{u}\|}.$$

With these choices, we have

$$r(\mathfrak{u}) = O\Big(\nu(\mathfrak{u})\frac{\sqrt{x}}{(\|\alpha\|\|\mathfrak{u}\|)^{1/2}|}\Big).$$

Then, for any even integer $m \geq 0$,

$$S(\mathcal{A},\mathcal{P}) = \frac{2\pi x}{\|\alpha\|}\prod_{\|\mathfrak{p}\|\leq z}\left(1-\frac{\nu(\mathfrak{p})}{\|\mathfrak{p}\|}\right) + O\Big(\frac{\sqrt{x}}{\|\alpha\|^{1/2}}\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\leq m}}\frac{\nu(\mathfrak{u})}{\|\mathfrak{u}\|^{1/2}}\Big) + O\Big(\frac{x}{\|\alpha\|}\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\geq m}}\delta(\mathfrak{u})\Big), \tag{4}$$

where $\mathfrak{P} = \prod_{\mathfrak{p}\in\mathcal{P}}\mathfrak{p}$.

For a prime $\mathfrak{p}$, we have $\nu(\mathfrak{p}) = 2$ if $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$ and $\nu(\mathfrak{p}) = 1$ otherwise. Therefore, the product in the first term is

$$\prod_{\substack{\|\mathfrak{p}\|\leq z\\ \mathfrak{p}\nmid(\alpha)}}\left(1-\frac{2}{\|\mathfrak{p}\|}\right)\prod_{\substack{\|\mathfrak{p}\|\leq z\\ \mathfrak{p}|(\alpha)}}\left(1-\frac{1}{\|\mathfrak{p}\|}\right)$$

$$\leq \prod_{\|\mathfrak{p}\|\leq z}\left(1-\frac{1}{\|\mathfrak{p}\|}\right)^2\prod_{\substack{\|\mathfrak{p}\|\leq z\\ \mathfrak{p}|(\alpha)}}\left(1-\frac{1}{\|\mathfrak{p}\|}\right)^{-1} \ll \frac{1}{(\log z)^2}\frac{\|\alpha\|}{\Phi(\alpha)},$$

where in the last step we used Proposition 2.3.

Choose $z = x^{\frac{1}{200(\log_2 x)^2}}$. Then our first term in (4) is

$$\ll \frac{x(\log_2 x)^4}{\Phi(\alpha)(\log x)^2}.$$

Recall that $\|\alpha\| = a$, and $a \leq x^{1-1/6\log_2 x}$. Since $\Phi(\alpha) \gg \|\alpha\|/\log_2 x$ (analogous to the minimal order for the usual Euler function, c.f. [HW00, Theorem 328]), the above is

$$\ll \frac{x(\log_2 x)^5}{\|\alpha\|(\log x)^2}.$$

We now show that this "main" term dominates the two O-terms uniformly for $\alpha \in S_a$ and $a \leq x^{1-1/6\log_2 x}$. For the first O-term, we begin by noting that $\nu(\mathfrak{u})/\|\mathfrak{u}\|^{1/2} \ll 1$. Then, taking $m = 10\lfloor\log_2 x\rfloor$, we have

$$\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\leq m}}\frac{\nu(\mathfrak{u})}{\|\mathfrak{u}\|^{1/2}} \ll \sum_{k=0}^{m}\binom{\pi_K(z)}{k} \leq \sum_{k=0}^{m}\pi_K(z)^k \leq 2\pi_K(z)^m \leq x^{1/20\log_2 x},$$

where $\pi_K(z)$ denotes the number of prime ideals $\mathfrak{p} \subset \mathbb{Z}[i]$ with norm up to z. Therefore, the inequality

$$\frac{x(\log_2 x)^5}{\|\alpha\|(\log x)^2} \gg \frac{x^{1/2+1/20\log_2 x}}{\|\alpha\|^{1/2}}$$

holds for all α with $\|\alpha\| \leq x^{1-1/6\log_2 x}$, as desired.

Next we handle the second O-term. The sum in this term is

$$\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\geq m}}\delta(\mathfrak{u}) \leq \sum_{s\geq m}\frac{1}{s!}\Big(\sum_{\|\mathfrak{p}\|\leq z}\frac{\nu(\mathfrak{p})}{\|\mathfrak{p}\|}\Big)^s.$$

Observe that, by Proposition 2.3, we have

$$\sum_{\|\mathfrak{p}\|\le z} \frac{\nu(\mathfrak{p})}{\|\mathfrak{p}\|} \le 2\log_2 x + O(1).$$

Thus, by the ratio test, one sees that the sum on s is

$$\ll \frac{1}{m!}(2\log_2 x + O(1))^m.$$

Using Proposition 2.3 followed by Stirling's formula, we obtain that the above quantity is

$$\begin{aligned}\frac{1}{m!}(2\log_2 x + O(1))^m &\le \Big(\frac{2e\log_2 x + O(1)}{10\lfloor \log_2 x\rfloor}\Big)^{10\lfloor \log_2 x\rfloor}\\ &\ll \Big(\frac{e}{5}\Big)^{9\log_2 x} \le \frac{1}{(\log x)^5}.\end{aligned}$$

So the second O-term is

$$\ll \frac{x}{\|\alpha\|(\log x)^5},$$

and this is certainly dominated by the main term. □

From Lemmas 3.6 and 3.7, we see (2) can be rewritten

$$N_k \ll \frac{x(\log_2 x)^5}{(\log x)^2} \sum_{\substack{a\le x^{1-1/6\log_2 x}\\ \omega(a)=k-1}} \frac{|S_a|}{a} + O\Big(\frac{x}{\log^A x}\Big),$$

noting that $\|\alpha\| = a$ for all a under consideration and all $\alpha \in S_a$. We are now in a position to bound N_k from above in terms of k.

Lemma 3.8. *We have*

$$\sum_{\substack{a\le x^{1-1/6\log_2 x}\\ \omega(a)=k-1}} \frac{|S_a|}{a} \le \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!}.$$

Proof. We have already seen that the size of S_a is $\prod_{p|a:p\equiv 1 \pmod 4}(v_p+1)$, where v_p is defined by $p^{v_p} \parallel a$. Recall that in the current case, each prime $p\equiv 3 \pmod 4$ dividing a appears to an even power. Therefore, we have

$$\sum_{\substack{a\le x\\ \omega(a)=k-1}} \frac{|S_a|}{a} \le \frac{1}{(k-1)!}\Bigg(\sum_{\substack{p^\ell\le x\\ p\not\equiv 3 \pmod 4}} \frac{|S_{p^\ell}|}{p^\ell} + \sum_{\substack{p^{2k}\le x\\ p\equiv 3 \pmod 4}} \frac{|S_{p^{2k}}|}{p^{2k}} + O(1)\Bigg)^{k-1}. \tag{5}$$

Note that $|S_{p^{2k}}| = 1$ for each prime $p\equiv 3 \pmod 4$. Thus we can absorb the sum corresponding to these primes into the $O(1)$ term, giving

$$\sum_{\substack{a\le x\\ \omega(a)=k-1}} \frac{|S_a|}{a} \ll \frac{1}{(k-1)!}\Bigg(\sum_{\substack{p^\ell\le x\\ p\not\equiv 3 \pmod 4}} \frac{|S_{p^\ell}|}{p^\ell} + O(1)\Bigg)^{k-1}. \tag{6}$$

Now

$$\begin{aligned}\sum_{\substack{p^\ell \le x\\ p\not\equiv 3 \ (\mathrm{mod}\ 4)}} \frac{|S_{p^\ell}|}{p^\ell} &= \sum_{\substack{p^\ell \le x\\ p\equiv 1 \ (\mathrm{mod}\ 4)}} \frac{\ell+1}{p^\ell} + O(1)\\ &= \sum_{\substack{p \le x\\ p\equiv 1 \ (\mathrm{mod}\ 4)}} \frac{2}{p} + O(1)\\ &= \log_2 x + O(1).\end{aligned}$$

Inserting this expression into (6) proves the lemma. □

3.2. **Finishing the upper bound.** We have shown so far that

$$N_k \ll \frac{x(\log_2 x)^5}{(\log x)^2} \cdot \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!}.$$

We now sum on $k > \gamma \log_2 x$ for fixed $\gamma > 1$ to complete the proof of Theorem 3.1. (The statement corresponding to $0 < \gamma < 1$ may be proved in a completely similar way.) Again using the ratio test and Stirling's formula, we have

$$\begin{aligned}\sum_{k>\gamma \log_2 x} \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!} &\ll \left(\frac{e\log_2 x + O(1)}{\lfloor \gamma \log_2 x\rfloor}\right)^{\lfloor \gamma \log_2 x\rfloor}\\ &\ll \left(\frac{e}{\gamma}\Big(1+O\Big(\frac{1}{\log_2 x}\Big)\Big)\right)^{\lfloor \gamma \log_2 x\rfloor} \ll \left(\frac{e}{\gamma}\right)^{\lfloor \gamma \log_2 x\rfloor} \ll_\gamma (\log x)^{\gamma - \gamma\log\gamma}.\end{aligned}$$

Thus, we have obtained an upper bound of

$$\ll_\gamma \frac{x(\log_2 x)^5}{(\log x)^{2+\gamma\log\gamma - \gamma}},$$

as desired.

4. A lower bound

Theorem 4.1. *Consider $E : y^2 = x^3 - x$ and fix $\gamma > 1$. Then*

$$\#\{p \le x : \omega(\#E(\mathbb{F}_p)) > \gamma \log_2 x\} \ge \frac{x}{(\log x)^{2+\gamma\log\gamma-\gamma+o(1)}}.$$

The same statement is true if instead $0 < \gamma < 1$ and the strict inequality is reversed on the left-hand side.

Our strategy in the case $\gamma > 1$ is as follows. As before, we write $\#E(\mathbb{F}_p) = \|\pi - 1\|$, where $\pi \equiv 1 \pmod{(1+i)^3}$ and $p = \pi\overline{\pi}$. Let k be an integer to be specified later and fix an ideal $\mathfrak{s} \in \mathbb{Z}[i]$ with the following properties:

(A) $((1+i)^3) \mid \mathfrak{s}$
(B) $\omega(\mathfrak{s}) = k$
(C) $P^+(\|\mathfrak{s}\|) \le x^{1/100\gamma\log_2 x}$
(D) Each prime ideal $\mathfrak{p} \mid \mathfrak{s}$ (with the exception of $(1+i)$) lies above a rational prime $p \equiv 1 \pmod 4$
(E) Distinct $\mathfrak{p}$ dividing $\mathfrak{s}$ lie above distinct p
(F) $\mathfrak{s}$ squarefree

Here $P^+(n)$ denotes the largest prime factor of n. Note that we have $\omega(\mathfrak{s}) = \omega(\|\mathfrak{s}\|)$. First, we will estimate from below the size of the set $\mathcal{M}_\mathfrak{s}$, defined to be the set of those $\pi \in \mathbb{Z}[i]$ with $\|\pi\| \le x$ satisfying the following properties:

(1) π prime (in $\mathbb{Z}[i]$)
(2) $\|\pi\|$ prime (in $\mathbb{Z}$)
(3) $\pi \equiv 1 \pmod{\mathfrak{s}}$
(4) $P^-\left(\frac{\|\pi-1\|}{\|\mathfrak{s}\|}\right) > x^{1/100\gamma \log_2 x}$.

Here $P^-(n)$ denotes the smallest prime factor of n. The conditions on the size of the prime factors of $\|\mathfrak{s}\|$ and $\|\pi - 1\|/\|\mathfrak{s}\|$ imply that each π with $\|\pi\| \leq x$ belongs to at most one of the sets $\mathcal{M}_\mathfrak{s}$. If k is chosen to be greater than $\gamma \log_2 x$, then carefully summing over $\mathfrak{s}$ satisfying the conditions above yields a lower bound on the count of distinct π corresponding to p with the property that $\omega(\#E(\mathbb{F}_p)) \geq k > \gamma \log_2 x$. The problem of counting elements π and $\overline{\pi}$ with $p = \pi\overline{\pi}$ is remedied by inserting a factor of $\frac{1}{2}$, which is of no concern for us.

More care is required in the case $0 < \gamma < 1$, which is handled in Section 4.3.

4.1. **Preparing for the proof of Theorem 4.1.** Suppose the fixed ideal $\mathfrak{s}$ is generated by $\sigma \in \mathbb{Z}[i]$. We will estimate from below the size of $\mathcal{M}_\mathfrak{s}$ using Theorem 2.1. Define $\mathcal{A}$ to be the sequence of elements of $\mathbb{Z}[i]$ of the form

$$\left\{\frac{\pi - 1}{\sigma} : \|\pi\| \leq x, \pi \text{ prime, and } \pi \equiv 1 \pmod{\sigma}\right\}.$$

Let $\mathcal{P}$ denote the set of prime ideals $\{\mathfrak{p} : \|\mathfrak{p}\| \leq z\}$, where $z := x^{1/50\gamma \log_2 x}$. Let $\mathfrak{P} := \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}$. If $\frac{\pi-1}{\sigma} \equiv 0 \pmod{\mathfrak{p}}$ implies $\|\mathfrak{p}\| \geq z$, then all primes $p \mid \|\frac{\pi-1}{\sigma}\|$ have $p > x^{1/100\gamma \log_2 x}$. Note also that if a prime $\pi \in \mathbb{Z}[i]$, $\|\pi\| \leq x$ is such that $\|\pi\|$ is not prime, then $\|\pi\| = p^2$ for some rational prime p, and so the count of such π is clearly $O(\sqrt{x})$. Therefore, we have

$$\#\mathcal{M}_\mathfrak{s} \geq S(\mathcal{A}, \mathcal{P}) + O(\sqrt{x}).$$

Lemma 4.2. *With $\mathcal{M}_\mathfrak{s}$ defined as above, we have*

$$\#\mathcal{M}_\mathfrak{s} \geq c \cdot \frac{\operatorname{Li}(x) \log_2 x}{\Phi(\mathfrak{s}) \log x} + O\Bigg(\sum_{\substack{\mathfrak{u}\mid\mathfrak{P} \\ \omega(\mathfrak{u})\leq m}} |r(\mathfrak{u}\mathfrak{s})|\Bigg) + O\left(\frac{1}{\Phi(\mathfrak{s})} \frac{\operatorname{Li}(x)}{(\log x)^{22}}\right) + O(\sqrt{x}),$$

where $r(\mathfrak{v}) = |\frac{\operatorname{Li}(x)}{\Phi(\mathfrak{v})} - \pi(x; \mathfrak{v}, 1)|$ and $c > 0$ is a constant.

Proof. First, note that we expect the size of $\mathcal{A}$ to be approximately $X := 4\frac{\operatorname{Li}(x)}{\Phi(\mathfrak{s})}$. Write $A_\mathfrak{u} = \#\{a \in \mathcal{A} : \mathfrak{u} \mid a\}$. Then

$$A_\mathfrak{u} = X\delta(\mathfrak{u}) + r(\mathfrak{u}\mathfrak{s}),$$

where $\delta(\mathfrak{u}) = \frac{\Phi(\mathfrak{s})}{\Phi(\mathfrak{u}\mathfrak{s})}$ and $r(\mathfrak{u}\mathfrak{s}) = |4\frac{\operatorname{Li}(x)}{\Phi(\mathfrak{u}\mathfrak{s})} - \pi(x; \mathfrak{u}\mathfrak{s}, 1)|$. By Theorem 2.1, for any even integer $m \geq 0$ we have

$$S(\mathcal{A}, \mathcal{P}) = 4\frac{\operatorname{Li}(x)}{\Phi(\mathfrak{s})} \prod_{\|\mathfrak{p}\|\leq z} \left(1 - \frac{\Phi(\mathfrak{s})}{\Phi(\mathfrak{p}\mathfrak{s})}\right) + O\Bigg(\sum_{\substack{\mathfrak{u}\mid\mathfrak{P} \\ \omega(\mathfrak{u})\leq m}} |r(\mathfrak{u}\mathfrak{s})|\Bigg)$$
$$+ O\Bigg(\frac{\operatorname{Li}(x)}{\Phi(\mathfrak{s})} \sum_{\substack{\mathfrak{u}\mid\mathfrak{P} \\ \omega(\mathfrak{u})\geq m}} \delta(\mathfrak{u})\Bigg).$$

Using Proposition 2.3, we have

$$\prod_{\|\mathfrak{p}\|\le z}\left(1-\frac{\Phi(\mathfrak{s})}{\Phi(\mathfrak{p}\mathfrak{s})}\right)=\prod_{\substack{\|\mathfrak{p}\|\le z\\ \mathfrak{p}\nmid\mathfrak{s}}}\left(1-\frac{1}{\Phi(\mathfrak{p})}\right)\prod_{\substack{\|\mathfrak{p}\|\le z\\ \mathfrak{p}\mid\mathfrak{s}}}\left(1-\frac{1}{\|\mathfrak{p}\|}\right)$$
$$=\prod_{\|\mathfrak{p}\|\le z}\left(1-\frac{1}{\|\mathfrak{p}\|}\right)\prod_{\substack{\|\mathfrak{p}\|\le z\\ \mathfrak{p}\nmid\mathfrak{s}}}\left(1-\frac{1}{(\|\mathfrak{p}\|-1)^2}\right)$$
$$\gg\frac{1}{\log z}=\frac{\log_2 x}{\log x}.$$

Take $m=14\lfloor\log_2 x\rfloor$. We leave aside the first O-term and concentrate for now on the second. This term is handled in essentially the same way as in the proof of the upper bound: The sum in the this term is bounded from above by

$$\sum_{s\ge m}\frac{1}{s!}\Big(\sum_{\|\mathfrak{p}\|\le z}\delta(\mathfrak{p})\Big)^s.$$

By Proposition 2.3, we have

$$\sum_{\|\mathfrak{p}\|\le z}\delta(\mathfrak{p})\le\log_2 x+O(1).$$

Now, one sees once again by the ratio test that the sum on s is

$$\ll\frac{1}{m!}\Big(\sum_{\|\mathfrak{p}\|\le z}\delta(\mathfrak{p})\Big)^m\le\frac{1}{m!}(\log_2 x+O(1))^m.$$

Thus, by the same calculations as in the proof of Theorem 3.1, the second O-term is

$$\ll\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{s})(\log x)^{22}},$$

completing the proof of the lemma. $\square$

We now sum this estimate over σ in an appropriate range to deal with the O-terms and establish a lower bound. Here, the cases $\gamma>1$ and $0<\gamma<1$ diverge.

4.2. **The case $\gamma>1$.** The argument in this case is somewhat simpler. Recall that $\mathfrak{s}$ is chosen to satisfy properties A through F listed below Theorem 4.1; in particular, $\omega(\mathfrak{s})=k$ for some integer k and $P^+(\|\mathfrak{s}\|)\le x^{1/100\gamma\log_2 x}$. Choose $k:=\lfloor\gamma\log_2 x\rfloor+2$. Since $\omega(\|\mathfrak{s}\|)=\omega(\mathfrak{s})$, we have that $\|\mathfrak{s}\|\le x^{k/100\gamma\log_2 x}\le x^{1/10}$. A lower bound follows by estimating the quantity

$$\mathcal{M}=\sum_{\mathfrak{s}}{}'\,\#\mathcal{M}_{\mathfrak{s}},$$

where the prime indicates a restriction to those ideals $\mathfrak{s}\subset\mathbb{Z}[i]$ satisfying properties A through F mentioned above.

Lemma 4.3. *We have*

$$\mathcal{M}\gg\frac{x\log_2 x(\log_2 x+O(\log_3 x))^k}{k!(\log x)^2}.$$

Proof. Since $\sum_{\|\mathfrak{s}\|\le x}1/\Phi(\mathfrak{s})\ll\log x$, the second O-term in Lemma 4.2 is, upon summing on $\mathfrak{s}$, bounded by a constant times $\mathrm{Li}(x)/(\log x)^{21}$. The third error term, $O(\sqrt{x})$, is therefore safely absorbed by this term.

We now handle the sum over $\mathfrak{s}$ of the first O-term. We have $|r(\mathfrak{u}\mathfrak{s})| = |\pi(x;\mathfrak{u}\mathfrak{s},1) - 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{u}\mathfrak{s})}|$. We can think of the double sum (over $\mathfrak{s}$ and $\mathfrak{u}$) as a single sum over a modulus $\mathfrak{q}$, inserting a factor of $\tau(\mathfrak{q})$ to account for the number of ways of writing $\mathfrak{q}$ as a product of two ideals in $\mathbb{Z}[i]$. (Here, $\tau(\mathfrak{q})$ is the number of ideals in $\mathbb{Z}[i]$ which divide $\mathfrak{q}$.) Recalling our choice of $m = 14\lfloor \log_2 x \rfloor$, we have

$$\sum_{\|\mathfrak{s}\| \le x^{1/10}} \sum_{\substack{\mathfrak{u}|\mathfrak{P} \\ \omega(\mathfrak{u}) \le m}} |r(\mathfrak{u}\mathfrak{s})| \ll \sum_{\|\mathfrak{q}\| < x^{2/5}} \left| \pi(x;\mathfrak{q},1) - \frac{\mathrm{Li}(x)}{\Phi(\mathfrak{q})} \right| \cdot \tau(\mathfrak{q}).$$

The restriction $\|\mathfrak{q}\| \le x^{2/5}$ comes from $\|\mathfrak{s}\| \le x^{1/10}$ and $\|\mathfrak{u}\| \le x^{m/50\gamma \log_2 x} \le x^{.28}$, recalling $m = 14\lfloor \log_2 x \rfloor$ and $\gamma > 1$. Now, for all $y > 0$ and nonzero $\mathfrak{i} \subset \mathbb{Z}[i]$ we have $\pi(y;\mathfrak{i},1) \ll y/\|\mathfrak{i}\|$; indeed, the same inequality is true with $\pi(y;\mathfrak{i},1)$ replaced by the count of all proper ideals $\equiv 1 \pmod{\mathfrak{i}}$. Thus

$$\left| \pi(x;\mathfrak{q},1) - 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{q})} \right| \ll \frac{x}{\Phi(\mathfrak{q})}.$$

Using this together with the Cauchy-Schwarz inequality and Proposition 2.2, we see that, for any $A > 0$,

$$\begin{aligned} \sum_{\|\mathfrak{q}\| < x^{2/5}} |\pi(x;\mathfrak{q},1) - 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{q})}| \tau(\mathfrak{q}) &\ll \sum_{\|\mathfrak{q}\| < x^{2/5}} |\pi(x;\mathfrak{q},1) - 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{q})}|^{1/2} \Big(\frac{x}{\Phi(\mathfrak{q})} \Big)^{1/2} \tau(\mathfrak{q}) \\ &\ll \Big(x \sum_{\|\mathfrak{q}\| < x^{2/5}} \frac{\tau(\mathfrak{q})^2}{\Phi(\mathfrak{q})} \Big)^{1/2} \Big(\frac{x}{(\log x)^A} \Big)^{1/2}. \end{aligned}$$

We can estimate this sum using an Euler product:

$$\begin{aligned} \sum_{\|\mathfrak{q}\| < x^{2/5}} \frac{\tau(\mathfrak{q})^2}{\Phi(\mathfrak{q})} &\ll \prod_{\|\mathfrak{p}\| \le x^{2/5}} \Big(1 + \frac{4}{\|\mathfrak{p}\|} \Big) \\ &\le \exp\Big\{ \sum_{\|\mathfrak{p}\| \le x^{2/5}} \frac{4}{\|\mathfrak{p}\|} \Big\} \ll (\log x)^4. \end{aligned}$$

Collecting our estimates, we see that the total error is at most $x/(\log x)^{A/2-2}$, which is acceptable if A is chosen large enough.

For the main term, we need a lower bound for the sum

$$\mathcal{M} = \sum_{\mathfrak{s}}{}' \frac{1}{\Phi(\mathfrak{s})}. \tag{7}$$

Let $I = (e^{(\log_2 x)^2/k}, x^{1/10k})$. Define a collection of prime ideals $\mathcal{P}$ such that each $\mathfrak{p} \in \mathcal{P}$ lies above a prime $p \equiv 1 \pmod 4$, each prime $p \equiv 1 \pmod 4$ has exactly one prime ideal lying above it in $\mathcal{P}$, and $\|\mathfrak{p}\| \in I$. We apply Lemma 2.4, with the y_i chosen to be of the form $1/\Phi(\mathfrak{p})$ with $\mathfrak{p} \in \mathcal{P}$, obtaining

$$\begin{aligned} &\frac{1}{\Phi((1+i)^3)} \sum_{\mathfrak{s}:\mathfrak{p}|(\mathfrak{s}/(1+i)^3) \implies \mathfrak{p} \in \mathcal{P}}{}' \frac{1}{\Phi(\mathfrak{s}/(1+i)^3)} \\ &\gg \frac{1}{(k-1)!} \Bigg(\sum_{\mathfrak{p} \in \mathcal{P}} \frac{1}{\Phi(\mathfrak{p})} \Bigg)^{k-1} \Bigg(1 - \binom{k-1}{2} \Big(\frac{1}{S_1^2} \Big) \sum_{\mathfrak{p} \in \mathcal{P}} \frac{1}{\Phi(\mathfrak{p})^2} \Bigg), \end{aligned} \tag{8}$$

where

$$S_1 = \sum_{\mathfrak{p}\in\mathcal{P}} \frac{1}{\Phi(\mathfrak{p})}.$$

By Theorem 2.3, $S_1 = \frac{1}{2}\log_2 x - 2\log_3 x + O(1)$. This introduces a factor of $\frac{1}{2^{k-1}}$ to the right-hand side of (8), but this is of no concern: If each of the k prime factors of $\mathfrak{s}$, excluding $(1+i)$, lies above a distinct prime $p \equiv 1 \pmod 4$, then there are 2^{k-1} such ideals $\mathfrak{s}$ of a given norm. Thus, if we extend the sum on the left-hand side of (8) to range over all $\mathfrak{s}$ counted in primed sums (cf. the discussion above Lemma 4.3), we obtain

$$\begin{aligned}\sum_{\mathfrak{s}}{}' \frac{1}{\Phi(\mathfrak{s})} \geq \frac{2^{k-1}}{(k-1)!}&\left(\frac{1}{2}\log_2 x - 2\log_3 x + O(1)\right)^{k-1} \\ &\times \left(1 - \binom{k-1}{2}\left(\frac{1}{S_1^2}\right)\sum_{\mathfrak{p}\in\mathcal{P}}\frac{1}{\Phi(\mathfrak{p})^2}\right).\end{aligned}$$

The quantity $\binom{k-1}{2}$ is bounded from above by $\lceil\gamma\log_2 x\rceil^2$, and the sum on $1/\Phi(\mathfrak{p})^2$ tends to 0 as $x \to \infty$. Therefore,

$$1 - \binom{k-1}{2}\left(\frac{1}{S_1^2}\right)\sum_{\mathfrak{p}\in\mathcal{P}}\frac{1}{\Phi(\mathfrak{p})^2} \geq 1 - 4\gamma^2\sum_{\mathfrak{p}\in\mathcal{P}}\frac{1}{\Phi(\mathfrak{p})^2} \geq \frac{1}{2}$$

for large enough x, and so

$$\frac{x\log_2 x}{(\log x)^2}\sum_{\mathfrak{s}}{}'\frac{1}{\Phi(\mathfrak{s})} \gg \frac{x\log_2 x(\log_2 x + O(\log_3 x))^{k-1}}{(k-1)!(\log x)^2},$$

as desired. □

With $k = \lfloor\gamma\log_2 x\rfloor + 2$ and by the more precise version of Stirling's formula $n! \sim \sqrt{2\pi n}(n/e)^n$, we have

$$\begin{aligned}\frac{(\log_2 x + O(\log_3 x))^{k-1}}{(k-1)!} &\gg \frac{1}{\sqrt{\log_2 x}}\left(\frac{e\log_2 x + O(\log_3 x)}{\lfloor\gamma\log_2 x\rfloor}\right)^{\lceil\gamma\log_2 x\rceil} \\ &= \frac{1}{\sqrt{\log_2 x}}\left(\frac{e}{\gamma}\left(1 + O\left(\frac{\log_3 x}{\log_2 x}\right)\right)\right)^{\lceil\gamma\log_2 x\rceil} \\ &= (\log x)^{\gamma - \gamma\log\gamma + o(1)}.\end{aligned}$$

This yields a main term of the shape

$$\frac{x}{(\log x)^{2+\gamma\log\gamma - \gamma + o(1)}},$$

which completes the proof of Theorem 4.1 in the case $\gamma > 1$.

4.3. **The case $\mathbf{0} < \gamma < \mathbf{1}$.** Above, we used the fact that if $\pi - 1$ is divisible by certain $\mathfrak{s} \subset \mathbb{Z}[i]$ with $\omega(\|\mathfrak{s}\|) = k$, then $\|\pi - 1\|$ will have at least $k > \gamma\log_2 x$ prime factors. The case $0 < \gamma < 1$ is requires more care: We need to ensure that the quantity $\|\pi - 1\|/\|\mathfrak{s}\|$ does not have too many prime factors.

Lemma 4.4. *For any $\mathfrak{s} \subset \mathbb{Z}[i]$ satisfying properties A through F listed below Theorem 4.1, we have*

$$\#\{\pi \in \mathcal{M}_{\mathfrak{s}} : \omega\left(\frac{\|\pi - 1\|}{\|\mathfrak{s}\|}\right) > \frac{\log_2 x}{\log_4 x}\} \ll \frac{x}{\|\mathfrak{s}\|(\log x)^A}.$$

Upon discarding those π counted by the above lemma, the remaining π will have the property that $\omega(\|\pi-1\|) \in [k, k+\log_2 x/\log_4 x]$. Choosing k to be the greatest integer strictly less than $\gamma \log_2 x - \log_2 x/\log_4 x$ ensures that $\|\pi - 1\| < \gamma \log_2 x$.

Proof of Lemma 4.4. We begin with the observation that, for any $\mathfrak{s} \subset \mathbb{Z}[i]$ under consideration and $\pi \in \mathcal{M}_{\mathfrak{s}}$, we have $\|\pi-1\|/\|\mathfrak{s}\| \le 2x/\|\mathfrak{s}\|$. Therefore, we estimate

$$\sum_{\substack{\|\mathfrak{a}\| \le \frac{2x}{\|\mathfrak{s}\|} \\ \omega(\|\mathfrak{a}\|) > \log_2 x/\log_4 x \\ P^-(\|\mathfrak{a}\|) > x^{1/100\gamma \log_2 x}}} 1 \le \frac{2x}{\|\mathfrak{s}\|} \sum_{\substack{\|\mathfrak{a}\| \le \frac{2x}{\|\mathfrak{s}\|} \\ \omega(\|\mathfrak{a}\|) > \log_2 x/\log_4 x \\ P^-(\|\mathfrak{a}\|) > x^{1/100\gamma \log_2 x}}} \frac{1}{\|\mathfrak{a}\|}.$$

Noting that $\omega(\|\mathfrak{a}\|) \le \omega(\mathfrak{a})$ for any $\mathfrak{a} \subset \mathbb{Z}[i]$, by Theorem 2.3 and Stirling's formula, we have

$$\begin{aligned}
\sum_{\substack{\|\mathfrak{a}\| \le \frac{2x}{\|\mathfrak{s}\|} \\ \omega(\|\mathfrak{a}\|) > \log_2 x/\log_4 x \\ P^-(\|\mathfrak{a}\|) > x^{1/100 \log_2 x}}} \frac{1}{\|\mathfrak{a}\|} &\le \sum_{\substack{\|\mathfrak{a}\| \le \frac{2x}{\|\mathfrak{s}\|} \\ \omega(\mathfrak{a}) > \log_2 x/\log_4 x \\ P^-(\|\mathfrak{a}\|) > x^{1/100 \log_2 x}}} \frac{1}{\|\mathfrak{a}\|} \\
&\le \sum_{\ell > \log_2 x/\log_4 x} \frac{1}{\ell!} \Big(\sum_{x^{1/100 \log_2 x} \le \|\mathfrak{p}\| \le \frac{2x}{\|\mathfrak{s}\|}} \sum_{m=1}^{\infty} \frac{1}{\|\mathfrak{p}\|^m} \Big)^{\ell} \\
&\ll \sum_{\ell > \log_2 x/\log_4 x} \Big(\frac{e \log_3 x + O(1)}{\ell} \Big)^{\ell}.
\end{aligned}$$

For each $\ell > \log_2 x/\log_4 x$, we have $(e\log_3 x + O(1))/\ell < 1/2$. Thus

$$\begin{aligned}
\sum_{\ell > \log_2 x/\log_4 x} \Big(\frac{e \log_3 x + O(1)}{\ell} \Big)^{\ell} &\ll \Big(\frac{e\log_3 x + O(1)}{\lfloor \log_2 x/\log_4 x \rfloor + 1} \Big)^{\lfloor \log_2 x/\log_4 x \rfloor + 1} \\
&\ll \Big(\frac{1}{(\log_2 x)^{1+o(1)}} \Big)^{\log_2 x/\log_4 x} \ll e^{-2\log_2 x \log_3 x/\log_4 x}.
\end{aligned}$$

This last expression is smaller than $(\log x)^{-A}$, for any $A > 0$. Therefore, for any fixed $A > 0$,

$$\#\{\pi \in \mathcal{M}_{\mathfrak{s}} : \omega\Big(\frac{\|\pi-1\|}{\|\mathfrak{s}\|}\Big) > \frac{\log_2 x}{\log_4 x}\} \ll \frac{x}{\|\mathfrak{s}\|(\log x)^A}. \qquad \square$$

Write

$$\mathcal{M}'_{\mathfrak{s}} = \{\pi \in \mathcal{M}_{\mathfrak{s}} : \omega\Big(\frac{\|\pi-1\|}{\|\mathfrak{s}\|}\Big) \le \frac{\log_2 x}{\log_4 x}\}.$$

Lemmas 4.2 and 4.4 show that $\#\mathcal{M}'_{\mathfrak{s}}$ satisfies

$$\begin{aligned}
\#\mathcal{M}'_{\mathfrak{s}} \ge c \cdot \frac{x \log_2 x}{\Phi(\mathfrak{s})(\log x)^2} &+ O\Big(\sum_{\substack{\mathfrak{u} \mid \mathfrak{P} \\ \omega(\mathfrak{u}) \le m}} |r(\mathfrak{u}\mathfrak{s})| \Big) \\
&+ O\Big(\frac{1}{\Phi(\mathfrak{s})} \frac{\mathrm{Li}(x)}{(\log x)^{22}} \Big) + O\Big(\frac{x}{\|\mathfrak{s}\|(\log x)^A} \Big) + O(\sqrt{x}),
\end{aligned}$$

for any $A > 0$. Here, all quantities are defined as in the previous section. Just as before, we sum this quantity over $\mathfrak{s} \subset \mathbb{Z}[i]$ satisfying conditions A through F listed below Theorem 4.1. Letting $'$ on a sum indicate a restriction to such $\mathfrak{s}$, we have, by the same calculations as before,

$$\mathcal{M}' \gg \frac{x \log_2 x (\log_2 x + O(\log_3 x))^{k-1}}{(k-1)!(\log x)^2},$$

where
$$\mathcal{M}' = \sum_{\mathfrak{s}}{}' \#\mathcal{M}'_{\mathfrak{s}}.$$
Recall that k is chosen to be the largest integer strictly less than $\gamma \log_2 x - \log_2 x/\log_4 x$; then by Stirling's formula,
$$\begin{aligned}\frac{(\log_2 x + O(\log_3 x))^{k-1}}{(k-1)!} &\gg \frac{1}{\sqrt{\log_2 x}}\Big(\frac{e\log_2 x + O(\log_3 x)}{k-1}\Big)^{k-1}\\ &\gg \frac{1}{\sqrt{\log_2 x}}\Big(\frac{e}{\gamma}\Big(1+O\big(\frac{1}{\log_4 x}\big)\Big)\Big)^{\gamma\log_2 x - \log_2 x/\log_4 x - 1}\\ &\gg (\log x)^{\gamma\log\gamma - \gamma + o(1)}.\end{aligned}$$
A final assembly of estimates yields Theorem 4.1 in the case $0 < \gamma < 1$.

References

[Coj05] A. C. Cojocaru, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. **119** (2005), no. 3, 265–289.

[dB66] N. G. de Bruijn, *On the number of positive integers $\leq x$ and free of prime factors $> y$. II*, Indag. Math. **28** (1966), 239 – 247.

[EN79] P. Erdős and J-L. Nicolas, *Sur la fonction nombre de facteurs premiers de n*, Séminaire Delange-Pisot-Poitou. Théorie des nombres **20** (1978-1979), no. 2, 1–19.

[HR83] H. Halberstam and K. F. Roth, *Sequences*, second ed., Springer-Verlag, New York-Berlin, 1983.

[Hux71] M. N. Huxley, *The large sieve inequality for algebraic number fields. III. Zero-density results*, J. London Math. Soc. (2) **3** (1971), 233–240.

[HW00] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, fifth ed., Oxford University Press, Oxford, 2000.

[JU08] J. Jiménez Urroz, *Almost prime orders of CM elliptic curves modulo p*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 74–87.

[Liu06] Y-R. Liu, *Prime analogues of the Erdős-Kac theorem for elliptic curves*, J. Number Theory **119** (2006), no. 2, 155–170.

[Pol09] P. Pollack, *Not always buried deep*, American Mathematical Society, Providence, RI, 2009.

[Polar] ———, *A Titchmarsh divisor problem for elliptic curves*, Math. Proc. Cambridge Philos. Soc. (to appear).

[Ros99] M. Rosen, *A generalization of Mertens' theorem*, J. Ramanujan Math. Soc. **14** (1999), no. 1, 1–19.

Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30602, USA

E-mail address: ltroupe@math.uga.edu