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

LEE TROUPE

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

\[
\#\{p \leq x : \omega(\#E(F_p)) > \gamma \log \log x\} = \frac{x}{(\log x)^2 + \gamma \log \gamma - \gamma + o(1)}.
\]

The same result holds for the quantity \#\{p \leq x : \omega(\#E(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

\[E(F_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}\]

where \(d_p\) and \(e_p\) are uniquely determined natural numbers such that \(d_p\) divides \(e_p\). Thus, \(\#E(F_p) = d_pe_p\). We concern ourselves with the behavior of \(\omega(\#E(F_p))\), 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 \(\omega(\#E(F_p))\) 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

\[\frac{\omega(\#E(F_p)) - \log \log p}{\sqrt{\log \log p}}\]

has a Gaussian normal distribution. In particular, \(\omega(\#E(F_p))\) 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 \(\omega(\#E(F_p))\), 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,

\[
\#\{p \leq x : \omega(\#E(F_p)) > \gamma \log \log x\} = \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}}.
\]

The same result holds for the quantity \#\{p \leq x : \omega(\#E(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 \( a \subset \mathbb{Z}_K \), we write \( \|a\| \) for the norm of \( a \) (that is, \( \|a\| = \#(\mathbb{Z}_K/a) \) and \( \Phi(a) = \#(\mathbb{Z}_K/a)^x \). The function \( \omega \) applied to an ideal \( a \subset \mathbb{Z}_K \) will denote the number of distinct prime ideals appearing in the factorization of \( a \) into a product of prime ideals. For \( \alpha \in \mathbb{Z}_K \), \( \|\alpha\| \) and \( \Phi(\alpha) \) denote those functions evaluated at the ideal \( (\alpha) \). If \( \alpha \) is invertible modulo an ideal \( u \subset \mathbb{Z}_K \), we write \( \gcd(\alpha, u) = 1 \). The notation \( \log_k x \) will be used to denote the \( k \)th 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
\[
S(\mathcal{A}, \mathcal{P}) := \# \{ a \in \mathcal{A} : \gcd(a, \mathfrak{P}) = 1 \}, \quad \text{where } \mathfrak{P} := \prod_{p \in \mathcal{P}} p.
\]

For an ideal \( u \subset \mathbb{Z}_K \), write \( A_u := \# \{ a \in \mathcal{A} : a \equiv 0 \pmod{u} \} \). Let \( X \) denote an approximation to the size of \( \mathcal{A} \). Suppose \( \delta \) is a multiplicative function taking values in \([0,1]\), and define a function \( r(u) \) such that
\[
A_u = X \delta(u) + r(u)
\]
for each \( u \) dividing \( \mathfrak{P} \). Then, for every even \( m \in \mathbb{Z}^+ \),
\[
S(\mathcal{A}, \mathcal{P}) = X \prod_{p \in \mathcal{P}} (1 - \delta(p)) + O \left( \sum_{u \mid \mathfrak{P}, \omega(u) \leq m} |r(u)| \right) + O \left( X \sum_{u \mid \mathfrak{P}, \omega(u) \geq m} \delta(u) \right).
\]

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 \( q \subset \mathbb{Z}_K \), write
\[
\pi(x; q, \alpha) = \# \{ \mu \in \mathbb{Z}_K : \|\mu\| \leq x, \mu \equiv \alpha \pmod{q} \}.
\]
Proposition 2.2. For every $A > 0$, there is a $B > 0$ so that
\[
\sum_{\|q\| \leq x^{1/2}(\log x)^{-\epsilon}} \max_{\gcd(\alpha, u) = 1} \max_{y \leq x} |\pi(y; q, \alpha) - w_K \cdot \text{Li}(y) / \Phi(q)| \ll \frac{x}{(\log x)^A},
\]
where the above sum and maximum are taken over $q \in \mathbb{Z}_K$ 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 $\alpha_K$ denote the residue of the associated Dedekind zeta function, $\zeta_K(s)$, at $s = 1$. Then
\[
\prod_{\|p\| \leq x} \left(1 - \frac{1}{\|p\|}\right)^{-1} \sim e^{\gamma} \alpha_K \log x,
\]
where the product is over all prime ideals $p$ in $\mathbb{Z}_K$. Here (and only here), $\gamma$ is the Euler-Mascheroni constant.

Note also that the “additive version” of Mertens’ theorem, i.e.,
\[
\sum_{\|p\| \leq x} \frac{1}{\|p\|} = \log_2 x + B_K + O_K \left(\frac{1}{\log x}\right)
\]
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 $\sigma_d$ is the $d$th elementary symmetric function of the $y_k$’s. Then, for each $d$, we have
\[
\sigma_d \geq \frac{1}{d!} \sigma_1^d \left(1 - \frac{1}{2} \sigma_1 \sum_{k=1}^{M} y_k^2\right).
\]

3. An upper bound

Theorem 3.1. Let $E$ be the elliptic curve $E: y^2 = x^3 - x$ and fix $\gamma > 1$. Then
\[
\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log_2 x\} \ll \frac{x(\log_2 x)^5}{(\log x)^{2+\gamma \log \gamma - \gamma}}.
\]
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
\[
\#E(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi}) = (\pi - 1)(\overline{\pi} - 1),
\]
where $\pi \in \mathbb{Z}[i]$ is chosen so that $p = \pi \overline{\pi}$ and $p \equiv 1 \pmod{(1+i)^3}$. (Such $\pi$ are sometimes called primary.) This determines $\pi$ 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) \( P(n)^2 \mid n \).

Then, for any \( A > 0 \), the size of \( \mathcal{X} \) is \( O(x/(\log x)^4) \).

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

\[
\Psi(x, y) \leq x/u^{\gamma + o(u)}.
\]

**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 \( O(x/(\log x)^4) \) for any \( A > 0 \), noting that \((\log x)^A \ll (\log x)^{\log_2 x} = (\log_2 x)^{\log_2 x} \). 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 \( O(x/(\log x)^4) \). \( \square \)

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 [11], \( b = \| \pi - 1 \| \), 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 \( \chi \) is the nontrivial character modulo 4. Now, using the Cauchy-Schwarz inequality and Lemma 3.2,

\[
4 \sum_{b \in \mathcal{X}} \sum_{d|b} \chi(d) \leq 4 \sum_{b \in \mathcal{X}} \tau(b) \leq 4 \left( \sum_{b \in \mathcal{X}} 1 \right)^{1/2} \left( \sum_{b \in \mathcal{X}} \tau(b)^2 \right)^{1/2}
\]

\[
\ll \left( \frac{x}{(\log x)^A} \right)^{1/2} \left( x \log^3 x \right)^{1/2} = \frac{x}{(\log x)^{A/2 - 3/2}}.
\]

Since \( A > 0 \) can be chosen arbitrarily, this completes the proof. \( \square \)

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 \( \gamma > 1 \),

\[
\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log \log x\} = \sum_{k > \gamma \log_2 x} N_k + O\left( \frac{x}{(\log x)^A} \right)
\]

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
\[
N_k \leq \sum_{\substack{a \leq x^{1-1/6 \log x} \\
\omega(a) = k-1}} \sum_{\substack{p \leq x \\
p \equiv 1 \pmod{4} \\
a \mid \#E(\mathbb{F}_p) \mid \#E(\mathbb{F}_p) / a \text{ prime}}} 1.
\]

To handle the inner sum, we need information on the integer divisors of $\#E(\mathbb{F}_p)$, where $p \leq x$ 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
\[
\sum_{\substack{a \leq x^{1-1/6 \log x} \\
\omega(a) = k-1}} \sum_{\substack{p \leq x \\
p \equiv 1 \pmod{4} \\
a \mid \#E(\mathbb{F}_p) \mid \#E(\mathbb{F}_p) / a \text{ prime}}} 1 = \frac{1}{2} \sum_{\substack{a \leq x^{1-1/6 \log x} \\
\omega(a) = k-1}} \sum_{\substack{\pi \leq x \\
\pi \equiv 1 \pmod{1+i^3} \\
a \mid \|\pi - 1\| \mid \|\pi - 1\| / a \text{ prime}}} 1,
\]

where the $'$ on the sum indicates a restriction to primes $\pi$ 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 $a = \prod q^v_q$, with each $q$ prime. For each $q \mid a$ with $q \equiv 1 \pmod{4}$, write $q = n_q \overline{n}_q$. Define a set $S_a$ which consists of all products $\alpha$ of the form
\[
\alpha = (1+i)^{v_2} \prod_{q \equiv 3 \pmod{4}} q^{[v_q/2]} \prod_{q \equiv 1 \pmod{4}} \alpha_q,
\]
where $\alpha_q \in \{n_q \overline{n}_q^{-i} : i = 0, 1, \ldots, v_q\}$.

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

Now, for any $\alpha \in S_a$, we have
\[
\frac{\alpha \overline{\alpha}}{a} = \prod_{q \equiv 3 \pmod{4}} q^{2[v_q/2]-v_q}.
\]

Observe that
\[
\frac{\|\pi - 1\|}{a} = \frac{(\pi - 1)(\overline{\pi - 1})}{\alpha \overline{\alpha}} \prod_{q \equiv 3 \pmod{4}} q^{2[v_q/2]-v_q}.
\]

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

\[
\sum_{a \leq x^{1/6} \log x} \sum_{\omega(a) = k-1} \sum'_{\pi : \|\pi\| \leq x} 1 = O\left(\frac{x}{\log^A x}\right),
\]

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

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

\[
\sum_{\omega(a) = k-1} \sum'_{\pi : \|\pi\| \leq x} 1 \leq 4 \sum_{a \leq x^{1/6} \log x} |S_a|.
\]

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

\[
\ll \sum_{a \leq x^{1/6} \log x} \tau(a) \ll x^{1/16} \log x (\log x),
\]

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

\[
\sum'_{\pi : \|\pi\| \leq x} 1 \ll \frac{x \log^2 x \|a\|}{\|\alpha\| (\log x)^2}
\]

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 \(\|\beta\| \leq \frac{2\pi}{\|\alpha\|}\). Let \(\mathcal{A}\) denote the sequence of elements in \(\mathbb{Z}[i]\) given by

\[
\left\{ \beta(1 + \alpha \beta) : \|\beta\| \leq \frac{2x}{\|\alpha\|} \right\}.
\]

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

\[
\sum'_{\pi : \|\pi\| \leq x} 1 \leq S(\mathcal{A}, \mathcal{P}) + O(z).
\]

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

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

\[
A_u = \frac{2\pi x \nu(u)}{\|\alpha\| \|u\|} + O\left(\nu(u) \frac{x}{\|\alpha\| \|u\|^{1/2}}\right),
\]
where
\[ \nu(u) = \#\{ \beta \pmod{u} : \beta(1 + \alpha\beta) \equiv 0 \pmod{u} \}. \]

We apply Theorem 2.1 with
\[ X = \frac{2\pi x}{\|\alpha\|} \quad \text{and} \quad \delta(u) = \frac{\nu(u)}{\|u\|}. \]

With these choices, we have
\[ r(u) = O\left(\frac{\sqrt{x}}{(\|\alpha\||\|u\|)^{1/2}}\right). \]

Then, for any even integer \( m \geq 0 \),
\[ S(A, \mathcal{P}) = 2\pi x \frac{\prod_{\|p\| \leq z} \left(1 - \frac{\nu(p)}{\|p\|}\right)}{\|\alpha\|} \prod_{\|p\| \leq z} \left(1 - \frac{1}{\|p\|}\right) \]
\[ \leq \prod_{\|p\| \leq z} \left(1 - \frac{1}{\|p\|}\right)^2 \prod_{\|p\| \leq z} \left(1 - \frac{1}{\|p\|}\right)^{-1} \ll \frac{1}{(\log z)^{2} \Phi(\alpha)}, \]

where \( \Psi = \prod_{p \in \mathcal{P}} p \).

For a prime \( p \), we have \( \nu(p) = 2 \) if \( \alpha \not\equiv 0 \pmod{p} \) and \( \nu(p) = 1 \) otherwise. Therefore, the product in the first term is
\[ \prod_{\|p\| \leq z} \left(1 - \frac{2}{\|p\|}\right) \prod_{\|p\| \leq z} \left(1 - \frac{1}{\|p\|}\right) \]
\[ \leq \prod_{\|p\| \leq z} \left(1 - \frac{1}{\|p\|}\right)^2 \prod_{\|p\| \leq z} \left(1 - \frac{1}{\|p\|}\right)^{-1} \ll \frac{1}{(\log z)^{2} \Phi(\alpha)}, \]

where in the last step we used Proposition 2.3.

Choose \( z = x^{200(\log_2 x)^2} \). 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 \( \nu(u)/\|u\|^{1/2} \ll 1 \).

Then, taking \( m = 10 \log_2 x \), we have
\[ \sum_{u \in \Psi} \sum_{\omega(u) \leq m} \frac{\nu(u)}{\|u\|^{1/2}} \ll \sum_{k=0}^{m} \left(\pi_K(z)\right)^k \leq \sum_{k=0}^{m} \pi_K(z)^k \leq 2\pi_K(z)^m \leq x^{1/20 \log_2 x}, \]

where \( \pi_K(z) \) denotes the number of prime ideals \( p \subset \mathbb{Z}[i] \) with norm up to \( z \). Therefore, the inequality
\[ \frac{x(\log_2 x)^5}{\|\alpha\|(\log x)^2} \gg \frac{x^{1/2 + 1/20 \log_2 x}}{\|\alpha\|^{1/2}} \]

must be satisfied.
holds for all \( \alpha \) 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

\[
\sum_{u|p, \omega(u) \geq m} \delta(u) \leq \sum_{s \geq m} \frac{1}{s!} \left( \sum_{\|p\| \leq z} \frac{\nu(p)}{\|p\|} \right)^s.
\]

Observe that, by Proposition 2.3, we have

\[
\sum_{\|p\| \leq z} \frac{\nu(p)}{\|p\|} \leq 2 \log_2 x + O(1).
\]

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

\[
\frac{1}{m!} (2 \log_2 x + O(1))^m \leq \left( \frac{2e \log_2 x + O(1)}{10 \log_2 x} \right)^{10 \log_2 x} \ll \left( \frac{e}{5} \right)^{9 \log_2 x} \leq \frac{1}{(\log x)^5}.
\]

So the second \( O \)-term is

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

and this is certainly dominated by the main term.

\[\square\]

From Lemmas 3.6 and 5.7, we see (2) can be rewritten

\[N_k \ll \frac{x \log_2 x}{(\log x)^2} \sum_{a \leq x^{1-1/6 \log_2 x}, \omega(a) = k-1} \frac{|S_a|}{a} + O\left( \frac{x}{\log^A x} \right),
\]

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

\[
\sum_{a \leq x^{1-1/6 \log_2 x}, \omega(a) = k-1} \frac{|S_a|}{a} \leq \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!}.
\]

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

\[5\]

\[
\sum_{a \leq x, \omega(a) = k-1} \frac{|S_a|}{a} \leq \frac{1}{(k-1)!} \left( \sum_{p^k \leq x, p \equiv 3 (\mod 4)} \frac{|S_{p^k}|}{p^k} + \sum_{p^k \leq x, p \equiv 3 (\mod 4)} \frac{|S_{p^{2k}}|}{p^{2k}} + O(1) \right)^{k-1}.
\]

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

\[6\]

\[
\sum_{a \leq x, \omega(a) = k-1} \frac{|S_a|}{a} \ll \frac{1}{(k-1)!} \left( \sum_{p^k \leq x, p \equiv 3 (\mod 4)} \frac{|S_{p^k}|}{p^k} + O(1) \right)^{k-1}.
\]
Now
\[
\sum_{p^f \leq x \atop p \equiv 1 \mod 4} \frac{|S_p|}{p^f} = \sum_{p^f \leq x \atop p \equiv 1 \mod 4} \frac{\ell + 1}{p^f} + O(1)
\]
\[
= \sum_{p^f \leq x \atop p \equiv 1 \mod 4} \frac{2}{p} + O(1)
\]
\[
= \log_2 x + O(1).
\]
Inserting this expression into (6) proves the lemma. \(\square\)

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
\[
\sum_{k > \gamma \log_2 x} \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!} \ll \left( \frac{e \log_2 x + O(1)}{[\gamma \log_2 x]} \right)^{[\gamma \log_2 x]}
\]
\[
\ll \left( \frac{\gamma}{\gamma + O(\frac{1}{\log_2 x}}) \right)^{[\gamma \log_2 x]} \ll \gamma (\log x)^{\gamma - \gamma \log \gamma}.
\]
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
\[
\#\{p \leq x : \omega(\#(E(F_p))) > \gamma \log_2 x\} \geq \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}}.
\]
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 \(#(E(F_p)) = \|\pi - 1\|\), where \(\pi \equiv 1 \mod (1 + i)^3\) and \(p = \pi \overline{\pi}\). Let \(k\) be an integer to be specified later and fix an ideal \(s \in \mathbb{Z}[i]\) with the following properties:

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

Here \(P^+(n)\) denotes the largest prime factor of \(n\). Note that we have \(\omega(s) = \omega(\|s\|)\).

First, we will estimate from below the size of the set \(\mathcal{M}_s\), defined to be the set of those \(\pi \in \mathbb{Z}[i]\) with \(\|\pi\| \leq x\) satisfying the following properties:
(1) \( \pi \) prime (in \( \mathbb{Z}[i] \))
(2) \( \|\pi\| \) prime (in \( \mathbb{Z} \))
(3) \( \pi \equiv 1 \pmod{\sigma} \)
(4) \( P^- \left( \frac{\|\pi-1\|}{\|\pi\|} \right) > x^{1/100 \gamma \log_2 x} \).

Here \( P^- (n) \) denotes the smallest prime factor of \( n \). The conditions on the size of the prime factors of \( \|\pi\| \) and \( \|\pi-1\|/\|\pi\| \) imply that each \( \pi \) with \( \|\pi\| \leq x \) belongs to at most one of the sets \( M_\pi \). If \( \gamma > 0 \) is chosen to be greater than \( \gamma \log_2 x \), then carefully summing over \( \sigma \) satisfying the conditions above yields a lower bound on the count of distinct \( \pi \) corresponding to \( p \) with the property that \( \omega(\#E(\mathbb{F}_p)) \geq k > \gamma \log_2 x \). The problem of counting elements \( \pi \) and \( \pi^* \) with \( p = \pi \pi^* \) is remedied by inserting a factor of \( \frac{1}{\pi} \), 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 \( M_\mathfrak{s} \) using Theorem 2.1. Define \( A \) 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 \( \{ p : \|p\| \leq z \} \), where \( z := x^{1/50 \gamma \log_2 x} \). Let \( \mathfrak{p} := \prod_{p \in \mathcal{P}} p \). If \( \frac{\pi-1}{\sigma} \equiv 0 \pmod{p} \) implies \( \|\pi\| \geq z \), then all primes \( p \mid \|\pi\| \) 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 \( \pi \) is clearly \( O(\sqrt{x}) \). Therefore, we have

\[
\#M_\mathfrak{s} \geq S(A, \mathcal{P}) + O(\sqrt{x}).
\]

Lemma 4.2. With \( M_\mathfrak{s} \) defined as above, we have

\[
\#M_\mathfrak{s} \geq c \cdot \frac{\operatorname{Li}(x) \log x}{\Phi(\mathfrak{s}) \log x} + O \left( \sum_{\|p\| \leq z} |r(us)| \right) + O \left( \frac{1}{\Phi(\mathfrak{s}) (\log x)^{22}} \right) + O(\sqrt{x}),
\]

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

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

\[
A_u = X \delta(u) + r(us),
\]

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

\[
S(A, \mathcal{P}) = 4 \frac{\operatorname{Li}(x)}{\Phi(\mathfrak{s})} \prod_{\|p\| \leq z} \left( 1 - \frac{\Phi(\mathfrak{s})}{\Phi(p\mathfrak{s})} \right) + O \left( \sum_{\|p\| \leq z} |r(us)| \right) + O \left( \frac{\operatorname{Li}(x)}{\Phi(\mathfrak{s})} \sum_{\|p\| \leq z} \delta(u) \right) + O(\sqrt{x}).
\]
Using Proposition 2.3, we have
\[ \prod_{\|p\| \leq z} \left( 1 - \frac{\Phi(s)}{\Phi(ps)} \right) = \prod_{\|p\| \leq z} \left( 1 - \frac{1}{\Phi(p)} \right) \prod_{\|p\| \leq z} \left( 1 - \frac{1}{\|p\|} \right) \]
\[ = \prod_{\|p\| \leq z} \left( 1 - \frac{1}{\|p\|} \right) \prod_{\|p\| \leq z} \left( 1 - \frac{1}{(\|p\| - 1)^2} \right) \]
\[ \gg \frac{1}{\log z} = \frac{\log x}{\log x} \]

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
\[ \sum_{s \geq m} \frac{1}{s!} \left( \sum_{\|p\| \leq z} \delta(p) \right)^s. \]
By Proposition 2.3, we have
\[ \sum_{\|p\| \leq z} \delta(p) \leq \log_2 x + O(1). \]
Now, one sees once again by the ratio test that the sum on \( s \) is
\[ \ll \frac{1}{m!} \left( \sum_{\|p\| \leq z} \delta(p) \right)^m \leq \frac{1}{m!} (\log_2 x + O(1))^m. \]
Thus, by the same calculations as in the proof of Theorem 3.1, the second \( O \)-term is
\[ \ll \frac{\operatorname{Li}(x)}{\Phi(s)(\log x)^{22}}, \]
completing the proof of the lemma.

We now sum this estimate over \( \sigma \) 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 \( s \) is chosen to satisfy properties A through F listed below Theorem 4.1; in particular, \( \omega(s) = k \) for some integer \( k \) and \( P^+(\|s\|) \leq x^{1/100\gamma \log_2 x} \). Choose \( k := \lfloor \gamma \log_2 x \rfloor + 2 \).
Since \( \omega(\|s\|) = \omega(s) \), we have that \( \|s\| \leq x^{k/100\gamma \log_2 x} \leq x^{1/10} \). A lower bound follows by estimating the quantity
\[ \mathcal{M} = \sum' \# M_s, \]
where the prime indicates a restriction to those ideals \( s \subset \mathbb{Z}[i] \) 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 \( \sum_{\|s\| \leq x} 1/\Phi(s) \ll \log x \), the second \( O \)-term in Lemma 4.2 is, upon summing on \( s \), bounded by a constant times \( \operatorname{Li}(x)/(\log x)^{21} \). The third error term, \( O(\sqrt{x}) \), is therefore safely absorbed by this term.
We now handle the sum over $s$ of the first $O$-term. We have $|r(us)| = |\pi(x; us, 1) - 4\text{Li}(x)/\Phi(us)|$. We can think of the double sum (over $s$ and $u$) as a single sum over a modulus $q$, inserting a factor of $\tau(q)$ to account for the number of ways of writing $q$ as a product of two ideals in $\mathbb{Z}[i]$. (Here, $\tau(q)$ is the number of ideals in $\mathbb{Z}[i]$ which divide $q$.) Recalling our choice of $m = 14[\log_2 x]$, we have

$$\sum_{|s| \leq x^{1/10}} \sum_{\omega(u) \leq m} |r(us)| \ll \sum_{|s| < x^{2/5}} |\pi(x; q, 1) - \frac{\text{Li}(x)}{\Phi(q)}\tau(q)|.$$

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

$$|\pi(x; q, 1) - \frac{\text{Li}(x)}{\Phi(q)}| \ll \frac{x}{\Phi(q)}.$$

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

$$\sum_{|q| < x^{2/5}} |\pi(x; q, 1) - \frac{4\text{Li}(x)}{\Phi(q)}\tau(q)| \ll \sum_{|q| < x^{2/5}} |\pi(x; q, 1) - \frac{4\text{Li}(x)}{\Phi(q)}|^{1/2} \left(\frac{x}{\Phi(q)}\right)^{1/2} \tau(q)$$

$$\ll \left(x \sum_{|q| < x^{2/5}} \frac{\tau(q)^2}{\Phi(q)}\right)^{1/2} \left(\frac{x}{(\log x)^A}\right)^{1/2}.$$

We can estimate this sum using an Euler product:

$$\sum_{|q| < x^{2/5}} \frac{\tau(q)^2}{\Phi(q)} \ll \prod_{|p| \leq x^{2/5}} \left(1 + \frac{4}{|p|}\right)$$

$$\leq \exp\left\{ \sum_{|p| \leq x^{2/5}} \frac{4}{|p|}\right\} \ll (\log x)^4.$$

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

$$(7) \quad M = \sum_{s} \frac{1}{\Phi(s)}.$$

Let $I = (e^{(\log_2 x)^2/k}, x^{1/10k})$. Define a collection of prime ideals $\mathcal{P}$ such that each $p \in \mathcal{P}$ 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 $|p| \in I$. We apply Lemma 2.3 with the $y_i$ chosen to be of the form $1/\Phi(p)$ with $p \in \mathcal{P}$, obtaining

$$(8) \quad \frac{1}{\Phi((1 + i)^3)} \sum_{\text{ord}(s/(1+i)^3) \Rightarrow p \in \mathcal{P}} \frac{1}{\Phi(s/(1 + i)^3)}$$

$$\gg \frac{1}{(k - 1)!} \left( \sum_{p \in \mathcal{P}} \frac{1}{\Phi(p)} \right)^{k-1} \left( 1 - \binom{k-1}{2} \frac{1}{\omega_i^2} \sum_{p \in \mathcal{P}} \frac{1}{\Phi(p)^2} \right),$$
where
\[ S_1 = \sum_{p \in P} \frac{1}{\Phi(p)}. \]

By Theorem 2.3, \( S_1 = \frac{1}{2} \log_2 x - 2 \log_3 x + O(1) \). This introduces a factor of \( \frac{1}{2} \) to the right-hand side of (5), but this is of no concern: If each of the \( k \) prime factors of \( s \), excluding \((1 + i)\), lies above a distinct prime \( p \equiv 1 \pmod{4} \), then there are \( 2^{k-1} \) such ideals \( s \) of a given norm. Thus, if we extend the sum on the left-hand side of (8) to range over all \( s \) counted in primed sums (cf. the discussion above Lemma 4.3), we obtain
\[ \sum_{s} \frac{1}{\Phi(s)} \geq \frac{2^{k-1}}{(k-1)!} \left( \frac{1}{2} \log_2 x - 2 \log_3 x + O(1) \right)^{k-1} \times \left( 1 - \left( \frac{k-1}{2} \right) \left( \frac{1}{S_1} \sum_{p \in P} \frac{1}{\Phi(p)^2} \right) \right). \]

The quantity \( \left( \frac{k-1}{2} \right) \) is bounded from above by \( \lceil \gamma \log_2 x \rceil^2 \), and the sum on \( 1/\Phi(p)^2 \) tends to 0 as \( x \to \infty \). Therefore,
\[ 1 - \left( \frac{k-1}{2} \right) \left( \frac{1}{S_1} \sum_{p \in P} \frac{1}{\Phi(p)^2} \right) \geq 1 - 4 \gamma^2 \sum_{p \in P} \frac{1}{\Phi(p)^2} \geq \frac{1}{2} \]
for large enough \( x \), and so
\[ \frac{x \log_2 x}{( \log x )^2} \sum_{s} \frac{1}{\Phi(s)} \geq \frac{x \log_2 x ( \log_2 x + O( \log_3 x ) )^{k-1}}{(k-1)! ( \log x )^2}, \]
as desired. \( \square \)

With \( k = \lceil \gamma \log_2 x \rceil + 2 \) and by the more precise version of Stirling’s formula \( n! \sim \sqrt{2\pi n} (n/e)^n \), we have
\[ \frac{\log_2 x + O( \log_3 x )}{(k-1)!} \gg \frac{1}{\sqrt{\log_2 x}} \left( \frac{e \log_2 x + O( \log_3 x )}{\lceil \gamma \log_2 x \rceil} \right)^{\lceil \gamma \log_2 x \rceil} \]
\[ = \frac{1}{\sqrt{\log_2 x}} \left( \frac{e}{\gamma} \left( 1 + O \left( \frac{\log_3 x}{\log_2 x} \right) \right) \right)^{\lceil \gamma \log_2 x \rceil} \]
\[ = (\log x)^{\gamma - \gamma \log \gamma + o(1)}. \]

This yields a main term of the shape
\[ \frac{x}{( \log x )^{2 + \gamma \log \gamma + o(1)}}, \]
which completes the proof of Theorem 4.1 in the case \( \gamma > 1 \).

4.3. The case \( 0 < \gamma < 1 \). Above, we used the fact that if \( \pi - 1 \) is divisible by certain \( s \subset \mathbb{Z}[i] \) with \( \omega(\|s\|) = k \), 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 \( \|\pi - 1\|/\|s\| \) does not have too many prime factors.

Lemma 4.4. For any \( s \subset \mathbb{Z}[i] \) satisfying properties A through F listed below Theorem 4.1, we have
\[ \# \{ \pi \in \mathcal{M}_s : \omega \left( \frac{\|\pi - 1\|}{\|s\|} \right) > \frac{\log_2 x}{\log_4 x} \} \ll \frac{x}{\|s\| (\log x)^\gamma}. \]
Upon discarding those $\pi$ counted by the above lemma, the remaining $\pi$ 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 $s \in \mathbb{Z}[i]$, we have $\|\pi - 1\|/\|s\| \leq 2x/\|s\|$. Therefore, we estimate

$$
\sum_{\|a\| \leq \frac{2x}{\|s\|}} 1 \leq \frac{2x}{\|s\|} \sum_{\|a\| \leq \frac{2x}{\|s\|}} \frac{1}{\|a\|}.
$$

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

$$
\sum_{\|a\| \leq \frac{2x}{\|s\|}} \frac{1}{\|a\|} \leq \sum_{\|a\| \leq \frac{2x}{\|s\|}} \frac{1}{\|a\|} \leq \sum_{\ell > \log_2 x / \log_4 x} \frac{1}{\ell^\ell} \sum_{x/100 \log_2 x \leq \|p\| \leq \frac{x^2}{\log_4 x}} \sum_{m=1}^\infty \frac{1}{\|p\|^m} \cdot \ell.
$$

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

$$
\sum_{\ell > \log_2 x / \log_4 x} \frac{1}{\ell^\ell} \leq \left( \frac{\log_4 x + O(1)}{\ell} \right)^{\log_2 x / \log_4 x + 1} \leq \left( \frac{1}{(\log_2 x)^{1+o(1)}} \right)^{\log_2 x / \log_4 x} \leq e^{-2 \log_2 x \log_3 x / \log_4 x}.
$$

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

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

Write

$$
\mathcal{M}_s' = \{\pi \in \mathcal{M}_s : \omega\left(\frac{\|\pi - 1\|}{\|s\|}\right) \leq \frac{\log_2 x}{\log_4 x}\}.
$$

Lemmas 4.2 and 4.4 show that $\#\mathcal{M}_s'$ satisfies

$$
\#\mathcal{M}_s' \geq c \cdot \frac{x \log_2 x}{\Phi(s)(\log x)^2} + O\left( \sum_{u \in \mathcal{F}, \omega(u) \leq m} |r(u\mathbf{s})| \right) + O\left( \frac{1}{\Phi(s)} \frac{\text{Li}(x)}{(\log x)^2} \right) + O\left( \frac{x}{\|s\|(\log x)^A} \right) + O(\sqrt{x}),
$$

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

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

where

$$M' = \sum_s' \#M'_s.$$ 

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,

$$\frac{\log x + O(\log_3 x))^{k-1}}{(k-1)!} \gg \frac{1}{\log_2 x} \left( \frac{e \log_2 x + O(\log_3 x)}{k-1} \right)^{k-1}$$

$$\gg \frac{1}{\log_2 x} \left( e \left( 1 + O \left( \frac{1}{\log_4 x} \right) \right)^{k-1} \right)$$

$$\gg (\log x)^{\gamma \log \gamma - \gamma + o(1)}.$$

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 Erdös-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.

[Pol99] 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