A Titchmarsh divisor problem for elliptic curves

By PAUL POLLACK†

Department of Mathematics,
University of Georgia, Athens, Georgia, USA
e-mail: pollack@uga.edu

(*Received*)

Abstract

Let $E/\mathbf{Q}$ be an elliptic curve with complex multiplication. We study the average size of $\tau(\#E(\mathbf{F}_p))$ as p varies over primes of good ordinary reduction. We work out in detail the case of $E\colon y^2 = x^3 - x$, where we prove that

$$\sum_{\substack{p\le x\\ p\equiv 1 \pmod 4}} \tau(\#E(\mathbf{F}_p)) \sim \left(\frac{5\pi}{16}\prod_{p>2}\frac{p^4-\chi(p)}{p^2(p^2-1)}\right)x, \quad \text{as } x\to\infty.$$

Here χ is the nontrivial Dirichlet character modulo 4. The proof uses number field analogues of the Brun–Titchmarsh and Bombieri–Vinogradov theorems, along with a theorem of Wirsing on mean values of nonnegative multiplicative functions.

Now suppose that $E/\mathbf{Q}$ is a non-CM elliptic curve. We conjecture that the sum of $\tau(\#E(\mathbf{F}_p))$, taken over $p \le x$ of good reduction, is $\sim c_E x$ for some $c_E > 0$, and we give a heuristic argument suggesting the precise value of c_E. Assuming the Generalized Riemann Hypothesis for Dedekind zeta functions, we prove that this sum is $\asymp_E x$. The proof uses combinatorial ideas of Erdős.

1. *Introduction*

Let $\{N_p\}$ be a sequence of positive integers indexed by a cofinite subset of the prime numbers. By a *Titchmarsh divisor problem*, we mean the task of estimating $\sum_{p\le x}\tau(N_p)$, as $x\to\infty$, where τ is the usual number-of-divisors function. The prototypical example was studied by Titchmarsh in 1930 [**33**], who took $N_p = p-a$ for some fixed integer a. He succeeded in proving an asymptotic formula for $\sum_{a<p\le x}\tau(p-a)$, as $x\to\infty$, conditional on the Generalized Riemann Hypothesis. Roughly 30 years later, Linnik [**26**] gave an unconditional proof of Titchmarsh's formula by the dispersion method. Nowadays, one can prove Titchmarsh's formula by a relatively straightforward application of the Brun–Titchmarsh and Bombieri–Vinogradov theorems; see, for instance, [**20**, pp. 110–112].

Akbary and Ghioca studied the following geometric Titchmarsh divisor problem. Let $E/\mathbf{Q}$ be an elliptic curve. (They work in the context of abelian varieties, but we will restrict our discussion here to the elliptic curve case.) If p is a prime of good reduction, then $E(\mathbf{F}_p)\cong \mathbf{Z}/d_p\mathbf{Z}\oplus\mathbf{Z}/e_p\mathbf{Z}$ for uniquely determined natural numbers d_p and e_p with

† This research was supported by NSF award DMS-1402268.

d_p dividing e_p. What is the average size of $\tau(d_p)$? In [**2**], Akbary and Ghioca showed that if GRH holds or if E has CM, then

$$\sum_{\substack{p\le x\\ p \text{ of good reduction}}} \tau(d_p) \sim c_E\cdot\pi(x), \quad \text{as } x\to\infty,$$

for a certain constant $c_E>0$. Thus, $\tau(d_p)$ has a well-defined, finite mean value. This is consistent with known results asserting that d_p itself is usually very small, such as Duke's theorem that for any function $\xi(p)$ tending to infinity, $d_p<\xi(p)$ for asymptotically 100% of primes p [**7**, Theorem 1.1]. (Once again, if E does not have CM, then GRH is assumed here.) Results analogous to those of Akbary and Ghioca, but for arithmetic functions of d_p other than τ, have been given by Felix and Murty [**14**], under the same hypotheses. Quite recently, Akbary and Felix [**1**] have shown unconditionally that mean value results of this kind hold on average over elliptic curves defined by equations whose coefficients lie in a suitable box.

In this paper, we study $\tau(d_pe_p)$. In other words, we investigate the average number of divisors of $\#E(\mathbf{F}_p)$.

In the case when E has CM, we obtain an asymptotic formula without any unproved hypotheses. The method is most intelligible if the details are carried out for a single representative example. This is the content of our first theorem.

THEOREM 1·1. *Let E be the elliptic curve $E\colon y^2=x^3-x$. As $x\to\infty$,*

$$\sum_{p\le x}{}^{*}\,\tau(\#E(\mathbf{F}_p))\sim\left(\frac{5\pi}{16}\prod_{p>2}\frac{p^4-\chi(p)}{p^2(p^2-1)}\right)x.$$

Here χ denotes the nontrivial Dirichlet character modulo 4. The $*$ on the sum indicates that p is restricted to primes of good ordinary reduction for E, i.e, $p\equiv 1 \pmod 4$.

Remarks.

(i) If $E/\mathbf{Q}$ is a CM elliptic curve, then a prime p of good reduction is supersingular precisely when it remains inert or ramifies in the CM field. This criterion is due to Deuring; see, e.g., [**24**, Theorem 12, p. 182]. Remaining inert or ramifying in the CM field is, by quadratic reciprocity, a congruence condition on p. Moreover, for each supersingular prime $p\ge 5$, one has $\#E(\mathbf{F}_p)=p+1$. Putting these facts together, one can determine the average order of $\tau(\#E(\mathbf{F}_p))$ along supersingular primes by the same methods used to solve the classical Titchmarsh divisor problem. Thus, it is natural to restrict the sum to primes p of good ordinary reduction, as we have done above.

(ii) While Theorem 1·1 is stated for a single elliptic curve, we emphasize that its method of proof can be adapted to any elliptic curve $E/\mathbf{Q}$ with CM. We discuss this briefly in §4.

It seems very plausible that a statement similar to Theorem 1·1 should hold for curves without complex multiplication.

CONJECTURE 1·2. *Let E be a non-CM elliptic curve over $\mathbf{Q}$. There is a constant $c_E>0$ with $\sum^*_{p\le x}\tau(\#E(\mathbf{F}_p))\sim c_Ex$, as $x\to\infty$. Here $\sum^*$ means that the sum is restricted to primes of good reduction.*

In fact, we will give a heuristic argument in favor of Conjecture 1·2 that allows us to predict the value of c_E. Since the description of c_E is a little complicated, we defer a full discussion of Conjecture 1·2 to the final section of the paper. Even assuming GRH, we do not have sharp enough estimates to establish Conjecture 1·2. However, on GRH we can at least obtain the correct order of magnitude for the sum in question.

THEOREM 1·3. *Assume GRH for Dedekind zeta functions. Let $E/\mathbf{Q}$ be a non-CM elliptic curve. Then*

$$\sum_{p \le x}^{*} \tau(\#E(\mathbf{F}_p)) \asymp_E x$$

for all $x > x_0(E)$.

Note that there is no reason in Conjecture 1·2 or Theorem 1·3 to further restrict the sum to primes of ordinary reduction. In fact, in the non-CM case it is known that the count of supersingular primes $p \le x$ is $O_E(x^{3/4})$ (a result of Elkies, Kaneko, and Ram Murty [**10**]), so that such a restriction would have a negligible impact on the size of the sum.

The proof of Theorem 1·3 uses a method introduced by Erdős [**12**] to study the partial sums of $\tau(F(n))$, where F is a fixed irreducible polynomial with integer coefficients. Erdős's method has proved fruitful in many contexts, a particularly prominent example being the work of Shiu on Brun–Titchmarsh results for multiplicative functions [**30**].

Notation. The letters p and q are reserved for (positive, rational) primes. Let K be an algebraic number field with ring of integers $\mathbf{Z}_K$. The fraktur letter $\mathfrak{p}$ always denotes a nonzero prime ideal of $\mathbf{Z}_K$, while π always denotes a prime element of $\mathbf{Z}_K$. For each nonzero ideal $\mathfrak{a}$ of $\mathbf{Z}_K$, we put $\|\mathfrak{a}\| = \#\mathbf{Z}_K/\mathfrak{a}$ (the norm of $\mathfrak{a}$) and $\Phi(\mathfrak{a}) = \#(\mathbf{Z}_K/\mathfrak{a})^\times$ (the analogue of the Euler function). If α is a nonzero element of $\mathbf{Z}_K$, we write $\|\alpha\|$ and $\Phi(\alpha)$ for the corresponding functions evaluated at the principal ideal (α). When $K = \mathbf{Q}$, we write φ instead of Φ. We use the notation $\mathbf{1}_*$ for the indicator function of the condition *; for example, $\mathbf{1}_{d|n}$ is 1 if d divides n and 0 otherwise. We write $[a, b]$ for the least common multiple of the integers a and b.

2. *Preliminaries for the proof of Theorem* 1·1

2·1. *Mean values*

The proof makes essential use of a celebrated result of Wirsing [**34**, Satz 1] concerning mean values of nonnegative multiplicative functions.

PROPOSITION 2·1. *Let f be a nonnegative multiplicative function. Suppose that for a certain constant $\kappa > 0$, we have*

$$\sum_{p \le x} f(p) = (\kappa + o(1))\frac{x}{\log x}, \quad \text{as } x \to \infty.$$

Suppose constants $\lambda_1 \ge 0$ and $\lambda_2 \in [0, 2)$ have the property that for all primes p and all integers $k \ge 2$, we have $f(p^k) \le \lambda_1 \lambda_2^k$. Then as $x \to \infty$,

$$\sum_{n \le x} f(n) \sim \frac{x}{\log x} \cdot \frac{e^{-\gamma\kappa}}{\Gamma(\kappa)} \prod_{p \le x}\left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \dots\right).$$

Here γ is the Euler–Mascheroni constant and $\Gamma(\cdot)$ is the usual gamma function.

2·2. *The distribution of primes in imaginary quadratic fields*

In addition, the proof of Theorem 1·1 requires some input from the algebro-analytic theory of numbers. We begin by stating Huxley's number field analogue of the Bombieri–Vinogradov theorem. This necessitates a brief review of the concept of strict equivalence of ideals. (For more details, see [**5**, Chapter 3].) For each nonzero ideal $\mathfrak{m}$ of $\mathbf{Z}_K$, set

$$\mathcal{I}(\mathfrak{m}) = \{\text{fractional ideals } \mathfrak{a} \subset K : \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ for all } \mathfrak{p} \mid \mathfrak{m}\},$$

$$\mathcal{P}_{\mathfrak{m}}^{+} = \{(\alpha) : \alpha \in K \text{ is totally positive}, \mathrm{ord}_{\mathfrak{p}}(\alpha - 1) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}) \text{ for all } \mathfrak{p} \mid \mathfrak{m}\}.$$

The quotient $\mathcal{I}(\mathfrak{m})/\mathcal{P}_{\mathfrak{m}}^{+}$ is called the *strict ray class group* for $\mathfrak{m}$. Fractional ideals $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}(\mathfrak{m})$ are called *equivalent modulo* $\mathfrak{m}$ if they represent the same class in the strict ray class group. The *strict ray class number* is $h(\mathfrak{m}) := \#\mathcal{I}(\mathfrak{m})/\mathcal{P}_{\mathfrak{m}}^{+}$. It is known [**5**, Proposition 2.1, p. 50] that

$$h(\mathfrak{m}) = \frac{h \cdot 2^{r_1} \Phi(\mathfrak{m})}{[\mathcal{U} : \mathcal{U}_{\mathfrak{m}}]}, \tag{2·1}$$

where h is the class number of K, r_1 is the number of real embeddings of K, $\mathcal{U}$ is the unit group of $\mathbf{Z}_K$, and

$$\mathcal{U}_{\mathfrak{m}} := \{\lambda \in \mathcal{U} : \lambda \text{ is totally positive}, \lambda \equiv 1 \pmod{\mathfrak{m}}\}.$$

We now have the background to state Huxley's analogue of the Bombieri–Vinogradov theorem. If $\mathfrak{a} \in \mathcal{I}(\mathfrak{m})$, we write

$$\pi(x; \mathfrak{m}, \mathfrak{a}) = \#\{\mathfrak{p} : \|\mathfrak{p}\| \leq x, \mathfrak{p} \text{ is equivalent to } \mathfrak{a} \text{ modulo } \mathfrak{m}\}.$$

PROPOSITION 2·2. *For each $A > 0$, one can choose $B > 0$ so that*

$$\sum_{\|\mathfrak{m}\| \leq x^{1/2}(\log x)^{-B}} \frac{h(\mathfrak{m})}{\Phi(\mathfrak{m})} \max_{\mathfrak{a}} \max_{y \leq x} \left| \pi(y; \mathfrak{m}, \mathfrak{a}) - \frac{\mathrm{Li}(y)}{h(\mathfrak{m})} \right| \ll \frac{x}{(\log x)^A}.$$

Here the first maximum is over $\mathfrak{a} \in \mathcal{I}(\mathfrak{m})$. The implied constant depends on A and K.

Proposition 2·2 is essentially Theorem 1 of [**21**]. Huxley's statement is in terms of the ($\mathbf{Z}_K$-analogue of the) von Mangoldt function; our statement follows from his by partial summation.

We now specialize Proposition 2·2 to the case when K is an imaginary quadratic field of class number 1, where it assumes a form entirely analogous to the classical Bombieri–Vinogradov theorem. If $\mu, \alpha \in \mathbf{Z}_K$, write

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

LEMMA 2·3. *Let K be an imaginary quadratic field of class number* 1*. For every $A > 0$, there is a $B > 0$ so that*

$$\sum_{\|\mu\| \leq x^{1/2}(\log x)^{-B}} \max_{\alpha:\ \gcd(\alpha,\mu)=1} \max_{y \leq x} \left| \pi(y; \mu, \alpha) - \#\mathcal{U}\frac{\mathrm{Li}(y)}{\Phi(\mu)} \right| \ll \frac{x}{(\log x)^A}.$$

Again, the implied constant may depend on A and K.

Proof. We begin by noting that since K has no real embeddings, all elements of K are totally positive, and so the total positivity conditions in the above definitions are automatically satisfied. Suppose that α and μ are coprime. If $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}$

is equivalent to (α) modulo (μ) precisely when $\mathfrak{p} = (\pi)$ for some prime $\pi \equiv \alpha \pmod{\mu}$. If any such π exists, then the number of such π is exactly $\#\mathcal{U}_{(\mu)}$. Hence, $\pi(y; \mu, \alpha) = \#\mathcal{U}_{(\mu)} \cdot \pi(y; (\mu), (\alpha))$. Since $h = 1$ and $r_1 = 0$, (2·1) shows that $h((\mu)) = \Phi(\mu)\frac{\#\mathcal{U}_{(\mu)}}{\#\mathcal{U}}$. Thus,

$$\left|\pi(y; \mu, \alpha) - \#\mathcal{U}\frac{\mathrm{Li}(y)}{\Phi(\mu)}\right| = \#\mathcal{U}\frac{h((\mu))}{\Phi(\mu)} \cdot \left|\pi(y; (\mu), (\alpha)) - \frac{\mathrm{Li}(y)}{h((\mu))}\right|.$$

Now as μ runs over the nonzero elements of $\mathbf{Z}_K$ of norm not exceeding x, the ideal (μ) runs over the nonzero ideals of $\mathbf{Z}_K$ not exceeding x, each hit precisely $\#\mathcal{U}$ times. Since $\#\mathcal{U} \le 6$, our lemma follows from Proposition 2·2. □

We also need a Brun–Titchmarsh type estimate for number fields. The following is due to Hinz and Lodemann; see [**18**, Theorem 4].

PROPOSITION 2·4. *Let K be a number field. If $\|\mathfrak{m}\| < x$ and $\mathfrak{a} \in \mathcal{I}(\mathfrak{m})$, then*

$$\pi(x; \mathfrak{m}, \mathfrak{a}) \le 2\frac{x}{h(\mathfrak{m})\log(x/\|\mathfrak{m}\|)}\left(1 + O\left(\frac{\log\log(3x/\|\mathfrak{m}\|)}{\log(x/\|\mathfrak{m}\|)}\right)\right),$$

where the implied constant depends on K.

For our purposes, the following slightly crude consequence is sufficient.

LEMMA 2·5. *Let K be an imaginary quadratic field of class number* 1. *If $\|\mu\| \le x$ and* $\gcd(\alpha, \mu) = 1$, *then*

$$\pi(x; \mu, \alpha) \ll \frac{x}{\Phi(\mu)\log(x/\|\mu\|)},$$

where the implied constant depends on K.

Lemma 2·5 can be deduced from Proposition 2·4 in a way similar to how we deduced Lemma 2·3 from Proposition 2·2. We omit the details.

3. *Proof of Theorem* 1·1

3·1. *Setup*

Throughout this section, we fix $K = \mathbf{Q}(i)$. The essential fact used in the proof of Theorem 1·1 is that for each prime $p \equiv 1 \pmod 4$, the size of $E(\mathbf{F}_p)$ is determined by the following recipe (see [**23**, Table 2] or [**31**]): Write $p = \pi\bar{\pi}$ in $\mathbf{Z}[i]$, where π is chosen so that $\pi \equiv 1 \pmod{(1+i)^3}$. (This condition is sometimes referred to by saying that π is *primary.*) These conditions determine π uniquely up to complex conjugation. Then

$$\begin{aligned}\#E(\mathbf{F}_p) &= p + 1 - (\pi + \bar{\pi})\\ &= (\pi - 1)\overline{(\pi - 1)}.\end{aligned}$$

Since $\#E(\mathbf{F}_p) \le (\sqrt{p} + 1)^2 \le 4x$, it follows that

$$\sum_{\substack{p \le x\\ p \equiv 1 \ (\mathrm{mod}\ 4)}} \sum_{d \mid \#E(\mathbf{F}_p)} 1 = \frac{1}{2}\sum_{d \le 4x} \sideset{}{'}\sum_{\substack{\|\pi\| \le x\\ \pi \equiv 1 \ (\mathrm{mod}\ (1+i)^3)\\ d \mid (\pi-1)\overline{(\pi-1)}}} 1,$$

where the $'$ on the sum indicates that we restrict to primes π lying over rational primes $p \equiv 1 \pmod 4$. Hence, we are led to investigate the number of primes π with $\|\pi\| \le x$ and with $\|\pi - 1\|$ possessing a given natural number divisor d.

3·2. *Integer divisors of* $\|\pi - 1\|$

We begin with an elementary lemma concerning factorizations of Gaussian integers.

LEMMA 3·1. *Let k be a positive integer. As functions on the set of nonzero $\alpha \in \mathbf{Z}[i]$,*

(i) $\mathbf{1}_{2^k|\alpha\bar{\alpha}} = \mathbf{1}_{(1+i)^k|\alpha}$,

(ii) *If $q \equiv 3 \pmod 4$ is prime, then* $\mathbf{1}_{q^k|\alpha\bar{\alpha}} = \mathbf{1}_{q^{\lceil k/2 \rceil}|\alpha}$.

(iii) *If $q \equiv 1 \pmod 4$ is prime and $q = \pi\bar{\pi}$, then*

$$\mathbf{1}_{q^k|\alpha\bar{\alpha}} = \sum_{i=0}^{k} \mathbf{1}_{\pi^i\bar{\pi}^{k-i}|\alpha} - \sum_{i=1}^{k} \mathbf{1}_{\pi^i\bar{\pi}^{k+1-i}|\alpha}.$$

Proof. Claims (i) and (ii) are immediate from unique factorization in $\mathbf{Z}[i]$, after recalling that $(2) = (1+i)^2$ and that (q) is a prime ideal for each prime $q \equiv 3 \pmod 4$. Claim (iii) requires more thought. Suppose that $q \equiv 1 \pmod 4$, and let

$$\mathcal{A}^+ = \{\pi^i\bar{\pi}^{k-i} : i = 0, \ldots, k\} \quad \text{and} \quad \mathcal{A}^- = \{\pi^i\bar{\pi}^{k+1-i} : i = 1, \ldots, k\}.$$

If $q^k \nmid \alpha\bar{\alpha}$, then α is not divisible by any element of $\mathcal{A}^+$ or $\mathcal{A}^-$. To complete the proof of (iii), it suffices to show that if $q^k \mid \alpha\bar{\alpha}$, then α is divisible by precisely one more element of $\mathcal{A}^+$ than of $\mathcal{A}^-$. Choose v_1 and v_2 with $\pi^{v_1}\bar{\pi}^{v_2} \parallel \alpha$. Since $q^k \mid \alpha\bar{\alpha}$, we see that $v_1 + v_2 \geq k$. In order that the element $\pi^i\bar{\pi}^{k-i}$ of $\mathcal{A}^+$ divide α, it is necessary and sufficient that

$$\max\{0, k - v_2\} \leq i \leq \min\{k, v_1\}.$$

Thus, the number of divisors of α from $\mathcal{A}^+$ is precisely

$$\min\{k, v_1\} - \max\{0, k - v_2\} + 1. \tag{3·1}$$

Similarly, in order for the element $\pi^i\bar{\pi}^{k+1-i}$ of $\mathcal{A}^-$ to divide α, it is necessary and sufficient that

$$\max\{1, k + 1 - v_2\} \leq i \leq \min\{k, v_1\}.$$

The number of values of i for which this occurs is

$$\min\{k, v_1\} - \max\{1, k + 1 - v_2\} + 1 = \min\{k, v_1\} - \max\{0, k - v_2\}. \tag{3·2}$$

Comparing (3·1) and (3·2) completes the proof. □

For each d, one can factor $\mathbf{1}_{d|n}$ as $\prod_{q^{v_q}\parallel d} \mathbf{1}_{q^{v_q}|n}$. This simple observation yields the following important extension of Lemma 3·1. We omit the straightforward proof.

LEMMA 3·2. *Let d be a natural number with prime factorization $d = \prod_q q^{v_q}$. For each prime $q \equiv 1 \pmod 4$ that divides d, write $q = \pi_q\bar{\pi}_q$, and put*

$$\mathcal{A}^+(q) = \{\pi_q^i\bar{\pi}_q^{v_q-i} : i = 0, \ldots, v_q\},$$
$$\mathcal{A}^-(q) = \{\pi_q^i\bar{\pi}_q^{v_q+1-i} : i = 1, \ldots, v_q\}.$$

Consider all formal products

$$\delta = (1+i)^{v_2} \prod_{\substack{q|d \\ q\equiv 3 \pmod 4}} q^{\lceil v_q/2 \rceil} \prod_{\substack{q|d \\ q\equiv 1 \pmod 4}} \delta_q, \quad \textit{where} \quad \delta_q \in \mathcal{A}^+(q) \cup \mathcal{A}^-(q).$$

To each of these, associate the formal sign

$$\operatorname{sgn}(\delta) := (-1)^{\#\{q \,:\, \delta_q \in \mathcal{A}^-(q)\}}.$$

If the δ are considered as elements of $\mathbf{Z}[i]$ rather than as formal products, then all of the δ are distinct. Thus, the set $\mathcal{A}(d)$ of these δ satisfies

$$\#\mathcal{A}(d) = \prod_{\substack{q \mid d \\ q \equiv 1 \pmod 4}} (2v_q + 1).$$

Moreover, as functions on nonzero $\alpha \in \mathbf{Z}[i]$,

$$\mathbf{1}_{d \mid \alpha\bar{\alpha}} = \sum_{\delta \in \mathcal{A}(d)} \operatorname{sgn}(\delta) \cdot \mathbf{1}_{\delta \mid \alpha}.$$

The following estimate, which is a Bombieri–Vinogradov result for integer divisors of $\|\pi - 1\|$, plays a critical role in our later analysis.

Lemma 3·3. *For every $A > 0$, there is a $B = B(A) > 0$ so that*

$$\sum_{d \le x^{1/2}(\log x)^{-B}} \sum_{\delta \in \mathcal{A}(d)} \left| \pi(x; \delta, 1) - 4\frac{\mathrm{Li}(x)}{\Phi(\delta)} \right| \ll \frac{x}{(\log x)^A}. \tag{3·3}$$

Here the implied constant may depend on A.

Lemma 3·3 is a close cousin of [**6**, Proposition 17]. However, that result only allows the sum on d to go up to $x^{1/4}(\log x)^{-B}$, which would not suffice for us.

Proof. We may assume without loss of generality that $A \ge 4$. Let $A_0 = 2A + 9$, and choose B_0 so that

$$\sum_{\|\mu\| \le x^{1/2}(\log x)^{-B_0}} \max_{\gcd(\alpha,\mu)=1} \left| \pi(x; \mu, \alpha) - 4\frac{\mathrm{Li}(x)}{\Phi(\mu)} \right| \ll \frac{x}{(\log x)^{A_0}}. \tag{3·4}$$

Lemma 2·3 ensures that this is possible. We will show that Lemma 3·3 holds with $B = B_0 + 2A$.

Observe that by construction, d divides $\|\delta\|$ for each $\delta \in \mathcal{A}(d)$, so that $\|\delta\| \ge d$. We will say $\delta \in \mathcal{A}(d)$ is *good* for d if $\|\delta\| \le d(\log x)^{2A}$ and *bad* for d otherwise.

If $d \le x^{1/2}(\log x)^{-B}$ and δ is good for d, then $\|\delta\| \le x^{1/2}(\log x)^{-B_0}$. Consequently, the contribution from good δ to the left-hand side of (3·3) is at most

$$\sum_{\|\delta\| \le x^{1/2}(\log x)^{-B_0}} \tau(\|\delta\|) \left| \pi(x; \delta, 1) - 4\frac{\mathrm{Li}(x)}{\Phi(\delta)} \right|.$$

By counting all nonunits $\equiv 1 \pmod{\mu}$ and not only primes, we see that $\pi(y; \mu, 1) \ll y/\|\mu\|$ for all choices of $y > 0$ and nonzero $\mu \in \mathbf{Z}[i]$. Thus,

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

Using this trivial bound along with (3·4) and Cauchy–Schwarz, we find that

$$\begin{aligned}\sum_{\|\delta\|\le x^{1/2}(\log x)^{-B_0}} &\tau(\|\delta\|)\left|\pi(x;\delta,1)-4\frac{\mathrm{Li}(x)}{\Phi(\delta)}\right| \\ &\ll \sum_{\|\delta\|\ll x^{1/2}(\log x)^{-B_0}} \tau(\|\delta\|)\left(\frac{x}{\Phi(\delta)}\right)^{1/2}\left|\pi(x;\delta,1)-4\frac{\mathrm{Li}(x)}{\Phi(\delta)}\right|^{1/2} \\ &\ll \left(x\sum_{\|\delta\|\le x^{1/2}(\log x)^{-B_0}}\frac{\tau(\|\delta\|)^2}{\Phi(\delta)}\right)^{1/2}\left(\frac{x}{(\log x)^{A_0}}\right)^{1/2}.\end{aligned}$$

Now $\Phi(\delta) \gg \|\delta\|/\log\log x$. (This is analogous to a well-known result on the minimal order of the Euler function — cf. the more precise [**22**, Theorem 328, p. 352] — and may be proved in the same way.) Hence,

$$\begin{aligned}\sum_{\|\delta\|\le x^{1/2}(\log x)^{-B_0}}\frac{\tau(\|\delta\|)^2}{\Phi(\delta)} &\ll \log\log x \sum_{m\le x^{1/2}(\log x)^{-B_0}}\frac{\tau(m)^2}{m}\sum_{\|\delta\|=m}1 \\ &\ll \log\log x \sum_{m\le x^{1/2}(\log x)^{-B_0}}\frac{\tau(m)^3}{m} \\ &\ll \log\log x \prod_{p\le x^{1/2}}\left(1+\frac{\tau(p)^3}{p}+\frac{\tau(p^2)^3}{p^2}+\dots\right) \ll (\log x)^9.\end{aligned}$$

In going from the first line to the second, we used that the number of elements of $\mathbf{Z}[i]$ of norm m is $4\sum_{d\mid m}\chi(d) \le 4\tau(m)$, where χ is the nontrivial character modulo 4 [**22**, Theorem 278, p. 314]. Collecting our estimates, we see that the "good case" makes a contribution of $\ll x/(\log x)^{(A_0-9)/2} = x/(\log x)^A$. This is acceptable for us.

For each of the remaining terms on the left-hand side of (3·3), we have $\|\delta\| \ge d(\log x)^{2A}$. Now using the trivial bound $\pi(x;\delta,1) \ll x/\|\delta\|$ noted previously, we find that each inner summand in (3·3) is

$$\ll \frac{x}{\Phi(\delta)} \ll \frac{x\log\log x}{\|\delta\|} \le \frac{x\log\log x}{d(\log x)^{2A}}.$$

Moreover, for each d, Lemma 3·2 implies that $\#\mathcal{A}(d) \le \tau(d^2)$. Thus, the bad terms make a contribution of

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

Here the sum on d has been bounded by an Euler product. Since $2A-4 \ge A$, this last upper bound is $O(x/(\log x)^A)$ and so is also acceptable for us. □

3·3. *Exploiting symmetry*

As in the usual Titchmarsh divisor problem, we can exploit the symmetry of the divisors of n around $\sqrt{n}$. Namely, we have

$$\tau(\#E(\mathbf{F}_p)) = 2\sum_{\substack{d\mid\#E(\mathbf{F}_p)\\ d\le\sqrt{\#E(\mathbf{F}_p)}}} 1 - \mathbf{1}_{\#E(\mathbf{F}_p)\text{ is a square}}.$$

Hence,

$$\sum_{\substack{p\le x\\ p\equiv 1 \pmod 4}} \tau(\#E(\mathbf{F}_p)) = 2\sum_{\substack{p\le x\\ p\equiv 1 \pmod 4}}\ \sum_{\substack{d\mid \#E(\mathbf{F}_p)\\ d\le\sqrt{\#E(\mathbf{F}_p)}}} 1 + O\left(\frac{x}{\log x}\right)$$

$$= 2\sum_{d\le 2\sqrt{x}}\ \sum_{\substack{p\le x\\ p\equiv 1 \pmod 4\\ d\mid \#E(\mathbf{F}_p)\\ \#E(\mathbf{F}_p)\ge d^2}} 1 + O\left(\frac{x}{\log x}\right). \tag{3·5}$$

Since we are shooting for an asymptotic formula whose main term is proportional to x, the error term in (3·5) is negligible. We now transform the main term.

Lemma 3·4. *Fix $B\ge 2$. Then*

$$\sum_{d\le 2\sqrt{x}}\ \sum_{\substack{p\le x\\ p\equiv 1 \pmod 4\\ d\mid \#E(\mathbf{F}_p)\\ \#E(\mathbf{F}_p)\ge d^2}} 1 = \sum_{d\le x^{1/2}(\log x)^{-B}}\ \sum_{\substack{p\le x\\ p\equiv 1 \pmod 4\\ d\mid \#E(\mathbf{F}_p)}} 1 + O\left(x\frac{\log\log x}{\log x}\right).$$

The implied constant may depend on B.

Proof. It suffices to show that

$$\sum_{d\le x^{1/2}(\log x)^{-B}}\ \sum_{\substack{p\le x\\ p\equiv 1 \pmod 4\\ d\mid \#E(\mathbf{F}_p)\\ d^2>\#E(\mathbf{F}_p)}} 1 \ll x\frac{\log\log x}{\log x} \tag{3·6}$$

and

$$\sum_{x^{1/2}(\log x)^{-B}<d\le 2\sqrt{x}}\ \sum_{\substack{p\le x\\ p\equiv 1 \pmod 4\\ d\mid \#E(\mathbf{F}_p)}} 1 \ll x\frac{\log\log x}{\log x}. \tag{3·7}$$

We take (3·6) first. If $d^2 > \#E(\mathbf{F}_p)$, then $p<(d+1)^2\le 4d^2$. Recalling Lemma 3·2, we see that the left-hand side of (3·6) is

$$\ll \sum_{d\le x^{1/2}(\log x)^{-B}}\ \sum_{\substack{p<4x(\log x)^{-2B}\\ p\equiv 1 \pmod 4\\ d\mid \#E(\mathbf{F}_p)}} 1 \le \sum_{d\le x^{1/2}(\log x)^{-B}}\ \sum_{\substack{\|\pi\|<4x(\log x)^{-2B}\\ d\mid(\pi-1)\overline{(\pi-1)}}} 1$$

$$\le \sum_{d\le x^{1/2}(\log x)^{-B}}\ \sum_{\delta\in\mathcal{A}(d)} \operatorname{sgn}(\delta)\cdot\pi(4x(\log x)^{-2B};\delta,1).$$

We have $d\le\|\delta\|\le d^2$ for all $\delta\in\mathcal{A}(d)$. Using $\pi(y;\delta,1)\ll y/\|\delta\|\le y/d$ with $y:=4x(\log x)^{-2B}$ along with the upper bound $\#\mathcal{A}(d)\le\tau(d^2)$, we conclude that the left-hand side of (3·6) is

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

Since $B\ge 2$, this is $O(x/\log x)$, which proves (3·6).

The proof of (3·7) is more delicate. First, observe that the left-hand side of (3·7) is bounded above by

$$\sum_{x^{1/2}(\log x)^{-B}<d\le 2\sqrt{x}}\ \sum_{\delta\in\mathcal{A}(d)} \operatorname{sgn}(\delta)\cdot\pi(x;\delta,1).$$

To proceed, we again divide the $\delta\in\mathcal{A}(d)$ into two classes. This time, we say δ is *good* for d if $\|\delta\|\le d(\log x)^4$ and *bad* otherwise. Using $\pi(x;\delta,1)\ll x/\|\delta\|$ and $\#\mathcal{A}(d)\le\tau(d^2)$, we see that the bad δ make a contribution to the double sum that is

$$\ll \frac{x}{(\log x)^4}\sum_{d\le 2\sqrt{x}}\frac{\tau(d^2)}{d}\ll\frac{x}{\log x},$$

which is acceptable. On the other hand, if δ is good for d, then $\|\delta\|\le 2\sqrt{x}(\log x)^4\ll x^{2/3}$. Lemma 2·5 then implies that $\pi(x;\delta,1)\ll\frac{x}{\Phi(\delta)\log x}$. Consequently, the good δ contribute

$$\ll\frac{x}{\log x}\sum_{x^{1/2}(\log x)^{-B}<d\le 2\sqrt{x}}\ \sum_{\delta\in\mathcal{A}(d)}\frac{1}{\Phi(\delta)}. \tag{3·8}$$

Put

$$g(d):=\sum_{\delta\in\mathcal{A}(d)}\frac{1}{\Phi(\delta)}.$$

Then g is multiplicative,

$$g(2^k)=\frac{1}{\Phi((1+i)^k)}=\frac{1}{2^{k-1}},$$
$$g(q^k)=\frac{1}{\Phi(q^{\lceil k/2\rceil})}=\frac{1}{q^{2\lceil k/2\rceil}(1-1/q^2)}\quad\text{for primes } q\equiv 3 \pmod 4,$$

and for primes $q\equiv 1 \pmod 4$, we have

$$\begin{aligned} g(q^k)&=\sum_{i=0}^{k}\frac{1}{\Phi(\pi^i\bar\pi^{k-i})}+\sum_{i=1}^{k}\frac{1}{\Phi(\pi^i\bar\pi^{k+1-i})}\\ &=\frac{2}{q^k(1-1/q)}+\frac{k-1}{q^k(1-1/q)^2}+\frac{k}{q^{k+1}(1-1/q)^2}.\end{aligned}$$

Let $G(d)=dg(d)$. Note that when $q\equiv 1 \pmod 4$, we have $G(q)=2+O(1/q)$, while when $q\equiv 3 \pmod 4$, we have $G(q)=O(1/q)$. Moreover, it is straightforward to check that $G(q^k)\le\lambda_1\lambda_2^k$ for certain constants $\lambda_1\ge 0$ and $\lambda_2\in[0,2)$. So from the prime number theorem for progressions, the hypotheses of Proposition 2·1 hold for G with $\kappa=1$. From the resulting asymptotic formula,

$$\sum_{d\le y}G(d)\ll\frac{y}{\log y}\prod_{q\le y}\left(1+g(q)+g(q^2)+\dots\right),$$

for all $y\ge 2$ (say). The Euler product factor corresponding to $q=2$ on the right-hand side has the value 3. For primes $q\equiv 3 \pmod 4$, the Euler factor is $1+O(1/q^2)$, while for $q\equiv 1 \pmod 4$, this factor is $1+2/q+O(1/q^2)$. Consequently, the product is $\ll\log y$ and $\sum_{d\le y}G(d)\ll y$. By partial summation,

$$\sum_{x^{1/2}(\log x)^{-B}<d\le 2\sqrt{x}}\ \sum_{\delta\in\mathcal{A}(d)}\frac{1}{\Phi(\delta)}=\sum_{x^{1/2}(\log x)^{-B}<d\le 2\sqrt{x}}\frac{G(d)}{d}\ll\log\log x.$$

Inserting this estimate back into (3·8), we see that the good δ contribute $O(x\frac{\log\log x}{\log x})$. This completes the proof of (3·7). □

3·4. *Completion of the proof of Theorem* 1·1

In view of (3·5) and Lemma 3·4, it suffices to show that for some fixed $B \geq 2$, we have

$$\sum_{d \leq x^{1/2}(\log x)^{-B}} \sum_{\substack{p \leq x \\ p \equiv 1 \ (\mathrm{mod}\ 4) \\ d \mid \#E(\mathbf{F}_p)}} 1 \sim \left(\frac{5\pi}{32}\prod_{p>2}\frac{p^4-\chi(p)}{p^2(p^2-1)}\right)x, \qquad \text{as } x \to \infty. \tag{3·9}$$

Choose B_0 so that the estimate (3·3) of Lemma 3·3 holds when $A = 1$. We prove (3·9) with $B = \max\{2, 1+B_0\}$.

Recall our notation $\sum'$ for a sum restricted to primes of $\mathbf{Z}[i]$ that lie above rational primes $p \equiv 1 \pmod 4$. We have

$$\begin{aligned}
\sum_{d \leq x^{1/2}(\log x)^{-B}} \sum_{\substack{p \leq x \\ p \equiv 1 \ (\mathrm{mod}\ 4) \\ d \mid \#E(\mathbf{F}_p)}} 1 &= \frac{1}{2}\sum_{d \leq x^{1/2}(\log x)^{-B}} \sideset{}{'}\sum_{\substack{\|\pi\| \leq x \\ \pi \equiv 1 \ (\mathrm{mod}\ (1+i)^3) \\ d \mid (\pi-1)\overline{(\pi-1)}}} 1 \\
&= \frac{1}{2}\sum_{d \leq x^{1/2}(\log x)^{-B}} \left(\sum_{\substack{\|\pi\| \leq x \\ \pi \equiv 1 \ (\mathrm{mod}\ (1+i)^3) \\ d \mid (\pi-1)\overline{(\pi-1)}}} 1 + O(x^{1/2})\right) \\
&= \frac{1}{2}\sum_{d \leq x^{1/2}(\log x)^{-B}} \sum_{\substack{\|\pi\| \leq x \\ \pi \equiv 1 \ (\mathrm{mod}\ (1+i)^3) \\ d \mid (\pi-1)\overline{(\pi-1)}}} 1 + O\left(\frac{x}{(\log x)^2}\right).
\end{aligned}$$

The requirement that $\pi \equiv 1 \pmod{(1+i)^3}$ is equivalent to $8 \mid (\pi-1)\overline{(\pi-1)}$. Thus, from Lemma 3·2,

$$\begin{aligned}
\frac{1}{2}\sum_{d \leq x^{1/2}(\log x)^{-B}} \sum_{\substack{\|\pi\| \leq x \\ \pi \equiv 1 \ (\mathrm{mod}\ (1+i)^3) \\ d \mid (\pi-1)\overline{(\pi-1)}}} 1 &= \frac{1}{2}\sum_{d \leq x^{1/2}(\log x)^{-B}} \sum_{\delta \in \mathcal{A}([8,d])} \mathrm{sgn}(\delta)\pi(x;\delta,1) \\
&= 2 \cdot \mathrm{Li}(x) \sum_{d \leq x^{1/2}(\log x)^{-B}} \sum_{\delta \in \mathcal{A}([8,d])} \frac{\mathrm{sgn}(\delta)}{\Phi(\delta)} + O\left(\frac{x}{\log x}\right).
\end{aligned} \tag{3·10}$$

We have used (3·3) to move from the first line to the second, noting that $[8,d] \leq 8d \leq x(\log x)^{-B_0}$ (for large x) and that each value of $[8,d]$ appears for only $O(1)$ values of d.

Define a multiplicative function g by setting

$$g(m) := \sum_{\delta \in \mathcal{A}(m)} \frac{\mathrm{sgn}(\delta)}{\Phi(\delta)}.$$

(This differs from our earlier definition of g in that the sgn factor is still present.) Then

$$g(2^k) = \frac{1}{\Phi((1+i)^k)} = \frac{1}{2^{k-1}},$$
$$g(q^k) = \frac{1}{\Phi(q^{\lceil k/2\rceil})} = \frac{1}{q^{2\lceil k/2\rceil}(1-1/q^2)} \quad \text{for primes } q \equiv 3 \pmod 4,$$

and on primes $q \equiv 1 \pmod 4$,

$$\begin{aligned} g(q^k) &= \sum_{i=0}^{k} \frac{1}{\Phi(\pi^i \bar{\pi}^{k-i})} - \sum_{i=1}^{k} \frac{1}{\Phi(\pi^i \bar{\pi}^{k+1-i})} \\ &= \frac{2}{q^k(1-1/q)} + \frac{k-1}{q^k(1-1/q)^2} - \frac{k}{q^{k+1}(1-1/q)^2}. \end{aligned}$$

Now let

$$G(d) = d \cdot \frac{g([8,d])}{g(8)}.$$

Then G is multiplicative with $G(2) = 2$, $G(q) = O(1/q)$ for primes $q \equiv 3 \pmod 4$, and $G(q) = 2 + O(1/q)$ for primes $q \equiv 1 \pmod 4$. Hence,

$$\sum_{p \le x} G(p) = \mathrm{Li}(x) + O(x \exp(-c\sqrt{\log x})), \tag{3·11}$$

by the prime number theorem for arithmetic progressions. This shows that the first hypothesis of Proposition 2·1 holds for G with $\kappa = 1$, and it is straightforward to check that the mild condition there on prime powers is also satisfied. Hence, as $y \to \infty$,

$$\sum_{d \le y} G(d) \sim e^{-\gamma} \frac{y}{\log y} \prod_{q \le y} \left(1 + \sum_{k=1}^{\infty} \frac{g([8,q^k])}{g(8)}\right).$$

For the prime $q = 2$,

$$1 + \sum_{k=1}^{\infty} \frac{g([8,2^k])}{g(8)} = 4 + \sum_{k=4}^{\infty} \frac{1/2^{k-1}}{1/4} = 5.$$

For primes $q \equiv 3 \pmod 4$,

$$\begin{aligned} 1 + \sum_{k=1}^{\infty} \frac{g([8,q^k])}{g(8)} &= 1 + \sum_{k=1}^{\infty} \frac{1}{q^{2\lceil k/2\rceil}(1-1/q^2)} \\ &= 1 + 2\sum_{\ell=1}^{\infty} \frac{1}{q^{2\ell}(1-1/q^2)} = 1 + 2\frac{q^2}{(q^2-1)^2} = \frac{q^4+1}{(q^2-1)^2}. \end{aligned}$$

For primes $q \equiv 1 \pmod 4$,

$$\begin{aligned} 1 + \sum_{k=1}^{\infty} \frac{g([8,q^k])}{g(8)} &= 1 + \sum_{k=1}^{\infty} \left(\frac{2}{q^k(1-1/q)} + \frac{k-1}{q^k(1-1/q)^2} - \frac{k}{q^{k+1}(1-1/q)^2}\right) \\ &= 1 + \sum_{k=1}^{\infty} \frac{2}{q^k(1-1/q)} = 1 + \frac{2q}{(q-1)^2} = \frac{q^2+1}{(q-1)^2}. \end{aligned}$$

Combining these expressions with Mertens' formula $\prod_{q \le y}(1-1/q) \sim e^{-\gamma}/\log y$, we find that

$$\sum_{d\le y} G(d) \sim \Bigg(\frac{5}{2} \prod_{\substack{q\le y\\ q\equiv 3 \pmod 4}} \frac{q^4+1}{q(q^2-1)(q+1)} \prod_{\substack{q\le y\\ q\equiv 1 \pmod 4}} \frac{q^2+1}{q(q-1)}\Bigg) y.$$

With χ the nontrivial character modulo 4, we have

$$L(1,\chi) = \prod_{q\equiv 3 \pmod 4} (1+1/q)^{-1} \prod_{q\equiv 1 \pmod 4} (1-1/q)^{-1},$$

and so the coefficient of y can be rewritten as

$$\frac{5}{2}L(1,\chi) \prod_{\substack{q\le y\\ q\equiv 3 \pmod 4}} \frac{q^4+1}{q^2(q^2-1)} \prod_{\substack{q\le y\\ q\equiv 1 \pmod 4}} \frac{q^2+1}{q^2}.$$

The products over y now converge (absolutely) as $y \to \infty$ and so are equal to the corresponding infinite products, up to factors of $1+o(1)$. Noting that $L(1,\chi) = \frac{\pi}{4}$ and that the Euler factors can be expressed uniformly as $\frac{q^4-\chi(q)}{q^2(q^2-1)}$, we conclude that

$$\sum_{d\le y} G(d) \sim \left(\frac{5\pi}{8} \prod_{q>2} \frac{q^4-\chi(q)}{q^2(q^2-1)}\right) y, \tag{3·12}$$

as $y \to \infty$. By partial summation,

$$\sum_{d\le y} \frac{g([8,d])}{g(8)} = \sum_{d\le y} \frac{G(d)}{d} \sim \left(\frac{5\pi}{8} \prod_{q>2} \frac{q^4-\chi(q)}{q^2(q^2-1)}\right) \log y.$$

Thus, as $x \to \infty$,

$$\begin{aligned} 2\cdot \mathrm{Li}(x) \sum_{d\le x^{1/2}(\log x)^{-B}} \sum_{\delta\in\mathcal{A}([8,d])} \frac{\mathrm{sgn}(\delta)}{\Phi(\delta)} &= 2g(8)\cdot \mathrm{Li}(x) \sum_{d\le x^{1/2}(\log x)^{-B}} \frac{g([8,d])}{g(8)} \\ &\sim \frac{\mathrm{Li}(x)}{2}\left(\frac{5\pi}{8} \prod_{q>2} \frac{q^4-\chi(q)}{q^2(q^2-1)}\right) \log(x^{1/2}(\log x)^{-B}) \\ &\sim \left(\frac{5\pi}{32} \prod_{q>2} \frac{q^4-\chi(q)}{q^2(q^2-1)}\right) x. \end{aligned} \tag{3·13}$$

Inserting this estimate into (3·10) completes the proof of (3·9) and so also the proof of Theorem 1·1.

Remark. Proposition 2·1 (Wirsing's fundamental result) does not include an error estimate, and so as it stands our proof of Theorem 1·1 also does not give any bound on the error. However, there are variants of Wirsing's theorem that incorporate error estimates. One such result is Moree and Cazaran's Theorem 6 in [**27**], which has the following useful consequence: If one replaces the first hypothesis of Proposition 2·1 with the stronger assumption that $\sum_{p\le x} f(p) = \kappa\cdot \mathrm{Li}(x) + O_A(x/(\log x)^A)$ for *every* A, then $\sum_{n\le x} f(n)$ has an asymptotic expansion of the form

$$\sum_{n\le x} f(n) = c_1 x(\log x)^{\kappa-1} + c_2 x(\log x)^{\kappa-2} + c_3 x(\log x)^{\kappa-3} + \dots .$$

(Here "asymptotic expansion" means that stopping the series at $c_k x(\log x)^{\kappa-k}$ results in an error that is $O(x(\log x)^{\kappa-k-1})$.) In view of (3·11), we can apply the Moree–Cazaran result to estimate $\sum_{d\le y} G(d)$. It follows that the asymptotic formula (3·12) holds as an equality up to an error of $O(y/\log y)$. Following this through, we conclude that (3·13) holds as an equality up to a factor of $1+O(\frac{\log\log x}{\log x})$. Glancing back through the proof, we see that the final error in Theorem 1·1 is of size $O(x\frac{\log\log x}{\log x})$.

4. *Generalization to other CM elliptic curves*

Let $E/\mathbf{Q}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in the imaginary quadratic field K. There is a canonical, $\mathbf{Q}$-rational isogeny $E\mapsto E'$, where $E'/\mathbf{Q}$ has CM by the maximal order $\mathbf{Z}_K$ (see, for instance, [**3**, Proposition 25]). So for all large primes p, the curves E and E' are $\mathbf{F}_p$-rationally isogenous and so $\#E(\mathbf{F}_p)=\#E'(\mathbf{F}_p)$. Thus, if our goal is to show the existence of an asymptotic formula of the sort given in Theorem 1·1, we can (and do) assume that E has CM by $\mathbf{Z}_K$. Note that since E is defined over $\mathbf{Q}$, the field K is necessarily one of the nine imaginary quadratic fields of class number 1.

For all large primes p of ordinary reduction, it is known that $\#E(\mathbf{F}_p)=\|\pi-1\|$ for *some* $\pi\in\mathbf{Z}_K$ above p. However, in the general case, making a correct choice of π is not as simple as for $E\colon y^2=x^3-x$, where it sufficed to take $\pi\equiv 1\pmod{(1+i)^3}$. While the general situation is complicated, it is now well understood. The introduction to [**31**] has a lucid discussion of this problem, while Table 2 of [**23**] presents explicit formulas for $\#E(\mathbf{F}_p)$ whenever $E/\mathbf{Q}$ has CM by a maximal order $\mathbf{Z}_K$. To take a representative example, suppose that $K=\mathbf{Q}(\sqrt{-7})$. Then E has a Weierstrass equation of the form

$$y^2=x^3-5\cdot 7\cdot\frac{g^2}{16}x-7^2\frac{g^3}{32}$$

for an integer g. Let p be a sufficiently large prime of good ordinary reduction and write $p=\pi\bar{\pi}$, where $\pi=u+v\sqrt{-7}\in\mathbf{Z}_K$. From [**23**, Table 2], we find that $\#E(\mathbf{F}_p)=\|\pi-1\|$ precisely when

$$\left(\frac{g}{p}\right)\left(\frac{4u}{7}\right)=1. \tag{4·1}$$

By Gauss's law of quadratic reciprocity, whether or not (4·1) holds is determined by the class of π mod $28g$ in $\mathbf{Z}_K$, since that class determines both p mod $4g$ and $4u$ mod 7 in $\mathbf{Z}$. Hence, the analogue of our earlier requirement that $\pi\equiv 1\pmod{(1+i)^3}$ is that π belong to a certain finite list of coprime residue classes modulo $28g$. These congruence conditions can be incorporated into our method at the cost of unpleasant but unimportant technical complications.

The situation is analogous in all of the remaining cases, in the sense that one can always specify a finite list of (necessary and sufficient) congruence conditions that replace the criterion $\pi\equiv 1\pmod{(1+i)^3}$. Once again, the precise conditions can be worked out from Table 2 of [**23**]. In the case when $K=\mathbf{Q}(\sqrt{-2})$, the congruence conditions are given explicitly in [**31**, Theorem 2.7] (due to Rajwade [**28**]). When $K=\mathbf{Q}(\sqrt{-1})$ or $K=\mathbf{Q}(\sqrt{-3})$, to work out these conditions one must appeal not only to quadratic reciprocity (as in the preceding paragraph) but to reciprocity laws for the quartic and sextic residue symbols, respectively. A convenient reference for higher reciprocity laws is [**11**, pp. 71–79]; that paper's Lemma 28 is particularly relevant.

The upshot of all of this is that whenever E has CM, $\sum_{p\le x}^{*}\tau(\#E(\mathbf{F}_p))\sim c_E x$ for some $c_E>0$, where the $*$ indicates a restriction to primes of good ordinary reduction.

5. *An order-of-magnitude result for elliptic curves without complex multiplication*

5·1. *Lower bound*

The lower bound half of Theorem 1·3 is an easy consequence of the following estimate of David and Wu (see [**8**, Theorem 12(a)]).

PROPOSITION 5·1 (conditional on GRH). *Let $E/\mathbf{Q}$ be a fixed elliptic curve without complex multiplication and with conductor N_E. There is a positive integer M_E (depending only on E) so that the following holds: For each squarefree integer d coprime to M_E, the number of primes $p \le x$ of good reduction for which $d \mid \#E(\mathbf{F}_p)$ is*

$$\left(\prod_{q \mid d} \frac{q^2-2}{(q-1)(q^2-1)}\right) \mathrm{Li}(x) + O(d^3 x^{1/2} \log(d \cdot N_E x)). \tag{5·1}$$

For the rest of §5, $\sum^*$ denotes a restriction to primes of good reduction. Implied constants may depend on E without further mention.

Proof of the lower bound in Theorem 1·3 Observe that

$$\sum_{p \le x}{}^{*} \tau(\#E(\mathbf{F}_p)) = \sum_{d} \sum_{\substack{p \le x \\ d \mid \#E(\mathbf{F}_p)}}{}^{*} 1 \ge \sum_{\substack{d \le x^{1/10} \\ \gcd(d, M_E)=1}} \mu^2(d) \sum_{\substack{p \le x \\ d \mid \#E(\mathbf{F}_p)}}{}^{*} 1.$$

We use (5·1) to evaluate the inner sum. This gives rise to an error of size $O(x^{9/10}\log x)$ and a main term of

$$\mathrm{Li}(x) \sum_{\substack{d \le x^{1/10} \\ \gcd(d, M_E)=1}} \mu^2(d) \prod_{q \mid d} \frac{q^2-2}{(q-1)(q^2-1)}.$$

Let $g(d) := \mu^2(d) \cdot \mathbf{1}_{\gcd(d,M_E)=1} \cdot \prod_{q \mid d} \frac{q^2-2}{(q-1)(q^2-1)}$, so that $G(d) := dg(d)$ satisfies the conditions of Wirsing's theorem with $\kappa = 1$. Applying that theorem and partial summation (in a manner seen already in the proof of Theorem 1·1), we find that $\sum_{d \le x^{1/10}} g(d) \gg \log x$ for large x. Hence, the main term here is $\gg x$. □

5·2. *Upper bound*

We require standard upper bounds on counts of smooth numbers. Recall that a positive integer n is said to be *y-smooth* (or *y-friable*) if no prime dividing n exceeds y. We write $\Psi(x, y)$ for the count of y-smooth numbers $n \le x$.

PROPOSITION 5·2. *Suppose that $x \ge y \ge 2$.*

(i) *If $u := \frac{\log x}{\log y}$ is sufficiently large (i.e., larger than a certain absolute constant) and $y \ge (\log x)^2$, then $\Psi(x, y) \le x \exp(-\frac{1}{2} u \log u)$.*

(ii) *Suppose $A > 1$ is fixed and put $y = (\log x)^A$. Then*

$$\Psi(x, y) = x^{1 - \frac{1}{A} + o(1)}, \quad \textit{as } x \to \infty.$$

Both results are discussed in Granville's survey article [**17**]; for (i), see his eq. (1.12), and for (ii), see his (1.14).

The required information about elliptic curves is contained in the following upper estimate, also due to David and Wu [**9**, Theorem 2.3(iii)].

PROPOSITION 5·3 (conditional on GRH). *Let $E/\mathbf{Q}$ be a fixed elliptic curve without* *complex multiplication. Uniformly for positive integers* $d \le x^{1/5}/\log x$*, the number of* $p \le x$ *of good reduction for which* $d \mid \#E(\mathbf{F}_p)$ *is*

$$\ll \frac{\mathrm{Li}(x)}{\varphi(d)}. \tag{5·2}$$

(In accordance with our convention, the implied constant here may depend on E*.)*

Proof of the upper bound in Theorem 1·3 Given a prime $p \le x$ of good reduction, let us write

$$\#E(\mathbf{F}_p) = (p_1 \cdots p_j)(p_{j+1} \cdots p_J),$$

where $p_1 \le p_2 \le \cdots \le p_J$ and j is the largest index with $p_1 \cdots p_j \le x^{1/6}$.

Suppose p is such that $J - j \le 12$. Then

$$\begin{aligned}\tau(\#E(\mathbf{F}_p)) &\le \tau(p_1 \cdots p_j)\tau(p_{j+1}) \cdots \tau(p_J)\\ &\le 2^{12}\tau(p_1 \cdots p_j) \le 2^{12} \sum_{\substack{d \mid \#E(\mathbf{F}_p)\\ d \le x^{1/6}}} 1.\end{aligned}$$

(In the first step, we used the easy-to-check fact that τ is *submultiplicative*: $\tau(ab) \le \tau(a)\tau(b)$ for every pair of positive integers a and b.) Using (5·2), the sum of $\tau(\#E(\mathbf{F}_p))$ over these p is

$$\ll \sum_{d \le x^{1/6}} \sideset{}{^*}\sum_{\substack{p \le x\\ d \mid \#E(\mathbf{F}_p)}} 1 \ll \mathrm{Li}(x) \sum_{d \le x^{1/6}} \frac{1}{\varphi(d)} \ll x,$$

since the final sum on d is $\ll \log x$ (by the now-familiar method of bounding sums by Euler products).

For the rest of the proof, we shall suppose that $J - j > 12$. Then $p_{j+1} < x^{1/12}$; otherwise, $\#E(\mathbf{F}_p) \ge p_{j+1} \cdots p_J \ge x^{13/12}$, contradicting that $\#E(\mathbf{F}_p) \le 2x$. (We assume here, as throughout the proof, that x is large.) The maximality of j now implies that

$$p_1 \cdots p_j > x^{1/6}/p_{j+1} > x^{1/12}.$$

Since $p_j < x^{1/12}$, one can choose an integer $r \ge 12$ so that

$$x^{\frac{1}{r+1}} \le p_j < x^{\frac{1}{r}}.$$

The plan for the remainder of the proof is to estimate the contribution from each possible value of r and then to sum on r.

Since $p_{j+1} \ge x^{\frac{1}{r+1}}$, we must have $J - j \le r + 1$; otherwise, $p_{j+1} \cdots p_J \ge p_J x \ge 2x > \#E(\mathbf{F}_p)$, which is absurd. Thus, $\tau(p_{j+1} \cdots p_J) \le 2^{r+1}$. An alternative upper bound is provided by the maximal order of the divisor function, which guarantees that every $n \le 2x$ has at most $\exp(\log x/\log\log x)$ divisors (see [**22**, Theorem 317, p. 345]). Putting these two facts together,

$$\tau(p_{j+1} \cdots p_J) \le \min\{2^{r+1}, \exp(\log x/\log\log x)\} =: M_r.$$

Thus,

$$\begin{aligned}\tau(\#E(\mathbf{F}_p)) \le \tau(p_{j+1}\cdots p_J)\tau(p_1\cdots p_j) &\le M_r\tau(p_1\cdots p_j)\\ &\le 2M_r \sum_{\substack{d\mid p_1\cdots p_j\\ d\ge\sqrt{p_1\cdots p_j}}} 1 \le 2M_r \sum_{\substack{d\mid \#E(\mathbf{F}_p)\\ x^{1/24}<d\le x^{1/6}\\ q\mid d\Rightarrow q\le x^{1/r}}} 1.\end{aligned}$$

We now sum on p (keeping (5·2) in mind) and then on r. We find that the sum of $\tau(\#E(\mathbf{F}_p))$ over the remaining values of p is

$$\ll \mathrm{Li}(x) \sum_{12\le r\le \frac{\log x}{\log 2}} M_r \sum_{\substack{x^{1/24}<d\le x^{1/6}\\ q\mid d\Rightarrow q\le x^{1/r}}} \frac{1}{\varphi(d)}. \tag{5·3}$$

Note that we have restricted r in order to have $x^{1/r}\ge 2$.

To continue, we investigate the contribution to (5·3) from various ranges of r. First suppose r is very large, meaning that $x^{1/r}\le(\log x)^2$. In this case, for all t with $x^{1/24}\le t\le x^{1/6}$, we have $x^{1/r}\le(\log t)^{5/2}$, and so $\Psi(t,x^{1/r})\le t^{2/3}$ (say), from Proposition 5·2(ii). Using the lower estimate $\varphi(d)\gg d/\log\log x$ along with partial summation,

$$\sum_{\substack{x^{1/24}<d\le x^{1/6}\\ q\mid d\Rightarrow q\le x^{1/r}}} \frac{1}{\varphi(d)} \ll \log_2 x\left(\frac{\Psi(x^{1/6},x^{1/r})}{x^{1/6}} + \int_{x^{1/24}}^{x^{1/6}} \frac{\Psi(t,x^{1/r})}{t^2}\,dt\right) \ll \log_2 x\cdot x^{-1/72}.$$

Using $M_r\le\exp(\log x/\log\log x)$ in (5·3), we see that these r contribute

$$\ll \mathrm{Li}(x)\cdot\exp(\log x/\log\log x)\cdot\log x\cdot(\log_2 x\cdot x^{-1/72}) \ll x^{0.99}.$$

Suppose now that $x^{1/r}\ge(\log x)^2$. Then also $x^{1/r}\ge(\log t)^2$ whenever $x^{1/24}\le t\le x^{1/6}$. Moreover, for t in this range we have $\frac{\log t}{\log(x^{1/r})}\ge\frac{1}{24}r$. Assuming that r exceeds a certain absolute constant, Proposition 5·2(i) shows that $\Psi(t,x^{1/r})\le t\exp(-\frac{1}{50}r\log r)$. Applying partial summation gives

$$\sum_{\substack{x^{1/24}<d\le x^{1/6}\\ q\mid d\Rightarrow q\le x^{1/r}}} \frac{1}{d} \ll \exp(-\frac{1}{50}r\log r)\log x.$$

To obtain a corresponding upper bound on the sum of $\frac{1}{\varphi(d)}$, we apply Cauchy–Schwarz:

$$\sum_{\substack{x^{1/24}<d\le x^{1/6}\\ q\mid d\Rightarrow q\le x^{1/r}}} \frac{1}{\varphi(d)} \ll \left(\sum_{\substack{x^{1/24}<d\le x^{1/6}\\ q\mid d\Rightarrow q\le x^{1/r}}} \frac{1}{d}\right)^{1/2} \left(\sum_{d\le x^{1/6}} \frac{d}{\varphi(d)^2}\right)^{1/2}.$$

We already estimated the first right-hand sum, while the second right-hand sum is $\ll \prod_{q\le x^{1/6}}(1+q/\varphi(q^2)+\dots)\ll\log x$. Consequently,

$$\sum_{\substack{x^{1/24}<d\le x^{1/6}\\ q\mid d\Rightarrow q\le x^{1/r}}} \frac{1}{\varphi(d)} \ll \exp(-\frac{1}{100}r\log r)\log x.$$

Inserting this estimate back into (5·3) and using $M_r\ll 2^r$, we see that this range of r

contributes

$$\ll \mathrm{Li}(x)\cdot \log x \cdot \sum_{r} 2^r \exp(-\frac{1}{100} r\log r) \ll x,$$

since the sum on r is $O(1)$.

It remains to consider absolutely bounded values of r. But these can be handled trivially. The sum on d in (5·3) is always $O(\log x)$, and so each individual r contributes only $O(x)$. So the contribution from absolutely bounded r is also $O(x)$. □

Remarks.

(i) Wolke has shown how Erdős's method can be applied to estimate the average of the divisor function (and similar functions) along general sequences satisfying standard sieve hypotheses [**35**]. Although his upper bound result [**35**, Satz 1] is stated in a form that precludes a direct application in our context, its proof has much in common with the arguments presented above.

(ii) Erdős's method, in an incarnation very similar to that presented above, can be used to improve a recent result of Gun and Murty [**16**]. Assume GRH for Artin L-series. Let f be a cusp form for $\Gamma_0(N)$ of even weight $k\ge 2$ that is a normalized eigenform for the Hecke operators. Assume that f does not have complex multiplication. Write $f(z)=\sum_{n\ge 1} a_n \exp(2\pi i n z)$, and suppose that each $a_n\in\mathbf{Z}$. Gun and Murty proved that for $x > x_0(f)$,

$$x \ll_f \sum_{\substack{p\le x\\ a(p)\neq 0}} \tau(a(p)) \ll_f x(\log x)^{O_f(1)}.$$

They used a majorant for the divisor function appearing in [**13**]. If Erdős's method is used in its stead, one gets an upper bound of $\ll_f x$, and thus the correct order of magnitude for the sum.

6. *Heuristic arguments*

We set up for the proof of Conjecture 1·2 by studying certain matrix counts modulo n. Let

$$N_C(n) = \#\{g\in \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) : \det(g)+1-\mathrm{tr}(g)=0\}.$$

By the Chinese remainder theorem, $N_C(n)$ is multiplicative in n, and so to determine $N_C(n)$ in general it suffices to study the case when $n=q^k$ is a prime power.

Let $N_C(r;n)$ be defined in the same way as $N_C(n)$ but with the additional restriction that $\det g = r$. The next result is a special case of a theorem of Castryck and Hubrechts [**4**].

PROPOSITION 6·1. *Let q be a prime, and let k be a positive integer. For every integer r coprime to q,*

$$N_C(r;q^k) = \begin{cases} q^{2k}+q^{2k-1} & \text{if } (r-1)^2 \not\equiv 0 \pmod{q^k},\\ q^{2k}+q^{2k-1}-q^{\lfloor (3k-1)/2\rfloor} & \text{otherwise.}\end{cases}$$

Proof. This follows from the formulas for $\Psi(\Delta)$ in [**4**] upon choosing $\Delta=(r-1)^2$; see [**4**, p. 234] for these formulas in the case of odd q (there denoted ℓ) and [**4**, p. 237] for the case $q=2$. □

COROLLARY 6·2. *For each positive integer k,*

$$N_C(q^k) = q^{3k} - q^{3k-2} - q^{2k-1}.$$

Proof. We sum $N_C(r;q^k)$ over a complete set of invertible residue classes r mod q^k. Since $(r-1)^2 \equiv 0 \pmod{q^k}$ precisely when $r \equiv 1 \pmod{q^{\lceil k/2 \rceil}}$, the number of such r mod q^k is $q^{\lfloor k/2 \rfloor}$. Hence,

$$N_C(q^k) = \sum_r N_C(r;q^k) = (q^{2k}+q^{2k-1})(\varphi(q^k)-q^{\lfloor k/2 \rfloor})+(q^{2k}+q^{2k-1}-q^{\lfloor (3k-1)/2 \rfloor})q^{\lfloor k/2 \rfloor}.$$

This simplifies, after straightforward computations, to the formula of the corollary. □

Derivation of Conjecture 1·2 Fix a non-CM elliptic curve $E/\mathbf{Q}$. For each integer d, let $L_d = \mathbf{Q}(E[d])$ be the field obtained by adjoining the coordinates of the d-torsion points over $\overline{\mathbf{Q}}$. Since $E[d](\overline{\mathbf{Q}}) \cong \mathbf{Z}/d\mathbf{Z} \oplus \mathbf{Z}/d\mathbf{Z}$, the action of $G(d) := \mathrm{Gal}(L_d/\mathbf{Q})$ on $E[d](\overline{\mathbf{Q}})$ induces (upon choosing a basis for the d-torsion) an injective homomorphism $\rho_d\colon G(d) \hookrightarrow \mathrm{GL}_2(\mathbf{Z}/d\mathbf{Z})$. A remarkable theorem of Serre [**29**] asserts the existence of a natural number M_E with the following properties:

- If $(d, M_E) = 1$, then ρ_d is an isomorphism,
- If $(d_1, M_E) = (d_1, d_2) = 1$, then $G(d_1 d_2) \cong G(d_1) \times G(d_2)$,
- If $M_E \mid d$, then $G(d) \subset \mathrm{GL}_2(\mathbf{Z}/d\mathbf{Z})$ is the full inverse image of the set $G(M_E) \subset \mathrm{GL}_2(\mathbf{Z}/M_E\mathbf{Z})$ under the projection map.

Suppose that p is a prime not dividing $d \cdot N_E$, where N_E is the conductor of E. Then $d \mid \#E(\mathbf{F}_p)$ precisely when some (and hence, every) Frobenius element g of p, viewed as an element of $\mathrm{GL}_2(\mathbf{Z}/d\mathbf{Z})$, satisfies

$$\det(g) + 1 - \mathrm{tr}(g) \equiv 0 \pmod{d}. \tag{6·1}$$

Let $C(d)$ consist of those $g \in G(d)$ satisfying (6·1). The Chebotarev density theorem now implies that if d is bounded by a suitably slow-growing function of x, then the number of primes $p \le x$ for which $d \mid \#E(\mathbf{F}_p)$ is $\approx \pi(x)\frac{\#C(d)}{\#G(d)}$. Indeed, this is how David and Wu established (5·1) and (5·2). To derive Conjecture 1·2, we pretend that this approximation is valid for d up to size $\approx x$, at least on average. By exploiting symmetry (in a way similar to that seen in the proof of Theorem 1·1), we could relax this assumption to the range $d \lessapprox x^{1/2}$ by a slightly more complex argument. Since even that limited range is beyond the limits of current technology, and since this would not affect our conclusion, we do not bother with this.

Write $d = d_1 d_2$, where every prime dividing d_1 divides M_E and where $\gcd(d_2, M_E) = 1$. Appealing again to Serre's results, we see that

$$\frac{\#C(d)}{\#G(d)} = \frac{\#C(d_1)}{\#G(d_1)} \cdot \frac{N_C(d_2)}{\#\mathrm{GL}_2(\mathbf{Z}/d_2\mathbf{Z})}.$$

If $p \le x$ and x is sufficiently large, then $\#E(\mathbf{F}_p) \le 2x$. The prediction of the last paragraph leads to the guess that

$$\sideset{}{^*}\sum_{p\le x} \tau(\#E(\mathbf{F}_p)) \overset{?}{\sim} \pi(x) \sum_{\substack{d_1 d_2 \le 2x\\ q\mid d_1 \Rightarrow q\mid M_E\\ \gcd(d_2, M_E)=1}} \frac{\#C(d_1)}{\#G(d_1)} \cdot \frac{N_C(d_2)}{\#\mathrm{GL}_2(\mathbf{Z}/d_2\mathbf{Z})}$$

$$= \pi(x) \sum_{\substack{d_1 \le 2x\\ q\mid d_1 \Rightarrow q\mid M_E}} \frac{\#C(d_1)}{\#G(d_1)} \sum_{\substack{d_2 \le 2x/d_1\\ \gcd(d_2, M_E)=1}} \frac{N_C(d_2)}{\#\mathrm{GL}_2(\mathbf{Z}/d_2\mathbf{Z})}.$$

For the moment, we focus attention on the sum on d_2. Let f be the multiplicative function $n \mapsto \frac{N_C(n)}{\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})}\mathbf{1}_{(n,M_E)=1}$. Corollary 6·2 gives us an exact expression for $N_C(q^k)$. Moreover, it is elementary to compute that

$$\#\mathrm{GL}_2(\mathbf{Z}/q^k\mathbf{Z}) = q^{4(k-1)} \cdot \#\mathrm{GL}_2(\mathbf{Z}/q\mathbf{Z}) = q^{4(k-1)} q(q-1)^2(q+1). \qquad (6{\cdot}2)$$

One can use these expressions to check that the function $F(n) := nf(n)$ satisfies the hypotheses of Proposition 2·1 with $\kappa = 1$. Applying Wirsing's theorem, Mertens' theorem, and partial summation as in the proof of Theorem 1·1 — specifically the computation there of the mean value of $g([8,d])/g(8)$ — we conclude that as $y \to \infty$,

$$\sum_{n\le y} f(n) \sim \left(\prod_{q\le y}\left(1-\frac{1}{q}\right)\left(1+f(q)+f(q^2)+\dots\right)\right)\log y$$

$$\sim \frac{\varphi(M_E)}{M_E} \prod_{\substack{q\le y\\ q\nmid M_E}} \left(\left(1-\frac{1}{q}\right)\left(1+\sum_{k=1}^{\infty}\frac{N_C(q^k)}{\#\mathrm{GL}_2(\mathbf{Z}/q^k\mathbf{Z})}\right)\right)\log y. \qquad (6{\cdot}3)$$

To handle the sum on k, we use the evaluation of $N_C(q^k)$ from Corollary 6·2 together with (6·2). After summing the geometric series that appear and simplifying, we find that

$$1+\sum_{k=1}^{\infty}\frac{N_C(q^k)}{\#\mathrm{GL}_2(\mathbf{Z}/q^k\mathbf{Z})} = \frac{q^5-q^3-1}{(q^2-1)^2(q-1)},$$

so that

$$\left(1-\frac{1}{q}\right)\left(1+\sum_{k=1}^{\infty}\frac{N_C(q^k)}{\#\mathrm{GL}_2(\mathbf{Z}/q^k\mathbf{Z})}\right) = 1+\frac{q^3-q-1}{(q^2-1)^2 q}.$$

Since this expression is always nonzero and has the form $1+O(1/q^2)$, the product over q in (6·3) tends, as $y\to\infty$, to the positive limit

$$c_{E,\mathrm{Euler}} := \prod_q \left(1+\frac{q^3-q-1}{(q^2-1)^2 q}\right).$$

Thus, $\sum_{n\le y} f(n) \sim \frac{\varphi(M_E)}{M_E} c_{E,\mathrm{Euler}} \cdot \log y$, as $y\to\infty$.

Ignoring the error in the above approximation of $\sum_{n\le y} f(n)$, we are led to expect that

$$\sum_{d_1\le 2x} \sum_{\substack{d_1 \le 2x\\ q\mid d_1 \Rightarrow q\mid M_E}} \frac{\#C(d_1)}{\#G(d_1)} \sum_{\substack{d_2 \le 2x/d_1\\ \gcd(d_2, M_E)=1}} \frac{N_C(d_2)}{\#\mathrm{GL}_2(\mathbf{Z}/d_2\mathbf{Z})}$$

$$\sim \frac{\varphi(M_E)}{M_E} c_{E,\mathrm{Euler}} \sum_{\substack{d_1 \le 2x\\ q\mid d_1 \Rightarrow q\mid M_E}} \frac{\#C(d_1)}{\#G(d_1)} \log\frac{2x}{d_1},$$

as $x \to \infty$. (In fact, this part of the argument could easily be made rigorous.) Now David and Wu have shown that for every d_1 supported on the primes dividing M_E, one has $\#C(d_1)/\#G(d_1) \ll 1/\varphi(d_1)$, where the constant may depend on E (see [**9**, Lemma 2.2]). Hence,

$$c_{E,\mathrm{bad}} := \sum_{\substack{d_1 \geq 1 \\ q \mid d_1 \Rightarrow q \mid M_E}} \frac{\#C(d_1)}{\#G(d_1)} < \infty.$$

(Indeed, the sum defining $c_{E,\mathrm{bad}}$ is $\ll \prod_{q \mid M_E} (\sum_{k=0}^{\infty} \varphi(q^k)^{-1})$.) Clearly, $c_{E,\mathrm{bad}} > 0$, since $d_1 = 1$ already contributes 1 to the sum. By partial summation,

$$\sum_{\substack{d_1 \leq 2x \\ q \mid d_1 \Rightarrow q \mid M_E}} \frac{\#C(d_1)}{\#G(d_1)} \log \frac{2x}{d_1} \sim c_{E,\mathrm{bad}} \log x.$$

Putting the pieces back together, we are left with the conjecture that

$$\sum_{p \leq x}{}^{*}\, \tau(\#E(\mathbf{F}_p)) \overset{?}{\sim} \frac{\varphi(M_E)}{M_E} c_{E,\mathrm{bad}} c_{E,\mathrm{Euler}} \cdot (\pi(x) \log x),$$

which is equivalent to Conjecture 1·2 with $c_E = \frac{\varphi(M_E)}{M_E} c_{E,\mathrm{bad}} c_{E,\mathrm{Euler}}$. □

Remark. We conclude the paper by describing a double average variant of Conjecture 1·2. Define

$$c_{\mathrm{Euler}} = \prod_{q} \left(1 + \frac{q^3 - q - 1}{(q^2-1)^2 q}\right).$$

It seems plausible that the average value of $\tau(\#E(\mathbf{F}_p))$, taken over all $p \leq x$ and curves E mod p, is $\sim c_{\mathrm{Euler}} \log x$, as $x \to \infty$.

Let us be more precise. By $\sum_{E/\mathbf{F}_p}^{\dagger}$, we agree to mean a sum over isomorphism classes of elliptic curves E mod p, where the terms corresponding to the class of E are weighted by the factor $\frac{1}{\#\mathrm{Aut}_{\mathbf{F}_p}(E)}$. If $p > 3$, then there are precisely $\frac{p-1}{\#\mathrm{Aut}_{\mathbf{F}_p}(E)}$ short Weierstrass equations over $\mathbf{F}_p$ defining curves isomorphic to E. Thus, our convention on $\sum_{E/\mathbf{F}_p}^{\dagger}$ corresponds to assigning each short Weierstrass equation equal weight. (The cases when $p = 2$ and $p = 3$ may be ignored for our purposes, since they make a vanishing contribution once we average over p.)

Gekeler [**15**, Corollary 5.2] has determined the 'probability' that a random elliptic curve over a prime finite field has order divisible by a fixed natural number d:

$$\frac{\sum_{p \leq x} \sum^{\dagger}_{E/\mathbf{F}_p} \mathbf{1}_{d \mid \#E(\mathbf{F}_p)}}{\sum_{p \leq x} \sum^{\dagger}_{E/\mathbf{F}_p} 1} \to g(d) \quad (\text{as } x \to \infty), \tag{6·4}$$

where

$$g(d) := \frac{1}{d} \prod_{q^k \| d} \frac{q^3 - q - q^{2-k}}{(q^2-1)(q-1)}.$$

For each $p \leq 2x$ and each curve $E/\mathbf{F}_p$, we have $\tau(\#E(\mathbf{F}_p)) = \sum_{d \leq 2x} \mathbf{1}_{d \mid E(\mathbf{F}_p)}$. Comparing with (6·4) suggests that perhaps

$$\frac{\sum_{p\le x}\sum^{\dagger}_{E/\mathbf{F}_p}\tau(\#E(\mathbf{F}_p))}{\sum_{p\le x}\sum^{\dagger}_{E/\mathbf{F}_p}1}\overset{?}{\sim}\sum_{d\le 2x} g(d)\quad (\text{as } x\to\infty). \tag{6·5}$$

The function $d\mapsto d\cdot g(d)$ satisfies the conditions of Proposition 2·1 with $\kappa=1$, and a now-familiar argument shows that

$$\sum_{d\le 2x} g(d)\sim\prod_{q\le 2x}\left(1-\frac{1}{q}\right)\left(1+g(q)+g(q^2)+\dots\right)\log x,$$

as $x\to\infty$. A direct computation shows that

$$\begin{aligned}\left(1-\frac{1}{q}\right)\left(1+g(q)+g(q^2)+\dots\right)&=\left(1-\frac{1}{q}\right)\left(1+\sum_{k=1}^{\infty}\frac{1}{q^k}\frac{q^3-q-q^{2-k}}{(q^2-1)(q-1)}\right)\\&=\left(1-\frac{1}{q}\right)\left(\frac{q^5-q^3-1}{(q^2-1)^2\cdot(q-1)}\right)=1+\frac{q^3-q-1}{(q^2-1)^2q},\end{aligned}$$

which is the qth factor in c_{Euler}. Thus, the right-hand side of (6·5) is $\sim c_{\text{Euler}}\log x$.

Gekeler's arguments rely on earlier work of Howe [**19**], who obtained his results from a detailed study of modular curves (extending an approach of Lenstra [**25**]). Unfortunately, the error terms in Howe's work are too large to rigorously justify the conjecture of the last paragraph. Nevertheless, the similarity between c_{Euler} and $c_{E,\text{Euler}}$ is rather encouraging, given that Conjecture 1·2 was suggested by an entirely distinct line of reasoning.

Acknowledgements. The author thanks Pete L. Clark for many enlightening discussions about elliptic curves, and in particular for supplying the argument at the start of §4 allowing us to reduce to the case when E has CM by $\mathbf{Z}_K$. He also thanks Greg Martin and Ethan Smith for useful conversations, and the referee for the pointer to the work of Castryck and Hubrechts, which led to a much shorter proof of Corollary 6·2. The application in §5 of Erdős's method owes much to a beautifully written blog post of Terence Tao [**32**].

REFERENCES

[**1**] A. Akbary and A. T. Felix. On invariants of elliptic curves on average. *Acta Arith.* **168** (2015) 31–70.

[**2**] A. Akbary and D. Ghioca. A geometric variant of Titchmarsh divisor problem. *Int. J. Number Theory* **8** (2012) 53–69.

[**3**] P. L. Clark, B. Cook, and J. Stankewicz. Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice). *Int. J. Number Theory* **9** (2013) 447–479.

[**4**] W. Castryck and H. Hubrechts. The distribution of the number of points modulo an integer on elliptic curves over finite fields. *Ramanujan J.* **30** (2013) 223–242.

[**5**] N. Childress. *Class field theory* (Springer, New York, 2009).

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

[**7**] W. Duke. Almost all reductions modulo p of an elliptic curve have a large exponent. *C. R. Math. Acad. Sci. Paris* **337** (2003) 689–692.

[**8**] C. David and J. Wu. Almost prime values of the order of elliptic curves over finite fields. *Forum Math.* **24** (2012) 99–119.

[**9**] ———, Pseudoprime reductions of elliptic curves. *Canad. J. Math.* **64** (2012) 81–101.

[**10**] N. D. Elkies. Distribution of supersingular primes. *Astérisque* (Proceedings of Journées Arithmétiques, Luminy, 1989) **198-200** (1992) 127–132.

[**11**] P. D. T. A. Elliott. On the mean value of $f(p)$. *Proc. London Math. Soc.* (3) **21** (1970) 28–96.

[**12**] P. Erdős. On the sum $\sum_{k=1}^{x} d(f(k))$. *J. London Math. Soc.* **27** (1952) 7–15.

[**13**] J. B. Friedlander and H. Iwaniec. Divisor weighted sums. *Zap. Nauchn. Sem. POMI* **322** (2005) 212–219.

[**14**] A. T. Felix and M. Ram Murty. On the asymptotics for invariants of elliptic curves modulo p. *J. Ramanujan Math. Soc.* **28** (2013) 271–298.

[**15**] E.-U. Gekeler. The distribution of group structures on elliptic curves over finite prime fields. *Doc. Math.* **11** (2006) 119–142 (electronic).

[**16**] S. Gun and M. Ram Murty. Divisors of Fourier coefficients of modular forms. *New York J. Math.* **20** (2014) 229–239.

[**17**] A. Granville. Smooth numbers: computational number theory and beyond. *Algorithmic number theory: lattices, number fields, curves and cryptography.* Math. Sci. Res. Inst. Publ. **44**, 267–323 (Cambridge Univ. Press, Cambridge, 2008).

[**18**] J. Hinz and M. Lodemann. On Siegel zeros of Hecke-Landau zeta-functions. *Monatsh. Math.* **118** (1994) 231–248.

[**19**] E. W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Math.* **85** (1993) 229–247.

[**20**] H. Halberstam and H.-E. Richert. *Sieve methods.* London Mathematical Society Monographs **4** (Academic Press, London-New York, 1974).

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

[**22**] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers (sixth ed.)* (Oxford University Press, Oxford, 2008).

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

[**24**] S. Lang. *Elliptic functions (second ed.).* Graduate Texts in Mathematics **112** (Springer-Verlag, New York, 1987).

[**25**] H. W. Lenstra, Jr.. Factoring integers with elliptic curves. *Ann. of Math.* (2) **126** (1987) 649–673.

[**26**] U. V. Linnik. *The dispersion method in binary additive problems.* Translations of mathematical monographs **4** (Amer. Math. Soc., Providence, RI, 1963).

[**27**] P. Moree and J. Cazaran. On a claim of Ramanujan in his first letter to Hardy. *Exposition. Math.* **17** (1999) 289–311.

[**28**] A. R. Rajwade. Arithmetic on curves with complex multiplication by $\sqrt{-2}$. Proc. Cambridge Philos. Soc. **64** (1968) 659–672.

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

[**30**] P. Shiu. A Brun-Titchmarsh theorem for multiplicative functions. *J. Reine Angew. Math.* **313** (1980) 161–170.

[**31**] A. Silverberg. Group order formulas for reductions of CM elliptic curves. *Arithmetic, geometry, cryptography and coding theory 2009.* Contemp. Math. **521**, 107–120 (Amer. Math. Soc., Providence, RI, 2010).

[**32**] T. Tao. Erdős's divisor bound. Blog post published July 23, 2011 at `http://terrytao.wordpress.com/2011/07/23/erdos-divisor-bound/`. To appear in the forthcoming book *Spending symmetry.*

[**33**] E. C. Titchmarsh. A divisor problem. *Rend. Circ. Mat. Palermo* **54** (1930) 414–429. Errata in **57** (1933) 478–479.

[**34**] E. Wirsing. Das asymptotische Verhalten von Summen über multiplikative Funktionen. *Math. Ann.* **143** (1961) 75–102.

[**35**] D. Wolke. Multiplikative Funktionen auf schnell wachsenden Folgen. *J. Reine Angew. Math.* **251** (1971) 54–67.