THE AVERAGE OF THE FIRST INVARIANT FACTOR FOR REDUCTIONS OF CM ELLIPTIC CURVES MOD p

TRISTAN FREIBERG AND PAUL POLLACK

ABSTRACT. Let $E/\mathbb{Q}$ be a fixed elliptic curve. For each prime p of good reduction, write $E(\mathbb{F}_p) \cong \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}$, where $d_p \mid e_p$. Kowalski proposed investigating the average value of d_p as p runs over the rational primes. For CM curves, he showed that $x \log\log x / \log x \ll \sum_{p \leq x} d_p \ll x\sqrt{\log x}$. It was shown recently by Felix and Murty that in fact $\sum_{p \leq x} d_p$ exceeds any constant multiple of $x \log\log x / \log x$, once x is sufficiently large. In the opposite direction, Kim has shown that the expression $x\sqrt{\log x}$ in the upper bound can be replaced by $x \log\log x$. In this paper, we obtain the correct order of magnitude for the sum: $\sum_{p \leq x} d_p \asymp x$ for all large x.

1. INTRODUCTION

Let $E/\mathbb{Q}$ be a fixed elliptic curve. For each rational prime p of good reduction, there are uniquely defined natural numbers d_p and e_p with $E(\mathbb{F}_p) \cong \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}$. From a statistical point of view, it is natural to inquire about the behavior of d_p and e_p as p varies. This is all the more true given that d_p and e_p have arithmetic significance: d_p is the largest integer prime to p for which all of the d-torsion is rational over $\mathbb{F}_p$, and e_p is the largest order of any element of $E(\mathbb{F}_p)$. Note that the sizes of d_p and e_p are closely intertwined, since $d_p e_p = \#E(\mathbb{F}_p) \in [(\sqrt{p}-1)^2, (\sqrt{p}+1)^2]$ by a celebrated theorem of Hasse.

For notational convenience, set $d_p = e_p = 0$ when E has bad reduction at p.

Responding to a suggestion of Silverman, Freiberg and Kurlberg [FK14] investigated the average size of e_p. They showed that as $x \to \infty$, one has $\sum_{p \leq x} e_p \sim c_E \mathrm{Li}(x^2)$ for a certain constant $c_E \in (0,1)$. Their result is unconditional if E has CM and conditional on the Generalized Riemann Hypothesis otherwise.

It is a simple consequence of the prime number theorem that $\sum_{p \leq x} p \sim \mathrm{Li}(x^2)$. Keeping in mind that $d_p e_p \sim p$, the result of Freiberg and Kurlberg suggests that d_p is usually quite small. In fact, Duke [Duk03] has shown that for any function $\xi(p) \to \infty$, one has $d_p < \xi(p)$ for asymptotically 100% of primes p. (Again, GRH is assumed here unless E has CM.) Duke's result tells us about the normal size of d_p. What about the average size?

In fact, the problem of determining the average order of d_p was proposed by Kowalski already in 2000. For reasons explained in [Kow06, §3.2], it is natural to conjecture that as $x \to \infty$, $\sum_{p \leq x} d_p$ is $\sim c'_E X$ when E has CM and $\sim c'_E \mathrm{Li}(x)$ otherwise, where $c'_E > 0$. These conjectures remain open, even under GRH.

There has been only meager progress towards Kowalski's conjectures in the case when E does not have complex multiplication. In what follows, we restrict our discussion to the CM case. There Kowalski showed that for large x,

$$\frac{x \log \log x}{\log x} \ll \sum_{p \leq x} d_p \ll x\sqrt{\log x};$$

moreover, under GRH, the sum is $\gg x$. Unconditionally, Felix and Murty [FM13] showed that for any A and all sufficiently large x, we have $\sum_{p \leq x} d_p > Ax \log \log x / \log x$. In the opposite direction, Kim showed (among other things) that in the upper bound, the expression $x\sqrt{\log x}$ can be replaced by $x \log \log x$ [Kim14].

In this paper, we establish the correct order of magnitude for the partial sums of d_p.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. Then*

$$\sum_{p \leq x} d_p \ll x;$$

here the implied constant is absolute. Moreover, for $x > x_0(E)$,

$$\sum_{p \leq x} d_p \gg_E x.$$

If one replaces d_p with d_p^α, for a fixed $\alpha \in (0,1)$, then Felix and Murty (op. cit.) have exhibited an asymptotic formula for the partial sums, conditional on GRH. The main term in their formula has the shape $c_{\alpha,E}\mathrm{Li}(x)$, so that d_p^α is bounded on average. Hence $\alpha = 1$ is a transition point, since, by our main theorem, d_p itself is $\asymp \log x$ on average over $p \leq x$.

The proofs of the upper and lower bounds are based on distinct principles. Hence, the upper bound is treated in §2 while the lower bound is treated separately in §§3 and 4.

Notation. We use the letter K for an algebraic number field. We let d_K denote the absolute value of the (absolute) discriminant of K. $\mathcal{O}_K$ denotes the the ring of integers of K. For $\alpha \in K$, we write $\mathrm{Nm}(\alpha)$ for the norm of α and $\mathrm{Tr}(\alpha)$ for its trace. For an ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we let $\mathrm{Nm}(\mathfrak{a}) := \#\mathcal{O}_K/\mathfrak{a}$ and we let $\Phi(\mathfrak{a}) := \#(\mathcal{O}_K/\mathfrak{a})^\times$. For $\alpha \in \mathcal{O}_K$, we let $\Phi(\alpha)$ be the Φ function applied to the principal ideal (α).

The case when K is an imaginary quadratic extension of $\mathbb{Q}$ plays a special role for us. If $K = \mathbb{Q}(\sqrt{g})$ where $g < 0$ is squarefree, then we set $\omega = \sqrt{g}$ if $g \equiv 2$ or $3 \pmod 4$ and $\omega = \frac{1+\sqrt{g}}{2}$ otherwise. Thus, $1, \omega$ form an integral basis of K. We use the symbol $\mathcal{O}$ to denote a possibly nonmaximal order of K.

The letters ℓ and p are reserved for rational primes. We use $\mathfrak{p}$ for a maximal ideal of $\mathcal{O}_K$. If $\mathfrak{p}$ lies over the rational prime p, then $\deg(\mathfrak{p})$ denotes the dimension of $\mathcal{O}_K/\mathfrak{p}$ over $\mathbb{Z}/p\mathbb{Z}$.

2. The upper bound in Theorem 1.1

2.1. **Preliminaries.** We begin by recording an important alternative description of d_p in the case when p is of good ordinary reduction. Let us fix notation. Suppose that

$E/\mathbb{Q}$ is an elliptic curve with complex multiplication by an order $\mathcal{O}$ in the imaginary quadratic field K. Since E is defined over $\mathbb{Q}$, the field K is one of the nine imaginary quadratic fields of class number 1, and $\mathcal{O}$ is one of the thirteen imaginary quadratic orders of class number 1. (See [Sil94, p. 483] for a list of these orders along with the corresponding curves.) A rational prime p of good reduction is an ordinary prime if and only if p splits completely in K; in that case, as long as p does not divide the conductor of $\mathcal{O}$, we can identify $\mathcal{O}$ with the ring of endormorphisms of the reduced curve E mod p. (For these last two statements, see [Lan87, Theorem 12, p. 182].) Since our orders $\mathcal{O}$ all have conductor at most 3, we can make this identification whenever $p > 3$.

Lemma 2.1. *Let $p > 3$ be a prime at which E has good ordinary reduction. Let $\pi_p \in \mathcal{O}$ be the Frobenius endormorphism of the reduced curve. Then d divides d_p if and only if $\pi_p \equiv 1 \pmod{d}$ in $\mathcal{O}$.*

Proof. For integers d coprime to p, we have

$$d \mid d_p \iff E[d](\overline{\mathbb{F}_p}) \subset E(\mathbb{F}_p) \qquad \text{(see [Kow06, Lemma 2.3(i)])}$$
$$\iff \pi_p \equiv 1 \pmod{d} \text{ in } \mathcal{O} \qquad \text{(see [Kow06, Lemma 2.6]).}$$

Now suppose that $p \mid d$. We will show that we have neither $d \mid d_p$ nor $\pi_p \equiv 1 \pmod{d}$. Since $d_p^2 \mid \#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_p) \le (\sqrt{p}+1)^2$, we have $d_p \le \sqrt{p}+1 < p$. Hence, d_p is not a multiple of p and so not a multiple of d. Since $\#E(\mathbb{F}_p) = \mathrm{Nm}(\pi_p - 1)$, if $\pi_p \equiv 1 \pmod{d}$, then $p^2 \mid d^2 \mid \#E(\mathbb{F}_p)$. This leads to the absurd inequality $p^2 \le \#E(\mathbb{F}_p) \le (\sqrt{p}+1)^2$. $\square$

We also require two items from the analytic toolchest. The first is a Brun–Titchmarsh inequality for imaginary quadratic fields. This appears as [Pol14, Lemma 2.5], where it is deduced from a Brun–Titchmarsh theorem for prime ideals established by Hinz and Lodemann [HL94, Theorem 4]. Let

$$\pi(x; \mu, \alpha) := \#\{\text{prime elements } \pi : \mathrm{Nm}(\pi) \le x, \pi \equiv \alpha \pmod{\mu}\}.$$

Lemma 2.2. *Let $x \ge 3$. Suppose that $\mu, \alpha \in \mathcal{O}_K$ generate comaximal ideals. If $\mathrm{Nm}(\mu) < x$, then*

$$\pi(x; \mu, \alpha) \ll \frac{x}{\Phi(\mu) \log \frac{x}{\mathrm{Nm}(\mu)}}.$$

The implied constant may depend on K.

Remark. In the statement of [Pol14], K is assumed to be of class number 1. In fact, the proof indicated in [Pol14] goes through without any restriction on the class number of K. Note that if we assume K has bounded class number, then there are only finitely many possibilities for K, and so the implied constant of the lemma can be chosen uniformly.

The following lemma, which is a weakened form of a theorem of Halberstam and Richert [HR79] (compare with [SS94, Theorem 3.2, p. 58]), is a versatile upper bound result for mean values of multiplicative functions.

Lemma 2.3. *Let λ_1, λ_2 be positive constants with $\lambda_2 < 2$. Suppose that g is a nonnegative-valued multiplicative function with $g(p^k) \leq \lambda_1 \lambda_2^k$ for all primes p and all positive integers k. Then*

$$\sum_{n \leq x} g(n) \ll_{\lambda_1, \lambda_2} x \prod_{p \leq x} \left(1 - \frac{1}{p}\right)\left(1 + \frac{g(p)}{p} + \frac{g(p^2)}{p^2} + \cdots\right).$$

2.2. **The proof proper.** We begin by discarding from $\sum_{p \leq x} d_p$ all supersingular primes p. It is simple to show that for each supersingular prime, one has $d_p \leq 2$, and so these terms contribute only $O(x/\log x)$. (For details, see the proof of [Kow06, Corollary 6.2].)

Let $\sum_p'$ denote a sum restricted to primes p of good ordinary reduction. To prove the upper bound in Theorem 1.1, it suffices to show that $\sum_{3 < p \leq x}' d_p \ll x$. Recall that $m = \sum_{d|m} \varphi(d)$ for every positive integer m. Since $d_p \leq \sqrt{p} + 1 \leq 2\sqrt{x}$ for all $p \leq x$,

$$\sum_{3 < p \leq x}' d_p = \sum_{3 < p \leq x}' \sum_{d | d_p} \varphi(d)$$

$$(1) \qquad\qquad = \sum_{d \leq 2\sqrt{x}} \varphi(d) \sum_{\substack{3 < p \leq x \\ d | d_p}}' 1.$$

We first show that those $d \leq x^{1/3}$ make a contribution to (1) of size $O(x)$. This estimate is already implicit in the works of both Kowalski and Kim, but we include the argument for completeness.

For each prime p counted in the inner sum of (1), the Frobenius element $\pi_p \in \mathcal{O}$ is a prime of $\mathcal{O}_K$ with $\pi_p \equiv 1 \pmod{d}$ and $\mathrm{Nm}(\pi_p) = p$. So by Lemma 2.2, that sum is $\ll \frac{1}{\Phi(d)} \frac{x}{\log x}$ uniformly for $d \leq x^{1/3}$, and thus the right-hand side of (1) is

$$\ll \frac{x}{\log x} \sum_{d \leq x^{1/3}} \frac{\varphi(d)}{\Phi(d)}.$$

Writing Δ for the discriminant of K, we have

$$\Phi(d) = d^2 \prod_{\ell | d} \left(1 - \frac{1}{\ell}\right)\left(1 - \frac{\left(\frac{\Delta}{\ell}\right)}{\ell}\right) \geq \varphi(d)^2$$

for all d. Thus, the contribution of $d \leq x^{1/3}$ to (1) is $\ll \frac{x}{\log x} \sum_{d \leq x^{1/3}} \frac{1}{\varphi(d)} \ll \frac{x}{\log x} \cdot \log x = x$, as claimed.

Handling those values of d with $x^{1/3} < d \leq 2\sqrt{x}$ requires a different strategy. Let $I_j = (2^j x^{1/3}, 2^{j+1} x^{1/3}]$, where j runs over all nonnegative integers with $2^j x^{1/3} < 2\sqrt{x}$. We consider the contribution to the right-hand side of (1) from d in each I_j.

Using Lemma 2.1, we see that

$$(2) \qquad\qquad \sum_{\substack{3 < p \leq x \\ d | d_p}}' 1 \leq \sum_{\substack{X, Y \in \mathbb{Z} \\ \mathrm{Nm}((X + Y\omega)d + 1) \leq x \\ \text{and prime}}} 1.$$

If $\mathrm{Nm}((X + Y\omega)d + 1) \leq x$, then $|(X + Y\omega)d| \leq 1 + \sqrt{x} \leq 2\sqrt{x}$. Hence, assuming $d \in I_j$, we must have

$$\mathrm{Nm}(X + Y\omega) \leq 4x/d^2 \leq 2^{2-2j}x^{1/3}.$$

Moreover, if $\mathrm{Nm}((X + Y\omega)d + 1)$ is prime, then $Y \neq 0$. Inserting (2) back into (1) and reversing the order of summation reveals that the $d \in I_j$ contribute at most

$$(3) \qquad \sum_{\substack{X,Y\in\mathbb{Z},\ Y\neq 0 \\ \mathrm{Nm}(X+Y\omega)\leq 2^{2-2j}x^{1/3}}} \sum_{\substack{d\in I_j \\ \mathrm{Nm}((X+Y\omega)d+1)\ \mathrm{prime}}} \varphi(d)$$

$$\ll 2^j x^{1/3} \sum_{\substack{X,Y\in\mathbb{Z},\ Y\neq 0 \\ \mathrm{Nm}(X+Y\omega)\leq 2^{2-2j}x^{1/3}}} \sum_{\substack{d\in I_j \\ \mathrm{Nm}((X+Y\omega)d+1)\ \mathrm{prime}}} 1.$$

The remaining sum on d can be estimated by Brun's sieve. For each $X, Y \in \mathbb{Z}$ with $\mathrm{Nm}(X + Y\omega) \leq 2^{2-2j}x^{1/3}$ and $Y \neq 0$, put

$$F(T) = \mathrm{Nm}(X + Y\omega) \cdot T^2 + \mathrm{Tr}(X + Y\omega) \cdot T + 1 \in \mathbb{Z}[T].$$

(Of course, F depends on X and Y but we suppress this.) Then F is a quadratic polynomial with discriminant $Y^2\Delta$, where as above Δ denotes the discriminant of K. The final sum on d in (3) counts the number of $d \in I_j$ for which $F(d)$ is prime. By the fundamental lemma of the sieve (see [HR74, Theorem 2.2 (5.2), p. 68]), the number of these d is

$$\ll 2^j x^{1/3} \prod_{\ell\leq x} \left(1 - \frac{\rho(\ell)}{\ell}\right),$$

where $\rho(\ell)$ counts the number of roots of F modulo ℓ. Put $D = 2 \cdot \mathrm{Nm}(X + Y\omega) \cdot |Y|$. For ℓ not dividing D, we have $\rho(\ell) = 1 + \left(\frac{\Delta}{\ell}\right)$. Consequently,

$$\prod_{\ell\leq x} \left(1 - \frac{\rho(\ell)}{\ell}\right) \ll \left(\frac{D}{\varphi(D)}\right)^2 \cdot \prod_{\ell\leq x} \left(1 - \frac{\left(\frac{\Delta}{\ell}\right)}{\ell}\right) \prod_{\ell\leq x} \left(1 - \frac{1}{\ell}\right).$$

The first right-hand product over ℓ is $O(1)$, since the product extended to infinity converges to $L(1, \left(\frac{\Delta}{\cdot}\right))^{-1}$. (Note that only finitely many values of Δ are possible, and so the O-constant is absolute.) The second product on ℓ is $\ll (\log x)^{-1}$. Thus,

$$\sum_{\substack{d\in I_j \\ \mathrm{Nm}((X+Y\omega)d+1)\ \mathrm{prime}}} 1 \ll \frac{2^j x^{1/3}}{\log x} \frac{D^2}{\varphi(D)^2},$$

and so the right-hand side of (3) is

$$(4) \qquad \ll \frac{2^{2j} x^{2/3}}{\log x} \sum_{\substack{X,Y\in\mathbb{Z},\ Y\neq 0 \\ \mathrm{Nm}(X+Y\omega)\leq 2^{2-2j}x^{1/3}}} \frac{D^2}{\varphi(D)^2}.$$

We now show that $\frac{D^2}{\varphi(D)^2}$ is bounded on average over X and Y. Notice that

$$\frac{D^2}{\varphi(D)^2} \ll \frac{\mathrm{Nm}(X + Y\omega)^2}{\varphi(\mathrm{Nm}(X + Y\omega))^2} \frac{Y^2}{\varphi(|Y|)^2}.$$

Applying the Cauchy–Schwarz inequality, we deduce that the sum on D in (4) is

$$\ll \left(\sum_{\substack{X,Y \in \mathbb{Z}, \ Y \neq 0 \\ \mathrm{Nm}(X+Y\omega) \leq 2^{2-2j} x^{1/3}}} \frac{\mathrm{Nm}(X + Y\omega)^4}{\varphi(\mathrm{Nm}(X + Y\omega))^4} \right)^{1/2} \left(\sum_{\substack{X,Y \in \mathbb{Z}, \ Y \neq 0 \\ \mathrm{Nm}(X+Y\omega) \leq 2^{2-2j} x^{1/3}}} \frac{Y^4}{\varphi(|Y|)^4} \right)^{1/2}.$$

The second sum on X and Y is the easier of the two to handle. The conditions on X and Y imply that $|X|$ and $|Y|$ are both $O(2^{-j} x^{1/6})$. We now use the known estimate

$$(5) \qquad\qquad \sum_{m \leq t} \frac{m^4}{\varphi(m)^4} \ll t \qquad (\text{for all } t \geq 0)$$

to deduce — summing first on Y and then on X — that this second sum is $O(2^{-2j} x^{1/3})$. The estimate (5) could be proved by applying Lemma 2.3; we omit this, as we shall see a similar but slightly more intricate calculation momentarily. In fact, (5) is classical and a more general result was known already to Schur (see [Ell79, p. 214] for a discussion).

Turning to the first sum, we let $m = \mathrm{Nm}(X + Y\omega)$. Since K has class number 1, the number of $X, Y \in \mathbb{Z}$ with $\mathrm{Nm}(X + Y\omega) = m$ is given by

$$r(m) := w \sum_{e|m} \left(\frac{\Delta}{e} \right),$$

where w is the number of roots of unity in K. (Indeed, in the general case, $\sum_{e|m} \left(\frac{\Delta}{e} \right)$ counts the number of integral ideals of norm m [cf. [Hec81, Theorem 148, p. 179]]. Thus, without using that K has class number 1, we could still conclude that $r(m)$ is an upper bound on the number of pairs X, Y, which would suffice below.) Put $r^*(m) = r(m)/w$ and note that r^* is a multiplicative function taking only nonnegative values. We can bound the first sum on X, Y by

$$w \sum_{m \leq 2^{2-2j} x^{1/3}} r^*(m) \frac{m^4}{\varphi(m)^4}.$$

Since $r^*(m) \leq \tau(m)$, it is easy to see that the hypotheses of Lemma 2.3 are satisfied for $g(n) := r^*(n) \frac{n^4}{\varphi(n)^4}$. Applying that lemma shows that the last displayed quantity is

$$(6) \qquad\qquad \ll 2^{-2j} x^{1/3} \prod_{p \leq 2^{2-2j} x^{1/3}} \left(1 - \frac{1}{p} \right) \left(1 + \sum_{k=1}^{\infty} \frac{r^*(p^k)(p/\varphi(p))^4}{p^k} \right).$$

Now $1 + \sum_{k=1}^{\infty} \frac{r^*(p^k)(p/\varphi(p))^4}{p^k} = 1 + \frac{1}{p} + \frac{\left(\frac{\Delta}{p} \right)}{p} + O(1/p^2)$, so that

$$\left(1 - \frac{1}{p} \right) \left(1 + \sum_{k=1}^{\infty} \frac{r^*(p^k)(p/\varphi(p))^4}{p^k} \right) = 1 + \frac{\left(\frac{\Delta}{p} \right)}{p} + O(1/p^2).$$

Since $\sum_p \left(\frac{\Delta}{p} \right)/p$ converges, we see now that the product in (6) is $\ll 1$, and so (6) itself is $O(2^{-2j} x^{1/3})$. Assembling the estimates of this paragraph and the last yields

$$\sum_{\substack{X, Y \in \mathbb{Z}, \ Y \neq 0 \\ \mathrm{Nm}(X + Y\omega) \leq 2^{2-2j} x^{1/3}}} \frac{D^2}{\varphi(D)^2} \ll 2^{-2j} x^{1/3}.$$

Now from (4), we see that the right-hand side of (3) is $O(x/\log x)$.

It remains to sum this upper bound over the possible values of j. There are only $O(\log x)$ of these, leading to a final upper bound of $O(x)$, as desired.

3. TECHNICAL PRELIMINARIES FOR THE PROOF OF THE LOWER BOUND

The proof of the lower bound half of Theorem 1.1 requires us to recall certain results from the literature on the equidistribution of primes in ray class groups. Our main reference for this material is the paper of Weiss [Wei83], where Linnik's fundamental result on the least prime in a progression is generalized to arbitrary algebraic number fields.

3.1. **Background and notation.** Let K be an algebraic number field. (We do not assume to begin with that K is imaginary quadratic, though in our application this will be the case.) Suppose $[K : \mathbb{Q}] = n = r_1 + 2r_2$, where r_1 is the number of real embeddings of K and r_2 the number of pairs of complex conjugate embeddings. If $\mathfrak{m}$ is a (nonzero) ideal of $\mathcal{O}_K$, let $I(\mathfrak{m})$ denote the group of fractional ideals relatively prime to $\mathfrak{m}$, and let $P_\mathfrak{m}$ be the subgroup defined by

$$P_\mathfrak{m} := \{\alpha \mathcal{O}_K : \alpha \in K^\times, \alpha \text{ totally positive }, \alpha \equiv 1 \bmod^* m\}.$$

The *narrow class group* mod $\mathfrak{m}$ is the quotient $I(\mathfrak{m})/P_\mathfrak{m}$. We say $\mathfrak{a}, \mathfrak{b} \in I(\mathfrak{m})$ are *strictly equivalent* modulo $\mathfrak{m}$, and write $\mathfrak{a} \sim \mathfrak{b} \pmod{\mathfrak{m}}$, if $\mathfrak{a}$ and $\mathfrak{b}$ represent the same coset modulo $P_\mathfrak{m}$. A *(Dirichlet) character modulo* $\mathfrak{m}$ is a character of the finite abelian group $I(\mathfrak{m})/P_\mathfrak{m}$. By a *congruence class group* mod $\mathfrak{m}$, we mean a subgroup H of $I(\mathfrak{m})$ containing $P_\mathfrak{m}$.

Whenever $\mathfrak{m} \mid \mathfrak{n}$, there is a canonical surjection $I(\mathfrak{n})/P_\mathfrak{n} \twoheadrightarrow I(\mathfrak{m})/P_\mathfrak{m}$. Composing with a character χ mod $\mathfrak{m}$ yields a character χ' mod $\mathfrak{n}$. We say χ *induces* χ'. Similarly, if H is a congruence class group mod $\mathfrak{m}$, taking the preimage of H under the specified surjection yields an *induced subgroup* H' mod $\mathfrak{n}$. The *conductor of* χ, denoted $\mathfrak{f}_\chi$, is the smallest modulus (with respect to the partial order by divisibility) from which χ can be induced. We similarly define the conductor $\mathfrak{f}_H$ of a congruence class group H. One can show that

$$\mathfrak{f}_H = \mathrm{lcm}\{\mathfrak{f}_\chi : \chi(H) = 1\}.$$

For each character χ, we set

$$d_\chi := d_K \cdot \mathrm{Nm}(\mathfrak{f}_\chi).$$

For each congruence class group H, we write

$$h_H := \#I(\mathfrak{m})/H \quad \text{and} \quad d(H) := \max\{d_\chi : \chi(H) = 1\}.$$

Let χ be a character modulo $\mathfrak{m}$. For $\sigma := \Re(s) > 1$, we define the L-series $L(s, \chi) = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) \cdot \mathrm{Nm}(\mathfrak{a})^{-s}$. Then $L(s, \chi)$ has an analytic continuation to the entire complex plane, except for a simple pole at $s = 1$ when χ is principal. The *nontrivial zeros* of $L(s, \chi)$ are those zeros belonging to the strip $0 < \sigma < 1$.

3.2. **A theorem of Weiss.** The goal of this section is to describe a variant of Weiss's theorem. In the following results, $c_1, c_2, \ldots$ denote absolute positive constants. For the reader's convenience, we have used the same numbering as in Weiss's paper.

Proposition 3.1. *For $Q \geq 1$ and $T \geq 1$, put $\mathscr{L} = \log(QT^n)$. Suppose that $\mathscr{L}$ exceeds a certain absolute constant. There is at most one primitive character χ with $d_\chi \leq Q$ for which $L(s, \chi)$ has a zero $\sigma + it$ with*

$$\sigma \geq 1 - c_1 \mathscr{L}^{-1} \quad and \quad |t| \leq T.$$

For the proof, see [Wei83, Theorem 1.9]. If the character χ of the last proposition exists, it is called the *exceptional character* with respect to Q and T. Similarly, $\mathfrak{f}_\chi$ is called the *exceptional modulus* and $\sigma + it$ is called the *exceptional zero*.

The following result is a short interval variant of Linnik's theorem, for prime ideals.

Theorem 3.2 (Weiss). *Let H mod $\mathfrak{m}$ be a congruence subgroup and let $\mathscr{C}$ be a coset of $I(\mathfrak{m})/H$. Define*

$$\pi_{\mathscr{C}}(x, \delta) := \sum_{\substack{\mathfrak{p} \in \mathscr{C} \\ x(1-\delta) < \mathrm{Nm}(\mathfrak{p}) < x \\ \deg(\mathfrak{p}) = 1}} 1.$$

Suppose that $Q \geq 1$ and that

$$(7) \qquad\qquad 0 < \delta \leq c_{10} h_H^{-\frac{1}{2n}} Q^{-\frac{1}{2n}}.$$

Let $\mathfrak{n}$ be the product of the primes dividing $\mathfrak{m}$ but not $\mathfrak{f}_H$, and suppose that

$$(8) \qquad\qquad x \geq \max\{(\log \mathrm{Nm}(\mathfrak{n}))^2, (30nQ^{\frac{1}{2n}}\delta^{-1})^{c_{11}n}\}.$$

With $T = (4(2n+3)\delta^{-1})^2$, assume that the exceptional character corresponding to Q and T — if it exists — does not induce a character χ mod $\mathfrak{m}$ having $\chi(H) = 1$. Then

$$\pi_{\mathscr{C}}(x, \delta) \gg n^{-1} \cdot \frac{\delta x}{h_H \log x}.$$

Here the implied constant is absolute.

Proof. This follows from making small modifications in Weiss's proof of his Theorem 5.2 [Wei83]. We now describe the necessary changes. We assume the reader has Weiss's paper in front of them for comparison.

Variation in hypotheses:

   In Weiss's version, Q is immediately set equal to $d(H)$. Correspondingly, when Weiss states his assumptions on x and δ, he has $d(H)$ where we have Q. However, his arguments all go through under the hypothesis that $Q \geq d(H)$, if the conditions on x and δ are stated as above.

Variation in the definition of $\pi_{\mathscr{C}}(x, \delta)$:

In Weiss's statement, $\pi_{\mathscr{C}}(x, \delta)$ counts primes $\mathfrak{p}$ with $x < \mathrm{Nm}(\mathfrak{p}) < x(1 + \delta)$, rather than $\mathfrak{p}$ satisfying $x(1 - \delta) < \mathrm{Nm}(\mathfrak{p}) < x$. This appears to be a minor oversight, stemming from the incorrect claim at the bottom of p. 89 that $ye^{kA^{-1}} = xe^{\delta/2} \leq x(1 + \delta)$. In fact, the weights $H_k(y/\mathrm{Nm}(\mathfrak{p}))$ are only nonzero when $e^{-kA^{-1}} < \mathrm{Nm}(\mathfrak{p})/y < e^{kA^{-1}}$ (by [Wei83, Lemma 3.2(a)]). Since

$$x = ye^{kA^{-1}} \quad \text{and} \quad ye^{-kA^{-1}} = xe^{-\delta/2} > x(1 - \delta),$$

the counting function $\pi_{\mathscr{C}}(x, \delta)$ ought instead to be defined as above.

Variation in the final lower bound on $\pi_{\mathscr{C}}(x, \delta)$:

Most significantly, the claimed lower bound on $\pi_{\mathscr{C}}(x, \delta)$ in [Wei83, Theorem 5.2] is quite a bit weaker than what we have asserted. This is because Weiss does not make any assumption on the (non)existence of exceptional characters.

To obtain the lower bound claimed in our Theorem 3.2, we proceed as follows. From the first and last displayed equations on Weiss's p. 89,

$$10n\frac{h_H \log x}{\delta x} \cdot \pi_{\mathscr{C}}(x, \delta) \geq 1 - \sum_{\chi(H)=1} \sum_{\rho_\chi} |h_k(\rho_\chi - 1)y^{\rho_\chi - 1}|$$
$$+ O(h_H y^{c_6 - 1} \cdot T \log(d(H)T^n)) + O(h_H A^k T^{1-k} \cdot \log(d(H)T^n)).$$

As argued at the top of p. 90, the second error term dominates if c_{11} is chosen sufficiently large (as we may assume).

If the exceptional zero ρ_* exists, then the argument at the top of p. 90 shows that the second error term is $O(\delta \Delta_*)$, provided that c_{10} is chosen small enough. Weiss claims that the same error estimate also holds when ρ^* does not exist, but the reason given does not appear adequate. (A factor of $\log(d(H)T^n)$ appears to have been overlooked.) However, we can prove a negligibly weaker estimate as follows:

$$\log(d(H)T^n) \leq \log(QT^n) = \log Q + 2n \log A$$
$$\ll \log Q + 2n \left(\log(2n) + \log \frac{1}{\delta} \right).$$

From the argument at the top of p. 90 already alluded to,

$$(2n)^{2n} Q \cdot h_H A^k T^{1-k} \leq \delta.$$

Now $\log(Q) + 2n \log(2n) = \log((2n)^{2n} Q) < (2n)^{2n} Q$, and $2n \log \frac{1}{\delta} < (2n)^{2n} Q \log \frac{1}{\delta}$. Hence, $h_H A^k T^{1-k} \cdot \log(d(H)T^n) \ll \delta \log \frac{1}{\delta}$, so that the second error term above is

$$O(\delta \log \frac{1}{\delta} \cdot \Delta_*);$$

we use here that Δ_* is a positive constant when ρ_* does not exist (see the definition of Δ_* at the bottom of p. 88). Hence, whether or not there is an exceptional zero,

$$10n \cdot \frac{h_H \log x}{\delta x} \cdot \pi_{\mathscr{C}}(x, \delta) \geq 1 - \sum_{\chi(H)=1} \sum_{\rho_\chi} |h_k(\rho_\chi - 1)y^{\rho_\chi - 1}| - O(\delta \log \frac{1}{\delta} \cdot \Delta_*).$$

We are assuming that either there is no exceptional zero or that the exceptional character χ does not satisfy $\chi(H) = 1$. The second paragraph on p. 90 shows that under this assumption, the double sum on χ and ρ_χ is $O(\Delta_* \exp(-c_1 \mathscr{L}^{-1} \log y))$. Moreover, earlier in the proof (see the very last statement of p. 88), it is pointed out that $y \geq \exp(\frac{1}{2} c_{11} \mathscr{L})$. Thus, $\exp(-c_1 \mathscr{L}^{-1} \log y) \leq \exp(-\frac{1}{2} c_1 c_{11})$. Inserting this above gives

$$10n \cdot \frac{h_H \log x}{\delta x} \cdot \pi_\mathscr{C}(x, \delta) \geq 1 - O(\Delta_* \exp(-\frac{1}{2} c_1 c_{11})) - O(\delta \log \frac{1}{\delta} \cdot \Delta_*).$$

Now $\Delta_* \ll 1$. If we choose c_{11} sufficiently large, then the first O-term will be smaller than $\frac{1}{3}$ (say). If c_{10} is chosen sufficiently small, then (7) forces δ to be small, and so the second O-term will also be smaller than $\frac{1}{3}$. Hence, $10n \cdot \frac{h_H \log x}{\delta x} > \frac{1}{3}$, yielding the theorem. $\square$

3.3. **A workhorse result.** To proceed, we need to modify Theorem 3.2 ever so slightly. Let $\mathscr{S}$ be a finite set of nonzero ideals of $\mathcal{O}_K$. We can choose a small positive constant c so that none of the finitely many L-functions $L(s, \chi)$, corresponding to characters χ mod $\mathfrak{m}$ with $\mathfrak{m} \in \mathscr{S}$, have a real zero $> 1 - c$. If we replace c_1 with $c_1' := \min\{c, c_1\}$ in Proposition 3.1, it follows automatically that these $L(s, \chi)$ have no exceptional zeros (regardless of the choices of Q and T). We call remaining exceptional zeros *exceptional with respect to Q, T, and $\mathscr{S}$*.

The proof of Theorem 3.2 can now be run as before, but with "exceptional zero corresponding to Q and T" replaced by "exceptional zero with respect to Q, T, and $\mathscr{S}$". This immediately gives an analogue of Theorem 3.2 that we will call Theorem 3.2'. Note that changing c_1 to c_1' has a trickle-down effect, so that in the statement of Theorem 3.2' the constants c_{10} and c_{11} are replaced by suitable constants c_{10}' and c_{11}' depending on $\mathscr{S}$.

We now formulate an important consequence of Theorem 3.2'. For each $\mathfrak{a} \in I(\mathfrak{m})$, let

$$\pi(x; \mathfrak{m}, \mathfrak{a}) = \sum_{\substack{\mathrm{Nm}(\mathfrak{p}) \leq x \\ \deg(\mathfrak{p}) = 1 \\ \mathfrak{p} \sim \mathfrak{a} \pmod{\mathfrak{m}}}} 1.$$

In what follows, we write $h(\mathfrak{m})$ for $\#I(\mathfrak{m})/P_\mathfrak{m}$. This replaces our previous, more cumbersome notation $h_{P_\mathfrak{m}}$ for the same quantity.

Theorem 3.3. *Let K be a number field, and let $\mathscr{S}$ be a finite set of nonzero ideals of $\mathcal{O}_K$. Let $X \geq y^{C_1}$, where $y \geq 2$. Suppose $\mathrm{Nm}(\mathfrak{m}) \leq y$ and that $\mathfrak{m}$ is not divisible by the exceptional modulus $\mathfrak{f}_\chi$ with respect to to $\mathscr{S}$, $Q := d_K y$, and $T := C_2 y^{1/n}$ (if it exists). Then*

$$\pi(X; \mathfrak{m}, \mathfrak{a}) \gg \frac{X}{h(\mathfrak{m}) \log X}.$$

Here the C_i are positive constants depending on K and $\mathscr{S}$, and the final implied constant can also depend on K and $\mathscr{S}$.

Proof. We apply Theorem 3.2' with $H = P_\mathfrak{m}$, with $\mathscr{C}$ the coset of $\mathfrak{a}$ modulo $P_\mathfrak{m}$, with $Q = d_K y$, and with $\delta = C_4 y^{-\frac{1}{2n}}$, for C_4 suitably small (to be specified momentarily). We

will choose $C_2 = 16(2n+3)^2 C_4^{-2}$; then the exceptional zero hypothesis made in Theorem 3.3 corresponds exactly to that in Theorem 3.2′, since $(4(2n+3)\delta^{-1})^2 = C_2 y^{1/n}$.

Let us check that hypotheses (7) and (8) of Theorem 3.3 are satisfied. It is classical (see, e.g., [Chi09, Proposition 2.1, p. 50]) that

$$h(\mathfrak{m}) = \frac{h \cdot 2^{r_1} \cdot \Phi(\mathfrak{m})}{[U : U_{\mathfrak{m}}^+]}.$$

Here h is the class number of K, the group U is the collection of units of $\mathcal{O}_K$, and $U_{\mathfrak{m}}^+$ is the subgroup of totally positive units congruent to 1 modulo $\mathfrak{m}$. Thus,

$$h(\mathfrak{m}) \leq h \cdot 2^{r_1} \Phi(\mathfrak{m}) \leq h \cdot 2^{r_1} y.$$

(Recall our assumption that $\mathrm{Nm}(\mathfrak{m}) \leq y$.) Also,

$$d(H) \leq d_K \cdot \mathrm{Nm}(\mathfrak{m}) \leq d_K y.$$

The quantities n, h, r_1, and d_K are determined by K. So if C_4 is chosen suitably small, depending on the field K and the value of c_{10}', then

$$C_4 y^{-\frac{1}{2n}} \leq c_{10}' h(\mathfrak{m})^{-\frac{1}{2n}} Q^{-\frac{1}{2n}}.$$

Thus, δ is in the desired range (7). Turning to (8), notice that if C_5 is chosen sufficiently large in terms of C_4, K, and c_{11}', then

$$(30nQ^{\frac{1}{2n}}\delta^{-1})^{c_{11}'n} \leq C_5 y^{c_{11}'}.$$

If C_1 is chosen sufficiently large in terms of C_5 and c_{11}', then

$$C_5 y^{c_{11}'} \leq \frac{1}{2} y^{C_1}.$$

We can assume that $C_1 \geq 2$, so that

$$(\log \mathrm{Nm}(\mathfrak{n}))^2 \leq (\log \mathrm{Nm}(\mathfrak{m}))^2 \leq (\log y)^2 \leq \frac{1}{2} y^{C_1}.$$

It follows that the hypothesis (8) holds for any $x \geq \frac{1}{2} y^{C_1}$. So by Theorem 3.2′,

$$\pi_{\mathscr{C}}(x, \delta) \gg \frac{\delta x}{h(\mathfrak{m}) \log x}.$$

We have absorbed the factor of n^{-1} into the implied constant, which we remind the reader is now allowed to depend on K.

We seek a lower bound on $\pi(X; \mathfrak{m}, \mathfrak{a})$ rather than a lower bound on primes in short intervals. Thus, we add up the lower bounds on $\pi_{\mathscr{C}}(x, \delta)$ over an appropriate set of values of x. Let $x_0 = \frac{1}{2} y^{C_1}$, and let $x_j = (1 - \delta)^{-j} x_0$. Choose J as large as possible with $x_J \leq X$. Then

$$\pi(X; \mathfrak{m}, \mathfrak{a}) \geq \sum_{j=0}^{J} \pi_{\mathscr{C}}(x_j, \delta) \gg \frac{\delta x_0}{h(\mathfrak{m}) \log X} \sum_{j=0}^{J} (1 - \delta)^{-j}$$

$$= \frac{\delta x_0}{h(\mathfrak{m}) \log X} \cdot \frac{(1 - \delta)^{-(J+1)} - 1}{(1 - \delta)^{-1} - 1} \gg \frac{x_0}{h(\mathfrak{m}) \log x} ((1 - \delta)^{-(J+1)} - 1).$$

By the choice of J, we have

$$x_0((1-\delta)^{-(J+1)} - 1) = x_{J+1} - x_0 \geq X - x_0 \geq \frac{1}{2}X,$$

using our assumption that $X \geq y^{C_1}$. Thus, $\pi(X; \mathfrak{m}, \mathfrak{a}) \gg \frac{X}{h(\mathfrak{m}) \log X}$. $\square$

4. The lower bound in Theorem 1.1

We let $E/\mathbb{Q}$ denote a fixed elliptic curve with complex multiplication. We will write $\sum'$ for a sum restricted to primes p of good reduction. By an argument seen earlier,

$$(9) \qquad \sum_{p \leq x} d_p = \sum_{d \leq 2\sqrt{x}} \varphi(d) \sideset{}{'}\sum_{\substack{p \leq x \\ d \mid d_p}} 1.$$

Our strategy is to obtain a lower bound for the double sum by carefully estimating the inner sum from below for a sufficiently dense set of values of d.

To avoid technical complications, we only consider integers $d > 2$. The primes p of good reduction for which d divides d_p are exactly those that split completely in $\mathbb{Q}(E[d])$ (see [Kow06, Lemma 2.7]). Since $d > 2$, we know that $K(E[d]) = \mathbb{Q}(E[d])$ [Mur83, Lemma 6]. Thus, p splits completely in $\mathbb{Q}(E[d])$ if and only if p splits completely in K and the primes of K lying above p split completely in $K(E[d])$. We analyze the $\mathfrak{p}$ that split completely in $K(E[d])$ by means of the following lemma.

Lemma 4.1. *There is an ideal $\mathfrak{m}'$ of $\mathcal{O}_K$, depending only on E, with the following property: For each positive integer d, a prime $\mathfrak{p}$ not dividing $d\mathfrak{m}'$ splits completely in $K(E[d])$ if and only if $\mathfrak{p}$ lies in one of $t(d)$ cosets modulo $P_{d\mathfrak{m}'}$, where*

$$t(d) = h(d\mathfrak{m}') \cdot [K(E[d]) : K]^{-1}.$$

Proof. Except for the formula for $t(d)$, this follows from [Mur83, Lemma 4]. From the asymptotic equidistribution of prime ideals mod $P_{\mathfrak{m}'}$ (see [Nar04, Corollary 4, p. 349]), the density of $\mathfrak{p}$ splitting completely in $K(E[d])$ is $t(d)/h(d\mathfrak{m}')$. On the other hand, the Chebotarev density theorem implies that this density is also $[K(E[d]) : K]^{-1}$. Comparing these two statements gives the stated formula. $\square$

In the following arguments, implied constants may depend on E unless otherwise stated.

Given d, we let $\mathfrak{a}_1, \ldots, \mathfrak{a}_{t(d)}$ be elements of $I(\mathfrak{m}')$ representing the cosets modulo $P_{d\mathfrak{m}'}$ appearing in Lemma 4.1. Piecing the above facts together, we deduce that when $d > 2$,

$$\sideset{}{'}\sum_{\substack{p \leq x \\ d \mid d_p \\ p \nmid d \cdot \mathrm{Nm}(\mathfrak{m}')}} 1 = \frac{1}{2} \sideset{}{'}\sum_{p \leq x} \sum_{\substack{\mathfrak{p} \mid p \\ e(\mathfrak{p}/p)=f(\mathfrak{p}/p)=1 \\ \mathfrak{p} \sim \mathfrak{a}_i \,(\mathrm{mod}\, d\mathfrak{m}')\, \text{for some } i}} 1 = \frac{1}{2} \sum_{i=1}^{t(d)} \pi(x; d\mathfrak{m}', \mathfrak{a}_i) + O(1).$$

Since only $O(\log(2d))$ primes divide $d \cdot \mathrm{Nm}(\mathfrak{m}')$, we conclude that

$$(10) \qquad \sideset{}{'}\sum_{\substack{p \leq x \\ d \mid d_p}} 1 = \frac{1}{2} \sum_{i=1}^{t(d)} \pi(x; d\mathfrak{m}', \mathfrak{a}_i) + O(\log(2d)).$$

We apply Theorem 3.3 with K the CM field, $\mathscr{S}$ consisting solely of the ideal $\mathfrak{m}'$ from Lemma 4.1, $X = x$, and $y = x^{1/C_1}$. If the exceptional modulus $\mathfrak{f}_\chi$ exists, then $\mathfrak{f}_\chi \nmid \mathfrak{m}'$. Hence, there is a prime $\mathfrak{q}$ dividing $\mathfrak{f}_\chi$ to a higher power than to which it divides $\mathfrak{m}'$. Let q be the rational prime below $\mathfrak{q}$. We obtain a lower bound on $\sum_{p \leq x} d_p$ by restricting the final sum on d in (9) to values

$$2 < d \leq x^{\frac{1}{2C_1}} \mathrm{Nm}(\mathfrak{m}')^{-1/2} =: Z, \quad \text{with} \quad d \text{ coprime to } q.$$

From (10),

$$\sum_{\substack{2 < d \leq Z \\ \gcd(d,q)=1}} \varphi(d) \sideset{}{'}\sum_{\substack{p \leq x \\ d \mid d_p}} 1 = \frac{1}{2} \sum_{\substack{2 < d \leq Z \\ \gcd(d,q)=1}} \varphi(d) \sum_{i=1}^{t(d)} \pi(x; d\mathfrak{m}', \mathfrak{a}_i) + O(x^{1/C_1} \log x).$$

Now C_1 is a large constant. Hence, the error term is $o(x)$, and so to complete the proof of Theorem 1.1 it remains only to show that the main term is $\gg x$. For d as above, the modulus $d\mathfrak{m}'$ is not divisible by $\mathfrak{f}_\chi$, and $\mathrm{Nm}(d\mathfrak{m}') \leq y$. By Theorem 3.3,

$$\sum_{i=1}^{t(d)} \pi(x; d\mathfrak{m}', \mathfrak{a}_i) \gg \frac{t(d)}{h(d\mathfrak{m}')} \frac{x}{\log x} = \frac{1}{[K(E[d]) : K]} \frac{x}{\log x}.$$

Since $[K(E[d]) : K] \ll d^2$, we conclude that

$$(11) \qquad \sum_{\substack{2 < d \leq Z \\ \gcd(d,q)=1}} \varphi(d) \sum_{i=1}^{t(d)} \pi(x; d\mathfrak{m}', \mathfrak{a}_i) \gg \frac{x}{\log x} \sum_{\substack{2 < d \leq Z \\ \gcd(d,q)=1}} \frac{\varphi(d)}{d^2}.$$

To show that the final sum on d is $\gg \log x$ (for large x), we use the following simple observation.

Lemma 4.2. *Let g be a multiplicative function taking only nonnegative values. For any positive integer k, and any real $t > 0$,*

$$\sum_{\substack{n \leq t \\ \gcd(n,k)=1}} \mu^2(n)g(n) \geq \left(\prod_{p \mid k}(1 + g(p))^{-1} \right) \left(\sum_{n \leq t} \mu^2(n)g(n) \right).$$

Proof. We can factor each squarefree $n \le t$ in the form $n = n_1 n_2$, where $n_1 \mid k$ and n_2 is coprime to k. Then

$$\sum_{n \le t} \mu^2(n)g(n) \le \left(\sum_{n_1 \mid k} \mu^2(n_1)g(n_1) \right) \left(\sum_{\substack{n_2 \le t \\ \gcd(n_2,k)=1}} \mu^2(n_2)g(n_2) \right)$$

$$= \left(\prod_{p \mid k} (1 + g(p)) \right) \left(\sum_{\substack{n_2 \le t \\ \gcd(n_2,k)=1}} \mu^2(n_2)g(n_2) \right).$$

Rearranging yields the result. $\qquad\square$

Applying Lemma 4.2 with $g(n) = \varphi(n)/n^2$ and $k = q$,

$$\sum_{\substack{2 < d \le Z \\ \gcd(d,q)=1}} \frac{\varphi(d)}{d^2} \ge \sum_{\substack{2 < d \le Z \\ \gcd(d,q)=1}} \mu^2(d)\frac{\varphi(d)}{d^2} \ge \frac{1}{2} \sum_{2 < d \le Z} \mu^2(d)\frac{\varphi(d)}{d^2}.$$

The multiplicative function $d \mapsto \mu^2(d)\frac{\varphi(d)}{d}$ has a well-defined nonzero mean value (for instance, by an elementary theorem of Wintner [SS94, Corollary 2.3, p. 51]). By partial summation, the final displayed sum on d is $\gg \log(Z) \gg \log x$, as desired. Inserting this back into (11) completes the proof.

Remark. It is natural to wonder whether our results generalize to CM elliptic curves defined over an arbitrary number field L. For the upper bound, proving such an extension is relatively straightforward. One obtains the same result but with the sum on $p \le x$ replaced with a sum over prime ideals of norm bounded by x and an implied constant that may now depend on L. It should also be possible to prove the analogous lower bound, by establishing a version of Lemma 4.1 with K replaced by the composite field LK. However, we have not carried out the details.

Acknowledgements

References

[Chi09] N. Childress, *Class field theory*, Universitext, Springer, New York, 2009.
[Duk03] 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.
[Ell79] P. D. T. A. Elliott, *Probabilistic number theory. I: Mean-value theorems*, Grundlehren der Mathematischen Wissenschaften, vol. 239, Springer-Verlag, New York-Berlin, 1979.
[FK14] T. Freiberg and P. Kurlberg, *On the average exponent of elliptic curves modulo p*, Int. Math. Res. Not. IMRN (2014), 2265–2293.
[FM13] A. T. Felix and M. R. Murty, *On the asymptotics for invariants of elliptic curves modulo p*, J. Ramanujan Math. Soc. **28** (2013), 271–298.

[Hec81] E. Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Mathematics, vol. 77, Springer-Verlag, New York-Berlin, 1981, Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

[HL94]   J. Hinz and M. Lodemann, *On Siegel zeros of Hecke-Landau zeta-functions*, Monatsh. Math. **118** (1994), 231–248.

[HR74]   H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, no. 4, Academic Press, London-New York, 1974.

[HR79]   _____, *On a result of R. R. Hall*, J. Number Theory **11** (1979), 76–89.

[Kim14] S. Kim, *Average behaviors of invariant factors in Mordell–Weil groups of CM elliptic curves modulo p*, Finite Fields Appl. **30** (2014), 178–190.

[Kow06] E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. **21** (2006), 19–114.

[Lan87] S. Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987.

[Mur83] M. R. Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), 147–168.

[Nar04] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.

[Pol14] P. Pollack, *A Titchmarsh divisor problem for elliptic curves*, submitted. Preprint available at `http://www.math.uga.edu/~pollack/work.html`, 2014.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[SS94]   W. Schwarz and J. Spilker, *Arithmetical functions*, London Mathematical Society Lecture Note Series, vol. 184, Cambridge University Press, Cambridge, 1994.

[Wei83] A. Weiss, *The least prime ideal*, J. Reine Angew. Math. **338** (1983), 56–94.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MISSOURI, COLUMBIA, MO 65211, USA
E-mail address: `freibergt@missouri.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602, USA
E-mail address: `pollack@uga.edu`