Frobenius distributions in short intervals for CM elliptic curves

Anthony Agwu, Phillip Harris, Kevin James, Siddarth Kannan, Huixi Li

PII: S0022-314X(18)30037-4
DOI: https://doi.org/10.1016/j.jnt.2018.01.007
Reference: YJNTH 5964

To appear in: *Journal of Number Theory*

Received date: 9 October 2017
Revised date: 28 January 2018
Accepted date: 28 January 2018

Please cite this article in press as: A. Agwu et al., Frobenius distributions in short intervals for CM elliptic curves, *J. Number Theory* (2018), https://doi.org/10.1016/j.jnt.2018.01.007

FROBENIUS DISTRIBUTIONS IN SHORT INTERVALS FOR CM ELLIPTIC CURVES

ANTHONY AGWU, PHILLIP HARRIS, KEVIN JAMES, SIDDARTH KANNAN, AND HUIXI LI

Abstract. For an elliptic curve $E/\mathbb{Q}$, Hasse's theorem asserts that $\#E(\mathbb{F}_p) = p + 1 - a_p$, where $|a_p| \leq 2\sqrt{p}$. Assuming that E has complex multiplication, we establish asymptotics for primes p for which a_p is in subintervals of the Hasse interval $[-2\sqrt{p}, 2\sqrt{p}]$ of measure $o(\sqrt{p})$. In particular, given a function $f = o(1)$ satisfying some mild conditions, we provide counting functions for primes p where $|a_p| \in (2\sqrt{p}(1 - f(p)), 2\sqrt{p})$, and for primes where $a_p \in (2\sqrt{p}(c - f(p)), 2c\sqrt{p})$, where $c \in (0, 1)$ is a constant.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime p of good reduction, we may consider $\#E(\mathbb{F}_p)$, the number of points on E modulo p. Putting the curve in its Weierstrass form $E : y^2 = x^3 + ax + b$ and arguing probablistically with the theory of quadratic residues, one sees that $\#E(\mathbb{F}_p)$ should be roughly $p+1$. Indeed, it is a classical result of Hasse [18] that $\#E(\mathbb{F}_p) = p+1-a_p$, where the error term a_p, called the *trace of Frobenius*, satisfies $|a_p| \leq 2\sqrt{p}$. The distribution of the quantity a_p within the *Hasse interval* $[-2\sqrt{p}, 2\sqrt{p}]$ has been of great interest in modern number theory, due in part to its role in the Birch and Swinnerton-Dyer conjecture, which relates the rank of the group $E(\mathbb{Q})$ to its local arithmetic data. More specifically, to such a curve, we can associate an L-series via an Euler product:

$$L(E, s) = \prod_{p \nmid \Delta_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}, \tag{1}$$

where $\Delta_E = -16(4a^3 + 27b^2)$ is the discriminant of E. This series converges for $\Re(s) > 3/2$, and as a consequence of the modularity theorem, it will always admit an analytic continuation to all of $\mathbb{C}$. The resulting function is called the *Hasse-Weil zeta function* of E. Birch and Swinnerton-Dyer [3] conjectured that the rank of $E(\mathbb{Q})$ is equal to the order of vanishing of the Hasse-Weil zeta function at $s = 1$. The product formula (1) makes it clear that the behavior of $L(E, s)$ will depend entirely on the distribution of a_p. The distributions of the normalized trace of Frobenius $b_p = a_p/2\sqrt{p}$ have been well-studied, with different results depending on whether or not E has complex multiplication (CM). The CM case is due to Hecke and Deuring:

Theorem 1.1 (Hecke [11, 12], Deuring [7, 8, 9, 10])**.** *Suppose that E is an elliptic curve over $\mathbb{Q}$ with complex multiplication. Then $a_p = 0$ for asymptotically half of all primes p. Moreover, for each subinterval $[\alpha, \beta] \subseteq [-1, 1]$,*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \# \left\{ p \leq x : \frac{a_p}{2\sqrt{p}} \in [\alpha, \beta] \backslash \{0\} \right\} = \frac{1}{2\pi} \int_\alpha^\beta \frac{dt}{\sqrt{1-t^2}}.$$

The distribution of the normalized trace in the non-CM case is much more difficult; the proof was finalized only in 2006, in a paper by Clozel, Harris, Taylor, and Shepherd-Barron. Until its proof, it was known as the Sato-Tate conjecture.

Theorem 1.2 (Clozel, Harris, Shepherd-Barron, Taylor [1])**.** *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Then, for each subinterval $[\alpha, \beta] \subseteq [-1, 1]$,*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \# \left\{ p \leq x : \frac{a_p}{2\sqrt{p}} \in [\alpha, \beta] \right\} = \frac{2}{\pi} \int_\alpha^\beta \sqrt{1-t^2}\, dt.$$

The distributions are markedly different based on whether or not E has CM: if it does, $a_p/2\sqrt{p}$ is concentrated toward the endpoints of the interval $[-1, 1]$. These theorems give us information about the number of primes whose trace of Frobenius lies in subintervals of measure proportionial to that of the Hasse interval, but they do not give information about primes which are in "density-zero" subintervals of the Hasse interval. In particular, the Lang-Trotter conjecture, which predicts the number of primes for which $a_p = r$ for a fixed integer r, remains unresolved.

Conjecture 1.3 (Lang-Trotter)**.** *Let E be an elliptic curve over $\mathbb{Q}$ and let $r \in \mathbb{Z}$. Then if $r = 0$ or E does not have CM, then*

$$\#\{p \leq x : a_p = r\} \sim C_{E,r}\frac{\sqrt{x}}{\log x},$$

where $C_{E,r}$ is an explicit constant depending on E and r.

In this paper, we extend the program begun by James, Tran, Trinh, and Wertheimer in [14] and continued by James and Pollack in [13]. In these papers, the authors study primes for which $|a_p|$ is as large as possible for CM elliptic curves. Adopting the conventions of these papers, we say a prime p is *extremal* for an elliptic curve $E/\mathbb{Q}$ if $|a_p| = \lfloor 2\sqrt{p} \rfloor$, additionally we say that p is a *champion prime* if $a_p = -\lfloor 2\sqrt{p} \rfloor$ (and consequently $\#E(\mathbb{F}_p)$ is as large as possible), and finally p is a *trailing prime* if $a_p = \lfloor 2\sqrt{p} \rfloor$. In [14], the authors established an asymptotic for the count of extremal primes, assuming the Generalized Riemann Hypothesis (GRH). In [13], James and Pollack removed the reliance on GRH and separated the counts of trailing and champion primes.

Theorem 1.4 (James, Pollack)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication, then*

$$\#\{p \leq x : p \text{ is a trailing prime for } E\} \sim \frac{2}{3\pi}\frac{x^{3/4}}{\log x},$$

and the same asymptotic holds for champion primes.

Here we adapt the techniques of [13] to establish asymptotics for primes p for which a_p is in short subintervals of the Hasse interval. Our main result gives a counting function for *nearly extremal* primes, which are primes for which a_p is within a small range of the endpoints of the Hasse interval. Our work also enables us to count primes within a small range of $2c\sqrt{p}$, where $c \in (0, 1)$ is a constant. In this context, "small" means that our intervals are of measure $o(\sqrt{p})$.

Definition 1.5. Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. We say p is

(i) *f-nearly extremal* for E if $|a_p| \in (2\sqrt{p}(1 - f(p)), 2\sqrt{p})$;
(ii) an *f-champion prime* if $a_p < -2\sqrt{p}(1 - f(p))$;
(iii) an *f-trailing prime* if $a_p > 2\sqrt{p}(1 - f(p))$;
(iv) a *(c, f)-prime* for E if $a_p \in (2\sqrt{p}(c - f(p)), 2c\sqrt{p})$ for some constant $c \in (0, 1)$.

Before we state our main theorem, we recall that a positive, measurable function $f : (0, \infty) \to (0, \infty)$ is called *regularly varying* if the limit

$$C(\lambda) = \lim_{x\to\infty} \frac{f(\lambda x)}{f(x)}$$

exists and is positive for all $\lambda > 0$, and f is *slowly varying* if the above limit is 1 for all $\lambda > 0$. In our work, the language of regularly varying functions gives the most precise description of the functions f that may be considered for f-nearly extremal and (c, f)-primes. We emphasize that this is not too serious a restriction on the function f, as for example, all polynomials are regularly varying, and $\log x$ and $1/\log x$ are slowly varying. Importantly, if f is regularly varying, then Karamata's theorem [2] gives that $f(x) = x^\alpha g(x)$ where g is slowly varying. Note that $\alpha = 0$ if and only if f is slowly varying. This parameter $\alpha = \alpha(f)$ is used in the statement of our main theorem.

Theorem 1.6. *Let E be an elliptic curve with complex multiplication, and let $f : (0, \infty) \to (0, 1)$ be a convex, differentiable, regularly varying function. If $x^{-1/2} \ll f(x) = o(1)$, then the number of f-trailing primes $p \leq x$ is*

$$\sim \frac{\sqrt{2}}{\pi(2 + \alpha)}\sqrt{f(x)}\frac{x}{\log x},$$

and the same asymptotic holds for f-champion primes. Moreover, if $1/f(x) = o(x^{.265})$ for sufficiently large x, the number of (c, f)-primes $p \leq x$ is

$$\sim \frac{1}{2\pi}\frac{1}{1 + \alpha}\frac{1}{\sqrt{1 - c^2}}f(x)\frac{x}{\log x}.$$

In Table 1, we compute asymptotics for f-extremal primes for several specific examples of f, and in Table 2 we include asymptotics for (c, f)-primes when $c = 1/2$. As Table 1 indicates, taking $f(p) = 1/2p^{1/2}$ recovers the asymptotic of Theorem 1.4. For the tables, we let $\pi_E^{f-\mathrm{Champ}}(x)$ and $\pi_E^{(1/2,f)}(x)$ denote the counting functions of f-champion and $(1/2, f)$-primes, respectively.

Table 1. Asymptotics for f-nearly extremal primes.

$f(p)$	Width of interval	$\pi_E^{f-\mathrm{Champ}}(x)$
$\frac{1}{2p^{1/2}}$	1	$\sim \frac{2}{3\pi}\frac{x^{3/4}}{\log x}$
$\frac{n}{2p^{1/2}},\ n \geq 1$	n	$\sim \frac{2\sqrt{n}}{3\pi}\frac{x^{3/4}}{\log x}$
$\frac{1}{2p^{1/4}}$	$p^{1/4}$	$\sim \frac{4}{7\pi}\frac{x^{7/8}}{\log x}$
$\frac{1}{2p^{1/2-\varepsilon}},\ \varepsilon \in \left[0, \frac{1}{2}\right)$	p^{ε}	$\sim \frac{2}{(3+2\varepsilon)\pi}\frac{x^{3/4+\varepsilon/2}}{\log x}$
$\frac{1}{2\log p}$	$\frac{p^{1/2}}{\log p}$	$\sim \frac{1}{2\pi}\frac{x}{(\log x)^{3/2}}$
$\frac{1}{2\log\log p}$	$\frac{p^{1/2}}{\log\log p}$	$\sim \frac{1}{2\pi}\frac{x}{\log x}\cdot\frac{1}{(\log\log x)^{1/2}}$
$\frac{\log p}{2\sqrt{p}}$	$\log p$	$\sim \frac{2}{3\pi}\frac{x^{3/4}}{\sqrt{\log x}}$
$\frac{\log\log p}{2\sqrt{p}}$	$\log\log p$	$\sim \frac{2}{3\pi}\frac{x^{3/4}}{\log x}\sqrt{\log\log x}$

2. Background

Here we discuss relevant background information about the complex multiplication of elliptic curves, the trace of Frobenius, and regularly varying functions. All of the facts about elliptic curves used here can be found in David Cox's *Primes of the form $x^2 + ny^2$* [5] and Joe Silverman's *The arithmetic of elliptic curves* [18].

2.1. Complex multiplication.

One means of studying an elliptic curve $E/\mathbb{Q}$ is to consider the endomorphism ring defined of its $\overline{\mathbb{Q}}$-valued points, which we denote by $\mathrm{End}(E)$. For $m \in \mathbb{Z}$, the multiplication-by-m map

$$[m] : E \to E$$

given by

$$P \mapsto \underbrace{P + P + \cdots + P}_{m \text{ times}}$$

provides an endomorphism of E. For almost all elliptic curves defined over $\mathbb{Q}$, such maps give all of the possible endomorphisms, i.e. $\mathrm{End}(E) \cong \mathbb{Z}$. However, for some elliptic curves, the endomorphism ring is strictly larger than $\mathbb{Z}$. For example, if (x, y) is a point on the elliptic curve given by the Weierstrass equation $E : y^2 = x^3 - x$, then $(-x, iy)$ is also a point on the curve. This gives rise to an endomorphism $[i] : E \to E$ which is not given by any multiplication-by-m map, so $\mathbb{Z} \subsetneq \mathrm{End}(E)$. Such curves are said to have *complex*

Table 2. Asymptotics for $(1/2, f)$-primes.

$f(p)$	Width of interval	$\pi_E^{(1/2,f)}(x)$
$\dfrac{1}{2p^{1/4}}$	$p^{1/4}$	$\sim \dfrac{2\sqrt{3}}{3\pi}\dfrac{x^{3/4}}{\log x}$
$\dfrac{1}{2p^{.265-\varepsilon}},\ \varepsilon \in (0, .265)$	$p^{.235+\varepsilon}$	$\sim \dfrac{\sqrt{3}}{(.735+\varepsilon)6\pi}\dfrac{x^{.735+\varepsilon}}{\log x}$
$\dfrac{1}{2\log p}$	$\dfrac{p^{1/2}}{\log p}$	$\sim \dfrac{\sqrt{3}}{6\pi}\dfrac{x}{\log^2 x}$
$\dfrac{1}{2\log\log p}$	$\dfrac{p^{1/2}}{\log\log p}$	$\sim \dfrac{\sqrt{3}}{6\pi}\dfrac{x}{\log x}\cdot\dfrac{1}{\log\log x}$

multiplication. To characterize the possible endomorphism rings of an elliptic curve, we first require the definition of an *order* in a quadratic field.

Definition 2.1. Let $\mathcal{A}$ be a $\mathbb{Q}$-algebra which is finitely generated over $\mathbb{Q}$. An *order* $\mathcal{R}$ of $\mathcal{A}$ is a subring of $\mathcal{A}$ such that $\mathcal{R} \otimes \mathbb{Q} = \mathcal{A}$.

Theorem 2.2. *Let $E/\mathbb{Q}$ be an elliptic curve. Then either* $\mathrm{End}(E) \cong \mathbb{Z}$ *or* $\mathrm{End}(E)$ *is an order in a quadratic extension of* $\mathbb{Q}$.

Any order in a quadratic extension K of $\mathbb{Q}$ is of the form $\mathbb{Z} + f\mathcal{O}_K$, where $f \geq 1$ is an integer. We say E has complex multiplication by the *maximal order* if $\mathrm{End}(E) \cong \mathcal{O}_K$.

2.2. **Trace of Frobenius.** Just as we consider the endomorphism ring of the $\overline{\mathbb{Q}}$-valued points of an elliptic curve defined over $\mathbb{Q}$, we may analyze the endomorphism ring of the $\overline{\mathbb{F}}_p$-valued points of an elliptic curve E defined over $\mathbb{F}_p$ for any prime p not dividing the discriminant Δ_E; write $\mathrm{End}_{\mathbb{F}_p}(E)$ for this ring. We again have $\mathbb{Z} \subseteq \mathrm{End}_{\mathbb{F}_p}(E)$. However, we also have the pth power *Frobenius endomorphism* given by

$$\sigma_p : (x, y) \mapsto (x^p, y^p).$$

One may verify that $\sigma_p \notin \mathbb{Z}$, in that this map does not correspond to any multiplication by m map, so we always have $\mathbb{Z} \subsetneq \mathrm{End}_{\mathbb{F}_p}(E)$. We thus have the chain of containments

$$\mathbb{Z} \subsetneq \mathbb{Z}[\sigma_p] \subseteq \mathrm{End}_{\mathbb{F}_p}(E),$$

where $\mathbb{Z}[\sigma_p]$ is finite over $\mathbb{Z}$. The element σ_p satisfies a monic relation of the form

$$\sigma_p^2 - a_p\sigma_p + p = 0 \in \mathrm{End}_{\mathbb{F}_p}(E), \tag{2}$$

where a_p is the *trace of Frobenius* as discussed in the introduction. The relation (2) motivates the use of the term "trace." Indeed, a_p also arises as the trace of the Frobenius endomorphism when viewed as an element of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ via its action on the *Tate module* $T_\ell(E)$, one can see the aforementioned reference [18] for an in-depth treatment of this perspective. In particular, this allows us to view the polynomial $x^2 - a_px + p$ arising from the relation (2) as the characteristic polynomial of σ_p, which we denote $\mathrm{char}_{\sigma_p}(x)$. For a curve E defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$, the polynomial factors as

$$\mathrm{char}_{\sigma_p}(x) = (x - \omega)(x - \overline{\omega}), \tag{3}$$

where ω is a prime of $\mathcal{O}_K$ that lies over p. Importantly, this implies that for the root ω of char_{σ_p}, we have

$$2\Re(\omega) = \omega + \overline{\omega} = a_p$$

and

$$|\omega|^2 = N\omega = \begin{cases} p^2 & \text{if } \omega \in \mathbb{Q}, \\ p & \text{otherwise,} \end{cases}$$

where N denotes the norm of the field extension; in the quadratic case, this agrees with the square of the usual complex modulus. Therefore, when an elliptic curve $E/\mathbb{Q}$ has CM by $\mathcal{O}_K$, we can associate to each splitting rational prime p two primes ω and $\overline{\omega}$ of $\mathcal{O}_K$ lying over p, each with real part $a_p/2$. This fact is integral to the proof of our main theorem, and we will refer to the equation (3) later, specifying the prime ω via congruence conditions.

2.3. **Regularly varying functions.** In this paper we require that $f(x) = o(1)$ be differentiable, strictly decreasing, convex, and *regularly varying*. We recall the definition as stated in the introduction.

Definition 2.3. A positive, measurable function $f : (0, \infty) \to (0, \infty)$ is called *regularly varying* if the limit

$$C(\lambda) = \lim_{x\to\infty} \frac{f(\lambda x)}{f(x)}$$

exists and is positive for all $\lambda > 0$. The function f is *slowly varying* if $C(\lambda) = 1$ for all $\lambda > 0$.

If f is regularly varying, then Karamata's characterization theorem [2] says that $f(x) = x^\alpha g(x)$ where g is slowly varying, and $C(\lambda) = \lambda^\alpha$. We will need two technical lemmas for dealing with regularly varying functions in our proof of Theorem 1.6.

Lemma 2.4. *If f is regularly varying and $\eta < 1$, then $f(X) \sim f(X + X^\eta)$. Moreover, if f is strictly decreasing with $f(x) \to 0$ as $x \to \infty$ and $p \in (X, X + X^\eta)$ is a rational prime, then $f(X) \sim f(p) \sim f(X + X^\eta)$, and*

$$f(p) < f(X) < (1 + h(X))f(p),$$

where

$$h(X) := \frac{f(X) - f(X + X^\eta)}{f(X + X^\eta)} = o(1).$$

Proof. We have $C(\lambda) = \lambda^\alpha \to 1$ as $\lambda \to 1$. Given $\varepsilon > 0$ there exists a $\lambda > 1$ such that $C(\lambda) > 1 - \varepsilon$. Then for sufficiently large X, we have

$$1 \geq \frac{f(X + X^\eta)}{f(X)} = \frac{f(X(1 + X^{\eta-1}))}{f(X)} > \frac{f(\lambda X)}{f(X)} > 1 - \varepsilon.$$

So letting $\varepsilon \to 0$ we have $f(X+X^\eta) \sim f(X)$. Therefore, we have $h(X) = o(1)$. When f is strictly decreasing, for $p \in (X, X + X^\eta)$, we have

$$f(p) < f(X) = \left(1 + \frac{f(X) - f(p)}{f(p)}\right) f(p) < \left(1 + \frac{f(X) - f(X + X^\eta)}{f(X + X^\eta)}\right) f(p) = (1 + h(X))f(p),$$

which completes the proof. □

Lemma 2.5. *Write $f(x) = x^\alpha g(x)$ where g is slowly varying. If f is convex, then*

$$\alpha = \lim_{X\to\infty} \frac{Xf'(X)}{f(X)}.$$

Proof. Fix a $\lambda > 1$. By convexity we have

$$\left|f'(\lambda X)\right| < \left|\frac{f(\lambda X) - f(X)}{(\lambda - 1)X}\right| < \left|f'(X)\right|.$$

Rearranging the left inequality yields

$$\left|\frac{f'(\lambda X)\lambda X}{f(\lambda X)}\right| < \lambda \left|\frac{1 - \frac{f(X)}{f(\lambda X)}}{\lambda - 1}\right|,$$

and substituting $X = X/\lambda$ we get

$$\left|\frac{f'(X)X}{f(X)}\right| < \lambda \left|\frac{1 - \frac{f(X/\lambda)}{f(X)}}{\lambda - 1}\right|.$$

Thus, after a similar rearrangement for the RHS we can bound

$$\left|\frac{\frac{f(\lambda X)}{f(X)}-1}{\lambda-1}\right|<\left|\frac{f'(X)X}{f(X)}\right|<\lambda\left|\frac{1-\frac{f(X/\lambda)}{f(X)}}{\lambda-1}\right|.$$

Taking $X\to\infty$ we obtain

$$\left|\frac{\lambda^{\alpha}-1}{\lambda-1}\right|\le\liminf_{X\to\infty}\left|\frac{f'(X)X}{f(X)}\right|\le\limsup_{X\to\infty}\left|\frac{f'(X)X}{f(X)}\right|\le\lambda\left|\frac{1-\lambda^{-\alpha}}{\lambda-1}\right|$$

Finally, taking $\lambda\to1$ we obtain the desired limit. □

3. Counting f-nearly extremal and (c,f)-primes

We now establish the framework for the proof of Theorem 1.6. As in [13], the proof involves replacing the problem of counting primes with prescribed trace of Frobenius with the problem of counting primes of imaginary quadratic fields lying in narrow sectors of the complex plane. Indeed, for an elliptic curve $E/\mathbb{Q}$ with CM by $\mathcal{O}_K$, the splitting of the characteristic polynomial of Frobenius (3) establishes the first connection between rational primes with prescribed trace and primes ω of $\mathcal{O}_K$. By imposing conditions on the trace, we are able to establish bounds on the argument of the primes ω. Of course, as discussed in Section 2.1, an elliptic curve E might have CM by an order strictly smaller than $\mathcal{O}_K$. However, for our purposes, we may assume without loss of generality that E has complex multiplication by the maximal order $\mathcal{O}_K$, as there is always a $\mathbb{Q}$-rational isogeny $\phi:E\to E'$, where $E'/\mathbb{Q}$ has CM by the maximal order. See [4], Proposition 25 for a reference for this fact. In particular, $a_p(E)=a_p(E')$ for all but a finite number of primes p, so this additional assumption on the CM of E will not alter our asymptotic estimates.

Deuring [6] showed that $a_p=0$ if and only if p is inert or ramified in K, so when p is sufficiently large and is either f-nearly extremal or a (c,f)-prime, it is split in K. It is known that for any elliptic curve over $\mathbb{Q}$ with CM by $\mathcal{O}_K$, the prime ω of (3) can be specified by congruence conditions, i.e. there is a nonzero element $\mu\in\mathcal{O}_K$ and an irredundant list of elements $\nu_1,\dots,\nu_r\in\mathcal{O}_K$ which are invertible modulo μ, such that for each split prime p which is coprime to μ, a prime ω lying over p satisfies (3) if and only if

$$\omega\equiv\nu_1,\dots,\nu_{r-1},\ \text{or}\ \nu_r \pmod{\mu}. \tag{4}$$

For more information on computing the exact congruence conditions to be imposed, one may consult [17]. As in [13], the work of Landau [15] allows us to argue that the number of congruence conditions r in (4) above satisfies

$$r=\varphi(\mu)/w_K,$$

where $\varphi(\mu)=\#(\mathcal{O}_K/\mu\mathcal{O}_K)^{\times}$ is the number of units in $\mathcal{O}_K/\mu\mathcal{O}_K$ and w_K denotes the number of roots of unity in K. The following theorem, due to Maknys [16], tells us how to count primes of $\mathcal{O}_K$ which occur in sectors.

Theorem 3.1 (Maknys)**.** *Let K be an imaginary quadratic field, fix a nonzero $\mu\in\mathcal{O}_K$, and let h_K denote the class number of K. If ν is an invertible residue class modulo μ, we have*

$$\sum_{\substack{\omega\ prime\\ N\omega\ prime\\ x<N\omega\le x+x^{\eta}\\ \omega\equiv\nu\pmod{\mu}\\ \theta_1<\arg(\omega)<\theta_2}}1\sim\frac{w_K}{h_K\varphi(\mu)}\cdot\frac{\theta_2-\theta_1}{2\pi}\cdot\frac{x^{\eta}}{\log x},$$

as $x\to\infty$, where $2\pi\ge\theta_2-\theta_1>x^{\eta-1}$ and $\eta=0.735$.

As E is defined over $\mathbb{Q}$, the field K is one of the nine imaginary quadratic fields of class number 1, i.e., for our purposes, we may take $h_K=1$ in the above theorem. Maknys' result will allow us to count primes in sectors of $\mathcal{O}_K$ which satisfy the congruence conditions (4), which are precisely the primes ω lying over rational primes p with $\Re(\omega)=a_p/2$. The following lemma establishes the sectors where primes ω of $\mathcal{O}_K$ must correspond to rational primes p which are f-trailing for E.

Lemma 3.2. *Let f be a strictly decreasing, regularly varying function with $f(x) \to 0$ as $x \to \infty$ and $f(x) \gg x^{-1/2}$. Let $\omega = a + bi \in \mathcal{O}_K$ be a prime of norm p, where $p \in (X, X + X^\eta)$ is a rational prime. Let $h(X)$ be as in Lemma 2.4. Then for sufficiently large X, if*

$$2a > 2\sqrt{p}(1 - f(p)),$$

then

$$|\arg(\omega)| < (1 + f(X))\sqrt{2f(X)} = (1 + o(1))\sqrt{2f(X)}.$$

Conversely, if

$$|\arg(\omega)| < (1 - h(X))\sqrt{2f(X)} = (1 - o(1))\sqrt{2f(X)},$$

then

$$2a > 2\sqrt{p}(1 - f(p)).$$

The analogous result holds for f-champion primes, with signs reversed.

Proof. First we prove the forward direction. By the Taylor expansion of $\cos(x)$ at $x = 0$, we have $\cos(x) < 1 - \frac{1}{2}x^2 + \frac{1}{24}x^4$ for x near 0. Then by assumption we have

$$\sqrt{p}(1 - f(p)) < a = \sqrt{p}\cos(\arg\omega) < \sqrt{p}\left[1 - \frac{1}{2}(\arg\omega)^2 + \frac{1}{24}(\arg\omega)^4\right],$$

i.e.,

$$f(p) > \frac{1}{2}(\arg\omega)^2 - \frac{1}{24}(\arg\omega)^4.$$

Since f in strictly decreasing, for $p \in (X, X + X^\eta)$ we have

$$|\arg\omega|\sqrt{1 - \frac{1}{12}(\arg\omega)^2} < \sqrt{2f(p)} < \sqrt{2f(X)}.$$

Then, as $f(X) = o(1)$ and $\arg\omega \in [-\pi, \pi]$, we get

$$|\arg\omega| < \frac{\sqrt{2f(X)}}{\sqrt{1 - \frac{\pi^2}{12}}} < 3\sqrt{2f(X)},$$

and therefore, for sufficiently large X, we have the bound

$$|\arg\omega| < \frac{\sqrt{2f(X)}}{\sqrt{1 - \frac{(\arg\omega)^2}{12}}} < \left(1 + \frac{(\arg\omega)^2}{18}\right)\sqrt{2f(X)} < (1 + f(X))\sqrt{2f(X)} = (1 + o(1))\sqrt{2f(X)},$$

which proves the first implication. For the reverse direction, suppose $|\arg\omega| < (1 - h(X))\sqrt{2f(X)}$. By Lemma 2.4, for sufficiently large X we have

$$|\arg\omega| < (1 - h(X))\sqrt{2f(X)} < (1 - h(X))\sqrt{2(1 + h(X))f(p)} < \pi/2.$$

Since $\cos(x)$ is even and it is decreasing on $[0, \pi/2]$, we have

$$a = \sqrt{p}\cos(\arg(\omega)) > \sqrt{p}\cos\left((1 - h(X))\sqrt{1 + h(X)}\sqrt{2f(p)}\right).$$

The Taylor series for cosine gives that $\cos(x) > 1 - \frac{1}{2}x^2$, so we have

$$\begin{aligned} 2a &> 2\sqrt{p}\left(1 - \frac{1}{2}\left((1 - h(X))\sqrt{1 + h(X)}\sqrt{2f(p)}\right)^2\right) \\ &= 2\sqrt{p}\left(1 - (1 - h(X))^2(1 + h(X))f(p)\right) \\ &= 2\sqrt{p}\left(1 - (1 - h(X)^2)(1 - h(X))f(p)\right) \\ &> 2\sqrt{p}(1 - f(p)). \end{aligned}$$

□

Remark 3.3. The previous lemma gives sectors in which one may count primes ω corresponding to f-trailing primes. In the following lemma, we establish an analogous result for (c, f)-primes.

Lemma 3.4. *Let $f, \omega = a + bi, p \in (X, X + X^\eta)$ and $h(X)$ be as in the previous lemma. Let $c \in (-1, 1)$. For sufficiently large X, if*

$$\sqrt{p}(c - f(p)) < a < c\sqrt{p},$$

then

$$\arccos(c) < |\arg\omega| < \arccos(c) + \left(1 - \frac{cf(X)}{2(1-c^2)} + o\left(f(X)^2\right)\right)\frac{f(X)}{\sqrt{1-c^2}} = \arccos(c) + (1 + o(1))\frac{f(X)}{\sqrt{1-c^2}}.$$

Conversely, if

$$\begin{aligned}\arccos(c) < |\arg\omega| &< \arccos(c) + \left(1 - \frac{|c|f(X)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right)\frac{f(X)}{\sqrt{1-c^2}}\\ &= \arccos(c) + (1 - o(1))\frac{f(X)}{\sqrt{1-c^2}},\end{aligned}$$

then

$$\sqrt{p}(c - f(p)) < a < c\sqrt{p}.$$

Proof. For the forward implication, since $f(X) = o(1)$, for sufficiently large X and any $p \in (X, X + X^\eta)$, we have $-1 < c - f(p) < c < 1$. Note that $\arccos(x)$ is decreasing on $[-1, 1]$, we have $a < c\sqrt{p}$ implies $|\arg\omega| = \arccos(a/\sqrt{p}) > \arccos(c)$.

Recall that f is strictly decreasing and that $a > \sqrt{p}(c - f(p))$. By the Taylor expansion for $\arccos(x)$ at $x = c$, we know for sufficiently large X and any $p \in (X, X + X^\eta)$, that

$$\begin{aligned}|\arg\omega| &= \arccos(a/\sqrt{p})\\ &< \arccos(c - f(p))\\ &= \arccos(c) + \frac{f(p)}{\sqrt{1-c^2}} - \frac{f(p)^2c}{2(1-c^2)^{3/2}} + o\left(f(p)^3\right)\\ &= \arccos(c) + \left(1 - \frac{cf(p)}{2(1-c^2)} + o(f(p)^2)\right)\frac{f(p)}{\sqrt{1-c^2}}\\ &< \arccos(c) + \left(1 - \frac{cf(X)}{2(1-c^2)} + o\left(f(X)^2\right)\right)\frac{f(X)}{\sqrt{1-c^2}}\\ &= \arccos(c) + (1 + o(1))\frac{f(X)}{\sqrt{1-c^2}}.\end{aligned}$$

For the reverse implication, since $f(X) = o(1)$, for sufficiently large X and any $p \in (X, X + X^\eta)$, by assumption we have

$$0 < \arccos(c) < |\arg\omega| < \arccos(c) + \left(1 - \frac{|c|f(X)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right)\frac{f(X)}{\sqrt{1-c^2}} < \pi.$$

Since $\arccos(c) < |\arg\omega|$ and $\cos(x)$ is decreasing on $[0, \pi]$, we have $a < c\sqrt{p}$.

For the other inequality, since

$$|\arg\omega| < \arccos(c) + \left(1 - \frac{|c|f(x)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right)\frac{f(X)}{\sqrt{1-c^2}}$$

and $\cos(\alpha + \beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$, we have

$$\begin{aligned}a/\sqrt{p} =& \cos(|\arg\omega|)\\ >& \cos\left(\arccos(c) + \left(1 - \frac{|c|f(x)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right)\frac{f(X)}{\sqrt{1-c^2}}\right)\\ =& c\cos\left(\left(1 - \frac{|c|f(x)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right)\frac{f(X)}{\sqrt{1-c^2}}\right)\\ &- \sqrt{1-c^2}\sin\left(\left(1 - \frac{|c|f(x)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right)\frac{f(X)}{\sqrt{1-c^2}}\right).\end{aligned}$$

For x near 0 we may use the bounds $\cos(x) > 1 - \frac{1}{2}x^2$ and $\sin(x) < |x|$ to get

$$\begin{aligned}
a/\sqrt{p} >& c\left(1 - \frac{1}{2}\left(1 - \frac{|c|f(X)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right)^2 \frac{f(X)^2}{1-c^2}\right)\\
&- \left(1 - \frac{|c|f(X)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right) f(X)\\
=& c - \left(1 + \frac{cf(X)}{2-2c^2}\left(1 - \frac{|c|f(x)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right)\right)\\
&\cdot \left(1 - \frac{|c|f(X)}{2-2c^2} - h(X) - \frac{|c|f(X)h(X)}{2-2c^2}\right) f(X).
\end{aligned}$$

Finally, when $0 \le c < 1$ we apply Lemma 2.4 to see that

$$\begin{aligned}
a/\sqrt{p} &> c - \left(1 + \frac{cf(X)}{2-2c}\right)\left(1 - \frac{|c|f(X)}{2-2c} - h(X) - \frac{|c|f(X)h(X)}{2-2c}\right)(1+h(X))f(p)\\
&= c - \left(1 - \left(\frac{|c|f(X)}{2-2c} + h(X) + \frac{|c|f(X)h(X)}{2-2c}\right)^2\right) f(p)\\
&> c - f(p).
\end{aligned}$$

When $-1 < c < 0$ we apply Lemma 2.4 to see that

$$\begin{aligned}
a/\sqrt{p} &> c - \left(1 - \frac{|c|f(x)}{2-2c} - h(X) - \frac{|c|f(X)h(X)}{2-2c}\right)(1+h(X))f(p)\\
&> c - f(p).
\end{aligned}$$

This completes the proof. □

We are now ready for the proof of our main result.

Proof of Theorem 1.6. As established, we may suppose that E has CM by the maximal order $\mathcal{O}_K$. We fix a number $p_0(E)$ which is large enough to ensure that all primes $p > p_0(E)$ are of good reduction for E, unramified in K, and coprime to μ. We call a prime $\omega \in \mathcal{O}_K$ *f-distinguished* if $N\omega = p$ is prime, $\omega \equiv \nu_1, \ldots, \nu_{r-1}$ or $\nu_r \pmod{\mu}$ (this ensures that (3) holds for ω and hence that $2\Re(\omega) = a_p$), and $2\Re(\omega) > 2\sqrt{p}(1 - f(p))$. If we count f-distinguished primes, we are double counting the rational primes they correspond to: if ω is f-distinguished, then so is $\overline{\omega}$. Therefore, if we let χ_{fd} denote the characteristic function of f-distinguished primes, we see that

$$\sum_{\substack{p_0 < p < x \\ p \text{ is } f\text{-distinguished}}} 1 = \frac{1}{2} \sum_{p_0 < N\omega < x} \chi_{\text{fd}}(\omega).$$

As in [13], we begin by considering a weighted version of the right-hand sum. Let $\eta = .735$ as in Theorem 3.1, and let x be a large real number. For each prime $\omega \in \mathcal{O}_K$ with $N\omega$ prime and $x^{1/2} < N\omega \le x$, we define

$$\mathcal{X}(\omega) = \{T \in \mathbb{R} : T < N\omega \le T + T^\eta\}.$$

Each $\mathcal{X}(\omega)$ is of length $\sim (N\omega)^\eta$, uniformly in ω. Therefore,

$$\begin{aligned}
\sum_{x^{1/2} < N\omega \le x} \chi_{\text{fd}}(\omega)(N\omega)^\eta &= (1 + o(1)) \sum_{x^{1/2} < N\omega \le x} \chi_{\text{fd}}(\omega) \int_{\mathcal{X}(\omega)} 1\, dX\\
&= (1 + o(1)) \int_{x^{1/2} - x^{\eta/2}}^{x} \sum_{\substack{X < N\omega \le X + X^\eta \\ x^{1/2} < N\omega \le x}} \chi_{\text{fd}}(\omega)\, dX. \qquad (5)
\end{aligned}$$

We first consider the range of integration where $x^{1/2} \le X \le x - x^\eta$; in this range the first restriction on the sum implies the second. The difference between the bounds in Lemma 3.2 is $\sim 2\sqrt{2f(X)}$, so we can apply

Theorem 3.1 with $\theta_2 - \theta_1 = 2\sqrt{2f(X)}$ and sum over the $r = \varphi(\mu)/w_K$ residue classes to get

$$\sum_{X < N\omega \leq X + X^\eta} \chi_{\mathrm{fd}}(\omega) \sim \frac{\sqrt{2f(X)}}{\pi} \frac{X^\eta}{\log X}.$$

We now let

$$F(t) = \frac{\sqrt{2}}{\pi} \cdot \frac{2}{2(\eta+1)+\alpha} \cdot \frac{t^{\eta+1}\sqrt{f(t)}}{\log t}, \tag{6}$$

where if f is regularly varying, α is given by Karamata's theorem; $f(x) = x^\alpha g(x)$ where g is slowly varying (indeed, $\alpha = 0$ if f is slowly varying). We now use Lemma 2.5 to compute

$$\begin{aligned}
\lim_{t\to\infty} F'(t) \cdot \frac{\pi}{\sqrt{2}} \frac{\log t}{\sqrt{f(t)} t^\eta} &= \frac{2}{2(\eta+1)+\alpha} \lim_{t\to\infty} \frac{\log t}{t^\eta \sqrt{f(t)}} \cdot \left(\frac{(1+\eta)t^\eta\sqrt{f(t)}}{\log t} - \frac{t^\eta\sqrt{f(t)}}{\log^2 t} + \frac{t^{1+\eta}f'(t)}{2\sqrt{f(t)}\log t} \right) \\
&= \frac{2}{2(\eta+1)+\alpha} \left((1+\eta) + \lim_{t\to\infty} \frac{tf'(t)}{2f(t)} \right) \\
&= \frac{2}{2(\eta+1)+\alpha} \left(1 + \eta + \frac{\alpha}{2} \right) = 1.
\end{aligned}$$

Written differently, we have

$$F'(t) \sim \frac{\sqrt{2}}{\pi} \frac{\sqrt{f(t)} t^\eta}{\log t}.$$

The contribution to the integral from the range $x^{1/2} \leq X \leq x - x^\eta$ is thus

$$\sim F(x - x^\eta) - F(x^{1/2}),$$

which we claim is $\sim F(x)$. Indeed, we have

$$\begin{aligned}
\lim_{x\to\infty} \frac{F(x-x^\eta) - F(x^{1/2})}{F(x)} &= \lim_{x\to\infty} \frac{\sqrt{f(x-x^\eta)}(x-x^\eta)^{\eta+1}}{\log(x-x^\eta)} \cdot \frac{\log x}{\sqrt{f(x)}x^{\eta+1}} \\
&\quad - \lim_{x\to\infty} \frac{\sqrt{f(x^{1/2})}x^{(\eta+1)/2}}{\log x^{1/2}} \cdot \frac{\log x}{\sqrt{f(x)}x^{\eta+1}} \\
&= \lim_{x\to\infty} \left(\frac{f(x-x^\eta)}{f(x)} \right)^{1/2} - 2 \lim_{x\to\infty} \left(\frac{f(x^{1/2})}{f(x)} \right)^{1/2} \cdot \frac{1}{x^{(\eta+1)/2}} \\
&=1 - 2 \lim_{x\to\infty} \left(\frac{f(x^{1/2})}{f(x)} \right)^{1/2} \cdot \frac{1}{x^{(\eta+1)/2}}.
\end{aligned}$$

As $x^{-1/2} \ll f(x)$, there is a constant C such that $Cx^{-1/4} \leq \sqrt{f(x)}$ for sufficiently large x, so that

$$\left(\frac{f(x^{1/2})}{f(x)} \right)^{1/2} \cdot \frac{1}{x^{(\eta+1)/2}} \leq \frac{C\sqrt{f(x^{1/2})}}{x^{(2\eta+1)/4}},$$

where the term on the RHS clearly goes to 0 as $x \to \infty$. We may conclude that $F(x - x^\eta) - F(x^{1/2}) \sim F(x)$. The remaining range of integration is the union of the intervals $[x^{1/2} - x^{\eta/2}, x^{1/2}]$ and $[x - x^\eta, x]$, which together make up a set of measure $x^\eta + x^{\eta/2} \ll x^\eta$, while the integrand itself is uniformly $\ll x^\eta/\log x$. Altogether, this interval makes a contribution of $\ll x^{2\eta}\log x$, and for large x and constants M and C we have

$$0 \leq \frac{x^{2\eta}}{F(x)\log x} = M \cdot \frac{x^{2\eta}}{\sqrt{f(x)}x^{\eta+1}} = M \cdot \frac{1}{\sqrt{f(x)}x^{.265}} \leq \frac{Cx^{.25}}{x^{.265}} = \frac{C}{x^{.015}} \to 0;$$

we may conclude that this contribution does not affect the asymptotic. It follows that

$$\sum_{x^{1/2} < N\omega \leq x} \chi_{\mathrm{fd}}(\omega)(N\omega)^\eta \sim \frac{\sqrt{2}}{\pi} \cdot \frac{2}{2(\eta+1)+\alpha} \cdot \frac{\sqrt{f(x)}x^{\eta+1}}{\log x}; \tag{7}$$

but for the corresponding sum over primes ω with $N(\omega) \leq x^{1/2}$, we have

$$\sum_{N\omega \leq x^{1/2}} \chi_{\mathrm{fd}}(\omega)(N\omega)^{\eta} \ll x^{(\eta+1)/2},$$

so we can delete the restriction that $N\omega > x^{1/2}$ on the sum in (7) without altering the asymptotic:

$$\sum_{N\omega \leq x} \chi_{\mathrm{fd}}(\omega)(N\omega)^{\eta} \sim \frac{\sqrt{2}}{\pi} \cdot \frac{2}{2(\eta+1)+\alpha} \cdot \frac{\sqrt{f(x)}x^{\eta+1}}{\log x}.$$

We will now remove the weights via partial summation. Put

$$A(t) = \sum_{N\omega \leq t} \chi_{\mathrm{fd}}(\omega)(N\omega)^{\eta}.$$

Then

$$\sum_{N\omega \leq x} \chi_{\mathrm{fd}}(\omega) = \int_2^x t^{-\eta} dA(t) = (1+o(1))\left(\frac{\sqrt{2}}{\pi} \cdot \frac{2}{2(\eta+1)+\alpha} \cdot \frac{\sqrt{f(x)}x}{\log x}\right) + \eta \int_2^x A(t)t^{-\eta-1}\,dt,$$

where

$$\int_2^x A(t)t^{-\eta-1}\,dt = \frac{\sqrt{2}}{\pi} \cdot \frac{2}{2(\eta+1)+\alpha} \int_2^x \frac{(1+o(1))\sqrt{f(x)}}{\log x} \sim \frac{\sqrt{2}}{\pi} \cdot \frac{2}{2(\eta+1)+\alpha} \cdot \frac{2}{2+\alpha} \cdot \frac{\sqrt{f(x)}x}{\log x};$$

this may be seen by differentiating both sides, using L'Hopital's rule and applying Lemma 2.5. We thus have

$$\begin{aligned}\sum_{N\omega \leq x} \chi_{\mathrm{fd}}(\omega) &\sim \frac{\sqrt{2}}{\pi} \cdot \frac{2}{2(\eta+1)+\alpha} \cdot \left(\frac{\sqrt{f(x)}x}{\log x} + \frac{2\eta}{2+\alpha} \cdot \frac{\sqrt{f(x)}x}{\log x}\right) \\ &= \frac{\sqrt{2}}{\pi} \cdot \frac{2}{2+\alpha} \cdot \frac{\sqrt{f(x)}x}{\log x}.\end{aligned}$$

The same argument, constraining $\arg(-\omega)$ rather than $\arg(\omega)$, gives the asymptotic for f-champion primes. For the (c, f)-primes, the calculation is essentially the same; in this case, the difference between the bounds constraining $\arg(\omega)$ comes from Lemma 3.4, it is

$$\theta_2 - \theta_1 \sim \frac{2f(X)}{\sqrt{1-c^2}} \tag{8}$$

instead of $2\sqrt{2f(X)}$. The function F as in (6) becomes

$$F(t) = \frac{1}{2\pi}\frac{1}{1+\eta+\alpha}\frac{1}{\sqrt{1-c^2}}\frac{f(t)t^{\eta+1}}{\log t}.$$

The remainder of the argument is similar, and the final asymptotic is then

$$\sum_{\substack{p_0 < p \leq x \\ p \text{ is a } (c,f)\text{-prime}}} 1 \sim \frac{1}{2\pi}\frac{1}{1+\alpha}\frac{1}{\sqrt{1-c^2}}\frac{f(x)x}{\log x}.$$

□

Remark 3.5. For (c, f)-primes, the condition $1/f(x) = o(x^{.265})$ ensures that f is large enough to apply Maknys's result in Theorem 3.1. We remark that conditional on the generalized Riemann Hypothesis, this restriction may be relaxed to $x^{-1/2+\varepsilon} \ll f$ for any $\varepsilon > 0$ using the methods in [14]. However, those techniques do not allow one to separate the count of primes on either side of the Hasse interval, i.e. one could find the asymptotic count of primes $p \leq x$ such that $a_p \in (2c\sqrt{p}(c - f(p), 2\sqrt{p}) \cup (-2c\sqrt{p}, -2\sqrt{p}(c + f(p)))$, but not the count of primes for which a_p is in either interval in the union. We do not see how to bypass this limitation, and consequently we do not pursue this direction in more detail.

4. Acknowledgements

The authors are grateful to Clemson University for hosting the REU at which this work was completed. The REU was made possible by an NSF Research Training Group (RTG) grant (DMS #1547399) promoting Coding Theory, Cryptography, and Number Theory at Clemson.

References

[1] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor. A family of Calabi-Yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.

[2] N.H. Bingham, C.M. Goldie, and J.L. Teugels. *Regular Variation*. Number no. 1 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1989.

[3] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[4] 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(2):447–479, 2013.

[5] D. A. Cox. *Primes of the form* $x^2 + ny^2$. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[6] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg*, 14(1):197–272, 1941.

[7] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. Math.-Phys.-Chem. Abt.*, 1953:85–94, 1953.

[8] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. II. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1955:13–42, 1955.

[9] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. III. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1956:37–76, 1956.

[10] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. IV. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1957:55–80, 1957.

[11] E. Hecke. Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Math. Z.*, 1(4):357–376, 1918.

[12] E. Hecke. Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Math. Z.*, 6(1-2):11–51, 1920.

[13] K. James and P. Pollack. Extremal primes for elliptic curves with complex multiplication. *Journal of Number Theory*, 172:383 – 391, 2017.

[14] K. James, B. Tran, M-T. Trinh, P. Wertheimer, and D. Zantout. Extremal primes for elliptic curves. *Journal of Number Theory*, 164:282 – 298, 2016.

[15] E. Landau. Über ideale und primideale in idealklassen. *Mathematische Zeitschrift*, 2(1):52–154, Mar 1918.

[16] M. Maknys. On the distance between consecutive prime ideal numbers in sectors. *Acta Mathematica Hungarica*, 42(1):131–138, Mar 1983.

[17] P. Pollack. A Titchmarsh divisor problem for elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 160(1):167–189, 2016.

[18] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

Department of Mathematics and Statistics, UMBC, Baltimore, MD 21250
E-mail address: aagwu1@umbc.edu

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL 61820
E-mail address: plharri2@illinois.edu

Department of Mathematics, Clemson University, Clemson, SC 29634
E-mail address: kevja@clemson.edu

Department of Mathematics, Pomona College, Claremont, CA 91711
E-mail address: siddarth.kannan@pomona.edu

Department of Mathematics, Clemson University, Clemson, SC 29634
E-mail address: huixil@g.clemson.edu