Journal of Number Theory 164 (2016) 282–298

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Extremal primes for elliptic curves

Kevin James [a,*], Brandon Tran [c], Minh-Tam Trinh [d], Phil Wertheimer [b], Dania Zantout [a]

[a] Department of Mathematical Sciences, Clemson University, Box 340975, Clemson, SC 29634, United States
[b] Department of Mathematics, University of Maryland, College Park, MD 20742, United States
[c] Department of Mathematics, MIT, Cambridge, MA 02142, United States
[d] Department of Mathematics, University of Chicago, Chicago, IL 60637, United States

ARTICLE INFO

Article history:
Received 26 June 2015
Received in revised form 25 December 2015
Accepted 2 January 2016
Available online 3 March 2016
Communicated by Steven J. Miller

Keywords:
Frobenius distributions
Trace of Frobenius
Distribution of primes
Elliptic curves
Lang–Trotter conjecture

ABSTRACT

For an elliptic curve $E/\mathbb{Q}$, we define an extremal prime for E to be a prime p of good reduction such that the trace of Frobenius of E at p is $\pm\lfloor 2\sqrt{p}\rfloor$, i.e., maximal or minimal in the Hasse interval. Conditional on the Riemann Hypothesis for certain Hecke L-functions, we prove that if $\mathrm{End}(E) = \mathcal{O}_K$, where K is an imaginary quadratic field of discriminant $\neq -3, -4$, then the number of extremal primes $\leq X$ for E is asymptotic to $X^{3/4}/\log X$. We give heuristics for related conjectures.

© 2016 Elsevier Inc. All rights reserved.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime of good reduction for E, and let $\overline{E}/\mathbb{F}_p$ be the corresponding reduction. The *trace of Frobenius of E modulo p* can be defined

* Corresponding author.
E-mail addresses: kevja@clemson.edu (K. James), btran115@mit.edu (B. Tran), mqt@uchicago.edu (M.-T. Trinh), phil.wertheimer@gmail.com (P. Wertheimer), dzantou@g.clemson.edu (D. Zantout).

http://dx.doi.org/10.1016/j.jnt.2016.01.009
0022-314X/© 2016 Elsevier Inc. All rights reserved.

by $a_p(E) = p + 1 - \#\overline{E}(\mathbb{F}_p)$. Hasse's theorem [Si1, Theorem V.1.1] famously asserts that

$$-2\sqrt{p} \leq a_p(E) \leq +2\sqrt{p}. \tag{1.1}$$

We therefore say $[-2\sqrt{p}, +2\sqrt{p}]$ is the *Hasse interval* of p. By [De], every integer in the Hasse interval of a fixed prime p is the trace of Frobenius of some rational elliptic curve modulo p. However, if we instead fix $E/\mathbb{Q}$ and vary p, then the statistical distribution of the $a_p(E)$ is not completely understood.

Hereafter, if f, g denote functions of X, then the phrase "$f \sim g$ as $X \to \infty$" stands for $\lim_{X\to\infty} f/g = 1$. In comparison with the *unnormalized* traces $a_p(E)$, we know much more about the distribution of the *normalized* traces $b_p(E) = a_p(E)/2\sqrt{p}$. Specifically, the latter depends only on whether E has complex multiplication (CM). In the CM case, the distribution of the b_p is due to Hecke, cf. [He1,He2]:

Theorem 1.1 *(Hecke). If E has CM and $[a, b] \subseteq [-1, +1]$, then the distribution of the $b_p(E)$ has a spike at 0 of measure $1/2$ and*

$$\begin{aligned} &\#\{p \leq X \text{ of good reduction for } E : b_p(E) \in [a, b] \setminus \{0\}\} \\ &\sim \frac{1}{2\pi} \left(\int_a^b \frac{1}{\sqrt{1-t^2}}\, \mathrm{d}t \right) \frac{X}{\log X} \end{aligned} \tag{1.2}$$

as $X \to \infty$.

In the non-CM case, the analogous result was known as the Sato–Tate conjecture until its recent proof by Clozel, Harris, Shepherd-Barron and Taylor, cf. [CHT,T,HST], and [BGHT]:

Theorem 1.2 *(Clozel, Harris, Shepherd-Barron, Taylor). If E does not have CM and $[a, b] \subseteq [-1, +1]$, then*

$$\begin{aligned} &\#\{p \leq X \text{ of good reduction for } E : b_p(E) \in [a, b]\} \\ &\sim \frac{2}{\pi} \left(\int_\alpha^\beta \sqrt{1-t^2}\, \mathrm{d}t \right) \frac{X}{\log X} \end{aligned} \tag{1.3}$$

as $X \to \infty$.

Finally, the current hypothesis for the distribution of the unnormalized $a_p(E)$ is known as the Lang–Trotter conjecture [LT]:

Conjecture 1.3 *(Lang–Trotter). Let $E/\mathbb{Q}$ be an elliptic curve and let $r \in \mathbb{Z}$. If either $r \neq 0$ or E does not have CM, then*

$$\#\{p \leq X \text{ of good reduction for } E : a_p(E) = r\} \sim C_{E,r} \frac{\sqrt{X}}{\log X}, \tag{1.4}$$

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

Related to these conjectures, one can also ask when, for fixed E, the value $a_p(E)$ is maximal or minimal in the Hasse interval. In other words, how often is p a witness to the effectiveness of Hasse's theorem?

Definition 1.4. Let p be a prime of good reduction for E. We say that p is an *extremal prime for E* if and only if $|a_p(E)| = \lfloor 2\sqrt{p} \rfloor$.

In [Hed], Jason Hedetniemi studies the primes p such that $a_p(E) = -\lfloor 2\sqrt{p} \rfloor$. He refers to them as *champion primes for E*, because at such primes, $\overline{E}$ attains the maximum number of $\mathbb{F}_p$-rational points possible among elliptic curves over $\mathbb{F}_p$.

Theorem 1.5 *(Hedetniemi). Let $X, A(X), B(X) > 0$ such that for some $\epsilon > 0$,*

1. $A(X), B(X) \geq \exp((1/4 + \epsilon)X))$.
2. $A(X)B(X) \geq \exp((5/4 + \epsilon)X))$.

For all $a, b \in \mathbb{Z}$ such that $4a^3 + 27b^2 \neq 0$, let $E_{a,b}$ be the elliptic curve whose affine equation is $y^2 = x^3 + ax + b$. Let

$$\mathcal{E}(A, B) = \{E_{a,b} : |a| \leq A \text{ and } |b| \leq B\}, \tag{1.5}$$

$$\mathcal{E}^-(A, B) = \{E_{a,b} \in \mathcal{E}(A, B) : E_{a,b} \text{ has a champion prime}\}. \tag{1.6}$$

Then $\#\mathcal{E}^-(A, B) \sim \#\mathcal{E}(A, B)$ as $X \to \infty$.

In other words, almost all elliptic curves $E/\mathbb{Q}$ have at least one champion, hence extremal, prime. We note that one can employ the Chinese Remainder theorem as in Hedetniemi's work to deduce that, for all $N \geq 1$, we can construct infinitely many elliptic curves having no extremal primes $\leq N$.

By Theorems 1.1 and 1.2, we expect the density of extremal primes to differ greatly depending on whether E has CM or not. In the CM case, $a_p(E)$ tends to live near the edges of the Hasse interval (excepting the spike at 0), whereas in the non-CM case, $a_p(E)$ tends toward the center.

In this note, we estimate the asymptotic density of extremal primes for any E such that $\mathrm{End}(E) = \mathcal{O}_K$, where K is an imaginary quadratic field of class number 1 and discriminant $\neq -3, -4$, conditional on the Riemann Hypothesis (RH) for certain Hecke L-functions. The idea of the proof is to obtain a correspondence between extremal primes of E and prime elements $\varpi \in \mathcal{O}_K$ in the region $\Re(z)^{1/2} \geq \Im(z) > 0$, after discarding a negligible subset of the ϖ. In Section 5, we provide heuristics for further conjectures in both CM and non-CM cases.

2. Statement of results

Throughout the rest of this paper, $\mathcal{O}_E = \mathrm{End}(E)$. We write $\pi_E^{\pm}(X)$ for the number of extremal primes for E that are less than X. If K is a number field, then we write $\mathfrak{a} \lhd \mathcal{O}_K$ to mean $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$. Our main result is the following theorem, proved in Sections 3 and 4:

Theorem 2.1. *Suppose $\mathcal{O}_E = \mathcal{O}_K$, where K is an imaginary quadratic field of class number 1 and discriminant $\Delta_K \neq -3, -4$. Let χ_∞ be the Hecke character of K that sends*

$$\mathfrak{a} \mapsto (\alpha/|\alpha|)^{\#\mathcal{O}_K^\times} \tag{2.1}$$

for all $\mathfrak{a} \lhd \mathcal{O}_K$, where α is any generator of $\mathfrak{a}$. If the Riemann Hypothesis (RH) for $L(s, \chi_\infty^n)$ holds for all n, then

$$\pi_E^{\pm}(X) = \frac{4}{3\pi}\frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{(\log X)^2}\right). \tag{2.2}$$

The heuristics in Section 5 lead us to the following general conjectures for the CM and non-CM cases, respectively:

Conjecture 2.2. *Suppose $\mathcal{O}_E = \mathcal{O}_K$, where K is an imaginary quadratic field of class number 1. Then*

$$\pi_E^{\pm}(X) \sim C_E \frac{X^{3/4}}{\log X}, \tag{2.3}$$

where $C_E = 2\#\mathcal{O}_K^\times/(3\pi)$.

Conjecture 2.3. *Suppose E does not have CM. Then*

$$\pi_E^{\pm}(X) \sim C_E \frac{X^{1/4}}{\log X}, \tag{2.4}$$

for some constant C_E depending only on E.

3. Proofs

We briefly review facts about orders in imaginary quadratic fields, following [Cox]. By definition, an *order* in a number field K is a finitely-generated sublattice $\mathcal{O}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$. If $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d < 0$, then $\mathcal{O}$ is called an *imaginary quadratic order* and

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K \tag{3.1}$$

for some $f \geq 1$ called the *conductor of* $\mathcal{O}$. The *fundamental discriminant of* $\mathcal{O}$, which depends only on K, is

$$\Delta_K = \begin{cases} d & \text{if } d \equiv 1 \pmod 4, \\ 4d & \text{if } d \equiv 2, 3 \pmod 4, \end{cases} \tag{3.2}$$

and the *discriminant of* $\mathcal{O}$ is $\Delta_{\mathcal{O}} = \Delta_K f^2$. Thus,

$$\mathcal{O} = \begin{cases} \mathbb{Z}\left[\frac{\sqrt{\Delta_{\mathcal{O}}}}{2}\right] & \text{if } \Delta \equiv 0 \pmod 2, \\ \mathbb{Z}\left[\frac{1+\sqrt{\Delta_{\mathcal{O}}}}{2}\right] & \text{if } \Delta \equiv 1 \pmod 2. \end{cases} \tag{3.3}$$

If E is an elliptic curve over $\mathbb{Q}$ with CM, then $\mathcal{O}_E = \mathrm{End}(E)$ is an imaginary quadratic order of one of the following 13 discriminants [Si2, p. 483]:

$$\begin{aligned} \Delta_{\mathcal{O}_E} = &-3, -4, -7, -8, -11, -19, -43, -67, -163, \\ &-2^2 \cdot 3, -2^2 \cdot 4, -2^2 \cdot 7, -3^2 \cdot 3. \end{aligned} \tag{3.4}$$

Observe that the imaginary quadratic field K_E to which $\mathcal{O}_E$ belongs always has class number 1. Thus, if $\mathcal{O}_E = \mathcal{O}_{K_E}$, then $\mathcal{O}_E$ has unique prime factorization.

The first step of our proof is the following proposition, which in turn will require two short lemmas.

Proposition 3.1. *Suppose $E/\mathbb{Q}$ has CM. If p is an extremal prime of E, then $p = \varpi\overline{\varpi}$ for some prime element $\varpi \in \mathcal{O}_E$ such that*

$$\Re(\varpi) \geq \begin{cases} \Im(\varpi)^2 & \text{if } \Re(\varpi) \in \mathbb{Z}, \\ \Im(\varpi)^2 + 3/4 & \text{otherwise.} \end{cases} \tag{3.5}$$

The converse holds if $\Delta_{K_E} \neq -3, -4$.

For all $a \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 0}$, abbreviate

$$D(a, n) = a^2 - 4n, \quad \text{and} \tag{3.6}$$

$$D(n) = \lfloor 2\sqrt{n} \rfloor^2 - 4n. \tag{3.7}$$

We always have $D(a, n) \equiv 0, 1 \pmod 4$.

Lemma 3.2. *Let $p \neq 2, 3$ be of ordinary reduction for $E/\mathbb{Q}$. Then $D(a_p(E), p) = \Delta_{\mathcal{O}_E} v^2$ for some $v \in \mathbb{Z}$.*

Proof. Let $\overline{E}$ be the reduction of E modulo p. By hypothesis, $\overline{E}$ is ordinary. Also, since E is defined over $\mathbb{Q}$, the conductor f of $\mathcal{O}_E$ satisfies $1 \leq f \leq 3$. Thus, p does not divide

the conductor of $\mathcal{O}_E$. So, $\mathcal{O}_{\overline{E}} \simeq \mathcal{O}_E$ by Theorem 12 of [La, Chapter 13]. Let $a = |a_p(E)|$. We know $\mathcal{O}_{\overline{E}}$ contains the Frobenius element ϖ, which must satisfy $\varpi^2 \pm a\varpi + p = 0$. Thus, $\mathbb{Z}[\varpi] \hookrightarrow \mathcal{O}_E$, where $D(a,p)$ is the discriminant of $\mathbb{Z}[\varpi]$, as in the proof of Theorem 14.16 in [Cox]. The result follows. □

Lemma 3.3. *If $n \in \mathbb{Z}_{\geq 0}$, then*

$$n = \begin{cases} u^2 + \dfrac{|D(n)|}{4} \text{ and } u \geq \dfrac{|D(n)|}{4} & \text{if } D(n) \equiv 0 \pmod 4, \\ u^2 + u + \dfrac{|D(n)|+1}{4} \text{ and } u \geq \dfrac{|D(n)|+1}{4} & \text{if } D(n) \equiv 1 \pmod 4, \end{cases} \tag{3.8}$$

for some $u \in \mathbb{Z}_{\geq 0}$.

Proof. Taking

$$u = \begin{cases} \frac{\lfloor 2\sqrt{n} \rfloor}{2} & \text{if } D(n) \equiv 0 \pmod 4, \\ \frac{\lfloor 2\sqrt{n} \rfloor - 1}{2} & \text{if } D(n) \equiv 1 \pmod 4, \end{cases} \tag{3.9}$$

one can easily verify the result. □

Proof of Proposition 3.1. We write $(\mathcal{O}, \Delta, K) = (\mathcal{O}_E, \Delta_{\mathcal{O}_E}, K_E)$ for convenience. Suppose p is extremal. Then $D(p) = D(a_p(E), p)$. So, by Lemma 3.2, $D(p) = a_p(E)^2 - 4p = \Delta v^2$ for some $v \in \mathbb{Z}$. So

$$p = \begin{cases} u^2 + \dfrac{|\Delta| v^2}{4} \text{ and } u \geq \dfrac{|\Delta| v^2}{4} & \text{if } \Delta v^2 \equiv 0 \pmod 4, \\ u^2 + u + \dfrac{|\Delta| v^2 + 1}{4} \text{ and } u \geq \dfrac{|\Delta| v^2 + 1}{4} & \text{if } \Delta v^2 \equiv 1 \pmod 4, \end{cases} \tag{3.10}$$

for some $u \in \mathbb{Z}_{\geq 0}$ by Lemma 3.3. We will refer to the top possibility as case (1) and the bottom as case (2).

Suppose Δ is even, so that $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = \sqrt{\Delta}/2$. Then case (1) must hold, so setting $\varpi = u + \tau v \in \mathcal{O}$, we are done. Suppose Δ is odd, so that $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1 + \sqrt{\Delta})/2$. Case (1) holds if $v \equiv 0 \pmod 2$ and (2) holds if $v \equiv 1 \pmod 2$. Set $\varpi = u_0 + \tau v \in \mathcal{O}$, where

$$u_0 = \begin{cases} u - v/2 & \text{if } v \equiv 0 \pmod 2, \\ u - (v-1)/2 & \text{if } v \equiv 1 \pmod 2. \end{cases} \tag{3.11}$$

Computation shows $p = \varpi\overline{\varpi}$ once again. The inequality relating u, v is equivalent to

$$u_0 + \frac{v}{2} \geq \frac{1}{4} \begin{cases} |\Delta| v^2 & \text{if } v \equiv 0 \pmod 2, \\ |\Delta| v^2 + 3 & \text{if } v \equiv 1 \pmod 2, \end{cases} \tag{3.12}$$

where $\Re(\varpi) = u_0 + v/2$ and $\Im(\varpi) = v\sqrt{|\Delta|}/2$, as needed.

Conversely, suppose $p = \varpi\overline{\varpi}$ for some $\varpi \in \mathcal{O}$ such that the appropriate inequality relating $\Re(\varpi)$ and $\Im(\varpi)$ in (3.5) holds. In $\mathcal{O}_K$, we know $\varpi\overline{\varpi}$ is a prime factorization of p, so ϖ is the unique prime element of norm p in $\mathcal{O}_K$ up to multiplication by units and conjugation. But the Frobenius element of $\mathcal{O}_{\overline{E}}$ is also a prime of norm p and trace $a_p(E)$, cf. the proof of Theorem 14.16 of [Cox]. If $\Delta_K \neq -3, -4$, then the only units of $\mathcal{O}_K$ are ± 1, so we conclude that ϖ corresponds to the Frobenius element of $\mathcal{O}_{\overline{E}}$, up to sign and conjugation, under the isomorphism $\mathcal{O}_{\overline{E}} \simeq \mathcal{O}$. Therefore,

$$2\Re(\varpi) = \varpi + \overline{\varpi} = \pm a_p(E), \tag{3.13}$$

from which

$$D(a_p(E), p) = (\varpi + \overline{\varpi})^2 - 4\varpi\overline{\varpi} = (\varpi - \overline{\varpi})^2 = -4\Im(\varpi)^2. \tag{3.14}$$

Next, observe that the inequality in (3.5) implies that $\Re(\varpi) > 0$ and $-4\Im(\varpi)^2 \geq -4\Re(\varpi)$. Combining these facts with (3.13) and (3.14), we deduce that

$$a_p(E)^2 - 4p \geq -4\Re(\varpi) = -2|a_p(E)|, \tag{3.15}$$

which implies $(|a_p(E)| + 1)^2 \geq 4p$. But $a_p(E)^2 < 4p$, so it follows that $|a_p(E)| = \lfloor 2\sqrt{p} \rfloor$, meaning p is extremal for E. □

In summary, Proposition 3.1 implies that:

$$\begin{aligned} &\{\text{primes } p = \varpi\overline{\varpi} \text{ such that } \Re(\varpi) \geq \Im(\varpi)^2\} \\ &= \{\text{extremal primes } p \text{ for } E\} \\ &\qquad \cup \{\text{primes } p = \varpi\overline{\varpi} \text{ such that } \Re(\varpi) \notin \mathbb{Z} \text{ and } 0 \leq \Re(\varpi) - \Im(\varpi)^2 \leq 3/4\}. \end{aligned} \tag{3.16}$$

Above, the size of the last set will be negligible in comparison to the sizes of the other two. In particular, its contribution will be negligible compared to the error term in Theorem 2.1. So to estimate the number of extremal primes, it suffices to estimate the number of ϖ such that $\Re(\varpi) \geq \Im(\varpi)^2$ and $\Im(\varpi) > 0$, i.e. counting each conjugate pair only once and discarding the inert primes. If $\mathcal{O}_E = \mathcal{O}_{K_E}$, then we can do this estimation using Hecke's theory of prime distribution in number fields.

In what follows, let K be a number field. For all $\mathfrak{a} \lhd \mathcal{O}_K$, let $\mathbb{N}\mathfrak{a} = \#(\mathcal{O}_K/\mathfrak{a})$ denote the absolute norm of $\mathfrak{a}$. Let $\mathcal{P}_K(X)$ be the set of prime ideals $\mathfrak{p} \lhd \mathcal{O}_K$ such that $\mathbb{N}\mathfrak{p} \leq X$, and let $\pi_K(X) = \#\mathcal{P}_K(X)$. If $\mathfrak{f} \lhd \mathcal{O}_K$, then we write $I_K^{\mathfrak{f}}$ for the group of fractional ideals of K coprime to $\mathfrak{f}$. We need a result of Hecke–Rajan in [Ra]; see also [AIW, Theorem 3.2.3]:

Theorem 3.4. *Let $\mathfrak{f} \lhd \mathcal{O}_K$, and let $\chi : I_K^{\mathfrak{f}} \to \mathbb{C}^\times$ be a Hecke character of infinite order. Then there exists a constant $A_K > 0$ such that, for all $[a, b] \subseteq [0, 1]$,*

$$\begin{aligned}&\#\{\mathfrak{p} \in \mathcal{P}_K(X) : (\mathfrak{p}, \mathfrak{f}) = 1 \text{ and } \arg \chi(\mathfrak{p}) \in [2\pi a, 2\pi b)\} \\ &= (b-a)\pi_K(X) + O\left(X \exp\left(-A_K(\log X)^{1/2}\right)\right). \end{aligned} \tag{3.17}$$

If RH for $L(s, \chi^n)$ holds for all $n \geq 1$, then the error term can be improved to $O_\epsilon(X^{1/2+\epsilon})$ for all $\epsilon > 0$.

Corollary 3.5. *Suppose K is an imaginary quadratic field of class number 1. Let $\theta_K = 2\pi/\#\mathcal{O}_K^\times$, and for all primes $\mathfrak{p} \lhd \mathcal{O}_K$, let $\theta_\mathfrak{p}$ be the argument modulo $\theta_K\mathbb{Z}$ of any generator of $\mathfrak{p}$. Then there exists a constant $B_K > 0$ such that, for all $[a, b] \subseteq [0, 1]$,*

$$\begin{aligned}&\#\{\mathfrak{p} \in \mathcal{P}_K(X) : \theta_\mathfrak{p} \in [a\theta_K, b\theta_K) + \theta_K\mathbb{Z}\} \\ &= (b-a)\pi_K(X) + O\left(X \exp\left(-B_K(\log X)^{1/2}\right)\right). \end{aligned} \tag{3.18}$$

If χ_∞ is as in Theorem 2.1 and RH for $L(s, \chi_\infty^n)$ holds for all $n \geq 1$, then the error term can be improved to $O_\epsilon\left(X^{1/2+\epsilon}\right)$ for all $\epsilon > 0$.

Proof. By the class number 1 condition on K, we know the generators of an ideal of $\mathcal{O}_K$ can differ only up to multiplication by a unit. Thus for $\mathfrak{p} \lhd \mathcal{O}_K$ and $\mathfrak{p} = \alpha_\mathfrak{p}\mathcal{O}_K$, we have that $\arg \alpha_\mathfrak{p} \in \theta_\mathfrak{p} + \theta_K\mathbb{Z}$ and that $\arg \chi_\infty(\mathfrak{p}) = \#\mathcal{O}_K^\times \cdot \arg \alpha_\mathfrak{p} = \#\mathcal{O}_K^\times \cdot \theta_\mathfrak{p}$. Thus $\theta_\mathfrak{p} \in [a\theta_K, b\theta_K) + \theta_K\mathbb{Z}$ if and only if $\arg \chi_\infty(\mathfrak{p}) \in [2\pi a, 2\pi b)$. This together with Theorem 3.4 implies the corollary. □

In the rest of this section, we assume the Riemann Hypothesis for χ_∞^n for all n, and in particular, the classical Riemann hypothesis. For ease of notation, set $K = K_E$. Let $\pi^{\text{split}}(X)$ be the number of integral primes $p \leq X$ that split in $\mathcal{O}_K$. By quadratic reciprocity and the strong version of Dirichlet's theorem for primes in arithmetic progressions that is conditional on RH, cf. [Dav, p. 124],

$$\pi^{\text{split}}(X) = \frac{1}{2}\frac{X}{\log X} + O_\epsilon\left(X^{1/2+\epsilon}\right), \tag{3.19}$$

for all $\epsilon > 0$. For example, in the case of $\mathbb{Q}(\sqrt{-2})$, the splitting primes are the primes congruent to $1, 3$ modulo 8. The following prime-counting function will be fundamental to the proof of our main result. For all intervals $I \subseteq [0, 2\pi)$, let

$$\pi_I(X) = \{p \in \mathbb{Z} : p = \varpi\overline{\varpi} \leq X \text{ for some } \varpi \in \mathcal{O}_K \text{ such that } \arg \varpi \in I\}. \tag{3.20}$$

From Corollary 3.5, we get the following estimate on $\pi_I(X)$:

Corollary 3.6. *Assume RH for χ_∞^n for all n. If $I = [a\theta_K, b\theta_K) \subseteq [0, \theta_K/2)$, an interval of width $\theta = (b-a)\theta_K$, then*

$$\pi_I(X) = \frac{\theta}{\theta_K}\frac{X}{\log X} + O_\epsilon\left(X^{1/2+\epsilon}\right) \tag{3.21}$$

for any $\epsilon > 0$.

Proof. First, recall that if the rational prime p is inert in K, then $\mathbb{N}(p\mathcal{O}_K) = p^2$. Thus the contribution of the inert primes to $\pi_K(X)$ is $O\left(\frac{X^{1/2}}{\log X^{1/2}}\right) = O(X^{1/2})$. Next, since $\theta < \theta_K/2$, each rational prime p that does split in $\mathcal{O}_K$ can be written in the form $p = \varpi\overline{\varpi}$ for at most one $\varpi \in \mathcal{O}_K$ such that $\arg\varpi \in I$. (That is, the condition $\arg\varpi \in I$ controls the sign and conjugation of ϖ.) Employing Corollary 3.5, we obtain

$$\begin{aligned}\pi_I(X) &= \#\{\mathfrak{p} \in \mathcal{P}_K(X) : \theta_{\mathfrak{p}} \in I + \theta_K\mathbb{Z}\} + O\left(X^{1/2}\right)\\ &= \frac{\theta}{\theta_K}\pi_K(X) + O_\epsilon\left(X^{1/2+\epsilon}\right).\end{aligned} \tag{3.22}$$

Finally, note that

$$\pi_K(X) = 2\pi^{\text{split}}(X) + O\left(X^{1/2}\right) = \frac{X}{\log X} + O_\epsilon\left(X^{1/2+\epsilon}\right) \tag{3.23}$$

and the theorem follows. □

4. Proof of Theorem 2.1

4.1. Partitioning into sectors

By Proposition 3.1 and the discussion following (3.16), we can compute the main term of the asymptotic for $\pi_E^{\pm}(X)$ by finding the number of rational primes $p \le X$ that split in $\mathcal{O}_K$ into $\varpi, \overline{\varpi}$ such that either $\varpi \in \mathcal{A}(X)$ or $\overline{\varpi} \in \mathcal{A}(X)$, where

$$\begin{aligned}\mathcal{A}(X) &= \{z \in \mathbb{C} : \Re(z) \ge \Im(z)^2 > 0 \text{ and } |z|^2 = z\overline{z} \le X\}\\ &= \left\{z = re^{i\alpha} \in \mathbb{C}^\times : 0 < r < \min\left\{X^{1/2}, \frac{\cos\alpha}{\sin^2\alpha}\right\} \text{ and } \alpha \in (0, \pi/2)\right\}.\end{aligned} \tag{4.1}$$

To employ Corollary 3.6, we will divide $\mathcal{A}(X)$ into regions of the form

$$\{re^{i\alpha} : 0 \le r \le R \text{ and } \theta(R) \le \alpha < \theta(R+\delta)\}, \tag{4.2}$$

where $\theta(r)$ is chosen so that $re^{i\theta(r)}$ is the unique point along the parabola $\Re(z) = \Im(z)^2$, within the first quadrant, that is precisely at distance r from the origin. By trigonometry,

$$\theta(r) = \arccos\left[\frac{-1+\sqrt{1+4r^2}}{2r}\right] \tag{4.3}$$

has the desired property. Using the first-order Taylor approximation at infinity $\sqrt{1+4r^2} = 2r + O(r^{-1})$, we obtain

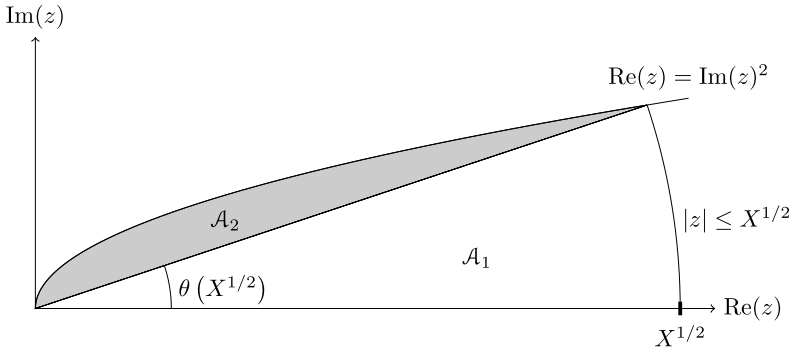

Fig. 1. Regions $\mathcal{A}_1$ and $\mathcal{A}_2$.

$$\frac{-1+\sqrt{1+4r^2}}{2r} = 1 - \frac{1}{2r} + O\left(r^{-2}\right). \tag{4.4}$$

We further recall that the Puiseux series of $\arccos(1-y)$ is given by

$$\arccos(1-y) = \sqrt{2}y^{1/2} + \frac{\sqrt{2}}{12}y^{3/2} + O\left(y^{5/2}\right). \tag{4.5}$$

Combining the last two estimates and a bit of algebra yields

$$\theta(r) = r^{-1/2} + O\left(r^{-3/2}\right). \tag{4.6}$$

From the above discussion, $\theta(r) \in (0, \pi/2)$ and $r = \cos\theta(r)/\sin^2\theta(r)$.

Let us first partition $\mathcal{A}$ into regions $\mathcal{A}_1, \mathcal{A}_2$ (see Fig. 1):

$$\begin{cases} \mathcal{A}_1(X) = \{re^{i\alpha} \in \mathbb{C}^\times : 0 < r < X^{1/2} \text{ and } \alpha \in (0, \theta(X^{1/2})]\}, \\ \mathcal{A}_2(X) = \{re^{i\alpha} \in \mathbb{C}^\times : 0 < r < \cos\alpha/\sin^2\alpha \text{ and } \alpha \in (\theta(X^{1/2}), \pi/2)\}. \end{cases} \tag{4.7}$$

Let $\pi_{\mathcal{A}_j}(X)$ be the contribution of the primes corresponding to $\mathcal{A}_j(X)$. In the hypothesis of our theorem, $\Delta_K \neq -3, -4$, which occurs if and only if $\#\mathcal{O}_K^\times = 2$, or equivalently, $\theta_K = \pi$. Therefore, by Corollary 3.6,

$$\begin{aligned} \pi_{\mathcal{A}_1}(X) = \pi_{[0,\theta(X^{1/2}))}(X) &= \frac{\theta(X^{1/2})}{\pi}\frac{X}{\log X} + O_\epsilon\left(X^{1/2+\epsilon}\right) \\ &= \frac{1}{\pi}\frac{(X^{3/4} + O\left(X^{1/4}\right))}{\log X} + O_\epsilon\left(X^{1/2+\epsilon}\right). \\ &= \frac{X^{3/4}}{\pi\log X} + O_\epsilon\left(X^{1/2+\epsilon}\right). \end{aligned} \tag{4.8}$$

We next turn our attention to the estimation of $\pi_{\mathcal{A}_2}(X)$. First, we wish to identify a power ρ of X for which the contribution of the primes in the region

$$\mathcal{C}_\rho = \{re^{i\alpha} : 0 \le r \le \cos\alpha/\sin^2\alpha;\ \alpha \in [\theta(X^\rho), \pi/2)\} \tag{4.9}$$

can be overestimated by $\pi_{[\theta(X^\rho),\pi/2)]}(X^{2\rho})$, and such that this overestimate remains negligible compared to our main term. Again by Corollary 3.6,

$$\begin{aligned}\pi_{\mathcal{C}_\rho} \le \pi_{[\theta(X^\rho),\pi/2)}(X^{2\rho}) &= \frac{\pi/2-\theta(X^\rho)}{\pi}\frac{X^{2\rho}}{(\rho)\log X} + O_{\epsilon'}\left(X^{\rho+(2\rho)\epsilon'}\right)\\ &= O\left(\frac{X^{2\rho}}{\log X}\right).\end{aligned} \tag{4.10}$$

So, taking $2\rho < 3/4$ will do. Since $5/7$ is close to and less than $3/4$, we will take $\rho = 5/14$ and set $\mathcal{C} = \mathcal{C}_{5/14}$ in what follows. Setting

$$\mathcal{B} = \{re^{i\alpha} : 0 \le r \le \cos\alpha/\sin^2\alpha;\ \alpha \in [\theta(X^{1/2}), \theta(X^{5/14}))\}, \tag{4.11}$$

and using (4.8) and (4.10), we have

$$\begin{aligned}\pi_E^{\pm}(X) &= \pi_{\mathcal{A}_1}(X) + \pi_{\mathcal{B}}(X) + \pi_{\mathcal{C}}(X)\\ &= \frac{X^{3/4}}{\pi\log X} + \pi_{\mathcal{B}}(X) + O\left(\frac{X^{5/7}}{\log X}\right).\end{aligned} \tag{4.12}$$

In order to estimate $\pi_{\mathcal{B}}(X)$, we set $r_t(X) = X^{1/2} - tX^{1/3}$ and define

$$\begin{cases}\overline{\mathcal{B}}_n = \{re^{i\alpha} : 0 < r < r_{n-1}(X) \text{ and } \alpha \in [\theta(r_{n-1}(X)), \theta(r_n(X)))\},\\ \underline{\mathcal{B}}_n = \{re^{i\alpha} : 0 < r < r_n(X) \text{ and } \alpha \in [\theta(r_{n-1}(X)), \theta(r_n(X)))\},\end{cases} \tag{4.13}$$

for $1 \le n \le \kappa := \lfloor X^{1/6} - X^{1/42}\rfloor$. For such n, observe that $r_n(X) \ge X^{5/14}$. Finally, define

$$\mathcal{D} = \{re^{i\alpha} \in \mathbb{C}^\times : 0 < r < \cos\alpha/\sin^2\alpha \text{ and } \alpha \in [\theta(r_\kappa(X)), \theta(X^{5/14}))\}, \tag{4.14}$$

so that

$$\bigcup_{n=1}^{\kappa} \underline{\mathcal{B}}_n \subseteq \mathcal{B} \subseteq \bigcup_{n=1}^{\kappa} \overline{\mathcal{B}}_n \cup \mathcal{D}. \tag{4.15}$$

Note that $r_\kappa(X) < X^{5/14} + X^{1/3}$, from which $r_\kappa^2(X) = X^{5/7} + O(X^{29/42})$. We now use Corollary 3.6 to estimate $\pi_{\mathcal{D}}(X)$:

$$\begin{aligned}\pi_{\mathcal{D}}(X) &\le \pi_{[\theta(r_\kappa(X)),\theta(X^{5/14}))}(r_\kappa^2(X))\\ &= \frac{\theta(X^{5/14}) - \theta(r_\kappa(X))}{\pi}\frac{r_\kappa^2(X)}{\log r_\kappa^2(X)} + O_{\epsilon'}\left(r_\kappa(X)^{1+2\epsilon'}\right)\end{aligned}$$

$$= O\left(\frac{\theta(X^{5/14}) + \theta(r_\kappa(X))}{\pi}\frac{X^{5/7}}{(5/7)\log X}\right) + O_{\epsilon'}\left(X^{5/14+(5/7)\epsilon'}\right)$$
$$= O\left(\frac{X^{5/7}}{\log X}\right), \tag{4.16}$$

given that $\theta(X^{5/14})$ and $\theta(r_\kappa(X))$ are both $O(1)$. Combining (4.15) and (4.16), we have

$$\sum_{n=1}^{\kappa} \pi_{\underline{\mathcal{B}}_n}(X) \le \pi_{\mathcal{B}}(X) \le \sum_{n=1}^{\kappa} \pi_{\overline{\mathcal{B}}_n}(X) + O\left(\frac{X^{5/7}}{\log X}\right). \tag{4.17}$$

4.2. Estimating the contribution of $\underline{\mathcal{B}}_n$

Consider the following Taylor-series expansion at infinity:

$$\begin{aligned} f_n(t) &:= (r_n(X) + t)^{-1/2} \\ &= \frac{1}{(X^{1/2} - nX^{1/3})^{1/2}} - \frac{t}{2(X^{1/2} - nX^{1/3})^{3/2}} \\ &\quad + O\left(\frac{t^2}{(X^{1/2} - nX^{1/3})^{5/2}}\right). \end{aligned} \tag{4.18}$$

From equations (4.6) and (4.18), we deduce that the angular width of each of $\overline{\mathcal{B}}_n$ and $\underline{\mathcal{B}}_n$ is:

$$\begin{aligned} \theta(r_n(X)) - \theta(r_{n-1}(X)) &= f_n(0) - f_n(X^{1/3}) + O\left(r_n(X)^{-3/2} + r_{n-1}(X)^{-3/2}\right) \\ &= \frac{X^{1/3}}{2(X^{1/2} - nX^{1/3})^{3/2}} + O\left(\frac{X^{2/3}}{(X^{1/2} - nX^{1/3})^{5/2}}\right). \end{aligned} \tag{4.19}$$

Recalling that for $1 \le n \le \kappa$, we have $(X^{1/2} - nX^{1/3}) \ge X^{5/14}$, we compute for $1 \le n \le \kappa$ that

$$\begin{aligned} &\pi_{\underline{\mathcal{B}}_n}(X) \\ &= \frac{1}{\pi}\left(\frac{X^{1/3}}{2(X^{1/2} - nX^{1/3})^{3/2}} + O\left(\frac{X^{2/3}}{(X^{1/2} - nX^{1/3})^{5/2}}\right)\right)\frac{\left(X^{1/2} - nX^{1/3}\right)^2}{2\log\left(X^{1/2} - nX^{1/3}\right)} \\ &\quad + O_{\epsilon'}\left((X^{1/2} - nX^{1/3})^{1+2\epsilon'}\right) \\ &= \frac{X^{1/3}(X^{1/2} - nX^{1/3})^{1/2}}{4\pi\log(X^{1/2} - nX^{1/3})} + O\left(\frac{X^{2/3}}{(X^{1/2} - nX^{1/3})^{1/2}\log(X^{1/2} - nX^{1/3})}\right) \\ &\quad + O_{\epsilon'}\left((X^{1/2} - nX^{1/3})^{1+2\epsilon'}\right) \\ &= \frac{X^{1/3}(X^{1/2} - nX^{1/3})^{1/2}}{4\pi\log(X^{1/2} - nX^{1/3})} + O\left(\frac{X^{41/84}}{\log X}\right) + O_{\epsilon'}\left((X^{1/2} - nX^{1/3})^{1+2\epsilon'}\right) \\ &= \frac{X^{1/3}(X^{1/2} - nX^{1/3})^{1/2}}{4\pi\log(X^{1/2} - nX^{1/3})} + O_{\epsilon'}\left(X^{1/2+\epsilon'}\right). \end{aligned} \tag{4.20}$$

(Later on, we will find that the same estimate holds for $\pi_{\overline{\mathcal{B}}_n}(X)$, cf. (4.30).) Hence,

$$\sum_{n=1}^{\kappa} \pi_{\underline{\mathcal{B}}_n}(X) = \sum_{n=1}^{\kappa} \left(\frac{X^{1/3}\left(X^{1/2} - nX^{1/3}\right)^{1/2}}{4\pi \log(X^{1/2} - nX^{1/3})} + O_{\epsilon'}(X^{1/2+\epsilon'}) \right)$$
$$= \frac{X^{1/3}}{4\pi} \sum_{n=1}^{\kappa} \frac{(X^{1/2} - nX^{1/3})^{1/2}}{\log(X^{1/2} - nX^{1/3})} + O_{\epsilon'}\left(X^{2/3+\epsilon'}\right). \tag{4.21}$$

If we interpret the main term as a Riemann sum, then we have the lower bound

$$\frac{1}{4\pi} \int_1^{\kappa+1} \frac{X^{1/3}(X^{1/2} - uX^{1/3})^{1/2}}{\log(X^{1/2} - uX^{1/3})}\,\mathrm{d}u = \frac{1}{4\pi} \int_{X^{1/2}-(\kappa+1)X^{1/3}}^{X^{1/2}-X^{1/3}} \frac{t^{1/2}}{\log t}\,\mathrm{d}t, \tag{4.22}$$

and the upper bound

$$\frac{1}{4\pi} \int_0^{\kappa} \frac{X^{1/3}(X^{1/2} - uX^{1/3})^{1/2}}{\log(X^{1/2} - uX^{1/3})}\,\mathrm{d}u = \frac{1}{4\pi} \int_{X^{1/2}-\kappa X^{1/3}}^{X^{1/2}} \frac{t^{1/2}}{\log t}\,\mathrm{d}t. \tag{4.23}$$

The integrals on the right can be computed by noting that $t^{1/2}/\log t$ is increasing. Namely, for $A < B$, we have

$$\int_A^B \frac{t^{1/2}}{\log t}\,\mathrm{d}t = \int_A^B \left(\frac{t^{1/2}}{\log t} - \frac{2t^{1/2}}{3\log^2 t} \right) \mathrm{d}t + O\left(\int_A^B \frac{2t^{1/2}}{3\log^2 t}\,\mathrm{d}t \right)$$
$$= \frac{2}{3}\left(\frac{B^{3/2}}{\log B} - \frac{A^{3/2}}{\log A} \right) + O\left(\frac{B^{1/2}}{\log^2 B} B \right). \tag{4.24}$$

Combining (4.21), (4.22), (4.23), and (4.24),

$$\frac{X^{1/3}}{4\pi} \sum_{n=1}^{\kappa} \frac{(X^{1/2} - nX^{1/3})^{1/2}}{\log(X^{1/2} - nX^{1/3})}$$
$$= \frac{1}{4\pi} \int_{X^{1/2}-\kappa X^{1/3}}^{X^{1/2}} \frac{t^{1/2}}{\log t}\,\mathrm{d}t \quad + \quad O\left(\int_{X^{1/2}-(\kappa+1)X^{1/3}}^{X^{1/2}-\kappa X^{1/3}} \frac{t^{1/2}}{\log t}\,\mathrm{d}t + \int_{X^{1/2}-X^{1/3}}^{X^{1/2}} \frac{t^{1/2}}{\log t}\,\mathrm{d}t. \right)$$
$$= \frac{1}{3\pi} \frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{(\log X)^2} \right) \; + \; O\left(\int_{X^{1/2}-(\kappa+1)X^{1/3}}^{X^{1/2}-\kappa X^{1/3}} \frac{t^{1/2}}{\log t}\,\mathrm{d}t + \int_{X^{1/2}-X^{1/3}}^{X^{1/2}} \frac{t^{1/2}}{\log t}\,\mathrm{d}t. \right)$$
$$= \frac{1}{3\pi} \frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{(\log X)^2} \right) \quad + \quad O\left(X^{1/3} \cdot \frac{X^{5/28}}{\log\left(X^{5/14}\right)} + X^{1/3} \cdot \frac{X^{1/4}}{\log\left(X^{1/2}\right)} \right)$$

$$= \frac{1}{3\pi}\frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{(\log X)^2}\right) + O\left(\frac{X^{7/12}}{\log X}\right)$$
$$= \frac{1}{3\pi}\frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{(\log X)^2}\right). \tag{4.25}$$

Substituting the above estimate into (4.21) yields

$$\sum_{n=1}^{\kappa} \pi_{\underline{\mathcal{B}}_n}(X) = \frac{1}{3\pi}\frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{(\log X)^2}\right). \tag{4.26}$$

4.3. Concluding the proof

We will relate the overestimate $\overline{\mathcal{B}}_n$ to the underestimate $\underline{\mathcal{B}}_n$. To this end, note that

$$\begin{aligned} r_{n-1}(X)^2 &= (X^{1/2} - nX^{1/3})^2 + 2X^{1/3}(X^{1/2} - nX^{1/3}) + X^{2/3} \\ &= (X^{1/2} - nX^{1/3})^2 + O\left(X^{1/3}(X^{1/2} - nX^{1/3})\right), \end{aligned} \tag{4.27}$$

where the last estimate holds because $X^{1/2} - nX^{1/3} > X^{5/14} > X^{1/3}$. Using a first-order approximation at infinity to the logarithm function, we find

$$\begin{aligned} \log r_{n-1}(X) &= \log(X^{1/2} - nX^{1/3}) + O\left(\frac{X^{1/3}}{X^{1/2} - nX^{1/3}}\right) \\ &= \log(X^{1/2} - nX^{1/3}) + O\left(X^{-1/42}\right). \end{aligned} \tag{4.28}$$

Thus,

$$\begin{aligned} &\frac{(X^{1/2} - (n-1)X^{1/3})^2}{2\log(X^{1/2} - (n-1)X^{1/3})} \\ &= \frac{(X^{1/2} - nX^{1/3})^2 + O\left(X^{1/3}(X^{1/2} - nX^{1/3})\right)}{2\log(X^{1/2} - nX^{1/3}) + O\left(X^{-1/42}\right)} \\ &= \frac{(X^{1/2} - nX^{1/3})^2}{2\log(X^{1/2} - nX^{1/3})} + O\left(\frac{X^{1/3}(X^{1/2} - nX^{1/3})}{\log(X^{1/2} - nX^{1/3})}\right), \end{aligned} \tag{4.29}$$

Finally, using Corollary 3.6, together with the above estimate and the estimate (4.19) for the angular width of the regions $\underline{\mathcal{B}}_n$ and $\overline{\mathcal{B}}_n$, we compute:

$$\begin{aligned} &\pi_{\overline{\mathcal{B}}_n}(X) - \pi_{\underline{\mathcal{B}}_n}(X) \\ &= \frac{1}{\pi}\left(\frac{X^{1/3}}{2(X^{1/2} - nX^{1/3})^{3/2}} + O\left(\frac{X^{2/3}}{(X^{1/2} - nX^{1/3})^{5/2}}\right)\right) \\ &\quad \cdot \left(\frac{(X^{1/2} - (n-1)X^{1/3})^2}{2\log(X^{1/2} - (n-1)X^{1/3})} - \frac{(X^{1/2} - nX^{1/3})^2}{2\log(X^{1/2} - nX^{1/3})}\right) \end{aligned}$$

$$= \frac{1}{\pi}\left(\frac{X^{1/3}}{2(X^{1/2}-nX^{1/3})^{3/2}} + O\left(\frac{X^{2/3}}{(X^{1/2}-nX^{1/3})^{5/2}}\right)\right)$$
$$\cdot O\left(\frac{X^{1/3}(X^{1/2}-nX^{1/3})}{\log(X^{1/2}-nX^{1/3})}\right)$$
$$= O\left(\frac{X^{2/3}}{(X^{1/2}-nX^{1/3})^{1/2}\log(X^{1/2}-nX^{1/3})}\right)$$
$$= O\left(X^{1/2}\right). \tag{4.30}$$

Therefore,

$$\sum_{n=1}^{\kappa}\pi_{\overline{\mathcal{B}}_n}(X) = \sum_{n=1}^{\kappa}\pi_{\underline{\mathcal{B}}_n}(X) + \kappa\cdot O\left(X^{1/2}\right) = \sum_{n=1}^{\kappa}\pi_{\underline{\mathcal{B}}_n}(X) + O\left(X^{1/6}\right)\cdot O\left(X^{1/2}\right)$$
$$= \sum_{n=1}^{\kappa}\pi_{\underline{\mathcal{B}}_n}(X) + O\left(X^{2/3}\right) \tag{4.31}$$

Combining (4.17), (4.26), and (4.31), we have

$$\pi_{\mathcal{B}}(X) = \frac{1}{3\pi}\frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{(\log X)^2}\right). \tag{4.32}$$

Finally substituting (4.32) into (4.12), we conclude that

$$\pi_E^{\pm}(X) = \frac{4}{3\pi}\frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{(\log X)^2}\right), \tag{4.33}$$

as needed.

5. Heuristics

5.1. The CM case

Define the approximate density function

$$\delta(r,\theta) = \frac{1}{\theta_K \log r}. \tag{5.1}$$

Then we can rewrite the right-hand side of (3.21): For all θ_1, θ_2 such that $\theta_2 - \theta_1 = \theta$,

$$\frac{\theta}{\theta_K}\frac{X}{\log X} + O_\epsilon\left(X^{1/2+\epsilon}\right) = \int_{\theta_1}^{\theta_2}\int_{2^{1/2}}^{X^{1/2}}\delta(r,\theta)r\,\mathrm{d}r\,\mathrm{d}\theta + O_\epsilon\left(\frac{X}{(\log X)^2}\right). \tag{5.2}$$

Integrating,

$$\begin{aligned}
&\int_{\mathcal{A}_1(X)} \delta(r,\theta) r \,\mathrm{d}r\,\mathrm{d}\theta + \int_{\mathcal{A}_2(X)} \delta(r,\theta) r \,\mathrm{d}r\,\mathrm{d}\theta \\
&= \int_{0}^{\theta(X^{1/2})} \int_{2^{1/2}}^{X^{1/2}} \delta(r,\theta) r \,\mathrm{d}r\,\mathrm{d}\theta + \int_{2^{1/2}}^{X^{1/2}} \int_{\theta(r)}^{\theta(X^{1/2})} \delta(r,\theta) r \,\mathrm{d}\theta\,\mathrm{d}r + O(1) \\
&\sim \frac{\theta(X^{1/2})}{\theta_K} \frac{X}{\log X} + \frac{1}{\theta_K} \int_{2^{1/2}}^{X^{1/2}} \frac{r}{\log r} \left(X^{-1/4} - r^{-1/2} + O\left(r^{-3/2}\right)\right) \mathrm{d}r \\
&= \frac{1}{\theta_K} \frac{X^{3/4}}{\log X} + \frac{1}{\theta_K} \frac{X^{3/4}}{\log X} - \frac{2}{3\theta_K} \frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{\log^2 X}\right) \\
&= \frac{4}{3\theta_K} \frac{X^{3/4}}{\log X} + O\left(\frac{X^{3/4}}{\log^2 X}\right), \qquad (5.3)
\end{aligned}$$

which yields the heuristic for Conjecture 2.2 and is supported by Theorem 2.1.

5.2. The non-CM case

Here, we use the Sato–Tate law to construct our heuristic. For a non-CM elliptic curve E, the probability that $a_p(E) = +\lfloor 2\sqrt{p} \rfloor$ is approximately

$$\begin{aligned}
\frac{2}{\pi} \int_{1-1/(2\sqrt{p})}^{1} \sqrt{1-t^2}\,\mathrm{d}t &= \frac{2}{\pi} \int_{1-1/(2\sqrt{p})}^{1} \left(\sqrt{2}(1-t)^{1/2} + O((1-t)^{3/2})\right) \mathrm{d}t \\
&= \frac{2}{\pi} \left(\frac{2\sqrt{2}}{3} \left(\frac{1}{2\sqrt{p}} \right)^{3/2} \right) + O\left(p^{-5/4}\right) \\
&= \frac{2}{3\pi} p^{-3/4} + O\left(p^{-5/4}\right). \qquad (5.4)
\end{aligned}$$

In order to estimate $\pi_E^{\pm}$, we will assume that the events $a_p(E) = \pm\lfloor 2\sqrt{p} \rfloor$ for different p are disjoint, a fortiori that their conjunctions contribute to lower-order, then sum over primes $p \leq X$, since there are only finitely many primes of bad reduction:

$$\begin{aligned}
\pi_E^{\pm}(X) &= \sum_{p \leq X} 2 \left(\frac{2}{3\pi} p^{-3/4} \right) \\
&\sim \frac{4}{3\pi} \int_{2}^{X} \frac{u^{-3/4}}{\log u}\,\mathrm{d}u \\
&\sim \frac{4}{3\pi} \frac{X^{1/4}}{\log X}. \qquad (5.5)
\end{aligned}$$

Due to the unique arithmetic behavior of each isogeny class of elliptic curves, it is not heuristically clear that the constant $4/(3\pi)$ above is meaningful. We replace it by a generalized constant C_E depending on E. This is the estimate in Conjecture 2.3.

Acknowledgments

This work began while the second, third and fourth authors were undergraduate participants in the 2012 NSF sponsored REU in Computational Algebraic Geometry, Combinatorics and Number Theory at Clemson University. The fifth author served as a graduate mentor and the first author was a supervisor of the program. We all wish to thank the host institution Clemson University and the National Science Foundation, who funded this REU through DMS-1156761. We also wish to thank the anonymous referee for his or her helpful comments.

References

[AIW] S. Arias-de-Reyna, I. Inam, G. Wiese, On conjectures of Sato–Tate and Bruinier–Kohnien, preprint, arXiv:1305.5443v3 [math.NT], 2013, 26 pp.

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

[CHT] L. Clozel, M. Harris, R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations, with Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras Publ. Math. Inst. Hautes Études Sci. 108 (2008) 1–181.

[Cox] D. Cox, Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication, John Wiley & Sons, Inc., 1989.

[Dav] H. Davenport, Multiplicative Number Theory, 2nd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York–Berlin, 1980, revised by Hugh L. Montgomery.

[De] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Hambg. 14 (1941) 197–272.

[HST] M. Harris, N. Shepherd-Barron, R. Taylor, A family of Calabi–Yau varieties and potential automorphy, Ann. of Math. (2) 171 (2) (2010) 779–813.

[He1] E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, I, Math. Z. 1 (1918) 357–376.

[He2] E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, 2, Math. Z. 6 (1919) 11–51.

[Hed] J. Hedetniemi, Champion primes for elliptic curves over fields of prime order, Masters thesis, Clemson University, Clemson, SC, 2012.

[La] S. Lang, Elliptic Functions, Springer-Verlag, 1987.

[LT] S. Lang, H. Trotter, Frobenius Distribution in GL(2) Extensions, Springer-Verlag, 1976.

[Ra] C.S. Rajan, Distribution of values of Hecke characters of infinite order, Acta Arith. LXXXV (3) (1998) 279–291.

[Si1] J. Silverman, The Arithmetic of Elliptic Curves, 2nd ed., Springer-Verlag, 1986.

[Si2] J. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, 1994.

[T] R. Taylor, Automorphy for some l-adic lifts of automorphic mod l Galois representations. II, Publ. Math. Inst. Hautes Études Sci. 108 (2008) 183–239.