FROBENIUS DISTRIBUTIONS IN SHORT INTERVALS FOR NON-CM ELLIPTIC CURVES

Neha Nanda

A Thesis

in

The Department

of

Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements

For the Degree of Master of Science at

Concordia University

Montreal, Quebec, Canada

November, 2020

Concordia University

School of Graduate Studies

This is to certify that the thesis prepared

By: Neha Nanda

Entitled: Frobenius Distributions in Short Intervals for Non-CM Elliptic Curves

and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Mathematics and Statistics)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final Examining Committee:

_____ Chair

Dr. Giovanni Rosso

_____Examiner

Dr. Hershy Kisilevsky

_____Supervisor

Dr. Chantal David

Approved by _____

Dr. Galia Dafni, Graduate Program Director

_____

Dr. Pascale Sicotte, Dean of Faculty of Arts and Science

Date December 7, 2020

Abstract

Frobenius Distributions in Short Intervals for Non-CM Elliptic Curves

Neha Nanda

Let E be an elliptic curve defined over $\mathbb{Q}$. An extremal prime for E is a prime p of good reduction such that the number of rational points on E modulo p is minimal or maximal in relation to the Hasse bound, i.e. $a_p(E) = \pm \left\lfloor 2\sqrt{p} \right\rfloor$. In the first case, we say that p is a trailing prime. In the second case, we say that p is a champion prime. The notion of extremal primes was generalized to primes such that $a_p(E)/2\sqrt{p}$ lie in a short interval around $c \in (0, 1]$ in [AHJ+18], who considered the case of curves with complex multiplication.

In this thesis, assuming E does not have complex multiplication, we study the distribution in short intervals for

$$\frac{a_p(E)}{2\sqrt{p}} \in (c - f(p), c) \tag{1}$$

where $c \in (-1, 1]$ and $f(x) = x^\delta$ such that $-1/2 \leq \delta < 0$. The distribution is different if $c = 1$ or $c \neq 1$, influenced by the Sato–Tate distribution (see Conjecture 1.1). We use the techniques of David, Gafni, Malik, Prabhu, and Turnage-Butterbaugh [DGM+19], who considered the extremal primes for elliptic curves without complex multiplication to get an upper bound for the number of primes such that (1) holds, under GRH (Theorem 1.4) and unconditionally (Theorem 1.5).

Acknowledgements

First and foremost, I am extremely grateful to my supervisor Chantal David for her continuous support, patience, kindness, and valuable suggestions during my whole graduate experience at Concordia University. Her expertise and experience in the field of Number Theory have helped me immensely to complete my research work. I can not describe my gratitude in words, for the time she has spent advising me, even on the weekends.

A thank you is extended to Jungbae Nam for his inputs in the numerical computations and for teaching me the usage of SageMath. I am also grateful to Zhenyi Wang for the important discussions we have shared during the program.

Many thanks to the Graduate Program Director Galia Dafni for guiding me throughout my master's degree.

I can not forget to mention Graduate Program Assistant, Debbie Arless. She has always replied to my queries very promptly and helped me to keep a track on the due dates.

Lastly, a very special thanks to my parents and brother for their unconditional love and unwavering support.

Contents

1 Introduction and Notations **1**

2 L-Functions and Elliptic Curves **5**

2.1 Elliptic Curves over Finite Fields 5

2.1.1 The Frobenius Endomorphism and Sato–Tate Conjecture . . 7

2.2 L-functions of elliptic curves 9

2.3 Chebyshev polynomials of the Second kind and $L(s, \mathrm{Sym}^k(E))$ . . . 10

3 Explicit Equidistribution **15**

3.1 Explicit Equidistribution 17

3.2 Chebyshev polynomials and the Sato–Tate measure 19

4 Upper bounds for f-extremal primes and (c, f)-primes **22**

4.1 Proof of Theorem 1.4 23

4.2 Proof of Theorem 1.5 26

5 Conjectural Formulae and Numerical Data **28**

5.1 Probabilistic Model for $c = 1$ 29

5.2 Probabilistic Model for $c \neq 1$ 32

5.3 Numerical Data 33

References **35**

Chapter 1

Introduction and Notations

Let E be an elliptic curve over $\mathbb{Q}$. For each prime p of good reduction, E reduces to a curve $\tilde{E}$ over the finite field $\mathbb{F}_p$. By a theorem of Hasse, we know that $\#\tilde{E}(\mathbb{F}_p) = p + 1 - a_p(E)$ where $a_p(E) \in [-2\sqrt{p}, 2\sqrt{p}]$. We start now by giving the basic definitions:

Definition 1.1. Let E be an elliptic curve defined over the field of rationals $\mathbb{Q}$ and p be a prime. A prime p of good reduction for E is called

(i) an **extremal prime** of E if $|a_p(E)| = \lfloor 2\sqrt{p} \rfloor$, where $\lfloor x \rfloor$ is the usual floor function.

(ii) a **champion prime** of E if $a_p(E) = -\lfloor 2\sqrt{p} \rfloor$.

(iii) a **trailing prime** of E if $a_p(E) = \lfloor 2\sqrt{p} \rfloor$.

We also call $a_p(E)$ the trace of the Frobenius endomorphism and we remark that the normalized trace $a_p(E)/2\sqrt{p}$ belongs to the interval [-1,1]. We will discuss that in detail in Chapter 2.

The distribution of the normalized traces is given by the Sato–Tate conjecture (now a theorem due to the work of Laurent Clozel, Michael Harris, Nicholas Shepherd-Barron [HST10], [BGHT11] and Richard Taylor in [Tay08],).

Theorem 1.1 (Sato–Tate conjecture)**.** Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. Then, for real numbers $-1 \leq \alpha < \beta \leq 1$

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

The distribution of extremal primes is a generalisation of the Sato–Tate conjecture since

$$\frac{a_p(E)}{2\sqrt{p}} \in \left(1 - \frac{1}{2\sqrt{p}}, 1\right)$$

implies that p is an extremal prime.

Extremal primes were studied first by Kevin James, Brandon Tran, Minh-Tam Trinh, Phil Wertheimer, Dania Zantout in [JTT+16] who gave a conjecture (refined by James and Pollack [JP17]) for the number of extremal primes in case of CM and non-CM elliptic curves stated in the following form:

$$\#\{p \leq x : a_p(E) = \pm\lfloor 2\sqrt{p}\rfloor\} \sim \begin{cases} \frac{16}{(3\pi)} \frac{x^{1/4}}{\log x} & \text{if } E \text{ is without CM} \\ \frac{4}{3} \frac{x^{3/4}}{\log x} & \text{if } E \text{ has CM.} \end{cases}$$

as $x \longrightarrow \infty$. By symmetry a similar conjecture has been stated for the trailing and champion primes. Notice that for fixed value of $a_p(E)$, the Lang-Trotter conjecture says, as $x \longrightarrow \infty$,

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

where $C_{E,h}$ is a constant depending on E and h. Assuming holomorphicity and the GRH for the symmetric power L-functions of E, Rouse and Thorner [RT16] obtained the following upper bound for the Lang-Trotter conjecture:

$$\#\{p \leq x : a_p(E) = h\} \ll_{E,h} \frac{x^{3/4}}{\sqrt{\log x}}.$$

Using similar techniques, David, Gafni, Malik, Prabhu, and Turnage-Butterbaugh proved upper bounds for the number of extremal primes for non-CM elliptic curves:

Theorem 1.2 ([DGM+19], Theorem 1.2)**.** Let E be a non-CM elliptic curve over $\mathbb{Q}$. Assume holomorphicity and the GRH for the symmetric power L-functions of E. Then

$$\#\{x < p \leq 2x : a_p(E) = [2\sqrt{p}]\} \ll_E \sqrt{x}. \tag{1.1}$$

We remark that one of the hypothesis in Theorem 1.2 is not necessary anymore, as it was proven by Newton and Thorne [NT19] that all functions $L(s, \mathrm{Sym}^k(E))$ are automorphic and have analytic continuation to the entire complex plane for all $k \geq 1$. The GRH for the $L(s, \mathrm{Sym}^k(E))$ functions is still open.

Definition 1.2. Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. We say p is

(i) *f-nearly extremal* for E if $|a_p(E)| \in (2\sqrt{p}(1-f(p)), 2\sqrt{p})$;

(ii) a *(c,f)-prime* for E if $a_p(E) \in (2\sqrt{p}(c-f(p)), 2c\sqrt{p})$ for some constant $c \in (0,1)$.

In [AHJ+18] , Agwu *et al* gave the generalisation for the distributions of normalized traces in short intervals for elliptic curves with complex multiplication.

Theorem 1.3 ([AHJ+18], Theorem 1.6)**.** Let E be an elliptic curve with complex multiplication, and let $f(x) = o(1)$ be a convex, differentiable, regularly varying function. If $x^{-\frac{1}{2}} \ll f(x)$, 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 $\frac{1}{f(x)} = o(x^{0.265}/\log x)$ for sufficiently large x, the number of (c,f)-primes $p \leq x$ is

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

where c is some constant in $(0,1)$ and α is some real number given by Karamata's Theorem: $f(x) = x^{\alpha}g(x)$ where g is slowly varying.

In this thesis, we consider nearly extremal primes for elliptic curves without complex multiplication. We prove an upper bound for the number of such primes generalising the work of David, Gafni, Malik, Prabhu, and Turnage-Butterbaugh [DGM+19].

Theorem 1.4. Let E be a non-CM elliptic curve over $\mathbb{Q}$ and suppose that the symmetric power L-functions of E satisfy the Generalized Riemann Hypothesis. Let $f(x) = x^{\delta}$ where $-1/2 \leq \delta < 0$. Then

$$\#\{x < p \leq 2x \ : \ \frac{a_p(E)}{2\sqrt{p}} \in (1-f(p), 1)\} \ll_E xf(x),$$

and for $c \in (0,1)$,

$$\#\{x < p \leq 2x \ : \ \frac{a_p(E)}{2\sqrt{p}} \in (c-f(p), c)\} \ll_E x\sqrt{f(x)}.$$

We also prove an unconditional bound.

Theorem 1.5. Let E be a non-CM elliptic curve over $\mathbb{Q}$ and let $f(x) = x^\delta$ where $-1/2 \leq \delta < 0$. Then, for sufficiently large x,

$$\#\{x < p \leq 2x \ : \ \frac{a_p(E)}{2\sqrt{p}} \in (1 - f(p), 1)\} \ll_E \frac{x(\log(\log x))^2}{(\log x)^2},$$

and for $c \in (0, 1)$,

$$\#\{x < p \leq 2x \ : \ \frac{a_p(E)}{2\sqrt{p}} \in (c - f(p), c)\} \ll_E \frac{x \log(\log x)}{(\log x)^{\frac{3}{2}}}.$$

We also present a conjecture for the number of f extremal and (c, f)-primes in short intervals, and we test it numerically. All the experiments are conducted using SageMath version 8.8.

Conjecture 1.1. Let E be a non-CM elliptic curve over $\mathbb{Q}$. Let $f(x) = x^\delta$ where $-1/2 \leq \delta < 0$. Then,

$$\#\{p \leq x \ : \ \frac{a_p(E)}{2\sqrt{p}} \in (1 - f(p), 1)\} \sim \frac{8\sqrt{2}}{3\pi} \frac{(f(x))^{3/2}}{(3\delta + 2)} \frac{x}{\log x}.$$

and

$$\#\{p \leq x \ : \ \frac{a_p(E)}{2\sqrt{p}} \in (c - f(p), c)\} \sim \frac{2}{\pi} \frac{\sqrt{1 - c^2}}{\delta + 1} f(x) \frac{x}{\log x}.$$

where $c \in (-1, 1)$ be a constant.

This thesis is divided into five chapters.

Following introduction, Chapter 2 gives an introduction to the theory of elliptic curves over finite fields and the symmetric k-th power L-functions of E. We also provide the link between $L(s, \mathrm{Sym}^k(E))$ and Chebyshev polynomials of second kind.

Chapter 3 discusses explicit distribution, and we prove the Theorem 1.4 and the Theorem 1.5 in Chapter 4, using those tools.

In Chapter 5, we present the conjecture 1.1 for the distribution of the primes in short intervals in case of elliptic curves without CM.

Chapter 2

L-Functions and Elliptic Curves

In this chapter, we present some basic definitions and results associated with the theory of elliptic curves over finite fields. Moreover, this chapter explains some analytic results related to L-functions of elliptic curves, which we will refer later in the thesis. For more detailed introduction, we suggest the reader to go through [ST92] along with its advanced version and continuation [Sil09]. Further, [Was08] gives a very gentle introduction to the theory of elliptic curves. One can also read the paper by Rouse and Thorner [RT16] to understand the background of proposition given in last section of this chapter.

2.1 Elliptic Curves over Finite Fields

Definition 2.1. Let K be a field. An **elliptic curve** E/K (E over K) is given by generalized Weierstrass equation of the form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where $a_i \in K$. Here, (x, y) denotes the set of solutions or set of points of E/K with an additional "point at infinity" $\mathcal{O}$.
If $\text{char}(K) \neq 2, 3$, (2.1) reduces to equation of the form:

$$E : y^2 = x^3 + ax + b \tag{2.2}$$

with coefficients $a, b \in K$. We also require that E is non-singular *i.e.* $\Delta_E = -16(4a^3 - 27b^2) \neq 0$, where Δ is the discriminant of E.

Let E be an elliptic curve over $\mathbb{Q}$. For each prime p not dividing Δ_E (also called the prime of good reduction) E reduces to an elliptic curve

$$\bar{E} : y^2 = x^3 + \bar{a}x + \bar{b}$$

over $\mathbb{F}_p$.

Clearly, the number of solutions of $\bar{E}/\mathbb{F}_p$ satisfies

$$\#\bar{E}(\mathbb{F}_p) \leq 2p + 1.$$

If we use the model that there is a probability of 50% for a "randomly chosen" quadratic equation to be solvable in $\mathbb{F}_p$, we have that

$$\#\bar{E}(\mathbb{F}_p) \approx p.$$

The following result, originally conjectured by Artin in his thesis and later proved by Hasse in early 1930s shows that the above reasoning is correct.

Theorem (**Hasse**)**.** Let E be an elliptic curve over $\mathbb{F}_p$ and $E(\mathbb{F}_p)$ denotes the set of points $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ along with the point at infinity. Then,

$$\#\bar{E}(\mathbb{F}_p) = p + 1 - a_p(E), \tag{2.3}$$

with $|a_p(E)| \leq 2\sqrt{p}$.

To know more about $a_p(E)$, we need to study the endomorphism ring $\mathrm{End}(E)$.

Theorem ([Sil09], Corollary 9.4)**.** Let K be any field. The endomorphism ring of E, denoted by $\mathrm{End}(E)$, can be one of the following three type :

$$\mathrm{End}(E) = \begin{cases} \mathbb{Z}, \\ \text{order of an imaginary quadratic field}, \\ \text{an order in a quaternion algebra.} \end{cases} \tag{2.4}$$

The first two cases occur when $\mathrm{char}(K) = 0$ and the third case is possible only when $\mathrm{char}(K) > 0$.

Let E be an elliptic curve over a field K of characteristic 0. If End(E) = $\mathbb{Z}$, the elliptic curve E does not have **complex multiplication**, commonly abbreviated as non-CM.

If End(E) $\neq \mathbb{Z}$, then End(E) is order of an imaginary quadratic field. The elliptic curve E in this case is said to have **complex multiplication**, abbreviated as CM.

Example. Consider the example as in [ST92], for the elliptic curve

$$E : y^2 = x^3 + x.$$

The endomorphism $\sigma : E \longrightarrow E$ defined by

$$\sigma(x, y) = (-x, iy)$$

satisfies $\sigma^2 = [-1]$.

2.1.1 The Frobenius Endomorphism and Sato–Tate Conjecture

Definition 2.2. The **Frobenius endomorphism** of E over $\mathbb{F}_p$ is the map

$$\psi_p : E \longrightarrow E \tag{2.5}$$

which maps

$$(x, y) \mapsto (x^p, y^p). \tag{2.6}$$

Theorem 2.1. ψ_p defined by (2.5) satisfies the equation

$$X^2 - a_p(E)X + p = 0. \tag{2.7}$$

By the Hasse bound, the roots are the complex conjugate roots $\beta_p(E)$ and $\overline{\beta}_p(E)$ such that $a_p(E) = \beta_p(E) + \overline{\beta}_p(E)$ and $|\beta_p(E)| = |\overline{\beta}_p(E)| = \sqrt{p}$.

In light of the above theorem, we call $a_p(E)$ the trace of Frobenius endomorphism. From the Hasse bound, it follows that the normalized trace $a_p(E)/2\sqrt{p}$ belongs to the interval (-1,1) and we write

$$\frac{a_p(E)}{2\sqrt{p}} = \cos\left(\theta_p(E)\right) \quad \text{with} \quad 0 \leq \theta_p(E) \leq \pi. \tag{2.8}$$

We also define $\beta_p(E) = \sqrt{p}\alpha_p(E)$, and we have $\alpha_p(E) = e^{i\theta_p(E)}$.

The distribution of the Frobenius traces for non-CM elliptic curves is given by a conjecture (now a theorem) formally known as Sato–Tate conjecture. The conjecture was given in early 1960s by Sato and Tate (independently) and proved later by Richard Taylor *et al.* ([HST10], [BGHT11], [Tay08]).

Theorem. (Sato–Tate Conjecture). Consider an elliptic curve without complex multiplication defined over $\mathbb{Q}$. Then, the distribution of the normalized Frobenius traces $a_p(E)/2\sqrt{p}$ is given by

$$\lim_{x\longrightarrow\infty} \frac{1}{\pi(x)} \# \left\{ p \leq x : \frac{a_p(E)}{2\sqrt{p}} \in (\alpha, \beta) \right\} \sim \frac{2}{\pi} \int_{\alpha}^{\beta} \sqrt{1-t^2} dt$$

with $-1 \leq \alpha < \beta \leq 1$ and $\alpha, \beta \in \mathbb{R}$.

Observe the following frequency histogram distribution plots of Sato–Tate conjecture for increasing prime powers.

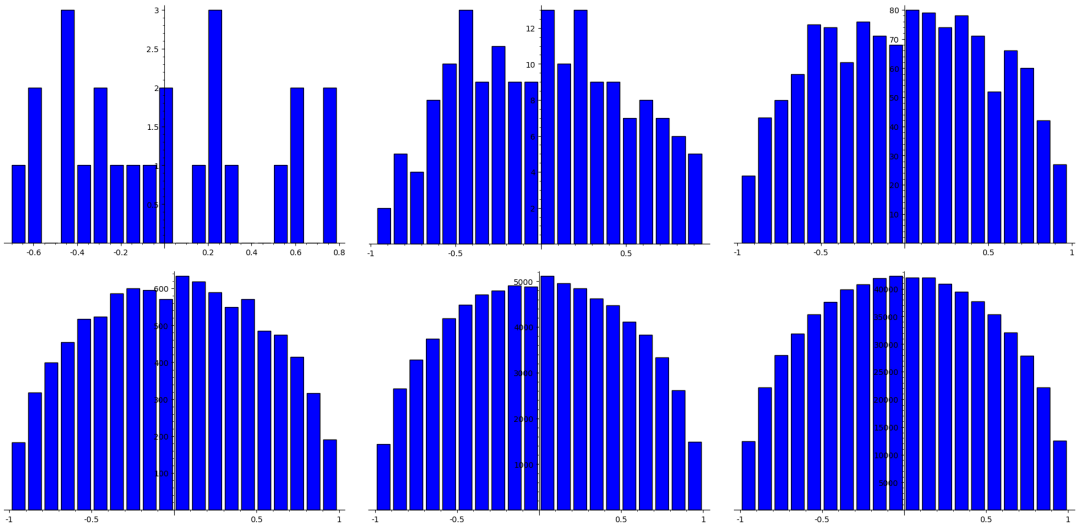


Figure 2.1: Frequency histogram distribution of Sato–Tate conjecture for different prime ranges; the first row shows $a_p(E)/2\sqrt{p}$ for p $\leq 10^2, 10^3, 10^4$ and the second row for $p \leq 10^5, 10^6, 10^7$ respectively for $E : y^2 + y = x^3 - x^2 - 10x - 20$.

Another invariant associated to elliptic curves which is important for the further discussion is the conductor N_E of E.

Definition 2.3. The **conductor** N_E of $\mathrm{E}/\mathbb{Q}$ is defined as:

$$N_E = \prod_p p^{\mathcal{F}_p}$$

where the product is over all the primes p and the exponent $\mathcal{F}_p$ depends on the reduction of E at p as

$$\mathcal{F}_p = \begin{cases} 0 & \text{if } E \text{ had good reduction at } p, \\ 1 & \text{if } E \text{ has multiplicative reduction at } p, \\ 2+\gamma_p & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

where, γ_p is a measure of "wild ramification" in the action of inertia group of Tate-module as explained in [Sil09] and [ST92]. Note here that $\gamma_p = 0$ for $p \neq 2, 3$.

2.2 L-functions of elliptic curves

Definition 2.4 (L-function of an Elliptic Curve)**.** Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. The L-function of E is the Dirichlet series

$$\begin{aligned} L(s,E) &= \prod_{p|N_E} \left(1 - \frac{a_p(E)}{p^s}\right)^{-1} \prod_{p\nmid N_E} \left(1 - \frac{\alpha_p(E)}{p^s}\right)^{-1} \left(1 - \frac{\overline{\alpha_p}(E)}{p^s}\right)^{-1} \\ &= \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s} \end{aligned}$$

where we recall that

$$\#E(\mathbb{F}_p) = p + 1 - \sqrt{p}(\alpha_p(E) + \overline{\alpha}_p(E)) \qquad \text{for} \qquad p \nmid N_E,$$

and $|\alpha_p(E)| = |\bar{\alpha}_p(E)| = 1$. Also, for the primes of bad reduction, $a_p(E) = 0, \pm 1$ depending on the type of bad reduction.

It is clear from above that $L(s,E)$ converges absolutely for $\mathrm{Re}(s) > 1$ and it was proven by Wiles that $L(s,E)$ has analytic continuation to the whole complex plane and satisfy a functional equation relating s to $(1-s)$.

For any integer $k \geq 1$, the symmetric k-th power L-functions of E are defined as:

$$L(s, \mathrm{Sym}^k(E)) = \prod_{p\nmid N_E} \prod_{j=0}^{k} \left(1 - \frac{\alpha_p(E)^j \overline{\alpha_p}(E)^{k-j}}{p^s}\right)^{-1} \prod_{p|N_E} L_p(s, \mathrm{Sym}^k(E)) \quad (2.9)$$

where the Euler factors $L_p(s, \mathrm{Sym}^k(E))$ for $p \mid N_E$ are described in ([DGM$^+$19], Appendix 1).

A note of Serre gives a relation between the Sato–Tate conjecture and analytic properties of $L(s, \mathrm{Sym}^k(E))$ (See section A.2[Ser68]). It was proven by Taylor in [Tay08], with the difference there that L-functions are not normalized, that all $L(s, \mathrm{Sym}^k(E))$ have analytic continuation to $\mathrm{Re}(s) \geq 1$, and do not vanish on the line $\mathrm{Re}(s) = 1$, which is enough to prove the Sato–Tate conjecture, but without any explicit error term.

More recently, it was shown by Newton and Thorne in [NT19] that $L(s, \mathrm{Sym}^k(E))$ has analytic continuation to the whole complex plane which makes it possible to obtain effective version of Sato–Tate conjecture without any hypothesis [Tho20].

2.3 Chebyshev polynomials of the Second kind and $L(s, \mathbf{Sym}^k(E))$

Please note that throughout this section, we use the notation θ_p to denote $\theta_p(E)$. The Chebyshev polynomials of the second kind are defined by the recurrence relation of the form :

$$U_0(x) = 1$$

$$U_1(x) = 2x$$

$$U_k(x) = 2xU_{k-1}(x) - U_{k-2}(x) \tag{2.10}$$

Now, consider the above relations for $x = \cos\theta$ and k = 0,1,2,3,.....

for $k = 0$,

$$U_0(\cos\theta) = 1$$

for $k = 1$,

$$U_1(\cos\theta) = 2\cos\theta$$

for $k = 2$,

$$U_2(\cos\theta) = 2xU_1(\cos\theta) - U_0(\cos\theta)$$

$$= 4\cos^2\theta - 1$$

and so on.

For increasing values of k, the Chebyshev polynomials of second kind satisfy

$$U_k(\cos\theta) = \frac{\sin\left((k+1)\theta\right)}{\sin\theta}. \tag{2.11}$$

We denote by $\Lambda_{\mathrm{Sym}^k(E)}(n)$ the coefficients of Dirichlet L-function

$$\frac{-L'}{L}(s, \mathrm{Sym}^k(E)) = \sum_{n=1}^{\infty} \frac{\Lambda_{\mathrm{Sym}^k(E)}(n)}{n^s}, \tag{2.12}$$

The following proposition describes the link between Chebyshev polynomials of second kind and symmetric k-th power L-functions of E.

Proposition 2.1. $\Lambda_{\mathrm{Sym}^k(E)}(n) = 0$ unless $n = p^m$ is a prime power, and for primes p not dividing N_E and $m \geq 1$

$$\Lambda_{\mathrm{Sym}^k(E)}(p^m) = U_k(\cos(m\theta_p))\log p,$$

where $k = 0, 1, 2, 3$, ...and so on.

Proof : Consider the symmetric k-th power L-function of E as in (2.9),

$$L(s, \mathrm{Sym}^k(E)) = \prod_{p\nmid N_E}\prod_{j=0}^{k}\left(1 - \frac{\alpha_p^j(E)\overline{\alpha}_p^{k-j}(E)}{p^s}\right)^{-1}\prod_{p|N_E} L_p(s, \mathrm{Sym}^k(E)).$$

Now, we define, the (partial) k-th symmetric power L-function as

$$L_1(s, \mathrm{Sym}^k(E)) := \prod_{p\nmid N_E}\prod_{j=0}^{k}\left(1 - \frac{\alpha_p^j(E)\overline{\alpha}_p^{(k-j)}(E)}{p^s}\right)^{-1}. \tag{2.13}$$

Taking logarithmic derivative in (2.13) gives

$$\begin{aligned}
\frac{L_1'}{L_1}(s, \mathrm{Sym}^k(E)) &= \frac{d}{ds}\log L_1(s, \mathrm{Sym}^k(E)) \\
&= \frac{d}{ds}\left[-\sum_{p\nmid N_E}\sum_{j=0}^{k}\log\left(1 - \alpha_p^j(E)\overline{\alpha}_p^{(k-j)}(E)p^{-s}\right)\right] \\
&= \frac{d}{ds}\left[\sum_{p\nmid N_E}\sum_{j=0}^{k}\sum_{m\geq 1}\frac{\alpha_p^{jm}(E)\overline{\alpha}_p^{(k-j)m}(E)}{mp^{ms}}\right] \\
&= -\sum_{p\nmid N_E}\sum_{j=0}^{k}\sum_{m\geq 1}\frac{\alpha_p^{jm}(E)\overline{\alpha}_p^{(k-j)m}(E)\log p}{p^{ms}},
\end{aligned} \tag{2.14}$$

where we have used

$$\log(1-t) = -\sum_{m\geq 1} \frac{t^m}{m}$$

and

$$\frac{d}{ds}\left(\frac{p^{-ms}}{m}\right) = (-p^{-ms})\log p.$$

From (2.12), now it is easy to show our result using our computation as in (2.14) and for increasing values of k.

For instance, comparing (2.12) and (2.14), we have

$$\Lambda_{\mathrm{Sym}^k(E)}(p^m) = \sum_{j=0}^{k} \alpha_p^{jm}(E)\overline{\alpha}_p^{(k-j)m}(E)\log p, \qquad m \geq 1 \tag{2.15}$$

where explicitly, $\alpha_p(E) = e^{i\theta_p}$, $\overline{\alpha}_p(E) = e^{-i\theta_p}$ and unique $\theta_p \in [0,\pi]$. For $k = 0$, the result follows trivially.

For $k = 1$,

$$\begin{aligned}
\Lambda_{\mathrm{Sym}^1(E)}(p^m) &= \sum_{j=0}^{1} \alpha_p^{jm}(E)\overline{\alpha}_p^{(1-j)m}(E)\log p \\
&= (\alpha_p^m(E) + \overline{\alpha}_p^m(E))\log p \\
&= 2\cos(m\theta_p)\log p \\
&= U_1(\cos(m\theta_p))\log p
\end{aligned}$$

which is the first Chebyshev polynomial of second kind.

For $k = 2$,

$$\begin{aligned}
\Lambda_{\mathrm{Sym}^2(E)}(p^m) &= \sum_{j=0}^{2} \alpha_p^{jm}(E)\overline{\alpha}_p^{(2-j)m}(E)\log p \\
&= \left\{\overline{\alpha}_p^{2m}(E) + \alpha_p^{2m}(E) + \alpha_p^m(E)\overline{\alpha}_p^m(E)\right\}\log p \\
&= \left\{(\alpha_p^m(E) + \overline{\alpha}_p^m(E))^2 - \alpha_p^m(E)\overline{\alpha}_p^m(E)\right\}\log p \\
&= \left\{4\cos^2(m\theta_p) - 1\right\}\log p \\
&= U_2(\cos(m\theta_p))\log p
\end{aligned}$$

which is the second Chebyshev polynomial of second kind.

For $k = 3$,

$$\begin{aligned}
\Lambda_{\mathrm{Sym}^3(E)}(p^m) &= \sum_{j=0}^{3} \alpha_p^{jm}(E)\overline{\alpha}_p^{(3-j)m}(E)\log p \\
&= \left\{\overline{\alpha}_p^{3m}(E) + \alpha_p^{3m}(E) + \alpha_p^{2m}(E)\overline{\alpha}_p^{m}(E) + \alpha_p^{m}(E)\overline{\alpha}_p^{2m}(E)\right\}\log p \\
&= \left\{\left(\alpha_p^{m}(E) + \overline{\alpha}_p^{m}(E)\right)^3 - 2\alpha_p^{m}(E)\overline{\alpha}_p^{m}(E)\left(\alpha_p^{m}(E) + \overline{\alpha}_p^{m}(E)\right)\right\}\log p \\
&= \left\{8\cos^3(m\theta_p) - 4\cos(m\theta_p)\right\}\log p \\
&= U_3\left(\cos(m\theta_p)\right)\log p
\end{aligned}$$

which is the third Chebyshev polynomial of second kind.

To prove this relation in general, we use the recurrence relation for Chebyshev polynomial of second kind given by (2.10). Since the result hold for $k = 1, 2, 3$, let us suppose by induction that the result holds for all $k \leq (r-1)$, *i.e.*,

$$\Lambda_{\mathrm{Sym}^{(r-1)}(E)}(p^m) = \frac{\sin(rm\theta_p)}{sin(m\theta_p)}\log p = U_{r-1}\left(\cos(m\theta_p)\right)\log p \tag{2.16}$$

i.e. for $k = 1, 2, .., (r-1)$.

Now, we check if the result for $k = r$. From (2.10) we have,

$$U_r\left(\cos(m\theta_p)\right) = 2\cos(m\theta_p)\{U_{r-1}\left(\cos(m\theta_p)\right)\} - U_{r-2}\left(\cos(m\theta_p)\right). \tag{2.17}$$

Consider,

$$2\cos(m\theta_p)\left\{\Lambda_{\mathrm{Sym}^{(r-1)}(E)}(p^m)\right\} - \Lambda_{\mathrm{Sym}^{(r-2)}(E)}(p^m). \tag{2.18}$$

Using the induction step (2.16), the recurrence formula (2.17) and trigonometric sum-difference formula for $\sin x$, above expression (4.2) becomes

$$\begin{aligned}
&\left[2\cos(m\theta_p)\{U_{r-1}\left(\cos(m\theta_p)\right)\} - U_{r-2}\left(\cos(m\theta_p)\right)\right]\log p \\
&= \left[2\cos(m\theta_p)\left\{\frac{\sin(rm\theta_p)}{\sin m\theta_p}\right\} - \frac{\sin((r-1)m\theta_p)}{\sin m\theta_p}\right]\log p \\
&= \left[\frac{\sin(r+1)m\theta_p}{\sin m\theta_p}\right]\log p \\
&= \left[U_r\left(\cos(m\theta_p)\right)\right]\log p \\
&= \Lambda_{\mathrm{Sym}^r(E)}(p^m).
\end{aligned}$$

Hence the result is holds for $k = r$. This implies, (2.16) holds for all values of k.

So, the result follows, *i.e.*, symmetric k-th power L-functions of E are related to the Chebyshev polynomial of second kind as

$$\Lambda_{\mathrm{Sym}^k(E)}(p^m) = U_k\left(\cos(m\theta_p)\right)\log p, \qquad p \nmid N_E.$$

□

Chapter 3

Explicit Equidistribution

Let us begin with any sequence (x_n) of real numbers. We say that the sequence (x_n) is equidistributed if the sequence $\{x_n\}$ of its fractional parts is equidistributed in $[0,1]$, where $\{x_n\} = x - [x_n]$ represents the fractional part of a sequence (x_n).

Definition 3.1. Let x_1, x_2, x_3,.... be a bounded sequence of real numbers, we say that this sequence is **equidistributed** or **uniformly distributed** (mod 1) if, for every subinterval $[\alpha, \beta] \in [0,1]$, we have

$$\lim_{N \longrightarrow \infty} \frac{\#\{n \geq 1 : 1 \leq n \leq N, \{x_n\} \in [\alpha, \beta]\}}{N} = \beta - \alpha.$$

The classical definition of equidistribution was given by Hermann Weyl in 1916 who studied the real line modulo integers, $\mathbb{R}/\mathbb{Z}$, and gave the celebrated Weyl's criterion:

Weyl's criterion: A sequence $\{x_n\}$ of real numbers is equidistributed modulo 1, if and only if for $m \neq 0$,

$$\lim_{N \longrightarrow \infty} \frac{1}{N} \sum_{n=1}^{N} e(mx_n) \longrightarrow 0.$$

Note that $e(x) := e^{2\pi i x}$.

Example 3.1 (Equidistributed sequence)**.** Let θ be an irrational number. The sequence $x_n = \{n\theta\}_{n \geq 1}$ is equidistributed in $\mathbb{R}/\mathbb{Z}$ i.e. $[0,1]$.

Proof: Given $x_n = n\theta$–$[n\theta]$, $n = 1, 2, ...$ and so on. We apply the Weyl's criterion to check the uniform distribution modulo 1.

$$\sum_{n=1}^{N} e^{(2\pi im(n\theta-[n\theta]))} = \sum_{n=1}^{N} e^{(2\pi im\theta)^n}$$
$$= \frac{e^{2\pi im\theta}(e^{(2\pi im\theta)^N}-1)}{e^{(2\pi im\theta)}-1}$$
$$\leq \frac{2}{|e^{2\pi im\theta}-1|},$$

and the denominator is bounded away from zero for any fixed θ and m, since $\theta \notin \mathbb{Q}$. We then have

$$\lim_{N\longrightarrow\infty} \frac{1}{N}\sum_{n=1}^{N} e^{(2\pi imn\theta)} \longrightarrow 0,$$

and the result follows.

Example 3.2. If θ is rational the sequence $x_n = \{n\theta\}_{n\geq 1}$ is not uniformly distributed.

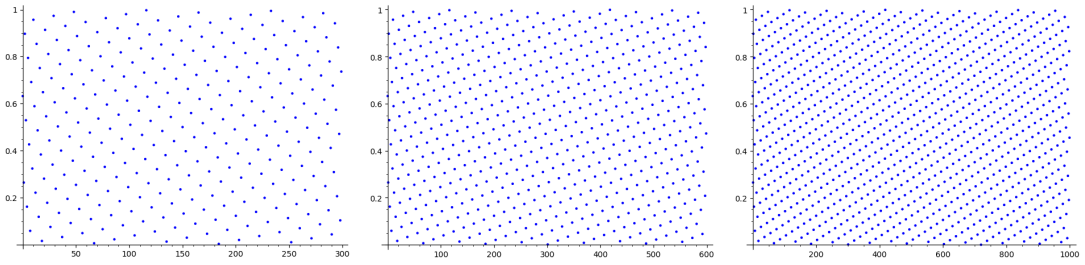
Proof. If θ is rational *i.e.* $\theta = p/q$ where p and q are coprime integers. Then, applying the Weyl's criteria for $m = q$,

$$\sum_{n=1}^{N} e^{2\pi inq(p/q)} = N.$$

So, the Weyl's criteria fails.

We plot the graphs of above sequence for different irrational values of θ to observe if the sequence of points are equidistributed or not.

(i) Equidistributed sequence: The sequence is $\{x_n\} = (\sqrt{0.4}n)_{n=1}^{N}$ where $\theta=\sqrt{0.4}$ is irrational.



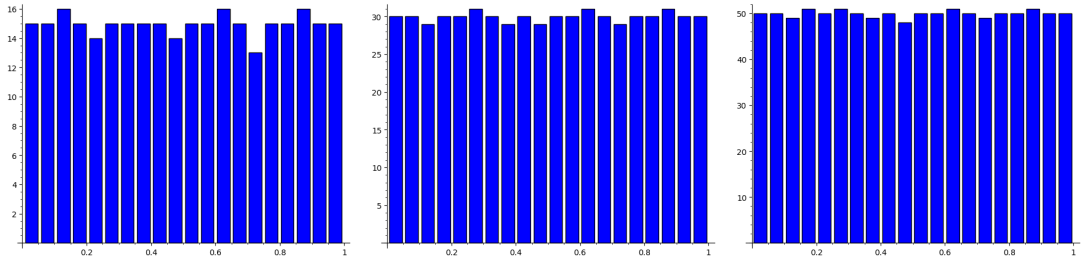


Figure 3.1: Point and histogram frequency distribution for $N = 300$, 600 and 1000 points of the sequence $(n, \sqrt{0.4}n)_{n=1}^{N}$.

(ii) Non-Equidistributed sequence: We consider a sequence which is not equidistributed, i.e.

$$\{x_n\} = \{p^{1/p}\}$$

Observe the histogram frequency and point distribution of the following sequence for $p \leq 10^3$ *and* $p \leq 10^5$ where p is prime.

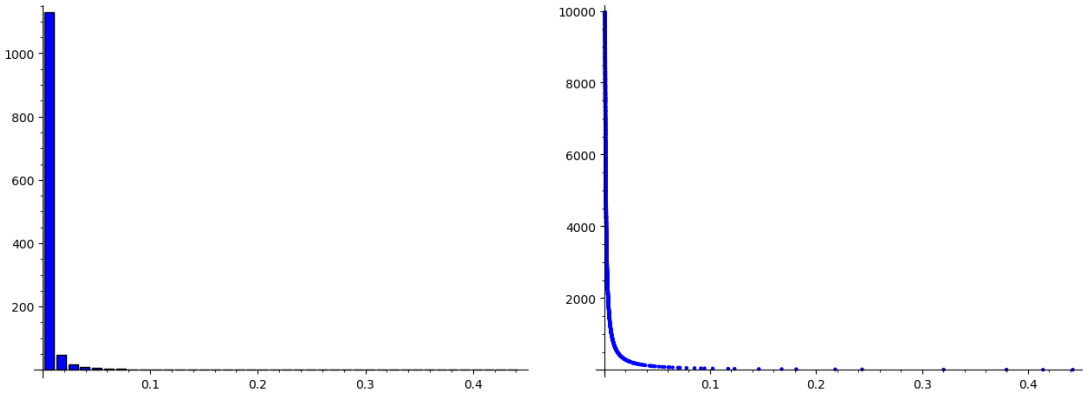


Figure 3.2: Histogram frequency distribution for $N = 10^3$ and $N = 10^5$ of the sequence $\{p^{1/p}, N\}_{p \leq N}$.

3.1 Explicit Equidistribution

This section gives brief introduction to the effective results of equidistribution, see ([Mon94], Chapter 1). Let $\chi_J(x)$ be the characteristic function of the interval $J = [\alpha, \beta] \subseteq [0, 1]$. Then, we can write

$$\chi_J(x) = \beta - \alpha + s(x - \beta) + s(\alpha - x) \tag{3.1}$$

where $s(x)$ denotes the saw-tooth function given by

$$s(x) = \begin{cases} \{x\} - 1/2 & x \notin \mathbb{Z}, \\ 0 & x \in \mathbb{Z}. \end{cases}$$

There exists trigonometric polynomials $S^+_{J,M}(x)$ and $S^-_{J,M}(x)$ which are good approximations to $\chi_J(x)$, defined by

$$S^+_{J,M}(x) = \beta - \alpha + B^*_M(x - \beta) + B^*_M(\alpha - x) \tag{3.2}$$

and

$$S^-_{J,M}(x) = \beta - \alpha - B^*_M(\beta - x) - B^*_M(x - \alpha),$$

where $B^*_M(x)$ is the M^{th} order Beurling polynomial defined as

$$\begin{aligned} B^*_M(x) = & \frac{1}{M+1} \sum_{k=1}^{M} \left(\frac{k}{M+1} - \frac{1}{2} \right) \Delta_{M+1} \left(x - \frac{k}{M+1} \right) \\ & + \frac{1}{2\pi(M+1)} \sin\left(2\pi(M+1)x\right) - \frac{1}{2\pi} \Delta_{M+1}(x) \sin\left(2\pi x\right) \\ & + \frac{1}{2\pi(M+1)} \Delta_{M+1}(x) \end{aligned}$$

and $\Delta_M(x)$ is the Féjer's kernel defined as

$$\begin{aligned} \Delta_M(x) &= \sum_{|k| \le M} \left(1 - \frac{|k|}{M} \right) e(kx) \\ &= \frac{1}{M} \left(\frac{\sin(\pi x M)}{\sin(\pi x)} \right)^2. \end{aligned}$$

We write

$$\chi_J(x) = \sum_{m \in \mathbb{Z}} \hat{\chi}_J(m) e^{-mx}$$

where $\hat{\chi}_J(m)$ is the m-th Fourier coefficient of $\chi_J(x)$ given by

$$\hat{\chi}_J(m) = \int_J e^{-mt} dt. \tag{3.3}$$

According to Vaaler's lemma, see ([Mon94], Chapter 1), these trigonometric polynomials $S^+_{J,M}(x)$ and $S^-_{J,M}(x)$ satisfy the following properties:
(1) For all $x \in \mathbb{R}$,

$$S^-_{J,M}(x) \le \chi_J(x) \le S^+_{J,M}(x). \tag{3.4}$$

(2) For $0 \leq |m| \leq M$, we have

$$|\hat{S}^{+}_{J,M}(m) - \hat{\chi}_J(m)| \leq \frac{1}{M+1}. \tag{3.5}$$

Note that since $\hat{\chi}_J(0) = \beta - \alpha$, from (3.3) and (3.5), we have

$$\hat{S}^{+}_{J,M}(0) = \beta - \alpha + O\left(\frac{1}{M+1}\right). \tag{3.6}$$

(3) We now require an estimate for $|\hat{S}^{+}_{J,M}(m)|$. If $m \neq 0$, equation (3.3) gives

$$\hat{\chi}_J(m) = \frac{e^{-m\alpha} - e^{-m\beta}}{2\pi i m} \tag{3.7}$$

and

$$\hat{\chi}_J(-m) = \frac{e^{m\beta} - e^{m\alpha}}{2\pi i m}. \tag{3.8}$$

Adding (3.7) and (3.8), we have

$$\begin{aligned}\hat{\chi}_J(m) + \hat{\chi}_J(-m) &= \frac{\sin(2\pi m\beta) - \sin(2\pi m\alpha)}{\pi m} \\ &= \frac{\sin(\pi m(\beta - \alpha))}{\pi m}.\end{aligned}$$

Hence

$$|\hat{\chi}_J(m)| = \left|\frac{\sin(\pi m(\beta - \alpha))}{\pi m}\right| \leq \min\left(\beta - \alpha, \frac{1}{\pi|m|}\right) \tag{3.9}$$

where $m \neq 0$.

Combining (3.5) and (3.9), we get, for $1 \leq |m| \leq M$,

$$|\hat{S}^{+}_{J,M}(m)| \leq \frac{1}{M+1} + \min\left(\beta - \alpha, \frac{1}{\pi|m|}\right).$$

A similar result hold true for $S^{-}_{J,M}(x)$. For a detailed exposition of these properties, please see ([Mon94], Chapter 1).

3.2 Chebyshev polynomials and the Sato–Tate measure

Definition 3.2. The sequence of polynomials $\{f_n(x)\}_{n\geq 0}$ is called **orthonormal**, if

$$< f_m(x), f_n(x) >= \int_I f_m(x) f_n(x) \mu_I(dx) = \begin{cases} 0 & \text{if } m \neq n, \\ 1 & \text{if } m = n. \end{cases}$$

where μ_I is the measure defined on the interval I, where $I = [\alpha, \beta]$.

Proposition 3.1. The Chebyshev polynomials of second kind $\{U_n(x)\}_{n\geq 0}$ form an orthonormal family with respect to the Sato–Tate measure $\mu_{ST}([\alpha,\beta])$.

Proof. Recall, the Sato–Tate measure $\mu_{ST}([\alpha,\beta])$ is given by

$$\mu_{ST}([\alpha,\beta]) = \frac{2}{\pi}\sqrt{1-x^2}dx,$$

where $[\alpha,\beta] \in [-1,1]$.

(i) For $m \neq n$, from definition and using trigonometric sum-difference formula,

$$\frac{2}{\pi}\int_{-1}^{1} U_m(x)U_n(x)\sqrt{1-x^2}dx = \frac{2}{\pi}\int_{-1}^{1} \frac{\sin\left((m+1)\cos^{-1}x\right)}{\sin\left(\cos^{-1}x\right)}\frac{\sin\left((n+1)\cos^{-1}x\right)}{\sin\left(\cos^{-1}x\right)}\sqrt{1-x^2}dx$$

With the change of variable $x = \cos(\theta)$, the last integral is

$$\begin{aligned}
&\frac{-2}{\pi}\int_{\pi}^{0} \frac{\sin\left((m+1)\theta\right)}{\sin(\theta)}\frac{\sin\left((n+1)\theta\right)}{\sin(\theta)}\sin^2(\theta)d\theta \\
&= \frac{1}{\pi}\int_{0}^{\pi} 2\sin((m+1)\theta)\sin((n+1)\theta)d\theta \\
&= 0
\end{aligned}$$

(ii) For $m = n$, using trigonometric sum-difference identities

$$\begin{aligned}
\frac{2}{\pi}\int_{-1}^{1} U_m(x)U_n(x)\sqrt{1-x^2}dx &= \frac{2}{\pi}\int_{0}^{\pi}\sin^2\left((n+1)\theta\right)d\theta \\
&= \frac{2}{\pi}\int_{0}^{\pi}\frac{1-\cos\left(2(n+1)\theta\right)d\theta}{2} \\
&= 1.
\end{aligned}$$

This proves the proposition.

Now, to get the main term as the Sato–Tate measure in the prime counting function, we need to change the basis and use the Chebyshev polynomials of second kind which are an orthonormal basis with respect to Sato–Tate measure as shown in Proposition 3.1. This has been discussed in detail in a paper by Rouse and Thorner, see ([RT16], Lemma 3.1).

Taking $J' = \frac{J}{2\pi}$, *i.e.*, $J' = [\frac{\alpha}{2\pi}, \frac{\beta}{2\pi}]$ for an interval $J = [\alpha,\beta] \subseteq [0,\pi]$ and $\theta \in [0,1]$. Define

$$F^{\pm}_{J,M}(\theta) = S^{\pm}_{J',M}\left(\frac{\theta}{2\pi}\right) + S^{\pm}_{J',M}\left(-\frac{\theta}{2\pi}\right)$$

The lemma is stated in the following form.

Lemma 3.1 ([RT16], Lemma 3.1)**.** Let $J = [\alpha, \beta] \subseteq [0, \pi]$, and let M be a positive integer. There exists trigonometric polynomials

$$F_{J,M}^{\pm}(\theta) = \sum_{m=0}^{M} \hat{F}_{J,M}^{\pm}(m) U_m(\cos(\theta))$$

that satisfies the following properties:

- For $0 \leq \theta \leq \pi$, we have

$$F_{J,M}^{-}(\theta) \leq \chi_J(\theta) \leq F_{J,M}^{+}(\theta).$$

- We have

$$|\hat{F}_{J,M}^{\pm}(0) - \mu_{ST}(J)| \leq \frac{4}{M+1}.$$

- For $1 \leq m \leq M$, we have

$$|\hat{F}_{J,M}^{\pm}(m)| \leq 4\left(\frac{1}{M+1} + \min\left(\frac{\beta-\alpha}{2\pi}, \frac{1}{\pi m}\right)\right).$$

The lemma follows directly from explicit uniform distribution and using the properties of Beurling Selberg polynomials as discussed in previous section.

The following proposition is the key result which will be used to obtain the sharper estimate for the Fourier coefficients when $J = [0, \beta]$.

Proposition 3.2 ([DGM$^+$19], proposition 2.2)**.** Let $I = [0, \frac{1}{M}] \subseteq [0, \pi]$ and $\hat{F}_{I,M}^{+}(m)$ is the m-th Fourier coefficient of $F_{I,M}^{+}(x)$ as defined earlier, then

$$\hat{F}_{I,M}^{\pm}(m) \ll \frac{1}{M^2} \qquad \text{where} \qquad 0 \leq m \leq M.$$

Chapter 4

Upper bounds for f-extremal primes and (c, f)-primes

In this Chapter, we prove the Theorem 1.4 and Theorem 1.5. Using the equidistribution tools described in Chapter 3, we write the characteristic function for

$$\cos\theta_p(E) \in (\alpha, \beta)$$

with the orthonormal basis for the Sato–Tate measure given by the Chebyshev's polynomials. We will need the estimates for

$$\sum_{p\leq x} U_n(\cos\theta_p(E)), \tag{4.1}$$

for E an elliptic curve over $\mathbb{Q}$ and $n \geq 1$.

As we proved in Chapter 2,

$$\frac{-L^{'}}{L}(s, \mathrm{Sym}^n(E)) = \sum_{\substack{p=\text{prime},\\ m\geq 1}} \frac{U_n(\cos(m\theta_p(E)))}{p^{ms}} \log p,$$

and then (4.1) can be evaluated by writing

$$\sum_{p^m\leq x} U_n(\cos(m\theta_p(E))) \log p = \frac{1}{2\pi i}\int_{(2)} \frac{-L^{'}}{L}(s, \mathrm{Sym}^n(E))\frac{x^s}{s}ds$$

with Perron's formula.

To get non-trivial upper bounds, we need to move the integral in the critical strip. This was done by Rouse and Thorner [RT16] under GRH for $L(s, \mathrm{Sym}^n(E))$.

At the time, holomorphicity of $L(s, \mathrm{Sym}^n(E))$ was proven only for Re(s) ≥ 1 by Taylor (see [Tay08], Theorem B), and it is an assumption in their theorem which can now be removed by the work of Newton and Thorne [NT19].

Proposition 4.1 ([RT16], Proposition 3.5)**.** For each $n \geq 0$, assume $L(s, \mathrm{Sym}^n(E))$ are automorphic and satisfy GRH. Then

$$\sum_p U_n(\cos(\theta_p(E)))g_x(p)\log p \ll \delta_{n,0}x + \sqrt{x}n\log n$$

for sufficiently large x and $\delta_{n,0} = 1$ if $n = 0$ and 0 otherwise. Here, $g_x(p)$ is a test function giving upper bound for the indicator function on $[x, 2x]$ such that

$$g(y) = \begin{cases} \exp\left(\frac{4}{3} + \frac{1}{(y-\frac{1}{2})(y-\frac{5}{2})}\right) & \text{if } \frac{1}{2} < y < \frac{5}{2}, \\ 0 & \text{otherwise,} \end{cases}$$

and $g_x(y) = g(y/x)$.

Using the recent work of Newton and Thorne [NT19] which proves holomorphicity of $L(s, \mathrm{Sym}^n(E))$ for all $n \geq 1$, Thorner [Tho20] obtained the bounds for (4.1) without GRH.

Proposition 4.2 ([Tho20], Proposition 2.1)**.** If $1 \leq n \ll \sqrt{\log x}/\sqrt{\log(2N_E \log x)}$ and $c_5 > 0$, $c_6 > 0$ absolutely computable constants, then

$$\left|\sum_{x<p\leq 2x} U_n(\cos\theta_p(E))\right| \ll \frac{x}{\log x}n^2\left(x^{-1/c_5 n} + \exp\left(-c_6\frac{\log x}{n^2\log(2N_E n)}\right) + \exp\left(-c_6\frac{\sqrt{\log x}}{\sqrt{n}}\right)\right),$$

where N_E is the conductor of the curve.

4.1 Proof of Theorem 1.4

To estimate the prime counting function

$$\#\{x \leq p < 2x : \frac{a_p(E)}{2\sqrt{p}} \in (1 - f(p), 1)\}, \tag{4.2}$$

we first perform the change of variable $a_p(E) = 2\sqrt{p}\cos\theta_p(E)$. Let I_ε be an interval of the form $[0, \varepsilon] \subseteq [0, \pi/2]$ and $I'_\varepsilon = [\cos(\varepsilon), 1]$ is such that

$$\cos\theta_p(E) \in I'_\varepsilon \iff \theta_p(E) \in I_\varepsilon.$$

If $\varepsilon = \varepsilon(x)$ is such that

$$\cos\varepsilon \leq 1 - f(x), \tag{4.3}$$

then for the primes counted on (4.2), we have

$$\cos\varepsilon \leq 1 - f(x) < 1 - f(p) < \frac{a_p(E)}{2\sqrt{p}},$$

and we obtain the upper bound

$$\begin{aligned}\#\{x \leq p < 2x : \frac{a_p(E)}{2\sqrt{p}} \in (1-f(p),1)\} &\leq \#\{x \leq p < 2x : \cos\theta_p(E) \in I'_\varepsilon\} \\ &= \#\{x \leq p < 2x : \theta_p(E) \in I_\varepsilon\} \\ &= \sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p(E)),\end{aligned}$$

where for any interval I, χ_I is the characteristic function of the interval.

Let $\varepsilon = \frac{1}{M}$ so that $I_\varepsilon = [0, \frac{1}{M}]$, where M will be chosen later. Using the first property of Lemma 3.1 in Chapter 3, we have

$$\begin{aligned}\sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p) &\leq \sum_{n=0}^{M} \hat{F}^+_{I_\varepsilon,M}(n) \sum_{x\leq p<2x} U_n(\cos\theta_p(E)) \\ &\leq \sum_{n=0}^{M} |\hat{F}^+_{I_\varepsilon,M}(n)| \left| \sum_{x\leq p<2x} U_n(\cos\theta_p(E)) \right|.\end{aligned} \tag{4.4}$$

From Proposition 4.1, we can bound the sums $|U_n(\cos\theta_p(E))|$ in the right hand side of above equation (4.4), we now have

$$\sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p(E)) \ll \frac{1}{\log x} \sum_{n=0}^{M} |\hat{F}^+_{I_\varepsilon,M}(n)| \left(\delta_{n,0}x + \sqrt{x}n\log n\right). \tag{4.5}$$

We now use Proposition 3.2 to bound the Fourier coefficients $\hat{F}^+_{I_\varepsilon,M}(n)$. Doing so, the right hand side of the above equation is

$$\begin{aligned}&\ll \frac{1}{M^2\log x}\left(x + \sqrt{x}\sum_{n=1}^{M} n\log n\right) \\ &\ll \frac{1}{M^2\log x}\left(x + \sqrt{x}M^2\log M\right) \\ &= \frac{x}{M^2\log x} + \frac{\sqrt{x}\log M}{\log x}\end{aligned}$$

We let

$$M = \frac{1}{\sqrt{f(x)\log x}}$$

which satisfies (4.3) since

$$\cos\left(\frac{1}{M}\right) = \cos(\sqrt{f(x)\log x}) = 1 - \frac{\log x}{2!}f(x) + O(\frac{(f(x)\log x)^2}{4!}) \leq 1 - f(x)$$

for sufficient large x.

Substituting the value of M,

$$\sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p(E)) \ll \frac{x}{M^2\log x} + \frac{\sqrt{x}\log M}{\log x} \ll xf(x).$$

Then, we have

$$\#\left\{x \leq p < 2x \ : \ a_p(E) \in (1-f(p),1)\right\} \leq \sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p(E)) \ll_E xf(x).$$

We now consider $c \neq 1$. The proof is identical except that we have a general interval $[\alpha,\beta] \subseteq [0,\pi]$ where $\alpha \neq 0$. Then, we can not use the bound of Proposition 3.2 for the Fourier coefficients and we use the weaker bound given by Lemma 3.1.

Let $c = cos(\varepsilon_0)$, and let I_ε be an interval of the form $[\varepsilon_0,\varepsilon] \subseteq [0,\pi/2]$ and $I'_\varepsilon = [\cos(\varepsilon), c]$ is such that

$$\cos\theta_p(E) \in I'_\varepsilon \iff \theta_p(E) \in I_\varepsilon.$$

If $\varepsilon = \varepsilon(x)$ is such that

$$\cos\varepsilon \leq c - f(x), \tag{4.6}$$

then using $x \leq p < 2x$, we have

$$\cos\varepsilon \leq c - f(x) < c - f(p) < \frac{a_p(E)}{2\sqrt{p}}.$$

Using this, we obtain the upper bound

$$\#\{x \leq p < 2x : \frac{a_p(E)}{2\sqrt{p}} \in (c-f(p),c)\} \leq \sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p(E)).$$

Let $I_{\varepsilon_0} = [\varepsilon_0, \varepsilon_0 + 1/M]$ where M will be chosen later. Using the Lemma 3.1 in Chapter 3,

$$\begin{aligned}\sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p) &\leq \sum_{n=0}^{M} \hat{F}^+_{I_\varepsilon,M}(n) \sum_{x\leq p<2x} U_n(\cos\theta_p(E)) \\ &\leq \sum_{n=0}^{M} |\hat{F}^+_{I_\varepsilon,M}(n)| \left|\sum_{x\leq p<2x} U_n(\cos\theta_p(E))\right| \\ &\ll \sum_{n=0}^{M} \frac{1}{M} \left|\sum_{x\leq p<2x} U_n(\cos\theta_p(E))\right|.\end{aligned} \tag{4.7}$$

Using Proposition 4.1, this gives

$$\sum_{x\le p<2x}\chi_{I_\varepsilon}(\theta_p(E)) \ll_E \frac{1}{M\log x}\left(x+\sqrt{x}\sum_{n=1}^{M} n\log n\right) \ll_E \frac{x}{M\log x}+\frac{\sqrt{x}M\log M}{\log x}. \tag{4.8}$$

We let

$$\frac{1}{M}=\sqrt{f(x)}\log x$$

which satisfies (4.6) since

$$\begin{aligned}\cos\left(\varepsilon_0+\frac{1}{M}\right) &= \cos\varepsilon_0-\frac{1}{2}\cos\varepsilon_0\left(\frac{1}{M}\right)^2+O\left(\left(\frac{1}{M}\right)^4\right)\\ &= c-\frac{c}{2}f(x)\log^2 x+O((f(x))^2\log^4 x)\\ &\le c-f(x).\end{aligned}$$

for sufficient large x.

We get the result by substituting value of M in (4.8),

$$\sum_{x\le p<2x}\chi_{I_\varepsilon}(\theta_p(E)) \ll_E \frac{x}{M\log x}+\frac{\sqrt{x}M\log M}{\log x} \ll_E x\sqrt{f(x)}+\frac{\sqrt{x}}{\sqrt{f(x)}}$$

and since we have

$$\frac{1}{\sqrt{f(x)}} \ll_E x^{1/4} \ll_E x^{1/2}\sqrt{f(x)}$$

$$\#\left\{x\le p<2x\ :\ a_p(E)\in(c-f(p),c)\right\} \le \sum_{x\le p<2x}\chi_{I_\varepsilon}(\theta_p(E)) \ll_E x\sqrt{f(x)}.$$

where $c\in(0,1)$.

4.2 Proof of Theorem 1.5

In the proof of Theorem 1.4, we are able to take n large in Proposition 4.1 to get a good bound, the only constraint being (4.3) where $\varepsilon=1/M$ and $n\le M$.

If we do not assume GRH and we use Proposition 4.2, then the largest value of n that we can take is

$$n=\frac{\sqrt{\log x}}{\sqrt{\log\log x}}.$$

This automatically satisfies (4.3) for any $f(x) = x^\delta$ with $-1/2 < \delta < 0$ as

$$\begin{aligned}\cos\left(\frac{1}{M}\right) &= 1 - \frac{(\log(\log x))^2}{2!\log x} + O\left(\frac{(\log(\log x))^4}{(\log x))^2}\right)\\ &\leq 1 - x^\delta.\end{aligned}$$

which is true for any $\delta < 0$.

Using Proposition 3.2 to bound the Fourier coefficients, for $c = 1$, we have the bound

$$\sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p(E)) \ll_E \frac{(\pi(2x) - \pi(x))}{M^2} + \frac{1}{M^2}\sum_{n=1}^{M}\left|\sum_{x<p\leq 2x} U_n \cos\theta_p(E)\right|.$$

Using

$$M = \frac{\sqrt{\log x}}{\log(\log x)}, \tag{4.9}$$

and Proposition 4.2, we get

$$\begin{aligned}\sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p(E)) &\ll_E \frac{(\pi(2x) - \pi(x))}{M^2} + \frac{1}{M^2}\sum_{n=1}^{M}\left|\sum_{x<p\leq 2x} U_n \cos\theta_p(E)\right|\\ &\ll_E \frac{x}{M^2\log x} + \frac{x}{\log x}\exp\left(-\frac{\log x}{M^2\log M}\right)\\ &\ll_E \frac{x(\log(\log(x)))^2}{(\log x)^2} + \frac{x}{(\log x)^2} \ll_E \frac{x(\log(\log(x)))^2}{(\log x)^2}\end{aligned}$$

and which proves the result for $c = 1$.

Note here that value of M is smaller than the maximal value allowed in the Proposition 4.2, because then the bound would be too big.

Now, we consider the case when $c \neq 1$ and we take any interval $[\alpha, \beta] \subseteq [0, \pi]$. Here again, we use Lemma 3.1 to bound the Fourier coefficients, we get

$$\begin{aligned}\sum_{x\leq p<2x} \chi_{I_\varepsilon}(\theta_p(E)) &\ll_E \frac{(\pi(2x) - \pi(x))}{M} + \frac{1}{M}\sum_{n=1}^{M}\left|\sum_{x<p\leq 2x} U_n \cos\theta_p(E)\right|\\ &\ll_E \frac{x}{M\log x} + \frac{Mx}{\log x}\exp\left(-\frac{\log x}{M^2\log M}\right)\end{aligned}$$

Using M as in (4.9) again, we get the result for $c \neq 1$.

Chapter 5

Conjectural Formulae and Numerical Data

We now give conjectures for the Frobenius distributions in short intervals for non-CM elliptic curves, and support them by providing numerical data. The conjectures as stated in the introduction (Conjecture 1.1) gives only the main term of the conjectural asymptotic, but there are secondary terms which affect significantly the fit with the data. For $c = 1$, the conjecture is obtained by summing the conjectural probabilities

$$\text{Prob}\left(\frac{a_p(E)}{2\sqrt{p}} \in (1 - f(p), 1)\right) \sim \frac{4\sqrt{2}}{3\pi} f(p)^{3/2} \tag{5.1}$$

over all $p \leq x$. This lead to a main term of order $xf(x)^{3/2}/\log x$ but also to terms of order $xf(x)^{3/2}/\log^2 x$, $xf(x)^{3/2}/\log^3 x$, etc. We computed the first 3 such terms, and we see in Tables 5.1 and 5.2 how adding more terms improves the fit with the data.

Another approximation occurs in the computation of the probabilistic model (5.1), where the Taylor series of the Sato–Tate measure around $c = 1$ was used. Keeping more terms in the Taylor series also improves the fit with the numerical data.

The same remarks apply to the case $c \neq 1$. In this case, the Taylor series around c has secondary terms with a very large constant when c is very close to 1, and those terms affect very significantly the fit with the data. Again, we refer

the reader to Tables 5.1 and 5.2.

We first state a refinement of Conjecture 1.1 according to the remarks above, and we then explain the probabilistic model leading to the conjecture.

Conjecture 5.1. Let E be a non-CM elliptic curve over $\mathbb{Q}$. Let $f(x) = x^\delta$ where $-1/2 \leq \delta < 0$. Then,

$$\begin{aligned}\pi^+_{\delta,\, c=1}(x) = &\left(\frac{8\sqrt{2}}{3\pi}\frac{f(x)^{3/2}}{(3\delta+2)} - \frac{2\sqrt{2}}{5\pi}\frac{f(x)^{5/2}}{(5\delta+2)}\right)\frac{x}{\log x}\\ &+\left(\frac{16\sqrt{2}}{3\pi}\frac{f(x)^{3/2}}{(3\delta+2)^2} - \frac{4\sqrt{2}}{5\pi}\frac{f(x)^{5/2}}{(5\delta+2)^2}\right)\frac{x}{\log^2 x}\\ &+\left(\frac{64\sqrt{2}}{3\pi}\frac{f(x)^{3/2}}{(3\delta+2)^3} - \frac{16\sqrt{2}}{5\pi}\frac{f(x)^{5/2}}{(5\delta+2)^3}\right)\frac{x}{\log^3 x}\\ &+O\left(\frac{x}{\log^4 x}\right)\end{aligned}$$

Let $c \in (-1, 1)$ be a constant. Then

$$\begin{aligned}\#\{p \leq x \ :\ \frac{a_p(E)}{2\sqrt{p}} \in (c - f(p), c)\} = &\left(\frac{2}{\pi}\frac{\sqrt{1-c^2}}{\delta+1}f(x) + \frac{c}{\pi\sqrt{1-c^2}}\frac{(f(x))^2}{2\delta+1}\right)\frac{x}{\log x}\\ &+\left(\frac{2}{\pi}\frac{\sqrt{1-c^2}}{(\delta+1)^2}f(x) + \frac{c}{\pi\sqrt{1-c^2}}\frac{(f(x))^2}{(2\delta+1)^2}\right)\frac{x}{\log^2 x}\\ &+\left(\frac{4}{\pi}\frac{\sqrt{1-c^2}}{(\delta+1)^3}f(x) + \frac{2c}{\pi\sqrt{1-c^2}}\frac{(f(x))^2}{(2\delta+1)^3}\right)\frac{x}{\log^3 x}\\ &+O\left(\frac{x}{\log^4 x}\right).\end{aligned} \tag{5.2}$$

5.1 Probabilistic Model for $c = 1$

We use the Sato–Tate law to construct our conjecture, similar to the authors of [JTT+16] who use the model

$$\begin{aligned}\text{Prob}\left(a_p(E) = \lfloor 2\sqrt{p}\rfloor\right) &= \frac{2}{\pi}\int_{1-\frac{1}{2\sqrt{p}}}^{1}\sqrt{1-t^2}dt\\ &= \frac{2}{3\pi}p^{-3/4} + O(p^{-5/4}).\end{aligned} \tag{5.3}$$

We remark that this is a heuristic as the Sato–Tate is not proven in such a small interval. We do the same for $f(p) = p^\delta$ and use the model

$$\text{Prob}\left(\frac{a_p(E)}{2\sqrt{p}} \in (1 - f(p), 1)\right) = \frac{2}{\pi}\int_{1-f(p)}^{1}\sqrt{1-t^2}dt$$

We will expand the Taylor series of $f(t) = \sqrt{1-t^2}$ around $t = 1$. Substituting $y = 1 - t$ in $\sqrt{1-t^2} = \sqrt{(1-t)(1+t)}$, we get

$$\begin{aligned}\sqrt{(1-t)(1+t)} &= \sqrt{y(2-y)} \\ &= \sqrt{2y}\sqrt{1-\frac{y}{2}}.\end{aligned} \tag{5.4}$$

Here, from $y = 1-t$, we can see that as $y \longrightarrow 0$, $t \longrightarrow 1$. So, we use the Taylor series expansion of $\sqrt{1-\frac{y}{2}}$ around the point $y \longrightarrow 0$, *i.e.*

$$\sqrt{1-\frac{y}{2}} = 1 - \frac{y}{4} + O(y^2).$$

So, (5.4) becomes

$$\begin{aligned}\sqrt{1-t^2} &= \sqrt{2y}\left(1 - \frac{y}{4} + O(y^2)\right) \\ &= \sqrt{2y} - \frac{1}{2\sqrt{2}}y^{3/2} + O(y^{5/2}) \\ &= \sqrt{2}\sqrt{1-t} - \frac{1}{2\sqrt{2}}(1-t)^{3/2} + O((1-t)^{5/2}).\end{aligned}$$

Hence,

$$\begin{aligned}&\text{Prob}\left(\frac{a_p(E)}{2\sqrt{p}} \in (1-f(p), 1)\right) \\ &= \frac{2}{\pi}\int_{1-f(p)}^{1}\sqrt{1-t^2}\,dt = \frac{2}{\pi}\int_{1-f(p)}^{1}\sqrt{2}\sqrt{1-t} - \frac{1}{2\sqrt{2}}(1-t)^{3/2} + O((1-t)^{5/2})\,dt.\end{aligned} \tag{5.5}$$

Summing the probabilities, we get

$$\#\left(p \le x : \frac{a_p(E)}{2\sqrt{p}} \in (1-f(p), 1)\right) = \sum_{p\le x}\frac{4\sqrt{2}}{3\pi}f(p)^{3/2} - \frac{\sqrt{2}}{5\pi}f(p)^{5/2} + O(f(p)^{7/2}).$$

We use

$$\sum_{p\le x} p^{\delta} = \pi(x)x^{\delta} - \delta\int_2^x \pi(t)t^{\delta-1}dt \tag{5.6}$$

and

$$\pi(t) = \int\frac{dt}{\log t} = \frac{t}{\log t} + \frac{t}{\log^2 t} + 2!\frac{t}{\log^3 t} + O\left(\frac{t}{\log^4 t}\right).$$

Then

$$\begin{aligned}\int_1^x \pi(t)t^{\delta-1}dt &= \int_1^x\left[\frac{t}{\log t} + \frac{t}{\log^2 t} + 2!\frac{t}{\log^3 t} + 3!\frac{t}{\log^4 t} + O\left(\frac{t}{\log^5 t}\right)\right]t^{\delta-1}dt \\ &= \int_1^x\left[\frac{t^{\delta}}{\log t} + \frac{t^{\delta}}{\log^2 t} + 2!\frac{t^{\delta}}{\log^3 t} + 3!\frac{t^{\delta}}{\log^4 t} + O\left(\frac{t^{\delta}}{\log^5 t}\right)\right]dt\end{aligned} \tag{5.7}$$

and we compute

$$\int_1^x \frac{t^\delta}{\log t} = \frac{1}{(\delta+1)}\frac{x^{\delta+1}}{\log x} + \frac{1}{(\delta+1)^2}\frac{x^{\delta+1}}{\log^2 x} + \frac{2!}{(\delta+1)^3}\frac{x^{\delta+1}}{\log^3 x} + \frac{3!}{(\delta+1)^4}\frac{x^{\delta+1}}{\log^4 x} + O\left(\frac{x^{\delta+1}}{\log^5 x}\right);$$
$$\int_1^x \frac{t^\delta}{\log^2 t} = \frac{1}{(\delta+1)}\frac{x^{\delta+1}}{\log^2 x} + \frac{2!}{(\delta+1)^2}\frac{x^{\delta+1}}{\log^3 x} + \frac{3!}{(\delta+1)^3}\frac{x^{\delta+1}}{\log^4 x} + O\left(\frac{x^{\delta+1}}{\log^5 x}\right);$$
$$\int_1^x 2!\frac{t^\delta}{\log^3 t} = \frac{2!}{(\delta+1)}\frac{x^{\delta+1}}{\log^3 x} + \frac{3!}{(\delta+1)^2}\frac{x^{\delta+1}}{\log^4 x} + O\left(\frac{x^{\delta+1}}{\log^5 x}\right);$$
$$\int_1^x 3!\frac{t^\delta}{\log^4 t} = \frac{3!}{(\delta+1)}\frac{x^{\delta+1}}{\log^4 x} + O\left(\frac{x^{\delta+1}}{\log^5 x}\right);$$

and so on.

Replacing in (5.7), we have

$$\begin{aligned}\int_1^x \pi(t)t^{\delta-1}dt = &\frac{1}{(\delta+1)}\frac{x^{\delta+1}}{\log x}\\ &+\left(\frac{1!}{(\delta+1)}+\frac{1!}{(\delta+1)^2}\right)\frac{x^{\delta+1}}{\log^2 x}\\ &+\left(\frac{2!}{(\delta+1)}+\frac{2!}{(\delta+1)^2}+\frac{2!}{(\delta+1)^3}\right)\frac{x^{\delta+1}}{\log^3 x}\\ &+\left(\frac{3!}{(\delta+1)}+\frac{3!}{(\delta+1)^2}+\frac{3!}{(\delta+1)^3}+\frac{3!}{(\delta+1)^4}\right)\frac{x^{\delta+1}}{\log^4 x}\\ &\vdots\\ &+\left(\frac{(k-1)!}{(\delta+1)}+\frac{(k-1)!}{(\delta+1)^2}+\frac{(k-1)!}{(\delta+1)^3}+...+\frac{(k-1)!}{(\delta+1)^k}\right)\frac{x^{\delta+1}}{\log^k x}\\ &+O\left(\frac{x^{\delta+1}}{\log^{k+1} x}\right)\\ &=\sum_{k=1}^{n}\frac{x^{\delta+1}(k-1)!}{\log^k x}\left(\frac{1}{(\delta+1)}+\frac{1}{(\delta+1)^2}+...+\frac{1}{(\delta+1)^k}\right)+O\left(\frac{x^{\delta+1}}{\log^{n+1} x}\right).\end{aligned} \tag{5.8}$$

Substituting (5.8) in (5.6), we get

$$\sum_{p\le x} p^\delta = \pi(x)x^\delta - \delta\sum_{k=1}^{n}\frac{x^{\delta+1}(k-1)!}{\log^k x}\left(\frac{1}{(\delta+1)}+\frac{1}{(\delta+1)^2}+...+\frac{1}{(\delta+1)^k}\right)+O\left(\frac{x^{\delta+1}}{\log^{n+1} x}\right). \tag{5.9}$$

Now, we estimate the first term of (5.5) using (5.9), replacing δ by $3\delta/2$ in (5.9) to get that

$$\sum_{p\le X}\frac{4\sqrt{2}}{3\pi}f(p)^{\frac{3}{2}} \tag{5.10}$$

$$= \frac{8\sqrt{2}}{3\pi}\frac{f(x)^{3/2}}{(3\delta+2)}\frac{x}{\log x} + \frac{16\sqrt{2}}{3\pi}\frac{f(x)^{3/2}}{(3\delta+2)^2}\frac{x}{\log^2 x} + \frac{64\sqrt{2}}{3\pi}\frac{f(x)^{3/2}}{(3\delta+2)^3}\frac{x}{\log^3 x} + O\left(\frac{x}{\log^4 x}\right). \tag{5.11}$$

We do the same computations with $5\delta/2$ and we get the conjecture for $c = 1$.

5.2 Probabilistic Model for $c \neq 1$

We now consider

$$\text{Prob}\left(\frac{a_p(E)}{2\sqrt{p}} \in (c - f(p), c)\right) = \frac{2}{\pi}\int_{c-f(p)}^{c} \sqrt{1-t^2}dt$$

when $c \neq \pm 1$.

The Taylor series of $\sqrt{1-t^2}$ around $t = c$ is given by

$$\sqrt{1-t^2} = \sqrt{1-c^2} - \frac{c(t-c)}{\sqrt{1-c^2}} + O((t-c)^2).$$

and

$$\begin{aligned}\frac{2}{\pi}\int_{c-f(p)}^{c} \sqrt{1-t^2}\,dt &= \frac{2}{\pi}\int_{c-f(p)}^{c}\left(\sqrt{1-c^2} - \frac{c(t-c)}{\sqrt{1-c^2}} + O((t-c)^2)\right)dt \\ &= \frac{2}{\pi}\sqrt{1-c^2}f(p) + \frac{c}{\pi\sqrt{1-c^2}}(f(p))^2 + O(f(p)^3).\end{aligned} \tag{5.12}$$

To estimate the first term in (5.12), we can follow the same procedure as above in (5.10), and we have

$$\begin{aligned}\sum_{p<x}\frac{2}{\pi}\sqrt{1-c^2}f(p) &= \frac{2}{\pi}\sqrt{1-c^2}\left(1 - \frac{\delta}{\delta+1}\right)\frac{x}{\log x}f(x) \\ &+ \frac{2}{\pi}\sqrt{1-c^2}\left(1 - \delta\left[\frac{1}{\delta+1} + \frac{1}{(\delta+1)^2}\right]\right)\frac{x}{\log^2 x}f(x) \\ &+ \frac{2}{\pi}\sqrt{1-c^2}\left(1 - \delta\left[\frac{1}{\delta+1} + \frac{1}{(\delta+1)^2} + \frac{1}{(\delta+1)^3}\right]\right)\frac{2x}{\log^3 x}f(x) \\ &+ O\left(\frac{x}{\log^4 x}\right) \\ &= \frac{2}{\pi}\sqrt{1-c^2}\frac{f(x)}{\delta+1}\frac{x}{\log x} + \frac{2}{\pi}\sqrt{1-c^2}\frac{f(x)}{(\delta+1)^2}\frac{x}{\log^2 x} \\ &+ \frac{4}{\pi}\sqrt{1-c^2}\frac{f(x)}{(\delta+1)^3}\frac{x}{\log^3 x} + O\left(\frac{x}{\log^4 x}\right).\end{aligned} \tag{5.13}$$

Now, estimating the second term in (5.12) in a similar way, we get

$$\sum_{p\leq x}\frac{c}{\pi\sqrt{1-c^2}}f(p)^2$$

$$=\frac{c}{\pi\sqrt{1-c^2}}\frac{(f(x))^2}{2\delta+1}\frac{x}{\log x}+\frac{c}{\pi\sqrt{1-c^2}}\frac{(f(x))^2}{(2\delta+1)^2}\frac{x}{\log^2 x}+\frac{2c}{\pi\sqrt{1-c^2}}\frac{(f(x))^2}{(2\delta+1)^3}\frac{x}{\log^3 x}$$
$$+O\left(\frac{x}{\log^4 x}\right). \tag{5.14}$$

and the conjecture for $c\neq 1$ follows.

5.3 Numerical Data

We used SageMath to check $f(x)=x^{-1/4}$ and $f(x)=x^{-1/10}$ at $c=1$, 0.99, $0.9, 0$ with x up to 10^{12}, $E: y^2+y=x^3-x^2-10x-20$.

$x=10^{12}$	**I**	**I+II**	**I+II+III**	**Numerical Data**
$\delta=-1/4$ $c=1$	$1.098356*10^6$	$1.161947*10^6$	$1.169310*10^6$	$1.171319*10^6$
$\delta=-1/10$ $c=1$	$4.00525073*10^8$	$4.17553931*10^8$	$4.19001657*10^8$	$4.19377511*10^8$
$\delta=-1/4$ $c=0$	$3.0707691*10^7$	$3.2189489*10^7$	$3.2332497*10^7$	$3.2333155*10^7$
$\delta=-1/10$ $c=0$	$1.614603578*10^9$	$1.679530747*10^9$	$1.684752508*10^9$	$1.684675291*10^9$
$\delta=-1/4$ $c=0.9$	$1.3432725*10^7$	$1.4082068*10^7$	$1.4144902*10^7$	$1.4169856*10^7$
$\delta=-1/10$ $c=0.9$	$8.22108289*10^8$	$8.55762016*10^8$	$8.58522424*10^8$	$8.45086360*10^8$
$\delta=-1/4$ $c=0.99$	$4.493481*10^6$	$4.714213*10^6$	$4.736080*10^6$	$4.733732*10^6$
$\delta=-1/10$ $c=0.99$	$6.29926217*10^8$	$6.57278566*10^8$	$6.59661274*10^8$	$4.87916384*10^8$

Table 5.1: The table shows the conjectural count obtained by taking the first two terms of the Taylor series $f(x)^{3/2}$ and $f(x)^{5/2}$ for $c=1$ and $f(x)$ and $f(x)^2$ for $c\neq 1$ and only the $x/\log x$ term (I), the first two terms $x/\log x$ and $x/(\log x)^2$ (I+II) and the first three terms $x/\log x$, $x/(\log x)^2$ and $x/(\log x)^3$(I+II+III).

$x = 10^{12}$	**I**	**I+II**	**I+II+III**	**Numerical data**
$\delta = -1/4$ $c = 1$	$1.098631 * 10^6$	$1.162249 * 10^6$	$1.169617 * 10^6$	$1.171319 * 10^6$
$\delta = -1/10$ $c = 1$	$4.04867796 * 10^8$	$4.22106212 * 10^8$	$4.23574163 * 10^8$	$4.19377511 * 10^8$
$\delta = -1/4$ $c = 0$	$3.0707691 * 10^7$	$3.2189489 * 10^7$	$3.2332497 * 10^7$	$3.2333155 * 10^7$
$\delta = -1/10$ $c = 0$	$1.614603578 * 10^9$	$1.679530747 * 10^9$	$1.684752508 * 10^9$	$1.684675291 * 10^9$
$\delta = -1/4$ $c = 0.9$	$1.3385172 * 10^7$	$1.4031073 * 10^7$	$1.4093409 * 10^7$	$1.4169856 * 10^7$
$\delta = -1/10$ $c = 0.9$	$7.03789383 * 10^8$	$7.32090480 * 10^8$	$7.34366593 * 10^8$	$8.45086360 * 10^8$
$\delta = -1/4$ $c = 0.99$	$4.331853 * 10^6$	$4.540886 * 10^6$	$4.561060 * 10^6$	$4.733732 * 10^6$
$\delta = -1/10$ $c = 0.99$	$2.27767863 * 10^8$	$2.36926967 * 10^8$	$2.37663587 * 10^8$	$4.87916384 * 10^8$

Table 5.2: The table shows the conjectural count obtained by taking only one term of the Taylor series. Notice that the effect on the fit with the data is particularly affected when c is very close to 1 due to the constant $1/\sqrt{1-c^2}$ in the second term of the Taylor series.

References

[AHJ+18] Anthony Agwu, Phillip Harris, Kevin James, Siddarth Kannan, and Huixi Li. Frobenius distributions in short intervals for cm elliptic curves. *Journal of Number Theory*, 188:263–280, 2018.

[BGHT11] Thomas Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of calabi–yau varieties and potential automorphy ii. *Publications of The Research Institute for Mathematical Sciences*, 47(1):29–98, 2011.

[DGM+19] C. David, A. Gafni, A. Malik, N. Prabhu, and Caroline LaRoche Turnage-Butterbaugh. Extremal primes for elliptic curves without complex multiplication. *Proceedings of the American Mathematical Society*, 148(3):929–943, 2019.

[HST10] Michael Harris, Nick Shepherd-Barron, and Richard L. Taylor. A family of calabi-yau varieties and potential automorphy. *Annals of Mathematics*, 171(2):779–813, 2010.

[JP17] Kevin James and Paul Pollack. Extremal primes for elliptic curves with complex multiplication. *Journal of Number Theory*, 172:383–391, 2017.

[JTT+16] Kevin L. James, Brandon Tran, Minh Tam Trinh, Phil Wertheimer, and Dania Zantout. Extremal primes for elliptic curves. *Journal of Number Theory*, 164:282–298, 2016.

[Mon94] Hugh L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume volume 84 of CBMS Regional Conference Series in Mathematics. Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, 1994.

[NT19] James Newton and Jack A. Thorne. Symmetric power functoriality for holomorphic modular forms. *arXiv preprint arXiv:1912.11261*, 2019.

[RT16] Jeremy Rouse and Jesse Thorner. The explicit sato-tate conjecture and densities pertaining to lehmer-type questions. *Transactions of the American Mathematical Society*, 369(5):3575–3604, 2016.

[Ser68] Jean Pierre Serre. *Abelian L-Adic Representations And Elliptic Curves*. 1968.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[ST92] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. 1992.

[Tay08] Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l galois representations. *Publications Mathématiques de l'IHÉS*, 108(1):183–239, 2008.

[Tho20] Jesse Thorner. Effective forms of the sato–tate conjecture. *arXiv preprint arXiv:2002.10450*, 2020.

[Was08] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. 2008 by Taylor and Francis Group, LLC, 2008.