Average Frobenius Distribution in Families of Elliptic Curves

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Arijit Chakraborty

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

July, 2021

Supervisor: Dr Kaneenika Sinha

Certificate

This is to certify that this dissertation entitled Average Frobenius Distribution in Families of Elliptic Curves towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Arijit Chakraborty at Indian Institute of Science Education and Research under the supervision of Dr Kaneenika Sinha, Associate Professor, Department of Mathematics , during the academic year 2020-2021.

Dr Kaneenika Sinha

Committee:

Dr Kaneenika Sinha

Dr Stephan Baier

This thesis is dedicated to Maa and Bapi

Declaration

I hereby declare that the matter embodied in the report entitled Average Frobenius Distribution in Families of Elliptic Curves are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Dr Kaneenika Sinha and the same has not been submitted elsewhere for any other degree.

Arijit Chakraborty

Acknowledgments

First of all, I would like to express my heartiest gratitude to my supervisor Professor Kaneenika Sinha, without whose patient guidance and help, this study would not be possible. Her expertise and vast knowledge in the field enabled me to learn the subject from scratch.

But her contribution to my academic career goes much beyond this thesis. This acknowledgement page is too small of an area to thank her enough for all her help.

I thank Professor Stephan Baier for sharing his expertise and helpful inputs on the thesis topic, and for his extremely encouraging correspondence.

I would also like to thank IISER Pune for providing me with a great learning atmosphere even at a challenging time like this, especially all the people in the Mathematics department for their kind guidance.

I thank my small group of Sounak, Writam, Gopal and Wridhdhi for their help and support throughout my stay here at IISER Pune.

Last but not least, I thank my parents for all the love and care and for being supportive all the time.

Abstract

An elliptic curve E over a field $\mathbb{F}$ can be defined by the equation

$$y^2 = x^3 + ax + b,$$

where a, $b \in \mathbb{F}$. For any $r \geq 1$, let $a_E(p^r)$ denote the trace of the Frobenius endomorphism of E over the field $\mathbb{F}_{p^r}$, p being a prime. For a natural number k, let κ denote the set of all k-th powers of natural numbers. James and Yu in their work [JY06] computed the distribution of

$$\{a_E(p) : \ a_E(p) \in \kappa\}$$

as the primes $p \to \infty$ by averaging over suitable families of elliptic curves. In this thesis we review the work of James and Yu [JY06]. In an effort to obtain a smooth analogue of the main result proved in [JY06], we present a methodology for the same and explain the technical problems encountered. At the end of this thesis we provide a result about the distribution of $a_E(p^2)$ by taking average over a family of elliptic curves.

Contents

Chapter 1

Introduction

The goal of this chapter is to introduce and state the primary topic of study in this thesis. We study a variant of the Sato-Tate distribution theorem that was addressed by K. James and G. Yu [JY06].

We begin by reviewing basic projective geometry that leads to the notion of elliptic curves over a field in Section 1.2.1. In Sections 1.2.2 and 1.2.3, we review the notions of an elliptic curve over a field $\mathbb{F}$ and the Mordell-Weil group of such a curve. In Section 1.2.4, we review a proof of the fundamental theorem which states that the Mordell-Weil group of an elliptic curve over the field of rational numbers $\mathbb{Q}$ is finitely generated. In Section 1.2.5, we turn our attention to Mordell-Weil groups of elliptic curves over finite fields and discuss an arithmetic important sequence arising from such curves. Finally, in Section 1.3, we recall the statement of Sato-Tate distribution theorem. In Chapter 2, we review a theorem of James and Yu on a variant of the Sato-Tate theorem upon averaging over suitable families of elliptic curves. We also review key ideas from their proof, most notably the use of the circle method.

1.1 Original contributions

In Chapter 3, we make an effort to derive a "smooth" analogue of the main theorem of James and Yu. We describe the technical difficulties encountered in the process and formulate a conjecture that could lead to the goal of deriving the smooth analogue. In Chapter

4, we compute the expected distribution measure of $\{\tilde{a_E}(p^2),\, p \text{ prime }, p \to \infty\}$ upon averaging over a suitable family of elliptic curves. This is done using the techniques previously developed in [BP19].

1.2 Preliminaries

1.2.1 Projective Geometry Basics

We will review the fundamental definitions and theorems related to elliptic curves that are needed to state the project goals. Our primary reference for the background material is [JT94].

Suppose $\mathbb{F}$ is an arbitrary field. Consider the following set of n-tuples:

$$S_n \coloneqq \{(x_1,\, x_2,\, \ldots,\, x_n) : (x_1,\, x_2,\, \ldots,\, x_n) \neq (0,\, 0,\, \ldots,\, 0)\}.$$

Define a relation '$\sim$' on this set as follows:

$(x_1,\, x_2, \ldots\, x_n) \sim (y_1,\, y_2,\, \ldots\, y_n)$ if and only if $x_1 = ty_1,\, x_2 = ty_2, \ldots,\, x_n = ty_n$ *for* $t(\neq 0) \in \mathbb{F}$.

Then one can easily prove that '$\sim$' defines an equivalence relation on the set S_n. This allow us to make the following definition.

Definition 1.1. ***Projective Plane*** *The n-projective plane(denoted as $\mathbb{P}^n$) is defined as the set S_{n+1} modulo the relation '$\sim$' , i.e,*

$$\mathbb{P}^n \coloneqq S_{n+1}/\sim .$$

We will be mainly interested in the case where the field $\mathbb{F}$ is $\mathbb{F}_p$ or $\mathbb{Q}$.

Let us denote the 2-affine plane by $\mathbb{A}^2$, which consists of all 2-tuples with entries in $\mathbb{F}$. Then we can interpret the the projective plane $\mathbb{P}^2$ by unifying it with the set $\mathbb{A}^2 \cup \mathbb{P}^1$. A

precise one-to-one correspondence can be given as follows:

$$f : \mathbb{P}^2 \longrightarrow \mathbb{A}^2 \cup \mathbb{P}^1$$

such that

$$\begin{aligned} &[(a,\, b,\, c)] \longrightarrow \left(\frac{a}{c},\, \frac{b}{c}\right) \in \mathbb{A}^2 && (\textit{if } c \neq 0) \\ &[(a,\, b,\, c)] \longrightarrow [a,\, b] \in \mathbb{P}^1 && (\textit{if } c = 0). \end{aligned}$$

Both of these interpretations of the projective plane will be important for our purposes.

Definition 1.2. ***Homogeneous Polynomial***

A polynomial $F(X,\, Y,\, Z)$ with coefficients from the field $\mathbb{F}$ is called a homogeneous polynomial of degree d if it satisfies the following relation:

$$F(tX,\, tY,\, tZ) = t^d F(X,\, Y,\, Z).$$

Definition 1.3. ***Projective Curve***

A projective curve or algebraic curve C in the projective plane $\mathbb{P}^2$ is the set of solutions(over the underlying field $\mathbb{F}$) of the polynomial equation

$$C : F(X,\, Y,\, Z) = 0$$

where F is a non-constant homogeneous polynomial. Moreover, the degree of the algebraic curve is the degree of the homogeneous polynomial F.

Definition 1.4. *A point P of the affine curve $C : f(x,\, y) = 0$ is called a singular point if*

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

A point P is non singular if it is not singular.

Definition 1.5. ***Straight Line*** *A line in the projective plane is given by the homogeneous*

equation of the following form:

$$\alpha X + \beta Y + \gamma Z = 0$$

where $\alpha, \beta, \gamma \in \mathbb{F}$.

Observe that, if $(a,\, b,\, c)$ is a point on the projective curve such that c is non-zero, then we have

$$F(a,\, b,\, c) = 0 \implies c^d F\left(\frac{a}{c},\, \frac{b}{c},\, 1\right) = 0 \implies F\left(\frac{a}{c},\, \frac{b}{c},\, 1\right) = 0.$$

Thus, if we define a new polynomial(which is not homogeneous) by $f(x, y) \coloneqq F(x,\, y,\, 1)$, then all the solutions of the equation $f(x, y) = 0$ will give us the points of the projective curve that are on the affine plane. Therefore, the curve $C_0 : f(x,\, y) = 0$ is called the *affine part* of the projective curve C.

we will end this section by describing two very important Theorems regarding projective curves which will be useful later.

For two projective curves C_1 and C_2 over the field $\mathbb{F}$, for each point $P \in \mathbb{P}^2$, we will formally define *multiplicity or intersection index*, denoted by $I(C_1 \cap C_2,\, P)$.

Let $f_1(x,\, y) = 0$ and $f_2(x,\, y) = 0$ denote the affine parts of the curve C_1 and C_2. Let us assume that the polynomials f_1 and f_2 do not have any common components and the line at infinity is not a component of either of the curve. Let $k = \bar{\mathbb{F}}$ denote the algebraic closure of $\mathbb{F}$.

Let $R = k[x,\, y]$ denote the polynomial ring in two variables and $(f_1,\, f_2)$ denote the ideal in R generated by f_1 and f_2. Let K be the fraction field of R, i.e, K is the field of rational functions in the variables $x,\, y$. If P is the point $(a,\, b)$ in the $X - Y$ plane then for a rational function $\phi \coloneqq \frac{f(x,\, y)}{g(x,\, y)} \in K$, we say that ϕ is defined at P if $g(a,\, b) \neq 0$. For a given point P we define the *local ring of* P to be the set of all $\phi \in K$ which are defined at P. We denote this ring by $\mathcal{O}_P$.

Now let $(f_1,\, f_2)_P$ denote the ideal generated by f_1 and f_2 in $\mathcal{O}_P$. Then the intersection index of C_1 and C_2 at the point P is defined as

$$I(C_1 \cup C_2,\, P) \coloneqq \dim\left(\frac{\mathcal{O}_P}{(f_1,\, f_2)_P}\right)$$

Observe that this definition does not account for the points P which are not in the affine plane. Our next goal is to define the *intersection index* for every point in $\mathbb{P}^2$.

As previous let $F_1(X,\, Y,\, ,Z)$ and $F_2(X,\, Y,\, Z)$ denote the homogeneous polynomial over $\mathbb{F}$ that represents the curves C_1 and C_2 respectively. We will define the ring K in this case as follows:

$$K \coloneqq \{\Phi = \frac{F(X,\, Y,\, Z)}{G(X,\, Y,\, X)} : F \text{ and } G \text{ are homogeneous polynomials of same degree over the field } k\}.$$

If $P = [A,\, B,\, C]$ is a point in $\mathbb{P}^2$ then we say that $\Phi = \frac{F(X,Y,Z)}{G(X,Y,X)} \in K$ is defined at P if $G(A,\, B,\, C) \neq 0$. In this case $\mathcal{O}_P$ will be defined as

$$\mathcal{O}_p \coloneqq \{\Phi \in K : \Phi \text{ is defined at } P\}.$$

Let us define:

$$(F_1,\, F_2)_P \coloneqq \left\{\frac{F}{G} \in \mathcal{O}_P : F \text{ is of the form } F = H_1F_1 + H_2F_2\right\}.$$

Finally, for any arbitrary $P \in \mathbb{P}^2$ we define the intersection index to be

$$I(C_1 \cup C_2,\, P) \coloneqq \dim \frac{\mathcal{O}_P}{(F_1,\, F_2)_P}.$$

The following properties of intersection index will be important to our case:

- If $P \notin C_1 \cap C_2$ then , $I(C_1 \cap C_2,\, P) = 0$.
- If $P \in C_1 \cap C_2$ and P is a non-singular point with C_1 and C_2 having different tangent directions at P, then $I(C_1 \cap C_2,\, P) = 1$.
- If C_1 and C_2 have same tangent directions at P then $I(C_1 \cap C_2,\, P) > 1$.

We are now in shape to state two very well-known results which will be important later on.

Theorem 1.6. ***Bezout's Theorem***

Let C_1 and C_2 be projective curves with no common components, then

$$\sum_{P \in\ C_1 \cap \mathbb{C}_2} I(C_1 \cap C_2,\, P) = (deg\, C_1)(deg\, C_2).$$

Theorem 1.7. ***Cayley - Bacharach Theorem***

If C_1 and C_2 are projective curves with no common components of respective degrees d_1 and d_2 and suppose that C_1 and C_2 intersect at $d_1 d_2$ distinct points. Let D be a curve in $\mathbb{P}^2$ of degree $d_1 + d_2 - 3$. If D passes through all but one points of $C_1 \cap C_2$ then D must pass through the remaining point also.

1.2.2 Elliptic Curves

One can prove that the affine part of a smooth projective curve of degree 3 can be reduced to the following form which is known as *Weierstrass Normal Form*

$$y^2 = f(x) = x^3 + bx + c.$$

Definition 1.8. ***Elliptic Curves***

An elliptic curve E over the field F with characteristic different from 2 is a nonsingular projective curve given by the equation

$$F(X,\, Y,\, Z) = Y^2 Z - (X^3 + aX^2 Z + bXZ^2 + cZ^3) = 0$$

where $a,\, b,\, c \in \mathbb{F}$.

Definition 1.9. *Let $E : y^2 = f(x)$ denote the affine part of an elliptic curve over the field $\mathbb{F}$. Then, the set of $\mathbb{F}$-rational points on E is the set*

$$E(\mathbb{F}) \coloneqq \{(x,\, y) : (x,\, y) \in \mathbb{F} \times \mathbb{F},\, y^2 = f(x)\}$$

If the underlying field is $\mathbb{Q}$, then the set $E(\mathbb{Q})$ will be called the set of $\mathbb{Q}$-rational points and an element of this set will be called a rational point of E.

1.2.3 The Mordell - Weil Group

For any arbitrary field $\mathbb{F}$ and an elliptic curve E over $\mathbb{F}$, let us consider the set $E(\mathbb{F})$ in greater detail. First of all, note that there is no guarantee that this set is non-empty. However, we will consider the elliptic curves for which this set is known to be non-empty. We wish to impose a group structure on this set. Since we have assumed this set to be non-empty, let $\mathcal{O}$ be a fixed element of this set. We define a binary operation $*$ on this set as follows:

- **Case 1** Suppose P and Q are two distinct points of the set $E(\mathbb{F})$. Then, by Bezout's Theorem the line joining the points P and Q has a third intersection point with the elliptic curve E. Note that, this third point can as well be any of the points P, Q or $\mathcal{O}$. We define $P * Q$ to be this point.

- **Case 2** Suppose P is any point on the elliptic curve E. Construct the tangent line to the elliptic curve at the point P in the projective plane. Again, by Bezout's Theorem this line will have a third point of intersection with the elliptic curve(can be the point P itself). Define this point to be $P * P$.

Now, define a binary operation '+' on the set $E(\mathbb{F})$ as follows:

If P and Q are any two points of the set $E(\mathbb{F})$, then $P + Q$ is defined to be the third point of intersection of the elliptic curve and the line joining $P * Q$ and $\mathcal{O}$.

One can prove that the set $E(\mathbb{F})$ with the binary operation '+' forms a commutative group with $\mathcal{O}$ being the identity element. This group is known as the ***Mordell - Weil group.***

1.2.4 The group $E(\mathbb{Q})$

We consider an elliptic curve E over $\mathbb{Q}$ in its Weierstrass normal form, i.e

$$E(a,\, b) : y^2 = f(x) = x^3 + ax + b,\ \textit{where } a,\, b \in \mathbb{Q}.$$

Note that if $(x_1,\, y_1)$ is a point of $E(\mathbb{Q})$, then so is $(x_1,\, -y_1)$.

For the constructon of the group $E(\mathbb{Q})$, we will take the point $[(0,\, 1,\, 0)]$ in the projective plane to be the point $\mathcal{O}$. Observe that if $[(x_1,\, x_2,\, 1)]$ is a point on the projective plane, then the affine part of the line joining these two points has the form:

$$x = x_1.$$

Therefore, the affine part of the line joining a point $[(x_1,\, y_1,\, 1)]$ with $\mathcal{O}$ is just the line parallel to Y-axis through the point $(x_1,\, y_1)$. Hence, from our definition of $P + Q$ and these observations, we can conclude that $P + Q$ is the reflection of $P * Q$ w.r.t $X-$ axis. If P is the point $(x_1,\, y_1)$ then $P * \mathcal{O}$ is the point $(x_1,\, -y_1)$ and clearly $-P = P * \mathcal{O}$. Moreover, if $P + Q + R = \mathcal{O}$ then P, Q and R are collinear.

Now, let us find a precise formula for this group operation.

Let $P = (x_1,\, y_1)$ and $Q = (x_2,\, y_2)$ are any two points on the elliptic curve E (not necessarily distinct). We denote the point $P + Q = R = (x_3,\, y_3)$. Let

$$y = \lambda x + \nu$$

denote the affine part of the line joining P and Q or the tangent at P if the points are same. Then, we have the following identity:

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3).$$

Equating the coefficient of x^2 on both side of this equation, we obtain

$$\lambda^2 = x_1 + x_2 + x_3 \implies x_3 = \lambda^2 - x_1 - x_2.$$

Equating the constant term of the identity we obtain:

$$\nu^2 = b + x_1x_2x_3.$$

If P and Q are distinct, then clearly $\lambda = \frac{y_2-y_1}{x_2-x_1}$. Therefore, in this case we have the following formula:

$$x_3 = \frac{(x_1+x_2)(a+x_1x_2)+2(b-y_1y_2)}{(x_2-x_1)^2}. \tag{1.1}$$

And if $P = Q$, then $\lambda = \frac{3x_1^2+a}{2y_1}$. In this case, we have

$$x_3 = \frac{x_1^4 - 2ax_1^2 - 8bx_1 + b^2}{4(x_1^3+ax_1+b)}. \tag{1.2}$$

One can use $y = \lambda x + \nu$ to obtain a similar formula for y_3.

Now, we will focus our attention on the size of the group $E(\mathbb{F})$. Observe that, the group $E(\mathbb{Q})$ need not be finite. However, one can prove that it is possible to obtain a finite number of points such that they generate the group $E(\mathbb{Q})$.

To precisely state and prove this result, we will introduce the concept of *'height of a rational number'.*

Definition 1.10. *The height of a rational number $\frac{m}{n}$ in the lowest form is given by*

$$H\left(\frac{m}{n}\right) \coloneqq \max\{|m|, |n|\}.$$

Definition 1.11. *Suppose, $P = (x, y) \in E(\mathbb{Q})$. The height of the point P is defined to be the height of its $X-$coordinate, i.e,*

$$H(P) = H(x).$$

We also define

$$h(P) \coloneqq \log H(P).$$

The following two lemmas regarding the height function will be instrumental to our proof.

Lemma 1.12. *Suppose $\mathbb{Q}_0 \in E(\mathbb{Q})$. Then, there is a constant κ_0 such that*

$$h(P + Q_0) \leq 2h(P) + \kappa_0.$$

Lemma 1.13. *There exists a constant κ such that*

$$h(2P) \geq 4h(P) - \kappa.$$

We will also require the following very interesting fact:

Theorem. *The group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

With these results, we can prove the following very important theorem:

Theorem 1.14. ***Mordell-Weil Theorem***

The group $E(\mathbb{Q})$ is finitely generated.

Proof. Let $\{Q_1, Q_2, \ldots\ldots, Q_n\}$ denotes the set of left coset representative of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$. If P is an element of $E(\mathbb{Q})$, then there exist Q_i and P_1 such that $P = Q_i + 2P_1$. Again, there exist Q_j and P_2 such that $P_1 = Q_j + 2P_2$. Continuing this process and renumbering $Q_i's$, we obtain the following equation:

$$P = Q_1 + 2Q_2 + ... + 2^{(n-2)}(Q_n + 2P_n).$$

Therefore, it will be sufficient to prove that for an arbitrary $P \in E(\mathbb{Q})$, the set of such possible P_n's will always be finite.

By Lemma 1.12 we have

$$h(2P_i) = h(P_{i-1} - Q_i) \leq 2h(P_{i-1}) + \kappa_i.$$

Also using Lemma 1.13 we obtain

$$h(2P_i) \geq 4h(P_i) - \kappa.$$

Therefore, combining the above two equations

$$4h(P_i) \leq 2h(P_{i-1}) + C,$$

with $C := \max_i \kappa_i + \kappa$. Thus,

$$\begin{aligned} h(P_i) \leq & \frac{1}{2}h(P_{i-1}) + \frac{C}{4} \\ & = \frac{3}{4}h(P_{i-1}) - \frac{1}{4}(h(P_{i-1} - C) \end{aligned}$$

If $h(P_{i-1}) \geq C$ then $h(P_i) \leq \frac{3}{4}h(P_{i-1})$. Hence, there must be an m such that $h(P_m) \leq C$. Now, clearly the set $\{P \in E(\mathbb{Q}) : h(P) \leq C\}$ is finite. Therefore, number of such P_n must be finite. This completes the proof.

□

1.2.5 The group $E(\mathbb{F}_p)$

Let p denote a prime number. Given an elliptic curve E over the field $\mathbb{F}_p$, again we are interested in the size of the Mordell-Weil group $E(\mathbb{F}_p)$. Observe that since $\mathbb{F}_p$ is a finite field, the group $E(\mathbb{F}_p)$ must be finite. Let us make the following definitions about primes.

Definition 1.15. *Let $E : y^2 = f(x) = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$, with integer coefficients and p be a prime. If we reduce the affine curve modulo p and the polynomial $\tilde{f(x)}$ has distinct roots over $\mathbb{F}_p$ we say that E has a good reduction at p. Otherwise, we say that E has a bad reduction at p.*

Observe that E has a good reduction at p is equivalent to saying that the discriminant Δ of $f(x)$ is not divisible by p.

Instead of directly dealing with the order of the group $E(\mathbb{F}_p)$ we will consider the following quantity:

$$a_E(p) := p + 1 - |E(\mathbb{F}_p)|.$$

Definition 1.16. ***Frobenius morphism***

Suppose K is a field of characteristic p and let $q = p^r$. If E/K is an elliptic curve given by the Weierstrass normal form. Then define a new curve $E^{(q)}/K$ by raising the coefficients of the equation representing E to the q-th power. Then the Frobenius morphism $\phi_q : E \longrightarrow E^{(q)}$ is given by

$$(x,\, y) \longrightarrow (x^q,\, y^q).$$

Definition 1.17. *If p is a prime and $q = p^r$, we denote the trace of the Frobenius endomorphism on $E(\mathbb{F}_q)$ by $a_E(q)$. Moreover we define*

$$\tilde{a_E}(p^r) \coloneqq \frac{a_E(p^r)}{p^{\frac{r}{2}}}.$$

In 1936, Hasse proved a bound for the quantity $a_E(p)$ in the series of papers [Has36a], [Has36b] and [Has36c].

Theorem 1.18. *If C is a non-singular irreducible elliptic curve of genus g over the field $\mathbb{F}_p$, then the number of points on C with coordinates in $\mathbb{F}_p$ is $p + 1 + \epsilon$ where the error term ϵ satisfies*

$$\epsilon \leq 2g\sqrt{p}.$$

By virtue of this Theorem one can define

$$\tilde{a_E}(p) \coloneqq \frac{a_E(p)}{2\sqrt{p}} = \cos \pi\, \theta_E(p), \;\; \theta_E(p) \in [0, 1]. \tag{1.3}$$

1.3 The Sato-Tate Conjecture

It is of great interest to ask how the quantity $\theta_E(p)$ behaves as we vary the prime p. With the experimental support of Sato, Tate provided theoretical evidence ([Tat65]) of the distribution of $a_E(p)/2\sqrt{p}$ in the interval $[-1,\, 1]$ which is known as Sato-Tate conjecture. Equivalently, it predicts the distribution of the cosine angles $\theta_E(p)$ in $[0,\, 1]$ as the primes $p \to \infty$. The Sato-Tate conjecture is now a proved Theorem by the work of Clozel, Harris, Shepherd-Barron and Taylor([CHT08], [HSBT10], [Tay08]). Before stating it we first need to make the following definition:

Definition 1.19. *Let C be an elliptic curve. We say that C has a complex multiplication if there is an endomorphism $\phi : C \longrightarrow C$ which is not a multiplication by n map.*

Suppose $E = E(a, b)$ is an elliptic curve given by the equation

$$y^2 = x^3 + ax + b,\ a, b \in \mathbb{Z}$$

such that E does not admit complex multiplication. For any $0 \leq \alpha \leq \beta \leq 1$ and $X > 1$, define

$$\pi_E^{(\alpha,\beta)}(X) := \#\left\{p \leq X :\ \alpha \leq \theta_E(p) \leq \beta\right\}.$$

Let $\pi(X)$ denote the number of primes less than or equal to X. Moreover, define $\tilde{\pi}(X) \coloneqq \pi(X) - \pi(\frac{X}{2})$.

The Sato-Tate distribution Theorem states that for any α, β as above,

$$\lim_{X\to\infty} \frac{\pi_E^{(\alpha,\beta)}(X)}{\pi(X)} = \int_\alpha^\beta 2\sin^2 \pi t\, dt.$$

This distribution theorem is counted among the deepest results in arithmetic geometry. However, before this theorem was proved, some interesting statistical questions were asked about the distribution of the cosine angles $\theta_E(p)$ and $a_E(p)$ even as one varies E over suitable families of elliptic curves. At the heart of these investigations is a fundamental result of Birch [Bir68] which evaluates the average moments of higher powers $(a_E(p))^k$ as one varies E over certain families of elliptic curves.

In 2006, James and Yu [JY06] turned around the above perspective and asked the following question: what can we say about the distribution of $\theta_E(p)$ in $[0, 1]$ if we only consider those primes p for which $a_E(p)$ itself is a k-th power (for a fixed positive power k)?

Let $k \in \mathbb{N}$. We consider the set $K = \{m^k :\ m \in \mathbb{N}\}$. For $0 \leq \alpha \leq \beta \leq 1$ and $X > 1$, let

$$\pi_E(\alpha, \beta, K; X) := \#\left\{p \leq X :\ \alpha \leq \theta_E(p) \leq \beta,\ a_E(p) \in K\right\}.$$

We average the above quantity over suitable families of elliptic curves. More precisely, for positive real numbers U, V, A, B, X, let

$$S_{\alpha,\beta}(U, V, A, B; K; X) = \frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} \pi_E(\alpha, \beta, K; X).$$

James and Yu [JY06] proved the following asymptotic for $S_{\alpha,\beta}(U,V,A,B;K;X)$.

Theorem 1.20. *Let $0 < \alpha < \beta < 1$ be fixed and let U, V be any real numbers. For X sufficiently large, if A, $B > X \log X$, then we have*

$$S_{\alpha,\beta}(U,V,A,B;K;X) \sim c_k(\alpha,\beta)\pi_k(X),$$

where

$$\pi_k(X) = \int_2^X \frac{t^{\frac{1}{2k}-\frac{1}{2}}}{\log t} dt$$

and

$$c_k(\alpha,\beta) = \left(\frac{1}{3} + \frac{2}{3}\delta(k)\right) \frac{2^{1/k}}{k} \int_\alpha^\beta |\cos \pi t|^{\frac{1}{k}-1} \sin^2 \pi t \, dt.$$

Here, $\delta(k) = 1$ if $k = 1$ and 0 if $k > 1$.

James and Yu also investigate the order of the error term in the asymptotic described in Theorem 1. They proved the following Theorem:

Theorem 1.21. *Let $0 < \alpha < \beta < 1$ be fixed and let U, V be any real numbers . Suppose that A, B and X are sufficiently large real numbers and that A, $B > (X \log X)^2$. Then, we have*

$$\frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} |\pi_E(\alpha,\beta,K;X) - c_k(\alpha,\beta)\pi_k(X)|^2 = \mathrm{o}((\pi_k(X))^2).$$

One of the key innovations in [JY06] was the use of the circle method in the proof of the above Theorems. The aim of this project is to understand the proof of the above theorems by James-Yu. An even stronger question is to investigate if one can find a function $F(X)$ such that

$$\frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} |\pi_E(\alpha,K;X) - c_k(\alpha)\pi_k(X)|^2 \sim \frac{(\pi_k(X))^2}{F(X)}.$$

In this thesis we introduce a methodology that can be used to derive a smooth analogue of Theorem 1.20. Although a complete answer to the question of a smooth analogue is still work in progress, we indicate the key arguments in our efforts to do so. We also make a conjecture and describe the current technical difficulties in proving it.

Another problem that will be discussed in this thesis is : what is the distribution of $\tilde{a_E}(p^2)$ as we vary over the primes? Specifically, if we average over a suitable family of elliptic curves ,say $\mathfrak{G}_{A,B}$, how does the following quantity behave, as $X \to \infty$

$$\frac{1}{\tilde{\pi}(X)} \frac{1}{|\mathfrak{G}_{A,B}|} \sum_{E \in \mathfrak{G}_{A,B}} \sum_{\frac{X}{2} < p \leq X} (\tilde{a_E}(p^2))^m, \quad m \geq 1?$$

For this problem we will be using the methodology described in [BP19] to obtain a precise closed-form formula for the distribution function.

Chapter 2

Problem of Representation

The goal of this chapter is to briefly review the use of circle method towards an additive problem that plays a key role in the proof of Theorem 1.20. In Section 2.1, we mention fundamental theorems in number theory which are needed for the application of the circle method to various additive problems. In the remaining sections, we review the proof of Theorem 1.20 by applying these techniques to the additive problem of our interest.

2.1 Additive number theory techniques

The primary reference for this section is [Nat13].

Theorem 2.1. ***Abel's Partial Summation***

Let $\mathbb{N}$ *and* $\mathbb{C}$ *denote the set of natural numbers and the set of complex numbers respectively. Let* $u : \mathbb{N} \longrightarrow \mathbb{C}$ *and let* f *be a continuous function which has a continuous derivative in the interval* $[1, x]$*. Also, let*

$$U(t) := \sum_{1 \leq n \leq x} u(n).$$

Then,

$$\sum_{1 \leq n \leq x} u(n) f(n) = U(x) f(x) - \int_1^x U(t) f'(t) dt \tag{2.1}$$

Another important Theorem that will be central to our discussion is the Siegel-Walfisz

theorem on the distribution of primes in arithmetic progressions.

Theorem 2.2. ***[Siegel-Walfisz Theorem]***

Let q and a be integers such that $q \geq 1$ and $(q, a) = 1$. For any $C > 0$,

$$v(x;\, q,\, a) \coloneqq \sum_{\substack{p \leq x \\ p \equiv a (\mathrm{mod}\ q)}} \log p = \frac{x}{\varphi(q)} + \mathrm{O}\left(\frac{x}{(\log(x))^C}\right) \tag{2.2}$$

where $\varphi(q)$ denotes the Euler's-phi function.

The following theorem of Vinogradov is useful to study exponential sums of the form

$$\sum_{p \leq N} \log p\, e(p\alpha).$$

Theorem 2.3. ***[Vinogradov's Inequality]*** *Suppose α is an irrational number satisfying*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2},$$

for some rational a/q where $1 \leq q \leq N$ and $(a, q) = 1$. Then,

$$\sum_{p \leq N} (\log p)\, e\,(p\alpha) \ll \left(\frac{N}{\sqrt{q}} + N^{4/5} + N^{1/2} q^{1/2}\right) (\log N)^4.$$

The following theorem is vital to investigate exponential sums of the form $\sum_{n \leq N} e(n^2\alpha)$.

Theorem 2.4. ***[Weyl's Inequality]***

Suppose α is an irrational number satisfying

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2},$$

for some rational a/q where $1 \leq q \leq N$ and $(a, q) = 1$. Let $f(x) = \alpha x^k + \ldots$ be a polynomial

of degree $k \geq 2$. Let $K = 2^{k-1}$ and $\epsilon > 0$. Then

$$\left|\sum_{n=1}^{N} e(f(n))\right| \ll N^{1+\epsilon}\left(\frac{1}{N} + \frac{1}{q} + \frac{q}{N^k}\right)^{\frac{1}{K}}.$$

2.2 Problem of Representation

The goal of this section is to study the application of the circle method to the following problem: Let $n \equiv 0,\ 1 (\mathrm{mod}\, 4)$, $n < 0$. Estimate

$$R(n) = \sum_{\substack{p \leq X \\ r \leq (2\alpha\sqrt{p})^{\frac{1}{k}} \\ r^{2k} - 4p = n}} \log p.$$

This estimation plays a vital role in proving Theorem 1.20. We closely follow Section 2 of [JY06]. We divide the study of $R(n)$ in two cases.

Case 1. $-n \leq \frac{X}{(\log X)^{2^{k+2}}}$

Note that $r^{2k} = n + 4p$. Thus, $4p + n \geq 0$ and $p \geq -\frac{n}{4}$. Therefore,

$$r \leq (2\alpha\sqrt{p})^{\frac{1}{k}} \ll (-n)^{\frac{1}{k}}.$$

Now, observe that for a fixed n, once r is chosen, p is automatically determined. Thus,

$$\begin{aligned} R(n) &\ll (\log X)\#\{(r,\, p) : r^{2k} - 4p = n\} \\ &\ll (\log X)\#\{r \ll (-n)^{\frac{1}{2k}}\} \\ &\ll (\log X)(-n)^{\frac{1}{2k}} \end{aligned}$$

Since we have assumed $-n \leq \frac{X}{(\log X)^{2^{k+2}}}$, we have

$$\begin{aligned} R(n) &\ll (\log X)\left(\frac{X}{(\log X)^{2^{k+2}}}\right)^{\frac{1}{2k}} \\ &\ll \frac{X^{\frac{1}{2k}}}{(\log X)^{\frac{2^{k+2}}{2k}}} \log X \end{aligned}$$

$$\ll X^{\frac{1}{2k}} \frac{\log X}{(\log X)^4} \qquad \text{(since } \frac{2^{k+1}}{k} \geq 4 \text{ for } k > 1\text{)}$$
$$\ll X^{\frac{1}{2k}} (\log X)^{-3}$$

This completes Case 1.

Case 2. $\frac{X}{(\log X)^{2^{k+2}}} < -n \leq 4X$

With this assumption we have the following range for p.

$$\frac{X}{(4\log X)^{2^{k+2}}} < p \leq X.$$

We partition the range of p into smaller intervals as follows:

We consider

$$\bigcup_{l=0}^{L} \left(\frac{X}{g^{l+1}}, \frac{X}{g^l} \right],$$

where $g = A \log X$ and $L = 2^{k+2} - 1$ with A being a constant such that $\frac{X}{g^{L+1}} = \frac{X}{(4\log X)^{2^{k+2}}}$.

We write

$$R(n) = \sum_{l=0}^{L} R_l(n),$$

where

$$R_l(n) = \sum_{\substack{\frac{X}{g^{l+1}} < p \leq \frac{X}{g^L} \\ r \leq \left(2\alpha\sqrt{p}\right)^{\frac{1}{k}} \\ r^{2k} - 4p = n}} \log p.$$

Let us denote

$$R_l^*(n) = \sum_{\substack{\frac{X}{g^{l+1}} < p \leq \frac{X}{g^L} \\ r \leq \left(2\alpha\sqrt{\frac{X}{g^l}}\right)^{\frac{1}{k}} \\ r^{2k} - 4p = n}} \log p.$$

We note that

$$0 \le R_l^*(n) - R_l(n) = \sum_{\substack{\frac{X}{g^{l+1}} < p \le \frac{X}{g^l} \\ (2\alpha\sqrt{p})^{\frac{1}{k}} < r \le \left(2\alpha\sqrt{\frac{X}{g^l}}\right)^{\frac{1}{k}} \\ r^{2k} - 4p = n}} \log p.$$

Thus, we have

$$R_l^*(n) - R_l(n) \ll \log X \# \left\{ \left(2\alpha\sqrt{\frac{X}{g^{l+1}}}\right)^{\frac{1}{k}} \le r \le \left(2\alpha\sqrt{\frac{X}{g^l}}\right)^{\frac{1}{k}} \right\} \ll \left(\frac{X}{g^l}\right)^{\frac{1}{2k}} \log X.$$

Thus,

$$\begin{aligned}
R(n) &= \sum_{l=0}^{L} R_l(n) \\
&= \sum_{l=0}^{L} (R_l^*(n) + R_l(n) - R_l^*(n)) \\
&= \sum_{l=0}^{L} R_l^*(n) + \sum_{l=0}^{L} (R_l(n) - R_l^*(n)) \\
&= \sum_{l=0}^{L} R_l^*(n) + \mathrm{O}\left(\sum_{l=0}^{L} \left(\frac{X}{g^l}\right)^{\frac{1}{2k}} \log X\right) \\
&= \sum_{l=0}^{L} R_l^*(n) + \mathrm{O}\left(LX^{\frac{1}{2k}} \log X\right) \\
&= \sum_{l=0}^{L} R_l^*(n) + \mathrm{O}_k\left(X^{\frac{1}{2k}} \log X\right) \qquad \text{(since } \ L = 2^{k+2} - 1)
\end{aligned}$$

The advantage of $R_l^*(n)$ over $R_l(n)$ is that the range of r does not depend on p. We now convert $R_l^*(n)$ into an integral over a suitable exponential sum. For $\beta \in \mathbb{R}$, we define the sums

$$s_l(\beta) = \sum_{\frac{X}{g^{l+1}} < p \le \frac{X}{g^l}} e(p\beta) \log p$$

and

$$t_l(\beta) = \sum_{r \le \left(2\alpha\sqrt{\frac{X}{g^l}}\right)^{\frac{1}{k}}} e(r^{2k}\beta).$$

We observe that

$$R_l^*(n) = \int_0^1 t_l(\beta) s_l(-4\beta) e(-n\beta) d\beta. \tag{2.3}$$

2.2.1 Major and minor arcs

We will apply the Ramanujan-Hardy-Littlewood circle method to evaluate the above integral. To invoke the circle method we first define the major and minor arcs. We choose $P = (\log X)^{2^{2k+3}}$.

Define for $1 \le q \le P$ and $0 \le a \le q$ with $(a, q) = 1$

$$\mathfrak{M}(q, a) := \{\beta \in [0,\, 1] :|\, \beta - \frac{a}{q} \,| \le \frac{P}{X}\}.$$

Then the major arc is defined as

$$\mathfrak{M} := \bigcup_{1 \le q \le P} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} \mathfrak{M}(q, a)$$

and the minor arc is defined as

$$\mathrm{m} := [0, 1] - \mathfrak{M}.$$

Observe that $\mathfrak{M}(a,\, q)$'s are disjoint for sufficiently large values of X. Also note that the length of the intervals $\mathfrak{M}(0,\, 0)$ and $\mathfrak{M}(1,\, 1)$ are half of the other intervals.

Now,

$$\begin{aligned} R_l^*(n) &= \int_0^1 t_l(\beta) s_l(-4\beta) e(-n\beta) d\beta \\ &= \int_{\mathfrak{M}} t_l(\beta) s_l(-4\beta) e(-n\beta) d\beta + \int_{\mathrm{m}} t_l(\beta) s_l(-4\beta) e(-n\beta) d\beta. \end{aligned} \tag{2.4}$$

We denote

$$E_l(n) = \int_{\mathrm{m}} t_l(\beta) s_l(-4\beta) e(-n\beta) d\beta.$$

Using some of the classical estimates of Vinogradov and Weyl for $s_l(\beta)$ and $t_l(\beta)$ respectively, namely Theorems 2.3 and 2.4, one can derive the bound

$$\sum_{-n \le 4X} |E_l(n)|^2 \ll \frac{X^{1+\frac{1}{k}}}{(\log X)^{33}} \tag{2.5}$$

2.2.2 Integral over Major Arcs

To evaluate the integral over major arcs

$$\int_{\mathfrak{M}} t_l(\beta) s_l(-4\beta) e(-n\beta) d\beta,$$

we first take $\beta = \frac{a}{q}$ and observe that

$$\begin{aligned} s_l\left(\frac{-4a}{q}\right) &= \sum_{r=1}^{q} \sum_{\substack{\frac{X}{g^{l+1}} < p \le \frac{X}{g^l} \\ p \equiv r (\mathrm{mod}\, q)}} \log p \, e\left(\frac{-4ar}{q}\right) \\ &= \sum_{\substack{1 \le r \le q \\ (r,q)=1}} e\left(\frac{-4ar}{q}\right) \sum_{\substack{\frac{X}{g^{l+1}} < p \le \frac{X}{g^l} \\ p \equiv r (\mathrm{mod}\, q)}} \log p + \mathrm{O}(\log q) \end{aligned} \tag{2.6}$$

By Theorem 2.2, we have, for any $C > 0$,

$$\sum_{\substack{\frac{X}{g^{l+1}} < p \le \frac{X}{g^l} \\ p \equiv r (\mathrm{mod}\, q)}} \log p = \frac{1}{\phi(q)} \left(\frac{X}{g^{l+1}} - \frac{X}{g^l}\right) + \mathrm{O}_C\left(\frac{X}{(\log X)^C}\right).$$

We also recall the Ramanujan sum

$$\sum_{r=1}^{q} e\left(\frac{-4ra}{q}\right) = \phi(q) \frac{\mu\left(\frac{q}{(q,4a)}\right)}{\phi\left(\frac{q}{(q,4a)}\right)}.$$

Since $(a,\, q) = 1$, the above expression equals

$$\phi(q)\frac{\mu\left(\frac{q}{(q,4)}\right)}{\phi\left(\frac{q}{(q,4)}\right)}.$$

Thus,

$$s_l\left(\frac{-4a}{q}\right) = \phi(q)\frac{\mu\left(\frac{q}{(q,4)}\right)}{\phi\left(\frac{q}{(q,4)}\right)}\frac{1}{\phi(q)}\left(\frac{X}{g^{l+1}} - \frac{X}{g^l}\right) + \mathrm{O}_C\left(\frac{qX}{(\log X)^C}\right). \tag{2.7}$$

For $\beta \in \mathfrak{M}(q,\, a)$ we denote $\gamma = \beta - \frac{a}{q}$. By an application of partial summation and using equation (2.7), for all $\beta \in \mathfrak{M}(q,\, a)$ we obtain

$$s_l(-4\beta) = \frac{\mu\left(\frac{q}{(q,4)}\right)}{\phi\left(\frac{q}{(q,4)}\right)}u_l\left(-4\gamma\right) + \mathrm{O}\left(\frac{P^2X}{(\log X)^C}\right) \quad (\text{for any } C > 0), \tag{2.8}$$

where $u_l(\gamma) = \sum_{\frac{X}{g^{l+1}} < m \leq \frac{X}{g^l}} e(m\gamma)$. Similarly, the major arc calculations for $t_l(\beta)$ show that

$$t_l(\beta) = \frac{S_{2k}(q,\, a)}{q}v_l\left(\beta - \frac{a}{q}\right) + \mathrm{O}(P^{\frac{2}{3}}), \tag{2.9}$$

where

$$v_l(\gamma) = \sum_{s \leq 4\alpha^2\frac{X}{g^l}} \frac{1}{2k}s^{\frac{1}{2k}-1}e(s\gamma),$$

and

$$S_{2k}(q,\, a) = \sum_{m=1}^{q} e\left(m^{2k}\frac{a}{q}\right).$$

Combining equations (2.8) and (2.9) into the integral for $R_l^*(n)$ over the major arcs, we get

$$\begin{aligned}
&\int_{\mathfrak{M}} t_l(\beta)s_l(-4\beta)e(-n\beta)d\beta \\
&= \sum_{q \leq P} \frac{\mu\left(\frac{q}{(q,4)}\right)}{q\phi\left(\frac{q}{(q,4)}\right)} \sum_{\substack{a=1 \\ (a,\,q)=1}}^{q} S_{2k}(q,\, a)e\left(\frac{-an}{q}\right) \\
&+ \int_{-\frac{1}{2}}^{\frac{1}{2}} u_l(-4\gamma)v_l(\gamma)e(-n\gamma)d\gamma + \mathrm{O}\left(\frac{X^{\frac{1}{2k}}}{(\log X)^{D_0}}\right)
\end{aligned} \tag{2.10}$$

for any $D_0 > 0$. We denote

$$\mathfrak{G}(n,\, P) = \sum_{q \le P} F(q,\, n),$$

where

$$F(q,\, n) = \frac{\mu\left(\frac{q}{(q,4)}\right)}{q\phi\left(\frac{q}{(q,4)}\right)} \sum_{\substack{a=1 \\ (a,\,q)=1}}^{q} S_{2k}(q,\, a) e\left(\frac{-an}{q}\right).$$

This is known as the singular series. The singular integral is

$$J_l(n) = \int_{-\frac{1}{2}}^{\frac{1}{2}} u_l(-4\gamma) v_l(\gamma) e(-n\gamma) d\gamma.$$

The evaluation of the sum $\mathfrak{G}(n,\, p)$ and the integral $J_l(n)$ is a delicate calculation. Evaluating $J_l(n)$ for each $0 \le l \le L$, recalling equation (2.5) and combining Cases 1 and 2, we get

Theorem 2.5.

$$R(n) = \sum_{l=0}^{L} \int_0^1 s_l(-4\beta) t_l(\beta) e(-n\beta) d\beta = \mathfrak{G}(n,\, p) J(n) + \mathrm{O}\left(\frac{X^{\frac{1}{2k}}}{(\log X)^3}\right) + E(n),$$

where

$$J(n) = \sum_{\substack{m \le X \\ s \le 4\alpha^2 m \\ s - 4m = n}} \frac{1}{2k} s^{\frac{1}{2k} - 1}$$

and

$$E(n) = \sum_{l=0}^{L} E_l(n), \quad \sum_{-n \le 4X} |E_l(n)|^2 \ll \frac{X^{1+\frac{1}{k}}}{(\log X)^{33}}.$$

2.3 Remarks

In this section we will briefly discuss about the application of the estimate obtained in the previous section in the proof of Theorem 1.20.

Let χ_d denote the Dirichlet character. Define

$$L_0(d) = \sum_{n \leq X^{\frac{2}{3}}} \frac{\chi_d(n)}{n}$$

and

$$K_0(X) = \frac{1}{2\pi} \sum_{p \leq X} \sum_{r \leq (2\alpha\sqrt{p})^{\frac{1}{k}}} \sum_{\substack{r^{2k} - 4p = df^2 \\ f \leq (\log X)^2 \\ d \equiv 0,\, 1 (\mathrm{mod}\, 4)}} \sqrt{|\, d\,|} L_0(d).$$

The proof of Theorem 1.20 proceeds through following steps.

Theorem 2.6. *We have*

$$K_0(X) = \left(\frac{2k}{3k+1} c_k(\alpha) + \mathrm{O}(\log X)^{-2}) \right) X^{\frac{3}{2} + \frac{1}{2k}}.$$

Proof. Using Theorem 2.5, we write

$$K_0(X) = \frac{1}{2\pi} \sum_{\substack{f \leq (\log X)^2 \\ 0 < -df^2 \leq 4X \\ d \equiv 0,\, 1 (\mathrm{mod}\, 4)}} \sqrt{|\, d\,|} L_0(d) (\mathfrak{G}(df^2,\, P) J(df^2) + E(df^2) + \mathrm{O}\left(\frac{X^{\frac{1}{2k}}}{(\log X)^3} \right)$$

One can prove that

$$\sum_{f,\, d} \sqrt{|\, d\,|}\, |\, L_0(d) E(df^2)\, | \ll \frac{X^{\frac{3}{2} + \frac{1}{2k}}}{(\log X)^7}.$$

Therefore, we have

$$K_0(X) = \frac{1}{2\pi} \sum_{\substack{f \leq (\log X)^2 \\ 0 < -df^2 \leq 4X \\ d \equiv 0,\, 1 (\mathrm{mod}\, 4)}} \sqrt{|\, d\,|} L_0(d) \mathfrak{G}(df^2,\, P) J(df^2) + \mathrm{O}(X^{\frac{3}{2} + \frac{1}{2k}} (\log X)^{-2}).$$

Properly estimating the above sum completes the proof of the theorem. □

Using Deuring's theorem ([Bir68]) one can prove the following: For a fixed prime p and $r \in \mathbb{Z} \cap (-2\sqrt{p},\, 2\sqrt{p})$, the number of elliptic curves $E(a,\, b) : y^2 = x^3 + ax + b$ with $a,\, b \in \mathbb{F}_p$

and $a_E(p) = r$ (denoted by $N(p,\, r)$), is given by

$$N(p,\, r) = \frac{pH(r^2-4p)}{2} + \mathrm{O}(p),$$

where $H(r^2-4p)$ is the Kronecker class number defined as

$$H(r^2-4p) = 2 \sum_{\substack{r^2-4p=df^2 \\ d\equiv o,\, 1(\mathrm{mod}\, 4)}} \frac{h(d)}{w(d)}.$$

Here $w(d)$ and $h(d)$ denote the number of units and the class number of the order of discriminant d respectively.

Therefore, we obtain

$$\begin{aligned} S_\alpha(U,\, V,\, A,\, B,\, \mathcal{K};\, X) &= \frac{1}{AB} \sum_{p\le X} \sum_{\substack{0<r\le 2\alpha\sqrt{p} \\ r\in K}} \left(\frac{A}{p} + \mathrm{O}(1)\right)\left(\frac{B}{p} + \mathrm{O}(1)\right) N(p,r) \\ &= (1 + \mathrm{O}(\log X)^{-1}))M(X) + (\mathrm{O}(X^{\frac{1}{2k}})), \end{aligned} \tag{2.11}$$

where $M(X) = \frac{1}{2}\sum_{\substack{p\le X \\ 0<r\le 2\alpha\sqrt{p} \\ r\in K}} \frac{H(r^2-4p)}{p}$. The following theorem is the final piece in the proof of 1.20. We will sketch the outline of the proof.

Theorem 2.7. *For fixed $0 < \alpha < 1$, and sufficiently large X we have*

$$M(X) \sim c_k(\alpha)\pi_k(X).$$

Here,

$$\pi_k(X) = \int_2^X \frac{t^{\frac{1}{2k}-\frac{1}{2}}}{\log t} dt$$

and

$$c_k(\alpha) = \left(\frac{1}{3} + \frac{2}{3}\delta(k)\right) \frac{2^{1/k}}{k} \int_0^\alpha |\cos \pi t|^{\frac{1}{k}-1} \sin^2 \pi t \, dt.$$

Proof.

$$M(X) = \sum_{p\le X} \frac{1}{p} \sum_{0<r\le(2\alpha\sqrt{p})^{\frac{1}{k}}} \sum_{\substack{r^{2k}-4p=df^2 \\ d\equiv 0,\, 1(\mathrm{mod}\, 4)}} \frac{h(d)}{w(d)} \tag{2.12}$$

One can prove that for $f > (\log X)^2$ this sum contributes

$$\sum_{p\leq X}\frac{1}{p}\sum_{0<r\leq(2\alpha\sqrt{p})^{\frac{1}{k}}}\sum_{\substack{r^{2k}-4p=df^2\\ f>(\log X)^2\\ d\equiv 0,\,1(\mathrm{mod}\,4)}}\frac{h(d)}{w(d)}\ll\frac{X^{\frac{1}{2}+\frac{1}{2k}}}{(\log X)^3}$$

Therefore, we obtain

$$M(X)=\sum_{p\leq X}\frac{1}{p}\sum_{0<r\leq(2\alpha\sqrt{p})^{\frac{1}{k}}}\sum_{\substack{r^{2k}-4p=df^2\\ f\leq(\log X)^2\\ d\equiv 0,\,1(\mathrm{mod}\,4)}}\frac{h(d)}{w(d)}+\mathrm{O}\left(\frac{X^{\frac{1}{2}+\frac{1}{2k}}}{(\log X)^3}\right).$$

Using Polya-Vinogradov theorem one can prove that

$$M(X)=M_0(X)+\mathrm{O}\left(\frac{X^{\frac{1}{2}+\frac{1}{2k}}}{(\log X)^3}\right),$$

where

$$M_0(X)=\frac{1}{2\pi}\sum_{p\leq X}\frac{1}{p}\sum_{0<r\leq(2\alpha\sqrt{p})^{\frac{1}{k}}}\sum_{\substack{r^{2k}-4p=df^2\\ f\leq(\log X)^2\\ d\equiv 0,\,1(\mathrm{mod}\,4)}}\sqrt{|\,d\,|}L_0(d).$$

Using Theorem 2.6 and partial summation, we have

$$M_0(X)=c_k(\alpha)\pi_k(X)+\mathrm{O}\left(\frac{X^{\frac{1}{2}+\frac{1}{2k}}}{(\log X)^3}\right).$$

This completes the proof. □

Chapter 3

Smooth Analogue

In this chapter we will consider a smooth periodic test function ϕ. Instead of studying the sum $\sum_{p\leq X}\chi_I$ which contains the discrete characteristic function, we will study the sum $\sum_{p\leq X}\phi(\theta_E(p))$. The smooth function ϕ is constructed in a way that the Fourier series is finite. We aimed at obtaining an analogue of Theorem 1.20 using a general template from Fourier analysis that was developed in [BPS20]. In the end we will make a comment about how far we reached and further developments that can be made in this process.

First we will recall the following lemma (Lemma 2.1 [BPS20])

Lemma 3.1.

$$2\cos(2\pi n\,\theta_E(p)) = \frac{a_E(p^{2n})}{p^n} - \frac{a_E(p^{2n-2})}{p^{n-1}} \tag{3.1}$$

Let us make the following definition.

Definition 3.2. *For any set A of real numbers, we define the characteristic function $\chi_A : \mathbb{R} \longrightarrow \{0, 1\}$ as follows:*

$$\begin{aligned}\chi_A(x) &= 0 \quad (\textit{if } x \notin A)\\ &= 1 \quad (\textit{if } x \in A)\end{aligned}$$

Let us briefly review Fourier transform and its properties which are important for our purpose.

Definition 3.3. *For a function $f : \mathbb{R} \longrightarrow \mathbb{C}$ of Schwartz class, we define the Fourier transform of f (denoted by $\hat{f}$) as follows*

$$\hat{f}(\epsilon) = \int_{-\infty}^{+\infty} f(x)e(-x\epsilon)dx,$$

where $e(t) := e^{2\pi it}$.

It is interesting to ask how Fourier transform of a function behaves under scaling or shifting of the variable.

- **Shifting property** If $h(x) = f(x - x_0)$ then $\hat{h}(\epsilon) = e(-x_0\epsilon)\hat{f}(\epsilon)$.
- **Scaling property** If $h(x) = f\left(\frac{x}{L}\right)$ then $\hat{h}(\epsilon) = \frac{1}{|L|}\hat{f}\left(\frac{\epsilon}{L}\right)$.
- **Poisson Summation formula** If $f : \mathbb{R} \longrightarrow \mathbb{C}$ is a function of the Schwartz class such that the series
$$\sum_{n\in\mathbb{Z}} f(n+x)$$
converges absolutely and uniformly in $\mathbb{R}$ and such that $\sum_{n\in\mathbb{Z}} \hat{f}(n)$ converges absolutely, then $\sum_{n\in\mathbb{Z}} f(n) = \sum_{m\in\mathbb{Z}} \hat{f}(m)$.

We have

$$\begin{aligned}
S_\alpha(U,\, V,\, A,\, B,\, \mathcal{K};\, X) &= \frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} \pi_E(\alpha;\, \mathcal{K},\, X) \\
&= \frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} \sum_{\substack{p\leq X \\ a_E(p)\in\mathcal{K} \\ \frac{a_E(p)}{2\sqrt{p}}\in[0,\alpha]}} 1 \\
&= \frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} \sum_{\substack{p\leq X \\ a_E(p)\in\mathcal{K}}} \chi_{[0,\alpha]}\left(\frac{a_E(p)}{2\sqrt{p}}\right) \\
&= \frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} \sum_{\substack{p\leq X \\ a_E(p)\in\mathcal{K}}} \chi_{[0,\alpha]}(\cos\pi\,\theta_E(p))
\end{aligned}$$

$$= \frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} \sum_{\substack{p\leq X \\ a_E(p)\in\mathcal{K}}} \chi_{[\frac{\theta}{\pi},\frac{1}{2}]}(\theta_E(p)) \qquad \text{(where } \arccos\alpha = \theta\text{)} \tag{3.2}$$

In general we will consider the function $\chi_{[-\frac{1}{L},\frac{1}{L}]}$.

3.1 Smooth Variation

For a function $f : \mathbb{R} \longrightarrow \mathbb{R}$, we denote $\hat{f}$ to be the Fourier transform of f. Let $\Phi \in \mathcal{C}^\infty(\mathbb{R})$ is an even function of Schwartz's class such that $\hat{\Phi}$ is compactly supported, i.e, $\hat{\Phi}(\mathbb{R}) \in [-1, 1]$. Then define

$$\phi_L(\theta) \coloneqq \sum_{n\in\mathbb{Z}} \Phi(L(\theta + n))$$

Let us define

$$\psi(t) \coloneqq \Phi(L(\theta + t)).$$

Then by the scaling and shfiting properties of Fourier transform we have

$$\hat{\psi}(t) = \frac{1}{L} e(\theta t)\hat{\Phi}\left(\frac{t}{L}\right)$$

Therefore,

$$\begin{aligned}
\phi_L(\theta) &= \sum_{n\in\mathbb{Z}} \Phi(L(\theta + n)) \\
&= \sum_{n\in\mathbb{Z}} \psi(n) \\
&= \sum_{n\in\mathbb{Z}} \hat{\psi}(n) \qquad \text{(By Poisson summation formula)} \\
&= \frac{1}{L} \sum_{n\in\mathbb{Z}} \hat{\Phi}\left(\frac{n}{L}\right) e(\theta n)
\end{aligned} \tag{3.3}$$

Here we have used the fact that there exists a ϕ with above mentioned properties such that $\chi_{[-\frac{1}{L},\frac{1}{L}]}$ is approximated by ϕ_L. We call ϕ_L as the smooth version of $\chi_{[-\frac{1}{L},\frac{1}{L}]}$. Let us

evaluate

$$\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\phi_L(\theta_E(p))$$

$$=\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\sum_{n\in\mathbb{Z}}\frac{1}{L}\hat{\Phi}\left(\frac{n}{L}\right)e(n\,\theta_E(p)) \qquad \text{(by (3.3))}$$

$$=\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\sum_{|n|\le L}\frac{1}{L}\hat{\Phi}\left(\frac{n}{L}\right)e(n\,\theta_E(p))$$

$$=\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\sum_{|n|\le L}\frac{1}{L}\hat{\Phi}\left(\frac{n}{L}\right)e(n\,\theta_E(p))$$

$$=\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\sum_{1\le n\le L}\frac{1}{L}\hat{\Phi}\left(\frac{n}{L}\right)\{e(n\,\theta_E(p))+e(-n\,\theta_E(p))\}$$

$$+\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\frac{1}{L}\hat{\Phi}(0) \quad \text{(since } \phi \text{ is even function, so is its Fourier transform)}$$

$$=\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\frac{1}{L}\hat{\Phi}(0)$$

$$+\frac{1}{L}\sum_{n=1}^{L}\hat{\Phi}\left(\frac{n}{L}\right)\left[\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}2\cos 2\pi n\,\theta_E(p)\right]$$

$$=\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\frac{1}{L}\hat{\Phi}(0)$$

$$+\frac{1}{L}\sum_{n=1}^{L}\hat{\Phi}\left(\frac{n}{L}\right)\left[\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\left(\frac{a_E(p^{2n})}{p^n}-\frac{a_E(p^{2n-2})}{p^{n-1}}\right)\right] \quad \text{(By Lemma 3.1)}$$

$$=\frac{1}{L}\sum_{n=0}^{L}\left[\hat{\Phi}\left(\frac{n}{L}\right)-\hat{\Phi}\left(\frac{n+1}{L}\right)\right]\frac{1}{AB}\sum_{\substack{U<a\le U+A\\ V<b\le V+B}}\sum_{\substack{p\le X\\ a_E(p)\in\mathcal{K}}}\frac{a_E(p^{2n})}{p^n} \qquad (3.4)$$

Denote

$$\mathcal{U}(n) \coloneqq \hat{\Phi}\left(\frac{n}{L}\right) - \hat{\Phi}\left(\frac{n+1}{L}\right).$$

From (3.4), we have

$$\frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} \sum_{\substack{p\leq X \\ a_E(p)\in\mathcal{K}}} \phi_L(\theta_E(p)) = \sum_{n=0}^{L} \mathcal{U}(n) \left[\frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} \sum_{\substack{p\leq X \\ a_E(p)\in\mathcal{K}}} \frac{a_E(p^{2n})}{p^n} \right].$$

Henceforth, let us denote, for any function $H(a,b)$,

$$\langle H(a,b) \rangle := \frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} H(a,b).$$

By (3.4), we have

$$\sum_{\substack{p\leq X \\ a_E(p)\in\mathcal{K}}} \phi_L(\theta_E(p)) - \mathcal{U}(0) \sum_{\substack{p\leq X \\ a_E(p)\in\mathcal{K}}} 1 = \sum_{n=1}^{L} \mathcal{U}(n) \sum_{\substack{p\leq X \\ a_E(p)\in\mathcal{K}}} \frac{a_E(p^{2n})}{p^n}. \tag{3.5}$$

3.2 Remark

In this direction one needs to determine the the connection between the properties of the Fourier coefficients of $\phi(t)$ in our chosen test function and the growth requirements for A and B in order to derive asymptotics of the form

$$\frac{1}{AB} \sum_{\substack{U<a\leq U+A \\ V<b\leq V+B}} \sum_{p\leq X} \phi(\theta_E(p)) \sim \pi_k(X) \left(\frac{1}{3} + \frac{2}{3}\delta(k)\right) \frac{2^{1/k}}{k} \int_0^1 g(t) |\cos \pi t|^{\frac{1}{k}-1} \sin^2 \pi t \, dt.$$

In this way one would like to prove an analogous result of 1.20 with $\chi_{[0,\alpha]}$ replaced by ϕ_L, $L = \frac{1}{\alpha}$.

We saw at the end of the previous chapter that one of the key steps in proving Theorem

1.20 is to show that, as $X \to \infty$,

$$\begin{aligned} M(X) &:= \frac{1}{2} \sum_{\substack{p \leq X \\ 0 < r \leq (2\alpha\sqrt{p})^{1/2k}}} \frac{H(r^{2k} - 4p)}{p} \\ &\sim \pi_k(X) \left(\frac{1}{3} + \frac{2}{3}\delta(k) \right) \frac{2^{1/k}}{k} \int_0^{\alpha} |\cos \pi t|^{\frac{1}{k}-1} \sin^2 \pi t \, dt. \end{aligned} \tag{3.6}$$

In order to obtain a smooth analogue of Theorem 1.20, therefore, we have to obtain a smooth analogue of equation (3.6). In this direction, we make the following conjecture, which we hope to prove in future work.

Conjecture 3.4.

$$\begin{aligned} &\frac{1}{2} \sum_{\substack{p \leq X \\ 0 < r < (2\sqrt{p})^{1/2k}}} \frac{H(r^{2k} - 4p)}{p} \sum_{n=0}^{L} \mathcal{U}(n) X_{2n}\left(\frac{r^k}{\sqrt{p}} \right) \\ &\sim \pi_k(X) \left(\frac{1}{3} + \frac{2}{3}\delta(k) \right) \frac{2^{1/k}}{k} \int_0^{1} \phi_L(t) |\cos \pi t|^{\frac{1}{k}-1} \sin^2 \pi t \, dt. \end{aligned}$$

Here, $X_{2n}(t)$ denotes the Chebychev polynomial

$$X_{2n}(t) := \sum_{j=0}^{n} (-1)^j \binom{2n-j}{j} \left(\frac{r^k}{\sqrt{p}} \right)^{2n-2j}.$$

Currently, the problem that we have encountered in proving this conjecture is that in the proof of equation (3.6), the estimation of $M(X)$ depends very strongly on the fact that the inner sum runs over

$$0 < r \leq (2\alpha\sqrt{p})^{1/2k}$$

for some fixed $\alpha < 1$. The argument of James and Yu to evaluate this sum does not work for $\alpha = 1$.

On the other hand, when we attempt to prove the above conjecture, our current difficulty arises from the fact that the corresponding inner sum now runs over

$$0 < r < (2\sqrt{p})^{1/2k}$$

(which is essentially the above sum with $\alpha = 1$ for which the argument of James and Yu

does not work).

Here, the dependence on $\alpha = 1/L$ moves to the innermost weighted sum

$$\sum_{n=0}^{L} \mathcal{U}(n) X_{2n} \left(\frac{r^k}{\sqrt{p}} \right).$$

We are currently working to resolve this difficulty.

Chapter 4

Distribution of $\tilde{a_E}(p^2)$

In 1968, B.J. Birch addressed the following question in his work [Bir68]: Instead of fixing the curve E and varying the prime p, one can fix p and vary E. There are only finitely many curves over the field $\mathbb{F}_p$. In his work, he computed the higher moments of $a_E(p)$ with respect to the measure $\mu(t) \coloneqq \frac{2}{\pi}\sin^2 t dt$. The following theorem was proved:

Theorem 4.1. $\text{mean}\left[(a_E(p))^{2R}\right] \sim \frac{2R!}{R!(R+1)!}p^R$ *as* $p \to \infty$.

This result inspired us to look into the following question : What is the distribution of $\tilde{a_E}(p^2)$ as we vary over the primes? Specifically, if we average over a suitable family of elliptic curves , say $\mathfrak{G}_{A,B}$, how does the following quantity behave, as $X \to \infty$

$$\frac{1}{\tilde{\pi}(X)}\frac{1}{|\mathfrak{G}_{A,B}|}\sum_{E\in\mathfrak{G}_{A,B}}\sum_{\substack{\frac{X}{2}<p\leq X\\(ab\Delta(a,b),p)=1}}(\tilde{a_E}(p^2))^m,\ \ m\geq 1(\text{where}\Delta(a,\,b)\coloneqq 4a^3+27b^2)?$$

(where $\Delta(a,\,b) \coloneqq 4a^3 + 27b^2$) This question was not addressed in the existing literature and we are able to prove a theorem that precisely predicts the distribution of $\tilde{a_E}(p^2)$.

In this context, let us recall an important result([BP19], Lemma 3.2)

Lemma 4.2. *Assume that* $m \in \mathbb{N}\cup\{0\}$, *and* E *has a good reduction at* p. *Define,*

$$f_m(x) \coloneqq \sum_{j=0}^{[\frac{m}{2}]}(-1)^j\binom{m-j}{j}x^{m-2j}.$$

Then,

$$f_m(\tilde{a_E}(p)) = \tilde{a_E}(p^m).$$

Using this result we can find coefficients $h_{2j}(l)$ such that

$$\tilde{a_E}(p)^{2j} = \sum_{l=0}^{j} h_{2j}(l)\ \tilde{a_E}(p^{2l}).$$

Among these coefficients, $h_{2j}(0)$ will be of our special interest, so let us find an explicit expression for it.

Lemma 4.3.

$$h_{2j}(0) = \frac{1}{2\pi}\int_{-2}^{2} t^{2j}\sqrt{4-t^2}dt$$

Proof. The Chebyshev polynomials defined in Lemma 4.2 forms an orthonormal basis with respect to the Sato-Tate measure. Therefore, we have an linear expression of the form:

$$t^{2j} = \sum_{n=0}^{2j} c_n f_n(t).$$

Taking inner product on both side with $f_0(t)$, which is just 1, gives us the required result. □

Denote

$$\begin{aligned}\delta(t) &= 1 \text{ if n is even}\\ &= 0 \text{ if n is odd}\end{aligned}$$

Let us recall the following results from [BP19].

Theorem 4.4. *For all $A,\ B \geq 1$ and $n \in \mathbb{N}$*

$$\sum_{\substack{|a|\leq A, |b|\leq B\\ (ab\Delta(a,b),n)=1}} \tilde{a_E}(n) = 4ABS(n) + \mathrm{O}\left(d(n)s(n)^2\right) + \mathrm{O}\left(d(n)s(n)(A+B)\right) \tag{4.1}$$

where $s(n)$ denote the largest squarefree number dividing n and

$$S(n) \coloneqq \frac{1}{s(n)^2} \sum_{\substack{1\le a\le s(n)\\ 1\le b\le s(n)\\ (ab\Delta(a,b),\, n)=1}} \tilde{a_E}(n).$$

Lemma 4.5. *Let $c > 0$. Let $m \in \mathbb{N}$. Then, we have*

$$\sum_{\frac{X}{2}<p\le X} S(p^m) = \mathrm{O}_c\left(\frac{mX^{\frac{1}{2}}}{(\log X)^c}\right). \tag{4.2}$$

We will now prove a result that will be instrumental for our computation.

Lemma 4.6. *Suppose $A = A(X) \ge 1$ and $B = B(X) \ge 1$ such that $\frac{\log A}{\log X}$, $\frac{\log B}{\log X} \to \infty$ as $X \to \infty$. Let*

$$\mathfrak{G}_{A,\,B} \coloneqq \{E(a,\,b) : 1 \le |a| \le A,\, 1 \le |b| \le B\}.$$

Then,

$$\lim_{X\to\infty} \frac{1}{\tilde{\pi}(X)}\,\frac{1}{|\mathfrak{G}_{A,B}|} \sum_{E\in\mathfrak{G}_{A,B}} \sum_{\substack{\frac{X}{2}<p\le X\\ (ab\Delta(a,b),\,p)=1}} (\tilde{a_E}(p^{2l})) = 1 \qquad \textit{(if } l = 0\textit{)}$$

$$= 0 \qquad \textit{(if } l \ge 1\textit{)}$$

Proof. The asymptotic for $l = 0$ is immediate. To prove the result for $l \ge 1$ we observe that by Theorem 4.4

$$\sum_{\substack{|a|\le A,|b|\le B\\ \left(ab(4a^3-27b^2),p\right)=1}} \tilde{a_E}(p^{2l}) = 4ABS(p^{2l}) + \mathrm{O}_\epsilon\left(d(p^{2l})s(p^{2l})(A+B)\right)$$

Clearly, $d(p^{2l}) = 2l + 1$ and $s(p^{2l}) = p$. Therefore, we have

$$\sum_{\substack{|a|\le A,|b|\le B\\ \left(ab(4a^3-27b^2),p\right)=1}} \tilde{a_E}(p^{2l}) = 4ABS(p^{2l}) + \mathrm{O}_\epsilon\left(p(2l+1)(A+B)\right) \tag{4.3}$$

We also note that from Lemma 4.5

$$\sum_{\frac{X}{2}<p\leq X} S(p^{2l}) = \mathrm{O}\left(\frac{lx^{\frac{1}{2}}}{(\log X)^c}\right),$$

for $c > 0$. Thus,

$$\begin{aligned}
&\frac{1}{\tilde{\pi}(X)}\,\frac{1}{|\mathfrak{G}_{A,B}|}\sum_{E\in\mathfrak{G}_{A,B}}\sum_{\substack{\frac{X}{2}<p\leq X\\(ab\Delta(a,b))=1}}(\tilde{a_E}(p^{2l}))\\
&=\frac{1}{\tilde{\pi}(X)}\,\frac{1}{4AB}4AB\sum_{\frac{X}{2}<p\leq X}\frac{1}{p^2}\sum_{\substack{1\leq a\leq p-1\\1\leq b\leq p-1\\(ab\Delta(a,b))=1}}\tilde{a_E}(p^{2l})+\mathrm{O}_c\left(\frac{1}{\tilde{\pi}(X)}\left(\frac{1}{A}+\frac{1}{B}\right)\sum_{\frac{X}{2}<p\leq X}p^{\frac{1}{2}+\epsilon}l\right)\\
&\ll\frac{1}{\tilde{\pi}(X)}\frac{X^{\frac{1}{2}}}{(\log X)^c}+X^{\frac{1}{2}+\epsilon}\left(\frac{1}{A}+\frac{1}{B}\right)
\end{aligned}\tag{4.4}$$

As $X\to\infty$, $\frac{X^{\frac{1}{2}}}{(\tilde{\pi}(X)\log X)^c}\to 0$, and as $\frac{\log A}{\log X}$, $\frac{\log B}{\log X}\to\infty$ we have $\frac{X^{\frac{1}{2}+\epsilon}}{A}$, $\frac{X^{\frac{1}{2}+\epsilon}}{B}\to 0$. Thus, we have proved the lemma for $l\geq 1$. □

This result will allow us to calculate the distribution of $\tilde{a_E}(p^2)$ in the following manner:

$$\begin{aligned}
\left\langle\frac{1}{\tilde{\pi}(X)}\sum_{\substack{\frac{X}{2}<p\leq X\\(ab\Delta(a,b),p)=1}}\tilde{a_E}(p^2)^m\right\rangle&=\left\langle\frac{1}{\tilde{\pi}(X)}\sum_{\substack{\frac{X}{2}<p\leq X\\(ab\Delta(a,b),p)=1}}(\tilde{a_E}(p)^2-1)^m\right\rangle\\
&=\left\langle\frac{1}{\tilde{\pi}(X)}\sum_{\substack{\frac{X}{2}<p\leq X\\(ab\Delta(a,b),p)=1}}\sum_{j=0}^{m}(-1)^{m-j}\binom{m}{j}\tilde{a_E}(p)^{2j}\right\rangle\\
&=\left\langle\frac{1}{\tilde{\pi}(X)}\sum_{\substack{\frac{X}{2}<p\leq X\\(ab\Delta(a,b),p)=1}}\sum_{j=0}^{m}(-1)^{m-j}\binom{m}{j}\sum_{l=0}^{j}h_{2j}(l)\,\tilde{a_E}(p^{2l})\right\rangle
\end{aligned}$$

As $X \to \infty$, (using Lemma 4.6) we have

$$\lim_{X\to\infty} \left\langle \frac{1}{\tilde{\pi}(X)} \sum_{\substack{\frac{X}{2}<p\leq X \\ (ab\Delta(a,b),p)=1}} \tilde{a_E}(p^2)^m \right\rangle = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} h_{2j}(0) \tag{4.5}$$

Now, combining the result of Lemma 4.6 and (4.5) we obtain

$$\begin{aligned}
\lim_{X\to\infty} \left\langle \frac{1}{\tilde{\pi}(X)} \sum_{\substack{\frac{X}{2}<p\leq X \\ (ab\Delta(a,b),p)=1}} \tilde{a_E}(p^2)^m \right\rangle &= \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} \frac{1}{2\pi} \int_{-2}^{2} t^{2j}\sqrt{4-t^2}dt \\
&= \int_{-2}^{2} \left(\sum_{j=0}^{m} \binom{m}{j} (-1)^{m-j} t^{2j} \right) \frac{\sqrt{4-t^2}}{2\pi} dt \\
&= \int_{-2}^{2} (t^2-1)^m \left(\frac{\sqrt{4-t^2}}{2\pi} \right) dt \\
&= \int_{-1}^{3} y^m \sqrt{\frac{3-y}{y+1}} dy \qquad \textit{(By changing the variable)}
\end{aligned} \tag{4.6}$$

Let us denote this new measure by

$$\overrightarrow{\mu}(y) \coloneqq \sqrt{\frac{3-y}{y+1}}.$$

4.1 Remarks

In this direction one can further study the distribution of the error term, precisely for any subinterval $I \subseteq [-1, 3]$ construct a function $G(X)$ and determine the bounds on A and B such that

$$\left| \frac{1}{\tilde{\pi}(X)} \left\langle \sum_{\substack{\frac{X}{2}<p\leq X \\ (ab\Delta(a,b),p)=1}} \chi_I(\tilde{a_E}(p^2)) \right\rangle - \int_I \overrightarrow{\mu}(y)dy \right| \leq G(X).$$

This is also a question of interest to us for our future work.

Bibliography

[Bir68] Bryan J Birch. How the number of points of an elliptic curve over a fixed prime field varies. *Journal of the London Mathematical Society*, 1(1):57–60, 1968.

[BP19] Stephan Baier and Neha Prabhu. Moments of the error term in the Sato-Tate law for elliptic curves. *Journal of Number Theory*, 194:44–82, 2019.

[BPS20] Stephan Baier, Neha Prabhu, and Kaneenika Sinha. Central limit theorems for elliptic curves and modular forms with smooth weight functions. *Journal of Mathematical Analysis and Applications*, 485(1), 2020.

[CHT08] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l Galois representations. *Publications Mathématiques de l'IHÉS*, 108:1–181, 2008.

[Has36a] Helmut Hasse. On the theory of abstract elliptical function fields i. The structure of the group of divisor classes of finite order. 1936.

[Has36b] Helmut Hasse. On the theory of abstract elliptical function fields ii. Automorphisms and meromorphisms. The addition theorem. 1936.

[Has36c] Helmut Hasse. On the theory of abstract elliptical function fields iii. The structure of the meromorphism ring. The Riemann hypothesis. 1936.

[HSBT10] Michael Harris, Nick Shepherd-Barron, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy. *Annals of Mathematics*, pages 779–813, 2010.

[JT94] Joseph H. Silverman John Tate. *Rational Points on Elliptic Curves*. Springer-Verlag, 1994.

[JY06] Kevin James and Gang Yu. Average Frobenius distribution of elliptic curves. *Acta Arithmatica*, 124(1):79, 2006.

[Nat13] Melvyn B Nathanson. *Additive Number Theory The Classical Bases*, volume 164. Springer Science & Business Media, 2013.

[Tat65] John Tate. Algebraic cycles and poles of zeta functions. *Arithmetical Algebraic Geometry, ed. O.F.G. Schilling(New York)*, pages 93–110, 1965.

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