Fourier expansions for Eisenstein series twisted by modular symbols and the distribution of multiples of real points on an elliptic curve

Alex Cowan

Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Graduate School of Arts and Sciences

COLUMBIA UNIVERSITY

2019
This thesis consists of two unrelated parts.

In the first part of this thesis, we give explicit expressions for the Fourier coefficients of Eisenstein series $E^*(z, s, \chi)$ twisted by modular symbols $\langle \gamma, f \rangle$ in the case where the level of $f$ is prime and equal to the conductor of the Dirichlet character $\chi$. We obtain these expressions by computing the spectral decomposition of an automorphic function closely related to $E^*(z, s, \chi)$. We then give applications of these expressions. In particular, we evaluate sums such as $\sum \chi(\gamma)\langle \gamma, f \rangle$, where the sum is over $\gamma \in \Gamma_\infty \backslash \Gamma_0(N)$ with $c^2 + d^2 < X$, with $c$ and $d$ being the lower-left and lower-right entries of $\gamma$ respectively. This parallels past work of Goldfeld, Petridis, and Risager, and we observe that these sums exhibit cancellation beyond what one might expect.

In the second part of this thesis, given an elliptic curve $E$ and a point $P$ in $E(\mathbb{R})$, we investigate the distribution of the points $nP$ as $n$ varies over the integers, giving bounds on the $x$ and $y$ coordinates of $nP$ and determining the natural density of integers $n$ for which $nP$ lies in an arbitrary open subset of $\mathbb{R}^2$. Our proofs rely on a connection to classical topics in the theory of Diophantine approximation.
# Table of Contents

1 Introduction 1

1.1 Fourier expansions for Eisenstein series twisted by modular symbols 1

1.2 The distribution of multiples of real points on an elliptic curve 5

2 Fourier expansions for Eisenstein series twisted by modular symbols 10

2.1 Spectral decomposition 10

2.2 Applications 19

   2.2.1 Twisted sums of modular symbols 19

   2.2.2 Distribution of modular symbols twisted by characters 20

   2.2.3 Central values of L-functions 22

3 The distribution of multiples of real points on an elliptic curve 25

3.1 Background 25

3.2 Growth Rates 27

3.3 Distributions 28

3.4 Spacing 29

3.5 An equation of Bremner and Macleod 32

Bibliography 33
ACKNOWLEDGEMENTS

I would like to thank my advisor, Dorian Goldfeld. I was very depressed during my time as a graduate student, and Dorian would always find a way to keep me going and keep me learning. His support made all the difference for me, and he’s impacted the course of my life a huge amount. I never could have imagined that it was possible to have such a good advisor. I’m so lucky. Thank you Dorian.

I would like to thank my close friends for being endlessly loving and encouraging. You’re all so special to me, and always found ways to pick me up when I needed it. Thank you Fabiola Alba Vivar, Vlad Danila, Antoine Devroede, Mathilde Gerbelli-Gauthier, Sophia Ir, Fang Xi Lin, Brian Senie, Bhavna Shewale, Michael Snarski, Melissa Thoeni, Irene Xie, and Ling Feng Ye.

Finally, I would like to thank my mom, Laura Cowan, for always being there for me, no matter what, my whole life. She talks to me every day, always makes sure I’m ok, helps me in every way possible, and loves me with all of her heart. I love you with all my heart too, mom.
To my mom
Chapter 1

Introduction

This thesis consists of two unrelated parts. The first part discusses the Fourier expansions for Eisenstein series twisted by modular symbols and the second discusses the distribution of multiples of real points on an elliptic curve.

1.1 Fourier expansions for Eisenstein series twisted by modular symbols

Let \( f(z) \) be a cusp form of weight 2 and level \( N \), with Fourier coefficients \( a_n \). For simplicity, assume \( N \) is prime. For \( \gamma \in \Gamma_0(N) \), define the modular symbol

\[
\langle \gamma, f \rangle := 2\pi i \int_{\infty}^{\gamma \infty} f(w) \, dw.
\]

Modular symbols have been very useful tools historically and are of significant interest in their own right. Merel in [20], for instance, used modular symbols extensively in his proof that the number of torsion points on an elliptic curve over an arbitrary number field is bounded, and that the bound depends only on the degree of the number field. Another very important use of modular symbols is in Cremona’s algorithms for elliptic curves [3] which he used to generate his tremendously influential databases of elliptic curves. His algorithms are based on the duality between cusp forms and modular symbols, and the resulting action of the Hecke operators on modular symbols. All the information about elliptic curves he derives is obtained by examining the corresponding spaces of modular symbols. There has also been considerable interest in statistical questions regarding modular symbols because they are connected to central values of \( L \)-functions.

Let \( \chi \) be a Dirichlet character of conductor \( m \), and define \( L_f(s, \chi) \) for \( \Re(s) > 2 \) via the series

\[
L_f(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)a_n}{n^s}.
\]
CHAPTER 1. INTRODUCTION

This function has an analytic continuation to all of \( \mathbb{C} \). The “central value” \( L_f(1, \chi) \) contains a large amount of arithmetic information about \( f(z) \). The value of \( L_f(1, \chi) \) can be given in terms of a finite sum of modular symbols when \( \chi \) is primitive:

\[
\tau(\bar{\chi}) L_f(1, \chi) = \sum_{a=1}^{m} \bar{\chi}(a) \frac{1}{2} \left( \left\langle \left( \begin{array}{c} a \\ m \\ * \end{array} \right), f \right\rangle \pm \left\langle \left( \begin{array}{c} -a \\ m \\ * \end{array} \right), f \right\rangle \right)
\]

where \( \pm \) is the sign of \( \chi \) and \( \tau(\bar{\chi}) \) is the Gauss sum \([25]\). The matrices that appear in this formula are not necessarily in \( \Gamma_0(N) \), but nevertheless they are defined via the same expression as before.

Petridis and Risager show in [23] that modular symbols are normally distributed when ordered by \( |cz + d|^2 \) for any fixed \( z \in \mathfrak{h} \), where \( c \) and \( d \) are the lower-left and lower-right entries of \( \gamma \) respectively, proving and greatly refining a conjecture of Goldfeld [9]. To prove this result, Petridis and Risager study the properties of an Eisenstein series twisted by modular symbols as proposed in Goldfeld’s paper. This series is defined as

\[
E^*(z, s, \chi) := \sum_{\Gamma_\infty \backslash \Gamma_0(N)} \chi(\gamma)(\gamma, f) \text{Im}(\gamma z)^s
\]

where \( \chi \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \) := \( \chi(d) \).

The Eisenstein series \( E^*(z, s, \chi) \) is not automorphic, but does satisfy a certain cocycle relation and can be related to automorphic functions in a simple way. This has led to several papers dedicated entirely to the study of \( E^*(z, s, \chi) \). Particularly, O’Sullivan in [22] proves that this function has various nice properties such as an analytic continuation and a functional equation, and proves many things about the form of its Fourier expansion. Petridis in [24] studies the poles and residues of this Eisenstein series.

The result of Petridis and Risager in [23] is very interesting and important when studying modular symbols for their own sake, but the chosen ordering is not conducive to studying central values of \( L \)-functions. Recently, Mazur and Rubin [19] made conjectures for the distribution of modular symbols when ordered in a way more similar to how the appear in the application to central values of \( L \)-functions, partially in an attempt to recover conjectures about ranks of twisted elliptic curves by David, Fearnley, and Kisilevsky, [6]. An average version of one of their conjectures was proven by Petridis and Risager in [25], and the full conjecture was proven by Diamantis, Hoffstein, Kiral, and Lee [7].

This thesis is focused on the case where \( \chi \) has conductor \( N \), the level of \( f(z) \). In the literature it is usually assumed that the conductor of \( \chi \) is coprime to \( N \). The techniques used in each case are quite different; surprisingly, the approach presented here fails completely if the conductor of \( \chi \) is not exactly \( N \). The objects used to obtain the results in this thesis can still be defined when the conductor of \( \chi \) is different from \( N \) but
it seems unlikely that they will have any reasonable properties.

Section 2.1 is dedicated to the main technical result of this thesis, giving the Fourier expansion of $E^*(z, s, \chi)$ in very explicit terms. Previously this Fourier expansion was given by O’Sullivan in terms of Kloosterman sums twisted by modular symbols [22].

Here we give a formulation of the Fourier coefficients which makes the analysis of $E^*(z, s, \chi)$ much easier.

**Theorem 1.1.1.** Let $N$ be a prime, let $\chi$ be an even character of conductor $N$, and let $f$ be a cusp form of weight 2 for $\Gamma_0(N)$. Then the constant term of the Fourier expansion for $E^*(z, s, \chi)$ is given by

$$
\int_0^1 E^*(x + iy, s, \chi) \, dx = \left(2\tau(\bar{\chi})L_f(1, \chi)\pi^2 N^{-2s} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} L_f(2s, \chi) \right)
$$

$$
-2\tau(\bar{\chi})L_f(1, \chi)\pi^2 N^{-2s} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} L_f(2s, \chi) \right) y^{1-s}.
$$

**Theorem 1.1.2.** Let $N$ be a prime, let $\chi$ be an even character of conductor $N$, and let $f$ be a cusp form of weight 2 for $\Gamma_0(N)$. Then, for $n \neq 0$, the $n$th term of the Fourier expansion for $E^*(z, s, \chi)$ is given by

$$
\int_0^1 E^*(x + iy, s, \chi) e^{-2\pi i mx} \, dx
$$

$$
= \sum_l \frac{(4\pi)^{1-s}}{2(M_l, M_l)} \frac{\Gamma(s + i\lambda_l - \frac{1}{2}) \Gamma(s - i\lambda_l - \frac{1}{2})}{\Gamma(s)} L\left(s + \frac{1}{2}, f \times M_l\right) \cdot c_{M_l}(n) y^{\frac{s}{2}} K_{i\lambda_l}(2\pi|n|y)
$$

$$
- \sum_{m=1} \frac{a_{\chi} e^{-2\pi my}}{N^2 \Gamma(s)} |n - m|^{\frac{1}{2} - s/2} \sigma_{2s-1}(n - m, \bar{\chi}) y^{\frac{s}{2}} K_{s-\frac{1}{2}}(2\pi|n - m|y)
$$

$$
+ \frac{2\pi^2 - \pi}{NT(s)} \sum_{k=0} \frac{\Gamma(2s + k - 1)}{k! \Gamma(s + k) \Gamma(1 - s - k)}
$$

$$
\cdot L_f(k) \left(\frac{L_f(1 - k, \chi)}{L(2s, \chi)L(2 - 2s - 2k, \chi)} \sigma_{1 - 2s - 2k}(n, \bar{\chi}) - \frac{L_f(1 - k, \chi)}{L(2s, \chi)L(2 - 2s - 2k, \chi)} \sigma_{1 - 2s - 2k}(n, \chi)\right)
$$

$$
+ \frac{2\pi^2 - \pi}{NT(s)} \sum_{\rho:L(2\rho, \chi)=0} \frac{\Gamma(s + \rho - 1) \Gamma(s - \rho)}{\Gamma(1 - \rho) \Gamma(\rho)} L_f(s + 1 - \rho) \frac{L_f(s + \rho, \chi)}{L(2s, \chi)L(2\rho, \chi)} \sigma_{2\rho-1}(n, \bar{\chi}) |n|^{\frac{s}{2} - \rho} y^{\frac{s}{2}} K_{\rho-\frac{1}{2}}(2\pi|n|y)
$$

$$
- \frac{2\pi^2 - \pi}{NT(s)} \sum_{\rho:L(2\rho, \bar{\chi})=0} \frac{\Gamma(s + \rho - 1) \Gamma(s - \rho)}{\Gamma(1 - \rho) \Gamma(\rho)} L_f(s + 1 - \rho) \frac{L_f(s + \rho, \bar{\chi})}{L(2s, \bar{\chi})L(2\rho, \bar{\chi})} \sigma_{2\rho-1}(n, \chi) |n|^{\frac{s}{2} - \rho} y^{\frac{s}{2}} K_{\rho-\frac{1}{2}}(2\pi|n|y).
$$
CHAPTER 1. INTRODUCTION

It was pointed out to me late in the process of writing this thesis that theorem 1.1.1 was derived in the work of Bruggeman and Diamantis [2]. There, they obtain an expression for the constant term which appears to be different than the one presented here, but by using the relationship in theorem 1.1.5 one can see that theorem 1.1 from their paper and theorem 1.1.1 here are the same. They also give an expression for the higher Fourier coefficients of these Eisenstein series, but in terms of a shifted convolution sum involving the Fourier coefficients of \( f \) and the sum of divisors function \( \sigma_s(n, \chi) \), and this leads to different applications than the ones presented here.

Section 2.2 then gives various applications of this explicit form of the Fourier expansion of \( E^*(z, s, \chi) \).

We can evaluate the Kloosterman sums given in [22], of which very little was known previously, obtaining results such as

**Corollary 1.1.3.** Let \( N \) be prime and let \( f \) be a weight 2 cusp form on \( \Gamma_0(N) \). For even primitive characters \( \chi \mod N \) and \( \text{Re}(s) > 2 \) we have

\[
\sum_{\gamma \in \Gamma_\infty \setminus \Gamma_0(N) / \Gamma_\infty} \frac{\chi(\gamma) \langle \gamma, f \rangle}{|c|^{2s}} = 2N^{-2s} L_f(2s) \left( \frac{\tau(\bar{\chi}) L_f(1, \chi)}{L(2s, \chi)} - \frac{\tau(\chi) L_f(1, \bar{\chi})}{L(2s, \bar{\chi})} \right),
\]

where \( c \) is the lower-left entry of \( \gamma \).

We also prove the following corollary, which is analogous to the main conjecture presented in [9].

**Corollary 1.1.4.** For even \( \chi \) and for any complex \( z = x + iy \) with positive imaginary part,

\[
\sum_{\gamma \in \Gamma_\infty \setminus \Gamma_0(N) / \Gamma_\infty} \chi(\gamma) \langle \gamma, f \rangle = \sum_{\substack{\rho: \text{L}(\rho, \chi) = 0 \\ \rho: \text{L}(\rho, \bar{\chi}) = 0}} \frac{(4\pi)^{-\frac{1}{2}}}{N} L_f(0) \Gamma(1 - \rho) \Gamma(1 - \frac{\rho}{2}) \sum_{n \neq 0} e^{2\pi i n z} \sigma_\rho(n, \chi) |n|^{\frac{1}{2} - \rho} \cdot y^{\frac{1}{2}} K_{\frac{1}{2} + \rho}(2\pi|n|y) \cdot X^{1 - \frac{\rho}{2}}
\]

\[
- \sum_{\rho: \text{L}(\rho, \chi) = 0} \frac{(4\pi)^{-\frac{1}{2}}}{N} L_f(0) \Gamma(1 - \rho) \Gamma(1 - \frac{\rho}{2}) L(1 - \rho, \chi) L'(\rho, \chi) \sum_{n \neq 0} e^{2\pi i n z} \sigma_\rho(n, \bar{\chi}) |n|^{\frac{1}{2} - \rho} \cdot y^{\frac{1}{2}} K_{\frac{1}{2} + \rho}(2\pi|n|y) \cdot X^{1 - \frac{\rho}{2}}
\]

\[
+ O(X^{\frac{1}{2}}),
\]

where \( c \) and \( d \) are the lower left and lower right entries of \( \gamma \) respectively.

The error term in this corollary can be made completely explicit. Results of this type for \( \chi \) with conductor different from the level \( f \) can be found in recent work of Nordentoft [21]. It is noteworthy that we appear to not observe the common phenomenon of “square root cancellation” in this situation.

In section 2.2 we also study central values of \( L \)-functions. We obtain the following result:
CHAPTER 1. INTRODUCTION

Theorem 1.1.5. Let $N$ be a prime, let $\chi$ be a primitive even character of conductor $N$, and let $f$ be a cusp form of weight 2 for $\Gamma_0(N)$. Then

$$\tau(\bar{\chi})L_f(1, \chi) = -\tau(\chi)L_f(1, \bar{\chi}).$$

Note that this implies, for example, that $L_f(1, \chi) = 0$ when $\chi$ is the quadratic character mod $N$. The vanishing in this case is known via the work of Schmidt [26], but the method used in his work relies on computing the root number of the $L$-function, whereas this thesis proves the vanishing directly, making no reference at all to root numbers. If $f(z)$ corresponds to an elliptic curve $E$, then the Birch and Swinnerton-Dyer conjecture implies the existence of a point of infinite order on the elliptic curve which is the twist of $E$ by $\chi$. The approach in this thesis is purely analytic, and to our knowledge the only previous example of proving that an elliptic curve has positive analytic rank using purely complex analytic techniques is the Gross-Zagier formula [11].

1.2 The distribution of multiples of real points on an elliptic curve

Let $E : y^2 = 4x^3 - g_2x - g_3$ be an elliptic curve with $g_2, g_3 \in \mathbb{R}$, and suppose that $P \in E(\mathbb{R})$. In this thesis we investigate the statistics of the coordinates $x(nP), y(nP) \in \mathbb{R}$ of $nP$ for $n \in \mathbb{Z}$. The set of points $(x, y) \in \mathbb{R}^2$ which satisfy the equation for $E$ form either one or two connected subsets of $\mathbb{R}^2$, depending on whether the polynomial $4x^3 - g_2x - g_3$ has one or three real roots. In the case where $4x^3 - g_2x - g_3$ has three real roots, the coordinates of points making up one of the connected subsets are bounded, while in the other the coordinates are unbounded. In this case we will say that $E(\mathbb{R})$ has two connected components, and we will refer to them as the “bounded component” and “unbounded component”. If instead $4x^3 - g_2x - g_3$ has only one real root, then we will say that $E(\mathbb{R})$ has only one component, we will refer to it as the “unbounded component”.

In section 3.2, we prove theorems which explain how large the coordinates of $nP$ get as a function of $n$.
CHAPTER 1. INTRODUCTION

**Theorem 1.2.1.** Suppose that $E/\mathbb{C}$ has periods $\omega_1$ and $\omega_2$, chosen such that $\omega_1 \in \mathbb{R}_{>0}$ and $\text{Im}(\omega_2) > 0$. Then for every point $P$ of infinite order in the unbounded component of $E(\mathbb{R})$, there exist infinitely many $n$ such that

$$x(nP) > \frac{5}{\omega_1^2} n^2 + O(n^{-2}) \quad \text{and} \quad y(nP) > \frac{2 \cdot 5^3}{\omega_1^3} n^3 + O(n^{-1}).$$

If $P$ is instead a point of infinite order on the bounded component of $E(\mathbb{R})$ (in the case where $E(\mathbb{R})$ has two connected components), then there exist infinitely many $n$ such that

$$x(nP) > \frac{5}{4 \omega_1^2} n^2 + O(n^{-2}) \quad \text{and} \quad y(nP) > \frac{5^3}{4 \omega_1^3} n^3 + O(n^{-1}).$$

The implied constants depend only on $E$.

**Figure 1.2.2.** $\{\log(x(nP) + 2) : 1 < n < 10^6\}$ for $P \approx (-0.406, 0.966)$ on $E : y^2 = x^3 + 1$, with the lower bound of theorem 1.2.1 in red.

**Theorem 1.2.3.** Let $f$ be a function from $\mathbb{N}$ to $\mathbb{R}_{>0}$. If $\sum_{n=1}^{\infty} f(n)^{-1}$ diverges, then for all points $P$ in $E(\mathbb{R})$ except for a set of points of Lebesgue measure zero, there exist infinitely many positive integers $n$ such that

$$x(nP) > f(n)^2 \quad \text{and} \quad y(nP) > f(n)^3,$$

while if $\sum_{n=1}^{\infty} f(n)^{-1}$ converges, then the set of points $P$ in $E(\mathbb{R})$ for which there exist infinitely many such $n$ has measure zero.

**Theorem 1.2.4.** For any $E$ and any function $f : \mathbb{N} \to \mathbb{R}_{>0}$, there exists a point $P$ in $E(\mathbb{R})$ such that, for infinitely many positive integers $n$,

$$x(nP) > f(n)^2 \quad \text{and} \quad y(nP) > f(n)^3.$$  

Variants of these theorems can be given for general $P \in E(\mathbb{C})$, and not just for $P \in E(\mathbb{R})$. For example,

**Theorem 1.2.5.** Let $P$ be a point in $E(\mathbb{C})$ of infinite order. Then

$$|x(nP)| \gg n \quad \text{and} \quad |y(nP)| \gg n^2,$$

where the implied constants depends only on $E$.

The proofs of these theorems rely on the work of Hurwitz [15], Khinchin [16] [17], and Dirichlet (see [12],
theorem 200) in the field of Diophantine approximation. The correspondence between results in Diophantine approximation and asymptotics for the size of the coordinates of \(nP\) can be extended further.

In section 3.3, we investigate the full distribution of the \(x\) and \(y\) coordinates of \(nP\). Let \(\omega_1\) and \(\omega_2\) be the periods of \(E/\mathbb{C}\), chosen such that \(\omega_1 \in \mathbb{R}_{>0}\) and \(\text{Im}(\omega_2) > 0\). Let \(\Lambda\) be the \(\mathbb{C}\)-lattice with basis \((\omega_1, \omega_2)\). Then \(E/\mathbb{C}\) is parameterized by elements \(z\) of \(\mathbb{C}/\Lambda\) via \(z \mapsto (\varphi(z), \varphi'(z))\), where

\[
\varphi(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left( \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right).
\]

We prove the following regarding the distribution of integer multiples of a fixed \(P \in E(\mathbb{R})\) in section 3.3:

**Theorem 1.2.6.** Let \(P\) be a point of infinite order in \(E(\mathbb{R})\), and let \(z_P\) be the preimage of \(P\) under the parameterization \(z \mapsto (\varphi(z), \varphi'(z))\). Let \(\omega_1\) and \(\omega_2\) be the periods of \(E/\mathbb{C}\), chosen such that \(\omega_1 \in \mathbb{R}_{>0}\) and \(\text{Im}(\omega_2) > 0\). Let \(\Lambda\) be the \(\mathbb{C}\)-lattice with basis \((\omega_1, \omega_2)\). Define \(I_P \subseteq \mathbb{C}/\Lambda\) as follows:

\[
I_P := \begin{cases} 
[0, \omega_1], & \text{Im}(z_P) = 0 \mod \Lambda, \\
[0, \omega_1] \cup ([0, \omega_1] + \frac{\omega_2}{2}), & \text{Im}(z_P) = \text{Im}(\frac{\omega_2}{2}) \mod \Lambda,
\end{cases}
\]

where \([0, \omega_1]\) denotes the interval of real numbers. Then, for any \(U \subseteq \mathbb{R}^2\), we have

\[
\lim_{n \to \infty} \frac{1}{2n^2} \# \left\{ |k| < n : (x(kP), y(kP)) \in U \right\} = \frac{\mu \left( \left\{ z \in I_P : (\varphi(z), \varphi'(z)) \in U \right\} \right)}{\mu(I_P)},
\]

where \(\mu\) is the Lebesgue measure.

**Corollary 1.2.7.** Fix \(P_0 = (x_0, y_0) \in E(\mathbb{R})\) and \(\varepsilon > 0\). For all \(P \in E(\mathbb{R})\) of infinite order, the natural density of integers \(n\) for which \((x(nP) - x_0)^2 + (y(nP) - y_0)^2 < \varepsilon^2\) is

\[
\frac{2\eta (\varepsilon + O(\varepsilon^2))}{\omega_1 \sqrt{y_0^2 + (6x_0^2 - \frac{\omega_2}{2})^2}},
\]

where \(\eta = 1\) if both \(P\) and \(P_0\) are on the unbounded component of \(E(\mathbb{R})\), \(\eta = \frac{1}{2}\) if \(P\) is on the bounded component of \(E(\mathbb{R})\), and \(\eta = 0\) if \(P_0\) is on the bounded component of \(E(\mathbb{R})\) but \(P\) is not. The implied constant depends on both \(E\) and \(P_0\).

**Figure 1.2.8.** \(\{nP : 1 < n < 3000\}\) for \(P = (0,4)\) on \(E37a: y^2 = x^3 - 16x + 16 [4]\), with contour lines of the limiting density. The top 16% and bottom 16% of points are not shown.
CHAPTER 1. INTRODUCTION

In figure 1.2.8 we illustrate the distribution of multiples of the point $P = (0, 4)$ on the curve $E_{37a}$: $y^2 = x^3 - 16x + 16$ for $1 \leq n \leq 3000$. This elliptic curve is the elliptic curve of smallest conductor with positive rank, and $P$ is a generator of the group of rational points. The top 16% and bottom 16% of points, when ordered by $y$-coordinate, are not displayed for clarity reasons.

We then obtain the following spacing law:

**Corollary 1.2.9.** Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, let $Q = (x_Q, y_Q)$ be an arbitrary fixed point in $E(\mathbb{R})$, and let $d$ be an arbitrary real number. Define

$$F_{\pm, Q}(x) := \left( \frac{\pm \sqrt{x^3 + ax + b - y_Q}}{x - x_Q} \right)^2 - 2x - x_Q$$

and

$$\rho(x) := \left[ \frac{1 + \frac{1}{4} \frac{(3x^2 + a)^2}{x^3 + ax + b}}{4(x^3 + ax + b) + (6x^2 + a)^2} \right]^\frac{1}{2}.$$

Let $x_1^\pm, \ldots, x_k^\pm$ be the real solutions to $F_{\pm, Q}(x) = d$. Then, for any point $P$ in $E(\mathbb{R})$ of infinite order, the distribution of the values $x(nP+Q) - x(nP)$ as $n$ varies over the integers is proportional to the function $f(d)$, defined as

$$f(d) := \sum_{i=1}^{k^+} \frac{\rho(x_i^+)}{F_{+, Q}(x_i^+)} + \sum_{i=1}^{k^-} \frac{\rho(x_i^-)}{F_{-, Q}(x_i^-)},$$

where $\sum^*$ indicates that, if $P$ is on the unbounded component of $E(\mathbb{R})$, then the sum omits the $x_i^\pm$ for which $x_i^\pm$ is not the $x$-coordinate of any point on the unbounded component of $E(\mathbb{R})$.

We also show in corollaries 3.4.1 and 3.4.2 that the raw moments of the function $f(d)$ diverge, and give an upper bound for the associated partial sums.

As an application of these growth and distribution results, we explain certain numerical observations of Bremner and Macleod made in [1]. There, Bremner and Macleod find the positive integer solutions $a, b, c$ to
the equation
\[ \frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = N. \] (1.1)
Solutions to (1.1) are given by certain rational points on certain elliptic curves \( E_N \). If \( E_N \) has rank 1 and \( P \) is a generator for \( E_N \), then Bremner and Macleod make numerical observations regarding the set of \( n \in \mathbb{Z} \) for which \( nP \) yields a solution to equation (1.1). In particular, they investigate what the least \( n \) that yields a solution is, as well as what proportion of integers \( n \) yield solutions. Using theorems 1.2.1 and 1.2.6 we can explain their observations.
Chapter 2

Fourier expansions for Eisenstein series twisted by modular symbols

2.1 Spectral decomposition

Define $A(z) = 2\pi i \int_{\infty}^{z} f(w) \, dw$. The approach is to introduce the function $D(z, s, \chi)$, defined as

$$D(z, s, \chi) := \sum_{\Gamma \backslash \Gamma_0(N)} \chi(\gamma)A(\gamma z) \text{Im}(\gamma z)^s.$$ 

It’s easily verified that $D(\alpha z, s, \chi) = \bar{\chi}(\alpha)D(z, s, \chi)$ and $E^*(z, s, \chi) = D(z, s, \chi) - A(z)E(z, s, \chi)$. Moreover $D(z, s, \chi)$ is $L^2$ for $\text{Re}(s) > 1$ ([25] § 3).

We give a Fourier expansion of $E^*(z, s, \chi)$ for even $\chi$ by getting an explicit spectral decomposition for $D(z, s, \chi)$ and using $E^*(z, s, \chi) = D(z, s, \chi) - A(z)E(z, s, \chi)$. The main obstacle to extending to non-prime $N$ and odd $\chi$ is obtaining Fourier expansions for $E(z, s, \chi)$ in those cases. Recent work of Young [29] may be helpful if one wishes to do this, but we chose to limit this work to prime $N$ and even $\chi$ to make the exposition more readable.

Let $M_j(z), j = 1, 2, \ldots$ be an orthogonal basis of Maass forms on $\Gamma_0(N)$ which transform as $M_j(\gamma z) = \bar{\chi}(\gamma)M_j(z)$ and normalized such that their Fourier coefficients are equal to their Hecke eigenvalues. The Selberg spectral decomposition [13] for $D(z, s, \chi)$ then gives

$$D(z, s, \chi) = \sum_j \frac{\langle D(*, s, \chi), M_j \rangle}{\langle M_j, M_j \rangle} M_j(z) + \frac{1}{4\pi i} \sum_a \int_{(\frac{1}{2})} \langle D(*, s, \chi), E_a(*, w, \chi) \rangle E_a(z, w, \chi) \, dw.$$
where

$$\langle f, g \rangle = \int_{\Gamma_0(N) \backslash \mathbb{H}} f(z) \overline{g(z)} \frac{dx dy}{y^2}$$

is the Petersson inner product, and

$$E_a(z, s, \chi) := \sum_{\Gamma_0(N) \backslash \Gamma_a} \chi(\gamma) \text{Im}(\sigma_a^{-1} \gamma z)^s,$$

with $\sigma_a$ the matrix such that $\sigma_a \Gamma_\infty \sigma_a^{-1}$ is the stabilizer $\Gamma_a$ of the cusp $a$, and $\sigma_\infty = a$. If $N$ is prime, there are only two cusps, $i\infty$ and 0, and $\sigma_0 = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$.

When dealing with Fourier expansions of Eisenstein series it is often more convenient to work with “completed” Eisenstein series, given by $L(2s, \chi)E(z, s, \chi)$. Using completed Eisenstein series in place of regular Eisenstein series in the spectral decomposition formula instead gives

$$D(z, s, \chi) = \sum_j \frac{\langle D(*, s, \chi), M_j \rangle}{\langle M_j, M_j \rangle} M_j(z)$$

$$+ \frac{1}{4\pi i} \int \frac{\langle D(*, s, \chi), E_{i\infty}(*, w, \chi) \rangle}{L(2w, \chi)} E_{i\infty}(z, w, \chi) dw$$

$$+ \frac{1}{4\pi i} \int \frac{\langle D(*, s, \chi), E_0(*, w, \chi) \rangle}{L(2 - 2w, \bar{\chi})} E_0(z, w, \chi) dw$$

when $N$ is prime. We for the rest of this section we will use this form of the spectral decomposition, using completed Eisenstein series.

To proceed we need:

- A Fourier expansion for $M_j(z)$.
- A Fourier expansion for $E_a(z, w, \chi)$.
- The evaluation of $\langle D(*, s, \chi), M_j \rangle$.
- The evaluation of $\langle D(*, s, \chi), E_a(*, w, \chi) \rangle$.

We give these in lemmas 2.1.1 through 2.1.5. From this spectral expansion for $D(z, s, \chi)$ and the Fourier expansions of $E(z, s, \chi)$ and $M_j(z)$ we obtain the Fourier expansion of $D(z, s, \chi)$.

From there, we can obtain the full Fourier expansion of $E^*(z, s, \chi)$. The $n^{th}$ Fourier coefficient is

$$\int_0^1 (D(z, s, \chi) - A(z) E(z, s, \chi)) e^{-2\pi inx} dx,$$
which is easily evaluated using the Fourier expansions of \( D(z, s, \chi) \), \( E(z, s, \chi) \), and \( f(z) \). This yields theorems 1.1.1 and 1.1.2.

**Lemma 2.1.1.** The Fourier expansion of a Maass form \( M_j \) of eigenvalue \( 1/4 + \lambda_j^2 \) is given by

\[
M_j(z) = \sum_{n \neq 0} c_{Mj}(n) y^{\frac{1}{2}} K_{i\lambda_j}(2\pi |n| y) e^{2\pi inx}
\]

where \( K_v(y) \) is the \( K \)-Bessel function, defined as

\[
K_v(y) = \frac{1}{2} \int_{0}^{\infty} \exp \left( \frac{1}{2} y(u + u^{-1}) \right) u^v \frac{du}{u}.
\]

**Proof.** [10], Theorem 3.5.1.

We normalize \( M_j(z) \) so that \( c_{Mj}(1) = 1 \). The quantity \( \langle M_j, M_j \rangle \) will appear later, and from the work of Hoffstein and Lockhart [14] for all \( \varepsilon > 0 \) we have the bound

\[
N^{-\varepsilon} \cosh(\pi \lambda_j) \frac{1}{2} \ll \langle M_j, M_j \rangle - \frac{1}{2} \ll N^{\varepsilon} \cosh(\pi \lambda_j) \frac{1}{2}.
\]

**Lemma 2.1.2.** The Fourier expansions of the completed Eisenstein series \( E_a(z, w, \chi) \) for even \( \chi \) are given by

\[
E_{i\infty}(z, w, \chi) = 2y^w L(2w, \chi) + \frac{4\pi(\chi)\pi^w}{N^{2w} \Gamma(w)} y^{\frac{1}{2}} \sum_{n \neq 0} |n|^{\frac{1}{2} - w} \sigma_{2w-1}(n, \bar{\chi}) K_{w-\frac{1}{2}}(2\pi |n| y) e^{2\pi inx}
\]

and

\[
E_0(z, w, \chi) = \frac{2\pi(\chi)\pi^{2w-1} \Gamma \left( \frac{1}{2} \right)}{N^{1-3w} \Gamma(w)} y^{1-w} L(2 - 2w, \bar{\chi}) + \frac{4\pi^w}{N^w \Gamma(w)} y^{\frac{1}{2}} \sum_{n \neq 0} |n|^{\frac{1}{2} - w} \sigma_{1-2w}(n, \chi) K_{w-\frac{1}{2}}(2\pi |n| y) e^{2\pi inx}.
\]

**Proof.** [8] along with the identity

\[
\Gamma(2w - 1) = 4^{w-1} \pi^{-\frac{1}{2}} \Gamma \left( w + \frac{1}{2} \right) \Gamma(w)
\]

and the functional equation

\[
L(2w - 1, \chi) = \frac{\tau(\chi)}{\sqrt{N}} \left( \frac{N}{\pi} \right)^{\frac{1}{2}} \frac{\Gamma(1-w)}{\Gamma \left( w - \frac{1}{2} \right)} L(2 - 2w, \bar{\chi}).
\]

The reference gives a Fourier expansion for \( E \left( \frac{-1}{N^2}, w, \chi \right) \) instead of \( E_0(z, w, \chi) \). However, for \( \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma_0(N) \), we have

\[
\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \left( \begin{array}{cc} 0 & -1 \\ N & 0 \end{array} \right) = \left( \begin{array}{cc} 0 & -1 \\ N & 0 \end{array} \right) \left( \begin{array}{cc} d & -\frac{c}{N} \\ -bN & a \end{array} \right).
\]
The rightmost matrix is an element of $\Gamma_0(N)$, and summing over all $\left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \Gamma_0(N)$ is the same as summing over all $\left( \begin{smallmatrix} d & a \\ -bN & c \end{smallmatrix} \right) \in \Gamma_0(N)$, so the Fourier expansion given is indeed for $E_0(z, s, \chi)$.

**Lemma 2.1.3.** The inner product of $D(z, s, \chi)$ with the Maass form $M_j(z)$ is given by

$$\langle D(*, s, \chi), M_j \rangle = (4\pi)^{1-s} \frac{\Gamma(s + i\lambda_j - \frac{1}{2}) \Gamma(s - i\lambda_j - \frac{1}{2})}{\Gamma(s)} L\left(s + \frac{1}{2}, f \times M_j\right).$$

**Proof.** Unfolding,

$$\langle D(*, s, \chi), M_j \rangle = \int_{\Gamma_0(N) \backslash \mathbb{H}} \chi(\gamma) A(\gamma z) \Im(\gamma z)^s \cdot \overline{M_j(z)} \frac{dx dy}{y^2}$$

$$= \frac{1}{n} \int_0^{1/2} \int_0^{\infty} A(z) y^s \cdot \overline{M_j(z)} \frac{dx dy}{y^2}$$

$$= \frac{1}{n} \int_0^{1/2} \int_0^{\infty} \sum_{n \geq 1} \frac{a_n}{n} e^{-2\pi ny} e^{2\pi nx} y^s \cdot \overline{c_M(j)}(n) y^{s+1/2} \int_0^{\infty} \exp(-\pi ny(u + u - 1)) u^{-i\lambda_j - 1} d\lambda_j \frac{dx dy}{y^2}$$

$$= \frac{\pi^{1-s}}{2} \frac{\Gamma(s + i\lambda_j - \frac{1}{2}) \Gamma(s - i\lambda_j - \frac{1}{2}) \Gamma(s + \lambda_j + 1/2) \Gamma(s - \lambda_j - 1/2)}{\Gamma(s)} \sum_{n \geq 1} \frac{a_n c_M(j)}{n^{s+\frac{1}{2}}}$$

$$= \frac{\pi^{1-s}}{2} \frac{\Gamma(s - \frac{1}{2}) \Gamma(s + i\lambda_j - \frac{1}{2}) \Gamma(s - i\lambda_j - \frac{1}{2}) \Gamma(s + \lambda_j + 1/2) \Gamma(s - \lambda_j - 1/2)}{\Gamma(s)} L\left(s + \frac{1}{2}, f \times M_j\right).$$

The integral in $u$ was evaluated with Mathematica.

**Lemma 2.1.4.** The inner product of $D(z, s, \chi)$ with the Eisenstein series $E_{i\infty}(z, s, \chi)$ is given by

$$\langle D(*, s, \chi), E_{i\infty}(s, w, \chi) \rangle = \frac{2\pi(\chi)\pi^{w-s+\frac{1}{2}} N^{-w}}{2\pi(\chi)\pi^{w-s+\frac{1}{2}} N^{-w}} \frac{\Gamma(s - \frac{1}{2}) \Gamma(s - w) \Gamma(s + w - 1) L_f(s - w + 1, \chi) L_f(\bar{w} + s)}{\Gamma(2s - 1) \Gamma(\bar{w})}.$$

**Proof.** We can evaluate $\langle D(z, s, \chi), E_{i\infty}(z, w, \chi) \rangle$ by unfolding $D(z, s, \chi)$:

$$\langle D(z, s, \chi), E_{i\infty}(z, w, \chi) \rangle = \int_{\Gamma_0(N) \backslash \mathbb{H}} \chi(\gamma) A(\gamma z) \Im(\gamma z) E(\gamma z, w, \chi) \frac{dx}{y^2}$$

$$= \int_0^{\infty} \int_0^{\infty} \sum_{n \geq 1} \frac{a_n}{n} e^{2\pi ny} e^{-2\pi ny} y^s \left( 2y^w L(2w, \chi) + \frac{4\pi^w \tau(\chi)}{N^{2w} \Gamma(w)} \sqrt{y} \sum_{n \neq 0} |n|^\frac{1}{2-w} \sigma_{2w-1}(n, \chi) K_{w-\frac{1}{2}}(2\pi|n|y) e^{2\pi ny} \right)^* \frac{dx dy}{y^2}.$$
CHAPTER 2. FOURIER EXPANSIONS FOR EISENSTEIN SERIES TWISTED BY MODULAR SYMBOLS

where \((\ldots)^\ast\) means the complex conjugate of \((\ldots)\). Integrating in \(x\) we get

\[
= \int_0^\infty \sum_{n=1}^{\infty} \frac{a_n e^{-2\pi n y^-2}}{n} \frac{4 \pi \tau'(\chi)}{N \Gamma(\bar{w})} \sqrt{y n \frac{1}{2}} \sum_{d|n} \chi(d) d^{2\bar{w}-1} \int_0^\infty \exp \left(-\pi n y(u + u^{-1})\right) u^{\bar{w}-\frac{1}{2}} du dy
\]

\[
= \frac{2 \pi \tau'(\chi)}{N \Gamma(\bar{w})} \sum_{n=1}^{\infty} a_n n^{-\frac{1}{2}} \sum_{d|n} \chi(d) d^{2\bar{w}-1} \int_0^\infty \int_0^\infty \exp \left(-\pi n y(u + u^{-1} + 2)\right) y^{s-\frac{1}{2}} u^{\bar{w}-\frac{1}{2}} du dy.
\]

Integrating in \(y\), this becomes

\[
= \frac{2 \pi \tau'(\chi)}{N \Gamma(\bar{w})} \sum_{n=1}^{\infty} a_n n^{-\frac{1}{2}} \sum_{d|n} \chi(d) d^{2\bar{w}-1} \int_0^\infty \frac{\Gamma(s - \frac{1}{2})}{(n \pi (u + u^{-1} + 2)) s^{\frac{1}{2}}} u^{\bar{w}-\frac{1}{2}} du.
\]

The integral in \(u\) can be evaluated with Mathematica. The expression becomes

\[
2 \pi \tau'(\chi) N^{-2\bar{w}} \frac{\Gamma(s - \frac{1}{2}) \Gamma(s - \bar{w}) \Gamma(s + \bar{w} - 1)}{\Gamma(\bar{w}) \Gamma(2s - 1)} \sum_{n=1}^{\infty} a_n n^{-\frac{1}{2}} \sum_{d|n} \chi(d) d^{2\bar{w}-1}.
\]

The sums can be rewritten as

\[
\sum_{d=1}^{\infty} \sum_{m=1}^{\infty} a(md) \chi(d) d^{2\bar{w}-1} (md)^{-s-\bar{w}} = \sum_{d=1}^{\infty} \sum_{m=1}^{\infty} a(md) \chi(d) d^{2\bar{w}-1} m^{-s-\bar{w}}.
\]

Consider the expression

\[
\sum_{d=1}^{\infty} \sum_{m=1}^{\infty} \chi(d) d^{2\bar{w}+m^{z_2} a(m)a(d).
\]

Using the Hecke relations this becomes

\[
\sum_{d=1}^{\infty} \sum_{m=1}^{\infty} \chi(d) d^{2\bar{w}+m^{z_2}} \sum_{r} \left(\frac{md}{r^2}\right).
\]

Bringing the \(r\) sum out turns this into

\[
\sum_{r=1}^{\infty} \sum_{d=1}^{\infty} \sum_{m=1}^{\infty} \chi(r) r^{1+z_1+z_2} \chi(d) d^{2\bar{w}+m^{z_2}} a(md),
\]

and so

\[
\sum_{d=1}^{\infty} \sum_{m=1}^{\infty} \chi(d) d^{2\bar{w}+m^{z_2}} a(md) = \sum_{r=1}^{\infty} \sum_{d=1}^{\infty} \sum_{m=1}^{\infty} \chi(r) r^{1+z_1+z_2} \chi(d) d^{2\bar{w}+m^{z_2}} a(md).
\]

These are \(L\)-functions. Substituting \(z_1 = \bar{w} - s - 1, z_2 = -\bar{w} - s\) we get

\[
\sum_{d=1}^{\infty} \sum_{m=1}^{\infty} a(md) \chi(d) d^{\bar{w}-s-1} m^{-s-\bar{w}} = \frac{L_f(s - \bar{w} + 1, \chi) L_f(\bar{w} + s)}{L(2s, \chi)}.
\]

Substituting this into our expression from earlier yields

\[
\langle D(\ast, s, \chi), E_{i\infty}(\ast, w, \chi) \rangle = \frac{2 \pi \tau'(\chi) N^{-2\bar{w}} \frac{\Gamma(s - \frac{1}{2}) \Gamma(s - \bar{w}) \Gamma(s + \bar{w} - 1) L_f(s - \bar{w} + 1, \chi) L_f(\bar{w} + s)}{\Gamma(2s - 1) \Gamma(\bar{w})} \frac{L(2s, \chi)}{L(2s, \chi)}.
\]
Lemma 2.1.5. The inner product of \( D(z, s, \chi) \) with the Eisenstein series \( E_0(z, s, \chi) \) is given by

\[
\langle D(*, s, \chi), E_0(*, w, \chi) \rangle = 2\pi^{-s+1}N^{-\overline{w}} \frac{\Gamma\left(s - \frac{1}{2}\right)\Gamma(s - w)\Gamma(s + \overline{w} - 1)}{\Gamma(2s - 1)} \frac{L_f(s + \overline{w}, \overline{\chi})L_f(1 - \overline{w} + s)}{L(2s, \overline{\chi})}.
\]

Proof. The computation of \( \langle D(*, s, \chi), E_0(*, w, \chi) \rangle \) is very similar to that of \( \langle D(*, s, \chi), E_{1\infty}(*, w, \chi) \rangle \):

\[
\langle D(*, s, \chi), E_0(*, w, \chi) \rangle = \int_0^\infty \int_0^\infty \sum_{n=1}^\infty \frac{a_n}{n} e^{2\pi inx} e^{-2\pi nuy} \left( 2\pi(\chi)\pi^{2w-1}\Gamma(1-w) \right) \frac{y^{1-w}L(2-2w, \overline{\chi})}{N^{w-\frac{1}{2}}\sqrt{\pi}n^{w-\frac{1}{2}}\sigma_{1-2w}(n, \chi)K_{w-\frac{1}{2}}(2\pi|n|y)\pi^{2\pi inx}} \ dx dy,
\]

again using (...)* to denote the complex conjugate of (...). Integrating in \( x \):

\[
= \int_0^\infty \sum_{n=1}^\infty \frac{a_n}{n} e^{-2\pi ny} y^{-\frac{1}{2}} \frac{4\pi^{\overline{w}}}{N^{w-\overline{w}}\Gamma(\overline{w})} n^{-\frac{1}{2}} \sum_{d|n} \overline{\chi}(d)d^{1-2\overline{w}} \int_0^\infty \exp(-\pi ny(u + u^{-1})) \overline{u}^{-\frac{1}{2}} du \ dy
\]

\[
= \frac{2\pi^{\overline{w}}}{N^{w-\overline{w}}\Gamma(\overline{w})} \sum_{n=1}^\infty a_n n^{-\frac{1}{2}} \sum_{d|n} \overline{\chi}(d)d^{1-2\overline{w}} \int_0^\infty \int_0^\infty \exp(-\pi ny(u + u^{-1} + 2)) y^{-\frac{1}{2}} u^{-\frac{1}{2}} du \ dy.
\]

These integrals are identical to the ones that appear in the computation of \( \langle D, E_{1\infty} \rangle \). The expression becomes

\[
= 2\pi^{-s+1}N^{-\overline{w}} \frac{\Gamma\left(s - \frac{1}{2}\right)\Gamma(s - w)\Gamma(s + \overline{w} - 1)}{\Gamma(2s - 1)} \sum_{n=1}^\infty a_n n^{-s-1} \sum_{d|n} \overline{\chi}(d)d^{1-2\overline{w}}.
\]

The sums are the same as the ones that appeared in the previous computation, but with \( \overline{w} \) replaced with \( 1 - \overline{w} \) and \( \chi \) replaced with \( \overline{\chi} \). Hence

\[
\langle D(*, s, \chi), E_0(*, w, \chi) \rangle = 2\pi^{-s+1}N^{-\overline{w}} \frac{\Gamma\left(s - \frac{1}{2}\right)\Gamma(s - w)\Gamma(s + \overline{w} - 1)}{\Gamma(2s - 1)} \frac{L_f(s + \overline{w}, \overline{\chi})L_f(1 - \overline{w} + s)}{L(2s, \overline{\chi})}.
\]

We can now prove theorem 1.1.1.

Proof of theorem 1.1.1. We compute directly:

\[
\int_0^1 E^*(x + iy, s, \chi) \ dx
\]

\[
= \int_0^1 D(x + iy, s, \chi) - A(x + iy)E(x + iy, s, \chi) \ dx
\]

\[
= \int_0^1 \left( \sum_j \frac{\langle D(*, s, \chi), M_j \rangle}{\langle M_j, M_j \rangle} M_j(x + iy) + \frac{1}{4\pi i} \sum_a \int_{\ell(\frac{1}{2})} \langle D(*, s, \chi), E_a(*, w, \chi) \rangle E_a(x + iy, w, \chi) \ dw \right) \ dx
\]

\[
- \int_0^1 A(x + iy)E(x + iy, s, \chi) \ dx.
\]
Similarly, the contribution from the Maass forms have no constant term, so they won’t contribute to the expression at hand. Using lemmas 2.1.2, 2.1.4, and 2.1.5 then gives

\[
\frac{1}{4\pi i} \int \left( \frac{1}{4} \right) 2\pi(s) \pi^{w-s+\frac{1}{2}} N^{-\frac{1}{2} w} \frac{\Gamma(s) \Gamma(s-w-1) L_f(s-w+1, \chi) L_f(s)}{\Gamma(2s-1) \Gamma(w)} \cdot 2y^w dw
\]

\[
\frac{1}{4\pi i} \int \left( \frac{1}{4} \right) 2\pi^{w-s+\frac{3}{2}} N^{2 w} \frac{\Gamma(s) \Gamma(s-w) \Gamma(s-w-1) L_f(s-w, \chi) L_f(s-w+1, \chi) \cdot 2\pi(\chi) \pi^{2w-1} \Gamma(1-w)}{N^{1-3w} \Gamma(w)} y^{1-w} dw.
\]

\[-\sum_{m=1}^{\infty} a_m e^{-2\pi my} 4\pi^s \tau(\chi) \frac{N^{2s} \Gamma(s) L(2s, \chi)}{y^{\frac{1}{2} m^{\frac{1}{2} - s} \sigma_{2s-1}(m, \chi) K(s, \chi) 2\pi my)}
\]

Note that \( \bar{w} = 1 - w \) on the line \( \text{Re}(w) = \frac{1}{2} \). Making this substitution and cleaning up a bit yields

\[
\frac{1}{4\pi i} \int \left( \frac{1}{4} \right) 2\pi(s) \pi^{1-w-s+\frac{1}{2}} N^{2 w-2} \frac{\Gamma(s) \Gamma(s+w) \Gamma(s+w-1) L_f(s+w, \chi) L_f(s+w+1, \chi) \cdot 2y^w dw}
\]

\[
\frac{1}{4\pi i} \int \left( \frac{1}{4} \right) 2\pi(s) \pi^{w-s+\frac{3}{2}} N^{2 w} \frac{\Gamma(s) \Gamma(s-w) \Gamma(s-w-1) L_f(s-w, \chi) L_f(s-w+1, \chi) \cdot 2\pi(\chi) \pi^{2w-1} \Gamma(1-w)}{N^{1-3w} \Gamma(w)} y^{1-w} dw.
\]

\[-\sum_{m=1}^{\infty} a_m e^{-2\pi my} 4\pi^s \tau(\chi) \frac{N^{2s} \Gamma(s) L(2s, \chi)}{y^{\frac{1}{2} m^{\frac{1}{2} - s} \sigma_{2s-1}(m, \chi) K(s, \chi) 2\pi my)}.
\]

From [22] we know that the constant term of \( E^*(z, s, \chi) \) is of the form \( \phi^*_\chi(s) y^{1-s} \). Therefore

\[
\phi^*_\chi(s) = \lim_{y \to \infty} y^{s-1} \int_0^1 E^*(x + iy, s, \chi) dx.
\]

As \( y \) goes to infinity, the contribution from \( A(z)E(z, s, \chi) \), the term in the last line, vanishes, because the \( K \)-Bessel functions have exponential decay in \( y \).

The contribution from \( E_{i\infty}(z, s, \chi) \) on the first line can be evaluated by shifting the contour to the left. There are poles whenever \( w = 1 - s - n \) for \( n \) a non-negative integer. After taking the above limit, the only term that will survive is when \( w = 1 - s \), which has residue

\[
2\pi i \cdot -i\tau(\chi)L_f(1, \chi) \pi^{-\frac{1}{2} s} N^{-2s} \frac{\Gamma(s) \Gamma(2s) L_f(2s)}{\Gamma(s)} y^{1-s}.
\]

Similarly, the contribution from \( E_0(z, s, \chi) \) can be evaluated by shifting the integral in the second line to the right. The only residue which will contribute after the limit in \( y \) is when \( w = s \), and is equal to

\[
-2\pi i \cdot -i\tau(\chi)L_f(1, \chi) \pi^{-\frac{1}{2} s} N^{-2s} \frac{\Gamma(s) \Gamma(2s) L_f(2s)}{\Gamma(s)} y^{1-s}.
\]
CHAPTER 2. FOURIER EXPANSIONS FOR EISENSTEIN SERIES TWISTED BY MODULAR SYMBOLS

From this we can conclude that for any $y$, we have

$$
\int_0^1 E^*(x + iy, s, \chi) \, dx = \left( 2\tau(\chi) L_f(1, \chi) \pi^{\frac{3}{2}} N^{-2s} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \frac{L_f(2s)}{L(2s, \chi)} \right. \\
\left. - 2\tau(\chi) L_f(1, \chi) \pi^{\frac{3}{2}} N^{-2s} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \frac{L_f(2s)}{L(2s, \chi)} \right) y^{1-s}.
$$

We can also prove theorem 1.1.2 in a similar way.

Proof of theorem 1.1.2. We compute directly:

$$
\int_0^1 E^*(x + iy, s, \chi)e^{-2\pi i nx} \, dx \\
= \int_0^1 (D(x + iy, s, \chi) - A(x + iy)E(x + iy, s, \chi))e^{-2\pi i nx} \, dx \\
= \int_0^1 \left( \sum_j \frac{\langle D(s, s, \chi), M_j \rangle}{\langle M_j, M_j \rangle} M_j(x + iy) + \frac{1}{4\pi i} \sum_a \int_{\frac{1}{2}}(D(s, s, \chi), E_a(s, w, \chi))E_a(x + iy, w, \chi) \, dw \right) e^{-2\pi i nx} \, dx \\
- \int_0^1 A(x + iy)E(x + iy, s, \chi)e^{-2\pi i nx} \, dx \\
= \sum_j \frac{(4\pi)^{1-s}}{2(M_j, M_j)} \frac{\Gamma(s + i\lambda_j - \frac{1}{2})}{\Gamma(s)} \frac{\Gamma(s - i\lambda_j - \frac{1}{2})}{\Gamma(s)} \frac{\Gamma(s + \frac{1}{2}, f \times M_j)}{\Gamma(s + \frac{1}{2}, f \times M_j)} \cdot c_{M_j}(n) y^{\frac{1}{2}} K_{i\lambda_j}(2\pi|n|y) \\
+ \frac{1}{4\pi i} \int_{\frac{1}{2}} \frac{4\pi^{\frac{3}{2}} \gamma(s) L_f(s - w + 1, \chi) L_f(s - \bar{w} + 1, \chi) L_f(s - \bar{w} + 1, \chi) L_f(\bar{w} + s)}{\Gamma(2s - 1) \Gamma(\bar{w})} \\
\cdot \frac{\frac{4\pi^w \tau(\chi)}{N^2 \Gamma(w) L(2w, \chi)} y^{\frac{1}{2}} |n|^{\frac{1}{2} - w} \sigma_{2w - 1}(n, \bar{w}) K_{\frac{1}{2}}(2\pi|n|y) \, dw}{
\quad \quad \\
+ \frac{1}{4\pi i} \int_{\frac{1}{2}} \frac{4\pi^{\frac{3}{2}} \gamma(s) L_f(s - w + 1, \chi) L_f(s - \bar{w} + 1, \chi) L_f(\bar{w} + s)}{\Gamma(2s - 1) \Gamma(\bar{w})} \\
\cdot \frac{\frac{4\pi^w}{N^2 \Gamma(w) L(2w, \chi)} y^{\frac{1}{2}} |n|^{\frac{1}{2} - w} \sigma_{2w - 1}(n, \bar{w}) K_{\frac{1}{2}}(2\pi|n|y) \, dw}{
\quad \quad \\
- \sum_{m=1}^\infty \frac{a_m e^{-2\pi my}}{m} \frac{4\pi^s \tau(\chi)}{N^2 \Gamma(s) L(2s, \chi)} y^{\frac{1}{2}} |n - m|^{\frac{1}{2} - s} \sigma_{2s - 1}(n - m, \chi) K_{\frac{1}{2}}(2\pi|n - m|y).}
$$
Again note that \(w = 1 - w\) on the line \(\text{Re}(w) = \frac{1}{2}\). Making this substitution and cleaning up a bit yields

\[
\sum_j \frac{(4\pi)^{1-s}}{2(M_j, M_j)} \Gamma \left( s + i\lambda_j - \frac{1}{2} \right) \Gamma \left( s - i\lambda_j - \frac{1}{2} \right) \frac{L \left( s + \frac{1}{2}, f \times M_j \right) \cdot c_{M_j}(n)y^{\frac{1}{2}} K_{i\lambda_j}(2\pi|n|y)}{\Gamma(s)} \\
+ \frac{1}{4\pi i} \int\limits_{\frac{1}{2}} 16\pi^{\frac{3}{2}-s} N^{-1} \frac{\Gamma \left( s + \frac{1}{2} \right) \Gamma(s + w - 1)\Gamma(s - w) L_f(s + w, \chi) L_f(s + 1 - w)}{\Gamma(2s - 1) \Gamma(1 - w) \Gamma(w)} \frac{L(2s, \chi) L(2w, \chi)}{L(2s, \chi)} \\
\cdot y^{\frac{1}{2}} |n|^{\frac{1}{2} - w} \sigma_{2w - 1}(n, \bar{\chi}) K_{w - \frac{1}{2}}(2\pi|n|y) \, dw \\
+ \frac{1}{4\pi i} \int\limits_{\frac{1}{2}} 16\pi^{\frac{3}{2}-s} N^{-1} \frac{\Gamma \left( s + \frac{1}{2} \right) \Gamma(s + w - 1) L_f(s + 1 - w, \bar{\chi}) L_f(s + w)}{\Gamma(2s - 1) \Gamma(1 - w) \Gamma(w)} \frac{L(2s, \bar{\chi}) L(2 - 2w, \bar{\chi})}{L(2s, \bar{\chi})} \\
\cdot y^{\frac{1}{2}} |n|^{\frac{1}{2} - 2w} \sigma_{1 - 2w}(n, \chi) K_{w - \frac{1}{2}}(2\pi|n|y) \, dw \\
- \sum_{m = 1}^{\infty} \frac{a_m e^{-2\pi my}}{m^{2s} \Gamma(s)} \frac{4\pi^s \tau(\chi)}{2^{2s} \Gamma(s) L(2s, \chi)} y^{\frac{1}{2}} |n - m|^{\frac{1}{2} - s} \sigma_{2s - 1}(n - m, \bar{\chi}) K_{s - \frac{1}{2}}(2\pi|n - m|y) \\
- \sum_{m = 1}^{\infty} \frac{a_m e^{-2\pi my}}{m^{2s} \Gamma(s)} \frac{4\pi^s \tau(\chi)}{2^{2s} \Gamma(s) L(2s, \chi)} |n - m|^{\frac{1}{2} - s} \sigma_{2s - 1}(n - m, \bar{\chi}) y^{\frac{1}{2}} K_{s - \frac{1}{2}}(2\pi|n - m|y) \\
+ \frac{2^{2s+1}\pi^{2-s}}{2\pi i \cdot N \Gamma(s)} \int\limits_{\frac{1}{2}} \frac{\Gamma(s + w - 1)\Gamma(s - w)}{\Gamma(1 - w) \Gamma(w)} L_f(s + 1 - w) \left( \frac{L_f(s + w, \chi)}{L(2s, \chi) L(2w, \chi)} \sigma_{2w - 1}(n, \bar{\chi}) - \frac{L_f(s + w, \bar{\chi})}{L(2s, \bar{\chi}) L(2w, \bar{\chi})} \sigma_{2w - 1}(n, \chi) \right) \\
\cdot |n|^{\frac{1}{2} - w} y^{\frac{1}{2}} K_{w - \frac{1}{2}}(2\pi|n|y) \, dw.
\]
CHAPTER 2. FOURIER EXPANSIONS FOR EISENSTEIN SERIES TWISTED BY MODULAR SYMBOLS

Shifting the contour to the left allows us to write the integral as a sum of residues. The expression becomes

\[
\int_0^1 E^*(x + iy, s, \chi)e^{-2\pi inx} \, dx = \sum_j \frac{(4\pi)^{1-s}}{2(M_j, M_j)} \frac{\Gamma(s + i\lambda_j - \frac{1}{2})}{\Gamma(s)} \Gamma(s - i\lambda_j - \frac{1}{2}) L\left(s + \frac{1}{2}, f \times M_j\right) \cdot c_{M_j}(n)y^{\frac{s}{2}} K_{s\lambda_j}(2\pi|y|)
\]

\[
- \sum_{m=1}^{\infty} \frac{a_m}{m} e^{-2\pi my} \frac{4\pi^s \tau(\chi)}{N^{2s} \Gamma(s)} \left|n - m\right|^{\frac{2}{2} - s} \sigma_{2s - 1}(n - m, \bar{\chi})y^{\frac{s}{2}} K_{s\frac{1}{2}}(2\pi|n - m|y)
\]

\[
+ \frac{2^{2s+1} \pi^{2-s}}{\Gamma(s)} \sum_{k=0}^{\infty} k! \Gamma(s + k) \Gamma(1 - s - k) 
\cdot \frac{L_f(1 - k, \chi)}{L(2s, \chi)L(2 - 2s - 2k, \chi)} \sigma_{1 - 2s - 2k}(n, \bar{\chi}) - \frac{L_f(1 - k, \chi)}{L(2s, \chi)L(2 - 2s - 2k, \chi)} \sigma_{1 - 2s - 2k}(n, \chi)
\]

\[
+ \frac{2^{2s-2-s}}{\Gamma(s)} \sum_{\rho : L(2\rho, \chi) = 0} \frac{\Gamma(s + \rho - 1) \Gamma(s)}{\Gamma(1 - \rho) \Gamma(\rho)} L_f(s + 1 - \rho) \frac{L_f(s + 2\rho, \chi)}{L(2s, \chi)L(2, 2\rho, \chi)} \sigma_{2\rho - 1}(n, \bar{\chi}) |n|^{\frac{2}{2} - \rho} y^{\frac{s}{2}} K_{s - \frac{1}{2}}(2\pi|n|y)
\]

\[
- \frac{2^{2s-2-s}}{\Gamma(s)} \sum_{\rho : L(2\rho, \chi) = 0} \frac{\Gamma(s + \rho - 1) \Gamma(s)}{\Gamma(1 - \rho) \Gamma(\rho)} L_f(s + 1 - \rho) \frac{L_f(s + 2\rho, \chi)}{L(2s, \chi)L(2, 2\rho, \chi)} \sigma_{2\rho - 1}(n, \bar{\chi}) |n|^{\frac{2}{2} - \rho} y^{\frac{s}{2}} K_{s - \frac{1}{2}}(2\pi|n|y).
\]

In the last and before last lines we evaluated the residues of \((L(2w, \chi))^{-1}\) under the assumption that the poles of this function are simple. If higher order poles are simple then these residues will have to be modified in a straightforward way to include higher derivatives of \((L(2w, \chi)).\) In the proof of theorem 1.1.1 we used an argument to be able to discard all but one of the terms appearing, but in the current situation no argument of that sort is immediately available to us.

\[\square\]

2.2 Applications

2.2.1 Twisted sums of modular symbols

Here we prove corollary 1.1.3 and evaluate other twisted Kloosterman sums introduced in [22].

**Proof of corollary 1.1.3.** [22] shows that, for \(\text{Re}(s) > 2\)

\[
\phi^*_\chi(s) = \sqrt{\pi} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \sum_{\gamma \in \Gamma_N \setminus \Gamma_0(N) / \Gamma_\infty} \frac{\chi(\gamma)\langle \gamma, f \rangle}{|c|^{2s}}
\]

where \(c\) is the lower-left entry of \(\gamma\), while theorem 1.1.1 gives

\[
\phi^*_\chi(s) = 2\pi^{\frac{1}{2}} N^{-2s} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(2s)} L_f(2s) \left(\frac{\tau(\bar{\chi}) L_f(1, \chi)}{L(2s, \chi)} - \frac{\tau(\chi) L_f(1, \bar{\chi})}{L(2s, \bar{\chi})}\right)
\]

19
CHAPTER 2. FOURIER EXPANSIONS FOR EISENSTEIN SERIES TWISTED BY MODULAR SYMBOLS

for even $\chi$. Equating these two expressions yields the evaluation of the twisted sum given in corollary 1.1.3.

Similarly we can evaluate the twisted Kloosterman sums which appear in the Fourier coefficients of $E^*(z, s, \chi)$, given in [22] equation (1.3), via theorem 1.1.2. This gives, for $n \neq 0$ and for arbitrary real $y$:

$$
2\sqrt{\pi} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \sum_{\gamma \in \Gamma \setminus \Gamma_0(N)/\Gamma} \frac{\chi(\gamma, f)e^{2\pi i n \gamma}}{|s|^{\frac{1}{2}}} |n|^{\frac{1}{2}} y^{\frac{1}{2}} K_{s - \frac{1}{2}}(2\pi |n|y)
$$

$$
= \sum_{j} \frac{(4\pi)^{1-s}}{2(M_j, M_j)} \Gamma(s + i\lambda_j - \frac{1}{2}) \Gamma(s - i\lambda_j - \frac{1}{2}) L\left(s + 1, j \times M_j\right) c_{M_j}(n) y^{\frac{1}{2}} K_{i\lambda_j}(2\pi |n|y)

+ \sum_{m=1} 2^{2s+1} \pi^{-2s} \frac{\Gamma(2s + k - 1)}{\Gamma(s + k-k)} \frac{L_f(1 - k, \chi)}{L(2s, \chi)L(2 - 2s - 2k, \chi)} \sigma_{1-2s-2k}(n, \chi) - \frac{L_f(1 - k, \chi)}{L(2s, \chi)L(2 - 2s - 2k, \chi)} \sigma_{1-2s-2k}(n, \chi)

+ \frac{2^{2s+1} \pi^{-2s}}{\Gamma(s + k-k)} \sum_{\rho \in L(2s, \chi) = 0} \frac{\Gamma(s + \rho - 1)}{(1 - \rho) \Gamma(\rho)} L_f(s + 1 - \rho) \frac{L_f(s + \rho, \chi)}{L(2s, \chi)L(2 - 2s - 2k, \chi)} \sigma_{2\rho - 1}(n, \chi) |n|^{\frac{1}{2}} y^{\frac{1}{2}} K_{\rho - \frac{1}{2}}(2\pi |n|y)

- \frac{2^{2s+1} \pi^{-2s}}{\Gamma(s + k-k)} \sum_{\rho \in L(2s, \chi) = 0} \frac{\Gamma(s + \rho - 1)}{(1 - \rho) \Gamma(\rho)} L_f(s + 1 - \rho) \frac{L_f(s + \rho, \chi)}{L(2s, \chi)L(2 - 2s - 2k, \chi)} \sigma_{2\rho - 1}(n, \chi) |n|^{\frac{1}{2}} y^{\frac{1}{2}} K_{\rho - \frac{1}{2}}(2\pi |n|y).
$$

2.2.2 Distribution of modular symbols twisted by characters

It was conjectured in [9] and proved in [23] that

$$
\sum_{\gamma : |\gamma| \leq X} \langle \gamma, f \rangle \sim \text{Res}_{w=1} \ E^*(z, w) \cdot X
$$

where $|\gamma| := |cz + d|^2$. Using the Fourier expansion of $E^*(z, s, \chi)$ we can obtain similar results when the sum on the left is twisted by $\chi$:

$$
\sum_{\gamma : |\gamma| \leq \text{Im}(z)X} \chi(\gamma) \langle \gamma, f \rangle = \sum_{s : \text{poles of } E^*(z, s, \chi)} \text{Res}_{w=s} \ E^*(z, w, \chi) \cdot X^s.
$$

This sum can be evaluated using theorems 1.1.1 and 1.1.2. Because $K_{\rho}(y)$ has exponential decay in $y$ the only poles of $E^*(z, s, \chi)$ will be the poles of the individual Fourier coefficients. Via inspection of the Fourier expansions in theorems 1.1.1 and 1.1.2, we see that the main term will be $O(X^{\frac{1}{2} + \frac{1}{2} \text{Re}(\rho)})$ where $\rho$ is the
rightmost zero of $L(s, \chi)$, coming from zeroes of Dirichlet $L$-functions, and the most significant error terms will be $O(X^{\frac{1}{2}})$ and come from the Maass part of the spectral decomposition of $E^*(z, s, \chi)$. GRH implies that the main term will be of size $O(X^{\frac{1}{2}})$. It is known that $\langle \gamma, f \rangle \ll \| \gamma \|_c^3$ [23], so it is reasonable to expect that the sum above will be of size $O(X^{\frac{1}{2}+\epsilon})$. However, corollary 1.1.4 shows that, conditional on the zeroes of $L(s, \chi)$ being bounded away from the line $\text{Re}(s) = 1$, there appears to be a correlation between the values of $\chi(\gamma)$ and the values of $\langle \gamma, f \rangle$ when $\chi$ is complex, leading to less cancelation than one might expect. All the error terms can be made completely explicit, and the secondary error term is of size $O(X^{\frac{1}{4}})$.

**Proof of corollary 1.1.4.** For $\sigma > 2$ we evaluate $\int_{(\sigma)} E^*(z, s, \chi)X^s \frac{ds}{s}$ in two different ways. First, using the series expansion

$$E^*(z, s, \chi) = \sum_{\gamma \in \Gamma \setminus \Gamma_0(N)} \chi(\gamma) \langle \gamma, f \rangle \frac{\text{Im}(z)^s}{|cz + d|^{2s}}$$

we have

$$\int_{(\sigma)} E^*(z, s, \chi)X^s \frac{ds}{s} = \sum_{\gamma \in \Gamma \setminus \Gamma_0(N)} \chi(\gamma) \langle \gamma, f \rangle \int_{(\sigma)} \frac{\text{Im}(z)^s}{|cz + d|^{2s}} X^s \frac{ds}{s} = \sum_{\gamma \text{: } \text{Im}(\gamma) \leq \text{Im}(z)X} \chi(\gamma) \langle \gamma, f \rangle.$$ 

On the other hand, we can also evaluate this integral as a sum of residues at the poles of $E^*(z, s, \chi)$. Because $K_v(y)$ has exponential decay in $y$, the only poles of $E^*(z, s, \chi)$ will be the poles of its individual Fourier coefficients. Via inspection of theorems 1.1.1 and 1.1.2 we see that the rightmost poles will have real part $\frac{1}{2} + \frac{1}{2}\text{Re}(\rho)$, where $\rho$ is the rightmost zero of $L(s, \chi)$, and the next most significant poles have real part $\frac{1}{2}$. Computing the residues at the most significant poles, we obtain

$$\sum_{\gamma \text{: } \text{Im}(\gamma) \leq \text{Im}(z)X} \chi(\gamma) \langle \gamma, f \rangle$$

$$= \sum_{\rho: L(\rho, \chi) = 0} \frac{(4\pi)^{1-\frac{\rho}{2}}}{N} \frac{\Gamma(1-\rho)}{\Gamma(1-\frac{\rho}{2})^2} \frac{L_f(1, \chi)}{L(1-\rho, \chi)\Gamma(\frac{\rho}{2})} \sum_{n \neq 0} e^{2\pi inx}\sigma_\rho(n, \chi)|n|^{\frac{1-\rho}{2}} y^\frac{1}{2} K_{\frac{1}{2}+\rho}(2\pi|n|y) \cdot X^{1-\frac{\rho}{2}}$$

$$- \sum_{\rho: L(\rho, \chi) = 0} \frac{(4\pi)^{1-\frac{\rho}{2}}}{N} \frac{\Gamma(1-\rho)}{\Gamma(1-\frac{\rho}{2})^2} \frac{L_f(1, \chi)}{L(1-\rho, \chi)\Gamma(\frac{\rho}{2})} \sum_{n \neq 0} e^{2\pi inx}\sigma_\rho(n, \chi)|n|^{\frac{1-\rho}{2}} y^\frac{1}{2} K_{\frac{1}{2}+\rho}(2\pi|n|y) \cdot X^{1-\frac{\rho}{2}}$$

$$+ O(X^{\frac{1}{4}}).$$

In writing the residues in this form we are making the assumption that the zeroes of $L(s, \chi)$ are all simple. If $L(s, \chi)$ vanishes to higher order then the terms involving $L'(s, \chi)$ must be replaced with terms involving higher derivatives of $L(s, \chi)$. This change is straightforward to make, and we present the residues in this form to avoid over-encumbering the notation. Note that there are no poles coming from the trivial zeroes of $L(s, \chi)$ because of the gamma factors. \qed
2.2.3 Central values of L-functions

Lemma 2.2.1. The central value of the $L$-function can be given via

$$L_f(1, \chi) = \tau(\bar{\chi})^{-1} \sum_{a \in \mathbb{Z}/N} \bar{\chi}(a) \left\langle \begin{pmatrix} a & * \\ N & * \end{pmatrix}, \gamma \right\rangle.$$  

Proof. Via the Mellin transform, we have

$$L_f(1, \chi) = 2\pi i \int_0^{i \infty} \sum_n a_n \chi(n) e^{2\pi i n z} dz.$$  

On the other hand, we have

$$\sum_{a \in \mathbb{Z}/N} \bar{\chi}(a) \left( \begin{pmatrix} a & b \\ N & d \end{pmatrix}, \gamma \right) = \sum_n a_n \bar{\chi}(a) e^{2\pi i n z}.$$  

First we show that

$$\sum_a \int_0^{i \infty} \bar{\chi}(a) e^{2\pi i n z} dz = \tau(\chi) \int_0^{i \infty} \bar{\chi}(n) e^{2\pi i n z} dz.$$  

Substitute $w = z - \frac{a}{N}$ on the left to get

$$\sum_a \bar{\chi}(a) e^{2\pi i \frac{an}{N}} \int_0^{i \infty} e^{2\pi i n z} dz.$$  

If $n = 0 \mod N$, then both sides are zero. Assume otherwise. Now multiply by $1 = \bar{\chi}(n) \chi(n)$, making the sum

$$\chi(n) \sum_a \bar{\chi}(an) e^{2\pi i \frac{an}{N}} \int_0^{i \infty} e^{2\pi i n z} dz.$$  

Substitute $b = an$. Because $N$ is prime, $n$ must be a unit mod $N$. Hence the sum still runs over $b \in \mathbb{Z}/N$. The sum becomes

$$\chi(n) \sum_b \bar{\chi}(b) e^{2\pi i \frac{b}{N}} \int_0^{i \infty} e^{2\pi i n z} dz,$$

which is exactly $\tau(\bar{\chi}) \int_0^{i \infty} \chi(n) e^{2\pi i n z} dz$.  

Lemma 2.2.2. Let $\sigma > 2$. Then

$$L_f(1, \chi) = \frac{\int_{(\sigma)} \phi_\chi(s) (N + \varepsilon)^{2s} ds}{\tau(\bar{\chi}) \int_{(\sigma)} 2\sqrt{\pi} \Gamma(s - \frac{1}{2}) \frac{1}{\Gamma(s)} \left( N e \right)^{2s} ds}$$

for every $\varepsilon \in (0, N)$, where $\phi_\chi(s)y^{1-s}$ is the constant term of the Fourier expansion of $E^*(z, s, \chi)$. This is with the normalization that the functional equation for $L_f(s, \chi)$ is $s \mapsto 2 - s$.  

22
CHAPTER 2. FOURIER EXPANSIONS FOR EISENSTEIN SERIES TWISTED BY MODULAR SYMBOLS

Proof. From [22], we know that

$$\phi^*_c(s) = \sqrt{\pi} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \sum_{\gamma \in \Gamma_{\infty}\backslash \Gamma_0(N)/\Gamma_{\infty}} \frac{\chi(\gamma)}{|c|^{2s}} \langle \gamma, f \rangle$$

for $\text{Re}(s) > 2$, where $c$ is the lower-left entry of $\gamma$. Now note that

$$\left( \begin{array}{ccc} 1 & u \\ a & b \\ c & d \end{array} \right) \left( \begin{array}{ccc} 1 & v \\ 0 & 1 \end{array} \right) = \left( \begin{array}{ccc} * & * \\ c & d + vc \end{array} \right).$$

Hence the double cosets $\Gamma_\infty \backslash \Gamma_0(N)/\Gamma_\infty$ are in bijection with pairs $(c, d)$ where $N \mid c$ and $0 \leq d < |c|$ when $c \neq 0$. In particular, we can write

$$\phi^*_\chi(s) = \sqrt{\pi} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \left[ \frac{2}{N^{2s}} \sum_{0 \leq d < N} \bar{\chi}(d^{-1}) \langle \left( \frac{\ast}{N}, d^{-1} \right), f \rangle + \sum_{|c| \geq 2N} \frac{1}{|c|^{2s}} \sum_{0 \leq d < c} \chi(d) \langle \left( \frac{\ast}{d} \right), f \rangle \right].$$

Here $d^{-1}$ is the inverse of $d$ mod $N$, which is the upper left entry of $\gamma$, so the first sum is the quantity we’re trying to evaluate.

Using this expression we see that

$$\int_{(\sigma)} \phi^*_\chi(s)(N + \epsilon)^{2s} ds = \sum_{\gamma \in \Gamma_{\infty}\backslash \Gamma_0(N)/\Gamma_{\infty}} \chi(\gamma) \langle \gamma, f \rangle \int_{(\sigma)} \sqrt{\pi} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \left( \frac{N + \epsilon}{|c|} \right)^{2s} ds,$$

where $\sigma$ is sufficiently large for the series representations to hold. When $|c| > N$, the contour can be shifted right and the integral vanishes. This gives

$$\sum_{0 \leq a < N} \bar{\chi}(a) \langle \left( \frac{\ast}{N}, a \right), f \rangle = \int_{(\sigma)} \phi^*_\chi(s)(N + \epsilon)^{2s} ds \int_{(\sigma)} 2\sqrt{\pi} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \left( \frac{N + \epsilon}{N} \right)^{2s} ds.$$

The result then follows from lemma 2.2.1. \qed

Note that similar expressions can be obtained by truncating at $c \leq \ell N$ for any positive integer $\ell$, not just the $\ell = 1$ case as done here. Doing this for $\ell \geq 2$ and using theorem 1.1.1, one obtains for any $\epsilon \in (0, 1)$

$$L_f(1, \chi) = \frac{\sum_{k=2}^{\ell} \sum_{0 \leq d < kN \atop (d, kN) = 1} \chi(d) \langle \left( \frac{\ast}{kN}, d \right) \rangle \int_{(\sigma)} \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \left( \frac{\ell + \epsilon}{k} \right)^{2s} ds}{\tau(\chi) \int_{(\sigma)} \left( 2L_f(2s) \left( \frac{L(2 - 2s, \chi)}{L(2s, \chi)} + \frac{L(2 - 2s, \bar{\chi})}{L(2s, \bar{\chi})} \right) - 1 \right) \frac{\Gamma(s - \frac{1}{2})}{\Gamma(s)} \left( \ell + \epsilon \right)^{2s} ds}.$$
CHAPTER 2. FOURIER EXPANSIONS FOR EISENSTEIN SERIES TWISTED BY MODULAR SYMBOLS

Lemma 2.2.3. For even $\chi$, the constant terms of $E^*(z, s, \chi)$ and $E^*(z, s, \bar{\chi})$ are related via the identity

$$\phi^*_\chi(s) = -\phi^*_{\bar{\chi}}(s).$$

Proof. This follows from inspection of theorem 1.1.1, but we present a different proof here which does not require us to compute the constant term of the Fourier expansion of $E^*(z, s, \chi)$.

Starting from the double coset decomposition from [22], we have

$$\phi^*_\chi(s) = \sum_{\gamma \in \Gamma_\infty \setminus \Gamma_0(N)/\Gamma_\infty} \frac{\chi(\gamma)\langle \gamma, f \rangle}{|c(\gamma)|^{2s}}$$

$$= \sum_{\gamma \in \Gamma_\infty \setminus \Gamma_0(N)/\Gamma_\infty} \frac{\chi(\gamma^{-1})\langle \gamma^{-1}, f \rangle}{|c(\gamma^{-1})|^{2s}}.$$ 

Since $c(\gamma) = -c(\gamma^{-1})$ the denominator is invariant. Thus the sum becomes

$$= \sum_{\gamma \in \Gamma_\infty \setminus \Gamma_0(N)/\Gamma_\infty} \frac{\bar{\chi}(\gamma)\langle \gamma^{-1}, f \rangle}{|c(\gamma)|^{2s}}.$$ 

To complete the proof of the lemma, we check that

$$\langle \gamma^{-1}, f \rangle = 2\pi i \int_{\gamma^{-1}\tau} f(w)dw$$

$$= 2\pi i \int_{\gamma^{-1}\tau} f(w)dw$$

$$= 2\pi i \int_{\gamma\tau} f(w)dw$$

$$= -2\pi i \int_{\gamma\tau} f(w)dw = -\langle \gamma, f \rangle.$$ 

Note that a similar argument can be made for higher powers of modular symbols.

Theorem 1.1.5 is a direct consequence of lemmas 2.2.2 and 2.2.3.
Chapter 3

The distribution of multiples of real points on an elliptic curve

3.1 Background

Let \( E : y^2 = 4x^3 - g_2x - g_3 \) be an elliptic curve with \( g_2, g_3 \in \mathbb{R} \), and periods \( \omega_1 \) and \( \omega_2 \), chosen such that \( \omega_1 \in \mathbb{R}_{>0} \) and \( \text{Im}(\omega_2) > 0 \). Let \( \Lambda \) be the \( \mathbb{C} \)-lattice with basis \( \langle 1, \frac{\omega_2}{\omega_1} \rangle \). Then \( E/\mathbb{C} \) is parameterized by elements \( z \) of \( \mathbb{C}/\Lambda \) via \( z \mapsto (\omega_1^{-2} \wp(\frac{z}{\omega_1}), \omega_1^{-3} \wp'(\frac{z}{\omega_1})) \), where

\[
\wp(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda, \lambda \neq 0} \left( \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right).
\]

This map is an isomorphism of groups and complex analytic varieties between \( \mathbb{C}/\Lambda \) and \( E/\mathbb{C} \). This is a different normalization of the parameterization \( \mathbb{C}/\Lambda \to E(\mathbb{C}) \) given in the introduction.

The function \( \wp \) is called the Weierstrass-\( \wp \) function, and is discussed at length in [27] and [5]. This function is meromorphic and periodic modulo \( \Lambda \), so \( \wp(z) \) can only be real when \( z \) either has imaginary part 0 or \( \frac{1}{2} \text{Im}(\omega_2/\omega_1) \) modulo \( \Lambda \). Furthermore, if \( z \) has imaginary part \( \frac{1}{2} \text{Im}(\omega_2/\omega_1) \), then \( \wp(z) \) will be real if and only if choosing \( \omega_1 \) to be real forces \( \omega_2 \) to be pure imaginary, in which case \( \Lambda \) is said to be "rectangular".

The function \( \wp(z) \) has a pole of order 2 when \( z \in \Lambda \) and has no other poles. From this it follows that the set of \( z \in \mathbb{C}/\Lambda \) which have imaginary part 0 modulo \( \Lambda \) maps to the unbounded component of \( E(\mathbb{R}) \), and, if \( \Lambda \) is rectangular, the set of \( z \in \mathbb{C}/\Lambda \) which have imaginary part \( \frac{1}{2} \text{Im}(\omega_2/\omega_1) \) modulo \( \Lambda \) maps to the bounded component of \( E(\mathbb{R}) \). If \( z_P \) has imaginary part \( \frac{1}{2} \text{Im}(\omega_2/\omega_1) \), then \( n z_P \) will as well exactly when \( n \) is
odd, and thus the $x$ and $y$ coordinates of $nP$ will be on the bounded component of $E(\mathbb{R})$ exactly when $n$ is odd.

For a real number $r$, let $\{r\}$ denote the distance from $r$ to the nearest integer. If $x(nP)$ and $y(nP)$ denote the $x$ and $y$ coordinates of $nP$ respectively, then, because $\wp(z)$ has a pole of order 2 when $z \in \Lambda$, we have

$$x(nP) \approx \omega_1^{-2} \left\{ \frac{n z_p}{\omega_1} \right\}^{-2} \quad \text{and} \quad y(nP) \approx -2\omega_1^{-3} \left\{ \frac{n z_p}{\omega_1} \right\}^{-3}$$

when $z_p$ is real modulo $\Lambda$ and $\left\{ \frac{n z_p}{\omega_1} \right\}$ is small.

The following lemmas will be useful for studying $\left\{ n \frac{z_p}{\omega_1} \right\}$:

**Lemma 3.1.1. (Hurwitz)** For all irrational $\alpha$ there exist infinitely many pairs of integers $(m, n)$ such that

$$\left| \alpha - \frac{m}{n} \right| < \frac{1}{\sqrt{5}n^2}.$$  

*Proof.* See [15]. \hfill \Box

**Lemma 3.1.2. (Dirichlet)** Let $\alpha_1, \ldots, \alpha_k$ be irrational numbers. For any natural number $N$ there exists an $n < N$ such that

$$\left\{ n \alpha_j \right\} < \frac{1}{N^\frac{k}{2}}$$

for all $j \in \{1, 2, \ldots, k\}$.

*Proof.* See [12], theorem 200. \hfill \Box

**Lemma 3.1.3. (Khinchin)** Let $f$ be a function from $\mathbb{N}$ to $\mathbb{R}_{>0}$. If $\sum_{n=1}^{\infty} f(n)^{-1}$ diverges, then for all real numbers $\alpha$ except for a set of Lebesgue measure zero, there exist infinitely many pairs of integers $(m, n)$ such that

$$\left| \alpha - \frac{m}{n} \right| < \frac{1}{nf(n)}.$$  

while if $\sum_{n=1}^{\infty} f(n)^{-1}$ converges, then the set of real numbers $\alpha$ for which there exist infinitely many pairs of integers $(m, n)$ such that

$$\left| \alpha - \frac{m}{n} \right| < \frac{1}{nf(n)}$$

has Lebesgue measure zero.

*Proof.* See [17]. \hfill \Box

In the opposite direction, we have the following:
Lemma 3.1.4. For any function \( f(n) : \mathbb{N} \to \mathbb{R}_{>0} \), there exists a real number \( \alpha \) such that the inequality

\[
|\alpha - \frac{m}{n}| < \frac{1}{nf(n)}
\]

is satisfied for infinitely many pairs of integers \((m, n)\).

**Proof.** See [16].

### 3.2 Growth Rates

Using lemmas 3.1.1, 3.1.2, 3.1.3, and 3.1.4 we can now prove theorems 1.2.1, 1.2.5, 1.2.3, and 1.2.4.

**Proof of theorem 1.2.1.** First suppose that \( P \) is a point of infinite order on the unbounded component of \( E(\mathbb{R}) \), and let \( z_P \) be the preimage of \( P \) under the parameterization \( \mathbb{C}/\Lambda \to E(\mathbb{C}) \) defined by \( z \mapsto (\omega^{-2} \wp\left( \frac{z}{\omega} \right), \omega^{-3} \wp'\left( \frac{z}{\omega} \right) ) \), where \( \Lambda \) is the \( \mathbb{C} \) lattice with basis \((1, \frac{\omega}{\omega_1})\). Then \( z_P \) is real modulo \( \Lambda \). When \( \left\{ \frac{n z_P}{\omega_1} \right\} \) is small we have

\[
\varphi\left( \frac{n z_P}{\omega_1} \right) = \left\{ \frac{n z_P}{\omega_1} \right\}^{-2} + \mathcal{O}\left( \left\{ \frac{n z_P}{\omega_1} \right\}^{2} \right)
\]

and

\[
\varphi'\left( \frac{n z_P}{\omega_1} \right) = -2 \left\{ \frac{n z_P}{\omega_1} \right\}^{-3} + \mathcal{O}\left( \left\{ \frac{n z_P}{\omega_1} \right\} \right),
\]

where the implied constant depends only on \( E \). Lemma 3.1.1 implies that the inequality \( \left\{ \frac{n z_P}{\omega_1} \right\} < \frac{1}{\sqrt{5n}} \) holds for infinitely many \( n \), so for these \( n \) we have

\[
\varphi\left( \frac{n z_P}{\omega_1} \right) > 5n^2 + \mathcal{O}(n^{-2}),
\]

and

\[
\varphi'\left( \frac{n z_P}{\omega_1} \right) > 2 \cdot 5^{\frac{3}{2}} n^3 + \mathcal{O}(n^{-1}).
\]

Now if instead \( P \) is on the bounded component of \( E(\mathbb{R}) \), then \( 2z_P \) is real modulo \( \Lambda \), so the argument above can be applied to \( 2P \).

Repeating this argument and using lemma 3.1.2 in the case where \( k = 2, \alpha_1 = \text{Re}(z_P), \) and \( \alpha_2 = \text{Im}(z_P) \) proves theorem 1.2.5. Repeating the argument and using lemma 3.1.3 instead of lemma 3.1.1 proves theorem 1.2.3. Finally, using lemma 3.1.4 in this argument proves theorem 1.2.4.
CHAPTER 3. THE DISTRIBUTION OF MULTIPLES OF REAL POINTS ON AN ELLIPTIC CURVE

3.3 Distributions

Next we turn our attention to results about the full distribution of $x(nP)$ and $y(nP)$ as $n$ varies. Let $X$ be a topological space with a measure $\mu$. We say that a sequence $(a_n)$ of elements of $X$ is equidistributed with respect to $\mu$ if and only if, for every function $f : X \to \mathbb{C}$, we have

$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} f(a_k) = \int_X f(x) \, d\mu.$$ 

Sometimes we will say that a sequence is equidistributed in a space if it’s clear what the associated measure is.

The following result, due Weyl [28], is an important tool for proving that certain sequences are equidistributed modulo 1:

**Lemma 3.3.1. (Weyl’s criterion)** A sequence $(a_n)$ of real numbers is equidistributed modulo 1 if and only if for every nonzero integer $\ell$ we have

$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \exp(2\pi i \ell a_k) = 0.$$ 

This lemma implies that, for any irrational $\alpha$, the sequence $a_n = \{n\alpha\}$ is equidistributed modulo 1 ([28], Satz 2). Theorem 1.2.6 is an immediate consequence of this fact.

One simple application of theorem 1.2.6 comes from taking $U = [X, \infty] \times \mathbb{R}$ for large $X$ or $U = \mathbb{R} \times [Y, \infty]$ for large $Y$. Then, if $P$ is on the unbounded component of $E(\mathbb{R})$, we have

$$\lim_{n \to \infty} \frac{1}{2n} \# \{ |k| < n : x(kP) > X \} = \frac{2}{\omega_1} X^{-\frac{3}{2}} + O(X^{-\frac{5}{2}})$$

and

$$\lim_{n \to \infty} \frac{1}{2n} \# \{ |k| < n : y(kP) > Y \} = \frac{2^4}{\omega_1} Y^{-\frac{3}{2}} + O(Y^{-\frac{5}{2}}),$$

where the implied constant depends only on $E$.

We now move to discussion of corollary 1.2.7. This corollary is useful because it gives a description of the distribution of $nP$ in a way which does not depend on knowledge of the function $\varphi$.

**Proof of corollary 1.2.7.** Let $z_0$ be the preimage of $P_0$ under the map $z \mapsto (\varphi(z), \varphi'(z))$, and let $\Delta u$ be a real number. Then

$$(\varphi(z_0 + \Delta u), \varphi'(z_0 + \Delta u)) = \left( \varphi(z_0) + \varphi'(z_0)\Delta u + O((\Delta u)^2), \ \varphi'(z_0) + \varphi''(z_0)\Delta u + O((\Delta u)^2) \right).$$
CHAPTER 3. THE DISTRIBUTION OF MULTIPLES OF REAL POINTS ON AN ELLIPTIC CURVE

Here the implied constant depends on both $E$ and $P_0$. From the equation of $E$ we can deduce that $\psi''(z_0) = 6\psi(z_0)^2 - 2z_0$. Using this fact and the preceding equation, we see that the point $(\psi(z_0 + \Delta u), \psi'(z_0 + \Delta u))$ will satisfy $(\psi(z_0 + \Delta u) - x_0)^2 + (\psi'(z_0 + \Delta u) - y_0)^2 < \varepsilon^2$ if and only if

$$|\Delta u| < \frac{\varepsilon}{\sqrt{y_0^2 + (6x_0^2 - z_0^2/2)^2}} \left( 1 - (\psi'(z_0) + \psi''(z_0))\frac{O((\Delta u)^3)}{\varepsilon^2} \right).$$

Then, after using theorem 1.2.6 and noting that $O((\Delta u)^3)\varepsilon^{-2} = O(\varepsilon)$, we can conclude the result.

The question of how quickly the set of multiples $nP$ will converge to the limiting density has been studied extensively in the theory of Diophantine approximation. See [18] chapter 2, section 3 for an overview. For a point $P$ and an open set $U \subseteq \mathbb{R}^2$, let $r : \mathbb{Z}_{>0} \to \mathbb{R}$ be the function which satisfies

$$\{ |k| < n : kP \in U \} = \rho n + r(n),$$

where $\rho$ is the natural density of multiples of $P$ which lie in the set $U$, as given by corollary 1.2.7. Then, for general $P$, it is not possible to give a better bound on $r(n)$ than $o(n)$, but for all but a set of points $P$ of measure 0, we have $r(n) = O(n^{1/2+\varepsilon})$ for every $\varepsilon > 0$.

### 3.4 Spacing

We can also study the statistics of the distances between the points $nP$ and $nP+Q$ for any fixed $Q$ in $E(\mathbb{R})$. The raw moments of the distribution of distances diverge as more and more multiples of a fixed point $P$ are taken, as described in corollary 3.4.1, and an upper bound for their growth in the number of multiples taken is given in corollary 3.4.2. We can, however, still find a distribution for these differences, as done in corollary 1.2.9.

**Corollary 3.4.1.** For any points $P$ and $Q$ in $E(\mathbb{R})$, and any positive integers $\ell$ and $r$, the limits

$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \left( x(kP + Q) - x(kP) \right)^\ell \quad \text{and} \quad \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} \left( y(kP + Q) - y(kP) \right)^r$$

diverge.

**Proof.** Suppose these limits did converge. Let $z_P$ and $z_Q$ be the preimages of $P$ and $Q$ under the parameterization $z \mapsto (\psi(z), \psi'(z))$. Let $\omega_1$ and $\omega_2$ be the periods of $E/\mathbb{C}$, chosen such that $\omega_1 \in \mathbb{R}_{>0}$ and $\text{Im}(\omega_2) > 0$. Let $\Lambda$ be the $\mathbb{C}$-lattice with basis $\langle \omega_1, \omega_2 \rangle$. Define $I_P \subset \mathbb{C}/\Lambda$ as follows:

$$I_P := \begin{cases} [0, \omega_1], & \text{Im}(z_P) = 0 \mod \Lambda, \\ [0, \omega_1] \cup ([0, \omega_1] + \frac{\omega_2}{2}), & \text{Im}(z_P) = \text{Im}(\frac{\omega_2}{2}) \mod \Lambda, \end{cases}$$

29
where \([0, \omega_1]\) denotes the interval of real numbers. Then theorem 1.2.6 implies that these limits would be equal to
\[
\frac{1}{\mu(I_P)} \int_{I_P} \left( \varphi(z + z_Q) - \varphi(z) \right)^r \, dz \quad \text{and} \quad \frac{1}{\mu(I_P)} \int_{I_P} \left( \varphi'(z + z_Q) - \varphi'(z) \right)^r \, dz,
\]
but both of these diverge because \(\varphi(z)\) has poles of order 2 at 0 and \(\omega_1\).

**Corollary 3.4.2.** Fix a point \(Q\) in \(E(\mathbb{R})\) and positive integers \(\ell\) and \(r\). Then
\[
\sum_{k=1}^{n} \left( x(kP + Q) - x(kP) \right)^r \ll n^{2r+1+\epsilon}
\]
and
\[
\sum_{k=1}^{n} \left( y(kP + Q) - y(kP) \right)^r \ll n^{3r+1+\epsilon}
\]
for all points \(P\) in \(E(\mathbb{R})\) except for a set of measure 0, and all \(\epsilon > 0\). The implied constants depend only on \(E, P,\) and \(\epsilon\).

**Proof.** Apply theorem 1.2.3 to \(f(n) = n^{1+\epsilon}\).

Using theorem 1.2.6 we can conclude immediately that, for any \(d \in \mathbb{R}\) and any \(\epsilon > 0\),
\[
\lim_{n \to \infty} \frac{1}{2n} \# \left\{ k \mid n < k : |x(nP + Q) - x(nP) - d| < \epsilon \} \right. = \frac{1}{\mu(I_P)} \mu \left( \left\{ z \in I_P : |\varphi(z + z_Q) - \varphi(z) - d| < \epsilon \right\} \right).
\]
Here we are using the notation from the proof of corollary 3.4.1 above. However, it is possible to write down the distribution of the spacings of these coordinates while avoiding making reference to the function \(\varphi(z)\). This is the content of corollary 1.2.9, which we now prove.

**Proof of corollary 1.2.9.** Given an elliptic curve \(E: y^2 = x^3 + ax + b\), a fixed point \(Q = (x_Q, y_Q) \in E(\mathbb{R})\), and a point \(P = (x_P, y_P) \in E(\mathbb{R})\) different from \(Q\), we can compute directly using the chord and tangent law for addition on \(E\) that
\[
x(P + Q) - x(P) = \left( \frac{y_P - y_Q}{x_P - x_Q} \right)^2 - 2x_P - x_Q.
\]
Fix \(d \in \mathbb{R}\) and \(\epsilon > 0\). We now wish to find the set of points \(P\) for which \(x(P + Q) - x(P) \in (d - \epsilon, d + \epsilon) \subset \mathbb{R}\). Substituting \(y_P = \pm \sqrt{x_P^3 + ax_P + b}\), the condition we’re interested in becomes
\[
\left| \left( \frac{\pm \sqrt{x_P^3 + ax_P + b} - y_Q}{x_P - x_Q} \right)^2 - 2x_P - x_Q - d \right| < \epsilon.
\]
Define
\[
F_{\pm, Q}(x) := \left( \frac{\pm \sqrt{x^3 + ax + b} - y_Q}{x - x_Q} \right)^2 - 2x - x_Q.
\]
Chapter 3. The Distribution of Multiples of Real Points on an Elliptic Curve

Let \( x_1^+, \ldots, x_{k^+}^+ \) and \( x_1^-, \ldots, x_{k^-}^- \) denote the real numbers which solve the equation \( F_{\pm, Q}(x) = d \). Then, by considering the Taylor series expansion of \( F_{\pm, Q}(x) \) around \( x_i^\pm \) for \( i = 1, \ldots, k^\pm \), we see that whenever

\[
x_i^\pm - \frac{\varepsilon}{F_{\pm, Q}(x_i^\pm)} + \mathcal{O}(\varepsilon^2) < x < x_i^\pm + \frac{\varepsilon}{F_{\pm, Q}(x_i^\pm)} + \mathcal{O}(\varepsilon^2)
\]

we will have \(|F_{\pm, Q}(x) - d| < \varepsilon\).

For any fixed \( P_0 \in E(\mathbb{R}) \) of infinite order, we can use corollary 1.2.7 to find the natural density of integers \( n \) for which \( nP_0 \) will lie in a specified open set of \( E(\mathbb{R}) \), and from this we can determine the natural density of integers \( n \) for which \( x(nP_0) \) satisfies the condition \(|F_{+, Q}(x(nP_0)) - d| < \varepsilon \) or \(|F_{-, Q}(x(nP_0)) - d| < \varepsilon \). For a fixed open interval \( I \subseteq \mathbb{R} \), the natural density of integers \( n \) for which \( x(nP_0) \in I \) is given by the expression

\[
c \int_{x \in I} \rho(x, y(x)) \sqrt{1 + y'(x)^2} \, dx,
\]

where \( c \) is a normalization constant, \( \rho(x, y(x)) \) is the density given in corollary 1.2.7, and \( y(x) = \pm\sqrt{x^3 + ax + b} \).

Now taking \( I = (x_0 - \varepsilon, x_0 + \varepsilon) \) for some \( x_0 \) which is the \( x \)-coordinate of a point in \( E(\mathbb{R}) \), we can approximate the above as

\[
c \int_{x \in I} \rho(x, y(x)) \sqrt{1 + y'(x)^2} \, dx = 2\varepsilon c \cdot \rho(x_0, y(x_0)) \sqrt{1 + y'(x_0)^2} + \mathcal{O}\left(\varepsilon^2 \left( \rho(x_0, y(x_0)) \sqrt{1 + y'(x_0)^2} \right) \right).
\]

Thus, if we define

\[
\rho(x) := \left[ \frac{1 + \frac{1}{4}(3x^2 + ax + b)^2}{4(x^3 + ax + b) + (6x^2 + \frac{a}{3})^2} \right]^{\frac{1}{2}},
\]

then, as \( n \) ranges over the integers, the values \( x(nP_0) \) will have a distribution proportional to \( \eta \cdot \rho(x) \), where \( \eta = 1 \) if \( x \) is the \( x \)-coordinate of a point in the unbounded component of \( E(\mathbb{R}) \), or \( x \) is the \( x \)-coordinate of a point in the bounded component of \( E(\mathbb{R}) \) and \( P_0 \) is in the bounded component of \( E(\mathbb{R}) \), and 0 otherwise. Hence, for fixed \( \varepsilon \), the natural density of integers \( n \) for which \( x(nP + Q) - x(nP) \in (d - \varepsilon, d + \varepsilon) \), as a function of \( d \), is proportional to

\[
\sum_{i=1}^{k^+} \rho(x_i^+) \left( (x_i^+)^3 + ax_i^+ + b \right)^{-\frac{1}{2}} + \sum_{i=1}^{k^-} \rho(x_i^-) \left( (x_i^-)^3 + ax_i^- + b \right)^{-\frac{1}{2}},
\]

where \( \sum^* \) indicates that, if \( P \) is on the unbounded component of \( E(\mathbb{R}) \), then the sum omits the \( i \) for which \( x_i^\pm \) is not the \( x \)-coordinate of any point on the unbounded component of \( E(\mathbb{R}) \).

Informally, we can view the distribution \( f(d) \) from theorem 1.2.9 as

\[
f(d) = \sum \rho\left( F_{+, Q}^{-1}(d) \right) \left( F_{+, Q}^{-1} \right)'(d) + \sum \rho\left( F_{-, Q}^{-1}(d) \right) \left( F_{-, Q}^{-1} \right)'(d),
\]
where the sums are taken over the $k^\pm$ “reasonable choices” of the pair of values $(F^{-1}_{\pm,Q}(d), (F^{-1}_{\pm,Q})'(d))$.

3.5 An equation of Bremner and Macleod

In [1], Bremner and Macleod give positive integer solutions $a, b, c$ to the equation

$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = N.$$ \hspace{1cm} (1.1)

This equation is the elliptic curve $E_N : y^2 = x^3 + (4N^2 + 12N - 3)x^2 + 32(N + 3)x$, and in the paper, the authors show that the positive integer solutions of (1.1) correspond to rational points on $E_N$ with $x$ coordinate satisfying either

$$\frac{3 - 12N - 4N^2 - (2N + 5)\sqrt{4N^2 + 4N - 15}}{2} < x < -2(N + 3) \left( N + \sqrt{N^2 - 4} \right)$$

or

$$-2(N + 3) \left( N - \sqrt{N^2 - 4} \right) < x < -\frac{4N + 3}{N + 2}.$$

Theorem 1.2.6 implies that for any $P \in E_N(\mathbb{Q})$ of infinite order on the bounded connected component of $E_N(\mathbb{R})$, the point $nP$ will correspond to a positive integer solution to (1.1) for a certain specific proportion of integers $n$ in the sense of natural density. Writing down what this specific proportion is for general $N$ can be done using corollary 1.2.7. For brevity, define

$$A := 4N^2 + 12N - 3, \quad B := 32(N + 3),$$

$$x_{1, \text{left}} := -\frac{A - 3(2N + 5)\sqrt{4N^2 + 4N - 15}}{6}, \quad x_{1, \text{right}} := -\frac{2(N + 3)(N + \sqrt{N^2 - 4}) + A}{3},$$

$$x_{2, \text{left}} := -2(N + 3)(N - \sqrt{N^2 - 4}) + \frac{A}{3}, \quad x_{2, \text{right}} := -\frac{4N + 3}{N + 2} + \frac{A}{3}.$$ 

Moreover, set

$$\rho(x) := \left[ \frac{1 + \frac{1}{4} x^3 + \frac{B - \frac{3}{4} A^2}{4}}{4x^3 + 4 \left(B - \frac{3}{4} A^2\right)x + \frac{16}{27} A^3 - \frac{3}{2} AB + (6x^2 + 2 \left(B - \frac{3}{4} A^2\right))^2} \right]^{-\frac{1}{2}}.$$ 

Then the natural density of integers $n$ for which $nP$ solves (1.1) is

$$\left( \int_{x_{1, \text{left}}}^{x_{1, \text{right}}} \rho(x) \, dx \right)^{-1} \left( \int_{x_{1, \text{left}}}^{x_{1, \text{right}}} \rho(x) \, dx + \int_{x_{2, \text{left}}}^{x_{2, \text{right}}} \rho(x) \, dx \right).$$
For $N = 4$, for example, the proportion is approximately 0.068, while for $N = 38$ the proportion is approximately 0.003. Additionally, one can use the ideas of theorem 1.2.1 to conclude that, for any $P \in E_N(Q)$ of infinite order on the bounded connected component of $E(\mathbb{R})$, the set $\{P, 2P, \ldots, nP\}$ contains a positive integer solution to (1.1) whenever $n \gg N^2$. 
Bibliography


BIBLIOGRAPHY


