DIRICHLET TWISTS OF L-FUNCTIONS OF ELLIPTIC CURVES OVER FUNCTION FIELDS

Antoine Comeau-Lapointe

A thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
For the Degree of DOCTOR OF PHILOSOPHY (Mathematics)
Concordia University
Montréal, Québec, Canada

July 2022

© Antoine Comeau-Lapointe, 2022

Concordia University
School of Graduate Studies

This is to certify that the thesis prepared

By: **Antoine Comeau-Lapointe**

Entitled: **Dirichlet Twists of L-functions of Elliptic Curves over Function Fields**

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

DOCTOR OF PHILOSOPHY (Mathematics)

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

Signed by the final examining commitee:

_____ Chair
Dr. Brigitte Jaumard

_____ External Examiner
Dr. Chris Hall

_____ Examiner
Dr. Dmitry Korotkin

_____ Examiner
Dr. Carlo Pagano

_____ Examiner
Dr. Giovanni Rosso

_____ Supervisor
Dr. Chantal David

Approved by _____
Dr. Yogen Chaubey, Graduate Program Director

August 21, 2022 _____
Dr. Pascale Sicotte, Dean
Faculty of Arts and Science

Abstract

Dirichlet Twists of L-functions of Elliptic Curves over Function Fields

Antoine Comeau-Lapointe, Ph.D.
Concordia University, 2022

Some of the most fundamental questions about L-functions are concerned with the location of their zeros, in particular at the central point, or on the critical line. Following the work of Montgomery [51], and then of Katz and Sarnak [38], number theorists have learned that it is very fruitful to study families of L-functions rather than individual L-functions. Given a family of L-functions, it is common to classify it according to its symmetry type. The symmetry type can be either symplectic, orthogonal, or unitary, which refers to the corresponding ensemble from random matrix theory that models most accurately the distribution of the zeros of the family.

This thesis presents two papers studying the zeros of the family of Dirichlet twists of the L-function of an elliptic curve E over $\mathbb{F}_q[t]$. In the first paper (Chapter 2), we show that the one-level density (the study of the low-lying zeros) for this family agrees with the conjecture of Katz and Sarnak based on random matrix theory, for test functions with limited support on the Fourier transform. For quadratic twists, the support of the Fourier transforms of the test functions is restricted to the interval $(-1, 1)$, and we observe an orthogonal symmetry. For higher order twists, the support is restricted to $(-1/2, 1/2)$ and we observe a unitary symmetry.

In the second paper (Chapter 3), we are taking the opposite point of view, and we construct certain elliptic curves over $\mathbb{F}_q[t]$ with infinitely many twists of high order vanishing at the central point, generalizing a construction of Li and Donepudi-Li [40, 24] for Dirichlet L-functions. This construction only works when $E/\mathbb{F}_q[t]$ is a constant curve. In the general case where E is not a constant curve, we performed extensive numerical computations that are compatible with the conjectures of David-Fearnley-Kisilevsky and Mazur-Rubin [18, 44] over number fields, which predict that such vanishing should be rare.

The last chapter presents an algorithm to construct the factorizations of the monic polynomials, a description of the zeros of $L(E \otimes \chi, u)$, and a family of quadratic twists such that the rank of $L(\chi, u)$ goes to infinity.

Acknowledgments

I would first like to thank my Ph. D. advisor, Chantal David, without whom this thesis wouldn't be possible. I am grateful to her for introducing me to this topic, her help during these years, and her corrections that vastly improved the quality of this thesis. I would like to thank the examiners of this thesis for their feedback. I would like to thank Matilde Lalín and Wanlin Li for the great discussions we had while working on the paper. I would also like to thank all the other students that I met. I am also grateful for the financial support I received from the Fond de recherche du Québec - Nature et technologies. Finally, I would like to thank my friends and family, with a special thank to Hélène, François, Gaston, and Bibiane. A very special thank to Etiene.

Contribution of Authors

Chapter 1 is an original contribution of the author.

Chapter 2 is an original contribution of the author, accepted for publication in the Journal of Number Theory.

Chapter 3 is an original contribution of Chantal David, Matilde Lalín, Wanlin Li, and the author. It has been accepted for publication in the proceedings of the Fifteenth Algorithmic Number Theory Symposium. The Algorithmic Number Theory Symposium meetings, held biannually since 1994, are the premier international forum for the presentation of new research in computational number theory and its applications.

Chapter 4 is an original contribution of the author.

Contents

List of Tables

Chapter 1

Introduction

This thesis consists of two research papers, both accepted in refereed journals, namely the Journal of Number Theory, and the proceedings of the Algorithmic Number Theory Symposium, associated to the Research in Number Theory journal. Both papers are about L-functions of elliptic curves over function fields twisted by Dirichlet characters.

The study of L-functions is a central theme of modern number theory, and many of the deepest questions in number theory surround the study of L-functions.

Some of the most fundamental questions about L-functions are concerned with the location of their zeros, in particular at the central point, or on the critical line. Following the work of Montgomery [51], and then of Katz and Sarnak [38], number theorists have learned that it is very fruitful to study families of L-functions rather than individual L-functions. Given a family of L-functions, it is common to classify it according to its symmetry type. The symmetry type can be either symplectic, orthogonal, or unitary, which refers to the corresponding ensemble from random matrix theory that models most accurately the distribution of the zeros of the family.

One very important statistics for a family of L-functions is the one-level density, which is the study of the low-lying zeros. The conjectures of Katz and Sarnak predict that the one-level density for a family of L-functions is given by the statistics of the corresponding random matrix theoritic object, which determines the symmetry type of the family of L-functions. Evidence for those conjectures can be obtained by choosing a test function with

Fourier transform of limited support, and this was addressed in the literature for various families (see the references in the introduction of Chapter 2).

In the first paper, we show for quadratic twists χ_D of a fixed elliptic curve $E/\mathbb{F}_q[t]$, we have

$$\lim_{N\to\infty} \frac{1}{|\mathcal{H}_N^*|} \sum_{D\in\mathcal{H}_N^*} \mathrm{ord}_{u=1/q} L(E\otimes\chi_D, u) \leq 3/2$$

and more generally

$$\lim_{N\to\infty} \frac{1}{|\mathcal{H}_{N,C}|} \sum_{D\in\mathcal{H}_{N,C}} \mathrm{ord}_{u=1/q} L(E\otimes\chi_D, u) \leq 3/2.$$

Since the sign of the functional equation is constant over $\mathcal{H}_{N,C}$, we conclude that at least 12.5% of the family have rank zero, and at least 37.5% have rank one. This result is in line with a conjecture of Goldfeld [30], predicting that 50% of the family have rank zero, and 50% have rank one.

Over number fields, analogous results of the same strength were obtained by Heath-Brown [35]. The proofs are different, as we follow the method developped by Rudnick [55] via duality (see Lemma 2.3.2).

For twists of order $\ell > 2$ coprime to q, duality cannot be used and we obtain

$$\lim_{N\to\infty} \frac{1}{|\mathcal{F}_{\mathcal{N}}|} \sum_{\chi\in\mathcal{F}_{\mathcal{N}}} \mathrm{ord}_{u=1/q} L(E\otimes\chi, u) \leq 5/2.$$

In the second paper, we investigate a generalization of the recent results of Donepudi and Li [40, 24] from Dirichlet L-functions to twisted L-functions of an elliptic curve. For Dirichlet L-functions over $\mathbb{Q}$, Chowla [14] conjectured that $L(\chi, s)$ never vanishes at $s = 1/2$, but over function fields, Li [40] showed that if one character exists such that $L(\chi, 1/\sqrt{q}) = 0$, then there are infinitely many characters with L-functions vanishing at $u = 1/\sqrt{q}$ when $q \equiv 1 \mod \ell$. In particular, Theorem 4.2 of [24] states that for $p \equiv -1 \mod \ell$, there exists $d > 1$ such that if q is a power of p^d, then the number of characters over $\mathbb{F}_q[t]$ with conductors of degree bounded by n such that their L-functions vanish at the central point is $\gg_\epsilon q^{2n/3+\epsilon}$.

We investigate the family of twists of the L-function of a fixed elliptic curve. Over $\mathbb{Q}$, it is predicted ([19, Conjecture 1.2], [44]) that there are only finitely many characters or order ≥ 7 with L-functions that vanish at the central point. By generalizing [40, 24] to the non-Kummer case using a result of Bary-Soroker and Meisner [2], we prove that for E_0 an elliptic curve over $\mathbb{F}_q$ considered over $\mathbb{F}_q[t]$, if there exists one character over $\mathbb{F}_q[t]$ of order $\ell \geq 3$ prime and of conductor of degree d_0 such that $L(E_0 \otimes \chi, 1/q) = 0$, then the number of characters with conductors of degree bounded by n such that their L-functions vanish at the central point is $\gg_\epsilon q^{2n/d_0+\epsilon}$. Explicit examples of such E_0 and χ are given in Section 3.5.3.

The thesis has the following structure. The rest of this chapter gives a brief introduction to the L-functions of elliptic curves over function fields. Chapters 2 and 3 present the two publications. Chapter 4 presents various unpublished results related to the numerical computations performed for the second paper.

The code used in Chapter 3 and 4 can be found at github.com/AntoineComeau/Lfuncff. It was coded from scratch in Java, using only the BigInteger and Arrays libraries, and the Math library for the floor and power functions on integers.

1.1 Elliptic Curves over Finite Fields and Function Fields

In addition to the papers, we give more details about the L-functions of varieties over finite fields and function fields.

1.1.1 Varieties over $\mathbb{F}_q$

We denote the finite field with q elements by $\mathbb{F}_q$. The only possibilities for q are powers of a prime number. All finite fields having the same number of elements are isomorphic to each other.

The simplest finite fields are given by reducing $\mathbb{Z}$ modulo a prime number. Similarly, by taking an irreducible polynomial $P(t)$ of degree n in $\mathbb{F}_p[t]$, we can construct $\mathbb{F}_{p^n} \cong \mathbb{F}_p[t]/(P(t))$. Finite fields of higher orders also appear when reducing the ring of integers of a number field

by one of its prime. Many questions about finite fields are still unanswered to this day. For example, it is not known if there exists a polynomial time algorithm to solve find b in $a^b = c$, which is known as the discrete logarithm problem.

The geometry over finite fields is an important area of modern research. Given a polynomial over $\mathbb{F}_q$, we want to compute the number of solutions over the extensions $\mathbb{F}_{q^n}$. These quantities are collected into what is called a local zeta function, defined by

$$\mathcal{Z}(F, u) = \exp\left(\sum_{n=1}^{\infty} N_n \frac{u^n}{n}\right)$$

where $F \in \mathbb{F}_q[X_1, \ldots, X_m]$ and N_n is the number of solutions of F defined over $\mathbb{F}_{q^n}$ in the projective space. The polynomial F must be homogenized so that its set of zeros is a projective variety. Then, the following facts have been proved to hold for $\mathcal{Z}(F, u)$ if the variety is non-singular (they are called the Weil's conjectures, although they have been proved [64]). We have

$$\mathcal{Z}(F, u) = \frac{P_1(u) \ldots P_{2m-1}(u)}{P_0(u) \ldots P_{2m}(u)} \tag{1.1.1}$$

where m is the dimension of the projective variety induced by F, $P_0(u) = 1 - u$, $P_{2m}(u) = 1 - q^m u$, and

$$P_k(u) = \prod_{j=1}^{M_k} \left(1 - q^{k/2} e^{i\theta_{k,j}} u\right) \tag{1.1.2}$$

where $M_i < \infty$ and $\theta_{k,j} \in [0, 2\pi)$. Furthermore, we have $P_k \in \mathbb{Z}[u]$. The numbers N_n are then given by

$$N_n = \sum_{k=0}^{2m} \sum_{j=1}^{M_k} (-1)^k q^{nk/2} e^{ni\theta_{k,j}}.$$

The analogy with the L-functions comes from the point of view of function fields. We consider the set $\mathbb{F}_q[t]$. The irreducible polynomials are the primes of this set. We have the following relation between the primes of $\mathbb{F}_q[t]$ and the points of $\overline{\mathbb{F}_q}$. Given $a \in \overline{\mathbb{F}_q}$, we define its degree to be the smallest n such that $a \in \mathbb{F}_{q^n}$ and we denote it by $\deg(a)$. If $\deg(a) = n$, then there exists a unique prime $P(t)$ of degree n in $\mathbb{F}_q[t]$ such that $P(a) = 0$. The other roots are given by $a^q, a^{q^2}, \ldots, a^{q^{n-1}}$. In the other direction, we have $\mathbb{F}_q[t]/(P(t)) \cong \mathbb{F}_{q^n}$ if $P(t)$ is a prime of degree n. The element t is a root of $P(t)$ under this quotient. This means that there is a one-to-one correspondence between the primes of $\mathbb{F}_q[t]$ and the Galois orbits of $\overline{\mathbb{F}_q}/\mathbb{F}_q$.

Given a polynomial $F \in \mathbb{F}_q[X_0, \ldots, X_m]$, if we evaluate, say X_0, at $a \in \mathbb{F}_{q^n}$, we get a polynomial G_1 over $\mathbb{F}_{q^n}$ and we lose one variable. If we evaluate X_0 at a^q, we get a polynomial that we call G_2. Then, under the map

$$(X_1, \ldots, X_m) \mapsto (X_1^q, \ldots, X_m^q)$$

we get that the affine variety associated to G_1 is isomorphic to the one associated to G_2. This means that if we want to count the number of solutions of F fiber by fiber on X_0, it is sufficient to go over the Galois orbits of $\overline{\mathbb{F}_q}/\mathbb{F}_q$. This gives a way to define L-functions using the Euler product. At each prime there is a fiber with an associated local zeta function. It is difficult in general to understand how the product over the fibers relates to the local zeta function of the variety, since the object lies in the projective space. A prime at infinity is introduced to the Euler product, the fiber at this prime is related to the subvariety at infinity. We recover the equation at this fiber using the substitution $t \mapsto 1/t$ and evaluating at $t = 0$. The difficult problem of resolving singularities is another obstacle in computing the local zeta function using the polynomial F. Elliptic curves over $\mathbb{F}_q[t]$ correspond to elliptic surfaces over $\mathbb{F}_q$, which are better understood than general surfaces.

Equation 1.1.2 is the analogue of the Riemann hypothesis in the function fields setting. If we do the change of variables $u = q^{-s}$, the zeros can be seen to share the same real part.

The local zeta functions have a finite number of zeros as a polynomial in u. To study the asymptotic distribution of the angles $\theta_{k,j}$, it is necessary to consider a family of zeta functions or L-functions. We can associate a matrix to each $P_i(u)$ in (1.1.1) if we interpret it as the characteristic polynomial of a matrix. The discussion of the previous section about the symmetry of a family also apply in the function field settings. In fact, Katz and Sarnak proved some equidistribution results. For example [55, 38], if we consider all the curves of the form

$$y^2 = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_0$$

with $a_i \in \mathbb{F}_q$ such that the polynomial in x is square-free and monic, then the matrices associated to the $P_1(u)$ factor of the local zeta functions of these curves are equidistributed in the unitary symplectic group of dimension $2g$ as $q \to \infty$. In the other direction, when q is fixed and g grows to infinity, equidistribution results are predicted to hold for suitable families, but

no proofs have been given yet. This is the direction that the two papers of this thesis focus on.

We refer to [54] for an in-depth analysis of number theory in function fields.

1.1.2 Elliptic Curves

Let E be an elliptic curve over $\mathbb{Q}$, which is a smooth projective curve of genus one with affine model given by

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

By reducing modulo a prime number, we obtain either an elliptic curve or a singular object. We say the elliptic curve has good reduction if we obtain an elliptic curve, and has bad reduction otherwise. There is only a finite number of primes of bad reduction and they are collected into what is called the conductor of the elliptic curve. For primes of good reduction, the local zeta function of the reduced elliptic curve has the form

$$\mathcal{Z}(E/\mathbb{F}_p, u) = \frac{(1-\alpha_p u)(1-\overline{\alpha_p} u)}{(1-u)(1-pu)}$$

where $|\alpha_p| = p^{1/2}$. We define the L-function of an elliptic curve E using these local factors in the Euler product with the change of variable $u = p^{-s}$

$$L(E,s) := \prod_{p \text{ good}} (1-\alpha_p p^{-s})^{-1}(1-\overline{\alpha_p} p^{-s})^{-1} \prod_{p \text{ bad}} (1-a_p p^{-s})^{-1}$$

where $a_p = -1, 0$, or 1 depending on the type of bad reduction. This product converges absolutely for $\mathrm{Re}(s) > 3/2$. The meromorphic continuation and the functional equation were conjectured by Shimura and Taniyama and proved by Wiles, and Wiles, Conrad, Diamond, Taylor, and Breuil [65, 15]. An important motivation for the study of the analytical rank of $L(E,s)$ is the Birch and Swinnerton-Dyer conjecture. It states that the rank of the abelian group $E(\mathbb{Q})$ should be the order of the zero of $L(E,s)$ at $s = 1$.

In the function fields setting, the L-functions are defined similarly. At every good prime P we have an elliptic curve over $\mathbb{F}_{q^{\deg(P)}}$ with local zeta function equal to

$$\frac{(1-\alpha_P u)(1-\overline{\alpha_P} u)}{(1-u)(1-q^{\deg(P)}u)}$$

with $|\alpha_P| = q^{\deg(P)/2}$. The L-function is then given by

$$L(E,u) := \prod_{P \text{ good}} (1-\alpha_P u^{\deg(P)})^{-1}(1-\overline{\alpha_P} u^{\deg(P)})^{-1} \prod_{P \text{ bad}} (1-a_P u^{\deg(P)})^{-1}$$

where $a_P = -1, 0$, or 1 depending on the type of bad reduction. The conductor of E, denoted by N_E, is defined by the product of the bad primes, and we square the bad primes such that $a_p = 0$. Under the change of variables $u = q^{-s}$, we have that $L(E,u)$ is a polynomial of degree $\deg(N_E) - 4$ and all zeros have norm $1/q$ [37] when the prime at infinity is considered in the Euler product.

Since $a, b \in \mathbb{F}_q[t]$, we can also consider $E/\mathbb{F}_q[t]$ as a surface over $\mathbb{F}_q$. This is a good example of how the local zeta function of the variety is related to the product of the local zeta functions of the fibers. This is called an elliptic fibration. There is a morphism $E \to \mathbb{P}^1(\overline{\mathbb{F}}_q)$ given by the projection on t. Then

$$\#E(\mathbb{F}_{q^n}) = \sum_{\deg(P)|n} \deg(P) \cdot \#E/P(\mathbb{F}_{q^n})$$

where the prime at infinity is considered and has degree one. This implies

$$\mathcal{Z}(E,u) = \prod_P \mathcal{Z}(E/P, u^{\deg(P)}).$$

Then

$$\frac{P_1(u)P_3(u)}{(1-u)P_2(u)(1-q^2u)} = \prod_{P \text{ good}} \frac{(1-\alpha_P u^{\deg(P)})(1-\overline{\alpha_P} u^{\deg(P)})}{(1-u^{\deg(P)})(1-(qu)^{\deg(P)})} \prod_{P \text{ bad}} \frac{(1-a_P u^{\deg(P)})}{(1-u^{\deg(P)})(1-(qu)^{\deg(P)})}.$$

It is known that $P_1(u) = P_3(u) = 1$, so we conclude

$$L(E,u) = \frac{P_2(u)}{(1-qu)^2}.$$

More information about elliptic curves can be found in the book of Silverman [58].

Chapter 2

One-level Density of the Family of Twists of an Elliptic Curve over Function Fields

This first paper presents the computation of the one-level density of the family of twists of an elliptic curve over function fields. For quadratic twists, the functional equation is used to increase the allowed support for the test functions. For higher order twists, the trivial bound is used.

This paper was accepted for publication in the Journal of Number Theory in March 2022. The format has been adjusted for this thesis, a paragraph in the introduction has been relocated, and the bibliography has been relocated to the end of the thesis.

One-level Density of the Family of Twists of an Elliptic Curve over Function Fields

Antoine Comeau-Lapointe, *Concordia University*

Abstract. We fix an elliptic curve $E/\mathbb{F}_q(t)$ and consider the family $\{E\otimes\chi_D\}$ of E twisted by quadratic Dirichlet characters. The one-level density of their L-functions is shown to follow orthogonal symmetry for test functions with Fourier transform supported inside $(-1,1)$. As an application, we obtain an upper bound of $3/2$ on the average analytic rank. By splitting the family according to the sign of the functional equation, we obtain that at least 12.5% of the family have rank zero, and at least 37.5% have rank one. The Katz and Sarnak philosophy predicts that those percentages should both be 50% and that the average analytic rank should be $1/2$. We finish by computing the one-level density of E twisted by Dirichlet characters of order $\ell \neq 2$ coprime to q. We obtain a restriction of $(-1/2, 1/2)$ on the support with a unitary symmetry.

Keywords: Zeta functions; Elliptic curves; L-function; Finite fields; Function fields; One-level density; Dirichlet characters; Twisted L-functions; Average rank

2.1 Introduction

We study the one-level density of the family of twists of an elliptic curve defined over $\mathbb{F}_q(t)$. Throughout this paper, a prime $p \neq 2, 3$ is fixed and we fix $q = p^n$ for any integer $n \geq 1$. We also fix an elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_q[t]$ under its minimal Weierstrass model such that it has at least one prime of multiplicative reduction, has good reduction at infinity, and such that its j-invariant isn't zero (see [58] for background). We write A instead of $A(t)$ for elements of $\mathbb{F}_q[t]$. The conductor of E is denoted by N_E.

Let $\mathcal{M}_N \subset \mathbb{F}_q[t]$ be the set of monic polynomials of degree N and let $\mathcal{H}_{N,C} \subset \mathcal{M}_N$ be the set of square-free polynomials of degree N congruent to C modulo N_E where C is coprime to N_E. We denote by $\mathcal{H}_N^*$ the set of square-free polynomials of degree N that are coprime to N_E. In particular, we have the partition $\mathcal{H}_N^* = \bigcup_{\substack{C \bmod N_E \\ (C,N_E)=1}} \mathcal{H}_{N,C}$. The main family of this paper is the set of quadratic twists of E. Each twist of E is denoted by $E \otimes \chi_D$ where χ_D is the unique quadratic Dirichlet character of conductor D, where $D \in \mathcal{H}_N^*$. To

each twist is associated a unitary matrix (up to conjugacy class) called the Frobenius of $E \otimes \chi_D$ denoted by

$$\Theta_D = \begin{pmatrix} e^{i\theta_{D,1}} & & \\ & \ddots & \\ & & e^{i\theta_{D,M}} \end{pmatrix} \tag{2.1.1}$$

where the $e^{i\theta_{D,j}}$ are called the Frobenius eigenvalues of $E \otimes \chi_D$ and $0 \leq \theta_{D,j} < 2\pi$. The average of traces of powers of Θ_D over $\mathcal{H}_{N,C}$ is defined by

$$\langle \text{tr } \Theta^n \rangle_{N,C} := \frac{1}{|\mathcal{H}_{N,C}|} \sum_{D \in \mathcal{H}_{N,C}} \sum_{j=1}^{M} e^{in\theta_{D,j}}.$$

We prove the following.

Theorem 2.1.1. *For $\epsilon > 0$, $n > 0$, and $N > 4\deg(N_E)$*

$$\langle \text{tr } \Theta^n \rangle_{N,C} = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd} \end{cases} + \mathcal{O}_{E,q}\left((n+N)N^{2\deg(N_E)+3}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}}\right) + n^2 q^{-n/4}\right).$$

This is in agreement with the mean values over $O(M)$ given in [23]

$$\int_{O(M)} \text{tr } \Theta^n d\Theta = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd} \end{cases} \tag{2.1.2}$$

with respect to the Haar measure where $O(M)$ is the orthogonal group of dimension M. The subgroup of matrices with determinant 1 is denoted by $SO(M)$. Two different symmetry types exist depending on the parity of M. They are denoted by $SO(\text{even})$ and $SO(\text{odd})$.

As an application we compute the one-level density of the family. The Schwartz space $\mathcal{S}(\mathbb{R})$ is a space of rapidly decreasing functions on $\mathbb{R}$ and is defined by

$$\mathcal{S}(\mathbb{R}) := \{f \in C^\infty(\mathbb{R}) \,|\, \forall \alpha, \beta \in \mathbb{N}, \|f\|_{\alpha,\beta} < \infty\} \text{ where } \|f\|_{\alpha,\beta} := \sup_{x \in \mathbb{R}} |x^\alpha f^{(\beta)}(x)|.$$

For an even function $\phi \in \mathcal{S}(\mathbb{R})$ and $M \geq 0$, we define

$$F(\theta) := \sum_{k \in \mathbb{Z}} \phi\left(M\left(\frac{\theta}{2\pi} - k\right)\right)$$

which has period 2π and is localized on an interval of size $\approx 1/M$ around 0 in $\mathbb{R}/2\pi\mathbb{Z}$. Let Θ be an $M \times M$ matrix with eigenvalues $e^{i\theta_j}$, where $0 \leq \theta_j < 2\pi$. We define

$$Z_\phi(\Theta) := \sum_{j=1}^{M} F(\theta_j). \tag{2.1.3}$$

The one-level density of the family $\mathcal{H}_{N,C}$ is the average

$$\langle Z_\phi \rangle_{N,C} := \frac{1}{|\mathcal{H}_{N,C}|} \sum_{D \in \mathcal{H}_{N,C}} Z_\phi(\Theta_D)$$

where Θ_D is given by (2.1.1). The one-level density picks up the θ_j near 0 and it reveals the symmetry type of our family. We prove the following result on the one-level density.

Corollary 2.10.1. *For $\phi \in \mathcal{S}(\mathbb{R})$ an even function such that $\mathrm{supp}(\hat{\phi}) \subset (-1, 1)$, we have for the one-level density of the family of quadratic twists of E*

$$\langle Z_\phi \rangle_{N,C} = \int_{O(M)} Z_\phi(\Theta) d\Theta + \mathcal{O}_{E,q}(1/N)$$

where $M = 2N + \deg(N_E) - 2$.

As an application, we get an upper bound on the average analytic rank. The analytic rank of $E \otimes \chi_D$ is defined as the number of $\theta_{D,j} = 0$ in Θ_D, and we denote it by $r(E \otimes \chi_D)$. We define

$$\langle r \rangle_{N,C} := \frac{1}{|\mathcal{H}_{N,C}|} \sum_{D \in \mathcal{H}_{N,C}} r(E \otimes \chi_D)$$

and the average analytic rank is defined as

$$r_C := \lim_{N \to \infty} \langle r \rangle_{N,C}$$

if the limit exists. We prove the followings.

Theorem 2.11.1. *We have* $\limsup_{N\to\infty} \langle r \rangle_{N,C} \leq 3/2$.

In particular, the average analytic rank is $\leq 3/2$ in the whole family of twists $D \in \mathcal{H}_N^*$. By splitting the family according to congruence classes we get the following result on the non-vanishing at the central point.

Theorem 2.11.3. *At least* 12.5% *of the family of quadratic twists of E have rank zero and at least* 37.5% *have rank one as $N \to \infty$.*

In the final section, we study the one-level density for the family of twists of E of order ℓ coprime to q. However, the results are too weak to produce any significant bound on the average analytic rank. We get the following restriction on the support of the Fourier transform of ϕ where $U(M)$ is the unitary group of dimension M.

Theorem 2.12.1. *For $\phi \in \mathcal{S}(\mathbb{R})$ an even function such that $\mathrm{supp}(\hat{\phi}) \subset (-1/2, 1/2)$, we have for the one-level density of the family of twists of E of order $\ell \neq 2$ and $(\ell, q) = 1$*

$$\langle Z_\phi \rangle_{N,C} = \int_{U(M)} Z_\phi(\Theta) d\Theta + \mathcal{O}_{E,q,\ell}(1/N)$$

where $M = 2N + \deg(N_E) - 2$.

The condition $\mathrm{supp}(\hat{\phi}) \subset (-1/2, 1/2)$ for twists of E is the analogous result of the condition $\mathrm{supp}(\hat{\phi}) \subset (-1/m, 1/m)$ for twists of a given cuspidal representation of $\mathrm{GL}_m(A_{\mathbb{Q}})$ obtained by Cho and Park over $\mathbb{Q}$ [13].

Over $\mathbb{Q}$, the one-level density of the family of this paper was studied by Heath-Brown [35] for quadratic twists. The first results obtained in the present paper are analogous to what he obtained. Under a hypothesis slightly stronger than the Riemann Hypothesis for elliptic curves, Fiorilli [26] showed that the average analytic rank of this family is exactly $1/2$. Over cyclic extensions such that the degree is a fixed odd prime, Cho [10] has shown that the average analytic rank of E is at most $2 + r_{\mathbb{Q}}(E)$ where $r_{\mathbb{Q}}(E)$ is the analytic rank of E over $\mathbb{Q}$. For cubic Dirichlet L-functions over $\mathbb{Q}$, Cho and Park [11] computed the one-level density and obtained the restriction of $(-1, 1)$ on the support of the test functions along with a unitary symmetry. They also computed [12] the n-level densities for the family of cubic twists of any given cuspidal representation of $\mathrm{GL}_m(A_{\mathbb{Q}})$, and they showed that the symmetry is unitary. Over cubic Galois number fields, Meisner [48] computed the one-level density of the associated L-functions and showed that the symmetry is unitary with a restriction of $(-1/2, 1/2)$ on the support. For the one-level density of Dirichlet L-functions of order r over $\mathbb{Q}$, Cho and Park [13] showed that the symmetry is unitary, and obtained the restriction of (-1,1) on the support. They also obtained the restriction of $(-1/m, 1/m)$ on the support for the family of twists of order r of any given cuspidal representation of $\mathrm{GL}_m(A_{\mathbb{Q}})$. All of the above results are under the Generalized Riemann Hypothesis. Over function fields, results are unconditional since the Weil's conjectures have been proved.

Over $\mathbb{F}_q(t)$, the one-level density of the family of quadratic Dirichlet L-functions was studied by Rudnick [55] where he obtained a restriction of $(-2, 2)$ on the support, with a symplectic symmetry. Under further restrictions on the support, Bui and Florea [7] were able to compute lower order terms for the one-level density of this family. The first four moments of this family were obtained by Florea [28], [27]. For cubic Dirichlet L-functions over $\mathbb{F}_q(t)$, David, Florea, and Lalín [20] computed the mean values of the L-functions. They also proved that a positive proportion of these L-functions do not vanish at the central point [21]. For twists of order r such that $q \equiv 1 \bmod r$, Meisner determined the number of $\mathbb{F}_q$-points of the associated curves [47].

2.2 Background

2.2.1 Elliptic Curves

The degree of a polynomial $A \in \mathbb{F}_q[t]$ is denoted by $\deg(A)$. We define N_E, the conductor of E, by

$$N_E = \prod_{\substack{P \in \mathbb{F}_q[t] \\ P \text{ prime}}} P^{f_P(E)}$$

where

$$f_P(E) := \begin{cases} 0, & \text{if } E \text{ has good reduction at } P \\ 1, & \text{if } E \text{ has multiplicative reduction at } P \\ 2, & \text{if } E \text{ has additive reduction at } P. \end{cases}$$

The prime at infinity does not divide the conductor since we assumed E has good reduction at infinity. A good reduction means that E/P, the reduction of E at a prime $P \in \mathbb{F}_q[t]$, is an elliptic curve over $\mathbb{F}_q[t]/(P) \cong \mathbb{F}_{q^{\deg(P)}}$, which is a finite field. By the Weil's conjectures, its zeta function is equal to

$$\mathcal{Z}(E/P, u) = \frac{(1 - \alpha_P(E)u)(1 - \overline{\alpha_P}(E)u)}{(1-u)(1-q^{\deg(P)}u)}$$

where $\alpha_P(E)$ and $\overline{\alpha_P}(E)$ may be swapped. We call those values the Frobenius eigenvalues of E at P and since we fixed E, we simply write them as α_P and $\overline{\alpha}_P$. For primes of good reduction, they may be computed using

$$a_P := \alpha_P + \overline{\alpha}_P = q^{\deg(P)} + 1 - \#(E/P)$$

where $\#(E/P)$ is the number of $\mathbb{F}_{q^{\deg(P)}}$-points of E/P. When E/P isn't an elliptic curve, we say that the reduction is bad. If the reduction is multiplicative, we have $a_P = \pm 1$, and if the reduction is additive, we have $a_P = 0$. We will often use the fact that $|\alpha_P| = q^{\deg(P)/2}$ from the Weil's conjectures for primes of good reduction.

2.2.2 L-functions

Let χ be a primitive Dirichlet character on $\mathbb{F}_q[t]$ (see [54] for background). Its L-function is defined by

$$L(\chi, u) := \prod_P (1 - \chi(P)u^{\deg(P)})^{-1}$$

where the product is over the primes of $\mathbb{F}_q[t]$ excluding the prime at infinity.

The L-function of E is defined by

$$L(E, u) := \prod_{P \nmid N_E} (1 - \alpha_P u^{\deg(P)})^{-1}(1 - \overline{\alpha}_P u^{\deg(P)})^{-1} \prod_{P | N_E} (1 - a_P u^{\deg(P)})^{-1}$$

and the L-function of E twisted by χ is defined by

$$L(E \otimes \chi, u) := \prod_{P \nmid N_E} (1 - \chi(P)\alpha_P u^{\deg(P)})^{-1}(1 - \chi(P)\overline{\alpha}_P u^{\deg(P)})^{-1} \prod_{P | N_E} (1 - \chi(P)a_P u^{\deg(P)})^{-1}$$

excluding the prime at infinity.

A Dirichlet character is uniquely factored into

$$\chi = \hat{\chi}\chi_0 \tag{2.2.1}$$

where $\hat{\chi}$ is primitive and χ_0 is principal with minimal modulus. The principal character of modulus C is given by

$$\chi_0(A) = \begin{cases} 1, & \text{if } (A, C) = 1 \\ 0, & \text{otherwise.} \end{cases}$$

We get

$$L(\chi, u) \prod_{\substack{P | \text{modulus}(\chi_0) \\ P \text{ prime}}} (1 - \hat{\chi}(P)u^{\deg(P)})^{-1} = L(\hat{\chi}, u).$$

A character is said to be even if it is trivial on $\mathbb{F}_q$. It is called odd otherwise.

We also split $\mathcal{H}_N^* = \mathcal{H}_{N,+} \cup \mathcal{H}_{N,-}$ depending on if the sign of the functional equation of $L(E \otimes \chi_D, u)$ for $D \in \mathcal{H}_N^*$ is 1 or -1 respectively.

2.2.3 Gauss Sums

As done by Hayes [34], we define the following function on $\mathbb{F}_q(t)$

$$e_q(A) := e^{\frac{2\pi i \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(A_1)}{p}}$$

where A_1 is the coefficient of $1/t$ in the Laurent expansion of A.
The Gauss sum of a primitive character χ of conductor F is defined as

$$G(\chi) := \sum_{A \bmod F} \chi(A) e_q\left(\frac{A}{F}\right)$$

and it does not depend on the choice of representatives.
We also define

$$\tau(\chi) := \sum_{a \in \mathbb{F}_q^*} \chi(a) e^{2\pi i \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)/p}.$$

We denote by $\omega(\chi)$ the sign of the functional equation of $L(\chi, u)$ and it is given in Lemma 2.3.2. When χ is quadratic, $\omega(\chi)$ is always 1 (see [55]).

2.3 Duality

We remark that the conductor of a primitive character of order ℓ coprime to q is always square-free.

Proposition 2.3.1 (Riemann Hypothesis)**.** *Let χ be a primitive Dirichlet character of order ℓ coprime to q of conductor $F \neq 1$ on $\mathbb{F}_q[t]$. Then*

$$L(\chi, u) = (1-u)^\lambda \prod_{j=1}^{M} (1 - q^{1/2} e^{i\theta_j} u)$$

where $M = \deg(F) - 1$ and $\lambda = 0$ if χ is odd or else $M = \deg(F) - 2$ and $\lambda = 1$.

Proof. We have by Theorem 9.16B of [54]

$$L(\chi,u)K_\infty(\chi,u)=\prod_{j=1}^{M}(1-q^{1/2}e^{i\theta_j}u)$$

where

$$K_\infty(\chi,u)=(1-\chi(P_\infty)u)^{-1}$$

is the Euler factor of the prime at infinity. This implies $L(\chi,u)$ have at most one zero on $|u|=1$ and all others are on $|u|=q^{-1/2}$.

We remark that Theorem 9.16B [54] only holds for geometric extensions. To each character χ is associated a cyclic field extension $K_\chi/\mathbb{F}_q[t]$ of degree equals to the order of χ. It is called a geometric extension if its field of constants is $\mathbb{F}_q$. A character associated to a field of constants extension has the form

$$\chi_c(D)=\zeta^{\deg(D)}$$

where ζ is a root of unity in $\mathbb{C}$. Those characters aren't Dirichlet characters since they are not periodic to any modulo (χ_c is never 0), which shows that K_χ is geometric in the case of Dirichlet characters.

We have the expansion

$$L(\chi,u)=\sum_{h=0}^{\infty}\left(\sum_{D\in\mathcal{M}_h}\chi(D)\right)u^h.$$

When $h\geq\deg(F)$, the polynomials become equidistributed modulo F so the coefficient of u^h is zero. We also have by [54] that

$$\sum_{D\in\mathcal{M}_{\deg(F)-1}}\chi(D)\neq 0$$

meaning that $L(\chi,u)$ is a polynomial of degree $\deg(F)-1$.

When χ is even

$$(q-1)L(\chi,1)=\left(\sum_{a\in\mathbb{F}_q^*}\chi(a)\right)\sum_{n=0}^{\deg(F)-1}\left(\sum_{D\in\mathcal{M}_n}\chi(D)\right)=\sum_{\substack{D\in\mathbb{F}_q[t]\\ \deg(D)\leq\deg(F)-1}}\chi(D)=0$$

so a zero is forced at $u = 1$.

When χ is odd, we refer to Tao's blog [61] Theorem 2 where it is stated that all zeros of $L(\chi, u)$ have norm $q^{-1/2}$. □

The following lemma can also be obtained using Poisson summation formula (see [7]). In this case, the character χ doesn't have to be primitive, but the summands become Gauss sums.

Lemma 2.3.2 (Duality)**.** *Let χ be a primitive Dirichlet character of order ℓ coprime to q of conductor $F \neq 1$. Then*

$$\sum_{B \in \mathcal{M}_j} \chi(B) = \omega(\chi) q^{j-\deg(F)/2} \sum_{k=0}^{\deg(F)-1-j} \sigma_\chi(k) \sum_{B \in \mathcal{M}_{\deg(F)-1-j-k}} \overline{\chi}(B)$$

where $\omega(\chi)$ is given by (2.3.2) and $\sigma_\chi(k)$ is given by (2.3.4). Furthermore, $\sigma_\chi(k)$ only depends on the parity of the character, $|\sigma_\chi(k)| \leq q$, and $|\omega(\chi)| = 1$.

Proof. This was proven by Rudnick ([55] Proposition 7) for quadratic Dirichlet characters. We adjust his computations for arbitrary orders.

Assume first that χ is odd. By the above proposition

$$L(\chi, u) = \prod_{j=1}^{M} (1 - q^{1/2} e^{i\theta_j} u)$$

where $M = \deg(F) - 1$. Since

$$L(\overline{\chi}, u) = \prod_{j=1}^{M} (1 - q^{1/2} e^{-i\theta_j} u)$$

we have

$$L\left(\overline{\chi}, \frac{1}{qu}\right) = \prod_{j=1}^{M} \left(1 - e^{-i\theta_j} \frac{1}{q^{1/2} u}\right) = \frac{\prod_{j=1}^{M} e^{-i\theta_j}}{(q^{1/2} u)^M} \prod_{j=1}^{M} (e^{i\theta_j} u q^{1/2} - 1) = \frac{1}{\omega(\chi) u^M q^{M/2}} L(\chi, u) \tag{2.3.1}$$

where

$$\omega(\chi) = \prod_{j=1}^{M} -e^{i\theta_j}. \tag{2.3.2}$$

Now, using

$$L(\chi, u) = \sum_{j=0}^{M} \left(\sum_{B \in \mathcal{M}_j} \chi(B) \right) u^j$$

and the last equation, we get by comparing powers of u

$$\sum_{B \in \mathcal{M}_j} \chi(B) = \omega(\chi) q^{j-M/2} \sum_{B \in \mathcal{M}_{M-j}} \overline{\chi}(B).$$

When χ is even, we have to deal with the extra factor $(1-u)$. Let

$$\frac{L(\chi, u)}{1-u} = \sum_{j=0}^{M} A_j u^j.$$

Since we removed the extra zero,

$$A_j = \omega(\chi) q^{j-M/2} \overline{A}_{M-j}.$$

Also, we have

$$\sum_{B \in \mathcal{M}_j} \chi(B) = A_j - A_{j-1}$$

which implies

$$A_j = \sum_{k=0}^{j} \sum_{B \in \mathcal{M}_k} \chi(B). \tag{2.3.3}$$

Then

$$\sum_{B \in \mathcal{M}_j} \chi(B) = A_j - A_{j-1} = \omega(\chi) q^{j-1-M/2} (q\overline{A}_{M-j} - \overline{A}_{M+1-j})$$

and by Equation (2.3.3) above

$$\sum_{B \in \mathcal{M}_j} \chi(B) = -\omega(\chi) q^{j-M/2-1} \left(\sum_{B \in \mathcal{M}_{M+1-j}} \overline{\chi}(B) - (q-1) \sum_{k=0}^{M-j} \sum_{B \in \mathcal{M}_k} \overline{\chi}(B) \right)$$

where $M = \deg(F) - 2$. For ease of use we define

$$\sigma_\chi(k) := \begin{cases} q^{1/2} & \text{if } k = 0 \\ 0 & \text{otherwise} \end{cases} \tag{2.3.4}$$

when χ is odd and

$$\sigma_\chi(k) := \begin{cases} -1 & \text{if } k = 0 \\ q-1 & \text{otherwise} \end{cases}$$

when χ is even. □

2.4 The Explicit Formula

Proposition 2.4.1 (Riemann Hypothesis)**.** *For χ a primitive Dirichlet character of order ℓ coprime to q of conductor $F \neq 1$ coprime to N_E*

$$L(E \otimes \chi, u) = \begin{cases} \prod_{j=1}^{M} \left(1 - qe^{i\theta_j}u\right) & \text{if } \chi \text{ is odd} \\ (1 - \sqrt{q}e^{i\theta_\infty}u)(1 - \sqrt{q}e^{-i\theta_\infty}u) \prod_{j=1}^{M-2} \left(1 - qe^{i\theta_j}u\right) & \text{if } \chi \text{ is even} \end{cases} \tag{2.4.1}$$

where $M = 2\deg(F) + \deg(N_E) - 2$ and θ_∞ is the eigenangle of E at infinity.

Proof. Let ℓ be the order of χ. We first assume ℓ to be prime. Let $K_\chi/\mathbb{F}_q(t)$ be the cyclic field extension associated to χ. By Artin's conjecture, which has been proved over function fields, we have

$$L^*(E/K_\chi, u) = L^*(E, u) \prod_{i=1}^{\ell-1} L^*(E \otimes \chi^i, u)$$

and all of these functions are entire. The star indicates the factor at infinity is included in the Euler product of the L-functions. When no field is specified in the parameters of the L-function, the Euler product is assumed to be over $\mathbb{F}_q[t]$, otherwise it is over the specified field. By [9] Theorem 1.1 (ii)

$$L^*(E/K_\chi, u) = \prod_{j=1}^{L} \left(1 - qe^{i\theta_j}u\right)$$

where $L = \ell \cdot \deg(N_E) + 2(2g-2)$ and g is the genus of K_χ.

The factor at infinity of $L^*(E \otimes \chi^i, u)$ is

$$(1 - \chi^i(P_\infty)\sqrt{q}e^{i\theta_\infty}u)^{-1}(1 - \chi^i(P_\infty)\sqrt{q}e^{-i\theta_\infty}u)^{-1}$$

where P_∞ is the prime at infinity. If χ is even, then $\chi^i(P_\infty) = 1$. We also have $2g = (\ell-1)(\deg(F)-2)$ and $L^*(E,u)$ has degree $\deg(N_E) - 4$ ([5], Appendix). This implies $L^*(E \otimes \chi^i, u)$ has degree $2\deg(F) + \deg(N_E) - 4$. If χ is odd, then $\chi^i(P_\infty) = 0$ and $2g = (\ell-1)(\deg(F)-1)$. This implies $L^*(E \otimes \chi^i, u)$ has degree $2\deg(F) + \deg(N_E) - 2$. The result can be generalized to composite orders using induction. □

Lemma 2.4.2 (Explicit Formula)**.** *For χ a primitive Dirichlet character of order ℓ coprime to q of conductor $F \neq 1$ coprime to N_E*

$$\sum_{d|n} \sum_{P \in \mathcal{P}_{n/d}} (n/d)(\alpha_P^d + \overline{\alpha}_P^d)\chi^d(P) = -q^n \sum_{j=1}^{M-\delta} e^{in\theta_j} + \mathcal{O}(q^{n/2})$$

where $\alpha_P^d + \overline{\alpha}_P^d$ is replaced by a_P^d for primes dividing N_E, $\delta = 0$ if χ is odd and $\delta = 2$ is χ is even.

Proof. We get the result by comparing the coefficients of the powers of u in the logarithmic derivative of (4.2.1) to those coming from the logarithmic derivative of the Euler product. □

2.5 The Sieve

We sieve for two conditions, the polynomials must be square-free and congruent to C modulo N_E for some C coprime to N_E. We use the techniques of [7] Lemma 2.2. The notation $A \mid B^\infty$ means that if a prime divides A, then it must divide B.

Lemma 2.5.1.

$$\sum_{D \in \mathcal{H}_{N,C}} \chi_D(P) =$$

$$\frac{1}{|(\mathbb{F}_q[t]/(N_E))^*|} \sum_{\psi \bmod N_E} \overline{\psi}(C) \sum_{k=0}^{N} \sum_{m=0}^{k} \alpha_\psi(m)$$

$$\sum_{\substack{Q_1 \mid M_\psi \\ Q_2 \mid (PN_\psi)^\infty \\ \deg(Q_1)+2\deg(Q_2)=k-m}} \mu(Q_1)\hat{\psi}(Q_1)\chi_{Q_1}(P)\hat{\psi}_2(Q_2) \sum_{D \in \mathcal{M}_{N-k}} \hat{\psi}(D)\chi_D(P)$$

where $\psi_2 := \psi^2$, $\psi = \hat{\psi}\psi_0$ and $\psi_2 = \hat{\psi}_2(\psi_2)_0$ as in Equation (2.2.1). The modulus of ψ_0 is denoted by M_ψ and the modulus of $(\psi_2)_0$ is denoted by N_ψ. The function α_ψ is given by (2.5.5) and $|\alpha_\psi(m)| \leq m^{\deg(N_E)} q^{m/2}$.

Proof. Polynomials $D \in \mathbb{F}_q[t]$ that are congruent to C mod N_E are picked up using

$$\frac{1}{|(\mathbb{F}_q[t]/(N_E))^*|} \sum_{\psi \bmod N_E} \overline{\psi}(C)\psi(D) = \begin{cases} 1 & \text{if } D \equiv C \bmod N_E \\ 0 & \text{otherwise} \end{cases} \tag{2.5.1}$$

where the sum is over all Dirichlet characters modulo N_E. So

$$\sum_{D \in \mathcal{H}_{N,C}} \chi_D(P) = \frac{1}{|(\mathbb{F}_q[t]/(N_E))^*|} \sum_{\psi \bmod N_E} \overline{\psi}(C) \sum_{D \in \mathcal{H}_N} \psi(D)\chi_D(P) \tag{2.5.2}$$

and we write the generating series as

$$\sum_{h=0}^{\infty}\left(\sum_{D\in\mathcal{H}_h}\psi(D)\chi_D(P)\right)u^h=\prod_{Q\text{ prime}}(1+\psi(Q)\chi_Q(P)u^{\deg(Q)})=\frac{\prod_Q(1-\psi_2(Q)\chi_Q^2(P)u^{2\deg(Q)})}{\prod_Q(1-\psi(Q)\chi_Q(P)u^{\deg(Q)})} \tag{2.5.3}$$

$$=\frac{\prod_Q(1-\hat{\psi}(Q)\chi_Q(P)u^{\deg(Q)})^{-1}\prod_{Q|M_\psi}(1-\hat{\psi}(Q)\chi_Q(P)u^{\deg(Q)})}{\prod_Q(1-\hat{\psi}_2(Q)u^{2\deg(Q)})^{-1}\prod_{Q|PN_\psi}(1-\hat{\psi}_2(Q)u^{2\deg(Q)})}.$$

We now expand all four products. We first have

$$\prod_Q(1-\hat{\psi}(Q)\chi_Q(P)u^{\deg(Q)})^{-1}=\sum_{h=0}^{\infty}\left(\sum_{D\in\mathcal{M}_h}\hat{\psi}(D)\chi_D(P)\right)u^h. \tag{2.5.4}$$

Also

$$\prod_Q(1-\hat{\psi}_2(Q)u^{2\deg(Q)})^{-1}=L(\hat{\psi}_2,u^2).$$

We assume first that $\hat{\psi}_2$ isn't trivial. We use Proposition 2.3.1 to expand

$$\frac{1}{L(\hat{\psi}_2,u^2)}=(1-u^2)^{-\lambda}\prod_{j=1}^{M}(1-q^{1/2}e^{i\theta_j,\psi}u^2)^{-1}=\left(\sum_{h=0}^{\infty}u^{2h}\right)^{\lambda}\prod_{j=1}^{M}\sum_{h=0}^{\infty}q^{h/2}e^{ih\theta_j,\psi}u^{2h}.$$

We expand again to get

$$\frac{1}{L(\hat{\psi}_2,u^2)}=\sum_{h=0}^{\infty}\alpha_\psi(h)u^h \tag{2.5.5}$$

and bounding trivially gives $|\alpha_\psi(h)|\leq h^{\deg(N_E)}q^{h/4}$.

If $\hat{\psi}_2$ is trivial, then $1/L(\hat{\psi}_2,u^2)=1-qu^2$ and so $\alpha_\psi(0)=1$, $\alpha_\psi(2)=-q$, and it is 0 everywhere else, which is the case of [7] Lemma 2.2. We use the bound $|\alpha_\psi(h)|\leq h^{\deg(N_E)}q^{h/2}$ to deal with both cases at once.

For the two remaining products, we use

$$(1-\hat{\psi}_2(Q)u^{2\deg(Q)})^{-1}=\sum_{h=0}^{\infty}\hat{\psi}_2(Q^h)u^{2h\deg(Q)}$$

to get

$$\frac{\prod_{Q|M_\psi}(1-\hat{\psi}(Q)\chi_Q(P)u^{\deg(Q)})}{\prod_{Q|PN_\psi}(1-\hat{\psi}_2(Q)u^{2\deg(Q)})}=\sum_{h=0}^{\infty}\left(\sum_{\substack{Q_1|M_\psi\\ Q_2|(PN_\psi)^\infty\\ \deg(Q_1)+2\deg(Q_2)=h}}\mu(Q_1)\hat{\psi}(Q_1)\chi_{Q_1}(P)\hat{\psi}_2(Q_2)\right)u^h. \tag{2.5.6}$$

We multiply the series (2.5.4), (2.5.5), and (2.5.6) and we compare powers of u in Equation (2.5.3). We put the result into Equation (2.5.2) to conclude. □

We now compute the size of $\mathcal{H}_{N,C}$ in a similar fashion, but we use Perron's formula instead of multiplying the generating series together.

Lemma 2.5.2. *For $(C,N_E)=1$ and any $\epsilon>0$*

$$|\mathcal{H}_{N,C}|=\frac{q^N}{|(\mathbb{F}_q[t]/(N_E))^*|}(1-q^{-1})\prod_{\substack{Q|N_E\\ Q\text{ prime}}}(1+q^{-\deg(Q)})^{-1}+\mathcal{O}_{E,q,\epsilon}(q^{N(1/4+\epsilon)}).$$

In particular, the family $\mathcal{H}_N^*$ is equidistributed in the invertible congruence classes modulo N_E as $N\to\infty$. Furthermore, $|\mathcal{H}_{N,C}|\asymp_{E,q}q^N$.

Proof. We deal with the congruence condition using (2.5.1). So

$$\sum_{D\in\mathcal{H}_{N,C}}1=\frac{1}{|(\mathbb{F}_q[t]/(N_E))^*|}\sum_{\psi\bmod N_E}\overline{\psi}(C)\sum_{D\in\mathcal{H}_N}\psi(D) \tag{2.5.7}$$

and we write the generating series as

$$\mathcal{L}(\psi,u):=\sum_{h=0}^{\infty}\left(\sum_{D\in\mathcal{H}_h}\psi(D)\right)u^h=\prod_{Q\text{ prime}}(1+\psi(Q)u^{\deg(Q)})=\frac{\prod_Q(1-\psi_2(Q)u^{2\deg(Q)})}{\prod_Q(1-\psi(Q)u^{\deg(Q)})}$$
$$=\frac{\prod_Q(1-\hat{\psi}(Q)u^{\deg(Q)})^{-1}\prod_{Q|M_\psi}(1-\hat{\psi}(Q)u^{\deg(Q)})}{\prod_Q(1-\hat{\psi}_2(Q)u^{2\deg(Q)})^{-1}\prod_{Q|N_\psi}(1-\hat{\psi}_2(Q)u^{2\deg(Q)})}=\frac{L(\hat{\psi},u)\prod_{Q|M_\psi}(1-\hat{\psi}(Q)u^{\deg(Q)})}{L(\hat{\psi}_2,u^2)\prod_{Q|N_\psi}(1-\hat{\psi}_2(Q)u^{2\deg(Q)})}$$

where $\psi_2:=\psi^2$, $\psi=\hat{\psi}\psi_0$ and $\psi_2=\hat{\psi}_2(\psi_2)_0$ as in Equation (2.2.1). The modulus of ψ_0 is denoted by M_ψ and the modulus of $(\psi_2)_0$ is denoted by N_ψ. Perron's formula works by dividing the generating series by u^{N+1} in order to create a pole at $u=0$ such that its residue is the Nth coefficient of the series. Here

$$\frac{\mathcal{L}(\psi,u)}{u^{N+1}}=\sum_{h=0}^{\infty}\left(\sum_{D\in\mathcal{H}_h}\psi(D)\right)u^{h-N-1}.$$

This sum is the Laurent expansion of $\frac{\mathcal{L}(\psi,u)}{u^{N+1}}$ at $u=0$, so the residue at $u=0$ is the coefficient of u^{-1}, which is

$$\sum_{D\in\mathcal{H}_N}\psi(D).$$

We're going to use Cauchy's residue theorem by integrating on the complex circle $\mathcal{C}_\epsilon : |u| = q^{-1/4-\epsilon}$ the following function

$$\frac{\mathcal{L}(\psi,u)}{u^{N+1}} = \frac{L(\hat{\psi},u)\prod_{Q|M_\psi}(1-\hat{\psi}(Q)u^{\deg(Q)})}{L(\hat{\psi}_2,u^2)\prod_{Q|N_\psi}(1-\hat{\psi}_2(Q)u^{2\deg(Q)})}\frac{1}{u^{N+1}}. \tag{2.5.8}$$

If $\hat{\psi}$ is trivial

$$L(\hat{\psi},u) = \frac{1}{1-qu}$$

and it has a unique simple pole at $u=1/q$ of residue $-1/q$. If $\hat{\psi}$ isn't trivial, then

$$L(\hat{\psi},u) = (1-u)^{\lambda_\psi}\prod_{j=1}^{K_\psi}(1-q^{1/2}e^{i\theta_{\psi,j}}u)$$

where $K_\psi \leq \deg(N_E)$ and it has no poles. If $\hat{\psi}_2$ is trivial

$$\frac{1}{L(\hat{\psi}_2,u^2)} = 1-qu^2$$

and it has no poles. If $\hat{\psi}_2$ isn't trivial

$$\frac{1}{L(\hat{\psi}_2,u^2)} = (1-u)^{-\lambda_{\psi_2}}\prod_{j=1}^{K_{\psi_2}}(1-q^{1/2}e^{i\theta_{\psi_2,j}}u^2)^{-1}$$

where $K_{\psi_2}\leq\deg(N_E)$ and it has poles of norm $q^{-1/4}$. The two remaining products of (2.5.8) have poles and zeros of norm one.

We define

$$A(E,q,\epsilon) := \sup_{\psi \bmod N_E}\sup_{|u|=q^{-1/4-\epsilon}}\left|\frac{L(\hat{\psi},u)\prod_{Q|M_\psi}(1-\hat{\psi}(Q)u^{\deg(Q)})}{L(\hat{\psi}_2,u^2)\prod_{Q|N_\psi}(1-\hat{\psi}_2(Q)u^{2\deg(Q)})}\right|.$$

We have $A(E,q,\epsilon)<\infty$ since these functions have no poles on $\mathcal{C}_\epsilon$. We also have $|1/u^{N+1}| = q^{N(1/4+\epsilon)+1/4+\epsilon}$ on $\mathcal{C}_\epsilon$, so

$$\left|\oint_{\mathcal{C}_\epsilon}\frac{\mathcal{L}(\psi,u)}{u^{N+1}}\right| \leq 2\pi A(E,q,\epsilon)q^{N(1/4+\epsilon)} \ll_{E,q,\epsilon} q^{N(1/4+\epsilon)}. \tag{2.5.9}$$

If $\hat{\psi}$ is trivial, then ψ is the principal character modulo N_E. In this case, we have by Cauchy's residue theorem

$$\frac{1}{2\pi i}\oint_{\mathcal{C}_\epsilon}\frac{\mathcal{L}(\psi,u)}{u^{N+1}} = \mathrm{Res}_{u=0}\frac{\mathcal{L}(\psi,u)}{u^{N+1}} + \mathrm{Res}_{u=1/q}\frac{\mathcal{L}(\psi,u)}{u^{N+1}} = \sum_{D\in\mathcal{H}_N}\psi(D) + (q^{-1}-1)q^N \prod_{\substack{Q|N_E\\ Q \text{ prime}}}(1+q^{-\deg(Q)})^{-1}$$

since $\hat{\psi}_2$ is also trivial, and M_ψ and N_ψ are both equal to the product of all the primes dividing N_E.
If ψ isn't the principal character modulo N_E, then there is only a pole at $u=0$ and

$$\frac{1}{2\pi i}\oint_{\mathcal{C}_\epsilon}\frac{\mathcal{L}(\psi,u)}{u^{N+1}} = \sum_{D\in\mathcal{H}_N}\psi(D).$$

We use those two results along with (2.5.9) in (2.5.7) to get

$$\sum_{D\in\mathcal{H}_{N,C}} 1 = \frac{q^N}{|(\mathbb{F}_q[t]/(N_E))^*|}(1-q^{-1})\prod_{\substack{Q|N_E\\ Q \text{ prime}}}(1+q^{-\deg(Q)})^{-1} + \mathcal{O}_{E,q,\epsilon}(q^{N(1/4+\epsilon)}).$$

By Proposition 1.4 and 1.6 [54] we have $|(\mathbb{F}_q[t]/(N_E))^*| \asymp q^{\deg(N_E)}$, so we can conclude

$$|\mathcal{H}_{N,C}| \asymp_{E,q} q^N.$$

□

2.6 Contribution of the Primes

The contribution of the primes in Equation (2.9.1) corresponds to the terms with $d=1$, which is

$$S_C(N,n) := \frac{-1}{q^n|\mathcal{H}_{N,C}|}\sum_{P\in\mathcal{P}_n} n(\alpha_P+\overline{\alpha}_P)\sum_{D\in\mathcal{H}_{N,C}}\chi_D(P).$$

We start with a lemma that will be useful for bounding some quantities coming from the sieve.

Lemma 2.6.1.

$$\sum_{\substack{Q|N_E^\infty\\ \deg(Q)=N}} 1 \le (N+1)^{\deg(N_E)}$$

Proof. In the worst case scenario, N_E is a product of distinct primes of degree one. We use induction on the degree of N_E. If N_E is prime, then there is only the possibility $Q = N_E^N$, the lemma is true in this case. Now, we assume the lemma is true for $\deg(N_E) = k$. Let $\deg(N_E) = k+1$ and fix a prime P_0 that divides N_E. We split the terms depending on the powers of P_0 dividing them

$$\sum_{\substack{Q \mid N_E^\infty \\ \deg(Q)=N}} 1 = \sum_{j=0}^{N} \sum_{\substack{Q \mid (N_E/P_0)^\infty \\ \deg(Q)=N-j}} 1 \leq (N+1)^{k+1}$$

and this concludes the induction. □

Proposition 2.6.2. *For any $\epsilon > 0$ and $N > 4\deg(N_E)$*

$$S_C(N,n) \ll_{E,q} (n+N)N^{2\deg(N_E)+3}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}}\right).$$

Proof. We apply the sieve (Proposition 2.5.1) and quadratic reciprocity

$$\chi_D(P) = (-1)^{\deg(D)\deg(P)(q-1)/2}\chi_P(D)$$

to write

$$S_C(N,n) = \frac{-1}{q^n|\mathcal{H}_{N,C}|}\sum_{P\in\mathcal{P}_n} n(\alpha_P + \overline{\alpha}_P)\frac{1}{|(\mathbb{F}_q[t]/(N_E))^*|}\sum_{\psi \bmod N_E}\overline{\psi}(C)\sum_{k=0}^{N}\sum_{m=0}^{k}\alpha_\psi(m)\sum_{\ell=0}^{\lfloor\frac{k-m}{2n}\rfloor}$$

$$\sum_{\substack{Q_1 \mid M_\psi \\ Q_2 \mid \tilde{N}_\psi^\infty \\ \deg(Q_1)+2\deg(Q_2)=k-m-2n\ell}} (-1)^{n(N-k)(q-1)/2}\mu(Q_1)\hat{\psi}(Q_1)\chi_{Q_1}(P)\hat{\psi}_2(Q_2P^\ell)\sum_{D\in\mathcal{M}_{N-k}}\hat{\psi}\chi_P(D) \tag{2.6.1}$$

where we split the sum over Q_2 according to powers of P, so we define $\tilde{N}_\psi := N_\psi/P$ if $P \mid N_\psi$, and $\tilde{N}_\psi := N_\psi$ if $P \nmid N_\psi$. Assume first that $n \leq N/4$. The degree of the conductor of $\hat{\psi}\chi_P$ is then bounded by $N/4 + \deg(N_E)$. Then, when $N - k \geq N/4 + \deg(N_E)$, the sum over the monic polynomials is zero, so it is bounded by $q^{N/4+\deg(N_E)}$. Using Lemma 2.5.2 and Lemma 2.6.1 and noticing Q_1 has at most $2^{\deg(N_E)}$ possibilities gives

$$S_C(N,n) \ll_{E,q} \frac{N^{2\deg(N_E)+3}}{q^{N/8}} \tag{2.6.2}$$

by bounding everything else trivially. Therefore, the contribution of the primes of low degrees tends to zero as $N \to \infty$.

Now, assume $n > N/4$. We also assume $N > 4\deg(N_E)$ so that $\hat{\psi}\chi_P$ is primitive. We split into two cases depending on whether $k \geq \epsilon N$ or $k < \epsilon N$.

We start with the case $k \geq \epsilon N$. We want to bring the sum over P inside in order to use the explicit formula (Lemma 2.4.2). The sum is then

$$\frac{-1}{q^n|\mathcal{H}_{N,C}|}\frac{1}{|(\mathbb{F}_q[t]/(N_E))^*|}\sum_{\psi \bmod N_E}\overline{\psi}(C)\sum_{k\geq\epsilon N}^{N}\sum_{m=0}^{k}\alpha_\psi(m)\sum_{\ell=0}^{\lfloor\frac{k-m}{2n}\rfloor}\sum_{\substack{Q_1|M_\psi\\ Q_2|\tilde{N}_\psi^\infty\\ \deg(Q_1)+2\deg(Q_2)=k-m-2n\ell}} \tag{2.6.3}$$
$$\mu(Q_1)\hat{\psi}(Q_1)\hat{\psi}_2(Q_2)\sum_{D\in\mathcal{M}_{N-k}}\hat{\psi}(D)\sum_{P\in\mathcal{P}_n}n(\alpha_P+\overline{\alpha}_P)\chi_D(P)\chi_{Q_1}(P)\hat{\psi}_2(P^\ell)$$

where we reapplied quadratic reciprocity on $\chi_P(D)$. Let $\Psi := \chi_{DQ_1}\hat{\psi}_2^\ell$ and $\Psi = \hat{\Psi}\Psi_0$ as in (2.2.1). The explicit formula for $L(E\otimes\hat{\Psi}, u)$ gives the bound

$$\sum_{d|n}\sum_{P\in\mathcal{P}_{n/d}}(n/d)(\alpha_P^d+\overline{\alpha}_P^d)\hat{\Psi}^d(P) \ll_E Nq^n.$$

It is important to mention here that the conductor of $\hat{\Psi}$ might not be coprime to N_E. The Riemann hypothesis is still valid for $L(E\otimes\hat{\Psi}, u)$, but the number of zeros given in Proposition 4.2.2 could be changed by a quantity bounded by $2\deg(N_E)$, which is why the bound remains valid. This bound also holds when $\hat{\Psi}$ is trivial, since then we get $L(E,u)$ which has $\deg(N_E)-4$ zeros of norm $1/q$ and two of norm $1/\sqrt{q}$. Now, since

$$\sum_{d|n}\sum_{P\in\mathcal{P}_{n/d}}(n/d)(\alpha_P^d+\overline{\alpha}_P^d)\hat{\Psi}^d(P) = \sum_{P\in\mathcal{P}_n}n(\alpha_P+\overline{\alpha}_P)\hat{\Psi}(P) + \sum_{\substack{d|n\\ d>1}}\sum_{P\in\mathcal{P}_{n/d}}(n/d)(\alpha_P^d+\overline{\alpha}_P^d)\hat{\Psi}^d(P)$$

and

$$\sum_{\substack{d|n\\ d>1}}\sum_{P\in\mathcal{P}_{n/d}}(n/d)(\alpha_P^d+\overline{\alpha}_P^d)\hat{\Psi}^d(P) = \mathcal{O}(nq^n)$$

we have

$$\sum_{P\in\mathcal{P}_n}n(\alpha_P+\overline{\alpha}_P)\hat{\Psi}(P) \ll_E q^n(N+n). \tag{2.6.4}$$

Also, we have

$$\sum_{P\in\mathcal{P}_n} n(\alpha_P+\overline{\alpha}_P)\Psi(P)=\sum_{P\in\mathcal{P}_n} n(\alpha_P+\overline{\alpha}_P)\hat{\Psi}(P)-\sum_{\substack{P\in\mathcal{P}_n\\ P|K_\Psi}} n(\alpha_P+\overline{\alpha}_P)\hat{\Psi}(P)$$

where K_Ψ is the modulus of Ψ_0. We have assumed $n>N/4$ and $N>4\deg(N_E)$, so only χ_D can contribute to K_Ψ, and it contributes at most two different primes. So

$$\sum_{P\in\mathcal{P}_n} n(\alpha_P+\overline{\alpha}_P)\Psi(P)=\sum_{P\in\mathcal{P}_n} n(\alpha_P+\overline{\alpha}_P)\hat{\Psi}(P)+\mathcal{O}(nq^{n/2}).$$

Then

$$\sum_{P\in\mathcal{P}_n} n(\alpha_P+\overline{\alpha}_P)\Psi(P)\ll_E q^n(N+n).$$

This sum is exactly the sum over $\mathcal{P}_n$ in (2.6.3). We use $|\alpha_\psi(m)|\le q^{k/2}N^{\deg(N_E)}$ from Lemma 2.5.1 since $m\le k$ and we bound everything else trivially as we did for (2.6.2). We get that (2.6.3) is bounded by

$$\ll_{E,q}\frac{(n+N)N^{2\deg(N_E)+3}}{q^{\epsilon N/2}} \tag{2.6.5}$$

which goes to zero as $N\to\infty$.

For the case $k<\epsilon N$, we apply duality (Lemma 2.3.2) to (2.6.1) to get

$$\begin{aligned}\frac{-1}{q^n|\mathcal{H}_{N,C}|}\sum_{P\in\mathcal{P}_n} n(\alpha_P+\overline{\alpha}_P)\frac{1}{|(\mathbb{F}_q[t]/(N_E))^*|}\sum_{\psi \bmod N_E}\overline{\psi}(C)\sum_{k=0}^{\lfloor\epsilon N\rfloor}\sum_{m=0}^{k}\alpha_\psi(m)\sum_{\ell=0}^{\lfloor\frac{k-m}{2n}\rfloor} \\ \sum_{\substack{Q_1|M_\psi\\ Q_2|\tilde{N}_\psi^\infty\\ \deg(Q_1)+2\deg(Q_2)=k-m-2n\ell}}(-1)^{n(N-k)(q-1)/2}\mu(Q_1)\hat{\psi}(Q_1)\chi_{Q_1}(P)\hat{\psi}_2(Q_2P^\ell) \\ \omega(\hat{\psi}\chi_P)q^{N-k-(n+\deg(C_{\hat{\psi}}))/2}\sum_{r=0}^{n+\deg(C_{\hat{\psi}})-1-N+k}\sigma_{\hat{\psi}\chi_P}(r)\sum_{D\in\mathcal{M}_{n+\deg(C_{\hat{\psi}})-1-N+k-r}}\overline{\hat{\psi}\chi_P}(D)\end{aligned} \tag{2.6.6}$$

where $C_{\hat{\psi}}$ is the conductor of $\hat{\psi}$.

The goal is again to sum over $\mathcal{P}_n$ first in order to use the explicit formula (Lemma 2.4.2). To bring the sum inside, we must deal with $\omega(\hat{\psi}\chi_P)$ to remove its dependency on P.

Definitions related to Gauss sums can be found at the end of Section 2.2. Corollary 2.4 [20] states that for primitive characters of conductor F

$$\omega(\chi) = \begin{cases} \frac{1}{\tau(\chi)} q^{-(\deg(F)-1)/2} G(\chi) & \text{if } \chi \text{ odd} \\ q^{-\deg(F)/2} G(\chi) & \text{if } \chi \text{ even} \end{cases}$$

and adjusting Lemma 2.12 (i) [20] for general Dirichlet characters gives

$$G(\hat{\psi}\chi_P) = \hat{\psi}(P)\chi_P(C_{\hat{\psi}})G(\hat{\psi})G(\chi_P)$$

because $\deg(P)$ is large enough for P to be coprime to $C_{\hat{\psi}}$. Then, assuming the most complicated case where all characters are odd

$$\begin{aligned} \omega(\hat{\psi}\chi_P) &= \frac{1}{\tau(\hat{\psi}\chi_P)} q^{-(\deg(C_{\hat{\psi}})+n-1)/2} G(\hat{\psi}\chi_P) = \frac{1}{\tau(\hat{\psi}\chi_P)} q^{-(\deg(C_{\hat{\psi}})+n-1)/2} \hat{\psi}(P)\chi_P(C_{\hat{\psi}})G(\hat{\psi})G(\chi_P) \\ &= \frac{1}{\tau(\hat{\psi}\chi_P)} q^{-1/2} \hat{\psi}(P)\chi_P(C_{\hat{\psi}})\omega(\hat{\psi})\tau(\hat{\psi})\omega(\chi_P)\tau(\chi_P). \end{aligned}$$

If $\deg(P)$ is even, then $\chi_P(a) = 1$ for all $a \in \mathbb{F}_q^*$ and if $\deg(P)$ is odd, $\chi_P(a) = 1$ if a is a square in $\mathbb{F}_q^*$ and $\chi_P(a) = -1$ otherwise. This implies $\tau(\hat{\psi}\chi_P)$ and $\tau(\chi_P)$ does not depend on the actual P, only on its degree, since the sum defining these quantities is over $\mathbb{F}_q^*$. We recall $\omega(\chi_P) = 1$ since χ_P is quadratic. This implies

$$\omega_n(\hat{\psi}) := \frac{\omega(\hat{\psi}\chi_P)}{\hat{\psi}(P)\chi_P(C_{\hat{\psi}})}$$

only depends on $\deg(P) = n$, hence the notation.

The other quantity that might depend on P is $\sigma_{\hat{\psi}\chi_P}(r)$. We recall that it only depends on the parity of the character, and by the discussion above, the parity of $\hat{\psi}\chi_P$ only depends on $\hat{\psi}$ and the degree of P. We therefore use the notation $\sigma_{\hat{\psi},n}(r) := \sigma_{\hat{\psi}\chi_P}(r)$.

Replacing in (2.6.6) gives

$$\frac{-1}{q^n|\mathcal{H}_{N,C}|}\frac{1}{|(\mathbb{F}_q[t]/(N_E))^*|}\sum_{\psi \bmod N_E}\overline{\psi}(C)\sum_{k=0}^{\lfloor \epsilon N\rfloor}\sum_{m=0}^{k}\alpha_\psi(m)\sum_{\ell=0}^{\lfloor\frac{k-m}{2n}\rfloor}\sum_{\substack{Q_1|M_\psi\\ Q_2|\tilde{N}_\psi^\infty\\ \deg(Q_1)+2\deg(Q_2)=k-m-2n\ell}} \tag{2.6.7}$$

$$\mu(Q_1)\hat{\psi}(Q_1)\hat{\psi}_2(Q_2)\omega_n(\hat{\psi})q^{N-k-(n+\deg(C_{\hat{\psi}}))/2}\sum_{r=0}^{n+\deg(C_{\hat{\psi}})-1-N+k}(-1)^{n(n-r-1)(q-1)/2}$$

$$\sigma_{\hat{\psi},n}(r)\sum_{D\in\mathcal{M}_{n+\deg(C_{\hat{\psi}})-1-N+k-r}}\overline{\hat{\psi}}(D)\sum_{P\in\mathcal{P}_n}n(\alpha_P+\overline{\alpha}_P)\chi_D(P)\hat{\psi}(P)\chi_{C_{\hat{\psi}}}(P)\chi_{Q_1}(P)\hat{\psi}_2(P^\ell)$$

after applying quadratic reciprocity on $\chi_P(D)$ and $\chi_P(C_{\hat{\psi}})$. We use (2.6.4) to bound the sum over $\mathcal{P}_n$. We have an extra $\hat{\psi}\chi_{C_{\hat{\psi}}}$ in the character, so it adds at most $2\deg(N_E)$ to the degree of the conductor. Bounding everything else trivially, we have that (2.6.7) is

$$\ll_{E,q}(n+N)N^{2\deg(N_E)+3}q^{n/2}q^{-N+\epsilon N/2}.$$

Combining this bound with (2.6.2) and (2.6.5) concludes to proof. □

2.7 Contribution of the Squares

The contribution of the squares comes from the terms with even d in Equation (2.9.1).

Proposition 2.7.1.

$$\frac{-1}{q^n|\mathcal{H}_{N,C}|}\sum_{\substack{d|n\\2|d}}\sum_{\deg(P)=n/d}(n/d)(\alpha_P^d+\overline{\alpha}_P^d)\sum_{D\in\mathcal{H}_{N,C}}\chi_D^d(P)=\begin{cases}1+\mathcal{O}_E\left(\tau(n)q^{-n/4}\right), & \text{if } 2\,|\,n\\ 0, & \text{if } 2\nmid n\end{cases}$$

where $\alpha_P^d+\overline{\alpha}_P^d$ is replaced by a_P^d for bad primes.

Proof. If $2\nmid n$, there are no terms, hence no contribution.

When $2\mid n$, we rewrite the sum as

$$\frac{-1}{q^{2m}|\mathcal{H}_{N,C}|}\sum_{d|m}\sum_{\deg(P)=m/d}(m/d)\left(\alpha_P^{2d}+\overline{\alpha_P}^{2d}\right)\sum_{D\in\mathcal{H}_{N,C}}\chi_D^{2d}(P) \tag{2.7.1}$$

where $m := n/2$. The character equals $\mathbb{1}_{P\nmid D}$ because its power is even. A simple sieving gives

$$\sum_{\substack{D\in\mathcal{H}_{N,C}\\(D,P)=1}} 1 = \sum_{j=0}^{\lfloor N/\deg(P)\rfloor} (-1)^j \sum_{D\in\mathcal{H}_{N-j\deg(P),CP^{-j}}} 1$$

if $(P, N_E) = 1$ so that P is invertible modulo N_E. If $P \mid N_E$, then

$$\sum_{\substack{D\in\mathcal{H}_{N,C}\\(D,P)=1}} 1 = |\mathcal{H}_{N,C}|$$

since every D is coprime to N_E because $(C, N_E) = 1$. In the case $(P, N_E) = 1$, the sum with $j = 0$ is exactly $|\mathcal{H}_{N,C}|$. When $j > 0$

$$\sum_{j=1}^{\lfloor N/\deg(P)\rfloor} (-1)^j \sum_{D\in\mathcal{H}_{N-j\deg(P),CP^{-j}}} 1 \asymp \sum_{j=1}^{\lfloor N/\deg(P)\rfloor} (-1)^j q^{N-j\deg(P)} \ll q^{N-\deg(P)} \sum_{j=0}^{\infty} q^{-j\deg(P)} \ll q^{N-\deg(P)}.$$

Then

$$\sum_{D\in\mathcal{H}_{N,C}} \chi_D^{2d}(P) = |\mathcal{H}_{N,C}| + \mathcal{O}(q^{N-\deg(P)}) \tag{2.7.2}$$

which holds in both cases.

Now, (2.7.1) is equal to

$$\frac{-1}{q^{2m}} \sum_{d|m} \sum_{\deg(P)=m/d} (m/d) \left(\alpha_P^{2d} + \overline{\alpha_P}^{2d}\right) + \mathcal{O}\left(\tau(m) q^{-m}\right).$$

We retrieve the double sum by looking at the symmetric square of $L(E, u)$, which is defined by

$$L(\mathrm{Sym}^2 E, u) := \prod_{P\nmid N_E} \left(1-\alpha_P^2 u^{\deg(P)}\right)^{-1} \left(1-\alpha_P\overline{\alpha}_P u^{\deg(P)}\right)^{-1} \left(1-\overline{\alpha}_P^2 u^{\deg(P)}\right)^{-1} \prod_{P|N_E} (1-a_P^2 u^{\deg(P)})^{-1}.$$

It is related to the variety

$$\mathrm{Sym}^2 E : y^2 = (x^3 + Ax + B)(z^3 + Az + B).$$

It is known that ([9] Theorem 1.1)

$$L^*(\mathrm{Sym}^2 E, u) = \prod_{j=1}^{M} (1 - q^{3/2} e^{i\theta_{\mathrm{Sym}^2 E,j}} u)$$

for some $M < \infty$ that only depends on E. We have

$$\sum_{d|m} \sum_{\deg(P)=m/d} (m/d) \left(\alpha_P^{2d} + q^{d\cdot\deg(P)} + \overline{\alpha_P}^{2d}\right) = q^{3m/2} \sum_{j=1}^{M} e^{im\theta_{\mathrm{Sym}^2 E,j}} + \mathcal{O}(q^m)$$

where we replace $\alpha_P^{2d} + q^{d\cdot\deg(P)} + \overline{\alpha_P}^{2d}$ by a_P^{2d} for bad primes. By Proposition 2.1 of [54], we have

$$\sum_{d|m} \sum_{\deg(P)=m/d} (m/d) q^{d\cdot\deg(P)} = q^{2m}$$

and we split the sum as

$$\sum_{d|m} \sum_{\deg(P)=m/d} (m/d) q^{d\cdot\deg(P)} = \sum_{d|m} \sum_{\substack{\deg(P)=m/d \\ P \text{ good}}} (m/d) q^{d\cdot\deg(P)} + \sum_{d|m} \sum_{\substack{\deg(P)=m/d \\ P \text{ bad}}} (m/d) q^{d\cdot\deg(P)}.$$

Since there are at most $\deg(N_E)$ bad primes

$$\sum_{d|m} \sum_{\substack{\deg(P)=m/d \\ P \text{ bad}}} (m/d) q^{d\cdot\deg(P)} \ll \deg(N_E) m q^m.$$

This implies

$$\sum_{d|m} \sum_{\deg(P)=m/d} (m/d) \left(\alpha_P^{2d} + \overline{\alpha_P}^{2d}\right) = -q^{2m} + \mathcal{O}_E(q^{3m/2})$$

where we replace $\alpha_P^{2d} + \overline{\alpha_P}^{2d}$ by a_P^{2d} for bad primes and this concludes the proof. □

2.8 Contribution of Higher Powers

Proposition 2.8.1.

$$\frac{1}{q^n |\mathcal{H}_{N,C}|} \sum_{\substack{d|n \\ d>2}} \sum_{\deg(P)=n/d} (n/d)(\alpha_P^d + \overline{\alpha}_P^d) \sum_{D \in \mathcal{H}_{N,C}} \chi_D^d(P) \ll \tau(n) q^{-n/6}.$$

Proof. We bound everything trivially. □

2.9 Average of Traces

The main theorem of this paper is the following.

Theorem 2.9.1. *For $\epsilon > 0$, $n > 0$, and $N > 4\deg(N_E)$*

$$\langle \operatorname{tr} \Theta^n \rangle_{N,C} = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd} \end{cases} + \mathcal{O}_{E,q}\left((n+N)N^{2\deg(N_E)+3}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}}\right) + \tau(n)q^{-n/6}\right).$$

Proof. By the explicit formula (Lemma 2.4.2)

$$\langle \operatorname{tr} \Theta^n \rangle_{N,C} = \frac{-1}{q^n |\mathcal{H}_{N,C}|} \sum_{d|n} \sum_{\deg(P)=n/d} (n/d)(\alpha_P^d + \overline{\alpha}_P^d) \sum_{D \in \mathcal{H}_{N,C}} \chi_D^d(P) \tag{2.9.1}$$

Combining each estimate of Sections 2.6, 2.7, and 2.8 concludes the proof. □

2.10 One-level Density

The definition of Z_ϕ is given by (2.1.3).

Corollary 2.10.1. *For $\phi \in \mathcal{S}(\mathbb{R})$ an even function such that $\operatorname{supp}(\hat{\phi}) \subset (-1,1)$, we have*

$$\langle Z_\phi \rangle_{N,C} = \int_{O(M)} Z_\phi(\Theta) d\Theta + \mathcal{O}_{E,q}(1/N)$$

where $M = 2N + \deg(N_E) - 2$.

Proof. The Fourier expansion of $Z_\phi(\Theta)$ is

$$Z_\phi(\Theta) = \int_{\mathbb{R}} \phi(x)dx + \frac{1}{M}\sum_{n \neq 0} \hat{\phi}\left(\frac{n}{M}\right) \operatorname{tr} \Theta^n.$$

When n is negative, we use $\operatorname{tr} \Theta^{-n} = \overline{\operatorname{tr} \Theta^n}$ to apply Theorem 2.9.1. Averaging over $\mathcal{H}_{N,C}$ and applying Theorem 2.9.1 gives

$$\begin{aligned} \langle Z_\phi \rangle_{N,C} &= \hat{\phi}(0) + \frac{1}{M}\sum_{n \neq 0} \hat{\phi}\left(\frac{n}{M}\right) \eta_n \\ &\quad + \mathcal{O}_{E,q}\left(\frac{1}{M}\sum_{n=1}^{\infty} \hat{\phi}\left(\frac{n}{M}\right)\left((n+N)N^{2\deg(N_E)+3}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}}\right) + \tau(n)q^{-n/6}\right)\right) \end{aligned}$$

where

$$\eta_n = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

By Equation (2.1.2)

$$\hat{\phi}(0) + \frac{1}{M}\sum_{n\neq 0}\hat{\phi}\left(\frac{n}{M}\right)\eta_n = \int_{O(M)} Z_\phi(\Theta)d\Theta. \tag{2.10.1}$$

For the error term, we have that

$$(n+N)N^{2\deg(N_E)+3}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}}\right)$$

tends to zero as $N \to \infty$ provided that $n < 2(1-2\epsilon)N$. The range of n is controlled by restricting the support of $\hat{\phi}$, so it must be inside $(-1,1)$ since $M \sim 2N$ as $N \to \infty$. For the second term of the error, notice that

$$\sum_{n=1}^{\infty}\tau(n)q^{-n/6}$$

converges, so

$$\frac{1}{M}\sum_{n=1}^{\infty}\hat{\phi}\left(\frac{n}{M}\right)\tau(n)q^{-n/6}$$

tends to zero as $N \to \infty$. □

Remark 1. *By (6) [66], we cannot distinguish between the symmetry types O, $SO(even)$, and $SO(odd)$ since they all have the same one-level density when the support of $\hat{\phi}$ is contained inside $(-1,1)$.*

2.11 Average Rank and Non-vanishing

One application of the one-level density is getting a bound on the average analytic rank.

Theorem 2.11.1. *The family $\mathcal{H}_{N,C}$ of quadratic twists of an elliptic curve over $\mathbb{F}_q[t]$ has average analytic rank $r_C \leq 3/2$.*

Proof. We adjust [66] Section 5.5. We use Corollary 2.10.1 with

$$\phi_\nu(x) = \left(\frac{\sin(\pi\nu x)}{\pi\nu x}\right)^2, \quad \hat{\phi}_\nu(y) = \frac{1}{\nu}\left(1 - \frac{|y|}{\nu}\right)$$

where $\hat{\phi}_\nu$ is supported in $[-\nu,\nu]$ and is the Fourier transform of ϕ_ν. Since $\phi_v(0) = 1$ and $\phi_v(x) \geq 0$, we have $F(0) \geq 1$ and $F(\theta) \geq 0$, where we defined $F(\theta)$ in Section 2.2. This implies $\mathrm{ord}_{u=1/q}L(E\otimes\chi_D,u) \leq Z_{\phi_\nu}(\Theta_D)$, so $r_{N,C} \leq \langle Z_{\phi_\nu}\rangle_{N,C}$. By Corollary 2.10.1

$$r_{N,C} \leq \int_{O(M)} Z_{\phi_\nu}(\Theta)d\Theta + \mathcal{O}_{E,q}(1/N).$$

By Equation (2.10.1), we need to evaluate

$$\begin{aligned}\hat{\phi}_\nu(0) + \frac{1}{M}\sum_{n\neq 0}\hat{\phi}_\nu\left(\frac{n}{M}\right)\eta_n &= \frac{1}{\nu} + \frac{2}{M\nu}\sum_{n=1}^{\lfloor M\nu/2\rfloor}\left(1-\frac{2n}{M\nu}\right)\\ &= \frac{1}{\nu} + \frac{2}{M\nu}\left(\lfloor M\nu/2\rfloor - \frac{2}{M\nu}\sum_{n=1}^{\lfloor M\nu/2\rfloor} n\right)\\ &= \frac{1}{\nu} + \frac{2}{M\nu}\left(M\nu/2 + \mathcal{O}(1) - \frac{2}{M\nu}\left(\frac{M^2\nu^2}{8} + \mathcal{O}(M\nu)\right)\right)\\ &= \frac{1}{\nu} + \frac{1}{2} + \mathcal{O}\left(\frac{1}{M\nu}\right).\end{aligned}$$

Setting $\nu = 1-\epsilon$ for any $\epsilon > 0$, we have

$$r_{N,C} \leq \frac{1}{1-\epsilon} + \frac{1}{2} + \mathcal{O}_{E,q}(1/N)$$

meaning that

$$\text{limsup}_{N\to\infty} r_{N,C} \leq 3/2.$$

If the limit exists, then

$$r_C \leq 3/2.$$

We remark that unlike [7], we cannot optimize the choice of the test function in order to improve our result as in [36] Appendix A, Corollary 2 since the symmetry is orthogonal. □

Let ϵ and ϵ_D be the sign of the functional equation of $L(E,u)$ and $L(E\otimes\chi_D,u)$ respectively. They are both ± 1.

Lemma 2.11.2. *The order of the central zero* $\text{ord}_{u=1/q}L(E\otimes\chi_D,u)$ *is even or odd depending on whether* $\epsilon_D = 1$ *or* $\epsilon_D = -1$ *respectively.*

Proof. Since $L(E,u)\in\mathbb{Z}[u]$, we also have $L(E\otimes\chi_D,u)\in\mathbb{Z}[u]$ because χ_D is quadratic. The functional equation is then

$$L\left(E\otimes\chi_D, \frac{1}{q^2u}\right) = \frac{1}{\epsilon_D u^M q^M} L(E\otimes\chi_D,u)$$

where M is the number of zeros of $L(E\otimes\chi_D,u)$. Applying the functional equation twice shows that $\epsilon_D = \pm 1$.

If $(1/q)e^{i\theta_j}$ is a zero of $L(E\otimes\chi_D,u)$, then $(1/q)e^{-i\theta_j}$ is also a zero by the functional equation. This means all zeros come in pairs expect those at $u=-1/q$ and $u=1/q$. We have

$$\epsilon_D=\prod_{i=1}^{M}-e^{i\theta_j}=(-1)^M(-1)^{\mathrm{ord}_{u=-1/q}L(E\otimes\chi_D,u)}$$

So for example if $\epsilon_D=1$ and M is even, then $\mathrm{ord}_{u=-1/q}L(E\otimes\chi_D,u)$ must be even and $\mathrm{ord}_{u=1/q}L(E\otimes\chi_D,u)$ must be even too. The argument is the same for the other cases. □

Theorem 2.11.3. *At least* 12.5% *of the family of quadratic twists of an elliptic curve have rank zero and at least* 37.5% *have rank one as* $N\to\infty$.

Proof. By (1.2) [8]

$$\epsilon_D=\alpha\cdot\epsilon\cdot\chi_{M_E}(D)$$

for $D\in\mathcal{H}_N^*$ where M_E is the product of the primes of multiplicative reduction of E, $\alpha=\pm1$ depending only on the degree of D, and χ_{M_E} is the unique quadratic Dirichlet character of conductor M_E. We recall that we assume $M_E\neq1$. Since χ_{M_E} is periodic modulo M_E and since $M_E\mid N_E$, we have that χ_{M_E} is constant on $\mathcal{H}_{N,C}$.

We recall that we split $\mathcal{H}_N^*=\mathcal{H}_{N,+}\cup\mathcal{H}_{N,-}$ depending on if $\epsilon_D=1$ or $\epsilon_D=-1$ respectively.

Let $\chi_{N_E}(D):=\mathbb{1}_{(D,N_E)=1}\chi_{M_E}(D)$, which is a Dirichlet character modulo N_E since $M_E\mid N_E$. We have $\chi_{N_E}=\chi_{M_E}$ on $\mathcal{H}_N^*$ since all elements are coprime to N_E. By Lemma 2.5.2, $\mathcal{H}_N^*$ becomes equidistributed modulo N_E as N grows, and since $\chi_{N_E}=1$ on half of $(\mathbb{F}_q[t]/(N_E))^*$ and $\chi_{N_E}=-1$ on the other half, we have

$$|\mathcal{H}_{N,+}|\sim|\mathcal{H}_{N,-}|\sim\frac{|\mathcal{H}_N^*|}{2}\quad\text{as } N\to\infty. \tag{2.11.1}$$

By Theorem 2.11.1, assuming all limits exist, the average analytic rank is $\leq 3/2$ for both $\mathcal{H}_{N,+}$ and $\mathcal{H}_{N,-}$, since both sets are disjoint unions of congruence classes modulo N_E. Then, by Lemma 2.11.2, the rank must be zero for at least 25% of the twists of $\mathcal{H}_{N,+}$, and for $\mathcal{H}_{N,-}$, the rank must be one for at least 75% of the twists in order to satisfy the bound as $N\to\infty$. We must divide these quantities by two to conclude. □

Remark 2. *We have the relation*

$$\epsilon_D=(-1)^M det\ \Theta_D=(-1)^{deg(N_E)}det\ \Theta_D$$

where M is the number of zeros of $L(E \otimes \chi_D, u)$. When $\deg(N_E)$ is even, the matrix Θ_D lies in $SO(M)$ or $O(M)\backslash SO(M)$ depending on if $D \in \mathcal{H}_{N,+}$ or $D \in \mathcal{H}_{N,-}$ respectively. Since M is even, the twists from $\mathcal{H}_{N,+}$ have SO(even) symmetry, and the twists from $\mathcal{H}_{N,-}$ have SO(odd) symmetry.

When $\deg(N_E)$ is odd, the matrix Θ_D lies in $SO(M)$ or $O(M)\backslash SO(M)$ depending on if $D \in \mathcal{H}_{N,-}$ or $D \in \mathcal{H}_{N,+}$ respectively. Since M is odd, the twists from $\mathcal{H}_{N,-}$ have SO(odd) symmetry, and the twists from $\mathcal{H}_{N,+}$ have SO(even) symmetry.

By (2.11.1), the twists from $\mathcal{H}_N^*$ have orthogonal symmetry. See (6) [66] for a table of statistics of the one-level density of some symmetry types.

Remark 3. *The Katz and Sarnak philosophy predicts that Corollary 2.10.1 should hold without any restriction on the support of $\hat{\phi}$. However, it is important to integrate over the appropriate symmetry group, since it matters when the support of $\hat{\phi}$ is greater than $(-1, 1)$. Then, we expect the average analytic rank of the family of twists from $\mathcal{H}_N^*$ to converge to $1/2$ as $N \to \infty$. For the family of twists from $\mathcal{H}_{N,+}$, we expect an average analytic rank of zero, and for $\mathcal{H}_{N,-}$ we expect an average of one. In other words, we expect half of the twists from $\mathcal{H}_N^*$ to have rank zero, and the other half to have rank one. Numerical computations done by Baig and Hall [1] seem to support these conjectures, even when N is small.*

Remark 4. *The contribution of the primes can be trivially bounded using the Riemann hypothesis (Proposition 4.2.2)*

$$S(N, n) := \sum_{D \in \mathcal{H}_N^*} \sum_{\deg(P)=n} (n/d)(\alpha_P + \overline{\alpha}_P)\chi_D(P) = \mathcal{O}_{E,q}(Nq^{n+N}).$$

The analogue of Hypothesis M from [26] is

$$S(N, n) = o_{E,q}(q^{n+N}).$$

This bound implies that the contribution of the primes goes to zero as $N \to \infty$ for any n, which is what we need to remove the restriction on the support of $\hat{\phi}$ and to show that the average analytic rank is $1/2$.

2.12 Trivial Bound for Arbitrary Order

We now study the one-level density when the order $\ell \neq 2$ of the Dirichlet characters is coprime to q. Using the Lindelöf hypothesis, we obtain the following restriction on the support of the Fourier transform of the test functions

$$\operatorname{supp} \hat{\phi} \subset \left(-\frac{1}{2}, \frac{1}{2}\right).$$

This is the analogue of $\operatorname{supp} \hat{\phi} \subset (-1, 1)$ for cubic Dirichlet L-functions. It is not clear how to use duality to extend the support in this case, as was done for quadratic characters. By restricting to a subfamily (of density zero), David and Güloğlu [22] were able to increase the support for cubic Dirichlet L-functions over $\mathbb{Q}(\zeta_3)$.

Theorem 2.12.1. *For $\phi \in \mathcal{S}(\mathbb{R})$ an even function such that $\operatorname{supp}(\hat{\phi}) \subset (-1/2, 1/2)$, we have for the one-level density of the family of twists of order $\ell \neq 2$ and $(\ell, q) = 1$*

$$\langle Z_\phi \rangle_{N,C} = \int_{U(M)} Z_\phi(\Theta) d\Theta + \mathcal{O}_{E,q,\ell}(1/N)$$

where $M = 2N + \deg(N_E) - 2$.

Proof. Let $a > 1$ be a divisor of ℓ and let k be the smallest integer such that $a \mid q^k - 1$, so k depends on a. We fix an isomorphism ψ from the a-roots of unity in $\mathbb{F}_{q^k}$ to those in $\mathbb{C}$ and we define the a-power residue symbol as

$$\left(\frac{A}{\mathfrak{q}}\right)_a := \psi\left(A^{\frac{q^k \deg(\mathfrak{q}) - 1}{a}} \bmod \mathfrak{q}\right)$$

for $A, \mathfrak{q} \in \mathbb{F}_{q^k}[t]$ where $\mathfrak{q}$ is prime. If $\mathfrak{q} \mid A$, the symbol equals zero by definition. This symbol is a Dirichlet character of modulus $\mathfrak{q}$ of order a over $\mathbb{F}_{q^k}[t]$. Let Frob_q act on $\mathbb{F}_{q^k}[t]$ by raising each coefficient to the qth power. On $\mathbb{F}_{q^k} \subset \mathbb{F}_{q^k}[t]$, this operator permutes the a-roots of unity and can be associated via ψ to some $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_a)/\mathbb{Q})$ which generates a normal cyclic subgroup $H \trianglelefteq \operatorname{Gal}(\mathbb{Q}(\zeta_a)/\mathbb{Q})$ of order k. Furthermore, we have

$$\left(\frac{\operatorname{Frob}_q(A)}{\operatorname{Frob}_q(\mathfrak{q})}\right)_a = \sigma\left(\frac{A}{\mathfrak{q}}\right)_a.$$

Now, over $\mathbb{F}_q[t]$, a prime modulus has primitive Dirichlet characters of order a if and only if its degree is divisible by k. In other words, the modulus must split totally in the extension

$\mathbb{F}_{q^k}[t]$. Moduli of prime powers do not have primitive characters of order a. For each prime Q such that $k \mid \deg(Q)$, we define $\chi_{a,Q,i}$ for $1 \le i \le \phi(a)$ to be the collection of characters of order a with conductor Q, and they are $\mathrm{Gal}(\mathbb{Q}(\zeta_a)/\mathbb{Q})$ conjugates. We extend this definition to composite conductors by multiplicativity. In the following generating series, we consider all primitive characters of order $a \mid \ell$ of conductor of degree h for $a > 1$. In the Euler product, we include for each prime all of its possible characters of order $a > 1$ dividing ℓ. Let $|u| = q^{-1/2-\epsilon}$ for any $\epsilon > 0$. We have

$$\mathcal{L}_P(u) := \sum_{h=0}^{\infty} \left(\sum_{\substack{\chi \text{ of order } a|\ell \\ \chi \text{ primitive} \\ \deg(\mathrm{cond}(\chi))=h \\ (\mathrm{cond}(\chi),N_E)=1 \\ a>1}} \chi(P) \right) u^h = \prod_{\substack{Q \text{ prime} \\ Q \nmid N_E}} \left(1 + \sum_{\substack{a|\ell \\ a \mid q^{\deg(Q)}-1 \\ a>1}} \sum_{i=1}^{\phi(a)} \chi_{a,Q,i}(P) u^{\deg(Q)} \right)$$

$$= \left(\prod_{Q \text{ prime}} \prod_{\substack{a|\ell \\ a \mid q^{\deg(Q)}-1 \\ a>1}} \prod_{i=1}^{\phi(a)} (1 - \chi_{a,Q,i}(P) u^{\deg(Q)})^{-1} + \mathcal{O}_{\epsilon,\ell,q}(1) \right) \cdot$$

$$\prod_{\substack{Q \text{ prime} \\ Q | N_E}} \left(1 + \sum_{\substack{a|\ell \\ a \mid q^{\deg(Q)}-1 \\ a>1}} \sum_{i=1}^{\phi(a)} \chi_{a,Q,i}(P) u^{\deg(Q)} \right)^{-1}$$

The error comes from the fact that the terms $u^{j \deg(Q)}$ with $j \ge 2$ in the product are negligible over $C_\epsilon : |u| = q^{-1/2-\epsilon}$, since there are at most q^m primes of degree m and the sum

$$\sum_{m=1}^{\infty} q^m q^{(-1-2\epsilon)m}$$

converges absolutely. We also have

$$\prod_{\substack{Q \text{ prime} \\ Q | N_E}} \left(1 + \sum_{\substack{a|\ell \\ a \mid q^{\deg(Q)}-1 \\ a>1}} \sum_{i=1}^{\phi(a)} \chi_{a,Q,i}(P) u^{\deg(Q)} \right)^{-1} \ll_{E,\ell,q} 1$$

over C_ϵ. Now, we fix $a > 1$ dividing ℓ and we collect the primes Q having characters of order a. Let k be the smallest integer such that $a \mid q^k - 1$. When we write "$\mathfrak{q}$ totally split" under the product, we mean that the prime in $\mathbb{F}_q[t]$ under $\mathfrak{q}$ splits completely in $\mathbb{F}_{q^k}[t]$. We have

$$\prod_{\substack{Q \text{ prime} \\ a \mid q^{\deg(Q)}-1}} \prod_{i=1}^{\phi(a)} (1 - \chi_{a,Q,i}(P) u^{\deg(Q)})^{-1} = \prod_{i=1}^{\phi(a)/k} \prod_{\substack{\mathfrak{q} \in \mathbb{F}_{q^k}[t] \\ \mathfrak{q} \text{ prime} \\ \mathfrak{q} \text{ totally split}}} (1 - \chi_{a,\mathfrak{q},i}(P) u^{k \deg(\mathfrak{q})})^{-1}$$

by defining

$$\chi_{a,\mathfrak{q},i}(A) := \sigma_i \left(\frac{A}{\mathfrak{q}} \right)_a$$

where the σ_i are a set of representatives of $\mathrm{Gal}(\mathbb{Q}(\zeta_a)/\mathbb{Q})/H$ where H was defined above. Since $\mathrm{Frob}_q(P) = P$, and since a character of conductor $\mathfrak{q}$ of order a over $\mathbb{F}_{q^k}[t]$ restricted to $\mathbb{F}_q[t]$ gives a character of conductor Q of order a over $\mathbb{F}_q[t]$, we have a one-to-one correspondence between these characters. By the a-power reciprocity law ([54] Theorem 3.5)

$$\prod_{\substack{\mathfrak{q} \in \mathbb{F}_{q^k}[t] \\ \mathfrak{q} \text{ prime} \\ \mathfrak{q} \text{ totally split}}} (1 - \chi_{a,\mathfrak{q},i}(P) u^{k \deg(\mathfrak{q})})^{-1} = L_{q^k}(\chi_{a,P,i}, (-1)^{\frac{q^k-1}{a} \deg(P)} u^k) \prod_{\substack{\mathfrak{q} \in \mathbb{F}_{q^k}[t] \\ \mathfrak{q} \text{ prime} \\ \mathfrak{q} \text{ not totally split}}} (1 - \chi_{a,\mathfrak{q},i}(P) u^{k \deg(\mathfrak{q})})$$

where the index q^k indicates that the L-function is taken over $\mathbb{F}_{q^k}[t]$. When $\mathfrak{q}$ is not totally split, we have $k \deg(\mathfrak{q}) \geq 2 \deg(Q)$, so the last product converges absolutely on C_ϵ since the number of primes above a given prime Q is bounded by ℓ. Finally, by the Lindelöf hypothesis ([20] Lemma 2.6), we have for any $\delta > 0$

$$L_{q^k}(\chi_{a,P,i}, u^k) \ll_{q,\delta} q^{k\delta \deg(P)} \qquad \text{for } |u| \leq q^{-1/2}.$$

Combining everything gives

$$\mathcal{L}_P(u) \ll_{q,\delta,\epsilon,E,\ell} q^{\delta \deg(P)}$$

on C_ϵ. We now apply Perron's formula

$$\sum_{\substack{\chi \text{ of order } a \mid \ell \\ \chi \text{ primitive} \\ \deg(\mathrm{cond}(\chi)) = h \\ (\mathrm{cond}(\chi), N_E) = 1 \\ a > 1}} \chi(P) = \frac{1}{2\pi i} \oint_{C_\epsilon} \frac{\mathcal{L}_P(u)}{u^h} \frac{du}{u}.$$

Since $\mathcal{L}_P(u)$ is entire inside C_ϵ and since $|1/u^{h+1}| \leq q^{(1/2+\epsilon)h+1}$, we have

$$\sum_{\substack{\chi \text{ of order } a \mid \ell \\ \chi \text{ primitive} \\ \deg(\mathrm{cond}(\chi)) = h \\ (\mathrm{cond}(\chi), N_E) = 1 \\ a > 1}} \chi(P) \ll_{q,\delta,\epsilon,E,\ell} q^{h/2} q^{\epsilon h} q^{\delta \deg(P)}$$

for any $\epsilon, \delta > 0$. Since this holds for any ℓ, we may isolate the characters of order ℓ

$$\sum_{\substack{\chi \text{ of order } \ell \\ \chi \text{ primitive} \\ \deg(\text{cond}(\chi))=h \\ (\text{cond}(\chi),N_E)=1}} \chi(P) \ll_{q,\delta,\epsilon,E,\ell} q^{h/2} q^{\epsilon h} q^{\delta \deg(P)}.$$

As in the quadratic case, the average of traces is given by

$$\langle \text{tr } \Theta^n \rangle_N = \frac{1}{q^n |\mathcal{F}_N|} \sum_{d|n} \sum_{\deg(P)=n/d} (n/d)(\alpha_P^d + \overline{\alpha}_P^d) \sum_{\substack{\chi \text{ of order } \ell \\ \chi \text{ primitive} \\ \deg(\text{cond}(\chi))=N \\ (\text{cond}(\chi),N_E)=1}} \chi^d(P)$$

where $\mathcal{F}_N$ denotes the family of primitive twists of order ℓ of conductor of degree N coprime to N_E. Using $|\mathcal{F}_N| \asymp q^N$ and the above, we have

$$\langle \text{tr } \Theta^n \rangle_N \ll_{q,\epsilon,E,\ell} n^2 q^{n/2} q^{-N/2} q^{\epsilon(n+N)}$$

since χ^2 isn't principal and higher powers are trivially bounded. This translates to a restriction of $(-1/2, 1/2)$ on the support of the test function for the one-level density. The symmetry is unitary since the contribution of the primes vanishes. □

We remark that for even twists, the L-functions are missing two zeros of norm $1/q$ compared to odd twists for conductors of the same degree. We show in this section how to go over the family by considering the set of all L-functions that have the same number of zeros of norm $1/q$. We show this change has no influence on the results. We can control the parity of the characters here by fixing $s := (\ell, q-1)$ and $\tilde{\chi}$ a character of order s on $\mathbb{F}_q^*$. The indexing of the collection $\{\chi_{a,Q,i}\}_{1 \le i \le \phi(a)}$ of characters over $\mathbb{F}_q[t]$ described above is now important. We set $\chi_{a,Q,1}$ to be any character from the collection such that it is equal to $\tilde{\chi}^{t_a \deg(Q)}$ when restricted to $\mathbb{F}_q^*$ where $t_a = (\ell, q-1)/(a, q-1)$. Then, we set the other characters as $\chi_{a,Q,i} := \chi_{a,Q,1}^{b_{a,i}}$ where $b_{a,i}$ is the ith element of $(\mathbb{Z}/a\mathbb{Z})^*$. To keep track of the values of the characters over $\mathbb{F}_q^*$, we modify the Euler product as

$$\prod_{\substack{Q \text{ prime} \\ Q \nmid N_E}} \left(1 + \sum_{\substack{a|\ell \\ a|q^{\deg(Q)}-1 \\ a>1}} \sum_{i=1}^{\phi(a)} \chi_{a,Q,i}(P) \zeta_s^{r t_a b_{a,i} \deg(Q)} u^{\deg(Q)} \right)$$

where ζ_s is the sth complex root of unity and $0 \leq r \leq s-1$. Doing so will change the L-function obtained above as

$$L_{q^k}(\chi_{a,P,i}, (-1)^{\frac{q^k-1}{a}\deg(P)}(\zeta_s^{rt_a b_{a,i}}u)^k)$$

so it doesn't change the bound we obtained

$$\sum_{\substack{\chi \text{ of order } \ell \\ \chi \text{ primitive} \\ \deg(\text{cond}(\chi))=h \\ (\text{cond}(\chi),N_E)=1}} \chi(P)\zeta_s^{rb(\chi)} \ll_{q,\delta,\epsilon,E,\ell} q^{h/2}q^{\epsilon h}q^{\delta \deg(P)}$$

where $0 \leq b(\chi) \leq s-1$ is the unique number such that

$$\chi|_{\mathbb{F}_q^*} = \tilde{\chi}^{b(\chi)}.$$

We can now control the congruence of $b(\chi)$ modulo s by summing over all r

$$\sum_{\substack{\chi \text{ of order } \ell \\ \chi \text{ primitive} \\ \deg(\text{cond}(\chi))=h \\ (\text{cond}(\chi),N_E)=1 \\ b(\chi)\equiv c \bmod s}} \chi(P) = \frac{1}{s}\sum_{r=0}^{s-1}\zeta_s^{-rc} \sum_{\substack{\chi \text{ of order } \ell \\ \chi \text{ primitive} \\ \deg(\text{cond}(\chi))=h \\ (\text{cond}(\chi),N_E)=1}} \chi(P)\zeta_s^{rb(\chi)}$$

so the bound also holds for this sum. We know that χ is even if and only if $b(\chi) \equiv 0 \bmod s$, so controlling the congruence gives us control over the genus.

2.13 Acknowledgments

I would like to thank Chantal David, my doctoral thesis advisor, for the idea of this project, for her support, her help, and the various improvements she suggested. I would also like to thank the Fonds de recherche du Québec - Nature et technologies (Bourse de doctorat 200482) for their financial support. Finally, thanks to the anonymous reviewer for all the corrections and improvements.

Chapter 3

On the Vanishing of Twisted L-functions of Elliptic Curves over Rational Function Fields

This second paper is joint work with Chantal David, Matilde Lalín, and Wanlin Li. It presents numerical data computed for the family of Dirichlet twists of an elliptic curve over function fields. By computing explicit Dirichlet L-functions, we were able to contradict some conjectures of David-Fearnley-Kisilevsky and Mazur-Rubin for constant elliptic curves in the function field setting.

This paper has been accepted for publication in the proceedings of the Fifteenth Algorithmic Number Theory Symposium. It has been reformatted for this thesis. The paper uses different notations than the rest of this thesis.

On the Vanishing of Twisted L-functions of Elliptic Curves over Rational Function Fields

Antoine Comeau-Lapointe, *Concordia University*

Chantal David, *Concordia University*

Matilde Lalín, *Université de Montréal*

Wanlin Li, *Centre de Recherches Mathématiques*

Abstract. We investigate in this paper the vanishing at $s = 1$ of the twisted L-functions of elliptic curves E defined over the rational function field $\mathbb{F}_q(t)$ (where $\mathbb{F}_q$ is a finite field of q elements and characteristic ≥ 5) for twists by Dirichlet characters of prime order $\ell \geq 3$, from both a theoretical and numerical point of view. In the case of number fields, it is predicted that such vanishing is a very rare event, and our numerical data seems to indicate that this is also the case over function fields for non-constant curves. For constant curves, we adapt the techniques of [40, 24] who proved vanishing at $s = 1/2$ for infinitely many Dirichlet L-functions over $\mathbb{F}_q(t)$ based on the existence of one, and we can prove that if there is one χ_0 such that $L(E, \chi_0, 1) = 0$, then there are infinitely many. Finally, we provide some examples which show that twisted L-functions of constant elliptic curves over $\mathbb{F}_q(t)$ behave differently than the general ones.

Keywords: Nonvanishing of L-functions; Twisted L-functions of Elliptic Curves; Function Fields; Elliptic Curve Rank in Extensions

3.1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ with L-function $L(E, s) = \sum_n a_n n^{-s}$, and χ be a Dirichlet character. Let $L(E, \chi, s) = \sum_n a_n \chi(n) n^{-s}$ be the twisted L-function. By the Birch and Swinnerton-Dyer conjecture, the vanishing of $L(E, \chi, s)$ at $s = 1$ should be related to the growth of the rank of the Mordell-Weil group of E in the abelian extension of $\mathbb{Q}$ associated to χ. Heuristics based on the distribution of modular symbols and random matrix theory ([19, Conjecture 1.2], [44]) have led to conjectures predicting that the vanishing of the twisted L-functions $L(E, \chi, s)$ at $s = 1$ is a very rare event as χ ranges over characters of prime order $\ell \geq 3$. For instance, it is predicted that there are only finitely many characters χ

of order $\ell > 5$ such that $L(E, \chi, 1) = 0$. Mazur and Rubin rephrased this in terms of "Diophantine Stability", and conjectured that if E is an elliptic curve over $\mathbb{Q}$ and $K/\mathbb{Q}$ is any real abelian extension such that K contains only finitely many subfields of degree $2, 3$, or 5 over $\mathbb{Q}$, then the group of K-rational points $E(K)$ is finitely generated. They also proved that for each ℓ (under some hypotheses that can be shown to hold in certain contexts), there are infinitely many cyclic extensions $K/\mathbb{Q}$ of order ℓ such that $E(K) = E(\mathbb{Q})$ (and then, assuming the Birch and Swinnerton-Dyer conjecture, such that the twisted L-functions $L(E, \chi, s)$ associated to the extensions $K/\mathbb{Q}$ do not vanish) [45].

We remark that the case of vanishing of quadratic twists is very different from the higher order case $\ell \geq 3$ considered in this work, as the L-function of E twisted by a quadratic character of conductor D corresponds to the L-function of another elliptic curve E_D, and for half of the quadratic twists, $L(E, \chi_D, 1) = 1$. Goldfeld has conjectured that half of the twists $E_D/\mathbb{Q}$ have rank 0, and half have rank 1 (asymptotically) [31]). Furthermore, Gouvea and Mazur [32] have shown that the analytic rank of E_D is at least two for $\gg X^{1/2-\epsilon}$ of the quadratic discriminants $|D| \leq X$. It is conjectured that the number of such discriminants $|D| \leq X$ should be asymptotic to $C_E X^{3/4} \log^{b_E}(X)$ [17], for some constants C_E and b_E depending on the curve E. The case of nonabelian extensions $K/\mathbb{Q}$ of degree d with Galois group S_d is also different from the abelian extensions of order $\ell \geq 3$: in recent work, Lemke Oliver and Thorne [39] showed that there are infinitely many such extensions where $\text{rank}(E(K)) > \text{rank}(E(\mathbb{Q}))$, for each $d \geq 2$, and Fornea [29] has shown that for some curves $E/\mathbb{Q}$, the analytic rank of E increases for a positive proportion of the quintic fields with Galois group S_5.

The vanishing (and non-vanishing) of twisted L-functions of elliptic curves is closely related to the one-level density, which is the study of low-lying zeroes, or the average analytic rank. This was studied over number fields and functions fields, for quadratic and higher order twists. For quadratic twists, it is possible to prove results on the one-level density strong enough to deduce that a positive proportion of twists with even (respectively odd) analytic rank do no vanish (respectively vanish of order 1) at the central critical point [35, 16]. The one-level density, or average rank, of higher order twists for elliptic curves L-functions was studied by [10] over number fields and [49, 16] over function fields. Quadratic twists of elliptic curve over functions fields were also studied by [8] who obtained results on the correlation of the analytic ranks of two twisted elliptic curves. The behavior of the algebraic rank of elliptic curves in cyclic extensions of $\mathbb{Q}$ was investigated by Beneish, Kundu, and Ray [3].

We investigate in this article the vanishing at $s = 1$ of the twisted L-functions of elliptic curves E defined over the rational function field $\mathbb{F}_q(t)$, [1] for twists by Dirichlet characters of prime order $\ell \geq 3$, from both a theoretical and numerical point of view. It is natural to ask if the recent results of Li [40] and Donepudi and Li [24], who have found infinitely many instances of vanishing for L-functions of Dirichlet characters at $s = 1/2$, can be extended to L-functions of elliptic curves twisted by Dirichlet characters. We find that this is the case when E is a constant elliptic curve over $\mathbb{F}_q(t)$[2], and we can produce infinitely many cases of vanishing at the central critical point for characters of order ℓ provided we find one (Theorem 3.1.2). Then, the conjectures of [19, 46] do not hold in the special case of constant elliptic curves, and we present specific numerical examples in Section 3.5.2.

We also study non-constant elliptic curves over $\mathbb{F}_q(t)$ where q is a power of a prime $p \geq 5$, say $E : y^2 = x^3 + a(t)x + b(t)$, for some polynomials $a(t), b(t) \in \mathbb{F}_q[t]$. The L-function of $E/\mathbb{F}_q(t)$ is defined analogously as for $E/\mathbb{Q}$, by an infinite Euler product over the primes of $\mathbb{F}_q(t)$ (see (3.2.6)), but in this case, it follows from the work of Weil and Deligne that, after setting $u = q^{-s}$, $L(E, s) = \mathcal{L}(E, u)$, a polynomial in $\mathbb{Z}[u]$. Similarly, the twisted L-function $\mathcal{L}(E, \chi, u)$ is a polynomial in $\mathbb{Z}[\zeta_\ell][u]$, where χ is a Dirichlet character of order ℓ over $\mathbb{F}_q(t)$. More details and all relevant definitions are given in Section 3.2.

We present in Section 3.5.3 computational results for the vanishing of numerous twists of two base elliptic curves over $\mathbb{F}_q(t)$, the Legendre curve and a second curve, chosen to have good reduction at infinity. The data seems to indicate that the conjectures of [19, 46] also hold for non-constant elliptic curves over function fields, while presenting some unexpected features. To our knowledge, this is the first data about the vanishing of L-functions of elliptic curves twisted by characters of order $\ell \geq 3$, over function fields. The case of quadratic twists of elliptic curves over function fields was considered by Baig and Hall [1] to test Goldfeld's conjecture in that context, and our numerical computations are similar.

The case of a constant curve $E/\mathbb{F}_q(t)$ is defined by taking an elliptic curve $E_0/\mathbb{F}_q$ and considering its base change to $\mathbb{F}_q(t)$, denoted by $E = E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(t)$. In this case, the roots of $\mathcal{L}(E, \chi, u)$ can be described in terms of the roots of the L-functions $\mathcal{L}(E_0, u)$ and $\mathcal{L}(C, u)$, where the L-functions are respectively associated to the elliptic curve $E_0/\mathbb{F}_q$ and the ℓ-cyclic

[1] Throughout this article, we assume that $\mathbb{F}_q$ is a finite field of q elements and characteristic ≥ 5.

[2] Constant elliptic curves, i.e. elliptic curves over $\mathbb{F}_q$ considered as a curve over $\mathbb{F}_q(t)$, were studied by many authors because of their special properties. In particular, Milne showed that the Birch and Swinnerton-Dyer conjecture is true for constant elliptic curves [50].

cover C over $\mathbb{P}^1_{\mathbb{F}_q}$ corresponding to the Dirichlet character χ (see Section 3.3). This allows us to use a generalized version of the results of Li [40] and Donepudi–Li [24] about vanishing of the Dirichlet L-functions $\mathcal{L}(\chi, u)$ to obtain some vanishing for $\mathcal{L}(E, \chi, u)$ at $u = q^{-1}$. The argument of [40, 24] has two distinct parts, first finding one character χ_0 such that $\mathcal{L}(\chi_0, u_0) = 0$ for some fixed u_0, and then sieving to produce infinitely many such characters. The order of q mod ℓ is related to the presence/absence of ℓ-th roots of unity in $\mathbb{F}_q(t)$, which makes the study of the characters of order ℓ delicate, and the authors of [40, 24] restrict to the Kummer case where $q \equiv 1 \bmod \ell$. As we need to treat all the cases (in particular, we often work over the finite field $\mathbb{F}_p$ where p is prime), we generalize their sieving beyond the Kummer case. We also need to consider vanishing at any u_0 where $\mathcal{L}(E_0, u_0) = 0$, and not only $u_0 = q^{-1/2}$ as in their work.

We recall that an algebraic integer α is called a q-Weil integer if $|\alpha| = q^{1/2}$ under every complex embedding.

Theorem 3.1.1. *Let ℓ be a prime and q be a prime power coprime to ℓ. Let u_0 be a q-Weil integer. Suppose there exists a Dirichlet character χ_0 over $\mathbb{F}_q(t)$ of order ℓ and with conductor of degree d_0 such that $\mathcal{L}(\chi_0, u_0^{-1}) = 0$. Then, there are at least $\gg q^{2n/d_0}$ Dirichlet characters χ of order ℓ over $\mathbb{F}_q(t)$ with conductor of degree bounded by n such that $\mathcal{L}(\chi, u_0^{-1}) = 0$.*

We prove the above theorem in Section 3.4. The next result is then a direct consequence of Theorem 3.1.1, using the properties of constant elliptic curves discussed in Section 3.3.

Theorem 3.1.2. *Let E_0 be an elliptic curve over $\mathbb{F}_q$, and let $E = E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(t)$. Suppose there exists a Dirichlet character χ_0 over $\mathbb{F}_q(t)$ of order ℓ and with conductor of degree d_0 such that $\mathcal{L}(E, \chi_0, q^{-1}) = 0$. Then, there are at least $\gg q^{2n/d_0}$ Dirichlet characters χ of order ℓ over $\mathbb{F}_q(t)$ with conductor of degree bounded by n such that $\mathcal{L}(E, \chi, q^{-1}) = 0$.*

Then, to guarantee that a constant elliptic curve $E/\mathbb{F}_q(t)$ has infinitely many twists of order ℓ such that $L(E, \chi, u)$ vanishes at q^{-1}, it suffices to find one. Using the results of Section 3.3, this can be rephrased in terms of finding curves $C/\mathbb{F}_q$ which are ℓ-cyclic covers of $\mathbb{P}^1_{\mathbb{F}_q}$ and such that $\mathcal{L}(E_0, u)$ divides $\mathcal{L}(C, u)$, and we investigate this question numerically in Section 3.5.2, where we find isogeny classes of elliptic curves E_0 over different prime fields such that $\mathcal{L}(E, \chi, q^{-1}) = 0$ for characters χ of prime order $\ell = 3, 5, 7, 11$. One observation from the data is the existence of supersingular curves defined over primes fields $\mathbb{F}_p$ which admit a degree ℓ cyclic map to $\mathbb{P}^1$ ramifying at 4 points where $p \equiv -1 \bmod \ell$. The existence

of such curves does not follow from previous results on the topic and one may hope to prove this statement following the strong evidence presented in Table 1.

It is natural to ask if the same dichotomy (no instances of vanishing or infinitely many cases of vanishing) also holds for non-constant elliptic curves over $\mathbb{F}_q(t)$, but there is no reason to believe it would be the case. The ideas leading to the proof of Theorem 3.1.2 for constant curves do not apply to the general case, as the change of variable trick used to produce infinitely many extensions where E acquires points would send points on E to points on a different elliptic curve when E is not constant. However, there are results of that type for an elliptic curve E over $\mathbb{Q}$ due to Fearnley, Kisilevsky, and Kuwata [25], where the authors prove that if there is one cyclic cubic field K such that $E(K)$ is infinite, then there are infinitely many, and there are always infinitely many such K when $E(\mathbb{Q})$ contains at least 6 points. On the non-vanishing side, Brubaker, Bucur, Chinta, Frechette and Hoffstein [4] use the method of multiple Dirichlet series to prove that if there exists a single non-vanishing order ℓ twist of an L–function associated to a cuspidal automorphic representation of $GL(2, \mathbb{A}_K)$, then there are infinitely many.

The structure of this article is as follows: we define in Section 3.2 the L-functions attached to Dirichlet characters and elliptic curves over $\mathbb{F}_q(t)$, and we recall their properties. We discuss in Section 3.3 the case of L-functions of constant elliptic curves. We describe the ℓ-cyclic covers of $\mathbb{P}^1_{\mathbb{F}_q}$ and their characters in Section 3.4, for all cases (not only the Kummer case $q \equiv 1 \bmod \ell$) using the work of Bary-Soroker and Meisner [2], and we then generalize the sieves of [40, 24] to those general ℓ-cyclic covers. We then use those results to prove Theorems 3.1.1 and 3.1.2. Finally, we describe our computations in Section 3.5.1, and we present our numerical data in Sections 3.5.2 and 3.5.3.

Acknowledgments. The authors would like to thank Patrick Meisner for helpful discussions, and the anonymous referees for helpful comments that greatly improved the exposition of this paper. This work is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC Discovery Grant `155635-2019` to CD, `335412-2013` to ML), by the Fonds de recherche du Québec - Nature et technologies (Projet de recherche en équipe `300951` to CD and ML, bourse de doctorat `200482` to ACL), and by the Centre de recherches mathématiques and the Institut des sciences mathématiques (CRM-ISM postdoctoral fellowship to WL). Some of the computations were checked using the computational software MAGMA. The datasets generated and analysed during the current study are available in the GitHub repository, `https://github.com/AntoineComeau/Lfuncff`.

3.2 Dirichlet characters, elliptic curves and L-functions over $\mathbb{F}_q(t)$

3.2.1 Dirichlet characters of order ℓ

Let ℓ be a prime not dividing q. We review here the theory of Dirichlet characters of order ℓ over $\mathbb{F}_q(t)$ and their L-functions. We refer the reader to [20] and [2] for more details.

Let n_q be the multiplicative order of q modulo ℓ. We say that we are in the Kummer case if $n_q = 1$ and in the non-Kummer case otherwise. We also say that a monic irreducible polynomial $P \in \mathbb{F}_q[t]$ is n_q-divisible if $n_q \mid \deg P$.

We fix once and for all an isomorphism Ω from the ℓ-th roots of unity in $\mathbb{F}_{q^{n_q}}^*$ to μ_ℓ, the ℓ-th roots of unity in $\mathbb{C}^*$.

We first define the ℓ-th order residue symbol

$$\chi_P : \mathbb{F}_q[t]/(P) \to \mu_\ell,$$

for P an irreducible n_q-divisible monic polynomial in $\mathbb{F}_q[t]$. It is clear that the ℓ-th residue symbols χ_P can be defined only for the n_q-divisible primes P, since we must have $\ell \mid q^{\deg P}-1$: indeed, unless $n_q \mid \deg(P)$, the order of the group of non-zero elements in the residue field $\mathbb{F}_P = \mathbb{F}_q[t]/(P)$ is not divisible by ℓ, and therefore it does not contain any non-trivial ℓ-th root of unity.

For any $a \in \mathbb{F}_q[t]$, if $P \mid a$, then $\chi_P(a) = 0$, and otherwise $\chi_P(a) = \alpha$, where α is the unique ℓ-th root of unity in $\mathbb{C}^*$ such that

$$a^{\frac{q^{\deg(P)}-1}{\ell}} \equiv \Omega^{-1}(\alpha) \bmod P. \tag{3.2.1}$$

If $F \in \mathbb{F}_q[t]$ is any monic polynomial supported only on n_q-divisible primes, writing $F = P_1^{e_1} \cdots P_s^{e_s}$ with distinct primes P_i, we define

$$\chi_F = \chi_{P_1}^{e_1} \cdots \chi_{P_s}^{e_s}.$$

Then, χ_F is a character of order dividing ℓ with conductor $P_1 \cdots P_s$. Conversely, the primitive characters of order ℓ and conductor $P_1 \cdots P_s$, where the P_i are n_q-divisible primes, are given by taking all choices $1 \le e_i \le \ell - 1$. Then, the conductors of the primitive characters are the square-free monic polynomials $F \in \mathbb{F}_q[t]$ supported on n_q-divisible primes, and for each

such conductor, there are $(\ell-1)^{\omega(F)}$ such characters, where $\omega(F)$ is the number of primes dividing F.

We can also write each primitive character of order ℓ with conductor F as

$$\chi_F = \chi_{F_1}\chi_{F_2}^2 \cdots \chi_{F_{\ell-1}}^{\ell-1} \tag{3.2.2}$$

corresponding to a decomposition $F = F_1 \cdots F_\ell$ where the F_i's are square-free and coprime.

For any Dirichlet character χ, we say that χ is even if its restriction to $\mathbb{F}_q$ is trivial; otherwise, we say that χ is odd.

Dirichlet characters are also defined at the prime at infinity P_∞. The following statement clarifies how to compute $\chi(P_\infty)$.

Lemma 3.2.1. *Let F be a monic squarefree polynomial in $\mathbb{F}_q[t]$, and χ be a Dirichlet character on $\mathbb{F}_q[t]$ of order ℓ with conductor F.*

If $q \not\equiv 1 \bmod \ell$, then χ does not ramify at infinity, $\chi(P_\infty) = 1$, and χ is even.

If $q \equiv 1 \bmod \ell$, let $\chi = \chi_{F_1}\chi_{F_2}^2 \cdots \chi_{F_{\ell-1}}^{\ell-1}$ as in (3.2.2). Then,
χ ramifies at $P_\infty \iff \ell \nmid \deg(F_1F_2^2\cdots F_{\ell-1}^{\ell-1}) \iff \chi$ is odd, and

$$\chi(P_\infty) = \begin{cases} 1 & \ell \mid \deg(F_1F_2^2\cdots F_{\ell-1}^{\ell-1}), \\ 0 & \ell \nmid \deg(F_1F_2^2\cdots F_{\ell-1}^{\ell-1}). \end{cases}$$

Proof. We first discuss under which conditions the characters are odd or even. Let P be an n_q-divisible prime. We remark that for $a \in \mathbb{F}_q^*$,

$$\chi_P(a) = \Omega\left(a^{\frac{q^{\deg(P)}-1}{\ell}}\right) = \Omega\left(a^{\frac{\deg(P)(q^{n_q}-1)}{n_q\ell}}\right). \tag{3.2.3}$$

Indeed, writing $\deg(P) = n_q k$, we have

$$\frac{q^{\deg(P)}-1}{\ell} = \frac{q^{n_q k}-1}{\ell} = \frac{q^{n_q}-1}{\ell}(1 + q^{n_q} + \cdots + q^{n_q(k-1)})$$

and we use the fact that $1 + q^{n_q} + \cdots + q^{n_q(k-1)} \equiv k \bmod \ell$.

Then by applying multiplicativity to equation (3.2.3), we find

$$\chi_F(a) = \Omega\left(a^{\frac{\deg(F_1F_2^2\cdots F_{\ell-1}^{\ell-1})(q^{n_q}-1)}{n_q\ell}}\right),$$

If $n_q = 1$, then χ is trivial on $\mathbb{F}_q$ iff $\ell \mid \deg(F_1F_2^2\cdots F_{\ell-1}^{\ell-1})$.

Now suppose that $n_q > 1$. Then, $\ell \nmid (q-1)$, and in fact, $(\ell, q-1) = 1$ since ℓ is prime. Now we have that both $\ell \mid (q^{n_q}-1)$ and $(q-1) \mid (q^{n_q}-1)$. It follows that $(q-1) \mid \frac{q^{n_q}-1}{\ell}$. Since $a \in \mathbb{F}_q^*$, we have

$$\chi_F(a) = \Omega\left(a^{\frac{\deg(F_1F_2^2\cdots F_{\ell-1}^{\ell-1})(q^{n_q}-1)}{n_q\ell}}\right) = 1,$$

and therefore χ_F is an even character.

The statement that P_∞ does not ramify in the non-Kummer case follows from the fact that the cyclic field extension associated to χ_F can only ramify at primes of degree divisible by $n_q > 1$ and P_∞ is a prime of degree 1. In the Kummer case, the character χ_F is associated with the cyclic cover $y^\ell = F_1F_2^2\cdots F_\ell^{\ell-1}$, and there is ramification at P_∞ iff $\ell \nmid \deg(F_1F_2^2\cdots F_{\ell-1}^{\ell-1})$, and $\chi_F(P_\infty) = 0$ in this case. If χ_F does not ramify at P_∞, then $\chi_F(P_\infty) = 1$ since we are only considering the case in which $F_1F_2^2\cdots F_{\ell-1}^{\ell-1}$ is monic. □

3.2.2 L-functions of Dirichlet characters

Let χ be a Dirichlet character, and let $\mathcal{L}(\chi, u)$ be the Dirichlet L-function defined by

$$\mathcal{L}(\chi, u) = \prod_P (1 - \chi(P)u^{\deg P})^{-1},$$

where the product includes the prime at infinity.

We define δ_χ by

$$\delta_\chi := \begin{cases} 0 & \text{when } \chi \text{ is even,} \\ 1 & \text{when } \chi \text{ is odd,} \end{cases} \tag{3.2.4}$$

and we remark from Lemma 3.2.1 that $\chi(P_\infty) = 1 - \delta_\chi$.

For a primitive character χ of conductor F, it follows from the work of Weil [64] that $\mathcal{L}(\chi, u)$ is a polynomial of degree $\deg(F) - 2 + \delta_\chi$ and satisfies the functional equation

$$\mathcal{L}(\chi, u) = \omega_\chi\, (\sqrt{q}u)^{\deg(F)-2+\delta_\chi}\, \mathcal{L}(\overline{\chi}, 1/(qu)). \tag{3.2.5}$$

The sign of the functional equation is

$$\omega_\chi = \begin{cases} \frac{G(\chi)}{|G(\chi)|} & \text{when } \chi \text{ is even,} \\ \\ \frac{\sqrt{q}}{\tau(\chi)}\frac{G(\chi)}{|G(\chi)|} & \text{when } \chi \text{ is odd,} \end{cases}$$

where if χ odd,

$$\tau(\chi) = \sum_{a \in \mathbb{F}_q^*} \chi(a) e^{2\pi i \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)/p},$$

and for any χ, $G(\chi)$ is the Gauss sum

$$G(\chi) = \sum_{a \bmod F} \chi(a) e_q\left(\frac{a}{F}\right).$$

Here e_q is the exponential defined by Hayes [34] for any $b \in \mathbb{F}_q((1/T))$:

$$e_q(b) = e^{\frac{2\pi i \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(b_1)}{p}},$$

where b_1 is the coefficient of $1/T$ in the Laurent expansion of b. We refer the reader to [20] for a proof of those results.

3.2.3 L-functions of elliptic curves over $\mathbb{F}_q(t)$

Let E be an elliptic curve over $\mathbb{F}_q(t)$. Let P be a prime of $\mathbb{F}_q(t)$, i.e $P = P(t) \in \mathbb{F}_q[t]$ is a monic irreducible polynomial or $P = P_\infty$, the prime at infinity. If P is a prime of good reduction, then the reduction of E (which we also denote by E) is an elliptic curve over the finite field $\mathbb{F}_P = \mathbb{F}_q[t]/(P) \cong \mathbb{F}_{q^{\deg P}}$ (where $\mathbb{F}_\infty \cong \mathbb{F}_q$ since the prime at infinity has degree 1), and

$$\#E(\mathbb{F}_P) = q^{\deg P} + 1 - a_P, \quad a_P = \alpha_P + \overline{\alpha}_P, \quad |\alpha_P| = \sqrt{q^{\deg P}}.$$

Let

$$\mathcal{L}_P(E, u) := 1 - a_P u + q^{\deg P} u^2 = (1 - \alpha_P u)(1 - \overline{\alpha}_P u)$$

be the L-function of $E/\mathbb{F}_P$.

If P is a prime of bad reduction, we define

$$\mathcal{L}_P(E, u) = (1 - a_P u),$$

where $a_P = 0, 1, -1$ depending on the type of bad reduction (additive, split multiplicative, and non-split multiplicative respectively).

Let N_E be the conductor of E, which is the product of the primes of bad reduction with the appropriate powers.[3] Let M_E (respectively A_E) be the product of the multiplicative (respectively additive) primes of E. Then $N_E = M_E A_E^2$.

[3] We emphasize that we include the prime at infinity in the conductor of the elliptic curve (if the curve has bad reduction at infinity of course). Our conductor is an effective divisor, written multiplicatively.

The L-function of E is defined by

$$\mathcal{L}(E,u) := \prod_{P\nmid N_E} \mathcal{L}_P(E,u^{\deg P})^{-1} \prod_{P|N_E} \mathcal{L}_P(E,u^{\deg P})^{-1}. \tag{3.2.6}$$

It is proven by Weil [37, 1] that $\mathcal{L}(E,u)$ is a polynomial of degree[4] $\deg N_E - 4$ for any non-constant elliptic curve defined over the rational function field $\mathbb{F}_q(t)$ and it satisfies the functional equation

$$\mathcal{L}(E,u) = \omega_E\ (qu)^{\deg(N_E)-4}\mathcal{L}(E,1/(q^2u)), \tag{3.2.7}$$

where $\omega_E = \pm 1$ is the sign of the functional equation. We refer the reader to [5, Appendix] and [1] for more details.

Let χ be a Dirichlet character of order ℓ and conductor F, and suppose that $(F, N_E) = 1$. If χ is odd, we also assume that E has good reduction at P_∞ (since the prime at infinity is not included in the conductor of the Dirichlet character, we need this additional condition to ensure that the places where χ ramifies and the places of bad reduction for E are disjoint). The L-function of E twisted by χ is defined by

$$\begin{aligned}\mathcal{L}(E,\chi,u) := &\prod_{P\nmid N_E} (1-\chi(P)\alpha_P u^{\deg(P)})^{-1}(1-\chi(P)\overline{\alpha}_P u^{\deg(P)})^{-1} \\ &\times \prod_{P|N_E} (1-\chi(P)a_P u^{\deg(P)})^{-1}.\end{aligned} \tag{3.2.8}$$

Let K be the cyclic field extension of degree ℓ of $\mathbb{F}_q(t)$ corresponding to χ. Then,

$$\mathcal{L}(E/K,u) = \mathcal{L}(E,u)\prod_{i=1}^{\ell-1}\mathcal{L}(E,\chi^i,u). \tag{3.2.9}$$

It follows from the Riemann Hypothesis that

$$\mathcal{L}(E/K,u) = \prod_{j=1}^{B}\left(1-qe^{i\theta_j}u\right).$$

Since $(F_\chi, N_E) = 1$ and E has good reduction at P_∞ when χ is odd, (3.2.9) and Theorem 3.2.2 (stated and proven below) imply that $B = \ell(\deg N_E - 4) + 2(\ell-1)(\deg F + \delta_\chi)$.

[4]The formula for the degree of $\mathcal{L}(E,u)$ implies in particular that there are no non-constant elliptic curves over $\mathbb{F}_q(t)$ with conductor of degree smaller than 4, which can be thought of as the analogue to the fact that there are no elliptic curves over $\mathbb{Q}$ with conductor smaller than 11.

It is well-known that $\mathcal{L}(E,\chi,u)$ satisfies a functional equation from the work of Weil [64]. The explicit formula for the sign of the functional equation is contained in [64] in a very general context, but we need a precise formula for the numerical computations, so we deduce it below from the work of Tan and Rockmore [59, 60].

Theorem 3.2.2. *Let ℓ be a prime, χ a primitive Dirichlet character of conductor F and order ℓ, and let E be a non-constant elliptic curve with conductor N_E such that $(N_E, F) = 1$. If $P_\infty \mid N_E$, we also assume that χ is even. The L-function $\mathcal{L}(E,\chi,u)$ is a polynomial of degree*

$$\mathfrak{n} := \deg N_E + 2\deg F - 4 + 2\delta_\chi,$$

where δ_χ is given by (3.2.4). Each $\mathcal{L}(E,\chi,u)$ satisfies the functional equation

$$\mathcal{L}(E,\chi,u) = \omega_{E\otimes\chi}\,(qu)^{\mathfrak{n}}\,\mathcal{L}(E,\overline{\chi},1/(q^2u)), \tag{3.2.10}$$

where $\omega_{E\otimes\chi}$ is the sign of the functional equation for $\mathcal{L}(E,\chi,u)$, given by

$$\omega_{E\otimes\chi} = \omega_\chi^2\,\omega_E\,\chi(N_E).$$

Proof. The sign of the functional equation (and the functional equation itself) can be deduced from the modularity of elliptic curves over function fields. We follow [59, 60] who use modular symbols over function fields. They consider different normalizations, so we explain here how to adjust their work to get the result that we need. Let $K = \mathbb{F}_q(t)$. For any place v, let $\mathcal{O}_v$ be the associated ring of integers. If $N = \sum_v N_v v$ is an effective divisor over K, let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left(\begin{pmatrix} a_v & b_v \\ c_v & d_v \end{pmatrix} \right)_v \in \prod_v \mathrm{GL}_2(\mathcal{O}_v) : c \equiv 0 \bmod N \right\}.$$

Let $\mathbb{A}_K$ be the ring of adeles over K. Then $\mathbb{A}_K^*$ embeds in $\mathrm{GL}_2(\mathbb{A}_K)$ as diagonal matrices. Also $\mathrm{GL}_2(K)$ embeds in $\mathrm{GL}_2(\mathbb{A}_K)$ by the diagonal map.

A $\mathbb{C}$-valued function on $\mathrm{GL}_2(\mathbb{A}_K)$ is called a modular function of level N if it satisfies that $f(\gamma\tau\kappa) = f(\tau)$ for all $\tau \in \mathrm{GL}_2(\mathbb{A}_K)$, $\gamma \in \mathrm{GL}_2(K)$, and $\kappa \in \mathbb{A}_K^* \cdot \Gamma_0(N)$. It is a fundamental result that if E is a non-constant elliptic curve over K, then there is a normalized cuspidal modular function f of level N_E such that the L-function of E is the L-function of f. This also holds for the twisted L-functions. To make that statement precise, and use it to get the functional equation, we will follow the notation of [59, 60], where the L-functions are normalized differently (and we will go back to our L-function at the end). Let f be

the normalized cuspidal modular function corresponding to E, χ a Dirichlet character of conductor coprime to N_E and we define as [59, (1.10)]

$$L_f(\chi, s) = \sum_M \frac{c_f(M)\chi(M)}{|M|^{s-1}},$$

where M runs through all effective divisors, χ is naturally extended over effective divisors, and the $c_f(M)$ are the normalized coefficients obtained from the Fourier expansion of f. This is also true when χ is a quasi-character, which for our purposes is the product of a Dirichlet character and a map χ_s given by $\chi_s(M) = |M|^{-s}$.

We now use the modular symbols $\Theta_{f,D}$ to get the functional equation. The modular symbols $\Theta_{f,D}$ are elements of the group ring $R[W_D]$, where $W_D = K^*\backslash \mathbb{A}_K^*/U_D$ is the Weil group of a divisor D of K, and R is a ring containing all the Fourier coefficients of f. We refer to [59] for all the relevant definitions. The modular symbols are used to interpolate special values of the twisted L-functions, and we have [59, Proposition 2],

$$L_f(\chi, 1) = \tau_\chi^{-1}\chi(\Theta_{f,D}), \tag{3.2.11}$$

where τ_χ is a Gauss sum. Using quasi-characters, we also have

$$L_f(\chi, s) = L_f(\chi\chi_{s-1}, 1) = \tau_{\chi\chi_{s-1}}^{-1}\,(\chi\chi_{s-1})(\Theta_{f,D}). \tag{3.2.12}$$

Using the Atkin–Lehner involution w_{N_E}, we have when $(D, N_E) = 1$ (including at P_∞) [59, Proposition 3]

$$\Theta_{f,D} = \Theta^t_{w_{N_E}(f),D}\; N_E, \tag{3.2.13}$$

where t is the involution on $R[W_D]$ sending $\sum_{w\in W_D} a_w w$ to $\sum_{w\in W_D} a_w w^{-1}$.

Applying a quasi-character χ to $\Theta = \sum_{w\in W_D} a_w w$ results in $\chi(\Theta) = \sum_{w\in W_D} a_w\chi(w)$, while applying χ together with the involution t results in $\chi(\Theta^t) = \sum_{w\in W_D} a_w\chi^{-1}(w) = \chi^{-1}(\Theta)$.

We apply $\chi\chi_{s-1}$ to (3.2.13), and we combine it with (3.2.12) to get

$$\begin{aligned}
L_f(\chi, s) =& \tau_{\chi\chi_{s-1}}^{-1}(\chi\chi_{s-1})(\Theta_{f,D}) \\
=& \tau_{\chi\chi_{s-1}}^{-1}\,(\chi\chi_{s-1})(\Theta^t_{w_{N_E}(f),D})\;\chi(N_E)|N_E|^{-(s-1)} \\
=& \frac{\tau_{\chi^{-1}\chi_{1-s}}}{\tau_{\chi\chi_{s-1}}} L_{w_{N_E}(f)}(\chi^{-1}\chi_{1-s}, 1)\chi(N_E)|N_E|^{-(s-1)} \\
=& \frac{\tau_{\chi^{-1}\chi_{1-s}}}{\tau_{\chi\chi_{s-1}}} L_{w_{N_E}(f)}(\chi^{-1}, 2-s)\chi(N_E)|N_E|^{-(s-1)}.
\end{aligned}$$

The third line above follows from using (3.2.11) with f replaced by $w_{N_E}(f)$ and $\chi\chi_{s-1}$ replaced by $(\chi\chi_{s-1})^{-1}$, together with the observation that the involution t has the effect of inverting the character. Using the fact that f is an eigenvector for the self-dual Atkin–Lehner operator, we have $w_{N_E}(f) = \omega_E f$, where $\omega_E = \pm 1$ is the sign of the functional equation (3.2.7), and then $L_{w_{N_E}(f)}(\chi^{-1}, 2-s) = \omega_E L_f(\chi^{-1}, 2-s)$.

To compute the Gauss sums associated with the quasi-characters, we use [60, (2.2.3)]

$$\tau_{\chi\chi_s} = q^{s(\deg D-2)}\tau_\chi,$$

where τ_χ is the Gauss sum of the Dirichlet character χ of conductor D. Replacing above, this gives

$$\tau_\chi L_f(\chi, s) = \omega_E \tau_{\chi^{-1}}\chi(N_E) q^{(1-s)(\deg(N_E)+2\deg(D)-4)} L_f(\chi^{-1}, 2-s), \tag{3.2.14}$$

where [59, (3.4)] is a particular case (for $s = 1$). The twisted L-function of the elliptic curve is given by

$$L(E, \chi, s) = \sum_M \frac{c_f(M)|M|\chi(M)}{|M|^s} = \mathcal{L}(E, \chi, u)$$

for $u = q^{-s}$. The functional equation can be obtained by noticing that $L_f(\chi, s) = L(E, \chi, s)$, and replacing in (3.2.14). This leads to

$$\tau_\chi L(E, \chi, s) = \omega_E \tau_{\chi^{-1}}\chi(N_E) q^{(1-s)(\deg(N_E)+2\deg(D)-4)} L(E, \chi^{-1}, 2-s).$$

Using $u = q^{-s}$, we finally get

$$\mathcal{L}(E, \chi, u) = \omega_{E\otimes\chi}(qu)^{(\deg(N_E)+2\deg(D)-4)}\mathcal{L}(E, \chi^{-1}, 1/(q^2u)), \tag{3.2.15}$$

where

$$\omega_{E\otimes\chi} = \left(\frac{\overline{\tau_\chi}}{|D|^{1/2}}\right)^2 \omega_E\chi(N_E).$$

In order to get exactly the statement of the theorem, we need to take into account the difference of notation between [59] and this paper. When χ is odd and there is ramification at P_∞, the conductor D of (3.2.15) is $P_\infty D'$, where $D' \in \mathbb{F}_q[t]$, and so D' is the definition of the conductor in this paper. Adjusting the formula to make it compatible with our notation, we get for all cases

$$\mathcal{L}(E, \chi, u) = \omega_{E\otimes\chi}(qu)^{(\deg(N_E)+2\deg(D)-4+2\delta_\chi)}\mathcal{L}(E, \chi^{-1}, q^2u^{-1}),$$

which is the functional equation (3.2.10). Finally, we remark that $\frac{\overline{\tau_\chi}}{|D|^{1/2}}$ is by definition the sign of the functional equation of $\mathcal{L}(\chi, u)$, since it is the product of the same local Gauss sums because $(D, N_E) = 1$, and we have $\omega_{E\otimes\chi} = \omega_\chi^2 \omega_E \chi(N_E)$.

□

Remark 5. *When E is a constant elliptic curve, we prove in the next section that $\mathcal{L}(E, \chi, u)$ satisfies the same functional equation with $\mathfrak{n} = 2\deg F - 4 + 2\delta_\chi$ and $\omega_{E\otimes\chi} = \omega_\chi^2$. This is consistent with the fact that such E has good reduction at all primes of K, and therefore $N_E = 0$.*

3.3 L-functions of constant elliptic curves over $\mathbb{F}_q(t)$

By class field theory, Dirichlet characters of order ℓ over $\mathbb{F}_q(t)$ correspond to cyclic extensions $K/\mathbb{F}_q(t)$ of order ℓ, where $K = \mathbb{F}_q(C)$ is the function field of a projective smooth curve C defined over $\mathbb{F}_q$. We call such a curve a ℓ-cyclic cover of $\mathbb{P}^1_{\mathbb{F}_q}$, or simply a ℓ-cyclic cover.

Let C be a ℓ-cyclic cover of $\mathbb{P}^1_{\mathbb{F}_q}$ of genus g, and let $K = \mathbb{F}_q(C)$ be the corresponding extension of $\mathbb{F}_q(t)$. The zeta function of C can be expressed as

$$\mathcal{Z}(C, u) = \mathcal{Z}(u)\mathcal{L}(C, u) = \frac{\prod_{j=1}^{2g}(1 - \beta_j u)}{(1-u)(1-qu)}, \tag{3.3.1}$$

where $|\beta_j| = q^{1/2}$ for $1 \leq j \leq 2g$, and

$$\mathcal{Z}(u) = \frac{1}{(1-u)(1-qu)}.$$

We also have

$$\mathcal{L}(C, u) = \prod_{i=1}^{\ell-1} \mathcal{L}(\chi^i, u),$$

where the χ^i are the characters of order ℓ associated to the extension $K/\mathbb{F}_q(t)$.

Let E_0 be an elliptic curve over $\mathbb{F}_q$ with L-function

$$\mathcal{L}(E_0, u) = (1 - \alpha_1 u)(1 - \alpha_2 u).$$

Theorem 3.3.1. *Let $E = E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(t)$, and let C, K and α_1, α_2, and the β_j's be as above. Then,*

$$\begin{aligned}\mathcal{L}(E/K, u) &= \mathcal{Z}(C, \alpha_1 u)\mathcal{Z}(C, \alpha_2 u) \\ &= \frac{\prod\limits_{\substack{1\le i\le 2\\ 1\le j\le 2g}} (1-\alpha_i\beta_j u)}{\prod\limits_{1\le i\le 2}(1-\alpha_i u)(1-\alpha_i q u)}.\end{aligned} \tag{3.3.2}$$

Moreover, $\mathcal{L}(E, \chi, u) = \mathcal{L}(\chi, \alpha_1 u)\mathcal{L}(\chi, \alpha_2 u)$, and writing

$$\mathcal{L}(\chi, u) = \prod_{1\le j\le 2g/(\ell-1)} (1-\gamma_j u),$$

then

$$\mathcal{L}(E, \chi, u) = \prod_{\substack{1\le i\le 2\\ 1\le j\le 2g/(\ell-1)}} (1-\alpha_i\gamma_j u).$$

Proof. We refer the reader to [50, Section 3] and to [52, Section 3.2] for the general proof. To illustrate the ideas, we prove (3.3.2) when $K = \mathbb{F}_q(t)$. Since $\#E_0(\mathbb{F}_{q^n}) = q^n + 1 - \alpha_1^n - \alpha_2^n$, if P is a prime, then

$$\#E(\mathbb{F}_P) = \#E_0(\mathbb{F}_P) = q^{\deg(P)} + 1 - \alpha_1^{\deg(P)} - \alpha_2^{\deg(P)}.$$

Since all the primes are of good reduction, we have

$$\begin{aligned}\mathcal{L}(E/\mathbb{F}_q(t), u) = \mathcal{L}(E, u) &= \prod_P \left(1 - (\alpha_1^{\deg(P)} + \alpha_2^{\deg(P)})u^{\deg(P)} + q^{\deg(P)}u^{2\deg(P)}\right)^{-1} \\ &= \prod_P \left(1-\alpha_1^{\deg(P)}u^{\deg(P)}\right)^{-1}\left(1-\alpha_2^{\deg(P)}u^{\deg(P)}\right)^{-1} \\ &= \frac{1}{(1-\alpha_1 u)(1-q\alpha_1 u)(1-\alpha_2 u)(1-q\alpha_2 u)} \\ &= \mathcal{Z}(\alpha_1 u)\mathcal{Z}(\alpha_2 u).\end{aligned}$$

□

Remark 6. *From the above result, it is easy to get the functional equation for $\mathcal{L}(E, \chi, u)$ when E is a constant curve, using the functional equation of $\mathcal{L}(\chi, u)$ given by (3.2.5). Let $m = \deg_u \mathcal{L}(\chi, u) = 2g/(\ell-1)$. In the notation of Section 3.2, we have $m = 2g/(\ell-1) =$*

$\deg F - 2 + \delta_\chi$, *and*

$$\begin{aligned}\mathcal{L}(E,\chi,u) &= \mathcal{L}(\chi,\alpha_1 u)\mathcal{L}(\chi,\alpha_2 u) = \omega_\chi\left(\sqrt{q}\alpha_1 u\right)^m \mathcal{L}(\overline{\chi},1/q\alpha_1 u)\,\omega_\chi(\sqrt{q}\alpha_2 u)^m\,\mathcal{L}(\overline{\chi},1/q\alpha_2 u)\\ &= \omega_\chi^2(q^2u^2)^m\mathcal{L}(\overline{\chi},\alpha_2/(q^2u))\mathcal{L}(\overline{\chi},\alpha_1/(q^2u))\\ &= \omega_\chi^2\left(qu\right)^{2m}\mathcal{L}(E,\overline{\chi},1/(q^2u)) = \omega_\chi^2\left(qu\right)^{2\deg F-4+2\delta_\chi}\mathcal{L}(E,\overline{\chi},1/(q^2u))\end{aligned}$$

Corollary 3.3.2. *Let $E = E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(t)$, and let χ be a Dirichlet character over $\mathbb{F}_q(t)$ with associated curve C and function field $K = \mathbb{F}_q(C)$ respectively. Then, $\mathcal{L}(E/K, q^{-1}) = 0$ if and only if $\mathcal{L}(C,\alpha_1^{-1}) = \mathcal{L}(C,\alpha_2^{-1}) = 0$,*

Proof. From equation (3.3.2) in Theorem 3.3.1, $\mathcal{L}(E/K,q^{-1}) = 0$ if and only if there is one $\beta_j = q/\alpha_1 = \alpha_2$ or $\beta_j = q/\alpha_2 = \alpha_1$, where the β_j's are given by (3.3.1), and both α_1^{-1} and α_2^{-1} are roots of $\mathcal{L}(C,u)$, because of the functional equation of $\mathcal{L}(C,u)$. □

3.4 Cyclic extensions of degree ℓ over $\mathbb{F}_q(t)$

We prove in this section the following result which extends the result of [24] to general q and ℓ (removing the restrictions $q \equiv 1 \bmod \ell$ and $y^\ell = F(t)$ with $\ell \mid \deg F$).

Proposition 3.4.1. *Let ℓ be an odd prime. Fix an ℓ-cyclic cover C_0 over $\mathbb{P}^1_{\mathbb{F}_q}$ with conductor of degree d_0. Then there are at least $\gg q^{2n/d_0}$ ℓ-cyclic covers C over $\mathbb{P}^1_{\mathbb{F}_q}$ with conductor of degree bounded by n admitting a non-constant map from C to C_0.*

The proof of this result is fairly long and will require several intermediate steps.

3.4.1 General ℓ-cyclic covers over $\mathbb{P}^1_{\mathbb{F}_q}$

The affine equations of ℓ-cyclic covers over $\mathbb{P}^1_{\mathbb{F}_q}$ are well-known in the Kummer case $q \equiv 1 \bmod \ell$, which is the case treated in [24]. In this case, such a cover C over $\mathbb{P}^1_{\mathbb{F}_q}$ has an affine equation $y^\ell = F_1F_2^2\cdots F_{\ell-1}^{\ell-1}$, where $F_i \in \mathbb{F}_q[t]$ are square-free and pairwise co-prime of degree d_i. The conductor of the ℓ-cyclic cover is $F_1\cdots F_{\ell-1}$ and by the Riemann–Hurwitz formula, the genus of C is $\frac{\ell-1}{2}(d_1+\cdots+d_{\ell-1}-2)$ if $\ell \mid (d_1+2d_2+\cdots+(\ell-1)d_{\ell-1})$ and $\frac{\ell-1}{2}(d_1+\cdots+d_{\ell-1}-1)$ otherwise. In this later case, there is ramification at infinity since $\ell \nmid (d_1+2d_2+\cdots+(\ell-1)d_{\ell-1})$ by Lemma 3.2.1.

To treat the general case and prove Proposition 3.4.1, we use the work of Bary-Soroker and Meisner [2], who explicitly give the affine equations of general ℓ-cyclic covers over $\mathbb{P}^1_{\mathbb{F}_q}$. We summarize their results in this section.

As before, let n_q be the multiplicative order of q modulo ℓ. As seen in Section 3.2, the conductors of the ℓ-cyclic covers of $\mathbb{P}^1_{\mathbb{F}_q}$ (or of Dirichlet characters of order ℓ) are monic square-free polynomials in $\mathbb{F}_q[t]$ supported on n_q-divisible primes. In order to count all the ℓ-cyclic covers, or characters of order ℓ, with such conductors, let

$$\mathcal{F}_{q,\ell} := \{F \in \mathbb{F}_q[t] \ : \ F = P_1^{e_1} \cdots P_s^{e_s}, \ n_q \mid \deg P_i, \ 1 \le e_i \le \ell - 1\},$$

where the P_i are monic irreducible n_q-divisible polynomials in $\mathbb{F}_q[t]$.

Let ϕ_q be the Frobenius automorphism of $\mathbb{F}_q$. Then, ϕ_q acts on $f(t) \in \mathbb{F}_{q^{n_q}}[t]$ by acting on the coefficients, and we define

$$N_{n_q}(f) := f\phi_q(f)\phi_q^2(f)\cdots\phi_q^{n_q-1}(f) \in \mathbb{F}_q[t].$$

Notice that $N_{n_q}(f)$ has degree $n_q \deg(f)$, which is always divisible by n_q.

By hypothesis, each prime P_i in the factorization of $F \in \mathcal{F}_{q,\ell}$ splits as a product of n_q primes in $\mathbb{F}_{q^{n_q}}[t]$, and we can write any $F \in \mathcal{F}_{q,\ell}$ as

$$F = \mathfrak{F}_1 \cdots \mathfrak{F}_{n_q}, \ \ \mathfrak{F}_i \in \mathbb{F}_{q^{n_q}}[t], \ \phi_q(\mathfrak{F}_i) = \mathfrak{F}_{i+1} \ 1 \le i \le n_q - 1, \ \phi_q(\mathfrak{F}_{n_q}) = \mathfrak{F}_1. \tag{3.4.1}$$

In other words, for $F \in \mathcal{F}_{q,\ell}$, $F = N_{n_q}(\mathfrak{F}_i)$ for any i. Since $\mathfrak{F}_1$ determines $\mathfrak{F}_i$ for all i, it suffices to work with $\mathfrak{F}_1$. Let

$$\mathcal{F}_{q,\ell}^{(1)} = \{\mathfrak{F}_1 \in \mathbb{F}_{q^{n_q}}[t] : N_{n_q}(\mathfrak{F}_1) \in \mathcal{F}_{q,\ell}\}.$$

Thus, $\mathfrak{F}_1 \in \mathcal{F}_{q,\ell}^{(1)}$ when $F \in \mathcal{F}_{q,\ell}$. We also have

$$\mathfrak{F}_1 = f_1 f_2^2 \cdots f_{\ell-1}^{\ell-1}, \tag{3.4.2}$$

where the $f_i \in \mathbb{F}_{q^{n_q}}[t]$ are pairwise co-prime and square-free.

For any vector $\mathbf{v} = (v_1, \ldots, v_{n_q}) \in \mathcal{V} = \{0, 1, 2, \ldots, \ell - 1\}^{n_q}$, and any $F \in \mathcal{F}_{q,\ell}$ written as in (3.4.1), let $F_{\mathbf{v}} = \mathfrak{F}_1^{v_1} \cdots \mathfrak{F}_{n_q}^{v_{n_q}}$. For $0 \le k \le n_q - 1$, let $\mathbf{v}_k = ([q^k]_\ell, [q^{k-1}]_\ell, \ldots, [q^{k+1-n_q}]_\ell)$, where $[\alpha]_\ell \equiv \alpha \pmod{\ell}$ and $0 \le [\alpha]_\ell \le \ell - 1$, in other words, $[\alpha]_\ell$ indicates the reduction modulo ℓ of α. Thus, we have $\mathbf{v}_k \in \mathcal{V}$. Let $\zeta_\ell \in \mathbb{F}_{q^{n_q}}$ be a fixed primitive ℓth root of unity. For any $F \in \mathcal{F}_{q,\ell}$, let C_F be the curve over $\mathbb{F}_q$ with affine model

$$C_F \ : \ \prod_{j=0}^{\ell-1} \left(y - \sum_{k=0}^{n_q-1} \zeta_\ell^{jq^k} \sqrt[\ell]{F_{\mathbf{v}_k}} \right) = 0. \tag{3.4.3}$$

Notice that there is no canonical choice for $\sqrt[\ell]{F_{\mathbf{v}_k}}$, but the above equation is still well defined, since the factors include all the Galois conjugates.

In the Kummer case $n_q = 1$, $F_{\mathbf{v}_0} = \mathfrak{F}_1 = F$, and C_F has affine model $y^\ell = F(t)$. In the case $\ell = 3$ and $q \equiv 2 \bmod 3$, $F = \mathfrak{F}_1\mathfrak{F}_2$ and by (3.4.3), C_F has equation

$$\begin{aligned} C_F : & \left(y - \sqrt[3]{\mathfrak{F}_1\mathfrak{F}_2^2} - \sqrt[3]{\mathfrak{F}_1^2\mathfrak{F}_2}\right)\left(y - \zeta_3\sqrt[3]{\mathfrak{F}_1\mathfrak{F}_2^2} - \zeta_3^2\sqrt[3]{\mathfrak{F}_1^2\mathfrak{F}_2}\right) \\ & \times \left(y - \zeta_3^2\sqrt[3]{\mathfrak{F}_1\mathfrak{F}_2^2} - \zeta_3\sqrt[3]{\mathfrak{F}_1^2\mathfrak{F}_2}\right) = 0 \\ \iff & y^3 - 3\mathfrak{F}_1\mathfrak{F}_2 y - \mathfrak{F}_1\mathfrak{F}_2(\mathfrak{F}_1 + \mathfrak{F}_2) = 0, \end{aligned}$$

which is defined over $\mathbb{F}_q$. In general, C_F is birationally equivalent to $y^\ell = F_{\mathbf{v}_0}$ over $\overline{\mathbb{F}}_q$. More explicit versions of (3.4.3) are given in Section 3.4.3, including a precise formula for the case $n_q = 2$.

Proposition 3.4.2. *[2, Proposition 2.14] Let $B = \{b \in \mathbb{F}_{q^{n_q}}^*/(\mathbb{F}_{q^{n_q}}^*)^\ell\}$. There is a $(\ell-1)$-to-1 correspondence between $\mathcal{F}_{q,\ell} \times B$ and the ℓ-cyclic covers of $\mathbb{F}_q(t)$, and then a 1-to-1 correspondence between $\mathcal{F}_{q,\ell} \times B$ and the characters of order ℓ over $\mathbb{F}_q(t)$.*

We restrict in this paper to characters with monic conductors, and it then suffices to work with the set $\mathcal{F}_{q,\ell}$.

Lemma 3.4.3. *With notation as above, assume $n_q > 1$. Then for each $0 \le k \le n_q - 1$, we have $\ell \mid \deg(F_{\mathbf{v}_k})$.*

Proof. By construction,

$$\begin{aligned} \deg(F_{\mathbf{v}_k}) &= \sum_{j=1}^{n_q} \mathbf{v}_{k,j} \deg(\mathfrak{F}_j) = \sum_{j=1}^{n_q} \mathbf{v}_{k,j} \deg\left(\phi^{j-1}\left(f_1 f_2^2 \cdots f_{\ell-1}^{\ell-1}\right)\right) \\ &\equiv \sum_{j=1}^{n_q} q^{k+1-j} \sum_{h=1}^{\ell-1} h \deg(\phi^{j-1}(f_h)) \equiv \sum_{h=1}^{\ell-1} h \deg(f_h) \sum_{j=1}^{n_q} q^{k+1-j} \bmod \ell. \end{aligned}$$

Since $n_q > 1$,

$$\sum_{j=1}^{n_q} q^{k+1-j} = \frac{q^{k+1-n_q}(q^{n_q}-1)}{q-1} \equiv 0 \bmod \ell. \qquad \square$$

3.4.2 From one to infinitely many ℓ-cyclic covers

Given an ℓ-cyclic cover C_0, we can build ℓ-cyclic covers C with a non-constant map to C_0 by a change of variables, as done in [24, Lemma 3.2] for the Kummer case when $\ell \mid \deg F$. We can detect the curves C_F with $F \in \mathcal{F}_{q,\ell}$ using the following lemma.

Lemma 3.4.4. *Let $f \in \mathbb{F}_{q^{n_q}}[t]$. Then, $N_{n_q}(f)$ is square-free iff $f = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ where the $\mathfrak{p}_i$ are such that $N_{n_q}(\mathfrak{p}_i)$ are distinct n_q-divisible primes of $\mathbb{F}_q[t]$.*

Proof. If $f = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, where the $\mathfrak{p}_i$ are such that $N_{n_q}(\mathfrak{p}_i)$ are distinct n_q-divisible primes of $\mathbb{F}_q[t]$, then it is clear that $N_{n_q}(f) = N_{n_q}(\mathfrak{p}_1) \cdots N_{n_q}(\mathfrak{p}_s)$ is square-free.

Now assume that $N_{n_q}(f) = N_{n_q}(\mathfrak{p}_1) \cdots N_{n_q}(\mathfrak{p}_s)$ is square-free. Then it is clear that the $N_{n_q}(\mathfrak{p}_i)$ are distinct primes in $\mathbb{F}_q[t]$. Finally, they are n_q-divisible, since they are the result of taking the N_{n_q}-norm. □

Definition 3.4.5. *For a one-variable polynomial $f(t) \in \overline{\mathbb{F}_q}[t]$, let $f^*(u,v) := v^{\deg(f)} f(u/v)$ denote the homogeneous polynomial in variables u, v resulting from the change of variables $t = u/v$.*

Lemma 3.4.6. *Let $F \in \mathcal{F}_{q,\ell}$, with $\mathfrak{F}_1 \in \mathcal{F}_{q,\ell}^{(1)}$ given by (3.4.1) and C_F given by (3.4.3). As in (3.4.2), we write $\mathfrak{F}_1 = f_1 f_2^2 \cdots f_{\ell-1}^{\ell-1}$, where $f_i \in \mathbb{F}_{q^{n_q}}[t]$ are pairwise co-prime and square-free.*

- *Let $h(t)$ be a non-constant polynomial in $\mathbb{F}_q[t]$ such that*

$$N_{n_q}(f_1(h(t)) f_2(h(t)) \cdots f_{\ell-1}(h(t)))$$

  is square-free. Then, $(F \circ h)(t) = N_{n_q}(\mathfrak{F}_1(h(t))) \in \mathcal{F}_{q,\ell}$. Let $C_{F\circ h}$ be given by (3.4.3). Then,

$$\begin{array}{ccc} C_{F\circ h} & \longrightarrow & C_F \\ (t,y) & \mapsto & (h(t),y) \end{array}$$

  is a non-constant map from $C_{F\circ h}$ to C_F.

- *Assume that $n_q > 1$. Let $u(t), v(t)$ be non-constant polynomials in $\mathbb{F}_q[t]$ such that*

$$N_{n_q}\left(f_1^*(u,v) \cdots f_{\ell-1}^*(u,v)\right)$$

is square-free. Then $G(t) = N_{n_q}\left(\mathfrak{F}_1^*(u(t), v(t))\right) \in \mathcal{F}_{q,\ell}$. *Let* C_G *be given by* (3.4.3). *Then*

$$\begin{array}{rcl} C_G & \longrightarrow & C_F \\ (t, y) & \mapsto & \left(u(t)/v(t), yv(t)^{-\deg(F_{\mathbf{v}_0})/\ell}\right) \end{array}$$

is a non-constant map from C_G *to* C_F.

- *Assume that* $n_q = 1$ *and write* $\deg F = A\ell - \delta$, *where* $0 \leq \delta \leq \ell - 1$. *Let* $u(t), v(t)$ *be non-constant polynomials in* $\mathbb{F}_q[t]$ *such that* $f_1^*(u,v)f_2^*(u,v)\cdots f_{\ell-1}^*(u,v)$ *is square-free. Let* $g_i^* = f_i^*$ *for* $i \neq \delta$ *and* $g_\delta^* = vf_\delta^*$. *Then,* $g_1^*(u,v)g_2^*(u,v)\cdots g_{\ell-1}^*(u,v)$ *is also square-free and* $G(t) = g_1^*(u,v)g_2^*(u,v)^2\cdots g_{\ell-1}^*(u,v)^{\ell-1} \in \mathcal{F}_{q,\ell}$. *Let* $C_G : y^\ell = G(t)$. *Then*

$$\begin{array}{rcl} C_G & \longrightarrow & C_F \\ (t, y) & \mapsto & \left(u(t)/v(t), yv(t)^{-A}\right) \end{array}$$

is a non-constant map from C_G *to* C_F.

Proof. We prove the second and third point in the statement, as the first point is a consequence of them. First consider the case where $n_q > 1$. We replace t by $u(t)/v(t)$ in equation (3.4.3) and we get

$$\prod_{j=0}^{\ell-1}\left(y - \sum_{k=0}^{n_q-1}\zeta_\ell^{jq^k}\sqrt[\ell]{\frac{F_{\mathbf{v}_k}^*(u,v)}{v^{\deg(F_{\mathbf{v}_k})}}}\right) = 0.$$

Recall from Lemma 3.4.3 that for the non-Kummer case, $\ell \mid \deg(F_{\mathbf{v}_k})$. Notice also that the $\mathbf{v}_k$ are all permutations of each other. In fact, $\mathbf{v}_{k+1}$ can be constructed from $\mathbf{v}_k$ by shifting each element one place to the right cyclically and using the fact that $q^{n_q} \equiv 1 \bmod \ell$. Writing $A = \frac{\deg(F_{\mathbf{v}_k})}{\ell}$, and making the change of variables $Y = v^A y$, we finally have

$$\prod_{j=0}^{\ell-1}\left(Y - \sum_{k=0}^{n_q-1}\zeta_\ell^{jq^k}\sqrt[\ell]{F_{\mathbf{v}_k}^*(u,v)}\right) = 0,$$

which is C_G for $G(t) = N_{n_q}\left(\mathfrak{F}_1^*(u(t), v(t))\right)$.

We now consider the Kummer case. We replace t by $u(t)/v(t)$ in $y^\ell = F(t)$ to get

$$v^{A\ell}y^\ell = v^\delta F^*(u,v) = g_1^*(u,v)g_2^*(u,v)^2\ldots g_{\ell-1}^*(u,v)^{\ell-1},$$

and with the change of variables $Y = v^A y$, we get

$$Y^\ell = g_1^*(u,v) g_2^*(u,v)^2 \dots g_{\ell-1}^*(u,v)^{\ell-1},$$

which is C_G for $G(t) = g_1^*(u,v) g_2^*(u,v)^2 \dots g_{\ell-1}^*(u,v)^{\ell-1}$. □

Then Lemma 3.4.6 translates the conditions for finding curves C_G with a map to C_F to detecting when $N_{n_q}\left(f_1^*(u,v)\cdots f_{\ell-1}^*(u,v)\right)$ is square-free. We can now proceed to the proof of Proposition 3.4.1.

Proof of Proposition 3.4.1. Our proof follows the argument of [24], but without restricting to the particular case where $n_q = 1$ and $\ell \mid \deg F$. We concentrate on the parts of their argument where using the general setting explained above introduces some changes, and we just refer to their article for the parts of their argument that can be directly used.

Let $F = F_0$ be as in Lemma 3.4.6 and let $C_0 = C_{F_0}$ be the curve (3.4.3). Let d_0 be the degree of the conductor. We now give a lower bound for the number of ℓ-cyclic covers with conductor of degree smaller than n that can be obtained by the process of Lemma 3.4.6 applied to F_0, by using the square-free sieve over $\mathbb{F}_q[t]$.

Let

$$\begin{aligned}\mathcal{P}(n) = \{&(D_1,\dots,D_{\ell-1}) \in (\mathbb{F}_{q^{n_q}}[t])^{\ell-1} \ : \ D_1,\dots,D_{\ell-1} \text{ pairwise co-prime, monic, square-free,}\\ &\mathfrak{F}_1 = D_1\cdots D_{\ell-1}^{\ell-1} \in \mathcal{F}_{q,\ell}^{(1)},\ \deg(D_1\cdots D_{\ell-1}) \le n\}\\ = \{&(D_1,\dots,D_{\ell-1}) \in (\mathbb{F}_{q^{n_q}}[t])^{\ell-1} \ : \ D_1,\dots,D_{\ell-1} \text{ monic}, N_{n_q}(D_1\cdots D_{\ell-1}) \text{ square-free,}\\ &\deg(D_1\cdots D_{\ell-1}) \le n\},\end{aligned}$$

where the second line follows from Lemma 3.4.4.

By the above discussion, each tuple $(D_1,\dots,D_{\ell-1}) \in \mathcal{P}(n)$ gives rise to the ℓ-cyclic cover C_F where $\mathfrak{F}_1 = D_1 D_2^2 \cdots D_{\ell-1}^{\ell-1}$ and $F = N_{n_q}(\mathfrak{F}_1)$. The conductor is $N_{n_q}(D_1\cdots D_{\ell-1})$ of degree $\le n_q n$, and then the genus is such that $g \le \frac{\ell-1}{2}(n_q n - 2)$.

We write $\mathfrak{F}_1^0 = f_1 f_2^2 \cdots f_{\ell-1}^{\ell-1}$ where $f_i \in \mathbb{F}_{q^{n_q}}[t]$ and $N_{n_q}(\mathfrak{F}_1^0) = F_0$. Notice that $d_0 = \deg(N_{n_q}(f_1\cdots f_{\ell-1})) = n_q(\deg(f_1) + \cdots + \deg(f_{\ell-1}))$. We count the number of distinct $(D_1,\dots,D_{\ell-1}) \in \mathcal{P}(n)$ such that there exists $(u,v) \in \mathbb{F}_q[t]^2$ with

$$D_1(t) = f_1^*(u(t),v(t)),\dots,D_{\ell-1}(t) = f_{\ell-1}^*(u(t),v(t)). \tag{3.4.4}$$

We then need to detect when $N_{n_q}(D_1 \cdots D_{\ell-1})$ is square-free. Let $G(u,v)$ denote the homogeneous polynomial such that

$$N_{n_q}(f_1^*(u,v) \cdots f_{\ell-1}^*(u,v)) = G(u,v).$$

We now apply a result of Poonen [53] which counts the number of square-free values of $G(u,v)$ as u, v runs over polynomials in $\mathbb{F}_q[t]$, as given in [24] in a form suitable for our application.

Proposition 3.4.7. *[53, Theorem 8.1] [24, Proposition 3.4] Let P be a finite set of primes in $\mathbb{F}_q[t]$, B be the localization of $\mathbb{F}_q[t]$ by inverting the primes in P, $K = \mathbb{F}_q(t)$, $f \in B[x_1, \ldots, x_m]$ be a polynomial that is square-free as an element of $K[x_1, \ldots, x_m]$ and for a choice of $x \in \mathbb{F}_q[t]^m$, we say that $f(x)$ is square-free in B if the ideal $(f(x))$ is a product of distinct primes in B. For $b \in B$, define $|b| = |B/(b)|$ and for $b = (b_1, \ldots, b_n) \in B^n$, define $|b| = \max |b_i|$. Let*

$$S_f := \{x \in \mathbb{F}_q[t]^m : f(x) \text{ is square-free in } B\},$$
$$\mu_{S_f} := \lim_{N \to \infty} \frac{|\{b \in S_f : |b| < N\}|}{N^m}.$$

For each nonzero prime π of B, let c_π be the number of $x \in (A/\pi^2)^m$ that satisfy $f(x) = 0$ in A/π^2. The limit μ_{S_f} exists and is equal to $\prod_\pi (1 - c_\pi/|\pi|^{2m})$.

We then apply Proposition 3.4.7 to $G(u,v)$. Following [24, Remark 3.5], let B be the localization of $\mathbb{F}_q[t]$ by the set of primes π with $|\pi| \leq \deg(N_{n_q}(f_1 \cdots f_{\ell-1})) = d_0$. This guarantees that

$$\mu_{S_G} = \lim_{N \to \infty} \frac{|\{b \in \mathbb{F}_q[t]^2, |b| \leq N : G(b) \text{ is square-free in } B\}|}{N^2} > 0.$$

The curve C_F associated to $F = N_{n_q}(D_1 D_2^2 \cdots D_{\ell-1}^{\ell-1}) = F_0^*(u(t), v(t))$ as in (3.4.4) has genus bounded by $\frac{\ell-1}{2}(d_0 \deg(u(t)/v(t)) - 2)$, and therefore, if we want to guarantee that the genus of C_F is less or equal than g, we can prescribe that

$$\deg(u(t)/v(t)) := \max\{\deg u(t), \deg v(t)\} \leq \frac{g + \ell - 1}{g_0 + \ell - 1}, \tag{3.4.5}$$

where g_0 is the genus of C_{F_0}.

Now we want to give an upper bound for the $b = (u,v) \in \mathbb{F}_q[t]^2$ satisfying condition (3.4.5) such that equation (3.4.4) is satisfied. Now take $N = q^n$, with $n = \frac{2g}{\ell-1} + 2$, and we

impose the condition $\max\{\deg u, \deg v\} \leq n/d_0$. Notice that

$$\frac{n}{d_0} = \frac{2g+2(\ell-1)}{d_0(\ell-1)} = \frac{2g+2(\ell-1)}{(d_0-2)(\ell-1)+2(\ell-1)} = \frac{g+\ell-1}{g_0+\ell-1},$$

and therefore condition (3.4.5) is satisfied. Applying Proposition 3.4.7, we get a positive proportion of $\gg \mu N^{2/d_0} = \mu q^{2n/d_0}$ such that $N_{n_q}(D_1 \cdots D_{\ell-1})$ is square-free.

To conclude, for a fixed tuple $(D_1, \ldots, D_{\ell-1})$ we need to find an upper bound on the number of pairs $(u(t), v(t))$ such that (3.4.4) is satisfied in order to correct a double counting. Following a similar reasoning to [24], we bound this number by $qn^2q^{\varepsilon n}$.

In total, for n sufficiently large, we have

$$\gg \mu q^{n(2/d_0-\varepsilon)}$$

elements in $\mathcal{P}(n)$ corresponding to ℓ-cyclic covers of $\mathbb{P}^1_{\mathbb{F}_q}$ with conductor of degree bounded by n that admit a non-constant map to C_0. □

We then need a geometric condition for the vanishing of $\mathcal{L}(C,u)$ at some point $u = u_0^{-1}$, where C is a curve over $\mathbb{F}_q$. This is given by the following theorem of Li [40, Section 2] relating the existence of a rational map between curves to the divisibility of the L-functions. The proof uses Honda–Tate theory, which states that every q-Weil number is an eigenvalue of the geometric Frobenius acting on the ℓ-adic Tate module of a simple abelian variety over $\mathbb{F}_q$, which is unique up to isogeny. We refer the reader to [40, Section 2] for the details, and the proof of the following theorem.

Theorem 3.4.8. *Let u_0 be a q-Weil number and let A_0 be (the isogeny class of) the unique simple Abelian variety over $\mathbb{F}_q$ having u_0 as a Frobenius eigenvalue, as guaranteed by the theorem of Honda–Tate. Let C be a curve over $\mathbb{F}_q$. Then, $\mathcal{L}(C, u_0^{-1}) = 0$ if and only if there exists a non-trivial map $C \to A_0$ if and only if $\mathcal{L}(A_0, u)$ divides $\mathcal{L}(C, u)$.*

Proof of Theorems 3.1.1 and 3.1.2. The proof of Theorem 3.1.1 follows directly from Proposition 3.4.1 and Theorem 3.4.8: let C_0 be the ℓ-cyclic cover associated to χ_0, i.e. $\mathcal{L}(C_0, u_0^{-1}) = 0$. By Proposition 3.4.1 and Theorem 3.4.8, there are at least q^{2n/d_0} ℓ-cyclic covers with conductor of degree $\leq n$ such that $\mathcal{L}(C_0, u) \mid \mathcal{L}(C, u) = \prod_{i=1}^{\ell-1} \mathcal{L}(\chi^i, u)$, and then at least q^{2n/d_0} characters of order ℓ and conductor of degree $\leq n$ such that $\mathcal{L}(\chi, u_0^{-1}) = 0$.

The proof of Theorem 3.1.2 follows directly from Corollary 3.3.2 and the above. Indeed, if $E = E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(t)$ and there exists χ_0 such that $\mathcal{L}(E, \chi_0, q^{-1}) = 0$, then by Corollary 3.3.2, $\mathcal{L}(C_{\chi_0}, \alpha_1^{-1}) = 0$, and we reason as above. □

3.4.3 Explicit equation for ℓ-cyclic covers

We now give more information about the equation (3.4.3), including a precise formula for $n_q = 2$, using the work of Gupta and Zagier [33]. We used these general formulas for $n_q = 2$ to obtain the equations for the curves C_1, C_2 and C_3 in Section 3.5.2.

Let ℓ be an odd prime number coprime to q, let ω_ℓ denote a complex ℓ-root of unity, and let $\mathcal{R}_{\ell,q}$ denote a set of coset representatives of $(\mathbb{Z}/\ell\mathbb{Z})^*$ modulo the cyclic subgroup $\langle q \rangle$. Following [33], we define the polynomial the complex polynomial

$$\Psi_{\ell,n_q}(y) = \prod_{j \in \mathcal{R}_{\ell,q}} \left(y - \sum_{k=0}^{n_q-1} \omega_\ell^{jq^k} \right), \tag{3.4.6}$$

This is a polynomial of degree $\frac{\ell-1}{n_q}$. Notice that for $n_q = 1$, $\Psi_{\ell,1}(y)$ gives the ℓth cyclotomic polynomial and for $n_q = 2$, $\Psi_{\ell,2}(y)$ gives the ℓth real cyclotomic polynomial.

Gupta and Zagier prove various results regarding the coefficients of $\Psi_{\ell,n_q}(y)$, and in particular, they recover a formula of Gauss:

$$\Psi_{\ell,2}(y) = \sum_{n=0}^{\frac{\ell-1}{2}} (-1)^{\left\lfloor \frac{\ell-1-2n}{4} \right\rfloor} \binom{\left\lfloor \frac{\ell-1+2n}{4} \right\rfloor}{n} y^n. \tag{3.4.7}$$

In the following result we relate the coefficients in the equation defining C_F in (3.4.3) to those of Ψ_{ℓ,n_q}. Together with the results of [33], and (3.4.7) in particular, this allows us to compute a more explicit formula for equation (3.4.3) in the case $n_q = 2$.

Proposition 3.4.9. *Let ℓ be an odd prime coprime to q and let $\Psi_{\ell,n_q}(y)$ be defined as in (3.4.6). Let a_m be the coefficients of the following polynomial*

$$y^\ell + \sum_{m=0}^{\ell-1} a_m y^m := \Psi_{\ell,n_q}(y)^{n_q}(y - n_q). \tag{3.4.8}$$

Then, $a_m \in \mathbb{Z}$, and there exists certain coefficients $b_{s_0,\dots,s_{n_q-1}} \in \mathbb{F}_p \subseteq \mathbb{F}_q$ such that the equation defining C_F in (3.4.3) can be written as

$$C_F : y^\ell + \sum_{m=0}^{\ell-1} \sum_{\substack{0 \le s_k \\ \sum_{k=0}^{n_q-1} s_k = \ell - m \\ \sum_{k=0}^{n_q-1} q^k s_k \equiv 0 \bmod \ell}} b_{s_0,\dots,s_{n_q-1}} \mathfrak{F}_1^{\frac{1}{\ell}\sum_{k=0}^{n_q-1} s_k [q^k]_\ell} \mathfrak{F}_2^{\frac{1}{\ell}\sum_{k=0}^{n_q-1} s_k [q^{k-1}]_\ell} \cdots \mathfrak{F}_{n_q}^{\frac{1}{\ell}\sum_{k=0}^{n_q-1} s_k [q^{k+1-n_q}]_\ell} y^m = 0. \tag{3.4.9}$$

Furthermore, the $b_{s_0,\ldots,s_{n_q-1}}$ *satisfy*

$$\sum_{\substack{0\le s_k \\ \sum_{k=0}^{n_q-1} s_k=\ell-m \\ \sum_{k=0}^{n_q-1} q^k s_k\equiv 0 \bmod \ell}} b_{s_0,\ldots,s_{n_q-1}} = a_m, \tag{3.4.10}$$

where the a_m *are given by* (3.4.8) *and the equality takes place in* $\mathbb{F}_p \subseteq \mathbb{F}_q$ *after reducing the* a_m *modulo* p *(the characteristic of* $\mathbb{F}_q$*).*

In particular, for $n_q = 2$*, we have*

$$C_F : y^\ell + \sum_{r=1}^{\frac{\ell-1}{2}} a_{2r-1}(\mathfrak{F}_1\mathfrak{F}_2)^{\frac{\ell+1}{2}-r} y^{2r-1} - \mathfrak{F}_1\mathfrak{F}_2(\mathfrak{F}_1^{\ell-2} + \mathfrak{F}_2^{\ell-2}) = 0. \tag{3.4.11}$$

Before proceeding to the proof, we remark that the condition $\sum_{k=0}^{n_q-1} q^k s_k \equiv 0 \bmod \ell$ implies that $\sum_{k=0}^{n_q-1} q^{k-j} s_k \equiv 0 \bmod \ell$ (since $(q,\ell)=1$), and therefore each of the exponents of the $\mathfrak{F}_j$ in (3.4.9) is an integer. One can also see that the $b_{s_0,\ldots,s_{n_q-1}}$ are invariant by cyclic permutation of the subindexes. Each of these cyclic permutations results in a permutation in the exponents of the $\mathfrak{F}_j$. Thus, the final polynomial is symmetric in the $\mathfrak{F}_j$.

Proof. The initial step of the proof follows from the elementary fact that

$$\Psi_{\ell,n_q}(y)^{n_q}(y-n_q) = \prod_{j=0}^{\ell-1}\left(y - \sum_{k=0}^{n_q-1} \omega_\ell^{jq^k}\right).$$

Since the above polynomial has coefficients in the algebraic integers $\overline{\mathbb{Z}}$, and is invariant under Galois action, we conclude that $\Psi_{\ell,n_q}(y)^{n_q}(y-n_q) \in \mathbb{Z}[y]$ and $a_m \in \mathbb{Z}$.

Following some ideas from [33], we consider more generally

$$f_{\ell,n_q}(A_0,\ldots,A_{n_q-1}) = \prod_{j=0}^{\ell-1}\left(1 - \sum_{k=0}^{n_q-1} \omega_\ell^{jq^k} A_k\right),$$

and we remark again that this polynomial has coefficients in $\mathbb{Z}$.

Taking the formal logarithm,

$$\begin{aligned}
-\log f_{\ell,n_q}(A_0,\dots,A_{n_q-1}) &= \sum_{j=0}^{\ell-1}\sum_{m=1}^{\infty}\frac{\left(\sum_{k=0}^{n_q-1}\omega_\ell^{jq^k}A_m\right)^m}{m}\\
&= \sum_{j=0}^{\ell-1}\sum_{m=1}^{\infty}\frac{1}{m}\sum_{\substack{h_0+\cdots+h_{n_q-1}=m\\ h_i\geq 0}}\binom{m}{h_0,\dots,h_{n_q-1}}\omega_\ell^{\sum_{k=0}^{n_q-1}jq^kh_k}A_0^{h_1}\cdots A_{n_q-1}^{h_{n_q-1}}\\
&= \sum_{m=1}^{\infty}\frac{1}{m}\sum_{\substack{h_0+\cdots+h_{n_q-1}=m\\ h_i\geq 0}}\binom{m}{h_1,\dots,h_{n_q}}A_0^{h_0}\cdots A_{n_q-1}^{h_{n_q-1}}\sum_{j=0}^{\ell-1}\omega_\ell^{j\sum_{k=0}^{n_q-1}q^kh_k}
\end{aligned}$$

and the innermost sum is zero unless $\sum_{k=0}^{n_q-1}q^kh_k\equiv 0 \bmod \ell$.

In conclusion, the only powers of $A_0,\dots,A_{n_q-1}$ appearing in the Taylor series of $\log f_{\ell,n_q}(A_0,\dots,A_{n_q-1})$ and consequently in the Taylor series of $f_{\ell,n_q}(A_0,\dots,A_{n_q-1})$ are of the form $A_0^{s_0}\cdots A_{n_q-1}^{s_{n_q-1}}$ such that

$$\sum_{k=0}^{n_q-1}q^ks_k\equiv 0 \bmod \ell. \tag{3.4.12}$$

But the total degree of f_{ℓ,n_q} is ℓ, and therefore $0\leq s_0+\cdots+s_{n_q-1}\leq \ell$. Putting this information together, we obtain

$$f_{\ell,n_q}(A_0,\dots,A_{n_q-1}) = 1+\sum_{m=0}^{\ell-1}\sum_{\substack{0\leq s_k\\ \sum_{k=0}^{n_q-1}s_k=\ell-m\\ \sum_{k=0}^{n_q-1}q^ks_k\equiv 0 \bmod \ell}} b_{s_0,\dots,s_{n_q-1}}A_0^{s_0}\cdots A_{n_q-1}^{s_{n_q-1}}. \tag{3.4.13}$$

Reducing modulo p (the characteristic of $\mathbb{F}_q$), making the change of variables

$$A_k = \frac{\sqrt[\ell]{F_{\mathbf{v}_k}}}{y} = \frac{1}{y}\mathfrak{F}_1^{\frac{[q^k]_\ell}{\ell}}\mathfrak{F}_2^{\frac{[q^{k-1}]_\ell}{\ell}}\cdots\mathfrak{F}_{n_q}^{\frac{[q^{k+1-n_q}]_\ell}{\ell}},$$

and multiplying by y^ℓ, we obtain equation (3.4.9). Identity (3.4.10) follows from comparing with (3.4.8).

When $n_q=2$, we have $q\equiv -1 \bmod \ell$. Equation (3.4.12) and condition $\sum_{k=0}^{n_q-1}s_k=\ell-m$ reduce the choices of s_0,s_1 to two cases: either $s_0=s_1$ and $m\neq 0$ or $(s_0,s_1)=(0,\ell),(\ell,0)$ and $m=0$.

For the case $s_0=s_1$, we can set $A_0=A_1$ and reduce to the case of [33, Theorem 3] to find the coefficients of each $(A_0A_1)^{s_1}$. We then replace $A_0=\frac{\sqrt[\ell]{\mathfrak{F}_1\mathfrak{F}_2^{\ell-1}}}{y}$, $A_1=\frac{\sqrt[\ell]{\mathfrak{F}_1^{\ell-1}\mathfrak{F}_2}}{y}$

(or equivalently, we replace A_0A_1 by $\frac{\mathfrak{f}_1\mathfrak{f}_2}{y}$), and obtain the coefficients a_m for $m \neq 0$ from the statement. In this case one can see from working with $\Psi_{\ell,2}(y)$ that $a_m = 0$ for m even different from 0.

The cases $(s_0, s_1) = (0, \ell), (\ell, 0)$ only occur for the constant coefficient in (3.4.9) which is

$$(-1)^\ell \omega_\ell^{0+\cdots+(\ell-1)}(A_0^\ell + A_1^\ell) = -(A_0^\ell + A_1^\ell).$$

Replacing again $A_0 = \frac{\sqrt[\ell]{\mathfrak{f}_1\mathfrak{f}_2^{\ell-1}}}{y}$, $A_1 = \frac{\sqrt[\ell]{\mathfrak{f}_1^{\ell-1}\mathfrak{f}_2}}{y}$ and multiplying by y^ℓ gives equation (3.4.11). □

3.5 Numerical data

3.5.1 Description of the code

We want to compute L-functions $\mathcal{L}(E, \chi, u)$ described by (3.2.8), where χ is a character of conductor F. To simplify, we are choosing $q = p$ to be prime.

Following Section 3.2, the L-functions are polynomials of degree $\mathfrak{n} = \deg N_E + 2\deg F - 4 + 2\delta_\chi$, and

$$\mathcal{L}(E, \chi, u) = \sum_{n=0}^{\mathfrak{n}} \left(\sum_{f \in \mathcal{M}_n} a_f \chi(f) \right) u^n = \sum_{n=0}^{\mathfrak{n}} c_n u^n,$$

where $\mathcal{M}_n$ is the set of monic polynomials of degree n in $\mathbb{F}_p[t]$.

Using the functional equation (3.2.10), we get

$$c_n = \omega_{E\otimes\chi}\, p^{2(n-\lfloor \mathfrak{n}/2 \rfloor - 1)}\, \overline{c_{\mathfrak{n}-n}}, \quad 0 \leq n \leq \mathfrak{n}, \tag{3.5.1}$$

and it suffices to compute c_i for $0 \leq i \leq \lfloor \mathfrak{n}/2 \rfloor$. [5]

We then need to compute the a_f appearing in (3.2.8), for $\deg f \leq \mathfrak{n}/2$. It follows from the Euler product that $a_{fg} = a_f a_g$ for $(f, g) = 1$, and for $P \in \mathbb{F}_p[t]$ and $n \geq 1$,

$$a_{P^n} = \begin{cases} a_P a_{P^{n-1}} - p a_{P^{n-2}}, & \text{if } P \nmid N_E, \\ a_P a_{P^{n-1}}, & \text{if } P \mid N_E. \end{cases}$$

[5] It follows from (3.5.1) that we can compute numerically the sign of the functional equation by computing $c_{\mathfrak{n}/2}$ when $\mathfrak{n}$ is even, and $c_{\lfloor \mathfrak{n}/2 \rfloor}$ and $c_{\lfloor \mathfrak{n}/2 \rfloor + 1}$ when $\mathfrak{n}$ is odd. We used this in the numerical data to compute twists of the Legendre curve by odd characters, as in this case Theorem 3.2.2 does not apply. Of course, this requires $c_{\mathfrak{n}/2} \neq 0$. When $c_{\mathfrak{n}/2} = 0$, we computed the next coefficient $c_{(\mathfrak{n}/2)+1}$ to get the sign of the functional equation. In all the cases considered, $c_{(\mathfrak{n}/2)+1}$ was not zero (when $c_{\mathfrak{n}/2} = 0$), so this was enough.

We now turn to the computation of the a_P of a fixed curve $E : y^2 = x^3 + a(t)x^2 + b(t)x + c(t)$. For P prime, we compute a_P using

$$a_P = - \sum_{\substack{x \in \mathbb{F}_p[t] \\ \deg(x) < \deg(P)}} \left(\frac{x^3 + a(t)x^2 + b(t)x + c(t)}{P} \right).$$

After we have computed all a_f for $\deg f \leq (\deg N_E + 2d - 4 + 2\delta_\chi)/2$, we can evaluate $\mathcal{L}(E, \chi, u)$ for any Dirichlet character with conductor of degree d over $\mathbb{F}_p[t]$. We go through the characters of order ℓ and conductor degree d in the following way. Let n_p be the multiplicative order of p modulo ℓ as before. Let $F \in \mathbb{F}_p[t]$ be a polynomial of degree d supported on n_p-divisible primes. We can enumerate all characters of order ℓ and conductor F by choosing only one character per cyclic extension of order ℓ of $\mathbb{F}_p(t)$, since the L-functions of the $\ell - 1$ characters associated to the same extension K vanish together. Writing $F = P_1 \cdots P_k$, where the P_i are distinct n_p-divisible primes, and $P_i = \mathfrak{P}_{i,1} \cdots \mathfrak{P}_{i,n_p}$ over $\mathbb{F}_{p^{n_p}}(t)$, we consider the (non-conjugate) characters of conductor F over $\mathbb{F}_p(t)$ given by

$$\chi(A) = \chi_{\mathfrak{P}_{1,1}}(A) \prod_{j=2}^{k} \chi_{\mathfrak{P}_{j,1}}^{a_j}(A), \tag{3.5.2}$$

for $a_j \in \{1, \ldots, \ell - 1\}$, and where each $\chi_{\mathfrak{P}_{j,1}}$ is the ℓth-power residue symbol modulo $\mathfrak{P}_{j,1}$ over $\mathbb{F}_{p^{n_p}}(t)$ defined in Section 3.2.

3.5.2 Vanishing of twists of constant curves: numerical data

Let E_0 be an elliptic curve over $\mathbb{F}_p$ with $\mathcal{L}(E_0, u) = (1 - \alpha_0 u)(1 - \overline{\alpha}_0 u)$, and let $E = E_0 \times_{\mathbb{F}_p} \mathbb{F}_p(t)$. By (3.2.9), $\mathcal{L}(E, \chi, p^{-1}) = 0$ for some character χ associated to $K/\mathbb{F}_p(t)$ if and only if $\mathcal{L}(E/K, p^{-1}) = 0$, and using the results of Section 3.3, this is equivalent to

$$\mathcal{L}(E_0, u) \mid \mathcal{L}(C_\chi, u) = \prod_{j=1}^{\ell-1} \mathcal{L}(\chi^j, u).$$

By Theorem 3.1.2, once we have found one χ_0 such that $\mathcal{L}(C_{\chi_0}, \alpha_0^{-1}) = 0$, then there are infinitely many, so we concentrate on finding χ_0. We examined degree 2 factors of $\mathcal{L}(\chi^j, u)$ which arise as $\mathcal{L}(E_0, u)$ for some E_0 over $\mathbb{F}_p$.

In particular, we considered the case where $\mathcal{L}(\chi, u)$ has degree 2, which in the case of even (respectively odd) characters means that the conductor of χ is a polynomial of degree

4 (respectively 3) in $\mathbb{F}_p[t]$. Table 1 presents results for this case: for fixed values of ℓ and p, we computed $\mathcal{L}(\chi, u)$ for all characters such that $\mathcal{L}(\chi, u)$ is a polynomial of degree 2, and we listed all the cases that we found where $\mathcal{L}(\chi, u) = \mathcal{L}(E_0, u)$ for some elliptic curve $E_0/\mathbb{F}_p$. Notice that this means $\mathcal{L}(C_\chi, u) = \mathcal{L}(E_0, u)^{\ell-1}$. Each entry in Table 1 may correspond to many characters χ. We did not count them, but our program keeps an instance for each case. For example, the curve $C_1/\mathbb{F}_5$ given by

$$y^3 + (2t^4 + 2t^3 + t^2 + 4t + 4)y + (3t^6 + 2t^5 + 2t^4 + 2t^3 + t^2 + t + 3) = 0$$

has L-function $\mathcal{L}(C_1, u) = (1 + 5u^2)^2$; the curve $C_2/\mathbb{F}_{59}$ given by

$$y^5 + (54t^4 + 18t^3 + 34t^2 + 18t + 39)y^3 + (5t^8 + 23t^7 + 44t^6 + 20t^5 + 35t^4 + 30t^3 + 17t^2 + 33t + 21)y$$
$$+ (57t^{10} + 18t^9 + 24t^8 + 58t^7 + 14t^6 + 9t^5 + 41t^4 + 17t^3 + 38t^2 + 48t + 44) = 0$$

has L-function $\mathcal{L}(C_2, u) = (1 + 59u^2)^4$; and the curve $C_3/\mathbb{F}_{13}$ given by

$$y^7 + (6t^4 + 6t^3 + 6t^2 + 12t + 1)y^5 + (t^8 + 2t^7 + 3t^6 + 6t^5 + t^4 + 5t + 4)y^3 +$$
$$(6t^{12} + 5t^{11} + 10t^{10} + 7t^8 + 2t^7 + 3t^6 + 9t^5 + 3t^4 + 2t^3 + 6t^2 + t + 4)y +$$
$$(11t^{14} + 6t^{13} + 12t^{12} + 10t^{11} + 5t^{10} + 8t^9 + 6t^8 + 2t^7 + 2t^6 + 10t^5 + 7t^4 + 12t^3 + 3t^2 + 3t + 9) = 0$$

has L-function $\mathcal{L}(C_3, u) = (1 + 13u^2)^6$.

Of course, it would be interesting to prove some criteria which guarantees the existence of a character of degree ℓ over $\mathbb{F}_p$ such that $\mathcal{L}(E_0, u)$ divides $\mathcal{L}(\chi, u)$. From the data, we are led to believe that this could always be the case when $n_p = 2$ and $\mathcal{L}(E_0, u) = 1 + pu^2$, corresponding to the isogeny class of supersingular elliptic curves over $\mathbb{F}_p$, but we currently do not have a proof. We present further evidence for larger values of ℓ in Table 2. Since this becomes more time-consuming, we only consider a thin family of the characters of order ℓ, where $a_j = 1$ for all j in (3.5.2). In some cases ($(\ell, p) = (13, 103), (17, 101), (31, 61)$, and $(37, 73)$), we did not go over all characters in the thin family, we stopped after we found $\mathcal{L}(\chi, u) = (1 + pu^2)$, so there might be other characters where $\mathcal{L}(\chi, u) = (1 + a_p u + pu^2)$. In summary, the following is true for all the cases that we tested: for every ℓ, p such that $n_p = 2$, there exists a character χ of order ℓ over $\mathbb{F}_p$ such that $\mathcal{L}(\chi, u) = 1 + pu^2$.

Remark 7. *There is a large amount of work in the literature on Newton polygons of cyclic covers of $\mathbb{P}^1$, in particular on the existence of supersingular and superspecial curves. See for example, [42, 41, 43]. But the existence of the curves we present in this paper does not*

follow from previous work. In fact, the existence of supersingular curves in families of cyclic covers which ramify at 4 points with growing degree ℓ is surprising from a dimension counting perspective. More surprisingly, these curves are defined over the prime field $\mathbb{F}_p$.

ℓ	p	n_p	$\mathcal{L}(\chi, u) = 1 + a_p u + pu^2$
3	5	2	$0, 3$
	7	1	$-2, -1, 1, 2, 4$
	11	2	$-3, 0, 3, 6$
	13	1	$-5, -4, -2, -1, 1, 2, 4, 5$
	17	2	$-6, -3, 0, 3, 6$
	19	1	$-8, -7, -5, -4, -2, -1, 1, 2, 4, 5, 7, 8$
5	3	4	$\varnothing$
	7	4	3
	11	1	$-2, 2, 3$
	13	4	$-1, 4$
	19	2	$0, 5$
	29	2	0
	31	1	$-2, 2, 3, 8$
7	13	2	0
	29	1	$-2, 2, 5$
11	23	1	$\varnothing$
	43	2	0
13	5	4	$\varnothing$
61	11	4	$\varnothing$

Table 1: All instances of E_0 for which there is a χ of order ℓ over $\mathbb{F}_p$ such that $\mathcal{L}(\chi, u) = \mathcal{L}(E_0, u)$ for some elliptic curve $E_0/\mathbb{F}_p$.

ℓ	p	n_p	$\mathcal{L}(\chi, u) = 1 + a_p u + pu^2$
13	103	2	0
17	67	2	0
	101	2	0
19	37	2	0
31	61	2	0
37	73	2	0

Table 2: More cases where there is a character χ of order ℓ over $\mathbb{F}_p$ such that $\mathcal{L}(\chi, u) = (1 + p^2 u)$. For the cases $(\ell, p) = (17, 67)$ and $(19, 37)$, we considered all characters in the thin family, and we did not find any other cases where $\mathcal{L}(\chi, u) = \mathcal{L}(E_0, u)$ except for $\mathcal{L}(E_0, u) = (1 + p^2 u)$. For the other cases, we stopped after finding χ such that $\mathcal{L}(\chi, u) = (1 + p^2 u)$, and we did not find any other $\mathcal{L}(E_0, u)$ up to that point.

3.5.3 Vanishing of twists of non-constant curves: numerical data

We now present data for the vanishing of $\mathcal{L}(E, \chi, p^{-1})$, where χ varies over characters of order ℓ over the finite field $\mathbb{F}_p$ for some prime p, and where E is a non-constant curve. We used the Legendre curve $E_1 : y^2 = x(x-1)(x-t)$ and the curve $E_2 : y^2 = (x-1)(x-2t^2-1)(x-t^2)$.

We remark that E_1 has conductor $N_1 = t(t-1)P_\infty^2$, discriminant $\Delta_1 = 16t^2(t-1)$, and j-invariant $j_1 = \frac{256(t^2-t+1)^3}{t^2(t-1)^2}$. Thus, it is smooth and non-constant and has bad reduction at P_∞. Since $\deg(N_1) = 4$, we conclude that $\mathcal{L}(E_1, u) = 1$. Since the algebraic rank is bounded by the analytic rank (see [62]) and this last one equals 0, we conclude that E_1 has (algebraic) rank 0 over $\mathbb{F}_p(t)$.

Similarly, E_2 has conductor $N_2 = t(t-1)(t+1)(t^2+1)$, discriminant $\Delta_2 = 64t^4(t-1)^2(t+1)^2(t^2+1)^2$, and j-invariant $j_2 = \frac{1728(t^4+1)^3}{t^4(t-1)^2(t+1)^2(t^2+1)^2}$. Thus, it is smooth and non-constant and has good reduction at P_∞. Since $\deg(N_2) = 5$, we have $\mathcal{L}(E_2, u) = 1 \pm pu$, and the rank of E_2 over $\mathbb{F}_p(t)$ is at most 1. Let i be a primitive four root of unity in $\overline{\mathbb{F}}_p$, and consider the point

$$P = ((1+i)t^2 + (1+i)t + 1, (-1+i)t(t+1)(t-i))$$

in $E_2(K)$, where $K = \mathbb{F}_p(t)(i)$. One can see that the Néron–Tate height of P is positive, and therefore P has infinite order (see the book of Shioda and Schütt [56] for a general reference). As before, we use that the algebraic rank is bounded by the analytic rank [62]. If $p \equiv 1 \mod 4$, then $K = \mathbb{F}_p(t)$, and we conclude that E_2 has (algebraic) rank exactly 1 over $\mathbb{F}_p(t)$. Therefore $\mathcal{L}(E_2, u) = 1 - pu$. If $p \equiv 3 \mod 4$, then $K = \mathbb{F}_{p^2}(t)$, and $K/\mathbb{F}_p(t)$ is a quadratic constant field extension. Therefore $\mathcal{L}(E/K, u) = 1 - p^2u$, since $\deg N_E - 4 = 1$. We also have

$$\mathcal{L}(E_2/K, u^2) = \mathcal{L}(E_2, u)\mathcal{L}(-E_2, u), \tag{3.5.3}$$

where

$$-E_2 : -y^2 = (x-1)(x-2t^2-1)(x-t^2).$$

We remark that we have $\mathcal{L}(E_2, u^2)$ and not $\mathcal{L}(E_2, u)$ in (3.5.3) because $K/\mathbb{F}_p(t)$ is a constant field extension (see [54, Chapter 8] for more details). When $p \equiv 3 \mod 4$, the point $2P = (t^2+1, it^2)$ defined over $\mathbb{F}_{p^2}(t)$ yields a (non-torsion) point $\tilde{P} = (t^2+1, t^2)$ defined over $\mathbb{F}_p(t)$ on $-E_2$. Thus the algebraic rank of $-E_2$ over $\mathbb{F}_p(t)$ is 1 and $\mathcal{L}(-E_2, u) = 1 - pu$. Now

(3.5.3) implies that $\mathcal{L}(E_2, u) = 1 + pu$. In conclusion, we have that

$$\mathcal{L}(E_2, u) = \begin{cases} 1 - pu & \text{if} \quad p \equiv 1 \bmod 4, \\ 1 + pu & \text{if} \quad p \equiv 3 \bmod 4. \end{cases}$$

We present in Tables 3, 4, and 5 our results for twists of the Legendre curve with characters of order 3, 5, and 7 respectively, and various ground fields $\mathbb{F}_p(t)$. For the curve given by $y^2 = (x-1)(x-2t^2-1)(x-t^2)$, we present in Tables 7, 8, and 9 our results for twists of this curve with characters of order 3, 5, and 7 respectively, and various ground fields $\mathbb{F}_p(t)$. We have also tested higher order twists ($\ell = 11, 13$ for E_1 and $\ell = 11, 31, 71$ for E_2) but without finding any vanishing. This data is presented in Tables 6 and 10.

Each table has the same format: the first three columns are the values of ℓ, p and n_p and the fourth column is the degree d of the conductors of the characters of order ℓ over $\mathbb{F}_p(t)$ considered (then, n_p always divides d). The L-functions $\mathcal{L}(E, \chi, u)$ are then computed for all χ of order ℓ over $\mathbb{F}_p(t)$ with conductor of degree d, and they are classified according to their analytic rank, which is defined as $\text{rank}(\chi) = r_{\text{an}}(E, \chi) = \text{ord}_{u=q^{-1}}\mathcal{L}(E, \chi, u)$. Since $\text{rank}(\chi^i) = \text{rank}(\chi^j)$, we only count one power per character in our data. Then, the next columns give the number of such χ where the analytic rank is 0, or 1, or $2, \ldots$ The most extensive computation that we did was for twists of order $\ell = 3$ of the curve E_2 for conductors of degree 8 over $\mathbb{F}_5(t)$, where we needed to compute a_P for primes of degree ≤ 8, which is the most involved part of computing the twisted L-functions $\mathcal{L}(E_2, \chi, u)$ for characters with conductors of degree 8. This took approximately 20 days on an Intel(R) Core(TM) i5-4300U CPU. This is also the only case where we found a twist of analytic rank 3.

The data for the Legendre curve is very compatible with the conjectures of [18] and [46], as we have found no instances of vanishing for any character of order 7 or higher. For the curve E_2, we have found many instances of vanishing for characters of order 7, but none for characters of higher order.

twist order	p	n_p	deg conductor d	rank 0	rank 1	rank 2
3	5	2	2	6	4	0
			4	205	32	3
			6	5784	260	16
			8	302640	116	4
	7	1	1	5	0	0
			2	37	4	0
			3	324	37	1
			4	2935	73	0

Table 3: Twists of order 3 for the Legendre curve.

twist order	p	n_p	deg conductor d	rank 0	rank 1
5	7	4	4	585	3
	11	1	1	9	0
			2	199	0
			3	3759	5
			4	65143	11
	19	2	2	170	1

Table 4: Twists of order 5 for the Legendre curve.

twist order	p	n_p	deg conductor d	rank 0
7	5	6	6	2580
	11	3	3	440
	13	2	2	78
			4	25116
	23	3	3	4048
	29	1	1	27
			2	2512
			3	179192
	41	2	2	820
	197	1	1	195
	337	1	1	335
	379	1	1	377

Table 5: Twists of order 7 for the Legendre curve. We have found no instances of vanishing in this case.

twist order	p	n_p	deg conductor d	rank 0
11	5	5	5	624
	23	1	1	21
	43	2	2	903
	67	1	1	65
	89	1	1	87
13	5	4	4	150
	29	3	3	8120
	53	1	1	51
			2	16678

Table 6: Twists of order 11 and 13 for the Legendre curve. We have found no instances of vanishing in this case.

twist order	p	n_p	deg conductor d	rank 0	rank 1	rank 2	rank 3
3	5	2	2	8	2	0	0
			4	214	26	0	0
			6	5780	280	0	0
			8	149222	2136	20	2
	7	1	1	4	0	0	0
			2	30	2	0	0
			3	264	22	2	0
			4	2299	49	4	0
			5	18670	240	2	0
			6	148537	1343	32	0
	11	2	2	53	0	1	0
	13	1	1	8	0	0	0
			2	122	12	0	0
			3	2140	56	4	0
	17	2	2	116	20	0	0
	19	1	1	14	2	0	0
			2	380	28	2	0
	23	2	2	244	6	2	0
	29	2	2	364	42	0	0
	31	1	1	26	2	0	0
			2	1190	24	6	0
	103	1	1	100	0	0	0
	109	1	1	104	0	0	0
	151	1	1	146	2	0	0

Table 7: Twists of order 3 for the curve $y^2 = (x-1)(x-2t^2-1)(x-t^2)$.

twist order	p	n_p	deg conductor d	rank 0	rank 1	rank 2
5	7	4	4	587	0	1
	11	1	1	8	0	0
			2	166	0	0
			3	3064	0	0
	19	2	2	170	0	0
	29	2	2	388	18	0
	31	1	1	28	0	0
			2	1975	0	1
	41	1	1	36	0	0
	101	1	1	96	0	0
	131	1	1	128	0	0

Table 8: Twists of order 5 for the curve $y^2 = (x-1)(x-2t^2-1)(x-t^2)$.

twist order	p	n_p	deg conductor d	rank 0	rank 1
7	5	6	6	2560	20
	11	3	3	440	0
	13	2	2	72	6
			4	24984	132
	29	1	1	24	0
			2	2046	16
	41	2	2	800	20

Table 9: Twists of order 7 for the curve $y^2 = (x-1)(x-2t^2-1)(x-t^2)$.

twist order	p	n_p	deg conductor d	rank 0
11	5	5	5	624
	23	1	1	20
			2	2152
			3	168448
	43	2	2	902
	67	1	1	64
			2	22370
	89	1	1	84
	199	1	1	196
31	5	3	3	40
71	5	5	5	624

Table 10: Twists of order 11, 31, and 71 for the curve $y^2 = (x-1)(x-2t^2-1)(x-t^2)$. We have found no instances of vanishing in this case.

Chapter 4

Numerical Computations

This chapter presents some unpublished results useful for numerical computations, and one result that was found by looking at the numerical data. An algorithm to cycle through the monic polynomials to obtain their factorizations and to construct the list of primes is presented. Then, a theorem that gives the number of zeros and their norms for $L(E \otimes \chi, u)$ depending on the parity of χ and the type of reduction at infinity of E is presented. Finally, a sequence of curves such that the analytical rank grows to infinity is presented.

4.1 Factorization of the Monic Polynomials

Let $\mathcal{M}_N$ be the set of monic polynomials of degree N, $\mathcal{P}_N$ be the set of prime polynomials of degree N, and $\mathcal{S}_N := \mathcal{M}_N - \mathcal{P}_N$. Suppose that we want to find the factorizations of all the polynomials in $\mathcal{M}_N$. The algorithm cycles through the factorizations of all the polynomials of $\mathcal{S}_N$ and computes their products. The remaining polynomials are primes. The algorithm is recursive, so the primes polynomials of degree $< N$ are already constructed in the memory.

Let $\pi(N)$ be the number of primes of degree N. We write $P_{i,j}$ to denote the jth prime of degree i in the lexicographical order. We define two functions on the primes: $\deg(P_{i,j}) = i$ and $\text{ind}(P_{i,j}) = j$. The variable $F_i^{(k)}$ is used to denote the ith prime factor of the kth polynomial constructed by the algorithm. They are ordered the following way. For any $i < j$, $\deg(F_i^{(k)}) \geq \deg(F_j^{(k)})$ and if $\deg(F_i^{(k)}) = \deg(F_j^{(k)})$, then $\text{ind}(F_i^{(k)}) \leq \text{ind}(F_j^{(k)})$. The variable n is the number of $F_i^{(k)} \neq 1$ for a given k.

The algorithm starts with $F_i^{(0)} = t$ for $1 \leq i \leq N$, so the initial polynomial is $F_1^{(0)} \dots F_N^{(0)} = t^N$. Given a polynomial $F_1^{(k)} \dots F_n^{(k)}$, the next monic polynomial is found the following way. The algorithm cycles through the factors, starting from $F_n^{(k)}$ to $F_1^{(k)}$, until it finds a factor that can be increased either on the index or the degree, with a priority given to the index. If no factors can be increased, the algorithm ends. The degree can be increased only if $\deg(F_i^{(k)}) < \deg(F_{i-1}^{(k)})$, to preserve the order among the prime factors. If $F_i^{(k)}$ is the factor that is changed by the algorithm, then $F_j^{(k+1)} = F_j^{(k)}$ for all $1 \leq j < i$. If the degree of $F_i^{(k)}$ is to be increased and $\deg(F_i^{(k)}) + 1 = \deg(F_{i-1}^{(k)})$, then $F_i^{(k+1)}$ is set to $F_{i-1}^{(k+1)}$, to preserve the order, otherwise $F_i^{(k+1)}$ is set to $P_{\deg(F_i^{(k)})+1,1}$. If the index of $F_i^{(k)}$ is to be increased and $\deg(F_i^{(k)}) = 1$, then $F_j^{(k+1)} = P_{1,\text{ind}(F_i)}$ for $j > i$ until the degree reaches N, otherwise $F_j^{(k+1)} = P_{1,1}$ is used. The following factors are then set to 1, if any. At the end of the algorithm, all monic polynomials of degree N that have not been constructed are prime.

We give an example of the algorithm for polynomials of degree four over $\mathbb{F}_2$.

ind	degree 1	degree 2	degree 3
1	t	t^2+t+1	t^3+t+1
2	$t+1$		t^3+t^2+1

Table 11: Primes of degree ≤ 3 over $\mathbb{F}_2$.

k	$F_1^{(k)}$	$F_2^{(k)}$	$F_3^{(k)}$	$F_4^{(k)}$
1	t	t	t	t
2	t	t	t	$t+1$
3	t	t	$t+1$	$t+1$
4	t	$t+1$	$t+1$	$t+1$
5	$t+1$	$t+1$	$t+1$	$t+1$
6	t^2+t+1	t	t	1
7	t^2+t+1	t	$t+1$	1
8	t^2+t+1	$t+1$	$t+1$	1
9	t^2+t+1	t^2+t+1	1	1
10	t^3+t+1	t	1	1
11	t^3+t+1	$t+1$	1	1
12	t^3+t^2+1	t	1	1
13	t^3+t^2+1	$t+1$	1	1

Table 12: Example of Algorithm 1 over $\mathbb{F}_2$ with $N = 4$. It finds all composite monic polynomials of degree 4 over $\mathbb{F}_2$. The remaining ones are prime.

Algorithm 1: Factorization of the Monic Polynomials of Degree N

```
1  for i ← 1 to N do
2  |  F_i ← P_{1,1};
3  end
4  n ← N;
5  do
6  |  i ← n + 1;
7  |  ℓ ← 1;
8  |  do
9  |  |  i ← i − 1;
10 |  |  if ind(F_i) < π(deg(F_i)) then
11 |  |  |  F_i ← P_{deg(F_i),ind(F_i)+1};
12 |  |  |  if deg(F_i) = 1 then
13 |  |  |  |  ℓ ← ind(F_i);
14 |  |  |  end
15 |  |  else
16 |  |  |  if i < n then
17 |  |  |  |  if i > 1 and deg(F_{i−1}) = deg(F_i) + 1 then
18 |  |  |  |  |  F_i ← F_{i−1};
19 |  |  |  |  else
20 |  |  |  |  |  if i = 1 or deg(F_{i−1}) > deg(F_i) then
21 |  |  |  |  |  |  F_i ← P_{deg(F_i)+1,1};
22 |  |  |  |  |  end
23 |  |  |  |  end
24 |  |  |  end
25 |  |  end
26 |  until F_i has been changed;
27 |  n ← i;
28 |  while deg(F_1 ... F_n) < N do
29 |  |  n ← n + 1;
30 |  |  F_n ← P_{1,ℓ};
31 |  end
32 until deg(F_1) = N;
```

One interesting feature of this algorithm is that it improves by $\log(N)\log\log(N)$ the asymptotic complexity of the algorithm presented in [6], at the cost of an exponential memory usage. Their method computes the product

$$(t-\alpha)(t-\alpha^q)\dots(t-\alpha^{q^{N-1}})$$

where $\alpha \in \mathbb{F}_{q^N}$ is a root of the prime polynomial. Their algorithm computes the prime polynomials of degree N, so the algorithm presented in this section computes N times more polynomials by the prime number theorem. However, their algorithm computes the prime polynomials over $\mathbb{F}_{q^N}$, where multiplication of two elements requires $\mathcal{O}_q(N\log(N)\log\log(N))$ bit operations ([57] Theorem A), while multiplication over $\mathbb{F}_q$ requires $\mathcal{O}_q(1)$ bit operations.

Proposition 4.1.1. *The asymptotic complexity of Algorithm 1 is* $\mathcal{O}_q(q^N N\log^2(N)\log\log(N))$.

Proof. The above pseudocode only describes how to cycle through $\mathcal{S}_N$. For an accurate computation of the asymptotic complexity, it is necessary to detail how the products of the prime factors should be computed. The products $F_1^{(k)}$, $F_1^{(k)}F_2^{(k)}$, $F_1^{(k)}F_2^{(k)}F_3^{(k)}$, $\dots$, $F_1^{(k)}\dots F_j^{(k)}$ where $F_j^{(k)}$ is the last factor such that $\deg(F_j^{(k)}) \neq 1$ are kept and updated in the memory during the construction of each polynomial. When the factor $F_i^{(k)}$ that is increased has $\deg(F_i^{(k)}) > 1$, two multiplications are needed to compute the polynomial, and each multiplication requires $\mathcal{O}(N\log(N)\log\log(N))$ operations by [57] Theorem B. The first multiplication is between $F_1^{(k)}\dots F_{i-1}^{(k)}$ and $F_i^{(k)}$, since $F_1^{(k)}\dots F_{i-1}^{(k)}$ is already in the memory. The second multiplication is between $F_1^{(k)}\dots F_i^{(k)}$ and $F_{i+1}^{(k)}\dots F_n^{(k)}$, where the latter are factors of degree one, and their product is computed in $\mathcal{O}(N\log^2(N)\log\log(N))$ operations using [57] Theorem B. When the factor $F_i^{(k)}$ that is increased has $\deg(F_i^{(k)}) = 1$, only one multiplication is necessary.

Finding which factor to increase for the next monic polynomial requires $\mathcal{O}_q(N\log(N))$ operations, since the comparison on line 10 of Algorithm 1 contributes at most

$$\sum_{i=1}^{n}\log(\pi(\deg(F_i^{(k)}))) \leq \sum_{i=1}^{n}\log(q^{\deg(F_i^{(k)})}) = \mathcal{O}_q(N)$$

operations, and there are also at most N comparisons on the degree where each comparison takes $\mathcal{O}(\log(N))$ operations. Increasing the factor and appending the degree one factors is done in $\mathcal{O}_q(N)$ operations.

We need to keep track of the monic polynomials constructed by the algorithm. Each coefficient needs $\lceil \log_2(q) \rceil$ bits to be stored, meaning that the memory addresses have length $N\lceil \log_2(q) \rceil$ by concatenating the coefficients, which implies a memory access in $\mathcal{O}_q(N)$.

After running the algorithm, it is necessary to cycle through all the q^N monic polynomials in order to find the ones that have not been constructed. Finding and writing the primes in the memory is done in $\mathcal{O}_q(q^N N)$.

We note that the above only holds if the primes of degree smaller than N are already constructed in the memory. Including their construction in the running time does not affect the asymptotic complexity, as

$$\sum_{i=1}^{N-1} \kappa q^i i \log^2(i) \log\log(i) \leq \kappa q^N N \log^2(N) \log\log(N)$$

where κ is the complexity constant of Algorithm 1.

□

4.2 Zeros of $L(E \otimes \chi, u)$

It is important to know how many zeros the L-functions have to know how many coefficients need to be computed. It is also important to know about the norms of the zeros to apply the functional equation. We recall a few definitions.

The prime(s) at infinity are excluded in the following products. However, they are included in N_E, the conductor of E.

The L-function of E is defined by

$$L(E,u) := \prod_{P \nmid N_E} (1 - \alpha_P u^{\deg(P)})^{-1} (1 - \overline{\alpha}_P u^{\deg(P)})^{-1} \prod_{P \mid N_E} (1 - a_P u^{\deg(P)})^{-1}.$$

The L-function of E twisted by χ of conductor F such that $(F, N_E) = 1$ is defined by

$$L(E \otimes \chi, u) := \prod_{P \nmid N_E} (1 - \chi(P)\alpha_P u^{\deg(P)})^{-1} (1 - \chi(P)\overline{\alpha}_P u^{\deg(P)})^{-1} \prod_{P \mid N_E} (1 - \chi(P) a_P u^{\deg(P)})^{-1}.$$

The L-function of E/K for a field extension $K/\mathbb{F}_q[t]$ is defined by

$$L(E/K,u) := \prod_{\mathfrak{p}\nmid\mathcal{N}_E}(1-\alpha_{\mathfrak{p}}u^{\deg_K(\mathfrak{p})})^{-1}(1-\overline{\alpha}_{\mathfrak{p}}u^{\deg_K(\mathfrak{p})})^{-1}\prod_{\mathfrak{p}|\mathcal{N}_E}(1-a_{\mathfrak{p}}u^{\deg_K(\mathfrak{p})})^{-1}$$

where the product is over the primes of K and $\mathcal{N}_E$ is the conductor of E over K. The function $\deg_K$ is defined by $\deg_K(\mathfrak{p}) := \log_q|K/(\mathfrak{p})|$ and extended using $\deg_K(\mathfrak{pq}) = \deg_K(\mathfrak{p}) + \deg_K(\mathfrak{q})$. In particular, for P a prime of $\mathbb{F}_q[t]$, we have $\deg_K(P) = \ell\cdot\deg(P)$.

Definition 4.2.1. *If E has additive reduction at infinity, the reduction type at infinity might change over an odd quadratic extension. We say E has type 0,1, or 2 if $a_{\mathfrak{p}_\infty} = 0, 1,$ or -1 respectively for the given extension. If the reduction becomes good, we say E has type 3.*

Remark 8. *We will see that the type number only depends on E and the order of the extension. Furthermore, for extensions of order ≥ 3, only type 0 is possible.*

Proposition 4.2.2 (Riemann Hypothesis)**.** *Let ℓ be prime and let χ be a primitive Dirichlet character of order ℓ of conductor $F \neq 1$ coprime to N_E*

$$L(E\otimes\chi,u) = G(u)\prod_{j=1}^{M}\left(1-qe^{i\theta_j}u\right) \tag{4.2.1}$$

where $G(u)$ and M are given in the table at the end of the proof.

Proof. Let $K/\mathbb{F}_q(t)$ be the cyclic field extension associated to χ. The following theorems hold with the prime(s) at infinity included in the product and we write $L^*(\cdot,\cdot)$ to indicate so. By Artin's conjecture, which has been proven over function fields, we have

$$L^*(E/K,u) = L^*(E,u)\prod_{i=1}^{\ell-1}L^*(E\otimes\chi^i,u)$$

and all of these functions are entire. By [5, Appendix]

$$L^*(E/K,u) = \prod_{j=1}^{L}\left(1-qe^{i\theta_j}u\right)$$

where $L = \deg_K(\mathcal{N}_E) + 4g - 4$ and g is the genus of K.

When χ is even, the prime at infinity is totally split in K and $\chi(P_\infty) = 1$. This means

$\deg_K(\mathcal{N}_E) = \ell \cdot \deg(N_E)$. Also, we have $2g = (\ell-1)(\deg(F)-2)$ and $L^*(E,u)$ has degree $\deg(N_E)-4$ ([5, Appendix]). The factors at infinity in Artin's conjecture are

$$\prod_{j=1}^{\ell}(1-a_{\mathfrak{p}_\infty,j}u)^{-1} = (1-a_{P_\infty}u)^{-1}\prod_{j=1}^{\ell-1}(1-\chi^j(P_\infty)a_{P_\infty}u)^{-1}.$$

The twisted L-functions have the same number of zeros, so we can conclude.

When χ is odd, the prime at infinity is totally ramified in K, which means $P_\infty = (\mathfrak{p}_\infty)^\ell$. We write $(1-I_{\infty,j}u)^{-1}$ or $(1-I_{\infty,j}u)^{-1}(1-\overline{I_{\infty,j}}u)^{-1}$ for the factor at infinity of $L^*(E\otimes\chi^j,u)$. The ramification prevents $I_{\infty,j}$ from being given by $\chi^j(P_\infty)a_{P_\infty}$. We first assume the reduction remains bad over K. The factors at infinity in Artin's conjecture are

$$(1-a_{\mathfrak{p}_\infty}u)^{-1} = (1-a_{P_\infty}u)^{-1}\prod_{j=1}^{\ell-1}(1-I_{\infty,j}u)^{-1}.$$

If $a_{P_\infty} = \pm 1$, then there is only the possibility $a_{\mathfrak{p}_\infty} = a_{P_\infty}$ and $I_{\infty,j} = 0$ for all j. Then $\deg_K(\mathcal{N}_E) = \ell\cdot\deg(N_E) - (\ell-1)$ and we can conclude using $2g = (\ell-1)(\deg(F)-1)$. If $a_{P_\infty} = 0$, then the reduction at infinity might change from $\mathbb{F}_q[t]$ to K since the $I_{\infty,j}$ are not necessarily zero. Using the fact that if $I_{\infty,j} = 0$ for some j then they are all zero, we can see that the reduction type at infinity can only change for quadratic twists.

For type 0, we write $N_E = P_\infty^2\tilde{N}_E$. Since the reduction at infinity stays additive, we have $\mathcal{N}_E = \mathfrak{p}_\infty^2\tilde{N}_E$. We also have $\deg_K(\tilde{N}_E) = \ell\cdot\deg(\tilde{N}_E)$. So $\deg_K(\mathcal{N}_E) = 2+\ell\cdot\deg(\tilde{N}_E)$. This along with $\deg(N_E) = 2+\deg(\tilde{N}_E)$ gives $\deg_K(\mathcal{N}_E) = \ell\cdot\deg(N_E) - 2\ell + 2$ for type 0. The computation is similar for types 1 and 2 and gives $\deg_K(\mathcal{N}_E) = \ell\cdot\deg(N_E) - 2\ell + 1$.

We now assume the reduction becomes good in K (type 3). The factors at infinity are

$$(1-\alpha_{\mathfrak{p}_\infty}u)^{-1}(1-\overline{\alpha}_{\mathfrak{p}_\infty}u)^{-1} = (1-a_{P_\infty}u)^{-1}\prod_{j=1}^{\ell-1}(1-I_{\infty,j}u)^{-1}(1-\overline{I_{\infty,j}}u)^{-1}$$

so we need $a_{P_\infty} = 0$ and $\ell = 2$ for this to possibly happen. This gives $\deg_K(\mathcal{N}_E) = 2\deg(N_E) - 4$ and the factor at infinity of $L^*(E\otimes\chi,u)$ is $(1-\alpha_{\mathfrak{p}_\infty}u)^{-1}(1-\overline{\alpha}_{\mathfrak{p}_\infty}u)^{-1}$. We note that $|\alpha_{\mathfrak{p}_\infty}| = \sqrt{q}$. We refer to [49] Appendix A for details on how to compute the reduction at infinity and to see how the type only depends on E for quadratic twists. □

	$a_{P_\infty} = 0$ type 0	$a_{P_\infty} = 0$ type 1 (χ quadratic)	$a_{P_\infty} = 0$ type 2 (χ quadratic)
χ even	$M = 2\deg(F) + \deg(N_E) - 4$ $G(u) = 1$	$M = 2\deg(F) + \deg(N_E) - 4$ $G(u) = 1$	$M = 2\deg(F) + \deg(N_E) - 4$ $G(u) = 1$
χ odd	$M = 2\deg(F) + \deg(N_E) - 4$ $G(u) = 1$	$M = 2\deg(F) + \deg(N_E) - 5$ $G(u) = 1 - u$	$M = 2\deg(F) + \deg(N_E) - 5$ $G(u) = 1 + u$

	$a_{P_\infty} = 0$ type 3 (χ quadratic)	$a_{P_\infty} = \pm 1$	E has good reduction at P_∞
χ even	$M = 2\deg(F) + \deg(N_E) - 4$ $G(u) = 1$	$M = 2\deg(F) + \deg(N_E) - 4$ $G(u) = 1 - a_{P_\infty} u$	$M = 2\deg(F) + \deg(N_E) - 4$ $G(u) = (1 - \alpha_{P_\infty} u)(1 - \overline{\alpha}_{P_\infty} u)$
χ odd	$M = 2\deg(F) + \deg(N_E) - 6$ $G(u) = (1 - \alpha_{\mathfrak{p}_\infty} u)(1 - \overline{\alpha}_{\mathfrak{p}_\infty} u)$	$M = 2\deg(F) + \deg(N_E) - 3$ $G(u) = 1$	$M = 2\deg(F) + \deg(N_E) - 2$ $G(u) = 1$

Table 13: Zeros of $L(E \otimes \chi, u)$

4.3 Unbounded Rank for Quadratic Dirichlet Characters

The following result comes from looking at the conductors of Dirichlet L-functions with large ranks. Hyperelliptic curves over function fields having arbitrarily large ranks were first constructed by Ulmer [63]. We construct a family of quadratic Dirichlet characters such that the rank of their L-functions is unbounded. It is already known [38, Introduction] that the number of different eigenvalues for these curves is dominated by the genus as it increases.

Theorem 4.3.1. *The following curve over* $\mathbb{F}_q$

$$C : y^2 = x^{q^{2^n}} - x$$

has zeta function

$$\mathcal{Z}_C(u) = \frac{(1 - q^{2^n} u^{2^{n+1}})^{\frac{q^{2^n}-1}{2^{n+1}}}}{(1-u)(1-qu)}$$

unless $n = 0$ *and* $q \equiv 3 \bmod 4$.

Proof. Let $m = 2^\ell$ with $\ell \leq n$. Let χ_m be the quadratic character on $\mathbb{F}_{q^m}$. Then

$$\sum_{x \in \mathbb{F}_{q^m}} \chi_m \left(x^{q^{2^n}} - x \right) = \sum_{x \in \mathbb{F}_{q^m}} \chi_m \left(x - x \right) = 0.$$

Let $m = 2^{n+1}$. Since the degree of the extension $\mathbb{F}_{q^m}/\mathbb{F}_{q^{2^n}}$ is even

$$\sum_{x \in \mathbb{F}_{q^m}} \chi_m \left(x^{q^{2^n}} - x \right) = \sum_{x \in A} \chi_m \left(x^{q^{2^n}} - x \right) \sum_{a \in \mathbb{F}_{q^{2^n}}} \chi_m(a) = (q^{2^n} - 1) \sum_{x \in A} \chi_m \left(x^{q^{2^n}} - x \right)$$

where A is any set of representatives when $\mathbb{F}_{q^{2^n}} \backslash \{0\}$ acts on $\mathbb{F}_{q^m}$ by multiplication. Fix a primitive element $\alpha \in \mathbb{F}_{q^{2^{n+1}}}$ and let

$$A = \{\alpha + c \mid c \in \mathbb{F}_{q^{2^n}}\} \cup \{0, 1\}.$$

Then

$$(\alpha + c)^{q^{2^n}} - (\alpha + c) = \alpha^{q^{2^n}} - \alpha = \alpha(\alpha^{q^{2^n}-1} - 1).$$

We have $\chi_m(\alpha^{q^{2^n}-1} - 1) = 1$ since it is a non-zero element of $\mathbb{F}_{q^{2^n}}$. We also have $\chi_m(\alpha) = -1$ since α is not a square. To see this, let ψ be a character of order 4 on $\mathbb{F}_{q^{2^n}}$. Then $\psi(\alpha^2) = \pm i$ since $\psi^2 \equiv \chi_{2^n}$ and $\chi_{2^n}(\alpha^2) = -1$. This means that the square roots of α lie in $\mathbb{F}_{q^{2^{n+2}}}$. So

$$\sum_{x \in \mathbb{F}_{q^m}} \chi_m \left(x^{q^{2^n}} - x \right) = -q^{2^n}(q^{2^n} - 1). \tag{4.3.1}$$

Since

$$x^{q^{2^n}} - x = \prod_{\substack{P \text{ prime} \\ \deg(P) | 2^n}} P$$

is square-free, the number of eigenvalues is $q^{2^n} - 1$. For $m > 0$

$$S_m := \sum_{x \in \mathbb{F}_{q^m}} \chi_m \left(x^{q^{2^n}} - x \right) = -q^{m/2} \sum_{j=1}^{q^{2^n}-1} e^{im\theta_j}$$

by the Weil's conjectures. From (4.3.1) we get $e^{2^{n+1} i\theta_j} = 1$ for all j, which implies the eigenvalues are (2^{n+1})th roots of unity. We also have $S_{2^n} = 0$, which means $e^{2^n i\theta_j}$ is equidistributed in $\{-1, 1\}$. If $e^{2^n i\theta_j} = 1$, then $e^{2^{n-1} i\theta_j} = \pm 1$. If $e^{2^n i\theta_j} = -1$, then $e^{2^{n-1} i\theta_j} = \pm i$. Since we also have $S_{2^{n-1}} = 0$ and since $[\mathbb{Q}(\zeta_{2^\ell}) : \mathbb{Q}] = \phi(2^\ell) = 2^{\ell-1}$, we must have that $e^{2^{n-1} i\theta_j}$ is equidistributed in $\{-1, 1, -i, i\}$. Repeating this argument shows that the eigenvalues are equidistributed in the (2^{n+1})th roots of unity and this concludes the proof. □

Remark 9. *This gives unbounded rank in the p, q, or g directions.*

Bibliography

[1] Salman Baig and Chris Hall. Experimental data for Goldfeld's conjecture over function fields. *Exp. Math.*, 21(4):362–374, 2012.

[2] Lior Bary-Soroker and Patrick Meisner. On the distribution of the rational points on cyclic covers in the absence of roots of unity. *Mathematika*, 65(3):719–742, 2019.

[3] Lea Beneish, Debanjana Kundu, and Anwesh Ray. Rank jumps and growth of shafarevich–tate groups for elliptic curves in $\mathbb{Z}/p\mathbb{Z}$-extensions. page arXiv:2107.09166.

[4] Ben Brubaker, Alina Bucur, Gautam Chinta, Sharon Frechette, and Jeffrey Hoffstein. Nonvanishing twists of GL(2) automorphic L-functions. *Int. Math. Res. Not.*, (78):4211–4239, 2004.

[5] Armand Brumer. The average rank of elliptic curves. I. *Invent. Math.*, 109(3):445–472, 1992.

[6] Nader H. Bshouty, Nuha Diab, Shada R. Kawar, and Robert J. Shahla. Enumerating all the irreducible polynomials over finite field. *WSEAS Transactions on Computers*, 15:248–257, 2016.

[7] Hung M. Bui and Alexandra Florea. Zeros of quadratic Dirichlet L-functions in the hyperelliptic ensemble. *Trans. Amer. Math. Soc.*, 370(11):8013–8045, 2018.

[8] Hung M. Bui, Alexandra Florea, Jonathan P. Keating, and Edva Roditty-Gershon. Moments of quadratic twists of elliptic curve L-functions over function fields. *Algebra Number Theory*, 14(7):1853–1893, 2020.

[9] Byungchul Cha, Daniel Fiorilli, and Florent Jouve. Independence of the zeros of elliptic curve L-functions over function fields. *Int. Math. Res. Not.*, 2017(9):2614–2661, 06 2016.

[10] Peter J. Cho. Analytic ranks of elliptic curves over number fields. page arXiv:2005.07909.

[11] Peter J. Cho and Jeongho Park. Low-lying zeros of cubic Dirichlet L-functions and the ratios conjecture. *J. Math. Anal. Appl.*, 474(2):876–892, 2019.

[12] Peter J. Cho and Jeongho Park. n-level densities for twisted cubic Dirichlet L-functions. *J. Number Theory*, 196:139–155, 2019.

[13] Peter J. Cho and Jeongho Park. Dirichlet characters and low-lying zeros of L-functions. *J. Number Theory*, 212:203–232, 2020.

[14] Sarvadaman Chowla. The Riemann hypothesis and Hilbert's tenth problem. *Norske Vid. Selsk. Forh. (Trondheim)*, 38:62–64, 1965.

[15] Fred Diamond Christophe Breuil, Brian Conrad and Richard Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises. *J. Amer. Math. Soc.*, 14, 2001.

[16] Antoine Comeau-Lapointe. One-level density of the family of twists of an elliptic curve over function fields. *Journal of Number Theory*, 2022.

[17] J. B. Conrey, J. P. Keating, M. O. Rubinstein, and N. C. Snaith. On the frequency of vanishing of quadratic twists of modular L-functions. In *Number theory for the millennium, I (Urbana, IL, 2000)*, pages 301–315. A K Peters, Natick, MA, 2002.

[18] Chantal David, Jack Fearnley, and Hershy Kisilevsky. On the vanishing of twisted L-functions of elliptic curves. *Experiment. Math.*, 13(2):185–198, 2004.

[19] Chantal David, Jack Fearnley, and Hershy Kisilevsky. Vanishing of L-functions of elliptic curves over number fields. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 247–259. Cambridge Univ. Press, Cambridge, 2007.

[20] Chantal David, Alexandra Florea, and Matilde Lalin. The mean values of cubic L-functions over function fields. *arXiv e-prints*, page arXiv:1901.00817, January.

[21] Chantal David, Alexandra Florea, and Matilde Lalín. Nonvanishing for cubic L-functions. *Forum Math. Sigma*, 9:e69, 2021.

[22] Chantal David and Ahmet M Güloğlu. One-level density and non-vanishing for cubic L-functions over the Eisenstein field. *Int. Math. Res. Not.*, 09 2021. rnab240.

[23] Persi Diaconis and Mehrdad Shahshahani. On the eigenvalues of random matrices. *J. Appl. Probab.*, 31A:49–62, 1994. Studies in applied probability.

[24] Ravi Donepudi and Wanlin Li. Vanishing of Dirichlet L-functions at the central point over function fields. *Rocky Mountain J. Math.*, 51(5):1615–1628, 2021.

[25] Jack Fearnley, Hershy Kisilevsky, and Masato Kuwata. Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves. *J. Lond. Math. Soc. (2)*, 86(2):539–557, 2012.

[26] Daniel Fiorilli. A conditional determination of the average rank of elliptic curves. *J. London Math. Soc.*, 94(3):767–792, 09 2016.

[27] Alexandra Florea. The fourth moment of quadratic Dirichlet L-functions over function fields. *Geom. Funct. Anal.*, 27(3):541–595, 2017.

[28] Alexandra Florea. The second and third moment of $L(1/2, \chi)$ in the hyperelliptic ensemble. *Forum Math.*, 29(4):873–892, 2017.

[29] Michele Fornea. Growth of the analytic rank of modular elliptic curves over quintic extensions. *Math. Res. Lett.*, 26(6):1571–1586, 2019.

[30] Dorian Goldfeld. *Conjectures on elliptic curves over quadratic fields*, volume 751 of *Lecture Notes in Math.* Springer, Berlin, 1979.

[31] Dorian M. Goldfeld. A simple proof of Siegel's theorem. *Proc. Nat. Acad. Sci. U.S.A.*, 71:1055, 1974.

[32] F. Gouvêa and B. Mazur. The square-free sieve and the rank of elliptic curves. *J. Amer. Math. Soc.*, 4(1):1–23, 1991.

[33] S. Gupta and D. Zagier. On the coefficients of the minimal polynomials of Gaussian periods. *Math. Comp.*, 60(201):385–398, 1993.

[34] D. R. Hayes. The expression of a polynomial as a sum of three irreducibles. *Acta Arith.*, 11:461–488, 1966.

[35] D. R. Heath-Brown. The average analytic rank of elliptic curves. *Duke Math. J.*, 122(3):591–623, 2004.

[36] Henryk Iwaniec, Wenzhi Luo, and Peter Sarnak. Low lying zeros of families of L-functions. *Publ. Math. Inst. Hautes Études Sci.*, 91:55–131, 2000.

[37] Nicholas M. Katz. *Twisted L-functions and monodromy*, volume 150 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2002.

[38] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.

[39] Robert J. Lemke Oliver and Frank Thorne. Rank growth of elliptic curves in non-abelian extensions. *Int. Math. Res. Not. IMRN*, (24):18411–18441, 2021.

[40] Wanlin Li. Vanishing of hyperelliptic L-functions at the central point. *J. Number Theory*, 191:85–103, 2018.

[41] Wanlin Li, Elena Mantovan, Rachel Pries, and Yunqing Tang. Newton polygons arising from special families of cyclic covers of the projective line. *Res. Number Theory*, 5(1):Paper No. 12, 31, 2019.

[42] Wanlin Li, Elena Mantovan, Rachel Pries, and Yunqing Tang. Newton polygons of cyclic covers of the projective line branched at three points. In *Research directions in number theory—Women in Numbers IV*, volume 19 of *Assoc. Women Math. Ser.*, pages 115–132. Springer, Cham, [2019] ©2019.

[43] Wanlin Li, Elena Mantovan, Rachel Pries, and Yunqing Tang. Newton Polygon Stratification of the Torelli Locus in Unitary Shimura Varieties. *International Mathematics Research Notices*, 12 2020. rnaa306.

[44] Barry Mazur and Karl Rubin. Arithmetic conjectures suggested by the statistical behavior of modular symbols. page arXiv:1910.12798.

[45] Barry Mazur and Karl Rubin. Diophantine stability. *Amer. J. Math.*, 140(3):571–616, 2018. With an appendix by Michael Larsen.

[46] Barry Mazur and Karl Rubin. Arithmetic conjectures suggested by the statistical behavior of modular symbols. *Experimental Mathematics*, 2021.

[47] Patrick Meisner. Distribution of points on cyclic curves over finite fields. *J. Number Theory*, 177:528–561, 2017.

[48] Patrick Meisner. One level density for cubic Galois number fields. *Canad. Math. Bull.*, 62(1):149–167, 2019.

[49] Patrick Meisner and Anders Södergren. Low-lying zeros in families of elliptic curve L-functions over function fields. page arXiv:2110.00102.

[50] J. S. Milne. The Tate-Šafarevič group of a constant abelian variety. *Invent. Math.*, 6:91–105, 1968.

[51] Hugh L. Montgomery. The pair correlation of zeros of the zeta function. *Proceedings of Symposia in Pure Mathematics*, 24, 1973.

[52] Joseph Oesterlé. Empilements de sphères. Number 189-190, pages Exp. No. 727, 375–397. 1990. Séminaire Bourbaki, Vol. 1989/90.

[53] Bjorn Poonen. Squarefree values of multivariable polynomials. *Duke Math. J.*, 118(2):353–373, 2003.

[54] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[55] Zeév Rudnick. Traces of high powers of the Frobenius class in the hyperelliptic ensemble. *Acta Arith.*, 143(1):81–99, 2010.

[56] Matthias Schütt and Tetsuji Shioda. *Mordell-Weil lattices*, volume 70 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer, Singapore, 2019.

[57] Igor E. Shparlinski. Finite fields: Theory and computation. *Mathematics and Its Applications*, 477, 1999.

[58] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2009.

[59] Ki-Seng Tan. Modular elements over function fields. *J. Number Theory*, 45(3):295–311, 1993.

[60] Ki-Seng Tan and Daniel Rockmore. Computation of L-series for elliptic curves over function fields. *J. Reine Angew. Math.*, 424:107–135, 1992.

[61] Terence Tao. A function field analogue of Riemann zeta statistics. *Blog post*, pages https://terrytao.wordpress.com/2019/05/17/a–function–field–analogue–of–riemann–zeta–statistics/, 2019.

[62] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1995.

[63] Douglas Ulmer. L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields. *Invent. Math.*, 167(2):379–408, 2007.

[64] André Weil. *Dirichlet Series and Automorphic Forms*, volume 189 of *Lect. Notes. Math.* Berlin–Heidelberg–New York, 1971.

[65] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141, 1995.

[66] Matthew Young. Low-lying zeros of families of elliptic curves. *J. Amer. Math. Soc.*, 19:205–250, 07 2006.