Università degli Studi "Roma Tre"

Scuola Dottorale in Scienze Matematiche e Fisiche

Dottorato di Ricerca in Matematica

QUESTIONS RELATED TO PRIMITIVE POINTS ON ELLIPTIC CURVES AND STATISTICS FOR BIQUADRATIC CURVES OVER FINITE FIELDS

Candidato:
Giulio Meleleo
Matricola 15854/311

Relatore:
Prof. Francesco Pappalardi

Coordinatore:
Prof. Luigi Chierchia

Dottorato di Ricerca in Matematica
XXVII Ciclo
A. A. 2014/2015

Introduction

Algebraic curves represent a very wide field of research in mathematics, and there are many possibilities about the point of view one can adopt to approach this topic. In this thesis we want to study some properties of two particular families of curves: elliptic curves and biquadratic curves. For this reason, we divided the thesis in two parts, one for each of these topics.

The first part begins with an introduction to the theory of elliptic curves. This is itself an incredibly rich area of research, because of the beautiful property of elliptic curves to have a group structure on the set of points with coordinates on a fixed field. We briefly give a definition by using Weierstrass equations and we give a description of the main properties of these curves depending on the field they are defined on ($\mathbb{Q}$, number fields, finite fields). Moreover, we say something about Galois representations attached to elliptic curves, a very important tool to discover properties of them, both algebraic and analytic. Then, we write about reduction modulo a prime number p of an elliptic curve E defined over $\mathbb{Q}$. This is an interesting thing in itself, because, if p does not divide the discriminant of the curve, we have a group homomorphism. Moreover, if we fix E and let the prime p vary in the set of prime numbers, we can ask very deep and interesting questions about the reduction modulo p. Most of these questions are about the density of primes for which a certain property holds in the reduction mod p of the elliptic curve (we denote the reduction of E as $\bar{E} \mod p$. One of these questions, called the Lang-Trotter conjecture for Primitive Points (cf. [LT77]), comes from a classical analytic number theoretical question about reductions of rational numbers, namely the Artin primitive root conjecture (cf. [Hoo67]). The main tool to attack this kind of problems is the Chebotarev Density Theorem, of which we write an effective version of Serre. At the end of the first chapter we give details about the paper of 1977 in which Lang and Trotter gave the statement of their conjecture.

In the second chapter we study a strange, but not so rare, situation when a point on an elliptic curve is "very far" from being primitive. A point P on an elliptic curve is primitive modulo p if $P \mod p$ generates the group $\bar{E}(\mathbb{F}_p)$. The aim of the Lang-Trotter conjecture is to give a density of the primes for which a fixed P in $E(\mathbb{Q})$ is primitive modulo p. Going in some sense in the opposite direction, we give the definition of a never-primitive point as a point P that is primitive modulo p only for a finite set of primes p. We give some necessary conditions for the presence of these points on a given elliptic curve and we give a non trivial example (cf. Section 2.2) where all points on an elliptic curve of positive rank are never-primitive. These conditions involve a precise structure of the Galois representations at a fixed prime p, both for curves with trivial (cf. Proposition 2.4.3) and non trivial (cf. Proposition 2.4.4) torsion in the group of rational points. Finally, in Section 2.5, we give a splitting condition on a polynomial depending on E, P and a prime p, to assure the fact that P is a never-primitive point.

In the third chapter we consider a problem that is weaker than the one in the Lang-Trotter conjecture. It is essentially the content of the submitted paper [Mel15]. Given an elliptic curve E over $\mathbb{Q}$ of rank at least $r > 0$, and a free subgroup Γ of $E(\mathbb{Q})$ of rank exactly r, we want to find the density of primes (of good reduction for E) for which $\bar{E}(\mathbb{F}_p)/\bar{\Gamma} \mod p$ is a cyclic group. This is the content of Theorem 3.1.1. For the proof of this result, we use Chebotarev Density Theorem on some special extensions of $\mathbb{Q}$, that are the equivalent of Kummer extensions, in the setting of elliptic curves. The splitting of a rational prime p in such extensions says something very precise about the structure of $\bar{E}(\mathbb{F}_p)/\bar{\Gamma} \mod p$, from which we can deduce a good asymptotic formula for the density. At the end of this chapter we give a list of the possible directions of research one can take starting from this problem about cyclicity of quotients of reductions.

The second part is an extract of a joint work (cf. [LMM15]) with Elisa Lorenzo Garcia, postdoctoral researcher at the University of Leiden, and Piermarco Milione, graduate student at the University of Barcelona.

The big area of research in which this work can be placed is Arithmetic Statistics, or more precisely Statistics about Curves over Finite Fields. The aim of our work is to extend, to families of biquadratic curves, some statistics that were already done for other families (i.e. hyperelliptic curves, cyclic trigonal curves and others). The interest is in the fact that we consider curves that are non-cyclic covers of the projective line, since this can be the starting point for future studies for general abelian covers.

The fourth chapter is dedicated to the introduction of notions and methods we need to do statistics on families of curves over finite fields. We start with the definition of zeta functions over function fields (i.e. finite extensions of $\mathbb{F}_q(t)$, with $\mathbb{F}_q$ finite field) starting with the example when the function field is $\mathbb{F}_q(t)$. We see that, as in the classical case of Riemann zeta function, we can write the zeta function of $\mathbb{F}_q(t)$ as an Euler product, in which the role of primes is played by irreducible polynomials in $\mathbb{F}_q[t]$. There is a whole dictionary between number fields and function fields, of which we give also a brief description (cf. Section 4.1). Then, we see that there is an equivalence of categories between smooth curves over $\mathbb{F}_q$ and finite extensions of $\mathbb{F}_q(t)$, that allows one to define a zeta function attached to a curve. The most important properties of zeta functions of curves over finite fields are expressed by Weil Theorem. Thanks to these properties we can do statistics about the number of points of curves in a given family looking at traces of matrices called Frobenius classes. We conclude the chapter with the exposition of some questions one can ask about families of curves, that are the questions we will answer for biquadratic curves.

In the fifth chapter, we first define a biquadratic curve (cf. Definition 5.2.1) and we describe the family of biquadratic curves of fixed genus. The main result is about a subfamily, that algebraic geometers call connected component of the coarse muduli space of biquadratic curves of genus g. We use some methods developed, among others, in [KR09] and [BDFL10] respectively for hyperelliptic curves and cyclic l-covers of the projective line. We prove that the number of points of curves in such a subfamily can be written, for the limit of g that tends to infinity, as a sum of $q + 1$ independent and identically distributed random variables. This is exactly the content of Theorem 5.3.1. Nowadays, we are trying to prove a version of this theorem for r-quadratic curves, namely curves whose function field has Galois group $(\mathbb{Z}/2\mathbb{Z})^r$ over $\mathbb{F}_q(t)$. We have a good description of the family, and we found an interesting generalization in this case (cf. [LMM15, Theorem 6.6]).

In the sixth and last chapter, we want to compute the average of the number of points on biquadratic curves in a certain family. A biquadratic curve has an affine model that is given by a system of two equations $y_i^2 = h_i(t)$ for $i = 1, 2$ and we can see that, up to a certain change of generators of the extension, one of the two polynomials has even degree. So we have to prove a result that Rudnick gave for hyperelliptic curves defined by polynomial of odd degree (cf. [Rud10]), in the case of polynomials of even degree. More precisely, we compute the average of (powers of) traces of the Frobenius classes in the family of hyperelliptic curves with affine model given by $y^2 = h(t)$, with $h(t)$ polynomial of degree $2g + 2$ (g is the genus of the curves), at the limit $g \to \infty$. Even if we use the methods of Rudnick, some intermediate results (like for example Proposition 6.3.1) are quite different, and so this is an interesting result in itself, contained in Theorem 6.1.1. The next step is the application of this result to a certain family of biquadratic curves, different from the one in Chapter 4, that is chosen to let the results for hyperellitpic curves be applicable. We do not arrive to a final version of an analogous theorem for biquadratic curves, but we strongly believe that if we can give an estimate for a certain sum of characters (cf. Section 6.7), we can finally have the desired result.

Notations

We give a list of notations we will use in the thesis. We denote with $\mathbb{Z}$ the ring of integers and with $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ respectively the field of rational, real and complex numbers. $\mathbb{F}_q$ is the finite field with q elements, where q is a power of a prime p. Given any field K, we denote with $\bar{K}$ an algebraic closure of it.

For two real functions $f(x), g(x)$, we write $f(x) = O(g(x))$ (or equivalently $f(x) \ll g(x)$) if and only if there exists a constant $C > 0$ such that $|f(x)| \leqslant Cg(x)$ for all values of x under consideration (generally we use it for $x \to \infty$).

Since the two parts of the thesis are mutually independent, there are some symbols used in different ways. Anyway, there is no risk of ambiguity, as the two contexts are very different. For this reason, we give a more specific description of the notations we are going to use.

Part I

Even if the symbol K is used in general to denote a field, sometimes in we use it to denote a number field. We always specify when this is the case. If so, we denote with $\mathcal{O}_K$ the ring of integers of K, with $\mathfrak{p}, \mathfrak{q}$ prime ideals of $\mathcal{O}_K$, and with $k_\mathfrak{p}$ (resp. $k_\mathfrak{q}$) the residue field $\mathcal{O}_K/\mathfrak{p}$ (resp. $\mathcal{O}_K/\mathfrak{q}$).

Part II

The letter p denotes a prime integer greater than 2, $q = p^r$ is a positive power of p, and $k := \mathbb{F}_q(t)$ is the field of rational functions over $\mathbb{F}_q$. We denote with (f, g) greatest common divisor of the polynomials f, g, with $\mathrm{lc}(f)$ the leading coefficient of the polynomial f, and $\tilde{f}$ is the polynomial obtained inverting the order of the coefficients of f. Moreover, K is generally a finite Galois extension of k.

Acknowledgements

First of all, I want to thank my advisor, Francesco Pappalardi, for all the help, answers and patience he has generously offered to me during all the period of preparation of this thesis. Moreover, I would like to thank him for his moral support and understanding in my difficult times.

For the interesting and extremely useful discussions about Elliptic Curves and Galois Representations (and many other topics), I thank René Schoof. He was the first one conveying his passion for number theory to me.

The second part of the thesis is about a joint work with Elisa Lorenzo Garcia and Piermarco Milione. It has been an honour and a pleasure working with such brilliant and talented mathematicians.

We started to work together at the Arizona Winter School in March 2014. In that occasion, we were introduced to Arithmetic Statistics on Curves over Finite Fields in a wonderful working group coordinated by Chantal David and Alina Bucur. I want to thank them for all the support and the precious comments about our work.

Finally, I want to thank Zéev Rudnick for his kind and enlightening answers about his work on hyperelliptic curves.

Contents

Introduction i

Notations v

Acknowledgements vii

I Primitive Points on Elliptic Curves 1

1 Elliptic Curves and the Lang-Trotter conjecture 3
1.1 Definition and the Group Law . . . 3
1.2 Points of m-torsion . . . 4
1.3 Elliptic Curves over Number Fields . . . 4
1.4 Elliptic Curves over Finite Fields . . . 5
1.5 Galois Representations attached to Elliptic Curves . . . 6
1.6 Reduction modulo p of Elliptic Curves . . . 7
1.6.1 Chebotarev Density Theorem . . . 8
1.7 The paper of Lang and Trotter . . . 9

2 Never-primitive points on Elliptic Curves 13
2.1 A curve with a 2-torsion rational point and no primitive points . . . 13
2.2 A curve of rank 1 with no rational torsion points and no primitive points . . . 14
2.3 Definition of Never-primitive Point . . . 16
2.4 Conditions for existence of Never-primitive points . . . 17
2.4.1 Elliptic Curves with trivial torsion . . . 17
2.4.2 Elliptic Curves with non-trivial torsion . . . 19
2.5 The reducibility of the polynomial $[p]Q = P$ . . . 21

3 Cyclicity of Quotients of Reductions 23
3.1 Presentation and context of the problem . . . 23
3.2 Some notations and definitions . . . 24
3.3 Preliminary lemmas . . . 24
3.4 Proof of Theorem 3.1.1 . . . 25
3.5 The Euler product for $c_{E,\Gamma}$ . . . 27
3.6 Possible paths of future research . . . 28

II Statistics on Biquadratic Curves over Finite Fields 29

4 Preliminaries to Arithmetic Statistics on Curves over Finite Fields 33
4.1 Zeta Functions over Function Fields . . . 33
4.2 From Function Fields to Curves . . . 36
4.3 Weil Theorem . . . 36
4.4 Number of Points in Families of Curves as a sum of Random Variables . . . 37

5 The fluctuations in the number of points of a Biquadratic Curve over a Finite Field 39
5.1 Number of points of Biquadratic Curves as a sum of Random Variables . . . 39
5.2 The family of biquadratic curves . . . 40
5.3 Proof of the Main Theorem . . . 43

6 Traces of High Powers of the Frobenius Class in the family of Biquadratic Curves 49
6.1 Introduction . . . 49
6.2 The family $\mathcal{H}_{2g+2}$ of hyperelliptic curves . . . 50
6.2.1 Averaging over $\mathcal{H}_{2g+2}$ . . . 51
6.2.2 Averaging quadratic characters . . . 51
6.2.3 A sum of Möbius values . . . 52
6.2.4 The probability that $P \nmid h$ . . . 52
6.2.5 Double character sums . . . 53
6.3 Proof of Theorem 6.1.1 . . . 53
6.3.1 Contribution of squares . . . 53
6.3.2 Contribution of primes . . . 54
6.3.3 Bounding the contribution of primes . . . 54
6.3.4 The contribution of higher prime powers . . . 59
6.3.5 Conclusion of the proof . . . 59
6.4 The number of points of a biquadratic curve over $\mathbb{F}_{q^n}$ . . . 60
6.5 The family $\mathcal{B}_{d_1,d_2}$ of biquadratic curves . . . 61
6.5.1 The average of a function on $\mathcal{B}_{d_1,d_2}$ . . . 62
6.6 Average of Traces of High Powers of the Frobenius Class in the family $\mathcal{B}_{2g_1+2,2g_2+2}$ 62
6.7 A new sum of characters . . . 66

Bibliography 67

Part I

Primitive Points on Elliptic Curves

Chapter 1

Elliptic Curves and the Lang-Trotter conjecture

1.1 Definition and the Group Law

The first part of this thesis is dedicated to results about points on Elliptic Curves with special properties. So, in this first chapter, we introduce these objects and we recall their properties, needed to prove our results. The main bibliographical reference is Silverman [Sil08], but we will also mention results from Washington [Was08], Silverman [Sil94], Serre [Ser72] and [Ser89].

Definition 1.1.1. An Elliptic Curve E over a field K is the projective locus (in $\mathbb{P}^2(K)$) of the (projectification of the) equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with $a_1, a_2, a_3, a_4, a_6 \in K$ and with the condition that the discriminant $\Delta_E = \Delta_E(a_1, a_2, a_3, a_4, a_6) \neq 0$ in K. This is equivalent to say that the curve is smooth. We will denote the point at infinity $[0 : 1 : 0]$ as $\mathcal{O}$.

The equation in 1.1.1 is called a *Weierstrass equation*. If $\mathrm{char}(K) \neq 2, 3$ it can be reduced to the easier form

$$E : \ Y^2 = X^3 + aX + b$$

where $a, b \in K$ are such that $\Delta = -16(4a^3 + 27b^2)$ is nonzero. For properties of Weierstrass equations see Section III.1 of [Sil08].

Proposition 1.1.2 (Section III.2 [Sil08])**.** *The set $E(K)$ of K rational points on E has a structure of abelian group $(E(K), +)$, with neutral element $\mathcal{O}$ given by the following geometric rule: the sum of three points equals $\mathcal{O}$ if and only if the points belong to the same line. As the group law is given by this geometric rule, there are rational functions defining it.*

We will need the following notion:

Definition 1.1.3 (Section III.4 [Sil08])**.** Let E_1, E_2 be two elliptic curves defined over a field K. An *isogeny* from E_1 to E_2 is a morphism (of algebraic curves) over K, $\phi : E_1 \to E_2$ that satisfies $\phi(\mathcal{O}) = \mathcal{O}$. An isogeny from E to itself is called an endomorphism.

One can see that the set $\mathrm{End}_K(E)$ of endomorphisms of E over K is in fact a ring, with operations defined by

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$
$$(\phi\psi)(P) = \phi(\psi(P))$$

1.2 Points of m-torsion

There are some natural maps that can be defined on $E(K)$, namely the *multiplication by n* maps, where n is a positive integer. If P is a point in $E(K)$, we will denote with $[n]P$ (or sometimes nP) the multiplication by n of P. These maps are endomorphisms of $E(K)$. We can also define multiplications by negative integers, just defining $[-1]P = -P$, where $-P$ is the inverse of P in the group law of E.

Given a positive integer m, we denote with $E[m]$ the subgroup of $E(\bar{K})$ annihilated by m. In other words, $E[m]$ is the kernel of the endomorphism $[m] : E(\bar{K}) \to E(\bar{K})$ that sends P to $[m]P$. The group $E[m]$ is called the *group of m-torsion points of E* (also known as m-division points). The following theorem gives the structure of $E[m]$ for elliptic curves defined over fields of any characteristic.

Theorem 1.2.1 (Theorem 3.2 [Was08])**.** *Let E be an elliptic curve over a field K and let m be a positive integer. Let C_m be the cyclic group of order m. If the characteristic of K does not divide m, or is 0, then*

$$E[m] \simeq C_m \oplus C_m.$$

If the characteristic of K is $p > 0$ and $p \mid m$, write $m = p^r m'$ with $p \nmid m'$. Then

$$E[m] \simeq C_{m'} \oplus C_{m'} \text{ or } E[m] \simeq C_{m'} \oplus C_m.$$

In the case of elliptic curves defined over $\mathbb{Q}$, the set of endomorphisms $[m]$, with $m \in \mathbb{Z}$, is a ring isomorphic to $\mathbb{Z}$. Then $\mathrm{End}_{\bar{\mathbb{Q}}}(E)$ contains $\mathbb{Z}$ as a subring.

If $\mathrm{End}_{\bar{\mathbb{Q}}}(E) = \mathbb{Z}$, we say that E is *without complex multiplication* (non-CM). If $\mathrm{End}_{\bar{\mathbb{Q}}}(E) \supsetneq \mathbb{Z}$, then E is *with complex multiplication* (CM) and $\mathrm{End}_{\bar{\mathbb{Q}}}(E)$ is an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, called the *CM field* of E. For an introduction to the theory of Complex Multiplication we refer the reader to Chapter II and Section A.3 of [Sil94].

1.3 Elliptic Curves over Number Fields

If K is a number field (i.e. a finite extension of $\mathbb{Q}$), we have an important result about the group structure of $E(K)$.

Theorem 1.3.1 (Mordell-Weil, [Sil08] Chapter VIII)**.** *Let E be an elliptic curve over a number field K. Then, the group $E(K)$ is finitely generated, that is*

$$E(K) \simeq \mathbb{Z}^r \oplus T$$

where r is an integer, called the arithmetic rank of E over K, and T is a finite group called the torsion subgroup of $E(K)$.

In 1977, Mazur gave a list of groups that can appear instead of T, in the case of $K = \mathbb{Q}$.

Theorem 1.3.2 ([Maz77]). *Let E be an elliptic curve defined over $\mathbb{Q}$. If C_n denotes the cyclic group of order n, then the possible torsion subgroups of $E(\mathbb{Q})$ are C_n with $1 \leqslant n \leqslant 10$, or C_{12} or either the direct sums of $C_2 \oplus C_{2m}$ with $1 \leqslant m \leqslant 4$.*

1.4 Elliptic Curves over Finite Fields

It is an obvious observation that, if an elliptic curve E is defined over a finite field $\mathbb{F}_q$, with q a power of a prime p, then the group $E(\mathbb{F}_q)$ is finite. In this section we will recall the main properties of this group.

Theorem 1.4.1 (Hasse, Section V.1 [Sil08]). *If $E/\mathbb{F}_q$ is an elliptic curve defined over a finite field, then*

$$|\, \#E(\mathbb{F}_q) - q - 1| \leqslant 2\sqrt{q}.$$

Hasse's theorem can be interpreted as the Riemann Hypothesis for the function field associated with the given elliptic curve, in a sense that will be explained in Part II (Section 4.3) of this thesis.

We can describe more precisely the group structure of $E(\mathbb{F}_q)$ in the following result, that is a consequence of the structure of torsion groups $E[m]$.

Proposition 1.4.2 (Theorem 4.1 [Was08]). *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then, $\exists n, k \in \mathbb{N}$ such that*

$$E(\mathbb{F}_q) \cong C_n \oplus C_{nk}.$$

Hence $E(\mathbb{F}_q)$ is a finite group of rank at most 2 (with the notation of the previous proposition, $E(\mathbb{F}_q)$ is cyclic if and only if $n = 1$). Moreover, by using the Hasse bound given in Theorem 1.4.1, we have that $q + 1 - 2\sqrt{q} \leqslant n^2 k \leqslant q + 1 + 2\sqrt{q}$.

Given a curve E over a finite field $\mathbb{F}_q$, an important endomorphism is the so called *Frobenius endomorphism*

$$\phi_q : E \to E$$
$$(x, y) \mapsto (x^q, y^q).$$

This endomorphism has many properties and is crucial for the proof of Hasse's Theorem. In fact, we have that

$$E(\mathbb{F}_q) = \ker(1 - \phi_q)$$

and (see Theorem 2.3.1 in Chapter V of [Sil08]) that, if we write

$$a = q + 1 - \#E(\mathbb{F}_q),$$

then the q-th Frobenius endomorphism satisfies

$$\phi_q^2 - a\phi_q + q = 0 \text{ in } \operatorname{End}_{\mathbb{F}_q}(E).$$

Moreover, let $\alpha, \beta \in \mathbb{C}$ be the roots of the polynomial $T^2 - aT + q$. Then α and β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$ and for every $n \geqslant 1$,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

1.5 Galois Representations attached to Elliptic Curves

Given an elliptic curve E defined over $\mathbb{Q}$, we know that $E[m] \simeq C_m \oplus C_m$ for every positive integer m.

We can define $\mathbb{Q}(E[m])$, adjoining to $\mathbb{Q}$ all the x and y-coordinates of the m-division points of E. This is called the *m-division field of E*. It can be proved (Corollary 3.11 of [Was08]) that

$$\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(E[m]),$$

where ζ_m is an m-th primitive root of 1.

Moreover, we can associate to $E[m]$ a *Galois representation*

$$\Phi_m : \mathrm{Gal}(\mathbb{Q}(E[m]/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

which can be seen to be injective. The question about the surjectivity of this representation leads to one of the most relevant differences between CM and non-CM elliptic curves. In fact, for a CM elliptic curve E, Φ_m is not surjective for any integer $m > 2$ (proved by Deuring in [Deu41], 1941) and in this case we have

$$\phi(m)^2 \leqslant [\mathbb{Q}(E[m]) : \mathbb{Q}] \leqslant m^2,$$

where ϕ is the Euler totient function. The case of non-CM elliptic curves is quite different. It was studied by Serre in 1972 (see [Ser72]). Serre showed that, if E has no complex multiplication, there exists a positive integer $A(E)$, depending on E, such that Φ_m is surjective for any integer m that is coprime to $A(E)$. Then, in the non-CM case, for such m we have

$$[\mathbb{Q}(E[m]) : \mathbb{Q}] = |\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})| = m^4 \prod_{q|m} \left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right)$$

where q are prime divisors of m.

Now, we want to give a brief description of what can happen when Φ_m is not surjective, in particular when $m = p$ is prime. Essentially, we want to see which are the subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$. This is the content of Section 2 of [Ser72]. A good rewriting of this paper of Serre can be found in [Dos10].

Suppose that V is a vector space of dimension 2 over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We have $\mathrm{GL}(V) \cong \mathrm{GL}_2(\mathbb{F}_p)$. Here are some of the possible subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$:

Cartan subgroups

Given two different lines in V, if C is the subgroup in $\mathrm{GL}(V)$ of all the elements for which those lines are stable, we call such group a *split Cartan subgroup*. Choosing a convenient basis of V, C can be written in the form

$$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix},$$

hence it is abelian of order $(p-1)^2$.

Let $k \subset \mathrm{End}(V)$ be a field with p^2 elements. We call the subgroup k^* of $\mathrm{GL}(V)$ a *non-split Cartan subgroup*. It is a cyclic group of order $p^2 - 1$.

Borel subgroups

Given one line in V, if B is the subgroup of $\mathrm{GL}(V)$ of all the elements for which that line is stable, we call such group a *full Borel subgroup* of $\mathrm{GL}(V)$. Choosing a convenient basis, the elements of B can be written in the form

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

and so B is of order $p(p-1)^2$. There are also proper subgroups of B. In the future we will denote with $pB.a.b$ the subgroup of B in $\mathrm{GL}_2(\mathbb{F}_p)$ generated by the matrices

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & r/b \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

where r is the least positive integer that generates $\mathbb{F}_p^*$. So, for example, $pB.1.r$ is the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ whose elements can be written in the form

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

and then it has cardinality $(p-1)p$.

Other subgroups

There are other groups occurring as subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, like normalizers of Cartan subgroups or other exceptional groups, but their treatment is not necessary to the development of this thesis.

We will need these notions in 2, where the presence of a Borel subgroup or a split Cartan subgroup as images of the Galois Representation at some prime will be related to the presence of points with a particular behavior.

1.6 Reduction modulo p of Elliptic Curves

Given an elliptic curve E defined over $\mathbb{Q}$ by a Weierstrass equation, a good way to understand better the nature of the group $E(\mathbb{Q})$ is to study reductions of E modulo primes. The reduction of E modulo a prime p is given by the equation

$$\bar{E} : Y^2 + a_1XY + a_3Y \equiv X^3 + a_2X^2 + a_4X + a_6 \mod p.$$

If we want $\bar{E}$ to be an elliptic curve over $\mathbb{F}_p$, p must not divide the discriminant Δ_E of E. Such a prime is called *prime of good reduction*. It is an interesting question to ask what are the structure and the properties of the group $\bar{E}(\mathbb{F}_p)$ as p varies. If there is ambiguity on which prime the curve is reduced, we will use the notation E_p instead of $\bar{E}$.

As $\bar{E} \mod p$ is an elliptic curve over $\mathbb{F}_p$, it will have all the properties described in Section 1.4. In particular

$$\bar{E}(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/d_pe_p\mathbb{Z}$$

with d_p, e_p uniquely determined positive integers.

For details about all the problems arising from reduction of elliptic curves modulo p, we refer the reader to the surveys of A.C. Cojocaru [Coj04] and E. Kowalski [Kow06].

In a more general situation, if E is defined over a number field K and $\mathfrak{p}$ is a prime (ideal) of the ring of integers $\mathcal{O}_K$ of K, we can define, in a similar way, the reduction $\bar{E}$ modulo $\mathfrak{p}$. If $\mathfrak{p} \nmid (\Delta_E)$, then $\bar{E}$ is an elliptic curve over $k_\mathfrak{p}$, that is the residue field of $\mathcal{O}_K$ at $\mathfrak{p}$.

1.6.1 Chebotarev Density Theorem

Let E be an elliptic curve over $\mathbb{Q}$. All the primes p not dividing the discriminant Δ_E of E are primes of good reduction, so one can ask the density of primes q for which a certain property is satisfied in $\bar{E}(\mathbb{F}_q)$. We will introduce in the next section a problem of this kind.

One of the most powerful tool to give an answer to these questions is the Chebotarev Density Theorem (CDT). A good reference to understand the history, context and original proof of this result is [LS96].

Before stating the theorem, we recall the definition of Artin symbol (Chapter X [Lan94]). Let $K/\mathbb{Q}$ be a finite Galois extension and let p be prime, unramified in K, and let $\mathfrak{p}$ be a prime of K above p. The *Frobenius element* $\sigma_\mathfrak{p} \in \mathrm{Gal}(K/\mathbb{Q})$ is the automorphism that has the following property:

$$\sigma_p(\alpha) = \alpha^{N\mathfrak{p}} \mod \mathfrak{p} \quad \forall \alpha \in \mathcal{O}_K.$$

It can also be denoted by $\mathrm{Frob}_\mathfrak{p}$ and it is essentially the lift to $\mathcal{O}_K$ of the Frobenius automorphism of $\mathcal{O}_K/\mathfrak{p} =: k_\mathfrak{p}$. The *Artin symbol*

$$\left[\frac{K/\mathbb{Q}}{p}\right]$$

is the conjugation class of all such $\sigma_\mathfrak{p}$.

Theorem 1.6.1 (Chebotarev Density Theorem)**.** *If $K/\mathbb{Q}$ is a finite Galois extension and $\mathcal{C} \subset \mathrm{Gal}(K/\mathbb{Q})$ is a union of conjugation classes of $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$, then the density of primes p such that the Artin symbol $\left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}$ equals $\frac{\#\mathcal{C}}{\#\mathcal{G}}$.*

The Chebotarev Density Theorem has also a quantitative version. The first one was proved by Lagarias and Odlyzko in [LO77]. Here we give a version that can be found in [Ser81] and [MMS88].

Theorem 1.6.2 (Effective CDT under GRH)**.** *Let*

$$\pi_{\mathcal{C}/\mathcal{G}}(x) := \#\left\{p \leqslant x : \left[\frac{K/\mathbb{Q}}{p}\right] \subset \mathcal{C}\right\}.$$

Then, assuming that the Dedekind zeta function of K satisfies the Generalized Riemann Hypothesis (GRH),

$$\pi_{\mathcal{C}/\mathcal{G}}(x) = \frac{\#\mathcal{C}}{\#\mathcal{G}} \int_2^x \frac{dt}{\log x} + O\left(\sqrt{\#\mathcal{C}}\sqrt{x}\log(xM\#\mathcal{G})\right)$$

where M is the product of primes numbers that ramify in $K/\mathbb{Q}$.

We will use this version of CDT to prove the main theorem of Chapter 3.

An analogue version, independent on the Generalized Riemann Hypothesis and then with a weaker error term, can be found in [Ser81].

1.7 The paper of Lang and Trotter

One problem about reductions of an elliptic curve modulo p comes from a classical problem, known today as *Artin's conjecture on primitive roots*, that predicts the density of primes p for which a given integer $a \in \mathbb{Z}$ (such that a is not a perfect square and different from ± 1) is a primitive root modulo p, i.e. the reduction of a modulo p generates the group $(\mathbb{Z}/p\mathbb{Z})^*$. This question can be translated in the language of elliptic curve theory in the following way:

Problem 1.7.1. Let E be an elliptic curve defined over $\mathbb{Q}$, with arithmetic rank $\geqslant 1$. Let $P \in E(\mathbb{Q})$ a point of infinite order. We want to know the asymptotic behavior of

$$\#\{p \leqslant x \mid \ p \nmid \Delta_E,\, \bar{E}(\mathbb{F}_p) = \langle P \mod p \rangle\}$$

as $x \to \infty$.

In other words, this problems asks the density of primes p for which P is a primitive point modulo p, in the sense given by the following definition.

Definition 1.7.2. Let E be an elliptic curve over $\mathbb{Q}$ and p a prime number. A point $P \in E(\mathbb{Q})$ is said to be a *primitive point modulo* p if $\bar{E}(\mathbb{F}_p) = \langle P \mod p \rangle$.

This problem is called the *Lang-Trotter conjecture for Primitive Points on Elliptic Curves*, from the names of the mathematicians who formulated it for the first time in 1977 ([LT77]). The main difference with the Artin's primitive root conjecture is that we even don't know a priori whether the group $\bar{E}(\mathbb{F}_p)$ is cyclic or not, while we know that $(\mathbb{Z}/p\mathbb{Z})^*$ is always cyclic. There are several results about cyclicity (see for example [CM04]), but we will focus principally on results related to the Lang-Trotter conjecture.

The conjecture, as stated in [LT77] can be synthesized in the following

Conjecture 1.7.3 (Lang–Trotter)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without CM, and $P \in E(\mathbb{Q})$ be a point of infinite order. Let Δ_E be the discriminant of E. Then $\exists \alpha_{E,P} \in \mathbb{Q}^{\geqslant 0}$ such that*

$$\frac{\#\{p \leqslant x : p \nmid \Delta_E, \bar{E}(\mathbb{F}_p) = \langle P \bmod p \rangle\}}{\pi(x)} \sim \alpha_{E,P} \prod_{\ell} \left(1 - \frac{\ell^3 - \ell - 1}{\ell^2(\ell-1)^2(\ell+1)}\right).$$

We can observe that there are some trivial cases in which $\alpha_{E,P} = 0$. For example this is the case when $E[2] \subset E(\mathbb{Q})$ or when $P = kQ$, $Q \in E(\mathbb{Q})$ and $d = \gcd(k, \#\operatorname{Tor}(E(\mathbb{Q}))) > 1$, since we have $\operatorname{ord} P \mid \frac{\#\bar{E}(\mathbb{F}_p)}{d}$.

Now, we want to describe the density we are looking for, introducing some tools that are necessary in a Chebotarev-based proof.

First, let $m \in \mathbb{N}$ and set

$$\frac{1}{m}P = \{Q \in E(\bar{\mathbb{Q}}) : mQ = P\}.$$

The cardinality of this set is m^2 because $\frac{1}{m}P$ is the fiber of P in the endomorphism $[m] : E \to E$, that has degree m^2. We can see in [BSS99] III.4 that the multiplication by m can be defined via some rational functions $\theta_m, \psi_m, \omega_m$, defined by induction, in the following way:

$$[m](x,y) = \left(\frac{\theta_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x)}\right) \in \mathbb{Q}(x) \times (2y + a_1x + a_3)\mathbb{Q}(x).$$

Since we want to find all Q such that $mQ = P$, we have to find the roots x_Q of the polynomial

$$\theta_m(x) - x_P\psi_m^2(x),$$

where x_Q, x_P refer to the first coordinates of Q and P, respectively. This polynomial is known to be separable and of degree m^2.

If we fix $Q_0 \in \frac{1}{m}P$, then

$$\frac{1}{m}P = Q_0 + E[m]$$

is a $\mathbb{Z}/m\mathbb{Z}$-affine space of dimension 2. So we can consider the group of affine transformations

$$\mathrm{Aff}\left(\tfrac{1}{m}P\right) := \mathrm{Aut}(E[m]) \ltimes E[m].$$

If $\sigma = (\gamma, \tau) \in \mathrm{Aff}(\frac{1}{m}P)$, then σ acts on $Q = Q_0 + R$, with $R \in E[m]$, as

$$(\gamma, \tau) : Q_0 + R \mapsto Q_0 + \gamma R + \tau.$$

Now let's introduce

$$G_m = \mathrm{Gal}\left(\mathbb{Q}(\tfrac{1}{m}P)/\mathbb{Q}\right)$$

where $\mathbb{Q}(\frac{1}{m}P)$ is the extension of $\mathbb{Q}$ obtained adjoining to $\mathbb{Q}$ all the x and y coordinates of the points $Q \in \frac{1}{m}P$. $\mathbb{Q}(\frac{1}{m}P)$ is the splitting field of $\theta_m - x_P\psi_m^2(x)$, then it's a finite Galois extension of $\mathbb{Q}$.

One easy thing to prove is that $\mathbb{Q}(\frac{1}{m}P) \supset \mathbb{Q}(E[m])$. In fact, if $Q_1, Q_2 \in \frac{1}{m}P$, and $Q_1 \neq Q_2$ then $\mathcal{O} \neq Q_1 - Q_2 \in E[m]$.

At this point we can look at

$$T_m = \mathrm{Gal}\left(\mathbb{Q}(\tfrac{1}{m}P)/\mathbb{Q}(E[m])\right)$$

that is the subgroup of *Galois translations* in G_m. This name comes from the fact that if $\tau \in T_m$, $R_\tau = \tau(Q_0) - Q_0$, then

$$\tau : \frac{1}{m}P \to \frac{1}{m}P, Q = R + Q_0 \mapsto Q + R_\tau,$$

so we can deduce the inclusion $T_m \hookrightarrow E[m], \tau \mapsto R_\tau$.

Since $\mathbb{Q}(E[m])$ is a normal extension of $\mathbb{Q}$, we have that T_m is a normal subgroup of G_m and $G_m/T_m \cong \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$. Finally, from a result of Bashmakov ([Bas70]), we know that $\exists B(E) \in \mathbb{N}$ such that, if $\gcd(B(E), m) = 1$, then

$$T_m \cong E[m].$$

Now we can describe the action of another subroup of G_m, namely

$$H_m = \mathrm{Gal}(\mathbb{Q}(\tfrac{1}{m}P)/\mathbb{Q}(Q_0)).$$

We can easily see that $H_m \cap T_m = \{\mathrm{id}_{\frac{1}{m}P}\}$, in fact $\mathbb{Q}(\frac{1}{m}P) = \mathbb{Q}(E[m], Q_0)$. Moreover, we have

$$H_m \cong \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$$

because, if $\gamma \in H_m$ and $R \in E[m]$, then

$$\gamma : \frac{1}{m}P \to \frac{1}{m}P, Q = Q_0 + R \mapsto Q_0 + \gamma(R)$$

Hence $\gamma \mapsto \gamma_{\mathbb{Q}(E[m])}$ is an isomorphism.

We can deduce the precise structure of G_m from all the properties we saw. In fact

$$G_m = H_m \ltimes T_m \lesssim Aut(E[m]) \ltimes E[m] \cong GL_2(\mathbb{Z}/m\mathbb{Z}) \ltimes \mathbb{Z}/m\mathbb{Z}^2$$

where the first equality is a consequence of basic Galois Theory. The action of G_m on $\frac{1}{m}P$ is

$$\sigma = (\gamma, \tau) : Q \mapsto Q_0 + \gamma(Q - Q_0) + \tau$$

and from the results of Bashmakov ([Bas70]) and Serre ([Ser72]) we can conclude that $\exists A(E)$ such that if $\gcd(m, A(E)) = 1$, then

$$G_m \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \ltimes \mathbb{Z}/m\mathbb{Z}^2.$$

As a first step towards the application of Chebotarev Density Theorem in this context, let's consider G_ℓ, with ℓ a prime number. Let $p \nmid \ell\Delta'_E$ and set $\sigma_p = (\gamma_p, \tau_p) \in G_\ell$ be a Frobenius element. If $\ell \mid \#\bar{E}(\mathbb{F}_p)$, $\bar{E}(\mathbb{F}_p)$ has an element of order ℓ. Thus, γ_p has 1 as eigenvalue. So, there are two cases:

- if $\gamma_p = \mathrm{id}_{E[\ell]} \Rightarrow E[\ell] \subseteq \bar{E}(\mathbb{F}_p)$. So $\ell \mid [\bar{E}(\mathbb{F}_p) : \langle P \bmod p \rangle]$
- If $\gamma_p \neq \mathrm{id}_{E[\ell]}$ has 1 as eigenvalue, then

$$\ell \mid [\bar{E}(\mathbb{F}_p) : \langle P \bmod p \rangle] \quad \iff \quad \sigma_p \text{ fixes } Q \in \frac{1}{\ell}P$$

But $\sigma = (\gamma, \tau)(Q) = Q$ if and only if $Q = Q_0 + \gamma(Q - Q_0) + \tau$, that is $\tau = (\gamma - \mathrm{id}_{E[\ell]})(Q_0 - Q)$.

Thus, we define

$$S_\ell := \left\{ (\gamma, \tau) \in G_\ell : \begin{array}{l} \gamma \text{ has eigenvalue 1 and either} \\ \gamma = \mathrm{id}_{E[\ell]} \text{ or} \\ \gamma \neq \mathrm{id}_{E[\ell]} \text{ and } \tau \in \mathrm{Im}(\gamma - \mathrm{id}_{E[\ell]}) \end{array} \right\}$$

and we notice that $\ell \mid [\bar{E}(\mathbb{F}_p) : \langle P \bmod p \rangle] \Leftrightarrow \sigma_p \in S_\ell$.

More generally, if m is square free, then the composite

$$\prod_\ell \mathbb{Q}\left(\tfrac{1}{\ell}P\right) = \mathbb{Q}\left(\tfrac{1}{m}P\right).$$

This construction allows one to define

$$S_m := \left\{ \sigma \in G_m : \forall \ell \mid m, \sigma_{|\mathbb{Q}(\frac{1}{\ell}P)} \in S_\ell \right\}.$$

Notice that, as the previous easier case, $m \mid [\bar{E}(\mathbb{F}_p) : \langle P \bmod p \rangle] \Leftrightarrow \sigma_p \in S_m$.

Finally, we have all the ingredients to state the following

Theorem 1.7.4 (Chebotarev Density Theorem)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ of rank at least 1. Let $P \in E(\mathbb{Q})$ a point of infinite order. Then*

$$\#\{p \leqslant x : \ p \nmid m\Delta'_E, m \mid [\bar{E}(\mathbb{F}_p) : \langle P \bmod p \rangle]\} \sim \frac{\#S_m}{\#G_m}\pi(x).$$

So, one needs a final (big) step to arrive to the

Conjecture 1.7.5 (Lang Trotter Primitive Points Conjecture)**.** *With the same notation as before,*

$$\#\{p \leqslant x : \ p \nmid \Delta'_E, \bar{E}(\mathbb{F}_p) = \langle P \bmod p \rangle\} \sim \sum_{m \in \mathbb{N}} \mu(m)\frac{\#S_m}{\#G_m}\pi(x).$$

The first thing to remark is the main difficulty to prove this conjecture, that is the size of S_m. This object, in fact, is too big to extend the proof Hooley gave for *Artin primitive root conjecture* in his paper of 1967 (see [Hoo67]).

The first (and biggest until now) step in solving this problem was made by R. Gupta and M. Ram Murty in 1986 [GM86]. Under GRH, they proved the Lang-Trotter conjecture for CM elliptic curves.

Chapter 2

Never-primitive points on Elliptic Curves

As a first step to understand the nature of primitive points on elliptic curves, we started doing some calculations with *Pari/GP* to calculate some densities in an empiric way. It turned out that there are some curves E for which a given rational point P of infinite order such that $\bar{E}(\mathbb{F}_p) \not\simeq \langle P \mod p \rangle$ for any prime p of good reduction. It's a very interesting phenomenon and we are going to discover it by giving two preliminary examples.

2.1 A curve with a 2-torsion rational point and no primitive points

Let $E : y^2 + xy = x^3 - x$ be the curve with conductor 65, called `65.a1` in Cremona Tables [Cre06]. This curve has rank 1 and torsion $T \cong \mathbb{Z}/2\mathbb{Z}$. More explicitly:

$$E(\mathbb{Q}) = \langle (1,0) \rangle \times \langle (0,0) \rangle \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

By an easy computation, we can find that

$$E[2] = \left\{ \mathcal{O}, (0,0), \left(\frac{-1 + (-1)^j \sqrt{65}}{8}, \frac{1 + (-1)^{j+1} \sqrt{65}}{16} \right) \right\}_{j=1,2}$$

with $\mathcal{O}$ the point at infinity. Then, $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{65})$.

Since we have the rational 2–torsion point $(0,0)$, we know that $\#E(\mathbb{F}_p)$ is divisible by 2 for every prime p, since the reduction of $(0,0)$ modulo p is always different from $\mathcal{O}$. We will see that the order of the reduction of $P = (1,0)$ modulo p is always a divisor of $\#E(\mathbb{F}_p)/2$, then $(1,0)$ can never be primitive.

If we want to solve the equation $2Q = P$ we obtain, in particular, the two solutions

$$Q_1 = \left(\frac{1 + \sqrt{5}}{2}, \frac{-3 + \sqrt{5}}{2} \right) \qquad Q_2 = \left(\frac{3 + \sqrt{13}}{2}, \frac{5 + \sqrt{13}}{2} \right).$$

Using quadratic symbols for primes p of good reduction for E ($p \neq 5, 13$), we can see that:

- if $\left(\frac{65}{p}\right) = 1$, then $E(\mathbb{F}_p)$ is not cyclic;
- in the case $\left(\frac{65}{p}\right) = -1$, i.e. $E(\mathbb{F}_p)$ is cyclic, if $\left(\frac{5}{p}\right) = -1$, we have by multiplicativity of symbols that $\left(\frac{13}{p}\right) = 1$, so the relation $2Q_2 = P$ holds in $E(\mathbb{F}_p)$;
- if $\left(\frac{65}{p}\right) = -1$ and $\left(\frac{13}{p}\right) = -1$, in the same way we deduce that $2Q_1 = P$ holds in $E(\mathbb{F}_p)$.

So we can deduce that P is not primitive for any prime of good reduction for E.

A nice thing we noticed from calculations on *Pari/GP* is that if we take the point $P' = (1,0) + (0,0) = (-1,1)$, that also generates a subroup of index 2 of $E(\mathbb{Q})$, then this point is primitive for "many" primes. So, it's evident that for such p' we cannot repeat an argument similar to what we said about P.

Another curious fact is that the curve `65.a2`, with conductor 65 and then isogenous to `65.a1`, has not a point like P. For this curve both generators of the free part of the Mordell-Weil group generates the reduction of the curve modulo p for "many" primes p. In the next sections we will try to understand why this can happen.

2.2 A curve of rank 1 with no rational torsion points and no primitive points

At a first sight of this phenomenon, one can think that it is necessary to have at least one rational torsion point to find a point on the curve that always fails to be primitive. We will see in this second example that this is not true.

Let $E : y^2 + y = x^3 - 3834x - 91375$ be the curve with conductor equal to 189, called `189.b1` on Cremona Tables [Cre06]. We know that it has no torsion and is of rank 1 and that:

$$E(\mathbb{Q}) = \langle \left(-\frac{143}{4}, -\frac{3}{8}\right) \rangle \cong \mathbb{Z}.$$

Moreover, from the same Cremona Tables, we obtain that the Galois representation on torsion points is surjective for every prime different from 3, for which the image of Galois is the subgroub of type `B.1.2` and this means that:

$$\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}) \cong \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_3) \right\} \cong S_3.$$

We can deduce that $3 \mid \#E(\mathbb{F}_p)$ for every prime p since there exists a curve isogenous to E (that has the same number of points modulo every prime) with a 3–torsion rational point, but we will prove it directly.

We need to prove that for every prime $p \notin \{2, 3, 7\}$, one of the following two conditions holds:

- $E[3] \subset E(\mathbb{F}_p)$ or
- $\left(-\frac{143}{4}, -\frac{3}{8}\right) = 3Q$, for some $Q \in E(\mathbb{F}_p)$.

From this we can say that either $E(\mathbb{F}_p)$ is not cyclic or the order of $\left(-\frac{143}{4}, -\frac{3}{8}\right)$ is a divisor of $\#E(\mathbb{F}_p)/3$.

Computing $E[3]$

The 3–division polynomial can be computed using the formulas at page 39 of the book of Blake, Seroussi and Smart [BSS99]. It is:

$$\psi_3(x) = 3(36+x)(-136107 - 6372x - 36x^2 + x^3).$$

We can easily compute 3-torsion from it:

$$E[3] = \left\{\infty, (-36, -1+3\zeta), (-36, -1+3\zeta^2)\right\} \cup$$
$$\left\{\left(3(4+4\zeta^j\sqrt[3]{63}+\zeta^{2j}\sqrt[3]{63^2}), \frac{1}{2} \pm 9(\frac{63}{2}+8\zeta^j\sqrt[3]{63}+2\zeta^{2j}\sqrt[3]{63^2})\right)\right\}_{j=1,2,3}$$

where $\zeta = e^{i\frac{2\pi}{3}}$. Looking at cubic residues mod p we can easily deduce from the coordinates of the 3-torsion points that $3|\#E(\mathbb{F}_p)$ for every prime p of good reduction.

Computing $\{Q \in E(\bar{\mathbb{Q}}) : 3Q = \left(-\frac{143}{4}, -\frac{3}{8}\right)\}$

Using the formula

$$[3](x,y) = \left(\frac{\vartheta_3(x)}{(\psi_3(x))^2}, \frac{\omega_3(x,y)}{(\psi_3(x,y))^3}\right),$$

we obtain that the coordinates (x,y) of points $Q \in E(\overline{\mathbb{Q}})$ such that $3Q = \left(-\frac{143}{4}, -\frac{3}{8}\right)$ satisfy

$$\frac{\vartheta_3(x)}{(\psi_3(x))^2} = -\frac{143}{4} \quad \text{e} \quad \frac{\omega_3(x,y)}{(\psi_3(x,y))^3} = -\frac{3}{8}$$

but this is:

$$2((x+30)^3 + 3^37)((x+42)^3 - 3^5)(190404 + 15336x + 423x^2 + 4x^3) = 0$$

So, we have the following 9 points $\{Q_1, Q_2, Q_3, Q_4, Q_5, Q_6, Q_7, Q_8, Q_9\}$:

$$Q_j = \begin{cases} \left(3(-14+\zeta^j\sqrt[3]{3^2}), 2(20-27\zeta^{2j}\sqrt[3]{3}+9\zeta^j\sqrt[3]{3^2})\right) & \text{if } j = 1,2,3; \\ \left(-3(10+\zeta^j\sqrt[3]{7}), 31+18\zeta^j\sqrt[3]{7}-18\zeta^{2j}\sqrt[3]{7^2}\right) & \text{if } j = 4,5,6; \\ \left(\frac{-141-9\zeta^j\sqrt[3]{21}+9\zeta^{2j}\sqrt[3]{21^2}}{4}, \frac{-571+81\zeta^j\sqrt[3]{21}+45\zeta^{2j}\sqrt[3]{21^2}}{8}\right) & \text{if } j = 7,8,9. \end{cases}$$

The subfields of $\mathbb{Q}\left(E[3], \frac{1}{3}(-\frac{143}{4}, -\frac{3}{8})\right)$

- $\mathbb{Q}\left(E[3]\right) = \mathbb{Q}\left(\zeta, \sqrt[3]{63}\right)$;
- $\mathbb{Q}\left(Q_j\right) = \begin{cases} \mathbb{Q}\left(\zeta^j\sqrt[3]{3^2}\right) & \text{if } j = 1,2,3; \\ \mathbb{Q}\left(\zeta^j\sqrt[3]{7}\right) & \text{if } j = 4,5,6; \\ \mathbb{Q}\left(\zeta^j\sqrt[3]{21}\right) & \text{if } j = 7,8,9; \end{cases}$
- $\mathbb{Q}\left(E[3], \frac{1}{3}(-\frac{143}{4}, -\frac{3}{8})\right) = \mathbb{Q}\left(\zeta, \sqrt[3]{3}, \sqrt[3]{7}\right)$

Then $\mathbb{Q}\left(E[3], \frac{1}{3}(-\frac{143}{4}, -\frac{3}{8})\right)$ has dimension 18 on $\mathbb{Q}$ and its Galois group is $C_2 \rtimes C_3^2$. Thus the lattice of subfields is easy to draw. The only quadratic subfield is $\mathbb{Q}(\zeta)$, because the only subroup of $C_2 \rtimes C_3^2$ of index 2 is C_3^2. The cubic subfields are listed above, and so on.

Proof that $\left(-\frac{143}{4}, -\frac{3}{8}\right)$ is never primitive

The case $p \equiv 2 \bmod 3$ is simple. In this case we have $\sqrt[3]{63}, \sqrt[3]{3^2}, \sqrt[3]{7}, \sqrt[3]{21} \in \mathbb{F}_p$,

$$E[3] \cap E(\mathbb{F}_p) = \left\{ (3(4 + 4\sqrt[3]{63} + \sqrt[3]{63^2}), \frac{1}{2} \pm 9(\frac{1}{2} \cdot 63 + 8\sqrt[3]{63} + 2\sqrt[3]{63^2})), \infty \right\}$$

and $\{Q_3, Q_6, Q_9\} \subset E(\mathbb{F}_p)$.

This implies that $\left(-\frac{143}{4}, -\frac{3}{8}\right)$ has order a divisor of $\#E(\mathbb{F}_p)/3$; so it cannot be primitive. Hence, we can assume that $p \equiv 1 \bmod 3$, in which case we can think at $\zeta \in \mathbb{F}_p$, $\mu_3 = \{1, \zeta, \zeta^2\} \subset \mathbb{F}_p$ and use cubic symbols. Then

$$E[3] \cap E(\mathbb{F}_p) \supseteq \left\{ \infty, (-36, -1 + 3\zeta), (-36, -1 + 3\zeta^2) \right\}.$$

Furthermore $E[3] \supseteq E(\mathbb{F}_p)$ if and only if $\sqrt[3]{63} \in \mathbb{F}_p$ and this is equivalent to

$$\left[\frac{63}{p}\right]_3 := 63^{\frac{p-1}{3}} \equiv 1 (\mathrm{mod} p).$$

Now, let us assume that $\left[\frac{63}{p}\right]_3 = \zeta$ (the case $\left[\frac{63}{p}\right]_3 = \zeta^2$ is completely analogous). If $\left[\frac{7}{p}\right]_3 = 1$, then $\{Q_4, Q_5, Q_6\} \subset E(\mathbb{F}_p)$;
If $\left[\frac{7}{p}\right]_3 = \zeta$, then $\left[\frac{9}{p}\right]_3 = \left[\frac{63}{p}\right]_3 \left[\frac{7^2}{p}\right]_3 = 1$ e $\{Q_1, Q_2, Q_3\} \subset E(\mathbb{F}_p)$.
If $\left[\frac{7}{p}\right]_3 = \zeta^2$, then $\left[\frac{21^2}{p}\right]_3 = \left[\frac{63}{p}\right]_3 \left[\frac{7}{p}\right]_3 = 1$ e $\{Q_7, Q_8, Q_9\} \subset E(\mathbb{F}_p)$.

We conclude that in every case the order of $\left(-\frac{143}{4}, -\frac{3}{8}\right)$ is a divisor of $\#E(\mathbb{F}_p)/3$. hence it cannot be primitive.

2.3 Definition of Never-primitive Point

In the first two sections of this chapter we saw that in some cases, for an elliptic curve E defined over $\mathbb{Q}$ of rank 1 and $P \in E(\mathbb{Q}) \setminus \mathrm{Tors}(E(\mathbb{Q}))$

$$\bar{E}(\mathbb{F}_q) \neq \langle P \mod q \rangle$$

for all the primes q.

In order to describe these points we give a definition that is slightly more general.

Definition 2.3.1 (Never–primitive Point)**.** Let E be an elliptic curve defined over a number field K and $P \in E(K)$ be a point of infinite order. Let $k_{\mathfrak{q}}$ denote the residue field of a prime ideal $\mathfrak{q}$ of the ring of integers of K. We say that P is *Never–primitive* over K if

$$\bar{E}(k_{\mathfrak{q}}) \neq \langle P \mod \mathfrak{q} \rangle,$$

for all but finitely many primes $\mathfrak{q}$.

For future computations we also need the notion of *good* prime.

Definition 2.3.2. Let E be an elliptic curve defined over a number field K and P be a point in $E(K)$. A prime $\mathfrak{q}$ of K is called *good* (for E and P) if $\mathfrak{q}$ does not divide (p), if E has good reduction modulo $\mathfrak{q}$ and if P is not trivial in $E(k_{\mathfrak{q}})$.

It is easy to see that for $P \in E(K)$ almost all primes of K are good.

2.4 Conditions for existence of Never-primitive points

From some calculations we did with Pari/GP, it seems that for any elliptic curve E over $\mathbb{Q}$ with $E(\mathbb{Q}) \cong \mathbb{Z} = \langle P \rangle$, if P is never primitive modulo any prime q, then the image of Galois representation of a certain prime p inside $\mathrm{GL}_2(\mathbb{F}_p)$ is of the type $p\,B.1.r$, that is the subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$ that can be written in the form

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},$$

with $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$. This is a Borel subgroup of $GL_2(\mathbb{F}_p)$ and has order $p(p-1)$.

We notice that a sufficient condition for the never-primitivity of P is the following:

$$\exists p \text{ prime s.t. } p \mid \left[\bar{E}(\mathbb{F}_q) : \langle P \mod q \rangle\right] \text{ for every prime } q \text{ of good reduction.} \tag{2.1}$$

2.4.1 Elliptic Curves with trivial torsion

Now we see what condition (2.1) implies on an elliptic curve over $\mathbb{Q}$ with trivial torsion group. As we will use just the fact that $E(\mathbb{Q})$ is free and finitely generated, we can prove our result for curves defined over a number field K. From this, the result for $\mathbb{Q}$ automatically follows.

Let E be an elliptic curve over a number field K and $P \in E(K)$ be a point of infinite order. Suppose that $E(K)$ is torsion-free and that P is not divisible by p in $E(K)$. If

$$V = \{Q \in E(\bar{K}) : [p]Q \in \langle P \rangle\}/\langle P \rangle$$

then V is a 3-dimensional representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let G be the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{GL}_3(\mathbb{F}_p)$. There is an exact sequence of G-modules

$$0 \to E[p] \to V \to \mathbb{Z}/p\mathbb{Z} \to 0. \tag{2.2}$$

Looking at this exact sequence we can deduce some interesting properties of the curves we are studying. Moreover, we moved our problem from an elliptic curve theoretical shape to a more group theoretic setting.

First, we need two preliminary lemmas.

Lemma 2.4.1. *Let V be a vector space of dimension 2 over a field k and let H be a subgroup of $\mathrm{Aut}(V)$. Assume that $\det(\mathrm{Id} - h) = 0$, for all $h \in H$. Then there exists a basis of V such that H, written in this base, is contained either in the subgroup $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ or in the subgroup $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$.*

Proof. This is Exercise 1) at page I-2 of the book of Serre [Ser89]. For completeness, we give here a proof of this result.

By hypothesis, for all $h \in H$ and basis (v, w) of V we have

$$\det(h(v) - v, h(w) - w) = 0.$$

Let $g \in H$ with $g \neq \mathrm{Id}$. Suppose first that 1 is the only eigenvalue of g. Then in some basis (v, w) the matrix of g is $\mathrm{Mat}(g) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Let $h \in H$, then for such a basis (v, w) we have:

(1) $\det(h(v) - v, h(w) - w) = 0$,

(2) $\det(hg(v)-v, hg(w)-w) = \det(h(v)-v, h(v)+h(w)-w) = 0.$

If $h(v)-v=0$, then $h(v)$ is collinear to v. If $h(w)-w$, then (2) shows that $h(v)$ is collinear to v. If $h(v)\neq v$ and $h(w)\neq w$, then $h(v)+h(w)-w$ is collinear to $h(v)-v$ (by (2)). The latter is collinear to $h(w)-w$ (by (1)). This implies that $h(v)$ is collinear to v. Hence kv is fixed by H and we are done in this case.

As a second case, suppose that g has two distinct eigenvalues 1 and a. Then in some basis (v,w) we have $\mathrm{Mat}(g) = \left(\begin{smallmatrix}1 & 0\\ 0 & a\end{smallmatrix}\right)$.

CLAIM: if $h\in H$ then either (i) $h(v)=v$ or (ii) $h(w)$ is collinear to w.
Indeed, we have

$$\det(h(v)-v, h(w)-w) = 0,$$

$$\det(hg(v)-v, hg(w)-w) = \det(h(v)-v, ah(w)-w) = 0.$$

If $h(v)\neq v$, then $h(w)-w$ and $ah(w)-w$ are collinear to each other (because they are both collinear to $h(v)-v$). Since $a\neq 1$, this implies that $h(w)$ is collinear to w. This proves the claim.

To conclude we have to show that either every $h\in H$ satisfies (i) or every $h\in H$ satisfies (ii). If not, then let $h_1\in H$ not satisfying (i) and $h_2\in H$ not satisfying (ii). The matrices of h_1 and h_2 have the forms $\mathrm{Mat}(h_1) = \left(\begin{smallmatrix}1 & 0\\ \alpha & *\end{smallmatrix}\right)$ and $\mathrm{Mat}(h_2) = \left(\begin{smallmatrix}1 & \beta\\ 0 & *\end{smallmatrix}\right)$ with $\alpha\neq 0$ and $\beta\neq 0$. It is easy to check that $\det(h_1h_2 - \mathrm{Id}) = -\alpha\beta \neq 0$ which is a contradiction. □

Lemma 2.4.2. *Let E be an elliptic curve over a number field K. Suppose $E(K)$ is torsion-free and $P\in E(K)$ is a point of infinite order. Let*

$$V = \{Q\in E(\bar{K}) : [p]Q \in \langle P\rangle\}/\langle P\rangle.$$

We have that $p \mid [\bar{E}(k_{\mathfrak{q}}) : \langle P \mod \mathfrak{q}\rangle]$ if and only if $\mathrm{Frob}_{\mathfrak{q}}$ fixes a subspace $W_{\mathfrak{q}}$ of V of dimension at least 2.

Proof. If the p-torsion $E[p]$ is $k_{\mathfrak{q}}$-rational, then clearly p divides $[E(k_q) : \langle P \mod \mathfrak{q}\rangle]$ and $W_{\mathfrak{q}}$ has at least dimension 2.

So, let us suppose that the p-torsion of $\bar{E}(k_{\mathfrak{q}})$ is trivial. Then $p\nmid \#\bar{E}(k_{\mathfrak{q}})$ and a fortiori $p\nmid [\bar{E}(k_{\mathfrak{q}}) : \langle P \mod \mathfrak{q}\rangle]$, so $W_{\mathfrak{q}}$ cannot have dimension 2, because by Grassmann formula

$$\dim(E[p]\cap W_{\mathfrak{q}}) \geqslant 1$$

and this implies that $E[p]$ contains a $\mathbb{F}_{\mathfrak{q}}$-rational point. But this is a contradiction, as we supposed that the p-part of $\bar{E}(k_{\mathfrak{q}})$ is trivial.

The last case left is when the p-torsion in $\bar{E}(k_{\mathfrak{q}})$ is cyclic, generated by a point $R\in\bar{E}(k_{\mathfrak{q}})$. In this case the p-part of $\bar{E}(k_{\mathfrak{q}})$ is cyclic (if not, there should be a point of order p that is independent to R, but this is a contradiction). With this assumption, if $p \mid [\bar{E}(k_{\mathfrak{q}}) : \langle P \mod \mathfrak{q}\rangle]$ then $\exists Q\in\bar{E}(k_{\mathfrak{q}})$ such that $[p]Q = P \mod \mathfrak{q}$. Hence, we have that $\langle Q, R\rangle$ has dimension 2 and is fixed by $\mathrm{Frob}_{\mathfrak{q}}$. Conversely, if $\dim(W_{\mathfrak{q}}) = 2$, then $W_{\mathfrak{q}}\neq E[p]$ (otherwise $E[p]$ should be $k_{\mathfrak{q}}$-rational). Let us take $Q\in W_{\mathfrak{q}}\backslash E[p]$. Then $[p]Q$ is non-zero in V and generates the group $\langle P\rangle/\langle [p]P\rangle$. Namely, $P = [ip]Q + [kp]P = [p]A$ with $A\in\bar{E}(k_{\mathfrak{q}})$. □

With these lemmas, we can prove the following result:

Proposition 2.4.3. *Let E be an elliptic curve defined over a number field K with $E(K)$ torsion-free. Let $P \in E(K)$ be a point of infinite order. If there is a prime p such that P is not divisible by p in $E(K)$ and p divides $\left[\bar{E}(k_{\mathfrak{q}}) : \langle \bar{P} \rangle\right]$ for almost every good prime $\mathfrak{q}$, then the image of Galois of $\mathrm{Gal}(\bar{K}/K)$ into $\mathrm{Aut}(E[p])$ is of the form*

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

with $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$. In symbols, this is the group $pB.1.r$, where r is a generator of $\mathbb{F}_p^*$.

Proof. Since the curve E has trivial torsion group, we know that G has no fixed points. In other words, the space of G-invariants V^G is zero. On the other hand, by hypothesis we know that $p \mid \left[\bar{E}(k_{\mathfrak{q}}) : \langle \bar{P} \rangle\right]$ for every prime q of good reduction, then Chebotarev Density Theorem implies that every $g \in G$ has a fixed point in V.

Let us now consider the exact sequence (2.2). As $E[p]$ has no non-zero rational points, we know from Lemma 2.4.2 that $p \mid \left[\bar{E}(k_{\mathfrak{q}}) : \langle \bar{P} \rangle\right]$ if and only if $\mathrm{Frob}_{\mathfrak{q}}$ fixes a subspace $W_{\mathfrak{q}}$ of V of dimension at least 2.

By Chebotarev Density Theorem, considering G the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(V)$, we have that every $g \in G$ fixes a subspace W_g of V of dimension at least 2.

Since $W_g \cap E[p]$ has at least dimension 1, every $g \in G$ has a fixed point in $E[p]$. By Lemma 2.4.1 we have that $G \subset \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ or $G \subset \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. But $E[p]$ has no G-invariants, so we have that $G \subset \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. □

2.4.2 Elliptic Curves with non-trivial torsion

Let E be an elliptic curve over a number field K and let P be a point of infinite order in the Mordell-Weil group $E(K)$.

Let p be a prime for which the p-torsion subgroup of $E(K)$ has order p. This means that the image G of the Galois group $G_K = \mathrm{Gal}(\bar{K}/K)$ acting on the group of p-torsion points $E[p]$ is conjugate to a subgroup of matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ of the form

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

Proposition 2.4.4. *Suppose that the point P is not divisible by p in $E(K)$. If for almost every prime ideal $\mathfrak{q}$ of K, the index of the subgroup generated by P inside the group $\bar{E}(k_{\mathfrak{q}})$ is divisible by p, then either K contains the p-th roots of unity or $\#G$ is not divisible by p. In other words, G is conjugate to a subgroup of matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ of the form*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}.$$

Using the Chebotarev Density Theorem we translate the proposition into a group theoretic statement. Let V be the $\mathbb{F}_p$-vector space

$$V = \{Q \in E(\bar{K}) : [p]Q \in \langle P \rangle\}/\langle P \rangle.$$

Then V has dimension 3 and admits continuous action by $\mathrm{Gal}(\bar{K}/K)$. It sits in the following exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \longrightarrow E[p] \longrightarrow V \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

If P is not divisible by p in $E(K)$, the extension is not split.

In fact, let us suppose that the exact sequence of Galois modules splits. Then $\exists Q \in E(\overline{K})$ with these properties:

1. $pQ = kP$ for some $k = 1 \mod p$
2. $\sigma(Q) = Q + mP$ for some $m \in \mathbb{Z}$

If we find a point $R \in E(K)$ with $pR = P$ we get a contradiction.

We want to take the G_K-invariants of the exact sequence $0 \longrightarrow \langle P \rangle \longrightarrow E(\overline{K}) \longrightarrow E(\overline{K})/\langle P \rangle \longrightarrow 0$ but since the action of G_K on $\langle P \rangle$ is trivial, we have $H^1(G_K, \langle P \rangle) = \mathrm{Hom}(G_K, \langle P \rangle)$ (see for example [Sil08, Appendix B, Remark 1.1]). Moreover $\mathrm{Hom}(G_K, \langle P \rangle) \cong \mathrm{Hom}(G_K, \mathbb{Z}) = 0$ because G_K is a profinite group and $\mathbb{Z}$ has no finite subgroups except $\{0\}$. So the sequence is still exact. More precisely we have $0 \longrightarrow \langle P \rangle \longrightarrow E(K) \longrightarrow \left(E(\overline{K})/\langle P \rangle\right)^{G_K} \longrightarrow 0$

The property 2) says that the point Q is G_K-invariant in $E(\overline{K})/\langle P \rangle$. Then, it exists a point Q' in $E(K)$ with $Q = Q + mP$ for some $m' \in \mathbb{Z}$. This means that $Q = Q' - m'P$ was already in $E[p]$. If we write $k = 1 + pk'$ (see property 1)), then $R = Q - k'P$ belongs to $E(K)$ and $pR = P$.

Let $\bar{G}$ denote the image of $\mathrm{Gal}(\bar{K}/K)$ in $\mathrm{Aut}(V)$. We choose an $\mathbb{F}_p$-basis $\{e_1, e_2, e_3\}$ as follows. For e_1 we take a non-zero rational point in $E[p]$. For e_2 we take any point in $E[p]$ that is independent of e_1. For e_3 we take any point in V that is not in $E[p]$. With respect to this basis, $\overline{G}$ is contained in the subgroup of matrices of the form

$$\begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & 0 & 1 \end{pmatrix}.$$

Lemma 2.4.5. *Le $\mathfrak{q}$ be a good prime. Then the index of the subgroup generated by P inside the group $E(k_\mathfrak{q})$ is divisible by p if and only if the Frobenius automorphism $\sigma_\mathfrak{q} \in \overline{G}$ fixes a subspace of V of dimension at least 2.*

Proof. Note that the dimension of the fixed point space of an element $\sigma \in G$ only depends on its conjugacy class, beacause taking a conjugate of σ is equivalent to consider a change of basis in the linear application induced by σ on V. If $\sigma_\mathfrak{q}$ fixes $E[p]$, the p-torsion of $E(k_\mathfrak{q})$ is not cyclic and the equivalence is clear.

If not, then the p-torsion of $E(k_\mathfrak{q})$ is cyclic and the index $[E(k_\mathfrak{q}) : \langle P \rangle]$ is divisible by p if and only if the reduction of P is divisible by p in $E(k_\mathfrak{q})$. The latter happens if and only if there is a point $Q \in V$ for which $[p]Q = P$ and that is fixed by $\sigma_\mathfrak{q}$. This means precisely that the fixed point space of $\sigma_\mathfrak{q}$ has dimension $\geqslant 2$. This proves the Lemma. □

By the Chebotarev Density Theorem every $\sigma \in \overline{G}$ is the Frobenius of some good prime $\mathfrak{q}$. Moreover the determinant of the Galois action on $E[p]$ is through the cyclotomic character. Therefore Proposition 2.4.4 follows from the following group theoretical proposition.

Proposition 2.4.6. *Let V be a 3-dimensional vector space over $\mathbb{F}_p$ with basis $\{e_1, e_2, e_3\}$. Let $\overline{G}$ be a finite group that acts faithfully on V. We write $E[p]$ for the span of e_1 and e_2. Suppose that $\overline{G}$ fixes e_1, preserves $E[p]$ and acts trivially on $V/E[p]$. If the extension*

$$0 \longrightarrow E[p] \longrightarrow V \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

is not split and if every $\sigma \in \overline{G}$ has a fixed point space of dimension $\geqslant 2$, then the image G of $\overline{G}$ in $\operatorname{Aut} E[p]$ either has order p or is not divisible by p.

Proof. The p-Sylow subgroup N of $\overline{G}$ is normal. Its elements have the form

$$\sigma = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}.$$

Since all $\sigma \in N$ have a fixed point space of dimension $\geqslant 2$, either x or z must vanish. This means that the p-Sylow subgroup is contained in the union of two subgroups. If it is contained in the subgroup of matrices for which $x = 0$, the group G contains no elements of order p and we are done. So N is contained in the subgroup for which $z = 0$.

If $\#G$ is not equal to p, then there is a matrix $\tau \in \overline{G}$ of the form

$$\tau = \begin{pmatrix} 1 & u & v \\ 0 & \zeta & w \\ 0 & 0 & 1 \end{pmatrix},$$

for some $\zeta \neq 1$ of maximal order. The fixed point space of τ has dimension $\geqslant 2$, by hypothesis. Therefore it must be $\{ae_1 + be_2 + ce_3 : (\zeta - 1)b + wc = 0\}$. In other words, it is the span of e_1 and $(\zeta - 1)e_3 - we_2$. Since the p-Sylow subgroup N acts trivially on $V/\langle e_1 \rangle$, the second row of the matrix $\tau\sigma$ is the same for all $\sigma \in N$. It follows that all elements in the coset τN have the same fixed point space.

Since the order of ζ is maximal, $\overline{G}$ is generated by N and τ. It follows that the group $\overline{G}$ fixes $(\zeta - 1)e_3 - we_2$. Therefore V is isomorphic to the product of $E[p]$ and the span of $(\zeta - 1)e_3 - we_2$. Since this contradicts the fact the extension is not split, the proposition is proved. □

2.5 The reducibility of the polynomial $[p]Q = P$

In this final section we will give a criterion to understand when, given an elliptic curve E defined over $\mathbb{Q}$ and a rational point P of infinite order that is not divisible by a prime p, it happens that $p \mid \left[\bar{E}(\mathbb{F}_q) : \langle P \mod q \rangle\right]$ for almost every prime q of good reduction, so in particular that the point $P \in E(\mathbb{Q})$ is never-primitive.

Just the divisibility of $\#\bar{E}(\mathbb{F}_q)$ by p itself implies that the image of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\operatorname{Aut}(E[p])$ is contained either in $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ or in $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. This is Lemma 2.4.1. So if we have no rational torsion points different from the point at infinity $\mathcal{O}$, we are in the case $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$.

Let Q be a point in $E(\bar{\mathbb{Q}})$ with $[p]Q = P$. Then

$$U_Q = \langle (\sigma - \mathrm{Id})Q : \sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rangle$$

is a subgroup of $E[p]$. Moreover, it is an $\mathbb{F}_p[H_p]$-submodule where H_p is the Galois group $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$.

We know that $G \subset \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$, with the entries denoted by the stars that are non-trivial (the first row is different from $(1 \;\; 0)$), because the first one is given by the cyclotomic character and the second one cannot be only zero, because otherwise there should be a rational point in $E[p]$, that is a contradiction since $E(\mathbb{Q}) \cong \mathbb{Z}$.

Then, $E[p]$ has a unique proper submodule by the action of G. This is the eigenspace L generated by e_1. So we have that

$$\{\mathcal{O}\} \subset L \subset E[p].$$

Now U_Q must be one of these three submodules. The first possibility is that $U_Q = \{\mathcal{O}\}$, but this means that either Q is rational or that P is divisible by p. So, this option is excluded by hypothesis.

Finally, we have

$$U_Q = L \qquad \text{or} \qquad U_Q = E[p].$$

Proposition 2.5.1. *With the notation as above, we have $U_Q = L$ if and only if*

$$p \mid \left[\bar{E}(\mathbb{F}_q) : \langle P \mod q \rangle\right]$$

for almost prime q of good reduction.

Proof. Using Chebotarev Density Theorem, we have to prove that only in the first case every $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ fixes either $E[p]$ or some point $Q + R$ with $R \in E[p]$. Indeed, saying that $\sigma = \mathrm{Frob}_q$ is the same as saying that $p \mid [\bar{E}(\mathbb{F}_q) : \langle P \rangle]$.

Then we have to analyze the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the F_p-vector space $V = \langle Q, E[p] \rangle / \langle P \rangle$.

This is the way: take an elliptic curve over $\mathbb{Q}$ with $G \subset \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ and a rational point P of infinite order and not divisible by a prime p. Then we write the equation that says $[p](X, Y) = P$. If $U_Q = E[p]$ the polynomial (in X) should be irreducible, while if $U_Q = L$ should decompose. $\square$

Chapter 3

Cyclicity of Quotients of Reductions

3.1 Presentation and context of the problem

Let E be an elliptic curve defined over $\mathbb{Q}$ of rank at least $r > 0$ and $\Gamma \subset E(\mathbb{Q})$ a free subgroup of rank exactly r. Consider the function

$$\pi_{E,\Gamma}(x) = \#\{p \leqslant x : p \nmid N_E,\ \bar{E}(\mathbb{F}_p)/\Gamma_p \text{ is cyclic}\}.$$

Here N_E is the conductor of E, $\bar{E}(\mathbb{F}_p)$ is the reduction of E modulo the prime p and $\Gamma_p \subset \bar{E}(\mathbb{F}_p)$ denotes the reduction of the subgroup Γ modulo p. The aim of this chapter is to find an asymptotic formula for $\pi_{E,\Gamma}$ when E is a non-CM elliptic curve.

A question related to the one considered here is finding the density of primes p such that $\bar{E}(\mathbb{F}_p)$ is cyclic. The first person who studied this problem was Serre and that was the motivation for several papers of Cojocaru and Ram Murty (see for example [Coj03] and [CM04]).

Several problems of this kind arise from an attempt to generalize to Elliptic Curves the classical Artin's primitive root conjecture, proved by Hooley in 1965 [Hoo67] under the assumption of the Generalized Riemann Hypothesis (GRH).

The analogue of the Artin conjecture for elliptic curves was first formulated by Lang and Trotter in 1977 in [LT77]. For this reason this is called the Lang–Trotter Conjecture for Primitive Points on Elliptic Curves.

The main (and almost only) step towards the proof of this conjecture was made by Gupta and Ram Murty [GM86] in 1986. They were obliged to assume GRH and they considered mainly CM curves. For non-CM curves, they got a result that is effective only considering curves of large rank.

A very useful survey to understand the history and evolution of Artin's primitive root conjecture, and its elliptic counterpart, is [Mor12].

The problem we consider in this chapter is weaker than the one formulated by Lang and Trotter, but it can be solved with much less difficulties than the ones found by Gupta and Ram Murty in [GM86].

In the next sections we will prove, assuming GRH, an asymptotic formula for $\pi_{E,\Gamma}(x)$ when E is an elliptic curve without Complex Multiplication and, in some cases, we will see that there are infinitely many primes such that $\bar{E}(\mathbb{F}_p)/\Gamma_p$ is a cyclic group.

The main result of this chapter is the following:

Theorem 3.1.1. *Let E be an elliptic curve over $\mathbb{Q}$ without Complex Multiplication, of rank at least $r > 0$. Let N_E be the conductor of E. Let $\Gamma = \langle P_1, \dots, P_r \rangle$ be a subgroup of $E(\mathbb{Q})$ of rank exactly r. Assuming the Generalized Riemann Hypothesis for the Dedekind zeta functions attached to the extensions $\mathbb{Q}(E[m], m^{-1}\Gamma)/\mathbb{Q}$, we have*

$$\pi_{E,\Gamma}(x) = c_{E,\Gamma} \operatorname{li} x + O_{E,\Gamma}\left(\frac{x}{\log^{2r+4} x}\right)$$

where $c_{E,\Gamma} \geqslant 0$ is a constant depending on E and Γ, and is given by the formula

$$c_{E,\Gamma} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(E[m], m^{-1}\Gamma) : \mathbb{Q}]}.$$

This chapter is also a paper (cf. [Mel15]) we submitted at the beginning of 2015. We refer the reader to [Sil08] for the basic theory of Elliptic Curves.

3.2 Some notations and definitions

Let E be an elliptic curve over $\mathbb{Q}$ and N_E be its conductor.

For a positive integer m, if $E[m] \subseteq E(\bar{\mathbb{Q}})$ is the group of m-division points of the curve, we denote by $\mathbb{Q}(E[m])$ the field obtained by adjoining to $\mathbb{Q}$ all the x and y coordinates of the points in $E[m]$.

If $\operatorname{rk}_{\mathbb{Q}} E \geqslant r > 0$ with r a positive integer, we can find r linearly independent points $P_1, \dots, P_r \in E(\mathbb{Q})$. Let $\Gamma := \langle P_1, \dots, P_r \rangle$ be a free abelian group of rank r. We define $\mathbb{Q}(E[m], m^{-1}\Gamma)$ as the field obtained by adjoining to $\mathbb{Q}(E[m])$ the x and y coordinates of all the points $Q \in E(\bar{\mathbb{Q}})$ such that $[m]Q = P_i$ for some $i = 1, \dots, r$. If i is fixed, it is easy to see that there are m^2 points in the set $\{Q \in E(\bar{\mathbb{Q}}) : \ [m]Q = P_i\}$. Moreover, $\mathbb{Q}(E[m], m^{-1}\Gamma)/\mathbb{Q}$ does not depend on the choice of the generators of Γ.

If p is a rational prime, we denote by $\bar{E}$ and Γ_p respectively the reductions of E and Γ modulo p.

Finally, we have $\pi_{sc}(x, \mathbb{Q}(E[m], m^{-1}\Gamma)/\mathbb{Q}) :=$

$$= \#\left\{p \leqslant x : \ p \nmid N_E, \ p \text{ splits completely in } \mathbb{Q}(E[m], m^{-1}\Gamma)/\mathbb{Q}\right\}$$

3.3 Preliminary lemmas

First, we give a condition for ramification of primes in field extensions involved in the proof of the main theorem. This first lemma is Proposition 1.5 (b) in Chapter VIII Section 1 of [Sil08].

Lemma 3.3.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ of rank at least $r > 0$, N_E its conductor, and let m be a positive integer. If $\Gamma = \langle P_1, \dots, P_r \rangle$ is a free subgroup of rank r of $E(\mathbb{Q})$, then the extensions $\mathbb{Q}(E[m])/\mathbb{Q}$ and $\mathbb{Q}(E[m], m^{-1}\Gamma)/\mathbb{Q}$ are ramified only at the primes that divide mN_E.*

In order to use the Chebotarev Density Theorem in the proof of our main theorem, we need the following two lemmas. The first one is a slight modification of what is stated in §2 of [GM86].

Lemma 3.3.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ of rank at least $r > 0$, N_E its conductor. Let $\Gamma = \langle P_1, \dots, P_r \rangle$ be a free subgroup of rank r of $E(\mathbb{Q})$. If p, q are two different rational primes with $p \nmid N_E$, then the q-primary part of $\bar{E}(\mathbb{F}_p)/\Gamma_p$ is non-cyclic if and only if p splits completely in $\mathbb{Q}(E[q], q^{-1}\Gamma)$.*

Proof. First of all, we are sure that $p \nmid qN_E$, because $p \nmid N_E$ and $p \neq q$. Then, Lemma 3.3.1 implies that p is unramified in $\mathbb{Q}(E[q], q^{-1}\Gamma)$. Let us denote with ϕ_p the Frobenius endomorphism of $\bar{E}$, that is the elliptic curve endomorphism

$$\phi_p : \bar{E}(\bar{\mathbb{F}}_p) \to \bar{E}(\bar{\mathbb{F}}_p)$$

obtained by raising to the p-th power the coordinates of the points in $\bar{E}(\bar{\mathbb{F}}_p)$. Observe that $\ker(\phi_p - \mathrm{Id}) = \bar{E}(\mathbb{F}_p)$. Now, the q-primary part of $\bar{E}(\mathbb{F}_p)/\Gamma_p$ is non-cyclic if and only if $\bar{E}(\bar{\mathbb{F}}_p)[q]$ is contained in $\bar{E}(\mathbb{F}_p)$ and there exists a point $Q_i \in \bar{E}(\mathbb{F}_p)$, with $i \in \{1, \dots, r\}$ such that $qQ_i = \bar{P}_i$. On the other hand, the q-primary part of $\bar{E}(\mathbb{F}_p)/\Gamma_p$ is non-cyclic if and only if $\bar{E}(\bar{\mathbb{F}}_p)[q] \subset \ker(\phi_p - \mathrm{Id})$ and p has a first degree factor in $\mathbb{Q}(q^{-1}\Gamma)$. But this happens if and only if p splits completely in $\mathbb{Q}(E[q], q^{-1}\Gamma)$. □

At this point it is easy to deduce the following:

Lemma 3.3.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ of rank at least $r > 0$, N_E its conductor. Let $\Gamma = \langle P_1, \dots, P_r \rangle$ be a free subgroup of rank r of $E(\mathbb{Q})$. Let p a prime of good reduction for E (i.e., $p \nmid N_E$). Then $\bar{E}(\mathbb{F}_p)/\Gamma_p$ is cyclic if and only if p does not split completely in $\mathbb{Q}(E[q], q^{-1}\Gamma)$ for any prime number $q \neq p$.*

Proof. We know that the p-primary part of $\bar{E}(\mathbb{F}_p)$ is always cyclic (see for example Theorem 3.2 of [Was08]). If q is a rational prime different from p, we know from lemma 3.3.2 that the q-primary part of $\bar{E}(\mathbb{F}_p)/\Gamma_p$ is cyclic if and only if p does not split completely in $\mathbb{Q}(E[q], q^{-1}\Gamma)$. The statement naturally follows from these remarks. □

3.4 Proof of Theorem 3.1.1

Here we assume the Generalized Riemann Hypothesis to deduce an asymptotic formula for $\pi_{E,\Gamma}(x)$ in the case when E has no CM (we will assume this last condition for the rest of the chapter).

As above, we let $\Gamma \subset E(\mathbb{Q})$ be a free subgroup of rank r and we set

$$\pi_{E,\Gamma}(x) = \#\{p \leqslant x : p \nmid N_E,\ \bar{E}(\mathbb{F}_p)/\Gamma_p \text{ is cyclic}\}.$$

From Lemma 3.3.3 and inclusion-exclusion principle, we obtain

$$\pi_{E,\Gamma}(x) = \sum_{m=1}^{\infty} \mu(m) \pi_{sc}(x, \mathbb{Q}(E[m], m^{-1}\Gamma)/\mathbb{Q}),$$

where $\pi_{sc}(x, \mathbb{Q}(E[m], m^{-1}\Gamma)/\mathbb{Q})$ is the counting function defined in §3.2.

The key ingredient of this discussion is the Chebotarev Density Theorem (CDT) subject to GRH as in Serre's [Ser81], Théorème 4.

$$\pi_{sc}(x, \mathbb{Q}(E[m], m^{-1}\Gamma)/\mathbb{Q}) - \frac{\operatorname{li} x}{[\mathbb{Q}(E[m], m^{-1}\Gamma) : \mathbb{Q}]} \ll_{E,\Gamma} \sqrt{x}\log(xm).$$

Following the idea of the proof of Theorem 1.1 of [Coj03], we split the sum in the following way

$$\pi_{E,\Gamma}(x) = \sum_{m\in\mathbb{N}} \mu(m)\pi_{sc}(x, \mathbb{Q}(E[m], m^{-1}\Gamma)) = N(x,y) + O(M(x,y,z) + M(x,z,2\sqrt{x})),$$

where

$$N(x,y) := \#\left\{p \leqslant x : p \nmid N_E,\ p \text{ does not split completely in any } \mathbb{Q}(E[q], q^{-1}\Gamma), q \leqslant y\right\}$$

and

$$M(x,y,z) := \#\left\{p \leqslant x : p \nmid N_E,\ p \text{ splits completely in some } \mathbb{Q}(E[q], q^{-1}\Gamma), y \leqslant q \leqslant z\right\}.$$

First we can estimate $M(x,z,2\sqrt{x})$ using Lemma 14 in [GM86]. It says that the number of primes p satisfying $|\Gamma_p| < y$ is $O(y^{1+2/r})$. In our case, if p splits completely in some $\mathbb{Q}(E[q], q^{-1}\Gamma)$, then $\bar{E}(\mathbb{F}_p)/\Gamma_p$ contains a subgroup of type (q,q), so $|\Gamma_p| \leqslant \frac{x}{q^2} \leqslant \frac{x}{z^2}$. Hence

$$M(x,z,2\sqrt{x}) \leqslant \#\left\{p \leqslant x : p \nmid N_E,\ \#\Gamma_p \leqslant \frac{x}{z^2}\right\} \ll \left(\frac{x}{z^2}\right)^{1+2/r}.$$

The above is $o(x/\log x)$ for $z \geqslant x^{1/(r+2)}\log x$, say.

As for $M(x,y,z)$, we can apply the CDT above. In fact

$$\begin{aligned} M(x,y,z) &\leqslant \sum_{y<q\leqslant z} \#\left\{p \leqslant x : p \nmid N_E,\ p \text{ splits completely in } \mathbb{Q}(E[q], q^{-1}\Gamma)\right\} \\ &\ll \frac{x}{\log x}\sum_{y<q\leqslant z}\frac{1}{q^{4+2r}} + O(\sqrt{x}\log(xq)) \\ &\leqslant \frac{x}{(\log x) y^{3+2r}\log y} + O(z\sqrt{x}\log x). \end{aligned}$$

The above is $o(x/\log x)$ for any $y \to \infty$ and for $z \leqslant \sqrt{x}/\log^3 x$, say. Note that in the above (and below) we use both the Serre's Open Mapping Theorem and the Theorem of Bashmakov [Bas70] as it was done in the original paper of Lang and Trotter [LT77]. Together they assure that for q large enough $[\mathbb{Q}(E[q], q^{-1}\Gamma) : \mathbb{Q}] \sim q^{4+2r}$.

Finally we estimate $N(x,y)$ by a direct application of CDT. We set $P(y) = \prod_{\ell\leqslant y}\ell$ and we

write

$$\begin{aligned} N(x,y) &= \sum_{\substack{m\in\mathbb{N},\\ m\mid P(y)}} \mu(m)\pi_{sc}(x,\mathbb{Q}(E[m],m^{-1}\Gamma)) \\ &= \sum_{\substack{m\in\mathbb{N},\\ m\mid P(y)}} \left(\frac{\mu(m)}{[\mathbb{Q}(E[m],m^{-1}\Gamma):\mathbb{Q}]}\operatorname{li} x + O(\sqrt{x}\log(xm))\right) \\ &= c_{E,\Gamma}\operatorname{li} x + O\left(\sum_{q>y}\frac{1}{q^{4+2r}}\frac{x}{\log x}\right) + 2^{\pi(y)}\sqrt{x}\log x. \end{aligned}$$

Here $\pi(y)$ is the prime–counting function.

By appropriate choices of $y = \log x/6$ and $z = \sqrt{x}/\log^{2r+5} x$, we obtain, on GRH,

$$\pi_{E,\Gamma}(x) = \left(c_{E,\Gamma} + O_{E,\Gamma}\left(\frac{1}{\log^{2r+3} x}\right)\right)\operatorname{li} x,$$

that is the statement of Theorem 3.1.1.

3.5 The Euler product for $c_{E,\Gamma}$

By Serre's Open Mapping Theorem and the Theorem of Bashmakov (see [1]), we know that there exists an integer M_E such that if for all squarefree $m \in \mathbb{N}$ we write $m = m_1m_2$ where $m_1 \mid M_E$ and $\gcd(m_2, M_E) = 1$, then

$$[\mathbb{Q}(E[m],m^{-1}\Gamma):\mathbb{Q}] = [\mathbb{Q}(E[m_1],m_1^{-1}\Gamma):\mathbb{Q}] \times m_2^{4+2r}\prod_{\ell\mid m_2}\left(1-\frac{1}{\ell}\right)\left(1-\frac{1}{\ell^2}\right).$$

Hence

$$c_{E,\Gamma} = \sum_{m\mid M_E}\frac{\mu(m)}{[\mathbb{Q}(E[m],m^{-1}\Gamma):\mathbb{Q}]} \times \prod_{\ell\nmid M_E}\left(1-\frac{1}{\ell^{2r}(\ell^2-\ell)(\ell^2-1)}\right).$$

Therefore $c_{E,\Gamma}$ is a rational multiple of

$$\prod_{\ell\geqslant 2}\left(1-\frac{1}{\ell^{2r}(\ell^2-\ell)(\ell^2-1)}\right) = \begin{cases} 0.95602472619424273635537 93 & \text{if } r=1 \\ 0.98932530204908223306810 93 & \text{if } r=2 \\ 0.99736719255575490012265 83 & \text{if } r=3 \\ 0.99934577965540562794682 54 & \text{if } r=4 \end{cases}$$

It would be interesting to test the accuracy of the asymptotic formula for $\pi_{E,\Gamma}(x)$ in some cases. The first candidates are Serre curves where often it might happen that $M_E = 2N_E$.

Serre curves were introduced by Serre himself in [Ser72]. A practical account can also be found in [LT76]. Some Serre curves are, for example, `37.a1`, `43.a1`, `53.a1`, `57.a1`, `58.a1`, `61.a1`, `77.a1`, `79.a1`, `83.a1`, `88.a1`, `89.a1`, `91.a1`, and `92.a1` in Cremona's Tables (see [Cre97] or [Cre06]).

In fact in the special case when $E/\mathbb{Q}$ is a Serre curve of prime conductor q of rank 1 (i.e., $E(\mathbb{Q}) = \langle P \rangle$) and such that $[\mathbb{Q}(E[m], m^{-1}P) : \mathbb{Q}(E[m])] = m$ for all square free integers m, we expect that $M_E = 2q$ and that

$$c_{E,\langle P\rangle} = \left(1 + \frac{1}{23(q^3(q^2-1)(q-1)-1)}\right) \times \prod_{\ell \geqslant 2} \left(1 - \frac{1}{\ell^3(\ell-1)(\ell^2-1)}\right).$$

The above should be the case for `37.a1`: $y^2 + y = x^3 - x$ and for `43.a1`: $y^2 + y = x^3 + x^2$.

3.6 Possible paths of future research

The result of Theorem 3.1.1 lives in a very wide and structured environment of research. For this reason it can be improved in many directions.

First of all, we can try to understand when the constant $c_{E,\Gamma}$ is positive. We have a sufficient condition for positivity, that is given by the results in Section 6 of [CM04], in which the authors consider the related problem of cyclicity of $\bar{E}(\mathbb{F}_p)$. The condition they give is just that $E[2]$ is not completely rational. To apply this to our problem, it suffices to note that if $\bar{E}(\mathbb{F}_p)$ is cyclic, so $\bar{E}(\mathbb{F}_p)/\Gamma_p$ is, because every quotient of a cyclic group is cyclic. It could be interesting to find also necessary conditions for the positivity of $c_{E,\Gamma}$.

Another interesting direction is the one we sketched in Section 3.5 of this chapter. Serre curves are always the first ones considered to compute explicitly the constants in density results like the one we consider here.

Finally, many generalizations or modifications of the classical Artin's primitive root conjecture can have a translation in the elliptic curve setting, so the same questions can often be made for the quotients of reductions $\bar{E}(\mathbb{F}_p)/\Gamma_p$. We refer the reader to Section 9 of [Mor12] for variations of Artin's problem.

Part II

Statistics on Biquadratic Curves over Finite Fields

This second part of the thesis is about a joint (ongoing) work with Elisa Lorenzo Garcia (University of Leiden) and Piermarco Milione (University of Barcelona).

Chapter 4

Preliminaries to Arithmetic Statistics on Curves over Finite Fields

In this chapter we give an overview of the topics and techniques related to Arithmetic Statistics on Families of Curves over Finite Fields. We will need these notions to develop the results contained the next two chapters. As general references, we will mainly use [Dav14] and [Ros02].

4.1 Zeta Functions over Function Fields

Let q be a power of a prime, and $\mathbb{F}_q$ the finite field with q elements. We want to study zeta functions and L-functions of function fields over $\mathbb{F}_q$.

The first step is to study the analogue of the classical Riemann Zeta Function. We are talking about the zeta function of the function field $\mathbb{F}_q(t)$. It is useful to point out that there is a sort of correspondence between the objects and functions related to number fields and the ones occurring in the study of function fields. This is expressed by the following list:

Number Fields		**Function Fields**
$\mathbb{Q}$	$\leftrightarrow$	$\mathbb{F}_q(t)$
$\mathbb{Z}$	$\leftrightarrow$	$\mathbb{F}_q[t]$
positive prime p	$\leftrightarrow$	$P(t)$ monic irreducible polynomial
$\lvert n\rvert$	$\leftrightarrow$	$\lvert F(t)\rvert = q^{\deg F}$

where $\mathbb{F}_q[t]$ is the ring of polynomials and $\mathbb{F}_q(t)$ the field of rational function. It is interesting to see that many properties of classical number field have a counterpart on the right hand side of the list. For example, we know that $\#(\mathbb{Z}/p\mathbb{Z}) = \#(\mathbb{F}_p) = p = |p|$ with p a prime number, and similarly $\#(\mathbb{F}_q(t)/P(t)) = q^{\deg P} = |P(t)|$, where $P(t)$ is a monic irreducible polynomial. From now on, every polynomial will be considered monic, unless otherwise stated.

The analogue of the Riemann zeta function, in the setting of funciton fields, is

$$\zeta_q(s) = \sum_{F \in \mathbb{F}_q[t]} |F|^{-s} = \prod_{P \text{ irreducible}} (1 - |P|^{-s})^{-1}. \tag{4.1}$$

The Euler product on the right hand side is deduced in the same way as in the classical Riemann zeta function, because $\mathbb{F}_q[t]$ is a UFD (another property in common with $\mathbb{Z}$).

As there are q^d monic polynomials of degree d, we see that

$$\zeta_q(s) = \sum_{d \geqslant 0} q^d q^{-ds} = \frac{1}{1 - q^{1-s}}. \tag{4.2}$$

We will now deduce a result that will be fundamental in the next two chapters. Let a_d be the number of irreducible polynomials of degree d over $\mathbb{F}_q$. Then, using (4.1) and (4.2), we get

$$\zeta_q(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d} = (1 - q^{1-s})^{-1},$$

and if we substitute q^{-s} with the variable u, we have

$$\frac{1}{1 - qu} = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}.$$

Taking logarithmic derivatives of both sides and multiplying by u, we get

$$u \frac{d}{du} \log(1 - qu) = u \sum_{d=1}^{\infty} a_d \frac{d}{du} \log(1 - u^d),$$

that is

$$\frac{qu}{1 - qu} = \sum_{d=1}^{\infty} \frac{d a_d u^d}{1 - u^d}.$$

We can expand both sides of this equality in power series, using geometric series. Then, equating coefficients of u^n, we have

$$\sum_{d|n} d a_d = q^n,$$

and, by Moebius inversion formula, we get

$$a_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}. \tag{4.3}$$

We can now deduce the following fundamental result:

Theorem 4.1.1 ([Ros02], Theorem 2.2)**.** (The prime number theorem for polynomials) *Let a_n denote the number of monic irreducible polynomials in $\mathbb{F}_q[t]$ of degree n. Then,*

$$a_n = \frac{q^n}{n} + O\left(\frac{q^{\frac{n}{2}}}{n}\right).$$

Proof. From (4.3), we have that

$$a_n = \frac{q^n}{n} + O\left(\frac{q^{\frac{n}{2}}}{n} + \frac{q^{\frac{n}{3}}}{n} \sum_{\substack{d|n \\ d \neq n, \frac{n}{2}}} |\mu(d)|\right),$$

and $\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime divisor of n. Since $2^{\omega(n)} \leqslant n$, the result follows. □

Using $\zeta_q(s)$, it is also possible to prove (see Lemma 3.2 of [Dav14]) that the set of monic square-free polynomials, which we denote $\mathcal{F}_d$, has cardinality

$$\#\mathcal{F}_d = \begin{cases} q^d - q^{d-1} = \frac{q^d}{\zeta_q(2)} & \text{if } d \geqslant 2 \\ q^d & \text{if } d = 0, 1 \end{cases}.$$

This result has its analogue in the language of number fields, where we know that the number of square-free positive integer up to x is asymptotic to $x/\zeta(2)$ ([Pap05], Section 1).

Now, we want to define general zeta funtions in the funtion field settings. This means that we have to consider, beside the finite primes of $\mathbb{F}_q(t)$, also the so-called prime at ∞. Moreover, we will consider not only $\mathbb{F}_q(t)$, but also finite extensions $K \supseteq \mathbb{F}_q(t)$. Such a K is called a *function field* over $\mathbb{F}_q$. A *prime* of K is by definition a discrete valuation ring R with maximal ideal P such that $\mathbb{F}_q \subseteq R$, and the quotient field of R is K. The notation P is properly chosen, because we refer to such a prime by P, and we denote with ord_P the discrete valuation associated to P. Also, we define $\deg P$ as the degree of the field extension $R/P \supseteq \mathbb{F}_q$ and we denote with $\mathcal{S}_K$ the set of primes of K. For more details about these definitions and properties we refer the reader to [Ros02, Chapter 5].

In the case that $K = \mathbb{F}_q(t)$, beside the primes given by the irreducible polynomials, we have the extra prime associated to the ring $A' = \mathbb{F}_q[t^{-1}]$, with prime ideal P' generated by t^{-1}. In fact, the localization of A' at P' is a discrete valuation ring and defines the prime at infinity of $\mathbb{F}_q(t)$. We notice that the degree of this prime is 1.

Let K be a function field, and let $\mathcal{D}_K$ be the *group of divisors* of K, which is the free abelian group generated by the primes. We denote this group additively, so a typical divisor is a finite sum

$$D = \sum_P a(P)P,$$

where P are primes of K. The degree of such a divisor is $\deg D = \sum_P a(P)\deg(P)$, and the norm of D is $|D| = q^{\deg D}$. A divisor D is said to be *effective* if $a(P) \geqslant 0$ for all P. We denote this by $D \geqslant 0$.

Definition 4.1.2. Let K be a function field over $\mathbb{F}_q(t)$. The *zeta function* of K, $\zeta_K(s)$, is defined by

$$\zeta_K(s) = \sum_{\substack{D \in \mathcal{D}_K \\ D \geqslant 0}} |D|^{-s} = \prod_{P \in \mathcal{S}_K} (1 - |P|^{-s})^{-1},$$

where the sum runs over all divisors $D \in \mathcal{D}_K$, and the product over all primes $P \in \mathcal{S}_K$. Moreover, we can define $Z_K(u)$ as $\zeta_K(u)$, where we use the change of variable $u = q^{-s}$.

If $K = F_q(t)$, we can see that

$$\zeta_K(s) = \frac{1}{(1 - q^{-s})(1 - q^{1-s})}.$$

This is the completed zeta function of $\zeta_q(s)$, which did not include the prime at ∞.

In Chapter 6 we will study the zeta function of biquadratic extensions of $\mathbb{F}_q(t)$ to compute some statistics on them.

In analogy with the number field setting, we can define Dirichlet charachters and L-functions also in this context. For details about this, we refer the reader to [Ros02, Chapter 4].

4.2 From Function Fields to Curves

At this point we want to define the zeta function of a curve over a finite field. First of all, we recall that there is an equivalence of categories between smooth projective curves over $\mathbb{F}_q$ and function fields over $\mathbb{F}_q$ (see for example [Sil08, Chapter 2] or [Har77, I, Theorem 6.9]). Let C be a smooth projective curve over $\mathbb{F}_q$ and suppose for simplicity that C has an affine plane model given by the equation $F(t,y)=0$, with $F(t,y)$ an irreducible polynomial in $\mathbb{F}_q[t,y]$. The coordinate ring $K[C]$ of C is $\mathbb{F}_q[t,y]/F(t,y)$ and the function field of C, denoted by $K(C)$, is the field of fraction of $K[C]$, that is $K(C)=\mathbb{F}_q(t,y)/(F(t,y))$. So, the correspondence $C\mapsto K(C)$ gives the equivalence of categories and then $K(C)$ is a finite extension of $\mathbb{F}_q(t)$. The corresponding maps inside the two categories are, on one side, surjective morphisms of curves over $\mathbb{F}_q$, and on the other side we have function field injections preserving $\mathbb{F}_q$.

Then, given a curve C over $\mathbb{F}_q$, with function field $K(C)$. One can prove that primes in $\mathcal{S}_K$ correspond to Galois orbits of points on C. For example, for the function field $\mathbb{F}_q(t)$, the finite primes are in one-to-one correspondence with irreducible polynomials in $\mathbb{F}_q[t]$ which are in one-to-one correspondence with $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-orbits of points in $\mathbb{A}^1(\bar{F}_q)$ (the Galois orbit associated to a given irreducible polynomial $P(t)\in\mathbb{F}_q[t]$ is the set of roots of $P(t)$). The degree of the polynomial is then the number of elements in the orbit. With this example in mind, it is natural to think that the set of primes of degree 1 in the function field $K_m=\mathbb{F}_{q^m}K$ must correspond to the points of C defined over $\mathbb{F}_{q^m}$. This brings to the definition of $Z_C(u)$, that is given in the next section.

4.3 Weil Theorem

Given a smooth projective curve C of genus g over a finite field $\mathbb{F}_q$, one of the first things one can ask is the number of its $\mathbb{F}_q$-rational points. An interesting way to answer to this question, or at least to get some information, is to introduce the zeta function associated to C, that is defined as

$$Z_C(u)=\exp\left(\prod_{n=1}^{\infty}\#C(\mathbb{F}_{q^n})\frac{u^n}{n}\right)$$

where $u=q^{-s}$ with $s\in\mathbb{C}$ and $\Re(s)>1$. One can prove that $Z_C(u)=Z_K(C)(u)$ where $Z_{K(C)}$ is the one defined in Definition 4.1.2 (see [Dav14, Section 3] for details). In 1948 André Weil ([Wei48]) proved the following properties of $Z_C(u)$:

- Rationality:
$$Z_C(u)=\frac{P_C(u)}{(1-u)(1-qu)}$$
where $P_C(u)$ is a polynomial of degree $2g$ in $\mathbb{Z}[u]$.
- Functional Equation:
$$Z_C(1/qu)=\pm q^{1-g}u^{2-2g}Z_C(u).$$
- Riemann Hypothesis:
$$P_C(u)=\prod_{j=1}^{2g}(1-u\alpha_j(C)),\quad |\alpha_j(C)|=\sqrt{q},$$

i.e. the roots $\alpha_j(C)^{-1}$ of $P_C(u)$ have absolute value $1/\sqrt{q}$. This is called Riemann Hypothesis for Curves over Finite Fields because, if we look at P_C as a function of s, with $q = u^{-s}$, we see that $|u| = 1/\sqrt{q} \Leftrightarrow \Re(s) = 1/2$, that is the formulation of the Riemann Hypothesis for the classical Riemann Zeta Function.

The generalization of all these properties to varieties of any dimension are known as Weil Conjectures and they were proved later by different mathematicians.

4.4 Number of Points in Families of Curves as a sum of Random Variables

We want to explain briefly the techniques we are going to use in Chapter 5. We refer the reader to [Dav14, Section 4] for more details.

For any curve of genus g, it follows from Section 4.3 that the number of points in C is given by

$$\#C(\mathbb{F}_q) - (q+1) = \sum_{j=1}^{2g} \alpha_j(C) = q^{1/2} \operatorname{tr} \Theta_C$$

where Θ_C is a $2g \times 2g$ unitary matrix with eigenvalues $q^{-1/2}\alpha_j(C) = e^{i\theta_j(C)}$, $j = 1, \dots, 2g$.

The matrix (or rather the conjugacy class) Θ_C is called the Unitarized Frobenius Class of C.

We want to study the fluctuations in the number of points in a family of curves over $\mathbb{F}_q$ of genus g. When the genus of the curves is fixed and q tends to ininity, $q^{-1/2}(\#C(\mathbb{F}_q) - (q+1)) = \operatorname{tr} \Theta_C$ is distributed as the trace of matrices in a symmetry group $M(2g)$ determined by the so-called monodromy group of the family, for natural families $\mathcal{F}(g;q)$ of curves of genus g over $\mathbb{F}_q$ where Deligne's equidistribution theorem and its generalisations hold. For example, these families can be moduli spaces, or connected components of moduli spaces. For more details about these studies, we refer the reader to [KS99, Chapter 9].

Here, and in the next two chapters, we consider the other limit, that is the limit for $g \to \infty$ and q fixed. In this case we will find that one can write in a natural way the distribution of $\#C(\mathbb{F}_q)$ as a sum of $q+1$ independent identically distributed random variables.

This was done for several families of curves, such as hyperelliptic curves, cyclic trigonal curves and many others. In Chapter 5 we will compute such statistics for a family of biquadratic curves.

Hyperelliptic Curves

As an example, we write the main result of [KR09]. Let $\mathcal{H}_g$ be the moduli space of hyperelliptic curves of genus g. Then

$$\lim_{g\to\infty} \frac{\#\{C \in \mathcal{H}_g : \#C(\mathbb{F}_q) = m\}}{\#\mathcal{H}_g} = \operatorname{Prob}\left(\sum_{i=1}^{q+1} X_i = m\right),$$

where the X_i are i.i.d. random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{q}{2(q+1)} \\ 1 & \text{with probability } \frac{1}{q+1} \\ -1 & \text{with probability } \frac{q}{2(q+1)} \end{cases}$$

Chapter 5

The fluctuations in the number of points of a Biquadratic Curve over a Finite Field

5.1 Number of points of Biquadratic Curves as a sum of Random Variables

One of the most influential results in class field theory is Chebotarev's density theorem. As it is well known, this result is a deep generalization of the Theorem of Dirichlet about equidistribution of rational primes in arithmetic progression and gives a complete understanding of the distribution of primes in a fixed Galois number field extension with respect to their splitting behavior (for an interesting discussion of the theorem and its original proof see [LS96]). In the function field case the parallel statement is carried over by the Sato-Tate conjecture for curves, which studies the distribution of the Frobenius endomorphism of the reduction modulo p of a fixed curve, when the prime p varies.

In order to complement this line of research in other directions, several mathematicians were led to consider the following new general problem: given a family of curves, satisfying certain properties, of genus g over $\mathbb{F}_q$, understand the distribution of the Frobenius endomorphism of the curves of the family. This is sometimes called the *vertical Sato-Tate conjecture*, since the prime p is fixed and the curve varies in the family. This study can be done in two different ways, depending on whether we let the genus g tend to infinity or the cardinality q of the field. It is then interesting to compare both limit results.

When g is fixed and q goes to infinity the problem can be solved thanks to Deligne's equidistribution theorem (cf. [KS99,]) while for the complementary case different techniques are applied depending on the particular family considered. The fluctuation in the number of points at the g-limit has been studied for different families of curves, such as:

- Hyperelliptic curves , cf. [KR09], [BDFL09],
- Cyclic trigonal curves (i.e. cyclic 3-covers of the projective line), cf. [BDFL09], [Xio10],
- General trigonal curves, cf. [MW12],

- p-fold cover of the projective line, [BDFL11],
- ℓ-covers of the projective line, cf. [BDFL09] and [BDF$^+$15].

In the present chapter, we study the distribution of the number of points over $\mathbb{F}_q$ for a genus g curve C defined over $\mathbb{F}_q$ which is a quartic non-cyclic cover of the projective line $\mathbb{P}^1_{\mathbb{F}_q}$, at the g-limit with q fixed.

Let $\mathcal{B}_g(\mathbb{F}_q)$ be the family of such genus g curves and consider the following decomposition

$$\mathcal{B}_g(\mathbb{F}_q) = \bigcup_{g_1+g_2+g_3=g} \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)$$

where $\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)$ denotes the subfamily of curves $C \in \mathcal{B}_g(\mathbb{F}_q)$ such that the three hyperelliptic quotients of C have genera g_1, g_2 and g_3.

The main theorem of this chapter is the following:

Theorem. *In the limit when the three genera g_1, g_2, g_3 go to infinity*

$$\frac{|\{C \in \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q) : \mathrm{Tr}(\mathrm{Frob}_C) = -M\}|'}{|\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)|'} = \mathrm{Prob}\left(\sum_{j=1}^{q+1} X_j = M\right)$$

where the X_j are i.i.d. random variables such that

$$X_i = \begin{cases} -1 & \text{with probability } \frac{3(q+2)}{4(q+3)} \\ 1 & \text{with probability } \frac{6}{4(q+3)} \\ 3 & \text{with probability } \frac{q}{4(q+3)} \end{cases}$$

These results are part of the joint work [LMM15]. We refer the reader to it, also for a comparison with the case of q-limit. Throughout all the chapter we denote with k the funtion field $\mathbb{F}_q(t)$.

5.2 The family of biquadratic curves

We first define and give the basic properties of the family of biquadratic curves. We determine its genus in terms of the equations defining the curves, and we study the irreducible components of the coarse moduli space of biquadratic curves.

Recall that if $K/\mathbb{F}_q(t)$ is a finite Galois extension such that $K \cap \bar{\mathbb{F}}_q = \mathbb{F}_q$, then there exists a unique nonsingular projective curve C with function field $\mathbb{F}_q(C) = K$, together with a regular morphism $\varphi : C \to \mathbb{P}^1_{\mathbb{F}_q}$ defined over $\mathbb{F}_q$ (cf. [Har77, I,Th. 6.6, Th.6.9]).

Definition 5.2.1. We will call biquadratic curve a smooth projective curve C, together with a regular morphism $\varphi : C \to \mathbb{P}^1_{\mathbb{F}_q}$ defined over $\mathbb{F}_q$, that induces a field extension with Galois group $\mathrm{Gal}(\mathbb{F}_q(C)/\mathbb{F}_q(t)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Since $\mathrm{char}(k) \neq 2$, it is clear that every non-cyclic quartic extension of k is of the form $K = k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$, for some $h_1(t), h_2(t) \in \mathbb{F}_q[t]$ different non-constant polynomials, that we can take to be square-free. Moreover, if the leading coefficient $\mathrm{lc}(h_i)$ is a square in $\mathbb{F}_q$, then

we can assume that this is equal to 1. Therefore, if C is a biquadratic curve, then an affine model of C in $\mathbb{A}^3_{\mathbb{F}_q}$ is given by

$$C : \begin{cases} y_1^2 = h_1(t) \\ y_2^2 = h_2(t). \end{cases}$$

Remark 5.2.2. If $K := k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$ is a biquadratic extension of k, then there are exactly 3 different quadratic subextensions of K, namely $k(\sqrt{h_1}), k(\sqrt{h_2})$ and $k(\sqrt{h_1 h_2})$.

If we write $h_i = f_i f$ for $i = 1, 2$, with $f = (h_1, h_2)$, then clearly we have that $(f_1, f_2) = (f_1, f) = (f_2, f) = 1$ and these three subextensions are $k(\sqrt{f f_1}), k(\sqrt{f f_2})$ and $k(\sqrt{f_1 f_2})$.

Two such extensions $k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$ and $k(\sqrt{h_1'(t)}, \sqrt{h_2'(t)})$ are the same if and only if we have the equality of sets:

$$\{h_1, h_2, \frac{h_1 h_2}{(h_1, h_2)^2}\} = \{h_1', h_2', \frac{h_1' h_2'}{(h_1', h_2')^2}\}.$$

Remark 5.2.3. Recall that if $\pi : C \to \mathbb{P}^1$, whose affine plane model is $y^2 = F(t)$, with $F(t)$ a square-free polynomial over $\mathbb{F}_q$, then the point at infinity is ramified in the cover π iff the degree d of F is odd. Indeed, if we take take $u = \frac{1}{t}$, then the function field of C is:

$$k(C) = k(\sqrt{F(t)}) = k(\sqrt{F(1/u)}) = k(\sqrt{u^{-d}\tilde{F}(u)})$$

and then it is clear that $t = \infty$ ramifies iff the point $u = 0$ ramifies, i.e. iff d is odd.

Proposition 5.2.4. *Let $h_1(t), h_2(t) \in \mathbb{F}_q[t]$ be different square-free polynomials, and let C be the curve whose function field is $k(C) = k(\sqrt{h_1(t)}, \sqrt{h_2(t)})$. For every $i = 1, 2$, write $h_i = f f_i$, with $f = (h_1, h_2)$, and define $h_3 := f_1 f_2$.*

If we denote by C_i the hyperelliptic curve whose affine plane model is given by the equation $y^2 = h_i(t)$, for $i = 1, 2, 3$, then we have the following formula for the genus of C:

$$g(C) = g(C_1) + g(C_2) + g(C_3)$$

Moreover, if we denote by $n := \deg(f)$ and $n_i := \deg(f_i)$,

$$g(C) = g(n_1, n_2, n) := n_1 + n_2 + n + e_\infty - 4,$$

where

$$e_\infty := \begin{cases} 2, & if\ n \equiv n_1 \equiv n_2 \equiv 0 \,(\mathrm{mod}\, 2) \\ 1, & otherwise \end{cases}.$$

Proof. Let us denote by $R := \mathrm{Ram}(\pi)$ the subset of all points of $\mathbb{P}^1_{\mathbb{F}_q}$ which are ramified in the cover $\pi : C \longrightarrow \mathbb{P}^1_{\mathbb{F}_q}$. Riemann-Hurwitz formula (cf. [Ros02, Theorem 7.16]) implies that $2g(C) - 2 = 4(2 \cdot 0 - 2) + 2|R|$. So, $g(C) = |R| - 3$. Again, for the hyperelliptic cover $\pi_i : C_i \longrightarrow \mathbb{P}^1$ and the ramification sets $R_i := \mathrm{Ram}(\pi_i)$, gives $g(C_i) = \frac{|R_i|}{2} - 1$. Now, the definition of h_3 implies that

$$2|R_1 \cup R_2 \cup R_3| = |R_1| + |R_2| + |R_3|.$$

Thus, the formula $g(C) = g(C_1) + g(C_2) + g(C_3)$ holds.

We can also apply Riemann-Hurwitz formula to the morphism π, and so we have:

$$2g - 2 = 4(2 \cdot 0 - 2) + 2 \cdot (n_1 + n_2 + n_3 + e_\infty - 1).$$

□

Now, we introduce some sets of polynomials that will be useful:

$$V_d = \{F \in \mathbb{F}_q[t] : F \text{ monic, } \deg(F) = d\}$$

$$\mathcal{F}_d = \{F \in \mathbb{F}_q[t] : F \text{ monic, square-free, } \deg(F) = d\}$$

$$\widehat{\mathcal{F}}_d = \{F \in \mathbb{F}_q[t] : F \text{ square-free, } \deg(F) = d\}$$

$$\mathcal{F}_{(n,n_1,n_2)} = \{(f, f_1, f_2) \in \mathcal{F}_n \times \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f, f_1) = (f, f_2) = (f_1, f_2) = 1\}$$

$$\widehat{\mathcal{F}}_{(n,n_1,n_2)} = \{(f, f_1, f_2) \in \mathcal{F}_n \times \widehat{\mathcal{F}}_{n_1} \times \widehat{\mathcal{F}}_{n_2} : (f, f_1) = (f, f_2) = (f_1, f_2) = 1\}$$

$$\mathcal{F}_{[n,n_1,n_2]} = \mathcal{F}_{(n,n_1,n_2)} \cup \mathcal{F}_{(n-1,n_1,n_2)} \cup \mathcal{F}_{(n,n_1-1,n_2)} \cup \mathcal{F}_{(n,n_1,n_2-1)}$$

$$\widehat{\mathcal{F}}_{[n,n_1,n_2]} = \widehat{\mathcal{F}}_{(n,n_1,n_2)} \cup \widehat{\mathcal{F}}_{(n-1,n_1,n_2)} \cup \widehat{\mathcal{F}}_{(n,n_1-1,n_2)} \cup \widehat{\mathcal{F}}_{(n,n_1,n_2-1)}$$

Definition 5.2.5. We denote by $\mathcal{B}_g(\mathbb{F}_q)$ the family of biquadratic curves defined over $\mathbb{F}_q$ and of fixed genus g. It can be written as a disjoint union of subfamilies indexed by unordered 3-tuples of positive integers g_1, g_2, g_3, i.e.

$$\mathcal{B}_g(\mathbb{F}_q) = \bigcup_{g_1+g_2+g_3=g} \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q),$$

where $\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)$ denotes the family of curves over the set of polynomials $\widehat{\mathcal{F}}_{[n,n_1,n_2]}$ such that $g_i = \lfloor \frac{n+n_i-1}{2} \rfloor$ for $i = 1, 2$ and $g_3 = \lfloor \frac{n_1+n_2-1}{2} \rfloor$.

The family $\mathcal{B}_g(\bar{\mathbb{F}}_q)$ of biquadratic curves defined over $\bar{\mathbb{F}}_q$ is a coarse moduli space over $\mathbb{Z}[1/2]$ (cf. [PG05b, Lemma 3.1]). A detailed geometric study of this moduli space can be found in [PG05b] and [PG05a].

Remark 5.2.6. One has the following equalities:

$$|\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)|' = \sum_{C \in \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)}{}' 1 = \sum_{F \in \widehat{\mathcal{F}}_{[n,n_1,n_2]}} \frac{1}{|\mathrm{Aut}(C)|} = \frac{|\widehat{\mathcal{F}}_{[n,n_1,n_2]}|}{q(q^2-1)},$$

where the $'$ notation, applied both to cardinality and summation, means that each one of the curves C in the moduli spaces is counted with the usual weight $\frac{1}{|\mathrm{Aut}(C)|}$.

Remark 5.2.7. Notice that $|\widehat{\mathcal{F}}_{(n,n_1,n_2)}| = (q-1)^2 |\mathcal{F}_{(n,n_1,n_2)}|$ and that we can see the set $\widehat{\mathcal{F}}_{(n,n_1,n_2)}$ as the set of the quadratic twists of elements in $\mathcal{F}_{(n,n_1,n_2)}$ given by the equations

$$C' : \begin{cases} y_1^2 = \alpha_1 f f_1(t) \\ y_2^2 = \alpha_2 f f_2(t) \end{cases}$$

where $\alpha_1, \alpha_2 \in \mathbb{F}_q^*$.

5.3 Proof of the Main Theorem

Let χ denote the quadratic character in $\mathbb{F}_q$, we set, for any element (f, f_1, f_2) in $\widehat{\mathcal{F}}_{(n,n_1,n_2)}$,

$$S(f, f_1, f_2) = \sum_{x \in \mathbb{F}_q} (\chi(f \cdot f_1(x)) + \chi(f \cdot f_2(x)) + \chi(f_1 \cdot f_2(x))), \text{ and}$$

$$\widehat{S}(f, f_1, f_2) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} (\chi(f \cdot f_1(x)) + \chi(f \cdot f_2(x)) + \chi(f_1 \cdot f_2(x))),$$

where for the point at infinity we define

$$\chi(F(\infty)) = \begin{cases} 0 & \deg(F) \text{ odd} \\ 1 & \deg(F) \text{ even, leading coefficient is a square in } \mathbb{F}_q \\ -1 & \deg(F) \text{ even, leading coefficient is not a square in } \mathbb{F}_q \end{cases}$$

Then, for the curve $C \in \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)$ defined by (f, f_1, f_2) we have that

$$\#C(\mathbb{F}_q) = q + 1 + \widehat{S}(f, f_1, f_2).$$

Hence, we have the equality

$$\frac{|\{C \in \mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q) : \mathrm{Tr}(\mathrm{Frob}_C) = -M\}|'}{|\mathcal{B}_{(g_1,g_2,g_3)}(\mathbb{F}_q)|'} = \frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n,n_1,n_2]} : \widehat{S}(f, f_1, f_2) = M\}|}{|\widehat{\mathcal{F}}_{[n,n_1,n_2]}|}$$

The goal of this section is to prove the following theorem, which is a more precise statement of the theorem we stated in section 5.1.

Theorem 5.3.1. *In the limit when the three degrees n, n_1, n_2 go to infinity*

$$\frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n,n_1,n_2]} : \widehat{S}(f, f_1, f_2) = M\}|}{|\widehat{\mathcal{F}}_{[n,n_1,n_2]}|} = \mathrm{Prob}\left(\sum_{j=1}^{q+1} X_j = M\right)$$

where the X_j are i.i.d. random variables such that

$$X_i = \begin{cases} -1 & \text{with probability } \frac{3(q+2)}{4(q+3)} \\ 1 & \text{with probability } \frac{6}{4(q+3)} \\ 3 & \text{with probability } \frac{q}{4(q+3)} \end{cases}$$

More precisely,

$$\frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n,n_1,n_2]} : \widehat{S}(f, f_1, f_2) = M\}|}{|\widehat{\mathcal{F}}_{[n,n_1,n_2]}|} = \mathrm{Prob}\left(\sum_{j=1}^{q+1} X_j = M\right)\left(1 + O(q^{-\frac{(1-\epsilon)}{2} min(n,n_1,n_2)+q})\right)$$

The proof of the Theorem runs as in [KR09] (resp. [BDFL09]) for the equivalent statement for hyperelliptic curves (resp. $l-$cyclic covers).

Lemma 5.3.2. *([BDFL09, Lemma 4.2]) For $0 \leqslant l \leqslant q$ let $x_1, ..., x_l$ be distinct elements of $\mathbb{F}_q$. Let $U \in \mathbb{F}_q[t]$ be such that $U(x_i) \neq 0$ for $i = 0, ..., l$. Let $a_1, ..., a_l \in \mathbb{F}_q^*$. The number of elements in the set*

$$\{F \in \mathcal{F}_d : (F, U) = 1,\ F(x_i) = a_i,\ 1 \leqslant i \leqslant l\}$$

is the number

$$S_d^U(l) = \frac{q^{d-l}}{\zeta_q(2)(1-q^{-2})^l} \prod_{P|U} (1 + q^{-deg(P)})^{-1} \left(1 + O(q^{l-d/2})\right).$$

Lemma 5.3.3. *For $0 \leqslant l \leqslant q$ let $x_1, ..., x_l$ be distinct elements of $\mathbb{F}_q$. Let $U \in \mathbb{F}_q[t]$ be such that $U(x_i) \neq 0$ for $i = 0, ..., l$. Let $a_1, ..., a_l, b_1, ..., b_l \in \mathbb{F}_q^*$. The number of elements in the set*

$$\{(f_1, f_2) \in \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f_i, U) = (f_1, f_2) = 1,\ f_1(x_i) = a_i,\ f_2(x_i) = b_i,\ 1 \leqslant i \leqslant l\}$$

is the number

$$R_{n_1,n_2}^U(l) = \frac{q^{n_1+n_2-2l}L}{\zeta_q^2(2)(1-q^{-2})^{2l}} \left(\frac{1+2q^{-1}}{(1+q^{-1})^2}\right)^{-l} \prod_{P|U} \left(\frac{1}{1+2|P|^{-1}}\right) \left(1 + O(q^{l-\frac{min(n_1,n_2)}{2}})\right),$$

where $L := \prod_{P\ prime}(1 - \frac{|P|^{-2}}{(1+|P|^{-1})^2})$.

Proof. By inclusion-exclusion principle (same notations as in [GGL95, Theorem 13.5]), with

$$f(D) = |\{(f_1, f_2) \in \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f_i, U) = 1,\ D|(f_1, f_2),\ f_1(x_i) = a_i,\ f_2(x_i) = b_i,\ 1 \leqslant i \leqslant l\}|,$$

$$g(D) = |\{(f_1, f_2) \in \mathcal{F}_{n_1} \times \mathcal{F}_{n_2} : (f_i, U) = 1,\ (f_1, f_2) = D,\ f_1(x_i) = a_i,\ f_2(x_i) = b_i,\ 1 \leqslant i \leqslant l\}|,$$

we have

$$R_{n_1,n_2}^U(l) = g(1) = \sum_{D,\, D(x_i)\neq 0, (D,U)=1} \mu(D) f(D).$$

But notice that when $(D, U) = 1$

$$f(D) = |\{(f_1, f_2) \in \mathcal{F}_{n_1-\deg(D)} \times \mathcal{F}_{n_2-\deg(D)} : (f_i, UD) = 1,\ f_1(x_i) = a_i,\ f_2(x_i) = b_i,\ 1 \leqslant i \leqslant l\}|,$$

hence Lemma 5.3.2 implies

$$f(D) = S_{n_1-\deg(D)}^{UD}(l) \cdot S_{n_2-\deg(D)}^{UD}(l) = \\ = \frac{q^{n_1+n_2-2l-2\deg(D)}}{\zeta_q^2(2)(1-q^{-2})^{2l}} \prod_{P|UD} (1 + |P|^{-1})^{-2} \left(1 + O(q^{l+\frac{\deg(D)}{2}-\frac{\min(n_1,n_2)}{2}})\right).$$

So, one has

$$R_{n_1,n_2}^U(l) = \sum_{D,\, D(x_i)\neq 0, (D,U)=1} \mu(D) f(D) = \\ \frac{q^{n_1+n_2-2l}}{\zeta_q^2(2)(1-q^{-2})^{2l}} \prod_{P|U} (1+|P|^{-1})^{-2} \sum_{\substack{D(x_i)\neq 0,\ (D,U)=1 \\ \deg(D)\leqslant \min(n_1,n_2)}} \mu(D)|D|^{-2} \prod_{P|D} (1+|P|^{-1})^{-2} \left(1 + O(q^{l-\frac{\min(n_1,n_2)}{2}})\right).$$

Now, we observe that

$$\sum_{\substack{D(x_i)\neq 0,\,(D,U)=1\\ \deg(D)\leqslant \min(n_1,n_2)}} \mu(D)|D|^{-2}\prod_{P|D}(1+|P|^{-1})^{-2} =$$

$$\sum_{D,\,D(x_i)\neq 0,\,(D,U)=1} \mu(D)|D|^{-2}\prod_{P|D}(1+|P|^{-1})^{-2} + O(q^{-2\min(n_1,n_2)}),$$

where we have that

$$\sum_{D,\,D(x_i)\neq 0,\,(D,U)=1} \mu(D)|D|^{-2}\prod_{P|D}(1+|P|^{-1})^{-2} =$$

$$= \left(\frac{1+2q^{-1}}{(1+q^{-1})^2}\right)^{-l}\prod_{P|U}\left(\frac{1+2|P|^{-1}}{(1+|P|^{-1})^2}\right)^{-1}\prod_{P\,\text{prime}}(1-\frac{|P|^{-2}}{(1+|P|^{-1})^2}) =$$

$$= \left(\frac{1+2q^{-1}}{(1+q^{-1})^2}\right)^{-l}\prod_{P|U}\left(\frac{1+2|P|^{-1}}{(1+|P|^{-1})^2}\right)^{-1} L.$$

We can prove that $0 < L < 1$ (see next Remark 5.3.4). So, finally

$$R^U_{n_1,n_2}(l) = \frac{q^{n_1+n_2-2l}L}{\zeta_q^2(2)(1-q^{-2})^{2l}}\left(\frac{1+2q^{-1}}{(1+q^{-1})^2}\right)^{-l}\prod_{P|U}\left(\frac{1}{1+2|P|^{-1}}\right)\left(1+O(q^{l-\frac{\min(n_1,n_2)}{2}})\right).$$

□

Remark 5.3.4. We need to prove that the infinite product $\prod_{P\,\text{prime}}(1-\frac{|P|^{-2}}{(1+|P|^{-1})^2})$ converges to a real number L such that $0 < L < 1$. The Prime Polynomial Theorem implies that this is equivalent to prove that the infinite product

$$\prod_{\nu\geqslant 1}\left(1-\frac{1}{(q^\nu+1)^2}\right)^{\frac{q^\nu}{\nu}}$$

converges to a real number $\tilde{L}$ such that $0 < \tilde{L} < 1$ (remember that $q \geqslant 3$).

Because $\left(1-\frac{1}{(q^\nu+1)^2}\right)^{\frac{q^\nu}{\nu}} < 1$, we have that $\tilde{L} < 1$. In order to prove that $0 < \tilde{L}$, and since for $z \in (0,1)$ we have $\log(1-z) \geqslant \frac{z}{z-1}$, it is enough to prove that

$$\sum_{\nu\geqslant 1}\frac{q^\nu}{\nu}\frac{\frac{1}{(q^\nu+1)^2}}{\frac{1}{(q^\nu+1)^2}-1} = -\sum_{\nu\geqslant 1}\frac{1}{\nu}\cdot\frac{1}{q^\nu+2}$$

is convergent. Indeed, we have

$$0 \leqslant \sum_{\nu\geqslant 1}\frac{1}{\nu}\cdot\frac{1}{q^\nu+2} \leqslant \sum_{\nu\geqslant 1}\frac{1}{\nu 3^\nu} = \log\frac{3}{2}.$$

Thus,

$$\prod_{\nu\geqslant 1}\left(1-\frac{1}{(q^\nu+1)^2}\right)^{\frac{q^\nu}{\nu}} \geqslant \frac{2}{3}.$$

Proposition 5.3.5. *Let $0 \leqslant l \leqslant q$, let $x_1, ..., x_l$ be distinct elements of $\mathbb{F}_q$, and $a_1, ..., a_l, b_1, ..., b_l \in \mathbb{F}_q^*$. Then, for any $1 > \epsilon > 0$, we have*

$$|\{(f, f_1, f_2) \in \mathcal{F}_{(n,n_1,n_2)} : f(x_i)f_1(x_i) = a_i,\ f(x_i)f_2(x_i) = b_i,\ 1 \leqslant i \leqslant l\}| =$$

$$= \frac{KLq^{n_1+n_2+n-2l}}{\zeta_q^3(2)} \left(\frac{q^3}{(q-1)^2(q+3)}\right)^l (1 + O(q^{-(1-\epsilon)n+\epsilon l} + q^{-n-\frac{min(n_1,n_2)}{2}+l})),$$

where $K := \prod_P (1 - \frac{2}{(|P|+1)(|P|+2)})$.

Proof. First we observe that

$$|\{(f, f_1, f_2) \in \mathcal{F}_{(n,n_1,n_2)} : f(x_i)f_1(x_i) = a_i,\ f(x_i)f_2(x_i) = b_i,\ 1 \leqslant i \leqslant l\}| =$$

$$= \sum_{\substack{f \in \mathcal{F}_n \\ f(x_i) \neq 0}} \sum_{\substack{f_1 \in \mathcal{F}_{n_1} \\ f_1(x_i) = a_i f(x_i)^{-1} \\ (f, f_1) = 1}} \sum_{\substack{f_2 \in \mathcal{F}_{n_1} \\ f_2(x_i) = b_i f(x_i)^{-1} \\ (ff_1, f_2) = 1}} 1 =$$

$$= \sum_{f \in \mathcal{F}_n,\, f(x_i) \neq 0} R^f_{n_1,n_2}(l).$$

Using Lemma 5.3.3 we have that

$$|\{(f, f_1, f_2) \in \mathcal{F}_{n,n_1,n_2} : f(x_i)f_1(x_i) = a_i,\ f(x_i)f_2(x_i) = b_i,\ 1 \leqslant i \leqslant l\}| =$$

$$= \frac{q^{n_1+n_2-2l}L}{\zeta_q^2(2)(1-q^{-1})^{2l}} \left(\frac{1}{1+2q^{-1}}\right)^l \sum_{U \in \mathcal{F}_n, U(x_i) \neq 0} \prod_{P|U} \frac{1}{1+2|P|^{-1}} + O(q^{n_1+n_2-\frac{\min(n_1,n_2)}{2}-l}) =$$

$$= \frac{q^{n_1+n_2-2l}L}{\zeta_q^2(2)(1-q^{-1})^{2l}} \left(\frac{1}{1+2q^{-1}}\right)^l \sum_{\deg(U)=n} c(U) + O(q^{n_1+n_2-\frac{\min(n_1,n_2)}{2}-l}),$$

where for any polynomial U, we define

$$c(U) = \begin{cases} \mu^2(U) \prod_{P|U} \frac{1}{1+2|P|^{-1}} & U(x_i) \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

In order to evaluate $\sum_{\deg(U)=n} c(U)$, we consider the Dirichlet series

$$G(w) = \sum_U \frac{c(U)}{|U|^w} = \prod_{P,\, P(x_i) \neq 0} (1 + \frac{1}{|P|^w} \cdot \frac{|P|}{(|P|+2)}) =$$

$$= \frac{\zeta_q(w)}{\zeta_q(2w)} H(w) (1 + \frac{1}{q^{w-1}(q+2)})^{-l},$$

where

$$H(w) = \prod_P (1 - \frac{2}{(1+|P|^w)(|P|+2)})$$

Notice that $H(w)$ converges absolutely for $\mathrm{Re}(w) > 0$, and $G(w)$ is meromorphic for $\mathrm{Re}(w) > 0$ with simple poles at the points w where $\zeta_q(w) = (1-q^{1-w})^{-1}$ has poles, that is, $1 + i\frac{2\pi n}{\log q}$. Thus, $G(w)$ has a simple pole at $w = 1$ with residue

$$\frac{K}{\zeta_q(2)\log(q)}\left(\frac{q+3}{q+2}\right)^{-l},$$

where $K = H(1)$.

Using Theorem 17.1 of [Ros02], which is the function field version of the Wiener-Ikehara Tauberian Theorem, we get that

$$\sum_{\deg(U)=n} c(U) = \frac{K}{\zeta_q(2)}\left(\frac{q+2}{q+3}\right)^{l} q^n + O_q(q^{\epsilon n}),$$

for all $\epsilon \geqslant 0$ and where, looking at the proof of the theorem and proceding as in Proposition 4.3 in [BDFL09], we can exchange $O_q(q^{\epsilon n})$ by $O(q^{\epsilon(n+l)})$. □

Corollary 5.3.6. *Let $0 \leqslant l \leqslant q$, let $x_1, ..., x_l$ be distinct elements of $\mathbb{F}_q$, and let $a_1, ..., a_l, b_1, ..., b_l \in \mathbb{F}_q$ such that $a_1 = ... = a_{r_0} = b_1 = ... = b_{r_0} = 0$, $a_{r_0+1} = ... = a_{r_0+r_1} = 0 = b_{r_0+r_1+1} = ... = b_{r_0+r_1+r_2}$ and $b_{r_0+1}, ..., b_{r_0+r_1}, a_{r_0+r_1+1}, ..., a_{r_0+r_1+r_2}, a_j, b_j \neq 0$ if $j > r_0 + r_1 + r_2 = m$. Then for every $\epsilon > 0$, the number*

$$|\{(f, f_1, f_2) \in \mathcal{F}_{(n,n_1,n_2)} : f(x_i)f_1(x_i) = a_i,\ f(x_i)f_2(x_i) = b_i,\ f_1(x_i)f_2(x_i) = c_i,\ 1 \leqslant i \leqslant l\}|,$$

where $f(x_i)^2 c_i = a_i b_i$, is equal to

$$q^{n+n_1+n_2}\left(\frac{1}{(q-1)(q+3)}\right)^m \left(\frac{q}{(q-1)^2(q+3)}\right)^{l-m}\left(1 + O(q^{-\frac{(1-\epsilon)}{2}min(n,n_1,n_2)+l})\right).$$

Proof. Let us write $f = (x - x_1)...(x - x_{r_0})f'$, $f_1 = (x - x_{r_0+1})...(x - x_{r_0+r_1})f_1'$, and $f_2 = (x - x_{r_0+r_1+1})...(x - x_{r_0+r_1+r_2})f_2'$. Now, apply Proposition 5.3.5 to the pairs (f', f_1', f_2') and sum. □

Corollary 5.3.7. *With notation in Corollary 5.3.6, the number*

$$\frac{|\{(f, f_1, f_2) \in \mathcal{F}_{(n,n_1,n_2)} : \chi(f(x_i)f_1(x_i)) = e_i^1,\ \chi(f(x_i)f_2(x_i)) = e_i^2,\ \chi(f_1(x_i)f_2(x_i)) = e_i,\ 1 \leqslant i \leqslant l\}|}{|\mathcal{F}_{(n,n_1,n_2)}|},$$

where $e_i^1, e_i^2, e_i \in \{-1, 0, 1\}$, $\chi(f(x_i)^2)e_i = e_i^1 e_i^2$, and exactly $2m$ of them are equal to zero, is equal to

$$C_m^l = \left(\frac{q-1}{2}\right)^m \left(\frac{q-1}{2}\right)^{2(l-m)} \left(\frac{1}{(q-1)(q+3)}\right)^m \left(\frac{q}{(q-1)^2(q+3)}\right)^{l-m}\left(1 + O(q^{-\frac{(1-\epsilon)}{2}min(n,n_1,n_2)+l})\right) =$$

$$= \left(\frac{1}{2(q+3)}\right)^m \left(\frac{q}{4(q+3)}\right)^{q-m}\left(1 + O(q^{-\frac{(1-\epsilon)}{2}min(n,n_1,n_2)+l})\right).$$

Corollary 5.3.8. *Let $0 \leqslant l \leqslant q$, let $x_1, ..., x_l$ be distinct elements of $\mathbb{P}^1(\mathbb{F}_q)$, and let $e_i^1, e_i^2, e_i \in \{-1, 0, 1\}$ be such that $\chi(f(x_i)^2)e_i = e_i^1 e_i^2$, and exactly $2m$ of them are equal to zero. Then*

$$\frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n,n_1,n_2]} : \chi(f(x_i)f_1(x_i)) = e_i^1,\ \chi(f(x_i)f_2(x_i)) = e_i^2,\ \chi(f_1(x_i)f_2(x_i)) = e_i\}|}{|\widehat{\mathcal{F}}_{[n,n_1,n_2]}|}$$

is also equal to the number C_m^l defined in Corollary 5.3.7.

Proof. Distinguish the case in which some x_j is the point at infinity or not. Generalize Corollary 5.3.7 for the sets $\widehat{\mathcal{F}}_{(n,n_1,n_2)}$ looking at the symmetry observed in Remark 5.2.7, and add for the different components of $\widehat{\mathcal{F}}_{[n,n_1,n_2]}$. □

Proof. (of Theorem 5.3.1) Apply Corollary 5.3.8 in order to compute

$$\frac{|\{(f, f_1, f_2) \in \widehat{\mathcal{F}}_{[n,n_1,n_2]} : \widehat{S}(f, f_1, f_2) = M|}{|\widehat{\mathcal{F}}_{[n,n_1,n_2]}|} =$$

$$= \sum_{(E_1,...,E_{q+1}) \in \{-1,1,3\},\, \sum E_i = M} \sum_{j=0}^{N_{-1}} \binom{N_{-1}}{j} 3^{N_1+N_{-1}} C_{N_1+j} =$$

$$= \sum_{(E_1,...,E_{q+1}) \in \{-1,1,3\},\, \sum E_i = M} \left(\frac{6}{4}\frac{1}{q+3}\right)^{N_1} \left(\frac{3}{4}\frac{q+2}{q+3}\right)^{N_{-1}} \left(\frac{1}{4}\frac{q}{q+3}\right)^{N_3} \left(1 + O(q^{-\frac{(1-\epsilon)}{2}\min(n,n_1,n_2)+q})\right)$$

$$= \text{Prob}\left(\sum_1^{q+1} X_i = M\right) \left(1 + O(q^{-\frac{(1-\epsilon)}{2}\min(n,n_1,n_2)+q})\right),$$

where we use the notation N_i for the number of elements equal to i in the vectors $(E_1, ..., E_{q+1})$. □

Chapter 6

Traces of High Powers of the Frobenius Class in the family of Biquadratic Curves

6.1 Introduction

In Section 4.3 we saw that, for any curve of genus g over a finite field $\mathbb{F}_q$, the number of points in C is given by

$$\#C(\mathbb{F}_q) - (q+1) = \sum_{j=1}^{2g} \alpha_j(C) = q^{1/2} \operatorname{tr} \Theta_C$$

where Θ_C is a $2g \times 2g$ unitary matrix (called Unitarized Frobenius Class of C) with eigenvalues $q^{-1/2}\alpha_j(C) = e^{i\theta_j(C)}$, $j = 1, \ldots, 2g$.

So, given the relation above, we can do statistics about $\#C(\mathbb{F}_q)$ in some family of curves $\mathcal{F}$ just doing statistics on $\operatorname{tr} \Theta_C$ with $C \in \mathcal{F}$ in some group of matrices, related to the the same family. To do this, we have many tools about distributions in group of matrices. One of the most important books about the Random Matrix Theory related to this kind of problems is [KS99].

One important fact that must be taken in account in order to make statistics on families of curves is the correspondence between a smooth projective curve over $\mathbb{F}_q$ and its function field, that is a finite extension of $\mathbb{F}_q(t)$. This correspondence is explained in Section 5.2 of this thesis and allows one to use Number Theory of Function Fields. For a wide introduction to this topic, we refer the reader to [Ros02], from which we briefly recalled in chapter 4 the results we are going to use. Among them, the Prime Polynomial Theorem will be consistently used in the following sections. It says that, if a_n denotes the number of monic irreducible polynomials in $F_q[t]$ of degree n, then

$$a_n = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Let $\mathcal{H}_{2g+1}$ be the family of hyperelliptic curves C_Q defined by the equation $y^2 = Q(x)$ with $Q \in \mathbb{F}_q[x]$ monic, square-free and with $\deg Q = 2g+1$. Given a function on the family, we denote with the angle brackets $\langle \cdot \rangle$ its average.

In this chapter we want to mimic the following result of Rudnick:

Theorem (Theorem 1, [Rud10])**.** *Consider the curves $C_Q \in \mathcal{H}_{2g+1}$. For all $n > 0$ we have*

$$\langle \operatorname{tr} \Theta_Q^n \rangle = \left\{ \begin{array}{ll} -\eta_n & 0 < n < 2g \\ -1 - \frac{1}{q-1} & n = 2g \\ 0 & n > 2g \end{array} \right\} + \eta_n \frac{1}{q^{n/2}} \sum_{\deg P | \frac{n}{2}} \frac{\deg P}{|P|+1} + O_q(nq^{n/2-2g} + gq^{-g})$$

where the function

$$\eta_n = \left\{ \begin{array}{ll} 1 & n \text{ even} \\ 0 & n \text{ odd} \end{array} \right.$$

and the sum is over monic irreducible polynomials ($|P| = q^{\deg P}$).

Instead, we consider the family $\mathcal{H}_{2g+2}$ of curves C_h defined by the equation $y^2 = h(x)$ with $h \in \mathbb{F}_q[x]$ monic, square-free and with $\deg h = 2g + 2$. We will prove:

Theorem 6.1.1. *Let $C_h \in \mathcal{H}_{2g+2}$. For all $n > 0$ we have*

$$\langle \operatorname{tr} \Theta_h^n \rangle = \left\{ \begin{array}{ll} -\frac{1}{q^{n/2}} - \eta_n & 0 < n < 2g+1 \\ \frac{q^{1/2}}{q-1} & n = 2g+1 \\ 0 & n > 2g+1 \end{array} \right\} + \eta_n \frac{1}{q^{n/2}} \sum_{\deg P | \frac{n}{2}} \frac{\deg P}{|P|+1} + O_q(nq^{n/2-2g} + gq^{-g})$$

From this theorem, the next result will easily follow:

Corollary 6.1.2. *Let $C_h \in \mathcal{H}_{2g+2}$. With the same notation as above, if n is sufficiently large, we have*

$$\langle \operatorname{tr} \Theta_h^n \rangle = \left\{ \begin{array}{ll} -\eta_n & 7 \log_q g < n < 2g+1 \\ \frac{q^{1/2}}{q-1} & n = 2g+1 \\ 0 & 2g+4 \leqslant n \leqslant 4g - 10 \log_q g \end{array} \right\} + o(\frac{1}{g}).$$

In the proof, we will use the methods used by Rudnick in his paper, but it will be often necessary to prove new formulas and lemmas. In this sense, Proposition 6.3.1 is a new result. We keep the titles of sections in [Rud10], to let the reader easily find the counterpart, for $\mathcal{H}_{2g+1}$, of the results we prove.

In the last two sections of the chapter, we will try to extend these results to a given family of biquadratic curves (see Sections 5.2 and 6.5 for definition and properties of such curves). The work is in progress, so we still do not have a final result, but we believe that this path is going in the right direction.

For an introduction about quadratic L-functions we refer the reader to sections 1 and 2 in [Rud10]. However, we will recall the content of these sections if needed.

6.2 The family $\mathcal{H}_{2g+2}$ of hyperelliptic curves

We want to study statistics on hyperelliptic curves of the form

$$C_h : \ y^2 = h(x)$$

where h is a square-free, monic polynomial in $\mathbb{F}_q[x]$ of degree $2g+2$ ($q = p^n$ with p odd prime number). So, C_h is a non–singular curve of genus g over $\mathbb{F}_q$.

We denote the family of such curves as $\mathcal{H}_{2g+2}$, and we introduce the uniform probability on it, so we can talk about ensemble when we refer to this family. With abuse of notation, we will write $h \in \mathcal{H}_{2g+2}$ instead of $C_h \in \mathcal{H}_{2g+2}$.

Given a function $\mathscr{F}$ on $\mathcal{H}_{2g+2}$, we define its expected value as

$$\langle \mathscr{F} \rangle := \frac{1}{\#\mathcal{H}_{2g+2}} \sum_{h \in \mathcal{H}_{2g+2}} \mathscr{F}(h).$$

6.2.1 Averaging over $\mathcal{H}_{2g+2}$

We already saw that

$$\#\mathcal{H}_{2g+2} = \left(1 - \frac{1}{q}\right) q^{2g+2} = (q-1)q^{2g+1}.$$

We define the (polynomial version of the) *Möbius function* μ as

$$\mu(A) = \begin{cases} 0 & \text{if } A \text{ is not square-free} \\ (-1)^r & \text{if } A = P_1 \dots P_r \text{ with } P_i \text{ irreducible } \forall i \end{cases}.$$

Given this definition, we can observe that

$$\sum_{A^2 | h} \mu(A) = \begin{cases} 1 & h \text{ is square–free} \\ 0 & \text{otherwise} \end{cases}$$

So, if we have to compute the expected value of a function $\mathscr{F}$ on $\mathcal{H}_{2g+2}$, we obtain

$$\langle \mathscr{F} \rangle = \frac{1}{(q-1)q^{2g+1}} \sum_{2\alpha+\beta=2g+2} \sum_{\deg B = \beta} \sum_{\deg A = \alpha} \mu(A) \mathscr{F}(A^2 B)$$

the sum over all monic A, B.

6.2.2 Averaging quadratic characters

We have the following quadratic character

$$\chi_h(f) = \left(\frac{h}{f}\right).$$

From this, we can get

$$\chi_{A^2 B}(f) = \left(\frac{B}{f}\right)\left(\frac{A}{f}\right)^2 = \begin{cases} \left(\frac{B}{f}\right) & \gcd(A, f) = 1 \\ 0 & \text{otherwise} \end{cases}.$$

As a consequence, we obtain

$$\langle \chi_h(f) \rangle = \frac{1}{(q-1)q^{2g+1}} \sum_{2\alpha+\beta=2g+2} \sigma(f;\alpha) \sum_{\deg B = \beta} \left(\frac{B}{f}\right)$$

where

$$\sigma(f;\alpha) := \sum_{\substack{\deg A=\alpha \\ \gcd(A,f)=1}} \mu(A).$$

6.2.3 A sum of Möbius values

If P is a prime polynomial of degree n, $k \geqslant 1$, $\alpha \geqslant 0$, we define

$$\sigma_n(\alpha) := \sigma(P^k;\alpha) = \sum_{\substack{\deg A=\alpha \\ \gcd(A,P^k)=1}} \mu(A).$$

We can see that this quantity is independent of k.

Lemma 4 of [Rud10] states the following properties about the sums $\sigma_n(\alpha)$:

i) For $n = 1$,

$$\sigma_1(0) = 1, \sigma_1(\alpha) = 1 - q \text{ for all } \alpha \geqslant 1.$$

ii) If $n \geqslant 2$ then

$$\sigma_n(\alpha) = \begin{cases} 1 & \alpha \equiv 0 \mod n \\ -q & \alpha \equiv 1 \mod n \\ 0 & \text{otherwise} \end{cases}$$

6.2.4 The probability that $P \nmid h$

We can see that the shape of Lemma 5 of [Rud10] can be imitated for the family $\mathcal{H}_{2g+2}$, but we check the proof, that is slightly different as the degree of h is even.

Lemma 6.2.1. *f P is a prime polynomial, then*

$$\langle \chi_h(P^2) \rangle = \frac{|P|}{|P|+1} + O(q^{-2g})$$

Proof. If we define

$$\iota_P(f) := \begin{cases} 1, & P \nmid f \\ 0, & P \mid f \end{cases}$$

then we have

$$\langle \chi_h(P^2) \rangle = \langle \iota_P \rangle = \frac{1}{(q-1)q^{2g+1}} \sum_{\deg A^2B=2g+2} \mu(A)\iota_P(A^2B)$$

$$\langle \chi_h(P^2) \rangle = \frac{1}{(q-1)q^{2g+1}} \sum_{0\leqslant\alpha\leqslant g+1} \sum_{\substack{\deg A=\alpha \\ P\nmid A}} \mu(A) \sum_{\substack{\deg B=2g+2-2\alpha \\ P\nmid B}} 1$$

Writing $m := \deg P$, we obtain

$$\#\{B : \deg B = \beta \quad P \nmid B\} = q^\beta \cdot \begin{cases} 1 & \text{if } m > \beta \\ 1 - \frac{1}{|P|} & \text{if } m \leqslant \beta \end{cases}$$

and

$$\sum_{\substack{\deg A=\alpha \\ P\nmid A}} \mu(A) = \sigma_m(A).$$

At this point

$$\begin{aligned}\langle \chi_h(P^2)\rangle &= \frac{1}{(q-1)q^{2g+1}} \sum_{0\leqslant\alpha\leqslant g+1} \sigma_m(\alpha) q^{2g+2-2\alpha} \cdot \begin{cases} 1-\frac{1}{|P|} & \text{if } 0\leqslant\alpha\leqslant g+1-\frac{m}{2} \\ 1 & \text{if } g+1-\frac{m}{2}<\alpha\leqslant g+1 \end{cases} \\ &= \frac{q}{q-1}\left(\sum_{\alpha=0}^{\infty}\frac{\sigma_m(\alpha)}{q^{2\alpha}} + O(q^{-2g})\right)\left(1-\frac{1}{|P|}\right)\end{aligned}$$

So we have the statement. □

6.2.5 Double character sums

We define

$$S(\beta;n) := \sum_{\substack{\deg P=n \\ P \text{ prime}}} \sum_{\substack{\deg B=\beta \\ B \text{ monic}}} \left(\frac{B}{P}\right).$$

We know from Lemma 6 of [Rud10] that if $n \leqslant \beta$ then $S(\beta;n)=0$.

Moreover, Lemma 8 says that for even β one has

$$S(\beta;n) = \frac{q^{n+\beta/2}}{n} + O\left(\frac{\beta}{n}q^{n/2+\beta}\right). \tag{6.1}$$

6.3 Proof of Theorem 6.1.1

Formula (2.4) of Section 2 of [Rud10], for h of even degree, is

$$\operatorname{tr}\Theta_h^n = -\frac{1}{q^{n/2}} - \frac{1}{q^{n/2}} \sum_{\deg f=n} \Lambda(f)\chi_h(f)$$

The presence of $\Lambda(f)$ means that the sum is over all monic prime powers.

6.3.1 Contribution of squares

If n is odd we have no contribution of squares. If n even, we have

$$\langle \square_n \rangle = -1 - \frac{1}{q^{n/2}} + O(\frac{n}{q^{n/2}}) + O(q^{-2g})$$

but

$$\frac{1}{q^{n/2}} = O(\frac{n}{q^{n/2}})$$

so this brings to the same result of [Rud10], that is

$$\langle \square_n \rangle = -1 + O(\frac{n}{q^{n/2}}) + O(q^{-2g}).$$

So, considering both parities of n, when $n > 3\log_q g$ the contribution of squares is

$$\langle \square_n \rangle = -\eta_n(1 + o(\frac{1}{g})).$$

6.3.2 Contribution of primes

We see that

$$\mathcal{P}_n = -\frac{1}{q^{n/2}} - \frac{n}{q^{n/2}} \sum_{\deg P = n} \chi_h(P).$$

We use the formula of subsection 6.2.2 in order to find that

$$\langle \mathcal{P}_n \rangle = -\frac{1}{q^{n/2}} - \frac{n}{q^{n/2}} \cdot \frac{1}{(q-1)q^{2g+1}} \sum_{\deg P = n} \sum_{\substack{2\alpha+\beta=2g+2 \\ \alpha,\beta \geqslant 0}} \sigma_n(\alpha) \sum_{\deg B = \beta} \left(\frac{B}{P}\right)$$

from which we can deduce

$$\langle \mathcal{P}_n \rangle = -\frac{1}{q^{n/2}} - \frac{n}{(q-1)q^{2g+1+n/2}} \sum_{\substack{2\alpha+\beta=2g+2 \\ \alpha,\beta \geqslant 0}} \sigma_n(\alpha) S(\beta; n) \tag{6.2}$$

Let us now assume $n > g+1$. Then $\sigma_n(\alpha) \neq 0 \Rightarrow \alpha \equiv 0, 1 \mod n$, but since $\alpha \leqslant g+1 < n$ this implies $\alpha = 0, 1$. So, if $n > g+1$

$$\langle \mathcal{P}_n \rangle = -\frac{1}{q^{n/2}} - \frac{n}{(q-1)q^{2g+1+n/2}} (S(2g+2; n) - qS(2g; n)) \tag{6.3}$$

This last two formulas will be very useful in the next section.

6.3.3 Bounding the contribution of primes

Consider first the case $n \leqslant g+1$. In formula (6.2) if $S(\beta; n) \neq 0$ then $\beta < n$ (Lemma 6). For those terms, we use the bound given in Lemma 8 when β is even, that is

$$|S(\beta; n)| \ll \frac{q^{n+\frac{\beta}{2}}}{n}$$

so, if we also use the fact that $\sigma_n(\alpha) \leqslant 1$ for all $n \geqslant 0$ and $\alpha \geqslant 0$, we obtain

$$\langle \mathcal{P}_n \rangle = -\frac{1}{q^{n/2}} + O\left(\frac{n}{q^{2g+1+n/2}} \sum_{\beta < n} \frac{q^{n+\beta/2}}{n}\right)$$

where we were allowed to cancel the term $\frac{1}{q-1}$ because the absolute value of $\frac{\sigma_n(\alpha)}{q-1}$ is limited. So

$$\begin{aligned}\langle \mathcal{P}_n \rangle &= -\frac{1}{q^{n/2}} + O\left(\frac{n}{q^{2g+1+n/2}} \cdot \frac{q^n}{n} \sum_{\beta<n} q^{\beta/2}\right) \\ &= -\frac{1}{q^{n/2}} + O\left(q^{n/2-2g-1} \cdot \frac{q^{n/2}-1}{q-1}\right) \\ &= -\frac{1}{q^{n/2}} + O\left(\frac{q^{n-2g-1}}{q-1}\right) \\ &= -\frac{1}{q^{n/2}} + O\left(q^{n-2g-1}\right).\end{aligned}$$

But $n \leqslant g+1$, so the error term tends to 0 if g tends to ∞. So we have

$$n \leqslant g+1 \text{ and } g \to \infty \quad \Longrightarrow \quad \langle \mathcal{P}_n \rangle = -\frac{1}{q^{n/2}} + o(1).$$

Moreover, if $n > 3\log_q g$, we get $\langle \mathcal{P}_n \rangle = o\left(\frac{1}{g}\right)$ when $g \to \infty$.

For the case $g+1 < n < 2g+1$, we use formula (6.3) and we know that

$$S(2g+2;n) = S(2g;n) = 0.$$

Then

$$\langle \mathcal{P}_n \rangle = -\frac{1}{q^{n/2}} \quad \text{if } g+1 < n < 2g+1$$

(note that it tends to 0 if g tends to ∞).

If $n = 2g+1$, then $S(2g+2;n) = 0$ and from formula (4.2) of Proposition 7 in [Rud10] we know

$$S(2g;2g+1) = \pi_q(2g+1)q^g.$$

So, by using formula (6.3)

$$\begin{aligned}\langle \mathcal{P}_n \rangle = \langle \mathcal{P}_{2g+1} \rangle &= -\frac{1}{q^{\frac{2g+1}{2}}} - \frac{2g+1}{(q-1)q^{3g+3/2}} \left(-q\pi_q(2g+1)q^g\right) \\ &= -\frac{1}{q^{\frac{2g+1}{2}}} + \frac{2g+1}{(q-1)q^{2g+1/2}} \pi_q(2g+1) \\ &= -\frac{1}{q^{\frac{2g+1}{2}}} + \frac{2g+1}{(q-1)q^{2g+1/2}} \cdot \frac{q^{2g+1}}{2g+1} + O\left(\frac{2g+1}{(q-1)q^g}\right) \\ &= -\frac{1}{q^{\frac{2g+1}{2}}} + \frac{q^{1/2}}{q-1} + O\left(gq^{-g}\right) \\ &= \frac{q^{1/2}}{q-1} + O\left(gq^{-g}\right)\end{aligned}$$

In case $n > 2g+1$, we have

$$\langle \mathcal{P}_n \rangle = -\frac{1}{q^{n/2}} - \frac{n}{(q-1)q^{2g+1+n/2}} \cdot \left(S(2g+2;n) - qS(2g;n)\right) \tag{6.4}$$

Next estimate is crucial to bound the contribution of primes for $n > 2g+1$.

Proposition 6.3.1. *If β is even and $0 \leqslant \beta < n \leqslant 2\beta + 2$ then*

$$S(\beta; n) = \pi_q(n) q^{\frac{\beta}{2}} (1 - \eta_n q^{\frac{\beta}{2} - \frac{n}{2}}) + O(q^n) \tag{6.5}$$

where $\eta_n = 1$ for n even and $\eta_n = 0$ for n odd.

Proof. First, let us consider the case in which n is even. We know, from Proposition 7 of [Rud10], that, if n is even and $1 \leqslant \beta \leqslant n - 2$, then

$$S(\beta; n) = q^{\beta - \frac{n}{2}} \left(-S(n - 1 - \beta; n) + (q - 1) \sum_{j=0}^{n-\beta-2} S(j; n) \right). \tag{6.6}$$

We note that in this case $n - 1 - \beta$ is odd and, using lemma 8 of [Rud10], we have

$$S(n - 1 - \beta; n) \ll \frac{n - 1 - \beta}{n} q^{\frac{3}{2}n - 1 - \beta} \ll q^{\frac{3}{2}n - 1 - \beta}.$$

Now, we need an estimate for

$$(q - 1) \sum_{j=0}^{n-\beta-2} S(j; n).$$

In order to do this, we split the sum in the following way:

$$\sum_{j=0}^{n-\beta-2} S(j; n) = \sum_{\substack{j=1 \\ j \text{ odd}}}^{n-\beta-3} S(j; n) + \sum_{\substack{j=0 \\ j \text{ even}}}^{n-\beta-2} S(j; n).$$

We have (again by lemma 8 of [Rud10])

$$\begin{aligned}
\sum_{\substack{j=1 \\ j \text{ odd}}}^{n-\beta-3} S(j; n) &= \sum_{k=0}^{\frac{n}{2} - \frac{\beta}{2} - 2} S(2k + 1; n) \\
&\ll \sum_{k=0}^{\frac{n}{2} - \frac{\beta}{2} - 2} \frac{2k + 1}{n} q^{\frac{n}{2} + 2k + 1} \\
&\ll \frac{n - \beta - 3}{n} q^{\frac{n}{2} + 1} \sum_{k=0}^{\frac{n}{2} - \frac{\beta}{2} - 2} q^{2k} \\
&= \frac{n - \beta - 3}{n} q^{\frac{n}{2} + 1} \frac{q^{n - \beta - 2} - 1}{q^2 - 1} \\
&\ll \frac{q^{\frac{3}{2}n - \beta - 1}}{q^2 - 1}
\end{aligned}$$

while for the other term

$$\begin{aligned}
\sum_{\substack{j=0\\ j \text{ even}}}^{n-\beta-2} S(j;n) &= \sum_{k=0}^{\frac{n}{2}-\frac{\beta}{2}-1} S(2k;n) \\
&= \sum_{k=0}^{\frac{n}{2}-\frac{\beta}{2}-1} \left(\pi_q(n) q^k + O(\frac{2k}{n} q^{\frac{n}{2}+2k}) \right) \\
&= \pi_q(n) \sum_{k=0}^{\frac{n}{2}-\frac{\beta}{2}-1} q^k + O\left(\sum_{k=0}^{\frac{n}{2}-g-2} \frac{n-\beta-2}{n} q^{\frac{n}{2}} \cdot q^{2k} \right) \\
&= \pi_q(n) \frac{q^{\frac{n}{2}-\frac{\beta}{2}}-1}{q-1} + O\left(\frac{n-\beta-2}{n} q^{\frac{n}{2}} \cdot \frac{q^{n-\beta}-1}{q^2-1} \right) \\
&= \pi_q(n) \frac{q^{\frac{n}{2}-\frac{\beta}{2}}-1}{q-1} + O\left(\frac{q^{\frac{3}{2}n-\beta}}{q^2-1} \right)
\end{aligned}$$

So, we obtain that

$$\begin{aligned}
S(\beta;n) &= q^{\beta-\frac{n}{2}} \left(O(q^{\frac{3}{2}n-1-\beta}) + O(\frac{q^{\frac{3}{2}n-1-\beta}}{q+1}) + \pi_q(n)(q^{\frac{n}{2}-\frac{\beta}{2}}-1) + O(\frac{q^{\frac{3}{2}n-\beta}}{q+1}) \right) \\
&= q^{\beta-\frac{n}{2}} \left(\pi_q(n)(q^{\frac{n}{2}-\frac{\beta}{2}}-1) + O(\frac{q^{\frac{3}{2}n-\beta}}{q+1}) \right) \\
&= \pi_q(n) q^{\frac{\beta}{2}} (1 - q^{\frac{\beta}{2}-\frac{n}{2}}) + O(q^n) \qquad (6.7)
\end{aligned}$$

Let us now consider the case in which n is odd. We know, from Proposition 7 of [Rud10] that, if β is even, n is odd and $0 \leqslant \beta \leqslant n-1$, then

$$S(\beta;n) = q^{\beta-\frac{n-1}{2}} S(n-1-\beta;n).$$

In this case $n-1-\beta$ is even, so

$$\begin{aligned}
S(\beta;n) &= q^{\beta-\frac{n-1}{2}} \left(\pi_q(n) q^{\frac{n-1-\beta}{2}} + O(\frac{n-1-\beta}{n} q^{\frac{n}{2}+n-1-\beta}) \right) \\
&= q^{\frac{\beta}{2}} \pi_q(n) + O\left(\frac{n-1-\beta}{n} q^{n-\frac{1}{2}} \right) \\
&= q^{\frac{\beta}{2}} \pi_q(n) + O\left(q^n\right) \qquad (6.8)
\end{aligned}$$

If we put together formulas (6.7) and (6.8) we obtain the statement. □

Let us now consider formula (6.4) when n is odd. In this case, we can use Proposition 6.3.1 to see that

$$\begin{aligned}
S(2g+2;n) &= \pi_q(n) q^{g+1} + O(q^n) \\
S(2g;n) &= \pi_q(n) q^g + O(q^n).
\end{aligned}$$

So, if we insert these terms in (6.4), we have that the contribution of the main terms is

$$\pi_q(n)q^{g+1} - q\pi_q(n)q^g = 0$$

and then we get

$$\langle \mathcal{P}_n \rangle \ll \frac{n}{(q-1)q^{2g+\frac{n}{2}}} q^n \ll nq^{\frac{n}{2}-2g}.$$

We can conclude that if n is odd and $2g+4 \leqslant n < 4g - 10\log_q g$ this contribution goes to zero as $g \to \infty$.

In the case when n is even, we see that

$$S(2g+2;n) = \pi_q(n)q^{g+1}(1 - q^{g+1-\frac{n}{2}}) + O(q^n)$$

and

$$S(2g;n) = \pi_q(n)q^g(1 - q^{g-\frac{n}{2}}) + O(q^n).$$

Then

$$\begin{aligned} S(2g+2;n) - qS(2g;n) &= \pi_q(n)q^{g+1}(1 - q^{g+1-\frac{n}{2}}) + O(q^{n-1}) - \pi_q(n)q^{g+1}(1 - q^{g-\frac{n}{2}}) + O(q^n) \\ &= \pi_q(n)q^{g+1}(q^{g-\frac{n}{2}}(1-q)) + O(q^n) \\ &= \pi_q(n)q^{2g+1-\frac{n}{2}}(1-q) + O(q^n) \end{aligned}$$

So, if we collect all these estimates together, we obtain

$$\begin{aligned} \langle \mathcal{P}_n \rangle &= -\frac{1}{q^{n/2}} - \frac{n}{(q-1)q^{2g+1+n/2}} \left(S(2g+2;n) - qS(2g;n) \right) \\ &= -\frac{1}{q^{n/2}} - \frac{n}{(q-1)q^{2g+1+n/2}} \left(\pi_q(n)q^{2g+1-\frac{n}{2}}(1-q) + O(q^n) \right) \\ &= -\frac{1}{q^{n/2}} + \frac{n\pi_q(n)}{q^n} + O\left(\frac{nq^{\frac{n}{2}-2g-1}}{q-1} \right) \end{aligned}$$

and using the Prime Polynomial Theorem we get

$$\langle \mathcal{P}_n \rangle = -\frac{1}{q^{n/2}} + 1 + O\left(\frac{n}{q^{n/2}} \right) + O\left(\frac{nq^{\frac{n}{2}-2g-1}}{q-1} \right).$$

But $-\frac{1}{q^{n/2}} = O\left(\frac{n}{q^{n/2}}\right)$ and the error terms go to zero when g tends to infinity (we recall that we are in the case $n > 2g$). So, in the limit when $g \to \infty$ when n is even, we have

$$\langle \mathcal{P}_n \rangle = 1 + o\left(\frac{1}{g}\right).$$

Finally, we can conclude that the contribution of primes in the case $2g+4 \leqslant n \leqslant 4g-10\log_q g$ is

$$\langle \mathcal{P}_n \rangle = \eta_n + o\left(\frac{1}{g}\right)$$

in the limit when g goes to infinity.

6.3.4 The contribution of higher prime powers

For the family $\mathcal{H}_{2g+2}$, we can easily see that the contribution of odd powers of primes P^d, with $d > 1$ odd, $\deg P^d = n$, is

$$\mathbb{H}_n = -\frac{1}{q^{\frac{n}{2}}} \left(1 + \sum_{\substack{d|n \\ 3 \leqslant d \text{ odd}}} \sum_{\deg P = \frac{n}{d}} \frac{n}{d} \chi_h(P^d) \right).$$

Since d is odd, $|\chi_h(P^d)| = |\chi_h(P)|$ and we use the simple bound $|\chi_h(P)| \leqslant 1$. In this way we have

$$\begin{aligned} \mathbb{H}_n &\ll \frac{1}{q^{\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leqslant d \text{ odd}}} \frac{n}{d} \pi_q(\frac{n}{d}) \\ &\ll \frac{1}{q^{\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leqslant d \text{ odd}}} q^{\frac{n}{d}} \\ &\ll \frac{n q^{\frac{n}{3}}}{q^{\frac{n}{2}}} \\ &= n q^{-\frac{n}{6}}. \end{aligned}$$

Then $|\mathbb{H}_n|$ is negligible when n goes to infinity and so it is the average $\langle \mathbb{H}_n \rangle$. This is the case when $n > \log_q g$ and $g \to \infty$. In particular we have $\mathbb{H}_n = o(\frac{1}{g})$ if $n > 7 \log_q g$.

6.3.5 Conclusion of the proof

We saw that

$$\langle \operatorname{tr} \Theta_h^n \rangle = \langle \square_n \rangle + \langle \mathcal{P}_n \rangle + \langle \mathbb{H}_n \rangle$$

and we computed the contribution of the each single term. These are:

$$\langle \square_n \rangle = -\eta_n (1 + O(\frac{n}{q^{n/2}}) + O(q^{-2g})),$$

$$\langle \mathcal{P}_n \rangle = \begin{cases} -\frac{1}{q^{n/2}} + O(q^{-g}), & 0 < n < 2g+1 \\ \frac{q^{1/2}}{q-1} + O\left(g q^{-g}\right), & n = 2g+1 \\ \eta_n + O\left(n q^{\frac{n}{2} - 2g}\right), & 2g+1 < n \end{cases}$$

and

$$\langle \mathbb{H}_n \rangle = O(n q^{-\frac{n}{6}}).$$

The sum of the three contributions gives the statement of Theorem 6.1.1.

In particular, we have

$$\langle \operatorname{tr} \Theta_h^n \rangle = \left\{ \begin{array}{ll} -\eta_n & 7 \log_q g < n < 2g+1 \\ \frac{q^{1/2}}{q-1} & n = 2g+1 \\ 0 & 2g+4 \leqslant n \leqslant 4g - 10 \log_q g \end{array} \right\} + o(\frac{1}{g}).$$

that gives Corollary 6.1.2.

6.4 The number of points of a biquadratic curve over $\mathbb{F}_{q^n}$

Let K denotes any function field over $\mathbb{F}_q$ and $\mathcal{S}_K$ the set of finite and infinite primes of K. Recall the definition of the zeta-function associated to K:

$$\zeta_K(s) := \sum_{F \in K} |F|^{-s} = \prod_{P \in \mathcal{S}_K} (1 - |P|^{-s})^{-1}. \tag{6.9}$$

We compute the quotient $\frac{\zeta_K(u)}{\zeta_k(u)}$, when K is a biquadratic function field of genus g (cf. Definition 5.2.1)

On one side, by Weil Theorem (Section 4.3), we know that

$$\zeta_K(s) = \frac{P_K(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})},$$

where $P_K(u) := \prod_{j=1}^{2g}(1 - \alpha_j u)$ is a degree $2g$ polynomial in $\mathbb{Z}[u]$, $\alpha_j := \sqrt{q}e^{i\theta_j(K)}$ for every $j = 1, \ldots, 2g$ and θ_K is the $2g \times 2g$ matrix representing the Frobenius class Frob_C of the biquadratic curve C associated to K.

It is well known that $\{\alpha_j\}_{j=1,\ldots,2g}$ are the eigenvalues of θ_K and so we have that

$$\operatorname{tr} \theta_K^n = q^{n/2} \sum_{j=1}^{2g} \alpha_j.$$

On the other side we can compute the quotient explicitly, using the Euler product of the zeta-functions, i.e.

$$\frac{\zeta_K(u)}{\zeta_k(u)} = \prod_{P \in S_{1111}} \frac{(1 - |P|^{-s})^{-4}}{(1 - |P|^{-s})^{-1}} \prod_{P \in S_{1^4}} \frac{(1 - |P|^{-s})^{-1}}{(1 - |P|^{-s})^{-1}} \prod_{P \in S_{1^2 1^2}} \frac{(1 - |P|^{-s})^{-2}}{(1 - |P|^{-s})^{-1}} \cdot$$
$$\cdot \prod_{P \in S_{22}} \frac{(1 - |P|^{-2s})^{-2}}{(1 - |P|^{-s})^{-1}} \prod_{P \in S_{2^2}} \frac{(1 - |P|^{-s2})^{-1}}{(1 - |P|^{-s})^{-1}} \tag{6.10}$$

where $\mathcal{S}_{****}$ is the subset of primes of $\mathcal{S}_k$ with a fixed ramification behavior (for example, a prime in S_{1111} is a prime that splits completely).

Denote by f_∞, r_∞ respectively the inertia degree and the number of primes appearing in the decomposition of the infinity prime of k inside the extension K. Then, after the usual change of variable $u = q^{-s}$, (6.10) can be written in the more elegant way using L-functions (cf. [Ros02, Chapter 4]):

$$\frac{\zeta_K(u)}{\zeta_k(u)} = \frac{(1 - u^{f_\infty})^{-r_\infty}}{1 - u} L(u, \chi_{K_1}) L(u, \chi_{K_2}) L(u, \chi_{K_1}\chi_{K_2}) \tag{6.11}$$

Taking logarithmic derivatives of both expressions (6.9) and (6.11), we obtain:

$$\begin{aligned}
&u\frac{d}{du}(\log L(u, \chi_{K_1}) + \log L(u, \chi_{K_2}) + \log L(u, \chi_{K_1}\chi_{K_2})) = \\
&= \sum_P \frac{\deg P \cdot \chi_{K_1}(P) u^{\deg P}}{1 - \chi_{K_2}(P) u^{\deg P}} + \sum_P \frac{\deg P \cdot \chi_{K_2}(P) u^{\deg P}}{1 - \chi_{K_2}(P) u^{\deg P}} + \sum_P \frac{\deg P \cdot \chi_{K_1}(P)\chi_{K_2}(P) u^{\deg P}}{1 - \chi_{K_1}(P)\chi_{K_2}(P) u^{\deg P}} = \\
&= \sum_{P \in S_k} \deg P \sum_{n=1}^{\infty} (\chi_{K_1}^n(P) + \chi_{K_2}^n(P) + \chi_{K_1}^n(P)\chi_{K_2}^n(P)) u^{n \cdot \deg P}
\end{aligned} \tag{6.12}$$

and

$$u\frac{d}{du}\log\left(\frac{1-u}{(1-u^{f_\infty})^{-r_\infty}}\right)+u\frac{d}{du}\sum_{j=1}^{2g}\log(1-\alpha_j u)=\frac{-r_\infty u^{f_\infty}}{1-u^{f_\infty}}-\frac{u}{1-u}+\sum_{j=1}^{2g}\frac{-\alpha_j u}{1-\alpha_j u}$$

So finally we have the following equality between power series:

$$\sum_{P\in S_k}\deg P\sum_{n=1}^{\infty}\left(\chi_{K_1}^n(P)+\chi_{K_2}^n(P)+\chi_{K_1}^n(P)\chi_{K_2}^n(P)\right)u^{n\deg P}=-r_\infty\sum_{n=1}^{\infty}u^{f_\infty n}-\sum_{n=1}^{\infty}u^n-\sum_{j=1}^{2g}\sum_{n=1}^{\infty}\alpha_j^n u^n \tag{6.13}$$

Equaling the n-th coefficients of the series, we reach the following formula for n-th powers of the Frobenius:

$$\begin{aligned}-q^{n/2}\operatorname{tr}\theta_K^n=-\sum_{j=1}^{2g(K)}\alpha_j^n=\\ =\sum_{\deg P|n}\deg P\cdot\left(\chi_{K_1}^{n/\deg P}(P)+\chi_{K_2}^{n/\deg P}(P)+\chi_{K_1}^{n/\deg P}(P)\chi_{K_2}^{n/\deg P}(P)\right)+r_\infty+1.\end{aligned}$$

We just proved the following fact:

Proposition 6.4.1. *Let K be a biquadratic extension and let K_1, K_2, K_3 be the three quadratic subextensions of K. Let denote by χ_{K_i} the quadratic Dirichlet character associated to the extension K_i.*

Then, for every integer $n \geqslant 2$, the trace of the n-th power of the Frobenius θ_K satisfies the following relation:

$$\begin{aligned}-q^{n/2}\operatorname{tr}\theta_K^n=r_\infty+1+&\sum_{\deg F=n}\Lambda(F)\chi_{K_1}(F)\\ &+\sum_{\deg F=n}\Lambda(F)\chi_{K_2}(F)\\ &+\sum_{\deg F=n}\Lambda(F)\chi_{K_1}(F)\chi_{K_2}(F)\end{aligned}$$

where Λ denotes the von Mangoldt function

$$\Lambda(F):=\begin{cases}\deg P & if\ F=P^k\\ 0 & otherwise\end{cases}$$

Thanks to this formula we can start to compute the average $<\operatorname{tr}\theta_K^n>$ on a given family of biquadratic curves, asymptotically for $g\to\infty$.

6.5 The family $\mathcal{B}_{d_1,d_2}$ of biquadratic curves

In this section we introduce families of biquadratic curves on which it is quite natural to compute the average of the traces of the Frobenius classes.

Let $\mathcal{B}_{d_1,d_2}$ be the family of biquadratic curves over $\mathbb{F}_q$ whose affine model is given by equations

$$C_{h_1,h_2} : \begin{cases} y_1^2 = h_1(t) \\ y_2^2 = h_2(t) \end{cases}$$

with h_1, h_2 monic square-free polynomials over $\mathbb{F}_q$ such that $\deg h_1 = d_1$, $\deg h_2 = d_2$ and $h_1 \neq h_2$. Remembering that the number of square-free monic polynomials of degree $d \geqslant 2$ over $\mathbb{F}_q$ is $(q-1)q^{d-1}$ we have that

$$\#\mathcal{B}_{d_1,d_2} = \frac{(q-1)^2 q^{d_1+d_2-2}}{1+\delta_{d_1 d_2}} - \delta_{d_1 d_2}\frac{(q-1)q^{d_1-1}}{2}$$

where δ_{d_1,d_2} is the Kronecker delta. So, in particular, if $d_1 \neq d_2$ we have

$$\#\mathcal{B}_{d_1,d_2} = (q-1)^2 q^{d_1+d_2-2} \tag{6.14}$$

6.5.1 The average of a function on $\mathcal{B}_{d_1,d_2}$

We can easily see that if a function $\mathscr{F}$ is defined on the family $\mathcal{B}_{d_1,d_2}$, then its average is computed by the following formula:

$$\langle \mathscr{F} \rangle := \frac{1}{\#\mathcal{B}_{d_1,d_2}} \sum_{C_{h_1,h_2} \in \mathcal{B}_{d_1,d_2}} \mathscr{F}(C_{h_1,h_2}).$$

With the same arguments used in [Rud10, Section 3.1] we see that

$$\langle \mathscr{F} \rangle = \frac{1}{\#\mathcal{B}_{d_1,d_2}} \sum_{2\alpha_1+\beta_1=d_1} \sum_{2\alpha_2+\beta_2=d_2} \sum_{\deg B_1=\beta_1} \sum_{\deg B_2=\beta_2} \sum_{\deg A_1=\alpha_1} \sum_{\deg A_2=\alpha_2} \mu(A_1)\mu(A_2)\mathscr{F}(C_{A_1^2B_1,A_2^2B_2}) \tag{6.15}$$

We will see that when $\mathscr{F}(C_{h_1,h_2}) = \operatorname{tr}\theta^n_{C_{h_1,h_2}}$ the previous formula will simplify significantly.

6.6 Average of Traces of High Powers of the Frobenius Class in the family $\mathcal{B}_{2g_1+2,2g_2+2}$

We want to generalize Theorem 1 of [Rud10] to a given family of biquadratic extensions. To do this, we will use also Theorem 6.1.1 that we proved in Section 6.3.

From Proposition 6.4.1 we know that

$$\begin{aligned} \operatorname{tr}\theta_K^n = -\frac{r_\infty+1}{q^{n/2}} &- \frac{1}{q^{n/2}} \sum_{\deg F=n} \Lambda(F)\chi_{K_1}(F) \\ &- \frac{1}{q^{n/2}} \sum_{\deg F=n} \Lambda(F)\chi_{K_2}(F) \\ &- \frac{1}{q^{n/2}} \sum_{\deg F=n} \Lambda(F)\chi_{K_1}(F)\chi_{K_2}(F) \end{aligned}$$

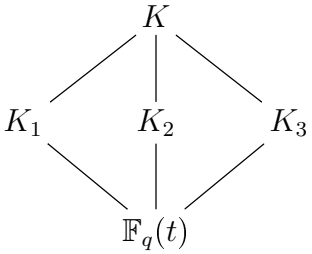
where the sum is over all prime powers because of the presence of Λ.

We use again the same idea of Rudnick and we split the sum in three contributions (plus a constant term) as follows

$$\operatorname{tr}\theta_K^n = -\frac{r_\infty+1}{q^{n/2}} + \mathcal{P}_{K,n} + \square_{K,n} + \mathbb{H}_{K,n}.$$

In the right hand side, $\frac{r_\infty+1}{q^{n/2}}$ is the constant term given by Proposition 6.4.1, $\mathcal{P}_{K,n}$ is the contribution of primes, $\square_{K,n}$ is the contribution of squares and $\mathbb{H}_{K,n}$ is the contribution of odd prime powers.

Remember that K is the function field of a biquadratic curve C_{h_1,h_2} as we defined it in Section 6.5, so we have:



The three subextensions of K are defined respectively by $K_1 : y^2 = h_1(t)$, $K_2 : y^2 = h_2(t)$ and $K_3 : y^2 = h_3(t) = f_1(t)f_2(t)$, following the notation of Theorem 5.2.4.

We can see that that at least one of the three subextensions of K is defined by a polynomial of even degree, so, for simplicity, we compute the average of $\operatorname{tr}\theta_K^n$ in the family $\mathcal{B}_{2g_1+2,2g_2+2}$. The computations for odd degree hyperelliptic curves in the subextensions will be very similar. Of course, g_1 and g_2 will be the genera of the two hyperelliptic curves defining the function fields K_1 and K_2 respectively. Moreover, we will suppose that $g_1 < g_2$.

Contribution of squares

We compute first the contribution to the trace given by squares of prime powers. There is such a contribution only when n is even.

$$\square_{K,n} = -\frac{1}{q^{n/2}}\left(\sum_{\deg h=\frac{n}{2}}\Lambda(h)\chi_{K_1}(h^2) + \sum_{\deg h=\frac{n}{2}}\Lambda(h)\chi_{K_2}(h^2) + \sum_{\deg h=\frac{n}{2}}\Lambda(h)\chi_{K_1}(h^2)\chi_{K_2}(h^2)\right)$$

Now $\chi_{K_1}(h^2), \chi_{K_2}(h^2) = 0, 1$, and $r_\infty \geqslant 0$, so

$$\square_{K,n} \leqslant 0$$

and

$$\square_{K,n} \geqslant -\frac{3}{q^{n/2}}\sum_{\deg h=\frac{n}{2}}\Lambda(h) = -3,$$

the last equality coming from the fact that

$$\sum_{\deg f=n}\Lambda(f) = q^n.$$

This says that the contribution of squares is bounded.

We can consider separately the average of the three summands of $\square_{K,n}$. The first one is

$$\left\langle -\frac{1}{q^{n/2}} \sum_{\deg h=\frac{n}{2}} \Lambda(h)\chi_{K_1}(h^2) \right\rangle = -\frac{1}{q^{n/2}} \frac{1}{(q-1)^2 q^{2(g_1+g_2)+2}} \sum_{C\in\mathcal{B}_{2g_1+2,2g_2+2}} \sum_{\deg h=\frac{n}{2}} \Lambda(h)\chi_{K_1}(h^2)$$
$$= -\frac{1}{q^{n/2}} \frac{1}{(q-1)q^{2g_2+1}} \sum_{\deg h=\frac{n}{2}} \Lambda(h) \sum_{h_2\in\mathcal{H}_{2g_2+2}} \frac{1}{(q-1)q^{2g_1+1}} \sum_{h_1\in\mathcal{H}_{2g_1+2}} \chi_{K_1}(h^2)$$

So, by the results of subsection 6.3.1, if we let $h = P^k$ with P prime polynomial, we have

$$\left\langle -\frac{1}{q^{n/2}} \sum_{\deg h=\frac{n}{2}} \Lambda(h)\chi_{K_1}(h^2) \right\rangle = -1 + \sum_{\deg P|\frac{n}{2}} \frac{\deg(P)}{|P|+1} + O(q^{-2g_1})$$

With the same kind of computations, we also prove that

$$\left\langle -\frac{1}{q^{n/2}} \sum_{\deg h=\frac{n}{2}} \Lambda(h)\chi_{K_2}(h^2) \right\rangle = -1 + \sum_{\deg P|\frac{n}{2}} \frac{\deg(P)}{|P|+1} + O(q^{-2g_2}).$$

The last term contributing to $\langle \square_{K,n} \rangle$ is

$$\left\langle -\frac{1}{q^{n/2}} \sum_{\deg h=\frac{n}{2}} \Lambda(h)\chi_{K_1}(h^2)\chi_{K_2}(h^2) \right\rangle =$$

$$= -\frac{1}{(q-1)^2 q^{2(g_1+g_2)+2+\frac{n}{2}}} \sum_{C\in\mathcal{B}_{2g_1+2,2g_2+2}} \sum_{\deg h=\frac{n}{2}} \Lambda(h)\chi_{K_1}(h^2)\chi_{K_2}(h^2)$$
$$= -\sum_{\deg h=\frac{n}{2}} \Lambda(h) \frac{1}{(q-1)^2 q^{2(g_1+g_2)+2+\frac{n}{2}}} \sum_{h_1\in\mathcal{H}_{2g_1+2}} \sum_{h_2\in\mathcal{H}_{2g_2+2}} \chi_{K_1}(h^2)\chi_{K_2}(h^2)$$
$$= -\frac{1}{q^{n/2}} \sum_{\deg h=\frac{n}{2}} \Lambda(h) \frac{1}{(q-1)q^{2g_1+1}} \sum_{h_1\in\mathcal{H}_{2g_1+2}} \chi_{K_1}(h^2) \frac{1}{(q-1)q^{2g_2+1}} \sum_{h_2\in\mathcal{H}_{2g_2+2}} \chi_{K_2}(h^2)$$
$$= -\frac{1}{q^{n/2}} \sum_{\deg P|\frac{n}{2}} \Lambda(P) \left(1 - \frac{1}{|P|+1} + O(q^{-2g_1})\right) \left(1 - \frac{1}{|P|+1} + O(q^{-2g_2})\right)$$
$$= -\frac{1}{q^{n/2}} \sum_{\deg P|\frac{n}{2}} \Lambda(P) \left(1 - \frac{2}{|P|+1} + \frac{1}{(|P|+1)^2} + O(q^{-2g_1}) + O(q^{-2g_2})\right)$$
$$= -1 + \frac{2}{q^{n/2}} \sum_{\deg P|\frac{n}{2}} \frac{\deg(P)}{|P|+1} - \frac{1}{q^{n/2}} \sum_{\deg P|\frac{n}{2}} \frac{\deg(P)}{(|P|+1)^2} + O(q^{-2g_1}) + O(q^{-2g_2}).$$

So, when n is even,

$$\langle \square_{K,n} \rangle = -3 + \frac{4}{q^{n/2}} \sum_{\deg P|\frac{n}{2}} \frac{\deg(P)}{|P|+1} - \frac{1}{q^{n/2}} \sum_{\deg P|\frac{n}{2}} \frac{\deg(P)}{(|P|+1)^2} + O(q^{-2g_1}) + O(q^{-2g_2})$$

and we can easily bound these terms as

$$\langle \square_{K,n} \rangle = -3 + O(\frac{n}{q^{n/2}}) + O(q^{-2g_1}) + O(q^{-2g_2}).$$

If we let g_1 and g_2 go to infinity, for $n \gg 3 \log_q g_2$ we have

$$\langle \square_{K,n} \rangle = -\eta_n \left(3 + o(\frac{1}{g}) \right)$$

Contribution of primes

We remind the reader that while we are averaging over the family $\mathcal{B}_{2g_1+1,2g_2+2}$ we always suppose $g_1 < g_2$.

The contribution of primes to $\operatorname{tr} \Theta_K^n$ is

$$\mathcal{P}_n = -\frac{n}{q^{n/2}} \left(\sum_{\deg P = n} \chi_{K_1}(P) + \sum_{\deg P = n} \chi_{K_2}(P) + \sum_{\deg P = n} \chi_{K_1}(P)\chi_{K_2}(P) \right).$$

We consider separately the three terms of this contribution, as we did before with the squares.

The first one is

$$\left\langle -\frac{n}{q^{n/2}} \sum_{\deg P = n} \chi_{K_1}(P) \right\rangle =$$

$$= -\frac{n}{q^{n/2}} \frac{1}{(q-1)^2 q^{2(g_1+g_2)+2}} \sum_{C \in \mathcal{B}_{2g_1+2,2g_2+2}} \sum_{\deg P = n} \chi_{K_1}(P)$$

$$= -\frac{n}{q^{n/2}} \frac{1}{(q-1)^2 q^{2(g_1+g_2)+2}} \sum_{h_1 \in \mathcal{H}_{2g_1+2}} \sum_{h_2 \in \mathcal{H}_{2g_1+2}} \sum_{\deg P = n} \chi_{K_1}(P)$$

$$= -\frac{n}{q^{n/2}} \cdot \frac{1}{(q-1)q^{2g_1+1}} \sum_{\deg P = n} \sum_{2\alpha_1 + \beta_1 = 2g_1+2} \sigma_n(\alpha_1) \sum_{\deg B_1 = \beta_1} \left(\frac{B_1}{P} \right) \frac{1}{(q-1)q^{2g_2+1}} \sum_{h_2 \in \mathcal{H}_{2g_2+2}} 1$$

$$= -\frac{n}{(q-1)q^{2g_1+1+\frac{n}{2}}} \sum_{\deg P = n} \sum_{2\alpha_1 + \beta_1 = 2g_1+2} \sigma_n(\alpha_1) \sum_{\deg B_1 = \beta_1} \left(\frac{B_1}{P} \right)$$

where we use the notation introduced in section 6.2. Notice that this last term is formula (6.2) for $g = g_1$. Then, like in that case, if $n > g_1 + 1$ we can simplify this formula as

$$\left\langle -\frac{n}{q^{n/2}} \sum_{\deg P = n} \chi_{K_1}(P) \right\rangle = -\frac{n}{(q-1)q^{2g_1+1+n/2}} (S(2g_1+2; n) - qS(2g_1; n))$$

At this point it is easy to see that the second term of $\langle \mathcal{P}_n \rangle$ is

$$\left\langle -\frac{n}{q^{n/2}} \sum_{\deg P = n} \chi_{K_2}(P) \right\rangle = -\frac{n}{(q-1)q^{2g_2+1+\frac{n}{2}}} \sum_{\deg P = n} \sum_{2\alpha_2 + \beta_2 = 2g_2+2} \sigma_n(\alpha_2) \sum_{\deg B_2 = \beta_2} \left(\frac{B_2}{P} \right).$$

When $n > 2g_2 + 2$ it becomes

$$\left\langle -\frac{n}{q^{n/2}} \sum_{\deg P=n} \chi_{K_2}(P) \right\rangle = -\frac{n}{(q-1)q^{2g_2+1+n/2}}(S(2g_2+2;n) - qS(2g_2;n)).$$

Finally, we have to consider the third term:

$$\left\langle -\frac{n}{q^{n/2}} \sum_{\deg P=n} \chi_{K_1}(P)\chi_{K_2}(P) \right\rangle =$$

$$\begin{aligned}
&= -\frac{n}{q^{n/2}} \frac{1}{(q-1)^2 q^{2(g_1+g_2)+2}} \sum_{C \in \mathcal{B}_{2g_1+2,2g_2+2}} \sum_{\deg P=n} \chi_{K_1}(P)\chi_{K_2}(P) \\
&= -\frac{n}{q^{n/2}} \frac{1}{(q-1)^2 q^{2(g_1+g_2)+2}} \sum_{h_1 \in \mathcal{H}_{2g_1+2}} \sum_{h_2 \in \mathcal{H}_{2g_1+2}} \sum_{\deg P=n} \chi_{K_1}(P)\chi_{K_2}(P) \\
&= -\frac{n}{q^{n/2}} \cdot \frac{1}{(q-1)q^{2g_1+1}} \sum_{\deg P=n} \sum_{2\alpha_1+\beta_1=2g_1+2} \sigma_n(\alpha_1) \sum_{\deg B_1=\beta_1} \left(\frac{B_1}{P}\right) \cdot \\
&\qquad \cdot \frac{1}{(q-1)q^{2g_2+1}} \sum_{2\alpha_2+\beta_2=2g_2+2} \sigma_n(\alpha_2) \sum_{\deg B_2=\beta_2} \left(\frac{B_2}{P}\right)
\end{aligned}$$

6.7 A new sum of characters

We see that there is something new to compute in order to estimate the contribution of primes. For hyperelliptic curves it was enough to define the double sums

$$S(\beta;n) := \sum_{\substack{\deg P=n \\ P \text{ prime}}} \sum_{\substack{\deg B=\beta \\ B \text{ monic}}} \left(\frac{B}{P}\right).$$

For biquadratic extensions we have to understand something that is more complicated. This is the following double sum:

$$\tilde{S}(\beta_1,\beta_2;n) := \sum_{\substack{\deg P=n \\ P \text{ prime}}} \sum_{\substack{\deg B_1=\beta_1 \\ B_1 \text{ monic}}} \left(\frac{B_1}{P}\right) \sum_{\substack{\deg B_2=\beta_2 \\ B_2 \text{ monic}}} \left(\frac{B_2}{P}\right).$$

This is what we get in the last two lines of the estimate of $\left\langle -\frac{n}{q^{n/2}} \sum_{\deg P=n} \chi_{K_1}(P)\chi_{K_2}(P) \right\rangle$.

If we want to average the trace of Frobenius classes in the given family, it seems necessary to write an expression for double sums like $\tilde{S}(\beta_1,\beta_2;n)$. At the moment, we cannot compute these double sums, but if we will be able to solve this problem, we are convinced that there are not going to be other major obstacles.

Bibliography

[Bas70] M. I. Bashmakov. Un théorème de finitude sur la cohomologie des courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 270:A999–A1001, 1970.

[BDF+15] A. Bucur, C. David, B. Feigon, N. Kaplan, M. Lalín, E. Ozman, and M. Matchett Wood. The distribution of points on cyclic covers of genus g. *(submitted)*, 2015.

[BDFL09] A. Bucur, C. David, B. Feigon, and M. Lalín. Statistics for traces of cyclic trigonal curves over finite fields. *International Mathematics Research Notices*, 2009.

[BDFL10] A. Bucur, C. David, B. Feigon, and M. Lalín. Fluctuations in the number of points of smooth plane curves over finite fields. *J. Number Theory*, 130:2528–2541, 2010.

[BDFL11] A. Bucur, C. David, B. Feigon, and M. Lalín. Biased statistics for traces of cyclic p-fold covers over finite fields. *WIN - Women in Number, Fields Institute Communications, American Mathematical Society,*, 2011.

[BSS99] I. Blake, G. Seroussi, and N. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1st edition, 1999.

[CM04] A. C. Cojocaru and M. Ram Murty. Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem. *Mathematische Annalen*, 330:601–625, 2004.

[Coj03] A. C. Cojocaru. Cyclicity of CM elliptic curves mod p. *Trans. Amer. Math. Soc.*, 355:2651–2662, 2003.

[Coj04] A. C. Cojocaru. Questions about the reductions modulo primes of an elliptic curve. In *Number theory*, volume 36 of *CRM Proceedings and Lecture Notes*, pages 61–79. Amer. Math. Soc., Providence, RI, 2004.

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[Cre06] J. E. Cremona. The elliptic curve database for conductors to 130000. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 11–29. Springer, Berlin, 2006.

[Dav14] C. David. Curves and zeta fuctions over finite fields - AWS 2014: Arithmetic statistics. `http://swc.math.arizona.edu/aws/2014/2014DavidNotes.pdf`, 2014.

[Deu41] M. Deuring. Die typen der multiplikatorenringe elliptischer functionenkorper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–292, 1941.

[Dos10] V. Dose. Serre's theorem on Galois representations attached to elliptic curves. Master's thesis, Università degli Studi di Roma "Tor Vergata", 2010.

[GGL95] R. L. Graham, M. Grotschel, and L. Lovasz. *Handbook of combinatorics, Volume 2.* 1995.

[GM86] R. Gupta and M. Ram Murty. Primitive points on elliptic curves. *Compositio Math.*, 58(1):13–44, 1986.

[Har77] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1977.

[Hoo67] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[Kow06] E. Kowalski. Analytic problems for elliptic curves. *J. Ramanujan Math. Society*, 2006.

[KR09] P. Kurlberg and Z. Rudnick. The fluctuation in the number of points on a hyperelliptic curve over a finite field. *J. Number Theory*, 129(3):580–587, 2009.

[KS99] N. M. Katz and P. Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications.* American Mathematical Society, Providence, RI, 1999.

[Lan94] S. Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics.* Springer–Verlag, New York, 2nd edition, 1994.

[LMM15] E. Lorenzo, G. Meleleo, and P. Milione. Statistics for biquadratic covers of the projective line over finite fields. (Preprint) `http://arxiv.org/abs/1503.03276`, 2015.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In A. Frohlich, editor, *Algebraic Number Fields*, pages 409–464. Academic press, New York, 1977.

[LS96] H. W. Lenstra and P. Stevenhagen. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18:26–37, 1996.

[LT76] S. Lang and H. Trotter. *Frobenius Distributions in* GL_2*-Extensions*, volume 504. Springer Lecture Notes in Mathematics, 1976.

[LT77] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Amer. Math. Soc.*, 1977.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186, 1977.

[Mel15] G. Meleleo. Cyclicity of quotients of non-CM elliptic curves modulo primes. Submitted, 2015.

[MMS88] M. Ram Murty, V. Kumar Murty, and N. Saradha. Modular forms and the Chebotarev density theorem. *American Journal of Mathematics*, 110(2):253–281, 1988.

[Mor12] P. Moree. Artin's primitive root conjecture a survey. *Integers*, 12(6):1305–1416, 2012.

[MW12] M. Matchett Wood. The distribution of the number of points on trigonal curves over $\mathbb{F}_q$. *Int. Math. Res. Not. IMRN*, 2012(23):5444–5456, 2012.

[Pap05] F. Pappalardi. A survey on k-power freeness. In *Proceeding of the Conference in Analytic Number Theory in Honor of Prof. Subbarao at I.M.Sc. Chennai, January 2003*, number 1 in Ramanujan Math. Soc. Lect. Notes Ser., pages 71–88, Mysore, 2005.

[PG05a] R. Pries and D. Glass. Hyperelliptic curves with prescribed p-torsion. *Manuscripta*, 117(3):299–317, 2005.

[PG05b] R. Pries and D. Glass. On the moduli space of Klein four covers of the projective line. *Computational Aspects of Algebraic Curves, Lecture Notes Series in Computing*, 13, 2005.

[Ros02] M. Rosen. *Number Theory in Function Fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[Rud10] Z. Rudnick. Traces of high powers of the Frobenius class in the hyperelliptic ensemble. *Acta Arithmetica*, 143(1), 2010.

[Ser72] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser81] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publications Mathématiques de l'IHÉS*, 54:123–201, 1981.

[Ser89] J.-P. Serre. *Abelian l-adic Representations and Elliptic Curves*. Advanced Book Classics. Addison-Wesley, Redwood City, California, 1989.

[Sil94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer Verlag, New York, 1994.

[Sil08] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer Verlag, New York, second edition, 2008.

[Was08] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman and Hall/CRC, second edition, 2008.

[Wei48] A. Weil. *Sur les Courbes Algébriques et les Variété qui s'en déduisent*. Hermann, Paris, 1948.

[Xio10] M. Xiong. The fluctuations in the number of points on a family of curves over a finite field. *Journal de Théorie de Nombres de Bordeaux*, 3:755–769, 2010.