Counting points on algebraic curves over finite fields and applications

A thesis submitted in fulfilment of the requirements

for the degree of Masters by research

by

Diptajit Roy

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

June 2025

Certificate

It is certified that the work contained in this thesis entitled **"Counting points on algebraic curves over finite fields and applications"** by **Diptajit Roy** has been carried out under my supervision and that it has not been submitted elsewhere for a degree.

Prof. Nitin Saxena

Professor

CSE Department

Indian Institute of Technology Kanpur

Declaration

This is to certify that the thesis titled **"Counting points on algebraic curves over finite fields and applications"** has been authored by me. It presents the research conducted by me under the supervision of **Prof. Nitin Saxena**.

To the best of my knowledge, it is an original work, both in terms of research content and narrative, and has not been submitted elsewhere, in part or in full, for a degree. Further, due credit has been attributed to the relevant state-of-the-art and collaborations with appropriate citations and acknowledgments, in line with established norms and practices.

Diptajit Roy
Roll No. 20111265
CSE Department
Indian Institute of Technology Kanpur

Abstract

Name of the student: **Diptajit Roy** Roll No: **20111265**

Degree for which submitted: **PhD** Department: **CSE Department**

Thesis title: **Counting points on algebraic curves over finite fields and applications**

Thesis supervisors: **Prof. Nitin Saxena**

Month and year of thesis submission: **June 2025**

Let $C/\mathbb{F}_q$ be a smooth projective curve over the finite fields $\mathbb{F}_q$ of characteristic p. By $C(\mathbb{F}_{q^r})$, we denote the set of points of C lying on a degree r extension of $\mathbb{F}_q$. We define its zeta function $Z(C/\mathbb{F}_q, T)$ as follows

$$Z(C/\mathbb{F}_q, T) := \exp\left(\sum_{i=1}^{\infty} \#C(\mathbb{F}_{q^i})\frac{T^i}{i}\right) \in \mathbb{Z}[[T]]$$

It is an important result in arithmetic geometry that $Z(C/\mathbb{F}_q, T)$ is a rational function of T.

A very well studied question in number theory is to compute $Z(C/\mathbb{F}_q, T)$ for a given curve $C/\mathbb{F}_q$. Over decades, the work of many mathematicians like Weil, Grothendieck and Deligne has captured what appears to be a purely number-theoretic question in terms of rich algebraic geometry. Following these, there have been many algorithmic results related to this problem. Motivated by a question posed by J.P.Serre, one can ask if there exists a polynomial-time algorithm to compute $\#C(\mathbb{F}_{q^r})$. Finding such an algorithm is still one of the major open questions in computational number theory. In this thesis, we construct a protocol to determine $\#C(\mathbb{F}_{q^r})$ which puts the problem in the complexity class AM $\cap$ coAM.

We also explore a special case of modular curves and their zeta functions. We will see how modular curves are linked with modular forms which will allow us to compute the pth Fourier coefficient of a modular form. We have explored some complexity results on computing the zeta function of modular curves and Fourier coefficients of modular forms.

Contents

List of Publications viii

1 Introduction 1
- 1.1 Motivation . . . 1
- 1.2 New results . . . 2
- 1.3 Organization of the Thesis . . . 2

2 Algebraic curves and complexity theory 4
- 2.1 Projective curves . . . 4
- 2.2 Homology theory of curves . . . 6
- 2.3 Cohomology theory of curves . . . 7
- 2.4 Complexity theory basics . . . 9

3 Computing zeta functions of algebraic curves 11
- 3.1 Zeta functions of varieties . . . 11
- 3.2 The Weil conjectures and the cohomological interpretation of zeta functions 14
- 3.3 Complexity of point counting on curves over finite fields . . . 16
- 3.4 Applications towards higher dimension and torsion counts . . . 19

4 Zeta functions of modular curves 22
- 4.1 Modular curves . . . 22
- 4.2 Modular forms . . . 24
- 4.3 Modular forms and Galois representations . . . 25
- 4.4 Modular forms as line bundles . . . 28
- 4.5 The defining equation for modular curves . . . 29
- 4.6 Computing Ramanujan Tau in polynomial time . . . 32
- 4.7 Some unconditional complexity results on counting points on modular curves and computing Hecke polynomials . . . 33

5 Conclusion 35

6 Appendix **36**
6.1 Torsions of modular curves 36

Bibliography **38**

List of Publications

Publications from Thesis

https://www.cse.iitk.ac.in/users/nitin/papers/etale-P1.pdf.

Dedicated to family.

Chapter 1

Introduction

The aim of this thesis is to show some algorithmic results related to counting points of algebraic curves over finite fields. In addition to being a mathematically interesting question, point counting of hyperelliptic curves over finite fields has vast applications in cryptography. In fact, the discrete logarithm problem of elliptic curves and Jacobian variety of hyperelliptic curves are applied in constructing cryptographic protocols; therefore, one would need to choose curves with large point counts over finite fields, in order to have secure protocols. In this thesis, we study this question for an input curve of given genus over finite fields of given characteristic.

1.1 Motivation

The problem of point counting of varieties defined over finite fields has applications in various areas of mathematics. This seemingly algebraic problem has found major application in analytic number theory. The study of number of solutions of polynomial systems over finite field dates back to Gauss. For example, Gauss studied equations of the form $ax^3 - by^3 \equiv 1 \bmod p$ and $ax^4 - by^4 \equiv \bmod p$ for primes p of the form $3n+1$ and $4n+1$ respectively, in connection to his investigation of Gaussian sums ([1],[2]), Hardy and Littlewood also applied point counting over finite fields while studying Waring's problem, which is purely analytic in nature. In addition to this, point counting has impacted algebraic geometry, representation theory. The Taniyama-Shimura-Weil conjecture whose proof led the path to proof of Fermat's last theorem ([3]) which relates the point count of elliptic curves defined over finite fields with modular forms. It also has a profound influence on the

Langlands program, where one studies the point counts of Shimura varieties and relates it to automorphic forms ([4],[5]).

Let $\mathbb{F}_q$ be a finite field of characteristic p and size $q = p^r$, for some $r \geq 0$. Then given an algebraic variety $X/\mathbb{F}_q$, one can ask what is the number of $\mathbb{F}_q$ (or a finite extension of $\mathbb{F}_q$) points lying on the curve C. The zeta function is an infinite series that encodes the point counts of X over all extensions of $\mathbb{F}_q$. Then, as we will see later, the zeta function can be given a finite description as a rational function in $\mathbb{Q}(T)$. Motivated by [6, Preface], the following question can be asked : Is there an algorithm that can compute the function $Z(C/\mathbb{F}_q, T)$ that has a run-time polynomial in the input parameters? Currently, the existence of such an algorithm is only conjectural. In this thesis, we will show that, in the case of curves, we have strong evidence that the problem is at least not NP-hard.

1.2 New results

This thesis aims to prove the following result.

Theorem 1.1. *Let C be a smooth projective geometrically irreducible curve defined over finite field $\mathbb{F}_q$ of characteristic p and genus g and $Z(C/\mathbb{F}_q, T)$ be its zeta function. Then computing $Z(C/\mathbb{F}_q, T)$ is in $AM \cap coAM$.*

This is the first classical complexity result on zeta functions of curves over finite fields where we allow both the prime characteristic of the field and the genus of the input curve to vary. Before our result, the existing classical algorithms assumes either the prime characteristic of the input field or the genus of the input curve to be fixed. This protocol can be seen as a classical analogue to Kedlaya's result on quantum complexity ([7]), where he has obtained an actual algorithm that runs in polynomial time.

1.3 Organization of the Thesis

In the second chapter, we focus on describing the basic tools that will be used throughout the thesis. We describe the technical details needed for the study of projective curves. We have introduced the basics of homology and cohomology theories and how these arose from topology. We have shown how these theories can be studied explicitly in connection with curves.

In the third chapter, we have stated the Weil conjectures and how cohomology theories are important in the context of counting points. We have also gone in brief on how the proof of Weil conjectures came about. Then we have described the details of our AM $\cap$ coAM protocol and explored some possible applications in computing zeta functions of Abelian varieties.

In the last chapter, we have explored a special case scenario of modular curves, stated how modular curves and modular forms are connected, and stated how counting points of modular curves over finite fields can help us to compute Fourier coefficients of a cuspform. We have explored a classical polynomial-time algorithm on this and also stated how our AM $\cap$ coAM result is impacting this.

Chapter 2

Algebraic curves and complexity theory

2.1 Projective curves

A projective curve defined over a field k is a projective variety that has dimension 1. For example, we can consider the elliptic curve defined over $\mathbb{Q}$, $E : Y^2Z = X^3 - AXZ^2 + BZ^3$; $A, B \in \mathbb{Q}$ in $\mathbb{P}^2_{\mathbb{Q}}$. Curves embedded in $\mathbb{P}^2$ are called plane projective curves. We call a point P of a projective curve singular if $\frac{\partial}{\partial X}P = \frac{\partial}{\partial Y}P = \frac{\partial}{\partial Z}P = 0$. A projective curve with no singular points is called smooth. A projective curve usually comes with a natural defining equation, therefore; often called a projective algebraic curve. A projective algebraic curve is called geometrically irreducible if the corresponding algebraic set in $\mathbb{P}^2_{\overline{k}}$ is not a union of two algebraic sets; in other words, the defining ideal of the curve (which has coefficients in k) does not factor in $\overline{k}$.

Curves can also arise in complex analytic ways where it is not directly evident what its defining equation is. Such curves are what we call analytic curves and are dealt with in terms of complex analytic geometry and topology. Examples of such curves are modular curves, where we usually describe it in terms of the action of group of matrices on the complex upper half-plane. As we will see later, obtaining the defining equations for these curves is not a hard problem, in fact, it is in polynomial time.

Definition 2.1 (Divisors)**.** Let C be a geometrically irreducible smooth projective curve defined over a field k. We define a divisor D on C as the formal sum

$$D = \sum_{P \in C(\overline{k})} n_P P$$

where $n_P \in \mathbb{Z}$ is called the order of P in D which is zero for all but finitely many $P \in C(\overline{k})$.

We call the set of all points $P \in C(\overline{k})$ for which $n_P \neq 0$, the support of D is denoted as $\mathrm{Supp}(D)$. We define the degree of D as $\sum n_P$. A divisor E is said to be effective if $n_P > 0$ for all $P \in \mathrm{Supp}(E)$. The set of divisors on X having degree zero is denoted as $\mathrm{Div}^0(C)$.

We denote the set of rational functions on C by $k(C)^*$. For $f \in k(C)^*$, the associated divisor in $\mathrm{Div}^0(C)$ is $(f) = \sum_{P \in C(\overline{k})} \mathrm{ord}_P(f) \cdot P$ called the principal divisor of f, where $\mathrm{ord}_P(f)$ denotes the order of vanishing of f at P. If P is a zero of f then $\mathrm{ord}_P(f) \geq 0$, $\mathrm{ord}_P(f) < 0$ if P is a pole of f. Therefore, we have the following injection

$$k(C)^* \hookrightarrow \mathrm{Div}^0(C)$$

and the quotient $\mathrm{Div}^0(X)/k(C)^*$ is termed the Jacobian variety or the Picard group of C. We denote it as $J(C)$ here. It is an algebraic group variety of dimension g, in particular, we can define a group structure on the g-fold product of C so that $C^g \cong J(C)$ (see [8, Ch. 5]).

Definition 2.2 (Differential)**.** Let X be a smooth affine curve defined over a field k, with a coordinate ring R. Then for $f \in R$ we call df the differential 1-form associated with f. The set of all symbols df, $f \in R$ modulo the relations $d(fg) - fdg - gdf$, $f, g \in R$ defines an R-module called the Kähler differential, which is denoted as $\Omega_{R/k}$.

More generally, we define the differential to be the map $d : R \to \Omega_{R/k}$ where $f \mapsto df$ $\forall f \in R$. We can define an element in $\Omega_{R/k}$ called the canonical form ω such that for all other differential form η, $\mathrm{Div}(\eta) = \mathrm{Div}(\omega) + f$. For example, consider the affine elliptic curve $E : Y^2 = P(X)$ defined over a field k, where $P(X) \in k[X]$ is a polynomial of degree three with three distinct roots; therefore we have $R(X), S(X) \in k[X]$ so that we have $(R(X)P(X), S(X)P'(X)) = 1$. Clearly, we have $2YdY = (3X^2 - 1)dX$ in $\Omega_{R/k}$ where R is the k-algebra represents the coordinate ring of E. In this scenario, one can show that every differential can be written in a canonical form as $A + BY(\omega)$ where $\omega = R(X)YdX + 2S(X)YdY$. Thus, ω is the canonical differential form associated with E.

For ω, we have an associated divisor defined as $(\omega) = \sum_{P \in C(\overline{k})} \mathrm{ord}_P(f) \cdot P$. By the notion of canonical form introduced in the last paragraph, every differential form has the same associated divisor called the canonical divisor. A canonical divisor is represented as K, its a known fact that $\deg(K) = 2g - 2$, where g is the genus of X.

2.2 Homology theory of curves

For any complex projective curve, there is a standard way to view it as a two-dimensional real manifold. The genus of a complex projective curve is the number of holes in the real manifold obtained from it. It forms a topological invariant of the curve. Its homology and cohomology groups are just different ways to measure its genus. This also helps to generalize the concept of genus to a projective curve over any field (for example, of nonzero characteristic). Simply speaking, we measure the holes in a two-dimensional real manifold by finding loops over it that do not enclose a region that lies on the manifold. For example, consider a hollow torus; clearly there are two loops which do not enclose a region falling on the torus. In other words, these are loops that are not contractable to a point.

In the following we will describe what is called the singular homology. In order to do this, we need to introduce a few terminologies. We call $\Delta \subset \mathbb{R}^n$ the standard n-simplex, the convex hull of the points $e_0, \ldots, e_n$; where $e_i \in \mathbb{R}^n$ so that $e_i(j) = 0$, $\forall j \neq i$ and $e_i(i) = 1$.

Definition 2.3 (Chains, cycles and boundaries)**.** Let X be a topological space. A n-simplex is a continuous map $s : \Delta^n \mapsto \mathcal{M}$. Let $s_{i|i \in I}$ be a set of n-simplices, where I is the indexing set. Then the group of n-chains $\mathcal{C}_n(X)$, is defined as a formal linear combination $\sum n_i s_i$, $n_i \in \mathbb{Z}$.

Denote $s(\Delta) = [p_0, \ldots, p_n]$, where $p_i = s(e_i)$. A n-boundary on the simplex $[p_0, \ldots, p_n]$ denoted as $\partial_n[p_0, \ldots, p_n]$ is defined as the alternating sum $\sum_{i=0}^{n} (-1)^i [p_0, \ldots p_{i-1}, p_{i-1} \ldots, p_n]$. A n-cycle is a n-chain having boundary zero.

From the above, we find that the boundary of an n-chain is a $n-1$-chain, which we denote as $\mathcal{C}_n(X) \xrightarrow{\partial_n} \mathcal{C}_{n-1}(X)$. It is clear from the above definition that $\partial_n \circ \partial_{n-1}$ is always zero. The following infinite sequence of maps is called a chain complex, denoted as $\mathcal{C}$.

$$\mathcal{C} : \ldots \xrightarrow{\partial_{n+2}} \mathcal{C}_{n+1}(X) \xrightarrow{\partial_{n+1}} \mathcal{C}_n(X) \xrightarrow{\partial_n} \mathcal{C}_{n-1}(X) \xrightarrow{\partial_{n-1}} \ldots.$$

In this scenario, the nth singular homology group is defined as

$$\mathcal{H}_n(X, \mathbb{C}) = \frac{\mathrm{Ker}(\partial_n)}{\mathrm{Im}(\partial_{n+1})}.$$

This gives us a $\mathbb{C}$-vector space of dimension equal to the number of n-dimensional holes in X.

Remark 2.4. Note that $\partial_n \circ \partial_{n-1} = 0$ implies $\mathrm{Im}(\partial_n) \subseteq \mathrm{Ker}(\partial_{n-1})$ in $\mathcal{C}$. The equality happens when $\mathcal{H}_n(X, \mathbb{C}) = 0$, then the complex $\mathcal{C}$ has $\mathrm{Im}(\partial_n) = \mathrm{Ker}(\partial_{n-1})$, which is called as $\mathcal{C}$ being exact at $\mathcal{C}_n$. Thus the homology groups measure the failure of a chain complex to be an exact sequence.

For our purpose of this thesis, we will stick to the case of a complex projective algebraic curve of genus g. This means that the corresponding two-dimensional real manifold has g one-dimensional holes. In case of complex projective curves; it is easy to see that $\mathcal{C}_n(\mathrm{X})$ for $n \geq 3$ is zero; therefore, we will only be concerned with $0, 1, 2$-cycles. We will be mostly interested in studying the first homology group $\mathcal{H}_1(X)$ for the modular curve $X_0(N)$ (more on this in the next chapter), in general of any genus g curve. The following theorem gives the structure of $\mathcal{H}_1(X)$ for an algebraic curve X of genus g.

Theorem 2.5. *Consider X to be an algebraic curve of genus g defined over a field k. Then $\mathcal{H}_1(X) \cong \mathbb{Z}^{\oplus 2g}$.*

Suppose X is an elliptic curve over $\mathbb{C}$, we can view it as a quotient $\mathbb{C}/\mathcal{L}$, for some $\mathbb{Z}$-lattice $\mathcal{L}$. That it is of genus one can be seen by identifying the opposite ends of the fundamental parallelogram and forming a hollow torus which has one hole. It can be shown that the generators of the group $\mathcal{H}_1(X, \mathbb{Z})$ are generated by cycles that cannot be contracted to a point. Clearly, there are two cycles for an elliptic curve and $2g$ for a genus g curve. The formal computation involves triangulating a surface and explicitly computing the groups $\mathcal{C}_0(X), \mathcal{C}_1(X)$ and $\mathcal{C}_2(X)$ which we will not do here. It can be referred from any standard text on algebraic topology.

2.3 Cohomology theory of curves

In the last section, we have seen what a singular homology group of a curve is. There is a similar notion of a singular cohomology theory; it comes up when we talk about the dual of a chain complex. Suppose $\mathcal{C}$ is as stated in the last section. Then we can define its dual $\mathcal{C}'$,

called a co-chain complex, which is obtained by replacing $\mathcal{C}_i$ by $C_i' = \mathrm{Hom}(\mathcal{C}_i, \mathbb{R})$. It is clear that if we have a map $\mathcal{C}_i \to \mathcal{C}_{i-1}$ then there is an opposite map $\mathrm{Hom}(\mathcal{C}_{i-1}, \mathbb{R}) \to \mathrm{Hom}(\mathcal{C}_i, \mathbb{R})$. Therefore, we have a cochain as follows.

$$C' : \ldots \xleftarrow{\delta n+1} C'_{n+1}(X) \xleftarrow{\delta n} C'_n(X) \xleftarrow{\delta n-1} C'_{n-1}(X) \xleftarrow{\delta n-2} \ldots;$$

Here, δ_i is called the co-boundary map. The nth singular cohomology group $H^n(X)$ is also defined similarly.

$$H^n_{\mathrm{sing}}(X) = \frac{\mathrm{Ker}(\delta_n)}{\mathrm{Im}(\delta_{n-1})};$$

As in the case of singular homology $H^n(X) = 0$ for $n \geq 2d + 1$.

Next we shall consider two important classes of cohomology theories called De-Rham cohomology and étale cohomology which was founded in the work of De-Rham and Grothendieck [9]. Both of these theories has proven to be important for the computation of zeta functions of varieties.

We will first describe the De-Rham cohomology. Let X be a smooth projective curve defined over a finite field $\mathbb{F}_q$ of characteristic p. Then, the ith cochain consists of the formal sums of the ith differential forms $\omega = \sum_I \omega_I dx^I$, where I is the multi-index $x_{i_1}, \ldots, x_{i_m}$ and $dx^I = dx_{i_1} \bigwedge \ldots \bigwedge dx_{i_m}$. Here $\bigwedge$ is the wedge product that satisfies the property $d\omega \bigwedge d\omega = 0$, $d\omega_i \bigwedge d\omega_j + d\omega_j \bigwedge d\omega_i = 0$. We have $d\omega = \sum_I \sum_{i_1 \in I} \frac{\partial \omega_I}{\partial x_{i_1}} dx_{i_1} \bigwedge dx^I$, thus $d\omega$ is a $k+1$ form if not zero. We call a k form ω closed if $d\omega = 0$ and exact if $\omega = d\omega^1$ for some $k-1$ for ω^1. We have $d^2\omega = 0$ applying the properties of the wedge product. Thus, we have a cochain complex of differential k-forms as follows.

$$\ldots \xleftarrow{\delta n+1} \Omega_{n+1}(X) \xleftarrow{\delta n} \Omega_n(X) \xleftarrow{\delta n-1} \Omega_{n-1}(X) \xleftarrow{\delta n-2} \ldots;$$

where Ω_n consists of all the differential n-forms and δ_i are the differential maps with $\delta_i \circ \delta_{i+1} = 0$. The nth De-Rham cohomology thus measures the closed n-forms that fails to be exact.

The De-Rham theorem shows that there is an isomorphism $H^n_{\mathrm{sing}}(X) \cong H^n_{\mathrm{dr}}(X)$. This goes by constructing an integration pairing between the nth singular homology $\mathcal{H}_n(X, \mathbb{C})$ and $H^n_{\mathrm{dr}}(X)$, which is non-degenerate. In particular, for a homology class of a cycle $[c] \in \mathcal{H}_n(X, \mathbb{C})$ and the De-Rham cohomology class of a differential form $\omega \in H^n_{\mathrm{dr}}(X)$, the

pairing is as $\langle [c], \omega \rangle = \int_{[c]} \omega$. Since $H^n_{\mathrm{dr}}(X)$ is finite-dimensional, we have the isomorphism and therefore, its dimension is also $2g$.

The De Rham cohomology is an example of p-adic cohomology which means that the field of definition of the cohomology group is a finite field of characteristic p. For smooth projective varieties defined over a field k, Grothendieck has developed the notion of étale cohomology which has its field of coefficients of characteristic $\ell \neq p$. The definition of étale cohomology for smooth varieties of arbitrary dimension requires a lot of new machineries which we will not need for this thesis. It basically arose from the notion of sheaf cohomology theories introduced by Serre, interested reader may refer to [10].

However, if we consider a X to be a smooth projective curve, the definition becomes much simpler. Recall that $J(X)$ is the Jacobian variety of X, which is of dimension g. Let $J(X)[\ell^i]$ denote the subgroup of ℓ^i-torsion points in $J(X)$. It is well known that $J(X)[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$. Then we have the following chain of maps

$$\ldots \xrightarrow{[\ell]} J(X)[\ell^{i+1}] \xrightarrow{[\ell]} J(X)[\ell^i] \xrightarrow{[\ell]} \ldots \xrightarrow{[\ell]} J(X)[\ell].$$

If we take the projective limit of the above map, then we get a $\mathbb{Z}_\ell$-module called the ℓ-adic Tate module isomorphic to $\mathbb{Z}_\ell^{2g}$. Then we have $H^1_{\text{ét}}(X, \mathbb{Q}_\ell)$ is isomorphic to the dual of the ℓ-adic Tate module base changed to $\mathbb{Q}_\ell$ [10, Ch. 5], so any computations that must be performed in $H^1_{\text{ét}}(X, \mathbb{Q}_\ell)$ can be carried out on the Tate module itself. This will be crucial for all the ℓ-adic point count algorithms that we will discuss.

2.4 Complexity theory basics

Here, we review some of the basic complexity classes in the computational complexity literature. For our computation purpose of the zeta function of curves, we will mainly focus on the complexity class AM∩coAM and the class BQP.

AM is a computational complexity class which is considered 'similar' in the complexity hierarchy to NP. The problems of this class can be verified by an *Arthur-Merlin protocol* consisting of two parties called the *prover* (Merlin) and *verifier* (Arthur). Merlin tries to convince Arthur about a decision problem, by sending some 'data' (*certificate*) which is verified by Arthur in probabilistic polynomial time. After a fixed number of steps, Arthur either accepts or rejects. If we restrict the number of interactions between the two parties to just two (e.g., a *challenge* followed by a *response*), this is a randomised version of the

classic NP protocol. A problem in the class AM $\cap$ coAM is considered unlikely to be NP-hard, as otherwise, the complexity class called Polynomial Hierarchy (PH) will collapse (see [11, 9.3] for details).

An example of a problem in AM $\cap$ coAM is the popular Goldwasser-Sipser protocol to compute set size lower bounds, which we closely follow to develop our protocol for curves [11]. Let $S \subset \{0,1\}^k$ and let $N \in \mathbb{Z}_{>0}$ be the claimed lowerbound of S which must be tested. Also, let us assume that the membership of the elements of $\{0,1\}^k$ in S can be tested. Merlin's goal is to convince Arthur that $|S| \geq N$, and Arthur should reject if $|S| \leq N/2$. Here, hash functions prove to be very useful, which are functions that map the domain to the range avoiding collisions with high probability. The trick is that Arthur sends Merlin a tuple consisting of a random hash function $h : \{0,1\}^k \to \{0,1\}^L$ and a random element $y \in \{0,1\}^L$. In this scenario, if $|S| \geq N$ then with probability greater than $2/3$ there exist $x \in S$ such that $h(x) = y$. Otherwise, the probability of existence of $x \in S$ such that $h(x) = y$ is less than $1/3$. Therefore, the challenge for Merlin is to find an $x \in S$, such that $h(x) = y$. We choose $2^{L-2} \leq N \leq 2^{L-1}$ to meet the probabilities.

We next come to the complexity class BQP. Suppose that we are given a finite solvable group whose order we have to compute. Classically, this is a very hard question; in fact, the problem of integer factoring reduces to it, so its at least as hard as factoring integers (in quantum, this actually helps solve integer factoring [12]). But by using quantum, we get a polynomial-time algorithm given that one has access to the generators of the group. The details of the steps are not needed for this thesis; interested readers are referred to [13]. We just need the fact that one needs to find a generating set of a finite solvable group to compute its order.

Chapter 3

Computing zeta functions of algebraic curves

In the following, we first develop the notion of zeta functions for algebraic curves or, in general, algebraic varieties over finite fields (Section 3.1). Then we state the Weil conjectures (Section 3.2 and give a basic outline of the proof. Finally, we give an AM $\cap$ coAM protocol to determine the zeta function for an input algebraic curve defined over finite fields (Section 3.3). Further, we describe some applications of point counting of curves to higher dimensions, namely surfaces and threefolds (Section 3.4).

3.1 Zeta functions of varieties

Let X be a smooth projective variety over the finite field $\mathbb{F}_q$. The Hasse-Weil local zeta function of X is defined as follows.

$$Z(X/\mathbb{F}_q, T) := \exp\left(\sum_{i=1}^{\infty} \#X(\mathbb{F}_{q^i})\frac{T^i}{i}\right) \in \mathbb{Z}[[T]]. \tag{3.1.1}$$

To understand the motivation of this definition, we need to reinterpret a projective variety as a projective scheme. From there we will see that the above definition of a zeta function becomes equivalent to a more familiar definition of a zeta function like the Riemann zeta function or the Dedekind zeta function.

We first recall the Riemann and the Dedekind zeta functions. The standard number-theoretic zeta function $\zeta(s)$, called the Riemann zeta function, is a meromorphic function from $\mathbb{C}$ to itself, is defined as follows,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s};$$

where s is a complex number. It can also be expanded as a Euler product as follows.

$$\zeta(s) = \prod_{p \in \mathbb{Z}} \left(\frac{1}{1 - p^{-s}} \right).$$

where p is a prime number. This satisfies a functional equation and can be analytically continued to $\mathbb{C}/\{1\}$, as it has a simple pole at $s = 1$. A generalization of the Riemann zeta function is the Dirichlet L-function, which we will see later. The famous Riemann hypothesis conjectures that all the zeros of the zeta function with the imaginary part non-zero, lie on the line $\mathrm{Re}(s) = 1/2$.

We can even generalize the Riemann zeta function to any number field, which gives another notion of a zeta function, by restating the definition as follows. For a commutative ring R, the set of its prime ideals (including the 0-ideal) is denoted as $\mathrm{Spec}(R)$. Let K be a number field and $\mathcal{O}_K$ be its ring of integers. For a prime ideal in $\mathcal{P} \in \mathcal{O}_K$ over a prime $p \in \mathbb{Z}$, $\mathcal{O}_K/\mathcal{P}$ is a finite extension of $\mathbb{F}_p$. Then we have

$$\zeta(s) = \prod_{\mathcal{P} \in \mathcal{O}_K} \left(\frac{1}{1 - N(\mathcal{P})^{-s}} \right);$$

where $\mathcal{P}$ is a prime ideal and N is the norm function, $N : \mathrm{Spec}(\mathcal{O}_K) \to \mathbb{Z}$ that gives the size of the residue field of a prime ideal in $\mathrm{Spec}(\mathcal{O}_K)$. Similarly to the standard zeta function, it satisfies a functional equation and has a Riemann hypothesis that is unsolved. It can be seen that for $K = \mathbb{Q}$ this is the standard Riemann zeta function.

Now we come to the setting of a more general object called a scheme (see [14] for the definition). We will not need schemes any further, just that if we consider only smooth projective varieties, it will not be clear why definition 3.1.1 generalizes the Riemann zeta function.

Let $X = \mathrm{Spec}(R)$, for a commutative ring R. For a point $p \in X$, let $R_{(p)}$ denote the localization of R at p and $\kappa(p) = R_{(p)}/\mathcal{M}(p)$, where $\mathcal{M}_p$ is the unique maximal ideal of $X_{(p)}$. Consider the following Euler product;

$$Z(X,s) = \prod_{p \in R} \left(\frac{1}{1 - |\kappa(p)|^{-s}} \right).$$

Note that $X = \mathrm{Spec}(\mathbb{Z})$ gives us the Riemann zeta function and $X = \mathrm{Spec}(\mathcal{O}_K)$ gives the Dedekind zeta function for K. We will show how the above definition is equivalent to that we saw in 3.1.1.

Let X be a smooth projective variety over a finite field $\mathbb{F}_q$, $\overline{X} = X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ and let R be the coordinate ring of X. Let $G = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, for a point $x \in \overline{X}$ denote x^G denote the orbit of x under the action of G. We have a one-to-one correspondence between the orbits x^G of $\overline{X}$ and the elements of $\mathrm{Spec}(R)$. These orbits are called closed points of X over $\mathbb{F}_q$. Let X_0 denote the set of all closed points over $\mathbb{F}_q$. Then we have

$$Z(X,s) = \prod_{p \in R} \left(\frac{1}{1 - |\kappa(p)|^{-s}} \right) = \prod_{x \in X_0} \left(\frac{1}{1 - |\kappa(x)|^{-s}} \right). \tag{3.1.2}$$

where, $\kappa(x)$ is the finite Galois extension of $\mathbb{F}_q$ that contains all the points of x^G. For a closed point $x \in \overline{X}$, $\deg(x) = [\kappa(x) : \mathbb{F}_q]$. The following lemma gives the connection of 3.1.1 and 3.1.2.

Lemma 3.1.

$$\#X(\mathbb{F}_{q^m}) = \sum_{x \in X_0, deg(x) | m} deg(x).$$

Taking the logarithm on both sides of 3.1.2 we have

$$\log(Z(X,s)) = \sum_{x \in X_0} \log \left(\frac{1}{1 - |\kappa(x)|^{-s}} \right) = \sum_{x \in X_0} \sum_{n=1}^{\infty} \frac{|\kappa(x)|^{-ns}}{n} = \sum_{n=1}^{\infty} \sum_{x \in X_0} \frac{q^{-\deg(x)ns}}{n}$$

$$= \sum_{m=1}^{\infty} \sum_{\deg(x) | m} \frac{q^{-ms}\deg(x)}{m} = \sum_{m=1}^{\infty} \left(\sum_{\deg(x) | m} \deg(x) \right) \frac{q^{-ms}}{m}$$

$$= \sum_{m=1}^{\infty} \left(\#X(\mathbb{F}_{q^m}) \frac{q^{-ms}}{m} \right)$$

Now we substitute $T = q^{-s}$ and exponentiate both sides to obtain the definition 3.1.1.

3.2 The Weil conjectures and the cohomological interpretation of zeta functions

In 1949 André Weil stated some conjectures concerning the zeta functions of algebraic varieties over finite fields which were motivated by his study of number of solutions of equations over finite fields [15]. These conjectures suggested some strong connections between the study of the number of solutions of polynomial equations over finite fields and the topology of complex algebraic varieties. In particular, he conjectured that there should exist a cohomology theory, analogous to the singular cohomology of complex algebraic varieties, which will prove his conjectures. In the following, we first state the conjectures without proof (the proof can be found in [10]) and then we will see why the cohomology groups are useful for studying point counts.

Theorem 3.2 (Weil Conjectures)**.** *Let X be a smooth projective variety defined over $\mathbb{F}_q$ of characteristic p and let $Z(X/\mathbb{F}_q, T)$ be its zeta function. Then the following are true.*

- *(Rationality) The zeta function $Z(X/\mathbb{F}_q, T) \in \mathbb{Z}[[T]]$ is a rational function in $\mathbb{Q}(T)$.*
- *(Functional equation) $Z(X/\mathbb{F}_q, \frac{1}{q^n T}) = q^{\frac{nE}{2}} T^E Z(X/\mathbb{F}_q, T)$; E being the Euler factor (see the last part of the theorem).*
- *(Riemann Hypothesis) $Z(X/\mathbb{F}_q, T) = \frac{P_1(T)\ldots P_{2n-1}T}{P_0(T)\ldots P_{2n}T}$; where $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$ and $P_i(T)\, 1 \leq i \leq 2n-1$; are characteristic polynomials for the action of the Frobenius operator on $H^i_{\acute{e}t}(X, \mathbb{Q}_\ell)$; $P_i(T) = \prod_{j \in B_i}(1 - \alpha_{ij}T)$, where $|\alpha_{ij}| = q^{i/2}$.*
- *(Betti numbers) Let $B_i = dim(H^i_{\acute{e}t}(X, \mathbb{Q}_\ell))$, $\ell \neq p$; then we have $E = \sum_i (-1)^i B_i$; where E is the Euler factor.*

The following examples demonstrate the fact that the zeta function is a rational function. The second example serves as a demonstration of the Riemann hypothesis of Weil conjectures. The first proof of the rationality of zeta functions is due to Dwork [16].

Example 3.1. *Let $X = \mathbb{P}^n_{\mathbb{F}_q}$ be the projective space of dimension n over $\mathbb{F}_q$. Then we have*

$$Z(\mathbb{P}^n/\mathbb{F}_q, T) = exp\left(\sum_{i=1}^{\infty} \frac{(qT)^i + T^i}{i}\right).$$

Expanding the exponent as a log series we have,

$$Z(\mathbb{P}^n/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)}$$

Recall that for smooth projective curves of genus g, we have $\dim(H^i_{\text{ét}}(X, \mathbb{Q}_\ell)) = 2g$ and that $H^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ is isomorphic to the ℓ-adic Tate module of the Jacobian of X. Grothendieck first gave the construction for ℓ-adic étale cohomology which gave the proof of the first and second parts of Theorem 3.2. Later Grothendieck and Berthlot gave another proof using crystalline cohomology which is a p-adic cohomology.

Example 3.2. *Let X be a smooth projective curve over $\mathbb{F}_q$ of genus g. Then $Z(C/\mathbb{F}_q, T) \in \mathbb{Q}(T)$ takes the following form.*

$$Z(C/\mathbb{F}_q, T) = \frac{P(T)}{(1-T)(1-qT)},$$

where $P(T)$ is a polynomial of degree $2g$, which is the characteristic polynomial of the action of the Frobenius on the ℓ-adic Tate module of $J(C)$ ($\ell \neq p$), the Jacobian variety of C.

The proof of the Weil conjectures was first carried out by Andre Weil for curves and for Abelian varieties using the Riemann-Roch theorem. He then conjectured the existence of some cohomology theories called Weil cohomology theories, in order to prove the Weil conjectures for general smooth varieties, which satisfies some common properties. Popular examples of such cohomology theories include the De-Rham cohomology, étale cohomology, singular cohomology, etc. One of the common properties is Lefschetz's fixed point formula for a smooth projective variety $X/\mathbb{F}_q$ of dimension d, which is actually motivated from topology. There is an analog formula for counting the fixed points of continuous maps of topological spaces involving the action of Frobenius on the singular cohomology group of a topological space.

$$\#X(\mathbb{F}_{q^r}) = \sum_{i=0}^{2d} (-1)^i \text{Tr}((\text{Frob}_q)^r; H^i_{\text{ét}}(X, \mathbb{Q}_\ell))$$

Substituting this into the definition of $Z(X/\mathbb{F}_q, T)$ we get the following.

$$Z(X/\mathbb{F}_q, T) = \prod_{i=0}^{2d} \left[\exp\left(\sum_{j=1}^{\infty} \text{Tr}((\text{Frob}_q)^r; H^i_{\text{ét}}(X, \mathbb{Q}_\ell)) \right) \frac{T^r}{r} \right]^{-1^i}$$

Then the Riemann hypothesis can be obtained form the following observation.

$$\left[\exp\left(\sum_{j=1}^{\infty}\mathrm{Tr}((\mathrm{Frob}_q)^r; H^i_{\text{ét}}(X,\mathbb{Q}_\ell))\right)\frac{T^r}{r}\right] = \det((1-\mathrm{Frob}_q T); H^i_{\text{ét}}(X,\mathbb{Q}_\ell))^{-1}$$

In general, it may be possible to come up with proofs of Weil conjectures using any Weil cohomology theory. For example, Kedlaya gave another p-adic proof of the Weil conjectures using Berthlot's rigid cohomology [17].

In the following section, we will see how these cohomology theories are useful in coming up with algorithms for counting points of varieties. As stated in the previous paragarph, an abundance of p-adic cohomology theories has been discovered compared to ℓ-adic cohomologies. Therefore, in practise most point counting algorithms are p-adic than ℓ-adic, more on this in the next section.

3.3 Complexity of point counting on curves over finite fields

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve where A, B lies in the finite field of characteristic p, $\mathbb{F}_q$. Then [18] gave an algorithm having a run-time polynomial in $\log(p)$, to explicitly compute the ℓ-adic Tate module of E. This gave the first computation of the zeta function of a variety that was also polynomial-time. Since the details of the algorithm form an important part of the literature on computing zeta functions, we give some details of the algorithm here.

Let $E/\mathbb{F}_q$ be an elliptic curve as above. Then we have explicit polynomials that are satisfied by the ℓ-torsion points of E called the ℓth division polynomial. The idea is to use these polynomials to work on the formal roots to compute the Frobenius action on it. This has been carried out in [18, Section 3]. However, as we will see, this is a very special scenario for constant genus curves, for varying genus we get into trouble. Recall that $Z(E/\mathbb{F}_q, T)$ is defined as follows,

$$Z(E/\mathbb{F}_q, T) = \frac{1 - a_q T + T^2}{(1-T)(1-qT)};$$

where $a_q \in \mathbb{Z}$. So, if we can compute a_q modulo ℓ for many ℓ, by Chinese remaindering, we will obtain a_q. The number of ℓ needed is specified by the Riemann hypothesis for E, namely $|a_q| \leq \sqrt{q}$. Let $\ell = O(\log q)$, we just need to make sure that $\prod_{i\in[r]} \ell_i > 2\sqrt{q}$, $\ell_i \neq p$; Therefore, we need $r > O(\frac{\log(q)}{\log\log q})$ many primes in order to obtain a_q absolutely in

poly$(\log q)$ time. This also forms the backbone of ℓ-adic algorithms to compute the zeta function. We will see the application of this in the next chapter.

The situation becomes complicated if g is also allowed to vary along with the prime characteristic of the field. In order to apply Schoof's trick, one has to go to an extension over the base field where all the ℓ-torsions are present. Let $X/\mathbb{Q}$ be a smooth projective curve of genus g and let $J(X)$ denote its Jacobian variety. Recall that the ℓ-torsion subgroup of $J(X)$ for a prime ℓ be denoted as $J(X)[\ell]$ and is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^{2g}$. For a prime $p \neq \ell$, consider $J(X)_{\mathbb{F}_p}$ the reduction of $J(X)$ at p, then there is an induced action of Frobenius at p on $J(X)_{\mathbb{F}_p}[\ell]$. This creates a representation of Frobenius at p on the ℓ-torsion points, and we have a $2g \times 2g$ matrix over $\mathbb{Z}/\ell\mathbb{Z}$. Let $\mathbb{F}_q$ be an extension of $\mathbb{F}_p$, so that the action of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is trivial on $J(X)_{\mathbb{F}_p}[\ell]$. The size of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ can be at most the size of $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$ and therefore $[\mathbb{F}_q : \mathbb{F}_p]$. Since $|\mathrm{GL}_{2g}(\mathbb{F}_\ell)|$ is exponential, the degree of extension may grow to be exponential. The following lemma proves that for an elliptic curve, $[\mathbb{F}_q : \mathbb{F}_p]$ is always a polynomial in g. We will see some applications of this in the next chapter, where we describe modular curve computations.

Lemma 3.3. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then the maximum extension $[\mathbb{F}'_q : \mathbb{F}_q]$ such that $Gal(\mathbb{F}'_q/\mathbb{F}_q)$ acts trivially on $E[\ell]$ is $(\ell^2 - 1)(\ell^2 - \ell)$.*

Proof. We have $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. The size of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is $(\ell^2 - 1)(\ell^2 - \ell)$. □

We have an algorithm in this scenario due to Pila ([19]) that has a run-time polynomial in $\log q$ but exponential in the genus. In general, we have a trade-off between the genus and the prime characteristic, which we fix in order to obtain polynomial-time algorithms. Like in Pila's algorithm, if the genus is allowed to stay fixed, we will get a poly$(\log q)$-time algorithm, the same as that of Schoof. There is a wide range of p-adic cohomology theory, Berthlot rigid cohomology, Monsky washnitzer cohomology, which has yielded efficient p-adic algorithms in practice ([20], [21]). Kedlaya [20] gave an algorithm to compute the zeta functions of hyperelliptic curves of arbitrary genus g defined over finite fields of small characteristics using the Monsky Washnitzer cohomology. The only drawback in p-adic algorithms is it runs exponentially in the size of the bit representation of p. In general, the ℓ-adic algorithms are polynomial in the field characteristic and exponetial in genus, where as p-adic algorithms are polynomial in the genus but exponential in the characteristic. As a side note we should mention that not all algorithms of point counting came from a cohomology theory. There is a quite recent example [22] where the authors used a Dwork's trace formula to obtain the zeta function. Another example is a quantum polynomial

time algorithm and is due to Kedlaya ([7]) which is polynomial in both genus and the characteristic. There is also an average polynomial time algorithm to compute the zeta functions due to David Harvey [23].

We now come to our contribution. We assume that the input curve $X/\mathbb{F}_q$ is presented as a system of polynomial equations over $\mathbb{F}_q$. The curve presented in this form is non-planar so we need to change it to a planer model first. It is well known that every curve $X \subset \mathbb{P}^n_{\mathbb{F}_q}$ is bi-rationally equivalent to a planer curve $X' \subset \mathbb{P}^2$ with singularities at most nodal. This means that the singular points of the curve $X' \subset \mathbb{P}^2_{\mathbb{F}_q}$ have a vanishing multiplicity of two in X', and the tangents are distinct. We can compute this X' via [24, Lemma 2.2]. This planar model is now used by our AM $\cap$ coAM protocol to verify $\#X(\mathbb{F}_{q^d})$ for any given extension d of $\mathbb{F}_q$.

Before we proceed to our protocol, we need some estimates of the point count and a structure theorem of the Jacobian variety, which we state below. For a proof, refer [25, pg 70-71] and also [26, pg 206].

Proposition 3.4 (Hasse-Weil bound)**.** *Let $X/\mathbb{F}_q$ be a smooth projective curve over $\mathbb{F}_q$ of genus g. Then its Jacobian $J(X)$ satisfies*

$$(\sqrt{q}-1)^{2g} \leq J(X)(\mathbb{F}_q) \leq \sqrt{q}+1)^{2g}$$

For the proof of the following lemma, see [24, lemma 2.4].

Lemma 3.5. *Let X be as in the above proposition. Let $D \in J(X)$ be a divisor. Then $\exists d \in [g]$ and an effective divisor E of degree D such that $D \cong E + d\infty$, where ∞ is a fixed point decided by injection $X \hookrightarrow J(X)$.*

Remark 3.6. Let $D \in J(X)(\mathbb{F}_q)$ and $D = \sum_{i=1}^{j \leq g} P_i - j\infty$, then the coordinates of P_i can be in at most g degree extension over $\mathbb{F}_q$. This is easy to see since D is fixed by the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ so P_i is permuted by the action.

Refer to [24, Algorithm 2] for the full details of our protocol. Here we will just provide the sketch. Let X be a smooth projective curve over $\mathbb{F}_q$, and N be a number in the Hasse-Weil range of Theorem 3.4, which Arthur will send to Merlin. In response, Merlin will send some certificate by which Arthur has to verify whether $N = X(\mathbb{F}_q)$. But Arthur also has to catch on Merlin's response if it is fraudulent. Merlin would always try to convince Arthur that N is the actual count.

To avoid this scenario, we need to do two things. Firstly, for a given genus g of X, we need to choose a q so that the Hasse-Weil gap (3.4) is small enough. This is done to ensure that $2N, N/2$ both falls outside the gap (see [24, pg 9]). Secondly, we need to use a tool called the Hash function $H : \{0,1\}^{2g \log q} \mapsto \{0,1\}^{L+1}$ where $2^{L-1} \leq N \leq 2^L$, which Arthur chooses randomly so that with high probability we can make sure Arthur catches Merlin's fraudulence ([24, Lemma 2.8]).

Therefore, Arthur chooses a random H and a random b from the range of H and sends this information to Merlin. Merlin then generates an x so that $H(x) = y$, by sending a basis of $J(X)(\mathbb{F}_q)$ along with their orders and a x presented expressed as a linear combination of that basis. From Lemma 3.5 Merlin can provide a basis for the space $J(X)(\mathbb{F}_q)$. Now, if $N = J(X)(\mathbb{F}_q)$, Merlin will provide the correct set of basis elements and Arthur can take the product of the order of the basis element to confirm the count. If not, then Merlin is fraudulent and Merlin only can send a set of elements that are dependent since the independence scenario is already ruled out by our choice of the Hasse-Weil bound. Since they are dependent, the space spanned by the basis is actually less than $\#J(X)(\mathbb{F}_q)/2$ and with high probability Arthur catches Merlin. The rest follows from [24, Lemma 2.8, 2.9]. □

Remark 3.7. Note the difference from the Goldwasser Sipser protocol we gave in Section 2.4. Here, the Hasse-Weil bound actually allows us to compute the exact size instead of just a lower bound.

3.4 Applications towards higher dimension and torsion counts

Let X be a smooth projective geometrically irreducible variety of dimension $n > 1$, for example, a surface or a cubic threefold. Let $H \subset \mathbb{P}^n$ be a hyperplane cutting X transversely. This means that for all points $x \in X \cap H$ with X, H does not contain the tangent space at x. In this scenario, $Y = H \cap X$ is a smooth irreducible subvariety of co-dimension one in X and is called a hyperplane section of X.

Theorem 3.8 (Lefschetz Hyperplane theorem)**.** *Let X be an n-dim smooth projective variety over $\mathbb{F}_q$. Then if $U = X/Y$ is smooth, then we have for $n > 2$*

$$H^1_{\acute{e}t}(X, \mathbb{Q}_\ell) \cong H^1_{\acute{e}t}(Y, \mathbb{Q}_\ell)$$

and

$$H^1_{\acute{e}t}(X, \mathbb{Q}_\ell) \hookrightarrow H^1_{\acute{e}t}(Y, \mathbb{Q}_\ell)$$

for $n = 2$.

So in order to compute the Frobenius action on the first étale group for a smooth projective variety of dimension n, it suffices to compute the first étale cohomology of a surface obtained by taking the hyperplane section repeatedly to come down to dimension 2, which we can do by the effective Bertini's theorem [24, Proposition 4.2]. For $n = 2$ the situation is more delicate and is done by using Hard Lefschetz and Deligne's pgcd theorem ([24, Theorem 3.3]) to reduce it to the curve case. This has been carried out by Madhavan Venkatesh and is covered in the second part of our paper.

Higher étale cohomology groups are even more difficult to handle. For a surface, this can be done (see [27]). For a general threefold, this is still open. However, we can do better for Abelian varieties of arbitrary dimension because of the following theorem (see [28]).

Theorem 3.9. *Let A be an abelian variety as in the last theorem. Then*

$$H^i_{\acute{e}t}(A, \mathbb{Q}_\ell) = \bigwedge_{n=1}^{n=i} H^1_{\acute{e}t}(A, \mathbb{Q}_\ell)$$

.

The following corollary is immediate since we can compute $P_i(T)$, the characteristic polynomial of the action of Frobenius on the ith étale cohomology group (see the Riemann hypothesis part of the Weil conjectures 3.2), we just have to compute $P_1(T)$.

Corollary 3.10. *Computing the zeta function of an abelian variety A over $\mathbb{F}_q$ is in $AM \cap coAM$.*

We now explore another application of point counting on curves over finite fields. We can give an effective bound on the number of torsion points of an Abelian variety over an extension of a number field. Let $X/\mathbb{Q}$ be a smooth curve and $J(X))$ be its Jacobian variety. Then the following is due to Katz (see [29, Appendix]).

Theorem 3.11. *Let K be a number field and A be an abelian variety. Let $\mathfrak{p} \in \mathcal{O}_K$ be an unramified prime ideal. Then*

$$A(K)_{tors} \hookrightarrow A(\mathbb{F}_\mathfrak{p}).$$

However, this does not give us an algorithm to count the torsion points. The first point that comes to mind is whether we can take a lot of primes so that we can compute the torsion size by taking gcd. In [29], Katz has shown a counterexample in which we cannot

get to the torsion point count by taking gcd. But this can help us to get better bounds on the torsion size over number fields. Under the assumption that the rank of the Jacobian is zero (rank in the sense of an abelian group), the above theorem gives us some results. To understand this, the reader needs to be familiar with the Chebotarev density theorem (see, for example, [30]). Let $C/\mathbb{Q}$ be a curve and $J(C)$ be its Jacobian. Since we assume the rank of $J(C)(\mathbb{Q})$ to be zero, under reduction by a good prime p, $\#J(X)(\mathbb{Q})$ divides $\#J(X)(\mathbb{F}_p)$. We have a very high probability that $J(X)(\mathbb{F}_p)$ contains a point that lies on a number field of degree three or more. This is because if this is not the case, then there are some polynomials that do not have $\mathbb{Q}$ roots but $\mathbb{F}_p$ roots. This probability is very low by Chebotarev density, and therefore one would expect to obtain better bounds by repetition with many random primes and taking gcd to remove the errors coming from quadratic extensions over $\mathbb{Q}$.

Chapter 4

Zeta functions of modular curves

In this chapter, we discuss point counting for a special class of curves called modular curves. A modular curve is not always available in the form of a defining equation; instead, there is a different parameter called the level of the modular curve, which we consider as input. We will show how to compute its equation and as a consequence we will be able to show that computing the characteristic polynomial of the action of Hecke operators on the space of cusp forms is in AM $\cap$ coAM.

The first algorithm to compute the zeta function of modular curves over finite field was due to Manin [31]. The key idea in [31] was to compute the action of Hecke operator T_p on the space of modular symbols and use Eichler-Shimura theorem to get to zeta functions. However, the algorithm was exponential in the bit representation of p. Here we provide a survey of a work of Bas Edixhoven [32], showing how to compute Ramanujan tau at a prime p in poly$(\log p)$. His results later gave a polynomial-time algorithm to compute the zeta function of modular curves, assuming the generalized Riemann hypothesis (GRH) over number fields. The result can be referred from [33] and [34] and also [33].

In the following, we will introduce modular curves, modular forms, Hecke operators and explore the connection between modular curves and modular forms. We will show how modular forms allow us to compute the defining equation for modular curves.

4.1 Modular curves

Let $\mathcal{H} \subset \mathbb{C}$ denote the complex upper half-plane and let $\Gamma_0(N)$ denote the congruence subgroup of level N which we define as follows.

$$\Gamma_0(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N}\}$$

It is trivial to check that the above forms a group, it acts on $\mathcal{H}$ as follows.

$$\gamma : z \in \mathcal{H} \mapsto \frac{az+b}{cz+d} \in \mathcal{H}$$

The action called fractional linear transformation defines an automorphism on $\mathcal{H}$ and these actions form the group of all automorphisms of $\mathcal{H}$. We can also see the group $\Gamma_0(N)$, as the group of all symmetries of $\mathcal{H}$. $\mathcal{H}$ quotiented by the action of $\Gamma_0(N)$, denoted as $Y_0(N) = \mathcal{H}/\Gamma_0(N)$ is known as the fundamental domain of the action of $\gamma_0(N)$ on $\mathcal{H}$. It turns out that $Y_0(N)$ is not compact as a topological space and one has to include finitely many points called cusps to compactify it. It follows that this construction makes it a compact Riemann surface. This is due to the Riemann existence theorem, which says that every compact Riemann surface is a complex projective algebraic curve. We denote this complex curve by $X_0(N)$. We denote the genus of $X_0(N)$ as g. It is well known that $g = O(N \log N \log\log N)$ ([35]).

Modular curves $X_0(N)$ are moduli spaces parameterizing complex elliptic curves having cyclic groups of order N. A pair of elliptic curves E, E' over $\mathbb{C}$ are called cyclic N-isogenic, if there exists a map $\phi : E \mapsto E'$ that has a kernel which is a cyclic subgroup of E of order N. Thus, $X_0(N)$ can be seen as parameterizing pairs of complex ellitic curves E, E' with a cyclic N-isogeny. To see this, recall that E can be seen as a quotient of the complex plane $\mathbb{C}$ by a complex lattice $\mathcal{L} = \langle 1, \tau \rangle$. Let $\mathcal{L}'$ be another lattice so that $\mathcal{L} \subseteq \mathcal{L}'$ and $\phi : E = \mathbb{C}/\mathcal{L} \mapsto \mathbb{C}/\mathcal{L}' = E'$, where the map ϕ from E to E' is induced by the inclusion $\mathcal{L} \subseteq \mathcal{L}'$. Let $N = [\mathcal{L}' : \mathcal{L}]$, then we have $N\mathcal{L}' \cong \mathcal{L}'$ and $N\mathcal{L}' \subseteq \mathcal{L}$; therefore, we have the following inclusion of lattice

$$N\mathcal{L}' \subseteq \mathcal{L} \subseteq \mathcal{L}';$$

where the former inclusion induces the maps $\hat{\phi}\, E' \mapsto E$ the dual of ϕ induced by the later inclusion.

4.2 Modular forms

A modular form $f(z)$ for $\Gamma_0(N)$, is a meromorphic function that remains bounded on $\mathcal{H}$ and satisfies the following,

$$f(\gamma z) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-k} f(z),$$

where

$$\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N),$$

where k is a non-negative integer. Note that the modular forms are not invariant under the action of $\Gamma_0(N)$ on $\mathcal{H}$, instead the factor $(cz+d)^{-k}$ appears as an extra term in the RHS. This extra term is called the automorphy factor associated to the form f and the integer k is called the weight of f. The form f has a Fourier series expansion $f(z) = \sum_{i=-\infty}^{\infty} a_n(f) q^n$ where $q = e^{2\pi i z}$, where a_n are zero for all $n < 0$, excluding finitely many. We obtain this Fourier expansion by taking the Laurent series expansion of f on $\mathcal{H}$ and applying the map $z \in \mathcal{H} \mapsto e^{2\pi i z} \in \mathcal{D}$, which maps $\mathcal{H}$ to the unit disc $\mathcal{D}$ centered at the origin of radius one. The Fourier coefficients of a form are related as $a_{mn} = a_m a_n$, for all co-prime m, n and $a_{p^r} = a_{p^{r-1}} a_p - p^{n-1} a p^{n-2}$ for p odd. Thus, a form gets uniquely specified by just the prime indexed coefficients.

The space of all modular forms of weight k for $\Gamma_0(N)$ is a complex vector space and is denoted $M_k(\Gamma_0(N))$. The subspace of $M_k(\Gamma_0(N))$ that vanishes on the cusps of $X_0(N)$ is denoted $S_k(\Gamma_0(N))$, known as the space of cusp forms of weight k.

Example 4.1. *Important examples of modular forms are the Eisenstein series of weight* $2k$; $k \geq 2$ *which are of the following form.*

$$G_{2k}(\tau) = \sum_{(m,n) \in \mathbb{Z}^2 / \{0,0\}} \frac{1}{(m+n\tau)^{2k}}.$$

These functions come up in the context of deriving an equation for complex elliptic curves.

Remark 4.1. Another important modular form that arises in connection with complex elliptic curves is the discriminant modular form $\Delta(z)$. It is a modular form of level 1 and weight 12 that has the following form.

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n = q \prod_{n>0} (1-q^n)^{24};\ q = e^{2\pi i z}.$$

where $\tau(n)$ is defined as the Ramanujan tau function. Ramanujan conjectured that $|\tau(p)| \leq 2p^{11/2}$, p being a prime, which was proved by Deligne using the theory of étale cohomology [36]. As we shall see, this connection between étale cohomology and Ramanujan tau actually gives us an algorithm to compute $\tau(p)$ in $\text{poly}(\log p)$. This was the result of [32]. In general, for the pth Fourier coefficent $a_p(f)$ of an eigen-cusp form f, its absolute value is upper bounded by $\sqrt{p}$ (see, for example, [37]).

Definition 4.2 (Hecke operator)**.** The mth Hecke operators denoted as T_m, for $m \geq 1$ are linear operators on $M_k(\Gamma_0(N))$ acting as follows. Let $f = \sum_{i=0}^{\infty} a_i q^i \in M_2(\Gamma_0(N), \mathbb{C})$ and let $T_p(f) = \sum_{i=0}^{\infty} b_i q^i$, then we have

$$b_n = \sum_{d>0,\, d|(n,p)} d^{k-1} a_{np/r^2} \tag{4.2.1}$$

The $\mathbb{Z}$-algebra generated by all T_m of weight k and level N is denoted as $\mathbb{T}(N, k)$. In addition, the Hecke operators of different levels are related as $T_{mn} = T_m T_n$ for co-prime m, n and $T_{p^r} = T_{p^{r-1}} T_p - p^{n-1} T p^{n-2}$ for p odd. Therefore, it is clear that $\mathbb{T}$ is generated by T_p for all prime p.

Definition 4.3 (Hecke polynomial)**.** Let the genus of $X_0(N)$ be g. The characteristic polynomial of the Hecke operator acting on $S_2(\Gamma_0(N))$ is called the Hecke polynomial. It is a monic integral polynomial of degree g.

4.3 Modular forms and Galois representations

There is a fundamental way via which modular forms rise from elliptic curves over $\mathbb{Q}$ that is worth mentioning. The Dirichlet L series is a series of the following form.

$$L(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s};$$

where $a_n \in \mathbb{C}$ and s is a complex variable. Provided that the growth of a_n is polynomial in n, the series locally uniformly converges in a region of the complex plane with $\text{Re}(s) > C$, C being a constant. The most famous example of an L series is the Riemann zeta function (substitute $a_{n\geq 1} = 1$). For every modular form $f = \sum_{n=1}^{\infty} a_n q^n$ we have an associated Dirichlet series as $L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Recall the Hasse-Weil zeta function of E reduced

at a prime p; it has the following form

$$\frac{L_p(T)}{(1-T)(1-pT)};$$

where $L_p(T) = 1 - a_pT + T^2$; $a_p \in \mathbb{Z}$. Let us denote the set of all good primes of reduction of E as $S \subset \mathbb{Z}$ (this means that E mod p is an elliptic curve for all $p \in S$). The L-function of E is defined as

$$L(E,s) = \prod_{p \in S}(1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \notin S}(1 - a_p p^{-s})^{-1} = \sum_{n=1}^{\infty} a_n n^{-s};$$

where $a_p = \{-1, 0, +1\}; \forall p \notin S$, depending on the type of bad reduction. If we expand the above as a Dirichlet series, the series corresponds to a Dirichlet series of a cusp eigenform of weight 2. We state this in the following.

Theorem 4.4 (Modularity theorem)**.** *Let E be an elliptic curve over $\mathbb{Q}$ and p be a prime of good reduction, that is, E stays non-singular when reduced at p. Then the sequence of integers $p + 1 - \#E(\mathbb{F}_p)$, for the primes of good reduction p, forms the pth coefficient of a cusp form of weight* 2.

This was proved by Wiles [3] to complete his proof of Fermat's last theorem. The proof of the above follows by showing that for level N integral modular forms, there exists an elliptic curve with conductor N and a map $J_0(N) \mapsto E$. These elliptic curves occur as quotients of the modular Jacobian $J_0(N)$. The connection between Hecke eigen values and the point counts (as stated above in the theorem) can be obtained by constructing a two-dimensional representation of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Recall from Schoof that we can compute the coefficients a_p in time $\mathrm{poly}(\log p)$. Therefore, this gives us the following result.

Corollary 4.5. *For an elliptic curve $E/\mathbb{F}_q$, one can compute the pth coefficient of the associated cuspform for an arbitrary p in run-time poly*$(\log p)$.

The basis for the proof of modularity is due to the work of Eichler, Shimura and Deligne, one can attach to every modular form of weight k, a two-dimensional representation of the absolute Galois group. In this section, we will give a brief overview of the proof. The following theorem due to Eichler and Shimura [38] states the relation between the Frobenius map at p and the Hecke operator T_p in the endomorphism ring of $J_0(N)$.

Theorem 4.6 (The Eichler-Shimura relation)**.** *Let $Frob_p$ and T_p denote the Frobenius Hecke action at p respectively, on $J_0(N)$ mod p. Then they are related as follows*

$$T_p = Ver_p + Frob_p$$

where $Ver_p \cdot Frob_p = Frob_p \cdot Ver_p = p$.

Due to the Eichler-Shimura theorem stated below, one can associate to every cusp form of weight two, a two-dimensional Galois representation as follows.

Theorem 4.7 (Two dimensional representation of modular forms)**.** *Let f be a cusp form of weight 2 for $\Gamma_0(N)$. Then one can attach a two-dimensional representation as follows,*

$$\rho_f : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \mapsto GL_2(\overline{\mathbb{Q}_\ell})$$

such that for all $p \nmid N\ell$, we have ρ_f unramified and the image of Frobenius at p has characteristic polynomial, $x^2 - a_p(f) + p$.

Here we give a basic overview of the proof. We assume some knowledge of sheaf. Recall that the first ℓ-adic étale cohomology group $H^1(X_0(N), \mathbb{Q}_\ell)$ is a $2g$ dimensional vector space over $\mathbb{Q}_\ell$, g being the genus of $X_0(N)$. This is isomorphic to the ℓ-adic Tate module of the modular Jacobian $J_0(N)$ base changed to $\mathbb{Q}_\ell$. We can consider the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the Tate module. Let Ω is defined as the sheaf of holomorphic differentials generated by the differential 1-forms df for a modular form f and $H^0(X_0(N), \Omega)$ is its global section (this is the zeroth De-Rham cohomology group described in Section 2.3). Now we have a Hodge decomposition, $H^1_{\text{sing}}(X_0(N), \mathbb{C}) \cong H^0(X_0(N), \Omega) \oplus \overline{H^0(X_0(N), \Omega)}$ and $S_2(\Gamma_0(N)) \cong H^0(X_0(N), \Omega)$ on the map $f \mapsto df$. From the comparison theorem ([14, Appendix C]) we have $H^1_{\text{sing}}(X_0(N), \mathbb{C}) \cong H^1_{\text{étale}}(X_0(N), \mathbb{C})$. Therefore we have the following,

$$H^1_{\text{ét}}(X_0(N), \mathbb{C}) \cong S_2(\Gamma_0(N) \oplus \overline{S_2(\Gamma_0(N)}) \tag{4.3.1}$$

From the observation that the Fourier coefficients of the eigenforms of T_p of $S_2(\Gamma_0(N))$ are totally real, $\overline{S_2(\Gamma_0(N)} \cong S_2(\Gamma_0(N)$. It also follows that T_p is diagonalizable. The eigenvalues of T_p are totally real; hence, the associated matrices are hermitian. Due to the existence of Petersson's inner product, we have a spectral decomposition. Therefore, with a cuspform f we can associate a two-dimensional subspace of $H^1_{\text{ét}}(X_0(N), \mathbb{C})$. Now we can use Theorem 4.6 to apply $\mathrm{Frob}_p + \mathrm{Ver}_p$ and the operator T_p on the LHS and the RHS of 4.3.1 respectively, to obtain the result. In case the cusp form f has integer coefficients, the

two-dimensional subspace of $H^1_{\text{ét}}(X_0(N), \mathbb{C})$ is precisely the ℓ-torsion subspace associated with the elliptic curve corresponding to f which occurs as a quotient of $J_0(N)$. □

We conclude this section by stating a connection between modular forms of weight $k > 2$ and weight 2 ([39]). We have seen how the modular forms of weight 2 are related to the first étale cohomology of modular curves. When $k > 2$ then the analogues result can be referred from [32, Theorem 2.5.2]. However, that does not give us efficient ways to compute coefficients of these higher weight modular forms. We have a way around it, which is due to the following.

Theorem 4.8. *Let f be a cuspidal eigenform of weight $\ell \geq k > 2$ and level N, ℓ being a prime. Then there is a weight 2 cuspform f' of level $N\ell$ such that $f \cong f' \bmod \ell$.*

Recall that the weight of the two cuspforms was realized under the Hodge decomposition of the first étale cohomology of $X_0(N)$. In the case of higher-weight modular forms of level N, we can realize it under the Hodge decomposition of the first étale cohomology of a separate variety called the Kuga sato variety ([32, Section 2.4]). For the proof of the reduction, refer [32, Section 2.5] and also [40]. The following corollary follows from [32, Thm 2.5.2].

Corollary 4.9. *Let f' be a weight k eigen-cuspform, of level N, then we have a two-dimensional representation of the absolute Galois group over $\mathbb{Q}$ similar to that of Theorem 4.7, the only difference being that the representation occurs in $J_0(N\ell)[\ell]$ and the characteristic polynomial of the Frobenius action is $x^2 - a_p x + p^{k-1}$.*

Consider $X_0(N)$, the modular forms of level N and weight 1 are the rational functions of $X_0(N)$. The higher-weight modular forms arise from a more geometric point of view. We will see this in the next section.

4.4 Modular forms as line bundles

We will now introduce modular forms in a more geometric way. In particular, we will state what a twisting sheaf is on a projective curve and what we mean by very ample line bundles. We will see that modular forms can be realized as a twisted sheaf on the modular curves. Using this machinery, we can use modular forms to find the equation of a modular curve, as we will see in the next section. In the following, we will briefly introduce the theory of sheaves.

Let $X/\mathbb{F}_q$ be an algebraic curve and let $\mathcal{O}_X$ denote its structure sheaf, the sheaf of regular functions on X. A line bundle $\mathcal{L}$ is an invertible sheaf, which associates a $\mathcal{O}_X(U)$ module to all open sets $U \subseteq X$. We can associate a divisor to every line bundle and vice versa (see, for example, [14, Chapter 2, Section 6]). The degree of a line bundle, denoted as $\deg(\mathcal{L})$, is the degree of the associated divisor, denoted as $\mathcal{L}(D)$.

Definition 4.10 (Very ample line bundles)**.** A line bundle $\mathcal{L}$ on an algebraic curve C over an algebraically closed field is very ample if $\deg(\mathcal{L}) \geq 2g + 1$, g being the genus of C.

A very ample line bundle $\mathcal{L}$ shares many important properties with regard to embeddings in projective space. For example, consider a line bundle $\mathcal{L}$ such that $\dim(H^0(X, \mathcal{L})) = n + 1$. Suppose that $\phi : X \to \mathbb{P}^n$ is an embedding of X in the n-dim projective space using the global sections of $\mathcal{L}$, where a point $P \in X$ is mapped to $s_1(P) : s_2(P) : \ldots : s_{n+1}(P) \in \mathbb{P}^n$. The global sections of a very ample line bundle $\mathcal{L}$ give rise to a closed immersion of X to $\mathbb{P}^n$ such that the pullback of the global sections of the sheaf $\mathcal{O}(1)$ (generated by $x_0, \ldots, x_n$) on $\mathbb{P}^n$ corresponds to the global sections of $\mathcal{L}$ on C.

Lemma 4.11. *A modular form of weight $2k$ can be seen as the global section of the canonical sheaf raised to power k. The divisor corresponding to it is the kth multiple of the canonical divisor K.*

For modular curves $X_0(N)$, let Ω denote the canonical bundle. The fact that the global sections of Ω are isomorphic to the space $S_2(\Gamma_0(N))$ follows from [41, Lemma 2]. Recall that K denotes the canonical divisor and since Ω is the corresponding line bundle, $\deg(\Omega) = 2g - 2$. Now we proceed to computing the defining equation.

4.5 The defining equation for modular curves

From the Riemann existence theorem we have $X_0(N)$ is a projective curve over $\mathbb{C}$ and, therefore, has an equation defined over $\mathbb{C}$. It can be shown that the defining equation of $X_0(N)$ is actually over $\mathbb{Z}$, there are several ways to show this. Shimura [38, Proposition 6.9] showed that $X_0(N)$ admits the structure of projective algebraic curve over $\mathbb{Q}$ by showing that the space $S_2(\Gamma_0(N), \mathbb{C})$ is spanned by basis elements having Fourier coefficients in $\mathbb{Q}$. After that, due to Deligne and Rapoport [42] we have $S_2(\Gamma_0(N), \mathbb{C})$ has a basis over $\mathbb{Z}$. Therefore, it has an equation over $\mathbb{Z}$ and hence, over $\mathbb{F}_p$ for all good primes p.

As a side note, we should remark that there is a standard polynomial called the modular polynomial that defines the equation of $X_0(N)$. Recall that a point $\tau \in X_0(N)$

parametrizes a complex elliptic curve by the lattice $\langle 1, \tau \rangle$. Consider the j-invariant, a modular form of level one and weight zero, which is defined via its Fourier expansion as follows.

$$j(\tau) = \frac{1}{q} + 744 + \sum_{i=1}^{\infty} a_n q^n;$$

where $q = e^{2\pi i n \tau}$ and $a_n \in \mathbb{Z}$. Then we can show that $j(\tau)$ and $j(N\tau)$ are algebraically dependent, and the annihilating polynomial is known as the Nth modular polynomial.

However, we did not compute this in our algorithm. Instead, we use the result of Fujita, St. Donat, and Mumford, which says that given a line bundle $\mathcal{L}$ with $\deg(\mathcal{L}) \geq 2g + 2$, the equation of the curve embedded in the projective space by the global sections of $\mathcal{L}$ is generated by quadrics. If we have access to global sections of such line bundles, we can use this to set up a system of linear equations to find the quadrics. We first give the construction of such line bundles and then we will explain how to find the quadrics.

From [43, corollary 12.3.12] we have $S_2(\Gamma_0(N), \mathbb{C}) \cong S_2(\Gamma_0(N), \mathbb{Z}) \otimes \mathbb{C}$. Therefore, we can take the base change $S_2(\Gamma_0(N), \mathbb{Z}) \otimes \mathbb{F}_p$ for $p \nmid N$ and from [43, Theorem 12.3.2] it follows that $S_2(\Gamma_0(N), \mathbb{Z}) \cong S_2(\Gamma_0(N), \mathbb{Z}) \otimes \mathbb{F}_p$.

From [44], it follows that any modular form can be uniquely specified by its first few Fourier coefficients $(a_1(f), \ldots, a_r(f))$ up to the index $r = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]/6$. Recall the definition of homology groups from Section 2.2. In the homology group, it is not easy to represent elements and perform computations. There is an explicit group called the group of modular symbols that is isomorphic to $\mathcal{H}_1(X_0(N), \mathbb{C})$ ([45, Section 8.1]). This allows one to compute the Hecke action explicitly and compute the Hecke polynomial. As follows from [45, Section 3,8], we can compute the Hecke polynomials for T_p in run-time polynomial in p (see [45, Section 8.3.3]). Then it comes down to finding the roots of the above polynomial over the field of definition of $X_0(N)$, which can be done in $\mathrm{poly}(N, \log p)$ by using standard root finding algorithms like Berlecamp Rabin. Therefore, we have the following lemma.

Lemma 4.12. *The Hecke eigenvalues of Hecke operators $T_2, \ldots, T_r$ can be computed over finite fields of characteristic p in time poly$(\log p, N)$, where p is coprime to N and $r = [SL_2(\mathbb{Z}) : \Gamma_0(N)]/6$.*

The only thing left is to map the eigenvalues obtained to a specific eigenform, which would give the eigenbasis of $S_2(\Gamma_0(N))$. In order to do so, we first group the individual eigenforms

which are conjugate to each other under the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. We factor the polynomials obtained from the lemma 4.12, factor them over $\mathbb{F}_p$ and map the irreducible factors to one another clearly this can be done in $\mathrm{poly}(g, \log p)$ and hence $\mathrm{poly}(N, \log p)$. Thus, the problem of mapping eigenvalues is reduced to groups of Hecke operators $f_1, \ldots, f_n$ stable under Galois action.

Now we need to map the eigenvalues among the stable Galois conjugacy classes of eigenforms, to do this we need eq. 4.2.1. Recall that we have obtained a set of irreducible polynomials of the same degree whose roots are the eigenvalues of eigenforms fixed under the action of the absolute Galois group over $\mathbb{F}_p$.

Algorithm Computing an eigenbasis for the space $S_2(\Gamma_0(N))$ over $\mathbb{F}_p$.
Input: A set of $r-1$ irreducible polynomials $V_2, \ldots, V_r$ where $r = [\Gamma_0(N) : SL_2(\mathbb{Z})]/6$, of fixed degree d whose roots over $\overline{\mathbb{F}}_p$ are eigenvalues corresponding to eigenforms stable under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.
Output: A set of eigenbasis stable under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

- Fix a degree d extension over $\mathbb{F}_p$, call it $\mathbb{F}_q$ where $q = p^d$. Find all the roots of the input polynomial V_2 in $\mathbb{F}_q$ using Berlekamp-Rabin algorithm.
- Let α be one eigenvalue obtained from the last step and let f_1 be the eigenform having α as the second Fourier coefficient. We apply eq. 4.2.1 to compute the second Fourier coefficient of $T_3(f)$, let it be α'.
- Compute the roots of V_3 in $\mathbb{F}_q$ and pick a root β_1 s.t. $\alpha_1\beta_1 = \alpha_1'$. Hence, β_1 is the third Fourier coefficient of f.
- For each $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, map α^σ to β^σ. It is clear that these satisfies $\alpha_1^\sigma\beta_1^\sigma = \alpha_1'^\sigma$. From this we obtain the q-expansion upto the third Fourier coefficient of $f_1, \ldots, f_d$.
- Apply the above steps repeatedly upto the Sturm bound r, so that we obtain the q-expansion of $f_1, \ldots, f_d$ upto the sturm bound. Return $f_1, \ldots, f_d$.

Lemma 4.13. *An eigenbasis for the space $S_2(\Gamma_0(N))$ reduced at a prime $p \nmid N$ can be efficiently computed in time poly$(N, \log p)$.*

Now, we can use this to set up a system of quadrics defining $X_0(N)$. Here we note that the Hecke eigenvalues may not be integers but algebraic integers. We use the eigenforms to compute the $\mathbb{Z}$-basis of $S_2(\Gamma_0(N))$. The quadrics in $\mathbb{P}^{g-1}$ are degree four homogeneous polynomials, applying the pullback map of $x_1, \ldots, x_n$, we get the same system with x_i

replaced by f_i. That would give us a zero modular form in $S_2(\Gamma_0(N))$ since all the points of $X_0(N)$ are evaluated to zero. We use the Z-basis of $S_2(\Gamma_0(N))$, multiply them to form a quadric with unknowns, and solve a system of linear equations over $\mathbb{F}_p$ to find the quadrics. However, to perform the linear algebra operation, one has to go to an exponentially large degree extension, to represent the set of all eigenvectors. We would achieve this by a little modification of the query request that Arthur makes to Merlin. We will talk in details on this in Section 4.7.

4.6 Computing Ramanujan Tau in polynomial time

Recall Corollary 4.5, which stated that given an elliptic curve over $\mathbb{F}_q$ one can compute the pth coefficient of the associated cusp form by modularity, in polynomial time by counting points on the elliptic curve. Now, the following question arises; Is there an algorithm that can compute the pth coefficient of the cusp form without having access to the associated elliptic curve? The answer to this question is yes, the idea being first to construct the modular curve and then come down to the elliptic curve by taking a quotient of the modular Jacobian by an Abelian subvariety. The material of this section is from [32].

In Schoof's algorithm (Section 3.3), we have seen that we can go to an extension so that we have all the ℓ-torsions present (Lemma 3.3). Recall from Theorem 4.7 we have a two-dimensional representation of the Galois group attached to all modular forms of weight k, where the Frobenius at p satisfies a characteristic polynomial $x^2 - a_p x + p$ where a_p is the pth Fourier coefficient of f. Therefore, similarly to Schoof, we can work on the ℓ-torsion points of $J_0(N)$ where the representation associated with f takes place, define it as V_f. The problem is how to explicitly find the ℓ-torsion subspace V_f for a particular modular form f.

The first thing to show is how to obtain an ℓ-torsion divisor. An approach is to consider cuspidal divisors. A divisor D in $J_0(N)$ is called a cuspidal divisor if the support of D consists of only the cuspidal points of $X_0(N)$. The significance of a cuspidal divisor is that it is always torsion (Manin-Drinfeld theorem). They have shown how to approximate a cuspidal point of appropriate order in $J_0(N)$. Instead of working on $J_0(N)$ directly, they work on $X_0(N)^g$ so we can identify a tuple of cusps $(P_1, \ldots, P_g) \in X_0(N)^g$ with a torsion divisor $P_1 + \ldots + P_g - g\infty$. This is the content of [32, Ch. 8-12] and requires a lot of heavy machinery from Arakaelov theory, and the techniques involved are purely complex analytic.

Another approach to obtain the ℓ-torsion is to assume access to the defining equation. This line of approach was given by Couveignes, see [46] and is more computation-friendly. By [31], the zeta function of $X_0(N)$ reduced at small primes p, is computable in poly(p). In this scenario, one can come up with the ℓ-torsions of $J_0(N)$ using [46, Theorem 1]. Using the Arakaelov theory, an explicit upper bound on the height of a torsion point embedded in $\mathbb{P}^1_{\mathbb{Q}}$ can be obtained. Therefore, if we can compute $V_{f,\mathbb{F}_p}$ for many primes p we can obtain $V_{f,\mathbb{Q}}$ by the Chinese remainder.

By [46, Lemma 22] we have the action of Hecke action on the torsions in polynomial time. Take $f = \Delta$, where $\Delta = \sum_{n-1}^{\infty} \tau(n)q^n$ is the discriminant modular form. Assume $\ell \nmid \tau(p)^2 - 4p^{11}$. Recall that the discriminant modular form is of level 1 so from Theorem 4.8 it follows that $V_\Delta \subset J_0(\ell)$. Now, the determination of $V_{f,\mathbb{F}_p}$ follows from [46, Section 12].

Recall that from Corollary 4.9, we have the characteristic polynomial of the Frobenius action at a prime $p \neq \ell$ on V_Δ is $x^2 - \tau(p) + p^{11}$. Recall that we have the Ramanujan bound $\tau(p) \leq 2p^{11/2}$, therefore, we can apply the same steps as in Schoof, compute $\tau(p)$ mod ℓ for many primes ℓ satisfying $\ell \nmid \tau(p)^2 - 4p^{11}$ and obtain $\tau(p)$ over $\mathbb{Z}$ by the Chinese remainder.

4.7 Some unconditional complexity results on counting points on modular curves and computing Hecke polynomials

Here, we give some unconditional algorithms and protocols to compute the zeta functions and Hecke polynomials for $X_0(N)$.

Recall the strategy we developed in Section 4.5. The coefficients of the $\mathbb{Z}$-basis of $S_2(\Gamma_0(N))$ can be upper bounded by the bound of the Fourier coefficients of the eigen-cusp forms. This gives a bound on the integer coefficients of the system of quartic polynomials that we will obtain.

Recall that for every eigen-cusp form we have a two-dimensional group of ℓ-torsions corresponding to the associated Galois representation. Also, the degree of extension over the base field of the field of Fourier coefficients of an eigen-cusp form is very less (Lemma 3.3). Therefore, the Galois-conjugate cuspforms have isomorphic fields of Fourier coefficients. Therefore, over finite fields we have this to be a unique extension over the base field. By

Chebotarev density, we have a lot of primes so that the Hecke polynomial has fewer number of irreducible factors. The idea is in the AM ∩ coAM protocol, Arthur queries Merlin to send a modified certificate consisting of all these primes. Now, we can compute the quartics modulo these primes and take the Chinese remaindering to obtain the quartics over integers. This now can be used to complete the protocol. Therefore, we have the following.

Theorem 4.14. *Computing the zeta function of the modular curve $X_0(N)$ is in AM ∩ coAM.*

Now we come to the computation of the Hecke polynomial.

Proposition 4.15. *Consider the modular curve $X_0(N)$ defined over $\mathbb{F}_p$. Let $T_p \in \mathbb{T}(N, 2)$ be the pth Hecke operator. Let $h(T)$ be the Hecke polynomial of T_p on $S_2(\Gamma_0(N), \overline{\mathbb{F}}_p)$. Then,*

$$h(q+1) = |J_0(N)_{\mathbb{F}_p})(\mathbb{F}_q)|,$$

where $\mathbb{F}_q$ is a degree d extension over $\mathbb{F}_p$.

Proof. Let Frob_p denote the pth and Ver_p are as in proposition 4.6. We have the identity

$$\mathrm{Frob}_p \cdot \mathrm{Ver}_p = p$$

over the endomorphism ring of $J_0(N)$ reduced at p. From the Eichler-Shimura relation we have the Hecke operator at p related to Frob_p as stated in Proposition 4.6. Over $\mathbb{F}_q$, we have $T_q = \mathrm{Ver}_q + \mathrm{Frob}_q$ over $J_0(N)(\mathbb{F}_q)$, where $T_q = (T_p)^d$ is computed by composing T_p with itself d times. Now, the above follows from the fact that $P(1) = |J_0(N)_{\mathbb{F}_q})(\mathbb{F}_q)|$, where $P(T)$ is the characteristic polynomial of the action of Frobenius at p on the Tate module of $J_0(N)$. □

We already have the verification of the group orders in AM ∩ coAM. For a given polynomial we generate the candidate counts over extensions of the base field and verify them. From ([7, Section 8]) we need to verify the count upto an extension that is maximum of 18 and $2g$, g being the genus. Therefore, we have the following.

Corollary 4.16. *Computing the Hecke polynomial for the action of T_p on $S_2(\Gamma_0(N))$ is in AM ∩ coAM.*

Chapter 5

Conclusion

After our result on the curves, the immediate improvement could be to show that the zeta functions of smooth projective curves is in NP $\cap$ coNP. However, from the algorithm we have seen so far, it did not give us an idea to show this. Modular curves are a special case where we have a two-dimensional representation associated to cuspforms. That allowed us to break the computation into parts. For a general curve, we do not have this structure. So, it is not clear what certificate Merlin could present that Arthur can verify efficiently.

At this point, it seems that computing zeta functions of varieties requires an entirely new mathematical idea. Some belief is there that it may come from mathematical physics, namely from the directions of Gauss-Manin connections (although these directions are all p-adic), or some analytic results on the zeta function might prove helpful.

Since we have shown that computing the zeta function of curves is in AM $\cap$ coAM, the problem is unlikely to be an NP-hard problem. Therefore, the search for a polynomial-time algorithm will continue. In case of ℓ-adic algorithms we can believe that it runs exponentially in the genus g, since mostly we use the ℓ-torsion points in this case and we cannot do better if we do not have a nice structure on the ℓ-torsions as in modular curves. But in the case of p-adic algorithms, we do not yet have a proof that the runtime will always be a polynomial in p and g. Why would a huge class of p-adic cohomology theories always yield the same runtime? Could there exist a p-adic algorithm that would perform better in both parameters? We need to answer these fundamental questions to find solutions to the bigger problem.

Chapter 6

Appendix

6.1 Torsions of modular curves

In this part, we provide some insight into the torsion subgroup of $X_0(N)$. We will see that the computation of torsion subgroup of prime levels is much easier to handle than that of a composite level. For prime leveled modular curves, Ogg conjectured ([47]) that $J_0(N)(\mathbb{Q})_{\text{tors}}$, the rational torsion subgroup of $J_0(N)$ equals the order of the cuspidal subgroup denoted as $\mathcal{C}_N$. Two years later, Mazur ([48]) proved the conjecture, showing that $J_0(N)(\mathbb{Q})_{\text{tors}}$ is a cyclic group, generated by the cuspidal divisor class of $(0) - (\infty)$. This element is the generator of all cuspidal divisors since, for prime levels (0) and (∞) are the only two cusps. Its order computation came from a third object called Tamagawa numbers, since for prime levels this equals both the order of $J_0(N)(\mathbb{Q}_{\text{tors}})$ and $\mathcal{C}_N$. Thus, for prime levels, Mazur gave the group structure as well.

However, these structural results do not give us an algorithm to compute the torsion order or even the cuspidal order. A standard approach to the upper bound on the order of the torsion subgroup comes from [29, Appendix], which says that for unramified primes $\mathfrak{p}$ in the Hecke field K, the reduction map

$$J_0(N)_{\mathcal{O}_K} \to J_0(N)_{\mathfrak{p}}$$

results in injection of the torsion points into $J_0(N)_{\mathfrak{p}}$. Now, under the assumption that the Mordell-Weil rank of $J_0(N)$ is zero over K, one can apply standard point counting algorithms to compute $J_0(N)(\mathbb{F}_{\mathfrak{p}})$. In fact, the order of $J_0(N)(K)_{\text{tors}}$ divides the order of $J_0(N)(\mathbb{F}_{\mathfrak{p}})$, so one can try to reduce it over many primes and take their gcd. But that does

not guarantee us the number of steps needed for this algorithm to halt. Also, it does not give us any control over the error (the number of torsion in an extension of K, lying in $J_0(N)(\mathbb{F}_{\mathfrak{p}})))$ occurring by reducing modulo $\mathfrak{p}$.

According to Manin-Mumford conjecture which is now a theorem due to Raynaud, says that for smooth, projective, geometrically irreducible curves C of genus at least 2, $C \cap J_{\text{tors}}$ is always finite. Here, J refers to the Jacobian variety of C. Matthew Baker showed that for the modular curve $X_0(N)$, $X_0(N) \cap J_0(N)_{\text{tors}}$ is precisely the cuspidal subgroup ([49, Proposition 4.1]). Few years later, Bjorn Poonen came up with an algorithm with run-time exponential in $\log p$ to compute the intersection $C \cap J_{\text{tors}}$ for a projective geometrically irreducible curve C of genus at least 2 ([50]). Therefore, this could be a promising direction for torsion count, although there is no guarantee of effectivity in complexity.

As pointed out in the previous section, the first result on the problem of counting torsion points of $X_0(N)$ was due to Mazur ([48]) for prime levels. In this case he provided a formula for counting torsion points over $\mathbb{Q}$, which also worked for the cuspidal subgroup since the two are equal in this case. Later, Takagi (see [51], [52]) gave a formula (class number formula) for the size of the cuspidal subgroup, for square-free levels. But since we need the factors of N for the formula to apply, it would be no better than a quantum algorithm. In the square full case, he gave a formula which only applies for $X_1(N)$ and it is quite disjoint approach from the case of $X_0(N)$.

Recall that the cuspidal subgroup of $X_0(N)$ always injects into the torsion subgroup of $J_0(N)$ ([31] and [53]). We only have some partial result towards the equality of the torsion and the cuspidal order for composite level modular curves, comes from Lorenzini's work ([54]). He showed that for a prime p, if $N = p^k$ the prime to $2p$ part are equal for these two groups. For N square-free, a recent work of Ribet and Wake has shown that for a prime p, the p-primary part ($p \nmid 6N$) of the cuspidal subgroup and rational torsion subgroup are equal.

Bibliography

[1] C. F. Gauss, *Werke*, vol. 1. Cambridge university press, Nov 2011.

[2] C. F. Gauss, *Werke*, vol. 1. Cambridge university press, Nov 2011.

[3] A. J. Wiles, "Modular elliptic curves and fermat's last theorem," *Annals of Mathematics*, vol. 141, pp. 443–551, 1995.

[4] R. P. Langlands and M. Rapoport, "Cshimuravariet¨aten und gerben," *Journal für die reine und angewandte Mathematik*, vol. 378, p. 113–220, 1987.

[5] N. B. Châu, "Endoscopy theory of automorphic forms," 2010.

[6] J.-P. Serre, *Lectures on $N_X(p)$*. CRC Press, 2016.

[7] K. S. Kedlaya, "Quantum computation of zeta functions of curves," *computational complexity*, vol. 15, pp. 1–19, 2006.

[8] J.-P. Serre, *Algebraic groups and class fields*. Springer, 1988.

[9] A. Grothendieck *et al.*, "Cohomologie ℓ-adique et fonctions L (SGA V)," *Lecture Notes in Math*, vol. 589, 1977.

[10] J. S. Milne, *Etale cohomology (PMS-33)*. Princeton University Press, 1980.

[11] S. Arora and B. Barak, *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[12] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM journal on Computing*, vol. 26, 1997.

[13] J. Watrous, "Quantum algorithms for solvable groups," *Annual ACM Symposium on Theory of Computing*, vol. 33, pp. 60–67, 6 July, 2001.

[14] R. Hartshorne, *Algebraic geometry*, vol. 52. Springer Science & Business Media, 2013.

[15] A. Weil, "Numbers of solutions of equations in finite fields," 1949.

[16] B. Dwork, "On the rationality of the zeta function of an algebraic variety," *Amer. J. Math*, vol. 82, pp. 631–648, 1960.

[17] K. S. Kedlaya, "Fourier transforms and p -adic 'weil ii'," *Compositio Mathematica*, vol. 142, no. 6, 2006.

[18] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," *Mathematics of Computation*, vol. 1968/69, pp. 139–172, 1971.

[19] J. Pila, "Frobenius maps of abelian varieties and finding roots of unity in finite fields," *Mathematics of Computation*, vol. 55, no. 192, pp. 745–763, 1990.

[20] K. S. Kedlaya, "Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology," *J. Ramanujan Math. Soc.*, 2001.

[21] A. G. Lauder, "Rigid cohomology and p-adic point counting," *Journal de Théorie des Nombres de Bordeaux*, vol. 17, pp. 169–180, 2005.

[22] A. G. Lauder and D. Wan, "Counting points on varieties over finite fields of small characteristic," *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, 2006.

[23] D. Harvey, "Counting points on hyperelliptic curves in average polynomial time," *Annals of Mathemetics*, vol. 179, no. 2, pp. 783–803, 2014.

[24] D. Roy, N. Saxena, and M. Venkatesh, "Computational complexity of the characteristic polynomial of Frobenius on the first étale cohomology group."

[25] A. Weil, *Variétés abéliennes et courbes algébriques*, vol. 32. Paris, 1948.

[26] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung.* Walter de Gruyter, Berlin/New York Berlin, New York, 1936.

[27] N. Saxena and M. Venkatesh, "Counting points on surfaces in polynomial time."

[28] J. S. Milne, "Abelian varieties (v2.00)," 2008. Available at www.jmilne.org/math/.

[29] N. M. Katz, "Galois properties of torsion points on abelian varieties," *Inventiones Mathematicae*, vol. 62, p. 481–502, 1981.

[30] H. Lenstra, "The chebotarev density theorem." Available at https://websites.math.leidenuniv.nl/algebra/Lenstra-Chebotarev.pdf.

[31] J. I. Manin, "Parabolic points and zeta functions of modular curves," *Mathematics of the USSR-Izvestiya,*, vol. 6, no. 1, 1972.

[32] J. M. C. Bas Edixhoven, J. Bosman and R. D. Jong, "Computational aspects of modular forms and galois representations," *Annals of Mathematics*, January 8, 2011.

[33] P. Bruin, "Computing coefficients of modular forms," *Publications mathématiques de Besançon*, pp. 19–36, December 2009.

[34] A. Javanpeykar and P. Bruin, "Polynomial bounds for arakelov invariants of belyi curves," *Algebra and Number Theory*, vol. 8, no. 1, p. 89–140, 2014.

[35] J. A. Csirik, J. L. Wetherell, and M. E. Zieve, "On the genera of $x_0(n)$."

[36] P. Deligne, "La conjecture de Weil : II," *Publications Mathématiques de l'IHÉS*, vol. 52, pp. 137–252, 1980.

[37] J. Serre, *A course in Arithmetic*. Springer, 1973.

[38] G. Shimura, "Introduction to the arithmetic theory of automorphic functions," *Publications of the Mathematical Society of Japan*, vol. 11, 1994.

[39] B. Edixhoven, "The weight in serre's conjectures on modular forms," *Inventiones Mathematicae*, vol. 109, pp. 563–594, 1992.

[40] B. H. Gross, "A tameness criterion for galois representation associated to modular forms (mod p)," *Duke Mathematical Journal*, vol. Vol. 61, no. 2, October 1990.

[41] N. Murabayashi, "On normal forms of modular curves of genus 2," *Osaka Journal of Mathematics*, vol. 29, p. 405–418, April 24, 1991.

[42] P. Deligne and M. Rapoport, "Les schémas de modules de courbes elliptiques," *Lecture notes in mathematics, Antwerp, Belgium*, vol. 349, pp. 143–316, 1972.

[43] F. Diamond and J. Im, "Modular forms and modular curves," *Canadian mathematical society, conference proceedings*, vol. 17, 1995.

[44] J. Sturm, "On the congruence of modular forms," 1987.

[45] W. Stein, *Modular forms: A computational approach*. AMS, 1991.

[46] J. M. Couveignes, "Linearizing torsion classes in the picard group of algebraic curves over finite fields," *Journal of Algebra*, vol. 321, no. 8, pp. 2085–2118, April 15, 2009.

[47] A. Ogg, "Rational points on certain elliptic modular curves," *Bulletin of the American Mathematical Sociaty*, vol. 81, no. 1, pp. 14–27, January 1975.

[48] B. Mazur, "Modular curves and the eisenstein ideal," *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, vol. 47, pp. 33–186, 1977.

[49] M. H. Baker, "Torsion points on modular curves," *Inventiones Mathematicae*, vol. 140, p. 487–509, 2000.

[50] B. Poonen, "Computing torsion points on curves," *Experimental Math.*, vol. 10, no. 3, pp. 449–466, 2001.

[51] T. Takagi, "The cuspidal class number formula for the modular curves $x_0(m)$ with m square-free.," *Journal of Algebra*, vol. 193, p. 180–213, 1997.

[52] T. Takagi, "The cuspidal class number formula for the modular curves $x_1(p^m)$," *Journal of Algebra*, vol. 157, p. 515–549, 1993.

[53] V. Drinfeld, "Two theorems on modular curves," *Functional Analysis and Its Applications*, vol. 7, p. 155–156, April 1973.

[54] D. Lorenzini, "Torsion points on the modular jacobian $j_0(n)$," *Compositio Mathematica*, vol. 96, no. 2, p. 149–172, 1995.

[55] A. Weil, *Sur les courbes algébriques et les variétés qui s' en déduisent.* No. 1041, Actualités Sci. Ind, 1948.

[56] W. Stein, "Explicit approaches to modular abelian varieties," 1994.

[57] P. Bruin, "Modular curves, arakelov theory, algorithmic applications," 1 September 2010.

[58] F. Diamond and J. Shurman, *A First Course in Modular Forms.* Springer, 2000.

[59] J. P. Serre, *Algebraic groups and class fields.* Springer, 1997.

[60] P. Deligne, "Formes modulaires et représentations ℓ -adiques," *Séminaire N. Bourbaki*, vol. 44, no. 170, pp. 483–494, April 1985.

[61] D. Harvey, "Computing zeta functions of arithmetic schemes," *Proceedings of the London Mathematical Society*, vol. 111, no. 6, pp. 1379–1401, 2015.

[62] C. F. Gauss, *Werke*, vol. 1. Cambridge university press, Nov 2011.