Topics in the Theory of Zeta Functions of Curves

Stephanie Chan

MMath Mathematics

Hilary Term 2016

Contents

Introduction

Let $p \in \mathbb{N}$ denote a prime number and q denote a power of p. This notation will be used throughout this dissertation.

The zeta function—generating function of point-counts

A fundamental and natural problem in number theory is finding integer solutions to a system of polynomial equations. We can reduce the problem modulo q and look at the solutions over the finite field $\mathbb{F}_q$. The solutions can be viewed as points in an algebraic variety X over $\mathbb{F}_q$. To study a sequence $N_s := \#X(\mathbb{F}_{q^s})$, the number of points on X in field extensions $\mathbb{F}_{q^s}$, we can look at the zeta function of X. The (local) zeta function is defined as a generating function packaging the point-counts N_s on X:

$$Z(T) := \exp\left(\sum_{s=1}^{\infty} \frac{N_s T^s}{s}\right).$$

Weil conjectures—properties of the zeta function

In 1949, Weil conjectured [Wei49] that for a smooth variety of dimension n over $\mathbb{F}_q$, the following hold:

(1). (Rationality) $Z(T)$ is a rational function;

(2). (Functional equation) $Z\left(\frac{1}{q^n U}\right) = \pm q^{n\chi/2} T Z(T)$, where χ is the Euler-Poincaré characteristic of X;

(3). (Riemann hypothesis) $Z(T) = \frac{P_1(T)P_3(T)\ldots P_{2n-1}(T)}{P_0(T)P_2(T)\ldots P_{2n}(T)}$, with $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$ and for $1 \leq h \leq 2n-1$, $P_h(T) = \prod_{i=1}^{B_h}(1 - \alpha_{h_i} T)$ where α_{h_i} are algebraic integers of absolute value $q^{h/2}$ and B_h are called Betti numbers which satisfy $\chi = \sum_h (-1)^h B_h$.

Earlier in 1948, Weil proved the conjectures for curves [Wei48a] and for abelian varieties [Wei48b]. The Weil conjectures give insight in understanding the points in a variety as they connect the geometry over finite fields to topology.

Proving Weil conjectures—cohomology and Dwork's p-adic method

In 1960, Dwork proved the first of the Weil conjectures [Dwo60], the rationality of the zeta function, using p-adic analysis. Instead of the usual real numbers, the p-adic numbers is a

different completion of the rational numbers, giving the field distinctive properties that facilitated the proof.

Before Dwork, it was thought that some cohomology theory would be the key in proving the Weil conjectures. The idea was that $X(\mathbb{F}_{q^s})$ are fixed points of the q^s-Frobenius over the algebraic closure of $\mathbb{F}_q$, so the Lefschetz fixed point formula for a suitable cohomology would allow us to find the numbers $\#X(\mathbb{F}_{q^s})$. Effort was made to find a suitable cohomology that would fit into the picture. Building on Serre's idea, Artin and Grothendieck constructed étale cohomology, which played a fundamental role in the proofs of the other statements of the Weil conjectures by Grothendieck and Deligne in the 1960s and 1970s.

Quite unexpectedly, Dwork's method did not involve the use of cohomology theory, but it led to the development of p-adic cohomology theory, an example of which is Monsky-Washnitzer cohomology [MW68, Mon71]. Monsky-Washnitzer cohomology satisfies the Lefschetz fixed point formula, which can be used to count points and hence to compute zeta functions of curves.

Computing the zeta function—Kedlaya's algorithm and variants

In 2001, Kedlaya developed an algorithm for counting points on hyperelliptic curves [Ked01], using Monsky-Washnitzer cohomology. The curve over $\mathbb{F}_q$ is lifted to a curve over the ring $\mathbb{Z}_q$ of characteristic 0, and a lift of the q-Frobenius is defined over $\mathbb{Z}_q$. The algorithm then p-adically approximates the action of the Frobenius on an explicit basis of cohomology. The same idea can be applied to other types of curves. The algorithm was generalised to nondegenerate curves in [CDV06].

Harvey optimised Kedlaya's algorithm for large primes [Har07] and further developed an algorithm that computes the zeta function simultaneously for a given curve for all primes smaller than a fixed integer, in average polynomial time [Har14]. These methods can be used to obtain numerical data for problems such as the Sato-Tate Conjecture.

Sato-Tate conjecture—computing statistical distributions

The original Sato-Tate conjecture was conjectured by Sato and Tate independently in the 1960s. For an elliptic curve E over $\mathbb{Q}$, we know by the Hasse bound that

$$a_p := p + 1 - \#E(\mathbb{F}_p) \in [-2\sqrt{p}, 2\sqrt{p}].$$

The conjecture concerns the distribution of $\bar{a}_p = a_p/\sqrt{p}$ in the interval $[-2, 2]$, where a_p is the trace of Frobenius. It turns out that the distribution of $\bar{a}_p$ obtained is the same for any elliptic curves without complex multiplication. The conjecture was only proved recently by Harris, Shepherd-Barron and Taylor [HSBT10].

The conjecture has been generalised to abelian varieties over number fields. The generalisation was formulated by Serre [Ser94]. The generalised conjecture suggests the equidistribution property of a sequence of polynomials $\bar{P}_{\mathfrak{q}}(T) = P_{\mathfrak{q}}(T/\sqrt{q})$ which determines the zeta function of the abelian variety modulo primes $\mathfrak{q}$. If the abelian variety is the Jacobian associated to a curve, the polynomial $P_{\mathfrak{q}}(T)$ is the numerator of the zeta function of the curve modulo primes. Therefore, by computing the zeta function of curves, numerical evidence can be obtained for the conjecture. The genus 1 case corresponds to elliptic curves and there are 3 possible distributions. The genus 2 case was studied in [FKRS12] and examples were computed for all 52 possible distributions. The conjecture in the general case still remains open.

Layout of this dissertation

In the first chapter, we will go through the basics of p-adic numbers and p-adic analysis, then in the second chapter give an overview of Dwork's proof of the rationality of the zeta function of an algebraic variety, as presented by Koblitz [Kob84]. In the third chapter we will introduce Monsky-Washnitzer cohomology. In the fourth chapter we will present Kedlaya's algorithm, using Monsky-Washnitzer cohomology to count points on hyperelliptic cuves [Ked01]. The fifth chapter will cover Harvey's algorithm, which counts points in average polynomial time [Har14]. In the last chapter, we will discuss the application of such algorithms in computing data for the Sato-Tate Conjecture and illustrate this idea with some explicit examples.

Chapter 1

p-adic Numbers and the Zeta Function

In this chapter we will give some background on p-adic numbers and the zeta function, summarising the key facts and ideas from Chapters I, III and IV of [Kob84].

1.1 p-adic Numbers

Definition 1.1.1 (p-adic norm)**.** *The p-adic norm $|\cdot|_p$ on $\mathbb{Q}$ is defined such that*

$$|x|_p = \begin{cases} p^{-\operatorname{ord}_p x} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases},$$

where $\operatorname{ord}_p : \mathbb{Q} \to \mathbb{Z}$ is the p-adic order

$$\operatorname{ord}_p x = \begin{cases} r \quad \text{such that} \quad x = p^r \frac{n}{m}, \quad m, n \in \mathbb{Z}, \quad p \nmid n, m & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases}.$$

Every nontrivial norm on $\mathbb{Q}$ is equivalent to the usual absolute value or a p-adic norm by Ostrowski's Theorem.

Definition 1.1.2 (non-Archimedean norm)**.** *A norm $\|\cdot\|$ is non-Archimedean if it satisfies the isosceles triangle principle $\|x + y\| \leq \max(\|x\|, \|y\|)$. Equality holds if $\|x\| \neq \|y\|$.*

$|\cdot|_p$ is a non-Archimedian norm on $\mathbb{Q}$. To avoid confusion, we will denote the usual absolute value $|\cdot|_\infty$.

Definition 1.1.3 (p-adic numbers and integers)**.** *The p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic norm. Its subring $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$ is the p-adic integers.*

Remark 1. *We can view p-adic numbers in a more concrete form. Any $a \in \mathbb{Q}_p$ can be written uniquely in the form*

$$a = \sum_{i=\operatorname{ord}_p a}^{\infty} b_i p^i,$$

where $b_i \in \{0, \ldots, p-1\}$ are the p-adic digits of a.

Alternatively, the p-adic integers $\mathbb{Z}_p$ can be defined as the inverse limit $\lim_{\leftarrow} \mathbb{Z}/p^k\mathbb{Z}$. The p-adic numbers $\mathbb{Q}_p$ is the field of fractions, or equivalently $\mathbb{Z}_p[1/p]$.

Theorem 1.1.4 (Hensel's Lemma)**.** *Let $F(x) = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{Z}_p[x]$. If $a_0 \in \mathbb{Z}_p$ satisfies $F(a_0) \equiv 0 \mod p$ and $F'(a_0) \not\equiv 0 \mod p$, then there exists a unique $a \in \mathbb{Z}_p$ such that $F(a) = 0$ and $a \equiv a_0 \mod p$.*

Proof. See Theorem 3 in Chapter I of [Kob84]. □

Hensel's Lemma can be viewed as a p-adic analogue of Newton's method, but stronger as it guarantees convergence to a solution.

Instead of $\{0, 1, \ldots, p-1\}$, we can take the p-adic digits from another set of representatives $\{\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\} \subset \mathbb{Z}_p$, where $\alpha_i \equiv i \mod p$.

Definition 1.1.5 (Teichmüller representatives)**.** *Consider $1, \ldots, p-1$, the distinct roots of $x^{p-1} - 1$ in $\mathbb{F}_p$. By Hensel's lemma, we can lift them to distinct roots $\alpha_1, \ldots, \alpha_{p-1}$ in $\mathbb{Z}_p^\times$ with $\alpha_i \equiv i \mod p$. Then $0, \alpha_1, \ldots, \alpha_{p-1}$ are the Teichmüller representatives of $0, 1, \ldots, p-1$ respectively.*

Naturally, we would want study the algebraic closure and completion of $\mathbb{Q}_p$ as we do in $\mathbb{R}$.

Definition 1.1.6. *$\mathbb{Q}_p^{alg}$ denotes the algebraic closure of $\mathbb{Q}_p$. If $\alpha \in \mathbb{Q}_p^{alg}$ has the minimal polynomial $x^n + a_1 x^{n-1} + \cdots + a_n$, then $|\alpha|_p = |a_n|_p^{1/n}$ and $\operatorname{ord}_p \alpha = -\log_p |\alpha|_p$.*

Although $\mathbb{C}$, the algebraic closure of $\mathbb{R}$ is complete, the algebraic closure of $\mathbb{Q}_p$ is not complete, see Theorem 12 in Chapter III of [Kob84]. We need to further extend to get a complete field.

Definition 1.1.7. *Ω denotes the completion of $\mathbb{Q}_p^{alg}$ with respect to $|\cdot|_p$. If $x \in \Omega$ is the limit of a sequence $\{x_i\}$ in $\mathbb{Q}_p^{alg}$, then $|x|_p = \lim_{i\to\infty} |x_i|_p$ and $\operatorname{ord}_p x = -\log_p |x|_p$.*

Ω is algebraically closed, see Theorem 13 in Chapter III of [Kob84]. Ω is the smallest field containing $\mathbb{Q}$ which is both algebraically closed and complete with respect to the norm $|\cdot|_p$.

1.2 p-adic Power Series

Since $|\cdot|_p$ is a non-Archimedean norm, by the isosceles triangle principle, a p-adic power series $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \Omega[[X]]$ converges for x if and only if $a_n x^n \to 0$ as $n \to \infty$.

Definition 1.2.1 (radius of convergence)**.** *Let $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \Omega[[X]]$. The radius of convergence of $f(X)$ is $r := \liminf |a_n|_p^{-\frac{1}{n}}$. $f(X)$ is an entire function if r is infinite.*

Definition 1.2.2 (discs)**.** *The closed disc of radius $r \in \mathbb{R}$ about a point $a \in \Omega$ is*

$$D_a(r) := \{x \in \Omega \mid |x - a|_p \leq r\}.$$

The open disc of radius $r \in \mathbb{R}$ about a point $a \in \Omega$ is

$$D_a(r^-) := \{x \in \Omega \mid |x - a|_p < r\}.$$

When $a = 0$, we omit the subscript in the notation and write $D(r) := D_0(r)$.

Note that both $D_a(r)$ and $D_a(r^-)$ are simultaneously topologically open and closed sets.

Definition 1.2.3 (p-adic exponential function)**.** *The p-adic exponential function is*

$$\exp_p(X) := \sum_{n=0}^{\infty} \frac{X^n}{n!} \in \mathbb{Q}_p[[X]].$$

Definition 1.2.4 (p-adic binomial expansion)**.** *The p-adic binomial expansion is*

$$B_{a,p}(X) := \sum_{n=0}^{\infty} \binom{a}{n} X^n = \sum_{n=0}^{\infty} \frac{a(a-1)\dots(a-n+1)}{n!} X^n \in \mathbb{Q}_p[[X]].$$

For $a \in \mathbb{Q}$, we have $B_{a,p}(X) = (1+X)^a$ in Ω.

The following lemma is a criterion for a formal power series over $\mathbb{Q}_p$ to have coefficients in $\mathbb{Z}_p$, which is used in Dwork's proof.

Lemma 1.2.5 (Dwork)**.** *Let $F(X) = \sum a_n X^n \in 1 + X\mathbb{Q}_p[[X]]$. Then $a_n \in \mathbb{Z}_p$ for all m and n if and only if $F(X^p)/(F(X))^p \in 1 + pX\mathbb{Z}_p[[X]]$.*

Proof. Suppose $F(X) = \sum a_n X^n \in 1 + X\mathbb{Z}_p[[X]]$. Since $(a+b)^p \equiv a^p + b^p \mod p$ and $a^p \equiv a \mod p$ for $a, b \in \mathbb{Z}_p$, we have $F(X^p) = (F(X))^p + pXG(X)$ for some $G(X) \in \mathbb{Z}_p[[X]]$. As $1 + X\mathbb{Z}_p[[X]]$ is a multiplicative group, we have

$$\frac{1}{(F(X))^p} \in 1 + X\mathbb{Z}_p[[X]] \quad \text{and} \quad \frac{F(X^p)}{(F(X))^p} = 1 + \frac{pXG(X)}{(F(X))^p} \in 1 + pX\mathbb{Z}_p[[X]].$$

Conversely, suppose $F(X^p)/(F(X))^p \in 1 + pX\mathbb{Z}_p[[X]]$, then $F(X^p) = (F(X))^p G(X)$ for some $G(X) \in 1 + pX\mathbb{Z}_p[[X]]$. Write $F(X) = \sum a_i X^i$ and $G(X) = 1 + \sum pb_i X^i$. By assumption $a_0 = 1$. Now carry out induction on n. Suppose $a_i \in \mathbb{Z}_p$ for any $i < n$. Equate the coefficients in $(F(X))^p G(X) = F(X^p)$:

$$\text{coefficient of } X^n \text{ in } \left(\sum_{i=0}^{n} a_i X^i\right)^p \left(1 + \sum_{i=1}^{n} pb_i X^i\right) = \begin{cases} a_{n/p}, & \text{if } p \mid n \\ 0, & \text{otherwise} \end{cases},$$

$$\begin{aligned} \left(\sum_{i=0}^{n} a_i X^i\right)^p &= \left(a_n X^n + \sum_{i=0}^{n-1} a_i X^i\right)^p \\ &= \left(\sum_{i=0}^{n-1} a_i X^i\right)^p + pa_n X^n \left(\sum_{i=0}^{n-1} a_i X^i\right)^{p-1} + \dots + a_n^p X^{np} \\ &= \sum_{i=0}^{n-1} (a_i + pc_i) X^{ip} + pa_n X^n + (\text{terms of order} > n) \quad \text{for some } c_i \in \mathbb{Z}_p, \end{aligned}$$

since $(a+b)^p \equiv a^p + b^p \equiv a + b \mod p$ for $a, b \in \mathbb{Z}_p$. We have

$$pa_n + \sum_{i=0}^{\lceil \frac{n}{p} - 1 \rceil} (a_i + pc_i) pb_{n-ip} = 0,$$

and hence

$$a_n = -\sum_{i=0}^{\lceil \frac{n}{p} - 1 \rceil} (a_i + pc_i) b_{n-ip} \in \mathbb{Z}_p.$$

□

The criterion can be generalised to the following form.

Corollary 1.2.5.1. *Let $F(x,y) = \sum a_{mn}X^nY^m \in 1+X\mathbb{Q}_p[[X,Y]]+Y\mathbb{Q}_p[[X,Y]]$. Then we have $a_{mn} \in \mathbb{Z}_p$ for all m and n if and only if $F(X^p,Y^p)/(F(X,Y))^p \in 1+pX\mathbb{Z}_p[[X,Y]]+pY\mathbb{Z}_p[[X,Y]]$.*

With this criterion, we can prove the following series has coefficients in $\mathbb{Z}_p$.

Lemma 1.2.6. *Define a function in $\mathbb{Q}_p[[X,Y]]$,*

$$\begin{aligned} F(X,Y) &= B_{X,p}(Y)B_{(X^p-X)/p,p}(Y)B_{(X^{p^2}-X)/p^2,p}(Y)\dots B_{(X^{p^n}-X)/p^n,p}(Y)\dots \\ &= (1+Y)^X(1+Y^p)^{(X^p-X)/p}(1+Y^{p^2})^{(X^{p^2}-X^p)/p}\dots(1+Y^{p^n})^{(X^{p^n}-X^{p^{n-1}})/p}\dots \\ &= \sum_{i=0}^{\infty}\binom{X}{i}Y^i\prod_{n=1}^{\infty}\sum_{i=0}^{\infty}\binom{(X^{p^n}-X^{p^{n-1}})/p}{i}Y^{ip^n}. \end{aligned}$$

Then $F(X,Y) \in \mathbb{Z}_p[[X,Y]]$.

Proof. Any coefficient of $F(X,Y)$ is a product of finitely many terms in $\mathbb{Q}_p$ so

$$F(X,Y) \in 1 + X\mathbb{Q}_p[[X,Y]] + Y\mathbb{Q}_p[[X,Y]]$$

and

$$\frac{F(X^p,Y^p)}{(F(X,Y))^p} = \frac{(1+Y^p)^{X^p}(1+Y^{p^2})^{(X^{p^2}-X^p)/p}(1+Y^{p^3})^{(X^{p^3}-X^{p^2})/p}\dots}{(1+Y)^{pX}(1+Y^p)^{X^p-X}(1+Y^{p^2})^{X^{p^2}-X^p}\dots} = \frac{(1+Y^p)^X}{(1+Y)^{pX}}.$$

Since $1+Y \in 1+Y\mathbb{Z}_p[Y]$, by Lemma 1.2.5,

$$\frac{1+Y^p}{(1+Y)^p} = 1+pYG(Y) \quad \text{for some} \quad G(Y) \in \mathbb{Z}_p[[Y]].$$

We have

$$\frac{(1+Y^p)^X}{(1+Y)^{pX}} = (1+pYG(Y))^X = \sum_{i=0}^{\infty}\binom{X}{i}p^i(YG(Y))^i \in 1+pX\mathbb{Z}_p[[X,Y]]+pY\mathbb{Z}_p[[X,Y]].$$

Hence, $F(X,Y) \in \mathbb{Z}_p[[X,Y]]$, by Corollary 1.2.5.1. □

Theorem 1.2.7 (p-adic Weierstrass Preparation Theorem)**.** *If $F(T)$ is a p-adic entire function, then for any R there exists a polynomial $P(T)$ and a p-adic power series $G(T) \in 1+T\Omega[[T]]$ which converges on the disc $D(R)$ of radius R, such that $P(T) = F(T)G(T)$.*

Proof. See Chapter IV of [Kob84] for a proof using Newton polygons. □

1.3 The Zeta Function

Definition 1.3.1 (zeta function)**.** *For a variety X, the zeta function is defined to be*

$$Z(X/\mathbb{F}_q;T) := \exp\left(\sum_{s=1}^{\infty}\frac{N_sT^s}{s}\right),$$

where $N_s := \#X(\mathbb{F}_{q^s})$.

The zeta function is a formal power series with positive integral coefficients bounded exponentially.

Lemma 1.3.2. *We have $Z(H_f/\mathbb{F}_q;T) \in 1+T\mathbb{Z}[[T]]$ and for any $j \in \mathbb{N}$, the coefficient of T^j is a positive integer $\leq q^{nj}$.*

Proof. Consider a point $P = (x_1, \ldots, x_n) \in H_f$. Let s_0 be the least s such that all $x_i \in \mathbb{F}_{q^s}$. Let $P_j = (x_{1j}, \ldots, x_{nj})$, $j = 1, \ldots, s_0$ be the conjugates of $P_1 = P$, so that $x_{i1}, \ldots, x_{is_0}$ are the conjugates of $x_i = x_{i1}$ over $\mathbb{F}_q$. If all of the x_i are fixed by an automorphism σ of $\mathbb{F}_{q^{s_0}}$ over $\mathbb{F}_q$, then all x_i are in a smaller field, which contradicts with the choice of s_0, so P_j are distinct.

Each $P_1, \ldots P_{s_0}$ is an $\mathbb{F}_{q^s}$-point of H_f precisely when $\mathbb{F}_{q^{s_0}} \subseteq \mathbb{F}_{q^s}$, i.e. $s_0 \mid s$. Thus, these points contribute s_0 to $N_{s_0}, N_{2s_0}, N_{3s_0}, \ldots$, so their contribution to $Z(H_f/\mathbb{F}_q;T)$ is

$$\exp\left(\sum_{j=1}^{\infty} \frac{s_0 T^{js_0}}{js_0}\right) = \exp(-\log(1-T^{s_0})) = \frac{1}{1-T^{s_0}} = \sum_{j=0}^{\infty} T^{js_0} \in 1+T^{s_0}\mathbb{Z}[[T]].$$

Then $Z(H_f/\mathbb{F}_q;T)$ is a product of series of this type and there are only finitely many such series with first T-term with degree $\leq s$ for any fixed s, so $Z(H_f/\mathbb{F}_q;T)$ has integer coefficients.

Finally, $N_s \leq \#\mathbb{A}^n_{q^s} = q^{ns}$, so the coefficient of T^j in $Z(H_f/\mathbb{F}_q;T)$ is less than the coefficient of T^j in

$$\exp\left(\sum_{s=1}^{\infty} \frac{q^{ns}T^s}{s}\right) = \exp(-\log(1-q^nT)) = \frac{1}{1-q^nT} = \sum_{j=0}^{\infty} q^{nj}T^j.$$

□

Chapter 2

Dwork's Proof on Rationality of the Zeta Function

Dwork proved that the zeta function of any affine or projective variety is a rational function. Although the Weil conjectures required the variety to be smooth, Dwork's proof does not assume smoothness of the variety so in fact the rationality holds more generally for any variety, including those with singularities.

In this chapter, we will follow Chapter V of [Kob84].

Let H_f denote the affine hypersurface defined by a polynomial f and $\tilde{H}_{\tilde{f}}$ denote the projective hypersurface defined by a homogeneous polynomial $\tilde{f}$.

Remark 2. *An affine or projective variety is an intersection of a finite number of hypersurfaces, so by the inclusion-exclusion principle* $X = \cup H_{f_i} - \cap H_{f_i f_j} + \cup H_{f_i f_j f_k} - \cap H_{f_i f_j f_k f_l} + \ldots$, *where the union and intersections runs through all distinct* $i, j, k, l, \ldots$. *We have*

$$Z(X/\mathbb{F}_q; T) = \frac{\prod Z(H_{f_i}/\mathbb{F}_q; T)}{\prod Z(H_{f_i f_j}/\mathbb{F}_q; T)} \frac{\prod Z(H_{f_i f_j f_k}/\mathbb{F}_q; T)}{\prod Z(H_{f_i f_j f_k f_l}/\mathbb{F}_q; T)} \cdots,$$

where the products runs through all distinct $i, j, k, l, \ldots$.

Since V *is defined on a finite set of polynomials,* $Z(X/\mathbb{F}_q; T)$ *is the product of a finite number of zeta functions of hypersurfaces. Thus, it suffices to consider the zeta function of hypersurfaces.*

Remark 3. *A projective plane* $\mathbb{P}_k^n$ *can be viewed as the disjoint union*

$$\mathbb{A}_k^n \cup \mathbb{A}_k^{n-1} \ldots \mathbb{A}_k^1 \cup \textit{point}$$

so a projective hypersurface $\tilde{H}_{\tilde{f}}$ *is a disjoint union of affine hypersurfaces and* $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ *is a product of a finite number of zeta functions of affine hypersurfaces. Hence it is enough to prove the rationality of the zeta function of affine hypersurfaces.*

2.1 Lifting of Characters

Definition 2.1.1. *An* Ω*-valued character of a finite group* G *is a homomorphism from* G *to the multiplicative group* $\Omega^\times$.

Let ϵ be a primitive pth root of unity in $\mathbb{Q}_p^{alg} \subset \Omega$, then $a \mapsto \epsilon^{\operatorname{Tr} a}$ is an Ω-valued character of the finite group $\mathbb{F}_q$. Now we proceed to find an analytic formula for this map.

Lemma 2.1.2. *Let $q = p^s$. Fix $a \in \mathbb{F}_q^\times$ and let $t \in \Omega$ be the corresponding Teichmüller representative. Then there exist a p-adic power series Θ such that $\epsilon^{\operatorname{Tr} a} = \Theta(T)\Theta(t^p)\Theta(t^{p^2}) \dots \Theta(t^{p^{s-1}})$.*

Proof. Let F be as previously defined in Lemma 1.2.6. Let $\lambda = \epsilon - 1$. It is easy to check that $\operatorname{ord}_p \lambda = 1/(p-1)$. Define

$$\Theta(T) = F(T, \lambda) = (1+\lambda)^T (1+\lambda^p)^{(T^p - T)/p} (1+\lambda^{p^2})^{(T^{p^2} - T^p)/p} \dots (1+\lambda^{p^n})^{(T^{p^n} - T^{p^{n-1}})/p} \dots,$$

where each term on the right is a binomial series in $\mathbb{Q}_p[[X, Y]]$. We have

$$F(T, \lambda) = \sum_{n=0}^{\infty} \left(T^n \sum_{m=0}^{\infty} a_{mn} \lambda^m \right), \quad a_{mn} \in \mathbb{Z}_p.$$

Since the power of T is less than or equal to the power of λ in each term of the binomial series, we have $a_{mn} = 0$ when $n < m$. Let

$$\Theta(T) = F(T, \lambda) = \sum_{n=0}^{\infty} a_n T^n, \quad a_n = \sum_{m=n}^{\infty} a_{mn} \lambda^m.$$

Since $\operatorname{ord}_p a_n \geq n/(p-1)$, and $\mathbb{Q}_p(\epsilon) = \mathbb{Q}_p(\lambda)$ is complete, we have $a_n \in \mathbb{Q}_p(\epsilon)$ and $\Theta(T) \in \mathbb{Q}_p(\epsilon)[[T]]$. Also, $\Theta(T)$ converges in $D(p^{1/(p-1)-})$. We compute

$$\operatorname{Tr} a = a + a^p + a^{p^2} + \dots + a^{p^{s-1}} \equiv t + t^p + t^{p^2} + \dots + t^{p^{s-1}} \mod p,$$

$$\begin{aligned}
&\Theta(T)\Theta(t^p)\Theta(t^{p^2}) \dots \Theta(t^{p^{s-1}}) \\
&= F(t, \lambda) F(t^p, \lambda) \dots F(t^{p^{s-1}}, \lambda) \\
&= (1+\lambda)^{t + t^p + \dots + t^{p^{s-1}}} (1+\lambda^p)^{(t^{p^s} - t)/p} (1+\lambda^{p^2})^{(t^{p^{s+1}} - t^p)/p^2} (1+\lambda^{p^3})^{(t^{p^{s+2}} - t^{p^2})/p^3} \dots \\
&= (1+\lambda)^{1 + t^p + \dots + t^{p^{s-1}}} \quad \text{since } t^{p^s} = t \\
&= \epsilon^{\operatorname{Tr} a} \quad \text{since } \epsilon^p = 1 \text{ and } \operatorname{Tr} a \equiv t + t^p + t^{p^2} + \dots + t^{p^{s-1}} \mod p.
\end{aligned}$$

□

2.2 Trace and Determinant

Define $U := \{(u_1, \dots, u_n) \mid u_i \in \mathbb{Z}, u_i \geq 0 \text{ for all } i\}$ and the norm $|\cdot|$ on U by $|\mathbf{u}| = \sum_{i=1}^n u_i$. Denote $X^{\mathbf{u}} := X_1^{u_1} \dots X_n^{u_n}$, where $\mathbf{u} = (u_1, \dots, u_n) \in U$.

Define $R := \Omega\langle X_1, X_2, \dots, X_n \rangle$ to be the set of power series which converges on $D(1)$,

$$R := \left\{ \sum_{\mathbf{w}} g_{\mathbf{w}} X^{\mathbf{w}} \in \Omega[[X_1, X_2, \dots, X_n]] \;\middle|\; \lim_{|\mathbf{u}|} |g_{\mathbf{u}}|_p = 0 \right\},$$

and its subspace

$$R^\dagger := \left\{ \sum_{\mathbf{w}} g_{\mathbf{w}} X^{\mathbf{w}} \in R \;\middle|\; \text{there exists } M > 0 \text{ such that } \operatorname{ord}_p g_{\mathbf{u}} \geq M|\mathbf{u}| \text{ for all } \mathbf{u} \in U \right\}.$$

Remark 4. *The following are equivalent conditions:*

(1). *There exists some* $M > 0$ *such that* $\operatorname{ord}_p g_{\mathbf{u}} \geq M|\mathbf{u}|$ *for all* $\mathbf{u} \in U$*;*

(2). *There exists some* $\lambda > 1$ *such that* $\lim_{|\mathbf{u}|} |g_{\mathbf{u}}|_p \lambda^{|\mathbf{u}|} = 0$*;*

(3). *There exists some* $M > 0$ *and* $0 < \rho < 1$ *such that* $|g_{\mathbf{u}}|_p < M\rho^{|\mathbf{u}|}$ *for all* $\mathbf{u} \in U$ *;*

(4). $\liminf_{|\mathbf{u}|}(\operatorname{ord}_p g_{\mathbf{u}}/|\mathbf{u}|) > 0$.

Define $T_q : R \to R$ such that $\sum_{\mathbf{u}\in U} a_{\mathbf{u}} X^{\mathbf{u}} \mapsto \sum_{\mathbf{u}} a_{q\mathbf{u}} X^{\mathbf{u}}$.

For any $G(X) = \sum_{\mathbf{w}} g_{\mathbf{w}} X^{\mathbf{w}} \in R^\dagger \subseteq R$, let L_G denote the map of multiplication by $G(X)$ and let $G_q(x) = \sum_{\mathbf{w}} g_{\mathbf{w}} X^{q\mathbf{w}}$. Define $\Psi_{q,G} := T_q \circ L_G$.

Lemma 2.2.1. *Let* $G(X) = \sum_{\mathbf{w}} g_{\mathbf{w}} X^{\mathbf{w}} \in R^\dagger$*. Let* $\Psi = \Psi_{q,G} = T_q \circ L_G$*, then* $\operatorname{Tr}(\Psi^s)$ *converges for* $s = 1, 2, 3, \ldots,$ *and*

$$(q^s - 1)^n \operatorname{Tr}(\Psi^s) = \sum_{\substack{x\in\Omega^n \\ x^{q^{s-1}}=1}} G(x)G(x^q)G(x^{q^2})\ldots G(x^{q^{s-1}}),$$

where $x = (x_1, \ldots, x_n)$*,* $x^{q^i} = (x_1^{q^i}, \ldots, x_n^{q^i})$ *and* $x^{q^{s-1}} = 1$ *denotes* $x_1^{q^{s-1}} = \cdots = x_n^{q^{s-1}} = 1$

Proof. First we prove the case when $s = 1$,

$$\Psi(X^{\mathbf{u}}) = T_q(L_G(X^{\mathbf{u}})) = T_q\left(\sum_{\mathbf{w}} g_{\mathbf{w}} X^{\mathbf{w}+\mathbf{u}}\right) = \sum_{\mathbf{w}} g_{q\mathbf{w}} X^{\mathbf{w}+\mathbf{u}} = \sum_{\mathbf{v}} g_{q\mathbf{v}-\mathbf{u}} X^{\mathbf{v}},$$

$$\operatorname{Tr}\Psi = \sum_{\mathbf{u}} g_{(q-1)\mathbf{u}},$$

which converges by definition of $R^\dagger$. We have

$$\sum_{\substack{x_i\in\Omega \\ x_i^{q-1}=1}} x_i^{w_i} = \begin{cases} q-1, & \text{if } q-1 \mid w_i \\ 0, & \text{otherwise} \end{cases}.$$

Moreover,

$$\sum_{\substack{x_i\in\Omega \\ x_i^{q-1}=1}} x^{\mathbf{w}} = \prod_{i=1}^{n}\left(\sum_{x_i^{q-1}=1} x_i^{w_i}\right) = \begin{cases} (q-1)^n, & \text{if } q-1 \mid \mathbf{w} \\ 0, & \text{otherwise} \end{cases},$$

and

$$\sum_{x^{q-1}=1} G(x) = \sum_{\mathbf{w}} g_{\mathbf{w}} \sum_{x^{q-1}=1} x^{\mathbf{w}} = (q-1)^n \sum_{\mathbf{u}} g_{(q-1)\mathbf{u}} = (q-1)^n \operatorname{Tr}\Psi.$$

It is easy to check that $L_G \circ T_q = T_q \circ L_{G_q} = \Psi_{q,G_q}$ Suppose $s > 1$, then

$$\begin{aligned}\Psi^s &= T_q \circ L_G \circ T_q \circ L_G \circ \Psi^{s-2} = T_q \circ T_q \circ L_{G_q} \circ L_G \circ \Psi^{s-2} \\ &= T_{q^2} \circ L_{G\cdot G_q} \circ \Psi^{s-2} = \cdots = T_{q^s} \circ L_{G\cdot G_q\cdots G_{q^{s-1}}} = \Psi_{q^s, G\cdot G_q\cdots G_{q^{s-1}}}.\end{aligned}$$

Note that $R^\dagger$ is closed under multiplication and under the map $G \mapsto G_q$, so $G \cdot G_q \cdots G_{q^{s-1}} \in R^\dagger$. From the $s = 1$ case, replacing q by q^s and G by $G \cdot G_q \cdots G_{q^{s-1}}$ gives

$$\begin{aligned}(q-1)^n \operatorname{Tr}(\Psi^s) = (q-1)^n \operatorname{Tr}\left(\Psi_{q^s, G\cdot G_q \cdots G_{q^{s-1}}}\right) &= \sum_{x^{q^{s-1}}=1} G(x)G_q(x)\cdots G_{q^{s-1}}(x) \\ &= \sum_{x^{q^{s-1}}=1} G(x)G(x^q)G(x^{q^2})\cdots G(x^{q^{s-1}}).\end{aligned}$$

□

Lemma 2.2.2. *Let $A = \{a_{ij}\}_{i,j=1}^r$. We have $\det(1 - AT) = \sum_{m=0}^r b_m T^m$, where*

$$b_m = (-1)^m \sum_{\substack{1 \le u_1 < \cdots < u_m \le r \\ \sigma \in S_m}} \operatorname{sgn}(\sigma) a_{u_1, u_{\sigma(1)}} a_{u_2, u_{\sigma(2)}} \cdots a_{u_m, u_{\sigma(m)}}.$$

Then $\det(1 - AT) = \exp_p\left(-\sum_{s=1}^\infty \frac{\operatorname{Tr}(A^s)T^s}{s}\right) \in \Omega[[T]]$.

Proof. Without loss of generality, we can assume A is upper triangular, then

$$\begin{aligned}\exp_p\left(-\sum_{s=1}^\infty \frac{\operatorname{Tr}(A^s)\,T^s}{s}\right) &= \exp_p\left(-\sum_{s=1}^\infty \sum_{i=1}^r \frac{a_{ii}^s T^s}{s}\right) \\ &= \exp_p\left(-\sum_{s=1}^r \log(1 - a_{ii}T)\right) = \prod_{s=1}^r (1 - a_{ii}T) = \det(1 - AT).\end{aligned}$$

□

Lemma 2.2.3. *Let $G(X) = \sum_{\mathbf{w}\in U} g_{\mathbf{w}} X^{\mathbf{w}} \in R^\dagger$. Let $\Psi = T_q \circ L_G$, then $\Psi(X^{\mathbf{u}}) = \sum_{\mathbf{v}\in U} g_{q\mathbf{v}-\mathbf{u}} X^{\mathbf{v}}$, so Ψ has matrix $A = \{a_{\mathbf{u},\mathbf{v}}\}_{\mathbf{u},\mathbf{v}\in U} = \{g_{q\mathbf{v}-\mathbf{u}}\}_{\mathbf{u},\mathbf{v}\in U}$. Then the series $\det(1 - AT) := \sum_{m=0}^\infty b_m T^m$, where*

$$b_m = (-1)^m \sum_{\substack{\text{distinct } \mathbf{u}_1,\ldots,\mathbf{u}_m \in U \\ \sigma \in S_m}} \operatorname{sgn}(\sigma) a_{\mathbf{u}_1, \mathbf{u}_{\sigma(1)}} a_{\mathbf{u}_2, \mathbf{u}_{\sigma(2)}} \cdots a_{\mathbf{u}_m, \mathbf{u}_{\sigma(m)}},$$

is well-defined, has infinite radius of convergence and satisfies the identity

$$\det(1 - AT) = \exp_p\left(-\sum_{s=1}^\infty \frac{\operatorname{Tr}(A^s)T^s}{s}\right) \in \Omega[[T]].$$

Proof. We have

$$\begin{aligned}&\operatorname{ord}_p\left(g_{q\mathbf{u}_{\sigma(1)}-\mathbf{u}_1} g_{q\mathbf{u}_{\sigma(2)}-\mathbf{u}_2} \cdots g_{q\mathbf{u}_{\sigma(m)}-\mathbf{u}_m}\right) \\ &\ge M\left(|q\mathbf{u}_{\sigma(1)} - \mathbf{u}_1| + |q\mathbf{u}_{\sigma(2)} - \mathbf{u}_2| + \cdots + |q\mathbf{u}_{\sigma(m)} - \mathbf{u}_m|\right) \\ &\ge M \sum_i \left(|q\mathbf{u}_{\sigma(i)}| - |\mathbf{u}_i|\right) = M(q-1)\sum_{i=1}^m |\mathbf{u}_i|.\end{aligned}$$

There are only finitely many distinct $\mathbf{u}_i \in U$ with $|\mathbf{u}_i|$ smaller than a fixed value, so we have $\sum_{i=1}^m |\mathbf{u}_i|/m \to \infty$ as $m \to \infty$. Then we have $\operatorname{ord}_p b_m \to \infty$ as $m \to \infty$ and $\operatorname{ord}_p b_m/m \to \infty$ as $m \to \infty$. For any fixed t, $\operatorname{ord}_p b_m t^m = m(\operatorname{ord}_p b_m/m + \operatorname{ord}_p t) \to \infty$ as $m \to \infty$. Hence $\det(1 - AT)$ has infinite radius of convergence. By taking $r \to \infty$ in Lemma 2.2.2, we obtain the identity $\det(1 - AT) = \exp_p(-\sum_{s=1}^\infty \operatorname{Tr}(A^s)\,T^s/s)$. □

2.3 Meromorphicity

Let $f(X_1,\dots,X_n)\in\mathbb{F}_q[X_1,\dots,X_n]$. We want to prove that $Z(H_f/\mathbb{F}_q;T)\in\mathbb{Z}[[T]]\subset\Omega[[T]]$ is p-adic meromorphic, i.e. a quotient of two power series in $\Omega[[T]]$ with infinite radius of convergence. First consider

$$Z'(H_f/\mathbb{F}_q;T):=\exp\left(\sum_{s=1}^{\infty}\frac{N'_sT^s}{s}\right),$$

where $N'_s=\#\{(x_1,x_2,\dots,x_n)\in\mathbb{A}^n_{\mathbb{F}_{q^s}}\mid f(x_1,x_2,\dots,x_n)=0 \text{ and } x_i\neq 0 \text{ for all } i\}$.

Lemma 2.3.1. *$Z'(H_f/\mathbb{F}_q;T)$ is p-adic meromorphic.*

Proof. Fix $s\in\mathbb{N}$ and let $q=p^r$. If t denotes the Teichmüller representative of $a\in\mathbb{F}_{q^s}$, then by Lemma 2.1.2 the pth root of 1 given by ϵ has a p-adic analytic formula

$$\epsilon^{\operatorname{Tr}a}=\Theta(T)\Theta\left(t^p\right)\Theta(t^{p^2})\dots\Theta(t^{p^{rs-1}}).$$

Suppose $u\in\mathbb{F}_{q^s}^{\times}$. For some $x\in\mathbb{F}_{q^s}$ such that $\operatorname{Tr}x\neq 0$,

$$\sum_{u\in\mathbb{F}_{q^s}}\epsilon^{\operatorname{Tr}u}=\sum_{u+x\in\mathbb{F}_{q^s}}\epsilon^{\operatorname{Tr}(u+x)}=\epsilon^{\operatorname{Tr}x}\sum_{u+x\in\mathbb{F}_{q^s}}\epsilon^{\operatorname{Tr}u}=\epsilon^{\operatorname{Tr}x}\sum_{u\in\mathbb{F}_{q^s}}\epsilon^{\operatorname{Tr}u},$$

$$\sum_{x_0\in\mathbb{F}_{q^s}}\epsilon^{\operatorname{Tr}(x_0u)}=\sum_{u\in\mathbb{F}_{q^s}}\epsilon^{\operatorname{Tr}u}=0\quad\text{since }\operatorname{Tr}x\neq 0.$$

When $u\in\mathbb{F}_{q^s}$,

$$\sum_{x_0\in\mathbb{F}_{q^s}}\epsilon^{\operatorname{Tr}(x_0u)}=\begin{cases}0, & \text{if } u\in\mathbb{F}_{q^s}^{\times}\\ q^s, & \text{if } u=0\end{cases}.$$

Subtracting the $x_0=0$ term gives

$$\sum_{x_0\in\mathbb{F}_{q^s}^{\times}}\epsilon^{\operatorname{Tr}(x_0u)}=\begin{cases}-1, & \text{if } u\in\mathbb{F}_{q^s}^{\times}\\ q^s-1, & \text{if } u=0\end{cases}.$$

Applying to $u=f(x_1,\dots,x_n)$ and summing over all $x_1,\dots,x_n\in\mathbb{F}_{q^S}^{\times}$ gives

$$\sum_{x_0,\dots,x_n\in\mathbb{F}_{q^s}^{\times}}\epsilon^{\operatorname{Tr}(x_0f(x_1,\dots,x_n))}=N'_s(q^s-1)+\left((q^s-1)^n-N'_s\right)(-1)=q^sN'_s-(q^s-1)^n.$$

Replace the coefficients in $X_0f(X_1,\dots,X_n)\in\mathbb{F}_q[X_0,X_1,\dots,X_n]$ by their Teichmüller representatives to get $\sum_{i=1}^N a_iX^{w_i}\in\Omega[X_0,X_1,\dots,X_n]$, where $a_i^{p^r}=a_i$ and X^{w_i} denotes $X_0^{w_{i0}}X_1^{w_{i1}}\dots X_n^{w_{in}}$, $w_i=(w_{i0},w_{i1},\dots,w_{in})$. We have

$$\begin{aligned}q^sN'_s&=(q^s-1)^n+\sum_{x_0,\dots,x_n\in\mathbb{F}_{q^s}^{\times}}\epsilon^{\operatorname{Tr}(x_0f(x_1,\dots,x_n))}\\&=(q^s-1)^n+\sum_{\substack{x_0,\dots,x_n\in\Omega\\ x_0^{q^s-1}=\dots=x_n^{q^s-1}=1}}\prod_{i=1}^{N}\Theta(a_ix^{w_i})\Theta(a_i^px^{pw_i})\dots\Theta\left(a_i^{p^{rs-1}}x^{p^{rs-1}w_i}\right).\end{aligned}$$

Let $G(X_0,\dots,X_n) := \prod_{i=1}^{N} \Theta\left(a_i X^{w_i}\right)\Theta\left(a_i^p X^{pw_i}\right)\dots\Theta\left(a_i^{p^{r-1}} X^{p^{r-1}w_i}\right) \in R^\dagger$ since $R^\dagger$ is closed under multiplication and $\Theta\left(a_i^{p^{j-1}} X^{p^{j-1}w_i}\right) \in R^\dagger$ by Remark 5. We compute

$$\begin{aligned} q^s N_s' &= (q^s-1)^n + \sum_{\substack{x_0,\dots,x_n\in\Omega \\ x_0^{q^s-1}=\dots=x_n^{q^s-1}=1}} G(x)G(x^q)G(x^{q^2})\dots G(x^{q^s-1}) \\ &= (q^s-1)^n + (q^s-1)^{n+1}\operatorname{Tr}(\Psi^s) \quad \text{by Lemma 2.2.1} \\ &= \sum_{i=0}^{n}\binom{n}{i}(-1)^i q^{s(n-i)} + \operatorname{Tr}(\Psi^s)\sum_{i=0}^{n+1}\binom{n+1}{i}(-1)^i q^{s(n+1-i)} \end{aligned}$$

so

$$N_s' = \sum_{i=0}^{n}\binom{n}{i}(-1)^i q^{s(n-i-1)} + \operatorname{Tr}(\Psi^s)\sum_{i=0}^{n+1}\binom{n+1}{i}(-1)^i q^{s(n-i)},$$

and

$$\begin{aligned} Z'(H_f/\mathbb{F}_q;T) &= \exp_p\left(\sum_{s=1}^{\infty}\frac{N_s' T^s}{s}\right) \\ &= \prod_{i=0}^{n}\exp_p\left(\sum_{s=1}^{\infty}\binom{n}{i}\frac{(-1)^i q^{s(n-i-1)}T^s}{s}\right)\prod_{i=0}^{n+1}\exp_p\left(\sum_{s=1}^{\infty}\binom{n+1}{i}\frac{(-1)^i q^{s(n-i)}\operatorname{Tr}(\Psi^s)T^s}{s}\right) \\ &= \prod_{i=0}^{n}(1-q^{n-i-1}T)^{(-1)^{i+1}\binom{n}{i}}\prod_{i=0}^{n}\det(1-A(q^{n-i}T))^{(-1)^{i+1}\binom{n}{i}}, \end{aligned}$$

where A is the matrix of Ψ. By Lemma 2.2.3, each term on the right is a p-adic entire function. □

Remark 5. *If $\Theta(T)=\sum_{n=0}^{\infty}a_nT^n$, we have $\Theta(aX^w)=\sum_{n=0}^{\infty}a_n a^n X^{wn}=\sum_{v=nw}g_vX^v$, where $g_v=a_{nw}a^n$ if $w\mid v$. Since $\operatorname{ord}_p a_n \geq n/(p-1)$, for any a with $|a|_p\leq 1$ $\operatorname{ord}_p g_v \geq |w|/|v|(p-1)$.*

Theorem 2.3.2. *$Z(H_f/\mathbb{F}_q;T)\in\mathbb{Z}[[T]]\subset\Omega[[T]]$ is p-adic meromorphic.*

Proof. Prove by induction on the number of variables n. Note that $n-1$ is the dimension of the hypersurface H_f.

If $n=0$, it is trivial since $H_f=\emptyset$.

Suppose the theorem holds for $1,\dots,n-1$. From Lemma 2.3.1, we have that $Z'(H_f/\mathbb{F}_q;T)$ is p-adic meromorphic. We have

$$Z(H_f/\mathbb{F}_q;T) = Z'(H_f/\mathbb{F}_q;T)\exp\left(\sum_{s=1}^{\infty}\frac{(N_s-N_s')T^s}{s}\right),$$

where $\exp\left(\sum_{s=1}^{\infty}(N_s-N_s')T^s/s\right)$ is the zeta function for $H=\cup_{i=1}^{n}H_i$, a disjoint union of H_i defined by $f(X_1,X_2,\dots,X_n)=0$ and $X_i=0$.

$$Z(H/\mathbb{F}_q;T) = \frac{\prod Z(H_i/\mathbb{F}_q;T)}{\prod Z(H_i\cap H_j/\mathbb{F}_q;T)}\frac{\prod Z(H_i\cap H_j\cap H_k/\mathbb{F}_q;T)}{\prod Z(H_i\cap H_j\cap H_k\cap H_l/\mathbb{F}_q;T)}\dots,$$

where products in the expression on the right runs through zeta functions of intersections of distinct H_i. The H_i have dimension less than $n-1$, and so do their intersections. By the induction assumption, the zeta functions in the expression are all meromorphic, so $Z(H/\mathbb{F}_q;T)$ as a finite product of such functions, is meromorphic too. Hence $Z(H_f/\mathbb{F}_q;T) := Z'(H_f/\mathbb{F}_q;T)Z(H/\mathbb{F}_q;T)$ is also meromorphic. □

2.4 Rationality of the Zeta Function of Affine Hypersurfaces

Lemma 2.4.1 (rationality criterion)**.** *Let K be a field and let $F(T) = \sum_{i=0}^{\infty} a_i T^i \in K[[T]]$. For $m, s \geq 0$, let $A_{s,m} = \{a_{s+i+j}\}_{0\leq i,j\leq m}$ and $N_{s,m} = \det(A_{s,m})$. If there exist integers $m \geq 0$ and S such that $N_{s,m} = 0$ whenever $s \geq S$, then $F(T) = P(T)/Q(T)$ for some $P(T), Q(T) \in K[T]$.*

Proof. Pick m minimal such that there exists some S such that $N_{s,m} = 0$ for $s \geq S$. Denote the $(i+1)$th row of $A_{s,m}$ by $\mathbf{r}_i$.

Suppose for a contradiction that $N_{s,m-1} = 0$ for some $s \geq S$. Then there exist a linear combination of $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{m-1}$, expressed as $\alpha_0\mathbf{r}_0 + \alpha_1\mathbf{r}_1 + \cdots + \alpha_{m-1}\mathbf{r}_{m-1}$ such that the first m entries become 0. Let k be minimal with $\alpha_k \neq 0$. In $A_{s,m}$, replace the $(k+1)$th row $\mathbf{r}_k$ with $\mathbf{r}_k + \alpha_k^{-1}(\alpha_{k+1}\mathbf{r}_{k+1} + \cdots + \alpha_{m-1}\mathbf{r}_{m-1})$ to get a new matrix

$$\tilde{A}_{s,m} = \{\tilde{a}_{s+i+j}\}_{0\leq i,j\leq m} = \begin{pmatrix} \tilde{a}_s & \tilde{a}_{s+1} & \cdots & \tilde{a}_{s+m} \\ \tilde{a}_{s+1} & \tilde{a}_{s+2} & \cdots & \tilde{a}_{s+m+1} \\ \vdots & & & \vdots \\ 0 & \cdots & 0 & \beta \\ \vdots & & & \vdots \\ \tilde{a}_{s+m} & \tilde{a}_{s+m+1} & \cdots & \tilde{a}_{s+2m} \end{pmatrix},$$

the determinant remains the same, and now the $(k+1)$th row is $(0, \ldots, 0, \beta)$.

If $k > 0$, $\tilde{A}_{s+1,m-1}$ has a row of 0, so $N_{s+1,m-1} = 0$. If $k = 0$, $\beta \cdot \det(\tilde{A}_{s+1,m-1}) = \beta N_{s+1,m-1} = N_{s,m} = 0$ so $N_{s+1,m-1} = 0$, otherwise $\beta = 0$, then $\tilde{A}_{s+1,m-1}$ has a row of 0, which implies $N_{s+1,m-1} = 0$.

By induction, $N_{s',m-1} = 0$ for any $s' \geq s$, which contradicts the minimality of m. Hence, we have shown that $N_{s,m-1} \neq 0$ for all $s \geq S$.

Since $N_{S,m} = 0$, there exist $\mathbf{u} = (u_m, u_{m-1}, \ldots, u_0)^T$ such that $A_{S,m}\mathbf{u} = 0$. For any $s \geq S$, $N_{s,m} = 0$ and $N_{s,m-1} \neq 0$, so $\mathbf{r}_m$ is a linear combination of $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{m-1}$. If $A_{s-1,m}\mathbf{u} = 0$, we have $\mathbf{r}_0\mathbf{u} = \mathbf{r}_2\mathbf{u} = \cdots = \mathbf{r}_{m-1}\mathbf{u} = 0$, $\mathbf{r}_m$ is a linear combination of $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{m-1}$ so $\mathbf{r}_m\mathbf{u} = 0$, then $A_{s,m}\mathbf{u} = 0$. By induction, for any $s \geq S$, we have $A_{s,m}\mathbf{u} = 0$, i.e.

$$a_s u_m + a_{s+1}u_{m-1} + \cdots + a_{s+m}u_0 = 0 \quad \text{for all } s \geq S,$$

which implies $(\sum_{t=0}^{m} u_i X^i)(\sum_{i=1}^{\infty} a_i X^i)$ is a polynomial of degree $< S + m$. □

By bounding $N_{s,m}$ with the p-adic norm and the Euclidean norm, and observing that they cannot both be small for large enough s, we can show that $Z(T)$ satisfies the criterion above, hence is rational.

Theorem 2.4.2. *$Z(H_f/\mathbb{F}_q;T)$ is a rational function.*

Proof. Write $Z(T) = Z(H_f/\mathbb{F}_q;T)$. By Theorem 2.3.2, $Z(T)$ is meromorphic, so we have $Z(T) = A(T)/B(T)$ for some p-adic entire functions $A(T)$ and $B(T)$. Take $R = q^{2n}$ and apply the p-adic Weierstrass Preparation Theorem (Theorem 1.2.7) to $B(T)$, so $B(T) = P(T)/G(T)$, where $P(T)$ is a polynomial and $G(T)$ converges on $D(R)$.

Let $F(T) = A(T)G(T)$, so $F(T) = P(T)Z(T)$. Let $Z(T) = \sum_{i=0}^{\infty} a_i T^i \in 1 + T\mathbb{Z}[[T]]$, $F(T) = \sum_{i=0}^{\infty} b_i T^i \in 1 + T\Omega[[T]]$ and $P(T) = \sum_{i=0}^{e} d_i T^i \in 1 + T\Omega[T]$. Let $m = 2e$, let

$$A_{s,m} = \{a_{s+i+j}\}_{0\le i,j\le m} = \begin{pmatrix} a_s & a_{s+1} & \dots & a_{s+m} \\ a_{s+1} & a_{s+2} & \dots & a_{s+m+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s+m} & a_{s+m+1} & \dots & a_{s+2m} \end{pmatrix}$$

and $N_{s,m} = \det(A_{s,m})$.

By Lemma 1.3.2, $|a_i|_\infty \le q^{in}$, so all entries in $A_{s,m}$ are less than $q^{n(s+2m)}$, hence

$$|N_{s,m}|_\infty \le (m+1)! q^{n(s+2m)(m+1)}.$$

Now equate coefficients in $F(T) = P(T)Z(T)$,

$$b_{j+e} = a_{j+e} + d_1 a_{j+e-1} + \cdots + d_e a_j.$$

Let $\mathbf{c}_i$ denote the ith column in $A_{s,m}$. For $0 \le j \le e$, replace each $(j+e)$th column $\mathbf{c}_{j+e}$ with

$$\mathbf{c}_{j+e} + d_1 \mathbf{c}_{j+e-1} + \cdots + d_e \mathbf{c}_j,$$

so that the new matrix has entries a_{s+i+j} in the first e columns and entries b_{s+i+j} in the last $e+1$ columns,

$$\begin{pmatrix} a_s & a_{s+1} & \dots & a_{s+e-1} & b_{s+e} & \dots & b_{s+m} \\ a_{s+1} & a_{s+2} & \dots & a_{s+e-1} & b_{s+e} & \dots & b_{s+m} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & \dots & a_{s+m+e-1} & b_{s+m+e} & \dots & b_{s+2m} \end{pmatrix}.$$

The new matrix has the same determinant $N_{s,m}$. $F(T)$ converges on $D(R)$ so for sufficiently large i, we have $|b_i|_p \le R^{-i} = q^{-2ni}$. Also, $a_i \in \mathbb{Z}$, so $|a_i|_p \le 1$. Then

$$|N_{s,m}|_p \le (max_{j\le s+e}|b_j|_p)^{e+1} < q^{-2n(s+e)(e+1)} < q^{-ns(m+2)}.$$

Multiplying the estimates,

$$|N_{s,m}|_p |N_{s,m}|_\infty < (m+1)! q^{n(s+2m)(m+1) - ns(m+2)} < (m+1)! q^{n(2m(m+1)-s)},$$

so we can pick large enough s such that

$$|N_{s,m}|_p |N_{s,m}|_\infty < 1.$$

But $a_i \in \mathbb{Z}$ so $N_{s,m} \in \mathbb{Z}$, hence we must have $N_{s,m} = 0$ for s sufficiently large. By Lemma 2.4.1, $Z(T)$ is a rational function. □

We have proved the rationality of zeta functions of affine hypersurfaces. Now Dwork's theorem follows from Remarks 3 and 2.

Theorem 2.4.3 (Dwork)**.** *The zeta function of any affine or projective variety is a rational function.*

Chapter 3

Monsky-Washnitzer Cohomology

It was believed that some cohomology theory would prove the Weil conjectures because cohomology can be used to count fixed points and points in a finite field $\mathbb{F}_q$ are fixed by the q-Frobenius. Although Dwork's proof did not involve cohomology, it inspired the construction of Monsky-Washnitzer cohomology. In 1971, Monsky proved the Lefschetz fixed point formula

$$\#X(\mathbb{F}_{q^s}) = \sum_{i=0}^{n} (-1)^i \operatorname{Tr}\left(\left(q^n F_*^{-1}\right)^s, H^i_{MW}(X/K)\right),$$

where $H^i_{MW}(X/K)$ are Monsky-Washnitzer cohomology groups. In this chapter, we will focus on Monsky-Washnitzer cohomology, so we will henceforth omit the subscripts and write $H^i(X/K) := H^i_{MW}(X/K)$. A consequence is

$$Z(X/\mathbb{F}_q; T) = \prod_i \det\left(1 - Tq^n F_*^{-1}, H^i(X/K)\right)^{(-1)^i}.$$

The idea was that if $H^i(X/K)$ are finite-dimensional, then this would provide a proof for the rationality of the zeta function. This was later proved by Berthelot [Ber97].

In this chapter, the background on affinoid algebra and Tate's Theorem are based on the first four chapters of [FvdP04]. The proof of the Lefschetz fixed point formula presented here is the refined proof by van der Put in [vdP86], which is also given in Chapter 7.6 of [FvdP04]. The original proof by Monsky can be found in [Mon71].

3.1 Discrete Valuation Rings

Definition 3.1.1 (discrete valuation)**.** *Let K be a field. A discrete valuation of K is a map $v : K \setminus \{0\} \to \mathbb{Z}$ such that for all $x, y \in K$, $x, y \neq 0$,*

(1). $v(xy) = v(x) + v(y)$,

(2). $v(x + y) \geq \min(v(x), v(y))$.

A non-Archimedean norm on K is defined by fixing some $0 < \rho < 1$ and setting $|x| = \rho^{-v(x)}$. K is a discrete valuation field if it is equipped with a discrete valuation. Its ring of integers $R := \{a \in K \mid |a| \leq 1\} = \{x \in K \mid v(x) \geq 0\}$ is a discrete valuation ring, with maximal ideal $\mathfrak{m} := \{a \in K \mid |a| < 1\}$. The residue field of K is $k = R/\mathfrak{m}$.

A discrete valuation and its corresponding non-Archimedean norm are generalisations of the p-adic order and p-adic norm, respectively. If K was taken to be $\mathbb{Q}_p$, the valuation ring R would be $\mathbb{Z}_p$, $\mathfrak{m}$ would be the ideal $p\mathbb{Z}_p$ and the residue field would be $k = \mathbb{F}_p$.

Throughout this chapter, K will denote a field with non-Archimedean norm, which we will denote as $|\cdot|$.

Definition 3.1.2 (spectrum of a ring)**.** *The spectrum of a ring R, denoted $Spec(R)$, is the set of all prime ideals of R. The maximal spectrum of a ring R, denoted $Sp(R)$, is the set of all maximal ideals of R.*

3.2 Tate's Theorem

Definition 3.2.1 (G-topologies)**.** *Let X be a set. A G-topology T on X consists of*

(1). *a family $\mathcal{F}$ of subsets of X;*

(2). *for each $U \in \mathcal{F}$, a set $Cov(U)$ of coverings of U by elements of $\mathcal{F}$;*

satisfying the properties:

(1). $\{U\} \in Cov(U)$;

(2). *For $V, U \in \mathcal{F}$ with $V \subset U$ and $\mathcal{U} \in Cov(U)$, $\{U' \cap V \mid U' \in \mathcal{U}\} \in Cov(V)$;*

(3). *If $U \in \mathcal{F}$, $\{U_i\}_{i\in I} \in Cov(U)$ and $\mathcal{U}_i \in Cov(U_i)$, then $\cup_{i\in I}\mathcal{U}_i \in Cov(U)$.*

$U \in \mathcal{F}$ are admissible sets and the elements of $Cov(U)$ are admissible coverings.

Definition 3.2.2 (sheaf)**.** *A presheaf F of abelian groups for a G-topology consists of the data:*

(1). *for every admissible U, an abelian group $F(U)$;*

(2). *for every inclusion $U \subseteq V$ of admissible sets, there is a morphism of abelian groups $\rho_U^V : F(V) \to F(U)$;*

satisfying the requirements:

(1). $F(\emptyset) = 0$;

(2). *for every admissible set U, $\rho_U^U = id$;*

(3). *for a sequence of admissible sets $U \subset V \subset W$, $\rho_U^V \circ \rho_V^W = \rho_U^W$.*

A presheaf is a sheaf if

(1). *if U is an admissible set, $\{V_i\} \in Cov(U)$ and $f \in F(U)$ such that $\rho_{V_i}^U f = 0$ for all i, then $f = 0$;*

(2). *if $\rho_{U_i\cap U_j}^{U_i} f_i = \rho_{U_i\cap U_j}^{U_j} f_j$ for each $U_i \cap U_j \neq \emptyset$, then there is a unique $f \in F(U)$ with $\rho_{U_i}^U f = f_i$ for all i.*

Definition 3.2.3 (Čech complex)**.** *Let S be a presheaf of abelian groups and $\mathcal{U} = \{U_i\}_{i\in I} \in Cov(U)$. The Čech complex is a complex of abelian groups $0 \to C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} \dots$, where*

$$C^n = \prod_{i_0,\dots,i_n\in I} S(U_{i_0} \cap U_{i_1} \cap \dots \cap U_{i_n}).$$

Write $\xi \in C^n$ as $\{\xi_{(i_0,\dots,i_n)}\}$. The map $d^n : C^n \to C^{n+1}$ is given by

$$d^n(\xi)_{(i_0,\dots,i_n)} = \sum_{j=0}^{n} \xi_{(i_0,\dots,i_{j-1},i_{j+1},\dots,i_n)}.$$

The nth cohomology group of the complex is $\check{H}^n(\mathcal{U}, S) = \ker(d^n)/\operatorname{im}(d^{n-1})$.

Definition 3.2.4 (affinoid algebra)**.** *$K\langle X_1, \dots, X_n\rangle$ is the subring of the ring of formal power series $K[[X_1, \dots, X_n]]$, consisting of all power series $\sum_\alpha c_\alpha z^\alpha \in K[[X_1, \dots, X_n]]$ satisfying $\lim |c_\alpha| = 0$. An affinoid algebra is a K-algebra A of the form $K\langle X_1, \dots, X_n\rangle/I$ for some ideal I in $K\langle X_1, \dots, X_n\rangle$. $X := Sp(A)$ is an affinoid space.*

Definition 3.2.5 (affinoid subspaces)**.** *$S \in X$ is an affinoid subspace if there exists a morphism of affinoid algebras over K, $\phi : A \to B$ such that $Sp(\phi)F \subseteq S \in X$ and for every morphism $\psi : A \to C$ such that $Sp(\psi)Sp(C) \subseteq S$, there exists a unique morhpism of affinoid algebras over K, $\tau : B \to C$ with $\psi = \tau \circ \phi$.*

Definition 3.2.6 (rational subsets)**.** *For an affinoid algebra A over K, $R \subset X := Sp(A)$ is rational if there exists $f_0, \dots, f_s \in A$ generating the unit ideal of A such that*

$$R = \{x \in X \mid |f_i(x)| \le |f_0(x)| \text{ for } i = 1, \dots, s\}.$$

Definition 3.2.7. *The presheaf O_X on X is defined by*

$$O_X(R) = A\langle Z_1, \dots, Z_s\rangle/(f_1 - f_0Z_1, \dots, f_s - f_0Z_s)$$

for any rational set $R = \{x \in X \mid |f_i(x)| \le |f_0(x)| \text{ for } i = 1, \dots, s\}$.

Definition 3.2.8 (very weak topology)**.** *The admissible subset of X for the very weak G-topology are the rational subsets. A covering $\{R_i\}_{i\in I}$ of a rational R by rational sets R_i is admissible if there exists a finite subset $J \subset I$ with $R = \cup_{i\in J} R_i$.*

Remark 6. *Lemma 4.1.3 in [FvdP04] shows that it is indeed a G-topology.*

Definition 3.2.9 (acyclic)**.** *Let F be any presheaf of abelian groups on X and U an admissible covering of X, then $\mathcal{U}$ is acyclic for F if $\check{H}^0(\mathcal{U}, F) = F(X)$ and $\check{H}^i(\mathcal{U}, F) = 0$ for all $i > 0$.*

Theorem 3.2.10 (Tate's acyclicity theorem)**.** *Let A be an affinoid algebra over K, M a finitely generated A-module and $\mathcal{U}$ a finite covering of $X := Sp(A)$ by affinoid subspaces, then $\mathcal{U}$ is acyclic for the presheaf defined by $M \otimes_A O_X$.*

The theorem implies that O_X is a sheaf. O_X is called the structure sheaf of X and the global section of the structure sheaf is the coordinate ring of its reduction to an affine variety. See Theorem 3.2 in Chapter I of [Har77].

3.3 Monsky-Washnitzer Cohomology

Consider a smooth affine variety X over a field $k = \mathbb{F}_q$ of characteristic $p > 0$ with coordinate ring $\bar{A}$. Let R be a complete mixed characteristic discrete valuation ring with residue field k and $\mathfrak{m}$ the maximal ideal of R. Let $K := Qt(R)$ be the field of fractions of R with characteristic 0.

Let π be a generator of the maximal ideal of the valuation ring R, then $R/\pi R = k$. A result of R. Elkik shows that there exists a finitely generated smooth R-algebra B, i.e. $Spec(B)$ is a smooth variety, such that $B/\pi B = \bar{A}$. Write $B = R[T_1, \ldots, T_n]/(f_1, \ldots, f_m)$.

We want to be able to define a lift of the q-Frobenius, but there is no ring endomorphism on $B = R[T_1, \ldots, T_n]/(f_1, \ldots, f_m)$ that lifts the Frobenius map on $\bar{A}$. Naturally, we would be looking to lift $\bar{A}$ to $R\langle T_1, \ldots, T_n\rangle/(f_1, \ldots, f_m)$ instead, but this leads to another problem. Specifically, $\sum_{i=0}^{\infty} p^n T^{p^n-1}$ would integrate to $\sum_{i=0}^{\infty} T^{p^n}$ which is not in $R\langle T_1, \ldots, T_n\rangle/(f_1, \ldots, f_m)$, so the space is not closed under formal integration, then the cohomology would be larger than that of A. Therefore, we define a slightly smaller space which excludes such elements.

Definition 3.3.1 (overconvergent elements)**.** *The subring of $R\langle T_1, \ldots, T_n\rangle$ consisting of all overconvergent elements is denoted by*

$$R\langle T_1, \ldots, T_n\rangle^\dagger := \left\{ \sum_u c_u T^u \in R\langle T_1, \ldots, T_n\rangle \;\middle|\; \text{there exists } \lambda > 1 \text{ such that } \lim_{|u|} |c_u|\lambda^{|u|} = 0 \right\}.$$

A weakly convergent finitely generated (wcfg) algebra is an R-algebra of the form $R\langle T_1, \ldots, T_n\rangle^\dagger/\mathfrak{I}$ for some finitely generated ideal $\mathfrak{I}$ in $R\langle T_1, \ldots, T_n\rangle^\dagger$.

Note that there are equivalent formulations of the overconvergent condition, as in Remark 4, resembling the space $R^\dagger$ in Dwork's proof.

Let $A = R\langle T_1, \ldots, T_n\rangle^\dagger/(f_1, \ldots, f_m)$, then the ring A satisfies $A/\pi A = \bar{A}$ and $A \otimes_R k = \bar{A}$.

Definition 3.3.2 (universal module of differentials)**.** *The universal module of differentials $\Omega_{\bar{A}/k}$ of $\bar{A}$ over k is the $\bar{A}$-module generated by all da for $a \in \bar{A}$, satisfying the following relations:*

(1). *$ds = 0$ for all $s \in k$;*

(2). *$d(a + b) = da + db$ for all $a, b \in \bar{A}$;*

(3). *$d(ab) = adb + bda$ for all $a, b \in \bar{A}$.*

The k-linear map $d : \bar{A} \to \Omega_{\bar{A}/k}$ is the differentiation map.

Definition 3.3.3 (de Rham cohomology)**.** *Suppose $A = R\langle T_1, \ldots, T_n\rangle^\dagger/(f_1, \ldots, f_m)$, then the module of differentials is defined by*

$$D^1(A) := (AdT_1 + \cdots + AdT_n) \,/\, \left(\sum_{i=1}^{m} A \left(\frac{\partial f_i}{\partial T_1} dT_1 + \cdots + \frac{\partial f_i}{\partial T_n} dT_n \right) \right).$$

The de Rham complex $D^\bullet(A)$ is

$$0 \to A \xrightarrow{d^0} D^1(A) \xrightarrow{d^1} D^2(A) \to \ldots$$

where $D^i(A) = \wedge^i D^1(A)$ and d^i is exterior differentiation. Since $\ker d^i / \operatorname{im} d^{i-1}$ only depends on the k-algebra $\bar{A}$, we can define the ith cohomology group of the complex

$$H^i(X/R) := H^i(\bar{A}/R) := H^i_{dR}(A) = \ker d^i / \operatorname{im} d^{i-1}.$$

Definition 3.3.4 (Monsky-Washnitzer cohomology)**.** *The Monsky-Washnitzer cohomology groups are the cohomology groups of the complex* $D^\bullet(X) = D^\bullet(A) \otimes_R K$*,*

$$H^i(X/K) := H^i(\bar{A}/K) := H^i(\bar{A}/R) \otimes_R K.$$

$R\langle T_1, \dots T_n\rangle^\dagger$ satisfies Weierstrass preparation and division, so $R\langle T_1, \dots T_n\rangle^\dagger$ is Noetherian and flat over $R[T_1, \dots, T_n]$.

The module $D^1(A) \otimes_R \bar{A} = \Omega_{\bar{A}/k}$ is projective, i.e. direct sum of free modules, and its rank equals the dimension d of $\bar{A}$. By flatness of $\bar{A}$, $D^1(A)$ is also projective of rank d.

3.4 The Lefschetz Fixed Point Formula

The Lefschetz fixed point formula for Monsky-Washnitzer cohomology is given by

$$\#X(F_{q^s}) = \sum_{i=0}^{n} (-1)^i \operatorname{Tr}\left(\left(q^n F_*^{-1}\right)^s, H^i(X/K)\right).$$

Note that it suffices to prove it for the case $s = 1$. Suppose the formula holds when $s = 1$. Let F_* be a lift of the q-Frobenius, then F_*^s is a lift of the q^s-Frobenius. By considering q^s instead of q we have

$$\#X(F_{q^s}) = \sum_{i=0}^{n} (-1)^i \operatorname{Tr}\left((q^s)^n (F_*^s)^{-1}, H^i(X/K)\right) = \sum_{i=0}^{n} (-1)^i \operatorname{Tr}\left((q^n F_*^{-1})^s, H^i(X/K)\right).$$

Definition 3.4.1 (nuclear map)**.** *Let* M *be a vector space over* K*. Consider a* K*-linear map* $L : M \to M$*. Let* K^{alg} *be the algebraic closure of* K*. A non-zero element* $\lambda \in K^{alg}$ *is an eigenvalue of* L *if its minimum polynomial* $g \in K[T]$ *has the property* $\ker(g(L), M) \neq 0$*.* L *is nuclear if*

(1). *for any eigenvalue* $\lambda \neq 0$ *with minimum polynomial* $g \in K[T]$*, there exists a direct sum decomposition* $M = A \oplus B$ *such that* A *and* B *are invariant under* L*;* $g(L)$ *is bijective on* A *and* $B = \cup_{m \geq 1} \ker(g(L)^m)$ *is finite dimensional;*

(2). *the non-zero eigenvalues of* L *form a finite set or a sequence with limit* 0*.*

A nuclear operator has a well-defined trace, which is the sum of its eigenvalues counted with multiplicities.

Theorem 3.4.2 (Hilbert's syzygy theorem)**.** *Any finitely generated module over the polynomial ring* $k[T_1, \dots, T_n]$ *admits a finite free resolution.*

Proof. See Chapter 19.2 in [Eis95]. □

Theorem 3.4.3. *Any finitely generated* $R\langle T_1, \dots T_n\rangle^\dagger$*-module admits a finite free resolution.*

Proof. The reduction of the module has a finite free resolution by the Hilbert's syzygy theorem, which can be then lifted. See Lemma 2.7 in [Mon71] for details. □

Definition 3.4.4 (Frobenius map)**.** *The lift of the q-Frobenius $F : A \to A$ is the homomorphism on A that satisfies $a \mapsto a^q \mod q$ for any $a \in A$.*

Definition 3.4.5 (Dwork operator)**.** *Given a wcfg R-algebra A and a lift $F : A \to A$ of q-Frobenius on $\bar{A}$, an additive operator $\theta : M \to M$ on a finitely generated A-module M is a Dwork operator if $\theta(F(a)m) = a\theta(m)$ holds for any $a \in A$ and $m \in M$.*

Note that the definition of a Dwork operator is somewhat similar to the operator T_q with $T_q \circ L_{G_q} = L_G \circ T_q$ in Dwork's proof.

Theorem 3.4.6. *Consider a wcfg R-algebra A, a lift $F : A \to A$ of the q-Frobenius on $\bar{A}$ and a finitely generated A-module M. Any Dwork operator $\theta : M \to M$ induces a nuclear map $\theta : M \otimes K \to M \otimes K$.*

Proof. There is a surjective homomorphism $R\langle T_1, \dots T_n\rangle^\dagger \to A$ and a lift of the q-Frobenius of $k[T_1, \dots, T_n]$ to $R\langle T_1, \dots, T_n\rangle^\dagger$ which induces the given F on A, so it suffices to prove for $A = R\langle T_1, \dots T_n\rangle^\dagger$.

By Theorem 3.4.3, the module M has a finite free resolution

$$0 \to M_s \xrightarrow{\phi_s} M_{s-1} \xrightarrow{\phi_{s-1}} \dots \xrightarrow{\phi_1} M_0 \xrightarrow{\phi_0} M \to 0.$$

On each M_i, we will construct Dwork operators θ_i such that the diagram

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & M_s & \xrightarrow{\phi_s} & M_{s-1} & \xrightarrow{\phi_{s-1}} & \dots & \xrightarrow{\phi_1} & M_0 & \xrightarrow{\phi_0} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \theta_s} & & \downarrow{\scriptstyle \theta_{s-1}} & & & & \downarrow{\scriptstyle \theta_0} & & \downarrow{\scriptstyle \theta} & & \\
0 & \longrightarrow & M_s & \xrightarrow{\phi_s} & M_{s-1} & \xrightarrow{\phi_{s-1}} & \dots & \xrightarrow{\phi_1} & M_0 & \xrightarrow{\phi_0} & M & \longrightarrow & 0
\end{array}$$

commutes. Let $e_1, \dots, e_m$ be a free basis of M_0. Since A is an $F(A)$-module with free basis $\{T^{\mathbf{u}} \mid 0 \le u_j < q \text{ for all } j\}$ and $\theta_0\left(\sum_{i=1}^m \sum_{\mathbf{u}} F\left(a_{\mathbf{u}i}\right) T^{\mathbf{u}} e_i\right) = \sum_{i=1}^m \sum_{\mathbf{u}} a_{\mathbf{u}i} \theta_0\left(T^{\mathbf{u}} e_i\right)$, θ_0 is completely determined by $\{\theta_0\left(T^{\mathbf{u}} e_i\right) \mid 1 \le i \le m, \quad 0 \le u_j < q \text{ for all } j\}$. $\theta_0\left(T^{\mathbf{u}} e_i\right)$ can be found by setting $\phi_0 \circ \theta = \theta_0 \circ \phi_0$. Repeating the process for $M_1, \dots, M_s$, we have the Dwork operators $\theta_0, \dots, \theta_s$. If $\theta_0, \dots, \theta_s$ are nuclear, then θ is also nuclear, hence it suffices to prove the theorem for free modules M.

Suppose that M is a free module over A with basis $e_1, \dots, e_m$. For $r > 1$, let $A(r)$ denote the subspace of A consisting of the power series $\sum a_{\mathbf{u}} T^{\mathbf{u}}$ with $\lim |a_{\mathbf{u}}| r^{|\mathbf{u}|} = 0$. $A(r)$ is a Banach space with respect to the norm $\| \sum a_{\mathbf{u}} T^{\mathbf{u}} \| = \max |a_{\mathbf{u}}| r^{|\mathbf{u}|}$. Let $M(r) = \oplus_{i=1}^m A(r) e_i$, which is also a Banach space.

Let $\sum_{\mathbf{w}} \sum_{\mathbf{u}} a_{\mathbf{uw}} T^{q\mathbf{w}+\mathbf{u}} \in A(r)$ where $0 \le u_j < q$, then $\lim_{|\mathbf{w}|} |a_{\mathbf{uw}}| r^{|q\mathbf{w}+\mathbf{u}|} = 0$ for any $\mathbf{u}$.

$$\theta\left(\sum_{\mathbf{w}} \sum_{\mathbf{u}} a_{\mathbf{uw}} T^{q\mathbf{w}+\mathbf{u}} e_i\right) = \sum_{\mathbf{w}} \sum_{\mathbf{u}} a_{\mathbf{uw}} T^{\mathbf{w}} \theta\left(T^{\mathbf{u}} e_i\right)$$

and $\{\theta\left(T^{\mathbf{u}} e_i\right) \mid 1 \le i \le m, \quad 0 \le u_j < q \text{ for all } j\}$ has finite elements. For $1 < r \le r_0$ for some small enough r_0, $\theta\left(M(r)\right) \subseteq M\left(r^q\right)$ and its restriction to $M(r)$, $\theta_r^1 : M(r) \to M\left(r^q\right)$ is continuous. The inclusion map $\theta_r^2 : M\left(r^q\right) \hookrightarrow M(r)$ is the uniform limit of R-linear operators of finite rank, and so $\theta_r = \theta_r^2 \circ \theta_r^1 : M(r) \xrightarrow{\theta_r^1} M\left(r^q\right) \xhookrightarrow{\theta_r^2} M(r)$ is also completely continuous.

Serre showed in [Ser62] that the uniform limit of R-linear operators of finite rank of a Banach space is nuclear. Thus for all r with $1 < r \leq r_0$, the map θ_r is nuclear. $\mathrm{Tr}(\theta_r)$ can be calculated with respect to any orthogonal basis $\{b_n \mid n \geq 1\}$ of $M(r)$. If $\theta_r(b_n) = \sum_{m=1}^{\infty} \lambda_{nm} b_m$ for $n \geq 1$, then $\mathrm{Tr}(\theta_r) = \sum_{n=1}^{\infty} \lambda_{nn}$. The spaces $M(r)$ have a common orthogonal basis $\{T^{\mathbf{u}} e_i \mid 1 \leq i \leq m, \quad \mathbf{u} \in \mathbb{Z}^n_{\geq 0}\}$. Hence $\mathrm{Tr}(\theta_r)$ for $1 < r \leq r_0$ does not depend on r and the same holds for $\mathrm{Tr}(\theta_r^n)$ and $\det(1 - t\theta_r)$ for $1 < r \leq r_0$. Therefore, $\theta = \lim \theta_r : M = \cup_{r>1} M(r) \to M$ is also nuclear. □

Theorem 3.4.7. *Let B be a wcfg algebra associated to a smooth connected affine variety over k. Let A be the integral closure of B in a finite extension of $Qt\,(B)$. Then there exists a $D^\bullet\,(B)$-linear trace map*

$$S_{A/B} : D^\bullet(A) \to D^\bullet\,(B)$$

extending the trace map $\mathrm{Tr}_{Qt(A)/Qt(B)} : Qt(A) \to Qt\,(B)$.

Proof. The natural map $D^\bullet\,(B) \to D^\bullet(A)$ extends to an isomorphism

$$D^\bullet\,(B) \otimes_B Qt(A) \xrightarrow{\cong} D^\bullet(A) \otimes_A Qt(A).$$

See Theorem 8.1 in [MW68].

Define the trace map

$$S_{A/B} : D^\bullet(A) \to D^\bullet(A) \otimes_A Qt(A) \xrightarrow{\cong} D^\bullet\,(B) \otimes_B Qt(A) \xrightarrow{id_{D^\bullet(B)} \otimes \mathrm{Tr}_{Qt(A)/Qt(B)}} D^\bullet\,(B) \otimes_B Qt\,(B)\,.$$

It remains to show that the image of $S_{A/B}$ is in $D^\bullet\,(B)$. See Theorem 8.3 in [MW68]. □

Theorem 3.4.8. *Let X be smooth affine and connected over $k = \mathbb{F}_q$ with dimension n. Suppose $\bar{A}$, the coordinate ring of X, is smooth and finitely generated. Consider an wcfg algebra A obtained by lifting $\bar{A}$ and a lift $F : A \to A$ of the q-Frobenius of $\bar{A}$. Define*

$$\psi : D^\bullet(A) \xrightarrow{S_{A/F(A)}} D^\bullet(F(A)) \underset{F}{\xleftarrow{\cong}} D^\bullet(A).$$

Then

(1). *$\psi(F(A)m) = a\psi(m)$ for $a \in A$ and $m \in D^\bullet(A)$.*

(2). *$\psi(D^i(A)) \subseteq D^i(A)$ and ψ commutes with the differentiation on $D^\bullet(A)$.*

(3). *$\psi \circ F$ is multiplication by q^n.*

(4). *Let F_* and ψ_* denote the actions of F and ψ on $H^*(X/K)$ respectively. Then F_* is bijective and $\psi_* = q^n F_*^{-1}$.*

(5). *$\psi : D^\bullet(A) \otimes K \to D^\bullet(A) \otimes K$ is nuclear. Moreover*

$$\sum_{i=0}^{n} (-1)^i \,\mathrm{Tr}\left(q^n F_*^{-1}, H^i(X/K)\right) = \sum_{i=0}^{n} (-1)^i \,\mathrm{Tr}(\psi, D^i(A) \otimes K).$$

Proof. (1) and (2) follow from the definition of ψ.

For (3), since $n = \dim \bar{A}$, $q = \#k$ and $S_{A/F(A)}$ is $D^\bullet(F(A))$-linear, $\psi \circ F = S_{A/F(A)}$ is multiplication by $S_{A/F(A)}(1) = [A : F(A)] = [\bar{A} : \bar{A}^q] = q^n$.

For (4), suppose $Qt(A)$ is a Galois extension of $Qt(F(A))$ with group G, then every $\sigma \in G$ maps A onto A and $\sigma \equiv id \mod \pi$. It follows that σ_* on $H^*(\bar{A}/K)$ is also the identity. Let i denote the inclusion $F(A) \hookrightarrow A$. From $i \circ S_{A/F(A)} = \sum_{\sigma \in G} \sigma : D^\bullet(A) \to D^\bullet(A)$, it follows that $i_* \circ \left(S_{A/F(A)}\right)_* : H^*(\bar{A}/K) \to H^*(\bar{A}/K)$ is multiplication by q^n. Hence $\left(S_{A/F(A)}\right)_*$ and ψ_* are injective. $\psi_* \circ F_* = q^n$ holds by (3). Hence ψ_* and F_* are bijective.

If $Qt(A)$ is not a Galois extension of $Qt(F(A))$, then we can work with $F(A) \subset A \subset C$, where C is the integral closure of $F(A)$ in a Galois extension containing $Qt(A)$. An analogous argument shows that $\left(S_{A/F(A)}\right)_*$ is injective.

For (5), ψ is nuclear on $D^i(A)$ by Theorem 3.4.6 and (4). □

Theorem 3.4.9 (Lefschetz fixed point formula)**.** *Let $N(\bar{A})$ denote the set of k-homomorphisms $\bar{A} \to k = \mathbb{F}_q$. Then*

$$\#N(\bar{A}) = \sum_{i=0}^{n} (-1)^i \operatorname{Tr}\left(q^n F_*^{-1}, H^i(\bar{A}/K)\right),$$

where $n = \dim \bar{A}$.

Remark 7. *If $\phi : \bar{A} \to k$ is a k-homomorphism, then ϕ is surjective and $\bar{A}/\ker\phi \cong k$. As $\ker\phi$ is a maximal ideal of $\bar{A}$, it corresponds to a point in the affine variety $X = Spec(\bar{A})$. Such a homomorphism is uniquely determined by the maximal ideal $x \in X$ defining the kernel, $\phi(f) = f(x)$, so $\#N(\bar{A}) = \#X(\mathbb{F}_q)$.*

Since $\psi_* = q^n F_*^{-1}$ is nuclear on each $H^i(\bar{A}/K)$, the sum $\sum_{i=0}^n (-1)^i \operatorname{Tr}(q^n F_*^{-1}, H^i(\bar{A}/K))$ can be written as $L(\bar{A}) := \sum_{i=0}^n (-1)^i \operatorname{Tr}(\psi, D^i(A) \otimes K)$, where A is a wcfg algebra obtained by lifting $\bar{A}$. Choose elements $\bar{f}_1, \ldots, \bar{f}_s \in \bar{A}$ generating the trivial ideal $(1) = \bar{A}$. Let $X_i = \{x \in X \mid \bar{f}_i(x) \neq 0\}$ and let $f_i \in A$ with norm 1 be a lift of $\bar{f}_i$. Then $X_{i_1} \cap \cdots \cap X_{i_a} = Sp\left(\bar{A}_{\bar{f}_{i_1} \cdots \bar{f}_{i_a}}\right)$ lifts to $A\langle 1/f_{i_1} \ldots f_{i_a}\rangle^\dagger$. $Sp(A)$ has a covering of $\left\{ Sp\left(A\left\langle \frac{1}{f_i}\right\rangle^\dagger\right) \,\middle|\, i = 1, \ldots, s \right\}$. By Tate's theorem, the sheaf $D^\bullet(\quad) \otimes K$ is acyclic with respect to finite affinoid coverings, so the Čech complex

$$0 \to \oplus_i D^\bullet\left(A\left\langle \frac{1}{f_i}\right\rangle^\dagger\right) \otimes K \to \oplus_{i<j} D^\bullet\left(A\left\langle \frac{1}{f_i f_j}\right\rangle^\dagger\right) \otimes K \to \ldots$$

has cohomology group $D^\bullet(A) \otimes K$ at degree 0 and the higher degree cohomology groups are trivial. There is an exact sequence:

$$0 \to D^\bullet(A) \otimes K \to \oplus_i D^\bullet\left(A\left\langle \frac{1}{f_i}\right\rangle^\dagger\right) \otimes K \to \oplus_{i<j} D^\bullet\left(A\left\langle \frac{1}{f_i f_j}\right\rangle^\dagger\right) \otimes K \to \ldots.$$

$$L(\bar{A}) = \sum_i L\left(\bar{A}_{\bar{f}_i}\right) - \sum_{i<j} L\left(\bar{A}_{\bar{f}_i \bar{f}_j}\right) + \ldots.$$

Hence it suffices to prove the formula or small enough affine subspaces, namely when $N(\bar{A}) = 0$ and when $N(\bar{A}) = 1$. Then by induction on the size of the generating set $\bar{f}_1, \ldots, \bar{f}_s$ we will have $N(\bar{A}) = L(\bar{A})$.

Lemma 3.4.10. *If $N(\bar{A}) = 0$, then $L(\bar{A}) = 0$.*

Proof. Let $\theta : M \to M$ be any Dwork operator. For $a \in A$, let L_a denote the multiplication on M by a. Then $\theta \circ L_{F(a)} = L_a \circ \theta$. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker L_a & \longrightarrow & M & \xrightarrow{L_a} & M & \longrightarrow & \operatorname{coker} L_a & \longrightarrow & 0 \\ & & \downarrow & & {\scriptstyle \theta\circ L_a}\downarrow & & {\scriptstyle L_a\circ\theta}\downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker L_a & \longrightarrow & M & \xrightarrow{L_a} & M & \longrightarrow & \operatorname{coker} L_a & \longrightarrow & 0 \end{array} .$$

The maps induced by $\theta \circ L_a$ and $L_a \circ \theta$ on $\ker(L_a)$ and $\operatorname{coker}(L_a)$ are 0. Eigenvalues of $\theta \circ L_a$ map to eigenvalues of $L_a \circ \theta$ by L_a so this map is one-to-one and onto. We have $\operatorname{Tr}(\theta \circ L_a) = \operatorname{Tr}(L_a \circ \theta)$ for every $a \in A$. Since $\theta \circ L_a$ and $L_a \circ \theta$ are nuclear operators, $\operatorname{Tr}(\theta \circ L_{F(a)-a}) = \operatorname{Tr}(\theta \circ L_{F(a)} - \theta \circ a) = \operatorname{Tr}(L_a \circ \theta - \theta \circ L_a) = 0$ for every $a \in A$.

$N(\bar{A}) = 0$ implies that the ideal in $\bar{A}$ generated by $\{\bar{a}^q - \bar{a} \mid \bar{a} \in \bar{A}\}$ equals $\bar{A}$. Then the ideal in A generated by $\{F(a) - a \mid a \in A\}$ is also a unit ideal, so $\sum_{i=1}^{s} b_i(F(a_i) - a_i) = 1$ for some $a_i \in A$, then $\theta = \sum_{i=1}^{s} (\theta \circ L_{b_i}) \circ L_{F(a_i)-a_i}$ and $\operatorname{Tr}(\theta) = 0$.

Putting $\theta = \psi$ and $M = D^i(A)$, we find that $L(\bar{A}) = 0$. □

Lemma 3.4.11. *Let $A = R\langle X_1, \ldots, X_m, Y\rangle^\dagger / (f_{n+1}, \ldots, f_m, gY - 1)$. There exists a residue map $\operatorname{Res} : A\langle X_n^{-1}\rangle^\dagger \otimes K \to (A/(X_n)) \otimes K$, with the following properties:*

(1). $\operatorname{Res} \circ \frac{\partial}{\partial X_n} = 0$,

(2). *every element of $A\langle X_n^{-1}\rangle^\dagger \otimes K$ can be written in the form $\frac{a}{X_n} + \frac{\partial F}{\partial X_n}$, where $a \in A \otimes K$ and $F \in A\langle X_n^{-1}\rangle^\dagger \otimes K$,*

(3). *if $G \in A\langle X_n^{-1}\rangle^\dagger \otimes K$ and $\frac{\partial G}{\partial X_n} \in A \otimes K$, then $G \in A \otimes K$.*

Proof. The completion of A with respect to the ideal $(X_1, \ldots, X_m)$ is

$$\hat{A} = \varprojlim A/(X_1, \ldots, X_m)^s = A[[T_1, \ldots, T_m]]/(T_1 - X_1, \ldots, T_m - X_m)$$

and can be viewed as $R[[X_1, \ldots, X_n]]$. The derivations $\frac{\partial}{\partial X_i}$ for $i = 1, \ldots, n$ on A extend to $\hat{A} = R[[X_1, \ldots, X_n]]$ and they are derivations of $\hat{A}/R$.

Let $R[[X_1, \ldots, X_n]]\langle X_n^{-1}\rangle$ denote the π-adic completion of $R[[X_1, \ldots, X_n]][X_n^{-1}]$. $\frac{\partial}{\partial X_n}$ extends in a unique continuous way. $A\langle X_n^{-1}\rangle^\dagger$ is a subring of $R[[X_1, \ldots, X_n]]\langle X_n^{-1}\rangle$ and the two derivations $\frac{\partial}{\partial X_n}$ coincide on $A\langle X_n^{-1}\rangle^\dagger$.

$G \in A\langle X_n^{-1}\rangle^\dagger$ can be expanded as

$$G = \sum_{m=-\infty}^{\infty} G_m(X_1, \ldots, X_{n-1}) X_n^m \in R[[X_1, \ldots, X_n]]\langle X_n^{-1}\rangle,$$

where $G_m \in R[[X_1, \ldots, X_{n-1}]]$. $\frac{\partial G}{\partial X_n} \in A$ implies $G \in R[[X_1, \ldots, X_n]]$ and (3) follows from $A = A\langle X_n^{-1}\rangle^\dagger \cap R[[X_1, \ldots, X_n]]$.

For $a \in A$ and $k \geq 1$,

$$\frac{a}{X_n^k} = -\frac{\partial}{\partial X_n}\left(\frac{a}{(k-1)X_n^{k-1}} + \frac{1}{(k-1)(k-2)X_n^{k-2}}\frac{\partial a}{\partial X_n} + \cdots + \frac{1}{(k-1)!X_n}\frac{\partial^{k-1}a}{\partial X_n^{k-1}}\right) + \frac{1}{(k-1)!X_n}\frac{\partial^k a}{\partial X_n^k}$$

For $a \in A$, $\frac{1}{k!}\frac{\partial^k a}{\partial X_n^k} \in (A \otimes K) \cap R[[X_1, \ldots, X_n]] = A$. Let $G = \sum_{k=1}^{\infty} a_k X_n^{-k} \in A\langle X_n^{-1}\rangle^\dagger \otimes K$, then $G = F' + aX_n^{-1}$, where $a = \sum_{k=1}^{\infty} \frac{1}{(k-1)!}\frac{\partial^k a_k}{\partial X_n}$ and

$$F = -\sum_{k=1}^{\infty}\left(\frac{a_k}{(k-1)X_n^{k-1}} + \frac{1}{(k-1)(k-2)X_n^{k-2}}\frac{\partial a_k}{\partial X_n} + \cdots + \frac{1}{(k-1)!}\frac{\partial^{k-1}a_k}{\partial X_n^{k-1}}\right).$$

The two infinite sums converge to elements $a \in A \otimes K$ and $F \in A\langle X_n^{-1}\rangle^\dagger \otimes K$, and this proves (2). The map Res is defined by $\mathrm{Res}\left(\frac{a}{X_n} + \frac{\partial F}{\partial X_n}\right) = a \mod X_n \in (A/(X_n)) \otimes K$. Res is well defined and has the property in (1). □

Lemma 3.4.12. *If $N(\bar{A}) = 1$, then there exists $\bar{f} \in \bar{A}\backslash\{0\}$ such that $N(\bar{A}_{\bar{f}}) = L(\bar{A}_{\bar{f}}) = 1$.*

Proof. We can localise at a small enough neighbourhood of the k-valued point of $Spec(\bar{A})$. By applying suitable transformations, we can assume $\bar{A}$ has the form

$$\bar{A} = k[X_1, \ldots, X_m]_{\bar{g}}/(\bar{f}_{n+1}, \ldots, \bar{f}_m),$$

where $n = \dim \bar{A}$, such that

(1). $(0, \ldots, 0)$ is the only k-rational point of $Spec(\bar{A})$;

(2). $\bar{f}_i = X_i +$ terms with order ≥ 2;

(3). $Spec(\bar{A})$ is isomorphic to $\mathbb{A}_k^n$ by the identity map restricted to the first n coordinates, so that $\left(\frac{\partial \bar{f}_i}{\partial x_j}\right)_{i,j=n+1}^m$ is invertible in $\bar{A}$ and $\det\left(\left(\frac{\partial \bar{f}_i}{\partial x_j}\right)_{i,j=n+1}^m\right) = \bar{g}$.

Put $A = R\langle X_1, \ldots, X_m, Y\rangle^\dagger/(f_{n+1}, \ldots, f_m, gY - 1)$ and define the complex $C^\bullet$ by the exact sequence

$$0 \to D^\bullet(A) \otimes K \to D^\bullet\left(A\langle X_n^{-1}\rangle^\dagger\right) \otimes K \to C^\bullet \to 0.$$

There is a well-defined degree 1 morphism $\tau : D^\bullet(A/(X_n)) \otimes K \to C^\bullet$ mapping ω to $\tilde{\omega} \wedge \frac{dX_n}{X_n}$ in $C^\bullet$, where $\tilde{\omega} \in D^\bullet(A) \otimes K$ has image ω in $D^\bullet(A/(X_n)) \otimes K$.

Define $\mathrm{Res} : C^\bullet \to D^\bullet(A/(X_n)) \otimes K$, a morphism of complexes by defining the Res of a q-form of $D^\bullet(A\langle X_n^{-1}\rangle^\dagger) \otimes K$.

$$\mathrm{Res}\left(\sum_{i_1<\cdots<i_q<n} a_i dx_{i_1} \wedge \cdots \wedge dx_{i_q} + \sum_{i_1<\cdots<i_{q-1}<n} b_i dx_{i_1} \wedge \cdots \wedge dx_{i_{q-1}} \wedge dx_n\right)$$
$$= \sum_{i_1<\cdots<i_{q-1}<n} \mathrm{Res}(b_i) dx_{i_1} \wedge \cdots \wedge dx_{i_{q-1}} \wedge dx_n \in D^\bullet\left(A/(X_n)\right)^{q-1} \otimes K.$$

By construction, $\mathrm{Res} \circ \tau = id$.

Suppose $\omega \in D^q(A\langle X_n^{-1}\rangle^\dagger) \otimes K$ satisfies $\mathrm{Res}\,\omega = 0$ and $d\omega \in D^{q+1}(A) \otimes K$. Every $\mathrm{Res}\, b_i = 0$ so $b_i = \frac{\partial B_i}{\partial X_n}$ for some $B_i \in A\langle X_n^{-1}\rangle^\dagger \otimes K$. Put

$$\eta_0 = (-1)^{q-1} \sum_{i_1 < \cdots < i_{q-1} < n} B_i dx_{i_1} \wedge \cdots \wedge dx_{i_{q-1}},$$

then

$$\omega - d\eta_0 = \sum_{i_1 < \cdots < i_q < n} \tilde{a}_i dx_{i_1} \wedge \cdots \wedge dx_{i_q}.$$

Since $d(\omega - d\eta_0) \in D^\bullet(A)^{q+1} \otimes K$, all $\frac{\partial \tilde{a}_i}{\partial X_n} \in A$, hence all $\tilde{a}_i \in A$. Then $\omega = d\eta_0 + \eta_1$ with $\eta_0 \in D^{q-1}(A\langle X_n^{-1}\rangle^\dagger) \otimes K$ and $\eta_1 \in D^q(A) \otimes K$. Hence, $\mathrm{Res} : H^r(C^\bullet) \to H^{r-1}(D^\bullet(A/(X_n)) \otimes K)$ is injective so $\tau \circ \mathrm{Res} = id$ on the cohomology groups.

τ induces an isomorphism on the cohomology groups, then $L(\bar{A}_{X_n}) = N(\bar{A}_{X_n})$ implies $L(\bar{A}) = L(\bar{A}/(X_n))$.

We have $N(\bar{A}) = N(\bar{A}/(X_n)) = 1$, then the formula follows by induction on the dimension of $\bar{A}$. □

Chapter 4

Counting Points with Kedlaya's Algorithm

Kedlaya developed an algorithm in [Ked01] to count points on hyperelliptic curves by considering the Monsky-Washnitzer cohomology of the curves. The algorithm was extended to nondegenerate curves in [CDV06].

Here we will present Kedlaya's algorithm, following [Ked01] and [Edi03].

Denote the unramified extension of $\mathbb{Q}_p$ of degree $n = \log_p q$ by $\mathbb{Q}_q$. This extension is unique and is obtained by adjoining the primitive $(p^n - 1)$th root of unity ξ, i.e. $\mathbb{Q}_q = \mathbb{Q}_p[\xi] \subset \mathbb{Q}^{alg}$ and equipped with the extension of the p-adic norm. Denote the ring of q-adic integers by $\mathbb{Z}_q$, i.e. the ring of Witt vectors $W(\mathbb{F}_q)$.

4.1 The Cohomology of Hyperelliptic Curves

We consider hyperelliptic curves over a field of characteristic $p > 2$. Let $\bar{Q}(x)$ be a polynomial of degree $d = 2g + 1$ over $\mathbb{F}_q$ without repeated roots, so that the closure in the projective plane of the affine curve $y^2 = \bar{Q}(x)$ is a smooth hyperelliptic curve C of genus g.

Note that the algorithm can be generalised to the case where $\deg \bar{Q}$ is even, as shown in [Har12].

Let C' be the affine curve obtained from C by removing the point at infinity and the zeros of y, i.e. points $(\alpha, 0)$ where α is root of $\bar{Q}$. Then the coordinate ring of C' is

$$\bar{A} = \mathbb{F}_q[x, y, y^{-1}]/(y^2 - \bar{Q}(x)).$$

Pick a lift Q of $\bar{Q}$ in $\mathbb{Z}_q[x]$. Let $A = \mathbb{Z}_q[x, y, y^{-1}]/(y^2 - Q(x))$ and let

$$A^\dagger = \mathbb{Z}_q\langle x, y, y^{-1}\rangle^\dagger/(y^2 - Q(x)) = \mathbb{Z}_q\langle x, y, z\rangle^\dagger/(y^2 - Q(x), yz - 1)$$

be the weak completion of A. $A^\dagger$ can be viewed as

$$\left\{ \sum_{n=-\infty}^{\infty} S_n(x) y^n \;\middle|\; S_n \in \mathbb{Z}_q[x], \quad \deg S_n \leq 2g, \quad \mathrm{ord}_p(S_n) > Cn \text{ for some } C > 0 \right\}.$$

The module of differentials of $A^\dagger$ is

$$D^1(A^\dagger) := \left(A^\dagger dx + A^\dagger dy + A^\dagger dz\right) / \left(A^\dagger \left(2ydy - Q'(x)dx\right) + A^\dagger \left(zdy + ydz\right)\right) = A^\dagger dx.$$

The de Rham complex $D^\bullet(A^\dagger)$ is

$$0 \to A^\dagger \xrightarrow{d} D^1(A^\dagger) \to 0.$$

The de Rham cohomology groups $H^i(\bar{A}/\mathbb{Z}_q) = 0$ for $i > 1$ so we only have to consider the groups $H^0(\bar{A}/\mathbb{Z}_q)$ and $H^1(\bar{A}/\mathbb{Z}_q)$. $H^0(\bar{A}/\mathbb{Z}_q) = \ker d$, $H^1(\bar{A}/\mathbb{Z}_q) = D^1(A^\dagger)/\operatorname{im} d = A^\dagger dx/\operatorname{im} d$. The Monsky-Washnitzer cohomology groups are $H^i(\bar{A}/\mathbb{Q}_q) = H^i(\bar{A}/\mathbb{Z}_q) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$.

Definition 4.1.1 (hyperelliptic involution)**.** *The hyperelliptic involution is the map $(x, y) \mapsto (x, -y)$ on C.*

Definition 4.1.2 (cohomologous)**.** *If a, b have the same image in cohomology, we say a and b are cohomologous and write $a \equiv b$.*

Now we look at the structure of the de Rham cohomology group $H^1(\bar{A}/\mathbb{Z}_q)$. We can consider elements in $A^\dagger dx$ as representatives of elements in the group, quotienting by $\operatorname{im} d$.

Lemma 4.1.3. *The de Rham cohomology of A splits into eigenspaces under the hyperelliptic involution, a positive eigenspace $H^1(\bar{A}/\mathbb{Z}_q)^+$ generated by $\{x^i dx/y^2 \mid i = 0, \ldots, 2g\}$ and a negative eigenspace $H^1(\bar{A}/\mathbb{Z}_q)^-$ generated by $\{x^i dx/y \mid i = 0, \ldots, 2g-1\}$.*

Proof. Any form in $H^1(\bar{A}/\mathbb{Z}_q)$ can be written as

$$\begin{aligned}\sum_{n=-\infty}^{\infty} S_n(x) y^n dx &= \sum_{m=0}^{\infty} (S_{2m-2}(x) + y S_{2m-1}(x)) y^{2m-2} dx + \sum_{n=3}^{\infty} \frac{S_{-n}(x)dx}{y^n} \\ &= \sum_{m=0}^{\infty} \frac{S_{2m-2}(x)Q(x)^m dx}{y^2} + \sum_{m=0}^{\infty} \frac{S_{2m-1}(x)Q(x)^m dx}{y} + \sum_{n=3}^{\infty} \frac{S_{-n}(x)dx}{y^n}\end{aligned}$$

where $\deg S_n \leq 2g$.

Consider a term $R(x) := S_{-n}(x)dx/y^n$ where $n > 2$. $Q(x)$ has no repeated roots, so we can find polynomials $A(x)$ and $B(x)$ such that $R(x) = A(x)Q(x) + B(x)Q'(x)$. Since

$$d\left(\frac{B(x)}{y^{s-2}}\right) = \frac{B'(x)dx}{y^{s-2}} - \frac{(s-2)\,B(x)dy}{y^{s-1}} \equiv 0$$

and $2ydy = Q'(x)dx$, we have

$$\frac{R(x)dx}{y^s} = (A(x)Q(x) + B(x)Q'(x))\,\frac{dx}{y^s} = \frac{A(x)dx}{y^{s-2}} + \frac{B(x)Q'(x)dx}{y^s} = \frac{A(x)dx}{y^{s-2}} + \frac{2B(x)dy}{y^{s-1}}.$$

The first reduction relation

$$\frac{R(x)dx}{y^s} \equiv \left(A(x)dx + \frac{2B'(x)}{s-2}\right)\frac{dx}{y^{s-2}} \tag{4.1}$$

can consolidate the terms to $n = 1$ and $n = 2$ terms.

Now rewriting the form,

$$\sum_{n=-\infty}^{\infty} S_n(x) y^n dx \equiv \frac{R_1(x)dx}{y} + \frac{R_2(x)dx}{y^2}.$$

If $R_1(x)$ has degree $m \geq 2g$, take $P(x) = x^{m-2g}$, then

$$d(2P(x)y) = 2P'(x)ydx + 2P(x)dy = (P(x)Q'(x) + 2P'(x)Q(x))\frac{dx}{y} \equiv 0.$$

The second reduction relation is

$$(P(x)Q'(x) + 2P'(x)Q(x))\frac{dx}{y} \equiv 0. \tag{4.2}$$

The term $(P(x)Q'(x) + 2P'(x)Q(x))$ has degree m and leading term $(2g+1) + 2(m-2g) = 2m - 2g + 1 \neq 0$ so a suitable multiple can be subtracted from $R_1(x)$ to reduce its degree to $m-1$. Cary out this process repeatedly reduces $R_1(x)$ to degree $\leq 2g-1$.

If $\deg R_2 \geq 2g+1$, subtracting a multiple of $dx = Q(x)dx/y^2$ reduces R_2 to degree $\leq \deg Q - 1 = 2g$. □

Note that the basis of the de Rham cohomology of A is also a basis of the Monsky-Washnitzer cohomology and we can view it as changing the base field from $\mathbb{Z}_q$ to $\mathbb{Q}_q$.

Remark 8. *Given a polynomial $R(x) = r_{2g}x^{2g} + \cdots + r_0$ of degree $\leq 2g$, we can find polynomials $A(x)$ and $B(x)$ with $\deg A < 2g$ and $\deg B < 2g+1$, such that $R(x) = A(x)Q(x) + B(x)Q'(x)$. Namely, write $Q(x) = x^{2g+1} + c_{2g}x^{2g} + \cdots + c_0$ and define a $(4g+1) \times (4g+1)$ matrix with the coefficients of $Q(x)$ and $Q'(x)$*

$$T := \begin{pmatrix} c_0 & & & c_1 & & \\ c_1 & \ddots & & 2c_2 & \ddots & \\ & \ddots & c_0 & & \ddots & \\ \vdots & & c_1 & \vdots & & c_1 \\ & & & & & 2c_2 \\ & & & (2g+1)c_{2g+1} & & \\ c_{2g+1} & & \vdots & & \ddots & \vdots \\ & \ddots & & & & \\ & & c_{2g+1} & & & (2g+1)c_{2g+1} \end{pmatrix},$$

and a vector $v := (r_0, \ldots, r_{2g}, 0, \ldots, 0)$. Note that columns of T are linearly independent since Q and Q' are coprime. Find $T^{-1}v = (a_0, \ldots, a_{2g-1}, b_0, \ldots, b_{2g})$ by solving the system of linear equations, for example applying the Cramer's rule, then we have $A(x) = a_{2g-1}x^{2g-1} + \cdots + a_0$ and $B(x) = b_{2g}x^{2g} + \cdots + b_0$ that satisfy $R(x) = A(x)Q(x) + B(x)Q'(x)$.

4.2 Consequences of the Weil Conjectures

As special case of the Weil conjectures, proved by Weil, we have for a smooth curve C of genus g over a finite field $\mathbb{F}_q$, that

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

where $P(T) = \prod_j (1 - \alpha_j T) = a_{2g}T^{2g} + a_{2g-1}T^{2g-1} + \cdots + 1 \in \mathbb{Z}[T]$ with degree $2g$. From the power series expansion of the quotient, we can see that for any $s > 0$,

$$q^s + 1 - \#C(\mathbb{F}_{q^s}) = \sum_{j=1}^{2g} \alpha_j^s.$$

Moreover, $\alpha_j \alpha_{g+j} = q$ for $j = 1, \ldots, g$, $|\alpha_j|_\infty = q^{1/2}$ for $j = 1, \ldots, 2g$ and $q^{g-i}a_i = a_{2g-i}$ for $i = 0, \ldots, 2g$. See Theorem 5.15 and Corollary 5.16 in [Sti09]. The relationship $q^{g-i}a_i = a_{2g-i}$ implies that it is enough to determine $a_1, \ldots, a_g$.

We are interested in finding $P(T)$ explicitly, so it would be helpful to find a bound for the coefficients.

Theorem 4.2.1. *$|a_i|_\infty \leq \binom{2g}{i} q^{i/2} \leq 2^{2g} q^{g/2}$ for $i = 1, \ldots, g$.*

Proof. We have

$$|a_i|_\infty = |\sum_{j_1 < \cdots < j_i} \alpha_{j_1} \ldots \alpha_{j_i}|_\infty \leq \sum_{j_1 < \cdots < j_i} |\alpha_{j_1} \ldots \alpha_{j_i}|_\infty = \binom{2g}{i} q^{i/2} \leq 2^{2g} q^{i/2} \leq 2^{2g} q^{g/2}.$$

□

Corollary 4.2.1.1 (Hasse-Weil Bound)**.** *Let C be as above, then*

$$|q + 1 - \#C(\mathbb{F}_q)| \leq 2gq^{1/2}.$$

4.3 Applying the Lefschetz Fixed Point Formula

We can apply Lefschetz fixed point formula to compute the zeta function of C.

Lemma 4.3.1. *We have*

$$q^s + 1 - \#C(\mathbb{F}_{q^s}) = \mathrm{Tr}\left((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^-\right).$$

Proof. Let $\tilde{C}'$ denote the quotient of C' under the hyperelliptic involution. Apply the Lefschetz fixed point formula to C' and $\tilde{C}'$, we have the following equations

$$\#C'(\mathbb{F}_{q^s}) = \mathrm{Tr}((qF_*^{-1})^s, H^0(\bar{A}/\mathbb{Q}_q)) - \mathrm{Tr}(q^i F_*^{-i}, H^1(\bar{A}/\mathbb{Q}_q)), \tag{4.3}$$

$$\#\tilde{C}'(\mathbb{F}_{q^s}) = \mathrm{Tr}((qF_*^{-1})^s, H^0(\bar{A}/\mathbb{Q}_q)^+) - \mathrm{Tr}(q^i F_*^{-i}, H^1(\bar{A}/\mathbb{Q}_q)^+). \tag{4.4}$$

$$\begin{aligned}
&\#C(\mathbb{F}_{q^s}) - \{\text{zeros of } y \text{ over } \mathbb{F}_{q^s}\} \\
&= \#C'(\mathbb{F}_{q^s}) \\
&= \mathrm{Tr}((qF_*^{-1})^s, H^0(\bar{A}/\mathbb{Q}_q)) - \mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)) \text{ by (4.3)} \\
&= \mathrm{Tr}((qF_*^{-1})^s, H^0(\bar{A}/\mathbb{Q}_q)) - \mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^+) - \mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^-) \\
&\qquad \text{since } H^1(\bar{A}/\mathbb{Q}_q) = H^1(\bar{A}/\mathbb{Q}_q)^- \oplus H^1(\bar{A}/\mathbb{Q}_q)^+ \\
&= q^s - \mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^+) - \mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^-) \\
&= \mathrm{Tr}((qF_*^{-1})^s, H^0(\bar{A}/\mathbb{Q}_q)^+) - \mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^+) - \mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^-) \\
&= \#\tilde{C}'(\mathbb{F}_{q^s}) - \mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^-) \text{ by equation 4.4} \\
&= q^s + 1 - \{\text{zeros of } y \text{ over } \mathbb{F}_{q^s}\} - \mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^-).
\end{aligned}$$

□

We now have

$$\mathrm{Tr}((qF_*^{-1})^s, H^1(\bar{A}/\mathbb{Q}_q)^-) = \sum_{j=1}^{2g} \alpha_j^s,$$

for all $s > 0$, so α_j are eigenvalues of qF_*^{-1} in $H^1(\bar{A}/\mathbb{Q}_q)^-$ and q/α_j are eigenvalues of F_*. Since $\alpha_j \alpha_{g+j} = q$, the α_j are eigenvalues of F_* and are the roots of the characteristic polynomial of the matrix of F_*^{-1} on $H^1(\bar{A}/\mathbb{Q}_q)^-$. If m is the the matrix of the Frobenius F_* on $H^1(\bar{A}/\mathbb{Q}_q)^-$ with respect to a basis, the characteristic polynomial $\chi(T)$ of m has roots $\alpha_0, \ldots, \alpha_{2g}$. Then the reciprocal polynomial $P(T) = T^{2g}\chi(1/T)$ is the required polynomial. By Theorem 4.2.1, we can bound the coefficients of the characteristic polynomial. If $\chi(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_{2g}$, then $|a_i|_\infty \leq 2^{2g} q^{g/2}$ for $i = 1, \ldots, g$, so a_i only have to be computed to finite p-adic digits.

4.4 Lifting the Frobenius

We can define explicitly a lift of the q-Frobenius F_* on $H^1(\bar{A}/\mathbb{Q}_q)^-$.

Lift the p-Frobenius to an endormorphism σ on $A^\dagger$. Define σ as the canonical Witt vector Frobenius on $\mathbb{Z}_q$, i.e. $(a_0, a_1, \ldots) \mapsto (a_0^p, a_1^p, \ldots)$, where $a_i \in \mathbb{F}_q$. Extend this to $\mathbb{Z}_q[x]$ by sending $x \mapsto x^p$, and then to satisfy $(y^\sigma)^2 = (y^2)^\sigma = Q(x)^\sigma = Q(x)^\sigma (y^2/Q(x))^p = y^{2p} Q(x)^\sigma / Q(x)^p$, send

$$y \mapsto y^p \left(\frac{Q(x)^\sigma}{Q(x)^p}\right)^{1/2} = y^p \left(1 + \frac{Q(x)^\sigma - Q(x)^p}{Q(x)^p}\right)^{1/2},$$

$$y^{-1} \mapsto (y^\sigma)^{-1} = y^{-p} \left(1 + \frac{Q(x)^\sigma - Q(x)^p}{Q(x)^p}\right)^{-1/2} = \sum_{k=0}^{\infty} \binom{-1/2}{k} \frac{(Q(x)^\sigma - Q(x)^p)^k}{y^{p(2k+1)}}.$$

Further extend to $H^1(\bar{A}/\mathbb{Q}_q)^-$ by setting $dx \mapsto p x^{p-1} dx$. Define $F_* = \sigma^{\log_p q}$, then F_* is a lift of the q-power Frobenius.

Note that a basis for $H^1(\bar{A}/\mathbb{Q}_q)^-$ is found in Lemma 4.1.3. We will compute explicitly the action of F_* with respect to this basis.

4.5 Precision

We will find $(x^i dx/y)^\sigma$, then reduce using relations (4.1) and (4.2) to obtain a cohomologous expression as a linear combination of the basis $\{x^i dx/y \mid i = 0, \ldots, 2g-1\}$. The reduction process is equivalent to repeatedly subtracting suitable multiples of $d(x^i y^{2j+1})$, $i \leq 0$, $j \in \mathbb{Z}$. Precision is lost when some division by power of p is carried out in the reduction algorithm. We will need to measure the loss of precision, to find the number of p-adic digits needed to begin the algorithm.

Lemma 4.5.1. *Let $A(x) \in \mathbb{Z}_q[x]$ be a polynomial of degree at most $2g$. For some $m > 0$, consider the reduction of $\omega := A(x)\frac{dx}{y^{2m+1}}$ by (4.1),*

$$\omega := A(x)\frac{dx}{y^{2m+1}} = B(x)\frac{dx}{y} + df,$$

for some $B(x) \in \mathbb{Q}_q[x]$ with $\deg B \leq 2g-1$ and $f = \sum_{k=-1}^{m-1} \frac{F_k(x)}{y^{2k+1}}$ where each $\deg F_k \leq 2g$, then $p^{\lfloor \log_p(2m-1) \rfloor} B(x) \in \mathbb{Z}_q[x]$.

Proof. Let $r_0, \ldots, r_{2g}$ be the roots of Q in the splitting field of Q, and let $T_0 = (r_0, 0), \ldots, T_{2g} = (r_{2g}, 0)$ be the corresponding points on the curve $y^2 = Q(x)$, then f has poles at $T_0, \ldots, T_{2g}$ and possibly at infinity. We have $r_i \in \mathbb{Z}_{q^r}$ for some r. Let R_i be the completion of the local ring of $\mathbb{Z}_{q^r}[x, y]/(y^2 - Q(x))$ at T_i, i.e. the localisation of $\mathbb{Z}_{q^r}[x, y]/(y^2 - Q(x))$ with respect to the ideal $\{f \in \mathbb{Z}_{q^r}[x, y] \mid f(r_i, 0) = 0\}$, then the maximal ideal of R_i is generated by y. x can be written as a power series in y with integral coefficients, so $R_i = \mathbb{Z}_{q^r}[[y]]$.

Let $K_i = Qt(R_i)$. The image of df in the module of differentials $D^1(K_i/\mathbb{Z}_{q^r})$ can be written as

$$\sum_{k=-\infty}^{m-1} \frac{a_{ik} dy}{y^{2k+2}},$$

where $a_{ik} \in \mathbb{Z}_{q^r}$ for $k \geq -1$ since they coincide with the corresponding coefficients in the expansion of ω. The map d commutes with the passage to the completed local ring R_i, so the image of f in K_i is

$$\sum_{k=-\infty}^{m-1} \frac{-a_{ik}}{(2k+1)y^{2k+1}}.$$

Now $f - \sum_{k=j+1}^{m-1} \frac{F_k(x)}{y^{2k+1}} = \sum_{k=-1}^{j} \frac{F_k(x)}{y^{2k+1}}$ has a pole of order at most $2j+1$ at each T_i, and its image in K_i is $\frac{F_j(r_i)}{y^{2j+1}} + \ldots$.

Take $n = p^{\lfloor \log_p(2m-1) \rfloor}$, then $na_{ik}/(2k+1)$ is integral for $i = 0, \ldots, 2g$ and $k = -1, 0, \ldots, m-1$. Now $nF_{m-1}(r_i) = -na_{i,m-1}/(2m-1)$ is integral for $i = 0, \ldots, 2g$, and since the r_i are distinct mod p, $nF_{m-1}(x)$ is integral. Apply the same argument to $nf - nF_{m-1}(x)$, $nF_{m-2}(x) = -na_{i,m-2}/(2m-3)$ is integral and so on. Hence nf is integral so $nB(x)$ is integral. □

Lemma 4.5.2. *Let $A(x) \in \mathbb{Z}_q[x]$ of degree at most $2g$. For some $m \geq 0$, consider the reduction by (4.2),*

$$\omega := A(x)y^{2m}\frac{dx}{y} = B(x)\frac{dx}{y} + df,$$

for some $B(x) \in \mathbb{Q}_q[x]$ with $\deg B \leq 2g-1$ and $f = Cy^{2m+1} + \sum_{k=0}^{m-1} F_k(x)y^{2k+1}$ where $C \in \mathbb{Q}_q$ and each $\deg F_k \leq 2g$, then $p^{\lfloor \log_p(d(2m+1)) \rfloor} B(x) \in \mathbb{Z}_q[x]$.

Proof. Consider the local ring at infinity. We can apply a birational transformation $(x, y) \mapsto (z, w) = (x^g/y, 1/y)$, then the point at infinity is mapped to $(0, 0)$. x and y can be expressed as power series in z. Let v_∞ denote the valuation at the unique pole ∞ of y, i.e., the order of z in the power series in z, then $v_\infty(x) = -2$, $v_\infty(y) = -d$ since $y^2 = Q(x)$ and $\deg Q = d$. $v_\infty(dx) = -3$, $v_\infty(dx/y) = d-3$, $v_\infty(f) \geq \min\{-d(2m+1), -2(2g) - d(2m-1)\} = -d(2m+1)$ and $v_\infty(B(x)dx/y) \geq -2(2g-1) + (d-3) = -d+1$.

The hyperelliptic involution maps z to $-z$. Since $v_\infty(df) \geq -d(2m+1) - 1$, the image of df is

$$\sum_{k \geq -d(2m+1)-1} a_k z^k dz,$$

where $a_k = 0$ if k is odd. We have $v_\infty(B(x)dx/y) \geq -d+1$, so $a_k \in \mathbb{Z}_{q^r}$ for $k \leq -d$ since they correspond to the coefficients in the expansion of ω. The image of f is

$$\sum_{k \geq -d(2m+1)-1} \frac{a_k z^{k+1}}{k+1}.$$

Take $n = p^{\lfloor \log_p(d(2m+1))\rfloor}$, then $na_k/(k+1) \in \mathbb{Z}_q$ if $k \le -d$. As $v_\infty(x^i y^j)$ are distinct and $\le -d$ for $0 \le i < d$ and $j > 0$, f is integral. □

Since we only need to find $a_1, \dots, a_g$ and $|a_i|_\infty \le 2^{2g} q^{g/2}$ for $i = 1, \dots, g$, it suffices to compute the action of F_* on a suitable basis of $H^1(\bar{A}/\mathbb{Q}_q)^-$ modulo p^N for some N such that $p^N \ge 2\left(2^{2g} q^{g/2}\right)$, i.e. $N \ge gn/2 + (2g+1)\log_p 2$, where $n = \log_p q$.

Let $pE(x) := Q(x)^\sigma - Q(x)^p$ and $d = \deg Q = 2g+1$. The action of the p-Frobenius σ on differentials $x^i dx/y$ for $i = 0, \dots, 2g-1$,

$$\left(\frac{x^i dx}{y}\right)^\sigma = \frac{p x^{ip+p-1} dx}{y^p}\left(1 + \frac{pE(x)}{y^{2p}}\right)^{-1/2} = \sum_{k=0}^{\infty} \binom{-1/2}{k} \frac{p^{k+1} x^{ip+p-1} E(x)^k dx}{y^{p(2k+1)}}.$$

Note that $\deg E \le pd - 1$.

For fixed i and k, write

$$\binom{-1/2}{k} \frac{x^{ip+p-1} E(x)^k dx}{y^{p(2k+1)}} := \sum_{m=c}^{(p(2k+1)-1)/2} A_m(x) \frac{dx}{y^{2m+1}},$$

where $\deg A_m \le 2g$ and

$$c := \frac{p(2k+1)-1}{2} - \left\lfloor \frac{ip+p-1+k\deg E}{d} \right\rfloor.$$

Since

$$\begin{aligned} \frac{ip+p-1+k\deg E}{d} &\le \frac{(d-2)p + p - 1 + k(pd-1)}{d} \\ &= \left(1 - \frac{1}{d}\right)p - \frac{1}{d} + k\left(p - \frac{1}{d}\right) < (k+1)p, \end{aligned}$$

we have

$$c \ge \frac{p(2k+1)-1}{2} - ((k+1)p - 1) = \frac{p(2k+1)+1}{2} - (k+1)p = \frac{1}{2}(1-p).$$

The reduction of $m > 0$ terms by (4.1) is integral upon multiplication by $p^{\lfloor \log_p(p(2k+1)-2)\rfloor}$ by Lemma 4.5.1. Since

$$(-2c+1)\,d < \left(-2\left(\frac{1}{2}(1-p)\right) + 1\right) d = pd,$$

the reduction of $m < 0$ terms by (4.2) is integral upon multiplication by $p^{\lfloor \log_p(pd)\rfloor}$ by Lemma 4.5.2.

We have the reduction

$$\binom{-1/2}{k} \frac{x^{ip+p-1} E(x)^k dx}{y^{p(2k+1)}} \equiv B(x)\frac{dx}{y},$$

where $\deg B(x) \le 2g - 1$.

The reduction of $\binom{-1/2}{k} \frac{p^{k+1} x^{ip+p-1} E(x)^k dx}{y^{p(2k+1)}}$ is divisible by $p^{k+1-\max\{\lfloor \log_p(p(2k+1)-2)\rfloor, \lfloor \log_p(pd)\rfloor\}}$. We only have to consider terms up $k = M-1$, where M is the smallest integer such that $M -$

$\max\{\lfloor \log_p(2M+1-2/p)\rfloor, \lfloor \log_p d\rfloor\} \geq N$ and the other terms will not contribute to the reduction modulo p^N. Note that $\lfloor \log_p(2M+1-2/p)\rfloor = \lfloor \log_p(2M-1)\rfloor$ since p is odd, so M is the smallest integer such that $M - \max\{\lfloor \log_p(2M-1)\rfloor, \lfloor \log_p d\rfloor\} \geq N$.

We have $\min\{k - \max\{\lfloor \log_p(2k-1)\rfloor, \lfloor \log_p d\rfloor\} \mid k \geq 0\} = -\lfloor \log_p d\rfloor$ so the matrix of σ with respect to the $\mathbb{Z}_q$-basis $\{x^i dx/y \mid i = 0, \ldots, 2g-1\}$ does not necessarily have coefficients in $\mathbb{Z}_q$. We will need extra precision of $\lfloor \log_p(2g-1)\rfloor$ by [Edi03].

Hence, to get N significant digits after reduction, we need to start with precision

$$\begin{aligned} N_1 &= N + \max\{\lfloor \log_p(2M-1-2/p)\rfloor, \lfloor \log_p d\rfloor\} + 1 + \lfloor \log_p(2g-1)\rfloor \\ &= N + \max\{\lfloor \log_p(2M-3)\rfloor, \lfloor \log_p d\rfloor\} + 1 + \lfloor \log_p(2g-1)\rfloor. \end{aligned}$$

Remark 9. *Alternatively, we could take a basis on which the matrix has integral entries. The existence of such a basis is shown in [Edi03]. Namely, let $z = x^g/y$, any basis of the submodule of the $\mathbb{Z}_q$-span of $\{x^i dx/y \mid i = 0, \ldots, 2g-1\}$ whose z-adic expansions can be integrated over $\mathbb{Z}_q$ gives an integral matrix.*

Remark 10. $\min\{k - \max\{\lfloor \log_p(2k-1)\rfloor, \lfloor \log_p d\rfloor\} \mid k \geq 0\} = -\lfloor \log_p d\rfloor = 0$ *if $p > d$ so the matrix is always integral if $p > d$. It was shown in [Har12] that if $p \leq d$, using an alternative basis $\{x^i dx/y^3 \mid i = 0, \ldots, 2g-1\}$ of $H^1(\bar{A}/\mathbb{Q}_q)^-$ instead will guarantee an integral matrix.*

Remark 11. *For some small q and d, namely, at least for $q \leq 17$ and $d \leq 25$,* $\max\{\lfloor \log_p(2M-3)\rfloor, \lfloor \log_p d\rfloor\} = \lfloor \log_p(2M-3)\rfloor$. *Specifically, when $q \leq 13$, and if $2M-3 < d$, i.e. $M \leq g+1$,*

$$M - \max\{\lfloor \log_p(2M-1)\rfloor, \lfloor \log_p d\rfloor\} \geq N = \lceil gn/2 + (2g+1)\log_p 2\rceil,$$

$$\begin{aligned} g+1 \geq M &\geq \max\{\lfloor \log_p(2M-1)\rfloor, \lfloor \log_p d\rfloor\} + \lceil gn/2 + (2g+1)\log_p 2\rceil \\ &\geq \lfloor \log_p(\max\{2M-1, 2g+1\}\rfloor) + \lceil g/2 + (2g+1)\log_p 2\rceil \\ &= \lfloor \log_p(2g+1)\rfloor + \lceil g/2 + (2g+1)\log_{13} 2\rceil \quad \textit{since } 2M-1 \leq 2g+1 \\ &\geq \lfloor \log_p(2g+1)\rfloor + g + 1 \quad \textit{since } p \leq 13, \end{aligned}$$

which is only possible if $\log_p(2g+1) < 1$. By checking the remaining cases, we see that in fact $2M-3 \geq d$ always holds for $q \leq 13$ so the formula giving N_1 can be simplified as $N_1 = N + \lfloor \log_p(2M-3)\rfloor + 1 + \lfloor \log_p(2g-1)\rfloor$. The function `adjusted_prec(p, prec)` *in Sage uses the formula $N_1 = N + \lfloor \log_p(2M-3)\rfloor + 1$, which should hold when $2g-1 \leq q = p \leq 13$.*

Remark 12. *If we start with a curve $C : y^2 = Q(x)$ over $\mathbb{Q}$, we have to make sure it has good reduction modulo p, i.e. its reduction $\bar{Q}$ has no repeated roots over $\mathbb{F}_p$ so that $y^2 = \bar{Q}(x)$ defines a smooth curve. This can be done by checking the p does not divide the discriminant of Q.*

Remark 13. *There were problems in the original precision estimate in [Ked01], which were pointed out by Edixhoven and corrections were made in the corresponding errata. The corrections were explained in [Edi03] but the formula stated for N_1 was inaccurate. For example, we consider the elliptic curve $y^2 = x^3 + x + 1$ with prime $p = 5$. We need to obtain the matrix modulo 5^2. The formula in [Edi03] would give $N_1 = 2$. If we carry out the computation with a precision of 2 digits, we would obtain the matrix*

$$\begin{pmatrix} 15 & 18 \\ 0 & 22 \end{pmatrix} \mod 5^2.$$

However, if we compute with a precision of 3 *digits, the resulting matrix would be*

$$\begin{pmatrix} 0 & 18 \\ 15 & 22 \end{pmatrix} \mod 5^2.$$

This shows that it is not sufficient to use 2 *digits in the computation. This example is explained in Section 4.7. Therefore, instead of restating the formulae in [Edi03], the formulae here were deduced following the idea in [Edi03].*

4.6 Kedlaya's Algorithm

4.6.1 Initialisation

Let $N := \lceil gn/2 + (2g+1)\log_p 2 \rceil$; this is the precision required to recover the characteristic polynomial of Frobenius. Let M be the smallest integer such that

$$M - \max\{\lfloor \log_p(2M-1) \rfloor, \lfloor \log_p d \rfloor\} \geq N,$$

which is the number of terms to be computed in the expansion of $(x^i dx/y)^\sigma$. Then

$$N_1 = N + \max\{\lfloor \log_p(2M-3) \rfloor, \lfloor \log_p d \rfloor\} + 1 + \lfloor \log_p(2g-1) \rfloor$$

is the precision to begin as required by the reduction algorithm.

4.6.2 Computing the Frobenius on Differentials

Compute the action of the Frobenius on $H^1(\bar{A}/\mathbb{Q}_q)^-$. Compute the reduction of $(x^i dx/y)^\sigma$ for $i = 0, \ldots, 2g-1$ up to modulo p^{N_1}, i.e. with precision of N_1 digits.

For each fixed i,

$$\left(\frac{x^i dx}{y}\right)^\sigma = \sum_{k=0}^{M-1} \binom{-1/2}{k} \frac{p^{k+1} x^{ip+p-1} E(x)^k dx}{y^{p(2k+1)}} + \cdots = \sum_{j=0}^{(p(2M-1)-1)/2} \frac{F_j(x) dx}{y^{2j+1}} \mod p^{N_1}$$

where F_j are polynomials and $\deg F_j \leq 2g$ for $j \geq 1$.

Remark 14. *In practice, to avoid any loss in precision during the reduction, the sum is first coerced into an expression over* $\mathbb{Z}$*, then the reduction is carried out over* $\mathbb{Q}$*. There is no need to keep track of the precision during the reduction, since we know that the expression after the reduction will be correct modulo* p^N *by the precision estimates.*

Let $K := (p(2M-1)-1)/2$. Set $S_K(x) = F_K(x)$ and compute a series of polynomials $S_k(x)$ inductively for $k = K-1, K-2, \ldots, 0$. Given $S_{k+1}(x)$, find polynomials A_{k+1} and B_{k+1} such that $A_{k+1}Q + B_{k+1}Q' = S_{k+1}$, then set $S_k(x) = F_k(x) + A_{k+1}(x) + 2B'_{k+1}(x)/(2k+1)$. Note that $2B'_{k+1}/(2k+1)$ denotes any polynomial over $\mathbb{Z}_q/(p^M)$ which when multiplied by $2k+1$ gives $2B'_{k+1}$. By the reduction relation (4.1),

$$\frac{S_k(x)dx}{y^{2k+1}} = \left(F_k(x) + A_{k+1}(x) + \frac{2B'_{k+1}(x)}{2k+1}\right)\frac{dx}{y^{2k+1}} \equiv \frac{F_k(x)dx}{y^{2k+1}} + \frac{S_{k+1}(x)dx}{y^{2k+3}}$$

$$\sum_{j=0}^{K} \frac{F_j(x)dx}{y^{2j+1}} \equiv \frac{S_K(x)dx}{y^{2K+1}} + \sum_{j=0}^{K-1} \left(\frac{S_j(x)dx}{y^{2j+1}} - \frac{S_{j+1}(x)dx}{y^{2j+3}} \right) = \frac{S_0(x)dx}{y}.$$

$(x^i dx/y)^\sigma$ can be reduced to $(S_0(x))dx/y$.

By construction, F_0 can have degree up to $2pg-1$ so S_0 can have degree up to $2pg-1$. Reduce S_0 using the relation (4.2) $x^{k-1}Q'(x)+2(k-1)x^{k-2}Q(x)$ for $k = \deg S_0 - 2g + 1, \deg S_0 - 2g, \ldots, 1$, obtaining $G(x)$ with degree $\leq 2g$. Then $(x^i dx/y)^\sigma$ is cohomologous to $G(x)dx/y \mod p^N$.

4.6.3 Computing the Characteristic Polynomial

We have $(x^i dx/y)^\sigma$ reduced in the form $G_i(x)dx/y$ where $\deg G_i \leq 2g-1$ for $i = 0, \ldots, 2g-1$. Write $G_j(x)$ in the form $\sum_{i=0}^{2g-1} a_{ij}x^i$, each a_{ij} is computed up to modulo p^N. Extract the matrix $m := \{a_{ij}\}_{i,j=0}^{2g-1}$. m approximates the action of σ on $H^1(\bar{A}/\mathbb{Z}_q)^-$. Compute $m' = m^n$. Determine the characteristic polynomial of m', $\det(T \cdot id - m') = T^{2g} + c_1 T^{2g-1} + \cdots + c_{2g} \in \mathbb{Z}_q[T]$.

Now we recover the characteristic polynomial of the Frobenius from the first g coefficients. For $1 \leq i \leq g$, let a_i be the unique integer with $|a_i| \leq 2^{2g} q^{g/2}$ such that $a_i \equiv c_i \mod p^N$. For $g < i \leq 2g$, let $a_i := q^{i-g} a_{2g-i}$. Then the characteristic polynomial is $\chi(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_{2g}$ and the numerator of the zeta function is the reciprocal polynomial $P(T) = T^{2g}\chi(1/T)$.

4.7 Explicit Example

Let us apply the algorithm to an example.

Let $Q(x) := x^3 + x + 1$ and consider the elliptic curve $C : y^2 = Q(x)$ and prime $p = 5$. Q has discriminant -31, which is not divisible by 5, so it has no repeated roots modulo 5, i.e. C has good reduction at 5.

C has genus $g = 1$, the precision required to recover the characteristic polynomial of the Frobenius is $N = 2$ and the number of terms to be considered in the series expansion of $(x^i dx/y)^\sigma$ is $M = 3$. $N_1 = 3$ is the precision required for the computation. See Appendix for the step-by-step implementation in Sage.

We have

$$\left(\frac{dx}{y}\right)^\sigma = \Big(\frac{25x+50}{y^{15}} + \frac{75x^2+100x+25}{y^{13}} + \frac{50x^2+50x+100}{y^{11}} + \frac{75x+50}{y^9} + \frac{50x^2+50x}{y^7} + \frac{70x^2+70x+25}{y^5} + \frac{5x}{y^3}\Big)dx \mod 5^3,$$

$$\left(\frac{xdx}{y}\right)^\sigma = \Big(\frac{100x^2+100x+75}{y^{15}} + \frac{25x^2+50x+75}{y^{13}} + \frac{50x^2+100x+100}{y^{11}} + \frac{25x^2+75x+75}{y^9} + \frac{75x^2+100}{y^7} + \frac{85x^2+90x+50}{y^5} + \frac{15x^2+30x+85}{y^3} + \frac{5x^3+65x+65}{y}\Big)dx \mod 5^3.$$

First consider the reduction of $(dx/y)^\sigma$. Let F_k be the polynomial in the term $F_k(x)dx/y^{2k+1}$, then compute the sequence S_k for $k = 7, 6, \ldots, 0$.

Set $S_7(x) := F_7(x) = 25x + 50$, and find $S_k(x)$ for each $k = 6, 5, \ldots, 0$. Find polynomials A_{k+1}, B_{k+1} such that $A_{k+1}Q + B_{k+1}Q' = S_{k+1}$ and set $S_k(x) := F_k + A_{k+1} + 2B'_{k+1}/(2k+1)$.

k	F_k	S_k	A_k	B_k	mod
7	$25x+50$	$25x+50$	$25x$	$75x^2+50$	5^3
6	$75x^2+100x+25$	$75x^2+100x+25$	$75x+100$	$100x^2+50x+50$	5^3
5	$50x^2+50x+100$	$50x^2+25x+50$	$75x+50$	$100x^2+25x$	5^3
4	$75x+50$	50	$100x+100$	$50x^2+50x+75$	5^3
3	$50x^2+50x$	$50x^2+25$	$100x+100$	$50x^2+50x+50$	5^3
2	$70x^2+70x+25$	$70x^2+10x+20$	$5x+20$	$15x^2+10x$	5^2
1	$5x$	$5x+10$	$5x$	$15x^2+10$	5^2
0	0	$15x$			5^2

We have

$$\left(\frac{dx}{y}\right)^{\sigma} \equiv 15x\frac{dx}{y} \mod 5^2.$$

Now reduce $(xdx/y)^{\sigma}$.

k	F_k	S_k	A_k	B_k	mod
7	$100x^2+100x+75$	$100x^2+100x+75$	$75x+100$	$100x^2+50x+100$	5^3
6	$25x^2+50x+75$	$25x^2+50x$	75	$100x+50$	5^3
5	$50x^2+100x+100$	$50x^2+100x$	25	$75x+100$	5^3
4	$25x^2+75x+75$	$25x^2+75x+75$	$75x$	$100x^2+75$	5^3
3	$75x^2+100$	$75x^2+25x+100$	$75x+50$	$100x^2+25x+50$	5^3
2	$85x^2+90x+50$	$85x^2+20x+10$	$20x$	$10x^2+10$	5^2
1	$15x^2+30x+85$	$15x^2+5x+10$	$20x+15$	$10x^2+20x+20$	5^2
0	$5x^3+65x+65$	$5x^3+20$			5^2

and

$$\left(\frac{xdx}{y}\right)^{\sigma} \equiv (5x^3+20)\frac{dx}{y} \mod 5^3.$$

We still have to reduce the term $5x^3dx/y$ in $(xdx/y)^{\sigma}$.

The relation $d(2xy) = (xQ'(x)+2Q)dx/y$ gives $(5x^3+3x+2)dx/y \equiv 0 \mod 5^3$. Subtracting from $(5x^3+20)dx/y$, we get

$$\left(\frac{xdx}{y}\right)^{\sigma} \equiv (22x+18)\frac{dx}{y} \mod 5^2.$$

We obtain the matrix of the Frobenius with respect to the basis $\{dx/y, xdx/y\}$:

$$m = \begin{pmatrix} 0 & 18 \\ 15 & 22 \end{pmatrix} \mod 5^2.$$

The characteristic polynomial of the matrix is

$$\chi(t) = t^2+3t+5 \mod 5^2.$$

The coefficients of the polynomial in the numerator of the zeta function are bounded by

$$2^{2g}p^{g/2} = 4\times 5^{1/2} < 9,$$

so we do not have to adjust by multiples of 5^2. We have

$$Z(C/\mathbb{F}_5;T) = \frac{5T^2+3T+1}{(1-T)(1-5T)}.$$

Chapter 5

Counting Points in Average Polynomial Time

To gather data more efficiently for the generalised Sato-Tate conjecture for abelian varieties, which relates to the distributions of the numerator of the zeta function of curves modulo primes, modifications to Kedlaya's algorithm can be helpful. We would like to compute the matrix of Frobenius more quickly for a fixed curve and large primes p.

Harvey presented an optimisation of Kedlaya's algorithm, which is more efficient for fixed g and large p in [Har07]. In [Har14], Harvey further developed an algorithm to compute the zeta function simultaneously for all primes $p < N$ given Q and a fixed integer N, in average polynomial time. We will present this algorithm here. Computations were done using this algorithm by Harvey and Sutherland [HS14], producing substantial results.

5.1 Setup

We begin with a hyperelliptic curve $C : y^2 = Q(x)$ over $\mathbb{Q}$. Take C' by removing the point at infinity and the Weierstrass points. The coordinate ring is $A = \mathbb{Q}[x, y, y^{-1}]/(y^2 - Q(x))$. Let $\Omega := D^1(A)$, Ω^- the negative eigenspace under the hyperelliptic involution. We will keep track of p by denoting $A_p = \mathbb{Z}_p[x, y, y^{-1}]/(y^2 - Q(x))$, $A_p^\dagger = \mathbb{Z}_p\langle x, y, y^{-1}\rangle^\dagger/(y^2 - Q(x))$, $\Omega_p := D^1(A_p^\dagger)$ and Ω_p^- the negative eigenspace. There is a natural map $\Omega^- \to \Omega_p^-$. σ_p is the lift of the p-Frobenius on Ω_p^-.

In Kedlaya's algorithm, we compute the action of σ_p in $\Omega_p^-/d(A_p^\dagger)$ with respect to the basis $\{x^i dx/y \mid i = 0, \ldots, 2g-1\}$. Here, we use the same basis, but we view $\sigma_p(x^i dx/y)$ as elements in Ω^- by truncating the series expansion of $\sigma_p(x^i dx/y)$, since we only require finite p-adic precision. Then the reduction is done in $\Omega^-/d(A)$.

A different series expression is considered so that the number of terms does not depend on p.

Lemma 5.1.1. *Let $\mu \geq 1$ and assume that $p > (2\mu - 1)(2g + 1)$. Let $C_{j,r} \in \mathbb{Z}$ such that $Q(x)^j = \sum_{r=0}^{(2g+1)j} C_{j,r} x^r$. For $0 \leq j < \mu$, let*

$$\alpha_j = \sum_{k=j}^{\mu-1} (-1)^{j+k} \binom{-1/2}{k} \binom{k}{j} \in \mathbb{Z}\left[\frac{1}{2}\right].$$

For $a, b \leq 1$, with b odd, let $U_p^{a,b}$ denote the reduction of $x^{pa-1}y^{-pb+1}dx/y$ in Ω^-. Then for $0 \leq i < 2g$,

$$\sigma_p\left(\frac{x^i dx}{y}\right) \equiv \sum_{j=0}^{\mu-1} \sum_{r=0}^{(2g+1)j} p\alpha_j C_{j,r} U_p^{i+r+1,2j+1} \mod p^\mu \text{ in } \Omega_p^-.$$

Proof. Let $pE(x) := Q(x)^\sigma - Q(x)^p$. Recall

$$\sigma_p\left(\frac{x^i dx}{y}\right) = \sum_{k=0}^{M-1} \binom{-1/2}{k} \frac{p^{k+1} x^{ip+p-1} E(x)^k dx}{y^{p(2k+1)}} \mod p^{N_1},$$

where M is the smallest integer such that $M - \lfloor \log_p(2M-1) \rfloor \geq \mu$ and $N_1 = \mu + \lfloor \log_p(2M-3) \rfloor + 1$. We have $M = \mu$ and $N_1 = \mu + 1$, so

$$\sigma_p\left(\frac{x^i dx}{y}\right) \equiv \sum_{k=0}^{\mu-1} \binom{-1/2}{k} \frac{p^{k+1} x^{ip+p-1} E(x)^k dx}{y^{p(2k+1)}} \mod p^\mu.$$

We compute

$$\begin{aligned}
&\sum_{k=0}^{\mu-1} \binom{-1/2}{k} \frac{p x^{ip+p-1} (Q(x)^\sigma - y^{2p})^k dx}{y^{p(2k+1)}} \\
&= \sum_{k=0}^{\mu-1} \binom{-1/2}{k} \frac{p x^{ip+p-1}}{y^{p(2k+1)}} \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} (Q(x)^j)^\sigma y^{2p(k-j)} dx \\
&= \sum_{k=0}^{\mu-1} \binom{-1/2}{k} \frac{p x^{ip+p-1}}{y^{p(2k+1)}} \sum_{j=0}^{k} (-1)^{j+k} \binom{k}{j} \left(\sum_{r=0}^{(2g+1)j} C_{j,r} x^r \right)^\sigma y^{2p(k-j)} dx \\
&= \sum_{k=0}^{\mu-1} \binom{-1/2}{k} p x^{ip+p-1} \sum_{j=0}^{k} \sum_{r=0}^{(2g+1)j} (-1)^{j+k} \binom{k}{j} C_{j,r} x^{rp} y^{-p-2pj} dx \\
&= \sum_{k=0}^{\mu-1} \sum_{j=0}^{k} \sum_{r=0}^{(2g+1)j} p(-1)^{j+k} \binom{-1/2}{k} \binom{k}{j} C_{j,r} x^{p(r+i+1)-1} y^{-p(2j+1)} dx \\
&= \sum_{j=0}^{\mu-1} \sum_{r=0}^{(2g+1)j} \sum_{k=j}^{\mu-1} p(-1)^{j+k} \binom{-1/2}{k} \binom{k}{j} C_{j,r} U_p^{i+r+1,2j+1}.
\end{aligned}$$

□

Lemma 5.1.2. *Let $F, G \in \mathbb{Z}[x]$ be nonzero and coprime. Let $m = \deg F$, $n = \deg G$. Let $\delta \in \mathbb{Z}$ be the resultant of F and G so $\delta \neq 0$. Then there exist polynomials $R_i, S_i \in \mathbb{Z}[x]$, for $0 \leq i < m + n$ with $FR_i + GS_i = \delta x^i$, $\deg R_i < n$ and $\deg S_i < m$.*

Proof. Define a $(m+n)\times(m+n)$ matrix with entries of coefficients of $F(x)$ and $G(x)$

$$T := \begin{pmatrix} F_0 & & & G_0 & & \\ F_1 & \ddots & & G_1 & \ddots & \\ \vdots & \ddots & F_0 & \vdots & \ddots & G_0 \\ F_m & & F_1 & G_n & & G_1 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & F_{2g+1} & & & G_n \end{pmatrix}.$$

T can be viewed as a map in the space of polynomials $\mathbb{P}_n \times \mathbb{P}_m \to \mathbb{P}_{m+n}$ given by $(R,S) \mapsto FR+GS$. Since $\delta = \det T$ by definition, applying Cramer's rule will give us the coefficients of the required polynomials R_i and S_i. □

5.2 Reduction

We will take δ as the resultant of $Q(x)$ and $Q'(x)$, which is also the discriminant of $Q(x)$.

For $s \geq 0$ and $t \in \mathbb{Z}$, define a collection of $\mathbb{Q}$-subspaces, denote

$$W_{s,t} := \{F(x)x^s y^{-2t}dx/y \mid F \in \mathbb{Q}[x], \quad \deg F \leq 2g\} \subseteq \Omega^-,$$

and

$$\begin{aligned} W_{-1,t} :&= \{F(x)x^{-1}y^{-2t}dx/y \mid F \in \mathbb{Q}[x], \quad \deg F \leq 2g, \quad F(0) \neq 0\} \\ &= \{F(x)y^{-2t}dx/y \mid F \in \mathbb{Q}[x], \quad \deg F \leq 2g-1\} \subseteq \Omega^-. \end{aligned}$$

Note that $W_{-1,0}$ is the space spanned by $\{x^i dx/y \mid i = 0,\ldots,2g-1\}$. The treatment here differs from Kedlaya's algorithm. The reduction in cohomology is represented by matrices with respect the natural basis of $W_{s,t}$. Linear maps are applied repeatedly to reduce each $x^{p(i+r+1)-1}y^{-p(2j+1)+1}dx/y \in W_{p(i+r+1)-1,(p(2j+1)-1)/2}$ in the expression of $\sigma_p(x^i dx/y)$ to

$$U_p^{i+r+1,2j+1} \in W_{-1,0}.$$

A fast matrix multiplying algorithm can be adapted the to speed up the computation.

Lemma 5.2.1 (horizontal reduction)**.** *Let $s \geq 0$, $t \in \mathbb{Z}$ and let $D_H(s,t) = (2g+1)(2t-1)-2s \in \mathbb{Z}[s,t]$, then $D_H(s,t) \neq 0$. There exists a matrix $M_H \in GL_{2g+1}(\mathbb{Z}[s,t])$ such that the map $D_H(s,t)^{-1}M_H(s,t)$ reduce $w \in W_{s,t}$ to a cohomologous differential in $W_{s-1,t}$ and the entries of M_H have degree at most 1.*

Proof. We have

$$d(x^s y^{-2t+1}) = sx^{s-1}y^{-2t+1}dx - (2t-1)x^s y^{-2t}dy = \left(sQ(x) - \frac{2t-1}{2}xQ'(x)\right)x^{s-1}y^{-2t}\frac{dx}{y}.$$

Substitute with $Q(x) = x^{2g+1} + P(x)$, where $P \in \mathbb{Z}[x]$ has degree at most $2g$,

$$x^{s+2g}y^{-2t}\frac{dx}{y} \equiv \frac{2sP(x) - (2t-1)xP'(x)}{D_H(s,t)}x^{s-1}y^{-2t}\frac{dx}{y}.$$

Let $C_i(s,t)$ be the coefficient of x^i in the polynomial $2sP(x) - (2t-1)xP'(x)$, then the required matrix is

$$M_H = \begin{pmatrix} 0 & 0 & \cdots & 0 & C_0 \\ D_H & 0 & & \vdots & C_1 \\ 0 & D_H & \ddots & & C_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & D_H & C_{2g} \end{pmatrix}.$$

□

Lemma 5.2.2 (diagonal reduction)**.** *Let $s \geq 0$, $t \in \mathbb{Z}$ and let $D_D(s,t) = 2t-1 \in \mathbb{Z}[s,t]$. There exists a matrix $M_D \in GL_{2g+1}(\mathbb{Z}[s,t])$ such that the map $\delta^{-1}D_D(T)^{-1}M_D(s,t)$ reduce $w \in W_{s,t}$ to a cohomologous differential in $W_{s-1,t-1}$ and the entries of M_D have degree at most 1.*

Proof. For each $0 \leq i \leq 2g$, there exist $R_i, S_i \in \mathbb{Z}[x]$ with $\deg R_i \geq 2g-1$ and $\deg S_i \geq 2g$, such that

$$\delta x^i = R_i(x)Q(x) + S_i(x)Q'(x).$$

$$\delta x^{s+i}y^{-2t}\frac{dx}{y} = (R_i(x)Q(x) + S_i(x)Q'(x))x^s y^{-2t}\frac{dx}{y} = x^s R_i(x)y^{-2t+2}\frac{dx}{y} + 2x^s S_i(x)y^{-2t}dy.$$

$$\begin{aligned} d(x^s S_i(x)y^{-2t+1}) &= (x^s S_i(x))' y^{-2t+2}\frac{dx}{y} + (-2t+1)x^s S_i(x)y^{-2t}dy \\ &= (x^s S_i'(x) + sx^{s-1}S_i(x))y^{-2t+2}\frac{dx}{y} - (2t-1)x^s S_i(x)y^{-2t}dy \end{aligned}$$

$$\begin{aligned} x^{s+i}y^{-2t}\frac{dx}{y} &= \frac{1}{\delta}(x^s R_i(x)y^{-2t+2}\frac{dx}{y} + 2x^s S_i(x)y^{-2t}dy) \\ &\equiv \frac{1}{\delta}\left(x^s R_i(x)y^{-2t+2}\frac{dx}{y} + \frac{2(x^s S_i'(x) + sx^{s-1}S_i(x))}{2t-1}y^{-2t+2}\frac{dx}{y}\right) \\ &= \frac{(2t-1)xR_i(x) + 2sS_i(x) + 2xS_i'(x)}{(2t-1)\delta}x^{s-1}y^{-2t+2}\frac{dx}{y}. \end{aligned}$$

Let M_D be the matrix such that its $(i+1)$th column consist of coefficients of the polynomial $(2t-1)xR_i(x) + 2sS_i(x) + 2xS_i'(x)$. □

Let c_0 be the constant term of $Q(x)$.

Lemma 5.2.3 (vertical reduction)**.** *Suppose $c_0 \neq 0$. Let $s \geq 0$, $t \in \mathbb{Z}$ and let $D_V(s,t) = 2t-1 \in \mathbb{Z}[t]$. There exists a matrix $M_H \in GL_{2g+1}(\mathbb{Z}[s,t])$ such that $(c_0\delta)D_V(T)^{-1}M_v(s,t) \neq 0$ reduce $w \in W_{s,t}$ to a cohomologous differential in $W_{s,t-1}$ and the entries of M_H have degree at most 1.*

Proof. Let S_i and R_i be as defined in the proof of Lemma 5.2.2. Write $S_i(x) = h_i + xT(x)$, where $h_i \in \mathbb{Z}, T_i \in \mathbb{Z}[x], \deg T_i \leq 2g-1$.

$$\begin{aligned} x^{s+i}y^{-2t}\frac{dx}{y} &\equiv \frac{(2t-1)xR_i(x) + 2sS_i(x) + 2xS_i'(x)}{(2t-1)\delta}x^{s-1}y^{-2t+2}\frac{dx}{y} \\ &= \frac{2h_i sx^{s-1} + x^s((2t-1)R_i(x) + 2sT(x) + 2S_i'(x))}{(2t-1)\delta}y^{-2t+2}\frac{dx}{y}. \end{aligned}$$

Write $Q(x) = c_0 + xP(x)$, where $P \in \mathbb{Z}[x]$ with $\deg P \geq 2g$.

$$\begin{aligned} d(x^s y^{-2t-1}) &= \left(sQ(x) - \frac{2t-3}{2} xQ'(x) \right) x^{s-1} y^{-2t+2} \frac{dx}{y} \\ &= \left(s(c_0 + xP(x)) - \frac{2t-3}{2} xQ'(x) \right) x^{s-1} y^{-2t+2} \frac{dx}{y} \\ &= \left(sc_0 x^{s-1} - \frac{1}{2} \left((2t-3)Q'(x) - 2sP(x) \right) x^s \right) y^{-2t+2} \frac{dx}{y} \end{aligned} .$$

$$2sx^{s-1} y^{-2t+2} \frac{dx}{y} \equiv \frac{(2t-3)Q'(x) - 2sP(x)}{c_0} x^s y^{-2t+2} \frac{dx}{y}.$$

$$\begin{aligned} x^{s+i} y^{-2t} \frac{dx}{y} &\equiv \frac{2h_i s x^{s-1} + x^s \left((2t-1)R_i(x) + 2sT(x) + 2S_i'(x) \right)}{(2t-1)\delta} y^{-2t+2} \frac{dx}{y} \\ &\equiv \frac{h_i((2t-3)Q'(x) - 2sP(x)) + c_0((2t-1)R_i(x) + 2sT(x) + 2S_i'(x))}{(2t-1)\delta c_0} x^s y^{-2t+2} \frac{dx}{y}. \end{aligned}$$

Let M_V be the matrix such that its $(i+1)$th column consist of coefficients of the polynomial $h_i((2t-3)Q'(x) - 2sP(x)) + c_0((2t-1)R_i(x) + 2sT(x) + 2S_i'(x))$. □

We say (a, b) is *admissible* if it satisfies the following conditions:

(1). $a, b \geq 1$ and b is odd;

(2). if $c_0 = 0$, then $b \leq 2a$.

Lemma 5.2.4 (Reduction towards zero)**.** *Let (a, b) be an admissible pair and $r \geq 1$. There exists a matrix $M_r^{a,b} \in GL_{2g+1}(\mathbb{Z})$ and $D_r^{a,b}$ such that the map $(D_r^{a,b})^{-1} M_r^{a,b}$ reduces a differential $\omega \in W_{a(2r+1)-1,(b(2r+1)-1)/2}$ to a cohomologous differential in $W_{a(2r-1)-1,(b(2r-1)-1)/2}$.*

Proof. Let $s = a(2r+1) - 1$ and $t = (b(2r+a) - 1)/2$. If $b \leq 2a$, perform b diagonal reductions followed by $2a - b$ horizontal reductions:

$$\begin{array}{ccccccc} & & & & & & (s,t) \\ & & & & & \swarrow & \\ & & & & (s-1,t-1) & & \\ & & & \swarrow & & & \\ & & \cdots & & & & \\ & \swarrow & & & & & \\ (s-2a,t-b) \leftarrow \ldots \leftarrow & (s-b-1,t-b) & \leftarrow & (s-b,t-b) & & & \end{array}$$

If $b > 2a$, perform $2a$ diagonal reductions followed by $b - 2a$ vertical reductions:

$$\begin{array}{ccccc} & & & & (s,t) \\ & & & \swarrow & \\ & & (s-1,t-1) & & \\ & \swarrow & & & \\ \cdots & & & & \\ \swarrow & & & & \\ (s-2a,t-2a) & & & & \\ \downarrow & & & & \\ (s-2a,t-2a-1) & & & & \\ \downarrow & & & & \\ \vdots & & & & \\ \downarrow & & & & \\ (s-2a,t-b) & & & & \end{array}$$

□

Lemma 5.2.5 (Final reduction)**.** *Let (a, b) be an admissible pair. There exists a matrix $M_0^{a,b} \in GL_{2g+1}(\mathbb{Z})$ and $D_0^{a,b}$ such that the map $(D_0^{a,b})^{-1}M_0^{a,b}$ reduces a differential $\omega \in W_{a-1,(b-1)/2}$ to a cohomologous differential in $W_{-1,0}$.*

Proof. If $b \leq 2a$, perform $(b-1)/2$ diagonal reductions followed by $a-(b-1)/2$ horizontal reductions. If $b > 2a$, perform $(b-1)/2-a$ vertical reductions followed by a diagonal reductions. □

5.3 The Algorithm

We say (a, b) is *p-admissible* if it satisfies the following conditions:

(1). $a, b \geq 1$ and b is odd;

(2). if $p \mid c_0$, then $b \leq 2a$;

(3). $p \nmid \delta$;

(4). $p > (2g+1)b + 2a$.

Note that if (a, b) is p-admissible, it is also admissible.

Let (a, b) be admissible, and let $N \geq 3$, $\nu \geq 1$. We can compute $U_p^{a,b}$ modulo p^ν simultaneously for all $p < N$ such that (a, b) is p-admissible.

Assume N is even, and put $B = N/2$.

Let $M_1^{a,b}, \ldots, M_{B-1}^{a,b}$ and $D_0^{a,b}, \ldots, D_{B-1}^{a,b}$ be as in Lemmas 5.2.4 and 5.2.5. Then the matrix

$$J_p^{a,b} = \left(D_0^{a,b} \ldots D_{(p-1)/2}^{a,b}\right)^{-1} \left(M_0^{a,b} \ldots M_{(p-1)/2}^{a,b}\right)$$

reduces any $\omega \in W_{ap-1,(bp-1)/2}$ to a cohomologous form in $W_{-1,0}$. The coordinates of $U_p^{a,b}$ are given by the first column of $J_p^{a,b}$.

5.3.1 Precision

As before, we need to find the p-adic precision lost in the reduction. We consider the p-adic valuation of $D_0^{a,b} \ldots D_{(p-1)/2}^{a,b}$.

Lemma 5.3.1. *We have $ord_p\left(D_0^{a,b} \ldots D_{(p-1)/2}^{a,b}\right) \leq (b-1)/2 + \max(0, 2a-b)$.*

Proof. The contributions from the vertical and diagonal reduction comes from the factor $2t-1$ for $t = 1, 2, \ldots, (bp-1)/2$, δ and c_0 do not contribute by assumptions. The integers divisible by p are $p, 3p, \ldots, (b-2)p$. Since $p > b$, the contribution is exactly $(b-1)/2$.

Horizontal reduction only happens when $b \leq 2a$. The contributions come from $(2g+1)(2t-1)-2s$ for a sequence of (s, t). As $t \leq (bp-1)/2$ and $s \leq ap-1$ so $|(2g+1)(2t-1)-2s| < p^2$. From Lemma 5.2.4, $s = a(2r+1)-b-1-j$ and $t = (b(2r-1)-1)/2$ for $1 \leq r \leq (p-1)/2$ and $0 \leq j \leq 2a-b$. We have

$$(2g+1)(2t-1)-2s = 2((2g+1)b-2a)r - ((2g+1)(b+2)+2(a-b-1-j)).$$

Since $|(2g+1)b-2a| < p$ is odd, for each j, $(2g+1)(2t-1)-2s$ divisible by p for at most one r. The $2a-b$ possible values of j give contribution of at most $2a-b$. From Lemma 5.2.5, $t=0$ and $0 \le s \le a-1-(b-1)/2$. $|(2g+1)(2t-1)-2s| \le 2g+1+2a < p$ so they do not contribute.

Hence $\mathrm{ord}_p \left(D_0^{a,b} \dots D_{(p-1)/2}\right)^{a,b} \le (b-1)/2 + \max(0, 2a-b)$. □

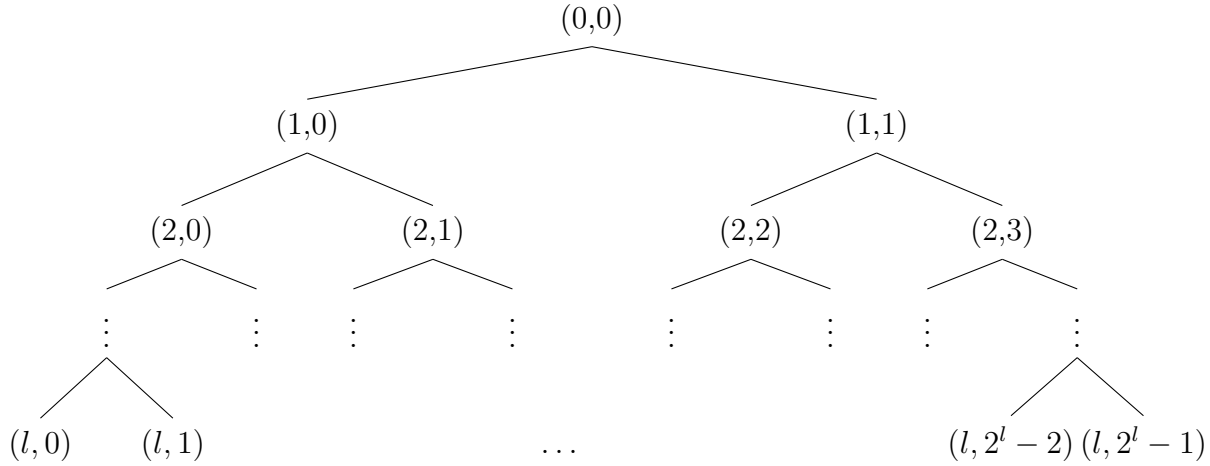
The Weil conjectures imply that for each p, it suffices to compute the Frobenius matrix modulo p^{N_p} where $N_p = \lceil g/2 + (2g+1)\log_p 2 \rceil$, so the bound $\mu = \lceil g/2 + (2g+1)\log_3 2 \rceil$ works for all p. For all $p < N$ such that (a,b) is p-admissible, it suffices to compute $D_0^{a,b} \dots D_{(p-1)/2}^{a,b}$ mod p^λ and $M_0^{a,b} \dots M_{(p-1)/2}^{a,b} \mod p^\lambda$ where $\lambda = \mu + (b-1)/2 + \max(0, 2a-b)$ by the precision estimate.

5.3.2 Computing Simultaneously for all Primes $p < N$

Let $n, \lambda \ge 1$ and $B \ge 2$ be integers. The reduction matrix is a product of matrices. To compute $M_0^{a,b} \dots M_{(p-1)/2}^{a,b} \mod p^\lambda$, a matrix multiplying algorithm using an accumulating remainder tree for matrices is adapted to compute this matrix for all primes $p < 2B$ simultaneously.

Lemma 5.3.2. *Given a sequence of matrices $M_0, M_1, \dots, M_{B-1} \in GL_n(\mathbb{Z})$, then we may compute $M_0 M_1 \dots M_{(p-1)/2} \mod p^\lambda$ for all primes $3 \le p < 2B$ simultaneously.*

Proof. Let $l = \lceil \log_2 B \rceil$. Construct binary trees of depth l, whose nodes are indexed by the pairs (i,j) with $0 \le i \le l$ and $0 \le j < 2^i$. The root node is $(0,0)$, the children of (i,j) are $(i+1, 2j)$ and $(i+1, 2j+1)$ and the leaf nodes are (l,j) for $0 \le j < 2^l$.



For each node (i,j), define

$$U_{i,j} = \left\{ k \in \mathbb{Z} \;\middle|\; \frac{jB}{2^i} \le k < \frac{(j+1)B}{2^i} \right\},$$

$$P_{i,j} = \prod_{\substack{p \text{ prime} \\ (p-1)/2 \in U_{i,j}}} p^\lambda,$$

$$A_{i,j} = \prod_{k \in U_{i,j}} M_{k+1} = M_{\lceil jB/2^i \rceil} \dots M_{\lfloor (j+1)B/2^i \rfloor},$$

$$C_{i,j} = M_0 A_{i,0} A_{i,1} \dots A_{i,j-1} \mod P_{i,j}.$$

For convenience, put $M_B = I$. Note that at the leaf nodes, $|U_{l,j}| = 0$ or 1 for every j. For every $0 \le k < B$, $U_{l,j} = \{k\}$ for $j = \lfloor 2^l k/B \rfloor$.

Compute the values of the $P_{i,j}$ tree. Enumerate primes less than $2B$, work from the bottom of the tree to the top, using the relation $P_{i,j} = P_{i+1,2j} P_{i+1,2j+1}$.

Similarly compute the $A_{i,j}$ tree from the bottom of the tree to the top, using the relation $A_{i,j} = A_{i+1,2j} A_{i+1,2j+1}$.

For the $C_{i,j}$ tree, work from the top of the tree to the bottom, using the initial condition $C_{0,0} = M_0 \mod P_{0,0}$ and the relations

$$C_{i+1,2j} = C_{i,j} \mod P_{i+1,2j},$$

$$C_{i+1,2j+1} = C_{i,j} A_{i+1,2j} \mod P_{i+1,2j+1}.$$

Suppose $3 \le p < 2B$, choose $j = \lfloor 2^{l-1}(p-1)/B \rfloor$ such that $U_{l,j} = \{(p-1)/2\}$, then $P_{l,j} = p^\lambda$ and $C_{l,j} = M_0 M_1 \dots M_{(p-1)/2} \mod p^\lambda$, so the output can be recovered from the leaf nodes of the $C_{i,j}$ tree. □

5.3.3 Recovering the Matrix of the Frobenius

By Lemma 5.1.1,

$$\sigma_p \left(\frac{x^i dx}{y} \right) \equiv \sum_{j=0}^{\mu-1} \sum_{r=0}^{(2g+1)j} p \alpha_j C_{j,r} U_p^{i+r+1,2j+1} \mod p^\mu.$$

Our aim is to find the $U_p^{a,b} \mod p^\mu$ in the expression, i.e. $(a,b) = (i+r+1, 2j+1)$ for $0 \le i \le 2g-1$, $0 \le j \le \mu - 1$ and $0 \le r \le (2g+1)j$. We find the ranges of a and b,

$$1 \le a = i + r + 1 \le 2g - 1 + (2g+1)j \le 2g - 1 + (2g+1)(\mu - 1) = (2g+1)\mu - 2,$$

$$1 \le b = 2j + 1 \le 2(\mu - 1) + 1 = 2\mu - 1.$$

For each admissible $(a,b) \in [1, (2g+1)\mu - 2] \times [1, 2\mu - 1]$, using the accumulating remainder tree method, compute $M_0^{a,b} \dots M_{(p-1)/2}^{a,b} \mod p^\lambda$ simultaneously for all $p < N$. Then compute $J_p^{a,b} = \left(D_0^{a,b} \dots D_{(p-1)/2}^{a,b} \right)^{-1} \left(M_0^{a,b} \dots M_{(p-1)/2}^{a,b} \right) \mod p^\mu$ and we can recover each $U_p^{a,b} \mod p^\mu$ from the first column of $J_p^{a,b}$.

For (a,b) not p-admissible, Kedlaya's algorithm is applied for each p.

Then the matrix of the Frobenius can be recovered for all $p < N$.

Chapter 6

Computing Data for the Sato-Tate Conjecture

This chapter is mainly based on [Ked15]. Construction of the Sato-Tate group is from [Fit15] and [FKRS12]. [FKRS12] provides a detailed coverage on the generalised Sato-Tate Conjecture, from the theoretical background to computational results, focusing on abelian surfaces.

We will denote $\mathfrak{q}$ a prime ideal over a number field K with norm q, where q is a power of a prime p.

6.1 Sato-Tate Conjecture for Elliptic Curves

A special case of the Weil conjectures, proved by Weil, shows that for an elliptic curve E over a finite field $\mathbb{F}_q$,

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

where $P(T) = (1-\alpha_1 T)(1-\alpha_2 T) = qT^2 - a_q T + 1 \in \mathbb{Z}[T]$ with degree $2g$. We have

$$\#E(\mathbb{F}_q) = q + 1 - (\alpha_1 + \alpha_2) = q + 1 - a_q,$$

and the Hasse-Weil bound gives

$$|a_q| \leq 2\sqrt{q}.$$

It is natural to consider the behaviour of the coefficient a_q.

Now let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$. Consider primes p at which E reduced modulo p gives an elliptic curve E_p over $\mathbb{F}_p$, i.e. primes not dividing the discriminant $\Delta = -16(4A^3 + 27B^2)$. Note that we are only excluding a finite number of primes. Normalise a_p by defining

$$\bar{a}_p = \frac{a_p}{\sqrt{p}} \in [-2, 2].$$

If E is defined over a number field K, we consider the reduction $E_\mathfrak{q}$ of E modulo prime ideals $\mathfrak{q}$ with norm q of the integer ring, then $E_\mathfrak{q}$ is a polynomial over the residue field $\mathbb{F}_q$. $a_\mathfrak{q}$ is normalised by defining

$$\bar{a}_\mathfrak{q} = \frac{a_\mathfrak{q}}{\sqrt{q}} \in [-2, 2].$$

We are interested to see how $\bar{a}_{\mathfrak{q}}$ varies in the interval $[-2, 2]$ for different prime ideals $\mathfrak{q}$ for a fixed curve.

Definition 6.1.1 (complex multiplication)**.** *For $m \in \mathbb{Z}$, $[m]\colon E \to E$ is a morphism defined by*

$$[m](P) = \begin{cases} P + \cdots + P \quad (m \text{ copies}) & \text{if} \quad m > 0 \\ O & \text{if} \quad m = 0 \\ [-m](-P) & \text{if} \quad m < 0 \end{cases}.$$

$\mathrm{End}(E)$ *denotes the endomorphism ring of E/K. E has no complex multiplication if*

$$[\ \ ]\colon \mathbb{Z} \to \mathrm{End}(E)$$

is an isomorphism, i.e. $\mathrm{End}(E) \cong \mathbb{Z}$*. Otherwise,* $\mathrm{End}(E)$ *is a finitely generated $\mathbb{Z}$-module and satisfies* $\mathrm{End}(E) \otimes \mathbb{Q} = M$ *for some field $M \supseteq K$, and we say E has complex multiplication over M.*

We call an elliptic curve generic if it has no complex multiplication.

Sato and Tate independently conjectured that for any generic elliptic curve, the sequence $\bar{a}_{\mathfrak{q}}$ follows the same distribution. To state the conjecture precisely, we need to formalise the definition of equidistribution.

Definition 6.1.2 (equidistribution)**.** *The sequence $\{\bar{a}_{\mathfrak{q}}\}$ is equidistributed with respect to the measure μ on $[-2, 2]$ if for any continuous function f,*

$$\lim_{N\to\infty} \frac{\sum_{q \le N} f(\bar{a}_{\mathfrak{q}})}{\#\{\mathfrak{q} : q \le N\}} = \int_{-2}^{2} f d\mu.$$

Theorem 6.1.3 (Sato-Tate)**.** *Suppose E is an elliptic curve over $\mathbb{Q}$ with no complex multiplication, then $\{\bar{a}_{\mathfrak{q}}\}$ is equidistributed with respect to the measure μ on $[-2, 2]$ where*

$$d\mu = \frac{\sqrt{4 - z^2}dz}{2\pi}.$$

We can think of $\sqrt{4 - z^2}/2\pi$ as the density function of $\bar{a}_p$ on $[-2, 2]$.

Note that the Sato-Tate conjecture can be extended to elliptic curves over any number field K, but it is only proved under certain conditions, for example when K is totally real [BLGG11].

The equidistribution property also extends to elliptic curves without complex multiplication.

Theorem 6.1.4 (Sato-Tate for CM elliptic curves)**.** *Suppose E is an elliptic curve over a number field K with complex multiplication in M. If $M \subseteq K$, then $\{\bar{a}_{\mathfrak{q}}\}$ is equidistributed with respect to the measure μ on $[-2, 2]$, where*

$$d\mu = \frac{dz}{\pi\sqrt{4 - z^2}}.$$

If $M \nsubseteq K$, then $\{\bar{a}_{\mathfrak{q}}\}$ is equidistributed with respect to the measure $\mu^{cont} + \mu^{disc}$ on $[-2, 2]$, where

$$d\mu^{cont} = \frac{dz}{2\pi\sqrt{4 - z^2}}$$

and $\mu^{disc} = \delta/2$ where δ is a Dirac point measure concentrated at 0.

6.2 Generalising to Abelian Varieties

The conjecture can be extended to abelian varieties, taking account for extra structures analogous to complex multiplication in the elliptic case.

6.2.1 Finding a Group that Defines the Distribution

Definition 6.2.1 (abelian variety)**.** *An abelian variety is a complete algebraic variety that is also an algebraic group with group operations defined by regular functions. An abelian surface is an abelian variety of dimension* 2*.*

For instance, the Jacobian variety attached to a hyperelliptic curve of genus g is an abelian variety of dimension g.

Let A be an abelian variety of dimension $g \geq 1$ over a number field K. For each prime ideal $\mathfrak{q}$ where A has good reduction, reduce modulo $\mathfrak{q}$ to obtain an abelian variety A_q over $\mathbb{F}_q$. Then by Weil,

$$Z(A_\mathfrak{q}/\mathbb{F}_q;T) = \frac{P_1(T)\dots P_{2g-1}(T)}{P_0(T)\dots P_{2g}(T)},$$

where $P_k(T) = \prod_{1\leq i_1<\dots<i_k\leq 2g}(1-\alpha_{i_1}\dots\alpha_{i_k}T) \in \mathbb{Z}[T]$. Note that P_1 determines the whole zeta function. Let $P_\mathfrak{q}(T) := P_1(T) = \prod_{j=1}^{2g}(1-\alpha_j T) = q^g T^{2g} + a_{2g-1,\mathfrak{q}}T^{2g-1} + \dots + 1$. We have

$$\#A(\mathbb{F}_q) = \prod_{j=1}^{2g}(1-\alpha_j),$$

$\alpha_j\alpha_{g+j} = q$ for $k = 1,\dots,g$, and $|\alpha_j| = q^{1/2}$ for $j = 1,\dots,2g$. Normalise the polynomial $\bar{P}_\mathfrak{q}(T) := P_\mathfrak{q}(T/\sqrt{q})$, then $\bar{P}(1/T) = T^{-2g}\bar{P}(T)$.

We will study how $P_\mathfrak{q}$ varies with $\mathfrak{q}$ for fixed abelian varieties. If A is a Jacobian variety associated to a curve C, then $P_\mathfrak{q}(T)$ of A is the numerator of the zeta function of $C_\mathfrak{q}$ the reduction of C at $\mathfrak{q}$, i.e.

$$Z(C_\mathfrak{q}/\mathbb{F}_q;T) = \frac{P_\mathfrak{q}(T)}{(1-T)(1-qT)}.$$

Hence, when we look for examples, we can consider Jacobian varieties associated to curves as $P_\mathfrak{q}(T)$ can be recovered from the zeta function of the curve.

Definition 6.2.2 (topological group)**.** *A topological group is a group which is also a topological space such that the group operations are continuous maps.*

Definition 6.2.3 (Lie group)**.** *A Lie group is a smooth manifold which is also a group such that the group operations are smooth maps.*

Theorem 6.2.4. *Any compact topological group admits a unique translation-invariant measure called the Haar measure. For a finite group with discrete topology, the Haar measure is the uniform measure.*

The aim is to define a topological group that would give us the correct measure that agrees with the distribution of the polynomials $\bar{P}_\mathfrak{q}(T)$ for abelian varieties.

By Weil, the roots of $\bar{P}_{\mathfrak{q}}(T)$ lie on the unit circle and occur in reciprocal pairs. Hence $\bar{P}_{\mathfrak{q}}(T)$ occurs as the characteristic polynomial of some matrix in the group $USp(2g)$ of unitary symplectic matrices.

$$USp(2g) = \{M \in GL_{2g}(\mathbb{C}) \mid M^{-1} = M^*, M^T JM = J\},$$

where

$$J = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_1 \end{pmatrix}, \quad J_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

A matrix is unitary, i.e. $M^{-1} = M^*$ is equivalent to saying it is normal and its eigenvalues have norm 1. A matrix is symplectic, i.e. $M^T JM = J$ if and only if its characteristic polynomial is a reciprocal polynomial. Normal matrices over $\mathbb{C}$ are similar if and only if they have the same characteristic polynomial. Hence $\mathrm{Conj}(USp(2g))$ can be identified with the space of reciprocal polynomials with roots on the unit circle.

The Sato-Tate group ST_A is defined as a compact Lie group which is a subgroup of $USp(2g)$, so that a sequence $\{s_{\mathfrak{q}}\} \subset \mathrm{Conj}(ST_A)$ corresponding to $P_{\mathfrak{q}}(T)$ are equidistributed with respect to the image on $\mathrm{Conj}(ST_A)$ of the normalised Haar measure μ_{ST_A}. For any continuous function $f : \mathrm{Conj}(ST_A) \to \mathbb{C}$,

$$\mu_{ST_A}(f) = \lim_{n\to\infty} \frac{\sum_{q\leq n} f(s_{\mathfrak{q}})}{\#\{\mathfrak{q} : q \leq n\}}.$$

6.2.2 Sato-Tate group of Elliptic Curves with Complex Multiplication

Here we present the construction of the Sato-Tate group for elliptic curves with complex multiplication as given in Section 2.4.2 in [Fit15].

Suppose E is an elliptic curve over K with complex multiplication in K. Let $\mathfrak{N}$ be the conductor of E, which is a product of all the bad primes, each with some exponent. Let S be the set of bad primes. For any good prime $\mathfrak{q}$, $P_{\mathfrak{q}}(T) = (1-\alpha_1 T)(1-\alpha_2 T) = qT^2 - a_{\mathfrak{q}}T + 1 \in \mathbb{Z}[T]$. We see that α_1 and α_2 are complex conjugates and

$$\#E(\mathbb{F}_q) = q + 1 - a_{\mathfrak{q}}.$$

By a result of Deuring, there exists an algebraic Hecke character ψ_E of K of modulo $\mathfrak{N}$ and infinity-type 1 that is attached to E such that $a_q = \psi_E(\mathfrak{q}) + \overline{\psi_E(\mathfrak{q})}$.

The L-function of ψ_E is $L(\psi_E, s) = \prod_{\mathfrak{q}}(1 - \psi_E(\mathfrak{q})q^{-s})^{-1}$. The unitary group of degree 1 is $U(1) = \{u \in \mathbb{C}^\times \mid u\overline{u} = 1\}$. Let μ be the Haar measure of $U(1)$. For $\mathfrak{q} \notin S$, define $x_{\mathfrak{q}} := \psi_E(\mathfrak{q})/q^{1/2} \in U(1)$.

Lemma 6.2.5. *Let G be a compact group and let X denote the set of conjugacy classes of G. Let $\{x_{\mathfrak{q}}\}$ be a sequence in X. Suppose for any irreducible nontrivial representation ϱ of G, the Euler product $L(\varrho, s)$ extends to a holomorphic function on $Re(s) \geq 1$ and is nonvanishing in $Re(s) \geq 1$. Then the sequence $\{x_{\mathfrak{q}}\}$ is μ-equidistributed over X.*

Proof. See Corollary 2.7 of [Fit15]. □

Lemma 6.2.6. *$\{x_\mathfrak{q}\}$ is μ-equidistributed on $U(1)$.*

Proof. The nontrivial irreducible characters of $U(1)$ are $\phi_a : U(1) \to \mathbb{C}^\times$ for $a \in \mathbb{Z}^\times$. By Lemma 6.2.5, taking $G = U(1)$, we have $X = U(1)$ and it is sufficient to show that $L(\phi_a, s)$ is holomorphic and nonvanishing for $Re(s) \geq 1$. This follows from the fact that a nontrivial power of ψ_E are Hecke characters and the L-function of a nontrivial unitarised Hecke character is holomorphic and nonvanishing for $Re(s) \geq 1$. See Theorem 2.4 of [Fit15]. □

Lemma 6.2.7. *$\{\bar{a}_\mathfrak{q}\}$ is equidistributed on $[-2, 2]$ with respect to $\frac{dz}{\pi\sqrt{4-z^2}}$.*

Proof. $\bar{a}_\mathfrak{q} = x_\mathfrak{q} + \overline{x_\mathfrak{q}}$. By Lemma 6.2.6, $x_\mathfrak{q}$ is μ-equidistributed on $U(1)$. The Haar measure is translation-invariant so μ is the uniform measure on $U(1)$. The projection of $U(1)$ on $[-2, 2]$ by $u \mapsto u + \overline{u}$ is the measure $\frac{dz}{\pi\sqrt{4-z^2}}$. □

6.2.3 Construction of the Sato-Tate Group

We will sketch the construction of the Sato-Tate group for general abelian varieties. Details of the construction can be found in Section 2 of [FKRS12].

Definition 6.2.8 (Tate module)**.** *The ℓ-adic Tate module of A is the group $V_\ell(A) = \lim_{\leftarrow} A[\ell^n]$, where $A[\ell^n]$ is the ℓ^n torsion group of A and the inverse limit is taken with respect to the maps $A[\ell^{n+1}] \to A[\ell^n]$.*

Remark 15. *We can make the identifications $V_\ell(A) \simeq H_{1,et}(A_\mathbb{C}, \mathbb{Q}_\ell) \simeq H_1(A_\mathbb{C}^{top}, \mathbb{Q})$, where $H_{1,et}(A_\mathbb{C}, \mathbb{Q}_\ell)$ is the étale homology group and $H_1(A_\mathbb{C}^{top}, \mathbb{Q})$ is the singular homology group.*

The action of the absolute Galois group $G_K = \mathrm{Gal}(K^{alg}/K)$ on the rational ℓ-adic Tate module $V_l(A)$ defines an ℓ-adic representation

$$\varrho : G_K \to Aut(V_\ell(A)) \subseteq GL_{2g}(\mathbb{Q}_\ell).$$

Let S be the set of bad primes. For $\mathfrak{q} \notin S$, $P_\mathfrak{q}(T) = L_\mathfrak{q}(\varrho, T) = \det(1 - \varrho(F_\mathfrak{q}^{-1})T, V_\ell(A))$, where $F_\mathfrak{q}^{-1}$ is the geometric Frobenius.

Definition 6.2.9 (cyclotomic character)**.** *The ℓ-adic cyclotomic character $\chi_\ell : G_K \to \mathbb{Z}_\ell^\times$ is defined as follows: for any $g \in G_K$ and any primitive ℓ^nth root of unity ζ_n in $K^\times$, $g : \zeta_n \mapsto \zeta_n^{a_n}$ for some $a_n \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$, then $\chi_\ell : g \mapsto (a_n)_{n\in\mathbb{N}}$.*

Let $G_\ell = \varrho(\ker \chi_\ell)^{Zar}$ be the Zariski closure of the image of the kernel of the cyclotomic character χ_ℓ.

Definition 6.2.10 (Sato-Tate group)**.** *Pick an embedding $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ and let $G_{\ell,\iota} = G_\ell \otimes_\iota \mathbb{C}$. The Sato-Tate group $ST(A)$ is defined to be the maximal compact subgroup of $G_{\ell,\iota}$.*

The group is only defined up to conjugation but this is sufficient for the purpose of proving equidistributions. We take $x_\mathfrak{q}$ as the conjugacy class of $\varrho(F_\mathfrak{q}^{-1}) \otimes q^{-1/2}$. Then

$$\bar{P}_\mathfrak{q}(T) = L_\mathfrak{q}(\varrho, T/q^{1/2}) = \det(1 - x_\mathfrak{q}T, V_\ell(A) \otimes_\iota \mathbb{C}).$$

6.2.4 The Generalised Sato-Tate Conjecture

For $g = 1$, no extra structure means no complex multiplication. In fact, for $g \leq 3$, no extra structure means the endomorphism ring consists of only multiplication by integers. For $g > 3$, the exclusion of extra endomorphisms is not sufficient, but we will not include the technicalities here.

When A has no extra structure, the Sato-Tate group is $USp(2g)$, but when A has extra structure, the group is cut down to a smaller subgroup.

Conjecture 6.2.11 (Generalised Sato-Tate Conjecture)**.** *Let A be an abelian variety of dimension g over a number field K, then the sequence $\{x_{\mathfrak{q}}\}$ in $\mathrm{Conj}(ST_A)$ corresponding to the polynomials $\bar{P}(T)$ is equidistributed with respect to the image of Haar measure.*

6.3 Distributions for Elliptic Curves

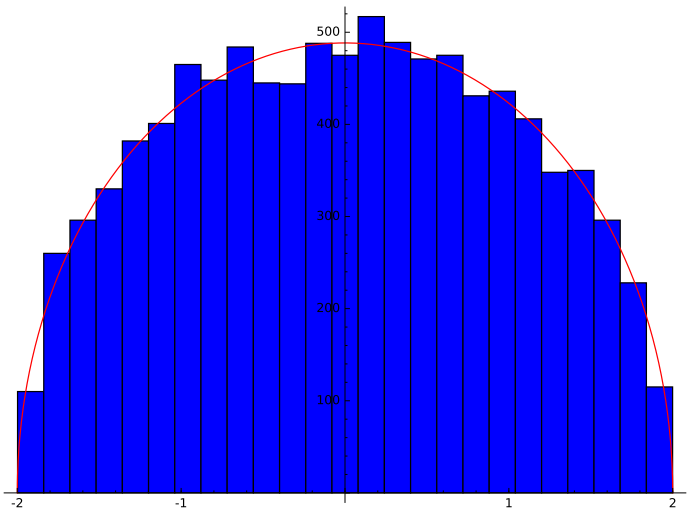
The examples in the section are computed in Sage and the code can be found in Appendix B.1.

6.3.1 Generic Case

In the generic case, the Sato-Tate group is $SU(2)$ and an example is the curve $y^2 = x^3 + x + 1$ over $\mathbb{Q}$. We have the polynomials

$$\bar{P}_{\mathfrak{q}}(T) = T^2 - \bar{a}_{\mathfrak{q}}T + 1.$$

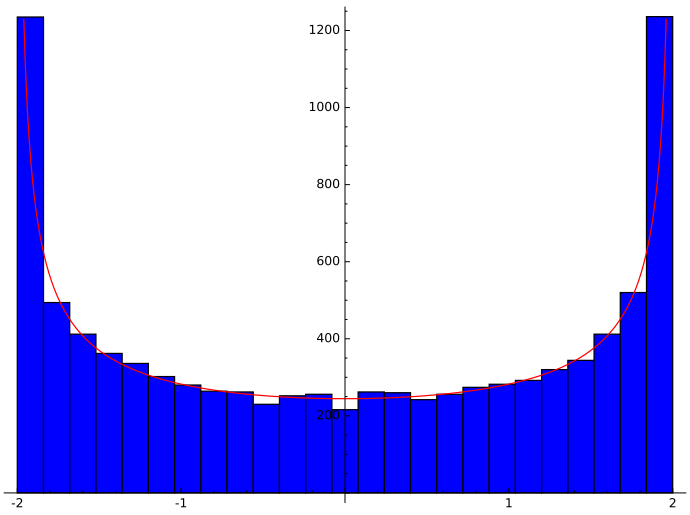
We plot the histogram of $\bar{a}_{\mathfrak{q}}$ and the expected distribution:



6.3.2 Complex Multiplication in Base Field

If an elliptic curve over K has complex multiplication in K, its Sato-Tate group is $U(1)$. An example is the curve $y^2 = x^3 + 1$ over $\mathbb{Q}(\sqrt{-3})$.

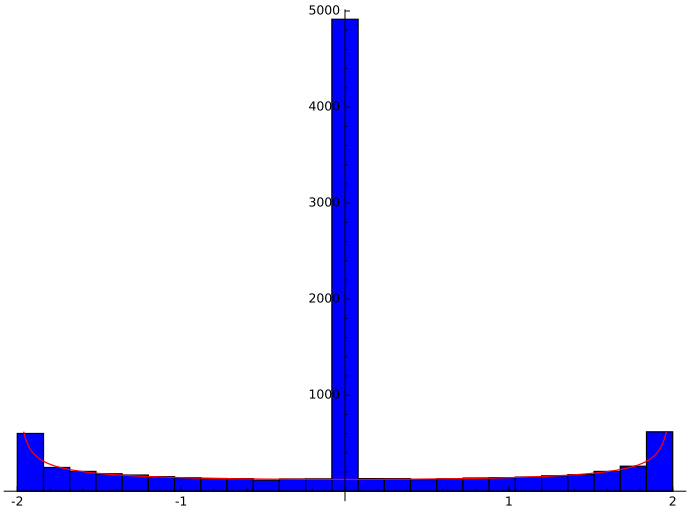
We plot the histogram of $\bar{a}_q$ and the expected distribution:



6.3.3 Complex Multiplication not in Base Field

If an elliptic curve over K has complex multiplication in some field not contained in K, its Sato-Tate group is $N(U(1))$. We can look at $y^2 = x^3 + 1$ over $\mathbb{Q}$.

We plot the histogram of $\bar{a}_q$ and the continuous part of the expected distribution:



Note that there is a Dirac point measure concentrated at 0.

6.4 Computing Data for Abelian Surfaces

Abelian surfaces are of dimension 2, so we can consider the case when they are Jacobian varieties of genus 2 curves. In [FKRS12], possible Sato-Tate groups were studied and an exhaustive search was done to numerically test the Sato-Tate conjecture for abelian surfaces. The normalised polynomial in the numerator of the zeta function of a genus 2 curve modulo $\mathfrak{q}$ is in the form

$$\bar{P}_{\mathfrak{q}}(T) = T^4 + \bar{a}_{1,\mathfrak{q}}T^3 + \bar{a}_{2,\mathfrak{q}}T^2 + \bar{a}_{1,\mathfrak{q}}T + 1.$$

It turns out that considering only $\bar{a}_{1,\mathfrak{q}}$ is insufficient, so we have to take $\bar{a}_{2,\mathfrak{q}}$ into account. Generic group algorithms were applied in [FKRS12] to compute the group orders of the Jacobian of the curves to obtain the coefficients $\bar{a}_{1,\mathfrak{q}}$ and $\bar{a}_{2,\mathfrak{q}}$ since they were more practical in the settings, namely for $q < 2^{30}$, although asymptotically Harvey's algorithm in [Har14] is more efficient.

Theorem 6.4.1 (Fité-Roger-Kedlaya-Sutherland)**.** *Up to conjugation within* USp(4)*, there are exactly* 52 *groups that occur as Sato-Tate groups of abelian surfaces over number fields, all of which can be realised using genus* 2 *curves. Of these groups, exactly* 34 *groups occur for abelian surfaces over* $\mathbb{Q}$*, all of which can be realised using genus* 2 *curves over* $\mathbb{Q}$*.*

Examples and data for all 52 possible Sato-Tate groups of abelian surfaces were tabulated in [FKRS12]. In practise, to determine the Sato-Tate group of the Jacobian variety of a given hyperelliptic curve of genus 2, one can compute the moments of the distribution of the coefficients $\bar{a}_{1,\mathfrak{q}}$ and $\bar{a}_{2,\mathfrak{q}}$ and compare against the standard table in [FKRS12] to identify the Sato-Tate group of the abelian surface.

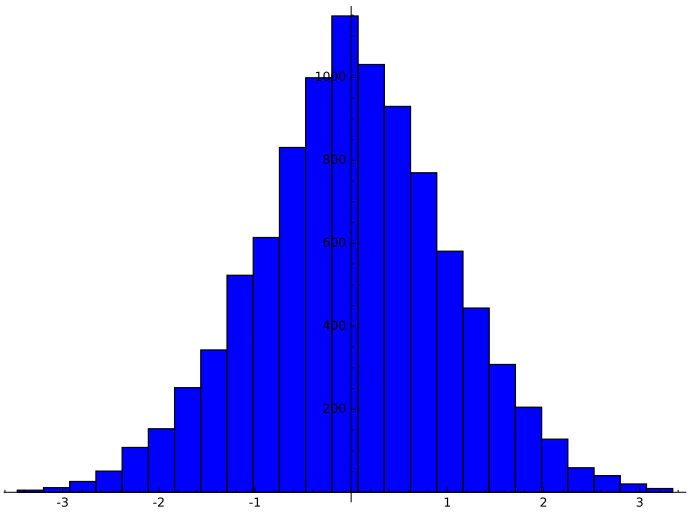
Notice the increase in the number of groups compared to that in the genus 1 case, where there are only 3 possible groups. There could be an explosion in the number of groups for higher genus cases, which means it might not be practical to obtain a list of all possible distributions using the same method for abelian varieties of higher dimensions $g \geq 3$.

Here we will obtain visualisations of the distributions for some examples of abelian surfaces which correspond to hyperelliptic curves of genus 2.

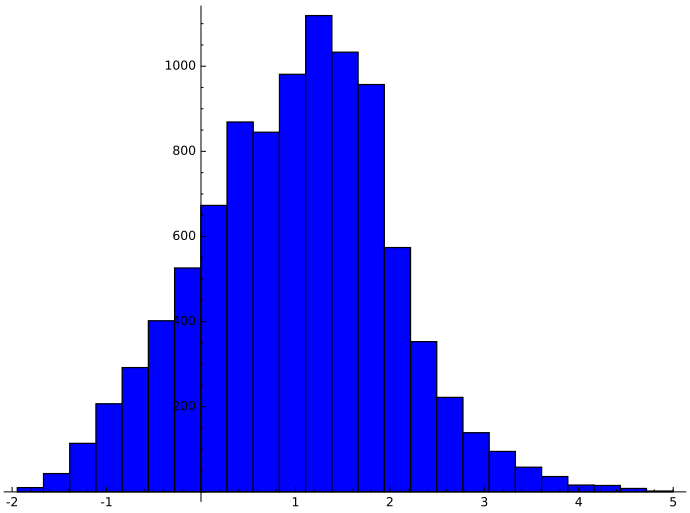
6.4.1 Generic case

The generic case we have $USp(4)$ as the Sato-Tate group, an example is the Jacobian variety of the curve $y^2 = x^5 - x + 1$ over $\mathbb{Q}$.

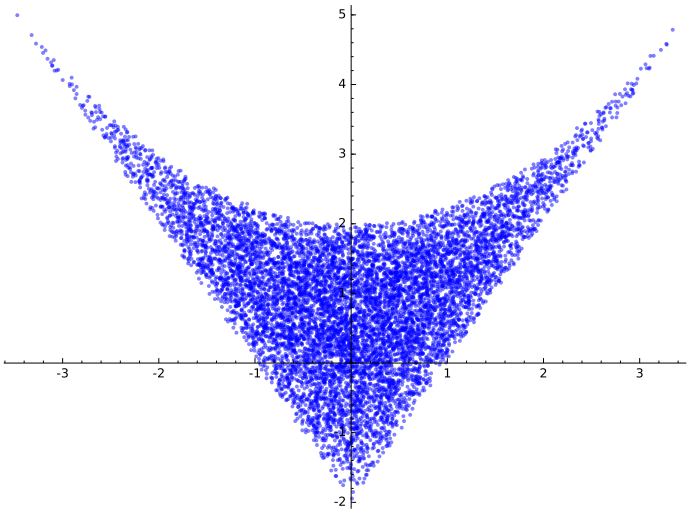
We obtain the histogram of $\bar{a}_{1,\mathfrak{q}}$:



and the histogram of $\bar{a}_{2,\mathfrak{q}}$:



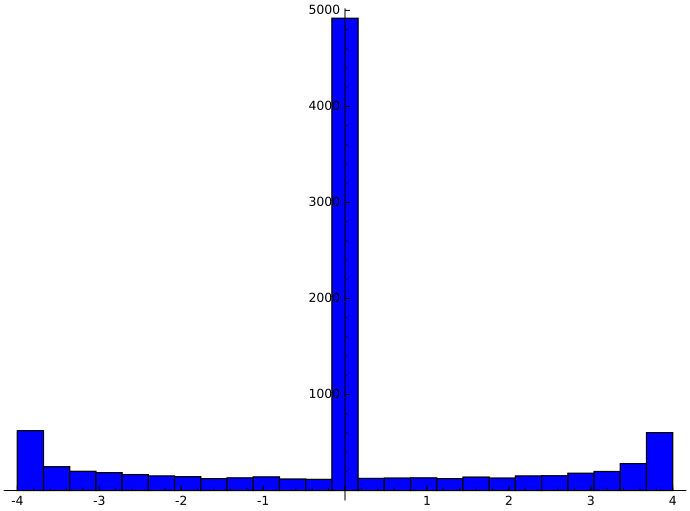
The joint distribution of $(\bar{a}_{1,\mathfrak{q}}, \bar{a}_{2,\mathfrak{q}})$:



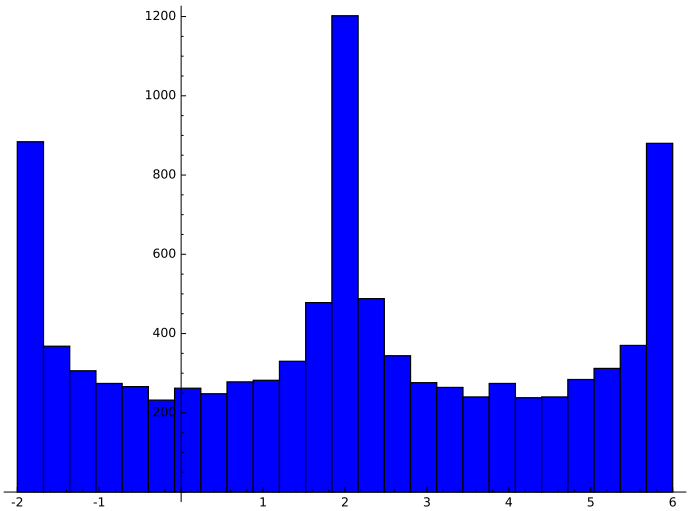
6.4.2 C_2

One of the 51 possible Sato-Tate groups of abelian surfaces with extra structures is C_2. An example is the Jacobian variety of the curve $y^2 = x^5 - x$ over $\mathbb{Q}(\sqrt{-2})$.

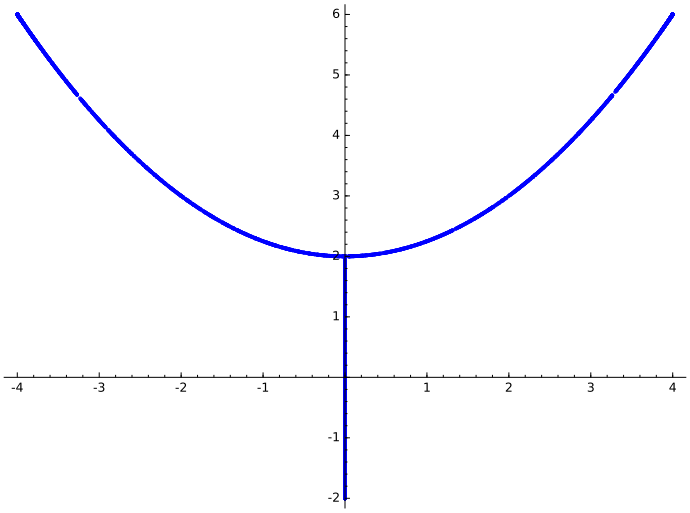
We obtain the histogram of $\bar{a}_{1,\mathfrak{q}}$:



and the histogram of $\bar{a}_{2,\mathfrak{q}}$:



The joint distribution of $(\bar{a}_{1,\mathfrak{q}}, \bar{a}_{2,\mathfrak{q}})$:



Appendix A

Implementation of Kedlaya's Algorithm

This is the computation done in SageMath for the elliptic curve $y^2 = x^3 + x + 1$ and prime $p = 5$ in Section 4.7.

```
q = 5
p,a = list(q.factor())[0]
Q_x.<x> = PolynomialRing(QQ)
Q = x^3+x+1
dQ = diff(Q,x)
Q.discriminant().factor()
```

```
-1 * 31
```

```
g = (Q.degree()-1)/2
n = ceil(g*a/2+(2*g+1)*log(2,p))
m = n+1
while m-max(floor(log(2*m-1,p)),floor(log(2*g+1,p))) < n: m = m+1
n1 = n+max(floor(log(2*m-3,p)),floor(log(2*g+1,p)))+floor(log(2*g-1,p))+1
print "n1 = %s, m = %s, n = %s"%(n1, m, n)
```

```
n1 = 3, m = 3, n = 2
```

```
Q_xz.<x,z> = PolynomialRing(QQ)
frob = Q_x.hom([x^p])
E = (frob(Q)-Q^p)/p
I = Q_xz.ideal(Q*z^2-1)
Zpring = Zp(p, n1, 'capped-abs',print_mode='terse',print_pos=True)
Zp_x.<x> = PolynomialRing(Zpring)
Zp_xz.<z> = PolynomialRing(Zp_x)
Qpring = Qp(p, n1, print_mode='series',print_pos=True)
Z_x.<x> = PolynomialRing(ZZ)
f = [Zp_xz(I.reduce(sum([binomial(-1/2,k)*p^(k+1)*x^(p*(i+1)-1)*E^k*z^(p*(2*k+1))\
                         for k in [0..m-1]]))).change_ring(Z_x) for i in [0..2*g-1]]
maxj=[(f[j].degree(z)-1)/2 for j in [0..2*g-1]]
```

```
F=[[f[j][2*i+1] for i in [0.. maxj[j]]] for j in [0..2*g-1]]
for j in [0..2*g-1]:
    for i in [0.. maxj[j]]:
        print "F(%s,%s): %s"%(j,i,F[j][i])
```

```
F(0,0): 0
F(0,1): 5*x
F(0,2): 70*x^2 + 70*x + 25
F(0,3): 50*x^2 + 50*x
F(0,4): 75*x + 50
F(0,5): 50*x^2 + 50*x + 100
F(0,6): 75*x^2 + 100*x + 25
F(0,7): 25*x + 50
F(1,0): 5*x^3 + 65*x + 65
F(1,1): 15*x^2 + 30*x + 85
F(1,2): 85*x^2 + 90*x + 50
F(1,3): 75*x^2 + 100
F(1,4): 25*x^2 + 75*x + 75
F(1,5): 50*x^2 + 100*x + 100
F(1,6): 25*x^2 + 50*x + 75
F(1,7): 100*x^2 + 100*x + 75
```

```
Qdeg=Q.degree()
dQdeg=dQ.degree()
T=matrix(Qdeg+dQdeg)
for i in [0..dQdeg-1]:
    for j in [0..Qdeg]: T[i+j,i]=Q[j]
for i in [0..Qdeg-1]:
    for j in [0..dQdeg]: T[i+j,i+Qdeg-1]=dQ[j]
T
```

```
[1 0 1 0 0]
[1 1 0 1 0]
[0 1 3 0 1]
[1 0 0 3 0]
[0 1 0 0 3]
```

```
Tinv = T.inverse()
O_dQ = sum([(O(p^n1))*x^i for i in [0..dQdeg-1]])
O_Q = sum([(O(p^n1))*x^i for i in [0..Qdeg-1]])
S = [F[j][maxj[j]]for j in [0..2*g-1]]
for j in [0..2*g-1]:
    print "reduce (x^%s zdx)^sigma"%j
    k = maxj[j]
    print "S(%s,%s) = %s"%(j,k,S[j])
```

```
    while k>0:
        v = zero_vector(QQ,Qdeg+dQdeg)
        for i in [0..S[j].degree()]:
            v[i] = S[j][i]
        AB = Tinv*v
        A = sum([(AB[i])*x^i for i in [0..dQdeg-1]])
        print "A(%s,%s) = %s"%(j,k,A+O_dQ)
        B = sum([(AB[i+dQdeg])*x^i for i in [0..Qdeg-1]])
        print "B(%s,%s) = %s"%(j,k,B+O_Q)
        k = k-1
        S[j] = F[j][k]+A+2*diff(B,x)/(2*k+1)
        print "S(%s,%s) = %s"%(j,k,S[j]+O_Q)
```

```
reduce (x^0 zdx)^sigma
S(0,7) = 25*x + 50
A(0,7) = (5^2 + O(5^3))*x + (O(5^3))
B(0,7) = (3*5^2 + O(5^3))*x^2 + (O(5^3))*x + (2*5^2 + O(5^3))
S(0,6) = (3*5^2 + O(5^3))*x^2 + (4*5^2 + O(5^3))*x + (5^2 + O(5^3))
A(0,6) = (3*5^2 + O(5^3))*x + (4*5^2 + O(5^3))
B(0,6) = (4*5^2 + O(5^3))*x^2 + (2*5^2 + O(5^3))*x + (2*5^2 + O(5^3))
S(0,5) = (2*5^2 + O(5^3))*x^2 + (5^2 + O(5^3))*x + (2*5^2 + O(5^3))
A(0,5) = (3*5^2 + O(5^3))*x + (2*5^2 + O(5^3))
B(0,5) = (4*5^2 + O(5^3))*x^2 + (5^2 + O(5^3))*x + (O(5^3))
S(0,4) = (O(5^3))*x^2 + (O(5^3))*x + (2*5^2 + O(5^3))
A(0,4) = (4*5^2 + O(5^3))*x + (4*5^2 + O(5^3))
B(0,4) = (2*5^2 + O(5^3))*x^2 + (2*5^2 + O(5^3))*x + (3*5^2 + O(5^3))
S(0,3) = (2*5^2 + O(5^3))*x^2 + (O(5^3))*x + (5^2 + O(5^3))
A(0,3) = (4*5^2 + O(5^3))*x + (4*5^2 + O(5^3))
B(0,3) = (2*5^2 + O(5^3))*x^2 + (2*5^2 + O(5^3))*x + (2*5^2 + O(5^3))
S(0,2) = (4*5 + 2*5^2 + O(5^3))*x^2 + (2*5 + O(5^3))*x + (4*5 + O(5^3))
A(0,2) = (5 + 2*5^2 + O(5^3))*x + (4*5 + 4*5^2 + O(5^3))
B(0,2) = (3*5 + 2*5^2 + O(5^3))*x^2 + (2*5 + 3*5^2 + O(5^3))*x + (5^2 + O(5^3))
S(0,1) = (O(5^3))*x^2 + (5 + 4*5^2 + O(5^3))*x + (2*5 + O(5^3))
A(0,1) = (5 + O(5^3))*x + (5^2 + O(5^3))
B(0,1) = (3*5 + 5^2 + O(5^3))*x^2 + (3*5^2 + O(5^3))*x + (2*5 + 4*5^2 + O(5^3))
S(0,0) = (O(5^3))*x^2 + (3*5 + 5^2 + O(5^3))*x + (2*5^2 + O(5^3))
reduce (x^1 zdx)^sigma
S(1,7) = 100*x^2 + 100*x + 75
A(1,7) = (3*5^2 + O(5^3))*x + (4*5^2 + O(5^3))
B(1,7) = (4*5^2 + O(5^3))*x^2 + (2*5^2 + O(5^3))*x + (4*5^2 + O(5^3))
S(1,6) = (5^2 + O(5^3))*x^2 + (2*5^2 + O(5^3))*x + (O(5^3))
A(1,6) = (O(5^3))*x + (3*5^2 + O(5^3))
B(1,6) = (O(5^3))*x^2 + (4*5^2 + O(5^3))*x + (2*5^2 + O(5^3))
S(1,5) = (2*5^2 + O(5^3))*x^2 + (4*5^2 + O(5^3))*x + (O(5^3))
A(1,5) = (O(5^3))*x + (5^2 + O(5^3))
B(1,5) = (O(5^3))*x^2 + (3*5^2 + O(5^3))*x + (4*5^2 + O(5^3))
```

```
S(1,4) = (5^2 + O(5^3))*x^2 + (3*5^2 + O(5^3))*x + (3*5^2 + O(5^3))
A(1,4) = (3*5^2 + O(5^3))*x + (O(5^3))
B(1,4) = (4*5^2 + O(5^3))*x^2 + (O(5^3))*x + (3*5^2 + O(5^3))
S(1,3) = (3*5^2 + O(5^3))*x^2 + (5^2 + O(5^3))*x + (4*5^2 + O(5^3))
A(1,3) = (3*5^2 + O(5^3))*x + (2*5^2 + O(5^3))
B(1,3) = (4*5^2 + O(5^3))*x^2 + (5^2 + O(5^3))*x + (2*5^2 + O(5^3))
S(1,2) = (2*5 + 3*5^2 + O(5^3))*x^2 + (4*5 + 2*5^2 + O(5^3))*x + (2*5 + O(5^3))
A(1,2) = (4*5 + 4*5^2 + O(5^3))*x + (2*5^2 + O(5^3))
B(1,2) = (2*5 + 3*5^2 + O(5^3))*x^2 + (5^2 + O(5^3))*x + (2*5 + 3*5^2 + O(5^3))
S(1,1) = (3*5 + O(5^3))*x^2 + (5 + 2*5^2 + O(5^3))*x + (2*5 + 4*5^2 + O(5^3))
A(1,1) = (4*5 + 4*5^2 + O(5^3))*x + (3*5 + 3*5^2 + O(5^3))
B(1,1) = (2*5 + 3*5^2 + O(5^3))*x^2 + (4*5 + 3*5^2 + O(5^3))*x + (4*5 + O(5^3))
```

```
for j in [0..2*g-1]:
    S[j]=S[j].change_ring(Zpring)
    print "S(%s,0) = %s"%(j,S[j])
```

```
S(0,0) = (40 + O(5^3))*x + (50 + O(5^3))
S(1,0) = (5 + O(5^3))*x^3 + (0 + O(5^3))*x^2 + (25 + O(5^3))*x + (95 + O(5^3))
```

```
sdeg=[S[j].degree() for j in [0..2*g-1]]
for j in [0..2*g-1]:
    while sdeg[j]>2*g-1:
        k=sdeg[j]-2*g
        red_poly=Q_x(x^k*dQ+2*k*x^(k-1)*Q)
        red_poly
        S[j]=S[j]-S[j][sdeg[j]]*red_poly/red_poly[k+2*g]
        sdeg[j]=S[j].degree()
    print "G(%s,0) = %s"%(j,S[j])
```

```
G(0,0) = (40 + O(5^3))*x + (50 + O(5^3))
5*x^3 + 3*x + 2
G(1,0) = (0 + O(5^3))*x^3 + (0 + O(5^3))*x^2 + (22 + O(5^2))*x + (18 + O(5^2))
```

```
M=matrix([[S[i][j]+O(p^n) for i in[0..2*g-1]] for j in[0..2*g-1]])
M
```

```
[ 0 + O(5^2) 18 + O(5^2)]
[15 + O(5^2) 22 + O(5^2)]
```

```
M.charpoly()
```

```
(1 + O(5^3))*x^2 + (3 + O(5^2))*x + (5 + O(5^2))
```

Appendix B

Computations of Sato-Tate Distributions

The following are computations done in SageMath for the examples in Sections 6.3 and 6.4.

B.1 Elliptic curves

B.1.1 Generic case

We compute for the curve $y^2 = x^3 + x + 1$ over $\mathbb{Q}$ in Section 6.3.1.

We define a function `nag1` to compute $\bar{a}_{\mathfrak{q}}$. For each $\mathfrak{q}$, the required precision N is computed, then Kedlaya's algorithm in [Ked01] `matrix_of_frobenius_hyperelliptic` is used when $p \leq (2g+1)(2N-1)$ and Harvey's optimisation in [Har07] `hypellfrob` is used when $p > (2g+1)(2N-1)$.

```
from sage.schemes.hyperelliptic_curves.hypellfrob import hypellfrob
def nag1(q, Q):
    p,n=list(q.factor())[0]
    if Q.discriminant()%p<>0:
        prec=ceil(n/2+log(4,p))
        prec1=prec+floor(log(3,p))
        R.<x>=PolynomialRing(ZZ)
        if p>3*(2*prec-1):
            A=hypellfrob(p, prec, R(Q))
        else:
            A,f=monsky_washnitzer.matrix_of_frobenius_hyperelliptic(\
                                                    R(Q), p, prec1)
        A=A^n
        a=ZZ(Integers(p**prec)(-A.trace()))
        bound=2*q^(1/2)
        if a>bound:a=a-p^prec
        return -a/q^(1/2).n(digits=3)
```

Here we compute for primes up to 10^5.

```
R.<x> = QQ['x']
Q1=x^3+x+1
D1=[]
for p in primes(3, 10^5):
    g=nag1(p,Q1)
    if g is not None:
        D1.append(g)


H1=histogram(D1, bins=25)
L1=plot((4*len(D1)/25)*sqrt(4-x^2)/(2*pi), (x,-2,2), color='red')
H1+L1
```

B.1.2 Complex multiplication in base field

We compute for the curve $y^2 = x^3 + 1$ over $\mathbb{Q}(\sqrt{-3})$ in Section 6.3.2.

First, we find a list of all prime ideals `q` with norm less than 10^5 by factorising the ideals (p) and get a list of their norms q.

```
R.<x> = QQ['x']
minpoly=x^2 + 3
K.<w> = NumberField(minpoly)
Q2=x^3+1
qlist=[]
for p in primes(3, 10^5):
    F=K.ideal(p).factor()
    for I,h in list(F):
        q=I.norm()
        if q<10^5:
            qlist.append(q)
qcounted=[(q,qlist.count(q)) for q in uniq(qlist)]
```

`qcounted` contains pairs (q, n) where n is the number of times q appeared. Run the function for all q in the list `qcounted`.

```
D2=[]
for q,a in qcounted:
    g=nag1(q,Q2)
    if g is not None:
        for i in [1..a]:
            D2.append(g)


H2=histogram(D2, bins=25)
L2=plot((4*len(D2)/25)/(pi*sqrt(4-x^2)), (x,-1.96,1.96), color='red')
H2+L2
```

B.1.3 Complex multiplication not in base field

We compute for the curve $y^2 = x^3 + 1$ over $\mathbb{Q}$ in Section 6.3.3.

```
R.<x> = QQ['x']
Q3=x^3+1
D3=[]
for p in primes(3, 10^5):
    g=nag1(p,Q3)
    if g is not None:
        D3.append(g)

H3 = histogram(D3, bins=25)
L3 = plot((4*len(D3)/25)/(2*pi*sqrt(4-x^2)), (x,-1.96,1.96), color='red')
H3+L3
```

B.2 Genus 2 curves

B.2.1 Generic case

We compute for the curve $y^2 = x^5 - x + 1$ over $\mathbb{Q}$ in Section 6.4.1. By modifying `nag1`, we define a new function `nag2` to find the pairs $(\bar{a}_{1,\mathfrak{q}}, \bar{a}_{2,\mathfrak{q}})$.

```
from sage.schemes.hyperelliptic_curves.hypellfrob import hypellfrob
def nag2(q, Q):
    p,n=list(q.factor())[0]
    if Q.discriminant()%p<>0:
        prec=ceil(n+log(12,p))
        prec1=prec+floor(log(5,p))
        R.<x>=PolynomialRing(ZZ)
        if p>5*(2*prec-1):
            A=hypellfrob(p, prec, R(Q))
        else:
            A,f=monsky_washnitzer.matrix_of_frobenius_hyperelliptic(\
                                                    R(Q), p, prec1)
        A=A^n
        P=A.charpoly()
        a1=ZZ(Integers(p**prec)(P[3]))
        a2=ZZ(Integers(p**prec)(P[2]))
        bound=6*q
        if a1>bound:a1=a1-p^prec
        if a2>bound:a2=a2-p^prec
        return (a1/q^(1/2).n(digits=3),a2/q.n(digits=3))

R.<x> = QQ['x']
Q1=x^5-x+1
D1=[]
```

```
for p in primes(3, 10^5):
    g=nag2(p,Q1)
    if g is not None:
        D1.append(g)
a1=[D1[i][0] for i in [0..len(D1)-1]]
a2=[D1[i][1] for i in [0..len(D1)-1]]

histogram(a1, bins=25)
histogram(a2, bins=25)
list_plot(D1, alpha=0.5)
```

B.2.2 C_2

We compute for the curve $Q(x) = x^5 - x$ over $\mathbb{Q}(\sqrt{-2})$ in Section 6.4.2. As in the elliptic case, we need to find a list of all prime ideals $\mathfrak{q}$ with norm less than 10^5.

```
R.<x> = QQ['x']
minpoly=x^2 + 2
K.<w> = NumberField(minpoly)
Q2=x^5-x
qlist=[]
for p in primes(3, 10^5):
    F=K.ideal(p).factor()
    for I,h in list(F):
        q=I.norm()
        if q<10^5:
            qlist.append(q)
qcounted=[(q,qlist.count(q)) for q in uniq(qlist)]

D2=[]
for q,a in qcounted:
    g=nag2(q,Q2)
    if g is not None:
        for i in [1..a]:
            D2.append(g)
aa1=[D2[i][0] for i in [0..len(D2)-1]]
aa2=[D2[i][1] for i in [0..len(D2)-1]]

histogram(aa1, bins=25)
histogram(aa2, bins=25)
list_plot(D2, alpha=0.5)
```

Bibliography

[Ber97] Pierre Berthelot, *Finitude et pureté cohomologique en cohomologie rigide*, Invent. Math. **128** (1997), no. 2, 329–377, With an appendix in English by Aise Johan de Jong.

[BLGG11] Thomas Barnet-Lamb, Toby Gee, and David Geraghty, *The Sato-Tate conjecture for Hilbert modular forms*, J. Amer. Math. Soc. **24** (2011), no. 2, 411–469.

[CDV06] Wouter Castryck, Jan Denef, and Frederik Vercauteren, *Computing zeta functions of nondegenerate curves*, IMRP Int. Math. Res. Pap. (2006), Art. ID 72017, 57.

[Dwo60] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.

[Edi03] Bas Edixhoven, *Point counting after Kedlaya. EIDMA-Stieltjes Graduate course*, 2003.

[Eis95] David Eisenbud, *Commutative algebra. with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.

[Fit15] Francesc Fité, *Equidistribution, L-functions, and Sato-Tate groups*, Trends in Number Theory, Contemporary Mathematics, vol. 649, Amer. Math. Soc., Providence, RI, 2015, pp. 63–88.

[FKRS12] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), no. 5, 1390–1442.

[FvdP04] Jean Fresnel and Marius van der Put, *Rigid analytic geometry and its applications*, Progress in Mathematics, vol. 218, Birkhäuser Boston, Inc., Boston, MA, 2004.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52.

[Har07] David Harvey, *Kedlaya's algorithm in larger characteristic*, Int. Math. Res. Not. IMRN (2007), no. 22, Art. ID rnm095, 29.

[Har12] Michael C. Harrison, *An extension of Kedlaya's algorithm for hyperelliptic curves*, J. Symbolic Comput. **47** (2012), no. 1, 89–101.

[Har14] David Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Ann. of Math. (2) **179** (2014), no. 2, 783–803.

[HS14] David Harvey and Andrew V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 257–273.

[HSBT10] Michael Harris, Nick Shepherd-Barron, and Richard Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Ann. of Math. (2) **171** (2010), no. 2, 779–813.

[Ked01] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338, errata, ibid. **18** (2003), 417-418.

[Ked15] ———, *Sato-Tate groups of genus 2 curves*, Advances on Superelliptic Curves and Their Applications, NATO Science for Peace and Security Series - D: Information and Communication Security, vol. 41, IOS Press, 2015, p. 117.

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984.

[Mon71] Paul Monsky, *Formal cohomology III. Fixed point theorems*, Ann. of Math. (2) **93** (1971), 315–343.

[MW68] Paul Monsky and Gerard Washnitzer, *Formal cohomology I*, Ann. of Math. (2) **88** (1968), 181–217.

[Ser62] Jean-Pierre Serre, *Endomorphismes complètement continus des espaces de Banach p-adiques*, Inst. Hautes Études Sci. Publ. Math. (1962), no. 12, 69–85.

[Ser94] ———, *Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 377–400.

[Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[vdP86] Marius van der Put, *The cohomology of Monsky and Washnitzer*, Mém. Soc. Math. France (N.S.) (1986), no. 23, 4, 33–59, Introductions aux cohomologies p-adiques (Luminy, 1984).

[Wei48a] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041, Hermann et Cie., Paris, 1948.

[Wei48b] ———, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064, Hermann & Cie., Paris, 1948.

[Wei49] ———, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.