Arithmetic Zeta-Function

Gaurish Korpal[1]
gaurish.korpal@niser.ac.in

Summer Internship Project Report

[1] 4^{th} year Int. MSc. Student, National Institute of Science Education and Research, Jatni (Bhubaneswar, Odisha)

Certificate

Certified that the summer internship project report "Arithmetic Zeta-Function" is the bona fide work of "Gaurish Korpal", 4^{th} year Int. MSc. student at National Institute of Science Education and Research, Jatni (Bhubaneswar, Odisha), carried out under my supervision during June 4, 2018 to July 4, 2018.

Place: Mumbai
Date: July 4, 2018

Prof. C. S. Rajan
Supervisor
Professor,
Tata Institute of Fundamental Research,
Colaba, Mumbai 400005

Abstract

We will give an outline of the motivation behind the Weil conjectures, and discuss their application for counting points on projective smooth curves over finite fields.

Acknowledgements

Foremost, I would like to express my sincere gratitude to my advisor *Prof. C. S. Rajan* for his motivation. I am also thankful to *Sridhar Venkatesh*[1], *Rahul Kanekar*[2] and *Monalisa Dutta*[3] for the enlightening discussions.
Last but not the least, I would like to thank

- Donald Knuth for TEX
- Michael Spivak for $\mathcal{AMS}$-TEX
- Sebastian Rahtz for TEX Live
- Leslie Lamport for LATEX
- American Mathematical Society for $\mathcal{AMS}$-LATEX
- Hàn Thế Thành for pdfTEX
  - Heiko Oberdiek for `hyperref` package
  - Steven B. Segletes for `stackengine` package
  - David Carlisle for `graphicx` package
  - Javier Bezos for `enumitem` package
  - Hideo Umeki for `geometry` package
  - Peter R. Wilson & Will Robertson for `epigraph` package
  - Jeremy Gibbons, Taco Hoekwater and Alan Jeffrey for `stmaryrd` package
  - Lars Madsen for `mathtools` package
- Philipp Khl & Daniel Kirsch for Detexify (a tool for searching LATEX symbols)
- TeX.StackExchange community for helping me out with LATEX related problems

[1]M.Sc. student, Chennai Mathematical Institute
[2]B.Sc. student, Chennai Mathematical Institute
[3]Int. Ph.D. student, IISER Kolkata

Contents

Abstract **1**

Introduction **2**

1 Zeta-Functions **3**
1.1 Analytic zeta-functions . . . 3
1.1.1 Euler zeta-function . . . 3
1.1.2 Riemann zeta-function . . . 4
1.2 Algebraic zeta-function . . . 4
1.2.1 Dedekind zeta-function . . . 4
1.3 Zeta-function of curves over finite fields . . . 5
1.3.1 Artin zeta-function . . . 5
1.3.2 Schmidt zeta-function . . . 5
1.3.3 Hasse-Weil zeta-function . . . 6
1.4 Arithmetic zeta-function . . . 6
1.4.1 Rings of finite type . . . 6
1.4.2 $\mathbb{F}_p$-algebras of finite type . . . 10

2 An overview of Weil conjectures **13**
2.1 The statement of conjectures . . . 13
2.2 Riemann hypothesis for projective smooth curves over finite field . . . 14
2.3 Counting points on elliptic curve . . . 16

Conclusion **18**

Bibliography **19**

Introduction

Arithmetic zeta-function was introduced by Jean-Pierre Serre[4] in a lecture delivered in 1963, and was popularised by Alexander Grothendieck[5]. This function was the outcome of following elementary problem in number theory: how to count the number of solutions to systems of polynomial equations over finite fields. This problem was, in fact, the main motivation behind the famous Weil conjectures. These conjectures suggested a deep connection between the arithmetic of algebraic varieties defined over finite fields and the topology of algebraic varieties defined over the complex numbers [1]. The Weil conjectures constitute one of the central landmarks of modern algebraic geometry: they served as a driving force behind a striking number of fundamental advances in the field [7].

In the first chapter we will discuss two aspects of artihmetic zeta-function. Firstly, we will have a look at the motivation behind defining the aritmetic zeta-function, following the expositiory articles by Srinivas and Pranajape [5], and Osserman [7]. Secondly, we will look at some of the properties of arithmetic zeta-function, and how these properties take care of all the older definitions of zeta-function.

In the second chapter we will give an overview of Weil conjectures. We will first state the general conjecture. Then will look at the outline of the proof Riemann hypothesis for the case of projective non-singular absolutely irreducible curve over finite fields; following the last exercise of Hartshorne's textbook [1, Exercise C.5.7]. We will conclude this chapter by illustrating an application of Weil conjectures to count the points on an elliptic curve; following the expository article by Oort [6].

The lecture notes[6] by Edixhoven and Taelman [8] has been used as the main reference for this report.

[4]Serre, J-P. "Zeta and L-functions", in *Arithmetical Algebraic Geometry* (Proceedings of a Conference held at Purdue University, December 5-7, 1963), edited by O. F. G. Schilling, 82–92. New York: Harper and Row, 1965. (Available in: *Oeuvres - Collected Papers II*, Springer Collected Works in Mathematics of J-P. Serre, pp. 249–259 (2003).)

[5]A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L, Séminaire Bourbaki 279 (1964), 41-55.

[6]During this internship I read the first seven lectures from these notes. But, most of the content discussed in this report is from the first two lectures.

Chapter 1

Zeta-Functions

In this chapter we will look at the motivation behind defining the *arithmetic zeta-function*, and will also study some of its properties.

1.1 Analytic zeta-functions

The study of zeta function was started by Leonhard Euler in the first half of the eighteenth century. He computed the values at even positive integers, and the first of them, $\zeta(2)$, provides a solution to the Basel problem. The values at negative integer points, also found by Euler, are rational numbers and play an important role in the theory of modular forms.

1.1.1 Euler zeta-function

For a given real number $k > 1$, consider the series

$$\sum_{n=1}^{\infty} \frac{1}{n^k} = 1 + \frac{1}{2^k} + \frac{1}{3^k} + \dots$$

Note that the series $\sum_{n=1}^{\infty} n^{-k}$ is uniformly convergent for $a \leq k \leq b$, if $1 < a < b$. Now let $s = \sigma + it$ be a complex number, then

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

converges for $\sigma > 1$ and is called the *Euler zeta-function* [10, §1.3.1]. Moreover, since the series $\sum_{n=1}^{\infty} n^{-s}$ is uniformly convergent throughout any finite region in which $\sigma \geq a > 1$, the function $\zeta(s)$ is continuous at all points of the region $\sigma > 1$.

Next, consider the product

$$\prod_p \left(1 - \frac{1}{p^s}\right)$$

where p runs through the primes $2, 3, 5, \dots$. This product is uniformly convergent in any finite region throughout which $\sigma > 1$, and one can prove that [10, §1.3.2]

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \sigma > 1$$

Moreover, since a convergent infinite product of non-zero factors is non-zero, we can conclude that $\zeta(s)$ has no zeros for $\sigma > 1$.

1.1.2 Riemann zeta-function

In 1859, Bernhard Riemann, in his remarkable 8-page paper, extended the Euler definition to whole of complex plane by its meromorphic continuation (with pole at $s = 1$)

$$\zeta(s) = \frac{e^{-i\pi s}\Gamma(1-s)}{2\pi i}\int_C \frac{w^{s-1}}{e^w - 1}dw$$

where the contour C starts at infinity on the positive real axis, encircles the origin once in the positive direction, excluding the points $\pm 2i\pi, \pm 4i\pi, \ldots$ and returns to positive infinity [10, §1.3.4]. He also found its functional equation

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

from which we can conclude that the only zeros of $\zeta(s)$ for $\sigma < 0$ are at the poles of $\Gamma\left(\frac{s}{2}\right)$, except 0 since it's a simple pole of $\zeta(1-s)$. So, the points $s = -2, -4, -6, \ldots$ are called the *trivial zeros* of $\zeta(s)$. The remainder of the plane, where $0 \leq \sigma \leq 1$, is called the *critical strip*. Moreover, in 1893, Jacques Hadamard proved that $\zeta(s)$ has infinitely many non-trivial zeros in the critical strip $0 \leq \sigma \leq 1$ [10, §1.3.5].

The famous Riemann hypothesis is that any non-trivial zero of $\zeta(s)$ has $\sigma = 1/2$. The location of zeros of Riemann zeta-function in the critical strip, also plays an important role in the proof of *prime number theorem* [10, §1.7.2].

1.2 Algebraic zeta-function

In 1877, Dedekind began generalizing some of Lejeune Dirichlet's work to number fields. His first paper was *Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers*. It appears that Erich Hecke named the Dedekind zeta-function after him[1].

1.2.1 Dedekind zeta-function

The Dedekind zeta-function ζ_K of a number field K is defined for $\sigma > 1$ by the Dirichlet series

$$\zeta_K(s) = \sum_{n=1}^{\infty}\frac{j_n}{n^s}$$

where j_n denotes the number of ideals $\mathfrak{a}$ of $\mathcal{O}_K$ with $|\mathcal{O}_K/\mathfrak{a}| = n$. One can also prove that ζ_K is analytic on the half-plane $\sigma > 1$. Moreover, the absolute convergence of the above series also justifies that

$$\zeta_K(s) = \sum_{\mathfrak{a}\subset\mathcal{O}_K}\frac{1}{|\mathcal{O}_K/\mathfrak{a}|^s} \quad \text{for } \sigma > 1$$

This last representation of ζ_K suggests writing

$$\zeta_K(s) = \prod_{\mathfrak{p}\subset\mathcal{O}_K}\left(1 - \frac{1}{|\mathcal{O}_K/\mathfrak{p}|^s}\right)^{-1} = \prod_{\mathfrak{p}\subset\mathcal{O}_K}\frac{1}{1-|\mathcal{O}_K/\mathfrak{p}|^{-s}}$$

due the property of unique factorization of ideals and multiplicative property of order of ideals [2, Theorem 22(a)]. Hence we can recover the original zeta-function for $K = \mathbb{Q}$.

As in the case of Riemann zeta-function, ζ_K can be extended to a meromorphic function on the half-plane $\sigma > 1 - \frac{1}{[K:\mathbb{Q}]}$, analytic everywhere except $s = 1$ where it has a simple pole.

[1] source: http://www.lmfdb.org/knowledge/show/lfunction.history.dedekind

In contrast to the situation for Riemann zeta-function, the functional equation for Dedekind zeta-function remained open until 1917, when it was settled by Hecke, who showed at the same time that Dedekind zeta-function could be extended to the complex plane, thereby ensuring that the Riemann hypothesis makes sense for them as well.

We can use the Dedekind zeta-function to obtain a formula for the number of ideal classes in $\mathcal{O}_K$, called the *class number formula* [2, Theorem 44].

1.3 Zeta-function of curves over finite fields

Emil Artin first introduced zeta functions and the Riemann hypothesis for certain curves over finite fields in his 1923 thesis, noting that the ring of polynomial functions on such a curve shares precisely the properties of rings of integers which Dedekind used to define his zeta functions. While in the number field case one can think of the zeta function as counting primes, in the case of a function field the zeta function may be expressed in terms of the more geometric data of counting points on the given curve [7, §1].

1.3.1 Artin zeta-function

Artin studied a certain class of curves in plane. Here, the plane means $\mathbb{F}_q^2$, where $\mathbb{F}_q$ is the finite field having q elements, and a curve C is simply the set of zeros of a polynomial $f(x, y) \in \mathbb{F}_q[x, y]$. In general, if F is any filed containing $\mathbb{F}_q$ then we define the curve corresponding to the polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ in the larger plane F^2 as

$$C(F) = \{(x, y) \in F^2 : f(x, y) = 0\}$$

If F is a finite field, then $F = F_{q^m}$ for $m \geq 1$ and $C(F)$ is finite. For $m \geq 1$ define $N_m(C)$ to be the number of points in the curve $C(\mathbb{F}_{q^m})$. The sequence $N_1(C), N_2(C), N_3(C), \ldots$ is what we wish to study.

The next step is along the lines of generating functions [5]. We define the zeta-function

$$Z_C(t) = \exp\left(\sum_{m=1}^{\infty} N_m(C)\frac{t^m}{m}\right)$$

For $t = q^{-s}$, the above definition coincides with the expression we would obtain using Dedekind zeta-function for the coordinate ring $\mathbb{F}_q[x, y]/\langle f(x, y)\rangle$. We will prove this equivalence later in this chapter.

1.3.2 Schmidt zeta-function

In a 1931 paper, Friedrich Karl Schmidt generalized Artin's work to all curves over finite fields, and exploited the geometry to prove a strong form of the functional equation for such zeta functions. The nicest form of Schmidt's theorem involves restricting to smooth projective curves [7, §2]. Schmidt proved that for a smooth projective curve C over $\mathbb{F}_q$ of genus g, we have

$$Z_C(t) = \frac{P(t)}{(1-t)(1-qt)}$$

where $P(t) \in \mathbb{Z}[t]$ with degree $2g$. Shortly thereafter, in a 1933 paper Helmut Hasse was able to prove the Riemann hypothesis in the special case of elliptic curves over finite fields.

The Riemann hypothesis for C is then the statement that the roots of $Z_C(q^{-s})$ all have $\sigma = 1/2$, or equivalently,

$$|N_m(C) - q^m - 1| \leq 2g\sqrt{q^m}$$

for all $m \geq 1$. We will prove this equivalence in the next chapter.

1.3.3 Hasse-Weil zeta-function

In 1940 and 1941, André Weil gave outline of two proofs of the Riemann hypothesis for curves over finite fields. Then Weil wrote his *Foundations of Algebraic Geometry*, which appeared in 1948, and in it he made the two proofs, outlined earlier, rigorous. The following year[2] Weil went further, studying zeta functions $Z_V(t)$ associated with higher-dimensional varieties V over finite fields, and taking as his definition the formula

$$Z_V(t) = \exp\left(\sum_{m=1}^{\infty} N_m(V)\frac{t^m}{m}\right)$$

While the situation is more complicated in this context, the behavior conjectured by Weil was nonetheless strikingly similar, an utterly natural extension of the case of curves. We will state these Weil conjectures in the next chapter.

Weil's generalization was motivated by the following two observations:

1. Hasse's proof of Riemann hypothesis for elliptic curves over finite field exploited the properties of *Frobenius automorphism*. Let F be a finite field containing $\mathbb{F}_{q^m}$ and $t \in F$, then $t^{q^m} = t$ if and only if $t \in \mathbb{F}_{q^m}$ [4, §14.3]. Now consider the *Frobenius map*

$$\begin{aligned} \sigma_{q^m} : F^2 &\to F^2 \\ (x, y) &\mapsto (x^{q^m}, y^{q^m}) \end{aligned}$$

   This is a bijective map with the $\mathbb{F}_{q^m}^2$ as the set of fixed points. As assumed by Artin, let C be a curve defined by $f(x, y) \in \mathbb{F}_q[x, y]$. Since $\mathbb{F}_{q^m} \supset \mathbb{F}_q$, it follows that [4, Exercise 13.5.8]

$$f(x, y) = 0 \quad \iff \quad f(\sigma_{q^m}(x, y)) = 0$$

   So we see that σ_{q^m} gives a map from C to itself. Thus, to study $N_m(C)$ it is enough to analyse the fixed points of Frobenious map on C.

2. In 1926, Solomon Lefschetz gave a "trace formula" that could count the number of fixed points of a continuous mapping from a compact manifold to itself, in terms of the action of the map on the associated singular cohomology spaces.

Forgetting for the moment that σ_{q^m} only makes sense over finite fields, if we imagine that C was defined over the complex numbers, then by using the complex topology we could study the fixed points of σ_{q^m} by the Lefschetz fixed-point theorem, obtaining a formula in terms of the action of σ_{q^m} on the cohomology groups.

1.4 Arithmetic zeta-function

In this section we formulate the modern definition[3] of zeta-function which takes care of the all the cases discussed above.

1.4.1 Rings of finite type

Definition 1 (Ring of finite type)**.** Let R be a commutative ring with identity. Let $S \subset R$ such that for all rings $R' \subset R$ with $S \subset R'$ we have $R' = R$. Then S is called the *generating subset of* R and the ring R is said to be of *finite type* if the set S is finite.

[2] A. Weil, "Numbers of solutions of equations in finite fields", Bull. Amer. Math. Soc. 55 (1949), 497–508.

[3] This definition should in terms of scheme of finite type over the integers. But since I don't have knowledge of schemes, I will state using a slightly different terminology [8].

Example 1. Some examples of rings of finite type:

1. $\mathbb{Z}$ (take $S = \emptyset$);
2. Any finite ring (take $S = R$);
3. If R is a ring of finite with generating set S, then $R[X]$ is also a ring of finite type with the generating set $S \cup \{X\}$;
4. If R is a ring of finite type with generating set S and $\mathfrak{a} \subset R$ is an ideal, then $R/\mathfrak{a}$ is also a ring of finite type with the generating set $\{\overline{s} : s \in S\}$ where $\overline{s}$ denotes the image of s in $R/\mathfrak{a}$.

Example 2. Some examples of rings which are not of finite type:

1. The ring $\mathbb{Z}[X_1, X_2, \ldots]$ is not of finite type. We can prove this claim as follows: On the contrary, let $S = \{X_{i_1}, X_{i_2}, \ldots, X_{i_k}\}$ be the finite set of variables occuring in the polynomials in S. Then S is contained in the proper subring $\mathbb{Z}[X_{i_1}, X_{i_2}, \ldots, X_{i_k}]$ of $\mathbb{Z}[X_1, X_2, \ldots]$ contradicting the fact that S was a generating set.
2. $\mathbb{Q}$ is not of finite type. We can prove this claim as follows: On the contrary, let S be a finite generating set, and N be the least common multiple of the denominators of the elements of S. Take $R' = \mathbb{Z}[1/N] = \{a/N^b : a \in \mathbb{Z}, b \in \mathbb{N}\}$. Then $S \subset R' \subsetneq \mathbb{Q}$, contradicting the fact that S was a generating set.

Remark 1. The above definition is equivalent to saying that R is a finitely generated $\mathbb{Z}$-algebra, i.e. R is a quotient of $\mathbb{Z}[X_1, \ldots, X_n]$ for some n.

Lemma 1 (Artin-Tate lemma)**.** *Let $A \subseteq B \subseteq C$ be rings. Suppose that A is Noetherian. If C is finitely generated as an A-algebra and C is finitely generated as a B-module, then B is finitely generated as an A-algebra.*

Proof. Let $x_1, \ldots, x_m$ generate C as an A-algebra, and $y_1, \ldots, y_n$ generate C as a B-module. Then there exist expressions of the form

$$x_i = \sum_j b_{ij} y_j \quad (b_{ij} \in B) \tag{1.1}$$

$$y_i y_j = \sum_k b_{ijk} y_k \quad (b_{ijk} \in B) \tag{1.2}$$

Let B_0 be the algebra generated over A by b_{ij} and b_{ijk}. Since A is Noetheiran, so is B_0 by Hilbert Basis Theorem [3, Theorem 7.7], and $A \subseteq B_0 \subseteq B$.

Any element of C is a polynomial in the x_i with coefficients in A. Substituting (1.1) and making repeated use of (1.2) shows that each element of C is a linear combination of the y_i with coefficients in B_0, and hence C is finitely generated as a B_0-module. Since B_0 is Noetherian, and C is a finitely generated B_0-module, it follows that C is Noetherian [3, Proposition 6.5]. Since C is a Noetherian B_0-module, it follows that B is finitely generated as a B_0-module [3, Proposition 6.2]. Since B_0 is finitely generated as an A-algebra, it follows that B is finitely generated as an A-algebra. □

Lemma 2 (Zariski's lemma)**.** *Let k be a field and let another field K be a finitely generated k-algebra. Then K is a finite algebraic extension of k.*

Proof. Let $K = k[x_1, \ldots, x_n]$. If K is not algebraic over k then we can re-number the x_i's so that $x_1, \ldots, x_r$ are algebraically independent over k, where $r \geq 1$, and each of $x_{r+1}, \ldots, x_n$ is algebraic over the field $F = k(x_1, \ldots, x_r)$. Hence K is a finite algebraic extension of F and

therefore finitely generated as a F-module. Applying Lemma 1 to $k \subseteq F \subseteq K$, it follows that F is a finitely generated k-algebra, say $F = k[y_1, \ldots, y_s]$. Each y_i is of the form f_i/g_i where f_i and g_i are polynomial is $x_1, \ldots, x_r$.

Note that there are infinitely many irreducible polynomials in the ring $k[x_1, \ldots, x_r]$ (just like there are infinite primes in $\mathbb{Z}$). Hence there is an irreducible polynomial h which is prime to each of the g_i, for $i = 1, \ldots, s$, say $h = g_1 g_2 \cdots g_s + 1$. Then the element $h^{-1} \in F$ is not a polynomial in y_i's. This contradicts the fact that $F = k[y_1, \ldots, y_s]$. Hence, K is algebraic over k, and therefore a finite algebraic extension. □

Remark 2. There is also a direct proof by Zariski [3, Exercise 5.18]. In fact, the characterization theorem for Jacobson rings contains Zariski's lemma as a special case [3, Exercise 5.25].

Moreover, this lemma is also a consequence of the Noether normalization lemma [13, Theorem 2.2]. Indeed, by the normalization lemma, K is a finitely generated module over the polynomial ring $k[x_1, \ldots, x_d]$ where $x_1, \ldots, x_d$ are elements of K that are algebraically independent over k. But since K has Krull dimension zero and since an integral ring extension preserves Krull dimensions, the polynomial ring must have dimension zero; i.e., $d = 0$.

Corollary 1 (Weak Nullstellensatz)**.** *Let k be a field, R be a finitely generated k-algebra. Let $\mathfrak{m}$ be a maximal ideal of R. Then the field $R/\mathfrak{m}$ is a finite algebraic extension of k.*

Proof. Take $K = R/\mathfrak{m}$ in Zariski's lemma. □

Remark 3. In particular, if k is algebraically closed then $R/\mathfrak{m} \cong k$. One can directly prove the weak form of Hilbert's nullstellensatz using Noether normalization lemma [3, Exercise 5.17].

Theorem 1. *Let R be a ring of finite type which is a field. Then R is a finite field.*

Proof. It is sufficient to prove that R can't have characteristic 0. On the contrary, let R be a field of characteristic 0. Then the prime subfield of R is isomorphic to $\mathbb{Q}$ [4, §13.1], and we have $\mathbb{Z} \subset \mathbb{Q} \subseteq R$. Since R is of finite type, it's a finitely generated $\mathbb{Z}$-algebra, and hence R is a finitely generated $\mathbb{Q}$-algebra. Applying Lemma 2 to R we get that R is a finitely generated $\mathbb{Q}$-module. But then Lemma 1 implies that $\mathbb{Q}$ is a finitely generated $\mathbb{Z}$-algebra. But, as seen in Example 2, this is not possible. If we had $\mathbb{Q} = \mathbb{Z}\left[\frac{m_1}{n_1}, \ldots, \frac{m_k}{n_k}\right]$, we could as well write $\mathbb{Q} = \mathbb{Z}[1/N]$ where $N = \operatorname{lcm}(n_1, \ldots, n_k)$. But then $1/q \in \mathbb{Q}$, for prime q not dividing N, can't be written as a polynomial in $1/N$.

Therefore, R must be of characteristic $p > 0$, i.e. a finitely generated $\mathbb{F}_p$-algebra. Then by Lemma 2 we get that $R = \mathbb{F}_{p^r}$ for some $r \geq 1$. □

Corollary 2 (Nullstellensatz over $\mathbb{Z}$)**.** *Let R be a ring of finite type and $\mathfrak{m} \subset R$ a maximal ideal. Then the quotient $R/\mathfrak{m}$ is a finite field.*

Proof. Use Corollary 1. □

Definition 2 (Arithmetic zeta-function)**.** Let R be a ring of finite type. The *zeta-function* of R is defined as

$$\zeta_R(s) = \prod_{\mathfrak{m} \subset R} \frac{1}{1 - |R/\mathfrak{m}|^{-s}}$$

for $s \in \mathbb{C}$ with $\operatorname{Re}(s)$ sufficiently large, and product taken over all maximal ideals of R.

Remark 4. We assume that there exists a $\rho \in \mathbb{R}$ such that $\zeta_R(s)$ converges absolutely for $\operatorname{Re}(s) > \rho$. Moreover, from now onwards we will manipulate certain products and series without carefully looking at convergence. We will implicitly assume that these manipulations are done in the domain of absolute convergence.

Example 3. We can recover the earlier definitions of zeta-functions as follows:

1. $\zeta_{\mathbb{Z}}(s) = \zeta(s)$ ($\mathbb{Z}$ is a principal ideal domain, hence every prime ideal is maximal)
2. $\zeta_{\mathcal{O}_K}(s) = \zeta_K(s)$ ($\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-algebra [2, Theorem 2] and a Dedekind domain [2, Theorem 14])

Proposition 1. *Let R_1 and R_2 be rings of finite type. Then $R_1 \times R_2$ is of finite type and $\zeta_{R_1 \times R_2}(s) = \zeta_{R_1}(s)\zeta_{R_2}(s)$.*

Proof. Let S_1 and S_2 be the finite generating set of R_1 and R_2, respectively. Then $S_1 \times S_2$ is the finite generating set of $R_1 \times R_2$. To prove the zeta-function formula, it is sufficient to prove that the maximal ideals of $R_1 \times R_2$ are either of the form $\mathfrak{m}_1 \times R_2$, where $\mathfrak{m}_1$ is maximal ideal in R_1, or of the form $R_1 \times \mathfrak{m}_2$, where $\mathfrak{m}_2$ is maximal ideal in R_2.

Let $\mathfrak{m}$ be a maximal ideal in $R_1 \times R_2$, then $(R_1 \times R_2)/\mathfrak{m}$ is a field. Suppose $\mathfrak{m}$ contains neither all of $R_1 \times \{0\}$ nor $\{0\} \times R_2$. Then we could pick non-zero elements $(r_1, 0) \in R_1 \times \{0\}$ and $(0, r_2) \in R_2 \times \{0\}$, neither of which is in $\mathfrak{m}$, and then $((r_1, 0) + \mathfrak{m})((0, r_2) + \mathfrak{m}) = (0, 0) + \mathfrak{m}$. But since a field does not contain zero-divisors, $\mathfrak{m}$ must contain all of R_1 or all of R_2. Using the fact an ideal is maximal if and only if the quotient ring is a field, we conclude that that the ideal $\mathfrak{m}$ is of the required form.

Hence we have

$$\begin{aligned}
\zeta_{R_1 \times R_2}(s) &= \prod_{\mathfrak{m} \subset R_1 \times R_2} \frac{1}{1 - |R_1 \times R_2/\mathfrak{m}|^{-s}} \\
&= \left(\prod_{\mathfrak{m}_1} \frac{1}{1 - |R_1 \times R_2/\mathfrak{m}_1 \times R_2|^{-s}} \right) \left(\prod_{\mathfrak{m}_2} \frac{1}{1 - |R_1 \times R_2/R_1 \times \mathfrak{m}_2|^{-s}} \right) \\
&= \zeta_{R_1}(s)\zeta_{R_2}(s)
\end{aligned}$$

□

Remark 5 (Riemann hypothesis for rings of finite type)**.** Let R be a ring of finite type. Then $s \mapsto \zeta_R(s)$ extends to a meromorphic function on $\mathbb{C}$, and for every $s \in \mathbb{C}$ at which ζ_R has a pole or a zero we have $2\mathrm{Re}(s) \in \mathbb{Z}$.

For $R = \mathbb{Z}$ this conjecture is equivalent to the Riemann hypothesis, as the zeros and poles of ζ with $\mathrm{Re}(s) > 1$ or $\mathrm{Re}(s) < 0$ are known.

Proposition 2. *Let R be a ring of finite type, then*

$$\zeta_R(s) = \prod_{p \in \mathbb{Z}_{>0}} \zeta_{R/\langle p \rangle}(s)$$

where p is a positive prime integer.

Proof. Let $\mathfrak{m} \subset R$ be a maximal ideal of R. Then Corollary 2 implies that $R/\mathfrak{m}$ is a finite field, hence it has a finite characteristic $p > 0$. This gives us the element $p = \sum_{i=1}^{p} 1 \in \mathfrak{m}$. Moreover, by fourth isomorphism theorem [4, Theorem 7.8(3)] we have the following bijection, where we only consider the maximal ideals :

$$\begin{aligned}
\{\mathfrak{m} \subset R : p \in \mathfrak{m}\} &\overset{1:1}{\longleftrightarrow} \{\mathfrak{m}' \subset R/\langle p \rangle\} \\
\mathfrak{m} &\longmapsto \mathfrak{m}/\langle p \rangle \\
\mathfrak{m}' + \langle p \rangle &\longmapsfrom \mathfrak{m}'
\end{aligned}$$

Also, by third isomorphism theorem [4, Theorem 7.8(2)] we have:

$$R/\mathfrak{m} \cong \frac{R/\langle p \rangle}{\mathfrak{m}/\langle p \rangle}$$

hence $|R/\mathfrak{m}| = |R/\langle p \rangle/\mathfrak{m}/\langle p \rangle|$. □

Example 4. We can now define zeta-function for various rings:

1. Let $R = \mathbb{F}_q$, then
$$\zeta_{\mathbb{F}_q}(s) = \frac{1}{1-q^{-s}}$$

2. Let n be a positive integer and $R = \mathbb{Z}/n\mathbb{Z}$. We have $n = p_1^{r_1} p_2^{r_2} \cdots p_\ell^{r_\ell}$ for some distinct primes $p_1, p_2, \ldots, p_\ell$. Then the maximal ideals of R are $p_i\mathbb{Z}/n\mathbb{Z}$ and $|R/\mathfrak{m}| = p_i$ for all i.
$$\zeta_{\mathbb{Z}/n\mathbb{Z}}(s) = \prod_{\substack{p \in \mathbb{Z}_{>0} \\ p|n}} \frac{1}{1-p^{-s}}$$

3. Let $R = \mathbb{Z}[X]/\langle X^n \rangle$. Recall that the maximal ideals of $\mathbb{Z}[X]$ are of the form $\langle p, f \rangle$ where p is a prime integer and f is a monic integral polynomial irreducible modulo p [13, Theorem 2.1]. Hence the maximal ideals of R are $\langle p, X \rangle / \langle X^n \rangle$ for all $p \in \mathbb{Z}_{>0}$, and we get
$$\zeta_{\mathbb{Z}[X]/\langle X^n \rangle}(s) = \prod_p \frac{1}{1-p^{-s}} = \zeta(s)$$

1.4.2 $\mathbb{F}_p$-algebras of finite type

Definition 3 ($\mathbb{F}_p$-algebra)**.** A ring R in which $p = \sum_{i=1}^{p} 1 = 0$ has the property that the ring homomorphism $\mathbb{Z} \to R$ factors as $\mathbb{Z} \to \mathbb{F}_p \to R$. Such rings are called $\mathbb{F}_p$-algebras.

Remark 6. Proposition 2 allows us to express the zeta-function of a ring of finite type as a product of zeta functions of $\mathbb{F}_p$-algebras.

Definition 4 (Special arithmetic zeta-function)**.** For p prime and R an $\mathbb{F}_p$-algebra of finite type, we define $Z_R(t)$ as follows:
$$Z_R(t) = \prod_{\mathfrak{m} \subset R} \frac{1}{1-t^{\deg(\mathfrak{m})}} \in \mathbb{Z}[[t]]$$
where $\deg(\mathfrak{m}) = [R/\mathfrak{m} : \mathbb{F}_p]$.

Proposition 3. *For p prime and R be an $\mathbb{F}_p$-algebra of finite type, then:*
$$\zeta_R(s) = Z_R(p^{-s})$$

Proof. We note that $R/\mathfrak{m} \cong \mathbb{F}_{p^r}$ for some $r \geq 1$, and $r = \deg(\mathfrak{m})$.
$$\zeta_R(s) = \prod_{\mathfrak{m} \subset R} \frac{1}{1-|R/\mathfrak{m}|^{-s}} = \prod_{\mathfrak{m} \subset R} \frac{1}{1-|\mathbb{F}_{p^r}|^{-s}} = \prod_{\mathfrak{m} \subset R} \frac{1}{1-(p^r)^{-s}} = \prod_{\mathfrak{m} \subset R} \frac{1}{1-(p^{-s})^r} = Z_R\left(p^{-s}\right)$$
□

Definition 5 (Logarithm of formal power series)**.** The logarithm of power series is defined as the map
$$\begin{aligned} \log : 1 + x\mathbb{Q}[[x]] &\longrightarrow \quad \mathbb{Q}[[x]] \\ 1 - a &\longmapsto -\sum_{n>0} \frac{a^n}{n} \end{aligned}$$

Remark 7. The sum defined above converges to a formal power series since x divides a, and only finitely many terms contribute to the coefficient of x^n in $\log(1-a)$. Moreover, the logarithm defines a group homomorphism from the multiplicative group $1+x\mathbb{Q}[[x]]$ to the additive group $\mathbb{Q}[[x]]$.

Lemma 3. *Consider the tower of finite fields $\mathbb{F}_p \subseteq \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. Then $|\operatorname{Hom}(\mathbb{F}_{p^d}, \mathbb{F}_{p^n})| = d$.*

Proof. Let $\varphi : \mathbb{F}_{p^d} \to \mathbb{F}_{p^n}$ be a ring homomorphism. Then φ is injective since $\mathbb{F}_{p^d}$ is a field [3, Proposition 1.2]. Moreover, $\operatorname{Im}(\varphi)$ is a subring of the finite field $\mathbb{F}_{p^n}$, hence is an integral domain. Since any finite integral domain is a field [4, Corollary 7.3], $\operatorname{Im}(\varphi) \subseteq \mathbb{F}_{p^n}$ is a subfield. Therefore, $\operatorname{Im}(\varphi)$ is isomorphic to a finite field of order p^d by the first isomorphism theorem [4, Theorem 7.7]. Hence, every ring homomorphism is actually an automorphism, i.e. $\operatorname{Hom}(\mathbb{F}_{p^d}, \mathbb{F}_{p^n}) = \operatorname{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p)$. Also, we know that the extension of finite fields $\mathbb{F}_{p^d}/\mathbb{F}_p$ is Galois [4, Corollary 14.6], hence $|\operatorname{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p)| = [\mathbb{F}_{p^d} : \mathbb{F}_p] = d$. □

Theorem 2. *For p prime and R an $\mathbb{F}_p$-algebra of finite type, then*

$$\log Z_R(t) = \sum_{n=1}^{\infty} \nu_n(R) \frac{t^n}{n}$$

where $\nu_n(R) = |\operatorname{Hom}(R, \mathbb{F}_{p^n})|$, i.e. the number of ring homomorphisms from R to $\mathbb{F}_{p^n}$.

Proof. Firstly, we have the following bijection involving ring homomorphisms and maximal ideals:

$$\begin{aligned}
\operatorname{Hom}(R, \mathbb{F}_{p^n}) &\overset{1:1}{\longleftrightarrow} \{(\mathfrak{m}, \alpha) : \alpha \in \operatorname{Hom}(R/\mathfrak{m}, \mathbb{F}_{p^n})\} \\
\beta &\longmapsto (\ker(\beta), \overline{\beta}) && \text{where } \overline{\beta} : R/\ker(\beta) \to \mathbb{F}_{p^n} \\
\widetilde{\alpha} &\longmapsfrom (\mathfrak{m}, \alpha) && \text{where } \widetilde{\alpha} : R \to R/\mathfrak{m} \xrightarrow{\alpha} \mathbb{F}_{p^n}
\end{aligned}$$

where $\ker(\beta)$ is a maximal ideal since $R/\ker(\beta)$ is isomorphic to some subfield of $\mathbb{F}_{p^n}$ [4, Corollary 7.3, Theorem 7.7].

Now, let $\mathfrak{m}$ be a maximal ideal of R. Note that $R/\mathfrak{m} \cong \mathbb{F}_{p^{\deg(\mathfrak{m})}}$, and $\mathbb{F}_{p^{\deg(\mathfrak{m})}}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if $\deg(\mathfrak{m})$ divides n [4, Theorem 13.14]. Hence, by Lemma 3, $|\operatorname{Hom}(R/\mathfrak{m}, \mathbb{F}_{p^n})| = \deg(\mathfrak{m})$ if $\deg(\mathfrak{m})$ divides n, and is zero otherwise. This gives us:

$$\nu_n(R) = \sum_{d|n} d \cdot |\{\mathfrak{m} \subset R : \deg(\mathfrak{m}) = d\}| \tag{1.3}$$

Let's now use the definition of $Z_R(t)$ and log to simplify the left hand side:

$$\begin{aligned}
\log Z_R(t) &= \log \prod_{\mathfrak{m} \subset R} \frac{1}{1 - t^{\deg(\mathfrak{m})}} \\
&= \sum_{\mathfrak{m} \subset R} \log \frac{1}{1 - t^{\deg(\mathfrak{m})}} \\
&= \sum_{\mathfrak{m} \subset R} \sum_{j=1}^{\infty} \frac{t^{j \deg(\mathfrak{m})}}{j} \\
&= \left(t^{\deg(\mathfrak{m}_1)} + \frac{t^{2\deg(\mathfrak{m}_1)}}{2} + \dots \right) + \left(t^{\deg(\mathfrak{m}_2)} + \frac{t^{2\deg(\mathfrak{m}_2)}}{2} + \dots \right) + \dots
\end{aligned}$$

Note that the numerator of the coefficients of t^n is $|\{\mathfrak{m} \subset R : \deg(\mathfrak{m}) = d\}|$ where $d|n$. Hence we have:

$$\log Z_R(t) = \sum_{n=1}^{\infty} \left(\sum_{d|n} d \cdot |\{\mathfrak{m} \subset R : \deg(\mathfrak{m}) = d\}| \right) \frac{t^n}{n}$$

Now using (1.3) we get:

$$\log Z_R(t) = \sum_{n=1}^{\infty} \nu_n(R) \frac{t^n}{n}$$

□

Proposition 4. *For p prime and $R = \mathbb{F}_p[X_1, \ldots, X_r]/\mathfrak{a}$ with $\mathfrak{a}$ the ideal generated by polynomials $f_1, \ldots, f_m$. Then*

$$\nu_n(R) = \left|\{(x_1, \ldots, x_r) \in \mathbb{F}_{p^n}^r : f_j(x_1, \ldots, x_r) = 0 \text{ for } j = 1, 2, \ldots, m\}\right|$$

Proof. Let $\varphi : R \to \mathbb{F}_{p^n}$ be a ring homomorphism. Note that the ring homomorphism is completely determined by its values at the generators X_i. Suppose a ring homomorphism sends X_i to $x_i \in \mathbb{F}_{p^n}$. Since a ring homomorphism sends 0 to 0, it follows that $f_j(x_1, \ldots, x_r) = 0$ in $\mathbb{F}_{p^n}$ for all j. On the other hand, if we have $(x_1, \ldots, x_r) \in \mathbb{F}_{p^n}^r$ such that $f_j(x_1, \ldots, x_r) = 0$ for all j, the ring homomorphism from $\mathbb{F}_p[X_1, , \ldots, X_r]$ to $\mathbb{F}_{p^n}$ that sends X_i to x_i, factors through R. Hence we get

$$\begin{aligned}\nu_n(R) &= |\operatorname{Hom}(R, \mathbb{F}_{p^n})| \\ &= \left|\{(x_1, \ldots, x_r) \in \mathbb{F}_{p^n}^r : f_j(x_1, \ldots, x_r) = 0 \text{ for } j = 1, 2, \ldots, m\}\right|\end{aligned}$$

That is, $\nu_n(R)$ is the size of the vanishing set of the ideal $\mathfrak{a}$. □

Example 5. Let q be a prime power and $R = \mathbb{F}_q[X, Y]/\langle XY - 1\rangle$. Then, since R is a $\mathbb{F}_p$-algebra of finite type, we have:

$$\log Z_R(t) = \sum_{m=1}^{\infty} N_m(C) \frac{t^m}{m}$$

where C is the vanishing set of the polynomial $XY - 1$ in the $\mathbb{F}_{q^m}^2$ plane, and $N_m(C) = \left|\{(x_1, x_2) \in \mathbb{F}_{q^m}^2 : x_1 x_2 = 1\}\right|$. Hence $N_m(C)$ is equal to the number of elements of $\mathbb{F}_{q^m}$ with multiplicative inverse, i.e. $N_m(C) = q^m - 1$. Hence we get:

$$\begin{aligned}\log Z_R(t) &= \sum_{m=1}^{\infty} \frac{(q^m - 1)t^m}{m} \\ &= \sum_{m=1}^{\infty} \frac{(qt)^m}{m} - \sum_{m=1}^{\infty} \frac{t^m}{m} \\ &= -\log(1 - qt) + \log(1 - t) \\ &= \log \frac{1 - t}{1 - qt}\end{aligned}$$

Hence we have $Z_R(t) = 1 - t/1 - qt$. Compare the result with the discussion in subsection 1.3.1 and subsection 1.3.2.

Chapter 2

An overview of Weil conjectures

In 1949, André Weil gave conjectures concerning the number of solutions of polynomial equations over finite field. While one might ultimately be more interested in solutions over the field of rational numbers, the problem of finding solutions is far more tractable over finite fields, and local-global principles [9] establish subtle relationships between the two cases.

2.1 The statement of conjectures

As seen in subsection 1.3.3, let V be any higher dimensional variety over finite fields, and the zeta-function be defined as

$$Z_V(t) = \exp\left(\sum_{m=1}^{\infty} N_m(V)\frac{t^m}{m}\right)$$

where $N_m(V)$ is the number of points in the variety V over $\mathbb{F}_{q^m}$. Then the following four conjectures were made:

1. *Rationality*: $Z_V(t)$ is a rational function of t.
2. *Factorization*: If $n = \dim V$, then we can write

$$Z_V(t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}$$

   Moreover, if V is the reduction modulo p of a variety $\tilde{V}$ defined over a subfield of $\mathbb{C}$, then $b_j = \deg P_j(t)$ is the j^{th} Betti number of $\tilde{V}$ using the usual topology.
3. *Functional equation*: The roots of $P_j(t)$ are interchanged with the roots of $P_{2n-j}(t)$ under the substitution $t \mapsto 1/q^n t$.
4. *Riemann hypothesis*: Each root of each $P_j(t)$ is a complex number of norm $q^{-j/2}$.

In 1960, using p-adic analysis, Bernard Dwork was able to prove the rationality of zeta-function. Later, in 1962, all the conjectures except Weil's Riemann hypothesis followed from the formulation of the suitable cohomology theory so that the Lefschetz theorem could be applied. One such theory was Alexander Grothendieck's *étale cohomology*, developed in collaboration with Michael Artin. However, Weil's Reimann hypothesis was first proved by Pierre Deligne in 1973 by developing another topological idea of Lefschetz (called the *weak Lefschetz theorem*) in the context of the étale theory of Grothendieck. Deligne gave a second proof of Weil's Reimann hypothesis in 1980, and in the process of this proof the second part of Lefschetz topological work (called the *hard Lefschetz theorem*) was shown in étale context.

2.2 Riemann hypothesis for projective smooth curves over finite field

The main step in Weil's proof of the Riemann Hypothesis for curves over finite fields is to establish the Hasse-Weil inequality.

Theorem A. *Let C be a projective non-singular absolutely irreducible curve over a finite field $\mathbb{F}_{q^m}$. Then*

$$|q^m + 1 - N_m(C)| \leq 2q^{m/2}g(C)$$

where $g(C)$ is the genus *of C.*

I don't have enough knowledge of algebraic geometry, to be able to discuss the proof of this result. However, we can see how this inequality is equivalent to Weil's Riemann hypothesis. As claimed in subsection 1.3.2, we will assume the rationality, factorization and functional equation of the curve.

Theorem B. *Let C be a projective non-singular absolutely irreducible curve over a finite field $\mathbb{F}_{q^m}$. Then*

1. *$Z_C(t)$ is a rational function in $\mathbb{C}(t)$ with factorization*

$$Z_C(t) = \frac{P(t)}{(1-t)(1-qt)}, \quad P(t) = \prod_{j=1}^{2g}(1-\alpha_j t)$$

   where $g = g(C)$ and $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$.

2. *$Z_C(t)$ satisfies the functional equation:*

$$Z_C\left(\frac{1}{qt}\right) = q^{1-g}t^{2-2g}Z_C(t)$$

Theorem 3 (Riemann hypothesis for projective smooth curves over finite field)**.** *Let C be a projective non-singular absolutely irreducible curve over a finite field $\mathbb{F}_{q^m}$. Then all roots of $Z_C(t)$ are the complex numbers of norm $q^{-1/2}$.*

Proof. As seen in Example 5, we have

$$\log Z_C(t) = \sum_{m=1}^{\infty} N_m(C)\frac{t^m}{m}$$

Using the rational function from Theorem B we get:

$$\begin{aligned}
\sum_{m=1}^{\infty} N_m(C)\frac{t^m}{m} &= \log \frac{P(t)}{(1-t)(1-qt)} \\
&= \log P(t) - \log(1-t) - \log(1-qt) \\
&= \log \prod_{j=1}^{2g}(1-\alpha_j t) - \log(1-t) - \log(1-qt) \\
&= \sum_{j=1}^{2g} \log(1-\alpha_j t) - \log(1-t) - \log(1-qt) \\
&= \sum_{m=1}^{\infty} \left(1 + q^m - \sum_{j=1}^{2g} \alpha_j^m\right) \frac{t^m}{m}
\end{aligned}$$

Hence we get the trace formula

$$\boxed{N_m(C) = q^m + 1 - \sum_{j=1}^{2g} \alpha_j^m} \tag{2.1}$$

Next, substituting (2.1) in the Hasse-Weil inequality from Theorem A, we get:

$$\left| \sum_{j=1}^{2g} \alpha_j^m \right| \leq 2g\sqrt{q^m} \tag{2.2}$$

Now we state the essential claim:

`Claim:` For all j, $|\alpha_j| \leq q^{1/2}$.

Consider the following function:

$$f(t) = \sum_{j=1}^{2g} \frac{\alpha_j t}{1 - \alpha_j t} \tag{2.3}$$

Observe that $f(t)$ is homomorphic in the disk $\mathbb{D} = \{t \in \mathbb{C} : |t| < \rho\}$ for

$$\rho = \frac{1}{\max\limits_{1 \leq j \leq 2g} |\alpha_j|} \tag{2.4}$$

Now consider the power series expansion of $f(t)$ around origin

$$f(t) = \sum_{n=0}^{\infty} a_n t^n \tag{2.5}$$

Next, observe that ρ is in fact the radius of convergence of the power series of $f(t)$, since $\mathbb{D}$ is the largest disk (around origin) in which the series converges (since $t = 1/\alpha_j$ is not possible). Moreover, by Cauchy-Hadamard theorem we know that the radius of convergence ρ is given by

$$\frac{1}{\rho} = \limsup_{n \to \infty} |a_n|^{1/n} \tag{2.6}$$

Equating (2.3) and (2.5) we get

$$\begin{aligned} \sum_{n=0}^{\infty} a_n t^n &= \sum_{j=1}^{2g} \frac{\alpha_j t}{1 - \alpha_j t} \\ &= \sum_{j=1}^{2g} \sum_{\ell=1}^{\infty} (\alpha_j t)^\ell \\ &= \sum_{\ell=1}^{\infty} \left(\sum_{j=1}^{2g} \alpha_j \right) t^\ell \end{aligned}$$

Comparing the coefficients we get

$$a_0 = 0, \qquad a_n = \sum_{j=1}^{2g} \alpha_j^n \quad \forall n \geq 1$$

Equating (2.4) and (2.6) we get:

$$\max_{1 \leq j \leq 2g} |\alpha_j| = \limsup_{n \to \infty} |a_n|^{1/n}$$

$$
\begin{aligned}
&= \limsup_{n\to\infty} \left| \sum_{j=1}^{2g} \alpha_j^n \right|^{1/n} \\
&\leq \limsup_{n\to\infty} \left(2gq^{n/2}\right)^{1/n} && \text{using (2.2)} \\
&= q^{1/2} && \left(\text{since } \limsup_{n\to\infty} a^{1/n} = \lim_{n\to\infty} a^{1/n} = 1 \text{ for } a \in \mathbb{R}\right)
\end{aligned}
$$

Hence proving our claim:

$$
|\alpha_j| \leq q^{1/2} \quad \forall\ j \in \{1, \ldots, 2g\} \tag{2.7}
$$

Next, consider the functional equation and substitute the rational function in it from Theorem B to get

$$
q^{1-g}t^{2-2g} = \frac{Z_C\left(1/qt\right)}{Z_C(t)} = \frac{(1-t)(1-qt)qt^2P(1/qt)}{(qt-1)(t-1)P(t)} = q^{1-2g}t^{2-2g}\frac{\prod_{\ell=1}^{2g}(qt-\alpha_\ell)}{\prod_{j=1}^{2g}(1-\alpha_j t)}
$$

Hence we have

$$
\prod_{\ell=1}^{2g}(qt-\alpha_\ell) = \prod_{j=1}^{2g}(q^g - \alpha_j q^g t)
$$

Now comparing the coefficients we conclude that there exist integers ℓ and j such that

$$
\left.\begin{aligned} qt &= -\alpha_j q^g t \\ -\alpha_\ell &= q^g \end{aligned}\right\} \Rightarrow\ \forall\ j \in \{1, \ldots, 2g\}\ \exists\ \ell \in \{1, \ldots, 2g\} \text{ such that } \alpha_j\alpha_\ell = q \tag{2.8}
$$

Now combining (2.8) and (2.7) we get $|\alpha_j| = q^{1/2}$ for all $j \in \{1, \ldots, 2g\}$. Hence completing the proof. □

Remark 8. As in Proposition 3, we can define $\zeta(s) := Z_C(p^{-s})$. From this we can conclude that all the roots of $\zeta(s)$ have real part $1/2$, because:

$$
q^{-1/2} = |\alpha_j^{-1}| = \left|q^{-(\mathrm{Re}(s)+i\mathrm{Im}(s))}\right| = q^{-\mathrm{Re}(s)}
$$

2.3 Counting points on elliptic curve

In this section we will see an application of Weil's conjectures to compute the points on an elliptic curve over a finite field [6]. First, let's recall the definition and properties of elliptic curves [11, Definition 2.29]:

Definition 6 (Elliptic curve)**.** An elliptic curve over a field k is a smooth projective curve E over k of genus 1, together with a specified k-rational point[1] O.

Theorem C. *Every elliptic curve over a field k is isomorphic to the projective curve corresponding to a non-singular affine cubic $Z_f(\bar{k})$ in Weierstrass form, i.e. $f(x, y) = 0$ being*

$$
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_1, a_2, a_3, a_4, a_6 \in k
$$

Remark 9. If the characteristic of k in not 2 or 3, then by completing the squares and cubes, we end up with an equation of the form $Y^2 = X^3 + aX + b$ equivalent to the general Weierstrass form.

[1] That is $O \in \mathbb{P}^n(k)$ for $O \in E \subset \mathbb{P}^n(\bar{k})$.

Example 6. Consider the elliptic curve over $\mathbb{F}_{2^m}$ given by the Weierstrass form:

$$\tilde{E} : y^2 - y = x^3 - x^2$$

We homogenize this equation to obtain a projective non-singular absolutely irreducible curve of genus 1:

$$E : y^2z - yz^2 = x^3 - x^2z$$

Next we observe that $[0:0:1], [0:1:0], [0:1:1], [1:0:1]$ and $[1:1:1]$ are the five solutions of E over $\mathbb{F}_2$. Hence we have $N_1(E) = 5$. Since $g = 1$, by Theorem B we know that

$$Z_E(t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-2t)}$$

for some $\alpha, \beta \in \mathbb{C}$. Now using (2.1) we

$$N_m(E) = 2^m + 1 - \alpha^m - \beta^m \tag{2.9}$$

We know the value for $m = 1$, hence we get the $\alpha + \beta = -2$. Also, by (2.8) we know that $\alpha\beta = 2$. Combining these two, we conclude that

$$\alpha = -1 \pm i \quad \text{and} \quad \beta = -1 \mp i$$

Substituting these values in (2.9) we get the points counting formula for our elliptic curve E over $\mathbb{F}_{2^m}$:

$$\boxed{N_m(E) = 2^m + 1 - (-1+i)^m - (-1-i)^m}$$

Now we can use this formula to count number of points in the elliptic curve E for any m. For example,

$$\begin{aligned} N_{10}(E) &= 2^{10} + 1 - (-1+i)^{10} - (-1-i)^{10} \\ &= 1025 - \left(\sqrt{2}e^{\frac{3\pi i}{4}}\right)^{10} - \left(\sqrt{2}e^{\frac{5\pi i}{4}}\right)^{10} \\ &= 1025 - 32(e^{-\frac{\pi i}{2}} + e^{\frac{\pi i}{2}}) \\ &= 1025 \end{aligned}$$

We can in fact re-write the formula as:

$$N_m(E) = 2^m + 1 - 2^{\frac{m}{2}+1}\cos\left(\frac{3m}{4}\pi\right) = \begin{cases} 2^m + 1 - 2^{\frac{m}{2}+1} & \text{if } m \equiv 0 \pmod 8 \\ 2^m + 1 + 2^{\frac{m+1}{2}} & \text{if } m \equiv \pm 1 \pmod 8 \\ 2^m + 1 & \text{if } m \equiv \pm 2 \pmod 8 \\ 2^m + 1 - 2^{\frac{m+1}{2}} & \text{if } m \equiv \pm 3 \pmod 8 \\ 2^m + 1 + 2^{\frac{m}{2}+1} & \text{if } m \equiv 4 \pmod 8 \end{cases}$$

From this we observe that $N_1(E) = N_2(E) = N_3(E) = 5$, hence no new solution can be found when we search in $\mathbb{F}_4$ and $\mathbb{F}_8$.

Conclusion

There are some basic questions that have non-obvious connections to the Weil conjectures. For example, consider the *discriminant modular form*

$$\Delta(z) = \frac{(2\pi)^{12}}{1728}\left(E_4(z)^3 - E_6(z)^2\right)$$

Then the Fourier coefficients of $(2\pi)^{-12}\Delta(z)$ define the Ramanujan τ-function[12, §3.3]

$$(2\pi)^{-12}\Delta(z) = \sum_{n=1}^{\infty} \tau(n)q^n = q - 24q^2 + 252q^3 + \dots$$

Ramanujan conjectured that $|\tau(p)| \leq 2p^{11/2}$ for any prime number p. Work of Martin Eichler, Goro Shimura, Michio Kuga, Yasutaka Ihara, and Pierre Deligne showed that, in fact, Ramanujans conjecture is a consequence of the Weil conjectures, so that Delignes proof of the latter in 1974 also resolved the former[7].

The Weil conjectures form the cornerstone to the further study of the topological and number-theoretical properties of varieties. In 1969 Grothendieck proposed a vast program going under the title *Motives*. He set out some standard conjectures which would prove Weil's Riemann hypothesis and much much more. Though Grothendieck's student Deligne proved the Weil conjectures, the standard conjectures are as yet unresolved and the grand program of Grothendieck is yet to be completed [5].

Bibliography

[1] Hartshorne, R. *Algebraic Geometry* (GTM 52). New York: Springer-Verlag, 1977.

[2] Marcus, D. A. *Number Fields*. New York: Springer-Verlag, 1977.

[3] Atiyah, M. F. and Macdonald, I. G. *Introduction to Commutative Algebra* (Indian edition). Howrah: Levant Books, 2007.

[4] Dummit, D. S. and Foote, R. M. *Abstract Algebra* (3rd edition). New Delhi: Wiley India Pvt. Ltd., 2011.

[5] Srinivas, V. and Paranjape, K. H. "The Weil Conjectures." *Resonance* 4, no. 5 (1999), 71–77. https://www.ias.ac.in/article/fulltext/reso/004/05/0071-0077

[6] Oort, F. "The Weil Conjectures." *Nieuw Archief voor Wiskunde* (fifth series) 15, no. 6 (2014), 211–219. http://www.nieuwarchief.nl/serie5/pdf/naw5-2014-15-3-211.pdf

[7] Osserman, B. "The Weil Conjectures." in *The Princeton Companion for Mathematics*, edited by T. Gowers, J. Barrow-Green and I. Leader, 729–732. Princeton and Oxford: Princeton University Press, 2008. https://www.math.ucdavis.edu/~osserman/math/pcm.pdf

[8] Edixhoven, B. and Taelman, L. "Algebraic Geometry." lecture notes available at http://pub.math.leidenuniv.nl/~edixhovensj/teaching/2010-2011/AG-mastermath/ag.pdf. *(accessed on 05 June 2018)*

[9] Korpal, G. "Reciprocity Laws." *Winter Internship Project Report*, guided by Prof. C. S. Dalawat (09 December 2016 – 07 January 2017). https://gaurish4math.files.wordpress.com/2015/12/reciprocity_laws-gaurish.pdf

[10] Korpal, G. "Prime Numbers." *Summer Internship Project Report*, guided by Prof. K. Srinivas (05 June 2017 – 15 July 2017). https://gaurish4math.files.wordpress.com/2015/12/prime_numbers_gaurish.pdf

[11] Korpal, G. "Arithmetic Geometry - I." *Semester Project Report*, guided by Prof. B. Sahu (28 July 2017 – 17 November 2017). https://gaurish4math.files.wordpress.com/2018/02/arithmetic-geometry-1-gaurish-rev.pdf

[12] Korpal, G. "Modular Forms." *Winter Internship Project Report*, guided by Prof. M. Manickam (08 December 2017 – 30 December 2017). https://gaurish4math.files.wordpress.com/2017/12/modular-forms_gaurish.pdf

[13] Korpal, G. "Arithmetic Geometry - II." *Semester Project Report*, guided by Prof. B. Sahu (05 January 2018 – 20 April 2018) https://gaurish4math.files.wordpress.com/2018/06/arithmetic-geometry-2-gaurish.pdf

Prepared in LaTeX 2_ε by Gaurish Korpal