Number of Solutions to Diophantine Equations and Relations to the Riemann Hypothesis

Zhuoer Gu
under guidance of Prof. Daniel Bump

August 2019

Abstract

With number theoretic tools of Gauss sums and Jacobi sums, we can develop a way to count number of solutions to Diophantine equations of the form $a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_rx_r^{l_r} \equiv b \pmod{p}$. Later on, we will define zeta functions on algebraic sets and elliptic curves, and see their analogy with the Riemann zeta function and their relation with the Riemann Hypothesis. Finally, we will look into some elliptic curves, and determine the number of points on them.

1 Introduction

Let $f(x_1, x_2, \cdots, x_m) = 0$ be a polynomial equation defined on variables $x_1, x_2, \cdots, x_m$. Equations of the above kind are Diophantine equations. Solutions to Diophantine equations have been intriguing number theorists for centuries. Mathematicians are especially interested in the integral solutions to some Diophantine equations. While finding integral solutions by solving the equations is generally hard, we can first attempt to find solutions over a finite field F_p where p is a prime number.

Starting from the easiest type of Diophantine equation, $x^2 = a,\ a \in F_p$, we use elementary number theoretic knowledge of the Jacobi symbol and the Legendre symbol to solve the equation. The next equations we will naturally think of are the type $x^n = a$ over F_p. Diophantine equation of this type is more interesting in fields than in $\mathbb{Z}$.

The next model we can think of are $x^2 + y^2 = a$ over F_p. While we can solve the equation by hand given a field F_p, we will also care about the number of solutions to the equation. Naturally, we interpret the equation as a being the sum of two operands that are squares in F_p. Let $N(f(x) = 0)$ denote the number of solutions to the equation $f(x) = 0$. By looping through all elements in F_p as one of the operands, we have

$$N(x^2 + y^2 = a) = \sum_{u+v=a} N(x^2 = u)N(y^2 = v).$$

From the equation $x^2 + y^2 = a$, we can first extend it to the homogeneous equation $x^n + y^n = a$. Though it would be impossible for us to find the solutions explicitly, we can write out the number of solutions with number theoretic techniques of the Gauss sums and Jacobi sums. Furthermore, we can estimate on the number of solutions. We can also extend the equation to the generalized form $a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_rx_r^{l_r} \equiv b \pmod{p}$, and discuss the number of solutions.

Now consider a polynomial and its zeros on a projective plane. On projective spaces, we deal with homogeneous polynomials. Particularly, we transform non-homogeneous polynomials into homogeneous ones, which makes many polynomials equations accessible to us. However, when counting zeros on the curves represented by the polynomials on projective spaces, we need to be particularly careful about points at infinity.

The number of solutions to a Diophantine equation over different algebraic objects may be given a generalized formula or imply existence of roots through estimate. At the same time, the number of solutions to an equation also gives rise to a zeta function defined by the corresponding polynomial. Surprisingly, the zeta function defined on an algebraic set is analogous to the Riemann zeta function. In 1964, André Weil proposed the Weil's conjecture[5], which is now proved based on the Hasse-Davenport relation. The conjectures led to the Riemann Hypothesis for projective curves over finite field. What's more, this is an analogy to the Riemann Hypothesis. In the end, we will particularly look into some elliptic curves and their zeta functions. Using characters and given a field, we can find all the points on some elliptic curves. We will also see an equivalence between Hasse's Theorem on elliptic curves and the Riemann Hypothesis.

In this paper, we will build up the Gauss sums and Jacobi sums in finding out the number of solutions to Diophantine equations. Then we introduce projective space and zeta functions. Finally we will see analogy and relations between the number of solutions and the Riemann Hypothesis.

2 Number of Solutions to $\mathbf{x^n + y^n = 1}$

To begin with, we consider solving the Diophantine equations of the form $\mathbf{x^n = a}$. In solving this equation, we introduce multiplicative characters.

2.1 Multiplicative Characters

Definition 2.1.1 A *multiplicative character* on F_p is a multiplicative map $\chi : F_p^* \to \mathbb{C}\backslash\{0\}$ that satisfies

$$\chi(ab) = \chi(a)\chi(b) \quad \text{for all } a, b \in F_p^*$$

.

In the rest of the paper, we will denote the trivial multiplicative character by ε and character of order two by ρ. The trivial character ε is defined by $\varepsilon(a) = 1$ for all $a \in F_p^*$. We can easily relate ρ to the Legendre symbol $\left(\frac{a}{p}\right)$ over F_p, which is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a = m^2 \text{ for some } m \in F_p^* \\ -1 & \text{otherwise.} \end{cases}$$

It is easy to check that the Legendre symbol is of order 2, which will be useful in specifying number of solutions to specific equations.

Remark To extend the definition on multiplicative characters on the case of 0, we set $\chi(0)$ to be 0 when the character $\chi \neq \varepsilon$ and $\varepsilon(0) = 1$.

From now on, by *character*, we mean multiplicative character. Now we turn to some basic properties of characters.

Proposition 2.1.2 Let χ be a character and $a \in F_p^*$. χ satisfies
(i) $\chi(1) = 1$.
(ii) $\chi(a)$ is a $(p-1)$st root of unity.
(iii) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Proof. To prove the first identity, we see that $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1)$. Since $\chi(1) \neq 0$, we have $\chi(1) = 1$. For the second identity, we first have $a^{p-1} = 1$ by Fermat's Little Theorem. Then by multiplicity of

characters, we have $1 = \chi(1) = \chi(a)^{p-1}$. Thus $\chi(a)$ is a $(p-1)$st root of unity.
To see the third identity, the left equality is trivial by multiplicity. For the rest, consider $\chi(a)\,\overline{\chi(a)} = |\chi(1)|^2$ which is 1 from the second identity. Thus $\chi(a)^{-1} = \overline{\chi(a)}$. □

Let χ, λ be characters. Define $\chi\lambda$ to be the map that takes $a \in F_p^*$ to $\chi(a)\lambda(a)$, and χ^{-1} to be the map that takes $a \in F_p^*$ to $\chi(a)^{-1}$. Then we have the following proposition concerning the multiplicative group of characters.

Proposition 2.1.3 The set of characters form a group which is cyclic of order $p-1$ and identity ε. If $a \in F_p^*$ and $a \neq 1$, then there exists a character χ with $\chi(a) \neq 1$.

Proof. With multiplicity of characters and the fact that F_p^* is cyclic of order $p-1$, we have the characters also form a cyclic group of order $p-1$. The identity is trivial to verify. Now pick a generator g of F_p^*. With the second identity in Proposition 2.1.2, we consider the map $\chi(g^n) = e^{\frac{2\pi i n}{p-1}}$. Then χ is a character of order $p-1$. The elements in this group of character are $\varepsilon, \chi, \chi^2, \ldots, \chi^{p-2}$. Pick an $a \in F_p^*$ and $a \neq 1$. Say $a = g^n$. Since $a \neq 1$, $(p-1) \nmid n$, thus $\chi(a) = e^{\frac{2\pi i n}{p-1}} \neq 1$. □

Remark The above proposition restricts the value of characters of certain orders. For example, if χ is of order 4, then χ can only take values within the set $\{1, -1, i, -i\}$. This fact is useful in justifying the coefficients in some relations about the Gauss sums. In addition, the existence of a χ with $\chi(a) \neq 1$ is essential to the sum of characters. With the same a in Proposition 2.1.3, we have $\sum_\chi \chi(a) = 0$ where the sum is over all characters.

One important proposition that relates multiplicative character to number of solutions to Diophantine equations could be found from Ireland and Rosen[3].

Proposition 2.1.4 If $n|p-1$, we have $N(x^n = a) = \sum_{x^n=\varepsilon} \chi(a)$ where the sum is over all characters of order dividing n.

Proof. We approach the problem by splitting into cases. Take a generator of F_p^* and consider the map $\chi(g^n) = e^{\frac{2\pi i n}{p-1}}$. $\varepsilon, \chi, \chi^2, \ldots, \chi^{n-1}$ are the n characters of order dividing n. The cases concerns if $a = 0$ and if the equation can be solved.
If $a = 0$, $N(x^n = 0) = 1 = \sum_\chi \chi(0)$. If $a \neq 0$ and the equation has solutions, then there are n solutions over a field and say b is a solution. Then $\chi(a) = \chi(b)^n = \chi^n(b) = 1$. There are n such b's. Thus $\sum_\chi \chi(a) = n = N(x^n = a)$.
If $a \neq 0$ and the equation has no solutions, then $N(x^n = a) = 0$. We want to show that $\sum_\chi \chi(a) = 0$. A usual technique to prove identities of such sums by Ireland and Rosen[3] is multiplying both sides by a number not equal to 1. Compared to Proposition 2.1.3, we can find a more restricted character λ such that λ has order dividing n and that $\lambda(a) \neq 1$.

Lemma 2.1.5 If $a \in F_p^*$ and $n \mid p-1$ with $x^n = a$ unsolvable, then there is a character λ such that $\lambda^n = \varepsilon$ and that $\lambda(a) \neq 1$.

Proof to Lemma As usual, let g be a generator of F_p^*. Consider the map $\lambda(g^n) = e^{\frac{2\pi i}{n}}$. This map makes $\lambda^n = \varepsilon$. Say $a = g^l$ and consider the map $\chi(g^n) = e^{\frac{2\pi i n}{p-1}}$. Then we have $\lambda = \chi^{\frac{p-1}{n}}$. $\lambda(a) = \chi(g)^{\frac{(p-1)l}{n}} = e^{\frac{2\pi i l}{n}}$. Since the equation is unsolvable, we must have $n \nmid l$, thus $\lambda(a) \neq 1$.

With such λ, we multiply both sides with $\lambda(a)$, and we have $\lambda(a)\sum_\chi \chi(a) = \sum_\chi \chi(a)$. So $\sum_\chi \chi(a) = 0$. □

The completion of Proposition 2.1.5 does not solve all Diophantine equations of the type $\mathbf{x^n = a}$ over F_p. To extend on the proposition, given an n, consider $d = gcd(m, p-1)$.

Proposition 2.1.6 $N(x^n = a) = \sum \chi(a)$ where the sum is over all χ such that $\chi^d = \varepsilon$.

Proof. The proof is similar to that of Proposition 2.1.4. Let χ be a character of order d. Then $\chi^d = \varepsilon = \chi^{p-1} = \chi^n$. Now take a generator g of F_p^* and define the map $\chi(g^m) = e^{\frac{2\pi i m}{p-1}}$. There are exactly d characters of order dividing d in the multiplicative group of characters, and they are exactly the characters $\varepsilon, \chi, chi^2, \ldots, \chi^{d-1}$.
If $a = 0$, the case is trivial. If $a \neq 0$ and $x^m = a$ solvable, then there exists an b such that $b^m = a$. And there are altogether m solutions to the equation. Since $\chi^d = \varepsilon$ and $d|m$, $\chi(a) = \chi^m(b) = \varepsilon(b)^{\frac{m}{d}} = 1$. Thus $\sum_{\chi^d=\varepsilon} \chi(a) = d$.
If $a \neq 0$ and $x^m = a$ unsolvable, then we want to show that $\sum \chi(a) = 0$. Denote the sum by T. From Lemma 2.1.5, we know that there is a character λ of such that $\lambda^d = \varepsilon$ and that $\lambda(a) \neq 1$. Then $\lambda(a)T = T$. $T = 0$. □

Now we finished our discussion on number of solutions to $\mathbf{x^n} = \mathbf{a}$ over F_p. This is fundamental in counting number of solutions to Diophantine equations, because given an equation whose terms are all univariate x_i's, we are now equipped with the method to split the equation and solve each terms $x_i^{n_i} = a_i$.

From the last subsection, it is easy to verify that $N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$ where $\left(\frac{a}{p}\right)$ denotes the Legendre symbol. Now we want to count solutions of equations of form $\mathbf{x^n} + \mathbf{y^n} = \mathbf{1}$ over F_p. We start with the simple case when $n = 2$ and we can prove many variations of the equation. In this subsection, we introduce Gauss and Jacobi sums to denote the inner product when counting number of solutions of split terms of the original equation.

Before we solve the equation $x^2 + y^2 = a$, we first introduce the Gauss sums and its important properties.

2.2 Gauss sums

Definition 2.2.1 Suppose a field F has p^n elements. Then we define the *trace* of α for $\alpha \in F$ to be $\mathrm{tr}(\alpha)$=$\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$. We also define the function $\phi: F \to \mathbb{C}$ by the formula $\phi(\alpha) = \zeta_p^{tr(\alpha)}$, where ζ_p is a p^{th} root of unity. Now we define the *Gauss sum* on the field F belonging to character χ.

Definition 2.2.2 Let χ be a character of F and $\alpha \in F^*$. Let $g_\alpha(\chi) = \sum_{t\in F} \chi(t)\phi(\alpha t)$ is called the *Gauss sum on* F belonging to character χ.

First we consider the case when $n = 1$. Then $|\mathbb{F}| = p$. Let ζ be a p^{th} root of unity. Then $\mathrm{tr}(\alpha)$=α and $\phi(\alpha) = \zeta^\alpha$. Let χ be a character on $\mathbb{F}_p$ and the Gauss sum is $g_\alpha(\chi) = \sum_{t\in F} \chi(t)\phi(\alpha t) = \sum_{t\in F} \chi(t)\zeta^{\alpha t}$. When $\alpha = 1$, we usually denote $g_1(\chi)$ as $g(\chi)$. Next we will show the relation between Gauss sums and characters.

Proposition 2.2.3 Consider a field $\mathbb{F}_p$ and a character χ on the field. If $\alpha \neq 0$ and $\chi \neq \varepsilon$, then $g_\alpha(\chi) = \chi(\alpha^{-1})g(\chi)$. If $\alpha \neq 0$ and $\chi = \varepsilon$ or $\alpha = 0$ and $\chi \neq \varepsilon$, then $g_\alpha(\varepsilon) = 0$. If $\alpha = 0$ and $\chi = \varepsilon$, then $g_0(\varepsilon) = p$.

Proof. In the first case when $\alpha \neq 0$ and $\chi \neq \varepsilon$, it follows that

$$g_\alpha(\chi) = \sum_{t\in F} \chi(t)\zeta^{\alpha t} = \chi(\alpha^{-1}) \sum_{t\in F} \chi(\alpha t)\zeta^{\alpha t}.$$

Since α and t are elements in $\mathbb{F}_p$, so αt covers all elements in the field. Therefore $g_\alpha(\chi) = \chi(\alpha^{-1})g(\chi)$. In the second case, $g_\alpha(\chi) = g_0(\chi) = \sum_{t\in F} \chi(t)$. Thus we are left to prove that $\sum_{t\in F} \chi(t) = 0$. We prove this with a previous technique by multiplying both sides with a number not equal to 1. Let $\sum_{t\in F} \chi(t) = S$. Choose an element $\beta \in F$ such that $\chi(\beta) \neq 1$. $\chi(\beta)S = \sum_{t\in F} chi(\beta t) = S$. Since $\chi(\beta) \neq 1$, $S = 0$. □

The next proposition inspires the connection between Gauss sums and Jacobi sums in the later subsections.

Proposition 2.2.4 If $\chi \neq \varepsilon$, then $|g(\chi)| = \sqrt{p}$.

Proof. The idea by Ireland and Rosen[3] is to evaluate the sum $\sum_a g_a(\chi)\overline{g_a(\chi)}$ in two ways with case studies on a.
If $a \neq 0$, by Proposition 2.2.3 and Proposition 2.1.2, $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$. Thus $|g(\chi)|^2 = g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})g(\chi)\chi(a)\overline{g(\chi)} = \chi(a^{-1})\chi(a)\underline{g(\chi)}\overline{g(\chi)}$.
If $a = 0$, by Prop 2.2.3, $g_a(\chi) = 0$. So $\sum_a g_a(\chi)g_a(\chi) = (p-1)|g(\chi)|^2$ for summation over all $a \in F_p$.

On the other hand, by definition of the Gauss sum,

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_a \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay}.$$

If $x \neq y$, then $\sum_a \zeta^{ax-ay} = \frac{\zeta^{bp}-1}{\zeta^b-1} = 0$. Else $\sum_a \zeta^{ax-ay} = \sum_a \zeta^0 = p$. Therefore $g_a(\chi)\overline{g_a(\chi)} = (p-1)p$ and thus $(p-1)|g(\chi)|^2 = (p-1)p$. This tells us $|g(\chi)| = \sqrt{p}$. □

Remark From the definition of Gauss sum, we can derive that $\overline{g(\chi)} = \sum_t \overline{\chi(t)}\zeta^{-t} = \chi(-1)g(\bar{\chi})$.

After the introduction to Gauss sum, we return to the goal of solving $\mathbf{x^2 + y^2 = a}$. We first consider the case when $a = 1$. In this case, we can derive that

$$N(x^2 + y^2 = 1) = \sum_{u+v=1} N(x^2 = u)N(y^2 = v)$$

where the sum is over all $u \in F_p$. By Proposition 2.1.4, we have that $N(x^2 = u) = \sum_{x^2=\varepsilon} \chi(u) = 1 + \left(\frac{u}{p}\right)$. Therefore we have

$$N(x^2 + y^2 = 1) = \sum_{u+v=1} (1 + \left(\frac{u}{p}\right))(1 + \left(\frac{v}{p}\right)) = p + \sum_u \left(\frac{u}{p}\right) + \sum_v bigg(\frac{v}{p}\right) + \sum_{u+v=1} \left(\frac{u}{p}\right)\left(\frac{v}{p}\right).$$

With remark following Prop. 2.1.3, we can cancel out the terms $\sum_u \left(\frac{u}{p}\right)$ and $\sum_v \left(\frac{v}{p}\right)$. The remaining summation value is unsolved at this moment and we will figure it out in the next subsection with Jacobi sums.
With Proposition 2.1.6, we can analyze on the equation $\mathbf{x^n + y^n = 1}$ over F_p where p is prime and $d = gcd(n, p-1)$. A natural way to count is

$$N(x^n + y^n = 1) = \sum_{u+v=1} N(x^d = u)N(y^d = v).$$

Let $\chi \neq \varepsilon$ be a character such that $\chi^d = \varepsilon$. Then $\varepsilon, \chi, \chi^2, \cdots, \chi^d$ are all characters of order dividing d. By Prop. 2.1.4,we have

$$N(x^n + y^n = 1) = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} \Big(\sum_{u+v=1} \chi^i(u)\chi^j(v) \Big).$$

We are interested in the inner product in the above expression with the restriction that $u + v = 1$. If we can generalize the inner sum, we can write the expression in a neat way and thus we introduce the Jacobi sums.

2.3 Jacobi sums

In this subsection, we introduce Jacobi sums and use its properties to finish the discussion on $N(x^2+y^2 = 1)$. Moreover, we shall see the basic connection between Gauss sums and Jacobi sums.

Definition 2.3.1 Let χ and λ be characters of F_p. The *Jacobi sum* $J(\chi, \lambda)$ is defined by $J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$.

To close up the discussion on $N(x^2+y^2=1)$, we present a theorem from Ireland and Rosen[3] that connects Gauss sums and Jacobi sums.

Theorem 2.3.2 Let χ and λ be nontrivial characters. Then $J(\chi, \chi^{-1}) = -\chi(-1)$. If $\chi\lambda \neq \varepsilon$, then $J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Proof. $J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{a\neq 1} \chi(\frac{a}{1-a})$. Since $\frac{a}{1-a}$ never reaches the value -1 and we know $\sum_a \chi(a) = 0$ from previous remark, we must have $J(\chi, \chi^{-1}) + \chi(-1) = 0$.
For the second part of the proof, first we write out $g(\chi)g(\lambda)$.

$$\begin{aligned} g(\chi)g(\lambda) &= \sum_{x,y} \chi(x)\lambda(y)\zeta^{x+y} \\ &= \sum_t \Big(\sum_{x+y=t} \chi(x)\lambda(y) \Big)\zeta^t. \end{aligned}$$

If $t = 0$, $g(\chi)g(\lambda) = \sum_x \chi(x)\lambda(-x) = \sum_x \lambda(-1)\chi\lambda(x) = 0$ when character $\chi\lambda \neq \varepsilon$. On the other hand, $J(\chi, \lambda)$ has the same expression. So the theorem holds in this case.
If $t \neq 0$, we try to relate to the restriction of $a + b = 1$ in a Jacobi sum by letting $x = ta$ and $y = tb$.
$g(\chi)g(\lambda) = \sum_t \Big(\sum_{a+b=1} \chi(ta)\lambda(tb) \Big)\zeta^t = \sum_t \chi\lambda(t)J(\chi, \lambda)\zeta^t = g(\chi\lambda)J(\chi, \lambda)$. □

Before we move on to more properties of Jacobi sums, we go back to the expression $N(x^2 + y^2 = 1) = p+\sum_{u+v=1} \big(\frac{u}{p}\big)\big(\frac{v}{p}\big)$. Now we write the Legendre symbol as character ρ of order 2. Then $\rho = \rho^{-1}$. With Theorem 2.3.2, we know that $J(\rho, \rho) = -\rho(-1)$. Notice that $J(\rho, \rho) = \sum_{u+v=1} \rho(u)\rho(v) = sum_{u+v=1} \big(\frac{u}{p}\big)\big(\frac{v}{p}\big)$. Thus $N(x^2 + y^2 = 1) = p - \rho(-1) = p + \big($
$frac-1p\big)$. With the Law of Quadratic Reciprocity, we have $N = p - (-1)^{fracp-12}$.

Example 2.3.3 We evaluate$N(x^3 + y^3 = 1)$ by taking $n = 3$, and assume that $p \equiv 1 \pmod 3$. Take a character χ of order 3. Then $N(x^3 + y^3 = 1) = p - \chi(-1) - \chi^2(-1) + J(\chi, \chi) + J(\chi^2, \chi^2)$. We call such χ a cubic character. Notice that for such χ, $\chi(-1) = \chi(-1)^3 = \chi^3(-1) = 1$. Also $\chi^2 = \chi^{-1} = \bar{\chi}$. Thus $\chi(-1) = \chi^(- 1) = 1$. Next, we have $J(\chi^2, \chi^2) = J(\bar{\chi}, \bar{\chi}) = \sum_{a+b=1} \chi(a)\chi(b) = J(\chi, \chi)$. Thus we have $N(x^3 + y^3 = 1) = p - 2 + 2 \text{ Re } J(\chi, \chi)$.

Corollary 2.3.4 If $\chi, \lambda,$ and $\chi\lambda$ are not equal to ε, then $|J(\chi, \lambda)| = \sqrt{p}$.

Proof. This corollary follows easily from Theorem 2.3.2 with the multiplicity of norm of complex numbers. $|J(\chi, \lambda)| = \frac{|g(\chi)||g(\lambda)|}{|g(\chi\lambda)|} = \sqrt{p}$. □

With this corollary, in the evaluation in Example 2.3.3, we can also say that $|N(x^3 + y^3 = 1) = p + 2| = |J(\chi, \chi) + J(\chi^2, \chi^2)| \leqslant 2\sqrt{p}$ by the triangular inequality. This gives us an intuition on estimating $N(x^n + y^n = 1)$.
For convenience, we assume that $p \equiv 1 \pmod n$. Let χ be a character of order dividing n. Then

$$N(x^n + y^n = 1) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} J(\chi^i, \lambda^j).$$

When $i = j = 0$, we have that $J(\chi^0, \chi^0) = J(\varepsilon, \varepsilon) = p$. When i or j is 0, we have $J(\chi^i, \chi^j) = J(\varepsilon, \chi^n) = 0$. When $i + j = n$ with $i, j \neq 0$, $J(\chi^i, \chi^j) = J(\chi^i, \chi^{-i}) = -\chi^i(-1)$ by Theorem 2.3.2. Notice that

$\sum_{i=0}^{n-1} J(\chi^i, \chi^{-i}) = -\sum_{i=0}^{n-1} \chi^i(-1)$. Now if -1 is an n^{th} power, then $\chi(-1) = \chi^n(-1) = 1$ and the sum $-\chi^i(-1) = n$. Otherwise, let the sum be T. Since $\chi(-1)$ is either 1 or -1, thus nonzero. $\chi(-1)T = T$ and $T = 0$. Therefore,$\sum_{i=1}^{n-1} -\chi^i(-1) = 1 - T$. Notice that this technique in evaluating sum of characters is very common.
Define the function

$$\delta_n(-1) = \begin{cases} 1 & \text{if -1 is an } n^{\text{th}} \text{ power} \\ 0 & \text{otherwise.} \end{cases}$$

With substitution, we have $N(x^n + y^n = 1) = p + 1 - n\delta_n(-1) + \sum_{1 \leqslant i,j \leqslant n-1 i+j \neq n} J(\chi^i, \chi^j)$. With similar estimation on the case of $n = 3$, for general n, the above derivation leads to the following proposition.

Proposition 2.3.5 $|N(x^n + y^n = 1) + \delta_n(-1)n - (p+1)| \leqslant (n-1)(n-2)\sqrt{p}$.

Proposition 2.3.5 tells us that for a given n and $p \equiv 1 \pmod{n}$, if the prime p is large enough, we are guaranteed that the equation $\mathbf{x^n + y^n = 1}$ has many non-trivial solutions. When we introduce projective space in the next section, we will read $n\delta_n(-1)$ as number of points at infinity on the curve $x^n + y^n = 1$, and the coefficient $(n-1)(n-2)$ is related to the genus[2] of the curve. In this paper, we will only look into the elliptic curves later whose genus is 1.

2.4 More on Characters, Jacobi Sums, and Gauss Sums

In this subsection, we will present several propositions and corollaries that describes the involves the three tools. Some of the relations might be useful for analysis on the number of solutions to more complicated Diophantine equations.

Proposition 2.4.1 Suppose that $p \equiv 1 \pmod{n}$ and that χ is a character of order n. Then $g(\chi)^n = p\chi(-1)J(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})$ for $n \geqslant 3$.

Proof. In the case of $n = 2$, use Theorem 2.3.2 and we have that $g(\chi)^2 = J(\chi,\chi)g(\chi^2)$ for all characters χ. For $n = 3$, by multiplying $g(\chi)$ on both sides, we have that $g(\chi)^3 = J(\chi,\chi)g(\chi^2)g(\chi) = J(\chi,\chi)g(\chi)g(\bar{\chi})$.

Lemma 2.4.2 $\overline{g(\chi)} = \chi(-1)g(\bar{\chi})$.

Proof to Lemma $\overline{g(\chi)} = \sum_t \overline{\chi(t)}\zeta^{-t} = \sum_t \chi(-1)\overline{\chi(-t)}\zeta^{-t} = \chi(-1)g(\bar{\chi})$.

$g(\chi)g(\bar{\chi}) = g(\chi)\overline{g(\chi)}/\chi(-1)$. Since $\chi(-1)$ is either 1 or -1, $1/\chi(-1) = \chi(-1)$. With Proposition 2.2.4, we have $g(\chi)\overline{g(\chi)} = p$. Thus when $n = 3$, $g(\chi^3) = p\chi(-1)J(\chi,\chi)$. Now for any $n \geqslant 3$, the identity that $g(\chi)^n = J(\chi,\chi)\dots J(\chi,\chi^{n-2})g(\chi^{n-1})g(bar\chi) = p\chi(-1)J(\chi,\chi)\dots J(\chi,\chi^{n-2})$. □

In the case of $n = 3$ in Proposition 2.4.1, the cubic character $\chi(-1)$ satisfies $\chi(-1) = \chi^3(-1) = 1$. Thus we have the following corollary.

Corollary 2.4.3 If χ is a cubic character, then $g(\chi)^3 = pJ(\chi,\chi)$.

Suppose that $p \equiv 1 \pmod{d}$, $\zeta = e^{2\pi i/p}$, and consider $\sum_x \zeta^{ax^d}$. Then $\sum_r N(x^d = r)\zeta^{ar} = \sum_x \zeta^{ax^d}$.

Corollary 2.4.4 Assume that $p \nmid a$, $\sum_\chi g_a(\chi) = \sum_\chi \zeta^{ax^d}$, where the sum is over all χ such that $\chi^d = \varepsilon$ and $\chi \neq \varepsilon$.

Proof.

$$\sum_\chi g_a(\chi) = \sum_{\chi^d=\varepsilon} \sum_r \chi(r)\zeta^{ar} = \sum_r \Big(\sum_{\chi^d=\varepsilon} \chi(r) \Big)\zeta^{ar} = \sum_r N(\chi^d = r)\zeta^{ar} = \sum_\chi \zeta^{ax^d}.$$

□

3 Number of Solutions to $a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_rx_r^{l_r} = b$

Our goal in the this section is count solutions to

$$a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_rx_r^{l_r} \equiv b \quad \text{over the field } F_p. \tag{1}$$

In the last section, we only dealt with two variables. To deal with more complicated Diophantine equations, we introduced extended Jacobi sums and reach a general formula.

3.1 Extended Jacobi Sums

Before we move on to the general form of $a_1x_1^{l_1} + a_2x_2^{l_2} + \cdots + a_rx_r^{l_r} \equiv b$,

Definition 3.1.1 Let $\chi_1, \chi_2, \cdots, \chi_l$ be characters on F_p. A *Jacobi sum* is defined by the formula

$$J(\chi_1, \chi_2, \cdots, \chi_l) = \sum_{t_1+t_2+\cdots+t_l=1} \chi_1(t_1)\chi_2(t_2)\ldots\chi_l(t_l).$$

In this section, we will also consider the case when $b = 0$ in (1). To deal with this case, we also extend the following definition.

Definition 3.1.2 Let the characters $\chi_1, \chi_2, \cdots, \chi_l$ be the same as in Definition 3.1.1. Set

$$J_0(\chi_1, \chi_2, \cdots, \chi_l) = \sum_{t_1+t_2+\cdots+t_l=0} \chi_1(t_1)\chi_2(t_2)\ldots\chi_l(t_l).$$

With these definitions, it is easy to verify that $J_0(\varepsilon, \varepsilon, \cdots, \varepsilon) = J(\varepsilon, \varepsilon, \cdots, \varepsilon) = p^{l-1}$ since there are only $l-1$ free variables in the linear Diophantine equation. The next identity we are curious about have the restriction that some but not all of the characters χ_i's are trivial ones. It turned out that this is also a special case.

Proposition 3.1.3 If some but not all of the characters χ_i's are trivial characters, then $J_0(\chi_1, \chi_2, \cdots, \chi_l) = J(\chi_1, \chi_2, \cdots, \chi_l) = 0$

Proof. Since the summation of both J_0 and J are over all the $l-$tuples of characters, the order of the $l-$tuples does not matter. Without loss of generality, say the characters $\chi_1, \chi_2, \cdots, \chi_i$ are all the nontrivial characters.

$$\begin{aligned} J_0(\chi_1, \chi_2, \cdots, \chi_l) &= \sum_{t_1+t_2+\cdots+t_l=0} \chi_1(t_1)\chi_2(t_2)\cdots\chi_i(t_i) \\ &= p^{l-s-1}\Pi_{k=1}^{i}\left(\sum_{t_k} \chi_k(t_k)\right) \end{aligned} .$$

The last step is understood as fixing those t_i's such that χ_i's are non-trivial. For the remaining trivial characters, only $l-s-1$ of the t_i's are free variables.
As for $J(\chi_1, \chi_2, \cdots, \chi_l)$, apply the same steps and yield the result 0. □

The proposition above will help cancel out many terms in counting solutions to complicated equations. The next propositions are analogous to the simpler ones in the last section. We will first show the result of $J_0(\chi_1, \chi_2, \cdots, \chi_l)$ in another special case.

Proposition 3.1.4 Assume that $\chi_l \neq \varepsilon$. Then

$$J_0(\chi_1, \chi_2, \cdots, \chi_l) = \begin{cases} 0 \quad \text{if } \chi_1\chi_2\cdots\chi_l \neq \varepsilon, \\ \chi_l(-1)(p-1)J(\chi_1, \chi_2, \cdots, \chi_{l-1}) \quad \text{otherwise.} \end{cases}$$

Proof. We omit the setp-by-step proof from Rosen and Ireland[3]. The main proof idea is that we get the intuition from the term $J(\chi_l(-1)(p-1)J(\chi_1,\chi_2,\cdots,\chi_{l-1})$, which indicates us to split the character χ_l from the rest and sum over all $\chi_l(s)$. The nonzero s contributes to the coefficient $p-1$. The inner sum that contributes to $J(\chi_l(-1)(p-1)J(\chi_1,\chi_2,\cdots,\chi_{l-1})$ has restriction $t_1+t_2+\cdots+t_{l-1}=-s$ reminds us of the technique of letting $t_i=-st_{i'}$. By using the technique, we can derive the extended Jacobi sum with an coefficient $\chi_1\chi_2\cdots\chi_{l-1}(-s)$, and this term has different values based on the two cases. □

Next we see the connection between Gauss sums and the extended Jacobi sum, which is an analogy to Theorem 2.3.2. This following theorem applies the previous proposition in different cases.

Theorem 3.1.5 Assume that $\chi_1,\chi_2,\ldots,\chi_l$ are nontrivial and that $\chi_1\chi_2 dots\chi_l\neq\varepsilon$. Then $g(\chi_1)g(\chi_2)\cdots g(\chi_l)=J(\chi_1,\chi_2,\ldots,\chi_l)g(\chi_1,\chi_2,\ldots,\chi_l)$.

Proof.

$$g(\chi_1)g(\chi_2)\cdots g(\chi_l)=\sum_s\big(\sum_{t_1+t_2+\cdots+t_l=s}\chi_1(t_1)\chi_2(t_2)\cdots\chi_l(t_l)\big)\zeta^s.$$

Then the case of $s=0$ and $s\neq 0$ corresponds to Proposition 3.1.4. □

Similar to our discussion on Jacobi sums in Section 2, we also want to know the norm of the extended Jacobi sums. Here we present a theorem from Ireland and Rosen[3] without proof. This theorem is an significant part in the number of solutions of a generalized equation.

Theorem 3.1.6 Assume that $\chi_1,\chi_2,\cdots,\chi_r$ are nontrivial.
If $\chi_1\chi_2\cdots\chi_r\neq\varepsilon$, then

$$|J(\chi_1,\chi_2,\cdots,\chi_r)|=p^{\frac{r-1}{2}}.$$

If $\chi_1\chi_2\cdots\chi_r=\varepsilon$, then

$$|J_0(\chi_1,\chi_2,\cdots,\chi_r)|=(p-1)p^{\frac{r}{2}-1}$$

and

$$|J(\chi_1,\chi_2,\cdots,\chi_r)|=p^{\frac{r}{2}-1}.$$

3.2 Generalization Formula of N

Now to count the solution to $a_1x_1^{l_1}+a_2x_2^{l_2}+\cdots+a_rx_r^{l_r}\equiv b\pmod p$, let N denote the number for easier notation. We then have

$$N=\sum N(x_1^{l_1}=u_1)N(x_2^{l_2}=u_2)\cdots N(x_r^{l_r}=u_r)$$

where the sum is over all $(u_1,u_2,\cdots,u_r)$ such that $a_1u_1+a_2u_2+\cdots a_ru_r=b$. For convenience of calculation, we assume that $l_i|p-1$ for all i and $\chi_i^{l_i}=\varepsilon$. Then by Proposition 2.1.4, we have that $N(\chi^i=u_i)=\sum_{\chi^{l_i}=\varepsilon}\chi_i(u_i)$. Now we derive that

$$N=\sum_{\chi_1,\chi_2,\cdots,\chi_r}\sum_{u_1,u_2,\cdots,u_r}\chi_1(u_1)\chi_2(u_2)\cdots\chi_r(u_r).$$

Again we have to discuss the case of $b=0$ and $b\neq 0$, since this affects which Jacobi sum to use.
If $b=0$, we should use the definition of J_0. If $b\neq 0$, then $t_i=\frac{a_iu_i}{b}$ and use the extended Jacobi sum. With all the cases together, we have the following theorem from Ireland and Rosen[3].

Theorem 3.2.1 If $b=0$, then

$$N=p^{r-1}+\sum\chi_1(a_1^{-1})\chi_2(a_2^{-1})\ldots\chi_r(a_r^{-1})J_0(\chi_1,\chi_2,\cdots,\chi_r).$$

The sum is over all r-tuples of characters where $\chi_i^{l_i}=\varepsilon$, $\chi_i\neq\varepsilon$ for $i=1,2,\cdots,r$, and $\chi_1\chi_2\ldots\chi_r=\varepsilon$. If M is the number of such r-tuples, then $|N-p^{r-1}|\leqslant M(p-1)p^{(\frac{r}{2}-1)}$.

If $b \neq 0$, then

$$N = p^{r-1} + \sum \chi_1\chi_2\cdots\chi_r(b)\chi_1(a_1^{-1})\chi_2(a_2^{-1})\ldots\chi_r(a_r^{-1})J(\chi_1,\chi_2,\cdots,\chi_r).$$

The sum is over all r-tuples of characters where $\chi_i^{l_i} = \varepsilon$, $\chi_i \neq \varepsilon$ for $i = 1, 2, \cdots, r$. If M_1 is the number of such r-tuples with $\chi_1\chi_2\cdots\chi_r = \varepsilon$, and M_2 the number of such r-tuples with $\chi_1\chi_2\cdots\chi_r \neq \varepsilon$, then $|N - p^{r-1}| \leqslant M_1 p^{(\frac{r}{2}-1)} + M_2 p^{\frac{(r-1)}{2}}$.

The proof of Theorem 3.2.1 applies the triangular inequality to the Theorem 3.1.6. Up until this theorem, we have obtained the way to count number of solutions to (1) and made estimations on the number. As connection to later sections, Theorem 3.2.1 will also help us on counting points on algebraic curves on projective hypersurface.

After finishing counting the number of solutions to the discussed Diophantine equations over F_p, in the rest of the paper, we will consider the number of solutions to the equations over more general finite fields. However, we will not focus entirely on finding out the formula to count as in the previous sections. One of our goal in this paper is to relate the number of solutions to Diophantine equations to the Riemann Hypothesis through zeta functions.

we will first try to understand the pojective hypersurface. Then we will the zeta function on a hypersurface related to a polynomial, and see how the zeta function is analogous to the Riemann zeta function.

4 Number of Points in Projective Space

In this section, we try to understand the projective space, and why we care about "points at infinity". This section provides background knowledge in the future calculation of zeta functions.

Definition 4.1 Let F be a field and let *affine n-space* be the set of all n-tuples $(a_1, a_2, \cdots, a_n)$ with each $a_i \in F$.

With the above definition, we can see the affine n-space as a vector space over F and each $n-$tuple as a point. The next concept *projective space* is more extensively used in the later discussions.

Definition 4.2 Consider the set $A^{(n+1)}(F)\backslash\{0\}$. Now pick two points $(a_0, a_1, \cdots, a_n)$ and $(b_0, b_1, \cdots, b_n)$ in this set. We define an equivalence relation between the two points as the following: $(a_0, a_1, \cdots, a_n)$ and $(b_0, b_1, \cdots, b_n)$ are equivalent if there is an $\gamma \in F^*$ such that $a_i = \gamma b_i$ for all $0 \neq i \neq n$. A *projective space* $P^n(F)$ is defined to be the set of all equivalence classes in $A^{(n+1)}(F)\backslash\{0\}$. Each equivalence class is called a point in $P^n(F)$.

Let F be a field with q elements. With basic field theory, we know that $P^n(F)$ has $q^n + q^{n-1} + \cdots + q + 1$ points. Clearly $P^n(F)$ has more points than $A^n(F)$. Pick a point $x = (x_0, x_1, \cdots, x_n) \in P^n(F)$. If $x_0 \neq 0$, consider a map ϕ such that $\phi(x) = (\frac{x_1}{x_0}, \frac{x_2}{x_0}, \cdots, \frac{x_n}{x_0})$ which falls in $A^n(F)$.

Definition 4.3 Let $\bar{H}$ be the set of points $x \in P^n(F)$ such that $x_0 = 0$. The set $\bar{H}$ is called the plane at infinity.

It is not hard to show that the map ϕ is a bijection from $P^n(F) - \bar{H}$ to $A^n(F)$. Moreover, we can say that $P^n(F)$ contains a copy of $A^n(F)$ and a copy of $P^{n-1}(F)$.
Next, we are going to relate the points in the projective space with polynomials. The most important object is *projective hypersurface*. Moreover, within projective space, we are particularly dealing with *homogeneous* polynomials.

Definition 4.4 Let $F[x_1, x_2, \ldots, x_n]$ be a polynomial ring in variables x_i's over field F. Let $f(x) \in F[x_1, x_2, \ldots, x_n$ be a polynomial. Write f as $f(x) = \sum_{(i_1,i_2,\cdots,i_n)} a_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. f is said to be *homogeneous* if the sums $\sum_{k=1}^{n} i_k$ over all $n-$tuple indices $(i_1, \cdots, i_n)$ are the same.

Now suppose $K \supseteq F$ is a field. Let $f(x) \in F[x_1, x_2, \ldots, x_n]$ be a polynomial and let a be a point in $A^n(K)$. Then plug in each coordinate of a into f and calculate $f(a)$. If $f(a) = 0$, we say a is a zero of $f(x)$. With the map f, we will define *projective hypersurface*.

Definition 4.5 Let $f(x)$ be a nonzero polynomial and define $\bar{H}_{\bar{f}}(F) = \{a \in A^n(F) \mid f(a) = 0\}$. $\bar{H}_{\bar{f}}(F)$ is called the *projective hypersurface* defined by f in $A^n(F)$.

Remark L et $f \in F[x_1, x_2, \ldots, x_n]$If we define $\bar{f}(y) = \bar{f}(y_0, y_1, \ldots, y_n)$ by $\bar{f}(y) = y_0^{\deg(f)} f\big(\frac{y_1}{y_0}, dots, \frac{y_n}{y_0}\big)$. Then $\bar{f}$ is homogeneous. This will be a widely used method of transforming a polynomial into homogenous one when working in projective hypersurface.

Now we are interested in the number of points a curve on the hypersurface, which is the same as the number of solutions to a Diophantine equation over a given field. When we count the number of points, we should not forget about the points at infinity, namely the point with $x_0 = 0$.

Recall the last theorem in Section 3 where we obtained a generalized formula for equation $a_1 x_1^{l_1} + a_2 x_2^{l_2} + \cdots + a_r x_r^{l_r} = b$. With the definition of projective hypersurface, we derive the following theorem from Theorem 3.2.1.

Theorem 4.6 Suppose F is a field with q elements with $q \equiv 1 \pmod{m}$. The homogeneous equation $a_0 x_0^m + a_1 x_1^m + \cdots + a_n x_n^m = 0$, $a_0, a_1, \cdots, a_n \in F^*$, defines a hypersurface in $P^n(F)$. The number of points on this hypersurface is given by

$$q^{n-1} + q^{n-2} + \cdots + q + 1 + \frac{1}{q-1} \sum_{\chi_0, \chi_1, \cdots, \chi_n} \chi_0(a_0^{-1}) \cdots \chi_n(a_n^{-1}) J_0(\chi_0, \chi_1, \cdots, \chi_n),$$

where $\chi^m = \varepsilon, \chi_i \neq \varepsilon$, and $\chi_0 \chi_1 \cdots \chi_n = \varepsilon$. Moreover, under these conditions, $J_0(\chi_0, \chi_1, \cdots, \chi_n) = \frac{1}{q} g(\chi_0) g(\chi_1) \cdots g(\chi_n)$.

Example 4.7 Let $f = -y_0^2 + y_1^2 + y_2^2 + y_3^2$ be a polynomial on $F[y_0, y_1, y_2, y_3]$ with F a field of q elements. Consider the projective hypersurface $\bar{H}_{\bar{f}}(F)$ defined by f. Then the number of points on this hypersurface $N_1 = q^2 + q + 1 + \chi(-1)\frac{1}{q} g(\chi)^4$. We know χ is of order 2. Thus $g(\chi)^2 = \chi(-1)q$. Thus $N_1 = q^2 + 1 + 1 + \chi(-1)q$.

Example 4.8 We use this example to review the Diophantine equation $x^n + y^n = 1$ that we analyzed in the first part of the paper. Write this equation in homogeneous form in a projective space. Now we have $x_1^n + x_2^n = x_0^n$. Suppose $(0, x_1, x_2)$ is a point at infinity. Then we need to solve $x_1^n = -x_2^n$ in a projective space. If -1 is a n^th power, then $x_1^n = (-x_2)^n$ and there are n solutions. If -1 is not a solution, then the equation does not have solutions. Therefore, the number of points at infinity is the same as the function $n\delta_n(-1)$ where

$$\delta_n(-1) = \begin{cases} 1 & \text{if -1 is an } n^{\text{th}} \text{ power} \\ 0 & \text{otherwise.} \end{cases}$$

as in Section 2.3.

5 Zeta Functions

In this section, we will introduce zeta functions defined on different objects. Most of the zeta functions here are based on number of points of a curve over different fields. One important topic in this section is the Weil's conjecture by André Weil [5], which is based on the Hasse-Davenport relation and has been proved now. The Weil's conjectures connects the rationality of zeta functions on algebraic curves to the Riemann Hypothesis. The zeta functions also reveal analogies to the Riemann Hypothesis.

5.1 Zeta Functions on Projective Hypersurface

For notation in this section, let F be a field with q elements and $f \in F[x_0, x_1, \cdots, x_n]$ be a homogeneous polynomial. Let field F_k be the field containing F with q^k elements. Let N_k be the number of zeros of f in $P^n(F_k)$.

Definition 5.1.1 The *zeta function* of the hypersurface defined by f is the series given by

$$Z_f(u) = \exp(\sum_{s=1}^{\infty} \frac{N_s u^s}{s}).$$

Example 5.1.2 Consider homogeneous equation $y_0^3 + y_1^3 + y_2^3 = 0$ over F_p where p is a prime and $p \equiv 1 \pmod 3$. Let homogenerous polynomial $f(y) = y_0^3 + y_1^3 + y_2^3$,

$$N_1 = p + 1 + \frac{1}{p} g(\chi)^3 + \frac{1}{p} g(\chi^2)^3$$

where χ is a cubic character on F_p.

In section 3, we have proved the following lemma.

Lemma 5.1.3 Let $\pi = J(\chi, \chi)$ where χ is a cubic character on F_p, then $g(\chi)^3 = p\pi$ and $\pi\bar{\pi} = p$.

With Lemma 5.1.3, we have $N_1 = p + 1 + \pi + \bar{\pi}$. However, in zeta function $Z_f(u)$, we need to know all of the N_s for $s = 0, 1, 2, \ldots$ The Hasse-Davenport relation proves the correctness of N_s that we will state immediately for all $s \in \mathbb{N}$. Let us assume the Hasse-Davenport relation at this moment. We state that

$$N_s = p^s + 1 - (-\pi)^s - (-\bar{\pi})^s.$$

Then we derive the zeta function on f from Example 5.1.2 to be

$$Z_f(u) = \frac{(1 + \pi u)(1 + \bar{\pi} u)}{(1 - u)(1 - pu)}.$$

Luckily, we have $Z_f(u)$ to be a rational function for this f, and the zeros of the zeta function in this case are $-\pi^{-1}$ and $-\bar{\pi}^{-1}$, both with absolute value $p^{-1/2}$.

The Weil's conjectures[5] say that if f is a degree-d non-singular nonzero homogeneous polynomial on algebraic extension of F on variables $x_0, x_1, \cdots, x_n$, then $Z_f(u)$ is a rational function of form

$$\frac{P(u)^{(-1)^n}}{(1 - u)(1 - qu) \ldots (1 - q^{n-1}u)},$$

with $P(u)$ having degree $(d-1)(d-2)/2$ and all zeros have absolute value $q^{(n-1)/2}$. In exploring the rationality of the zeta function, with the expansion of the zeta function, we may set $Z_f(u) = \frac{P(u)}{Q(u)}$ where P, Q are polynomials. Since $Z(0) = 1$, we have $P(0) = Q(0)$. On the other hand, since expansion around 0 has left only constant terms, we have $P(0) = Q(0) = 1$. Assume that $Z_f(u) = \frac{\Pi_i}{}(1 - \alpha_i u)\Pi_j\ (1 - \beta_j u)$ where α_i, β_j are complex.

Proposition 5.1.4 The zeta function is rational if and only if there exists complex numbers α_i and β_j such that

$$N_s = \sum_j \beta_j^s \ - \sum_i \alpha_i^s.$$

Remark We are not proving for this proposition in detail here. The main idea from Ireland and Rosen[3] is to evaluate the zeta function in two ways. Evaluate the zeta function by both its definition and the factorization. Take logarithmic derivative and compare the coefficients in the expanded geometric series. It is noteworthy that this technique of taking logarithmic derivative and comparing coefficients used in proving this proposition is extensively used in learning zeta functions.

5.2 Analogy to Riemann Zeta Function

In this subsection, we will define prime divisors on an algebraic variety, and find the analogy between zeta function on the algebraic variety and the Riemann zeta function.
Let F be a finite field with q elements and let V be an algebraic set in affine space $A^n(F)$. Then the zeta function of V is

$$N_V(u) = \exp(\sum_{s=1}^{\infty} \frac{N_s u^s}{s})$$

where N_s denotes the number of points in $A^n(F_{q^s})$ satisfying equations that defines V. Now let $K \supset F$ be an s-degree extension over F. extend V to the algebraic set in $A^n(K)$ without changing the notation. Thus V has N_s points with their coordinates in K.

Definition 5.2.1 If $\alpha = (a_1, a_2, \cdots, a_n) \in V$, let F_{q^d} be the smallest field containing F and $a_1, a_2, \cdots, a_n$. We say that α is a point of degree d. A *prime divisor* on V is a set, denoted by β, of the form $\{\alpha^{q^j} | j = 0, 1, 2, \cdots, d-1\}$ where α is a point on V of degree d. We also define b_d to be the number of prime divisors on V of degree d. Denote prime divisors by $\mathfrak{B}$ and its degree by d.

Now we state the following proposition:

Proposition 5.2.2 $Z_V(u) = \Pi_{\mathfrak{B}} \ (\frac{1}{1-u^{\deg \mathfrak{B}}})$

Proof. Based on our definition of b_d in Definition 5.2.1, we have

$$\Pi_{\mathfrak{B}} \ (\frac{1}{1-u^{\deg \mathfrak{B}}}) = \Pi_{n=1}^{\infty} \ \big(\frac{1}{1-u^n}\big)^{b_n}. \tag{2}$$

Take logarithmic derivative of the right hand side of (2) and we have

$$\begin{aligned} \frac{1}{u} \sum_{n=1}^{\infty} \frac{n b_n u^n}{1-u^n} &= \frac{1}{u} \sum_{n=1}^{\infty} n b_n (u^n + u^{2n} + u^{3n} + \dots) \\ &= \frac{1}{u} \sum_{n=1}^{\infty} \big(\sum_{d|n} d b_d\big) u^n \end{aligned}.$$

Compare with the coefficients of each term of u^n in $Z_V(u)$. We want to show that $N_s = \sum_{d|s} \ db_d$.

Lemma 5.2.3 $N_s = \sum_{d|s} \ db_d$.

Proof to Lemma I f we fix a base field of F_{q^s}, the prime divisors are disjoint and of same size, therefore partitioning the algebraic set V. Notice that subfields of F_{q^s} are all of size q^d where $d|s$. On the other hand, for a fixed α, the smallest subfield of F_{q^s} that α lies in defines a unique prime divisor with degree $d|s$. Thus with the definition of b_d in Definition 5.2.1, we have $N_s = \sum_{d|s} \ db_d$. With the completion of the lemma, the proposition holds.

□

Remark If we let $u = q^{-s}$, we have $Z(q^{-s}) = \Pi_{\mathfrak{B}} \ (\frac{1}{1-q^{-s \deg \mathfrak{B}}}) = \Pi_{\mathfrak{B}} \ \frac{1}{1-(\frac{1}{q^{\deg \mathfrak{B}}})^s}$. Here we can see an the zeta function has an analogy with the expression of the Riemann zeta function, which is defined as $\zeta(s) = \sum_{n=1}^{\infty} \ n^{-s} = \Pi_p \ (1-p^{-s})^{-1}$.

5.3 Hasse-Davenport Relation

As mentioned earlier, we counted N_s on the assumption of the Hasse-Davenport Relation. This relation[1] is proved with manipulation of characters and Gauss sums. And the significance of the relation is that it tells us the number of zeros of a homogeneous polynomial of type $a_0x_0^m + a_1x_1^m + \cdots + a_nx_n^m$ over different fields F_{q^s} in its projective hypersurface. Here F_{q^s} is the s^{th} extension of the field F_q.

In this section, we will not present a complete proof of the Hasse-Davenport relation[1]. Instead, we will make more attempt to understand the significance of the theorem and how it relates to the rationality of zeta funcion. Let us start from stating the theorem.

Definition 5.3.1 Let F be a field with q elements and E is an s^{th} extension of F. If $\alpha \in \mathbb{E}$, the *trace* of α from $\mathbb{E}$ to F is defined as $tr(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{s-1}}$. The *norm* of α is defined as $N_{E/F}(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^{s-1}}$.

Let χ be a nontrivial character of F and define $\chi' = \chi \circ N_{F_{q^s}/F}$. Thus χ' is a character of F_{q^s}. Then the Hasse-Davenport relation states that

Theorem 5.3.2 $(-g(\chi))^s = -g(\chi')$.

Now we return to the homogeneous polynomial $f(x_0, x_1, \ldots, x_n) = a_0x_0^m + a_1x_1^m + \cdots + a_nx_n^m$. For convenience, assume that $q \equiv 1 \pmod{m}$. By Theorem 4.6, we have that

$$N_s = \sum_{i=0}^{n-1} \ q^{si} + \frac{1}{q^s} \sum_{\chi_0^{(s)}, \cdots, \chi_n^{(s)}} \chi_0(a_0^{-1}) \cdots \chi_n^{(s)}(a_n^{-1}) g(\chi_0^{(s)}) \cdots g(\chi_n^{(s)}).$$

From Ireland and Rosen[3], the Hasse-Davenport relation and the above expression of N_s show that

$$N_s = \sum_{k=0}^{n-1} \ q^{ks} + (-1)^{n+1} + \sum_{\chi_0, \ldots, \chi_n} [\frac{(-1)^{n+1}}{q} \chi_0(\alpha_n^{-1}) \cdots \chi_n(\alpha_n^{-1}) g(\chi_0) \cdots g(\chi_n)]^s.$$

Besides giving out a clean expression of N_s with just characters and Gauss sums, this expansion of N_s coincides with the expression of Proposition 5.1.4. Then with Prop 5.1.4, the zeta function $Z_f(u)$ will be rational. In fact, Ireland and Rosen[3] tells us that under this condition,

$$Z_f(u) = \frac{P(u)^{(-1)^n}}{(1-u)(1-qu)\cdots(1-q^{n-1}m)}.$$

The results brought by the Hasse-Davenport takes the $Z_f(u)$ to an analogy with the zeta function.

6 Elliptic Curves

In this section, we will first learn about elliptic curves over fields and their zeta functions. Then we will find their relation to the Riemann Hypothesis. In the end, we will study two widely studied curves of form $y^2 = x^3 + D$ and $y^2 = x^3 - Dx$, and focus on the number of points on them.

Definition Consider a curve defined by a homogeneous polynomial $f(x_0, x_1, \ldots, x_n) \in F[x_0, x_1, \ldots, x_n]$ where K is a field. *Elliptic curves* are non-singular cubic curves $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ if there is at least one rational root.

The next definition explains nonsingularity on algebraic geometry.

Definition Let L be a field that contains K. A point a in the projective hypersurface $\bar{H}_f(L)$ is called *nonsingular* if there is no solution to the equations

$$\frac{\partial f}{\partial x_i} = 0 \quad \textit{for all } 0 \leqslant i \leqslant n.$$

If a curve in $f[x_0, x_1, \ldots, x_n]$ is *nonsingular*, all the points in $\bar{H}_F(L)$ are *nonsingular* for any extensions L of K. all the points in of the form $y^2 = x^3 + ax + b$ over $\mathbb{Q}$.

Remark We will use the notation $E(L)$ instead of $\bar{H}_F(L)$. WHile there are many interesting aspects of elliptic curves to be read about, we are more focused on the number theoretic aspects.

With the technique of completing the cube on a cubic elliptic curve over field K, we can transform the curve into the form $x_0x_2^2 = x_1^3 - Ax_0^2x_1 - Bx_0^3, \qquad A, B \in K$. However, we will see terms with coefficients $\frac{1}{2}$ and $\frac{1}{3}$. Therefore, when the characteristic of K is not 2 or 3, we can transform every elliptic curve into the above form. $(0, 0, 1)$ is the only point at infinity and the affine form of the curve is $y^2 = x^3 - Ax - B$. More details could be find in [4]

Now we are interested in the behavior of an elliptic curve E defined over field F_p where $p \nmid \Delta$. $\Delta = 16(4A^3 - 27B^2)$ is the discriminant. Let E_p denote the reduction of E modulo p.

6.1 Zeta Functions of Elliptic Curves

In this section, we will introduce two kinds of zeta functions related to elliptic curves. We will also see an equivalence related to Riemann Hypothesis for algebraic curves over finite fields.

Let N_{p^m} denote the number of points in $E_p(F_{p^m})$. If we see all points on the curve form an algebraic set, we have that the zeta function

$$Z(E_p, u) = exp\Big(\sum_{m=1}^{\infty} \frac{N_{p^m}u^m}{m}\Big).$$

Elliptic curves are of genus[2] 1. According to Ireland and Rosen[3], by the Riemann-Roch theorem[4], we can prove that

$$Z(E_p, u) = \frac{1 - a_pu + pu^2}{(1 - u)(1 - pu)}, \quad a_p \in \mathbb{Z}.$$

Write $1 - a_pu + u = (1 - \alpha u)(1 - \beta u)$ where α and β are complex conjugates. Then $\alpha + \beta = a_p$ and $\alpha\beta = p$. What interests us is the Hasse's theorem which says $|N_p - (p + 1)| \leqslant 2\sqrt{p}$. The significance of the Hasse's theorem is that it is connected with the Riemann Hypothesis for elliptic curves.
Before proving the equivalence, we first see how N_{p^m} is calculated. With the common technique of logarithmic derivation, we have $N_{p^m} = p^m + 1 - \alpha^m - \beta^m$. For N_p, we will have $N_p = p + 1 - \alpha - \beta$.

Proposition 6.1.1 The Hasse's theorem for N_p is the equivalent statement to Riemann Hypothesis for elliptic curves.

Proof. Suppose that $\alpha + \beta \leqslant 2\sqrt{p}$. Notice that α, β are the two roots of the quadratic equation $x^2 - a_px + p = 0$. Therefore, the discriminant $\Delta = (\alpha + \beta)^2 - 4\alpha\beta = (\alpha - \beta)^2$. Since α and β are complex conjugates, this forces $\Delta \leqslant 0$. Clearly, the two roots exists. Thus $\Delta = 0$, and the zeros of the zeta function $Z(E_p, u)$ lie on

the circle of radius
$frac1\sqrt{p}$ on the complex plane. This implies the Riemann Hypothesis for elliptic curves, which says $|\alpha| = |\beta| = \sqrt{p}$.
On the other hand, if we assume the Riemann Hypothesis for elliptic curves, then $|\alpha| = |\beta| = \sqrt{p}$. Then $|N_p - 1 - p| = |\alpha + \beta| \leqslant 2\sqrt{p}$. □

Definition 6.1.2 For $p \nmid \Delta$, substitute u with s^{-s} in $Z(E_p, p^{-s})$. Then define the result as the *local zeta function of E at p*,

$$\zeta(E_p, s) = \frac{1 - a_p p^{-s} + p^{1-2s}}{(1 - p^{-s})(1 - p^{1-s})}.$$

For $p \mid \Delta$, define

$$\zeta(E_p, s) = \frac{1}{(1 - p^{-s})(1 - p^{1-s})}.$$

Definition 6.1.3 The *global zeta function* is defined as the product of the local zeta functions over all primes.

$$\zeta(E, s) = \Pi_p \, \zeta(E_p, s).$$

Since $\zeta(s) = \Pi_p$
$frac11 - p^{-s}$, we can write

$$\zeta(E, s) = \zeta(s)\zeta(s-1)\Pi_{p \nmid \Delta} \, (1 - a_p \, p^{-s} + p^{1-2s}).$$

The product part gives rise to a new concept.

Definition 6.1.4 The function $L(E, s) = \Pi_{p \nmid \Delta} \, (1 - a_p \, p^{-s} + p^{1-2s})^{-1}$ is defined as the *L-function of E*.

Now we are interested in a general formula for the number of solution of elliptic curves over finite field F_p and integral solutions over $\mathbb{Z}$. The previous case is called the *local case* while the latter one is called the *global case*. We are looking into curves of form $y^2 = x^3 + D$ and $y^2 = x^3 - Dx$ where in both forms D is an integer. In the local cases, we will finally reach the goal of proving that the number of points on these curves can be completely determined with the help of Jacobi sums. Meanwhile, for the global cases, we will also care about analytic continuation.

6.2 Local case for $y^2 = x^3 + D$

For this curve E, the discriminant $\Delta = -s^4 3^3 D^2$, so we only need to restrict primes p such that $p \neq 2$ or 3 and $p \nmid D$. Restrict the curve under mod p, and denote the E_p by $y^2 = x^3 + \bar{D}$ with $\bar{D}$ being the equivalence class of D under modulo p. This curve E has only one point at infinity, $(x_0, x_1, x_2) = (0, 0, 1)$. Therefore, $N_p = 1 + N(y^2 = x^3 + \bar{D})$. So Now we need to consider two cases of $p \equiv 1$ and 2 mod 3. If $p \equiv 2$ mod 3, then $\phi : \, x \to x^3$ is an automorphism on F_p^*. Thus $N(E_p) = N(y^2 = x + D) = p + 1$.
On the other hand, if $p \equiv 1$ mod 3, let χ be a character of order 3 and ρ a character of order 2. Then with findings in earlier sections,

$$N(y^2 = x^3 + D) = p + \sum_{a+b=D} \rho(a)\chi(b) + \sum_{a+b=D} \rho(a)\chi^2(b).$$

Let $a = Da'$ and $b = Db'$ to use Jacobi sums, we have

$$N_p = p + 1 + \rho\chi(D)J(\rho, \chi) + \overline{\rho\chi(D)}\overline{J(\rho, \chi)}.$$

At this point, we can say that the number of solutions of this curve over finite field is determined up to p. In some cases, we can write out the Jacobi sums explicitly.

6.3 Local case for $y^2 = x^3 - Dx$

Similar to the analysis for the previous local case, we first find out the discriminant $\Delta = 2^6 D^3$ and there is only one point at infinity (0,0,1). Therefore, we have $N_p = 1 + N(y^2 = x^3 - \bar{D}x.)$ Thus we consider primes such that $p \neq 2$ and $p \nmid D$ this time. For this curve, we use a more complicated way by setting up a bijective map[3].
Let the curve $y^2 = x^3 - Dx$ be denoted by C and consider the curve $u^2 = v^4 + 4D$ denoted by C'. Define the map $T(u, v) = (\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)$ and the map $S(x, y) = (2x - \frac{y^2}{x^2}, \frac{y}{x})$. Let number of points on C be N and that on C' be N'. With simple calculation, it can be shown that $N = N' + 1$ because (0,0) can only be mapped one way. Again, we consider the congruence of p. Let λ be a character on F_p of order 4. If $p \equiv 1 \bmod 4$, by similar calculation, we have

$$N = \sum_{a+b=4D} N(u^2 = a)N(v^4 = -b) = p - 1 + \lambda(\overline{-4D})J(\rho, \lambda) + \lambda(-4D)\overline{J(\rho, \lambda)}.$$

If $p \equiv 3 \bmod 4$, $N_p = 2 + N' = 2 + p - 1 = p + 1$ because of the method of descent. Now we have proved that in this case, the number of points on this elliptic curve can also be completely determined.

6.4 Improvement on N_p

In the past two subsections, we were able to write N_p for both curves in terms of Jacobi sums. Ireland and Rosen[3] showed that we can actually do better and write out N_p in local cases with explicit functions. Once again, identities linked to characters, Gauss sums and Jacobi sums are the crucial part.

For both cases, developing the explicit functions needs cubic reciprocity and higher power residue symbols. Here we present the function from Ireland and Rosen[3] as following.

Theorem 6.4.1 Suppose $p \neq 2$ or 3, and $p \nmid D$. Consider the elliptic curve $y^2 = x^3 + D$ over F_p. If $p \equiv 2 \pmod 3$ then $N_p = p + 1$. If $p \equiv 1 \pmod 3$, let $p = \pi\bar{\pi}$ with $\pi \in \mathbb{Z}[\omega]$ and $\pi \equiv 2 \pmod 3$. Then

$$N_p = p + 1 + \left(\frac{\overline{4D}}{\pi}\right)_6 \pi + \left(\frac{4D}{\pi}\right)_6 \bar{\pi}.$$

Theorem 6.4.2 Suppose $p \neq 2$ and $p \nmid D$. Consider the elliptic curve $y^2 = x^3 - Dx$ over F_p. If $p \equiv 3 \pmod 4$ then $N_p = p + 1$. If $p \equiv 1 \pmod 4$, let $p = \pi\bar{p}i$ with $\pi \in \mathbb{Z}[i]$ and $\pi \equiv 1 \pmod{()2 + 2i}$. Then

$$N_p = p + 1 - \left(\frac{\bar{D}}{\pi}\right)_4 \pi - \left(\frac{D}{\pi}\right)_4 \bar{\pi}.$$

Now we replace the ξ in Lemma 6.4.1 and replace it with a character χ of order 3 in N_p at the end of subsection 6.2. $N_p = p + 1 + \rho\chi(D)\chi(4)J(\chi, \chi) + \overline{\rho\chi(D)}\chi(4)\overline{J(\chi, \chi)}$. Since $\rho(4) = 1$, $\rho\chi(D)\chi(4) = \rho\chi(4)$.

6.5 Hecke L-function and the Global Cases

Similar to the local cases, in global cases we can still prove that the number of points on the elliptic curve over $\mathbb{Z}$ is deterministic. But the analysis on the global cases, by Ireland and Rosen[3], requires the $L-$function we defined earlier in this section and *Hecke L-function.* about the analytic continuation of the L-function.

7 More Topics

From the reading on the topic of number of solutions to Diophantine equations, we are mostly dealing with equations of the well-formed kind $\sum_{i=1}^{n} a_i x_i^{l_i} = b$. We can explore on complicated equations. As for the

connection between various zeta functions and Riemann Hypothesis, more could be studied with some taste in analytic number theory and complex analysis. We can also think about construction in algebraic number theory to express some characters and Jacobi sums as explicit functions as in the Section 6.4.

References

[1] H. Davenport and H. Hasse. "Die Nullstellen der Kongruenz Zetafunktion in gewissen zyklischen Fällen". In: *J. Reine und Angew. Math.* 175 (1935).

[2] *Genus(Mathematics)*. URL: https://en.wikipedia.org/wiki/Genus_(mathematics).

[3] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, New York, NY, 1990.

[4] Silverman Joseph H. *The Arithmetic of Elliptic Curves*. Springer, New York, NY, 2009.

[5] André Weil. "Numbers of solutions of equations in finite fields". In: *Bull. Amer. Math. Soc.* 55.5 (May 1949), pp. 497–508. URL: https://projecteuclid.org:443/euclid.bams/1183513798.