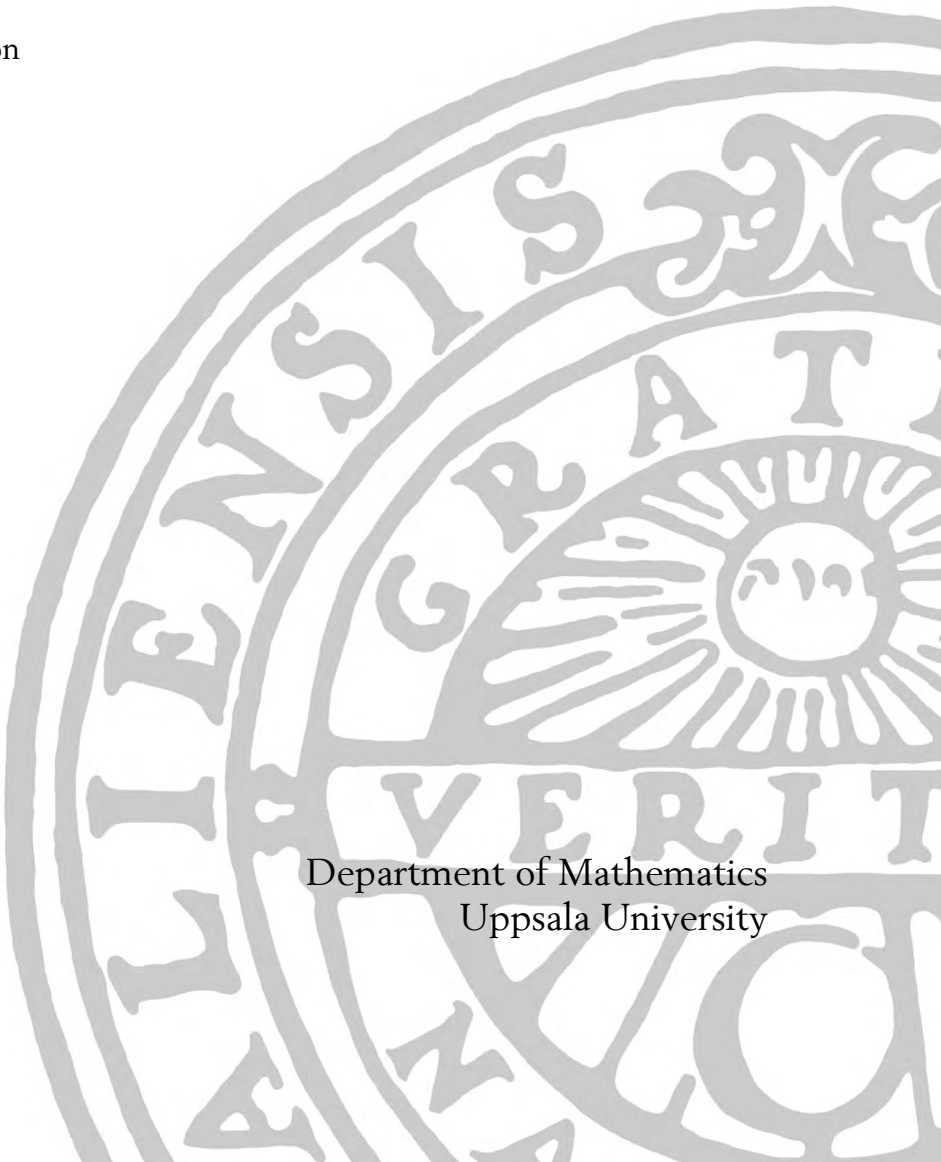
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2018:19

Gauss and Jacobi Sums and the Congruence Zeta Function

Einar Waara

Examensarbete i matematik, 15 hp
Handledare: Andreas Strömbergsson
Examinator: Martin Herschend
Juni 2018



Department of Mathematics
Uppsala University

GAUSS AND JACOBI SUMS AND THE CONGRUENCE ZETA FUNCTION

BACHELOR'S THESIS
DEPARTMENT OF MATHEMATICS
UPPSALA UNIVERSITY

EINAR WAARA

Contents

Date: January 2018.

1. Introduction

The German mathematician Carl Friedrich Gauss (1777-1855) was the first to introduce the notion of what is now called quadratic Gauss sums, which are sums of the form $g_a = \sum_{t \in F_p} (t/p) e^{2\pi i a t/p}$, where F_p is the finite field of order p and $(\cdot/p)$ is the quadratic reciprocity symbol. Among many other things, Gauss proved that g_1 takes the values $\sqrt{p}$ or $i\sqrt{p}$ when $p \equiv 1\ (4)$ or $p \equiv 3\ (4)$ respectively. These sums can be, and have been, greatly generalized and appear very often in areas related to modern number theory, in the study of theta functions and the discrete Fourier transform for instance. In this exposition we present an introduction to the theory of Gauss and Jacobi sums (and their interrelations) and apply these notions to study the (congruence) zeta function. We give a proof of the Hasse-Davenport relation, which is a lifting relation relating the Gauss sums of two different finite fields. We outline a proof of a special case of the first part of the Weil conjectures (named after André Weil (1906-1998)) proved in 1959 by Bernard Dwork (1923-1998), which states that *any* algebraic set V has a rational zeta function $Z_V(u)$. We state (and prove) a characterization of rational zeta functions $Z_f(u)$ and use this characterization to prove that $Z_f(u)$ is rational when $f(x_0 \ldots, x_n) = a_0 x_0^m + a_1 x_1^m + \ldots + a_n x_n^m$ where $a_0, \ldots, a_n \in F^*$ and F is a finite field of order $q \equiv 1\ (m)$. We also further display the potency of Gauss and Jacobi sums by providing a short proof of the famous law of quadratic reciprocity, a theorem first proved by Gauss (who refereed to it as the "golden theorem") and who subsequently provided five additional proofs, the final of which was published in 1818. This exposition is greatly inspired by the excellent classic

IR. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1990.

This is the main reference for the present thesis.

2. Prerequisite Theory

Here we present some basic definitions and results from elementary number theory for future reference. We start with the concept of a quadratic residue.

Definition 1. Let $a \in \mathbb{Z}$ and suppose $(a, m) = 1$. Then a is called a **quadratic residue** modulo m if $x^2 \equiv a\ (m)$ has a solution, i.e. a is a perfect square modulo m. If a is not a quadratic residue, we say that a is a quadratic nonresidue.

For the remainder of this section, let p be an odd prime number. Next we define a convenient symbol for dealing with quadratic residues.

Definition 2. The **Legendre symbol** $(\cdot/p)$ is defined by

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \\ 0 & \text{if } p \mid a \end{cases}$$

Proposition 2.1. *(IR, 5.1.2)*

(I) $a^{(p-1)/2} \equiv (a/p)\ (p)$

(II) $(ab/p) = (a/p)(b/p)$

(III) $a \equiv b\ (p) \implies (a/p) = (b/p)$

Proof. Assume that $p \nmid a$ and $p \nmid b$ (if not, the proof is trivial). Since $a^{p-1} \equiv 1\ (p)$ we have $(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) = a^{p-1} - 1 \equiv 0\ (p)$ and thus $a^{(p-1)/2} \equiv \pm 1\ (p)$. By a well-known fact we have $a^{(p-1)/2} \equiv 1\ (p)$ if and only if a is a quadratic residue modulo p. The second part is easily proved using the first. The third part is trivial. ∎

Corollary 2.2. *(IR, 5.1.2 corollary) Modulo p there is an equal number of quadratic residues as there are quadratic nonresidues.*

Proof. The equation $a^{(p-1)/2} \equiv 1\ (p)$ has $(p-1)/2$ solutions, hence there are $(p-1)/2$ quadratic residues and $p - 1 - \big((p-1)/2\big) = (p-1)/2$ quadratic nonresidues. ∎

Corollary 2.3. *(IR, 6.3 lemma 2)* $\sum_{t=0}^{p-1}(t/p) = 0$.

Proof. $p \mid 0$ so $(0/p) = 0$ by definition. Thus there are $p - 1$ (p odd so that $p - 1$ even) terms of ± 1's left, and we know these terms cancel by the previous corollary. ∎

Let F be a finite field of order q.

Proposition 2.4. *(IR, 7.1.2) The equation $x^n = \alpha \in F^*$ is solvable if and only if $\alpha^{(q-1)/d} = 1$, where $d = (n, q-1)$. If the equation is solvable, then there are d solutions.*

Proof. The multiplicative group F^* of F is cyclic. Let g be a generator of F^*. Set $\alpha = g^a$ and $x = g^b$ for some $a, b \in \{1, 2, \ldots, q-1\}$. Substituting this into the equation yields $g^{nb} = g^a$ if and only if $g^{nb-a} = 1$, thus $q - 1 \mid nb - a$ i.e. $nb \equiv a\ (q-1)$, which proves the result by basic facts about congruences. ∎

2.1. Multiplicative Characters.

The definitions of Gauss and Jacobi sums rely on the notion of a multiplicative character, we therefore provide a brief introduction of this topic here. We follow [IR, Ch. 8.1].

Definition 3. A multiplicative character on F_p is a group homomorphism from the multiplicative group of F_p to the multiplicative group of the complex numbers: $\chi : F_p^* \longrightarrow (\mathbb{C} \setminus \{0\}, \times)$.

The Legendre symbol can therefore be regarded a special case of a character.

The set of characters on F_p constitute a group under the following definitions. Let λ and χ be characters. We define $\lambda\chi$ as the map $a \mapsto \lambda(a)\chi(a)$, and χ^{-1} as $a \mapsto \chi(a)^{-1}$. The identity will be denoted by ϵ and is characterized by $\epsilon(a) = 1$ for all $a \in F_p^*$. It will be useful to extend the domain and let $\chi(0) = 0$ for all $\chi \neq \epsilon$ while $\epsilon(0) = 1$. Notice that this is in accordance with the Legendre symbol. We shall denote the group of characters on F_p by Ω_p. Since we are now dealing with a group, we naturally define the order of a character as the smallest positive integer n such that $\chi^n = \epsilon$. The Legendre symbol is thus a character of order two.

It turns out that Ω_p is a cyclic group of order $p-1$. In order to prove this, we need a few basic results easily proved from the definitions.

Proposition 2.5. *Let $\chi \in \Omega_p$ and $a \in F_p^*$, then*

(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. $\chi(1) = \chi(1^2) = \chi(1)^2$ and since $\chi(1) \neq 0$ we have $\chi(1) = 1$. Also, since $|F_p^*| = p-1$ we have $a^{p-1} = 1$ and thus $\chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1} = 1$. Lastly $\chi(a^{-1})\chi(a) = \chi(a^{-1}a) = \chi(1) = 1$ hence $\chi(a)^{-1} = \chi(a^{-1})$. The complex number $\chi(a)$ lies on the unit circle in $\mathbb{C}$ since $|\chi(1)| = |\chi(a^{p-1})| = |\chi(a)^{p-1}| = |\chi(a)|^{p-1} = 1$ implies $|\chi(a)| = 1$. Due to the definition of complex multiplication we have $\chi(a)^{-1} = \overline{\chi(a)}$. ∎

Proposition 2.6. *Let $\chi \in \Omega_p$, then* $\sum_{t \in F_p} \chi(t) = \begin{cases} 0 & \text{if } \chi \neq \epsilon \\ p & \text{otherwise} \end{cases}$

Proof. The equality is trivial when $\chi = \epsilon$. If $\chi \neq \epsilon$, then there is some $a \in F_p^*$ such that $\chi(a) \neq 1$. Then $\chi(a)\sum_{t \in F_p} \chi(t) = \sum_{t \in F_p} \chi(at) = \sum_{t \in F_p} \chi(t)$, hence $\sum_{t \in F_p} \chi(t) = 0$. ∎

Proposition 2.7. *Ω_p is a cyclic group of order $p-1$.*

Proof. We show that there exists a generator to Ω_p. The multiplicative group F_p^* is cyclic. Let $g \in F_p^*$ be a generator. If $a \in F_p^*$ then $a = g^l$ for some $l \in \{0, 1, \ldots, p-1\}$. Thus any character $\chi \in \Omega_p$ is completely determined by its action on g since $\chi(a) = \chi(g^l) = \chi(g)^l$. In general the number of n'th roots of unity is n. Hence since $\chi(g) \in \mathbb{C} \setminus \{0\}$ is a $(p-1)$st root of unity, it follows that $|\Omega_p| \leq p-1$. We claim that a generator to Ω_p is given by $\lambda(g^k) = e^{2\pi i(k/(p-1))}$. Firstly λ is well defined since $\lambda(g^{k+p-1}) = \lambda(g^k)e^{2\pi i} = \lambda(g^k)$. Since $\lambda(g^{k_1}g^{k_2}) = \lambda(g^{k_1})\lambda(g^{k_2})$ we also know that λ is character, hence $\lambda \in \Omega_p$. We now show that λ is a character of order $p-1$. Assume that $\lambda^n = \epsilon$. Then $\lambda^n(g) = \lambda(g)^n = e^{2\pi i n/(p-1)} = \epsilon(g) = 1$ thus $(p-1) \mid n$. Now, $\lambda^{p-1}(a) = \lambda(a)^{p-1} = \lambda(a^{p-1}) = \lambda(1) = 1$ thus $\lambda^{p-1} = \epsilon$. There are no smaller positive integers which divide $p-1$ than $p-1$ itself. Thus $p-1$ is the smallest positive integer n such that $\lambda^n = \epsilon$ and therefore the order of λ is $p-1$. Hence we know that $\epsilon, \lambda, \lambda^2, \ldots, \lambda^{p-2}$ are all distinct members of Ω_p and since there are $p-1$ of them and $|\Omega_p| \leq p-1$ we know that $\Omega_p = p-1$. Thus λ is indeed a generator, and hence Ω_p is cyclic. ∎

Remark. Let $a \in F_p^* \setminus \{1\}$ then $a = g^l$ for some $l \in \{1, 2, \ldots, p-2\}$, so $p-1 \nmid l$. Thus $\lambda(a) = \lambda(g)^l = e^{2\pi i(l/(p-1))} \neq 1$. We conclude that given $a \in F_p^* \setminus \{1\}$ there is always some character χ such that $\chi(a) \neq 1$. This is crucial for the following corollary.

Corollary 2.8. *If $a \in F_p^* \setminus \{1\}$ then* $\sum_{\chi \in \Omega_p} \chi(a) = 0$.

Proof. Let z be the complex number $\sum_{\chi\in\Omega_p}\chi(a)$. Since $a\neq 1$ there is (by the remark above) some character χ such that $\chi(a)\neq 1$, thus

$$\lambda(a)z=\sum_{\chi\in\Omega_p}\lambda(a)\chi(a)=\sum_{\chi\in\Omega_p}\lambda\chi(a)=z.$$

The last equality holds since $\{\lambda\chi\}_{\chi\in\Omega_p}=\Omega_p$. This follows from the implication $\lambda\chi_1=\lambda\chi_2\implies\chi_1=\chi_2$. Thus, since $\lambda(a)\neq 1$, we see that $z=0$. ∎

We shall see how characters can be used in the study of equations in finite fields. The following proposition is an early tool in this direction.

Proposition 2.9. *If $a\in F_p^*$, $n|p-1$ and the equation $x^n=a$ is unsolvable, then there is a character χ such that $\chi^n=\epsilon$ and $\chi(a)\neq 1$.*

Proof. Let g and λ be as in the proof of proposition 2.7. We know that $a=g^l$ for some l and by assumption $x^n=a$ is not solvable, thus $n\nmid l$ (otherwise $g^{l/n}$ would be a solution). Let $\chi=\lambda^{(p-1)/n}$. Then $\chi(g)=\lambda(g)^{(p-1)/n}=e^{2\pi i/n}$ and thus $\chi(a)=\chi(g)^l=e^{2\pi i(l/n)}\neq 1$. Lastly $\chi^n=\lambda^{p-1}=\epsilon$ since λ was determined to be a generator to Ω_p. ∎

Let $N(x^n=a)$ denote the number of solutions to the equation $x^n=a$ in F_p. The following proposition will be a useful tool for counting the number of solutions to more complicated equations in F_p and will be used often.

Proposition 2.10. *If $n\mid p-1$, then $N(x^n=a)=\sum_{\chi^n=\epsilon}\chi(a)$ where the sum is taken over all characters χ such that $\chi^n=\epsilon$.*

Proof. If χ is a character such that $\chi^n=\epsilon$, then $\chi(g)\in\mathbb{C}$ is a n'th root of unity since $\chi(g)^n=\chi^n(g)=\epsilon(g)=1$. Thus there are at most n such characters in Ω_p. But in the previous proposition we defined $\chi=\lambda^{(p-1)/n}$ which meant that $\chi(g)=e^{2\pi i/n}$, thus $\epsilon,\chi,\chi^2,\ldots,\chi^{n-1}$ are n distinct characters, all of order n. Thus, these are the characters in the sum of consideration. To prove the equality we consider three cases. First, if $a=0$, clearly there is only one solution to $x^n=a$, namely $x=0$. Since $\chi(0)=0$ except for when $\chi=\epsilon$ which maps 0 to 1 the equality holds in this case. Next, assume $a\neq 0$ and that the equation $x^n=a$ is solvable. Let b be a solution, then $\chi(a)=\chi(b^n)=\chi(b)^n=\epsilon(b)=1$ and thus $\sum_{\chi^n=\epsilon}\chi(a)=n=N(x^n=a)$. Lastly, assume that $a\neq 0$ and that the equation $x^n=a$ is unsolvable. By proposition 2.9, there is a $\rho\in\Omega_p$ such that $\rho^n=\epsilon$ and $\rho(a)\neq 1$. We have $\{\chi:\chi^n=\epsilon\}<\Omega_p$, thus $\rho(a)\sum_{\chi^n=\epsilon}\chi(a)=\sum_{\chi^n=\epsilon}\chi\rho(a)=\sum_{\chi^n=\epsilon}\chi(a)$, hence $\big(\rho(a)-1\big)\big(\sum_{\chi^n=\epsilon}\chi(a)\big)=0$ which proves the result. ∎

2.2. **Basic Notions from Algebraic Geometry.** In order to discuss the congruence zeta function, we need some fundamental definitions from algebraic geometry. We follow [IR, Ch. 10.1]. For the remainder of this section, let F be a field of order q.

Definition 4. $A^n(F)=\{(a_1,a_2,\ldots,a_n):a_i\in F \text{ for } i=1,2,\ldots,n\}$ is called the **affine n-space** over F.

$A^n(F)$ can be considered to be a vector space over F with the usual definitions of scalar multiplication and vector addition. Let us consider $A^{n+1}(F)\setminus\{(0,0,\ldots,0)\}$ and define an equivalence relation $\sim$ on this set by

$$(a_0,a_1,\ldots,a_n)\sim(b_0,b_1,\ldots,b_n)\iff\exists\gamma\in F^*\text{ such that }a_i=\gamma b_i\text{ for }i=0,1,\ldots,n.$$

Definition 5. $P^n(F)=\big(A^{n+1}(F)\setminus\{(0,0,\ldots,0)\}\big)\big/\!\sim$ is called the **projective n-space** over F. The equivalence class of $a\in A^{n+1}(F)\setminus\{(0,0,\ldots,0)\}$ is denoted by $[a]$.

The size of the affine n-space is q^n, while the size of the projective n-space is $\frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \ldots + q + 1$.

A homogeneous polynomial $f(x_1, x_2, \ldots x_n) = \sum_{(i_1,i_2,\ldots,i_n)} a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ in $F[x_1, x_2, \ldots, x_n]$ is one where each nonzero term have the same degree.

For the rest of this section, let $F \subseteq K$ be a field extension. Given some nonzero (not necessarily homogeneous) polynomial $f \in F[x_1, x_2, \ldots x_n]$ we can view it as a function $f : A^n(K) \longrightarrow K$ by evaluating f at points in $A^n(K)$ in the usual way.

Definition 6. $H_f(K) = \{a \in A^n(K) : f(a) = 0\}$ is called the **affine hypersurface** of f in $A^n(K)$.

Let $g \in F[x_0, x_1, \ldots, x_n]$ be some homogeneous polynomial of degree d.

Definition 7. $\overline{H}_g(K) = \{[a] \in P^n(K) : g(a) = 0\}$ is called the **projective hypersurface** of g in $P^n(K)$.

The set $\overline{H}_g(K)$ is well defined since if $\gamma \in F^*$ we have $g(\gamma x) = \gamma^d g(x)$. This is because g is homogeneous of degree d. Thus if $g(a) = 0$ for some representative a in $[a]$, then g maps all elements in that equivalence class to 0.

We define a similar set as above, but for several polynomials instead of only one. In words, it is the set of common zeros to a finite set of polynomials. Let $f_1, f_2, \ldots, f_m \in F[x_1, x_2, \ldots, x_n]$.

Definition 8. $V = \{a \in A^n(K) : f_j(a) = 0 \text{ for } j = 1, 2, \ldots, m\}$ is called an **algebraic set** defined over K.

2.3. **Trace and Norm in Finite Fields.** In this short section we provide some basic definitions and results which we will need later. We follow [IR, Ch. 11.2]. Let F be a field of order $q = p^n$ and let $E \supseteq F$ be a field of order q^s.

Definition 9. The **trace** of $\alpha \in E$ from E to F is defined as $tr_{E/F}(\alpha) = \sum_{i=0}^{s-1} \alpha^{q^i}$ and the **norm** of α from E to F is defined as $N_{E/F}(\alpha) = \prod_{i=0}^{s-1} \alpha^{q^i}$.

Proposition 2.11. *Let $\alpha, \beta \in E$ and $a \in F$, then*

(I) $tr_{E/F}(\alpha) \in F$

(II) $tr_{E/F}(\alpha + \beta) = tr_{E/F}(\alpha) + tr_{E/F}(\beta)$

(III) $tr_{E/F}(a\alpha) = a\ tr_{E:F}(\alpha)$

(IV) $tr_{E/F} : E \longrightarrow F$ *is a surjective mapping.*

(V) $N_{E/F}(\alpha) \in F$

(VI) $N_{E/F}(\alpha\beta) = N_{E/F}(\alpha)N_{E/F}(\beta)$

(VII) $N_{E/F}(a\alpha) = a^s N_{E/F}(\alpha)$

(VIII) $N_{E/F} : E^* \longrightarrow F^*$ *is a surjective mapping.*

Proof. We prove the last part. Note that $N_{E/F}$ is a group homomorphism, so that $\alpha \in ker(N_{E/F})$ if and only if $N_{E/F}(\alpha) = \prod_{i=0}^{s-1} \alpha^{q^i} = \alpha^{(q^s-1)/(q-1)} = 1$. By proposition 2.4 we know that the equation $x^{(q^s-1)/(q-1)} = 1$ has $(q^s - 1)/(q - 1)$ solutions in E^*. The first isomorphism theorem gives $|im(N_{E/F})| = |E^*|/|ker(N_{E/F})| = q - 1 = |F^*|$, hence $N_{E/F}$ is indeed surjective. ∎

3. Gauss and Jacobi Sums

We start by introducing the notion of Gauss and Jacobi sums over F_p, after which we widen our view and consider Gauss and Jacobi sums over arbitrary finite fields of order $q = p^r$. We then give a short proof of the law of quadratic reciprocity using Gauss and Jacobi sums. We follow [IR, Ch. 8.2-7].

3.1. Gauss Sums.

Let $\chi \in \Omega_p$, $a \in F_p$ and $\zeta = e^{2\pi i/p}$.

Definition 10. A sum of the form $\sum_{t\in F_p} \chi(t)\zeta^{at}$ is called a Gauss sum belonging to the character χ and will be denoted $g_a(\chi)$, and $g_1(\chi)$ in particular will be denoted $g(\chi)$.

Lemma 3.1. $\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p & \text{if } a \equiv 0 \ (p) \\ 0 & \text{otherwise} \end{cases}$

Proof. If $a \equiv 0 \ (p)$ then a/p is an integer so $\zeta^a = 1$, hence $\sum_{t=0}^{p-1} \zeta^{at} = p$. Otherwise, if $a \not\equiv 0 \ (p)$, then $\zeta^a \neq 1$ and $\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap}-1}{\zeta^a-1} = 0$. ∎

Notice that, as suggested by the notation, the Gauss sum depends on two objects: a and χ. The following proposition gives some insight in how the Gauss sum behaves with respect to these in extreme cases.

Proposition 3.2.

(I) $a \neq 0$ *and* $\chi \neq \epsilon \implies g_a(\chi) = \chi(a^{-1})g_1(\chi)$

(II) $a \neq 0$ *and* $\chi = \epsilon \implies g_a(\epsilon) = 0$

(III) $a = 0$ *and* $\chi \neq \epsilon \implies g_0(\chi) = 0$

(IV) $a = 0$ *and* $\chi = \epsilon \implies g_0(\epsilon) = p$

Proof. We prove each statement in turn. Notice that $\chi(a)g_a(\chi) = \chi(a)\sum_{t\in F_p} \chi(t)\zeta^{at} = \sum_{t\in F_p} \chi(at)\zeta^{at} = g_1(\chi)$. Multiplying both sides by $\chi(a)^{-1} = \chi(a^{-1})$ proves the first statement. Next we see that $g_a(\epsilon) = \sum_{t\in F_p} \epsilon(t)\zeta^{at} = \sum_{t\in F_p} \zeta^{at} = 0$ by lemma 3.1, this proves the second statement. Lastly, $g_0(\chi) = \sum_{t\in F_p} \chi(t)$, hence the third and fourth statement both follow from proposition X. ∎

Proposition 3.3. *If* $\chi \neq \epsilon$, *then* $|g(\chi)| = \sqrt{p}$.

Proof. Our strategy will be to evaluate the sum

$$S = \sum_{a\in F_p} g_a(\chi)\overline{g_a(\chi)}$$

in two different ways. First, suppose that $a \neq 0$, then we have

$$\begin{aligned} g_a(\chi)\overline{g_a(\chi)} &= \chi(a^{-1})g(\chi)\overline{\chi(a^{-1})g(\chi)} \\ &= \chi(a^{-1})g(\chi)\chi(a)\overline{g(\chi)} \\ &= |g(\chi)|^2. \end{aligned}$$

By proposition 3.2 we have $g_0(\chi) = 0$, thus $S = (p-1)|g(\chi)|^2$. Next we use the definition 10 directly to get

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

thus, by lemma 3.1 we have

$$\sum_a \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\delta(x,y)p = (p-1)p$$

where $\delta(x,y) = 1$ if $x \equiv y\ (p)$ and $\delta(x,y) = 0$ if $x \not\equiv y\ (p)$. Equating these two different ways of expressing S proves the result. ■

3.2. **Jacobi Sums and Applications.** We define the Jacobi sum and show how it can be used to count the solutions to certain equations over F_p. Let $\chi_1, \ldots, \chi_k \in \Omega_p$.

Definition 11. A sum of the form $J(\chi_1, \ldots, \chi_k) = \sum_{t_1+\ldots+t_k=1} \chi_1(t_1)\cdots\chi_k(t_k)$ is called a Jacobi sum.

We start by considering the familiar equation $x^2 + y^2 = 1$ where $x, y \in F_p$. Let $N(x^2+y^2 = 1)$ denote the number of solutions to this equation. First, notice that $N(x^2+y^2=1) = \sum_{a+b=1} N(x^2=a)N(y^2=b) = \sum_{a+b=1}(1+(a/p))(1+(b/p)) = p + \sum_a(a/p) + \sum_b(b/p) + \sum_{a+b=1}(a/p)(b/p) = p + \sum_{a+b=1}(a/p)(b/p)$ where the last equality follows from corollary 2.3. We are left with evaluating the sum

$$\sum_{a+b=1} (a/p)(b/p). \tag{1}$$

Let us pause this problem for a moment and consider $N(x^3+y^3=1)$ instead. Again, notice that $N(x^3+y^3=1) = \sum_{a+b=1} N(x^3=a)N(y^3=b)$. Now, if $p \equiv 2\ (3)$ this sum is easily evaluated to be p by proposition 2.4. However if $p \equiv 1\ (3)$ then it is not as simple. Let $\chi \in \Omega_p \setminus \{\epsilon\}$ be a character of order 3. Since $(2,3) = 1$, χ^2 is also a character of order 3. Since Ω_p is cyclic, the number of elements of order $d \mid p-1$ is $\phi(d)$, where ϕ denotes Euler's totient function. Thus there are $\phi(3) = 2$ characters of order 3, and since 3 is prime, a character must have order 3 (or 1) for its order to divide 3. Thus by proposition 2.10 we have

$$\begin{aligned} N(x^3+y^3=1) &= \sum_{a+b=1} \sum_{i=0}^{2} \chi^i(a) \sum_{j=0}^{2} \chi^j(b) \\ &= \sum_i \sum_j \left(\sum_{a+b=1} \chi^i(a)\chi^j(b) \right) \end{aligned} \tag{2}$$

In summary, with both these examples we are eventually forced to deal with a *Jacobi sum.* This motivates the notion of such sums and we shall see how the properties of these sums will allow us to finally evaluate (at least partially) (1) and (2). The following theorem (which we soon shall generalize), provides us with the necessary tools for this purpose. Part four shows how the Jacobi and Gauss sums are related in an surprisingly simple way.

Theorem 3.4. *Let $\chi, \lambda \in \Omega_p \setminus \{\epsilon\}$. Then*

(I) $J(\epsilon, \epsilon) = p$

(II) $J(\epsilon, \chi) = 0$

(III) $J(\chi, \chi^{-1}) = -\chi(-1)$

(IV) $\chi\lambda \neq \epsilon \implies J(\chi,\lambda) = \dfrac{g(\chi)g(\lambda)}{g(\chi\lambda)}$

Proof. The first part is trivial since the number of pairs a, b such that $a + b = 1$ is p and the second part follows from proposition 2.6. For part three, notice that

$$\begin{aligned} J(\chi, \chi^{-1}) &= \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \chi(1)\chi^{-1}(0) \ + \sum_{a+b=1 \ \wedge \ b\neq 0} \chi(ab^{-1}) \\ &= \sum_{a\neq 1} \chi\big(a(1-a)^{-1}\big). \end{aligned}$$

Let $c = a(1-a)^{-1}$, then if $c \neq 1$ we have $a = c(1+c)^{-1}$. Hence, when a varies over $F_p \setminus \{1\}$, c varies over $F_p \setminus \{-1\}$. Thus,

$$J(\chi, \chi^{-1}) = \sum_{c\neq -1} \chi(c) = \sum_{c\in F_p} \chi(c) - \chi(-1) = -\chi(-1)$$

by proposition 2.6. To prove the last part, notice that

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

If $t = 0$ then

$$\sum_{x+y=0} \chi(x)\lambda(-x) = \lambda(-1)\sum_x \chi\lambda(x) = 0.$$

If $t \neq 0$, let $x = tX$ and $y = tY$. Then we have

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{X+Y=1} \chi(tX)\lambda(tY) = \sum_{X+Y=1} \chi\lambda(t)\chi(X)\lambda(Y) = \chi\lambda(t)J(\chi, \lambda).$$

Thus,

$$g(\chi)g(\lambda) = J(\chi, \lambda)\sum_t \chi\lambda(t)\zeta^t = J(\chi, \lambda)g(\chi\lambda).$$

■

Corollary 3.5. $\chi, \lambda, \chi\lambda \neq \epsilon \implies |J(\chi, \lambda)| = \sqrt{p}$.

Proof. $|J(\chi, \lambda)| = \left|\dfrac{g(\chi)g(\lambda)}{g(\chi\lambda)}\right| = \dfrac{\sqrt{p}\sqrt{p}}{\sqrt{p}} = \sqrt{p}$ by proposition 3.3. ■

Using these identities, we can definitively evaluate (1) and make further progress with (2). For (1) simply note that an application of part three yields $\sum_{a+b=1}(a/p)(b/p) = -(-1/p) = -(-1)^{(p-1)/2}$. The last equality follows from the first part of proposition 2.1 since

$$(-1)^{(p-1)/2} \equiv (-1/p) \ (p) \iff p \mid (-1)^{(p-1)/2} - (-1/p) \iff (-1)^{(p-1)/2} - (-1/p) = 0.$$

Hence, the number of solutions to $x^2 + y^2 = 1$ in F_p turns out to be

$$N(x^2 + y^2 = 1) = p - (-1)^{(p-1)/2}.$$

We can use the first three parts of proposition 3.4 to simplify (2) as

$$\sum_i \sum_j \left(\sum_{a+b=1} \chi^i(a)\chi^j(b)\right) = p - \chi(-1) - \chi^2(-1) + J(\chi, \chi) + J(\chi^2, \chi^2). \tag{3}$$

Since χ is a character of order 3 we have $\chi(-1) = \chi\big((-1)^3\big) = \chi^3(-1) = \epsilon(-1) = 1$ and $\chi^2 = \chi^{-1} = \overline{\chi}$. Hence

$$J(\chi,\chi) + J(\chi^2,\chi^2) = J(\chi,\chi) + J(\overline{\chi},\overline{\chi}) = \sum_{a+b=1} \chi(ab) + \overline{\sum_{a+b=1} \chi(ab)} = 2\mathfrak{Re}J(\chi,\chi).$$

Thus (3) simplifies to

$$N(x^3 + y^3 = 1) = p - 2 + 2\mathfrak{Re}J(\chi,\chi). \tag{4}$$

Clearly, this is not as precise as the value of $N(x^2 + y^2 = 1)$. However, we can now give a estimate to the number of solutions to $x^3 + y^3 = 1$ in F_p. By corollary 3.5 we have

$$|N(x^3 + y^3 = 1) - p + 2| \leq 2\sqrt{p}. \tag{5}$$

which tells us that, the number of solutions to $x^3+y^3 = 1$ is approximately $p-2$ with an error term $2\sqrt{p}$, hence for large primes p there will always exist many solutions to this equation.

To begin generalizing some of the results above, the following sum will be useful

$$J_0(\chi_1,\ldots,\chi_k) := \sum_{t_1+\ldots+t_k=0} \prod_{i=1}^{k} \chi_i(t_i).$$

This is the same as the Jacobi sum except that $\sum_i t_i = 0$ instead of 1. Also, let $\psi : F_p \longrightarrow \mathbb{C}$ be the map $t \mapsto \zeta^t$, then $\psi(\sum_i t_i) = \prod_i \psi(t_i)$.

Proposition 3.6.

(I) $J_0(\epsilon,\ldots,\epsilon) = J(\epsilon,\ldots,\epsilon) = p^{k-1}$

(II) If some but not all $\chi_i = \epsilon$, *then* $J_0(\chi_1,\ldots,\chi_k) = J(\chi_1\ldots,\chi_k) = 0$

(III) Suppose $\chi_k \neq \epsilon$, *then*

$$J_0(\chi_1,\ldots,\chi_k) = \begin{cases} 0 & \text{if } \prod_{i=1}^{k} \chi_i \neq \epsilon \\ (p-1)\chi_k(-1)J(\chi_1,\ldots,\chi_{k-1}) & \text{otherwise} \end{cases}$$

(IV) $\chi_1,\ldots,\chi_k, \chi_1\cdots\chi_k \neq \epsilon \implies \prod_{i=1}^{k} g(\chi_i) = J(\chi_1,\ldots,\chi_k)g(\prod_{i=1}^{k} \chi_i)$.

Proof. If $k-1$ of the terms in $\sum_i t_i$ is chosen, the last term is uniquely determined by the requirement that the whole sum equals 0 or 1. These $k-1$ terms can be chosen in p^{k-1} ways, this proves part one. For the second part we can assume we have ordered the characters in such a way that $\chi_1,\ldots,\chi_s \neq \epsilon$ and $\chi_{s+1},\ldots,\chi_k = \epsilon$. Then, for $J_0(\chi_1,\ldots,\chi_k)$ we have

$$\sum_{t_1+\ldots+t_k=0} \prod_{i=1}^{k} \chi_i(t_i) = \sum_{t_1,\ldots,t_{k-1}} \prod_{i=1}^{s} \chi_i(t_i) = p^{k-s-1} \prod_{i=1}^{s} \Big(\sum_{t_i \in F_p} \chi_i(t_i) \Big) = 0$$

where the last equality follows from proposition 2.6. The proof for $J(\chi_1,\ldots,\chi_k) = 0$ is similar. To prove part three we rewrite $J_0(\chi_1,\ldots,\chi_k)$ as

$$J_0(\chi_1,\ldots,\chi_k) = \sum_s \Big(\sum_{t_1+\ldots,t_{k-1}=-s} \prod_{i=1}^{k-1} \chi_i(t_i) \Big) \chi_k(s) \tag{6}$$

where $s \neq 0$ since this term gets deleted by $\chi_k(0) = 0$. Thus we may define T_i by $t_i = -sT_i$. This gives

$$\sum_{t_1+\ldots t_{k-1}=-s} \prod_{i=1}^{k-1} \chi_i(t_i) = \prod_{j=1}^{k-1} \chi_j(-s) \sum_{T_1+\ldots+T_{k-1}=1} \prod_{i=1}^{k-1} \chi_i(T_i) = \prod_{j=1}^{k-1} \chi_j(-s) J(\chi_1,\ldots,\chi_{k-1}), \tag{7}$$

substituting the last expression in (7) into (6) yields

$$J_0(\chi_1,\ldots,\chi_k) = \chi_1\cdots\chi_{k-1}(-1)J(\chi_1,\ldots,\chi_{k-1})\sum_{s\neq 0}\chi_1\cdots\chi_k(s).$$

If $\prod_{i=1}^k \chi_i \neq \epsilon$ then $\sum_{s\neq 0}\chi_1\cdots\chi_k(s) = 0$, otherwise the sum equals $p-1$ by proposition (2.6). Also, $\chi_1\cdots\chi_{k-1}(-1) = \pm 1$ and $\chi_k(-1) = \pm 1$. In the case when $\prod_{i=1}^k \chi_i \neq \epsilon$ then $\chi_1\cdots\chi_{k-1}(-1)\chi_k(-1) = \epsilon(-1) = 1$ hence we can replace $\chi_1\cdots\chi_{k-1}$ with χ_k.

To prove part four, notice that

$$\prod_i g(\chi_i) = \prod_i\Big(\sum_{t_i}\chi_i(t_i)\psi(t_i)\Big) = \sum_s\Big(\sum_{t_1+\ldots+t_k=s}\prod_i\chi_i(t_i)\Big)\psi(s). \tag{8}$$

Since by assumption $\chi_1,\ldots,\chi_k \neq \epsilon$, part three above implies that $\sum_{t_1+\ldots+t_k=s}\prod_i\chi_i(t_i) = 0$ if $s = 0$, so we can suppose $s \neq 0$ and define $t_i = sT_i$ as before. Then

$$\sum_{t_1+\ldots+t_k=s}\prod_i\chi_i(t_i) = \sum_{T_1+\ldots+T_k=1}\chi_1\cdots\chi_k(s)\prod_i\chi_i(T_i) = \chi_1\cdots\chi_k(s)J(\chi_1,\ldots,\chi_k), \tag{9}$$

substituting the last expression in (9) into (8) gives

$$\prod_i g(\chi_i) = J(\chi_1,\ldots,\chi_k)\sum_{s\neq 0}\chi_1\cdots\chi_k(s)\psi(s) = J(\chi_1,\ldots,\chi_k)g(\prod_i\chi_i).$$

■

Part four has a couple of corollaries of interest.

Corollary 3.7. *Suppose that $\chi_1,\ldots,\chi_k \neq \epsilon$ and $\chi_1\cdots,\chi_k = \epsilon$ then*

$$\prod_{i=1}^k g(\chi_i) = p\chi_k(-1)J(\chi_1,\ldots,\chi_{k-1}).$$

Proof. Use part four of proposition 3.6 and multiply both sides by $g(\chi_k)$. Note that if $k = 2$ we have $J(\chi_1) = 1$ in the right hand side, by definition.

Corollary 3.8. *Under the same assumptions as in corollary 3.7 we have*

$$J(\chi_1,\ldots,\chi_k) = -\chi_k(-1)J(\chi_1,\ldots,\chi_{k-1}).$$

Proof. The case when $k = 2$ is the content of theorem 3.4 part three, hence suppose $k > 2$. Use equations (8) and (9) above combined with the assumptions to get

$$\begin{aligned}\prod_i g(\chi_i) &= J_0(\chi_1,\ldots,\chi_k) + \sum_{s\neq 0}\Big(\sum_{t_1+\ldots+t_k=s}\prod_i\chi_i(t_i)\Big)\psi(s)\\ &= J_0(\chi_1,\ldots,\chi_k) + \sum_{s\neq 0}\epsilon(s)J(\chi_1,\ldots,\chi_k)\psi(s)\\ &= J_0(\chi_1,\ldots,\chi_k) + J(\chi_1,\ldots,\chi_k)\sum_{s\neq 0}\psi(s)\\ &= J_0(\chi_1,\ldots,\chi_k) - J(\chi_1,\ldots,\chi_k)\end{aligned}$$

where the last equality follows from part two of proposition 3.2. By corollary 3.7 and part three of proposition 3.6 we have

$$\begin{aligned}p\chi_k(-1)J(\chi_1,\ldots,\chi_{k-1}) &= J_0(\chi_1,\ldots,\chi_k) - J(\chi_1,\ldots,\chi_k)\\ &= (p-1)\chi_k(-1)J(\chi_1,\ldots,\chi_{k-1}) - J(\chi_1,\ldots,\chi_k).\end{aligned}$$

which concludes the proof. ■

Theorem 3.9. *If $\chi_1,\ldots,\chi_k \neq \epsilon$, then*

(I) $\chi_1 \cdots \chi_k \neq \epsilon \implies |J(\chi_1, \ldots, \chi_k)| = p^{(k-1)/2}$.

(II) $\chi_1 \cdots \chi_k = \epsilon \implies |J_0(\chi_1, \ldots, \chi_k)| = (p-1)p^{(k/2)-1}$ *and* $|J(\chi_1, \ldots, \chi_k)| = p^{(k/2)-1}$.

Proof. Since each $\chi_i \neq \epsilon$ we have by proposition 3.3 $|g(\chi_i)| = \sqrt{p}$ for each $i \in \{1, 2, \ldots, k\}$. Thus

$$|J(\chi_1, \ldots, \chi_k)| = \frac{\prod_i |g(\chi_i)|}{|g(\chi_1, \ldots, \chi_k)|} = \frac{\sqrt{p}^k}{\sqrt{p}} = p^{(k-1)/2}.$$

For the second part note that

$$J_0(\chi_1, \ldots, \chi_k) = (p-1)\chi_k(-1)J(\chi_1, \ldots, \chi_{k-1}).$$

by proposition 3.6 part three. Since $\chi_1 \cdots \chi_{k-1} \neq \epsilon$ we have by corollary 3.7 and 3.8

$$|J_0(\chi_1, \ldots, \chi_k)| = \frac{(p-1)\prod_i |g(\chi_i)|}{p} = \frac{(p-1)\sqrt{p}^k}{p} = (p-1)p^{(k/2)-1}$$

and

$$|J(\chi_1, \ldots, \chi_k)| = |-\chi_k(-1)J(\chi_1, \ldots, \chi_{k-1})| = \frac{\prod_i |g(\chi_i)|}{p} = \frac{\sqrt{p}^k}{p} = p^{(k/2)-1}.$$

■

We now consider the most general case needed for our purposes, namely the number of solutions N to the equation $a_1x_1^{n_1} + a_2x^{n_2} + \ldots + a_kx_k^{n_k} = b$ where $a_1, \ldots, a_k \in F_p^*$ and $b \in F_p$. Here is the main theorem of this section, and we will see later how it will be useful for our study of the congruence zeta function.

Theorem 3.10.

(I) $b = 0 \implies N = p^{k-1} + \sum \prod_{i=1}^{k} \chi_i(a_i^{-1})J_0(\chi_1, \ldots, \chi_k)$ *where the sum is over all k-tuples* $(\chi_1, \ldots, \chi_k)$ *where* $\chi_i \neq \epsilon$, $\chi_i^{n_i} = \epsilon$ *for* $i = 1, 2, \ldots, k$ *and* $\chi_1 \cdots \chi_k = \epsilon$. *If* M *is the number of such k-tuples, then* $|N - p^{r-1}| \leq M(p-1)p^{(k/2)-1}$.

(II) $b \neq 0 \implies N = p^{r-1} + \sum \chi_1 \cdots \chi_k(b) \prod_{i=1}^{k} \chi_i(a_i^{-1})J(\chi_1, \ldots, \chi_k)$ *where the sum is over all k-tuples* $(\chi_1, \ldots, \chi_k)$ *where* $\chi_i \neq \epsilon$ *and* $\chi_i^{n_i} = \epsilon$ *for* $i = 1, 2, \ldots, k$. *If* M_1 *is the number of such k-tuples with* $\chi_1 \cdots \chi_k = \epsilon$ *and* M_2 *is the number of such k-tuples with* $\chi_1 \cdots \chi_k \neq \epsilon$, *then* $|N - p^{r-1}| \leq M_1p^{(k/2)-1} + M_2p^{(k-1)/2}$.

Proof. Let $L(u) = L(u_1, \ldots, u_k) = \sum_{i=1}^{k} a_iu_i$ and $N_i(u_i) = N(x_i^{n_i} = u_i)$. Similarly as before, notice that

$$N = \sum_{L(u)=b} N_1(u_1)N_2(u_2) \cdots N_k(u_k) \tag{10}$$

where the sum is over all k-tuples $u = (u_1, \ldots, u_k)$ such that $L(u) = b$. By proposition 2.10 we know that

$$N_i(u_i) = \sum_{\chi_i} \chi_i(u_i)$$

where χ_i ranges over all character of order dividing n_i. Inserting this into equation (10) gives

$$N = \sum_{L(u)=b} \left(\sum_{\chi_1} \chi_1(u_1) \cdots \sum_{\chi_k} \chi_k(u_k) \right) = \sum_{\chi_1, \ldots, \chi_k} \sum_{L(u)=b} \chi_1(u_1) \cdots \chi_k(u_k). \tag{11}$$

We consider the two cases $b = 0$ and $b \neq 0$ separately. If $b = 0$ we define $t_i = a_i u_i$, then

$$\begin{aligned}\sum_{L(u)=b} \chi_1(u_1)\cdots\chi_k(u_k) &= \sum_{t_1+\ldots+t_k=0} \chi_1(t_1)\chi_1(a_1^{-1})\cdots\chi_k(t_k)\chi_k(a_k^{-1}) \\ &= \chi_1(a_1^{-1})\cdots\chi_k(a_k^{-1}) \sum_{t_1+\ldots+t_k=0} \chi_1(t_1)\cdots\chi_k(t_k) \\ &= \chi_1(a_1^{-1})\cdots\chi_k(a_k^{-1}) J_0(\chi_1,\ldots,\chi_k). \qquad (12)\end{aligned}$$

If $b \neq 0$ we define $t_i = b^{-1}a_i u_i$, then

$$\begin{aligned}\sum_{L(u)=b} \chi_1(u_1)\cdots\chi_k(u_k) &= \sum_{t_1+\ldots+t_k=1} \chi_1(a_1^{-1})\chi_1(b)\chi(t_1)\cdots\chi_k(a_k^{-1})\chi_k(b)\chi(t_k) \\ &= \chi_1\cdots\chi_k(b)\chi_1(a_1^{-1})\cdots\chi_k(a_k^{-1}) J(\chi_1,\ldots,\chi_k). \qquad (13)\end{aligned}$$

Now, in the first case (11) becomes

$$\sum_{\chi_1,\ldots,\chi_k} \chi_1(a_1^{-1})\cdots\chi_k(a_k^{-1}) J_0(\chi_1,\ldots,\chi_k) \qquad (14)$$

If $\chi_i = \epsilon$ for all i, then $J_0(\chi_1,\ldots,\chi_k) = p^{k-1}$. If some but not all $\chi_i = \epsilon$ then $J_0(\chi_1,\ldots,\chi_k) = 0$ and if $\prod_{i=1}^k \chi_i \neq \epsilon$ then $J_0(\chi_1,\ldots,\chi_k) = 0$, all this follows directly from proposition 3.6. Given these facts we are left with the expression for N as stated in the theorem. If $b \neq 0$ the proof is similar. Both estimates follow directly from the fact that (for any $\chi \in \Omega_p$ and $a \in F_p^*$) $|\chi(a)| = 1$ since $\chi(a)$ is a $(p-1)$st root of unity by proposition 2.5. ■

Using the tools outlined in the earlier sections, we can generalize the notions of Gauss and Jacobi sums in the following way. Let F be an arbitrary finite field of order $q = p^r$. Let $\psi : F \longrightarrow \mathbb{C}$ be the map $\alpha \mapsto \zeta_p^{tr_{F/F_p}(\alpha)}$, where $F_p = \mathbb{Z}/p\mathbb{Z}$ and $\zeta_p = e^{2\pi i/p}$. The multiplicative group of any finite field is cyclic, thus the propositions of multiplicative characters (which hinges on this fact) naturally extend to fields of arbitrary order, simply replace p with q. Given the following definition, the same extension to arbitrary finite fields is also valid for Gauss sums, Jacobi sums and the interrelations we saw between them earlier in this section. Let χ be a character of F and $\alpha \in F^*$.

Definition 12. A sum of the form $\sum_{t\in F} \chi(t)\psi(\alpha t)$ is called a Gauss sum on F belonging to the character χ and will be denoted $g_\alpha(\chi)$.

Note that this definition reduces to the previous one if $F = F_p$. To generalize the definition of Jacobi sums, simply let the characters be characters on F instead of F_p.

Next we prove a theorem which will be of great use later on. Consider the equation $f(y_0,\ldots,y_n) = \sum_{i=0}^n a_i y_i^m = 0$ where $a_i \in F^*$. This is a homogeneous equation, so it defines a hypersurface $\overline{H}_f(F) \subseteq P^n(F)$.

Theorem 3.11. *Suppose F is a finite field of order $q \equiv 1\ (m)$. Then*

$$|\overline{H}_f(F)| = \sum_{i=0}^{n-1} q^i + \frac{1}{q-1} \sum_{\chi_0,\ldots,\chi_n} \left(J_0(\chi_0,\ldots,\chi_n) \prod_{j=0}^n \chi_j(a_j^{-1}) \right)$$

where the sum is over all $(n+1)$-tuples $(\chi_0,\ldots,\chi_n)$ such that $\chi_i \neq \epsilon$, $\chi_i^m = \epsilon$ and $\chi_0\cdots\chi_n = \epsilon$. Moreover, under the same conditions we also have

$$\frac{1}{q-1} J_0(\chi_0,\ldots,\chi_n) = \frac{1}{q} \prod_{i=0}^n g(\chi_i).$$

Proof. The first part is a corollary of the first part of theorem 3.10, we have

$$|H_f(F)| = q^n + \sum_{\chi_0,\cdots,\chi_n} \prod_i \chi_i(a_i^{-1}) J_0(\chi_0, \ldots, \chi_n). \tag{15}$$

where the sum is over all $(n+1)$-tuples $(\chi_0, \ldots, \chi_n)$ as given by the theorem. The number $|\overline{H}_f(F)|$ is obtained from dividing (15) by $q-1$. For the second part, recall that

$$J_0(\chi_0, \ldots, \chi_n) = \chi_n(-1)(q-1)J(\chi_0, \ldots, \chi_{n-1}) \tag{16}$$

where we have extended proposition 3.6 to fields of arbitrary order q as discussed. By the same proposition we have

$$J(\chi_0, \ldots, \chi_{n-1}) = \frac{g(\chi_0)\cdots g(\chi_{n-1})}{g(\chi_0 \cdots \chi_{n-1})}. \tag{17}$$

Multiply the numerator and denominator of the right hand side of (17) by $g(\chi_n)$ and apply corollary 3.7 to get

$$J_0(\chi_0, \ldots, \chi_{n-1}) = \frac{g(\chi_0)\cdots g(\chi_n)}{g(\chi_0 \cdots \chi_{n-1})g(\chi_n)} = \frac{g(\chi_0)\cdots g(\chi_n)}{\chi_n(-1)q}, \tag{18}$$

substituting (18) into (16) concludes the proof. ■

3.2.1. *A Proof of the Law of Quadratic Reciprocity.* Here we provide an elegant proof of the famous law of quadratic reciprocity, using what we know about Jacobi and Gauss sums.

Theorem 3.12 (Law of Quadratic Reciprocity)**.** *Let p and q be two distinct odd prime numbers, then*

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Proof. Let χ denote the character on F_p of order two. Then $\chi^{q+1} = \epsilon$ since $q+1$ is even. By corollary 3.7 we have

$$g(\chi)^{q+1} = \left(g(\chi)^2\right)^{\frac{q+1}{2}} = p^{\frac{q+1}{2}}(-1)^{\frac{p-1}{2}\frac{q+1}{2}} = p(-1)^{\frac{p-1}{2}} J(\chi, \ldots, \chi)$$

where there are q components in $J(\chi, \ldots, \chi)$. Thus,

$$J(\chi, \ldots, \chi) = \sum_{t_1+\ldots+t_q=1} \chi(t_1)\cdots\chi(t_q) = p^{\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

If $t_1 = \ldots = t_q$, then $t_i = 1/q$ and $\chi(1/q)\cdots\chi(1/q) = \chi(1/q)^q = \chi(q)^{-q} = \chi(q)$. If $t_i \neq t_j$ for at least two indexes, then there are q terms in $J(\chi, \ldots, \chi)$, all of equal value, found by permutating $(t_1, \ldots, t_q)$ cyclicly. Thus in modulo q all of these terms vanish, hence

$$p^{\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \equiv \chi(q) \ (q).$$

Thus,

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}(p/q) \equiv (q/p) \ (q) \tag{19}$$

by proposition 2.1. Since q divides the difference in (19), we must in fact have equality. Multiplying both sides by (p/q) concludes the proof. ■

4. The Zeta Function

E. Artin introduced the concept of the congruence zeta function in 1924. In 1949 A. Weil formulated a set of conjectures known as the Weil conjectures related to the zeta function. The first part of the Weil conjectures states that any algebraic set has a rational zeta function, this was proved in 1959 by B. Dwork.

We define the congruence zeta function, show how it and the Riemann zeta function satisfy analogous relations, and prove that (under certain criteria) $Z_f(u)$ is rational. We follow [IR, Ch. 11.1] and [IR, Ch. 11.3-4].

It can be shown that if F is a finite field of order q then there exists a field $F_s \supseteq F$ of order q^s where $s \geq 1$ is an integer. Given a homogeneous polynomial $f(x) \in F[x_0, x_1, \ldots, x_n]$ we let N_s denote the number $|\overline{H}_f(F_s)|$. We wish to study the numbers N_s by studying the power series $\sum_{s=1}^{\infty} \frac{N_s u^s}{s}$ of a complex variable u. We can (and will) view this as a formal power series, which enables the exclusion of all questions of convergence. However, this is not necessary. Notice that

$$N_s \leq |P^n(F_s)| = \frac{q^{s(n+1)} - 1}{q^s - 1} = \sum_{k=0}^{n} (q^s)^k < (n+1)q^{sn}.$$

If $|u| < q^{-n}$ and $s \geq 1$, then

$$\sum_{s=1}^{\infty} |N_s||u^s| < (n+1) \sum_{s=1}^{\infty} x^s \tag{20}$$

where $0 \leq x = q^n|u| < 1$. Thus (20) converges, i.e. $\sum_{s=1}^{\infty} N_s u^s$ converges absolutely for all $|u| < q^{-n}$.

Definition 13. The zeta function of the hypersurface defined by f is the series given by

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

If the zeta function is expanded about the origin we see that the constant term is 1. We can therefore assume that $Z_f(u) = \frac{p(u)}{q(u)}$ where $p(0) = q(0) = 1$. To see this, assume that is not the case. Then $Z_f(0) = \frac{p(0)}{q(0)} = 1$ if and only if $p(0) = q(0) = c$. Now if $p(u) = \sum_{i=0}^{n} a_i u^i$ and $q(u) = \sum_{i=0}^{m} b_i u^i$ then

$$\frac{p(u)}{q(u)} = \frac{c \sum_{i=0}^{n} c^{-1} a_i u^i}{c \sum_{i=0}^{m} c^{-1} b_i u^i} = \frac{\sum_{i=0}^{n} c^{-1} a_i u^i}{\sum_{i=0}^{m} c^{-1} b_i u^i} = \frac{p'(u)}{q'(u)}$$

where $p'(u)$ and $q'(u)$ have the desired property. Hence the zeta function can be expressed in the form

$$Z_f(u) = \frac{\prod_i (1 - \alpha_i u)}{\prod_j (1 - \beta_j u)} \tag{21}$$

where $\alpha_i, \beta_j \in \mathbb{C}$. We now characterize rational zeta functions, this will be useful later when we consider $Z_f(u)$ for particular homogeneous polynomials f.

Proposition 4.1. *$Z(u) \in \{\frac{p(u)}{q(u)} : p(u), q(u) \in \mathbb{C}[u]\}$ if and only if there exist $\alpha_i, \beta_j \in \mathbb{C}$ such that $N_s = \sum_j \beta_j^s - \sum_i \alpha_i^s$*

Proof. We start by assuming that there exist $\alpha_i, \beta_j \in \mathbb{C}$ such that $N_s = \sum_j \beta_j^s - \sum_i \alpha_i^s$. By inserting this expression for N_s we get

$$\begin{aligned}\sum_{s=1}^{\infty} \frac{N_s u^s}{s} &= \sum_{s=1}^{\infty} \left(\frac{\big(\sum_j \beta_j^s - \sum_i \alpha_i^s\big) u^s}{s} \right) \\ &= \sum_{s=1}^{\infty} \left(\frac{\sum_j (\beta_j u)^s - \sum_i (\alpha_i u)^s}{s} \right) \\ &= \sum_j \left(\sum_{s=1}^{\infty} \frac{(\beta_j u)^s}{s} \right) - \sum_i \left(\sum_{s=1}^{\infty} \frac{(\alpha_i u)^s}{s} \right).\end{aligned}$$

Further simplify the last expression above by using the identity $\sum_{s=1}^{\infty} \frac{z^s}{s} = -ln(1-z)$ to get

$$\sum_i ln(1-\alpha_i u) - \sum_j ln(1-\beta_j u) \tag{22}$$

Finally, to find the zeta function, we exponentiate (22) to get

$$\begin{aligned}Z_f(u) = exp\left(\sum_i ln(1-\alpha_i u) - \sum_j ln(1-\beta_j u) \right) &= \frac{exp\big(\sum_i ln(1-\alpha_i u)\big)}{exp\big(\sum_j ln(1-\beta_j u)\big)} \\ &= \frac{\prod_i exp\big(ln(1-\alpha_i u)\big)}{\prod_j exp\big(ln(1-\beta_j u)\big)} \\ &= \frac{\prod_i (1-\alpha_i u)}{\prod_j (1-\beta_j u)}\end{aligned}$$

which is a rational function of u. We now show the other direction. Suppose therefore that the zeta function is rational so that

$$Z_f(u) = \frac{\prod_i (1-\alpha_i u)}{\prod_j (1-\beta_j u)} \tag{23}$$

where $\alpha_i, \beta_j \in \mathbb{C}$. Take the logarithmic derivative of both sides of (4.1) to get

$$\begin{aligned}\frac{Z_f'(u)}{Z_f(u)} &= \frac{d}{du} ln\left(\frac{\prod_i (1-\alpha_i u)}{\prod_j (1-\beta_j u)} \right) \\ &= \frac{d}{du}\left(\sum_i ln(1-\alpha_i u) - \sum_j ln(1-\beta_j u) \right) \\ &= \sum_i \frac{-\alpha_i}{1-\alpha_i u} - \sum_j \frac{-\beta_j}{1-\beta_j u}.\end{aligned}$$

Multiply the first and last expressions above by u and expand the denominators in the last expression in a geometric series to get

$$\begin{aligned}u\frac{Z_f'(u)}{Z_f(u)} &= \sum_i \frac{-\alpha_i u}{1-\alpha_i u} - \sum_j \frac{-\beta_j u}{1-\beta_j u} \\ &= \sum_i \left(-\alpha_i u \sum_{s=0}^{\infty} (\alpha_i u)^s \right) - \sum_j \left(-\beta_j u \sum_{s=0}^{\infty} (\beta_j u)^s \right) \\ &= \sum_j \sum_{s=1}^{\infty} (\beta_j u)^s - \sum_i \sum_{s=1}^{\infty} (\alpha_i u)^s \\ &= \sum_{s=1}^{\infty} \left(\sum_j \beta_j^s - \sum_i \alpha_i^s \right) u^s.\end{aligned}$$

We now compare this last power series with an alternate way of computing $u\frac{Z_f'(u)}{Z_f(u)}$. By definition $Z_f(u) = exp\sum_{s=1}^{\infty}\frac{N_s u}{s}$. By taking the logarithmic derivative and then multiplying by u we get

$$u\frac{Z_f'(u)}{Z_f(u)} = u\frac{d}{du}\sum_{s=1}^{\infty}\frac{N_s u^s}{s} = \sum_{s=1}^{\infty} N_s u^s,$$

hence we have

$$\sum_{s=1}^{\infty}\left(\sum_j \beta_j^s - \sum_i \alpha_i^s\right)u^s = \sum_{s=1}^{\infty} N_s u^s$$

and thus

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

■

Next we show that N_s is independent of the choice of F_s, so that N_s only depends on s. This is a consequence of the following proposition.

Proposition 4.2. *Let E and E' be field extensions over F of the same order q^s. Then there is an isomorphism $\sigma : E \xrightarrow{\sim} E'$ such that $\sigma\big|_F = id$.*

We can use σ to induce a map from the respective projective n-spaces in a natural way by letting $\overline{\sigma} : P^n(E) \longrightarrow P^n(E')$ map $[\alpha_0, \ldots, \alpha_n] \mapsto [\sigma(\alpha_0), \ldots, \sigma(\alpha_n)]$. This map is well-defined since if $[\alpha_o, \ldots, \alpha_n] = [\beta_0, \ldots, \beta_n]$, then by definition there is some $\gamma \in E^*$ such that $\alpha_i = \gamma\beta_i$ for $i = 0, 1, \ldots, n$, thus $[\sigma(\alpha_0), \ldots, \sigma(\alpha_(n)] = [\sigma(\gamma)\sigma(\beta_0), \ldots, \sigma(\gamma)\sigma(\beta_n)] = [\beta_0, \ldots, \beta_n]$. By virtue of the isomorphic property of σ, $\overline{\sigma}$ is a bijection. Indeed, let $\alpha = [\alpha_0, \ldots, \alpha_n] \in P^n(E')$ be arbitrary, then $\overline{\sigma}$ maps $[\sigma^{-1}(\alpha_0), \ldots, \sigma^{-1}(\alpha_n)] \mapsto \alpha$, hence $\overline{\sigma}$ is surjective. Also, both $P^n(E)$ and $P^n(E')$ are finite sets, hence $\overline{\sigma}$ is injective. It is moreover true that $\overline{\sigma}\big|_{\overline{H}_f(E)}$ is bijection to $\overline{H}_f(E')$. We already know that the restriction is injective. Let $\alpha = [\alpha_0, \ldots, \alpha_n] \in \overline{H}_f(E')$, then $f(\alpha_0, \ldots, \alpha_n) = 0$ and $\overline{\sigma}\big([\sigma^{-1}(\alpha_0), \ldots, \sigma^{-1}(\alpha_n)]\big) = \alpha$. We need to show that $[\sigma^{-1}(\alpha_0), \ldots, \sigma^{-1}(\alpha_n)] \in \overline{H}_f(E)$. Now, σ acts as the identity on F, hence $f\big(\sigma^{-1}(\alpha_0), \ldots, \sigma^{-1}(\alpha_n\big) = \sigma^{-1}\big(f([\alpha_0, \ldots, \alpha_n])\big) = \sigma^{-1}(0) = 0$, hence $[\sigma^{-1}(\alpha_0), \ldots, \sigma^{-1}(\alpha_n)] \in \overline{H}_f(E)$. We conclude that $|\overline{H}_f(E)| = |\overline{H}_f(E')|$ and hence N_s indeed only depends on s as claimed, since this result holds also for the trivial field extensions $F \subseteq F$ and $F \subseteq F' \cong F$.

4.1. **The Zeta Analogy.** The congruence zeta function and the Riemann zeta function satisfy a highly analogous relation. In the case of the Riemann zeta function we have

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p \frac{1}{(1 - \frac{1}{p^s})}, \qquad s > 1$$

where the product is over all primes $p > 0$.

So far we have dealt with the congruence zeta function defined by one polynomial f. Let us now consider it over a set of polynomials $\{f_1, \ldots, f_m\} \subseteq F[x_1, \ldots, x_n]$. Let F be a finite field of order q and let $V = \{a \in A^n(F) : f_j(a) = 0 \text{ for } j = 1, 2, \ldots, m\}$ be an algebraic set in $A^n(F)$.

Definition 14. The function

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

where N_s is the number of points in $A^n(F_s)$ satisfying the equations defined in V, is called the zeta function of V over F.

Let K be the algebraic closure of F. One can show that K is the countable union of isomorphic copies to F_s of order q^s for all positive integers s. It is natural to consider a field containing all fields related to the numbers N_s and K will serve as that field. We can then extend V so that $V \subseteq A^n(K)$ and with N_s points whose coordinates all lie in F_s.

Suppose $a = (a_1, \ldots, a_n) \in V$ and let L be the smallest field containing $F \cup \{a_1, \ldots, a_n\}$. Suppose $|L| = q^d$, we then call a to be a point of degree d.

Lemma 4.3. *The points $a, a^q, \ldots, a^{q^{d-1}}$ all lie in V and are pairwise distinct.*

Proof. Suppose that $a = a^{q^j}$ for some $j \in \{1, 2 \ldots, d-1\}$, and let j be the minimal element with this property. Notice that this implies that $a^{q^{kj}} = a$ for all $k \in \mathbb{Z}_+$. Additionally, we have that $a^{q^d} = a$ since $a_i \in L$ for $i = 1, 2, \ldots, n$. Thus, by the choice of j we have that $j \mid d$. By basic facts about finite fields, there exists a subfield $L' \subseteq L$ of order q^j and since $a = a^{q^j}$ is equivalent to $a_i \in L'$ or $i = 1, 2 \ldots, n$ we have a contradiction by definition of L. This proves that the points $a, a^q, \ldots, a^{q^{d-1}}$ are pairwise distinct.

To show that the points all lie in V, we need to verify that they satisfy the polynomial equations defining V. Let $\psi : L \xrightarrow{\sim} L$ be the automorphism which maps $x \mapsto x^q$, so that $\psi\big|_F = id$. Let $a = (a_1, \ldots, a_n) \in V$ and let $j \in \{1, \ldots, m\}$ correspond to a polynomial defining V. Then, by definition, $f_j(a_1, \ldots, a_n) = 0$. But then $\psi^k(0) = \psi^k\big(f_j(a_1, \ldots, a_n)\big) = f_j\big(\psi^k(a_i), \ldots, \psi^k(a_n)\big) = f_j\big(a_i^{q^k}, \ldots, a_i^{q^k}\big) = 0$. Since this holds for any $j \in \{1, 2, \ldots, m\}$ and $k \in \{1, 2, \ldots, d-1\}$, we are done. ∎

Definition 15. Let $a \in V$ be a point of degree d. A set of the form $\mathfrak{P} = \{a, a^q, \ldots, a^{q^{d-1}}\}$ is called a **prime divisor** on V. The degree of $\mathfrak{P}$ is denoted $\delta(\mathfrak{P})$ and is equal to d.

Proposition 4.4. *Let F be a finite field such that $[F : \mathbb{Z}/p\mathbb{Z}] = n$. Then the subfields of F are in one-to-one correspondence with the divisors of n.*

Lemma 4.5. *$N_s = \sum_{d|s} d n_d$ where n_d is the number of prime divisors on V of degree d.*

Proof. The prime divisors partition V. Let $\alpha \in V$ be a point such that all coordinates lie in F_s. This F_s could be a larger field than necessary i.e. there is some d such that $F_d \subseteq F_s$ is the smallest field such that $\alpha \in F_d$. We know from proposition 4.4 that $d \mid s$, so that α defines a (unique) prime divisor of degree d which is a divisor of s. This proves the lemma. ∎

Now we are in a position to show how the congruence zeta function and the Riemann zeta function bear considerable resemblance.

Theorem 4.6. $Z_V(u) = \prod_{\mathfrak{P}} \dfrac{1}{1 - u^{\delta(\mathfrak{P})}}$.

Proof. By merging the factors corresponding to prime divisors of the same degree, the product can be rewritten as

$$\prod_{k=1}^{\infty} \left(\frac{1}{1-u^k}\right)^{n_k}. \tag{24}$$

By taking the logarithmic derivative of (24) we get

$$\begin{aligned} \frac{d}{du}\left(ln\left(\prod_{k=1}^{\infty}\left(\frac{1}{1-u^k}\right)^{n_k}\right)\right) &= \frac{d}{du}\left(\sum_{k=1}^{\infty} -n_k ln(1-u^k)\right) \\ &= \frac{1}{u}\sum_{k=1}^{\infty} n_k \frac{k u^k}{1-u^k}. \end{aligned}$$

Expand the denominator into a geometric series and compute the coefficient of u^m to get

$$\frac{1}{u}\sum_{m=1}^{\infty}\Big(\sum_{d|m} dn_d\Big)u^m = \sum_{m=1}^{\infty} N_m u^{m-1} \tag{25}$$

by lemma 4.5. Integrating the right hand side of (25) and then taking the exponential concludes the proof. ■

4.2. **The Rationality of the Zeta Function.** In this section we prove that the zeta function $Z_f(u)$ of $f(x_0,\ldots,x_n) = a_0x_0^m + a_1x_1^m + \ldots + a_nx_n^m$, where $a_0,\ldots,a_n \in F^*$ and F is a field of order $q \equiv 1\ (m)$, is rational. In order to do this, we first outline a proof of the Hasse-Davenport relation, which is an interesting result in its own right.

Clearly f is a homogeneous polynomial, it therefore defines a projective hypersurface $\overline{H}_f(F_s)$ where $F \subseteq F_s$ is a field extension of degree s. Theorem 3.11 gives

$$N_s = \sum_{i=0}^{n-1} q^{si} + \frac{1}{q^s}\sum_{\chi_0^{(s)},\ldots,\chi_n^{(s)}}\prod_{j=0}^{n}\chi_i^{(s)}(a_i^{-1})g(\chi_i^{(s)}) \tag{26}$$

where $\chi_i^{(s)}$ are characters of F_s such that $\chi_i^{(s)m} = \epsilon$, $\chi_i^{(s)} \neq \epsilon$ and $\chi_0^{(s)}\cdots\chi_n^{(s)} = \epsilon$. Let χ be a character of F, compose it with $N_{F_s/F}$ to get $\chi' = \chi \circ N_{F_s/F} : F_s \longrightarrow \mathbb{C}$. This mapping is in fact a character on F_s since $\chi'(ab) = \chi\big(N_{F_s/F}(ab)\big) = \chi\big(N_{F_s/F}(a)N_{F_s/F}(b)\big) = \chi\big(N_{F_s/F}(a)\big)\chi\big(N_{F_s/F}(b)\big) = \chi'(a)\chi'(b)$ by proposition 2.11.

Lemma 4.7.

(I) $\chi \neq \rho \implies \chi' \neq \rho'$.

(II) $\chi^m = \epsilon \implies \chi'^m = \epsilon$.

(III) $\chi'(a) = \chi(a)^s$ *for all* $a \in F$.

Proof. The first follows from the last part of proposition 2.11. For the second part, note that $\big((\chi \circ N_{F_s/F})(a)\big)^m = \chi^m\big(N_{F_s/F}(a)\big) = \epsilon\big(N_{F_s/F}(a)\big) = 1$ for all $a \in F_s^*$, hence it is the trivial character. For the third part, simply note that $\chi'(a) = \chi\big(N_{F_s/F}(a\cdot 1)\big) = \chi(a^s) = \chi(a)^s$, by proposition 2.11. ■

This lemma shows that by letting χ vary over all characters of F of order diving m, the same happens for the corresponding characters χ' of F_s. Thus equation (26) can now be rewritten as

$$N_s = \sum_{i=0}^{n-1} q^{si} + \frac{1}{q^s}\sum_{\chi_0,\ldots,\chi_n}\prod_{j=0}^{n}\chi_i(a_i^{-1})^s g(\chi_i') \tag{27}$$

where χ_i are characters of F such that $\chi_i^m = \epsilon$, $\chi_i \neq \epsilon$ and $\chi_0\cdots\chi_n = \epsilon$. It turns out that $g(\chi')$ and $g(\chi)$ satisfy a simple relationship.

Theorem 4.8 (Hasse-Davenport Relation)**.**

$$\big(-g(\chi)\big)^s = -g(\chi')$$

Remark. We remind that s is an integer which depends on χ', which is a character on $F_s \supseteq F$ defined above.

In order to prove this, we first need two lemmas, the proofs of which will be omitted (see [IR, Ch. 11.4]). Given a monic polynomial $f(x) = x^n - a_1x^{n-1} + \ldots + (-1)^n a_n \in F[x]$, we define a mapping λ by $\lambda(f) = \psi(a_1)\chi(a_n)$ and let $\lambda(1) = 1$.

Lemma 4.9. $\lambda(fg) = \lambda(f)\lambda(g)$ *for all monic* $f, g \in F[x]$.

Lemma 4.10. *$g(\chi') = \sum \delta(f)\lambda(f)^{s/\delta(f)}$ where the sum is over all irreducible monic polynomials of degree s in $F[x]$.*

Given this definition of λ we have the identity

$$\sum_f \lambda(f)t^{\delta(f)} = \prod_f \frac{1}{1-\lambda(f)t^{\delta(f)}}$$

where the sum is over all monic polynomials, and the product is over all monic irreducible polynomials in $F[x]$. Let us spend some time outlining the legitimacy of this identity. We express the factors in the right hand side as a geometric series

$$\frac{1}{1-\lambda(f)t^{\delta(f)}} = \sum_{k=0}^{\infty}(\lambda(f)t^{\delta(f)})^k.$$

Using the fact that λ is multiplicative by lemma 4.9 we get

$$\begin{aligned}\prod_f \frac{1}{1-\lambda(f)t^{\delta(f)}} &= \prod_f \sum_{k=0}^{\infty} \lambda(f^k)t^{k\delta(f)} \\ &= \prod_f \Big(1 + \lambda(f)t^{\delta(f)} + \ldots + \lambda(f^k)t^{k\delta(f)} + \ldots\Big).\end{aligned}$$

Now, the ring $F[x]$ is a UFD so in particular each monic polynomial can be expressed as a product of irreducible (monic) polynomials in a unique way. Now, since each power of each monic irreducible polynomial is found in the sum above, we see, by multiplying the factors in the last expression, that each monic polynomial occurs in the argument of λ in the resulting sum. Inductively applying lemma 4.9 gives $\prod_{i=1}^n \lambda(f_i^{a_i}) = \lambda(\prod_{i=1}^n f_i^{a_i})$. This together with the basic fact that $\delta(\prod_{i=1}^n f_i^{a_i}) = \sum_{i=1}^n a_i\delta(f_i)$ shows that the identity holds.

4.2.1. *Proof of the Hasse-Davenport Relation.* By collecting terms of equal degree, we have

$$\sum_f \lambda(f)t^{\delta(f)} = \sum_{s=0}^{\infty}\Big(\sum_{\delta(f)=s}\lambda(f)\Big)t^s. \tag{28}$$

where the left hand side is as in (28). We proceed by analyzing the sums $\sum_{\delta(f)=s}\lambda(f)$. If $s = 1$, then

$$\sum_{\delta(f)=s}\lambda(f) = \sum_{a\in F}\lambda(x-a) = \sum_{a\in F}\chi(a)\psi(a) = g(\chi) \tag{29}$$

If $s > 1$ it turns out that the sums vanish, since

$$\sum_{\delta(f)=s}\lambda(f) = \sum_{a_i\in F}\lambda(x^s - a_1x^{s-1} + \ldots + (-1)^s a_s). \tag{30}$$

Now, λ only depends on the coefficients a_1 and a_n. By fixing those and letting the others vary over F, we see that (30) is equal to

$$q^{s-2}\sum_{a_1,\,a_n}\chi(a_s)\psi(a_1) = q^{s-2}\Big(\sum_{a_s}\chi(a_s)\Big)\Big(\sum_{a_1}\psi(a_1)\Big) = 0$$

by proposition 2.6 extended to characters on arbitrary finite fields. Thus we have

$$\sum_f \lambda(f)t^{\delta(f)} = 1 + g(\chi)t = \prod_f \frac{1}{1-\lambda(f)t^{\delta(f)}}.$$

By taking logarithmic derivatives, we get

$$\frac{d}{dt}\Big(ln(1+g(\chi)t)\Big) = \frac{g(\chi)}{1+g(\chi)t}$$

and

$$\frac{d}{dt}\left(ln\Big(\prod_f \frac{1}{1-\lambda(f)t^{\delta(f)}}\Big)\right) = \frac{d}{dt}\Big(-\sum_f ln\big(1-\lambda(f)t^{\delta(f)}\big)\Big)$$
$$= \sum_f \frac{\lambda(f)\delta(f)t^{\delta(f)-1}}{1-\lambda(f)t^{\delta(f)}}.$$

By multiplying these expressions by t, we have

$$\frac{g(\chi)t}{1+g(\chi)t} = \sum_f \frac{\lambda(f)\delta(f)t^{\delta(f)}}{1-\lambda(f)t^{\delta(f)}}.$$

Expand the denominators in geometric series to get

$$\sum_{s=1}^{\infty}(-1)^{s-1}g(\chi)^s t^s = \sum_f \Big(\sum_{k=1}^{\infty}\lambda(f)^k\delta(f)t^{k\delta(f)}\Big).$$

By comparing coefficients for t^s we get

$$(-1)^{s-1}g(\chi)^s = \sum_{\delta(f)|s}\delta(f)\lambda(f)^{s/\delta(f)} = g(\chi')$$

where the last equality is the content of lemma 4.10. This concludes the proof of theorem 4.8. ■

We now make use of the Hasse-Davenport relation to conclude our analysis of the numbers N_s associated with $Z_f(u)$, where $f(x_0,\ldots,x_n) = a_0x_0^m + a_1x_1^m + \ldots + a_nx_n^m \in F[x_0,\ldots,x_n]$. Substituting $g(\chi') = (-1)^{s+1}g(\chi)^s$ into equation (27) we get

$$N_s = \sum_{i=0}^{n-1} q^{si} + (-1)^{n+1}\sum_{\chi_0,\ldots,\chi_n}\left(\frac{(-1)^{n+1}}{q}\prod_{j=0}^{n}\chi_i(a_i^{-1})g(\chi_i)\right)^s, \tag{31}$$

where χ_i are characters of F such that $\chi_i^m = \epsilon$ (where m is as in the polynomial f), $\chi_i \neq \epsilon$ and $\chi_0\cdots\chi_n = \epsilon$.

Finally, we are in a position to state the main theorem of this section, which establishes the rationality of $Z_f(u)$ under certain conditions.

Theorem 4.11. *Let $a_0,\ldots,a_n \in F^*$ where $|F| = q \equiv 1\ (m)$ and $f(x_0,\ldots,x_n) = a_0x_0^m + a_1x_1^m + \ldots + a_nx_n^m$. Then the congruence zeta function $Z_f(u)$ is a rational function of the form*

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

where

$$P(u) = \prod_{\chi_0,\ldots,\chi_n}\left(1-(-1)^{n+1}\frac{1}{q}\chi_0(a_0^{-1})\cdots\chi_n(a_n^{-1})g(\chi_0)\cdots g(\chi_n)u\right)$$

and the product is over all $(n+1)$-tuples $(\chi_0,\ldots,\chi_n)$ such that $\chi_i^m = \epsilon, \chi_i \neq \epsilon$ and $\chi_0\cdots\chi_n = \epsilon$.

Proof. This is a direct result of our characterization of rational zeta functions i.e. proposition 4.1 applied to the current situation. Note that if n is even, then (31) can be written as $N_s = \sum_{j=0}^{n-1}\beta_j^s - \sum_i \alpha_i^s$, where $\beta_j = q^j$ and $\alpha_i = (-1)^{n+1}\frac{1}{q}\chi_0(a_0^{-1})\cdots\chi_n(a_n^{-1})g(\chi_0)\cdots g(\chi_n)$ for some $(n+1)$-tuple $(\chi_0,\ldots,\chi_n)$ subject to the conditions above. If n is odd, then (31) can be written as $\sum_j\beta_j - \sum_i\alpha_i$ where $\beta_j = N_s$ and $\alpha_i = 0$. Hence the exponent $(-1)^n$ in the numerator of $Z_f(u)$, since the zeta function is of the form $\dfrac{\prod_i(1-\alpha_iu)}{\prod_j(1-\beta_ju)}$. ■