Gauss and Jacobi Sums, Weil Conjectures

March 27, 2004

In this note, we define the notions of Gauss and Jacobi sums and apply them to investigate the number of solutions of polynomial equations over finite fields. Then using them we will verify the validity of the Weil conjectures for a class of projective hypersurfaces defined over finite fields.

1 Trace and Norm in Finite Fields

Throughout this note, except in the course of the proof of quadratic reciprocity law in Section 4, we assume that q is a power of prime number p, and that $F_k = \mathbb{F}_{q^k}$ is the unique finite field with q^k elements containing $F = \mathbb{F}_q$ in a fixed algebraic closure of $\mathbb{F}_q$.

Definition 1.1 *For $\alpha \in F_k$, the* **trace** *and* **norm** *of α respect to the field extension F_k/F are defined by*

$$\mathrm{Tr}_{F_k/F}(\alpha) := \alpha + \alpha^q + \cdots + \alpha^{q^{k-1}}, \quad \mathrm{N}_{F_k/F}(\alpha) := \alpha\alpha^q \cdots \alpha^{q^{k-1}}$$

respectively.

The following lemma describes the basic properties of trace and norm.

Lemma 1.2 *For $\alpha,\ \beta \in F_k$, and for $a \in F$,*

(a) $\mathrm{Tr}_{F_k/F}(a\alpha + \beta) = a\mathrm{Tr}_{F_k/F}(\alpha) + \mathrm{Tr}_{F_k/F}(\beta)$.

(b) $\mathrm{N}_{F_k/F}(\alpha\beta) = \mathrm{N}_{F_k/F}(\alpha)\mathrm{N}_{F_k/F}(\beta)$.

(c) $\mathrm{Tr}_{F_k/F}(a) = ka$ and $\mathrm{N}_{F_k/F}(a) = a^k$.

(d) $\mathrm{Tr}_{F_k/F}$ *and* $\mathrm{Tr}_{F_k/F}$ *map F_k onto F.*

Proof We only prove the last one. The fact that $\alpha \in F$ iff $\alpha^q = \alpha$ together with the very definition imply that $\mathrm{Tr}_{F_k/F}(\alpha),\ \mathrm{N}_{F_k/F}(\alpha) \in F$.

The polynomial $x + x^q + \cdots + x^{q^{k-1}}$ has less roots in F_k than the polynomial $x^{q^k} - x$, so there exists an $\alpha_0 \in F_k$ such that $\mathrm{Tr}_{F_k/F}(\alpha_0) = a_0 \neq 0$. Now for $b \in F$ given, $\mathrm{Tr}_{F_k/F}(ba_0^{-1}\alpha_0) = b$. Thus $\mathrm{Tr}_{F_k/F} : F_k \longrightarrow F$ is onto.

Using the polynomial $xx^q \cdots x^{q^{k-1}}$ and applying a similar argument will establish the surjectivity of $\mathrm{N}_{F_k/F} : F_k \longrightarrow F$. □

2 Gauss Sums

This section aims to introduce the important notion of a Gauss sum and to establish its basic properties. Before we do so, let us recall that:

The group $\widehat{F^\times}$ of (multiplicative) characters of $F^\times$ is a cyclic group of order $q-1$ isomorphic to $F^\times$. For any $\chi \in \widehat{F}$ (abuse of notation!), we extend the domain of definition of χ to whole F by setting

$$\chi(0) := \begin{cases} 1 & \text{if } \chi = \epsilon \\ 0 & \text{otherwise,} \end{cases}$$

where ϵ stands for the trivial character, i.e., $\epsilon(a) = 1$ for all $a \in F$. Note that by this convention,

$$\frac{1}{q}\sum_{a\in F}\chi(a) = \begin{cases} 1 & \text{if } \chi = \epsilon \\ 0 & \text{otherwise.} \end{cases}$$

Definition 2.1 *The* **additive character** $\psi : F \longrightarrow \mathbb{C}$ *(see part (a) of the following proposition) is defined by* $\psi(\alpha) := \zeta_p^{\mathrm{tr}(\alpha)}$, *where* $\mathrm{tr} = \mathrm{Tr}_{F/\mathbb{F}_p}$ *and* $\zeta_p = e^{\frac{2\pi i}{p}}$.

Lemma 2.2 *(a) For* $\alpha,\ \beta \in F$, $\psi(\alpha+\beta) = \psi(\alpha)\psi(\beta)$.[1]

(b) $\psi(\alpha_0) \neq 1$, *for some* $\alpha_0 \in F$.

(c) $\displaystyle\sum_{\alpha\in F}\psi(\alpha) = 0.$

(d) $\displaystyle\frac{1}{q}\sum_{\alpha\in F}\psi(\alpha(x-y)) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise.} \end{cases}$

Proof *(a)* Immediate form the definition.

(b) See the proof of Lemma 1.2.

(c) Since $\psi(\alpha_0)\displaystyle\sum_{\alpha\in F}\psi(\alpha) = \sum_{\alpha\in F}\psi(\alpha+\alpha_0) = \sum_{\beta\in F}\psi(\beta)$, by *(b)* we are done.

(d) Immediate from *(c)*. □

Definition 2.3 *For* $\chi \in \widehat{F}$ *and* $\alpha \in F$, *the* **Gauss sum** *associated to* χ *(and* α*) is defined by*

$$g_\alpha(\chi) := \sum_{t\in F}\chi(t)\psi(\alpha t).$$

For brevity, we will denote $g_1(\chi)$ *by* $g(\chi)$.

[1] It can be shown that for any function $\psi : F \longrightarrow \mathbb{C}^\times$ satisfying $\psi(\alpha+\beta) = \psi(\alpha)\psi(\beta)$, $\alpha, \beta \in F$, there exists an $\gamma \in F$ such that $\psi(x) = \zeta_p^{\mathrm{tr}(\gamma x)}$ for all $x \in F$.

In the following proposition we will prove the basic properties of Gauss sums.

Proposition 2.4 *(a)* $g_\alpha(\chi) = \begin{cases} 0 & \text{if } \alpha = 0 \text{ and } \chi \neq \epsilon, \\ 0 & \text{if } \alpha \neq 0 \text{ and } \chi = \epsilon, \\ q & \text{if } \alpha = 0 \text{ and } \chi = \epsilon, \\ \chi(\alpha^{-1})g(\chi) & \text{if } \alpha \neq 0 \text{ and } \chi \neq \epsilon. \end{cases}$

(b) $g(\overline{\chi}) = g(\chi^{-1}) = \chi(-1)\overline{g(\chi)}$.

(c) If $\chi \neq \epsilon$, *then* $g(\chi)g(\overline{\chi}) = \chi(-1)q$, *or equivalently,* $|g(\chi)| = \sqrt{q}$.

Remark For any function $f : F \longrightarrow \mathbb{C}$, the **Fourier coefficient** of f at $\alpha \in F$ is defined by

$$\hat{f}(\alpha) := \frac{1}{q} \sum_{t \in F} f(t)\overline{\psi(\alpha t)},$$

and one has the (finite) **Fourier series** expansion of f, namely,

$$f(t) = \sum_{\alpha} \hat{f}(\alpha)\psi(\alpha t).$$

In this terminology, the Gauss sum $g_\alpha(\chi)$ is merely the Fourier coefficient of χ at $-\alpha$ up to the constant q, i.e., $g_\alpha(\chi) = q\widehat{\chi}(-\alpha)$. So, what we are doing here can be translated completely into the language of Fourier analysis over finite abelian groups (see [N, Chapter 4], for a comprehensive account.)

Proof of the proposition *(a)* Assume that $\alpha \neq 0$ and $\chi \neq \epsilon$. Then we have

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

The other parts are obvious.

(b) Easy!

(c) Let $S = \sum_{\alpha \in F} g_\alpha(\chi)\overline{g_\alpha(\chi)}$. On the one hand

$$S = \sum_{\alpha \neq 0} \chi(\alpha^{-1})g(\chi)\overline{\chi(\alpha^{-1})}\ \overline{g(\chi)} = (q-1)|g(\chi)|^2.$$

On the other hand

$$\begin{aligned} S &= \sum_{\alpha} \left(\sum_{x} \chi(x)\psi(\alpha x) \right) \left(\sum_{y} \overline{\chi(y)}\psi(-\alpha y) \right) \\ &= \sum_{x} \sum_{y} \left(\chi(x)\overline{\chi(y)} \sum_{\alpha} \psi(\alpha(x-y)) \right) = (q-1)q. \end{aligned}$$

This completes the proof. □

Gauss sums play crucial roles in different parts of number theory. For example, they appear in the functional equation satisfied by the Dirichlet L-functions. Let χ be a Dirichlet character with conductor $\mathfrak{f}$, let $g(\chi) := \sum_{a=1}^{\mathfrak{f}} \chi(a) e^{\frac{2\pi i a}{\mathfrak{f}}}$ be the (classical) Gauss sum associated to χ, and let $L(s,\ \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ be the Dirichlet L-function attached to χ. Then we have

$$\left(\frac{\mathfrak{f}}{\pi}\right)^{\frac{s}{2}} \Gamma\left(\frac{s+\delta}{2}\right) L(s,\ \chi) = \frac{g(\chi)}{\sqrt{\mathfrak{f}}\ i^{\delta}} \left(\frac{\mathfrak{f}}{\pi}\right)^{\frac{1-s}{2}} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s,\ \overline{\chi}),$$

where

$$\delta = \begin{cases} 0 & \text{if } \chi \text{ is even, i.e., } \chi(-1) = 1 \\ 1 & \text{if } \chi \text{ is odd, i.e., } \chi(-1) = -1. \end{cases}$$

Furthermore, one can show that

$$L(1,\ \chi) = \pi i \frac{g(\chi)}{\mathfrak{f}} \frac{1}{\mathfrak{f}} \sum_{a=1}^{\mathfrak{f}} \overline{\chi}(a) a, \quad \text{if } \ \chi(-1) = -1;$$

$$L(1,\ \chi) = -\frac{g(\chi)}{\mathfrak{f}} \sum_{a=1}^{\mathfrak{f}} \overline{\chi}(a) \log|1 - e^{\frac{2\pi i a}{\mathfrak{f}}}|, \quad \text{if } \ \chi(-1) = 1,\ \chi \neq \chi_{\text{triv.}}.$$

For more information, see [K, Chapter 2] or [W, Chapter 4].

Another important example is the Stickelberger theorem about the factorization of Gauss sums in the ring of cyclotomic integers $\mathbb{Z}[\zeta_m]$, $\zeta_m = e^{\frac{2\pi i}{m}}$. Let us explain it precisely. Suppose $\mathfrak{P}$ is an unramified prime in $\mathbb{Z}[\zeta_m]$, i.e., $m \notin \mathfrak{P}$ or equivalently $p \nmid m$ where $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$. Let $F = \frac{\mathbb{Z}[\zeta_m]}{\mathfrak{P}}$ be the (finite) residue field, and write $\#F = q(= p^f)$. It is fairly easy to see that $q \equiv 1 \pmod{m}$, that the cosets of $1,\ \zeta_m,\ \cdots, \zeta_m^{m-1}$ (as elements of F) are distinct, and that for any $\alpha \in \mathbb{Z}[\zeta_m]$ off $\mathfrak{P}$, there is an integer i, unique mod m, such that $\alpha^{\frac{q-1}{m}} \equiv \zeta_m^i \pmod{\mathfrak{P}}$. We define the m-th **power residue symbol** $\left(\frac{\alpha}{\mathfrak{P}}\right)_m$ as follows

$$\left(\frac{\alpha}{\mathfrak{P}}\right)_m := \begin{cases} 0 & \text{if } \alpha \in \mathfrak{P} \\ \zeta_m^i & \text{if } \alpha \notin \mathfrak{P}. \end{cases}$$

This gives rise to the following we-defined multiplicative character for F,

$$\chi_{\mathfrak{P}}(t) := \left(\frac{\gamma}{\mathfrak{P}}\right)_m^{-1} = \overline{\left(\frac{\gamma}{\mathfrak{P}}\right)_m},$$

where $\gamma \in \mathbb{Z}[\zeta_m]$ is an arbitrary representative for $t \in F$. Corresponding to this character we have the Gauss sum $g(\chi_{\mathfrak{P}})$. The Stickelberger theorem asserts that

the principal ideal generated by $g(\chi_{\mathfrak{P}})^m$ factors in $\mathbb{Z}[\zeta_m]$ as

$$(g(\chi_{\mathfrak{P}})^m) = \prod_{\sigma_t \in G} \sigma_t^{-1}(\mathfrak{P})^t,$$

where $G = \mathrm{Gal}\,(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \{\sigma_t : \ 1 \leq t \leq m, \ \text{g.c.d}(t,m) = 1, \ \sigma_t(\zeta_m) = \zeta_m^t\}$. To see a proof of this deep relation and its substantial role in the proof of the Eisenstein reciprocity law, consult [IR, Chapter 14] or [W, Chapter 6].

3 Jacobi Sums

Our first objective here is to investigate the number of solutions of (polynomial) equations over finite fields. We will see that along the way the notion of a Jacobi sum comes up naturally.

To begin with, let's start with the simple equation $x^m = \alpha$. Since the number of solutions of this equation in any finite cyclic group G is the same as the number of solutions for the equation $x^d = \alpha$, where $d = \text{g.c.d}(m, \ |G|)$, so without loss of generality and **from now on**, we assume that $m \mid q-1$. Also we recall that this number is m, if α is an m-th power in G; and is 0 otherwise.

Lemma 3.1 *$N(x^m = \alpha)$, the number of solutions of the equation $x^m = \alpha$ in F is equal to* $\displaystyle\sum_{\chi^m = \epsilon} \chi(\alpha)$.

Proof For $\alpha = 0$ the assertion is trivial. So, assume that $\alpha \in F^\times$. If $\alpha = \beta^m$, then

$$\sum_{\chi^m = \epsilon} \chi(\alpha) = \sum_{\chi^m = \epsilon} \chi^m(\beta) = m = N(x^m = \alpha).$$

Now suppose that α is not m-th power. There is a character χ_1 of order m such that $\chi_1(\alpha) \neq 1$ (for example the one that takes a given generator of $F^\times$ to $e^{\frac{2\pi i}{m}}$ works.) We have

$$\sum_{\chi^m = \epsilon} \chi(\alpha) = \chi_1(\alpha) \sum_{\chi^m = \epsilon} \chi(\alpha),$$

and therefore $\displaystyle\sum_{\chi^m = \epsilon} \chi(\alpha) = 0 = N(x^m = \alpha)$. □

Next, we wish to evaluate $N(x^m + y^m = 1)$, the number of solutions of the equation $x^m + y^m = 1$ in F. By the above lemma, we have

$$\begin{aligned} N(x^m + y^m = 1) &= \sum_{a+b=1} N(x^m = a) N(y^m = b) \\ &= \sum_{a+b=1} \left(\sum_{\chi_1^m = \epsilon} \chi_1(a) \sum_{\chi_2^m = \epsilon} \chi_2(b) \right) \end{aligned}$$

$$= \sum_{\chi_1^m=\chi_2^m=\epsilon} \left(\sum_{a+b=1} \chi_1(a)\chi_2(b) \right)$$

The above calculation prompts the following definition.

Definition 3.2 *The* **Jacobi sum** *attached to* $\chi_1,\ \chi_2 \in \widehat{F}$ *is defined by*

$$J(\chi_1,\ \chi_2) := \sum_{a+b=1} \chi_1(a)\chi_2(b).$$

More generally, for $\chi_1, \cdots, \chi_l \in \widehat{F}$*, we set*

$$J(\chi_1,\ \cdots, \chi_l) := \sum_{a_1+\cdots+a_l=1} \chi_1(a_1)\cdots\chi_l(a_l).$$

It is also useful to introduce the following sum

$$J_0(\chi_1, \cdots, \chi_l) := \sum_{a_1+\cdots+a_l=0} \chi_1(a_1)\cdots\chi_l(a_l).$$

The following summarizes all we need to know about Jacobi sums for the purpose of this note.

Proposition 3.3 *(a) If* $\chi_1 = \cdots = \chi_l = \epsilon$*, then*

$$J(\chi_1, \cdots, \chi_l) = J_0(\chi_1, \cdots, \chi_l) = q^{l-1}.$$

(b) If $\chi_1, \cdots, \chi_k \neq \epsilon,\ \chi_{k+1} = \cdots = \chi_l = \epsilon$*, then*

$$J(\chi_1, \cdots, \chi_l) = J_0(\chi_1, \cdots, \chi_l) = 0.$$

(c) If $\chi_l \neq \epsilon$*, then*

$$\begin{aligned} J_0(\chi_1, \cdots, \chi_l) &= \chi_1\cdots\chi_{l-1}(-1)J(\chi_1, \cdots, \chi_{l-1}) \sum_{s\neq 0} \chi_1\cdots\chi_l(s) \\ &= \begin{cases} \chi_l(-1)(q-1)J(\chi_1, \cdots, \chi_{l-1}) & \text{if } \chi_1\cdots\chi_l = \epsilon \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

(d) If $\chi_1, \cdots, \chi_l, \chi_1\cdots\chi_l \neq \epsilon$*, then*

$$J(\chi_1, \cdots, \chi_l) = \frac{g(\chi_1)\cdots g(\chi_l)}{g(\chi_1\cdots\chi_l)},$$

and therefore

$$|J(\chi_1, \cdots, \chi_l)| = q^{\frac{l-1}{2}}.$$

(e) If $\chi_1, \cdots, \chi_l \neq \epsilon, \chi_1\cdots\chi_l = \epsilon$*, then*

$$J(\chi_1, \cdots, \chi_l) = -\frac{g(\chi_1)\cdots g(\chi_l)}{q} = -\chi_l(-1)J(\chi_1, \cdots, \chi_{l-1}),$$

and therefore $|J(\chi_1, \cdots, \chi_l)| = q^{\frac{l-2}{2}}$.

Proof *(a)* Just count the number of summands.

(b) We have

$$\begin{aligned} J_0(\chi_1,\cdots,\chi_l) &= \sum_{a_1,\cdots,a_{l-1}} \chi_1(a_1)\cdots\chi_k(a_k) \\ &= q^{l-k-1}\left(\sum_{a_1}\chi_1(a_1)\right)\cdots\left(\sum_{a_k}\chi_k(a_k)\right) \\ &= 0. \end{aligned}$$

And similar for $J(\chi_1,\cdots,\chi_l)$.

(c) For the first equality, we have

$$\begin{aligned} J_0(\chi_1,\cdots,\chi_l) &= \sum_{s\neq 0}\left(\sum_{a_1+\cdots+a_{l-1}=-s}\chi_1(a_1)\cdots\chi_{l-1}(a_{l-1})\right)\chi_l(s) \\ &= \sum_{s\neq 0}\left(\sum_{a_1'+\cdots+a_{l-1}'=1}\chi_1\cdots\chi_{l-1}(-s)\chi_1(a_1')\cdots\chi_{l-1}(a_{l-1}')\right)\chi_l(s) \\ &= \sum_{s\neq 0}\left(\chi_1\cdots\chi_{l-1}(-s)J(\chi_1,\cdots,\chi_{l-1})\right)\chi_l(s) \\ &= \chi_1\cdots\chi_{l-1}(-1)J(\chi_1,\cdots,\chi_{l-1})\sum_{s\neq 0}\chi_1\cdots\chi_l(s). \end{aligned}$$

And the second equality is immediate form the first one.

(d) First notice that

$$\begin{aligned} g(\chi_1)\cdots g(\chi_l) &= \left(\sum_{a_1}\chi(a_1)\psi(a_1)\right)\cdots\left(\sum_{a_l}\chi(a_l)\psi(a_l)\right) \\ &= \sum_{s}\left(\sum_{a_1+\cdots+a_l=s}\chi_1(a_1)\cdots\chi_l(a_l)\right)\psi(s) \\ &= J_0(\chi_1,\cdots,\chi_l)+J(\chi_1,\cdots,\chi_l)\sum_{s\neq 0}\chi_1\cdots\chi_l(s)\psi(s) \\ &= J_0(\chi_1,\cdots,\chi_l)+J(\chi_1,\cdots,\chi_l)\left(g(\chi_1\cdots\chi_l)-\chi_1\cdots\chi_l(0)\right). \quad (\star) \end{aligned}$$

Now *(d)* follows from $(\star)$ and *(c)*.

(e) By what we just proved in *(d)*,

$$g(\chi_1)\cdots g(\chi_{l-1}) = g(\chi_1\cdots\chi_{l-1})J(\chi_1,\cdots,\chi_{l-1}).$$

Multiplying both sides of this by $g(\chi_l)$, using $\chi_1\cdots\chi_{l-1}=\chi_l^{-1}$ together with the last part of Proposition 2.4 will establish the second equality of *(e)*. Putting now together this with $(\star)$ and *(c)* will result in the first equality of *(e)*. □

4 Some Applications

This section is devoted to some applications of Gauss and Jacobi sums. Historically, Gauss sums appeared in Gauss' fourth proof of the quadratic reciprocity law in 1811, although he had worked with them since 1801 and had found some of their basic properties. Afterwards, Gauss sums were utilized extensively by Jacobi, Eisenstein, kronecker and others in various proofs of quadratic reciprocity law as well as reciprocity laws of higher degrees. Here and for the first application, we expose an elegant proof of quadratic reciprocity law by means of Gauss and Jacobi sums.

Let p and q be two distinct odd prime numbers, and let χ be the unique character of order 2 on $\mathbb{F}_p$, i.e., the Legendre symbol $\left(\frac{\cdot}{p}\right)$. We have

$$J(\underbrace{\chi,\cdots,\chi}_{q \text{ times}}) = \sum_{t_1+\cdots+t_q=1} \chi(t_1)\cdots\chi(t_q).$$

If all the t_i's are equal, then the corresponding term of the sum has value $\chi\left(q^{-1}\right)^q = \left(\frac{q}{p}\right)$. And if not, then there are q different q-tuples obtained from $(t_1,\cdots,t_q)$ by cyclic permutation. This implies that $J(\chi,\cdots,\chi) \equiv \left(\frac{q}{p}\right) \pmod{q}$, (the congruence relation to be understood in the ring of algebraic integers), and therefore

$$\begin{aligned}
\left(\frac{q}{p}\right) &\equiv J(\chi,\cdots,\chi) \pmod{q} \\
&= \frac{1}{p}(-1)^{\frac{p-1}{2}} g(\chi)^{q+1} \\
&= \frac{1}{p}(-1)^{\frac{p-1}{2}} \left(g(\chi)^2\right)^{\frac{q+1}{2}} \\
&= \frac{1}{p}(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q+1}{2}} p^{\frac{q+1}{2}} \\
&= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} \\
&\equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod{q},
\end{aligned}$$

a *fortiori* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

In the sequel of this section we derive a formula, and through that, an estimate for $N = N(a_1x_1^{m_1} + \cdots + a_lx_l^{m_l} = b)$, the number of solutions of the equation

$$a_1x_1^{m_1} + \cdots + a_lx_l^{m_l} = b, \quad a_i \in F^\times.$$

Moreover, we will find, as a by-product, the number of projective points on the hypersurface defined by $a_0x_0^m + \cdots a_lx_l^m = 0$ in $\mathbb{P}^l_F$.

As before there will be no restriction if we assume that $m_i \mid q-1$.

Theorem 4.1 *(a) If* $b = 0$, *then*

$$N = q^{l-1} + \sum \chi_1(a_1^{-1}) \cdots \chi_l(a_l^{-1}) J_0(\chi_1, \cdots, \chi_l). \tag{1}$$

The sum is over all l*-tuples of characters* $\chi_1, \cdots, \chi_l$, *where* $\chi_i \neq \epsilon$, $\chi_i^{m_i} = \epsilon$, *and* $\chi_1 \cdots \chi_l = \epsilon$. *If* M *stands for the number of such* l*-tuples, then*

$$\left|N - q^{l-1}\right| \leq M(q-1)q^{\frac{l-2}{2}}. \tag{2}$$

(b) If $b \neq 0$, *then*

$$N = q^{l-1} + \sum \chi_1 \cdots \chi_l(b) \chi_1(a_1^{-1}) \cdots \chi_l(a_l^{-1}) J(\chi_1, \cdots, \chi_l), \tag{3}$$

where $\chi_i \neq \epsilon$, $\chi_i^{m_i} = \epsilon$. *If* M_1 *denotes the number of such* l*-tuples with* $\chi_1 \cdots \chi_l \neq \epsilon$, *then*

$$\left|N - q^{l-1}\right| \leq Mq^{\frac{l-2}{2}} + M_1 q^{\frac{l-1}{2}}. \tag{4}$$

Proof Note that

$$\begin{aligned} N &= \sum_{a_1 u_1 + \cdots + a_l u_l = b} N(x_1^{m_1} = u_1) \cdots N(x_l^{m_l} = u_l) \\ &= \sum_{\substack{\chi_1, \cdots, \chi_l \\ \mathrm{ord}(\chi_i) \mid m_i}} \left(\sum_{a_1 u_1 + \cdots + a_l u_l = b} \chi_1(u_1) \cdots \chi_l(u_l) \right). \end{aligned}$$

If $b = 0$, the inner sum is

$$\chi_1(a_1^{-1}) \cdots \chi_l(a_l^{-1}) J_0(\chi_1, \cdots, \chi_l);$$

and if $b \neq 0$, it is

$$\chi_1 \cdots \chi_l(b) \chi_1(a_1^{-1}) \cdots \chi_l(a_l^{-1}) J(\chi_1, \cdots, \chi_l).$$

Now (1) and (3) will follow from parts *(a), (b)* and *(c)* of the Proposition 3.3. Invoking parts *(d)* and *(e)* of the same proposition will establish the proof of (2) and (4). □

Remark In the proof of Weil conjectures, we will see that

$$M = \frac{1}{m}\left((m-1)^{l+1} + (-1)^{l+1}(m-1)\right) \text{ and } M_1 = (m-1)^{l+1} - M.$$

Corollary 4.2 *The number of the points (in* $\mathbb{P}_F^l$*) on the hypersurface defined by* $a_0 x_0^m + \cdots a_l x_l^m = 0$ *(*$a_i \in F^\times$*) is equal to*

$$q^{l-1} + \cdots + q + 1 + \frac{1}{q} \sum_{\chi_0, \cdots, \chi_l} \chi_0(a_0^{-1}) \cdots \chi_l(a_l^{-1}) g(\chi_0) \cdots g(\chi_l)$$

where $\chi_i \neq \epsilon$, $\chi_i^m = \epsilon$ *and* $\chi_0 \cdots \chi_l = \epsilon$.

Proof By previous theorem, the desired number is equal to

$$\frac{1}{q-1}\left(q^l + \sum \chi_0(a_0^{-1})\cdots\chi_l(a_l^{-1})J_0(\chi_0,\cdots,\chi_l) - 1\right).$$

However, by parts (c) and *(d)* of Proposition 3.3 and by part *(c)* of Proposition 2.4, we have

$$\begin{aligned}\frac{1}{q-1}J_0(\chi_0,\cdots,\chi_l) &= \chi_0(-1)J(\chi_1,\cdots,\chi_l)\\ &= \chi_0(-1)\frac{g(\chi_0)g(\chi_1)\cdots g(\chi_l)}{g(\chi_0)g(\chi_1\cdots\chi_l)}\\ &= \frac{g(\chi_0)\cdots g(\chi_l)}{q}.\end{aligned}$$

This completes the proof. □

5 Weil Conjectures

In this section we will recover the Weil conjectures for the hypersurface H defined by $a_0x_0^m + \cdots a_lx_l^m = 0$. So, let us first recall the definition of $\mathcal{Z}(H/F,\ T)$.

For any $k \geq 1$, let N_k denote the number of points on H defined over F_k. The **zeta function** $\mathcal{Z}(H/F,\ T)$ of H is defined by

$$\mathcal{Z}(H/F,\ T) := \exp\left(\sum_{k=1}^{\infty} N_k\frac{T^k}{k}\right),$$

where $\exp(u) := 1 + u + \dfrac{u^2}{2!} + \dfrac{u^3}{3!} + \cdots$.

Lemma 5.1 *We have*

$$\mathcal{Z}(H/F,\ T) = \frac{(1-\alpha_1T)\cdots(1-\alpha_rT)}{(1-\beta_1T)\cdots(1-\beta_sT)},\quad \alpha_i,\beta_j \in \mathbb{C}$$

iff

$$N_k = \beta_1^k + \cdots + \beta_s^k - \alpha_1^k - \cdots - \alpha_r^k$$

for $k = 1, 2, 3, \cdots$.

Proof On the one hand,

$$\log \mathcal{Z}(H/F,\ T) = \sum_{k=1}^{\infty} N_k\frac{T^k}{k}.$$

And on the other hand,

$$\begin{aligned}\log\frac{(1-\alpha_1T)\cdots(1-\alpha_rT)}{(1-\beta_1T)\cdots(1-\beta_sT)} &= -\sum_j\log(1-\beta_jT)+\sum_i\log(1-\alpha_iT)\\ &= \sum_{k=1}^{\infty}\left(\sum_j\beta_j^k-\sum_i\alpha_i^k\right)\frac{T^k}{k}.\end{aligned}$$

This completes the proof. □

Before we proceed to state and prove of Weil conjectures, we need to investigate the relation between the characters of F with those of F_k. The key link will be provided by the norm function $\mathrm{N}_{F_k/F}$.

Let $\chi \in F^\times$, and set $\chi^{(k)} = \chi\ o\ \mathrm{N}_{F_K/F}$, i.e., $\chi^{(k)}(a) = \chi(\mathrm{N}_{F_k/F}(a))$ for $a \in F_k$. The following affirmations can be easily verified:

1. $\chi^{(k)} \in \widehat{F_k}$.

2. $\chi_1^{(k)} = \chi_2^{(k)}$ iff $\chi_1 = \chi_2$.

3. $\mathrm{ord}(\chi^{(k)}) \mid m$ iff $\mathrm{ord}(\chi) \mid m$.

4. $\chi^{(k)}(a) = \chi(a)^k$ for all $a \in F$.

It immediately follows from **3** that if χ runs the set of characters of order dividing m (in $\widehat{F}$), then $\chi^{(k)}$ will do the same in $\widehat{F}_k$.

And finally, the following classical result–the interrelation between Gauss sums $g(\chi)$ and $g(\chi^{(k)})$–will provide our last ingredient.

Theorem 5.2 (Hasse-Davenport) *With the above notations,*

$$g(\chi^{(k)}) = (-1)^{k+1}g(\chi)^k.$$

Proof See [IR, Chapter 11], for an elegant proof. It is also outlined in [K, Chapter 2], as a long exercise. □

Now we have all necessary tools to prove the following special case of the Weil conjectures.

Theorem 5.3 (Weil) *The zeta function $\mathcal{Z}(H/F,\ T)$ of the hypersurface H defined by the equation $a_0x_0^m + \cdots a_lx_l^m = 0$ has the following properties:*

(a) **(Rationality)** $\mathcal{Z}(H/F,\ T) = \dfrac{P(T)^{(-1)^l}}{(1-T)(1-qT)\cdots(1-q^{l-1}T)}$,

where $P(T)$ is the polynomial

$$\prod\left(1-(-1)^{l+1}\frac{1}{q}\chi_0(a_0^{-1})\cdots\chi_l(a_l^{-1})g(\chi_0)\cdots g(\chi_l)T\right).$$

The characters χ_i are subject to the conditions $\chi_i \neq \epsilon,\ \chi_i^m = \epsilon$, and $\chi_0 \cdots \chi_l = \epsilon$. Moreover, we claim that $P(T) \in \mathbb{Z}[T]$.

(b) The degree of $P(T)$ is equal to $d = \dfrac{1}{m}\left((m-1)^{l+1} + (-1)^{l+1}(m-1)\right)$.

(c) **(Functional Equation)** *The mapping $\alpha \longrightarrow \frac{1}{q^{l-1}\alpha}$ is a bijection of the set of zeros of $P(T)$. Equivalently, $\mathcal{Z}(H/F,\ T)$ satisfies the following functional equation*

$$\mathcal{Z}(H/F,\ \frac{1}{q^{l-1}T}) = \omega T^{l-(-1)^l d} q^{\frac{l-1}{2}(l-2(-1)^l d)} \mathcal{Z}(H/F,\ T),$$

where

$$\omega = (-1)^{d-l} \left(\prod_{P(\alpha)=0} \alpha \right)^{(-1)^l}.$$

(d) The reciprocals of zeros of $P(T)$ are algebraic integers.

(e) **(Riemann Hypothesis)** *The zeros of $P(T)$ have absolute value $q^{-\frac{l-1}{2}}$.*

Proof *(a)* By Corollary 4.2, N_k is equal to

$$q^{k(l-1)} + \cdots + q^k + 1 + \frac{1}{q^k} \sum_{\chi_0^{(k)}, \cdots, \chi_l^{(k)}} \chi_0^{(k)}(a_0^{-1}) \cdots \chi_l^{(k)}(a_l^{-1}) g(\chi_0^{(k)}) \cdots g(\chi_l^{(k)}),$$

where $\chi_i^{(k)} \neq \epsilon,\ \chi_i^{(k)m} = \epsilon,\ \chi_0^{(k)} \cdots \chi_l^{(k)} = \epsilon$ (we are using ϵ simultaneously for the trivial character of all F_k's.) So, by **3** and **4** of the above and by Hasse-Davenport relation, we infer that

$$\begin{aligned} N_k &= \sum_{i=0}^{l-1} q^{ik} + \frac{1}{q^k} \sum_{\chi_0, \cdots, \chi_l} \left((-1)^{(k+1)(l+1)} \chi_0(a_0^{-1})^k \cdots \chi_l(a_l^{-1})^k g(\chi_0)^k \cdots g(\chi_l)^k \right) \\ &= \sum_{i=0}^{l-1} \left(q^i\right)^k + (-1)^{l+1} \sum_{\chi_0, \cdots, \chi_l} \left(\frac{(-1)^{l+1}}{q} \chi_0(a_0^{-1}) \cdots \chi_l(a_l^{-1}) g(\chi_0) \cdots g(\chi_l) \right)^k. \end{aligned}$$

This proves *(a)*, except the fact that $P(T)$ is in $\mathbb{Z}[T]$. We postpone its proof until part *(d)*.

(b) Set

$$A_l = \{(\chi_0, \cdots, \chi_l) :\ \chi_i \neq \epsilon,\ \chi_i^m = \epsilon,\ \chi_0 \cdots \chi_l = \epsilon\},$$

$$B_l = \{(\chi_0, \cdots, \chi_l) :\ \chi_i \neq \epsilon,\ \chi_i^m = \epsilon,\ \chi_0 \cdots \chi_l \neq \epsilon\}.$$

Clearly deg $P(T) = |A_l|$. Since the map $(\chi_0, \cdots, \chi_l) \longrightarrow (\chi_0, \cdots, \chi_{l-1})$ is a bijection between A_l and B_{l-1}, we get

$$|A_l| + |A_{l+1}| = |A_l| + |B_l| = (m-1)^{l+1}.$$

Using this and the initial $|A_1| = m - 1$, *(b)* will follow by a simple induction.

(c) To prove the first statement it is sufficient to show that $\alpha \longrightarrow \dfrac{1}{q^{l-1}\alpha}$ is a well-defined map from the set of zeros of $P(T)$ to itself. So, let

$$\alpha = (-1)^{l+1} q \chi_0(a_0) \cdots \chi_l(a_l) g(\chi_0)^{-1} \cdots g(\chi_l)^{-1}$$

be a zero of $P(T)$ corresponding to $(\chi_0, \cdots, \chi_l) \in A_l$. We have

$$\begin{aligned} q^{l-1}\alpha &= (-1)^{l+1} q^l \chi_0(a_0) \cdots \chi_l(a_l) g(\chi_0)^{-1} \cdots g(\chi_l)^{-1} \\ &= (-1)^{l+1} \frac{1}{q} \chi_0^{-1}(a_0^{-1}) \cdots \chi_l^{-1}(a_l^{-1}) \frac{q}{g(\chi_0)} \cdots \frac{q}{g(\chi_l)} \\ &= (-1)^{l+1} \frac{1}{q} \chi_0^{-1}(a_0^{-1}) \cdots \chi_l^{-1}(a_l^{-1}) \chi_0(-1) g(\chi_0^{-1}) \cdots \chi_l(-1) g(\chi_l^{-1}) \\ &= (-1)^{l+1} \frac{1}{q} \chi_0^{-1}(a_0^{-1}) \cdots \chi_l^{-1}(a_l^{-1}) g(\chi_0^{-1}) \cdots g(\chi_l^{-1}). \end{aligned}$$

and the last quantity is the reciprocal of that zero of $P(T)$ which is corresponding to $(\chi_0^{-1}, \cdots, \chi_l^{-1}) \in A_l$.

Checking that $\mathcal{Z}(H/F,\ T)$ satisfies the aforesaid functional equation is a very straightforward but somehow tedious calculation, left to the reader.

(d) Obviously, the values of any character are algebraic integers. In fact, if $\chi^m = \epsilon$, then every value that χ takes is a unit in $\mathbb{Z}[\zeta_m]$. Therefore, by part *(e)* of Proposition 3.3, if $(\chi_0, \cdots, \chi_l) \in A_l$, then

$$(-1)^{l+1} \frac{1}{q} \chi_0(a_0^{-1}) \cdots \chi_l(a_l^{-1}) g(\chi_0) \cdots g(\chi_l)$$

$$= (-1)^{l+1} \chi_0^{-1}(a_0) \cdots \chi_l^{-1}(a_l) \chi_l(-1) J(\chi_0, \cdots, \chi_{l-1}) \in \mathbb{Z}[\zeta_m].$$

Now we accomplish the proof of part *(a)* by showing that $P(T) \in \mathbb{Z}[T]$. From the rationality of the zeta function and working inside the field $\mathbb{Q}[[T]]$, it is almost clear that

$$P(T) \in \mathbb{Q}[T].$$

(notice it is immediate from the very definition that $\mathcal{Z}(H/F,\ T) \in \mathbb{Q}[[T]]$.) On the other hand, *(d)* implies that $P(T) \in \mathbb{A}[T]$, where $\mathbb{A}$ is the ring of algebraic integers. Hence, the coefficients of $P(T)$ are in $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$.

(e) Immediately from part *(c)* of Proposition 2.4 we deduce that

$$\left| (-1)^{l+1} \frac{1}{q} \chi_0(a_0^{-1}) \cdots \chi_l(a_l^{-1}) g(\chi_0) \cdots g(\chi_l) \right| = \frac{q^{\frac{l+1}{2}}}{q} = q^{\frac{l-1}{2}},$$

which is equivalent to the desired statement. □

References

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics 52, Springer-Verlag, New York, 1990.

[K] N. Koblits, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics 97, Springer-Verlag, 1983.

[N] Melvyn B. Nathanson, *Elementary Methods in Number Theory*, Graduate Texts in Mathematics 195, Springer-Verlag, 2000.

[W] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83, Springer-Verlag, 1982.