GAUSS SUM AND JACOBI SUM

1. Characters and Gauss sums

Definition 1.1 (Characters)**.** Let G be a finite abelian group. A character χ of G is a group homomorphism $\chi : G \to \mathbf{C}^\times$. Let $\widehat{G}$ be the set of characters of G. Then $\widehat{G}$ naturally is also an abelian group. For $\chi_1, \chi_2 \in \widehat{G}$, $\chi_1\chi_2(g) := \chi_1(g)\chi_2(g)$. We call $\widehat{G}$ the character group of G.

Example 1.2. When $G = \mathbb{F}_p^\times$, we have seen Legendre symbol $x \mapsto \left(\frac{x}{a}\right)$ is a quadratic character of $\mathbb{F}_p^\times$. In the case $G = \mathbb{F}_p$, we define the standard additive character $\psi : \mathbb{F}_p \to \mathbf{C}^\times$ by

$$\psi(x \pmod p) = e^{\frac{2\pi\sqrt{-1}x}{p}}.$$

We can verify easily that $\psi(x+y) = \psi(x)\psi(y)$ for all $x, y \in \mathbb{F}_p$, so ψ is a (additive) character of $\mathbb{F}_p$.

Lemma 1.3. *Let $\chi : G \to \mathbf{C}^\times$ be a character. Then*

$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & \cdots \chi \neq 1, \\ \#G & \cdots \chi = 1. \end{cases}$$

The following special cases of Lemma 1.3 are extremely useful.

Lemma 1.4. *Let $a \in \mathbb{F}_p$. Then*

$$\sum_{x\in\mathbb{F}_p} \psi(ax) = \begin{cases} 0 & \cdots a \neq 0, \\ p & \cdots a = 0. \end{cases}$$

If $\chi : \mathbb{F}_p^\times \to \mathbf{C}^\times$ is a character, then

$$\sum_{x\in\mathbb{F}_p^\times} \chi(x) = \begin{cases} 0 & \cdots \chi \neq 1, \\ p-1 & \cdots \chi = 1. \end{cases}$$

Definition 1.5 (Gauss sum)**.** Let $\chi : \mathbb{F}_p^\times \to \mathbf{C}^\times$ be a character. We define the Gauss sum $\mathfrak{g}(\chi)$ by

$$\mathfrak{g}(\chi) := \sum_{x\in\mathbb{F}_p^\times} \chi(x)\psi(x) \in \mathbf{C}.$$

If $\chi = 1$ is the trivial character, then $\mathfrak{g}(\chi) = -1$.

Proposition 1.6. *For $a \in \mathbf{C}$, we write $\overline{a}$ for the complex conjugation of a. Suppose that $\chi \neq 1$. Then we have*

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

PROOF. We have

$$\mathfrak{g}(\chi)\overline{\mathfrak{g}(\chi)} = \sum_{x,y\in\mathbb{F}_p^\times} \chi(xy^{-1})\psi(x-y) = \sum_{x,y\in\mathbb{F}_p^\times} \chi(x)\psi((y(x-1))$$
$$= (p-1) + \sum_{x\in\mathbb{F}_p^\times, x\neq 1} \chi(x)(-1) = p.$$

We used Lemma 1.4 in the equation of the second line. □

Example 1.7. Let $\tau_p : \mathbb{F}_p^\times \to \mathbf{C}^\times$ be the quadratic character $a \mapsto \left(\frac{a}{p}\right)$ defined by Legendre symbol. Then

$$\mathfrak{g}\left(\tau_p\right)^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p.$$

One can actually prove that

$$\mathfrak{g}(\tau_p) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \,(\mathrm{mod}\ 4), \\ \sqrt{-1}\sqrt{p} & \text{if } p \equiv 3 \,(\mathrm{mod}\ 4). \end{cases}$$

2. The number of solutions of Fermat equations over finite fields

Given a polynomial $f = f(x_1, \cdots, x_n) \in \mathbf{Z}[x_1, \cdots, x_n]$, what we can say about the number of solutions of $f = 0$ in $\mathbb{F}_p$? Let m be a positive integer. The aim of this section is to estimate the size of $\#X_f(\mathbb{F}_p)$ for the three-variable Fermat equation $f(x_1, x_2, x_3) = ax_1^m + bx_2^m + cx_3^m$, $a, b, c \in \mathbb{F}_p^\times$ by using the exponential sums.

Definition 2.1. For any function $f : \mathbb{F}_p^n \to \mathbb{F}_p$, define the *exponential sum* for f by

$$S(f) := \sum_{x\in\mathbb{F}_p^n} \psi(f(x)).$$

For $x \in \mathbb{F}_p$, put

$$N_m(x) := \#\left\{y \in \mathbb{F}_p \mid y^m = x\right\}.$$

The following observation is extremely important.

Theorem 2.2. *Let $f \in \mathbf{Z}[x_1, \cdots, x_n]$. Then*

$$\#X_f(\mathbb{F}_p) = \frac{1}{p} \sum_{x\in\mathbb{F}_p^n} \sum_{a\in\mathbb{F}_p} \psi(af(x)) = \frac{1}{p} \sum_{a\in\mathbb{F}_p} S(af).$$

Example 2.3. Let $a_1, a_2, a_3 \in \mathbb{F}_p^\times$ and let

$$f(x_1, x_2, x_3) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2.$$

Use the equation

$$\sum_{x\in\mathbb{F}_p} \psi(bx^2) = 1 + \sum_{y\in\mathbb{F}_p^\times} \psi(by)\left(\left(\frac{y}{p}\right) + 1\right) = \left(\frac{b}{p}\right)\mathfrak{g}(\left(\frac{\cdot}{p}\right)).$$

to show that $\#X_f(\mathbb{F}_p) = p^2$. In what follows, we put

$$d = \gcd(m, p-1).$$

Lemma 2.4. *For $x \in \mathbb{F}_p^\times$, we have*

$$N_m(x) := \#\{y \in \mathbb{F}_p \mid y^m = x\} = \begin{cases} 0 & \text{if } x \notin (\mathbb{F}_p^\times)^d, \\ d & \text{if } x \in (\mathbb{F}_p^\times)^d. \end{cases}$$

PROOF. This follows from the fact that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$. □

Let $\zeta_{p-1} = e^{\frac{2\pi i}{p-1}} \in \mathbf{C}$ be a primitive $(p-1)$-th root of unity in $\mathbf{C}$. Fixing a generator α of $\mathbb{F}_p^\times$, we define the special character

$$\begin{aligned} \chi : \mathbb{F}_p^\times &\longrightarrow \mathbf{C}^\times \\ \alpha^n &\longmapsto \chi(\alpha^n) := \zeta_{p-1}^n \text{ for all } n = 0, \cdots, p-2. \end{aligned} \tag{2.1}$$

Then χ is a generator of the character group $\widehat{\mathbb{F}_p^\times} \simeq \mathbf{Z}/(p-1)\mathbf{Z}$. Namely, every character of $\mathbb{F}_p^\times$ is of the form χ^j for some $0 \le j < p-1$.

Every character ρ of $\mathbb{F}_p^\times$ shall be extended to a multiplicative function on $\mathbb{F}_p$ by setting $\rho(0) = 0$ if $\rho \neq 1$ and $\rho(0) = 1$ if $\rho = 1$ is the trivial character.

Lemma 2.5. *Let $k = \frac{p-1}{d}$. For $a \in \mathbb{F}_p$, we have*

$$N_m(a) = \sum_{i=0}^{d-1} \chi^{ki}(a).$$

PROOF. This is a simple consequence of Lemma 1.3. □

Proposition 2.6. *For $a \in \mathbb{F}_p^\times$,*

$$|S(ax^m)| \le (d-1)\sqrt{p}.$$

PROOF. By definition and Lemma 2.4,

$$\begin{aligned} S(ax^m) &:= \sum_{z \in \mathbb{F}_p} \psi(az^m) = 1 + d \sum_{w \in (\mathbb{F}_p^\times)^d} \psi(aw) \\ &= 1 + \sum_{y \in \mathbb{F}_p^\times} \psi(ay) \sum_{i=0}^{d-1} \chi^{ki}(y) = \sum_{i=1}^{d-1} \chi^{ki}(a^{-1}) \mathfrak{g}(\chi^{ki}). \end{aligned}$$

The proposition follows from Proposition 1.6. □

Theorem 2.7. *Let*

$$f(x,y,z) = a_1x^m + a_2y^m + a_3z^m \in \mathbb{F}_p[x,y,z],\ a_1, a_2, a_3 \in \mathbb{F}_p^\times.$$

Then

$$\left|\#X_f(\mathbb{F}_p) - p^2\right| \le (d-1)^3(p-1)\sqrt{p}.$$

PROOF. By Theorem 2.2, we find that

$$\#X_f(\mathbb{F}_p) = p^2 + \frac{1}{p} \sum_{b \in \mathbb{F}_p^\times} S(ba_1x^m) S(ba_2x^m) S(ba_3x^m),$$

the theorem follows from Proposition 2.6. □

Definition 2.8 (Projective space over finite fields)**.** For $n \in \mathbf{Z}_+$, we define

$$\begin{aligned}\mathbf{P}^n(\mathbb{F}_p) &= \text{the set of all lines in } \mathbb{F}_p^{n+1} \\ &= \left\{(a_0, a_1, \cdots, a_n) \in \mathbb{F}_p^{n+1} \mid (a_0, a_1, \cdots, a_n) \neq (0, 0, \cdots, 0)\right\} / \sim .\end{aligned}$$

Here the equivalent relation

$$(a_0, a_1, \cdots, a_n) \sim (b_0, b_1, \cdots, b_n) \iff (a_0, a_1, \cdots, a_n) = \alpha \cdot (b_0, b_1, \cdots, b_n) \text{ for some } \alpha \in \mathbb{F}_p^\times.$$

The set $\mathbf{P}^n(\mathbb{F}_p)$ is called the n-dimensional *projective space over* $\mathbb{F}_p$. It is obvious that

$$\#\mathbf{P}^n(\mathbb{F}_p) = \frac{p^{n+1} - 1}{p - 1}.$$

In particular $\#\mathbf{P}^1(\mathbb{F}_p) = p + 1$.

Let $f(x, y, z) = ax^m + by^m + cz^m$ be a homogenous polynomial of degree m. It makes sense to consider the following set :

$$\mathcal{C}_f(\mathbb{F}_p) := \left\{[a_0, a_1, a_2] \in \mathbf{P}^2(\mathbb{F}_p) \mid f(a_0, a_1, a_2) = 0\right\}.$$

This set $\mathcal{C}_f(\mathbb{F}_p)$ can be regarded as a *curve* in the *surface* $\mathbf{P}^2(\mathbb{F}_p)$, and it is clear that

$$\#\mathcal{C}_f(\mathbb{F}_p) = \frac{\#X_f(\mathbb{F}_p) - 1}{p - 1},$$

so Theorem 2.7 can be rephrased as the following theorem:

Theorem 2.9 (Riemann hypothesis for the Fermat curve $\mathcal{C}_f$)**.**

$$|\#\mathcal{C}_f(\mathbb{F}_p) - p - 1| \leq (d - 1)^3 \sqrt{p}.$$

3. Jacobi sums

Given characters χ_1, χ_2 of $\mathbb{F}_p^\times$, define the Jacobi sum

$$J(\chi_1, \chi_2) := \sum_{t \in \mathbb{F}_p} \chi_1(t)\chi_2(1 - t).$$

In general, given characters $\chi_1, \chi_2, \cdots, \chi_n$, the Jacobi sum is defined by

$$J(\chi_1, \cdots, \chi_n) = \sum_{\substack{t_1 + \cdots t_n = 1 \\ (t_1, \cdots, t_n) \in \mathbb{F}_p^n}} \chi_1(t_1)\chi_2(t_2) \cdots \chi_n(t_n).$$

Lemma 3.1. *We have*

(1) $J(1, 1) = p$ *and* $J(1, \chi) = 0$ *if* $\chi \neq 1$*;*
(2) $J(\chi, \chi^{-1}) = -\chi(-1)$*;*
(3) if $\chi_1, \chi_2, \chi_1\chi_2 \neq 1$*, then* $|J(\chi_1, \chi_2)| = \sqrt{p}$*. In fact,*

$$J(\chi_1, \chi_2) = \frac{\mathfrak{g}(\chi_1)\mathfrak{g}(\chi_2)}{\mathfrak{g}(\chi_1\chi_2)} = \chi_2(-1)J(\chi_2, \chi_1^{-1}\chi_2^{-1}).$$

PROOF. It suffices to show the first equation of (3). By a direct computation, we have

$$\begin{aligned}\mathfrak{g}(\chi_1)\mathfrak{g}(\chi_2) &= \sum_{(s,t)\in\mathbb{F}_p^2} \chi_1(s)\chi_2(t-s)\psi(t)\\ &= \sum_{s\in\mathbb{F}_p^\times}\sum_{t\in\mathbb{F}_p^\times} \chi_1(s)\chi_2(t-s)\psi(t) \quad (\chi_1\chi_2\neq 1)\\ &= \sum_{v,t\in\mathbb{F}_p^\times} \chi_1(tv)\chi_2(t(1-v))\psi(t) \quad (s\mapsto tv)\\ &= \mathfrak{g}(\chi_1\chi_2)J(\chi_1,\chi_2).\end{aligned}$$

This completes the proof. □

Remark 3.2. An algebraic number $\alpha\in\overline{\mathbf{Q}}\subset\mathbf{C}$ is called a Weil number if

$$|\sigma(\alpha)| = |\alpha| \text{ for all } \alpha\in \mathrm{Aut}(\mathbf{C}).$$

The Gauss sums and Jacobi sums are examples of Weil numbers.

We give two applications of Jacobi sums.

Theorem 3.3. *Let $f(x,y)=y^2-x^3-c\in\mathbb{F}_p[x,y]$ with $c\in\mathbb{F}_p^\times$. Then*

$$|\#X_f(\mathbb{F}_p)-p|\le 2\sqrt{p}.$$

Example 3.4. Let $p=19$ and $f(x,y)=y^2-x^3-5$. Then $\#X(\mathbb{F}_{19})=27$.

One can use the Jacobi sums to prove Fermat's two square theorem.

Theorem 3.5 (Fermat)**.** *Let p be a prime. Then p is a sum of squares if and only if $p\equiv 1\,(mod\ 4)$.*

PROOF. It suffices to prove the "if" part. Now we assume that $p\equiv 1\,(\mathrm{mod}\ 4)$. We shall offer three proofs.

First proof: The group $\mathbb{F}_p^\times$ is a cyclic group with order divisible by 4, so we can find non-trivial characters $\chi_1,\chi_2:\mathbb{F}_p^\times\to\{\pm 1,\pm\sqrt{-1}\}$ such that $\chi_1\chi_2\neq 1$. we can thus write the Jacobi sum $J(\chi_1,\chi_2)=a+b\sqrt{-1}$ with $a,b\in\mathbf{Z}$. By Lemma 3.1, we have $|J(\chi_1,\chi)|=\sqrt{p}$ and hence $a^2+b^2=p$.

Second proof: Since $\left(\frac{-1}{p}\right)=1$, there exists $s\in\mathbb{F}_p$ with $s^2=-1\in\mathbb{F}_p$. Consider the set $T=\{(x,y)\in\mathbf{Z}^2\mid 0\le x,y<\sqrt{p}\}$. Then $\#(T)=(1+\lfloor p\rfloor)^2>p$. Applying the pigeonhole principle to the map

$$T\mapsto\mathbb{F}_p,\quad (x,y)\mapsto x+sy\,(\mathrm{mod}\ p),$$

we find that there exist distinct $(x,y),(x',y')\in T$ with

$$x+sy=x'+sy'\in\mathbb{F}_p.$$

It follows that $(x-x')^2+(y-y')^2$ is divisible by p, but $|x-x'|,|y-y'|<\sqrt{p}$, so $0<(x-x')^2+(y-y')^2<2p$. We conclude that $(x-x')^2+(y-y')^2=p$.

Thrid proof: This is famous Zagier's *one sentence* proof. Put

$$S:=\{(x,y,z)\in\mathbf{Z}_{>0}^3\mid x^2+4yz=p\}.$$

Consider subsets A, B, C of S defined by

$$\begin{aligned} A &= \{(x,y,z) \in S \mid x < y - z\}, \\ B &= \{(x,y,z) \in S \mid y - z < x < 2y\}; \\ C &= \{(x,y,z) \in S \mid x > 2y\}. \end{aligned}$$

Then $S = A \sqcup B \sqcup C$. Define the map $\varphi : S \to S$ by

$$\varphi(x,y,z) = \begin{cases} (x + 2z, z, y - x - z) & \text{if } (x,y,z) \in A, \\ (2y - x, y, x + z - y) & \text{if } (x,y,z) \in B, \\ (x - 2y, z + x - y, y) & \text{if } (x,y,z) \in C. \end{cases}$$

It is easy to verify that $\varphi(A) \subset C$, $\varphi(C) \subset A$ and $\varphi(B) \subset B$. Moreover, $\varphi^2 = \mathrm{Id}_S$ and φ has only one fixed point $(1, 1, \frac{p-1}{4})$. It follows that $\#S$ must be odd, which implies the involution map $(x,y,z) \mapsto (x,z,y)$ also has a fixed point. This yields an integral solution to $x^2 + y^2 = p$. $\square$

Homework: (Due date 09/26)

Exercise 1 (5pts)**.** Let $\mathbf{C}[\mathbb{F}_p]$ be the $\mathbf{C}$-vector space consisting of all functions $f : \mathbb{F}_p \to \mathbf{C}$. For each $a \in \mathbb{F}_p$, define $\psi_a : \mathbb{F}_p \to \mathbf{C}$ by $\psi_a(x) = \psi(ax)$, where ψ is the additive character in Example 1.2 (or in the class). It is obvious that for every $x \in \mathbb{F}_p$,

$$\psi_0(x) = \psi(0) = 1.$$

So ψ_0 is the constant function which takes every $x \in \mathbb{F}_p$ to 1. Show that

(1) $\dim_{\mathbf{C}} \mathbf{C}[\mathbb{F}_p] = p$.
(2) $\{\psi_a\}_{a\in\mathbb{F}_p}$ is a $\mathbf{C}$-basis of $\mathbf{C}[\mathbb{F}_p]$.

Exercise 2 (5pts)**.** Let $\chi : \mathbb{F}_p^\times \to \mathbf{C}^\times$ be the special character defined in (2.1) (or in the class). Let $j \in \{0, \cdots, p-2\}$. Recall that χ^j has been extended to a function on $\mathbb{F}_p$ in the class. By the previous exercise, we can write

$$\chi^j = \sum_{a\in\mathbb{F}_p} g_a \cdot \psi_a \in \mathbf{C}[\mathbb{F}_p],\ g_a \in \mathbf{C}.$$

The above can be regarded as *the Fourier expansion* of χ^j, and we call g_a the a-th Fourier coefficient of χ^j (why?). Prove the following

(1) if $j \neq 0$, then $g_0 = 0$ and
$$g_a = p^{-1}\chi^j(-a^{-1})\mathfrak{g}(\chi^j) \text{ for } a \in \mathbb{F}_p^\times,$$
where $\mathfrak{g}(\chi^k)$ is the Gauss sum of χ^j;
(2) the functions $\left\{\chi^j\right\}_{j=0,1,\ldots,p-2}$ are linearly independent over $\mathbf{C}$.

Exercise 3 (5 pts)**.** Let $f = f(x_1, \cdots, x_n) = a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 \in \mathbb{F}_p[x_1, \ldots, x_n]$ with $a_i \in \mathbb{F}_p^\times$ for all $1 \leq i \leq n$. Show that if n is odd, then $\#X_f(\mathbb{F}_p) = p^{n-1}$, and if n is even, then

$$\#X_f(\mathbb{F}_p) = p^{n-1} + (p-1)\left(\frac{(-1)^{n/2}d}{p}\right)p^{n/2-1},\ d = a_1a_2\cdots a_{n-1}a_n.$$

Note that when $n = 3$, we have $\#\mathcal{C}_f(\mathbb{F}_p) = p + 1 = \#\mathbf{P}^1(\mathbb{F}_p)$.

Exercise 4 (5 pts)**.** Show that for every prime p, the equation

$$f(x, y, z) = 3x^3 + 4y^3 + 5z^3 \equiv 0 \,(\mathrm{mod}\ p)$$

has a non-zero solution, or equivalently, $\mathcal{C}_f(\mathbb{F}_p) \neq \emptyset$ for every prime p.
(Hint: Use Riemann hypothesis for curves over finite fields.)

Exercise 5 (10 pts)**.** Modify the proof of Theorem 3.5 to show that if $p \equiv 1 \,(\mathrm{mod}\ 7)$, then $p = a^2 + 7b^2$ for some integers a, b. You may need to use Galois theory.