# Lecture 1: Gauss sum, number of solutions of equations over finite fields and Weil conjecture

August 9, 2016

We start with two results of Gauss:

1. (Gauss sum) Let $p$ be an odd prime and $a$ be an integer prime to $p$. For a nontrivial Dirichlet character $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$, we define $\chi(0) = 0$ so that $\chi$ is now defined on the field $\mathbb{Z}/p\mathbb{Z}$. Define the Gauss sum
$$\tau_a(\chi) = \sum_{x=0}^{p-1} \chi(x) e(\frac{ax}{p}),$$
here $e(z) = e^{2\pi iz}$. Then it satisfies the property that $|\tau_a(\chi)| = \sqrt{p}$;

2. (counting number of solutions of equations over finite fields) Again let $p$ be an odd prime. We are interested in the number
$$N_p = \sharp\{(x, y) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) | y^2 = x^3 - x\}.$$
Gauss computed this number and his result can be stated as follows: when $p \equiv 3(mod\ 4)$, $N_p = p$; when $p \equiv 1(mod\ 4)$, we can find integers $r$ and $s$ such that $p = r^2 + s^2$. If we further require that $r$ is odd, $s$ is even and $r + s \equiv 1(mod\ 4)$ then $r$ and $s$ are uniquely determined. Under this setting, $N_p = p - 2r$. In particular, we have the estimation $|N_p - p| \leq 2\sqrt{p}$ as $|r| \leq \sqrt{p}$.

Question: is there any relation between the above two results? In the following, I will use an example to explain the relation between the Gauss sum and number of solutions of equations over finite fields.

**Exercise 1.** *Prove the above statements. (Hint: Actually only the computation of $N_p$ when $p \equiv 1(mod\ 4)$ is complicated. A good reference of this result is [1] Chapter 11).*

**Remark 1.** *Let $(\frac{\cdot}{p})$ be the Legendre symbol. Then we have*
$$N_p = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (1 + (\frac{x^3 - x}{p})) = p + \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (\frac{x^3 - x}{p}).$$
*So the above estimation becomes*
$$|\sum_{x \in \mathbb{Z}/p\mathbb{Z}} (\frac{x^3 - x}{p})| \leq 2\sqrt{p}.$$
*Since the Legendre is the quadratic character of $(\mathbb{Z}/p\mathbb{Z})^\times$, we see that the number $N_p$ can be expressed as the sum of some values of characters. We will use this idea in the following discussion.*

Now let $p$ be an arbitrary prime and $q$ be a power of $p$. Let $k = \mathbb{F}_q$ be the finite field with $q$ elements. We consider the homogeneous equation

$$a_0x_0^n + a_1x_1^n + \ldots + a_rx_r^n = 0 \tag{2}$$

over $k$, for $a_i \in k^\times$, $i = 0, \ldots r$. We make a further assumption $q \equiv 1(mod\ n)$ to simplify the notations. We want to study the number of solutions of this homogenous equation over $k$, which is denoted by $N_q$.

For each $(r+1)$-tuple $u = (u_0, u_1, \ldots, u_r)$, define a linear equation $L(u) = a_0u_0 + a_1u_1 + \ldots a_ru_r$. Then the homogenous equation (2) is equivalent to the following system of equations:

$$\begin{cases} L(u) = 0 \\ x_0^n = u_0 \\ \quad \ldots \\ x_r^n = u_r \end{cases} \tag{3}$$

So we have

$$N_q = \sum_{L(u)=0} N_0(u_0) \ldots N_r(u_r),$$

here $N_i(u_i)$ is the number of solutions of the equation $x_i^n = u_i$ over $k$. More precisely, we have:

$$N_i(u_i) = \begin{cases} 1, & \text{if } u_i = 0 \\ n, & \text{if } u_i \text{ is an n-th power in } k^\times \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

Notice that here we use the assumption that $q \equiv 1(mod\ n)$. Since the multiplicative group $k^\times$ is cyclic, it has a unique subgroup of order $n$.

As mentioned in Remark 1, we want to express the number $N_i(u_i)$ as the sum of some values of characters of $k^\times$. First we need a concrete description of such characters. Fix a generator $w$ of $k^\times$, then any character of $k^\times$ is of the form

$$\chi_\alpha(w) = e^{2\pi i\alpha},$$

for some $\alpha \in \mathbb{Q}$ satisfying $(q-1)\alpha \in \mathbb{Z}$. As before, we extend $\chi_\alpha$ to $k$ by requiring

$$\chi_\alpha(0) = \begin{cases} 0, & \text{if } \alpha \notin \mathbb{Z} \\ 1, & \text{if } \alpha \in \mathbb{Z} \end{cases} \tag{5}$$

Under the above notations, we have:

$$N_i(u_i) = \sum_{\alpha \in [0,1), n\alpha \in \mathbb{Z}} \chi_\alpha(u_i).$$

**Exercise 2.** *Verify this equality. (Hint: When $u_i = 0$, both sides are equal to 1. When $u_i \neq 0$, the right hand side becomes $\sum_{i=0}^{n-1} \zeta^i$, for $\zeta = \chi_{\frac{1}{n}}(u)$. Notice that $\zeta = 1$ if and only if $u$ is an $n$-th power).*

Now we can write $N_q$ as the sum:

$$\begin{aligned} N_q &= \sum_{L(u)=0} \Big( \sum_{\alpha=(\alpha_0,\ldots,\alpha_r), \alpha_i \in [0,1), n\alpha_i \in \mathbb{Z}} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) \Big) \\ &= \sum_{\alpha=(0,\ldots,0)} \sum_{L(u)=0} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) + \sum_{\text{some } \alpha_i \text{ are 0, but not all}} \Big( \sum_{L(u)=0} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) \Big) \\ &+ \sum_{\alpha=(\alpha_i \in (0,1), n\alpha_i \in \mathbb{Z}} \sum_{L(u)=0} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) \end{aligned}$$

**Exercise 3.** *Compute the first two sums in the above expression and show that*

$$\sum_{\alpha=(0,\ldots,0)} \sum_{L(u)=0} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r) = q^r,$$

*and*

$$\sum_{\text{some } \alpha_i \text{ are 0, but not all}} (\sum_{L(u)=0} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r)) = 0$$

*(Hint: For the second sum, without loss of generality, you can assume that $\alpha_0 = \ldots = \alpha_s = 0$ and $\alpha_{s+1}, \ldots \alpha_r$ are nonzero for some $0 \leq s \leq r-1$. Then do the computation.)*

By the above exercise, we have:

$$N_q = q^r + \sum_{\alpha=(\alpha_0,\ldots,\alpha_r),\alpha_i\in(0,1),n\alpha_i\in\mathbb{Z}} \sum_{L(u)=0} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r).$$

Replacing $u_i$ by $u_i/a_i$, the sum becomes

$$N_q = q^r + \sum_{\alpha=(\alpha_0,\ldots,\alpha_r),\alpha_i\in(0,1),n\alpha_i\in\mathbb{Z}} \chi_{\alpha_0}(a_0^{-1})\ldots\chi_{\alpha_r}(a_r^{-1})S(\alpha)$$

where

$$S(\alpha) = \sum_{u_0+\ldots u_r=0} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r)$$

We can decompose $S(\alpha)$ into two parts:

$$S(\alpha) = \sum_{u_0+\ldots u_r=0,u_0=0} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r) + \sum_{u_0+\ldots u_r=0,u_0\neq 0} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r).$$

Since $\chi_{\alpha_0}(0) = 0$, the first sum in the above expression is 0. For the second sum, since $u_0 \neq 0$, we can do the change of variables $u_i = u_0 v_i$, $i = 1, \ldots, r$. Then

$$S(\alpha) = \sum_{1+v_1+\ldots+v_r=0} \chi_{\alpha_1}(v_1)\ldots\chi_{\alpha_r}(v_r) \sum_{u_0\neq 0} \chi_\beta(u_0),$$

for $\beta = \alpha_0 + \ldots + \alpha_r$.

**Exercise 4.** *Show that*

$$\sum_{u_0\neq 0} \chi_\beta(u_0) = \begin{cases} q-1, & \text{if } \beta \in \mathbb{Z} \\ 0, & \text{if } \beta \notin \mathbb{Z} \end{cases}$$

For any $(r+1)$-tuple $\alpha = (\alpha_0, \ldots, \alpha_r)$ satisfying $\alpha_i \in (0,1), n\alpha_i \in \mathbb{Z}$ and $\sum_{i=0}^r \alpha_i \in \mathbb{Z}$, define

$$J(\alpha) = \sum_{1+v_1+\ldots+v_r=0} \chi_{\alpha_1}(v_1)\ldots\chi_{\alpha_r}(v_r) = \frac{1}{q-1} \sum_{u_0+\ldots u_r=0} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r),$$

which is called the Jacobi sum of the characters $\chi_{\alpha_0}, \ldots, \chi_{\alpha_r}$. Under this definition, we have

$$N_q = q^r + (q-1) \sum_{\alpha_i\in(0,1),n\alpha_i\in\mathbb{Z},\sum_{i=0}^r \alpha_i\in\mathbb{Z}} \chi_{\alpha_0}(a_0^{-1})\ldots\chi_{\alpha_r}(a_r^{-1})J(\alpha).$$

The Jacobi sum is closely related to the Gauss sum, which we will define now. If $\chi : k^\times \to \mathbb{C}^\times$ is a nontrivial character, for any $a \in k^\times$, define the Gauss sum as

$$\tau_a(\chi) = \sum_{t \in k} \chi(t)\zeta_p^{\mathrm{Tr}(at)},$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$ and $\mathrm{Tr} : k \to \mathbb{F}_p$ is the trace map. Notice that when $k = \mathbb{F}_p$, this definition coincides with the definition we give at the beginning and similarly we have $|\tau_a(\chi)| = \sqrt{q}$. For simplicity, we set $\tau(\chi) = \tau_1(\chi)$. Under this definition, we have:

$$J(\alpha) = \frac{1}{q}\tau(\chi_{\alpha_0}) \dots \tau(\chi_{\alpha_r}).$$

**Exercise 5.** *Prove the above equality. (Hint: You can start with some simple cases, e.g. $k = \mathbb{F}_p$ and $r = 2$ to get some feeling about what this equality says.)*

As a consequence of the above equality, we have an estimation

$$|N_q - q^r| = M(q-1)q^{\frac{r-1}{2}},$$

here $M$ is the cardinality number of the set $\{\alpha = (\alpha_0, \dots, \alpha_r) | \alpha_i \in (0,1), n\alpha_i \in \mathbb{Z}, \sum_{i=0}^r \alpha_i \in \mathbb{Z}\}$.

Since the equation (2) is homogenous, it defines a hypersurface $S$ in the projective space $\mathbb{P}^r(k)$. Recall that

$$\mathbb{P}^r(k) = \{[X_0, X_1, \dots, X_r] \in k^{r+1} | X_i's \text{ are not all zero}\}/\sim,$$

and $[X_0, X_1, \dots, X_r] \sim [Y_0, Y_1, \dots, Y_r]$ if and only if there exists $c \in k^\times$ such that $X_i = cY_i$ for all $i$.

Let $N'_q$ be the number of $k$-rational points on the hypersurface $S$. Then

$$N'_q = \frac{N_q - 1}{q-1} = 1 + q + \dots + q^{r-1} + \sum_\alpha \chi_{\alpha_0}(a_0^{-1}) \dots \chi_{\alpha_r}(a_r^{-1}) J(\alpha).$$

Since the hypersurface $S$ is defined over $k$, we can do similar discussion as above for any finite extension of $k$. To be more precise, for any positive integer $s$, let $k_s/k$ be the finite extension of degree $s$ so $k_s$ has $q^s$ elements. Let $N'_{q^s}$ be the number of $k_s$-rational points on $S$. Then from the above discussion, we have

$$N'_{q^s} = 1 + q^s + \dots + q^{s(r-1)} + \sum_\alpha \chi^{(s)}_{\alpha_0}(a_0^{-1}) \dots \chi^{(s)}_{\alpha_r}(a_r^{-1}) J^{(s)}(\alpha),$$

here $\chi^{(s)}_\alpha$ is the character of $k_s^\times$ which sends a fixed generator $w^{(s)}$ to $e^{2\pi i\alpha}$.

If we want to compare the numbers $N'_q$ and $N'_{q^s}$, we need to know relations between characters of $k^\times$ and $k_s^\times$. In fact, let $\mathrm{Nm} : k_s^\times \to k^\times$ be the norm map, which is known to be surjective. Hence the norm map must maps a generator of $k_s^\times$ to a generator of $k^\times$. If we choose the generators suitably, we will have the equality $\chi^{(s)}_\alpha = \chi_\alpha \circ \mathrm{Nm}$. Based on this fact, Davenport and Hasse proved the following relation on Jacobi sums (see [1] Chapter 11 or [1]):

$$J^s(\alpha) = (-1)^{(s-1)(r-1)} J(\alpha)^s.$$

From this we have:

$$N'_{q^s} = 1 + q^s + \dots + q^{s(r-1)} + \sum_\alpha (-1)^{(s-1)(r-1)} (\chi_{\alpha_0}(a_0^{-1}) \dots \chi_{\alpha_r}(a_r^{-1}) J(\alpha))^s. \tag{6}$$

If we want to record the numbers $N'_{q^s}$ for all $s$, we can consider the formal power seris

$$f(U) = \sum_{s=1}^{\infty} N'_{q^s} U^{s-1}.$$

Using the equality (6), and the identity

$$\sum_{s=1}^{\infty} X^s U^{s-1} = \frac{\mathrm{d}}{\mathrm{d}U}(-\log(1-XU)),$$

we have

$$f(U) = \sum_{i=0}^{r-1} \frac{\mathrm{d}}{\mathrm{d}U}(-\log(1-q^i U)) + (-1)^r \sum_{\alpha} \frac{\mathrm{d}}{\mathrm{d}U}(-\log(1-C(\alpha)U))$$

here $C(\alpha) = (-1)^{r-1}\chi_{\alpha_0}(a_0^{-1})\dots\chi_{\alpha_r}(a_r^{-1})J(\alpha)$.

**Definition 7.** *The zeta function of the hypersurface $S_{/k}$ is defined to be the formal power series*

$$Z(S/k, U) = \exp(\sum_{s=1}^{\infty} \frac{N'_{q^s}}{s} U^s).$$

From the above discussion, we see that the zeta function is of the form

$$Z(S/k, U) = \frac{P(U)^{(-1)^r}}{(1-U)(1-qU)\dots(1-q^{r-1}U)},$$

for $P(U) = \prod_{\alpha}(1 - C(\alpha)U)$.

Here are some observations on the zeta function:

1. $Z(S/k, U)$ is a rational function of $U$;
2. Write $P(U) = (1-b_1U)\dots(1-b_mU)$, then all the $b_i$'s are algebraic integers with absolute value $q^{\frac{r-1}{2}}$. Moreover, the map $b \mapsto q^{r-1}/b$ is a permutation of the set $\{b_1, b_2, ..., b_m\}$.

A.Weil made a conjecture predicting some properties of the zeta functions of smooth projective varieties over finite fields and gave a proof for projective curves. In the following lectures, I will give the precise statement of Weil's conjecture and explain his proof for curves.

# References

[1] K. Ireland, M. Rosen. A Classical Introduction to Modern Number Theory, Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990

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