Weil conjecture for curves over finite fields

August 16, 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 χ 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 [4] 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:

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

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 χ_α 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:

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

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

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

(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:

$$S(\alpha) = \sum_{u_0+\ldots u_r=0,u_0=0} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r) + \sum_{u_0+\ldots u_r=0,u_0\neq0} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r).$$

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

$$S(\alpha) = \sum_{1+v_1+\ldots+v_r=0} \chi_{\alpha_1}(v_1)\ldots\chi_{\alpha_r}(v_r) \sum_{u_0\neq0} \chi_\beta(u_0),$$

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

Exercise 4. *Show that*

$$\sum_{u_0\neq0} \chi_\beta(u_0) = \begin{cases} q-1, & \textit{if } \beta\in\mathbb{Z} \\ 0, & \textit{if } \beta\notin\mathbb{Z} \end{cases}$$

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 [4] Chapter 11 or [4]):

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

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 $P(U) = (1 - b_1 U) \dots (1 - b_m U)$, 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, I will give the precise statement of Weil's conjecture and explain his proof for curves.

Weil conjecture for curves over finite fields: Let $C/\mathbb{F}_q$ be a smooth projective curve over the finite field $\mathbb{F}_q$. Define the zeta function of $C/\mathbb{F}_q$ as

$$Z(C/\mathbb{F}_q, T) = \exp(\sum_{m=1}^{\infty} \frac{N_m}{m} T^m),$$

here N_m is the number of $\mathbb{F}_{q^m}$-rational points on $C/\mathbb{F}_q$. Then this function satisfies the following properties:

1. (rationality) There exists an integer $g \geq 0$ (the genus of $C/\mathbb{F}_q$) and a polynomial $P(T) \in \mathbb{Z}[T]$ of degree $2g$ such that
$$Z(C/\mathbb{F}_q, T) = \frac{L(T)}{(1-T)(1-qT)};$$

2. (functional equation)
$$Z(C/\mathbb{F}_q,T)=q^{g-1}T^{2g-2}Z(C/\mathbb{F}_q,\frac{1}{qT});$$

3. (Riemann hypothesis) There exists algebraic integers $\alpha_1,\dots,\alpha_{2g}$,such that
$$L(T)=(1-\alpha_1T)\dots(1-\alpha_{2g}T),$$
and $|\alpha_i|=\sqrt{q}$ for $i=1,\dots,2g$.

Corollary 8. *For all $m\geq 1$, we have*
$$N_m=1+q^m-\sum_{i=1}^{2g}\alpha_i^m.$$
In particular, when $g=1$, $N_m>0$ for all m, i.e. any genus one curve over $\mathbb{F}_q$ (equivalently, any elliptic curve over $\mathbb{F}_q$) has a rational point.

Remark 9. *1. Without assuming the Riemann hypothesis, the functional equation is equivalent to the fact that the map $\alpha\mapsto\frac{q}{\alpha}$ is a permutation of the set $\{\alpha_1,\dots,\alpha_{2g}\}$;*

2. If we define $\zeta(C/\mathbb{F}_q,s)=Z(C/\mathbb{F}_q,q^{-s})$. Then the last part of Weil conjecture is equivalent to the fact that if s is a zero of $\zeta(C/\mathbb{F}_q,s)$, then $\Re(s)=\frac{1}{2}$. This is why it is called the Riemann hypothesis.

First we will prove the rationality and functional equation of the zeta functions. Before we start the proof, we need to introduce some tools in algebraic geometry. We start with divisors on curves.

Definition 10. *Let C/k be a projective smooth curve over an algebrically closed field k. A divisor of C/k is a formal finite sum $D=\sum_P n_P\cdot P$, where $P\in C(k)$'s are k-rational points of C, $n_P\in\mathbb{Z}$ and $n_P=0$ for all but finitely many P's. The set* Div(C/k) *of divisors of C/k forms an abelian group in the obvious way. For any divisor $D=\sum_P n_P\cdot P$, its degree is defined to be the number* deg$D=\sum_P n_P$. *We introduce a partial order on* Div(C/k)*:*
$$D=\sum_P n_P\cdot P\geq D'=\sum_P n'_P\cdot P \textit{ if and only if } n_P\geq n'_P \textit{ for all } P.$$
A divisor $D=\sum_P n_P\cdot P$ is called effective if and only if $D\geq 0$, i.e. $n_P\geq 0$ for all P.

Now we turn to the case that k is not necessarily algebraically closed. A naive guess is to define
$$\mathrm{Div}(C/k)=\{\sum_P n_P\cdot P|n_P\in\mathbb{Z},P\in C(k)\text{ and }n_P=0\text{ for all but finitely many }P\}.$$
The problem is that the curve C may have very few k-rational pionts when k is not algebraically closed. Then the above set will be too small and useless for the study of the curve. Before we give the correct definition, first let's see an example.

Example 1. *Let $C=\mathbb{P}^1/\mathbb{Q}$ be the projective line over $\mathbb{Q}$ and consider the divisor $D=P_1+P_2$, here P_1 (resp.P_2) is the point on C with coordinate $[\sqrt{2}:1]$ (resp. $[-\sqrt{2}:1]$). Neither of the points P_1, P_2 are defined over $\mathbb{Q}$, but we may think that the divisor D is defined over $\mathbb{Q}$ as the two points P_1,P_2 are the zeroes of the rational homogenous function X^2-2Y^2. Moreover, the two points P_1,P_2 are defined over the quadratic extension $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$, and the nontrivial element in* Gal$(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ *switches the two points.*

In the following discussion, we assume that $k = \mathbb{F}_q$ is a finite field and fix an algebraic closure $\bar{k}$ of k. Let P be a $\bar{k}$-rational point on C. Then we can find a finite extension K/k of k such that P is defined over K. We can choose K such that there is no intermediate field K' between K and k on which the point P is defined. As is indicated from the above example, we can consider the divisor

$$D = \sum_{\sigma \in \mathrm{Gal}(K/k)} \sigma(P).$$

This divisor is effective and stable under the action of $\mathrm{Gal}(K/k)$. So it is expected that D is 'defined' over k.

Definition 11. *We define the divisor group* $\mathrm{Div}(C/k)$ *of* C/k *as the subgroup of* $\mathrm{Div}(C/\bar{k})$ *generated by divisors of the above form. The divisors constructed above are called irreducible divisors over* k *as they cannot be written as the sum of two nonzero effective divisors in* $\mathrm{Div}(C/k)$*.*

Definition 12. *Define* $\mathrm{Div}^0(C/k)$ *as the subgroup of* $\mathrm{Div}(C/k)$ *of degree* 0*. Let* $f \neq 0$ *be a rational function on the curve* C/k*, it defines a divisor*

$$\mathrm{div}(f) = \sum_{P \in C(\bar{k})} \mathrm{ord}_P(f) P,$$

here $\mathrm{ord}_P(f)$ *is the order of* f *at* P*. Since* f *is defined over* k*, the divisor* $\mathrm{div}(f)$ *belongs to* $\mathrm{Div}(C/k)$*. Such a divisor is called principal and its degree is* 0*. So the set of principal divisors* Prin(C/k) *is a subgroup of* $\mathrm{Div}^0(C/k)$*. Finally, two divisors* D_1 *and* D_2 *are called linearly equivalent (denoted by* $D_1 \sim D_2$*) if* $D_1 - D_2$ *is principal.*

Exercise 6. *Show that the equality* $\mathrm{Prin(C/k)} = \mathrm{Div}^0(C/k)$ *holds (i.e. all the divisors of degree* 0 *are principal) if and only if* $C = \mathbb{P}^1/k$*.*

By the language of divisors, we can rewrite the zeta function as

$$Z(C/k, T) = \prod_D (1 - T^{\deg D}) = \sum_{n=0}^{\infty} A_n T^n,$$

here in the product D ranges in the set of irreducible effective divisors over k, and in the last sum, A_n is the number of effective divisors of degree n over k.

in fact, let Φ_l be the number of irreducible effective divisors of degree m over k. Then we have the relation:

$$N_m = \sum_{n|m} n\Phi_n,$$

as an irreducible divisor of degree n will provide exactly n $\mathbb{F}_{q^n}$-rational points on C if $n|m$. Then we have

$$\begin{aligned}
\log Z(C/k, T) &= \sum_{m=1}^{\infty} \frac{N_m}{m} T^m = \sum_{m=1}^{\infty} \sum_{n|m} \frac{n\Phi_n}{m} T^m \\
&\overset{\mathrm{m=nh}}{=} \sum_{n=1}^{\infty} \sum_{h=1}^{\infty} \frac{n\Phi_n}{hn} T^{nh} = \sum_{n=1}^{\infty} \Phi_n(-\log(1 - T^n)) \\
&= \sum_{n=1}^{\infty} \sum_{\deg D = n} -\log(1 - T^{\deg(D)}),
\end{aligned}$$

and the first equality follows.

$$\prod_D (1-T^{\deg D})^{-1} = \prod_D (\sum_{m=0}^{\infty} T^{m\deg D}) = \sum_{n=0}^{\infty} (\sum_{m_1\deg D_1+\ldots+m_r\deg D_r=n} 1)T^n = \sum_{n=1}^{\infty} A_n T^n,$$

then the second equality follows. To compute the zeta function, it is enough to compute the numbers A_n's, and now we need the Riemann-Rock theorem.

Definition 13. *Let D be a divisor of C/k. Define a set*

$$L(D) = \{f \in k(C) | f \neq 0, \mathrm{div}(f) + D \geq 0\} \cup \{0\},$$

here $k(C)$ is the filed of rational functions on C.

Remark 14. *Since $\mathrm{ord}_P(f_1+f_2) \geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2))$, and a principal divisor has degree 0, we have the following properties for $L(D)$:*

1. *$L(D)$ is a finite dimensional vector space over k, and we denote its dimension by $l(D)$;*
2. *If $D \sim D'$, then $l(D) = l(D')$;*
3. *$L(0) = k$ and hence $l(0) = 1$;*
4. *$l(D) = 0$ if $\deg D < 0$.*

Theorem 1. *Let C/k be a smooth projective curve. Then there exists an integer $g \geq 0$ (called the genus of C/k) and a divisor K_C (called the canonical divisor of C/k) such that for all divisor D, we have*

$$l(D) - l(K_C - D) = \deg D - g + 1.$$

Remark 15. *The canonical divisor is unique up to linear equivalence. When $C/k = \mathbb{P}^1/k$, $K_C = -2P$, here P is an arbitrary k-rational point on the projective line. For other curves, there is a holomorphic differential ω on C/k (unique up to constant scalars). The canonical divisor can be taken as $K_C = \mathrm{div}(\omega)$ (we can associate a divisor to a holomorphic differential in a similar manner as what we do for rational functions). For example, we consider the elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$. One can check that the formula*

$$\omega = \frac{\mathrm{d}x}{2y} = \frac{\mathrm{d}y}{3x^2+a}$$

defines a holomorphic 1-form on E. Moreover, it has no zeroes or poles. So $K_E = 0$.

Taking $D = 0, K_C$ in the Riemann-Rock theorem, we have:

Corollary 16. *1. $l(K_C) = g$;*

2. *$\deg(K_C) = 2g - 2$;*
3. *If $\deg D \geq 2g - 1$, then $l(D) = \deg D - g + 1$.*

Now we are able to prove the rationality of the zeta functions. Let h be the cardinality number of the group $\mathrm{Div}^0(C/k)/\mathrm{Prin}(C/k)$, which is known to be a finite number. We assume the following fact:

Assumption : there exists a divisor c_1 of degree 1 on C/k.

This fact can be proved by Galois cohomology, but we do not give a proof here to make the notes in a reasonable length.

Under this assumption, we have a bijection of sets:

$$\{D \in \mathrm{Div}(C/k) | \mathrm{deg} D = n\} \leftrightarrow \{D \in \mathrm{Div}(C/k) | \mathrm{deg} D = 0\}$$
$$c \leftrightarrow c - nc_1$$

Let Σ_0 be a set of representatives of $\mathrm{Div}^0(C/k)/\mathrm{Prin}(C/k)$, then $\Sigma_n = \{c + nc_1 | c \in \Sigma_0\}$ is a set of representatives of divisors of degree n under linear equivalence. Then

$$\begin{aligned}\{D|D \text{ is an effective divisor of } C/k, \mathrm{deg}D = n\} &= \bigsqcup_{c\in\Sigma_n} \{D|D \text{ is an effective divisor of } C/k, \mathrm{deg}D = n, D \sim c\} \\ &= \bigsqcup_{c\in\Sigma_n} \{c + \mathrm{div}(f) | 0 \neq f \in k(C), c + \mathrm{div}(f) \geq 0\}.\end{aligned}$$

In view of Definition 13, we can compute the number A_n as:

$$A_n = \sum_{c\in\Sigma_n} \frac{q^{l(c)} - 1}{q - 1} = \frac{1}{q-1}(\sum_{c\in\Sigma_n} q^{l(c)} - \sum_{c\in\Sigma_n} 1) = \frac{1}{q-1}(\sum_{c\in\Sigma_n} q^{l(c)} - h).$$

If $n = \deg(c) > 2g - 2$, $l(c) = \deg(c) - g + 1 = n - g + 1$. So the zeta function becomes

$$Z(C/k, T) = \frac{1}{q-1}(\sum_{n=0}^{2g-2} \sum_{c\in\Sigma_n} q^{l(c)}T^n + \sum_{n=2g-1}^{\infty} hq^{n+1-g}T^n - h\sum_{n=0}^{\infty} T^n)$$

Define

$$A(T) = \sum_{n=0}^{2g-2} \sum_{c\in\Sigma_n} q^{l(c)}T^n, B(T) = \sum_{n=2g-1}^{\infty} q^{n+1-g}T^n - \sum_{n=0}^{\infty} T^n$$

Then $A(T) \in \mathbb{Z}[T]$ of degree $\leq 2g - 2$ and $B(T) = \frac{q^g T^{2g-1}}{1-qT} - \frac{1}{1-T}$. If we define the polynomial

$$L(T) = \frac{1}{q-1}(A(T)(1 - qT)(1 - T) + h((1 - T)q^g T^{2g-1} - (1 - qT))) \in \mathbb{Q}[T],$$

which is of degree at most $2g$, then the zeta function is of the form

$$Z(C/k, T) = \frac{L(T)}{(1 - T)(1 - qT)}.$$

Moreover, we have $L(1) = h, L(\frac{1}{q}) = hq^{-g+1}$. Since $Z(C/k, T) \in \mathbb{Z}[[T]]$, we have $L(T) \in \mathbb{Z}[T]$. So we see that the zeta function is a rational function of T.

We continue to prove the functional equation. The map $c \mapsto K_C - c = c'$ is a bijection of the set $\{c | 0 \leq \mathrm{deg} c \leq 2g - 2\}$ and by the Riemann-Rock theorem, we have

$$l(c') = l(c) - \deg(c) - 1 + g.$$

So

$$\begin{aligned}q^{g-1}T^{2g-2}A(\frac{1}{qT}) &= \sum_{n=0}^{2g-2} \sum_{c\in\Sigma_n} q^{l(c)+g-1-n}T^{2g-2-n} \\ &= \sum_{n=0}^{2g-2} \sum_{c\in\Sigma_n} q^{l(c')}T^{\deg(c')} = A(T).\end{aligned}$$

On the other hand, by direct computation we have

$$B(T) = q^{g-1}T^{2g-2}B(\frac{1}{qT}).$$

So the zeta function satisfies the desired functional equation, which implies that the degree of the polynomial $L(T)$ is $2g$. Since $L(T) \in \mathbb{Z}[T]$ and has constant term 1, we can find algebraic integers $\alpha_1, \ldots, \alpha_{2g}$, such that

$$L(T) = \prod_{i=1}^{2g}(1 - \alpha_i T),$$

and the map $\alpha \mapsto \frac{q}{\alpha}$ is a permutation of the set $\{\alpha_1, \ldots, \alpha_{2g}\}$.

It remains to prove the Riemann Hypothesis, i.e. $|\alpha_i| = \sqrt{q}$ for all $i = 1, \ldots, 2g$. We need to make some preparation on algebraic geometry before the proof.

We start with the definition of the degree of smooth projective curves. Given a polynomial $f(X) = a_nX^n + \ldots + a_0 \in \mathbb{C}[X]$ with no multiple roots, we know that its degree is n if $a_n \neq 0$. We can interpret the degree of a polynomial in a geometric way.

The equation $Y = f(X)$ defines a curve on the affine plane. It intersects the line $Y = 0$ at n points. So we can regard the degree n as the intersection number of these two plane curves. Notice that on the affine plane, two lines may have intersection number 0 or 1, depending on whether they are parallel or not. This suggests that we'd better work in the projective spaces to get a satisfactory intersection theory.

In $\mathbb{P}^2$, if a smooth projective curve is defined as the zero locus of a single homogenous polynomial $F(X, Y, Z)$, then the degree of C is defined to be the degree of $F(X, Y, Z)$. In general, in $\mathbb{P}^n$, if a smooth projective curve C is defined by $n-1$ homogeneous polynomials $F_1, \ldots, F_{n-1}$, then the degree of C is defined to be the product $\prod_{i=1}^{n-1} \deg(F_i)$. However, not all the projective curves can be defined in this way (the above curves are called complete intersections and this is a very strong condition on the curves). To define the degree of a general curve, we need a geometric definition of the degree. In fact, the degree of a curve $C \subset \mathbb{P}^n$ is the number of intersection points of C and H, where H is a hyperplane in $\mathbb{P}^n$ which intersects with C transversally. The last sentence means that if $P \in H \cap C$, then the tangent space of H and C at P should span the tangent space of $\mathbb{P}^n$ at P. In the general situation, we can define a multiplicity for each intersection point and the degree of the curve is equal to the sum of these multiplicities.

Remark 17. *Unlike the genus, the degree of a curve is not intrinsic. It depends on the embedding of the curve to the projective space. For example, consider the elliptic curve $E : Y^2Z = X^3 + AXZ^2 + BZ^3$ in $\mathbb{P}^2$. Under this embedding, E has degree 3. On the other hand, we can embed E in to $\mathbb{P}^3$:*

$$\begin{aligned} E &\to \mathbb{P}^3 \\ [X : Y : Z] &\mapsto [Z^2 : XZ : YZ : X^2]. \end{aligned}$$

Under this embedding, E has degree 4.

Theorem 2. *(Bézout) Let C_1 and C_2 be two distinct curves (not necessarily smooth) in $\mathbb{P}^2$ of degree d_1 and d_2. Then the intersection of C_1 and C_2 is finite and the number of intersection points is d_1d_2 (counted with multiplicity).*

Let S/k be an algebraic surface over an algebraically closed field k. A divisor of S is a formal finite sum $\sum_C n_C C$, where C's are irreducible projective curves (not necessarily smooth) on S, and as before we can define the group of divisors $\mathrm{Div}(S/k)$, the principal divisor $\mathrm{div}(f)$ associated to any nonzero rational function f on S and the notion of linear equivalence.

When $S = \mathbb{P}^2$, by Bézout Theorem, we can define a bilinear form on $\mathrm{Div}(S/k)$, such that $C_1 \cdot C_2 = d_1d_2$ if $C_1 \neq C_2$ and $C \cdot C = (\mathrm{deg}C)^2$. This construction can be generalized to an arbitrary smooth projective surface S. If $D_1, D_2 \in \mathrm{Div}(S/k)$, then $D_1 \cdot D_2$ is called the intersection number of D_1 and D_2. It satisfies the property that $D \cdot \mathrm{div}(f) = 0$ for any divisor D and nonzero rational function f. However, Bézout Theorem is not true for general surfaces, and the definition of the self intersection number of a curve C on S could be tricky. If we can find another curve C' which is linearly equivalent to C, then $C \cdot C = C \cdot C'$ as $C - C'$ is principal, and the number $C \cdot C'$ is defined. But one may not find such a curve C'. In algebraic geometry, we define the self intersection number of C as the degree of the line bundle $\mathcal{N}_{\mathcal{S}/\mathcal{C}}$, where $\mathcal{N}_{\mathcal{S}/\mathcal{C}}$ is the normal bundle of the embedding $C \subset S$. As we will see in the computation below, $C \cdot C$ can be negative or 0 if S is not $\mathbb{P}^2$.

The reason that we care the intersection theory on surfaces is that we can interpret the number $N_q = \sharp C(\mathbb{F}_q)$ as an intersection number, here $C/\mathbb{F}_q$ is a smooth projective curve of genus g. To be more precise, let $\mathrm{Frob} : C \to C$ be the Frobenius map. Then $C(\mathbb{F}_q)$ are exactly the Frob-invariant points in $C(\bar{\mathbb{F}}_q)$. Let S be the surface $C \times C$ over $\mathbb{F}_q$. We define several curves on S: let Γ be the graph of the Frobenius map, i.e. Γ is the image of the morphism $(\mathrm{id}, \mathrm{Frob}) : C \to C \times C$; let Δ be the diagonal curve of $C \times C$, i.e. Δ is the image of the morphism $(\mathrm{id}, \mathrm{id}) : C \to C \times C$; finally, set $F_1 = C \times \{P\}$ and $F_2 = \{P\} \times C$, for a fixed point $P \in C(\bar{\mathbb{F}}_q)$.

Lemma 18. *(calculation of the intersection numbers) Under the above notations, we have*

$$\Gamma \cdot \Delta = N_q, \Delta \cdot \Delta = 2 - 2g, \Gamma \cdot \Gamma = q(2 - 2g), \Gamma \cdot F_1 = q, \text{ and } \Gamma \cdot F_2 = 1.$$

Proof. The equalities $\Gamma \cdot \Delta = N_q, \Gamma \cdot F_1 = q,$ and $\Gamma \cdot F_2 = 1$ can be checked by the geometric interpretation of intersection numbers. The calculation of $\Delta \cdot \Delta$ relies on the adjunction formula: if $C_1 \subset S$ is a smooth projective curve, then

$$K_{C_1} = (K_S + C_1)|_{C_1},$$

where K_{C_1} is the canonical divisor on C_1, and K_S is the canonical divisor on S. More precisely, we have

$$K_S = p_1^* K_C + p_2^* K_C = K_C \times C + C \times K_C,$$

where $p_i : S \to C$ is the projection map to the i-th factor, for $i = 1, 2$.

Taking the degrees of both sides of the adjunction formula, we have

$$\mathrm{deg} K_{C_1} = K_S \cdot C_1 + C_1 \cdot C_1.$$

Now we take $C_1 = \Delta$, and we have

$$K_S \cdot \Delta + \Delta \cdot \Delta = \mathrm{deg} K_\Delta = 2g - 2 \text{ as } \Delta \cong C. \tag{19}$$

On the other hand, we have

$$K_S \cdot \Delta = (K_C \times C) \cdot \Delta + (C \times K_C) \cdot \Delta = (2g - 2) + (2g - 2).$$

Then equation (19) gives $\Delta \cdot \Delta = 2 - 2g$. Notice that this self intersection number is negative if $g > 1$.

Finally, notice that Γ is the pre-image of Δ under the map $\mathrm{Frob} \times \mathrm{id}_C : S \to S$, so we have

$$\Gamma \cdot \Gamma = \deg(\mathrm{Frob} \times \mathrm{id}_C) \Delta \cdot \Delta = q(2 - 2g).$$

□

To prove the Riemann hypothesis, we need the following:

Theorem 3. *(Castelnuovo inequality) Let D be a divisor on the surface $S = C \times C$. If $d_1 = D \cdot F_1$, $d_2 = D \cdot F_2$, then*

$$D \cdot D \leq 2 d_1 d_2.$$

We refer to [3] Chapter 2 or [4] for a proof of the above theorem.

For any integers r and s, define a divisor $D = r\Gamma + s\Delta$ on S. Then

$$d_1 = D \cdot F_1 = rq + s, d_2 = D \cdot F_2 = r + s.$$

By Castelnuovo inequality,

$$D \cdot D = r^2 q(2 - 2g) + 2rsN_q + s^2(2 - 2g) \leq 2(rq + s)(r + s).$$

So we have

$$gqr^2 + (q + 1 - N_q)rs + gs^2 \geq 0 \text{ for all } r, s \in \mathbb{Z}.$$

This implies that

$$|q + 1 - N_q| \leq 2g\sqrt{q}.$$

From the rationality of the zeta function, this is equivalent to

$$|\sum_{i=1}^{2g} \alpha_i| \leq 2g\sqrt{q}.$$

We can repeat the above argument for any finite extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$, and we have

$$|\sum_{i=1}^{2g} \alpha_i^m| \leq 2g\sqrt{q^m}.$$

Then the Riemann hypothesis follows from the following lemma:

Lemma 20. *If $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$, such that there exists a constant C satisfying*

$$|\sum_{i=1}^{k} \lambda_i^n| \leq C$$

for all $n \geq 1$, then $|\lambda_i| \leq 1$ for all i.

Exercise 7. *Prove the above lemma.*

By this lemma, we have

$$|\alpha_i| \leq \sqrt{q},$$

for all i. On the other hand, from the functional equation of the zeta function, we see that the map $\alpha \mapsto \frac{q}{\alpha}$ preserves the set $\{\alpha_1, \ldots, \alpha_{2g}\}$. So we have

$$|\frac{q}{\alpha_i}| \leq \sqrt{q},$$

for all i. Combining the above two equalities together, we have $|\alpha_i| = \sqrt{q}$ for all i.

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.

[3] L. Badescu. Algebraic Surfaces, Universitext, Springer, New York, 2001

[4] M. Hindry. La preuve par André Weil de l'hypothèse de Riemann pour une courbe sur un corps fini. Henri Cartan and André Weil, mathématiciens du XXe siècle, 6398, Ed. Éc. Polytech., Palaiseau, 2012.