Zeta function of a curve

1 Example

Consider the curve C with equation $X^3Y+Y^3Z+Z^3X=0$ defined over $k=\mathbf{F}_2$. Let N_d be the number of points with coordinates in $\mathbf{F}_{2^d}$.

We have $N_1=3$: there are three points defined over $\mathbf{F}_2=\{0,1\}$, namely $(0,0,1)$, $(0,1,0)$ and $(1,0,0)$.

We have $N_2=5$: there are five points defined over $\mathbf{F}_4=\{0,1,\omega,\omega^2\}$, namely three over $\mathbf{F}_2$ and the two points $(1,\omega,\omega^2)$, $(1,\omega^2,\omega)$.

We have $N_3=24$: there are 24 points defined over $\mathbf{F}_8=\{0,1,\zeta,...,\zeta^6\}$ where $\zeta^7=1$, namely three over $\mathbf{F}_2$ and the 21 points $(1,\zeta^i,\zeta^{-2i}\alpha)$ where $0\le i\le 6$ and $\alpha^3+\alpha+1=0$.

Continuing, we find

d	1	2	3	4	5	6	...	9
N_d	3	5	24	17	33	38	...	528

and more generally: $N_d=2^d+1$ if $3\nmid d$, and $N_d=2^d+1-a_d$ if $3|d$, where the a_i are found from $a_3=-15$, $a_6=27$, $a_{3k+6}+5a_{3k+3}+8a_{3k}=0$ $(k\ge 1)$.

Put $Z(C,t)=\exp(\sum\frac{1}{i}N_it^i)$. Then in this example

$$Z(C,t)=\frac{1+5t^3+8t^6}{(1-t)(1-2t)},$$

a simple rational function that encodes the values of all N_i.

A simpler example is the projective line L. Over $\mathbf{F}_q$ there are $N=q+1$ points. Now $Z(L,t)=\exp(\sum\frac{1}{i}(q^i+1)t^i)$. But $\sum\frac{1}{i}t^i=-\log(1-t)$ (for $|t|<1$), and $\sum\frac{1}{i}q^it^i=-\log(1-qt)$ (for $|qt|<1$), so $Z(L,t)=1/(1-t)(1-qt)$.

Comparing this with the previous we see that a zeta function $Z(C,t)=(1+5t^3+8t^6)/(1-t)(1-2t)$ corresponds to $N_i=q^i+1$ when $3\nmid i$. The recurrence $a_{3k+6}+5a_{3k+3}+8a_{3k}=0$ has solution $a_{3k}=c_1\alpha^k+c_2\beta^k$ if α,β are the two solutions of $x^2+5x+8=0$. From $a_0=6$, $a_3=-15$, we see $c_1=c_2=3$. Now $-3\sum\frac{1}{3i}\alpha^it^{3i}=\log(1-\alpha t^3)$ so $Z(C,t)=(1-\alpha t^3)(1-\beta t^3)/(1-t)(1-2t)=(1+5t^3+8t^6)/(1-t)(1-2t)$. In other words, the given expression for $Z(C,t)$ is equivalent to the given values of N_i.

2 Zeta function

Let X be an absolutely irreducible algebraic curve defined over $\mathbf{F}_q$ with N_i points over $\mathbf{F}_{q^i}$. The zeta function of X is defined as $Z(X,t):=\exp(\sum\frac{1}{i}N_it^i)$.

Hasse (for $g=1$) and Weil (for the general case) showed that this function is a rational function of the form $P(t)/(1-t)(1-qt)$ where $P(t)$ is a polynomial in t. The degree of $P(t)$ is $2g$, where g is the genus of X. The polynomial $P(t)$ has the factorization $P(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ where $|\alpha_i| = \sqrt{q}$ for all i.

Taking logarithms we find

$$N_i = 1 + q^i - \sum \alpha^i$$

(where α^{-1} runs through the $2g$ roots of $P(t)$). It follows that

$$|N_1 - (q + 1)| \leq 2g\sqrt{q}.$$

This Hasse-Weil bound was improved by Serre to

$$|N_1 - (q + 1)| \leq g[2\sqrt{q}].$$

(Proof: The α's are algebraic integers and occur in complex conjugate pairs; if a runs through the g sums $\alpha + \bar{\alpha}$, then for both choices of the sign the product $\prod([2\sqrt{q}] + 1 \pm a)$ is a positive integer, hence at least 1; by the arithmetic-geometric mean inequality we have $\sum([2\sqrt{q}] + 1 \pm a) \geq g$. □)

Ihara's bound is better for $g > (q - \sqrt{q})/2$:

$$N_1 \leq q + 1 - \frac{1}{2}g + \sqrt{2(q + \frac{1}{8})g^2 + (q^2 - q)g}.$$

(Proof: We have $1 + q - \sum \alpha = N_1 \leq N_2 = 1 + q^2 - \sum \alpha^2$. The α's occur in complex conjugate pairs with product q, and if a runs through the g sums $\alpha + \bar{\alpha}$ then $1 + q - \sum a \leq 1 + q^2 + 2qg - \sum a^2$. Now use $g \sum a^2 \geq (\sum a)^2$. □)

If $g = (q - \sqrt{q})/2$ then both Hasse-Weil and Ihara say $N_1 \leq q\sqrt{q} + 1$, and this upper bound is achieved (when q is a square) by the Hermitean curves $X^{r+1} + Y^{r+1} + Z^{r+1} = 0$ where $q = r^2$ (and by no other curves).