Math 203C (Number Theory), UCSD, spring 2015
More about zeta functions for function fields

Let K be a finite extension of $\mathbb{F}_q(t)$ for some prime power q in which $\mathbb{F}_q$ is integrally closed. Previously, we talked about the zeta function of K and of the associated curve C, and we stated Weil's theorem that

$$\zeta_C(z) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

where $P(T)$ is a polynomial of degree $2g$ (for g the genus of the curve, which is some nonnegative integer) with integer coefficients and complex roots all on the circle $|T| = q^{1/2}$ (i.e., $\mathrm{Re}(s) = 1/2$). Moreover, if I write $P(T) = P_0 + P_1 T + \cdots$, then $P_0 = 1$ and $P_{g+i} = q^i P_{g-i}$.

In case you want some concrete examples, take C to be a *hyperelliptic curve* by taking $K = \mathbb{F}_q(t)(\sqrt{Q(t)})$ where $Q(t)$ is a polynomial of degree d with no repeated roots. Then it can be shown that

$$g = \left\lfloor \frac{d}{2} - 1 \right\rfloor.$$

Or, take C to be a smooth curve in $\mathbb{P}^2$ defined by a homogeneous polynomial of degree d; then it can be shown that

$$g = \binom{d-1}{2}.$$

Let me now state some more facts about this zeta function. For each positive integer n, we have

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \alpha_1^n - \cdots - \alpha_{2g}^n;$$

in fact this can be deduced from the Riemann-Roch theorem, which implies that for $d \geq 2g-1$, the number of effective divisors of degree d on C is $(q^{d+1-g}-1)/(q-1)$. (In fact this is the usual way to prove the rationality of ζ_C.) In particular, for $n = 1$ we get the *Weil bounds*

$$q + 1 - 2g\sqrt{q} \leq \#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

For example, for $g = 1$ we get $\#C(\mathbb{F}_q) = (\sqrt{q}-1)^2 > 0$, so every genus 1 curve over $\mathbb{F}_q$ has a rational point. This becomes false if we either enlarge g or stop working over finite fields; however, we can still say that $\#C(\mathbb{F}_q) > 0$ if g is not so large compared to q.

In the other direction, the upper bound is nearly optimal when q is large compared to g; in fact, there are many pairs (q, g) for which it is achieved. However, when q is small compared to g it turns out to be suboptimal; more on this later.

Theorem 1 (Class number formula)**.** *The order of the class group of C is $P(1)$.*

Here the class group of C is not quite the same as the class group of $\mathfrak{o}_K$: it is the *Picard group* of degree 0 divisors (formal $\mathbb{Z}$-linear combinations of closed points) moduli principal divisors (the ones measuring zeroes and poles of a rational function). For instance, if C is an elliptic curve, this coincides with the group law on rational points.

Interesting consequence: for $\alpha_1, \ldots, \alpha_{2g}$ the roots of $P(T)$, the class number $h(C)$ satisfies

$$(\sqrt{q} - 1)^{2g} \leq h(C) \leq \left| \prod_{i=1}^{2g} (1 - \alpha_{2g}) \right| \leq (\sqrt{q} + 1)^{2g}.$$

For example, say we want to solve the class number one problem for curves; we can then immediately rule out all cases where $q > 4$. Starting from this observation, Leitzel–Madan–Queen solved the problem in the 1970s *except* that they missed a case which was only discovered in 2014! See `http://arxiv.org/pdf/1406.5365v5.pdf`.