

# PROJECT: NUMBER OF POINTS ON HYPERELLIPTIC CURVES

Richard Griffon

r.m.m.griffon@math.leidenuniv.nl

Let  $\mathbb{F}_q$  be a finite field of odd characteristic, and let  $C$  be a smooth projective curve defined over  $\mathbb{F}_q$ , of genus  $g_C$ . The zeta function of  $C$  is *a priori* defined as a formal power series in  $T$ :

$$Z(C/\mathbb{F}_q, T) = \exp \left( \sum_{n=1}^{\infty} |C(\mathbb{F}_{q^n})| \cdot \frac{T^n}{n} \right).$$

It is known that the zeta function is actually a rational function in the variable  $T$ , and that it has the following shape:

$$Z(C/\mathbb{F}_q, T) = \frac{L(C/\mathbb{F}_q, T)}{(1-T)(1-qT)},$$

where  $L(C/\mathbb{F}_q, T)$  is a polynomial with integral coefficients, of degree  $2g_C$ , and whose zeroes  $t \in \mathbb{C}$  have absolute value  $|t| = q^{-1/2}$ . One can then write  $L(C/\mathbb{F}_q, T)$  under the following form:

$$L(C/\mathbb{F}_q, T) = \prod_{j=1}^{2g_C} \left( 1 - \sqrt{q} \cdot e^{i\theta_{j,C}} \cdot T \right),$$

for some  $\theta_{j,C} \in [0, 2\pi[$ , which are called the Frobenius angles of  $C$ .

Recall that a projective curve is called hyperelliptic if it can be defined (affinely) by an equation

$$y^2 = f(x),$$

where  $f \in \mathbb{F}_q[x]$  is a square-free polynomial. The genus of  $C$  is then given by  $g_C = \left\lfloor \frac{\deg f - 1}{2} \right\rfloor$ .

The question is to study how the set of angles  $\{\theta_{j,C}\}_j$  change as we vary the curve  $C$  over a family of hyperelliptic curves of a given (large) genus  $g$ . In other words, if we draw a “random” curve  $C$  from the family of hyperelliptic curves over  $\mathbb{F}_q$ , what does the typical set of angles  $\{\theta_{j,C}\}_j$  look like?

In this setting, the problem was only recently solved (by Rudnick and Faifman). Their proof is based on an adaptation to the function field setting of techniques from analytic number theory. From this, one can deduce other “statistics” for hyperelliptic curves of large genus over  $\mathbb{F}_q$ : on average, how many rational points do they have? how big is the group of rational points on their Jacobians? etc.

---