PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 3-8

Alp Bassa

Rational point on curves over finite fields and Drinfeld modular varieties

Written by Dario Antolini

Let's consider C a smooth projective absolutely irreducible curve over a finite field $\mathbb{F}_q$ (shortly, a *curve*). As usual, one can associate to C a Zeta function together with a corresponding Riemann Hypothesis, which we know to be true thanks to the result of Hasse–Weil.

In particular, they gave us the so-called Hasse–Weil bound for the number of $\mathbb{F}_q$-rational points of C:

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

where $g(C)$ denotes the genus of the curve C. Here, we write down just the upper bound because, as the genus increases over a fixed finite field, the lower bound becomes useless.

A first improvement of this bound was given by Ihara ([6]). Starting from the inequality

$$\#C(\mathbb{F}_{q^2}) \geq \#C(\mathbb{F}_q),$$

together with the Weil conjectures, he showed that the upper bound (1) is not good as $g(C) \gg 0$.

Moreover, Ihara considered the following quantity:

$$A(q) := \limsup_{g(C)\to\infty} \frac{\#C(\mathbb{F}_q)}{g(C)}$$

where the lim sup is taken over all the curves C over the (fixed) field $\mathbb{F}_q$ when $g(C)$ tends to infinity. He showed that the number $A(q)$ always exists and depends only on the base field $\mathbb{F}_q$. Thus, from the Hasse–Weil bound (1), we have

$$A(q) \leq 2\sqrt{q}.$$

An important result on these side was given by Drinfeld and Vlăduţ ([3]) proving that

$$A(q) \leq \sqrt{q} - 1, \tag{2}$$

and this bound is the best known since 1983.

Conversely, the lower bound case was (historically) more difficult.

The first result is due to Serre ([7]) showing that the number $A(q)$ is always nonzero:

$$A(q) > 0,$$

while Ihara ([5]) specilized in the case $q = l^2$, with l prime power, obtaining:

$$A(q) \geq \sqrt{q} - 1. \tag{3}$$

So, by comparison with (2), we can conclude the equality:

$$A(l^2) = l - 1.$$

The last improvement on this side is given by Zink ([8]) when $q = p^3$ and it states the following inequality:

$$A(p^3) \geq \frac{2(p^2 - 1)}{p + 2}. \tag{4}$$

On proving his result (3), Ihara considered a sequence of Shimura curves over a same base field with increasing genus. Let's sketch the main ideas due to Ihara in the case of modular curves.

Let N be a positive integer. Denote by $X_0(N)$ the modular curve with $\Gamma_0(N)$-structure, where the affine locus (non-cuspidal points) parametrizes isomorphism classes of elliptic curves over $\mathbb{C}$ (also over $\overline{\mathbb{Q}}$) together with a cyclic N isogeny. It is a well-known result that $X_0(N)$ can be described over $\mathbb{Q}$, and, furthermore, after the work of Deligne–Rapoport ([2]), it has a (smooth projective irreducible) model in $\mathbb{Z}[1/N]$. Hence, for every prime number $p \nmid N$, we can reduce $X_0(N)$ mod p and obtain a (irreducible) curve $\widetilde{X_0}(N)$ over $\mathbb{F}_p$.

Moreover, this curve classifies the isomorphism classes of elliptic curves over $\overline{\mathbb{F}_p}$ + additional structure (and cusps). The interesting fact is that $\widetilde{X_0}(N)$ has many $\mathbb{F}_{p^2}$-points, whose non-cuspidal points correspond to the so-called supersingular elliptic curves.

Now, let's consider an increasing sequence of positive integers $\{N_i\}$, with $p \nmid N_i$ for all i and $N_i \to \infty$ as $i \to \infty$. Then, Ihara proved that

$$\lim_{i\to\infty} \frac{\#\widetilde{X_0}(N_i)(\mathbb{F}_{p^2})}{g(\widetilde{X_0}(N_i))} = p - 1$$

by using computations involving Shimura curves.

Now, let's point out the key points on the proof. In particular, why do we get just a result for $\mathbb{F}_{p^2}$-points and not other extensions of $\mathbb{F}_p$?

What Ihara was able to discover is the existence of $\mathbb{F}_{p^2}$-points in the modular curves $\widetilde{X_0}(N_i)$, in particular of supersingular elliptic curves. It is well-known that their j-invariant lie inside $\mathbb{F}_{p^2}$, and one obtains exactly this degree-2 extension because the modular curve parametrizes (isomorphism classes of) elliptic curves over $\mathbb{C}$ as well as $\mathbb{Z}$-lattices of rank 2 inside $\mathbb{C}$ (up to homothety).

So, in order to generalize this bound for $q = l^n$ with l prime integer and $n > 2$, one has to look at lattices of rank n, but inside another algebraically closed field, since the field complex numbers offer us just rank-2 lattices. (We cannot consider rank-1 lattices because their moduli space will be 0-dimensional.) First, replace the integers $\mathbb{Z}$ inside its fraction field $\mathbb{Q}$ by the ring $A := \mathbb{F}_q[T]$ inside the field $F := \mathbb{F}_q(T)$; hence, consider its completion F_∞ at the ∞ place and its algebraic

closure $\overline{F_\infty}$. Since this extension is of infinite degree, the latter is no more complete, meanwhile its completion C_∞ is still algebraically closed.

In this equal-characteristic setting, we need an analogue of the elliptic curve: it is called Drinfeld module, and it can be shown ([4, Theorem 4.6.9]) that the moduli space of (isomorphism classes of) Drinfeld modules with rank n is equivalent to the moduli spaces of A-lattices of rank n inside C_∞ (up to homothety), as far as for elliptic curve (with $n = 2$).

In a similar way, one can define a level structure on Drinfeld modules: it turns out that the moduli space of rank-n Drinfeld modules together with (nontrivial) level structure can be represented by an $(n-1)$-dimensional affine scheme $\mathcal{M}$ over A. Then, as in the elliptic curve case, we want to reduce this scheme modulo a prime element of A. In this case, we look for an ideal "not intersecting the level structure" (in some sense, like $V(p)$ does not intersect $V(N)$ for $p \nmid N$ inside Spec $\mathbb{Z}$), and this is generated by a polynomial $P(T) \in A = \mathbb{F}_q[T]$, since the ring A is a PID. The reduction modulo this ideal gives us a representable moduli space $\widetilde{\mathcal{M}}$ of dimension $n-1$ with many $\mathbb{F}_{p^n}$-rational points over a degree-n extension of $\mathbb{F}_q[T]/(P(T))$. Finally, there is a similar notion of supersingular Drinfeld modules and they are defined over this extension of degree n.

Let's come back to Ihara's trick. Consider a family of moduli spaces of rank-n Drinfeld modules $\{\mathcal{M}_i\}_i$ with nontrivial level structure and a polynomial $P(T)$ not intersecting any of these level structures. So, it makes sense to consider the family $\{\widetilde{\mathcal{M}_i} := \mathcal{M}_i \mod P\}$ given by reduction modulo the (ideal generetad by) $P(T)$. Starting with the scheme $\widetilde{\mathcal{M}_1}$, look at a supersingular point inside it and a *suitable* curve passing through this special point, where suitable means that it is (and can be) chosen so that it contains many supersingular points. Then, pull back this curve to the schemes $\widetilde{\mathcal{M}_i}$ and get other nice curves, so that one has a family of 1-dimensional sub-locus containing supersingular points.

Beside this theory, in [1] Bassa, Beelen, Garcia and Stichtenoth write down explicit recursive equations for these nice curves. In this way, they get a lower bound for $A(q)$ when $q = p^{2m+1}$ is an odd power of a prime number p (and $m \geq 1$). They indeed find a sort of harmonic average between two successive Drinfeld–Vlăduţ upper bounds (2):

$$A(p^{2m+1}) \geq \frac{2}{\frac{1}{p^m-1} + \frac{1}{p^{m+1}-1}}. \tag{5}$$

In particular, This lower bound can recover Zink's inequality (4) just setting $m = 1$ (so that $q = p^3$).

Last, we want to mention some applications of this result. After the historical Hasse–Weil bound, the problem of finding curves with many rational points becomes again important (ACTUAL) after the formulation of codes theory and the Goppa's construction of good codes, as long as other applications to cryptography.

In a theoretical side, this result can be used on the study of automorphisms and level structures of those curves, and also on their covering (in this case, not Galois).

References

[1] A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth, *Towers of function fields over non-prime finite fields*. Mosc. Math. J. 15 (2015), no. 1, 1–29, 181.

[2] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*. In: *Modular functions of one variable II*. Springer, Berlin, Heidelberg, 1973. p. 143-316.

[3] V.G. Drinfeld and S.G. Vlăduţ, *The number of points of an algebraic curve*. Funktsional Anal. i Prilozhen 17, 68-69, 1983.

[4] D. Goss, *Basic structures of function field arithmetic*. Springer Science & Business Media, 2012.

[5] Y. Ihara, *Congruence relations and Shimura curves*. Automorphic forms, representations and L-functions, Sympos. Pure Math., Oregon State Univ. 1977, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 291-311 (1979).

[6] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*. J. Fac. Sci. Tokyo 28, 721-724, 2000.

[7] J.-P. Serre, *Sur le nombre des points rationnels dâĂŹune courbe algebrique sur un corps fini*. C.R. Acad. Sc. Paris 296, 397-402, 1983.

[8] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*. Fundamentals of Computation Theory (ed. L.Budach), Lecture Notes Comp. Sc. LNCS 199, 503-511 (1985).

Dario Antolini
Department of Mathematics
Università degli Studi di Roma "Tor Vergata"
Via della Ricerca Scientifica, 1
00133 – Roma (Italy).
email: antolini@mat.uniroma2.it - dario.ant27@gmail.com