Serre Problem: $g = 1$.
Lecture 6.

Elisa Lorenzo García

14th March 2016

Contents

In lectures'today, we follow Gouvêa's notes [1] on the famous course taught by J.-P. Serre at Harvard University during Fall 1985. We will introduce what we call Serre's Problem that is the main object of study of this course.

1 Serre's Problem

Let C be a smooth, irreducible, projective curve of genus g defined over a finite field $\mathbb{F}_q$. The Hasse-Weil bound, that is a consequence of the Riemann Hypothesis over finite field proved by Weil and studied in lecture 2, states that

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

For a given pair (q, g), we define $\mathrm{N}_q(g) = \underset{C}{\mathrm{Sup}} \#C(\mathbb{F}_q)$. Weil's equality implies

$$\mathrm{N}_q(g) \leq q + 1 + 2g\sqrt{q}.$$

We have already seen an improvement, due to Serre, of this bound when q is not a square in lecture 2. Namely, $\mathrm{N}_q(g) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor$. We recover the notation from that result. The number of point of a curve can be computed by $\#C(\mathbb{F}_q) = q + 1 - t$ where $t = \mathrm{Tr}(\pi)$ is the trace of the Frobenius endomorphism π. We denote the roots of the characteristic polynomial of the Frobenius endomorphism by π_i. This polynomial is the numerator of the Zeta Function of the curve, it has integer coefficients and degree equal to $2g$. Moreover, its roots are conjugate numbers with norm equal to $q^{1/2}$, so they are what we called Weil-numbers in lecture 5. We call $a_i = \pi_i + \overline{\pi}_i$ for $i = 1,..,g$, we put $m = \lfloor 2\sqrt{q} \rfloor$ and we write $x_i = m + 1 + a_i$.

MOTIVATION: CODING THEORY, CRYPTO, PROBLEM STUDIED BY MANY PEOPLE

1.1 Defect 1 and 2

Theorem 1.1. *With previous notation, we have*
i) if $Tr(\pi) = gm$, *then* $a_1 = ... = a_g = m$,
ii) if $Tr(\pi) = -gm$, *then* $a_1 = ... = a_g = -m$.

Proof. It is an easy consequence of Lemma 2.1 in lecture's notes 2. □

Theorem 1.2. *Let* A *be an abelian variety of dimension* g *over* $\mathbb{F}_q$, *and* π *its Frobenius endomorphism.*
i) If $Tr(\pi) = gm - 1$ *("down by 1"), then*

$$(a_1, ..., a_g) = \begin{cases} (\underbrace{m, ..., m}_{g-1}, m-1) \\ (\underbrace{m, ..., m}_{g-2}, m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}) \ \textit{if } g \geq 2 \end{cases}$$

ii) If $Tr(\pi) = gm - 2$ *("down by 2"), then one of the seven following cases occurs:*

$$(a_1, ..., a_g) = \begin{cases} (m, ..., m, m-2) \\ (m, ..., m, m-1, m-1) \ \textit{if } g \geq 2 \\ (m, ..., m, m+\sqrt{2}-1, m-\sqrt{2}-1) \ \textit{if } g \geq 2 \\ (m, ..., m, m+\sqrt{3}-1, m-\sqrt{3}-1) \ \textit{if } g \geq 2 \\ (m, ..., m, m-1, m+\frac{-1+\sqrt{5}}{2}, m+\frac{-1-\sqrt{5}}{2}) \ \textit{if } g \geq 3 \\ (m, ..., m, m+\frac{-1+\sqrt{5}}{2}, m+\frac{-1-\sqrt{5}}{2}, m+\frac{-1+\sqrt{5}}{2}, m+\frac{-1-\sqrt{5}}{2}) \ \textit{if } g \geq 4 \\ (m, ..., m, m+1-4cos^2(\frac{\pi}{7}), m+1-4cos^2(\frac{2\pi}{7}), m+1-4cos^2(\frac{3\pi}{7})) \ \textit{if } g \geq 3 \end{cases}$$

Proof. We assume Siegel's Theorem stated in these notes as Theorem 1.3. Then, for all $k \geq 0$ a positive integer, the number of totally positive integers α with $\mathrm{Tr}(\alpha) = d(\alpha) + k$ is finite for each k, and these α's can be explicitly computed. By Siegel, $d + k > 3/2d$, so $d < 2k$. These α's are the possibilities for $m + 1 - a_i$ ($\mathrm{Tr}(\alpha_i) = \sum \alpha_i = gm - k$, then $\sum(m + 1 - \alpha_i) = k + g$). The number α satisfies $x^d - (d + k)x^{d-1} + ... = 0$. Since all its conjugates are also positive, we get bounds for the other coefficients, and then there is a finite number of possibilities.

For $k = 0$, we get $\alpha = 1$. For $k = 1$, we get $\alpha = \frac{3\pm\sqrt{5}}{2}$ or $d = 1$, so $\alpha = 2$. Case, $k = 2$, so defect 2 case is left as an exercise. □

Theorem 1.3 (Siegel). *Let $\alpha \neq 1, \frac{3\pm\sqrt{5}}{2}$ be an algebraic integer that is totally positive (it and all its conjugates are positive real numbers) and of degree d. Then $Tr(\alpha) > \frac{3}{2}d$.*

For curious reader, the proof can be found in the main reference [1].

Remark 1.4. *The second defect 1 case is possible only if $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$, since $m + \frac{-1+\sqrt{5}}{2} \leq 2\sqrt{q}$.*

Remark 1.5. *All the possibilities listed in Theorem 1.2 occur for abelian varieties, but there are not necessarily jacobians of curves. The schotky problem is the problem of deciding which abelian varieties are jacobians. For dimension 2 and 3, it is proved, that all principal polarized abelian variety with an "indecomposable" polarization are jacobians of curves.*

1.2 Other results

Theorem 1.6. *Suppose $\{1,...,g\}$ can be partitioned in two non-empty subsets I and J such that:*

a) The a_i $(i \in I)$ are stable by $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Idem for J.

b) All the $a_i - a_j$ for $i \in I$ and $j \in J$ are units.

Then the given abelian variety is not a Jacobian.

Proof. Maybe, it is better to skip it .... but I would like to start to talk about decomposable polarizations .... □

Theorem 1.7 (Beauville). *If $q = p^e$ is either of the form $x^2 + 1$ $(x \in \mathbb{Z})$ or $x^2 + x + 1$ $(x \in \mathbb{Z})$, then, if C is a curve of genus $g \geq 2$ over $\mathbb{F}_q$, $\#C(\mathbb{F}_q) \neq q + 1 \pm gm$, where $m = \lfloor 2q^{1/2} \rfloor = 2x$ or $2x + 1$, respectively.*

Proof. Consider the case $q = x^2 + 1$, so $m = 2x$, and assume that $\#C(\mathbb{F}_q) = q + 1 - gm$. Then we can arrange the eigenvalues π_i of the Frobenius endomorphism π as

$$\begin{cases} \pi_1 + \overline{\pi}_1 = m \text{ and } \pi_1\overline{\pi}_1 = q \\ \dots \\ \pi_g + \overline{\pi}_g = m \text{ and } \pi_g\overline{\pi}_g = q \end{cases}$$

So, $\pi_1 = ..., \pi_g$ and $\overline{\pi}_1 = ... = \overline{\pi}_g$. And necessarily $\pi_1 = x + i$ and $\overline{\pi}_1 = x - i$. Put $\sigma = \pi - x \in \text{End}(\text{Jac}(C))$, then $\sigma^2 = -1$. We know that the action of the Frobenius is trivial in the tangent space at the identity in the Jacobian, then the action of σ is the action of $-x$, but $x^2 \neq -1$, so we get a contradiction. □

2 Case $g = 1$

For the elliptic curve case, the characteristic polynomial of the Frobenius endomorphism has degree 2, let call π and $\overline{\pi}$ to the two roots. The trace of the Frobenius is $a = \pi + \overline{\pi}$, so that $\#E(\mathbb{F}_q) = q + 1 - a$. The question is, given q, which a's occurs for elliptic curves over $\mathbb{F}_q$?

Theorem 2.1. *Let $a \in \mathbb{Z}$ such that $| a | \leq 2q^{1/2}$.*

i) If a is prime to p, then there exists an elliptic curve over $\mathbb{F}_q$ with that value of a. (Ordinary case)

ii) If $p \mid a$, then there exists such an elliptic curve if and only if either: e is even and $a = \pm 2p^{e/2}$; e is even, $p \not\equiv 1 \bmod 3$ and $a = \pm p^{e/2}$; e even, $p \not\equiv 1 \bmod 4$ and $a = 0$; e is odd, $p = 2$, or 3 and $a = 0, \pm p^{\frac{e+1}{2}}$. (Supersingular case)

Proof. i) We construct the elliptic curve over the complex numbers, characteristic zero, and then we reduce. We will see how to do this in next lecture.

ii) should we skip it? □

Theorem 2.2. *We have $N_q(1) = q + 1 + m$, except when $q = p^e$, $e \geq 5$ is odd and $m \equiv 0 \bmod p$, in which case $N_q(1) = q + m$.*

Proof. If q is not exceptional, this is a consequence of Theorem 2.1. Otherwise, just notice that if $p \mid m$, then $p \nmid m - 1$. □

The smallest exceptional case is for $q = 128 = 2^7$.

The exceptional values of $q = p^{2e'+1}$ are those for which the $2 < e'$th decimal digit in the p-adic expansion of $2\sqrt{q}$ is a zero. Let us see this in an example: $2\sqrt{2} = 10.110101000001...$, so 2^7, 2^{11}, 2^{15}, 2^{17}, .. are exceptional and there infinitely many exceptional powers of 2. For $p = 3$, $2\sqrt{3} = 3.110112022...$, so 3^7 is also exceptional.

3 Exercises

Exercise 3.1. *Prove Theorem 1.2 for defect 2.*

Exercise 3.2. *Find the equivalent formula in remark 1.4 for the defect 2 cases.*

Exercise 3.3. *Check that the smallest exceptional case after Theorem 2.2 is $q = 128$.*

Exercise 3.4. *Prove that the construction of exceptional numbers using p-adic expansion after Theorem 2.2 works. Compute the first exceptional 7-power.*

Exercise 3.5. *Provide maximal elliptic curves over $\mathbb{F}_q$ for $q = 2, 3, 4, 5$ and 7.*

References

[1] F.Q. Gouvêa, *Rational Points on Curves over Finite Fields*, Lecture notes given at Havard University by J.-P. Serre in Fall 1985.