Serre Problem: $g = 2$.
Lecture 6.

Elisa Lorenzo García

18th April 2016

Contents

In lectures'today, we keep following Gouvêa's notes [1] on the famous course taught by J.-P. Serre at Harvard University during Fall 1985. During the last lecture we show the main Theorem for $g = 1$.

Theorem 0.1. *We have $N_q(1) = q+1+m$, except when $q = p^e$, $e \geq 5$ is odd and $m \equiv 0$ mod p, in which case $N_q(1) = q + m$.*

1 Serre Problem $g = 2$

We will prove this Theorem today.

Theorem 1.1. *Set $m = \lfloor 2\sqrt{q} \rfloor$.*
If q is a square, then

- *If $q \neq 4, 9$, then $N_q(2) = q + 1 + 2m$*
- *If $q = 4$, then $N_q(2) = 10$ (down by 3)*
- *If $q = 9$, then $N_q(2) = 20$ (down by 2)*

If q is not a square, we define q to be special if either $p \mid m$ or q is represented by one of the quadratic polynomials $x^2 + 1$, $x^2 + x + 1$ or $x^2 + x + 2$.

- *If q is not special,* $N_q(2) = q + 1 + 2m$
- *If q is special,* $N_q(2) = \begin{cases} q + 2m \text{ if } \{2\sqrt{q}\} > \frac{\sqrt{5}-1}{2} \text{ down by } 1 \\ q + 2m - 1 \text{if not.} \end{cases}$

We will see that if Theorem 0.1 were constructive, then the proof of Theorem 1.1 would also be.

Corollary 1.2. $| Weyl - N_q(2) | \leq 3$

Conjecture 1.3. *For $g = 3, 4, 5$ and not others,* $| Weyl - N_q(g) | \leq c(g)$.

Remark 1.4. *For $g = 1, 2$, all the curves are hyperelliptic, so given a curve C, there exists a quadratic twist C' such that $N(C) + N(C') = 2(q + 1)$, that is, they have opposite traces.*

The idea to prove theorem 1.1 is finding a curve whose jacobian is the product of two elliptic curves. All abelian surfaces together with a principal polarization are jacobians (Schotcky Problem).

Example 1.5 (Jacobi, Legendre)**.** *Let us consider the genus 2 curve $C : y^2 = x(x-1)(x-\alpha)(x-\beta)(x-\alpha\beta)$ and the elliptic curves $E_\pm : y^2 = (x \pm 2\sqrt{\alpha\beta})(x - (\alpha + \beta))(x - (1 + \alpha\beta))$. Then, the jacobian of C is isogenous to $E \times E'$.*

To prove it, we just need to consider the maps $C \to E_\pm$ given by $(x, y) \to (x + \frac{\alpha\beta}{x}, y\frac{x \pm \sqrt{\alpha\beta}}{x^2})$ and check that the pullback of the regular differentials $\omega_{E_\pm}$ are linearly independent.

2 Glueing elliptic curves

We will see now Legendre's idea to "glue" two elliptic curves. An elliptic curve E_i is determined by the $2:1$-map to $\mathbb{P}^1$ given by the hyperelliptic involution ι, $E_i \to E/ < \iota > \mathbb{P}^1$, or equivalently by the ramification points Q_i, P_1, P_2, P_3 of such morphism. If we look at the function fields (draw the field extension diagram!!), we get that $K_i = \bar{k}(C_i)$ are quadratic extension of $K = \bar{k}(x) = \bar{k}(\mathbb{P}^1)$. The biquadratic extension $K_{12} = K_1K_2$ has another quadratic subextension K_0 corresponding to a curve C_0 together with a map to $\mathbb{P}^1$ only ramified at Q_1, Q_2. Hence, Riemann-Hurwitz implies that $g(C_0) = 0$, and the the curve C corresponding with the function field K_{12} has genus 2 and jacobian isogeny to $E_1 \times E_2$. In order to get the curve C defined over $\mathbb{F}_q$ and also the isogeny to $E_1 \times E_2$, we need that the points Q_i are $\mathbb{F}_q$-rationals.

Definition 2.1. *We say that two elliptic curves $E_i/\mathbb{F}_q$ can be glued, if there exists a genus 2 curve $X/\mathbb{F}_q$ such that $Jac(X) \sim_{\mathbb{F}_q} E_1 \times E_2$.*

Now, given two elliptic curves E_i, in order to glue them along the 2-torsion $E_i[2]$, we need that the Galois action of the Frobenious endomorphism on the two torsion is the same one. The 2-torsion of an elliptic curve $y^2 = f(x)$ is given by $(x_i, 0)$ where x_i is a root of $f(x) = 0$.

Theorem 2.2. *We can glue E_1 and E_2 if the Frobenious action on $E_i[2]$ is the same one, except maybe if:*

- *$ord(Frob) = 1$, $p = 3$ and $j(E_i) = 0$,*
- *$ord(Frob) = 2$, any p, and $j(E_i) = 1728$,*
- *$ord(Frob) = 3$, any p, and $j(E_i) = 0$.*

So, if $Aut(E_i) = \{\pm 1\}$, we can always glue them.

We skip the proof that can be found in [1], but the idea is to find a morphism $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ that sends $\{P_1, P_2, P_3\}$ to $\{P_1', P_2', P_3'\}$ but $\phi(\infty) \neq \infty'$.

Example 2.3. *Let us take $q = 9$ and E a supersingular elliptic curve with $\pi = 3$ ($Tr(3) = 6$). Then $E(\mathbb{F}_q) = 1 + 9 - 6 = 4$ and we cannot glue E with itself because we will get a curve with $q + 1 - 6 - 6 = -2$ points!*

Example 2.4. *If $q = 4$, Weyl bound is equal to 13, but a covering argument: $C \to \mathbb{P}^1$ shows that all hyperelliptic curves has at most $2(q+1)$ points. In this case $2(q+1) = 10$. For $q = 9$, Weyl bound equals 22, but $2(q+1) = 20$.*

We know state without proof (see the appendix in [3] if you have curiosity) that a polarization in an abelian variety $E^g = E \times ... \times E$ is given by a positive definite g times g matrix with entries in $\mathrm{End}(E)$.

Example 2.5. *If $End(E) \simeq \mathbb{Z}$, then a polarization $\phi : E^g \to (E^*)^g \simeq E^g$ is given by a matrix*

$$\phi = \begin{pmatrix} a_{11} & \dots & a_{1g} \\ \dots & & \dots \\ a_{g1} & \dots & a_{gg} \end{pmatrix},$$

that is positive definite, namely, $v^t \phi v \geq 0$ for all $v \in \mathbb{Z}^g$.

Example 2.6. *Let $E/\mathbb{F}_q$ be an elliptic curve with $Frob = -q^{1/2}$ ($q = p^e$ with $e \geq 2$). Then, in order to find a genus 2 curve whose jacobian is isogenous to $E \times E$, we just need to find a principal polarization, that is, a 2 by 2 matrix*

$$\begin{pmatrix} p & \alpha \\ \bar{\alpha} & p \end{pmatrix},$$

such that $p^2 - \alpha\bar{\alpha} = p$.

Theorem 2.7. *If $q = p^{2e}$ is a square but $q \neq 4, 9$, the Weyl bound is attained. Otherwise we get down by 3 and 2 respectively.*

Proof. If $p \neq 2, 3$, we take a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ (Frob $= p$) and we glue two copies by Theorem 2.2.

If $q = 4, 9$, we use example 2.4.

If $q = 2^{2e}$ with $e > 1$, we start with the supersingular elliptic curve over $\mathbb{F}_2$: $E : y^2 + y = x^3$ and we glue it to $y'^2 + y' = (x + c)^3$ for a right c. We can check that the function field composition $\mathbb{F}_q(x, y, y')$ corresponds to a genus 2 curves with the wanted number of points.

If $q = 9^e$ for some $e > 1$, we use lemma 2.6. See more details in the main reference [1]. □

Theorem 2.8. *If q is not a square and it is not special, the Weyl bound is attained.*

Proof. Use glueing of elliptic curves, Theorem 2.2, and Theorem 0.1. The special condition is made in order to avoid the exception in Theorem 2.2: for example, we want to avoid $m^2 - 4q = -4$ ($\implies j = 0$), but then $q = 1 = x^2$. □

Theorem 2.9. *If q is not a square and it is special, we get the results in Theorem 1.1.*

We will not show the detailed proof because there are so many computations. But basically, follows by discarding cases with Theorem 1.2 in Lectures Notes CFF6 and the glueing Theorem 2.2. You can find the details in [1]. The extra problem here is that we have to give a principal and indecomposable polarization to the product of elliptic curves.

3 Hermitian forms

Example 3.1. *Let us consider the elliptic curve E with complex multiplciation by $R = \mathbb{Z}(\sqrt{-2})$. Let us consider the polarization*

$$\phi = \begin{pmatrix} 2 & 1+\sqrt{-2} \\ 1-\sqrt{-2} & 2 \end{pmatrix}.$$

It is a principal polarization since it has determinant one and it is indecomposable since all the integers that represents are even. Moreover, the finite order 2 by 2 matrices that commute with ϕ form a group isomorphic to a double cover of S_4. There exists a single genus 2 curve $C : y^2 = x^5 - x$ up to isomorphism with such automorphism group. Then, $Jac(C) = E^2$.

In [2], it is proved that except for discriminants $-3, -4, -7$, we always can find indecomposable principal polarizations.

Lemma 3.2. *If a principal polarization in $E \times E$ is given by a matrix*

$$\phi = \begin{pmatrix} 2 & \alpha \\ \bar{\alpha} & \mu \end{pmatrix},$$

then, it is indecomposable.

We will skip the proof of this lemma, but as a first approach you can see previous example.

Now, if the discriminant $-d$ is such that $d \equiv 0 \bmod 8$, we can take $\alpha = 1 + \sqrt{-d/4}$. The cases $d \equiv 3, 4 \bmod 8$ are left as an exercise. If the discriminant is $d \equiv 7 \bmod 8$, we should use class field theory to get such an α, the curious reader can check the main reference [1].

4 Exercises

Exercise 4.1. *Prove that the* 2*-torsion of an elliptic curve* $y^2 = f(x)$ *is given by* $(x_i, 0)$ *where* x_i *is a root of* $f(x) = 0$.

Exercise 4.2. *Find maximal genus* 2 *curves for* $q = 4$ *and* $q = 9$.

Exercise 4.3. *Give the details in the proof of Theorem 2.7 for the case* $q = 2^{2e}$.

Exercise 4.4. *Find an* α *that gives a idecomposable polarization when* $d \equiv 3, 4$ *mod* 8 *using lemma 3.2.*

Exercise 4.5. *Explain why there are not genus* 2 *curves attaining Weyl bound for special values of* q.

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.

[2] Hayashida, Nishi Existence of curves of genus two on a product of two elliptic curves, Volume 17, Number 1 (1965), 1-16, J. Math. Soc. Japan.

[3] K. Lauter, The maximum or minimum number of rational points on genus three curves over finite fields with an Appendix by J.-P. Serre, Compositio Math. 134 (2002) 87-111.