Jacobians in isogeny classes of abelian surfaces over finite fields

Enric Nart

Sevilla, December 15th of 2006

Joint work with:

Everett Howe, Daniel Maisner and Christophe Ritzenthaler

Algebraic curves of genus 2 over a finite field $\mathbb{F}_q$

$$C: \ y^2 = 2x^6 + 3x^5 - 7, \qquad C: \ y^2 + y = x^3 + x^{-1}$$

We are interested in the numerical data $N_n := |C(\mathbb{F}_{q^n})|$. This information is captured by the *Zeta function* of $C/\mathbb{F}_q$:

$$Z(C/\mathbb{F}_q, x) = exp\left(\sum_{n\geq 1} \frac{N_n}{n} x^n\right) = \frac{1 + ax + bx^2 + qax^3 + q^2x^4}{(1-x)(1-qx)}$$

for some a, $b \in \mathbb{Z}$.

The whole family N_n is determined by N_1 and N_2.

Fix $k = \mathbb{F}_q$ a finite field of characteristic p.

Question. What polynomials occur as the numerator of the zeta function of a projective smooth curve of genus 2 defined over $\mathbb{F}_q$?

Question. For what values of (N_1, N_2) there exists a projective smooth curve C of genus 2 defined over $\mathbb{F}_q$ such that $|C(\mathbb{F}_q)| = N_1$, $|C(\mathbb{F}_{q^2})| = N_2$?

For elliptic curves this question was answered by W.C. Waterhouse in his 1969 thesis.

For curves of genus 2 this question was raised by H.G. Rück in his 1990 thesis.

Jacobians enter into the game

We attach to C a more feasible object: its Jacobian J_C, which is an abelian surface defined over k.

The richer algebraic structure of abelian varieties allows a deeper understanding of these objects.

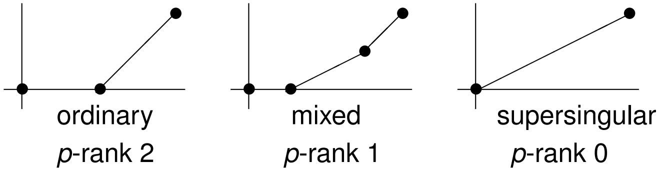
An important invariant of an abelian surface A over a finite field is the *Weil polynomial*, which is the characteristic polynomial of the Frobenius endomorphism

$$f_A(x) = x^4 + ax^3 + bx^2 + qax + q^2 \in \mathbb{Z}[x]$$

If A is the Jacobian of a curve C then the integers a, b are the same integers that appeared in the numerator of the zeta function of C.

J. Tate and T. Honda in the sixties:

1. $f_A(x) = f_B(x)$ iff A and B are k-isogenous
2. The p-Newton polygon of $f_A(x)$ has three possibilities according to $\dim_{\mathbb{F}_p} A[p] = 2, 1, 0$



3. We know all polynomials that occur as $f_A(x)$ for some abelian surface A/k

Our problem is, then, to identify the family of all Weil polynomials of Jacobians inside the well-known family of all Weil polynomials of abelian surfaces

$$\{f_{J_C}(x) \mid C/k \text{ curve of genus } 2\} \subseteq \{f_A(x) \mid A \text{ abelian surface}/k\}$$

Question. What isogeny classes of abelian surfaces$/k$ do contain a Jacobian?

Oort and Ueno proved in 1973 that all isogeny classes of abelian surfaces contain Jacobians if $k = \overline{k}$.

Thus, there is no geometric obstruction to our problem.

p-rank	Condition on p and q	Conditions on s and t
—	—	$\lvert s-t\rvert = 1$
2	—	$s = t$ and $t^2 - 4q \in \{-3, -4, -7\}$
2	$q = 2$	$\lvert s\rvert = \lvert t\rvert = 1$ and $s \neq t$
1	q square	$s^2 = 4q$ and $s - t$ squarefree
0	$p > 3$	$s^2 \neq t^2$
0	$p = 3$ and q nonsquare	$s^2 = t^2 = 3q$
0	$p = 3$ and q square	$s - t$ is not divisible by $3\sqrt{q}$
0	$p = 2$	$s^2 - t^2$ is not divisible by $2q$
0	$q = 2$ or $q = 3$	$s = t$
0	$q = 4$ or $q = 9$	$s^2 = t^2 = 4q$

Table: Conditions that ensure that the split isogeny class with Weil polynomial $(x^2 - sx + q)(x^2 - tx + q)$ does not contain a Jacobian. Here we assume that $\lvert s\rvert \geq \lvert t\rvert$.

p-rank	Condition on p and q	Conditions on a and b
—	—	$a^2 - b = q$ and $b < 0$ and all prime divisors of b are 1 mod 3
2	—	$a = 0$ and $b = 1 - 2q$
2	$p > 2$	$a = 0$ and $b = 2 - 2q$
0	$p \equiv 11 \bmod 12$ and q square	$a = 0$ and $b = -q$
0	$p = 3$ and q square	$a = 0$ and $b = -q$
0	$p = 2$ and q nonsquare	$a = 0$ and $b = -q$
0	$q = 2$ or $q = 3$	$a = 0$ and $b = -2q$

Table: Conditions that ensure that the simple isogeny class with Weil polynomial $x^4 + ax^3 + bx^2 + aqx + q^2$ does not contain a Jacobian.

Jacobians are determined by principal polarizations

Theorem (Weil 1957). An abelian surface $A/\mathbb{F}_q$ is not $\mathbb{F}_q$-isomorphic to the Jacobian of a smooth projective curve$/\mathbb{F}_q$ iff for all principal polarizations λ of A defined over $\mathbb{F}_q$

$$(A, \lambda) \simeq_{\mathbb{F}_{q^2}} (E \times E', \lambda_{\text{split}})$$

as polarized surfaces.

Corollary. If $A/\mathbb{F}_q$ is simple over $\mathbb{F}_{q^2}$ then it is $\mathbb{F}_q$-isomorphic to a Jacobian iff it admits a principal polarization$/\mathbb{F}_q$.

Question. What isogeny classes of abelian surfaces$/k$ do contain a surface admitting a principal polarization$/k$?

We say that such isogeny class is *principally polarizable*

This (weaker) question was studied by E. Howe in a series of papers (1995,1996, 2001), where he expressed the obstruction to the existence of principal polarizations in an isogeny class $\mathcal{A}$ of abelian varieties in terms of the vanishing of an element $I_{\mathcal{A}}$ of a group $\mathcal{B}_{\mathcal{A}}$ constructed from the Grothendieck group of the category of finite group schemes that are kernels of isogenies between two abelian varieties in $\mathcal{A}$.

Using class field theory the obstruction group $\mathcal{B}_{\mathcal{A}}$ and the obstruction element $I_{\mathcal{A}}$ could be described in terms of purely arithmetic data.

Theorem (HMNR 2006). Let $\mathcal{A}$ be an isogeny class of abelian surfaces$/\mathbb{F}_q$ with Weil polynomial $x^4 + a\,x^3 + b\,x^2 + aq\,x + q^2$. Then, $\mathcal{A}$ is not principally polarizable iff $a^2 - b = q$, $b < 0$ and all prime divisors of b are congruent to 1 mod 3.

Jacobians in isogeny classes: sketch of the methods

$\mathcal{A}$ **simple over** $\mathbb{F}_{q^2}$**.** Howe's obstruction group and element for $\mathcal{A}$ to be principally polarizable. H95 + MN02 + HMNR06

$\mathcal{A}$ **split over** $\mathbb{F}_q$**.** Kani's construction of split Jacobians by tying two elliptic curves together along their n-torsion groups. HNR06

$\mathcal{A}$ **ordinary, simple over** $\mathbb{F}_q$**, split over** $\mathbb{F}_{q^2}$**.** Counting non Jacobians and p. p. Deligne modules. Comparison of the two numbers by Brauer relations in biquadratic fields. H04 + M04

$\mathcal{A}$ **supersingular, simple over** $\mathbb{F}_q$**, split over** $\mathbb{F}_{q^2}$**.** Mass formulas for quaternion hermitian forms and descent theory. HNR06

$\mathcal{A}$ **supersingular,** $p = 2, 3$**.** Computation of the zeta function of a curve in terms of the defining equation. MN05 + H06

$\mathcal{A}$ split over k: Kani's construction

E, E' elliptic curves$/k$, n positive integer

$\psi\colon E[n] \xrightarrow{\sim} E'[n]$ isomorphism of group schemes that is an anti-isometry with respect to the Weil pairings.

The natural isogeny $E \times E' \longrightarrow (E \times E')/\operatorname{Graph}(\psi) =: A$ induces a principal polarization λ on A because $\operatorname{Graph}(\psi)$ is a maximal isotropic subgroup of $(E \times E')[n]$.

Kani finds necessary and sufficient conditions on E, E', n, ψ for (A, λ) to be a Jacobian. For instance, for n prime:

Theorem (Kani 1997). (A, λ) is not a Jacobian iff there is an integer $o < i < n$ and a geometric isogeny $\varphi\colon E \longrightarrow E'$ of degree $i(n-i)$ such that $i\psi = \varphi_{|E[n]}$.

$\mathcal{A}$ ordinary, simple over $\mathbb{F}_q$, split over $\mathbb{F}_{q^2}$

$f_{\mathcal{A}}(x) = x^4 + ax^2 + q^2$, $|a| < 2q$, $p \nmid a$, $2q - a$ nonsquare in $\mathbb{Z}$

If $f_{\mathcal{A}}(\pi) = 0$, the number field $K = \mathbb{Q}(\pi)$ is biquadratic with intermediate quadratic subfields:

$$L = \mathbb{Q}(a^2 - 4q^2), \qquad K^+ = \mathbb{Q}(2q - a), \qquad L' = \mathbb{Q}(-2q - a)$$

$$\mathcal{A}_{\mathrm{PP}} := \{(A, \lambda) \mid A \in \mathcal{A}\}_{/k-}\text{isomorphism of polarized surfaces}$$

$$\mathcal{A}_{\mathrm{NJ}} := \left\{(A, \lambda) \in \mathcal{A}_{\mathrm{PP}} \mid (A, \lambda) \text{ splits over } \mathbb{F}_{q^2}\right\} \subseteq \mathcal{A}_{\mathrm{PP}}$$

$$|\mathcal{A}_{\mathrm{NJ}}| = \frac{1}{2}\left(\sum_{\mathbb{Z}[\pi^2] \subseteq \mathcal{O} \subseteq \mathcal{O}_L} h(\mathcal{O}) + \left[\sum_{\mathbb{Z}[i\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_{L'}} h(\mathcal{O}) \right]_{L' = \mathbb{Q}(i)} + [1]_{L', K^+} \right).$$

Counting polarizations

Consider the order $R = \mathbb{Z}[\pi, \overline{\pi}]$ of $\mathcal{O}_K$. Let $\mathcal{F}(R)$ be the category whose objects are nonzero finitely generated sub-R-modules of K and

$$\mathrm{Hom}_{\mathcal{F}(R)}(M, N) = \{\alpha \in K \mid \alpha M \subseteq N\}$$

Deligne established in 1969 an equivalence of categories $D\colon \mathcal{A} \longrightarrow \mathcal{F}(R)$ through which duality of abelian varieties is translated into: $M^\wedge := \overline{M}^*$, where $(\ )^*$ indicates dual under the trace pairing of $K/\mathbb{Q}$.

Theorem (Howe 1995). An isomorphism $\alpha M = M^\wedge$ is a principal polarization on M iff α is D-positive.

$$|\mathcal{A}_{\mathrm{PP}}| = |\{(M, \alpha) \mid M \in \mathcal{F}(R),\ \alpha \text{ pp on } M\}_{/\text{iso of pol. modules}}|$$

$$\mathcal{F}(R) = \coprod_{R \subseteq \mathcal{O} \subseteq \mathcal{O}_K} \mathcal{F}_{\mathcal{O}} := \{M \in \mathcal{F}(R) \mid \mathrm{End}(M) = \mathcal{O}\}$$

$$|\mathcal{A}_{\mathrm{PP}}| = \sum_{R \subseteq \mathcal{O} \subseteq \mathcal{O}_K} |\mathcal{A}_{\mathrm{PP}, \mathcal{O}}|.$$

If $\mathcal{O}$ Gorenstein and flat over $\mathcal{O}^+ := \mathcal{O} \cap \mathcal{O}_{K^+}$:

$$|\mathcal{A}_{\mathrm{PP},\mathcal{O}}| = \big(U^+_{>0}\colon\ \mathrm{N}(U)\big)\,|\operatorname{Coker}(N)|\frac{h(\mathcal{O})}{h^+(\mathcal{O}^+)}$$

The comparison of these formulas with the formulas for $|\mathcal{A}_{\mathrm{NJ}}|$ is still involved. If for an order $\mathcal{O}$ in a number field K we denote:

$$g(\mathcal{O}) := 2^{r_1} h(\mathcal{O}) R(\mathcal{O})/w(\mathcal{O}) t(\mathcal{O})$$

R =regulator, w =number of roots of unity, $t = |\operatorname{tor}(I(\mathcal{O}))|$ and r_1 =number of real embeddings, we have:

Dedekind-Sands. $g(\mathcal{O}) = g(\mathcal{O}_K)$

Brauer. $g(\mathcal{O}_K) = g(\mathcal{O}_L) g(\mathcal{O}_{K^+}) g(\mathcal{O}_{L'})$

$|\mathcal{A}_{\mathrm{PP}}| = \sum_{\mathcal{O}} |\mathcal{A}_{\mathrm{PP},\mathcal{O}}| = |\mathcal{A}_{\mathrm{NJ}}|$, for $a = -2q + 2$ H04

$|\mathcal{A}_{\mathrm{PP}}| \geq \sum_{\mathcal{O}\text{“good”}} |\mathcal{A}_{\mathrm{PP},\mathcal{O}}| > |\mathcal{A}_{\mathrm{NJ}}|$, for $a > -2q + 2$ M04

$\mathcal{A}$ supersingular, simple over $\mathbb{F}_q$, split over $\mathbb{F}_{q^2}$

E elliptic curve$/\mathbb{F}_p$ with null trace of Frobenius: $\pi_E^2 = -p$

$\mathcal{O} := \mathrm{End}(E)$ maximal order in the definite quaternion algebra B with discriminant p

$E[p] \simeq \alpha_p$ finite group scheme, $\quad \mathrm{Hom}(\alpha_p, E) = \mathrm{End}(\alpha_p) = \overline{k}$

$(i,j) \in \mathbb{P}^1(\overline{k})$ determines an exact sequence of group schemes

$$0 \to \alpha_p \xrightarrow{(i,j)} E \times E \longrightarrow (E \times E)/\alpha_p =: A_{ij} \to 0$$

Theorem (Oort 1975). $A/\overline{k}$ supersingular abelian surface. According to A being isomorphic to the product of two elliptic curves or not, it has only two possibilities

$$A \simeq E \times E, \qquad A \simeq A_{ij}, \quad (i,j) \in \mathbb{P}^1(\overline{k}) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$$

Polarizations and quaternion hermitian forms

Theorem (Serre,Ibukiyama,Katsura,Oort 1986). The set of principal polarizations on $E \times E$ (resp. A_{ij}) is in bijection with the following set Λ^{princ} (resp. Λ^{nprinc}) of quaternion hermitian forms:

$$\Lambda^{\text{princ}} = \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix} \mid s, t \in \mathbb{Z}_+, \ r \in \mathcal{O}, \ st - r\bar{r} = 1 \right\}$$

$$\Lambda^{\text{nprinc}} = \left\{ \begin{pmatrix} ps & r \\ \bar{r} & pt \end{pmatrix} s, t \in \mathbb{Z}_+, \ r \in \mathcal{O}, \ p^2 st - r\bar{r} = p \right\}.$$

Thus, for any (A, λ) p.p. abelian surface$/k$, the p.p. surface $(A, \lambda) \otimes_k \overline{k}$ is determined by the following data

$(E \times E, H), \ H \in \Lambda^{\text{princ}}$, or

$(E \times E, H), \ H \in \Lambda^{\text{nprinc}}, \quad (i, j) \in \mathbb{P}^1(\overline{k}) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$

In the latter case (A, λ) is automatically a Jacobian.

Descent to a given isogeny class in k

For simplicity we assume from now on that $q = p^{2n}$.

Theorem. The p.p. surface$/\overline{k}$ associated to the data

$$(E \times E, H) \qquad \left[\text{plus } (i,j) \in \mathbb{P}^1(\overline{k}) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})\right]$$

descends to k iff there exists $\alpha \in \mathrm{GL}_2(\mathcal{O}) = \mathrm{Aut}(E \times E)$ s.t.

$$\alpha^\dagger H \alpha = H \qquad \left[\text{plus } \tilde{\alpha}(i^\sigma, j^\sigma) = (i,j) \text{ in } \mathbb{P}^1(\overline{k})\right]$$

and the descended surface A lies in the following isogeny class:

$$\begin{array}{lll}
f_A(x) = (x^2 \pm 2\sqrt{q}x + q)^2 & \text{iff} & \alpha = \mp(-1)^n \\
f_A(x) = x^4 + 2qx^2 + q^2 & \text{iff} & \alpha^2 = -1 \\
f_A(x) = x^4 - qx^2 + q^2 & \text{iff} & \alpha^4 - \alpha^2 = -1 \\
f_A(x) = x^4 + q^2 & \text{iff} & \alpha^4 = -1
\end{array}$$

Descent to a Jacobian

Nonprincipal descent. The existence and non existence of a descent to a given isogeny class can be determined using results of T. Ibukiyama (1989) on mass formulas for quaternion hermitian forms with a given structure of the automorphism group.

Principal descent. For positive results one starts with a curve C having many automorphisms and such that J_C is geometricaly isomorphic to $E \times E$. From the structure of $\mathrm{Aut}(C)$ one can deduce the existence of an automorphism α of $E \times E$ satisfying the required conditions. The descended surface is a Jacobian because it is geometrically isomorphic to J_C.

For negative results one shows that if the Jacobian of a curve C lies in a certain isogeny class this forces the curve C to have automorphisms of certain order. Then one checks that such a curve does not exist.