Abelian surfaces over finite fields with prescribed groups

Chantal David (Concordia), Derek Garton (Portland State), Zachary Scherr (U. Penn), Arul Shankar (Harvard), Ethan Smith (Liberty) & Lola Thompson (Oberlin)

January 16, 2013

Definitions

Definition

An *elliptic curve* is a curve given by an equation of the form

$$y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{Q}$ and $\Delta := -16(4a^3 + 27b^2)$ is nonzero.

We can represent the set of points on an elliptic curve as

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is the point at infinity.

So, $\#E(\mathbb{Q}) = 1 + \#(\text{rational solutions to } y^2 = x^3 + ax + b)$.

Elliptic curves over finite fields

We can reduce $E/\mathbb{Q}$ to a curve over $\mathbb{F}_p$:

$$E(\mathbb{F}_p) := \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{\mathcal{O}\}.$$

Example: Consider $E : y^2 = x^3 + 2x + 1$ over $\mathbb{F}_5$.

x	$x^3 + 2x + 1 \pmod{5}$	y
0	1	1, 4
1	4	2, 3
2	3	–
3	4	2, 3
4	3	–

$\therefore \#E(\mathbb{F}_5) = 2 + 2 + 2 + 1 = 7.$

The **group** of points on $E/\mathbb{F}_p$

The rational points on E over $\mathbb{F}_p$ form an abelian group $E(\mathbb{F}_p)$ with

$$E(\mathbb{F}_p) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1 n_2\mathbb{Z}.$$

One could ask: How often do certain groups occur as $E(\mathbb{F}_p)$ as we vary over E and p?

Cohen-Lenstra heuristics

The **Cohen-Lenstra heuristics** predict that random abelian groups naturally occur with probability inversely proportional to the size of their automorphism groups.

An example of the Cohen-Lenstra phenomenon

Example: Cohen and Lenstra looked at the class groups of quadratic imaginary fields. They observed that, when $9 \mid\mid h(-D)$:

An example of the Cohen-Lenstra phenomenon

Example: Cohen and Lenstra looked at the class groups of quadratic imaginary fields. They observed that, when $9 \mid\mid h(-D)$:

- $\#\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) = \varphi(9) = 6$

An example of the Cohen-Lenstra phenomenon

Example: Cohen and Lenstra looked at the class groups of quadratic imaginary fields. They observed that, when $9 \mid\mid h(-D)$:

- $\#\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) = \varphi(9) = 6$
- $\#\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = 48.$

An example of the Cohen-Lenstra phenomenon

Example: Cohen and Lenstra looked at the class groups of quadratic imaginary fields. They observed that, when $9 \mid\mid h(-D)$:

- $\#\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) = \varphi(9) = 6$
- $\#\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = 48$.
- So, we would expect $\mathbb{Z}/9\mathbb{Z}$ to occur with probability proportional to $1/6$ and we would expect $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ to occur with probability proportional to $1/48$.

An example of the Cohen-Lenstra phenomenon

Example: Cohen and Lenstra looked at the class groups of quadratic imaginary fields. They observed that, when $9 \mid\mid h(-D)$:

- $\#\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) = \varphi(9) = 6$
- $\#\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = 48$.
- So, we would expect $\mathbb{Z}/9\mathbb{Z}$ to occur with probability proportional to $1/6$ and we would expect $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ to occur with probability proportional to $1/48$.
- Thus, $\mathbb{Z}/9\mathbb{Z}$ should be 8 times more likely to occur than $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(Experimental results show that the ratio of occurrence of $\mathbb{Z}/9\mathbb{Z}$ versus $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is about 8 to 1.)

How often do certain groups occur as $E(\mathbb{F}_p)$?

Conjecture (Banks, Pappalardi, Shparlinski, 2012)

Completely split groups (when $n_2 = 1$) and very split groups (when n_2 is very small compared to n_1) occur with density 0.

Results for elliptic curves




Theorem (Chandee, David, Koukoupoulopoulos, Smith)

Let $S(N_1, N_2)$ *denote the set of integer pairs* $n_1 \leq N_1$, $n_2 \leq N_2$ *for which there exists a prime* p *and a curve* $E/\mathbb{F}_p$ *with* $E(\mathbb{F}_p) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1 n_2 \mathbb{Z}$. *Then*

$$\#S(N_1, N_2) = o(N_1 N_2)$$

when $N_1 \geq \exp(N_2^{1/2-\varepsilon})$.

The group of points on an abelian surface

Let A be an abelian surface over $\mathbb{F}_q$. The points on A over $\mathbb{F}_q$ form an abelian group $A(\mathbb{F}_q)$ with

$$A(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}.$$

The group of points on an abelian surface

Let A be an abelian surface over $\mathbb{F}_q$. The points on A over $\mathbb{F}_q$ form an abelian group $A(\mathbb{F}_q)$ with

$$A(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}.$$

Q. How often do certain groups occur as the group of points on $A/\mathbb{F}_q$?

Cohen-Lenstra predicts:

The group of points on an abelian surface

Let A be an abelian surface over $\mathbb{F}_q$. The points on A over $\mathbb{F}_q$ form an abelian group $A(\mathbb{F}_q)$ with

$$A(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}.$$

Q. How often do certain groups occur as the group of points on $A/\mathbb{F}_q$?

Cohen-Lenstra predicts:

- Cyclic groups are the most likely to occur

The group of points on an abelian surface

Let A be an abelian surface over $\mathbb{F}_q$. The points on A over $\mathbb{F}_q$ form an abelian group $A(\mathbb{F}_q)$ with

$$A(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}.$$

Q. How often do certain groups occur as the group of points on $A/\mathbb{F}_q$?

Cohen-Lenstra predicts:

- Cyclic groups are the most likely to occur
- "Very split" groups (groups when n_1, n_2 are very large relative to n_3, n_4) are not very likely to occur.

Group classification results for abelian surfaces

Theorem (David, Garton, Scherr, Shankar, Smith, T.)

Suppose that n_1, n_2, n_3, n_4 are positive integers. If

$$n_1 > 60 n_2^{1/4} n_3^{3/2} n_4^{3/4} + 1,$$

then there are **no** *abelian surfaces $A/\mathbb{F}_q$ with*

$$A(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1 n_2\mathbb{Z} \times \mathbb{Z}/n_1 n_2 n_3\mathbb{Z} \times \mathbb{Z}/n_1 n_2 n_3 n_4\mathbb{Z}.$$

Facts about Weil polynomials

Let $f_A(T)$ be the characteristic polynomial of the Frobenius element π_A of $A/\mathbb{F}_q$, which we call a *Weil polynomial*:

Facts about Weil polynomials

Let $f_A(T)$ be the characteristic polynomial of the Frobenius element π_A of $A/\mathbb{F}_q$, which we call a *Weil polynomial*:

- Its roots are $\{\omega_1, \overline{\omega_1}, \omega_2, \overline{\omega_2}\}$, where the ω_i's are *Weil numbers* (algebraic integers whose conjugates have absolute value $q^{1/2}$).

Facts about Weil polynomials

Let $f_A(T)$ be the characteristic polynomial of the Frobenius element π_A of $A/\mathbb{F}_q$, which we call a *Weil polynomial*:

- Its roots are $\{\omega_1, \overline{\omega_1}, \omega_2, \overline{\omega_2}\}$, where the ω_i's are *Weil numbers* (algebraic integers whose conjugates have absolute value $q^{1/2}$).
- Tate-Honda theory gives a bijection between the set of conjugacy classes of Weil numbers and the set of isogeny classes of simple abelian varieties over $\mathbb{F}_q$.

Facts about Weil polynomials

Let $f_A(T)$ be the characteristic polynomial of the Frobenius element π_A of $A/\mathbb{F}_q$, which we call a *Weil polynomial*:

- Its roots are $\{\omega_1, \overline{\omega_1}, \omega_2, \overline{\omega_2}\}$, where the ω_i's are *Weil numbers* (algebraic integers whose conjugates have absolute value $q^{1/2}$).
- Tate-Honda theory gives a bijection between the set of conjugacy classes of Weil numbers and the set of isogeny classes of simple abelian varieties over $\mathbb{F}_q$.
- The number of $\mathbb{F}_q$-rational points on A is equal to $f_A(1)$.

$\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$: a field, or not a field?

Sometimes the algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field; other times it is not. (In general, the cases where $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is not a field are much rarer.)

To handle these exceptional cases:

Theorem (Waterhouse, Xing)

The Weil polynomials $f_A(T)$ corresponding to abelian varieties A over k of dimension 2 whose algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is **not** *a field are:*

$$f_A(T) = (T^2 - q)^2$$

$$f_A(T) = (T^2 + q)^2$$

$$f_A(T) = (T^2 \pm q^{1/2}T + q)^2$$

Characterization when $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is not a field

Xing proved that the group structures that arise are precisely:

$$
\begin{aligned}
A(\mathbb{F}_q) &\simeq (\mathbb{Z}/(q-1)\mathbb{Z})^2 \\
A(\mathbb{F}_q) &\simeq \left(\mathbb{Z}/\tfrac{q-1}{2}\mathbb{Z}\right)^2 \times (\mathbb{Z}/2\mathbb{Z})^2 \\
A(\mathbb{F}_q) &\simeq \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/\tfrac{q-1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\
A(\mathbb{F}_q) &\simeq (\mathbb{Z}/(q+1)\mathbb{Z})^2 \\
A(\mathbb{F}_q) &\simeq \left(\mathbb{Z}/(q \pm q^{1/2} + 1)\mathbb{Z}\right)^2 .
\end{aligned}
$$

Characterization when $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is not a field

Xing proved that the group structures that arise are precisely:

$$
\begin{aligned}
A(\mathbb{F}_q) &\simeq (\mathbb{Z}/(q-1)\mathbb{Z})^2 \\
A(\mathbb{F}_q) &\simeq \left(\mathbb{Z}/\tfrac{q-1}{2}\mathbb{Z}\right)^2 \times (\mathbb{Z}/2\mathbb{Z})^2 \\
A(\mathbb{F}_q) &\simeq \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/\tfrac{q-1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\
A(\mathbb{F}_q) &\simeq (\mathbb{Z}/(q+1)\mathbb{Z})^2 \\
A(\mathbb{F}_q) &\simeq \left(\mathbb{Z}/(q \pm q^{1/2}+1)\mathbb{Z}\right)^2 .
\end{aligned}
$$

Conclusion: We know exactly which groups can appear as the group of $\mathbb{F}_q$-rational points on an Abelian surface whose algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is **not** a field!

Abelian surfaces with prescribed groups

David, Garton, Scherr, Shankar, Smith, Thompson

Theorem (Rück)

The set $f_A(T)$ for all abelian surfaces A whose algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a field is equal to the set of polynomials $f(T) = T^4 + a_1T^3 + a_2T^2 + a_1qT + q^2$, where the integers a_1 and a_2 satisfy the following conditions:

(a) $|a_1| < 4q^{1/2}$ *and* $2|a_1|q^{1/2} - 2q < a_2 < a_1^2/4 + 2q$.

(b) $a_1^2 - 4a_2 + 8q$ *is not a square in* $\mathbb{Z}$

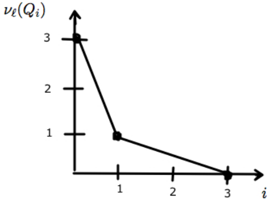
(and some conditions on $\nu_p(a_1)$ and $\nu_p(a_2)$.)

Newton polygons

Definition

Let ℓ be a prime and let $Q(T) = \sum_i Q_i T^i$ be a polynomial of degree d with $Q(0) = Q_0 \neq 0$. The *Newton polygon* $N_{p_\ell}(Q)$ is the boundary of the lower convex hull of the points $(i, \nu_\ell(Q_i))$ for $0 \leq i \leq d$ in $\mathbb{R}^2$.

Example The Newton polygon corresponding to $f(x) = x^3 + 6x^2 + 10x + 8$ over $\mathbb{Q}_2$ is:

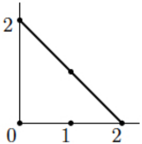


Hodge polygons

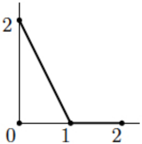
Definition

Let $0 \leq m_1 \leq m_2 \leq \cdots \leq m_r$ be nonnegative integers and let $H = \oplus_{i=1}^{m} \mathbb{Z}/\ell^{m_i}\mathbb{Z}$ be an abelian group of order ℓ^m. The *Hodge polygon* $H_{p_\ell}(H, r)$ is the convex polygon with vertices $(i, \sum_{j=1}^{r-i} m_j)$ for $0 \leq i \leq r$. It has $(0, m)$ and $(r, 0)$ as its endpoints, and its slopes are $-m_r, \ldots, -m_1$.

Example Hodge polygons corresponding to $H = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $H = \mathbb{Z}/\ell^2\mathbb{Z}$ (respectively):



Pic. 1



Pic. 2

Key lemma

Theorem (Rybakov, 2010)

Let A be an abelian variety over a finite field with Weil polynomial f_A. Suppose f_A has no multiple roots. Let G be an abelian group of order $f_A(1)$. Then G is a group of points on some variety in the isogeny class of A if and only if the Newton polygon $N_{p_\ell}(f_A(1-t))$ lies on or above the Hodge polygon $H_{p_\ell}(G_\ell, 2g)$ for any prime number ℓ.

Corollary to Rybakov's criterion

Corollary (David, Garton, Scherr, Shankar, Smith, T.)

Suppose that

$$G = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1n_2\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3\mathbb{Z} \times \mathbb{Z}/n_1n_2n_3n_4\mathbb{Z}.$$

Then, in order for G to appear as the group of points on an abelian surface, the following system of congruences must be satisfied:

$$q^2 + a_1q + a_2 + a_1 + 1 \equiv 0 \pmod{n_1^4n_2^3n_3^2n_4}$$

$$4 + 3a_1 + 2a_2 + qa_1 \equiv 0 \pmod{n_1^3n_1^2n_3}$$

$$6 + 3a_1 + a_2 \equiv 0 \pmod{n_1^2n_2}$$

$$4 + a_1 \equiv 0 \pmod{n_1}.$$

Proof of Corollary

Let $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z} \times \mathbb{Z}/N_3\mathbb{Z} \times \mathbb{Z}/N_4\mathbb{Z}$ where $N_1 \mid N_2 \mid N_3 \mid N_4$. We will show that G is the group of points on some $A/\mathbb{F}_q$ iff

$$\prod_{j=1}^{4-k} N_j \text{ divides } \frac{f_A^{(k)}(1)}{k!} \text{ for } k = 0, \ldots, 3.$$

- Write the Taylor expansion $f_A(1-T) = \sum_{k=0}^{4} \frac{f_A^{(k)}(1)}{k!}(-T)^k$.

Proof of Corollary

Let $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z} \times \mathbb{Z}/N_3\mathbb{Z} \times \mathbb{Z}/N_4\mathbb{Z}$ where $N_1 \mid N_2 \mid N_3 \mid N_4$. We will show that G is the group of points on some $A/\mathbb{F}_q$ iff

$$\prod_{j=1}^{4-k} N_j \text{ divides } \frac{f_A^{(k)}(1)}{k!} \text{ for } k = 0, \ldots, 3.$$

- Write the Taylor expansion $f_A(1-T) = \sum_{k=0}^{4} \frac{f_A^{(k)}(1)}{k!}(-T)^k$.
- For each prime ℓ, Rybakov's condition that $N_{p_\ell}(f_A(1-T))$ lies on or above $H_{p_\ell}(G_\ell, 4)$ means that

$$\nu_\ell(\prod_{j=1}^{4-k} N_j) \leq \nu_\ell\left(\frac{f_A^{(k)}(1)}{k!}\right) \text{ for } k = 0, \ldots, 3.$$

A "density 0" result

Theorem (David, Garton, Scherr, Shankar, Smith, T.)

If

$$\frac{N_1 N_2^{1/4}}{N_3^{1/2} N_4^{1/4}} \to \infty \quad \text{as } N_2 N_4 \to \infty,$$

then

$$\#S(N_1, N_2, N_3, N_4) = o(N_1 N_2 N_3 N_4) \quad \text{as } N_2 N_4 \to \infty.$$

Thank you!