Can You Hear the Shape of a Curve?

ICERM Project with Vishal Arul, Steven R Groen, Everett W Howe, Wanlin Li, Vlad Matei, Rachel Pries and Caleb Springer

Warmup: E_1: $y^2 = x^3 - x$ E_2: $y^2 = x^3 + 1$

p	$\#E_1(\mathbb{F}_p)$	$\#E_2(\mathbb{F}_p)$
3	4	4
5	8	6
7	8	12
11	12	12
13	8	12
17	16	18

How often is $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$?

Weil bound: $\approx \frac{c}{\sqrt{p}}$ choices

Another Example E_1: $y^2 = x^3 - x$ E_3: $y^2 = x^3 - 11x - 14$

p	$\#E_1(\mathbb{F}_p)$	$\#E_3(\mathbb{F}_p)$
3	4	4
5	8	8
7	8	8
11	12	12
13	8	8
17	16	16

$j_{E_1} = 1728$, $j_{E_3} = 287496$ } not isomorphic

E_1 and E_2 2-isogenous over $\mathbb{Q}$

$\Phi_2(j_{E_1}, j_{E_3}) = 0$

Isogenies Over $\mathbb{F}_q$ and Zeta Functions

Definition: nice $X/\mathbb{F}_q$: $Z(X,T) = \prod_{x \in X} \left(1 - T^{\deg x}\right)^{-1}$

Separated, finite type

$$= \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right)$$

Calculation: E elliptic curve/$\mathbb{F}_q$

$a = q + 1 - \#E(\mathbb{F}_q)$

$$Z(E,T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

reversed characteristic polynomial on $T_\ell E$ $(\ell, q) = 1$

The following are equivalent for elliptic curves $E, E'/\mathbb{F}_q$:

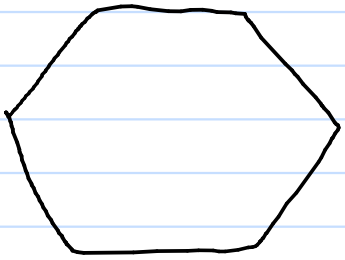
1) $Z(E,T) = Z(E',T)$
2) $T_\ell E \simeq T_\ell E'$ as Galois modules
3) $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$
4) E and E' isogenous (Tate)

Generalization: C, C' curve $/\mathbb{F}_q$

$Z(C,T) = Z(C',T) \iff \mathrm{Jac}(C)$ isogenous to $\mathrm{Jac}(C')$

Can you hear the shape of...

a drum



Spectrum of Laplacian

Answer: no

But... gives a lot of information

a curve

zeta function / spectrum of Frobenius

no

curves isogenous

Question: Can additional information about covers help?

Does $\tilde{C} \to C$

$$\left.\begin{array}{l} Z(C,T) = Z(C',T) \\ Z(\tilde{C},T) = Z(\tilde{C}',T) \\ \cdots \end{array}\right\} \Rightarrow C \simeq C' ?$$

Versions: Which cover(s)? L-functions instead of zeta?

Curves from a family? Computationally effective?

Which Covers?

C curve / $\mathbb{F}_q$. Geometric class field theory

$$\begin{array}{ccc} \tilde{C} & \to & \tilde{X} \\ \downarrow & & \downarrow \\ C & \to & Jac(C) \end{array}$$

finite étale

$P \mapsto [P - D_1]$

Today focus on: $\tilde{X} = Jac(C)$

Map:	$[2]$	$Frob^* - Id$
Galois Group: (geometric)	$Jac(C)[2]$	$Jac(C)(\mathbb{F}_q)$
	ICERM	work w/ Voloch

ICERM Project: Arul-B-Groen-Howe-Li-Matei-Pries-Springer

Z: $y^2 = c(x^2+1)(x^4+5x^2+1)$ genus 2

↑ family in s $\quad \mathrm{Aut}(Z) > D_4$

$$\begin{array}{ccc} \tilde{Z} & \to & \mathrm{Jac}(Z) \\ \downarrow & & \downarrow [2] \\ Z & \to & \mathrm{Jac}(Z) \end{array} \qquad \sim E^2$$

Howe, Sutherland, and Voloch looked at genus two curves with aut. of order 3. Similar story, different details

Genus of $\tilde{Z}$: 17

$$\mathrm{Jac}(\tilde{Z}) \sim E^2 \times \prod_{i=1}^{15} E_i$$

Count (Z_1, Z_2) in this family w/ $\mathrm{Jac}(Z_1) \sim \mathrm{Jac}(Z_2)$:

Expect $\quad c \cdot q^2 \cdot \frac{1}{\sqrt{q}} = c\, q^{3/2}$

Definition: Z_1 and Z_2 doubly isogenous if

$\mathrm{Jac}(Z_1) \sim \mathrm{Jac}(Z_2)$ and $\mathrm{Jac}(\tilde{Z}_1) \sim \mathrm{Jac}(\tilde{Z}_2)$

Main Question: How many pairs of doubly isogenous curves?

$$\mathrm{Jac}(\tilde{Z}) \sim E^2 \times \prod_{i=1}^{15} E_i$$

0th Guess: two members of family doubly isogenous if 16 elliptic curves are isogenous by chance

1st Guess: actually only 6 elliptic curves in $\mathrm{Jac}(\tilde{Z})$ $\mathcal{S}_{D_4}$ that depend on parameter

Expect $C \cdot q^2 \cdot \left(\frac{1}{\sqrt{q}}\right)^6 = \frac{C}{q}$

Experimentally:

Doubly isogenous pairs for 1024 primes closest to 2^n

n	pairs
15	820
16	580
17	407
18	282
19	218
20	138
21	100
22	58
23	42

suggests actually $C/\sqrt{q}$ doubly isogenous pairs

What's Going on?

Unexpected Coincidences in $\mathrm{Jac}(\tilde{Z}_1)$ and $\mathrm{Jac}(\tilde{Z}_2)$ ← 6 varying ell. curves

parameter: s_1 s_2

★ If s_1, s_2 satisfy certain poly. relations,

only need three coincidences to be doubly isogenous

Number of Pairs: $c \cdot q \cdot \frac{1}{(\sqrt{q})^3} = \frac{c}{\sqrt{q}}$

(Modular polynomial $\Phi_n(j_{E_1,s_1}, j_{E_2,s_2}) = 0$ gives relation for one isogeny) repeated!

★ Can be expressed as isogenies of Prym varieties.

for subcovers of $\tilde{Z} \to Z$

★ Doubly isogenous pairs for 1024 primes closest to 2^n

n	total	not in families
15	820	234
16	580	86
17	407	84
18	282	86
19	218	22
20	138	6
21	100	10
22	58	0
23	42	2

in line with c/q heuristic

Project with Felipe Voloch:

Use Hilbert class field covers: a max étale ext'n over $\mathbb{F}_q$

$\mathrm{Jac}(C)(\mathbb{F}_q)$-cover

$$\begin{array}{ccc} H(C) & \to & \mathrm{Jac}(C) \\ \downarrow & & \downarrow \quad \text{Frob-Id} \\ C & \to & \mathrm{Jac}(C) \end{array}$$

Question: To what extent is C determined by zeta function $Z(H(C), T) = \prod_{\chi} L(\chi, T)$

$\chi : \mathrm{Gal}(H(C)/C) \to \mathbb{C}^\times$

Fact: (Mochizuki, Tamagawa)

X hyperbolic curve/$\mathbb{F}_q$ $\pi_1^{\text{ét}}(X)$ determines X.

hyperbolic: projective genus ≥ 2 or enough points removed...

Thm (B-Voloch) Let C be smooth proj curve genus ≥ 2

L-functions for $H(C_{\mathbb{F}_{q^n}}) / C_{\mathbb{F}_{q^n}}$ $n \geq 1$ determine C.

ie given C, C' and $\mathrm{Jac}(C)(\bar{\mathbb{F}}_q) \simeq \mathrm{Jac}(C')(\bar{\mathbb{F}}_q)$ as groups such that L-functions agree, $C \simeq C'$.

uses result of Zilber

Cor: Direct Proof of Mochizuki's result for proj. hyp. curves.