Visualizing elements of order 7 in the Tate-Shafarevich group of an elliptic curve

Tom Fisher

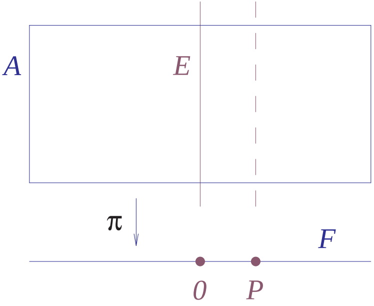
DPMMS
University of Cambridge

Workshop on Arithmetic of Hyperelliptic Curves
ICTP, Trieste 7th September 2017

Visibility (Mazur, 1999)

Exact sequence of abelian varieties over $\mathbb{Q}$

$$0 \longrightarrow E \xrightarrow{\iota} A \xrightarrow{\pi} F \longrightarrow 0$$



$$\longrightarrow A(\mathbb{Q}) \longrightarrow F(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, E) \xrightarrow{\iota_*} H^1(\mathbb{Q}, A) \rightarrow$$

Definition. $\mathrm{Vis}_A H^1(\mathbb{Q}, E) = \mathrm{im}(\delta) = \ker(\iota_*)$

Definition. $Ш(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E) \rightarrow \prod_v H^1(\mathbb{Q}_v, E)\right)$

Examples of Visible Ш

We take $A = \dfrac{E \times F}{\Delta}$ $\qquad \left. \begin{array}{l} \Delta \subset E \\ \Delta \subset F \end{array} \right\}$ common finite Galois submodule

Cremona and Mazur (2000)

$\dim E = \dim F = 1 \qquad \Delta = E[n] = F[n]$

$n = 2, 3, 4, 5$

Agashe and Stein (2005)

$\dim E > 1 \quad \dim F = 1 \qquad \Delta = F[n] \subset E[n]$

$n = 3, 5, 7, \ldots, 31$

This talk

$\dim E = 1 \quad \dim F = 1 \qquad \Delta = E[7] = F[7]$

$\dim F = 2 \qquad \Delta = E[7] = F[3 + \sqrt{2}]$

The Visibility Dimension

$E/\mathbb{Q}$ elliptic curve.

Definition. The *visibility dimension* of $\xi \in Ш(E/\mathbb{Q})$ is the least dimension of an abelian variety A such that $\xi \in \mathrm{Vis}_A H^1(\mathbb{Q}, E)$.

- Restriction of scalars shows $\quad \mathrm{vis\,dim}(\xi) \leqslant \mathrm{order}(\xi)$
- Mazur (1999) : $\mathrm{order}(\xi) = 3 \implies \mathrm{vis\,dim}(\xi) \leqslant 2$
- Fisher (2014) : $\exists\, \xi$ of orders 6 and 7 with $\mathrm{vis\,dim}(\xi) > 2$

Observation. The visibility dimension is often much smaller than the bound coming from restriction of scalars.

Examples from Cremona's Tables

$E/\mathbb{Q}$ with $Ш(E/\mathbb{Q})[7] \neq 0$ (and no rational 7-isogeny)

E	F	E	F	E	F
$3364c$	$10092c$	$10800y$	$10800u$	$15219c$	
$6552y$	$6552ba$	$11970o$	$11970s$	$17271g$	
$6622b$		$12927e$	$12927d$	$17816c$	
$7139a$		$13432b$		$18513b$	
$9450p$	$9450t$	$13673a$		$18550c$	
$9510e$	$561090*$	$14938n$		$18832a$	$1712d$

We searched for rational points on twists of the Klein quartic

$$X(7) = \{x^3y + y^3z + z^3x = 0\} \subset \mathbb{P}^2.$$

The appropiate twists are given by formulae of Halberstadt, Kraus and Poonen, Schaefer, Stoll.

Examples from Cremona's Tables

$E/\mathbb{Q}$ with $\text{Ш}(E/\mathbb{Q})[7] \neq 0$ (and no rational 7-isogeny)

E	F	E	F	E	F
$3364c$	$10092c$	$10800y$	$10800u$	$15219c$	
$6552y$	$6552ba$	$11970o$	$11970s$	$17271g$	x
$6622b$		$12927e$	$12927d$	$17816c$	x
$7139a$	x	$13432b$	x	$18513b$	x
$9450p$	$9450t$	$13673a$	x	$18550c$	x
$9510e$	$561090\,*$	$14938n$		$18832a$	$1712d$

In the cases indicated we found an elliptic curve $F/\mathbb{Q}$ with $E[7] \cong F[7]$ and rank $F(\mathbb{Q}) = 2$. Therefore

$$(\mathbb{Z}/7\mathbb{Z})^2 \cong \frac{F(\mathbb{Q})}{7F(\mathbb{Q})} \hookrightarrow H^1(\mathbb{Q}, E).$$

First Example

$E = 6622b \qquad N_E = 6622 = 2 \times 7 \times 11 \times 43.$

There are 10 isogeny classes of this conductor, but the elliptic curves in the other 9 isogeny classes are not 7-congruent to E.

However we find $f \in S_2(\Gamma_0(6622))$ with

p	2	3	5	7	11	13
$a_p(E)$	-1	2	2	-1	1	6
$a_p(f)$	-1	$-\sqrt{2}-1$	$\sqrt{2}-2$	-1	1	$2\sqrt{2}-2$

$$a_p(f) \equiv a_p(E) \mod (3+\sqrt{2}) \qquad \text{for all } p$$

Question. Can we find $C/\mathbb{Q}$ genus 2 curve with

$$\mathrm{Trace}(a_p(f)) = p + 1 - n_1$$
$$\mathrm{Norm}(a_p(f)) = (n_1^2 + n_2)/2 - (p+1)n_1 - p$$

where $n_i = \#\widetilde{C}(\mathbb{F}_{p^i})$?

First Example (continued)

$E = 6622b \qquad N_E = 6622 = 2 \times 7 \times 11 \times 43.$

Question. Can we find $C/\mathbb{Q}$ genus 2 curve with

$$\begin{aligned} \mathrm{Trace}(a_p(f)) &= p + 1 - n_1 \\ \mathrm{Norm}(a_p(f)) &= (n_1^2 + n_2)/2 - (p+1)n_1 - p \end{aligned}$$

where $n_i = \#\widetilde{C}(\mathbb{F}_{p^i})$?

Answer. Yes.

$$\begin{aligned} y^2 &= 20x^6 + 44x^5 - 23x^4 - 10x^3 + 81x^2 - 52x + 4 \\ &= \mathrm{Norm}_{K/\mathbb{Q}}\left((-\alpha + 1)x^2 - \frac{\alpha^2 + \alpha}{2} x + \alpha + 3 \right) \end{aligned}$$

where $K = \mathbb{Q}(\alpha)$ and $\alpha^3 + \alpha^2 + \alpha + 17 = 0$.

Using formulae of Bending (1998) we found 35 similar examples with $N_E < 10^5$ and F a genus 2 Jacobian with real multiplication by $\sqrt{2}$.

Remarks.

- These examples were found *without* having to compute any modular forms. However in most cases $N_F = N_E^2$ (up to powers of 2).
- In all but 3 cases we found rank $F(\mathbb{Q}) = 4$. Therefore

$$(\mathbb{Z}/7\mathbb{Z})^2 \cong \frac{F(\mathbb{Q})}{(3+\sqrt{2})F(\mathbb{Q})} \hookrightarrow H^1(\mathbb{Q}, E).$$

Favourite Example

$E = 67080r \qquad N_E = 67080 = 2^3 \times 3 \times 5 \times 13 \times 43.$
We find $f \in S_2(\Gamma_0(13416))$ with

p	2	3	5	7	11	13
$a_p(E)$	0	-1	-1	2	4	-1
$a_p(f)$	0	-1	$-\sqrt{2}-2$	$\sqrt{2}-2$	$-2\sqrt{2}-2$	-1

$$a_p(E) \equiv a_p(f) \mod (3+\sqrt{2}) \qquad \text{for all } p \neq 5$$

Genus 2 curve $C/\mathbb{Q}$: $\quad y^2 = x(x+4)(x^4+2x^3-x-3).$

Following Poonen, Schaefer, Stoll:
$J = \mathrm{Jac}(X_E(7))$: $\quad \mathrm{rank}\, J(\mathbb{Q}) = 2 < 3 = \dim J \quad$ (under GRH)
Chabauty + Mordell-Weil sieve gives $\# X_E(7)(\mathbb{Q}) = 2$.

Conclusion. Every non-trivial element of $Ш(E/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^2$ has visibility dimension exactly 3.

Checking the Congruences

We must prove $E[7] = F[3+\sqrt{2}]$ as Galois modules.

Possible methods.

1. Fix F. Find the twist of the Klein quartic parametrising the elliptic curves E with $E[7] = F[3+\sqrt{2}]$.
2. Use modularity (Ribet, Khare, Wintenberger)
   Bottlenecks : Computing modular forms.
   Computing 2-part of conductor.
   Possible variant : Use Faltings-Serre method.
3. Exhibit torsion points on $E/\pm 1$ and $F/\pm 1$ with the same field of definition. (Following Kraus, Oesterle (1992)).

We used method 3.

Checking Local Solubility

Using $F/\mathbb{Q}$ with dim $F = 1$ or 2 we have exhibited

$$(\mathbb{Z}/7\mathbb{Z})^2 \hookrightarrow H^1(\mathbb{Q}, E).$$

Question. Do we get elements of $\text{Ш}(E/\mathbb{Q})$?

We have $\Delta = E[7] = F[\phi]$ where $\phi = 7$ or $3 + \sqrt{2}$.

The Selmer groups $S^{(7)}(E/\mathbb{Q})$ and $S^{(\phi)}(F/\mathbb{Q})$ are subgroups of $H^1(\mathbb{Q}, \Delta)$ defined by local conditions.

If these local conditions match up, we do get elements of $\text{Ш}(E/\mathbb{Q})$. This is true in all cases checked so far.

Examples from Cremona's Tables (revisited)

$E/\mathbb{Q}$ with $Ш(E/\mathbb{Q})[7] \neq 0$ (and no rational 7-isogeny)

E	F	E	F	E	F
$3364c$	$10092c$	$10800y$	$10800u$	$15219c$	$\boxed{\text{genus 2}}$
$6552y$	$6552ba$	$11970o$	$11970s$	$17271g$	x
$6622b$	$\boxed{\text{genus 2}}$	$12927e$	$12927d$	$17816c$	x
$7139a$	x	$13432b$	x	$18513b$	x
$9450p$	$9450t$	$13673a$	x	$18550c$	x
$9510e$	$561090 *$	$14938n$	$\boxed{\text{genus 2}}$	$18832a$	$1712d$

The examples with $F/\mathbb{Q}$ a genus 2 Jacobian have

$$E[7] \cong F[3 + \sqrt{2}].$$

Further Examples (in progress)

$E/\mathbb{Q}$ with $Ш(E/\mathbb{Q})[11] \neq 0$

E	F	E	F	E	F
8350c	genus 2	36166j		52416dm	52416dl
13790a	genus 2	36762h	x	55660v	
14570c		38088t	38088u	56144v	genus 2
20806a	x	40755n	x	58029f	genus 2
30940a	x	44082c	genus 2	58558e	genus 2
36076b	x	49450k	x	61275j	x

The examples with $F/\mathbb{Q}$ a genus 2 Jacobian have

$$E[11] \cong F[4-\varphi] \qquad \text{where } \varphi = \frac{1+\sqrt{5}}{2}.$$