Visualising Ш[2] in Abelian surfaces

Nils Bruin (PIMS, SFU, UBC)

The Pacific Institute for the Mathematical Sciences

NOUS SOMMES PRETS

Setting

- K is a number field.
- Elliptic Curve $E : y^2 = x^3 + a_2 x^2 + a_4 x + a_6 = F(x)$ with $F(x) \in K[x]$.
- Rational points $E(K)$ form a finitely generated commutative group.
- $E(K) \simeq \mathbb{Z}^r \oplus E(K)^{\mathrm{tor}}$. *Torsion* $E(K)^{\mathrm{tor}}$ is finite. The *rank* of $E(K)$ is r.
- The group $E(K)^{\mathrm{tor}}$ can effectively and practically be determined.
- $E(K)/2E(K) \simeq E[2](K) \oplus (\mathbb{Z}/2\mathbb{Z})^r$, where $E[2](K) \subset E(K)^{\mathrm{tor}}$.
- We focus on determining $E(K)/2E(K)$.

The Selmer group

From

$$0 \to E[2] \to E \xrightarrow{2} E \to 0$$

we obtain

$$0 \mapsto E(K)/2E(K) \to H^1(K, E[2]) \to H^1(K, E)[2].$$

The set $H^1(K, E[2])$ is represented by the *twists* of $E \xrightarrow{2} E$:

That is: Covers $T \to E$ that are isomorphic to $E \xrightarrow{2} E$ over $\overline{K}$.

The image $E(K)/2E(K)$ in $H^1(K, E[2])$ are those T with $T(K) \neq \emptyset$.

By: $P \in E(K) \mapsto$ the twist of T with a rational point above P.

An approximation is the 2-*Selmer-group*:

$$S^{(2)}(E/K) := \left\{ T \in H^1(K, E[2]) : T(K_p) \neq \emptyset \text{ for all primes } p \text{ of } K \right\}.$$

The Tate-Shafarevich group

By definition,

$$0 \to E(K)/2E(K) \to S^{(2)}(E/K) \to Ш(E/K)[2] \to 0.$$

The group $Ш(E/K)[2]$ is conjectured to be a square.

In practice it is often (but not always!) trivial.

A 2-descent determines $S^{(2)}(E/K)$. Gives upper bound on $\mathrm{rk}(E(K))$.

Finding points on $E(K)$ gives lower bound on rank.

Need a way to get good lower bounds on $\#Ш(E/K)[2]$.

Strategy: Force a point on $T \in H^1(K, E[2])$ (by base extension). Try and see if anything changed.

Subcovers

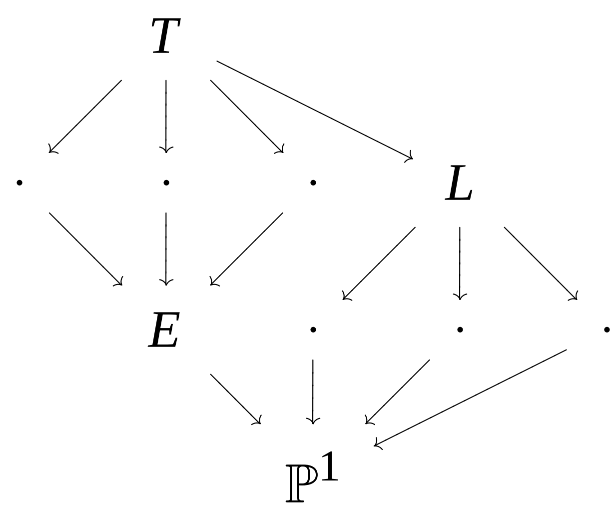
E is a double cover of $\mathbb{P}^1$ by $(x,y) \mapsto x$. It is ramified above $F(x) = 0$ and ∞.

$T \to E$ is unramified and $\mathrm{Aut}_{\overline{K}}(T/E) = E[2](\overline{K}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\mathrm{Aut}_{\overline{K}}(T/\mathbb{P}^1) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Let L be the maximal subcover of $T \to \mathbb{P}^1$ unramified at ∞.

Then $T = E \times_{\mathbb{P}^1} L$.



L is of genus 0. By Hasse's principle, if $T \in S^{(2)}(E/K)$, then $L(K) \neq \emptyset$.

Twisting $Ш[2]$ away

(Example with 2-torsion over $\mathbb{Q}$ in Kenneth Kramer, *Arithmetic of elliptic curves upon quadratic extension*, TAMS 1981)

Let $Q \in L(K)$ with image $x_Q \in \mathbb{P}^1(K)$.

Take d such that $F(x_Q) = d \cdot \square$.

$$E^{(d)} : dy^2 = F(x) \text{ and } T^{(d)} = E^{(d)} \times_{\mathbb{P}^1} L.$$

The curve $E^{(d)}$ has a rational point above x_Q. So has $T^{(d)}$.

Over $K(\sqrt{d})$, we have $E \simeq E^{(d)}$ and $T \simeq T^{(d)}$.

We know $\mathrm{rk}(E(K(\sqrt{d}))) = \mathrm{rk}(E(K)) + \mathrm{rk}(E^{(d)}(K))$.

We hope $\mathrm{rk}(S^{(2)}(E/K(\sqrt{d}))) < \mathrm{rk}(S^{(2)}(E/K)) + \mathrm{rk}(S^{(2)}(E^{(d)}/K))$.

An example

Take $K = \mathbb{Q}$ and consider the curve (from Schaefer, Stoll):

$$E : y^2 = x^3 - 22x^2 + 21x + 1.$$

It has rank at least 2: $(0,1),(1,1) \in E(\mathbb{Q})$

$(0,1)+(1,1) = (21,-1)$ and $(0,1)-(1,1) = (25,49)$.

We compute

$$S^{(2)}(E/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^4$$

We suspect

$$Ш(E/\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Information on $S^{(2)}(E/\mathbb{Q})$

We write $T^{[\mathrm{nr}]}$ for elements of $S^{(2)}(E/\mathbb{Q})$ and $L^{[\mathrm{nr}]}$ for the curve below it.

nr	some x-coordinates of points on $L^{[\mathrm{nr}]}$	corresponding ds
0	∞	1
1	$9/10, 13/17$	$10, 17$
2	1	1
3	$-4/3, -1/20$	$-3, -5$
4	$1/2$	2
5	$-1/4, -16/23$	$-1, -23$
6	$-25/4, -9/8, -4/11, -16/15$	$-1, -2, -11, -15$
7	$1/6, 1/17$	$6, 17$
8	$-1/7, -1/14$	$-7, -14$
9	$1/4, 1/8, 4/13$	$313, 2, 13$
10	$1/12, 12/13$	$3, 13$
11	$-1/2, -1/6$	$-2, -4038$
12	0	1
13	$-9/2, -1/15, -13/23$	$-2, -15, -23$
14	$21, 25, -1/18, -1/22$	$1, 1, -2, -2$
15	$4/5, 25/24$	$5, 6$

Rank information

d	x-coords[nr]	$\mathrm{rk}(E^{(d)})$	$\mathrm{rk}(E(K(\sqrt{d})))$
-4038	$-1/6$[11]	2	4
-23	$-16/23$[5], $-13/23$[13]	2	4
-22	$-1/22$[14]	2	6
-15	$-16/15$[6], $-1/15$[13]	3	5
-14	$-1/14$[8]	2	4
-11	$-4/11$[6]	1	5
-7	$-1/7$[8]	2	4
-5	$-1/20$[3]	2	4
-3	$-4/3$[3]	2	4
-2	$-9/2$[13], $-9/8$[6], $-1/2$[11], $-1/18$[14]	3	5
-1	$-25/4$[6], $-1/4$[5]	2	4
1	0[12], 1[2], 21[14], 25[14]	.	.
2	$1/8$[9], $1/2$[4]	2..4	4
3	$1/12$[10]	1..3	5
5	$4/5$[15]	1..3	5
6	$1/6$[7], $25/24$[15]	2..4	4
10	$9/10$[1]	2..4	4
13	$4/13$[9], $12/13$[10]	3	5
17	$1/17$[7], $13/17$[1]	2..4	4
313	$1/4$[9]	2..4	6

Visualisation of $Ш[2]$

Idea from Cremona, Mazur. Studied in Modular setting by William Stein.

Put $A = \Re_{K(\sqrt{d})/K}(E)$. We have $0 \to E \to A \to E^{(d)} \to 0$.

Note that $E[2]$ and $E^{(d)}[2]$ are isomorphic.

$$\begin{array}{c} 0 \\ \downarrow \\ E(K)/2E(K) \\ \downarrow \\ H^1(K, E[2]) \\ \downarrow \\ H^1(K, E) \end{array}$$

Visualisation of Ш[2]

Idea from Cremona, Mazur. Studied in Modular setting by William Stein.

Put $A = \Re_{K(\sqrt{d})/K}(E)$. We have $0 \to E \to A \to E^{(d)} \to 0$.

Note that $E[2]$ and $E^{(d)}[2]$ are isomorphic.

$$\begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ & & E(K)/2E(K) & & \\ & & \downarrow & & \\ E^{(d)}(K) & \longrightarrow & H^1(K,E[2]) & \to & H^1(K,E^{(d)}) \\ & & \downarrow & & \\ & & H^1(K,E) & & \end{array}$$

Visualisation of Ш[2]

Idea from Cremona, Mazur. Studied in Modular setting by William Stein.

Put $A = \Re_{K(\sqrt{d})/K}(E)$. We have $0 \to E \to A \to E^{(d)} \to 0$.

Note that $E[2]$ and $E^{(d)}[2]$ are isomorphic.

$$\begin{array}{ccccc} & & 0 & & \\ & & \downarrow & & \\ & & E(K)/2E(K) & & \\ & & \downarrow & & \\ E^{(d)}(K) & \longrightarrow & H^1(K, E[2]) & \to & H^1(K, E^{(d)}) \\ \downarrow & & \downarrow & & \downarrow \\ E^{(d)}(K) & \longrightarrow & H^1(K, E) & \longrightarrow & H^1(K, A) \end{array}$$

The map $E^{(d)}(K) \to H^1(K,E)$ sends $P \in E^{(d)}(K)$ to the fiber of A over P.

A more general construction

We don't need $A = \Re_{K(\sqrt{d})/K}(E)$.

Take E_1, E_2 with $E_1[2] \simeq E_2[2]$. We construct A isogenous to $E_1 \times E_2$.

$$E_1 : y^2 = F(x) = x^3 + a_2 x^2 + a_4 x + a_6$$

$$L_0 : y^2 = d(x-a) \qquad C = E_1 \times_{\mathbb{P}^1} L_0 : \; z^2 = F(\frac{y^2}{d} + a)$$

$$E_2 : y^2 = d(x-a)F(x)$$

$$\begin{array}{ccccc} & & C & & \\ & \swarrow & \downarrow & \searrow & \\ E_1 & & L_0 & & E_2 \\ & \searrow & \downarrow & \swarrow & \\ & & \mathbb{P}^1 & & \end{array} \qquad 0 \to E_1 \to \mathrm{Jac}_C \to E_2 \to 0$$

Solve a and d so that E_2 visualises 2 elements of $S^{(2)}(E_1/K)$ in Jac_C.

Example of bi-elliptic construction

Consider (again) $E_1 : y^2 = x^3 - 22x^2 + 21x + 1 = F(x)$ over $\mathbb{Q}$.

Take $x_1 = 9/10$[1] and $x_2 = 1/2$[4].

Take a and d so that $d(x_1 - a)F(x_1) = \square$ and $d(x_2 - a)F(x_2) = \square$:

$$a = 1,\ d = -1.$$

$$C : z^2 = F(-y^2 + 1) = -y^6 - 19y^4 + 20y^2 + 1, \quad E_2 : y^2 = -(x+1)F(x)$$

We find

$$\mathrm{rk}(\mathrm{Jac}_C(\mathbb{Q})) \leq 5, \quad \mathrm{rk}(E_2(\mathbb{Q})) = 3.$$

Since Jac_C is isogenous to $E_1 \times E_2$:

$$\mathrm{rk}(E_1(\mathbb{Q})) = \mathrm{rk}(\mathrm{Jac}_C(\mathbb{Q})) - \mathrm{rk}(E_2(\mathbb{Q}))$$

Again, we find $\mathrm{rk}(E_1(\mathbb{Q})) = 2$ and $\text{Ш}(E_1/\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.