Visualising Sha[2] in Abelian surfaces

Nils Bruin, PIMS/SFU/UBC

We consider an elliptic curve

$$E : y^2 = x^3 + a_2\,x^2 + a_4\,x + a_6$$

over a number field K. Its set of rational points $E(K)$ forms a finitely generated commutative group. We have that $E(K) \simeq \mathbb{Z}^r \times E(K)^{\mathrm{tor}}$, where $E(K)^{\mathrm{tor}} \subset E(K)$ is the finite subgroup of elements of finite order. This group is effectively and in practice usually easily determinable. In order to determine r, the *rank* of $E(K)$, it would be sufficient to determine the size of $E(K)/2E(K)$. From Galois-cohomology we obtain

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

The middle term, $H^1(K, E[2])$, classifies twists of $E \xrightarrow{2} E$, that is, unramified $E[2]$-covers $T \to E$ that are isomorphic to $E \to E$ over $\overline{K}$. The image of $E(K)/2E(K)$ corresponds to $T \in H^1(K, E[2])$ with $T \neq \emptyset$. An effectively determinable approximation of $E(K)/2E(K)$ is given by the *Selmer-group*

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

The error in this approximation is defined to be the Tate-Shafarevich group

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

It is represented by T that have points locally at all primes of K but not globally over K.

Given an elliptic curve E and a $T \in S^{(2)}(E/K)$ that we suspect to have a non-trivial image in $Ш(E/K)[2]$, we can do the following. We compute a value $d \in K$ so that $T(K(\sqrt{d})) \neq \emptyset$. We use that

$$\mathrm{rk}(E(K(\sqrt{d}))) = \mathrm{rk}(E(K)) + \mathrm{rk}(E^{(d)}(K)),$$

where

$$E^{(d)} : d\,(y')^2 = x^3 + a_2\,x^2 + a_4\,x + a_6.$$

We get an upper bound on $\mathrm{rk}(E(K(\sqrt{d})))$ by computing $S^{(2)}(E/K(\sqrt{d}))$. If we can get a sufficiently high lower bound on $\mathrm{rk}(E^{(d)}(K))$ (for instance, by exhibiting sufficiently many independent points on $E^{(d)}(K)$), then we can show that the rank bound obtained from $S^{(2)}(E/K)$ is not sharp.

A rather striking example is given by

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

We find $\#S^{(2)}(E/\mathbb{Q}) = 16$ and $\mathrm{rk}(E(\mathbb{Q})) > 2$. Furthermore, we get $\#S^{(2)}(E^{(2)}/\mathbb{Q}) = 16$ and $\mathrm{rk}(E^{(2)}(\mathbb{Q})) > 2$. However, we compute $\#S^{(2)}(E/\mathbb{Q}(\sqrt{2})) = 16$. Therefore, we find that $\#Ш(E/\mathbb{Q})[2] = \#Ш(E^{(2)}/\mathbb{Q})[2] = 4$.

We see that $E/\mathbb{Q}$ and $E^{(2)}/\mathbb{Q}$ mutually visualise $Ш[2]$ in the sense of Cremona-Mazur in the Weil-restriction $\Re_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(E)$.

We do not need to restrict to Abelian surfaces that are Weil-restrictions of elliptic curves. Note that $E : y^2 = F(x)$ is a double cover of $\mathbb{P}^1$ by $(x, y) \mapsto x$. Let

$$L : z^2 = d(x - a) \text{ and } C = L \times_{\mathbb{P}^1} E.$$

Then C is a curve of genus 2 given by $y^2 = F(z^2/d + a)$. Apart from E and L, the curve C also covers

$$E' : (y')^2 = d(x - a)F(x).$$

This implies that

$$\mathrm{rk}(\mathrm{Jac}_C(K)) = \mathrm{rk}(E(K)) + \mathrm{rk}(E'(K)).$$

We can bound the left hand side from above by determining the 2-Selmer group of Jac_C.

For instance, if we choose $a = 1$, $d = -1$ in the example above, we find $\mathrm{rk}(\mathrm{Jac}_C(\mathbb{Q})) \leq 5$ and $\mathrm{rk}(E'(\mathbb{Q})) = 3$. Again we find $\mathrm{rk}(E(\mathbb{Q})) = 2$ and $\#Ш(E/\mathbb{Q})[2] = 4$.

An advantage of the latter construction is that the two degrees of freedom (a and d) allow us solve for visualisation of two elements of $S^{(2)}(E/K)$ simultaneously. This helps because, conjecturally, Ш[2] always has square order.