Can the 5-part of the Shafarevich-Tate group of an elliptic curve get arbitrarily large

Ed Schaefer
Santa Clara University
At Leiden, 28 June, 2000

Jaap Top asked me if the 5-part of the Shafarevich-Tate group of an elliptic curve over $\mathbf{Q}$ can get arbitrarily large. The answer is yes, but I can't prove it.

Let $E/\mathbf{Q}$ be an elliptic curve. We have

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus E(\mathbf{Q})_{\mathrm{tors}}.$$

r is called the Mordell-Weil rank. $E(\mathbf{Q})_{\mathrm{tors}}$ is easy to determine. How to find r: It suffices to find $E(\mathbf{Q})/2E(\mathbf{Q})$ since $\dim E(\mathbf{Q})/2E(\mathbf{Q}) = r + \dim E(\mathbf{Q})[2]$. To determine $E(\mathbf{Q})/2E(\mathbf{Q})$, we embed it into a cohomology group.

$$\begin{tikzcd} 0 \arrow[r] & E(\mathbf{Q})/2E(\mathbf{Q}) \arrow[r] & H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), E[2]) \arrow[r] \arrow[dr, "\prod \beta_q"] & H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), E(\overline{\mathbf{Q}}))[2] \arrow[r] \arrow[d, "\prod \mathrm{res}_q"] & 0 \\ & & & \prod_q H^1(\mathrm{Gal}(\overline{\mathbf{Q}_q}/\mathbf{Q}_q), E(\overline{\mathbf{Q}_q}))[2] & \end{tikzcd}$$

We would like to find everything in $H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), E[2])$ that maps to 0 in $H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), E(\overline{\mathbf{Q}}))[2]$. There is no known effective algorithm for doing this. Instead we find everything in $H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), E[2])$ that maps to 0 in $H^1(\mathrm{Gal}(\overline{\mathbf{Q}_q}/\mathbf{Q}_q), E(\overline{\mathbf{Q}_q}))[2]$, for every prime q. There is an effective algorithm to do that. Since $\mathrm{Gal}(\overline{\mathbf{Q}_q}/\mathbf{Q}_q)$ is isomorphic to a decomposition subgroup of $\mathrm{Gal}(\overline{Q}/Q)$, there is a restriction map from the global cohomology group to each local one.

The 2-Selmer group $S^2(\mathbf{Q}, E) = \ker \prod \beta_q$. It is effectively computable and provably finite. We have

$$0 \to E(\mathbf{Q})/2E(\mathbf{Q}) \to S^2(\mathbf{Q}, E) \to \ker \prod \mathrm{res}_q \to 0.$$

The obstruction (omit [2]):

$$Ш(\mathbf{Q}, E) = \ker : H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), E(\overline{\mathbf{Q}})) \stackrel{\prod \mathrm{res}_q}{\to} \prod_q H^1(\mathrm{Gal}(\overline{\mathbf{Q}_q}/\mathbf{Q}_q), E(\overline{\mathbf{Q}}_q))$$

is called the Shafarevich-Tate group. There is no known effective algorithm for determining it. It measures the failure of a local/global principle.

So the obstruction to computing $E(\mathbf{Q})/2E(\mathbf{Q})$ is $Ш(\mathbf{Q}, E)[2]$.

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

In general, for any prime p we have

$$0 \to E(\mathbf{Q})/pE(\mathbf{Q}) \to S^p(\mathbf{Q}, E) \to Ш(\mathbf{Q}, E)[p].$$

The group $S^p(\mathbf{Q}, E)$ is finite, so the group $Ш(\mathbf{Q}, E)[p]$ is finite. The group $Ш(\mathbf{Q}, E)$ is conjectured to be finite. Rubin provided the first provably finite examples.

Note
$$\dim S^p(\mathbf{Q},E) = r + \dim E(\mathbf{Q})[p] + \dim Ш(\mathbf{Q},E)[p].$$

Facts: Because of the (alternating) Cassels-Tate pairing, if $Ш(\mathbf{Q},E)$ is finite, then its order is a square and $\dim Ш(\mathbf{Q},E)[p]$ is even.

Bölling and Cassels have shown that $Ш(\mathbf{Q},E)[2]$ and $Ш(\mathbf{Q},E)[3]$ can get arbitrarily large. Of course all elliptic curves have an automorphism of order 2 and the $Ш(\mathbf{Q},E)[3]$ case was shown for elliptic curves with an automorphism of order 3 ($j = 0$). No elliptic curve has an automorphism of order 5. So, how about $Ш(\mathbf{Q},E)[5]$?

Look at the Birch and Swinnerton-Dyer conjecture.

The expected number of points on an elliptic curve mod q is $q+1$. Let $a_q = q+1-\#E(\mathbf{F}_q)$ (for primes of good reduction, which is all but finitely many) and
$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_q \frac{q^s}{q^s - a_q + q^{1-s}}.$$

(Again, the term $q^2 - a_q + q^{1-s}$ is only correct for good primes.) The analytic rank of E, denoted r', is the order of the zero of $L(E,s)$ at $s = 1$.

Why is $s = 1$ special. To see one reason, note $L(E,1) = \prod q/(\#E(\mathbf{F}_q))$.

If $E(\mathbf{Q})$ infinite (i.e. $r > 0$), then typically $\#E(\mathbf{F}_q) \geq q+1$ so we'll guess that $L(E,1) = 0$ and $r' > 0$.

If $E(\mathbf{Q})$ finite (i.e. $r = 0$) then typically $\#E(\mathbf{F}_q) \leq q$ so we'll guess that $L(E,1) \neq 0$ and $r' = 0$.

Birch and Swinnerton-Dyer conjecture 1: $r = r'$.

Kolyvagin and Logachev: $r' = 0 \Rightarrow r = 0$ and $r' = 1 \Rightarrow r = 1$. $r' = 0,1 \Rightarrow \#Ш(\mathbf{Q},E) < \infty$.

Birch and Swinnerton-Dyer conjecture 2:
$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\Omega \cdot \prod c_p \mathrm{Reg} \# Ш(\mathbf{Q},E)}{(\#E(\mathbf{Q})_{\mathrm{tors}})^2}$$

(For deeper explanations of the following definitions, see Silverman's Arithmetic of Elliptic Curves). Ω is $\int_{E(\mathbf{R})} dx/(2y + a_1x + a_3)$ for a global minimal Weierstrass equation.

$c_p = \#E(\mathbf{Q}_p)/E^0(\mathbf{Q}_p)$ where $E^0(\mathbf{Q}_p)$ is the group of points with non-singular reduction when using a global minimal Weierstrass equation.

$$\mathrm{Reg} = \det \begin{bmatrix} \text{canonical} \\ \text{height} \\ \text{pairing} \\ \text{matrix} \end{bmatrix}$$

using a set of generators of the free-$\mathbf{Z}$-part of $E(\mathbf{Q})$.

The L-series is $\mathbf{Q}$-isogeny invariant. So the second BSD conjecture predicts the right hand side of the equation is also.

Cassels: If $Ш(\mathbf{Q}, E)$ is finite, then the right hand side is $\mathbf{Q}$-isogeny invariant.

Let $\phi/\mathbf{Q} : E \to E'$ and $\phi'/\mathbf{Q} : E' \to E$ be the dual isogeny with $\phi' \circ \phi = p$ (the multiplication-by-p map). The kernels of ϕ and ϕ (over $\overline{\mathbf{Q}}$) each have size p. Instead of defining ϕ-Selmer group, I will put it into an exact sequence.

$$0 \to E'(\mathbf{Q})/\phi E(\mathbf{Q}) \to S^{\phi}(\mathbf{Q}, E) \to Ш(\mathbf{Q}, E)[\phi] \to 0$$

Cassels: (Based on no conjecture):

$$\frac{\#S^{\phi'}(\mathbf{Q}, E')}{\#S^{\phi}(\mathbf{Q}, E)} = \frac{\#E'(\mathbf{Q})[\phi'] \cdot \Omega_E \cdot \prod c_{E,q}}{\#E(\mathbf{Q})[\phi] \cdot \Omega_{E'} \cdot \prod c_{E',q}}$$

How are these related to the p-Selmer group?

$$0 \to \frac{E(\mathbf{Q})[\phi]}{\phi'(E'(\mathbf{Q})[p])} \to S^{\phi'}(\mathbf{Q}, E') \to S^{p}(\mathbf{Q}, E')$$

$$\to S^{\phi}(\mathbf{Q}, E) \to \frac{Ш(\mathbf{Q}, E)[\phi]}{\phi(Ш(\mathbf{Q}, E')[p])} \to 0$$

How to find large $Ш[p]$ game plan:

Find E and E' for which $\prod c_q$ large and small, respectively. Then $S^{\phi'}(\mathbf{Q}, E')$ should be large. So $S^p(\mathbf{Q}, E')$ should be large also. Since MW-ranks tend to be small, and $\dim E(\mathbf{Q})_{\text{tors}}$ is small, that means $Ш(\mathbf{Q}, E')[p]$ should be large.

For $p = 5$, let $E_n : y^2 + (n+1)xy + ny = x^3 + nx^2$. Note $(0,0)$ has order 5. We have $E/\langle(0,0)\rangle \cong$

$E'_n : y^2 + (n+1)xy + ny = x^3 + nx^2 + (5n^3 - 10n^2 - 5)x + (n^5 - 10n^4 - 5n^3 - 15n^2 - n)$.

$\Delta_{E_n} = -n^5(n^2+11n-1)$. Let n be squarefree. Then $q|n \Rightarrow c_q = 5$. (q has split multiplicative reduction).

$\Delta_{E'_n} = -n(n^2 + 11n - 1)^5$. If $q|n$, then $c_q = 1$.

Proposition. For any positive integer m, there exists infinitely many integers n such that $\dim S^5(\mathbf{Q}, E'_n) \geq m$.

Corollary: For this family, MW ranks or $Ш[5]$'s are getting arbitrarily large.

No one would believe for this family that $Ш[5]$'s are bounded and what explains S^5's getting arbitrarily large is the MW-ranks getting arbitrarily large.

Proof. Let q_i be the ith prime. It follows from a sieving theorem (in Halberstam/Richert) that there are infinitely many primes q such that if

$$n = q \cdot \prod_{i=1}^{m+7} q_i, \text{ then } n^2 + 11n - 1 = \prod r_i^{\alpha_i}$$

where r_i prime and $\sum \alpha_i \leq 7$.

Now (dropping subscripts)

$$\frac{\#E'(\mathbf{Q})[\phi']}{\#E(\mathbf{Q})[\phi]} = \frac{1}{5}.$$

And

$$\frac{\Omega_E}{\Omega_{E'}} = 5.$$

For each $q|n$ we have $\frac{c_{E,q}}{c_{E',q}} = \frac{5}{1}$.

For each $q|n^2+11n-1$ we have $\frac{c_{E,q}}{c_{E',q}} = 1$ or $1/5$. Thus $\prod \frac{c_{E,q}}{c_{E',q}} = 5^l$ where $l \geq m+8-7$. So

$$\frac{\#S^{\phi'}(\mathbf{Q},E')}{\#S^{\phi}(\mathbf{Q},E)} = 5^{l'} \text{ where } l' \geq m+1.$$

Thus $\dim S^{\phi'}(\mathbf{Q},E') \geq m+1$ and $\dim S^5(\mathbf{Q},E') \geq m$.

$$\begin{array}{ccccccc} & & \leq 1 & & \geq m+1 & \Rightarrow & \geq m \\ 0 & \to & \frac{E(\mathbf{Q})[\phi]}{\phi'(E'(\mathbf{Q})[p])} & \to & S^{\phi'}(\mathbf{Q},E') & \to & S^p(\mathbf{Q},E') \end{array}$$

If anyone has an idea on how to show for this family, (or some appropriate subset of it) that the Mordell-Weil ranks are bounded ....