Shafarevich-Tate Groups of Higher Rank Elliptic Curves

William Stein

May 15, 2011

Abstract

These are the notes for a talk I gave at the conference on BSD in Cambridge, UK in May 2011. The talk is about some approaches to trying to prove something about finiteness of Shafarevich-Tate groups of elliptic curves over $\mathbb{Q}$ of rank at least 2.

1 Finiteness of $Ш(E/\mathbb{Q})$

Consider elliptic curves E and primes p. Let

$$X = \{(E,p) : \mathrm{rank}(E) \geq 2 \text{ and } Ш(E/\mathbb{Q})(p) \text{ is finite}\}. \tag{1.1}$$

Since Shafarevich and Tate conjectured that $Ш(E/\mathbb{Q})$ is finite for all E, we have the following much weaker but still open conjecture:

Conjecture 1.1. *X is infinite.*

Theorem 1.2 (M. Bhargava, Wei Ho, –)**.** *Assume one of the following conditions holds:*

1. *$\#Ш(E/\mathbb{Q})[2]$ is a perfect square for all E,*
2. *$\#Ш(E/\mathbb{Q})[3]$ is a perfect square for all E,*
3. *$\mathrm{rank}(E) \equiv r_{\mathrm{an}}(E) \pmod 2$ for all E.*

Then X is infinite.

Proof. Use the method of Bhargava applied to a certain family of curves with either 1 or 2 marked points. The details are substantial. □

Next suppose we fix a particular E and consider the set

$$X_E = \{p : Ш(E/\mathbb{Q})(p) \text{ is finite}\},$$

and the subset

$$X_E^0 = \{p : Ш(E/\mathbb{Q})(p) = 0\}.$$

If we wish to show that either of these sets is infinite, there are at least two directions in which we can go: (1) p-adic L-series and Iwasawa theory, and (2) Heegner point methods. First we consider p-adic methods.

1.1 p-adic Methods

Much theoretical and computational work on p-adic heights and Iwasawa theory has made explicit application of p-adic analogues of the Birch and Swinnerton-Dyer conjecture much more effective in particular cases. For example:

Theorem 1.3 (Coates-Sujatha-Liang)**.** *Let E be the CM elliptic curve $y^2 = x^3 - 82x$, which has rank $r = 3$. Then*

$$X_E^0 \supset \{p : p < 30000 \textit{ is prime}, \quad p \equiv 1 \pmod 4, \quad p \neq 41\}.$$

The following "theorem" is an enormous computation that is currently only 99.9999...% done.

Theorem 1.4 (Stein-Wuthrich [SW11])**.** *For every non-CM elliptic curve E with $N_E \leq 30000$ and $r_E \geq 2$, we have*

$$X_E^0 \supset \{p : 5 \leq p \leq 1000, \quad p \textit{ is good ordinary, and } \rho_{E,p} \textit{ is surjective}\}.$$

Let E be the rank 2 elliptic curve 389a, which is the unique curve of conductor 389. Using optimized code in Sage (and Psage), the calculation of the theorem takes a total of 4 minutes: 2 minutes to compute p-adic L-functions, and 2 minutes more to compute p-adic regulators. The above gives:

Proposition 1.5.

$$X_E^0 \supset \{5 \leq p < 1000 : p \neq 107, 599\}.$$

I personally see *no hope* that I can extend this p-adic strategy to prove something about infinitely many p, or even about infinitely many pairs (E, p). At least, from the above we know that the set X of Equation (1.1) has cardinality at least one million.

1.2 Heegner Points

The second approach is to use Heegner points, which is a strategy pioneered by Kolyvagin in the 1980s. The following theorem, which is stated in the abstract of one of his first papers on Euler systems, is notable because it does not rely on any other deep theorems such as Gross-Zagier, modularity, nonvanishing of twists, etc.; those deep results are needed only to verify the hypothesis of the argument are satisfied by any curve with analytic rank at most 1.

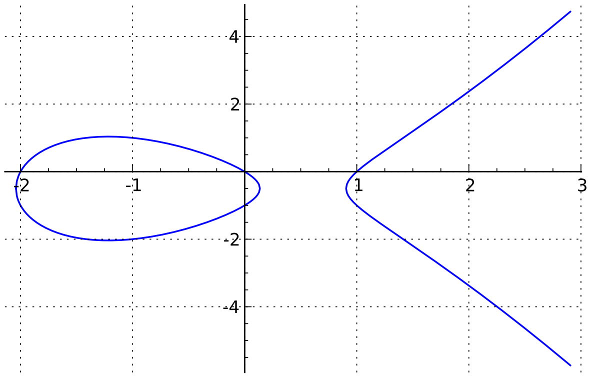
Theorem 1.6 (Kolyvagin)**.** *Let E be the elliptic curve $X_0(17)$. Then $\text{Ш}(E)$ is finite.*

The proof of this theorem involves constructing Heegner points on $X_0(17)$, and using them to define a set of elements of $\mathrm{H}^1(K, E[p^n])$ for every prime power p^n, and finally using the elements to bound $\text{Ш}(E)(p)$ for all p.

I have not yet given up all hope that someday we will be able to extend some argument like this to one specific elliptic curve of rank 2. The rest of this talk is about some details in this direction.

2 Heegner Points on 389a

For the rest of this article, let E be the elliptic curve 389a, which has rank 2 with generators $P = (-1, 1)$ and $Q = (0, 0)$.



The torsion subgroup of E is trivial; moreover, the mod p representations $E[p]$ are surjective, for all p. The curve E has modular degree 40:

$$\phi : X_0(389) \to E, \qquad\qquad \deg(\phi) = 40.$$

Also, let $K = \mathbb{Q}(\sqrt{-7})$, which has class number 1 and satisfies the Heegner hypothesis since $N = 389$ is split in K. We have $r_{\mathrm{an}}(E/K) = 3$. Fix one of the two choices $\mathcal{N}$ of primes over 389, so we have $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. The Heegner point

$$x_1 = (\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K) \in X_0(N)(K)$$

maps to 0 in E:

$$y_1 = \phi(x_1) = 0 \in E(K).$$

That y_1 is torsion follows from the Gross-Zagier formula, since $r_{\mathrm{an}}(E/K) > 1$. Since $y_1 = 0$, we are motivated to consider higher Heegner points y_p, which are indexed by the primes p that are inert in K, which are the primes congruent to $3, 5, 6 \pmod 7$:

$$\mathcal{I} = \{\text{ inert primes }\} = \{3, 5, 13, 17, 19, 31, 41, \ldots\}.$$

For any $p \in \mathcal{I}$, let $\mathcal{O}_p = \mathbb{Z} + p\mathcal{O}_K$ be the order of conductor p and $\mathcal{N}_p = \mathcal{N} \cap \mathcal{O}_p$. We have a Heegner point

$$x_p = (\mathbb{C}/\mathcal{O}_p, \mathcal{N}_p^{-1}/\mathcal{O}_p) \in X_0(N)(K_p)$$

where K_p is the ring class field associated to p (we also will sometimes write K_1 for the Hilbert class field of K, which is just K for our example); thus

$$\mathrm{Gal}(K_p/K_1) \cong (\mathcal{O}_K/p\mathcal{O}_K)^*/(\mathbb{Z}/p\mathbb{Z})^*$$

is cyclic of order $p+1$, and K_p is totally ramified at p. Finally, let

$$y_p = \phi(x_p) \in E(K_p).$$

Proposition 2.1. *The point y_p has infinite order for* all $p \in \mathcal{I}$.

Proof. Using Galois theory and that $\rho_{E,p}$ is surjective, one can show that $E(K_p)_{\mathrm{tor}} = 0$, so if y_p has finite order, then $y_p = 0$. Since $0 \in E(\mathbb{Q})$ the fiber $F = \phi^{-1}(0) \in X_0(N)(\overline{\mathbb{Q}})$ is closed under the action of $G_{\mathbb{Q}}$. Since $\phi(x_p) = 0$, we have that $x_p \in F$. But by CM theory, there is a simply transitive group action of $\mathrm{Gal}(K_p/K)$ on the $\mathrm{Gal}(K_p/K)$-orbit of x_p, so $\#F \geq p+1$. We thus have

$$p + 1 \leq \#\phi^{-1}(0) \leq \deg(\phi) = 40,$$

so $p \leq 39$.

To finish the proof we check that $y_p \neq 0$ for each inert prime $p \leq 39$, via either of the following two approaches:

1. **Numerical:** We use the classical complex analytic approach to numerically computing Heegner points and find, e.g., that
$$y_3 \sim (.63 - .73i, -.47 + 1.39i) \neq 0.$$
It takes only moments to compute all the other relevant y_p.

2. **Algebraic:** This method is vastly more complicated and much slower than the numerical method above, but it is purely algebraic and generalizes to allow us to later verify nontriviality of certain cohomology classes. The main idea is to simply reduce everything modulo a prime λ of $\overline{\mathbb{Z}}$ over an inert prime, and use rational quaternion algebras to make each object computable directly modulo λ, hence avoiding any characteristic 0 computations. Supposing, for example, that $\lambda \mid 5$, we have the following commuting diagram of abelian groups:
$$\begin{tikzcd}
 & X_0(N)(K_p) \arrow[dl] \arrow[dr] & \\
\mathrm{Div}(X_0(N)(\mathbb{F}_{5^2})^{\mathrm{ss}}) \otimes \mathbb{F}_3 \arrow[dr, "\pi"] & & E(K_p) \arrow[dl] \\
 & E(\mathbb{F}_{5^2}) \otimes \mathbb{F}_3 &
\end{tikzcd}$$
We compute the divisor group as the free abelian group on the set of right ideal classes in an Eichler order of level N in the rational quaternion algebra ramified at 5 and ∞. We then compute $\overline{x}_1 = x_1 \pmod{\lambda}$ by finding (using ternary quadratic forms as suggested by [JK10]) a right ideal class $[I]$ such that the left order R_I contains $\mathcal{O}_K$. We use that $T_p(\overline{x}_1) = \sum_{\sigma \in \mathrm{Gal}(K_p/K_1)} \sigma(x_p) \pmod{\lambda}$ to find all conjugates of x_p. We compute the map π in the diagram only up to scaling by an automorphism by using that it is $\mathbb{T}$-invariant and surjective (slight generalization of Ihara's lemma). For more details, see [Ste11].

□

Remark 2.2. For a generalize of the above proposition, see [JLS09, §3].

Though it is exciting that y_p has infinite order for all inert primes p, we must temper our enthusiasm with the fact that
$$\mathrm{Tr}_{K_p/K_1}(y_p) = a_p(E) y_1 = 0 \in E(K),$$
so that the y_p do not provide a direct source of nonzero elements of $E(K)$.

3 Selmer Elements for 389a: Kolyvagin's Idea

For every positive integer n, the (classical) n-Selmer group over a field M sits in the exact sequence
$$0 \to E(M)/nE(M) \xrightarrow{\delta} \mathrm{Sel}^{(n)}(E/M) \to \text{Ш}(E/M)[n] \to 0.$$

Also, we view $\mathrm{Sel}^{(n)}(E/M)$ as a subgroup of the first Galois cohomology group $\mathrm{H}^1(M, E[n])$.

For any prime $p \in \mathcal{I}$, let $n_p = \gcd(p+1, \#E(\mathbb{F}_p))$. By the Chebotarev density theorem, we can make n_p divisible by any power of any prime that we want. We have the following table of values of n_p for the first few p, and our elliptic curve 389a:

p	3	5	13	17	19	31	41	47	59	61	73	83	89	97
n_p	2	3	1	6	5	4	3	2	3	2	1	12	2	1

Fix any choice of generator σ_p of $\mathrm{Gal}(K_p/K_1)$, and let

$$z_p = \sum_{i=1}^{p} i\sigma_p^i(y_p) \in E(K_p). \tag{3.1}$$

We emphasize that z_p depends on the choice of generator. From z_p we obtain a class τ_p in the Selmer group as follows:

$$\begin{tikzcd}
{[z_p] \in (E(K_p)/n_pE(K_p))^{\mathrm{Gal}(K_p/\mathbb{Q})}} \arrow[r] & \mathrm{H}^1(K_p, E[n_p])^{\mathrm{Gal}(K_p/\mathbb{Q})} \\
 & \mathrm{H}^1(\mathbb{Q}, E[n_p]) \arrow[u, "\cong"'] \\
 & \tau_p \in \mathrm{Sel}^{(p)}(E/\mathbb{Q}) \arrow[u]
\end{tikzcd}$$

(If we replace σ_p by a different choice, then τ_p is scaled by a unit.) That τ_p is in the Selmer group, and not just H^1 uses that $r_{\mathrm{an}}(E/\mathbb{Q}) > 1$, as explained in [Gro91, Prop. 6.2].

Theorem 3.1 (Kolyvagin)**.** *If a prime ℓ divides $\mathrm{order}(\tau_p)$ for some inert prime p, then $\text{Ш}(E/\mathbb{Q})(\ell)$ is finite. If $\mathrm{ord}_\ell(\mathrm{order}(\tau_p)) = \mathrm{ord}_\ell(n_p) \geq 1$, then $\text{Ш}(E/\mathbb{Q})[\ell] = 0$.*

The following is implied by conjectures in [Kol91]. We emphasize that here we are only making a conjecture about the curve 389a.

Conjecture 3.2 (Kolyvagin)**.** *For every prime ℓ there is some $p \in \mathcal{I}$ with $\ell \mid \mathrm{order}(\tau_p)$.*

In fact, because $\text{Ш}(E/K)_{\mathrm{an}} = 1$, we expect more strongly that for every prime ℓ, there is a $p \in \mathcal{I}$ such that $\mathrm{ord}_\ell(\mathrm{order}(\tau_p)) = \mathrm{ord}_\ell(n_p) \geq 1$.

As evidence for the conjecture, the paper [JLS09] gave numerical evidence that τ_5 has order $n_5 = 3$; however, we emphasize that this was only evidence, since the method of that paper was not made rigorous (in theory it could have been wrong due to insufficient numerical precision). As more evidence, the paper [Ste11] proves, using a generalization of the algebraic construction of the proof of Proposition 2.1 above, that many classes τ_p are nonzero (for a few dozen triples (E, K, p), for various E); that computation also led to some interesting results about how the images of the classes τ_p are distributed in $\mathrm{Sel}^{(\ell)}(E/K)$, which will appear in a future paper of Stein-Weinstein.

We have the following table, where the three ? cases mean that the indicated computation is not 100% certain yet.

p	n_p	order(τ_p)	τ_p (up to scalar!)
3	2	2	$\delta(Q)$
5	3	3	$\delta(P+Q)$
13	1	1	$\delta(0)$
17	6	1?	$\delta(0)$
19	5	5	$\delta(P)$
31	4	4?	$\delta(Q)$
41	3	3	$\delta(P+2Q)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
419	35	35?	?

Applying Kolyvagin's Theorem 3.1, we have

Proposition 3.3. $\{3,5\} \subset X_E^0$.

This is much less impressive than Proposition 1.5, but there is (in my opinion) vastly more hope that an approach using Heegner points could eventually generalize to show that X_E is infinite.

4 A Higher Rank Gross-Zagier Formula

We continue to let E be the elliptic curve 389a, but allow the quadratic imaginary field K to vary. We require only that 389 split in K and $r_{\text{an}}(E/K) = 3$, so $D = -7, -11, -19, -20, -24, -35, \ldots$ are all allowed, but $D = -264$ is not (since $r_{\text{an}}(E/K) = 5$). Let $\ell \in \mathcal{I}$ be any inert prime and fix $\lambda \mid \ell$ a prime in $\overline{\mathbb{Z}}$. Let p be an inert prime with $\#E(\mathbb{F}_\ell) \mid n_p$. Recall the point z_p from (3.1), and let $\overline{z}_p$ be the image of z_p under the map $E(K_p) \to E(\mathbb{F}_{\ell^2})$ got by reduction modulo λ. In fact, z_p lands in $E(\mathbb{F}_\ell)$, because z_p is fixed by complex conjugation. Since $E(\mathbb{F}_\ell)/n_pE(\mathbb{F}_\ell) = E(\mathbb{F}_\ell)$, the point z_p does not depend on the choice of λ (though it does depend up to a unit scaling on the choice of σ_p). Let $\pi_\ell : E(\mathbb{Q}) \to E(\mathbb{F}_\ell)$ be the reduction modulo ℓ homomorphism.

Definition 4.1. Let

$$W_\ell = \pi_\ell^{-1}(\langle \overline{z}_p : \text{ all such } p\rangle) \subset E(\mathbb{Q}).$$

It is trivial that W_ℓ is a finite index subgroup of $E(\mathbb{Q})$.

I make the following conjecture about the subgroups W_ℓ, which would imply Conjecture 3.2.

Conjecture 4.2. *The set of indexes $\{[E(\mathbb{Q}) : W_\ell] : \ell \in \mathcal{I}\}$ is bounded.*

The following conjecture is then a higher-rank analogue of the Gross-Zagier formula:

Conjecture 4.3. *If W_ℓ has maximal index, then $[E(\mathbb{Q}) : W_\ell] = \sqrt{\#\text{Ш}(E/K)}$, and moreover*

$$\frac{L^{(3)}(E/K,1)}{3!} = \Omega_{E/K} \cdot \text{Reg}(W_\ell) \cdot \text{Reg}(E^D(\mathbb{Q})),$$

up to a power of 2. *Here $\Omega_{E/K} = 2\,\text{Vol}(\mathbb{C}/\Lambda)/\sqrt{|D|}$.*

"It is always a good idea to try to prove true theorems." – Bryan Birch

References

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, `http://wstein.org/papers/bib/gross-kolyvagins_work_on_modular_elliptic_curves.pdf`, pp. 235–256.

[JK10] Dimitar Jetchev and Ben Kane, *Equidistribution of Heegner Points and Ternary Quadratic Forms*, Preprint (2010), `http://arxiv.org/abs/0908.3905`.

[JLS09] Dimitar Jetchev, Kristin Lauter, and William Stein, *Explicit Heegner points: Kolyvagin's conjecture and non-trivial elements in the Shafarevich-Tate group*, J. Number Theory **129** (2009), no. 2, 284–302, `http://wstein.org/papers/kolyconj/`. MR 2473878 (2009m:11080)

[Kol91] V. A. Kolyvagin, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259, `http://wstein.org/papers/stein-ggz/references/kolyvagin-structure_of_selmer_groups/`. MR 93e:11073

[Ste11] William Stein, *Verification of kolyvagin's conjecture for specific elliptic curves*, Submitted (2011), `http://wstein.org/papers/kolyconj2/`.

[SW11] William Stein and Christian Wuthrich, *Computations About Tate-Shafarevich Groups Using Iwasawa Theory*, in preparation (2011), `http://wstein.org/papers/shark/`.