Kolyvagin's Conjecture and Congruences Between Modular Forms

William Stein

July 11, 2011

Abstract

We use congruences to give a method to verify Kolyvagin's conjecture for specific elliptic curves, and give a table of examples that illustrates our method. This approach gives the largest list of specific curves to date that satisfy the conjecture.

1 Introduction

In this paper we provide an approach using congruences to verify Kolyvagin's Conjecture A from [Kol91, pg. 255] for certain elliptic curves of higher rank. Let E be an elliptic curve over $\mathbb{Q}$, let K be an imaginary quadratic field such that each prime dividing the conductor $N = N_E$ of E splits in K, let ℓ be an odd prime that does not divide the discriminant of $R = \mathrm{End}(E_{\mathbb{C}})$, and assume that $G_{\mathbb{Q}} \to \mathrm{Aut}_R(\mathrm{Tate}_\ell(E))$ is surjective. Let

$$\tau_{\lambda,\ell^n} = \mathrm{res}^{-1}_{K_\lambda/K}(\delta_{\ell^n}(D_\lambda(\phi_E(x_\lambda)))) \in \mathrm{H}^1(K, E[\ell^n])$$

be the cohomology class defined in [Kol91] using Heegner points, where $x_\lambda \in X_0(N)(K_\lambda)$ is the Heegner point over the ring class field K_λ, the map $\phi_E : X_0(N) \to E$ is the modular parametrization, $D_\lambda \in \mathrm{Gal}(K_\lambda/K)$ is the Kolyvagin derivation operator, $\delta_{\ell^n} : E(K_\lambda) \to \mathrm{H}^1(K_\lambda, E[\ell^n])$ is the connecting homomorphism in Galois cohomology, and $\mathrm{res}_{K_\lambda/K}$ is the restriction map in Galois cohomology.

Conjecture 1.1 (Kolyvagin)**.** *There exists n and λ such that $0 \neq \tau_{\lambda,\ell^n}$.*

When $r_{\mathrm{an}}(E/K) = 1$, Conjecture 1.1 is an immediate consequence of the Gross-Zagier formula [GZ86] by taking $\lambda = 1$ and $\ell^n \nmid [E(K)_{/\,\mathrm{tor}} : \mathbb{Z}y_K]$. When $r_{\mathrm{an}}(E/K) > 1$, the conjecture was only known for a handful of explicit triples (E, K, ℓ), as explained in [Ste11].

The main idea of this paper is related to Mazur's notion of visibility of elements of Galois cohomology groups (see [CM00, AS02, AS05, JS07, Ste07]). We consider pairs (E, F) of elliptic curves of possibly different conductors with $E[\ell] = F[\ell]$, and study how the truth of Conjecture 1.1 for E and F are related. For example, we use congruences to verify Conjecture 1.1 for ???? pairs (E, ℓ) with E having rank 3 over K...

In Section 2 we prove a theorem that gives hypotheses on a pair of elliptic curves of the same conductor N under which one can deduce Kolyvagin's conjecture. Section 4 gives a table of examples that satisfy the hypothesis of the theorem. We thus obtain substantial new evidence in support of Kolyvagin's conjecture, using a third completely different approach to that of both [JLS09] and [Ste11].

The main contributions of this paper are:

1. Hypothesis under which Conjecture 1.1 for one curve implies it for another.
2. Improved techniques for efficiently computing with Heegner points.
3. Verification of nontriviality and visibility of many elements of Shafarevich-Tate groups of elliptic curves, and corresponding evidence for Conjecture 1.1.

2 Theorems

2.1 Preliminaries

Let M be a number field and $E, F \subset J$ two elliptic curves over M contained in a self-dual abelian variety J over M, and let $\phi_E : J \to E$ and $\phi_F : J \to F$ be the corresponding dual morphisms. Let $G = E \cap F$. Suppose that n is a positive integer such that $E[n] = F[n] = G[n]$ and $\gcd(n, \#G/n) = 1$, so $G \cong G[n] \oplus G'$ with $\gcd(\#G', n) = 1$. The equality $E[n] = F[n]$ induces an isomorphism $\mathrm{H}^1(M, E[n]) \cong \mathrm{H}^1(M, F[n])$. Let $\delta_{E,n} : E(M) \to \mathrm{H}^1(M, E[n])$ be the connecting homomorphism, and likewise for $\delta_{F,n}$.

Proposition 2.1. *For any $z \in J(M)$, we have $\delta_{E,n}(\phi_E(z)) = \delta_{F,n}(\phi_F(z))$.*

Proof. Let $A = (E + F)^\vee$, which we view as an optimal quotient of J via the map $\phi_A : J \to A$ that is dual to the inclusion $E + F \subset J$. We have an exact sequence

$$0 \to G \xrightarrow{x \mapsto (x,-x)} E \times F \to A^\vee \to 0.$$

The Weil pairing induces a self-duality $G^* \cong G$, so the dual exact sequence is

$$0 \to G \to A \to E \times F \to 0.$$

The corresponding long exact sequence is

$$0 \to G(M) \to A(M) \xrightarrow{f} E(M) \times F(M) \xrightarrow{\delta} \mathrm{H}^1(M, G) \to \mathrm{H}^1(M, A) \to \cdots$$

We have that $f(\phi_A(z)) = (\phi_E(z), \phi_F(z))$.

We have a canonical direct sum decomposition $G \cong G[n] \oplus G'$ with G' the subgroup of elements of G of order coprime to n. This decomposition induces an isomorphism $\mathrm{H}^1(M, G) \to \mathrm{H}^1(M, G[n]) \oplus \mathrm{H}^1(M, G')$, and we let π denote projection onto the first factor. We obtain the following commutative diagram with exact rows:

$$\begin{array}{ccccc}
J(M) & & & & \\
\downarrow{\scriptstyle \phi_A} & & & & \\
A(M) & \longrightarrow & E(M) \times F(M) & \longrightarrow & \mathrm{H}^1(M, G) \\
 & & \downarrow{\scriptstyle \delta_n} & & \downarrow{\scriptstyle \pi} \\
 & & \mathrm{H}^1(M, E[n] \times F[n]) & \xrightarrow{(x,y) \mapsto x - y} & \mathrm{H}^1(M, G[n])
\end{array}$$

Taking the northern route through the diagram, we see that z maps to 0 in $\mathrm{H}^1(M, G[n])$, since the middle 3-term row is exact. Taking the southern route, we see that z maps to $\delta_{E,n}(\phi_E(z)) - \delta_{F,n}(\phi_F(z))$, which proves that $\delta_{E,n}(\phi_E(z)) = \delta_{F,n}(\phi_F(z))$, as claimed. □

2.2 Elliptic Curves of the Same Conductor

Suppose E and F are optimal elliptic curves of the same conductor N, and suppose that K and ℓ are as in Conjecture 1.1; in particular, $E[\ell]$ is irreducible. Let Λ_{ℓ^n} be the set of all squarefree products $\lambda = p_1 \cdots p_k$ of primes p_i such that $\ell^n \mid \gcd(a_{p_i}(E), p_i + 1)$ for all i. By duality, we also view E and F as abelian subvarieties of $J = J_0(N)$.

Theorem 2.2. *If $E[\ell^n] = F[\ell^n]$ as subsets of J, then for all $\lambda \in \Lambda_{\ell^n}$, the two cohomology classes $\tau_{E,\lambda,\ell^n} \in \mathrm{H}^1(K, E[\ell^n])$ and $\tau_{F,\lambda,\ell^n} \in \mathrm{H}^1(K, F[\ell^n])$ are identified by the canonical isomorphism induced by the equality $E[\ell^n] = F[\ell^n]$ in J.*

Proof. Let $G = E \cap F \subset J$. By hypothesis, we have $E[\ell^n] \subset G$, but G could be much larger. Let $M = K_\lambda$. By

□

2.3 Elliptic Curves of Different Conductors

2.4 Abelian Varieties

In this section, we generalize the definition of Kolyvagin classes and the main results of the previous section to abelian varieties.

3 Algorithms

There are many ways to try to verify that XXX (hypo) holds for an elliptic curve F.

3.1 p-adic L-series

Using the algorithm of shark we can compute the quadratic twist L-series in time $|D|$ times how long it takes to compute the non-twisted L-series (so super fast once we have the modular symbols) and if the coefficient of T is a unit, then we conclude that $Ш[p] = 0$. Hopefully we do not have to use anything about the p-adic height being nondegenerate! I had a discussion with Wuthrich about this. Anyway, if not, we're set, and should get that Sha is trivial there, hence according to the structure them $m_\infty = 0$. This will in practice require thinking through details and writing much better code in PSAGE.

4 Tables

We make a table enumerating elliptic curves of rank ≥ 2 with conductor up to xxx, and for each list the elliptic curves F with $E[p] = F[p]$ for an odd prime p such that $\rho_{E,p}$ is surjective. For each such F, we list the first few D and $\mathrm{ord}_p([F(K) : \mathbb{Z}y_{F,K}])$.

To compute $\mathrm{ord}_p([F(K) : \mathbb{Z}y_{F,K}])$, we numerically compute the point $y_{F,K}$, find the unique element $w \in F(K)$ such that $pw = y_{F,K}$ (which must exist by Proposition **??**), then verify that w is not divisible by p using division polynomials.

E	$r(E)$	p	F	$r(F)$	$\sqrt{Ш(F)_{\mathrm{an}}}$	??
681c1	2	3	681b1	0	3	Heegner $D \geq -179$
1058c1	2	5	1058d1	0	5	-7
1102a1	2	3	1102d1	0	3	
1246c1	2	5	1246b1	0	5	
1611d1	2	3	1611a1			
1664n1	2	5	1664k1			
1701j1	2	3	1701a1			
1701j1	2	3	1701b1			
1701j1	2	3	1701f1			
1701j1	2	3	1701g1			
1913a1	2	3	1913b1			
1918c1	2	3	1918e1			
2006d1	2	3	2006e1			
2366e1	2	5	2366f1			
2429d1	2	3	2429b1			
2451d1	2	3	2451b1			
2451d1	2	3	2451c1			
2451d1	2	3	2451e1			
2482b1	2	3	2482e1			
2534g1	2	3	2534e1			
2534g1	2	3	2534f1			
2541c1	2	3	2541d1			
2574g1	2	5	2574d1			
...	2	..	. ...			
6552ba1	2	7	6552y1			
38088u1	?	11	38088t1			
60552c1	?	13	60552d1			

References

[AS02] A. Agashe and W. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185.

[AS05] Agashe Agashe and William Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur, `http://wstein.org/papers/shacomp/`. MR 2085902

[CM00] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR 1 758 797

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, `http://wstein.org/papers/bib/Gross-Zagier_Heegner_points_and_derivatives_of_Lseries.pdf`. MR 87j:11057

[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)

[JS07] Dimitar P. Jetchev and William Stein, *Visibility of the Shafarevich-Tate group at higher level*, Doc. Math. **12** (2007), 673–696, `http://wstein.org/papers/vishigher/`. MR 2377239 (2009c:11081)

[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

[Ste07] William A. Stein, *Visibility of Mordell-Weil groups*, Doc. Math. **12** (2007), 587–606, http://wstein.org/papers/vismw/. MR 2377241 (2009a:11128)

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