Verifying the Full Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves of Analytic Rank 0 or 1

Stephen Donnelly and Stefan Patrikis and William A. Stein and Michael Stoll*

July 21, 2004

Abstract

Suppose E is an elliptic curve over $\mathbf{Q}$ with conductor at most 87 and rank one or conductor at most 19 and rank zero. Then the full Birch and Swinnerton-Dyer conjecture is true for E. We prove this by ...

1 TODO

1. Define Ш – mention that it is torsion since $\mathrm{H}^1(\mathbf{Q}, E)$ is torsion.
2. Write up argument that $E(K)$ is a direct sum of $E(\mathbf{Q})$ and $E^K(\mathbf{Q})$ up to powers of 2 (i.e., up to tensoring with $\mathbf{Z}[1/2]$).
3. Summarize that Kolyvagin proves triviality of Sha for 23 curves in "On the MW and Sha for Weil Elliptic Curves". Verify that this proves BSD for these curves (by looking them up in Cremona).
4. Cremona's remark that says one should do a project like this. Where is it in his book?
5. Formalize how to use the Gross-Zagier theorem to reduce computing the index $I_K = [E(K) : \mathbf{Z}y_K]$ to computing only quantities associated to elliptic curves over $\mathbf{Q}$. Distinction between the two cases when $E/\mathbf{Q}$ has rank 0 and when it has rank 1.
6. Stoll can show triviality of Ш when there is a p-isogeny or $p = 2$.

*Some of these authors might not even know they are authors, so don't blame them for any mistakes below. Blame William Stein.

7. Mention Cremona-Mazur table of nontrivial Sha, and that we don't expect any nontrivial Sha for levels up to 500.

8. Write something about isogeny invariance.

9. Karl Rubin and other people have papers that prove full BSD up to power of 2 or 3 for CM elliptic curves of rank 0 or 1, maybe. I haven't read any of these papers in detail. Look at them, and list the ones of conductor up to 500 that they deal with. Deal with power of 2 as well. (E.g., MathSciNet...)

10. Write up in tex with more details Donnelly's argument, justify details more with precise reference, and attribute everything to Donnelly.

11. To what extent do we need to compute Heegner points?
    (a) Pete Green's package.
    (b) My package.
    (c) Cremona probably has PARI code.
    (d) ???

12. Domain of applicability of Kato's theorems on BSD. Just copy Theorem 0.3 from Grigor's kato3.dvi with appropriate reference. Will need Proposition 1.1 in Section 1.1.1 of Ribet-Stein.

13. Ultimate goal: Give a provably correct complete *algorithm* that takes as input an elliptic curve E over $\mathbf{Q}$ of analytic rank at most 1 and outputs either "yes" the BSD conjecture is true for E, or "no" it is not true for E and here is why. This should be an algorithm in the classical sense that it terminates on any valid input. Connection with old paper of Manin.

2 Introduction

Theorem 2.1. *Suppose E is an elliptic curve over $\mathbf{Q}$ of rank one with conductor at most bndone or rank zero and conductor at most* 19*. Then the full Birch and Swinnerton-Dyer conjecture is true for E.*

The rest of this paper is devoted to proving Theorem 2.1. By work of Cremona, Wiles et al., and Tate it suffices to prove that $\#\text{Ш}(E) = 1$ except for $\underline{681B}$ and $\underline{571A}$ where we must show that $\text{Ш}(E)$ has order 9 and 4, respectively.

3 BSD Theorems of Kolyvagin, Kato, et al.

3.1 Mazur-Rubin: Kolyvagin Systems

Let E be an elliptic curve. Suppose $p > 3$ and $\rho_{E,p} : G_{\mathbf{Q}} \to \mathrm{Aut}(E[p^\infty])$ is surjective.

4 Problems

1. **Surjective:** Give an algorithm that, given a non-CM elliptic curve $E/\mathbf{Q}$, determines the primes p such that $\rho_{E,p}$ is not surjective. Should be reasonable using Serre's paper, etc.

2. **Tamagawa Number Problem:** Consider the following rank 0 example:

   ```
   114C     5        4       [5]                            [20,1,1]         2C
   ```

   Our methods only proved that $\#Ш(E) \mid 25$, but in fact we have to show that $\#Ш(E) = 1$. Using Kato, and assuming that $r_E = 1$, an assumption we could check ..., we only get again that $\#Ш(E) \mid 25$, since $L_N(E,1)/\Omega_E$ is divisible by 25: we get one 5 from $L(E,1)/\Omega$ because of the Tamagawa number, and another 5 from the bad factor at 19, which is $1/(19 - (-1))$.

   If we use Kato as improved by Mazur and Rubin (see page 75 of "Kolyvagin Systems"), and if their $r_E = 1$, then we get that

   $$\mathrm{ord}_5(\#Ш(E)[5^\infty]) < \mathrm{ord}_5(L_N(E,1)/\Omega_E) = 2.$$

   Since $\mathrm{ord}_5(\#Ш(E)[5^\infty])$ is even, it follows that $5 \mid \#Ш(E)[5^\infty]$. **There is a problem with this: Mazur-Rubin assume that the representation on $E[5^\infty]$ is surjective, but I only know that the representation on $E[5]$ is surjective.** The problem isn't a problem because Lemma 3 on page IV-23 of Serre's *Abelian ℓ-adic representations and elliptic curves* shows that if $p \geq 5$ then $G_{\mathbf{Q}} \to \mathrm{Aut}(E[p])$ is surjective if and only if $G_{\mathbf{Q}} \to \mathrm{Aut}(E[p^\infty])$ is surjective.

   The programs in my directory /home/was/people/rubin/r$_e seemtosuggestthe 5 \mid$ r_E.

   Alternative idea, which doesn't work: In this case the Heegner point reduces to a point in the identity component, but $E(K)$ reduces to something of order divisible by 5. Thus if we could prove the following refinement of McCallum,Kolyvagin, then we could resolve this example:

Conjecture 4.1. *Suppose y_K has infinite order. Then $E(K)$ has rank 1 and $Ш(E/K)$ is finite. Further, if p is an odd prime which is unramified in F and such that $\rho_{E,p}$ is surjective, then*

$$\mathrm{ord}_p(\#Ш(E/K)) \leq 2\,\mathrm{ord}_p([E_0(K) : \mathbf{Z}y_K]),$$

where

$$E_0(K) := \ker\left(E(K) \to \bigoplus_v \Phi_{E,v}(\mathbf{F}_v)\right).$$

3. **Heegner:** My Heegner point program needs to be improved. Precision; maybe use best discriminant, which might not be the smallest (in abs. value). Look at Cremona's and Peter's. OR – just compute L-function and use mwrank to find what multiple it is of the generator. However, in using mwrank we need to know that we've really found a generator.

```
E = elliptic curve
G = GCD(H)
B = gcd(#(E(F_p)) : p < 1000, p odd and good)
H = odd part of indexes of Heegner points corr to first five quad imag fields
T = Tamagawa numbers

Thus Sha(E/Q) divides G^2*B^oo*2^oo.
```

E	G	B	H	T	verify	deg
11A	1	5	[1]	[5]	2C5TP	1
14A	1	6	[1]	[2,3]	2C3TP	1
15A	1	8	[1]	[2,4]	2C	1
17A	1	4	[1]	[4]	2C	1
19A	1	3	[1]	[3]	2C3TP	1
20A	skip					
21A	1	8	[1]	[4,2]	2C	1
24A	skip					
26A	1	3	[1]	[1,3]	2C3TP	2
26B	1	7	[1]	[7,1]	2C7TP	2
30A	1	12	[1]	[2,3,1]	2C3TP	1
33A	1	4	[1]	[2,2]	2C	
35A	1	3	[1]	[1,3]	2C3TP	
36A	1(skip)		[1]			

37B	1	3	[1]	[3]	2C3TP
38A	1	3	[1]	[1,3]	2C3TP
38B	1	5	[1]	[5,1]	2C5TP
39A	1	4	[1]	[2,2]	2C
40A	1(skip)		[1]		
42A	1	8	[1]	[8,1,1]	2C
43A					
44A	1				
45A	1				
46A	1	2		[2,1]	2C
48A	skip				
49A	skip				
50A	skip				
50B	skip				
51A	1	3		[3,1]	2C3TP
52A	skip				
54A					
54B					
55A	1	4		[2,2]	2C
56A					
56B					
57B	1	4		[2,2]	2C
57C	1	5		[10,1]	2C5TP
58B	1	5		[10,1]	2C5TP
62A	1	4		[4,1]	2C
63A	skip				
64A	skip				
66A	1	6		[2,3,1]	2C3TP
66B	1	4		[4,1,1]	2C
66C	?	10		[10,5,1]	2C5TP
67A	?	1		[1]	2C
69A	1	2		[2,1]	2C
70A	1	4		[4,2,1]	2C
72A	skip				
73A	1	2	[3,1]	[2]	2C
77B	1	3		[6,1]	2C3TP
77C	1	2		[1,2]	2C
114C	5	4	[5]	[20,1,1]	2C

```
C  = Cremona's mwrank (2-descent)
TP = Torsion point paper of Stoll (p-isogeny descent in presence of
     a rational point of order p).
```

5 Misc

Proposition 5.1. *Suppose E is an elliptic curve over $\mathbf{Q}$ and $p \geq 5$ is a prime such that E does not have a rational p-isogeny (equivalently, so that $E[p]$ is an irreducible* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *module). If K is a quadratic extension of $\mathbf{Q}$, then $E(K)$ has no p torsion.*

Proof. Suppose $z \in E[p]$ is nonzero. Because $E[p]$ is irreducible, the Galois closure L of $\mathbf{Q}(z)$ has Galois group isomorphic to the image H of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in $\mathrm{Aut}(E[p])$. Because of the Weil pairing, H has order at least $p-1$, so since $p \geq 5$, we see that L has degree ≥ 4. If $z \in E(K)$, then $K = L$ since K is Galois, and this contradicts that L has degree ≥ 4. $\square$

Conjecture 5.2. *Suppose $p \geq 5$ and there are no K-rational p-isogenies. Then* $\mathrm{H}^i(K(E[p])/K, E[p]) = 0$ *for $i = 1, 2$.*

6 11

Algorithm 6.1. Let E be an elliptic curve over $\mathbf{Q}$ of analytic rank at most 1. The following algorithm computes $\text{Ш}(E/\mathbf{Q})[p]$ for *all* primes p.

1. [Choose K] Choose the first quadratic imaginary field K that satisfies the Heegner hypothesis, is such that E/K has analytic rank 1, and whose discriminant is divisible by at least two primes. Let D be the discriminant of K. Note that the condition that D be divisible by two primes and that $(D, N_E) = 1$, implies that $\mathbf{Q}(E[p])$ is linear disjoint from K for all primes p. In fact, this is a necessary and sufficient condition, since if D is divisible by only one prime p, then because of the Weil pairing $\mathbf{Q}(E[p])$ will automatically contain K. [[Note: we'll need a density argument here to know that such a K exists.]]

2. [Find p-torsion] Decide for which primes p, there is a curve E' that is $\mathbf{Q}$-isogenous to E such that $E'(K)[p] \neq 0$. (We enumerate the $\mathbf{Q}$-isogeny class of E using [standard method]. Then for each E' in the $\mathbf{Q}$-isogeny class, compute the torsion subgroup of $E'(K)$ using [standard method], and see whether or not p divides its order.) Let B be the product of 2 and these primes.

3. [Root number] Compute the root number of E using the algorithm in [section blah of Cohen's Algorithms for ...].

4. [Compute Mordell-Weil]

   - If the root number is -1, compute $E(\mathbf{Q})$ (using ..., [possible because of [] implies that the algebraic rank equals the analytic rank since the analytic rank is at most 1]), and let z be a generator modulo torsion.
   - If the root number is $+1$, compute $E^D(\mathbf{Q})$, and let z be a generator modulo torsion.

5. [Height of Heegner point] Compute the height $h_K(y_K)$ relative to K of the Heegner point associated to K using the Gross-Zagier formula:

$$h_K(y_K) = \alpha \cdot L'(E/K, 1) = \begin{cases} \alpha \cdot L'(E_D/\mathbf{Q}, 1) \cdot L(E/\mathbf{Q}, 1) & \text{if } E \text{ has rank } 0 \\ \alpha \cdot L(E_D/\mathbf{Q}, 1) \cdot L'(E/\mathbf{Q}, 1) & \text{if } E \text{ has rank } 1, \end{cases}$$

where $\alpha = \frac{u^2\sqrt{|D|}}{\|\omega_E\|^2}$. Here u is half the number of units in the ring of integers of K and $\|\omega_E\|^2$ is the volume of $E(\mathbf{C})$, which is the volume of the period lattice $\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ associated to E and ω_E. The differential ω_E is the $c \cdot \omega$, where c is the Manin constant for E and ω is a Néron differential on E (we are assuming E is modular here, which is OK.) [[say something about computing $c\omega$... cite Section 2.14 of Cremona's book.]] If $\pi : X_0(N) \to E$ is the modular parametrization, then $\pi^*(\omega) = c \cdot \omega_E$, where $\omega_E = f(q)\frac{dq}{q} \in \mathrm{H}^0(X_0(N), \Omega_{X_0(N)})$ is the normalized cuspidal eigenform corresponding to E.

6. [Index of Heegner point] Compute

$$I_K = \sqrt{h_K(y_K)/h_K(z)} = [E(K) : \mathbf{Z}y_K],$$

up to primes that divide the B from step 2. Note that $h_K(z) = 2 \cdot h_{\mathbf{Q}}(z)$, and that we do *not* compute $E(K)$ or $\mathbf{Z}y_K$ directly, but instead compute the index using properties of heights.

7. [Annihilate Ш] Then $Ш(E/\mathbf{Q})[p] = 0$ for all primes $p \nmid B \cdot I_K$.

8. [p-descent] For each prime $p \mid B \cdot I_K$, do a p-descent and compute $Ш(E/\mathbf{Q})[p]$. (Note that this is likely not too difficult because there is a p-torsion point over K on a curve F that is $\mathbf{Q}$-isogenous to E. Ideas: If an isogeny from E to F has degree divisible by p, then E has a rational p-isogeny, which makes p-descent eiser. If an isogeny from E to F has degree coprime to p, then $Ш(F/\mathbf{Q})[p] \cong Ш(E/\mathbf{Q})[p]$, and F has a K-rational p-torsion point, so p-descent on F should be relatively easy.) To reduce the number of p for which one must do a p-descent, use several K.

[K exists by Murty-Murty or Bump-Friedberg-Hoffstein....] □

Remark 6.2. Possible different approach, which might be especially useful when $E(\mathbf{Q})$ has rank 0: Use half integral weight forms to compute the index $[E(K) : \mathbf{Z}y_K]$ as the coefficient of a modular form. This could be, in some sense (?), more efficient than directly computing $E^D(\mathbf{Q})$.

Example 6.3. We run through the algorithm for the "first" elliptic curve $E = X_0(11)$:

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

1. By Cremona's table, there is only a 5-isogeny, $t = 10$.

2. The Heegner hypothesis is that 11 splits completely in K, and the discriminant of K should be coprime to 11. Try $K = \mathbf{Q}(\sqrt{-1})$. Nope. Try $K = \mathbf{Q}(\sqrt{-2})$; yes, this works.

3. From the table, the sign is $+1$.

4. The twist of E by $D = -8$ has minimal model

$$y^2 = x^3 - x^2 - 41x + 199.$$

This is **704K2** in Cremona's tables. The Mordell-Weil group is generated by $(2, 11)$. (Should the following MAGMA code be believed? No.)

```
> G, f:=MordellWeilGroup(F);
> G;
Abelian Group isomorphic to Z
Defined on 1 generator (free)
> f(G.1);
(2 : 11 : 1)
```

5. Using `BG.gp`, we find that

$$L(E, 1) \sim 0.25384188059478054785841444442$$

and

$$L'(E^D, 1) \sim 1.8879135590194764767316140990$$

```
? \r BG
? e=ellinit([ 0, -1, 1, -10, -20 ]);
? ellanalyticrank(e)
Summing 7 a_n terms
Rank is even
L^(0)=0.25384188059478054785841444442
[0, 0.25384188059478054785841444442, 1.0000000777604993792773708900]
? e=ellinit([ 0, -1, 0, -41, 199 ]);
? ellanalyticrank(e)
Summing 53 a_n terms
Rank is odd
L^(1)=1.8879135590194764767316140990
[1, 1.8879135590194764767316140990, 0.18301909429552156871247861210]
```

Also

```
? e=ellinit([ 0, -1, 1, -10, -20 ])
? e.omega
[1.2692093042795534216887946170, \
    0.63460465213977671084439730848 + 1.4588166169384952293308896130*I]
```

```
? e.omega[1]*imag(e.omega[2])
1.8515436234559593177080067 12
? sqrt(8)/%
1.527604907016368150928945837
```

So We have $u = 1$, $D = -8$, and $\|\omega_E\| \sim 1.8515436234$, so

$$\alpha = \frac{u^2\sqrt{|D|}}{\|\omega_E\|} \sim 1.527604907016368150928945837$$

Finally,

$$h(y_K) \sim 0.7320764341087109483011606701$$

```
? 1.887913559019476476731614099 *  \
    0.2538418805947805478584144442 * \
        1.527604907016368150928945837
0.7320764341087109483011606701
```

6.
```
? e=ellinit([ 0, -1, 0, -41, 199 ]);
? 2*ellheight(e,[2,11])
0.1830190931500931069448448415
```

   We have

```
? 0.7320764341087109483011606701 / 0.1830190931500931069448448415
4.000000336076075243576248085
```

   Thus $I_K = 2$.

7. We conclude that $Ш(E/\mathbf{Q})[p] = 0$ for $p \neq 2, 5$.

8. Leave this to Stoll...

References

[Tat74] John T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206. MR 54 #7380