Computations About the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties

William Stein
http://modular.fas.harvard.edu

IHP MAGMA Workshop: October 7, 2004

Abstract

In this talk I will describe the Birch and Swinnerton-Dyer conjecture in the case of modular abelian varieties and how to use MAGMA to do computations with the quantities that appear in this conjecture. I will focus on how to do such computations in MAGMA, and will say little about the general results of the computations I've run over the years or theoretical results about the conjecture.

1 Newform Abelian Varieties A_f

They are specified by giving a newform $f = \sum a_n q^n \in S_2(\Gamma_0(N))$. Let $I_f = \mathrm{Ann}_{\mathbf{T}}(f)$. The connected component $A_f = J_0(N)[I_f]^0$ is an abelian variety over $\mathbf{Q}$. We have $\dim(A_f) = [\mathbf{Q}(a_2, a_3, \ldots) : \mathbf{Q}]$ and $\mathrm{End}(A_f) \otimes \mathbf{Q} = \mathbf{Q}(a_2, a_3, \ldots)$.

Listing 1.1 (Newform Abelian Varieties).

```
> J0 := JZero;    // personal customization...
> J := J0(37);
> S := CuspForms(37);  // defaults: k=2, trivial character
> N := Newforms(S); N;
[* [* q - 2*q^2 - 3*q^3 + 2*q^4 - 2*q^5 + 6*q^6 - q^7 + O(q^8) *],
   [* q + q^3 - 2*q^4 - q^7 + O(q^8) *] *]
> f := N[1][1];
> A_f := ModularAbelianVariety(f); A_f;
Modular abelian variety Af of dimension 1 and level 37 over Q
> E := EllipticCurve(A_f); E;
Elliptic Curve defined by y^2 + y = x^3 - x over Rational Field
```

Listing 1.2 (More Newform Abelian Varieties...).

```
> J := J0(389);         // J_0(389)
> D := Decomposition(J); D;   // contains the A_f's
[   Modular abelian variety 389A of dimension 1, level 389 and
    conductor 389 over Q,
    Modular abelian variety 389B of dimension 2, level 389 and
    conductor 389^2 over Q,
    Modular abelian variety 389C of dimension 3, level 389 and
    conductor 389^3 over Q,
    Modular abelian variety 389D of dimension 6, level 389 and
    conductor 389^6 over Q,
    Modular abelian variety 389E of dimension 20, level 389 and
    conductor 389^20 over Q
]
> EllipticCurve(D[1]);
Elliptic Curve defined by y^2 + y = x^3 + x^2 - 2*x over Rational Field
> EllipticCurve(D[2]);
 ... Runtime error in 'EllipticCurve': Argument 1 must have dimension 1.
```

Remark. BSD for all modular abelian varieties over $\mathbf{Q}$ $\iff$ BSD for all A_f with $f \in S_2(\Gamma_1(N))$.

2 The Birch and Swinnerton-Dyer Conjecture

Conjecture (BSD-rank): $r := \mathrm{ord}_{s=1} L(A_f, s) = \mathsf{rank}\, A_f(\mathbf{Q})$.

Conjecture (BSD-formula): Set $A := A_f$, for some f. Then

$$\frac{L^{(r)}(A,1)}{r!} = \frac{\prod_{p|N} c_p \cdot \Omega_A \cdot \mathrm{Reg}_A}{\#A(\mathbf{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}} \cdot \#Ш(A).$$

Here $\Longrightarrow\Longrightarrow$

1. $L(A,s) = \prod_\sigma \left(\sum_{n\geq 1} \frac{\sigma(a_n)}{n^s} \right)$
2. $\#A(\mathbf{Q})_{\mathrm{tor}}, \#A^\vee(\mathbf{Q})_{\mathrm{tor}}$ – torsion orders
3. c_p – Tamagawa numbers for primes $p \mid N$.
4. Ω_A – The integral $\int_{A(\mathbf{R})} \omega$.
5. Reg_A – regulator of A
6. $Ш(A) = \ker(\mathrm{H}^1(\mathbf{Q}, A) \to \oplus \mathrm{H}^1(\mathbf{Q}_v, A))$ – Shafarevich-Tate group

Motivating Problem. Given f, compute all quantities in this conjecture.

3 Computing The L-Series

Listing 3.1 (L-series of the elliptic curve factor).

```
> D := Decomposition(J0(389));
> E := D[1]; E;
Modular abelian variety 389A of dimension 1, level 389 and conductor 389 over Q
> L := LSeries(E);
> alpha, r := LeadingCoefficient(L,1,300);
> alpha;   --> 0.759316500292246790657626003l9
> r;  --> 2
> EE := EllipticCurve(E);
> AnalyticRank(EE);   // Watkins
2 0.7593000000
> Rank(EE);          // so BSD-rank true for E
2
```

Listing 3.2 (L-series of two-dimensional factor).

```
> D := Decomposition(J0(389));
> B := D[2]; B;       // dimension 2
Modular abelian variety 389B of dimension 2, level 389 and conductor 389^2 over Q
> L := LSeries(B);
> time alpha, r := LeadingCoefficient(L,1,300);
Time: 0.170
> alpha;
1.487184621319347115775638940885
> r;
2     // equals dim(B), so Kolyvagin-Logachev implies BSD-rank
```

Listing 3.3 (The twenty-dimensional simple factor!!).

```
> D := Decomposition(J0(389));
> A := D[5]; A;       // dimension 20 !!
Modular abelian variety 389E of dimension 20, level 389 and
conductor 389^20 over Q
> L := LSeries(A); L;
L(389E,s): L-series of Modular abelian variety 389E of dimension
20, level 389 and conductor 389^20 over Q
> alpha, r := LeadingCoefficient(L,1,300);      // takes a while
> alpha;
2300.74238082371353307813447937329 +  0.E-25*i
> r;
0         // so Kolyvagin-Logachev implies BSD-rank (=0)
> LeadingCoefficient(L,1,350);
2313.363547793384317135564620832928 +  0.E-25*i 0
```

(mention bug...)

4 Computing the Ratio $L(A,1)/\Omega_A$

When $r = 0$, (bsd-formula) is

$$\frac{L(A,1)}{\Omega_A} = \frac{\prod_{p|N} c_p}{\#A(\mathbf{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}} \cdot \#\text{Ш}(A).$$

For $A = A_f$, the command `LRatio(L,1)` computes the exact rational number

$$c \cdot \frac{L(A^\vee,1)}{\Omega_{A^\vee}} \in \mathbf{Q},$$

where c is the "Manin constant" of A, i.e., the index of $\mathrm{H}_1(\mathcal{A}^\vee, \Omega_{\mathcal{A}^\vee/\mathbf{Z}})$ in $\mathrm{H}_1(A, \Omega_{A/\mathbf{Q}}) \cap \mathbf{Z}[[q]]$. (Here $\mathcal{A}$ is the Néron model.)

Theorem (Agashe, Stein). We have (1) $c \in \mathbf{Z}$ and (2) that $p \mid c \implies p^2 \mid 4N$.

Conjecture (Agashe, Stein). $c = 1$ for all $A = A_f$.

Listing 4.1 (The L-Ratio).

```
> D := Decomposition(J0(389));
> [<Dimension(A), LRatio(LSeries(Dual(A)),1)> : A in D];
[ <1, 0>, <2, 0>, <3, 0>, <6, 0>, <20, 51200/97> ]
```

Remark. The BSD conjecture predicts that $L(A,1)/\Omega_A = L(A^\vee,1)/\Omega_{A^\vee}$, since $L(A,s) = L(A^\vee,s)$, $\#\text{Ш}(A) = \#\text{Ш}(A^\vee)$, and likewise for Reg_A and (I think!) the c_p.

5 The Order of the Torsion Subgroup

Torsion Multiple

If $p \nmid 2N$ then there is a natural injective homomorphism

$$A(\mathbf{Q})_{\rm tor} \hookrightarrow \mathcal{A}(\mathbf{F}_p).$$

Amazingly, it is straightforward to compute $\#\mathcal{A}(\mathbf{F}_p)$ and $\#\mathcal{A}^\vee(\mathbf{F}_p)$, using the "Eichler-Shimura" formula

$$\#\mathcal{A}(\mathbf{F}_p) = \#\mathcal{A}^\vee(\mathbf{F}_p) = F(p+1),$$

where F is the characteristic polynomial of $a_p = a_p(f)$. We thus obtain a multiple of $\#A(\mathbf{Q})_{\rm tor}$ and $\#A(\mathbf{Q})^\vee_{\rm tor}$.

Listing 5.1 (Torsion Multiples).

```
> D := Decomposition(J0(389));
> [<Dimension(A), TorsionMultiple(A,7)> : A in D];
[ <1, 1>, <2, 1>, <3, 1>, <6, 1>, <20, 97> ]
```

6 The Order of the Torsion Subgroup

Torsion Divisor

We obtain a divisor of $\#A(\mathbf{Q})_{\rm tor}$ using that differences of certain cusps lie in $J_0(N)(\mathbf{Q})_{\rm tor}$.

Listing 6.1 (Torsion Divisor).

```
> J := J0(389);
> D := Decomposition(J);
> [<Dimension(A), #RationalCuspidalSubgroup(Dual(A))> : A in D];
[ <1, 1>, <2, 1>, <3, 1>, <6, 1>, <20, 97> ]   // multiples of torsion for A^dual

> C := RationalCuspidalSubgroup(J) ;
> [<Dimension(A), #(C meet A)> : A in D];      // divisors of torsion order for A
[ <1, 1>, <2, 1>, <3, 1>, <6, 1>, <20, 97> ]
```

Thus $\#A(\mathbf{Q})_{\rm tor} = \#A(\mathbf{Q})^{\vee}_{\rm tor} = 1$, except for the A of dimension 20 where $\#A(\mathbf{Q})_{\rm tor} = \#A^{\vee}(\mathbf{Q})_{\rm tor} = 97$.

Remark. RationalCuspidalSubgroup computes the group generated by rational cusps, not the largest $\mathbf{Q}$-rational subgroup of the group generated by all cusps, which might sometimes give a better bound.

7 Tamagawa Numbers

When $p \mid N$ the Tamagawa number at p is $c_p = \#(\mathcal{A}_{\mathbf{F}_p}/\mathcal{A}^0_{\mathbf{F}_p})(\mathbf{F}_p)$.

- When $p \mid\mid N$, in my thesis I give an algorithm to compute c_p (sometimes only up to a power of 2). This uses Mumford-Tate uniformization (a higher-dimensional analogue of Tate curves), modular degree algorithm, and supersingular points or quaternion algebras.
- When $p^2 \mid N$, Lenstra and Oort proved that so if $\ell \mid c_p$ then $\ell \leq 2 \cdot \dim(A_f) + 1$ or $\ell = p$.

The **TamagawaNumber** command combines all this and returns a divisor d of c_p, an integer m some power of which is a multiple of c_p, and whether or not $d = c_p = m$.

Listing 7.1 (Tamagawa Numbers).

```
> J := J0(389);
> D := Decomposition(J);
> for A in D do print "dim =",Dimension(A)," tam =",TamagawaNumber(A,389); end for;
dim = 1  tam = 1 1 true
dim = 2  tam = 2 2 false
dim = 3  tam = 2 2 false
dim = 6  tam = 2 2 false
dim = 20  tam = 97 97 true
```

8 Tamagawa Numbers

Another Example...

Listing 8.1 (Tamagawa Numbers Example).

```
> J := J0(19*20);
> time D := Decomposition(NewSubvariety(J));   // takes a while (much overhead)
Time: 17.820
> [Dimension(A) : A in D];
[ 1, 1, 2, 2 ]
> A := D[#D]; A;  // dimension 2
> TamagawaNumber(A,2);
1 30 false
> TamagawaNumber(A,5);    // hard work!
3 3 true
> TamagawaNumber(A,19);
2 2 true
```

Listing 8.2 (Tamagawa Numbers Example (continued)).

```
> B := D[3];    // dimension 2
> TamagawaNumber(B,2);
1 30 false
> TamagawaNumber(B,5);
7 7 true
> TamagawaNumber(B,19);
2 2 true
> E := D[1];   // dim 1
> TamagawaNumber(E,2);     // uses Lenstra-Oort
1 6 false
> TamagawaNumber(E,5);     // uses my algorithm
1 1 false            // ** stupid -- should return true!!
> TamagawaNumber(E,19);    // uses my algorithm
2 2 false
> EE := EllipticCurve(E);
> TamagawaNumber(EE,2);    // uses Tate's algorithm
3
> TamagawaNumber(EE,5);
1
> TamagawaNumber(EE,19);
2
```

9 The Néron Real Volume Ω_A

The Néron volume is $\Omega_A = |\int_{A(\mathbf{R})} \omega|$, where $\mathrm{H}^d(\mathcal{A}, \Omega_{\mathcal{A}/\mathbf{Z}}) \approx \mathbf{Z}\omega$.

RealVolume on corresponding modular symbols space (!) computes $\Omega_{A^\vee}/c$, where c is the Manin constant.

Algorithm: Compute basis for $S_2(\Gamma_0(N), \mathbf{Z})[I_f]$, and integrate against basis of integral modular symbols.

Listing 9.1 (Real Neron Volume).

```
> D := Decomposition(J0(389));
> [<Dimension(A), RealVolume(ModularSymbols(A)[1],200)> : A in D];
[ <1, 4.980354644089219778568132200033753610666>,
  <2, 11.551729242815293051778318488 24>,
  <3, 34.8706655102786863021936976896 0>,
  <6, 244.7190660413415964243358490163 5>,
  <20, 4.1570866968444264694412485970 99> ]   <--- big 20-dim abvar. is small!
> EE := EllipticCurve(D[1]);
> 2*RealPeriod(EE);        // uses Gauss AGM (?)
4.98042512171011015064271558388460492031211636067914008011 00
```

10 Regulator of A

$$r = 0 \implies \mathrm{Reg}_A = 1$$

But when $r > 0$, so far I think nobody knows how to compute Reg_A without finding equations for A, finding explicit points, doing "descent", etc. See [Flynn-Leprévost-Schaefer-Stein-Stoll-Wetherell] for examples of this when $\dim(A) = 2$. This is perhaps hopeless when $\dim(A)$ is large. (If we assume $\#\text{Ш}(A) = 1$ and the BSD conjecture, we can often compute what Reg_A would be, which could be useful for numerical experiments.)

HOPELESS???

Question: Assume full BSD conjecture is true and $A = A_f$. Give an algorithm to decide whether $p \mid \#\text{Ш}(A)$. (When $\dim(A) = 1$, Manin proved one can do this, but the general case is unclear to me. I have an idea that uses congruences between modular forms.)

11 Computing Conjectural $\#Ш(A)$

Let $\#Ш(A)_?$ be BSD-conjectural order of $Ш(A)$. Using everything above, we can compute $l_p, u_p \in \mathbf{Z} \cup \{\infty\}$ such that

$$l_p \leq \mathrm{ord}_p(\#Ш(A)_?) \leq u_p.$$

For example, $l = 0$ and $u = \infty$! When $A \subset J_0(389)$ is the 20-dimensional factor, we find that $l_p = u_p = 0$ for all $p \neq 2, 5$. Also $l_2 = 11$ and $u_2 = 31$ and $\boxed{l_5 = u_5 = 2}$.

Computation. I computed *an* l_p and u_p for *all* 19608 A_f with $N \leq 2333$. I found 168 A_f of rank 0 such that $l_p > 0$ for some odd p. See Agashe-Stein, "Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties of Analytic Rank Zero" in this month's AMS Math. Comp. (For $J_1(p)$ computations, see Conrad-Edixhoven-Stein.)

12 Computing the Group $\text{Ш}(A)$

One can sometimes use Mazur's notion of **visibility** as a computational tool to construct a provably-nontrivial subgroup of $\text{Ш}(A)$.

Theorem 12.1 (Agashe-Stein). *Let A and B be abelian subvarieties of an abelian variety C over $\mathbf{Q}$ such that $A \cap B$ is finite and that A has rank 0. Suppose p is an odd prime such that $B[p] \subset A$ and p satisfies certain technical hypothesis (e.g., it doesn't divide any Tamagawa numbers). Then there is an inclusion*

$$B(\mathbf{Q})/pB(\mathbf{Q}) \hookrightarrow \text{Ш}(A).$$

Conjecture (Stein). If $A \subset J_0(N)$ is modular, then all of $\text{Ш}(A)$ can be **explicitly constructed** in terms of Mordell-Weil groups using appropriate generalizations of the above theorem and abelian varieties $B \subset J_0(NM)$ for multiples M of N.

Example of Constructing Elements of $Ш(A)$

Listing 12.2 (Sha of Order 5).

```
> D := Decomposition(J0(389));
> B := D[1];
> Rank(EllipticCurve(B));
2
> A := D[5];
> B5 := Kernel(nIsogeny(B,5));
> B5 subset A;
true
```

Thus $E(\mathbf{Q})/5E(\mathbf{Q}) \cong (Z/5\mathbf{Z})^{\oplus 2}$ is a subgroup of $Ш(A)$. This conclusion assumes no conjectures.

(Done – Questions?)