SAGE Progress Report: August 19, 2004

William Stein

August 19, 2004

Contents

1 Tables of Elliptic Curves over Number Fields

Jennifer Sinnott's project was initially to investigate torsion points on elliptic curves over number fields. It has morphed into a project to create large tables of elliptic curves over number fields. I checked the formated tables listed in Jennifer's directory, and they already contain 367000 curves over 13 quadratic fields, two cubic fields, and 2 quartic fields. She is only considering class number one fields, because MAGMA only contains an algorithm for computing the conductor when the class number is one. These tables are already posted online, and will likely be of interest to number theorists.

Each line of each table contains:

- the norm of the conductor,
- a Weierstrass equation of the form $y^2 = x^3 + ax + b$,
- the structure and order of the torsion subgroup,

- the j-invariant, and
- the conductor, as a principal ideal.

For example, the table for $\mathbf{Q}(\sqrt{-1})$ begins as follows:

```
25   [-2*a-1,0]       [10,1]  10 1728                     (-4*a+3)
25   [2*a-1,0]        [10,1]  10 1728                     (4*a+3)
64   [-1,0]           [2,4]   8  1728                     (8)
200  [-7,-6]          [2,4]   8  148176/25                (-10*a+10)
200  [-2,-1]          [4,1]   4  55296/5                  (-10*a+10)
256  [1,0]            [2,2]   4  1728                     (16)
324  [0,-1]           [6,1]   6  0                        (18)
392  [1,-2]           [4,1]   4  432/7                    (-14*a-14)
648  [6,-7]           [4,1]   4  2048/3                   (-18*a+18)
656  [4*a+1,4*a-2]    [2,1]   2  1/41*(-1458*a+24192)     (20*a+16)
656  [-4*a+1,-4*a-2]  [2,1]   2  1/41*(1458*a+24192)      (-20*a+16)
```

Jennifer is also investigating computing the first few traces of Frobenius of the reduction of the curve, which will allow us to divide the curves of given level up into very-likely-isogenous classes; these traces might also be useful for those studying L-series and Galois representations attached to elliptic curves over number fields.

2 Modular Abelian Varieties

Tseno Tselkov and I went through some algorithms I found last summer for explicitly computing with modular abelian varieties. We wrote descriptions of most of them down, and extended one of them. When the project started we didn't know how to find the minimal degree of an isogeny between two explicitly given simple modular abelian varieties, but now we do. With some polishing, what we wrote up will be suitable to submit to a journal. We also need to add a table that lists pairs (A_f, d) where A_f is attached to a newform and d is the minimal degree of an isogeny $A_f \to A_f^\vee$. We should run this for $\Gamma_0(N)$ and levels up to 1000, and $\Gamma_1(N)$ and level up to 100, where we stop any computation if it takes more than 1 hour.

Some questions arose from our work during the summer, which could form the basis for further investigation:

1. To what extent is it possible to enumerate every modular abelian variety defined over $\mathbf{Q}$ that is $\mathbf{Q}$-isogenous to an abelian variety A_f attached to a modular form? Surprisingly, this probably does not seem totally intractible, since one knows the exact endomorphism ring of the abelian variety, and there are results about the possible isogenous.

2. A related question is to efficiently compute the Shimura subgroup Σ of $J_0(N)$ efficiently. This the kernel of the natural map $J_0(N) \to J_1(N)$. By looking at Ling-Oesterle for a while, we came up with a recipe that involves the intersection

pairing on $\mathrm{H}_1(X_0(N), \mathbf{Z})$. Alternatively, the Shimura subgroup contains the kernels of the maps from $J_0(N)$ to higher level, so we could try to compute the union of a few of those kernels, and see if we gets the full Shimura subgroup. We know when we are done, because there is a simple formula for the order of Σ. However, this approach is slow because the higher level is an "order of magnitude" larger than N.

3. Find the minimal degree of a *polarization* on a simple modular abelian variety A, instead of just the minimal degree of an isogeny $A \to A^\vee$.

3 A Massive Table of Elliptic Curves

Baur was not around until recently, so we haven't yet made very much progress on this project. The goal is to take the hard-to-use Stein-Watkins table of about **250 million** elliptic curves over $\mathbf{Q}$, which took many months to compute, and do some of the following:

1. Make it easy (via a web-based interface) to get all curves from the data for a given range of levels, formated exactly as in Cremona's tables, with non-minimal twists included.

2. Extract statistics from the data:

   (a) Exactly how many curves are there in the database?

   (b) How many curves does Cremona find (up to level 25000) that we missed?

   (c) What is the largest size of an isogeny class?

   (d) How many curves have each rank?

   (e) Find pairs of curves as in Cremona-Mazur, where one curve has rank n, the other has rank $n+2$, and the traces of Frobenius for the two curves are the same.

4 Fibers over Points on Elliptic Curves of Rank 2

Andrei's original project was to find a satisfactory interpretation of points on elliptic curves of rank 2. This is one of the central open problems in the theory of elliptic curves, and as such it is very difficult. Nick Ramsey found the 2002 Ph.D. thesis *Formes modulaires et invariants de courbes elliptiques definies sur* $\mathbf{Q}$ by Christophe Delaunay, which discusses how in some cases to compute something about the fiber in $X_0(N)$ over a point $P \in E(\mathbf{Q})$, when E is the curve of conductor 389 and rank 2. The algorithm of the thesis, which involves an analytic iteration procedure, seemed "extremely nasty" to Andrei, and he did not pursue implementing it. Instead of continuing with this project, Andrei spent the second half of the summer working on the Birch and Swinnerton-Dyer conjecture project.

Table 5.1: The 4 optimal curves with nontrivial $Ш(E)_?$ and $N_E \leq 1000$

Curve	Equation	$Ш(E)_?$
571A	[0,-1,1,-929,-105954]	4
681B	[1,1,0,-1154,-15345]	9
960D	[0,-1,0,-900,-10098]	4
960N	[0,1,0,-20,-42]	4

5 The Birch and Swinnerton-Dyer Conjecture

5.1 Introduction

This project begins with the following lofty goal:

Goal 5.1. Prove the full Birch and Swinnerton-Dyer for every elliptic curve over $\mathbf{Q}$ of conductor at most 1000.

The BSD conjecture asserts that $\mathrm{ord}_{s=1} L(E,s) = \dim E(\mathbf{Q}) \otimes \mathbf{Q}$ and

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \prod c_p \cdot \mathrm{Reg}_E \cdot \#Ш(E)}{\#E(\mathbf{Q})^2_{\mathrm{tor}}}$$

The rank part is a theorem of Kolyvagin, when $\mathrm{ord}_{s=1} L(E,s) \leq 1$.

By Tate's theorem about isogeny invariance of the BSD conjecture, to achieve the goal it suffices to prove the conjecture for each optimal elliptic curve quotient of $X_0(N)$ for $N \leq 1000$. The rank part of the conjecture (when $\mathrm{ord}_{s=1} L(E,s) > 1$) has been verified by Cremona for curves with $N \leq 25000$, and all of the quantities in the conjecture, except for $\#Ш(E/\mathbf{Q})$ have been computed for curves of conductor ≤ 25000. Inspecting that data shows that Goal 5.1 amounts to proving that $Ш(E)$ is *trivial* for all but four optimal elliptic curves with conductor at most 1000. The four exceptions are given in Table 5.1.

We can prove that $Ш(E)$ is at least as big as expected for $571A$ using the method of Cremona-Mazur or a 3-descent, and expect to be able to show that $Ш(E)$ is at most of order 9 using the thoerem stated at the beginning of McCallum's article on Kolyvagin's work, and possibly also Kato's theorem. We can hopefully show the 2-primary part of $Ш(E)$ is exactly as predicted for the other three curves by computing $\mathrm{Sel}^{(4)}(E/\mathbf{Q})$ for each of them (note that the two curves of conductor 960 have rational 2-torsion, which might simplify this computation).

Another critical obstruction to Goal 5.1 is that nobody has proved that $Ш(E)$ is finite for *any* elliptic curve of rank greater than 1. Up to isogeny, there are 18 such curves with conductor at most 1000:

389A, 433A, 446D, 563A, 571B, 643A, 655A, 664A, 681C,
707A, 709A, 718B, 794A, 817A, 916C, 944E, 997B, 997C

For these curves we have no hope, using present techniques, to show that $Ш(E)$ is trivial, let alone finite. We make the following new goal:

Goal 5.2. Prove the full Birch and Swinnerton-Dyer for every elliptic curve over $\mathbf{Q}$ of conductor at most 1000 and rank zero or one. (The rank condition excludes the 18 curves of rank two.)

5.2 The Plan

There are 2463 optimal curves of conductor at most 1000. Of these, 18 have rank 2, which leaves 2445 curves. Our plan for computationally verifying the full BSD conjecture for these curves is as follows:

1. Prove a refinement of Kolyvagin's theorem, which bounds $Ш(E)$ for elliptic curves of (analytic) rank at most one. (Stefan will talk about this). Also read about Kato's theorem, which applies to E of rank 0.

2. Create an algorithm based on a refined Kolyvagin theorem and Kato's theorem that with the following input and output (Andrei's talk is about this):

   Input: An elliptic curve over $\mathbf{Q}$.
   Output: A square-free integer B such that if a p is a prime and $p \nmid B$, then $p \nmid \#Ш(E)$.

   Note that if E has (analytic) rank greater than one, then this algorithm outputs $B = 0$. When E has analytic rank at most one, it would be desirable that B only be divisible by primes such that it is reasonably easy to compute $\dim_{\mathbf{F}_p} \mathrm{Sel}^{(p)}(E/\mathbf{Q})$, e.g., when there is a rational p-isogeny; our current algorithm sometimes fails in this regard.

3. Implement the algorithm from step 2 in MAGMA, then run it on the curves of conductor at most 1000. One step of the algorithm is to find generators for the Mordell-Weil groups of certain elliptic curves of rank one. MAGMA does not include a command that finds such generators with certainty, so we record the curve along with the generators MAGMA claims are correct.

4. Prove correct the generators that MAGMA claims are correct, probably using a new program of Cremona for saturating Mordell-Weil groups.

5. Compute $\dim_{\mathbf{F}_2} \mathrm{Sel}^{(2)}(E/\mathbf{Q})$ for all E, in order to prove that $Ш(E)[2] = 0$ for most E, by using the exact sequence

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

6. Analyze the output from the previous steps to see how often a difficult bound on $Ш(E/\mathbf{Q})$ arises.

7. Prove a new theorem that allows us to show triviality of $\text{Ш}(E)$ for the curves with a difficult B. It appears that the one case in which $p \mid B$ but there is no rational p-isogeny and $\text{Ш}(E/\mathbf{Q})[p] = 0$ is when p divides some Tamagawa number and E has rank 1 (when E has rank 0, a theorem of Kato applies).
8. Prove correctness of the order of $\text{Ш}(E)$ for the four examples with nontrivial $\text{Ш}(E)$ (see discussion above).
9. Recode everything using only open source programs (e.g., C++, PARI), and rerun it to see that we get the same results.
10. Publish with complete source code that other people can read and run.

5.3 Status

We have completed steps 1–3, and run the program on all curves of conductor up to 25000, but stop the program for a given curve after a certain amount of time (so the data is incomplete). We have so far done nothing about step 4. Regarding step 5, we have computed $\dim \mathrm{Sel}^{(2)}(E/\mathbf{Q})$ using MAGMA for most curves of conductor up to 25000, and expect this computation to finish in a few days. We have not done steps 7–10 yet. See Section 5.4 for step 6.

Remark 5.3. Tony Scholl mentioned to me last week that even if E has rank 1 over $\mathbf{Q}$, over the cyclotomic $\mathbf{Z}_p$ extension $\mathbf{Q}_\infty$ of $\mathbf{Q}$ it has bounded rank, and Kato gives information about E over $\mathbf{Q}_\infty$, i.e., about the p-adic L-function of E.

5.4 Analysis

This is a snapshot of the situation as of August 18, at 2pm. I ran the first computation with each job limited to 2 minutes of real time, so a heavily loaded processor would stop prematurely. I then reran the jobs that failed, but now limiting to 30 minutes, and after 18 hours all levels up to 360 had rerun (these really do take a long time). Recall that we are considering all 2463 optimal curves of level up to 1000.

- There are 18 curves of rank greater than one.

```
was$ awk '$5>=2' 00001-00999-shabound  |wc -l
18
was$ awk '$5>=2' 00001-00999-shabound
389   A    1    0    2    2    0.38  [0,0] [0,0] [0,1,1,-2,0]
433   A    1    0    2    2    0.45  [0,0] [0,0] [1,0,0,0,1]
446   D    1    0    2    2    0.59  [0,0] [0,0] [1,-1,0,-4,4]
563   A    1    0    2    2    0.48  [0,0] [0,0] [1,1,1,-15,16]
571   B    1    0    2    2    0.43  [0,0] [0,0] [0,1,1,-4,2]
643   A    1    0    2    2    0.44  [0,0] [0,0] [1,0,0,-4,3]
655   A    1    0    2    2    0.47  [0,0] [0,0] [0,0,1,-13,18]
664   A    1    0    2    2    0.61  [0,0] [0,0] [0,0,0,-7,10]
```

```
681   C   1   0   2   2   0.46  [0,0] [0,0] [0,-1,1,0,2]
707   A   1   0   2   2   0.53  [0,0] [0,0] [0,1,1,-12,12]
709   A   1   0   2   2   0.45  [0,0] [0,0] [0,-1,1,-2,0]
718   B   1   0   2   2   0.43  [0,0] [0,0] [1,0,1,-5,0]
794   A   1   0   2   2   0.54  [0,0] [0,0] [1,0,1,-3,2]
817   A   1   0   2   2   0.39  [0,0] [0,0] [0,1,1,1,6]
916   C   1   0   2   2   0.54  [0,0] [0,0] [0,0,0,-4,1]
944   E   1   0   2   2   0.54  [0,0] [0,0] [0,0,0,-19,34]
997   B   1   0   2   2   0.47  [0,0] [0,0] [0,-1,1,-5,-3]
997   C   1   0   2   2   0.44  [0,0] [0,0] [0,-1,1,-24,54]
```

- There are 318 curves for which the computation still doesn't complete in the alloted time. For these curves, we set $B = 0$ and do not include them in the lists below.

  ```
  was$ grep timeout 00001-00999-shabound |wc -l
  318
  ```

- There are 1363 curves for which $B = 1$ (note that B incorporates the 2-descent computation).

  ```
  was$ awk '$4==1' 00001-00999-shabound |wc -l
  1363
  ```

- There are curves for which B is divisible by 2 and nonzero.

  ```
  was$ awk '$4%2==0 && $4 != 0' 00001-00999-shabound |wc -l
  10
  was$ awk '$4%2==0 && $4 != 0' 00001-00999-shabound
  278   B   1   6   0   -1   233.0 [6,6] [-15,-15]
  571   A   1   2   0   2    1.19  [14,2] [-7,-8]
  786   C   1   2   1   -1   73.2  [46,94] [-23,-47]
  804   B   1   6   1   -1   1.31  [6,6] [-95,-95]
  873   C   1   2   1   -1   43.8  [2,22] [-8,-11]
  886   C   1   2   0   -1   23.9  [14,2] [-7,-15]
  906   A   1   2   1   -1   3.84  [46,142] [-23,-71]
  954   E   1   6   1   -1   2.35  [282,42] [-47,-95]
  960   D   1   2   0   3    2.64  [142,2] [-71,-119]
  960   N   1   2   0   3    2.58  [142,2] [-71,-119]
  ```

  The 6th column is the dimension of the 2-selmer group, and the -1 means the computation failed, hence we can't rule it. The 3 that don't have -1 really do have nontrivial Ш of order 2. There are 14 curves where computation of the 2-selmer group failed for some reason:

```
was$ awk ’$6==-1’ 00001-00999-shabound |wc -l
14
was$ awk ’$6==-1’ 00001-00999-shabound
278   B    1    6    0    -1   233.0 [6,6] [-15,-15]
645   C    1    0    0    -1   0     [0,0] [0,0] timeout
658   A    1    0    0    -1   0     [0,0] [0,0] timeout
742   F    1    0    0    -1   0     [0,0] [0,0]  timeout
774   C    1    0    0    -1   0     [0,0] [0,0] timeout
777   B    1    0    0    -1   0     [0,0] [0,0] timeout
786   C    1    2    1    -1   73.2  [46,94] [-23,-47]
804   B    1    6    1    -1   1.31  [6,6] [-95,-95]
873   C    1    2    1    -1   43.8  [2,22] [-8,-11]
886   C    1    2    0    -1   23.9  [14,2] [-7,-15]
906   A    1    2    1    -1   3.84  [46,142] [-23,-71]
942   B    1    0    0    -1   0     [0,0] [0,0] timeout
954   E    1    6    1    -1   2.35  [282,42] [-47,-95]
978   C    1    0    0    -1   0     [0,0] [0,0]  timeout
```

- There are 94 curves for which $B \geq 11$.

```
was$ awk ’$4> 10’ 00001-00999-shabound |wc -l
93
```

- There are 39 curves for which $B \geq 19$.

```
was$ awk ’$4>=19’ 00001-00999-shabound  |wc -l
39
was$ awk ’$4>=19’ 00001-00999-shabound
348   D  1  21 1  1    1.35  [966,2982] [-23,-71]
350   F  1  33 1  1    1.96  [2046,66] [-31,-111]
462   E  1  21 1  2    3.75  [42,42] [-215,-215]      warning
470   F  1  21 1  1    0.99  [1302,42] [-31,-39]
494   D  1  39 1  1    2.11  [8034,9906] [-103,-127]
550   I  1  21 1  1    8.89  [3318,42] [-79,-391]     warning
574   I  1  21 1  1    3.67  [1302,42] [-31,-87]
600   E  1  21 1  1    1.69  [2982,42] [-71,-119]
618   F  1  77 1  1    1.72  [10934,154] [-71,-95]    warning
650   K  1  21 1  1    3.72  [8358,42] [-199,-231]    warning
670   D  1  19 1  1    1.79  [1178,38] [-31,-111]
674   C  1  31 1  1    1.75  [434,62] [-7,-39]
682   B  1  57 1  1    10.8  [30894,114] [-271,-415]  warning
702   K  1  21 1  1    3.2   [966,8022] [-23,-191]    warning
702   M  1  57 1  1    18.9  [29982,114] [-263,-623]  warning
706   B  1  23 1  1    0.84  [46,46] [-15,-15]
715   B  1  21 1  1    1.02  [42,42] [-51,-51]
```

```
730   J  1  21 1  1    1.47  [2982,3318] [-71,-79]
735   F  1  21 1  1    10.3  [10542,42] [-251,-404]   warning
762   E  1  33 1  1    1.65  [66,66] [-95,-95]        warning
786   J  1  21 1  1    1.13  [966,1974] [-23,-47]
786   L  1  35 1  1    1.55  [1610,4970] [-23,-71]    warning
804   D  1  21 1  1    1.51  [42,42] [-95,-95]
806   D  1  33 1  1    29.9  [17358,66] [-263,-703]   warning
854   D  1  21 1  1    2.95  [1974,7014] [-47,-167]
858   F  1  55 1  1    40.0  [110,110] [-959,-959]    warning
861   C  1  35 1  1    1.58  [70,70] [-20,-20]
870   F  1  35 1  2    9.21  [16730,30170] [-239,-431]warning
886   D  1  19 1  1    3.57  [266,38] [-7,-15]
894   E  1  23 1  1    1.71  [46,46] [-95,-95]
894   G  1  77 1  1    1.64  [154,154] [-95,-95]      warning
906   H  1  55 1  1    2.48  [7810,110] [-71,-143]    warning
910   H  1  51 1  1    5.64  [20298,31722] [-199,-311]
910   K  1  35 1  2    2.48  [70,70] [-159,-159]
918   H  1  33 1  1    4.97  [3102,17358] [-47,-263]  warning
975   I  1  21 1  1    2.22  [42,42] [-116,-116]      warning
986   E  1  35 1  1    3.31  [7210,70] [-103,-111]
988   B  1  39 1  1    81.5  [6162,8034] [-79,-103]
996   B  1  39 1  1    2.35  [5538,78] [-71,-143]
```

Note that in every case the rank (column 5) is 1.

- The largest B is 77.

```
was$ sort -n -r -k 4 00001-00999-shabound |more
894   G  1  77 1  1    1.64  [154,154] [-95,-95] warning
618   F  1  77 1  1    1.72  [10934,154] [-71,-95] warning
```

- The largest prime divisor of a B is 31.

```
was$ awk ’$4%17==0 && $4 != 0’ 00001-00999-shabound |wc -l
5
was$ awk ’$4%19==0 && $4 != 0’ 00001-00999-shabound |wc -l
4
was$ awk ’$4%23==0 && $4 != 0’ 00001-00999-shabound |wc -l
2
was$ awk ’$4%29==0 && $4 != 0’ 00001-00999-shabound |wc -l
0
was$ awk ’$4%31==0 && $4 != 0’ 00001-00999-shabound |wc -l
1
was$ awk ’$4%37==0 && $4 != 0’ 00001-00999-shabound |wc -l
0
```

```
was$ awk '$4%43==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%47==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%53==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%59==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%61==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%67==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%71==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%73==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%31==0 && $4 != 0' 00001-00999-shabound
674   C  1  31 1  1    1.75  [434,62] [-7,-39]
```

5.5 A Potentially Serious Obstruction

We next list the most difficult curves, from our point of view. These are the curves with E of rank 1 such that B is divisible by a prime $p \geq 5$ for which no element of the $\mathbf{Q}$-isogeny class of E has a K-rational point of order p, i.e., such that divisor p of B also divides $[E(K)_{/\,\mathrm{tors}} : \mathbf{Z}y_K]$ for the two K we chose. We consider $p \geq 5$, because it is standard to do a p-descent in general for $p = 2, 3$, and we consider only rank 1, since when the rank is 0 Kato's theorem gives extremely strong results independent of the index.

There are 176 such curves in our data, for levels ≤ 1000, and for which our computation of Heegner points succeeded, and these are displayed below. The notation of the table is (E, n), where n is the greatest common divisor of the odd parts of the two indexes $[E(K)_{/\,\mathrm{tors}} : \mathbf{Z}y_K]$. Again, we emphasize that every curve below has rank 1.

141A1	7
190A1	11
214A1	7
238A1	7
258C1	5
262A1	11
274A1	7
280B1	15
285A1	5
286B1	13
302C1	5
303A1	7
309A1	5
318D1	11
322D1	5
326B1	5
346B1	7
348D1	21
350F1	33
354F1	7
357D1	7
362B1	7
364A1	15
366G1	5
381A1	5
408D1	5
414D1	5
418B1	13
430B1	5
430D1	75
434D1	5
446B1	7
458B1	5
462E1	21
470C1	7
470F1	21
474B1	5
490G1	5
494D1	39
497A1	5
498B1	5
506D1	5
506F1	13
522I1	5

522J1	13
530C1	5
542B1	7
550I1	21
550J1	11
551C1	7
558F1	5
558G1	7
560E1	5
561B1	5
574G1	11
582C1	5
585I1	7
594D1	5
598D1	17
600E1	21
605A1	15
605C1	5
608E1	5
615B1	7
618D1	5
618E1	5
618F1	77
620B1	15
622A1	7
629D1	5
642C1	13
650K1	21
658E1	11
665A1	5
666D1	5
666E1	13
670A1	11
670C1	5
670D1	19
672B1	15
674C1	31
678C1	7
681E1	5
682B1	57
690E1	5
696C1	5
700D1	15
702K1	21

702L1	15
702M1	57
705B1	15
705E1	5
706B1	23
706D1	5
710B1	17
710C1	7
715B1	21
726E1	5
726G1	15
730I1	7
730J1	63
735F1	21
738E1	5
738F1	11
742E1	5
742G1	5
762D1	5
762E1	33
777E1	5
777G1	5
786H1	7
786J1	21
786L1	35
794C1	5
798C1	5
798D1	5
798G1	15
804D1	21
806C1	5
806D1	33
814B1	5
816I1	11
817B1	5
822D1	5
830C1	5
831A1	5
834F1	7
842B1	13
850D1	7
850L1	7
854D1	21
858F1	55

861B1	17
861C1	35
861D1	5
870F1	35
874D1	5
876B1	15
880G1	5
886D1	19
886E1	5
890F1	13
894E1	23
894F1	5
894G1	77
897D1	15
897E1	5
901E1	15
906H1	55
910F1	55
910G1	5
910H1	51
910K1	35
912H1	5
918H1	33
920A1	15
924B1	15
924E1	15
930D1	7
930H1	15
933B1	11
938B1	5
939C1	5
942C1	5
954H1	7
954I1	5
954J1	17
974H1	15
975I1	21
975J1	5
978F1	11
978G1	7
986E1	35
987E1	15
988B1	39
996B1	39

If we assume the BSD conjecture, then the formulas at the beginning of McCallum's article suggest that in each case one of the following occurs:

1. We did not choose enough K's.

2. If p is a prime that divides the gcd of indexes, then p divides some Tamagawa number c_ℓ of E.

In the latter case all of the points P_n of McCallum's article are "divisible by p, in the sense described in that article, and Kolyvagin's method doesn't seem to yield the precise bound we require.

We now consider the first examples in more detail. The curve E called 141A and given by $y^2 + y = x^3 + x^2 - 12x + 2$ has rank 1, conductor $141 = 3 \cdot 47$, has $c_3 = 7$, and using all the results I know toward BSD we only see that Ш(E) is finite of order a power of 7. The curve E is isolated in its isogeny class. The modular degree of E is divisible by 7. The Jacobian $J_0(47)$ is of rank 0 and is simple of dimension 4, and we find that $E[7]$ sits in the old subvariety of $J_0(3 \cdot 47)$. Thus my hope is that proving something about the Shafarevich-Tate group of simple rank 0 abelian variety $J_0(47)$ will imply something about Ш$(E)[7]$. Also we have $L(J_0(47), 1)/\Omega = 16/23$, so BSD predicts that the Selmer group of $J_0(47)$ at 7 is trivial (since we know $c_{47} = 23...$).

Question 5.4 (Gross). In your data, do all the Tamagawa numbers divide the index of the Heegner point?

I don't have things setup so I can trivially check whether all these indexes also come from Tamagawa numbers. However, I just tried three more examples:

- 190A1: We have $190 = 2 \cdot 5 \cdot 19$ and $c_2 = 11$. There is a 4-dimensional abelian variety over rank 0 and level 95 with Ш[11] trivial that contains $E[11]$.

- 214A1: We have $214 = 2 \cdot 107$ and $c_2 = 7$. There is a rank 0 simple abelian variety over level 107 and dimension 7 that contains $E[7]$.

- 674C1: We have $214 = 2 \cdot 337$ and $c_2 = 31$. For this one, there is a rank 0 simple abelian variety of level 337 and dimension 15 that contains $E[31]$ and according to BSD has trivial Ш[31].

Is there a connection with Gross's recent work on level raising, Heegner points, and Selmer group? First, he has the hypothesis $p \not\equiv 1 \pmod{\ell}$. For the 141A example, $p = 3$ and $\ell = 7$, which is OK. For the 190A, 214A, and 674A examples, $p = 2$ and $\ell \geq 5$ is odd, so in each case that hypothesis is satisfied.

5.6 Some Other Questions (for Dick Gross)

1. $\int \omega \wedge \overline{(i\omega)} < 0$? *I think it's right, but maybe not...*

2. Density $\alpha x/\log(x)$. What is α? *I don't know.*

3. Connection between level changing idea (Section 5.5) and your (Gross's) research from one year ago. *My was sort of the other direction, but it seems similar.*

4. CM curves: Unramified in F. Rank 0, OK; Rank 1, only get p that split. *Yes. Ben Howard adds that in principal one could use the Mazur-Rubin machinery in the case of Kolyvagin's Euler system to prove this in rank 1, but nobody has done this. In Ben Howard's thesis he pushes through this approach, but avoids Tamagawa numbers (for simplicity), and does some Iwasawa theory (for complexity).*

5. In the Gross-Zagier formula, is it necessary that $(D, 2N) = 1$? *No. We only wrote it up that way so that D would be square free. Ben Howard adds that published work of Zhang should already deal with the case that D is even.*