Math 583: Project Set 1

Spring 2007, University of Washington

March 28, 2007

1. **Robert Bradshaw:** 2-*descent on elliptic curves.* Do the following, in some order (not necessarily linearly).

   (a) Learn something about how 2-descent works, e.g., by reading Silverman, Cremona, etc., or even by looking at this Harvard senior thesis that I advised: `http://www.wstein.org/projects/danielle_li.pdf/`.

   (b) SAGE contains two distinct approaches to descent – the invariants method described in Cremona's book and implemented in mwrank, and the algebraic method as implement by Denis Simone. Look at the algebraic method's code in SAGE: `SAGE_ROOT/data/extcode/pari/simon/` and `SAGE_ROOT/devel/sage/sage/schemes/elliptic_curves/gp_simon.py`.

   (c) Finish the wrapper of Simon 2-descent so it works over number fields instead of just over $\mathbb{Q}$. (Your knowledge of French will help.)

2. **Robert Miller:** *Graphs associated to elliptic curves.* There are at least two very different extremely interesting graphs associated to elliptic curves. I'll tell you about one in this project, and about the other, which involves congruences between modular forms, and is much more subtle – but still easy to describe, in a later project.

   (a) Read the definition of *isogeny* in a book on elliptic curves. (It's just a homomorphism of finite degree between elliptic curves.) By the way, it's a deep theorem of John Tate that the BSD conjecture is true for a curve E if and only if it is true for any curve F that is isogenous to E.

   (b) Try this in SAGE:

   ```
   sage: e = EllipticCurve('11a')
   sage: e.isogeny_class()
   (...,
   [0 5 5]
   [5 0 0]
   [5 0 0])
   ```

   Note that the second part of the output is a labeled graph (with three vertices), which desribes the *isogeny class* of the elliptic curve 11a. The labels are the degrees of the isogenies.

   (c) Create a command in SAGE (in the `ell_rational_field.py` file) called `isogeny_graph()` that calls isogeny class and uses it to construct the isogeny graph and outputs that.

(d) Conjecturally classify all possible graphs that occur with and without the labelings. Also, what automorphism groups appear, with and without labelings? You can enumerate the first few thousand elliptic curves like this:

```
sage: for e in cremona_optimal_curves(range(1,50)):
...   print e
```

Important Note: Tom Boothby did this last summer, so you should compare notes with him.

3. **Dustin Moody:** *Computing* $\#E(\mathbb{F}_p)$.

   (a) Learn something about algorithms for computing $\#E(\mathbb{F}_p)$ for p *small*, e.g., from Cohen's number theory book. Small means $p < 10^{15}$, say.

   (b) Setup and start a distributed computation that creates a table, easily usable from SAGE (or any software), of the Fourier coefficients a_p for $p < 10^7$, for every elliptic curve over $\mathbb{Q}$ of conductor up to 5077. Such a table currently doesn't exist, would be very useful for some computations I'm doing with Barry Mazur right now, will be useful for the second graph project that Robert Miller will do, and is generally useful for investigations into the BSD conjecture. This table should have rows like

   ```
   11a -2 -1 1 -2 1 4 -2 0 -1 0 ...
   ```

   I hope computing all a_p for $p < 10^7$ is reasonable. This computation could be done almost entirely using the gp command `ellan`, or the SAGE command `anlist(n, pari_ints=True)`. However, you'll need to break the computation up into groups in order to take advantage of parallel computation (e.g., that `sage.math.washington.edu` has 16 CPU cores).

4. **Ralph Greenberg:** I used David Harvey's amazingly fast implementation of computation of p-padic regulators to compute the regulator of the rank 2 curve 389a for each good ordinary prime $p \leq 62591$. There is exactly one prime p such that $\mathrm{ord}_p(\mathrm{Reg}_p(E)) > 0$, and it's $p = 16231$, where the regulator is

$$1930 \cdot 16231 + 2051 \cdot 16231^2 + \cdots$$

Can you think of any interesting questions related to the BSD conjecture (or its p-adic analogues) that one might investigate in this case?