Modular Elliptic Curves over $\mathbf{Q}(\sqrt{5})$

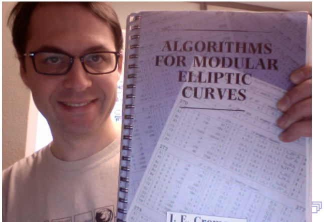
William Stein (joint work with Aly Deines, Joanna Gaski)

October 2010

The Problem

Cremona's Book over $\mathbf{Q}(\sqrt{5})$

Create a document like Cremona's book, but over the real quadratic field $F = \mathbf{Q}(\sqrt{5})$. It will contain a table of every (modular) elliptic curve over F of conductor $\mathfrak{n}$ such that $\mathrm{Norm}(\mathfrak{n}) \leq 1000$, along with extensive data about every such curve (much more than what is in Cremona's book – info like Robert Miller is computing about elliptic curves over $\mathbf{Q}$, which is relevant to the BSD conjecture). Then go up to norm *one hundred thousand* or more!



Conductor

What is the "Conductor" of an Elliptic Curve?

If E, given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ is a Weierstrass equation for an elliptic curve over F, it has a discriminant, which is a polynomial in the a_i:

$$\Delta = -a_1^4a_2a_3^2 + a_1^5a_3a_4 - a_1^6a_6 - 8a_1^2a_2^2a_3^2 + a_1^3a_3^3 + 8a_1^3a_2a_3a_4 + a_1^4a_4^2 - 12a_1^4a_2a_6 - 16a_2^3a_3^2 + 36a_1a_2a_3^3 + 16a_1a_2^2a_3a_4 - 30a_1^2a_3^2a_4 + 8a_1^2a_2a_4^2 - 48a_1^2a_2^2a_6 + 36a_1^3a_3a_6 - 27a_3^4 + 72a_2a_3^2a_4 + 16a_2^2a_4^2 - 96a_1a_3a_4^2 - 64a_2^3a_6 + 144a_1a_2a_3a_6 + 72a_1^2a_4a_6 - 64a_4^3 - 216a_3^2a_6 + 288a_2a_4a_6 - 432a_6^2$$

Among all models for E, there are some that simultaneously minimize $\mathrm{ord}_{\mathfrak{p}}(\Delta)$ for all primes $\mathfrak{p}$: the *minimal discriminant*.
Reducing such a model modulo $\mathfrak{p}$ will give either an elliptic curve, or a nodal cubic (e.g., $y^2 = x^2(x-1)$), or a cuspidal cubic (e.g., $y^2 = x^3$). The *conductor* of E is the ideal

$$\mathfrak{n} = \prod_{\mathfrak{p}\mid\Delta} \mathfrak{p}^{f_{\mathfrak{p}}}$$

where $f_{\mathfrak{p}} = 1$ if reduction is nodal, and $f_{\mathfrak{p}} \geq 2$ if cuspidal...

A Concrete Problem

Concrete Problem

What is the "simplest" (smallest conductor) elliptic curve over $F = \mathbf{Q}(\sqrt{5})$ of rank 2? See my recent NSF grant proposal for motivation, at `http://wstein.org/grants/2010-ant/`.

To the best of my knowledge, this is open. I asked Lassina Dembele, who has a big systematic tables of curves over F of *prime* conductor with norm ≤ 5000 and he didn't know of any

So we still don't know!

Upper Bound

The following search finds the first curve over $\mathbf{Q}(\sqrt{5})$, which has all $a_i \in \mathbf{Q}$, with rank 2:

```
for E in cremona_optimal_curves([1..100]):
    r = rank_over_F(E)
    print E.cremona_label(), r
    if r == 2: break
```

It finds **61a**:

$$E : \qquad y^2 + xy = x^3 - 2x + 1,$$

for which $E(\mathbf{Q})$ and $E^5(\mathbf{Q})$ both have rank 1.
The norm of the conductor $\mathfrak{n}$ over F is $61^2 = 3721$.

Naive Enumeration

In 2004 I had Jennifer Sinnot (a Harvard undergrad) make big tables of elliptic curves (by just running through a_i) over various quadratic fields, including $F = \mathbf{Q}(\sqrt{5})$. See

http://wstein.org/Tables/e_over_k/

```
Norm(N)  [a4,a6]        Torsion         j-invariant             Conductor N
320 [-7,-6]         [2,4] 8 148176/25 (-8*a)
320 [-2,1]          [2,4] 8 55296/5 (-8*a)
1024 [-2*a+6,0]      [2,1] 2 1728 (32)
1024 [-1,0]          [2,2] 4 1728 (32)
1024 [4,0]           [4,1] 4 1728 (32)
1280 [-7,6]          [2,4] 8 148176/25 (-16*a)
1280 [-a-3,-a-2]     [2,2] 4 55296/5 (-16*a)
1280 [-a-3,a+2]      [2,2] 4 55296/5 (-16*a)
1280 [-2,-1]         [2,2] 4 55296/5 (-16*a)
1296 [0,1]           [6,1] 6 0 (36)
...
```

Joanni Gaski is doing her masters thesis right now at UW on extending this...

Dembele's Ph.D. Thesis $\sim$ 2002

Dembele's Ph.D. Thesis

- Around 2002, Lassina Dembele did a Ph.D. thesis with Henri Darmon at McGuill university on explicit computation of Hilbert modular forms.
- **Application:** assuming modularity conjectures, enumerate *all* elliptic curves over $\mathbf{Q}(\sqrt{5})$ of each conductor!
- Table of curves of prime conductor with norm up to 5000.
- There are 431 conductors $\mathfrak{n}$ with norm ≤ 1000, and Lassina's tables contain 50 distinct conductors with norm ≤ 1000 (out of the 163 prime conductors of norm ≤ 1000).

Hilbert Modular Forms?

Hilbert Modular Forms

- These are holomorphic functions on a product of two copies of the upper half plane.
- But there is a purely algebraic/combinatorial reinterpretation of them due to Jacquet and Langlands, which involves quaternion algebras.
- Explicit definition of a finite set S and an action of commuting operators T_n on the free abelian group X on the elements of S such that the systems of Hecke eigenvalues in $\mathbf{Z}$ correspond to elliptic curves over $\mathbf{Q}(\sqrt{5})$, up to isogeny.
- Flip to Dembele's thesis and show the tables of Hecke eigenvalues and explain them. (page 40)

The Plan: Finding Curves

Computing Hilbert Modular Forms

Implement an optimized variant of Dembele's algorithm, which is fast enough to compute a few Hecke operators for any level $\mathfrak{n}$ with $\mathrm{Norm}(\mathfrak{n}) \leq 10^5$. The dimensions of the relevant space are mostly less than 2000, so the linear algebra is likely very feasible. I did this yesterday *modulo bugs...*:

```
sage: N = F.factor(100019)[0][0]; N
Fractional ideal (65*a + 292)
sage: time P = IcosiansModP1ModN(N)
CPU times: user 0.19 s, sys: 0.00 s, total: 0.19 s
sage: P.cardinality()
1667
sage: time T5 = P.hecke_matrix(F.primes_above(5)[0])
CPU times: user 0.38 s, sys: 0.11 s, total: 0.49 s
sage: N.norm()
100019
sage: 10^5
100000
```

Yes, that just took a total less than one second!!!

Magma?

But Magma can compute Hilbert Modular Forms...

Why not just use Magma, which already has Hilbert modular forms in it, due to the great work of John Voight, Lassina Dembele, and Steve Donnelly?

```
[wstein@eno ~]$ magma
Magma V2.16-13    Fri Nov  5 2010 18:09:32 on eno
[Seed = 666889163]
Type ? for help.  Type <Ctrl>-D to quit.
> F<w> := QuadraticField(5);
> time M := HilbertCuspForms(F, Factorization(Integers(F)*10
Time: 0.030
> time T5 := HeckeOperator(M, Factorization(Integers(F)*5)[1
Time: 235.730      # 4 minutes
```

The value in Magma's HMF's are that the implementation is *very* general. But slow. And the above was just one Hecke operator. We'll need many, and Magma gets *much* slower as the subscript of the Hecke operator grows. A factor of 1000 in speed kind of matters.

Computing Hilbert Modular Forms

Overview of Dembele's Algorithm

1. Let R = maximal order in Hamilton quaternion algebra over $F = \mathbf{Q}(\sqrt{5})$.
2. Compute the finite set $S = R^* \backslash \mathbf{P}^1(\mathcal{O}_F/\mathfrak{n})$. Let X = free abelian group on S.
3. To compute the Hecke operator $T_\mathfrak{p}$ on X, compute (and store once and for all) $\#\mathbf{F}_\mathfrak{p} + 1$ elements $\alpha_{\mathfrak{p},i} \in B$ with norm $\mathfrak{p}$, then compute

$$T_\mathfrak{p}(x) = \sum \alpha_{\mathfrak{p},i}(x).$$

That's it! Now scroll through the 1500 line file I wrote yesterday that implements this in many cases... but still isn't done.
Deines-Stein: article about how to do 2-3 above *quickly*?

Computing Equations for Curves and Ranks

1. Hilbert modular forms, as explained above, will allow us to find by linear algebra the Hecke eigenforms corresponding to all curves over $\mathbf{Q}(\sqrt{5})$ with conductor of norm $\leq 10^5$.
2. Finding the corresponding Weierstrass equations is a whole different problem. Joanni Gaski will have made a huge table by then, and we'll find some chunk of them there.
3. Noam Elkies outlined a method to make an even better table, and we'll implement it and try.
4. Fortunately, if Sage is super insanely fast at computing Hecke operators on Hilbert modular forms, then it should be possible to compute the *analytic ranks* of the curves found above without finding the actual curves. By BSD, this should give the ranks. This should answer the problem that started this lecture, at least assuming standard conjectures (and possibly using a theorem of Zhang).