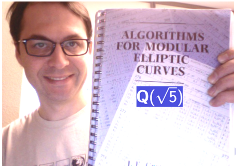
Elliptic Curves over $\mathbf{Q}(\sqrt{5})$

William Stein, University of Washington

This is part of the NSF-funded AIM FRG project on Databases of L-functions.

This talk had much valuable input from Noam Elkies, John Voight, John Cremona, and others.

February 25, 2011 at Stanford University



1. Finding Curves

Finding Elliptic Curves over $\mathbf{Q}$

Tables of Elliptic Curves over $\mathbf{Q}$

1. Table(s) 0: Published books. Antwerp IV and Cremona's **book** – curves of conductor up to 1,000.
   http://wstein.org/tables/antwerp/
2. Table 1: All (modular) elliptic curves over $\mathbf{Q}$ with *conductor* up to 130,000. Cremona's
   http://www.warwick.ac.uk/~masgaj/ftp/data/.
3. Table 2: Over a hundred million elliptic curves over $\mathbf{Q}$ with conductor $\leq 10^8$. Stein-Watkins. http://db.modform.org
4. Table 3: Rank records.
   http://web.math.hr/~duje/tors/rankhist.html

Tables of Elliptic Curves over $\mathbf{Q}$

Example Application of Tables of Elliptic Curves over $\mathbf{Q}$

- Having tables lets you do things like ask: "Give me smallest (known!) conductor example of an elliptic curve over $\mathbf{Q}$ with rank 2 and nontrivial $Ш(E/\mathbf{Q})[3]$."
  Answer (Watkins): $y^2 + xy = x^3 - x^2 + 94x + 9$, which has (prime) conductor 53,295,337.
- Or 'Give the simplest (known) example of an elliptic curve of rank 4.'"
  Answer: $y^2 + xy = x^3 - x^2 - 79x + 289$ of conductor 234,446. (Who cares? Open problem, show that the analytic rank of this curve is 4.)

Problem 1: Finding Elliptic Curves over $\mathbf{Q}(\sqrt{5})$

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

Our ultimate goal is to create the following tables (not done yet!), along with BSD invariants, etc.

1. Table 1: All (modular) elliptic curves over $\mathbf{Q}(\sqrt{5})$ with *norm conductor* up to 10^6.
2. Table 2: Around one hundred million elliptic curves over $\mathbf{Q}(\sqrt{5})$ with norm conductor $\leq 10^8$ (say).
3. Table 3: Rank records.

Any table starts with the smallest conductor curve over $\mathbf{Q}(\sqrt{5})$:

$$y^2 + xy + ay = x^3 + (a+1)\,x^2 + ax$$

of conductor having norm 31, where $a = (1+\sqrt{5})/2$.

My Motivation for Making Tables over $\mathbf{Q}(\sqrt{5})$

1. $\mathbf{Q}(\sqrt{5})$ is the simplest totally real field besides $\mathbf{Q}$; extra structure coming from Shimura curves and Hilbert modular forms
2. Shou-Wu Zhang's "program": Heegner points, Gross-Zagier, Kolyvagin, etc., over totally real fields. Make this more explicit and refine his theoretical results. Provide examples.
3. Deep understanding over **one** number field besides $\mathbf{Q}$ suggests what is feasible, setting the bar higher over other fields.
4. Some phenomenon over $\mathbf{Q}$ becomes simpler or different over number fields: *rank 2 curves of conductor 1?*
5. Numerical tests of published formulas... sometimes (usually?) shows they are slightly wrong, or at least forces us to find much more explicit statements of them. See, e.g., http://wstein.org/papers/bs-heegner/; at least three published generalizations of the Gross-Zagier formula are wrong.
6. New challenges, e.g., prove that the full BSD formula holds for specific elliptic curves over $\mathbf{Q}(\sqrt{5})$.

Finding Curves via Modular Forms

1. **Standard Conjecture:** *Rational Hilbert modular newforms over $\mathbf{Q}(\sqrt{5})$ correspond to isogeny classes of elliptic curves over $\mathbf{Q}(\sqrt{5})$.* So we enumerate newforms over $\mathbf{Q}(\sqrt{5})$.
2. There is an approach of Dembele to compute (very sparse!) Hecke operators on modular forms over $\mathbf{Q}(\sqrt{5})$. (I designed and implemented the fastest code to do this.) Table got by computing space:

   http://wstein.org/Tables/hmf/sqrt5/dimensions.txt
3. Linear algebra and the Hasse bound to get rational eigenvectors.
4. http://wstein.org/Tables/hmf/sqrt5/ellcurve_aplists.txt

Computing Modular Forms over $\mathbf{Q}(\sqrt{5})$

Overview of Dembele's Algorithm to Compute Forms of level $\mathfrak{n}$

1. Let R = maximal order in Hamilton quaternion algebra B over $F = \mathbf{Q}(\sqrt{5})$.
2. Let $S = R^\times \backslash \mathbf{P}^1(\mathcal{O}_F/\mathfrak{n})$, and $X = \bigoplus_{s \in S} \mathbf{Z}[s]$.
3. To compute the Hecke operator $T_\mathfrak{p}$ on X, compute (and store) certain $R^\times$-representative 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! Making this *really fast* took thousands of lines of tightly written Cython code, treatment of special cases, etc.

http://code.google.com/p/purplesage/source/browse/psage/modform/hilbert/sqrt5/sqrt5_fast.pyx

Rational Newforms over $\mathbf{Q}(\sqrt{5})$

Norm	Cond	Number	a2 a3 a5 a7 a11a a11b ... (hecke eigenvalues) ...
31	5*a-2	0	-3 2 -2 2 4 -4 4 -4 -2 -2 ? ? -6 -6 12 -4 6 -2 -8 0 0 16 10 -6
31	5*a-3	0	-3 2 -2 2 -4 4 -4 4 -2 -2 ? ? -6 -6 -4 12 -2 6 0 -8 16 0 -6 10
36	6	0	? ? -4 10 2 2 0 0 0 0 -8 -8 2 2 -10 -10 2 2 12 12 0 0 10 10
41	a+6	0	-2 -4 -1 -6 -2 5 6 -1 2 9 -10 4 ? ? -3 4 6 -8 -12 9 -11 -4 -1 -8
41	a-7	0	-2 -4 -1 -6 5 -2 -1 6 9 2 4 -10 ? ? 4 -3 -8 6 9 -12 -4 -11 -8 -1
45	6*a-3	0	-3 ? ? -14 -4 -4 4 4 -2 -2 0 0 10 10 -4 -4 -2 -2 -8 -8 0 0 -6 -6
49	7	0	0 5 -4 ? -3 -3 0 0 5 5 2 2 2 2 -10 -10 -8 -8 -8 -8 5 5 0 0
55	a+7	0	-1 -2 ? 14 ? ? 8 -4 -6 6 8 -4 -6 6 -12 0 -10 2 0 0 -4 8 -18 6
55	-a+8	0	-1 -2 ? 14 ? ? -4 8 6 -6 -4 8 6 -6 0 -12 2 -10 0 0 8 -4 6 -18
64	8	0	? 2 -2 10 -4 -4 4 4 -2 -2 0 0 2 2 12 12 -10 -10 8 8 -16 -16 -6 -6
71	a+8	0	-1 -2 0 -4 0 0 2 -4 6 -6 2 8 6 12 -12 6 -4 -10 ? ? 14 -4 6 18
71	a-9	0	-1 -2 0 -4 0 0 -4 2 -6 6 8 2 12 6 6 -12 -10 -4 ? ? -4 14 18 6
76	-8*a+2	0	? 1 -3 -4 -6 3 ? ? -6 3 5 5 6 6 6 -12 8 8 -9 0 -1 -1 9 0
76	-8*a+2	1	? -5 1 0 2 -3 ? ? -10 5 -3 7 2 2 10 0 12 -8 7 -8 15 5 -15 0
76	-8*a+6	0	? 1 -3 -4 3 -6 ? ? 3 -6 5 5 6 6 -12 6 8 8 0 -9 -1 -1 0 9
76	-8*a+6	1	? -5 1 0 -3 2 ? ? 5 -10 7 -3 2 2 0 10 -8 12 -8 7 5 15 0 -15
79	-8*a+3	0	1 -2 -2 -2 -4 0 8 4 -2 6 0 -8 -2 2 4 -4 10 14 12 -16 ? ? 18 -14
79	-8*a+5	0	1 -2 -2 -2 0 -4 4 8 6 -2 -8 0 2 -2 -4 4 14 10 -16 12 ? ? -14 18
80	8*a-4	0	? -2 ? -10 0 0 -4 -4 6 6 -4 -4 6 6 12 12 2 2 -12 -12 8 8 -6 -6
81	9	0	-1 ? 0 14 0 0 -4 -4 0 0 8 8 0 0 0 0 2 2 0 0 -16 -16 0 0
89	a-10	0	-1 4 0 -4 -6 0 -4 2 6 6 -4 -4 0 6 12 0 14 -4 0 12 -16 2 ? ?
89	a+9	0	-1 4 0 -4 0 -6 2 -4 6 6 -4 -4 6 0 0 12 -4 14 12 0 2 -16 ? ?
95	2*a-11	0	-1 -2 ? 2 0 0 ? ? -6 6 -4 8 -6 -6 12 12 -10 14 12 0 -16 8 6 -6
95	-2*a-9	0	-1 -2 ? 2 0 0 ? ? 6 -6 8 -4 -6 -6 12 12 14 -10 0 12 8 -16 -6 6
99	9*a-3	0	1 ? -2 2 ? ? 4 -4 6 -2 -8 8 -6 2 12 12 -2 -2 8 -8 16 8 2 -14
99	9*a-6	0	1 ? -2 2 ? ? -4 4 -2 6 8 -8 2 -6 12 12 -2 -2 -8 8 8 16 -14 2
100	10	0	? -5 ? -10 -3 -3 5 5 0 0 2 2 -3 -3 0 0 2 2 12 12 -10 -10 15 15
100	10	1	? 5 ? 10 -3 -3 -5 -5 0 0 2 2 -3 -3 0 0 2 2 12 12 10 10 -15 -15

Implementation in Sage: Uses Cython=C+Python

Install PSAGE: http://code.google.com/p/purplesage/.

Hecke Operators over $\mathbf{Q}(\sqrt{5})$ in Sage

```
sage: import psage.modform.hilbert.sqrt5 as H
sage: N = H.tables.F.factor(100019)[0][0]; N
Fractional ideal (65*a + 292)

sage: time S = H.HilbertModularForms(N); S
Time: CPU 0.31 s, Wall: 0.34 s
Hilbert modular forms of dimension 1667, level 65*a+292
(of norm 100019=100019) over QQ(sqrt(5))

sage: time T5=S.hecke_matrix(H.tables.F.factor(5)[0][0])
Time: CPU 0.05 s, Wall: 0.05 s
sage: time T19=S.hecke_matrix(H.tables.F.factor(19)[0][0])
Time: CPU 0.25 s, Wall: 0.25 s
```

(Yes, that just took much less than a second.)

Why Not Use Only Magma?

Why not just use Magma, which already has modular forms over totally real fields in it (Voight, Dembele, and Donnelly)?

```
[wstein ]$ magma
Magma V2.17-4     Thu Feb 24 2011 14:43:58 on deep
> F<w> := QuadraticField(5);
> M := HilbertCuspForms(F,
            Factorization(Integers(F)*100019)[1][1]);
> time T5 := HeckeOperator(M,
             Factorization(Integers(F)*5)[1][1]);
Time: 81.770
> time T19 := HeckeOperator(M,
              Factorization(Integers(F)*19)[1][1]);
Time: 6.600
```

My code took less than 0.05s for T_5 and 0.25s for T_{19}.

In fairness, Magma's implementation is *very* general, whereas Sage's is specific to $\mathbf{Q}(\sqrt{5})$, and Magma is doing slightly different calculations.

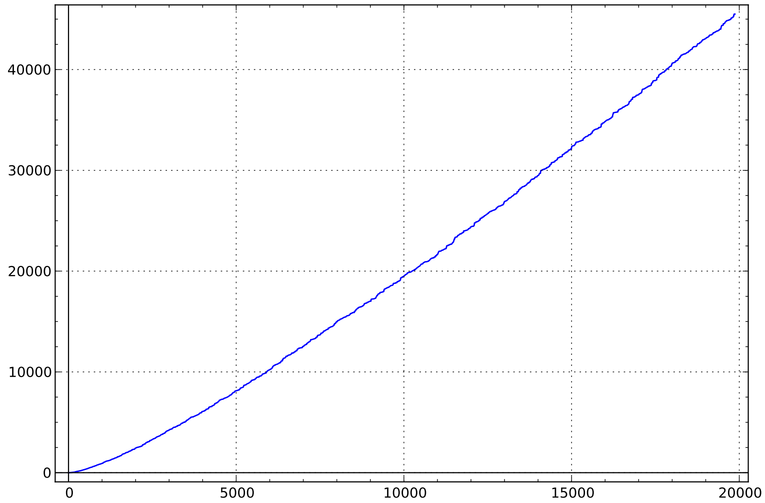
Use Sage (not just Magma)

1. Many of these computations are very intricate and have never been done before, hence having two (mostly) independent implementations raises my confidence.
2. I want to run some of the computations on a supercomputer, and Magma is expensive.
3. Visualization – of resulting data
4. Cython – write Sage code that is as fast as anything you can write in C.
5. Lcalc – zeros of L-functions
6. I think I can implement code to compute $L(E,s)$ for E over $\mathbf{Q}(\sqrt{5})$ about 20 times faster than Magma (2.17). This speedup is **crucial** for large scale tables:

   1 month versus 20 months.

How Many Isogeny Classes of Curves?

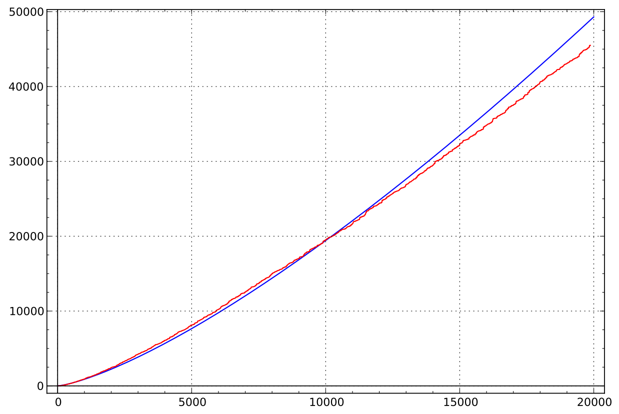
Rational Newforms over $\mathbf{Q}(\sqrt{5})$ of (norm) level up to X



How Many Isogeny Classes of Curves?

Rational Newforms over $\mathbf{Q}(\sqrt{5})$ of level $\leq X$ (Least Squares)

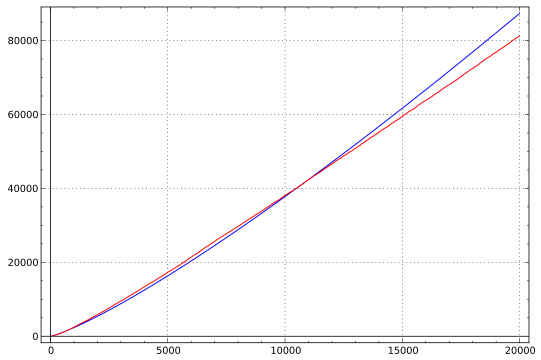
$$\#\{\text{newforms with norm level up to } X\} \sim 0.082 \cdot X^{1.344}$$



For comparison, Cremona's tables up to 20,000

Cremona's tables

$$\#\{\text{newforms with norm level up to } X\} \sim 0.55 \cdot X^{1.21}$$



Conjecture (Watkins): Number of elliptic curves over **Q** with level up to X is $\sim cX^{5/6}$.

Rational Newforms $\mapsto$ Curves over $\mathbf{Q}(\sqrt{5})$

1. *Big search through equations*, compute corresponding modular forms by a point count, and look up in table. (Joanna Gaski and Alyson Deines doing this now: http://wstein.org/Tables/hmf/sqrt5/finding_weierstrass_equations/)
2. Or, apply Dembele's paper *An Algorithm For Modular Elliptic Curves Over Real Quadratic Fields* (I haven't implemented this yet; how good in practice?)
3. Or, apply the *method of Cremona-Lingham* to find the curves by finding S-integral points on other curves over $\mathbf{Q}(\sqrt{5})$. (Not implemented in Sage yet; only in Magma.) Example: Cremona's program found the curve
$$y^2 + xy + ay = x^3 + (-a+1)x^2 + (416a - 674)x + (5120a - 8285)$$
with conductor norm $124 = 4 \cdot 31$; the first unknown curve.
4. Or, Elkies' new method...

Elkies λ method...

Elkies Method for Finding Weierstrass Equations

Noam Elkies: "Apropos Cremona-Lingham: remember that at Sage Days 22 I suggested a way to reduce this to solving S-unit equations (via the λ-invariant), which is effective, unlike finding S-integral points on $y^2 = x^3 + k$."

Isogeny Class

Enumerate the curves in an isogeny class.

1. For a specific curve, bound the degrees of isogenies using the Galois representation. (Don't know how to do this yet.)
2. Explicitly compute all possible isogenies, e.g., using Cremona's student Kimi Tsukazaki's Ph.D. thesis full of isogeny formulas, and work of Elkies. (I'm not sure how to do this.)
3. Open problem: give an explicit analogue of Mazur's theorem but over $\mathbf{Q}(\sqrt{5})$. What are the degrees of rational isogenies of prime degree of elliptic curves over $\mathbf{Q}(\sqrt{5})$? (At least finiteness is now known, due to a recent result of two Harvard undergraduates.)

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

Joanna Gaski and Alyson Deines make tables like this ($a = (1 + \sqrt{5})/2$)

31	5*a-2	0	-3 2 -2 2 ...	[1,a+1,a,a,0]
31	5*a-3	0	-3 2 -2 2 ...	[1,-a-1,a,0,0]
36	6	0	? ? -4 10 ...	[a,a-1,a,-1,-a+1]
41	a+6	0	-2 -4 -1 -...	[0,-a,a,0,0]
41	a-7	0	-2 -4 -1 -...	[0,a-1,a+1,0,-a]
45	6*a-3	0	-3 ? ? -14...	[1,1,1,0,0]
49	7	0	0 5 -4 ? -...	[0,a,1,1,0]
55	a+7	0	-1 -2 ? 14...	[1,-a+1,1,-a,0]
55	-a+8	0	-1 -2 ? 14...	[1,a,1,a-1,0]
64	8	0	? 2 -2 10 ...	[0,a-1,0,-a,0]
71	a+8	0	-1 -2 0 -4...	[a,a+1,a,a,0]
71	a-9	0	-1 -2 0 -4...	[a+1,a-1,1,0,0]
76	-8*a+2	0	? 1 -3 -4 ...	[a,-a+1,1,-1,0]
76	-8*a+2	1	? -5 1 0 2...	[1,0,a+1,-2*a-1,0]
76	-8*a+6	0	? 1 -3 -4 ...	[a+1,0,1,-a-1,0]
76	-8*a+6	1	? -5 1 0 -...	[1,0,a,a-2,-a+1]
79	-8*a+3	0	1 -2 -2 -2...	[a,a+1,0,a+1,0]
79	-8*a+5	0	1 -2 -2 -2...	[a+1,a-1,a,0,0]
80	8*a-4	0	? -2 ? -10...	[0,1,0,-1,0]
81	9	0	-1 ? 0 14 ...	[1,-1,a,-2*a,a]
89	a-10	0	-1 4 0 -4 ...	[a+1,-1,1,-a-1,0]
89	a+9	0	-1 4 0 -4 ...	[a,-a,1,-1,0]
95	2*a-11	0	-1 -2 ? 2 ...	[a,a+1,a,2*a,a]
95	-2*a-9	0	-1 -2 ? 2 ...	[a+1,a-1,1,-a+1,-1]
99	9*a-3	0	1 ? -2 2 ?...	[a+1,0,0,1,0]
99	9*a-6	0	1 ? -2 2 ?...	[a,-a+1,0,1,0]
100	10	0	? -5 ? -10...	[1,0,1,-1,-2]
100	10	1	? 5 ? 10 -...	[a,a-1,a+1,-a,-a]

Database

A MongoDB Database

Text files (http://wstein.org/Tables/hmf/sqrt5) and an indexed queryable MongoDB database:

http://db.modform.org

Canonical Minimal Weierstrass Model

Canonical Minimal Weierstrass Models over $\mathbf{Q}$

Fact: Every elliptic curve over $\mathbf{Q}$ has a unique minimal Weierstrass equation $[a_1, a_2, a_3, a_4, a_6]$ with $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{0, -1, 1\}$?

What about $\mathbf{Q}(\sqrt{5})$?

Something similar is true for $\mathbf{Q}(\sqrt{5})$.

- Idea: Make a canonical choice of Δ, then transform so that a_1, a_3 are unique mod $2\mathcal{O}_F$ and a_2 is unique mod $3\mathcal{O}_F$. (Easy: this nails down the equation.)
- Aly Deines and Andrew Ohana — writing up and coding it.
- Annoying unresolved problem: **agree** on a "canonical" choice of "nice" generator for each ideal in $\mathcal{O}_F$!

Huge Table: Like Stein-Watkins over $\mathbf{Q}(\sqrt{5})$

1. As in [Stein-Watkins], use Kraus's *Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique* so we only enumerate over pairs (c_4, c_6) mod 1728 that satisfy certain congruence conditions so they define a minimal curve, with bounded discriminant and conductor. (Details being worked out by Joanna and Aly; they estimate that there are about 600,000 pairs c_4, c_6 modulo 1728 to consider.)
2. Compute first few $a_{\mathfrak{p}}$ (how many??) for each curve; use these $a_{\mathfrak{p}}$ as a key, and thus keep at most one curve from each isogeny class.
3. Get a table of hundreds of millions of curves over $\mathbf{Q}(\sqrt{5})$.

2. What to do with the curves

Problem 2: Computing With Curves

Some Invariants of an Elliptic Curve over $\mathbf{Q}(\sqrt{5})$

1. Torsion subgroup
2. Tamagawa numbers and Kodaira symbols
3. Rank and generators for $E(\mathbf{Q}(\sqrt{5}))$: Simon 2-descent program.
4. Regulator
5. $L(E, s)$: analytic rank, leading coefficient, zeroes in critical strip
6. $\#Ш(E)_{\text{an}}$: conjectural order of $Ш(E/\mathbf{Q}(\sqrt{5}))$.

Other Interesting things to compute

Other invariants...

1. **All integral points:** a recent student (Nook) of Cremona did this in Magma, so port it. (See next slide.)
2. Compute **Heegner points**, as defined by Zhang. Find their height using his generalization of the Gross-Zagier formula. (Requires level is not a square.) Will provide a first numerical check on the formula.
3. **Congruence number**:
   1. define using quaternion ideal Hecke module,
   2. or define via congruences between q-expansions.
4. **Galois representations**: Image of Galois (like Sutherland did for elliptic curves over $\mathbf{Q}$); Sato-Tate distribution.
5. **Congruence graph**: mod p congruences between all elliptic curves up to some conductor.

Integral Points over Number Fields


```
Hi William,

I saw the slides for your talk on elliptic curves over Q(sqrt(5)).
You mention translating Nook's Magma code for integral points as
a future project. That's exactly what Jackie Anderson and I did
at Sagedays 22. If someone is interested in that, make sure they
look at our work first.

The translation is done. There is a speed up against Magma version
by using Python generators. What needs to be done is a bit more
testing (against the Magma version). John Cremona warned us to be
careful with this algorithm because it produces an upper bound and
exhaustively searches up to it. If the bound is a bit lower it
might fail on rare occasions.

Rado Kirov
```

(This code depends on code to compute $E(\mathbf{Q}(\sqrt{5}))$, which Sage doesn't quite have yet.)

Integral Points for curve with norm conductor 199

Demo of Rado Kirov and Jackie Anderson's Code...

```
sage: F.<a> = NumberField(x^2-x-1)
sage: E = EllipticCurve([0,-a-1,1,a,0])
sage: E.conductor().norm()
199
sage: load "intpts.sage"
sage: time integral_points(E, E.gens())
[(a : -1 : 1), (a + 1 : a : 1), (2*a + 2 : -4*a - 3 : 1),
(-a + 3 : 3*a - 5 : 1), (-a + 2 : -2*a + 2 : 1),
(6*a + 3 : 18*a + 11 : 1),
(-42*a + 70 : -420*a + 678 : 1), (1 : 0 : 1), (0 : 0 : 1)]
CPU times: user 4.24 s, sys: 0.19 s, total: 4.43 s
Wall time: 7.31 s
```

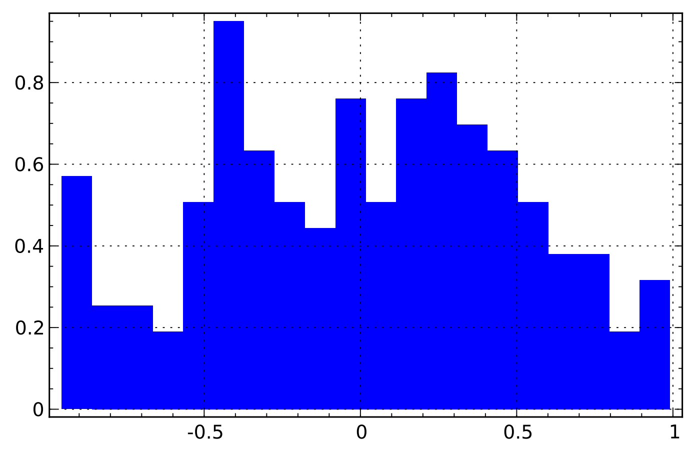
(This exists mainly as an email attachment. Get it into psage...)

Magma 2.17 doesn't come with integral points code over number fields, but Nook's code exists...

Example: Rank 0 Curve of Norm Conductor 31

$$E : y^2 + xy + ay = x^3 + (a+1)\,x^2 + ax$$

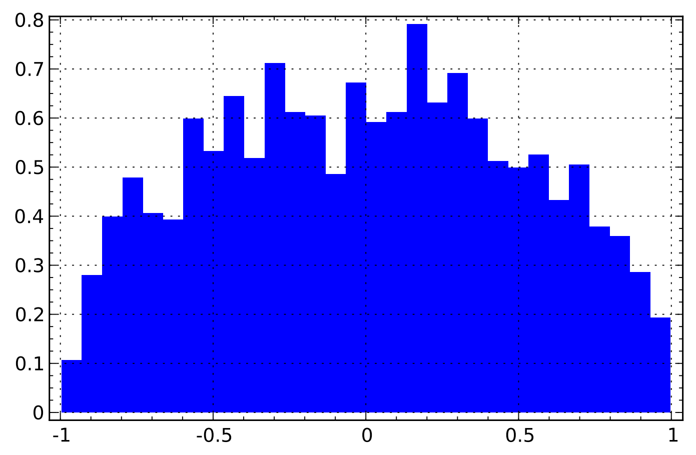
Sato-Tate Distribution: Primes up to Norm 1000



Example: Rank 0 Curve of Norm Conductor 31

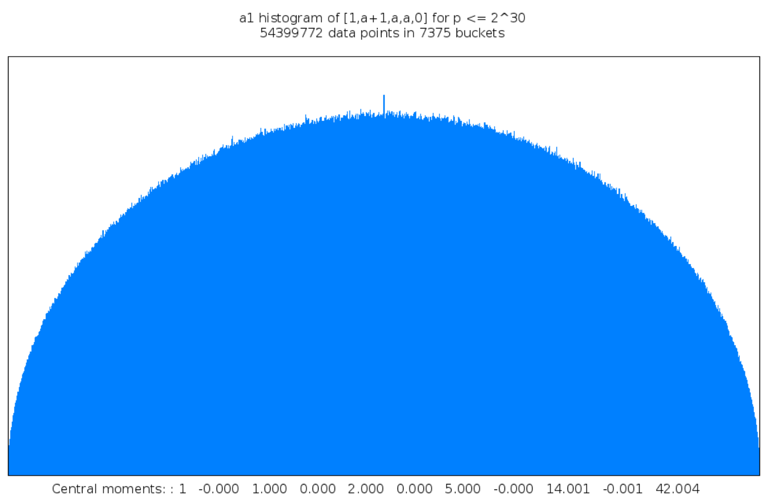
$$E : y^2 + xy + ay = x^3 + (a+1)\,x^2 + ax$$

Sato-Tate Distribution: Primes up to Norm 20,000



Sato-Tate

Drew Sutherland: Primes up to 10^9



Computing $a_{\mathfrak{p}}$ for $N(\mathfrak{p}) \leq 10^6$

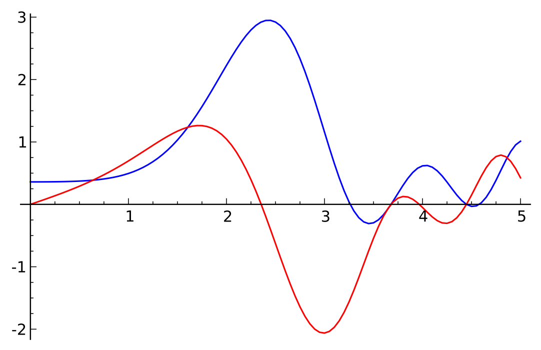
Computing enough $a_{\mathfrak{p}}$ to compute $L(E, s)$

1. To compute $L(E, s)$ to double precision for any E with norm conductor $\leq 10^8$ requires $a_{\mathfrak{p}}$ for $N(\mathfrak{p}) \leq 10^6$.
2. This requires computing $\#E(\mathcal{O}_F/\mathfrak{p})$.
3. Only *89 primes* of $\mathcal{O}_F$ of norm up to 10^6 are inert.
4. Count points mod split primes using Drew Sutherland's very fast code (smalljac), which uses baby-step-giant-step.
5. Count points mod inert primes by making a table. Probably take a CPU month to make; size 200MB.
6. Hope to compute any L-series in about 2 seconds.
7. That's about 6 years (or a month on a hundred processes) to compute every L-series I want to compute.

Example: Rank 0 Curve of Norm Conductor 31

$$E : y^2 + xy + ay = x^3 + (a+1)\,x^2 + ax$$

Finding a zero in the Critical Strip: real and imag parts



Zero at $1 + 3.678991i$.

Rank Records

The Rank Problem

What are the "simplest" (smallest norm conductor) elliptic curves over $\mathbf{Q}(\sqrt{5})$ of ranks 0, 1, 2, 3, 4, 5,...? Best known records:

Rank	Norm(N)	Equation	Person
0	31 (prime)	[1,a+1,a,a,0]	Dembele
1	199 (prime)	[0,-a-1,1,a,0]	Dembele
2	1831 (prime)	[0,-a,1,-a-1,2a+1]	Dembele
3	$26{,}569 = 163^2$	[0,0,1,-2,1]	Elkies
4	1,209,079 (prime)	[1, -1, 0, -8-12a, 19+30a]	Elkies
5	64,004,329	[0, -1, 1, -9-2a, 15+4a]	Elkies

Best possible? (Over $\mathbf{Q}$ the corresponding best *known* conductors are 11, 37, 389, 5,077, 234,446, and 19,047,851. We don't know if the last two are best.)

BSD Challenges

Some Challenges

1. Verify that $\#Ш(E)_{\mathrm{an}}$ is approx. perfect square for curves with norm conductor up to some bound.
2. Prove the full BSD conjecture for a curve over $\mathbf{Q}(\sqrt{5})$
3. Prove the full BSD conjecture for a curve over $\mathbf{Q}(\sqrt{5})$ that doesn't come by base change from a curve over $\mathbf{Q}$.
4. Make and verify an analogue of Kolyvagin's conjecture for a curve of rank ≥ 2. (Elaborate in talk.)

Proving BSD for specific curves may require explicit computation with Heegner points, the Gross-Zagier formula, etc., following Zhang. Also, prove something new using Euler systems.

Examples: Compute BSD Invariants for First Curves of rank 0,1,2

Using Sage, I computed all BSD invariants and solved for $Ш_{\mathrm{an}}$ for the first curves of rank 0,1,2.

None of these curves are a base change from $\mathbf{Q}$ (in fact, none have j-invariant in $\mathbf{Q}$).

Example: Rank 0 Curve of Norm Conductor 31

$$E : y^2 + xy + ay = x^3 + (a+1)\,x^2 + ax$$

Conductor	$5a - 2$
Torsion	$\mathbf{Z}/8\mathbf{Z}$
Tamagawa Numbers	$c_\mathfrak{p} = 1$ (I1)
Rank and gens	0
Regulator	1
$L^*(E,1)$	0.359928959498039
Real Periods	6.1043463067145 2, 8.43805988789973

$$\text{Ш}(E)_{\mathrm{an}} = \frac{\sqrt{D} \cdot L^*(E,1) \cdot T^2}{\Omega_E \cdot \mathrm{Reg}_E \cdot \prod c_\mathfrak{p}}$$
$$= \sqrt{5} \cdot 0.35992 \cdot 8^2/(6.104346 \cdot 8.43805) = 1.0000000\ldots$$

Example: Rank 1 Curve of Norm Conductor 199

$$E : y^2 + y = x^3 + (-a-1)\,x^2 + ax$$

Table for the curve 199

Conductor	$3a + 13$
Torsion	$\mathbf{Z}/3\mathbf{Z}$
Tamagawa Numbers	$c_{\mathfrak{p}} = 1$ (I1)
Rank and gens	1, gen $(0, 0)$
Regulator	0.0771542842715149
$L^*(E,1)$	0.657814883009960
Real Periods	7.06978549315474, 6.06743219455559

$$Ш(E)_{\rm an} = \frac{\sqrt{D}\cdot L^*(E,1)\cdot T^2}{\Omega_E \cdot \mathrm{Reg}_E \cdot \prod c_{\mathfrak{p}}}$$

$$= \sqrt{5}\cdot 0.657 \cdot 3^2/(3.534\cdot 6.067\cdot 0.15430\cdot 1) = 1.00000\,.$$

Example: Rank 2 Curve of Norm Conductor 1831

$$E : y^2 + y = x^3 + (-a)\,x^2 + (-a-1)\,x + (2a+1)$$

Table for the curve 1831

Conductor	$7a + 40$
Torsion	1
Tamagawa Numbers	$c_{\mathfrak{p}} = 1$ (I1)
Rank 2; Gens	$(0, -a-1)\,,\ \left(-\frac{3}{4}a + \frac{1}{4}, -\frac{5}{4}a - \frac{5}{8}\right)$
Regulator	0.767786510776225
$L^*(E,1)$	2.88288222151816
Real Periods	7.51661850836325, 5.02645072067941

$$Ш(E)_{\mathrm{an}} = \frac{\sqrt{D} \cdot L^*(E,1) \cdot T^2}{\Omega_E \cdot \mathrm{Reg}_E \cdot \prod c_{\mathfrak{p}}} = 0.111111111111111\ldots \sim \frac{1}{9}$$

Wrong. Why? The regulator is wrong (saturation).

Remark About Saturation

1. Elkies: " So we must also explore your suggestion about saturation. Indeed a naive search quickly returns a point $(1, -a)$, and then 3 times this point plus 6 times your generator $(0, -a-1)$ gives your second generator. So indeed we find a group containing the span of your two generators with index 3."
2. Note: Simon's 2-descent program in Sage does not claim to make any attempt to saturate.
3. Cremona: I have had students do Ph.D. theses involving saturation over number fields.

Summary

1. Three tables: all curves up to given conductor (like Cremona), large number of curves (like Stein-Watkins), rank records (like Elkies)
2. Compute all BSD invariants
3. L-functions: zeros, Sato-Tate data, etc.
4. Integral points
5. For everything, much work remains.

Questions or Comments?