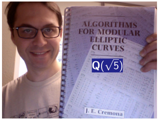
Elliptic Curves over $\mathbf{Q}(\sqrt{5})$

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 11, 2011



1. Finding Curves

Problem 1: Finding Elliptic Curves

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

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

Finding Curves via Modular Forms

1. **Standard Conjecture:** *Rational newforms over* $\mathbf{Q}(\sqrt{5})$ *correspond to the isogeny classes of elliptic curves over* $\mathbf{Q}(\sqrt{5})$. So we expect to get *all* curves of given conductor by enumerating modular forms over $\mathbf{Q}(\sqrt{5})$.
2. There is an approach of Dembele to compute sparse Hecke operators on modular forms over $\mathbf{Q}(\sqrt{5})$. (I have designed and implemented the fastest practical implementation.) Table got by computing space: `http://wstein.org/Tables/hmf/sqrt5/dimensions.txt`
3. Combine with linear algebra over finite fields and the Hasse bound to get all rational eigenvectors. (Not optimized yet. Requires fast sparse linear algebra – Gonzalo Tornaria has been working on this in Sage lately.)
4. Resulting table of eigenforms: `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 X = free abelian group on $S = R^*\backslash\mathbf{P}^1(\mathcal{O}_F/\mathfrak{n})$.
3. To compute the Hecke operator $T_\mathfrak{p}$ on X, compute (and store once and for all) certain $\#\mathbf{F}_\mathfrak{p}+1$ 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! 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 a11 a11 ...
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+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+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	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)/2

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 0.07 s, Wall: 0.09 s
```

(Yes, that just took much less than a second!)
See http://nt.sagenb.org/home/pub/30/ for all code.

Magma?

Why not just use Magma, which already has modular forms over totally real fields in it, due to the general work of John Voight, Lassina Dembele, and Steve Donnelly:

```
[wstein ]$ magma
Magma V2.16-13    Fri Nov  5 2010 18:09:32
> F<w> := QuadraticField(5);
> M := HilbertCuspForms(F,
            Factorization(Integers(F)*100019)[1][1]);
> time T5 := HeckeOperator(M,
             Factorization(Integers(F)*5)[1][1]);
Time: 235.730      # 4 minutes
```

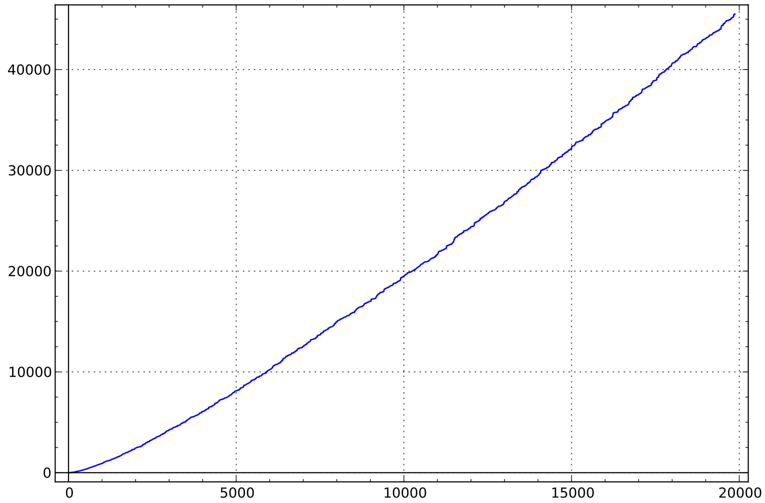
Thousand times slower than my implementation in Sage.

Magma's implementation is *very* general. 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.

(REMARK: After the talk, John Voight and I decided that with the newest Magma V2.17, and with very careful use of Magma (diving into the source code), one could do the above computation with it only taking 100 times longer than Sage.)

How Many Isogeny Classes of Curves?

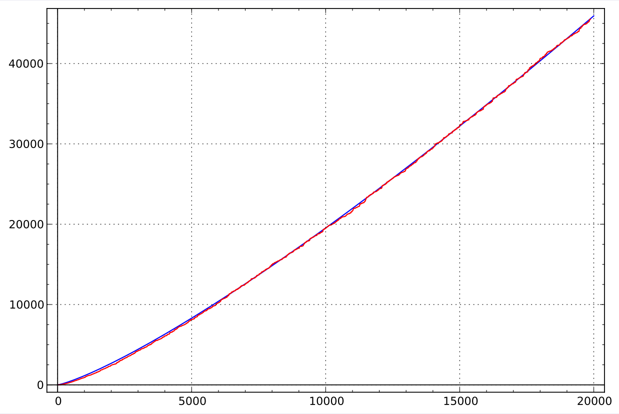
Rational Newforms over $\mathbf{Q}(\sqrt{5})$ of level up to N



How Many Isogeny Classes of Curves?

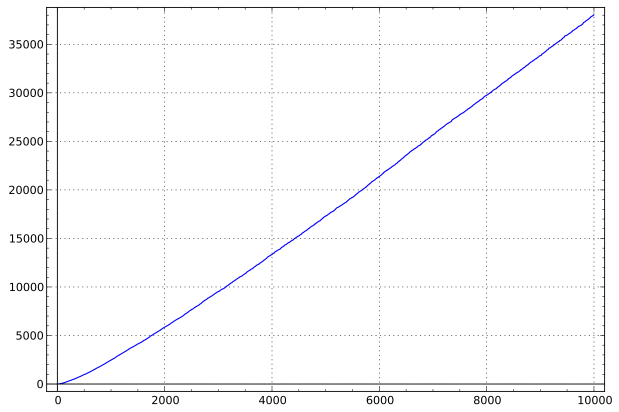
Rational Newforms over $\mathbf{Q}(\sqrt{5})$ of level $\leq X$ (Least Squares)

$$\#\{\text{newforms with norm level up to } X\} \sim 0.227X^{1.234}$$



For comparison, Cremona's tables up to 10,000

Cremona's tables



Conjecture (Watkins): Number of elliptic curves over $\mathbf{Q}$ 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 form 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 over number fields. (Not implemented in Sage.)
4. 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. (I'm not sure how to do this.)

Comment from Noam Elkies about previous Slide

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 lambda-invariant), which is effective, unlike finding S-integral points on $y^2 = x^3 + k$.
Also, see my Atkin paper
http://www.math.harvard.edu/~elkies/xisog.pdf?"

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+6	0	? 1 -3 -4 ...	[a+1,0,1,-a-1,0]
76	-8*a+2	1	? -5 1 0 2...	[1,0,a+1,-2*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

Try it out.

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 number fields, for appropriate choices of conventions.

- Main 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 $3\mathcal{O}_F$. Prove that this nails down the equation.
- Aly Deines and Andrew Ohana — writing up and coding it.

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

1. Enumerate over pairs (c_4, c_6) that satisfy certain congruence conditions so they define a minimal curve, with bounded discriminant and conductor. (Details being worked out by Joanni and Aly; they estimate that there are about 600,000 pairs c_4, c_6 modulo 1728 to consider.)
2. Compute first few $a_{\mathfrak{p}}$ for each curve; use these $a_{\mathfrak{p}}$ as a key, and keep only one curve from each isogeny class.
3. Get a table of hundreds of millions of curves over $\mathbf{Q}(\sqrt{5})$.
4. Compute data, e.g., analytic rank, about each.

2. What to do with 'em

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 is relevant
4. Regulator
5. $L(E, s)$: analytic rank, leading coefficient, zeroes in critical strip
6. $\#Ш(E)_{\mathrm{an}}$: conjectural order of Ш.

BSD Challenges

Some Challenges

1. Verify that $\#\text{Ш}(E)_{\text{an}}$ is approx. perfect square for curves with norm conductor up to some bound.
2. Prove the full BSD conjecture for a curve over $\mathbf{Q}(\sqrt{5})$ (RLM: Just do for a curve over $\mathbf{Q}$ and its twist by $\mathbf{Q}(\sqrt{5})$, then do a 2-descent 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. Verify Kolyvagin's conjecture for a curve of rank ≥ 2.

Proving BSD for specific curves will likely require explicit computation with Heegner points, the Gross-Zagier formula, etc., following Zhang. It also likely requires proving something new using Euler systems.

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.)
3. **Congruence number**:
   1. define using quaternion ideal Hecke module,
   2. or define via congruences between q-expansions.
4. **Galois representations**: Images of Galois (like Sutherland did for elliptic curves over $\mathbf{Q}$)
5. **Congruence graph**: between all elliptic curves up to some conductor, where two curves are connected if they have the same mod p representations.

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 our
work first (code attached).

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 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
```

Rank Records

The Rank Challenge Problem

What is the "simplest" (smallest norm conductor) elliptic curve over $\mathbf{Q}(\sqrt{5})$ of rank 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	$26569 = 163^2$	[0,0,1,-2,1]	Elkies
4	1209079 (prime)	[1, -1, 0, -8-12a, 19+30a]	Elkies
5	64004329	[0, -1, 1, -9-2a, 15+4a]	Elkies

Best possible? (Over $\mathbf{Q}$ the corresponding best known conductors are 11, 37, 389, 5077, 234446, and 19047851.)

Examples: Curves of rank 0,1,2 in detail

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

Example: Rank 0 Curve of Norm Conductor 31

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

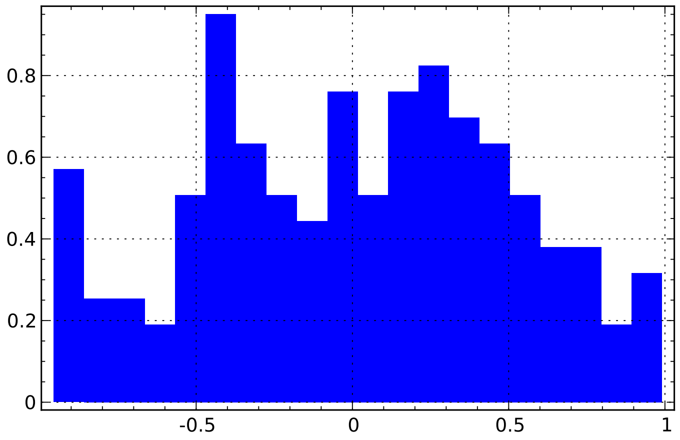
Conductor	$5a - 2$
Torsion	$\mathbf{Z}/8\mathbf{Z}$
Tamagawa Numbers	$c_{\mathfrak{p}} = 1$ (I1)
Rank and gens	0
Regulator	1
$L^*(E,1)$	0.359928959498039
Real Periods	6.10434630671452, 8.43805988789973

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

Example: Rank 0 Curve of Norm Conductor 31

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

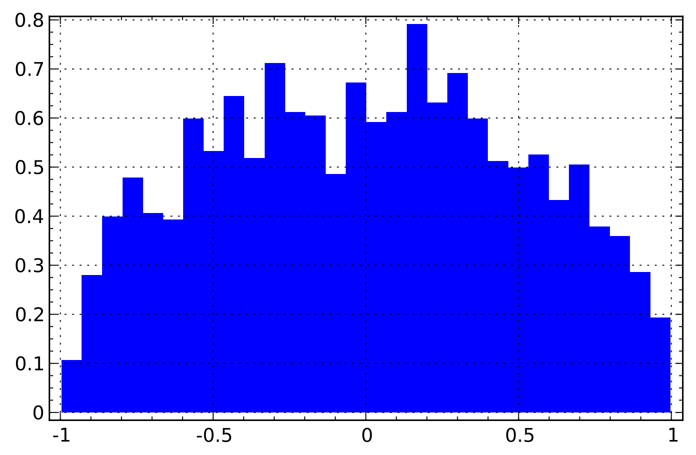
Sato-Tate Distribution: Primes up to Norm 1000



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 20000



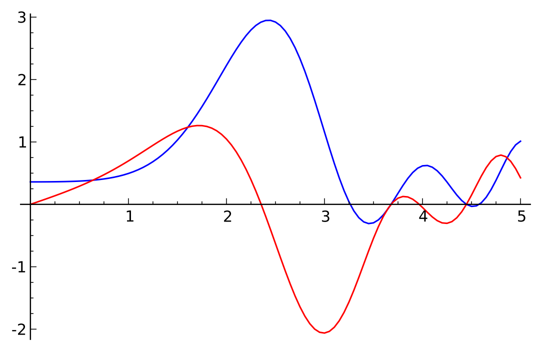
Sato-Tate

Switch to Drew's Animations

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 $1 + 3.678991i$.

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

$$\text{Ш}(E)_{\mathrm{an}} = \frac{\sqrt{D} \cdot L^*(E,1) \cdot T^2}{\Omega_E \cdot \mathrm{Reg}_E \cdot \prod c_{\mathfrak{p}}}$$
$$= \sqrt{5} \cdot 0.657 \cdot 3^2/(3.534 \cdot 6.067 \cdot 0.15430 \cdot 1) = 1.00000\,.$$

Integral Points for curve 199

Rado Kirov and Jackie Anderson's Code...

```
sage: E = EllipticCurve([0,-a-1,1,a,0]); show(E)
sage: 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)]
```

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 and gens	2, gens $(0 : -a-1 : 1)$, $\left(-\frac{3}{4}a + \frac{1}{4} : -\frac{5}{4}a - \frac{5}{8} : 1\right)$
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 From Elkies

Noam 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."

Summary

1. Three kinds of 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: much work remains
3. L-functions: zeros, Sato-Tate data, etc.
4. Integral points
5. For everything, much work remains.

Questions or Comments?