Elliptic Curves Over $F = \mathbb{Q}(\sqrt{5})$

William Stein
ANTS X at UC San Diego

University of Washington

July 10, 2012

Thanks...

Joint work: Jonathan Bober, Alyson Deines, Joanna Gaski, Ariah Klages-Mundt, Benjamin LeVeque, R. Andrew Ohana, Sebastian Pancratz, Ashwath Rabindranath, Paul Sharaba, Ari Shnidman and Christelle Vincent.

Acknowledgement: John Cremona, Lassina Dembele, Noam Elkies, Tom Fisher, Richard Taylor, and John Voight for helpful conversations and data. I used Sage (`http://www.sagemath.org`) extensively.

Thanks to the organizers of ANTS X for organizing.

Contents

1. Tables

Tables...

Flip through the file `table.pdf`...

Remark: If E/F and $\sigma(\sqrt{5}) = -\sqrt{5}$, then E^σ is another curve over F. Our tables **do** include *both* E and E^σ! We tried to avoid this redundancy but it caused too much confusion.

Rank Data

Table: Counts of classes and curves with bounded norm conductors and specified ranks

	#isog				#isom			
	rank				rank			
bound	0	1	2	**total**	0	1	2	**total**
200	62	2	0	64	257	6	0	263
400	151	32	0	183	580	59	0	639
600	246	94	0	340	827	155	0	982
800	334	172	0	506	1085	285	0	1370
1000	395	237	0	632	1247	399	0	1646
1200	492	321	0	813	1484	551	0	2035
1400	574	411	0	985	1731	723	0	2454
1600	669	531	0	1200	1970	972	0	2942
1800	729	655	0	1384	2128	1178	0	3306
1831	745	667	2	**1414**	2174	1192	2	**3368**

Number of Isogeny Classes of Given Size over F

Table: Number of Isogeny classes of a given size

	size							
bound	1	2	3	4	6	8	10	**total**
199	2	21	3	20	8	9	1	64
1831	498	530	36	243	66	38	3	1414

Isogeny Degrees

Table: Isogeny degrees

degree	**#isog**	**#isom**	**example curve**	Norm($\mathfrak{n}$)
None	498	498	$[\varphi+1,1,1,0,0]$	991
2	652	2298	$[\varphi,-\varphi+1,0,-4,3\varphi-5]$	99
3	289	950	$[\varphi,-\varphi,\varphi,-2\varphi-2,2\varphi+1]$	1004
5	65	158	$[1,0,0,-28,272]$	900
7	19	38	$[0,\varphi+1,\varphi+1,\varphi-1,-3\varphi-3]$	1025

But note:

```
sage: EllipticCurve('17a').quadratic_twist(5).rank()
1
```

Torsion Comparison: F versus $\mathbb{Q}$

Table: Distribution of torsion subgroups up to (norm) conductor 1831

structure	**#isom over F**	**#isom over $\mathbb{Q}$**
1	796	3603
$\mathbb{Z}/2\mathbb{Z}$	1453	4580
$\mathbb{Z}/3\mathbb{Z}$	202	523
$\mathbb{Z}/4\mathbb{Z}$	243	481
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	312	726
$\mathbb{Z}/5\mathbb{Z}$	56	54
$\mathbb{Z}/6\mathbb{Z}$	183	208
$\mathbb{Z}/7\mathbb{Z}$	13	11
$\mathbb{Z}/8\mathbb{Z}$	21	16
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	51	60
$\mathbb{Z}/9\mathbb{Z}$	6	4
$\mathbb{Z}/10\mathbb{Z}$	12	8
$\mathbb{Z}/12\mathbb{Z}$	6	2
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	11	6
$\mathbb{Z}/15\mathbb{Z}$	**1**	**0**
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	2	1

Shafarevich-Tate Groups

Table: $Ш$

#$Ш$	**#isom**	**first curve having #$Ш$**	Norm($\mathfrak{n}$)
1	3191	$[1, \varphi+1, \varphi, \varphi, 0]$	31
4	84	$[1, 1, 1, -110, -880]$	45
9	43	$[\varphi+1, -\varphi, 1, -54686\varphi - 35336, -7490886\varphi - 4653177]$	76
16	16	$[1, \varphi, \varphi+1, -4976733\varphi - 3075797, -6393196918\varphi - 3951212998]$	45
25	2	$[0, -1, 1, -7820, -263580]$	121
36	2	$[1, -\varphi+1, \varphi, 1326667\varphi - 2146665, 880354255\varphi - 1424443332]$	1580

2. Finding all E attached to a rational newform

The Modularity Conjecture

We *assume* the standard modularity conjecture.

Conjecture

$$\{L(E,s) : E/F \text{ cond } \mathfrak{n}\} = \{L(f,s) : \text{ newform } f \in S_{(2,2)}(\Gamma_0(\mathfrak{n}); \mathbb{Q})\}$$

Unpublished Remark (Taylor): If $E[3]|_{\mathrm{Gal}(\overline{\mathbb{Q}}/F(\zeta_3))}$ is absolutely irreducible, then modularity should follow from work of Gee and Kisin.

Finding an E attached to a rational newform

Theorem

Assume the modularity conjecture. There is an algorithm that takes as input a newform $f \in S_{(2,2)}(\Gamma_0(\mathfrak{n}); \mathbb{Q})$ and outputs an elliptic curve E/F with $L(E, s) = L(f, s)$.

Proof.

1. **Bound.** By computing all the rational newforms in $S_{(2,2)}(\Gamma_0(\mathfrak{n}); \mathbb{Q})$, find a bound B so that the eigenvalues $a_{\mathfrak{p}}$ for $N(\mathfrak{p}) \leq B$ determine a newform.
2. **Enumerate** the countably many elliptic curves E/F in any way you like; when you find one with conductor $\mathfrak{n}$, use the bound B to determine whether or not $L(E, s) = L(f, s)$.
3. **Terminates.** Since E corresponds to *some* newform, this procedure must terminate with the correct answer.

More efficiently finding an E corresponding to f

1. **Sieved enumeration** – use $a_{\mathfrak{p}}(f)$ to impose congruence conditions on coefficients in Weierstrass equation.
2. **Torsion families** – use $a_{\mathfrak{p}}(f)$ to determine whether $\ell \mid \#E(F)$, and if so search over the family of curves with ℓ-torsion.
3. **Congruence families** – if you know some E' and that $E'[\ell] \approx E[\ell]$, use Tom Fisher's explicit families.
4. **Twisting** – find a minimal conductor twist.
5. **Cremona-Lingham** – find curves with good reduction outside $\mathfrak{n}$.
6. **Dembele** – determine periods from special values of L-series.
7. **Elkies** – use the λ invariant.

There is no analogue of Cremona's approach (modular symbols + periods).

Enumerating the isogeny class of a curve over a number field

Compute the isogeny class of a curve using the following two steps repeatedly on each curve we find until we find nothing new.

1. **Billerey (2011).** Compute a superset S of the set of prime degrees of isogenies $E \to E'$.
2. **Velu.** For each $\ell \in S$, use Velu's formulas (e.g., as in Kohel's thesis) to find all $\psi : E \to E'$ of degree ℓ.

Thus... no analogue of Mazur's theorem is needed!

3. Finding newforms

Lasina Dembele's Thesis...

1. **Quaternions over F.** ramified only at the two infinite places.
2. **Maximal order.** Let $R = \mathbb{Z}[(1+\sqrt{5})/2] = \mathbb{Z}[\varphi]$.

$$S = R\Big[\frac{1}{2}(1-\overline{\varphi}i+\varphi j),\ \frac{1}{2}(-\overline{\varphi}i+j+\varphi k),\ \frac{1}{2}(\varphi i-\overline{\varphi}j+k),\ \frac{1}{2}(i+\varphi j-\overline{\varphi}k)\Big].$$

3. $\mathbb{P}^1(R/\mathfrak{n}) =$ equivalence classes of column vectors with two coprime entries $a, b \in R/\mathfrak{n}$, modulo the action of $(R/\mathfrak{n})^*$.
4. **Split.** For each $\mathfrak{p} \mid \mathfrak{n}$, fix isomorphism $F[i,j,k] \otimes F_{\mathfrak{p}} \approx M_2(F_{\mathfrak{p}})$; induces left action of S^* on $\mathbb{P}^1(R/\mathfrak{n})$.
5. **Jacquet-Langlands.** Isomorphism of Hecke modules $\mathbb{C}[S^*\backslash\mathbb{P}^1(R/\mathfrak{n})] \cong M_{(2,2)}(\Gamma_0(\mathfrak{n}))$.
6. **Icosians.** S^* acts on $\mathbb{P}^1$ through the *icosian* group of order 120.
7. $T_{\mathfrak{p}}([x]) = \sum[\alpha x]$, where sum is over the classes $[\alpha] \in S/S^*$ with $N_{\mathrm{red}}(\alpha) = \pi_{\mathfrak{p}}$, where $\pi_{\mathfrak{p}}$ is fixed choice of positive generator of $\mathfrak{p}$.

Implementation Notes

I did an optimized implementation of the above algorithm.

1. Critical to compute with $\mathbb{P}^1(R/\mathfrak{n})$ very, very quickly.
2. **Prime power $\mathfrak{n} = \mathfrak{p}^e$ case:** Each $[x : y] \in \mathbb{P}^1(R/\mathfrak{p}^e)$ has a unique representative $[1 : b]$ or $[a : 1]$ with a divisible by $\mathfrak{p}$. Easy to put any $[x : y]$ in this canonical form.
3. **General case:** factor $\mathfrak{n} = \prod_{i=1}^m \mathfrak{p}_i^{e_i}$. Have a bijection $\mathbb{P}^1(R/\mathfrak{n}) \cong \prod_{i=1}^m \mathbb{P}^1(R/\mathfrak{p}_i^{e_i})$, thus reducing to the prime power case. Represent elements of $R/\mathfrak{n}$ as m-tuples in $\prod R/\mathfrak{p}_i^{e_i}$, making computation of the bijection trivial.
4. **Very fast:** compute presentation of space and a Hecke operator in a few seconds for norm level hundreds of thousands.

(Even sparser matrices and faster presentation than modular symbols give over $\mathbb{Q}$!)

Current Work in Progress

Goal: Find all rational newforms of norm conductor up to the first of *analytic rank 4*, which might be norm conductor 1,209,079.

Sparse linear algebra: S. Pancratz and I implemented fast mod-p linear algebra that I am now running (uses Linbox/BLAS for dense).

Status: have found all rational newforms for over 83% of the levels of norm conductor up to 252,089.

Estimate: (Schneidman) $<$ **200,000 hours** CPU time to achieve goal.

rank	**norm**$(\mathfrak{n})$	**equation**	**person**
0	31 (prime)	$[1, \varphi+1, \varphi, \varphi, 0]$	Dembele
1	199 (prime)	$[0, -\varphi-1, 1, \varphi, 0]$	Dembele
2	1831 (prime)	$[0, -\varphi, 1, -\varphi-1, 2\varphi+1]$	Dembele
3	$26{,}569 = 163^2$	$[0, 0, 1, -2, 1]$	Elkies
4	1,209,079 (prime)	$[1, -1, 0, -8-12\varphi, 19+30\varphi]$	Elkies
5	64,004,329	$[0, -1, 1, -9-2\varphi, 15+4\varphi]$	Elkies

(Cremona has found all elliptic curves over $\mathbb{Q}$ up to the first of rank 4.)