Computing Tables of Elliptic Curves over $\mathbb{Q}(\sqrt{5})$.

Alyson Deines
University of Washington

Joint work with:
Jonathan Bober, Ariah Klages-Mundt, Benjamin LeVeque, R. Andrew Ohana, Sebastian Pancratz, Ashwath Rabindranath, Paul Sharaba, Ari Shnidman, William Stein, and Christelle Vincent

Outline

Exciting Times for Elliptic Curves

- Computations
  - Antwerp tables, all curves up to conductor 200, tables of curves with bad reduction only at 2 and 3
  - For the past 20+ years Cremona has been building tables of elliptic curves over $\mathbb{Q}$.
  - Stein-Watkins tables, lots of curves with small-ish coefficients
  - Stein-Miller tables, verify full BSD for curves ≤ 5000 (for all but 11 curves)

Why $\mathbb{Q}(\sqrt{5})$?

Let $F = \mathbb{Q}(\sqrt{5})$ and $\varphi = \frac{1+\sqrt{5}}{2}$.

- F is a totally real number field with ring of integers $\mathcal{O}_F = \mathbb{Z}[\varphi]$.
- Ordering by discriminants $\mathbb{Q}(\sqrt{5})$ is the **next** totally real number field after $\mathbb{Q}$.
- F has narrow class number one.
- The unit group is $\{\pm 1\} \times \langle \varphi \rangle$.
- F has 31 CM j-invariants ($\mathbb{Q}$ only has 13)
- $X_0(17)$ has rank 1 over F, so lots of (infinitely many) isogenies of degree 17 over F.

Outline

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

Theorem

The field $\mathbb{Q}(\sqrt{5})$ has 31 distinct $\bar{\mathbb{Q}}$-isomorphism classes of CM elliptic curves, more than any other quadratic field.

Let H_D be the minimal polynomial of the j-invariant of any elliptic curve with CM by the order $\mathcal{O}_D$. Excluding degree 1 H_D:

Field	D so that H_D has roots in field
$\mathbb{Q}(\sqrt{2})$	$-24, -32, -64, -88$
$\mathbb{Q}(\sqrt{3})$	$-36, -48$
$\mathbb{Q}(\sqrt{5})$	$-15, -20, -35, -40, -60, -75, -100, -115, -235$
$\mathbb{Q}(\sqrt{6})$	-72
$\mathbb{Q}(\sqrt{7})$	-112
$\mathbb{Q}(\sqrt{13})$	$-52, -91, -403$
$\mathbb{Q}(\sqrt{17})$	$-51, -187$
$\mathbb{Q}(\sqrt{21})$	-147

These tables and much of the code were produced at a summer REU at UW last summer. The tables (and a little code) can be found at

`https://github.com/williamstein/sqrt5`

Quick remark: Let $\sigma(\sqrt{5}) = -\sqrt{5}$. If $E/\mathbb{Q}(\sqrt{5})$, then E^σ is another curve over $\mathbb{Q}(\sqrt{5})$ and **both** are in our tables!

Curve Counts up to Rank 2

rank	#isog	#isom	smallest Norm($\mathfrak{n}$)
0	745	2174	31
1	667	1192	199
2	2	2	1831
total	1414	3368	–

Rank Records

The following are the smallest known curves of given ranks over $\mathbb{Q}(\sqrt{5})$.

rank	Norm($\mathfrak{n}$)	equation	person
0	31(prime)	$[1, \varphi + 1, \varphi, \varphi, 0]$	Dembélé
1	199(prime)	$[0, -\varphi - 1, 1, \varphi, 0]$	Dembélé
2	1831(prime)	$[0, -\varphi, 1, -\varphi - 1, 2\varphi + 1]$	Dembélé
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

Number of Isogeny Classes of a Given Size

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

Due to Kenku, over $\mathbb{Q}$ isogeny classes only have up to 8 curves.

Isogeny Degrees

degree	#isog	#isom
None	498	498
2	652	2298
3	289	950
5	65	158
7	19	38

Note: These are the isogeny degrees of curves found in our tables. For example, 17 isogenies will occur, we just haven't gone far enough to get examples.

Torsion Subgroups: $\mathbb{Q}(\sqrt{5})$ vs. $\mathbb{Q}$

structure	#isom over $\mathbb{Q}(\sqrt{5})$	#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
$\mathbb{Z}/2 \oplus \mathbb{Z}/4\mathbb{Z}$	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
$\mathbb{Z}/2 \oplus \mathbb{Z}/8\mathbb{Z}z$	2	1

Outline

Strategies for Finding Elliptic Curves attached to HMF's

As in Cremona's tables, we have (at the time we assumed) modularity:

Theorem

Siksek et al. For elliptic curves over real quadratic number fields, there is a bijection

$$\{L(E,s) : E/\mathbb{Q}(\sqrt{5}) \textit{ with conductor } \mathfrak{n}\} \to$$

$$\{L(f,s) : \textit{ newform } f \in S_{(2,2)}(\mathfrak{N})\}.$$

We will also assume we can quickly compute $a_{\mathfrak{p}}(f)$'s for $f \in S_{(2,2)}(\mathfrak{N}; \mathbb{Q}))$.

Naive Enumeration

1. Compute all $a_{\mathfrak{p}}(f)$ up to a large bound $N(\mathfrak{p}) \leq B$ for all rational newforms forms $f \in S_{(2,2)}(\mathfrak{N}; \mathbb{Q})$. Pick B large enough that the $a_{\mathfrak{p}}(f)$ uniquely determine f.
2. Systematically enumerate all curves

$$E : y^2 = x^3 + ax + b,$$

compute $a_{\mathfrak{p}}(E)$, and compare with rational newforms. If we find a match, compute the conductor.
This is deterministic and terminates, but ridiculously slow.

Why bad? E_f could have large coefficients and relatively small conductor.

Sieved Enumeration

For several primes $\mathfrak{p}$, find all curves mod $\mathfrak{p}$ with a given $a_{\mathfrak{p}}$. In other words, find curves E such that $\#E(\mathcal{O}_F/\mathfrak{p}) = N(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$.

Then use the Chinese Remainder Theorem to lift to a curve over $\mathcal{O}_F$ with the given $a_{\mathfrak{p}}$'s.

Again, if E has large coefficients, it will not be found quickly. In practice, this works well if the number of primes is optimally chosen.

Torsion Families

The following two theorems we can refine our search space:

Theorem

(Kamienny-Najman) The following is a complete list of torsion structures for elliptic curves over $\mathbb{Q}(\sqrt{5})$*:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z}, & 1 \leq m \leq 10, m = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & 1 \leq m \leq 4 \\ \mathbb{Z}/15\mathbb{Z}. & \end{array}$$

Moreover, there is a unique elliptic curve with 15-torsion.

Theorem

Let ℓ *be a prime and* E *an elliptic curve over* $\mathbb{Q}(\sqrt{5})$*. Then* $\ell | \#E'(\mathbb{Q}(\sqrt{5}))_{tor}$ *for some elliptic curve* E' *in the isogeny class of* E *if and only if* $\ell | N(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$ *for all odd primes* $\mathfrak{p}$ *at which* E *has good reduction.*

Torsion Families

- We use the $a_{\mathfrak{p}}$ to decide if it is likely some elliptic curve in the isogeny class of E_f has an F-rational ℓ torsion point.
- Search over ℓ torsion families.

Example: This is how we found

$$y^2 + \varphi y = x^3 + (27\varphi - 43)x + (-80\varphi + 128)$$

with norm conductor 145 and torsion subgroup $\mathbb{Z}/7\mathbb{Z}$.

Congruence Families

Tom Fisher has explicit families so that once you know E', you can twist to find other curves E so that $E'[\ell] \cong E[\ell]$.
Example: We had already found

$$E' : y^2 + (\varphi + 1)y = x^3 + (\varphi - 1)x^2 + (-2\varphi)x$$

with norm conductor 369. We found $E[7] \cong E'[7]$ and used formulas to write down

$$E : y^2 + \varphi xy = x^3 + (\varphi - 1)x^2 + (-257364\varphi - 159063)x + (-75257037\varphi - 46511406)$$

with norm conductor 1476.

Twisting

If $E : y^2 = x^3 + ax + b$ has conductor $\mathfrak{n}$ and $d \in \mathcal{O}_F^*$ is square-free and coprime to $\mathfrak{n}$, then $E^d : dy^2 = x^3 + ax + b$ is the twist of E by d and the conductor of E^d is divisible by $d^2\mathfrak{n}$.

To find more curves, just twist by d in some range. Specifically, d so that $N(d) \leq \sqrt{B/C}$ where B is the bound on the size of conductors and C is the conductor of E.

Elliptic Curves with Good Reduction Outside S

We used Magma's implementation of Cremona and Lingham's algorithm for finding elliptic curves with good reduction outside a set of primes S.
Example:

$$y^2 + (\varphi + 1)xy + y = x^3 - x^2 + (-19\varphi - 39)x + (-143\varphi - 4)$$

with norm conductor 1331.

Special values of twisted L-series

This method is due to Dembélé. It uses special values of L-functions to guess the periods of a given curve E. All it takes as input are the level $\mathfrak{N}$ and the L-series (i.e., a large number of $a_{\mathfrak{p}}$'s.)

Outline

Modularity over $\mathbb{Q}(\sqrt{5})$

Let $f \in S_2(\mathfrak{N})$ with Fourier coefficients $a_{\mathfrak{p}}$, then the L-series of f is

$$L(f,s) = \sum_{\mathfrak{n} \in \mathcal{O}_F} \frac{a_{\mathfrak{m}}(f)}{N(\mathfrak{m})^s}$$

For $\mathfrak{p} \not| \mathfrak{N}$, $a_{\mathfrak{p}}(E) = N(\mathfrak{p}) + 1 - \#\bar{E}(\mathbb{F}_{\mathfrak{p}}$ and

$$L(E,s) = \prod_{\mathfrak{p}|\mathfrak{N}} \left(1 - \frac{a_{\mathfrak{p}}(E)}{N(\mathfrak{p})^s}\right)^{-1} \prod_{\mathfrak{p} \not| \mathfrak{N}} \left(1 - \frac{a_{\mathfrak{p}}(E)}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s-1}}\right)^{-1}.$$

Then there exists an elliptic curve E_f such that $L(E_f, s) = L(f,s)$.

Mixed Periods

Let σ_1, σ_2 be the real embeddings of F. For each E, we get two embeddings into the complex numbers, so two period lattices.
Let Ω_E^+ be the smallest positive real period corresponding to σ_1, Ω_E- is similarly the smallest imaginary period. Let $\Omega_{\bar{E}}^+, \Omega_{\bar{E}}^-$ be similarly for σ_2.

Mixed Periods:

$$\Omega_E^{++} = \Omega_E^+ \Omega_{\bar{E}}^+ \qquad \Omega_E^{+-} = \Omega_E^+ \Omega_{\bar{E}}^-$$
$$\Omega_E^{-+} = \Omega_E^- \Omega_{\bar{E}}^+ \qquad \Omega_E^{--} = \Omega_E^- \Omega_{\bar{E}}^-$$

Recovering a Curve from Mixed Periods:

From mixed periods, we have a few choices for the j-invariant of E: $\sigma_1(j(E)) = j(\tau_1(E)$ or $j(\tau_2(E)$ and $\sigma_2(j(E)) = j(\tau_1(\bar{E})$ or $j(\tau_2(\bar{E})$ where

$$\tau_1(E) = \frac{\Omega_E^{-+}}{\Omega_E^{++}} \qquad \tau_2(E) = \frac{1}{2}\left(1 + \frac{\Omega_E^{-+}}{Omega_E^{++}}\right)$$
$$\tau_1(\bar{E}) = \frac{\Omega_E^{+-}}{\Omega_E^{++}} \qquad \tau_2(\bar{E}) = \frac{1}{2}\left(1 + \frac{\Omega_E^{+-}}{Omega_E^{++}}\right)$$

Assuming we know the discriminant Δ, we can find the elliptic curve. Note: we have to guess at Δ and then try to recognize c_4, c_6 invariants algebraically.

Twisted L-functions

Given f and a primitive quadratic character $\chi : (\mathcal{O}_F/\mathfrak{p})^* \to \pm 1$, we can construct the twisted L-function:

$$L(f, \chi, s) = \sum_{\mathfrak{n} \in \mathcal{O}_F} \frac{\chi(m) a_{\mathfrak{m}}(f)}{N(\mathfrak{m})^s}$$

where m is a totally positive generator of $\mathfrak{m}$.

Oda's Conjecture

Let $s, s' \in \{+,-\} = \{\pm 1\}$ and pick χ so that $\chi(\varphi) = s'$ and $\chi(1-\varphi) = s$. Let

$$\tau(\chi) = \sum_{\alpha \pmod{\mathfrak{p}}} \chi(\alpha) \exp(2\pi i \mathrm{Tr}(\alpha / m\sqrt{5}))$$

be the Gauss sum and let c_χ be some integer.

Conjecture (Oda, reformulated by Dembélé)

Using the above notation:

$$\Omega_E^{s,s'} = c_\chi \tau(\bar{\chi}) L(E, \chi, 1)\sqrt{5}.$$

Computing Mixed Periods

- Compute $\Omega_E^{s,s'} = c_\chi \tau(\bar{\chi}) L(E,\chi,1)\sqrt{5}$ for several characters.
- Try to recognize quotients of $\frac{c_\chi}{c_{\chi'}}$ as rational numbers for for several characters χ'.
- Use a good guess to try and construct E:
$\Omega_{E,\text{guess}}^{s,s'} = \tau(\bar{\chi}) L(E,\chi,1)\sqrt{5} \left(\text{lcm}\{\text{numerator}\frac{c_\chi}{c_{\chi_i}}, i = 1,2,...\}\right)^{-1}$

Slow, but did the job

- Need to make a large number of guesses
- Must compute many Hecke eigenvalues, i.e., slow.
- It was what finally filled out the tables!

Outline

Enumerating the Elliptic Curves in an Isogeny Class

Over $\mathbb{Q}$ this relies on:

- Mazur's theorem bounds the degree of the isogeny over $\mathbb{Q}$ to less than 163.
- Vélu's formulas allow us to enumerate all p-isogenies (if any)

Over a number field F Larson-Vaintrob show there is a computable constant C_F which bounds the degree, but in general we do not have Mazur's theorem. Using Billerey (2011) we don't need it.
Over $\mathbb{Q}(\sqrt{5})$:

- Using Billerey, we can compute a superset S of the prime degrees of isogenies $E \to E'$.
- Using Velu, for each $\ell \in S$ we can find all $\phi : E \to E'$ of degree ℓ.

End result: We were able to enumerate all isomorphism classes of elliptic curves isogenous to the elliptic curves found above.

Outline

Computing Hilbert Modular Forms

We need lots of Hecke Eigenvalues to compute the L-functions from Dembélé's algorithm.

- The algorithm is from Lassina Dembélé's thesis.
- Generalizes the method of Brandt matrices.
- Dembélé's speed up: Computing right ideal classes is the same as computing $\mathbb{P}^1(\mathcal{O}_F/\mathfrak{n})$.

Dembélé's Algorithm

Let $F = \mathbb{Q}(\sqrt{5})$, $B = F[i, j, k]$ be the Hamilton quaternion algebra over F and the icosian ring R a maximal order of B:
$R = \mathcal{O}_F[\frac{1}{2}(1 - \bar{\varphi}i + \varphi j), \frac{1}{2}(-\bar{\varphi}i + \varphi j), \frac{1}{2}(\varphi i - \bar{\varphi}j + k), \frac{1}{2}(i + \varphi j - \bar{\varphi}k)]$

Eichler-Shimura +Jaquet-Langlangs correspondence:

$$S_{(2,2)}(\mathfrak{N}) \cong S_2^B(\mathfrak{N}).$$

Dembélé's Algorithm

- Computing $S_2^B(\mathfrak{N})$ as the vector space $\mathbb{C}[R^* \setminus \mathbb{P}^1(\mathcal{O}_F/\mathfrak{N})]$:
  - View $\mathbb{P}^1(\mathcal{O}_F/\mathfrak{N})$ as column vectors $\begin{pmatrix} a \\ b \end{pmatrix}$
  - For $\mathfrak{p}|\mathfrak{N}$, $B \otimes F_\mathfrak{p} \cong M_2(F_\mathfrak{p})$ - induces left action of R^* on $\mathbb{P}^1(\mathcal{O}_F/\mathfrak{N})$
  - Mod out by R^*.
  - Get $\mathbb{C}$-vector space $\mathbb{C}[R^* \setminus \mathbb{P}^1(\mathcal{O}_F/\mathfrak{N})]$!
- For $\mathfrak{p} \not| \mathfrak{N}$, left action is $T_\mathfrak{p}([x]) = \sum [\alpha x]$, $[\alpha] \in R/R^*$ with $N_{\text{red}}([\alpha]) = \pi_p$

Dembélé's Algorithm

What makes it fast:
Instead of changing Eichler orders of level $\mathfrak{N}$, change $\mathbb{P}^1(\mathcal{O}_F/\mathfrak{N})$
Issue: Need tens of thousands of $\mathbb{P}^1(\mathcal{O}_F/\mathfrak{N})$.
Keys for computing $\mathbb{P}^1(\mathcal{O}_F/\mathfrak{N})$ quickly:

- Write in terms of prime powers $\mathfrak{N} = \prod_{i=1}^{m} \mathfrak{p}^{e_i}$
- Fix the largest size of ${\mathfrak{p}_\mathfrak{i}}^{e_i}$ and m.
- Hash out exactly what happens to primes $p \in \mathbb{Z}$ in each case (inert, split, ramified.)

Some Code:

https://github.com/williamstein/psage

Outline

Ranks up to rank 3

At the MRC in June, 2012, we started working on verifying (conjecturally) that Elkie's curve is the first curve over $\mathbb{Q}(\sqrt{5})$ of rank 3.
How:

- Compute dimension one subspaces of Hilbert modular forms with rational $a_{\mathfrak{p}}$, use sparse linear algebra to make this fast.
  Important: we don't need to find the curves.
- From $a_{\mathfrak{p}}$ compute derivatives of L-functions.

`https://github.com/williamstein/mrc-2012`

Future Work

1. Currently working on rank 3, rank 4?
2. Stein-Watkins type tables
3. Modular Abelian Varieties

Thank you!