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

William Stein (University of Washington)
in Chicago (UIC) at the Atkin Memorial Workshop

University of Washington

April 27–29, 2012

Joint Work...

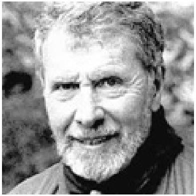
This talk represents joint work with Jonathan Bober, Alyson Deines, Joanna Gaski, Ariah Klages-Mundt, Benjamin LeVeque, R. Andrew Ohana, Ashwath Rabindranath, and Paul Sharaba.

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.

Motivation

"The object of numerical computation is theoretical advance."

- Oliver Atkin



Contents

1: Tables

Source: These tables and much code were made at a summer REU[1] at University of Washington last summer.

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

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

[1] Research Experience for Undergraduates

Counts of Curves over F up to Norm Conductor 1831

Table: Curves over $\mathbb{Q}(\sqrt{5})$

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

Number of Isogeny Classes over F up to Norm Conductor 1831

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

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

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

Torsion Subgroups of Elliptic Curves over F

(I don't trust this table.)

Table: Distribution of torsion subgroups up to norm conductor 1831

structure	**#isom**	**example curve**	Norm($\mathfrak{n}$)
1	296[2]	$[0, -1, 1, -8, -7]$	225
$\mathbb{Z}/2\mathbb{Z}$	1453	$[\varphi, -1, 0, -\varphi - 1, \varphi - 3]$	164
$\mathbb{Z}/3\mathbb{Z}$	202	$[1, 0, 1, -1, -2]$	100
$\mathbb{Z}/4\mathbb{Z}$	243	$[\varphi + 1, \varphi - 1, \varphi, 0, 0]$	79
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	312	$[0, \varphi + 1, 0, \varphi, 0]$	256
$\mathbb{Z}/5\mathbb{Z}$	56	$[1, 1, 1, 22, -9]$	100
$\mathbb{Z}/6\mathbb{Z}$	183	$[1, \varphi, 1, \varphi - 1, 0]$	55
$\mathbb{Z}/7\mathbb{Z}$	13	$[0, \varphi - 1, \varphi + 1, 0, -\varphi]$	41
$\mathbb{Z}/8\mathbb{Z}$	21	$[1, \varphi + 1, \varphi, \varphi, 0]$	31
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	51	$[\varphi + 1, 0, 0, -4, -3\varphi - 2]$	99
$\mathbb{Z}/9\mathbb{Z}$	6	$[\varphi, -\varphi + 1, 1, -1, 0]$	76
$\mathbb{Z}/10\mathbb{Z}$	12	$[\varphi + 1, \varphi, \varphi, 0, 0]$	36
$\mathbb{Z}/12\mathbb{Z}$	6	$[\varphi, \varphi + 1, 0, 2\varphi - 3, -\varphi + 2]$	220
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	11	$[0, 1, 0, -1, 0]$	80
$\mathbb{Z}/15\mathbb{Z}$	1	$[1, 1, 1, -3, 1]$	100
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	2	$[1, 1, 1, -5, 2]$	45

[2] On the previous slide there were 498 with no isogenies, so this or that

Comparison: F versus $\mathbb{Q}$

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

structure	#isom over F	#isom over $\mathbb{Q}$
1	296 (*)	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 newform g

The Modularity Conjecture

Modularity is critical to making systematic tables.

Conjecture

There is a bijection[a]

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

[a] We consider L-series to be equal only if all of their Euler factors are equal!

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

Finding an E attached to a newform g

Theorem

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

Proof.

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. 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 $L(E,s) = L(g,s)$. Since E corresponds to *some* newform, this procedure must terminate with the correct answer. $\square$

1. Similar argument for abelian varieties of GL_2-type.
2. Cremona: "this algorithm is not *respectable*!"

Finding an E attached to a newform g

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

Jon Bober's talk next will have a lot more to say about this.

Finding *all* E attached to a newform g

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

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

Billerey in Code

```
def _plstar1(E, q):
    R.<x> = F[]
    t12 = 2048*x^12 -6144*x^10 + 6912*x^8 -3584*x^6 + 840*x^4 -72*x^2 + 1
    t12p = 2048*x^6 -6144*x^5 + 6912*x^4 -3584*x^3 + 840*x^2 -72*x + 1
    t24 = 2*(t12)^2 - 1
    #this is only for primes that have no ramification and have good reduction
    if len(F.primes_above(q)) == 1:
        w1 = 1 - 2*(q^12)*t12(x/(2*q)) + q^24
        t1 = E.change_ring(F.ideal(q).residue_field()).trace_of_frobenius()
        w = w1(t1)
        m = []
        for zee in factor(ZZ(w)):
            m.append(zee[0])
        return m
    else:
        v = F.primes_above(q)
        t1 = E.change_ring(v[0].residue_field()).trace_of_frobenius()
        t2 = E.change_ring(v[1].residue_field()).trace_of_frobenius()
        w1 = t12p(x^2/(4*q))
        w = 1 - 4*(q^12)*w1(t1)*w1(t2) - 2*(q^24)*(1- 2*(w1(t1)^2 + w1(t2)^2)) \
               - 4*(q^36)*w1(t1)*w1(t2) + q^48
        m = []
        for zee in factor(ZZ(w)):
            m.append(zee[0])
        return m

def _plstar12(E, q):
    #same caveat, only for unramified and good reduction
    if len(F.primes_above(q)) == 1:
       t1 = E.change_ring(F.prime_above(q).residue_field()).trace_of_frobenius()
       m = [q]
       try:
           for v in factor(t1):
```

```
            m.append(v[0])
        for v in factor(t1^2 - q^2):
            m.append(v[0])
        for v in factor(t1^2 - 4*q^2):
            m.append(v[0])
        for v in factor(t1^2 - 3*q^2):
            m.append(v[0])
        s1 = set(m)
        m = list(s1)
        return m
    except ArithmeticError:
        return 0
else:
    t1 = E.change_ring(F.primes_above(q)[0].residue_field()).trace_of_frobenius()
    t2 = E.change_ring(F.primes_above(q)[1].residue_field()).trace_of_frobenius()
    m = [q]
    try:
        for v in factor((t1^2 + t2^2 - q^2)^2 - 3*(t1^2)*(t2^2)):
            m.append(v[0])
        for v in factor(t1^2 - t2^2):
            m.append(v[0])
        for v in factor(t1^2 +t2^2 - 4*q^2):
            m.append(v[0])
        for v in factor((t1^2 + t2^2 - 3*q^2)^2 - (t1*t2)^2):
            m.append(v[0])
        s1 = set(m)
        m = list(s1)
        return m
    except ArithmeticError:
        return 0
```

```
def billerey_primes(E):
    ans = set([])
    Bad = [v[0] for v in E.conductor().norm().factor()]
    Pr = prime_range(1000)
    num = 0
    i = 0
    X = [set([3])]
    while num < 3:
        if not Pr[i] in Bad and Pr[i] != 5:
            try:
                X.append(set(_plstar1(E, Pr[i]) + _plstar12(E, Pr[i])))
                num += 1
            except TypeError:
                pass
        i += 1
    ans = (X[1].intersection(X[2])).intersection(X[3])
    ans = ans.union(set(Bad)).union(set([2,3,5]))
    return list(sorted(ans))
```

3: Finding newforms

Computing Hilbert Modular Forms over F

1. The algorithm is from Lassina Dembele's Ph.D. thesis. See his *Explicit computation of Hilbert modular forms on* $\mathbb{Q}(\sqrt{5})$ (2005).
2. Jacquet-Langlands: Computing Hecke module of Hilbert modular forms of level $\mathfrak{n}$ over F same as computing Hecke module with basis that right ideal classes in a certain order (of level $\mathfrak{n}$) in the Hamilton quaternion algebra over F.
3. Dembele: Computing right ideal classes same as computing $\mathbb{P}^1(R/\mathfrak{n})$, where $R = \mathbb{Z}[\varphi] \subset F$.

Dembele's Algorithm in One Slide

1. Hamiltonian quaternions $F[i,j,k]$ ramified at the infinite places.
2. Maximal order
$$S = R\Big[\frac{1}{2}(1-\overline{\varphi}i+\varphi j),\ \frac{1}{2}(-\overline{\varphi}i+j+\varphi k),\ \frac{1}{2}(\varphi i-\overline{\varphi}j+k),\ \frac{1}{2}(i+\varphi j-\overline{\varphi}k)\Big].$$
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. For each $\mathfrak{p} \mid \mathfrak{n}$, fix *choice* of isomorphism $F[i,j,k] \otimes F_\mathfrak{p} \approx M_2(F_\mathfrak{p})$, which induces a *choice* of left action of S^* on $\mathbb{P}^1(R/\mathfrak{n})$.
5. Jacquet-Langlands: There's an isomorphism of $\mathbb{T}$-modules
$$\mathbb{C}[S^*\backslash\mathbb{P}^1(R/\mathfrak{n})] \cong M_{(2,2)}(\Gamma_0(\mathfrak{n})).$$
6. S^* acts through the *octonian* group (which is finite and explicit).
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

1. Critical that we can compute with $\mathbb{P}^1(R/\mathfrak{n})$ very, 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. (Drew Sutherland-style tricks) We minimize dynamic memory allocation speeding up the code by an order of magnitude, by making some arbitrary bounds.
5. Painful to implement, but it is *fast*. Not included in Sage yet: `http://trac.sagemath.org/sage_trac/ticket/12465`

What Next?

My group's project at the 2012 MRC in Snowbird Utah (June 24–30, 2012) will be to compute Hilbert newforms in $S_{(2,2)}(\Gamma_0(\mathfrak{n}))$ as far as possible, gather *arithmetic statistics* about them (e.g., analytic ranks), make conjectures, and perhaps prove something.

Example Goal: Does the first elliptic curve of rank 3 have norm conductor 163^2 or not?

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

Epilogue (or Prologue)

```
On Wed, Feb 2, 2011 at 12:18 PM, William Stein <wstein@gmail.com> wrote:
> Hi John [Voight],
>
> I'm planning to try to say something about these sorts of things...
> mainly that I'm ignorant in each case.  But I'm curious what thoughts
> you might have about these...
>
>       -- stein-watkins style search
>       -- elkies approach: Q(sqrt(5)) curves
>       -- rank info
>       -- gens (simon 2-descent output)
>       -- L-function (fast computation of a_p?)
>       -- congruence number
>       -- isogeny class (enumerate)
>       -- root number
>       -- torsion subgroup
>       -- tamagawa numbers
>       -- all integral points
>       -- Kodaira symbols
>       -- zeros of L(E/F,s) in critical strip
>       -- notion of "canonical" minimal weierstrass model
>       -- picture
>       -- height pairing / regulator
>       -- heegner points
>       -- #Sha(E/F) -- when hypo of Zhang's work satisfied, there is hope.
>       -- images of Galois reps?
>       -- as much as possible of the above for modular abelian varieties A_f.
```