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...

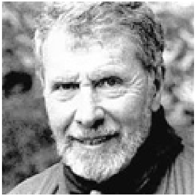
This talk represents joint work with Jonathan Bober, Alyson Deines, Joanna Gaski, Ariah Klages-Mundt, Benjamin LeVeque, R. Andrew Ohana, Ashwath Rabindranath, and Paul Sharaba.

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



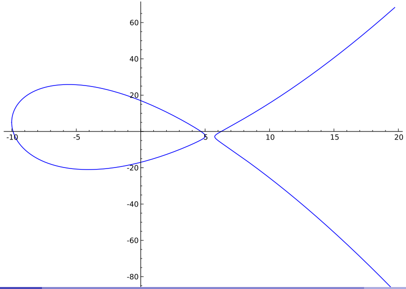
My Two Talks

- **Talk 1:** (Fri at 3pm) Survey talk about elliptic curves over F.

- **Talk 2:** (Sun at 8:30am) Tables of elliptic curves over F.

Background: Elliptic Curves

```
sage: E = EllipticCurve([1,-1,0,-79,289]); E
Elliptic Curve defined by
   y^2 + x*y = x^3 - x^2 - 79*x + 289
over Rational Field
sage: v = E.gens(); v
[(-9:19:1), (-8:23:1), (-7:25:1), (4:-7:1)]
sage: v[0] + 2*v[1]
(-467/529:235410/12167:1)
sage: E.plot()
```



Background: The Million Dollar Question – BSD

Analogue of Riemann Zeta function for E is the L-function:

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where, e.g., $a_p = p + 1 - \#E(\mathrm{GF}(p))$ for primes p.

Birch and Swinnerton-Dyer Rank Conjecture:

$$\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}(E(\mathbb{Q}))$$

Here $E(\mathbb{Q}) \approx \mathbb{Z}^{\mathrm{rank}(E(\mathbb{Q}))} \times E(\mathbb{Q})_{\mathrm{tor}}$.

Birch and Swinnerton-Dyer Formula: $r = \mathrm{rank}(E(\mathbb{Q}))$.

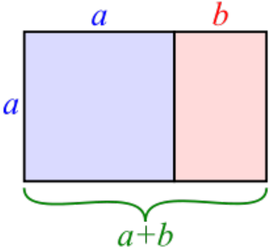
$$\frac{L^{(r)}(E/\mathbb{Q},1)}{r!} = \frac{\Omega_E \cdot \prod_p c_{E,p} \cdot \mathrm{Reg}_E \cdot \#Ш(E)}{\#E(\mathbb{Q})^2_{\mathrm{tor}}}$$

Elliptic Curves over $\mathbb{Q}$ (in one very dense slide!)

- **Computation:**
  1. Cremona: data about *all* curves with conductor $\leq 234446+$.
  2. First of ranks $0, 1, 2, 3, 4$ have $N_E = 11$, 37, 389, 5077, 234446.
  3. Stein-Watkins: table of data about 136,832,795 curves with conductor $N \leq 10^8$, and 11,378,911 with prime conductor $N \leq 10^{10}$.
  4. (Stein, Miller, et al.) Full BSD for conductor ≤ 5000 and rank ≤ 1 (for all but 11 curves with reducible mod $5, 7$).
  5. (Stein, Wuthrich) For a rank 2 curve: BSD "at p" for all but 19 primes $p \leq 48,859$.
- **Theory:**
  1. **Theorem** (Wiles et al.) All elliptic curves over $\mathbb{Q}$ are modular.
  2. **Theorem** (Gross-Zagier, Kolyvagin, et al.) Heegner Points, Euler System $\implies$ the Birch and Swinnerton-Dyer rank conjecture is true for curves with $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$.
  3. **Iwasawa Theory** (Kato, Mazur, Skinner, et al.): p-adic L-functions; much known toward analogues of BSD.
- **Theorem** (Mazur) Classification of isogenies and torsion.
- **Theorem** (Gauss, Heegner et al.): Classification of CM curves.

The Golden Ratio (obligatory colloquium slide)

$$\frac{a+b}{a} = \frac{a}{b} = \varphi$$



Thus $1 + \varphi^{-1} = \varphi$, so $\varphi^2 - \varphi - 1 = 0$, hence $\varphi = (1+\sqrt{5})/2$.

> *"[...] the Golden Ratio has inspired thinkers of all disciplines like no other number in the history of mathematics."*
>
> *– Mario Livio (wrote a prize-winning popular book on φ)*

The Field F

1. $F = \mathbb{Q}(\sqrt{5}) = \{a + b\varphi : a, b \in \mathbb{Q}\}$
2. F is the **next** totally real field after $\mathbb{Q}$ (order by $|D|$).
3. Class number 1, so $R = \mathbb{Z}[\varphi]$ is a PID.
4. Unit group: $\{\pm 1\} \times \langle \varphi \rangle$, where $\varphi = \frac{1+\sqrt{5}}{2}$.
5. Totally real fields are *hospitable* for elliptic curves:
    1. Hilbert modular forms and **the Modularity Conjecture** (major area of research since Taylor and Wiles 1990s breakthroughs!):

       $$\{L(E,s) : E/F\} \xrightarrow{\text{conj} \cong} \{L(f,s) : f \text{ certain Hilbert modular forms }\}$$

    2. Shimura curves, Heegner points, Euler systems


Elliptic Curves over F

- **Computation:**
  1. (Pinch) See his talk tomorrow – bounded reduction tables.
  2. (Donnely-Voight) Tables of Hilbert modular newforms up to around norm conductor 7500 (and equations for many curves).
  3. (Stein et al.) Complete (assuming modularity) table of elliptic curves of norm conductor up to 1831 (first rank 2).
  4. Code using Sage to (often) compute BSD invariants.
  5. Classification of CM curves: those with $\mathrm{Aut}(E/\mathbb{C}) \neq \{\pm 1\}$.
- **Theory:**
  1. (Zhang) Gross-Zagier theorem for modular abelian varieties over totally real fields and an Euler system. Consequence: mild (but essential) hypothesis $\implies$ the Birch and Swinnerton-Dyer rank conjecture is true for many curves with $\mathrm{ord}_{s=1} L(E/F, s) \leq 1$.
  2. (Taylor, Gee, Kisin et al.) Modularity theorems
  3. **Iwasawa theory, *p*-adic *L*-functions**: no cusps, so no obvious-to-me construction; but Coates et al. makes me wonder...

Classification of CM Elliptic Curves over F

Proposition

There are 31 distinct $\overline{\mathbb{Q}}$-isomorphism classes of CM elliptic curves defined over F, more than for any other quadratic field.

Let $H_D(X)$ = minimal polynomial of the j-invariant of any elliptic curve with CM by the order $\mathcal{O}_D$. Excluding H_D of degree 1, we find[1]:

Field	D so H_D has roots in field	Field	D so H_D has roots in field
$\mathbb{Q}(\sqrt{2})$	$-24, -32, -64, -88$	$\mathbb{Q}(\sqrt{21})$	-147
$\mathbb{Q}(\sqrt{3})$	$-36, -48$	$\mathbb{Q}(\sqrt{29})$	-232
$\mathbb{Q}(\sqrt{5})$	$-15, -20, -35, -40, -60, -75, -100, -115, -235$	$\mathbb{Q}(\sqrt{33})$	-99
$\mathbb{Q}(\sqrt{6})$	-72	$\mathbb{Q}(\sqrt{37})$	-148
$\mathbb{Q}(\sqrt{7})$	-112	$\mathbb{Q}(\sqrt{41})$	-123
$\mathbb{Q}(\sqrt{13})$	$-52, -91, -403$	$\mathbb{Q}(\sqrt{61})$	-427
$\mathbb{Q}(\sqrt{17})$	$-51, -187$	$\mathbb{Q}(\sqrt{89})$	-267

$$\#\{\text{ CM } j\text{-invariants in } F\ \} = 2 \times 9 + 13 = 31$$

[1] with help from Cremona and Watkins

CM j-invariants over F: here they are

```
sage: cm_j_invariants(QuadraticField(5))
[-12288000, 54000, 0, 287496, 1728, 16581375, -3375,
8000, -32768, -884736, -884736000, -147197952000,
-262537412640768000, 146329141248*a - 327201914880,
-146329141248*a - 327201914880, 9845745509376*a +
22015749613248, -9845745509376*a + 22015749613248,
16554983445/2*a + 37018076625/2, -16554983445/2*a +
37018076625/2, 85995/2*a - 191025/2, -85995/2*a-191025/2,
282880*a + 632000, -282880*a + 632000,
26378240*a - 58982400, -26378240*a - 58982400,
95178240*a + 212846400, -95178240*a + 212846400,
956734355865 60*a - 213932305612800, -9567343558656 0*a
- 213932305612800, 18406806674317737 9840*a -
41158870972471296 0000, -184068066743177379840*a
- 411588709724712960000]
sage: len(_)
31
```

Image of Galois

The next few slides may be connected to what Elkies' will talk about this weekend (*Remarks on Isogenies over F...*)

Torsion Subgroups of Elliptic Curves over F

Theorem (Kamienny-Najman)

The following is a complete list of torsion structures for elliptic curves over F:

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

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

This is exactly the same as the list over $\mathbb{Q}$, except for the $\mathbb{Z}/15\mathbb{Z}$ curve.

Torsion Subgroups of Elliptic Curves over F

This exotic 15-torsion example is a curve of conductor $\mathfrak{n} = (10)$; over $\mathbb{Q}$ it has conductor 50:

```
sage: F.<phi> = NumberField(x^2 - x - 1)
sage: E = EllipticCurve(F, [1,1,1,-3,1]); E
y^2 + x*y + y = x^3 + x^2 + -3*x + 1
sage: E.torsion_subgroup()
Torsion Subgroup isomorphic to Z/15
sage: P = E.torsion_subgroup().gens()[0]
sage: P
(-2*phi + 1 : 2*phi - 4 : 1)
sage: E.conductor()
Fractional ideal (10)
sage: E = EllipticCurve([1,1,1,-3,1]); E.conductor()
sage: E.torsion_order()
5
sage: E.quadratic_twist(5).torsion_order()
3
```

Torsion Subgroups of Elliptic Curves over F

Table: Distribution of torsion subgroups up to norm conductor 1831

structure	#isom	example curve	Norm($\mathfrak{n}$)
1	296	$[0, -1, 1, -8, -7]$	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

Isogenies of Elliptic Curves over $\mathbb{Q}$

isogeny = nonzero homomorphism

Theorem (Mazur)

If $\psi : E/\mathbb{Q} \to E'/\mathbb{Q}$ is of prime degree, then $\deg(\psi) \le 163$.

Rational Isogenies of Prime Degree

B. Mazur
(with an appendix by D. Goldfeld)
Department of Mathematics, Harvard University, One Oxford Street, Cambridge, MA 02138, USA

Let N be a positive integer. Examples of elliptic curves over $\mathbf{Q}$ possessing rational cyclic N-isogenies are known for the following values of N:

N	g	v	N	g	v	N	g	v
≤ 10	0	∞	11	1	3	27	1	1
12	0	∞	14	1	2	37	2	2
13	0	∞	15	1	4	43	3	1
16	0	∞	17	1	2	67	5	1
18	0	∞	19	1	1	163	13	1
25	0	∞	21	1	4			

Isogenies of Elliptic Curves over F

Open Problem: Fill in the blank. If $\psi : E/F \to E'/F$ is of prime degree, then $\deg(\psi) \leq$ ____________.

Theorem (Larson-Vaintrob)

Assume GRH. There is an effectively computable constant[a] C such that any prime degree isogeny over F has degree at most C.

[a] Which nobody knows yet.

For making tables[2]:

Theorem (Billerey, 2011)

If E is a specific elliptic curve over F, then there is an algorithm *to compute the degrees of all rational isogenies $\psi : E \to E'$.*

[2] These two theorems are much more general.

Rational 17-Isogenies over F

The elliptic curve $X_0(17)$, which parametrizes 17-isogenies, has rank 0 over $\mathbb{Q}$, but rank 1 over F.

```
sage: CuspForms(Gamma0(17), 2).dimension()
1
sage: E = EllipticCurve('17a'); E
y^2 + x*y + y = x^3 - x^2 - x - 14
sage: E.rank()
0
sage: E.quadratic_twist(5).rank()
1
```

$\Longrightarrow$ There are infinitely many isogenies of degree 17 over F.

Isogeny Class Size

Theorem (Has anybody actually proved this?)

The largest isogeny class of elliptic curves over $\mathbb{Q}$ is 8.

Open Problem: Fill in the blank. The largest isogeny class of elliptic curves over F is ____________.

There is an isogeny class of cardinality 10 over F (here $a = \varphi$):

```
45a  1 [1,1,1,-80,242]
45a  2 [1,1,1,-5,2]
45a  3 [1,1,1,0,0]
45a  4 [1,1,1,-10,-10]
45a  5 [1,1,1,-135,-660]
45a  6 [1,1,1,35,-28]
45a  7 [1,1,1,-2160,-39540]
45a  8 [1,1,1,-110,-880]
45a  9 [1,-a+1,a,4976732*a-8052529,6393196917*a-10344409915]
45a 10 [1,a,a+1,-4976733*a-3075797,-6393196918*a-3951212998]
```

Modularity of Elliptic Curves over F

Hilbert modular forms = certain holomorphic functions on $\mathfrak{h} \times \mathfrak{h}$

Conjecture (Modularity)

Bijection between L-functions of rational Hilbert modular newforms of weight $(2, 2)$ over F and L-functions of elliptic curves over F.

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

General case hard, mainly because $\sqrt{5} \in F$.

Applications of Modularity

Assume: Some prime $\mathfrak{p}$ exactly divides the conductor $\mathfrak{n}$ of E. Then:

$$\text{Shimura curve parameterization } \psi : X \to E.$$

Here $X = G \backslash \mathfrak{h}$, where $G \subset \mathrm{SL}_2(\mathbb{R})_+$ is a discrete subgroup constructed using the quaternion algebra over F ramified at $\mathfrak{p} \cdot \infty$.

1. **Heegner points:** (Zhang) heights of image in E of the analogue of Heegner points on X. Theorem: *if* $\mathrm{ord}_{s=1} L(E,s) \leq 1$*, then* $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}(E(F))$*.*
2. **Tables:** Modularity makes it possible to enumerate all curves over F of given conductor. (my next talk)
3. **Modular degree:** $\mathfrak{p}$-modular degree of E is $\deg(\psi)$. (Deines is studying this for her Ph.D. thesis.)
4. **Visibility of Ш:** Mazur's idea relating Ш and Mordell-Weil.
5. **Chow-Heegner points:** New creative ways to construct points...
6. ETC!

Table of Curves over F with Norm Conductor ≤ 1831

Bober, Deines, Gaski, Klages-Mundt, LeVeque, Ohana, Rabindranath, Sharaba, and I made tables about all[3] elliptic curves E over F with $\mathrm{Norm}(\mathfrak{n}_E) \leq 1831$.

Preview of my second talk:

1. Find a list of all rational Hilbert modular newforms f in $S_{(2,2)}(\mathfrak{n}_E)$. (Uses: Quaternion algebras and linear algebra)
2. Find Weierstrass equations for all corresponding elliptic curves. (Uses: Many search techniques and computing isogenies)
3. Compute invariants of each curve (Uses: descent, Tate's algorithm, L-series, etc.)

[3] assuming the modularity conjecture