(101) UT NTS

2011-10-28

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

§1. Tables over $\mathbb{Q}$:

- Antwerp IV { • all curves with $N \leq 200$; • all curves with $N = 2^a 3^b$.
- Cremona's book { - all curves with $N \leq 1000$ (big) ; - complete desc. of algorithms (modular symbols, numerical periods)
- Cremona's online tables : • all curves with $N \leq 200{,}000$; • goal: 234,446 (first rank 4) $|\Delta| \leq 10^{12}$
- S-Watkins { • "many" (= 136,832,795) curves with $N \leq 10^8$; • 11,378,911 prime $N \leq 10^{10}$

(See Bektemirov-Mazur-Stein-Watkins)

§2. Why $F = \mathbb{Q}(\sqrt{5})$? $\varphi = \frac{1+\sqrt{5}}{2}$

- F totally real: - Hilbert modular forms || (Major recent progress)
  - Shimura curves
  - Heegner points, Euler systems
  - Gross-Zagier formula (Zhang)
- $\mathcal{O}_F^* \simeq \{\pm 1\} \times \langle \varphi \rangle$ has rank 1 = rank $(\mathbb{Z}^*)$.
- F is first tot. real field after $\mathbb{Q}$.
- F has (27) CM j-invariants ($\mathbb{Q}$ only has 13). (most?)
- $X_0(17)$ has rank 1 over F (genus 1)

2011-10-28

§3. Finding all curves of conductor n.

§3.1 Modularity

Conj (Modularity):

$$\left\{ L(E,s) : E/\mathbb{Q}(\sqrt{5}) \right\} = \left\{ L(f,s) : \begin{array}{l} f \text{ Hilbert cuspidal} \\ \text{newform with rational} \\ \text{Hecke eigenvalues} \end{array} \right\}$$

Taylor: True if $E[3]|_{G_{F(\sqrt{5})}}$ absolutely irreducible (Gee + Kisin)

- Not known in general
- Optimistic

We assume modularity for rest of talk.

§3.2 Computing Hilbert Modular Forms

Dembele's Thesis (Darmon)

$$R = \mathcal{O}_F\Big[\tfrac{1}{2}(1-\bar{\varphi}i+\varphi j), \tfrac{1}{2}(-\bar{\varphi}i+j+\varphi k), \tfrac{1}{2}(\varphi i-\bar{\varphi}j+k), \tfrac{1}{2}(i+\varphi j-\bar{\varphi}k)\Big] \subseteq \underbrace{F[i,j,k]}_{\text{Hamilton quaternions over } F}$$

R: icosian ring (maximal order)

$F[i,j,k]$: ramified only at 2 infinite real places.

$$\left\{ \begin{array}{l} \text{Hilbert modular forms} \\ \text{of level } n \text{ and weight } (2,2) \end{array} \right\} \approx \underset{T = \mathbb{Z}[\ldots, T_{\mathfrak{p}}, \ldots]}{\mathbb{C}\left[R^* \backslash \mathbb{P}^1(\mathcal{O}_F/n)\right]}$$

R^* acts by $R \hookrightarrow R_{\mathfrak{p}} \approx M_2(\mathcal{O}_{F,\mathfrak{p}})$ for $\mathfrak{p} \mid n$.

$$T_{\mathfrak{p}}\left([x]\right) = \sum_{[\alpha] \in R/R^*} [\alpha x], \quad \text{for } \mathfrak{p} \nmid n$$

$(\pi_{\mathfrak{p}}) = \mathfrak{p} \subseteq \mathcal{O}_F$ $\quad N(\alpha) = \pi_{\mathfrak{p}}$

That's it!

2011-10-28

§3.3: Finding $E_f \longleftrightarrow f$ = Hilbert newform $= \{a_p\}_{p \text{ prime}}$,

$$a_p = N(p) + 1 - \#E_f(\mathcal{O}_F/p) \in \mathbb{Z}.$$

Strategies:

1. Naive enumeration: for loops over $y^2 = x^3 + ax + b$
2. Torsion families: can tell from $\{a_p\}$
   if $\ell \mid \#E_f(F)$ some E_f in isogeny class.
   Write down family of curves with point of order ℓ.
3. Twist: find all twists of known curves
   , twist to minimal conductor.
4. Specified a_p: Search family of curves with specified a_{71a}, a_{71b}, say. Use CRT.
5. Good reduction outside S: Cremona-Lingham (Magma only)
6. Special Values: $\{L(f, \chi, 1)$; various $\chi\}$) Works!
   (Dembele, Bober) $\rightsquigarrow$ conjectures $\{$period lattice of $E_f\}$) $\{a_p\}_{N(p) \leq \text{space}}$
   Requires VERY fast §3.2 to be useful.
7. Family with given E[7]: Tom Fisher & M. Stoll.

§3.4 Result:

Combine above finds all curves $E_f/\mathbb{Q}(\sqrt{5})$ with

$$N(\mathfrak{n}) \leq \underbrace{1831}$$

first of rank 2.

rank	# iso classes
0	750
1	650
2	2
Total	1402

} includes Gal(F/ℚ) - conjugates

Cremona: 5260 classes

§3.5 Isogenous Curves

Find all $E_{/F}$ isogenous to E_f.

Theorem (Mazur): $E/\mathbb{Q}$, $\deg(E \to E') \leq 163$.

+Velu's formulas. ⇝ algorithm to compute isogeny class of E.

- Generalization not known for any other fields.

But: [Billeray, 2011] ⇝ new algorithm: INPUT: E over number field
OUTPUT: possible isogeny primes

Easy over quadratic fields.

Billeray + Vélu = algorithm.

Find 3338 curves with $N(\mathfrak{n}) \leq 1831$

Cremona: 10283 classes

§4. Related / Future Projects

1. To first known of rank 3:
$$N(\Gamma) \leq 163^2 = 26{,}569$$
2. Prove modularity conjecture / $\mathbb{Q}(\sqrt{5})$
3. Generalize Mazur's theorem / $\mathbb{Q}(\sqrt{5})$
4. S-Watkins style table
(need fast $L(E,s)$ code ~ new work of D. Sutherland)
5. Cremona-Lingham in Sage
6. Saturation of $E(K)$ in Sage
(we have p-saturation code — need bound on p)
7. Modular degree: $\mathfrak{P} \| \mathfrak{n}$, $Q_{\mathfrak{P},\infty} \rightsquigarrow X$ Shimura curve

$$\deg(\Phi_E)$$

$\downarrow \Phi_E$

E

Watkins over $\mathbb{Q}$: Use $L(Sym^2 E, 2) = (*) \cdot \deg(\Phi_E)$
↑ Flach.

Generalize to F.

8. Does $\deg(\Phi_E)$ | congruence number (Hilbert mod forms)
↑ analogue of theorem of Ribet.
9. Compute Chow-Heegner points $P_{E,E'} \in E(F)$.
10. Generalize much to A_f = abelian varieties when coeffs of f not rational.