Torsion subgroups of elliptic curves over quintic and sextic number fields

Andrew V. Sutherland
(joint with Maarten Derickx)

Massachusetts Institute of Technology

September 1, 2016

http://arxiv.org/abs/1608.07549

Torsion subgroups of elliptic curves over number fields

Let $\Phi(d)$ be the set of pairs (m, mn) for which there exists an elliptic curve E over a number field K of degree d with

$$E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}.$$

By Merel's theorem (1996), $\Phi(d)$ is finite. Mazur (1977) proved

$$\Phi(1) = \{(1, n) : 1 \leq n \leq 12,\ n \neq 11\} \cup \{(2, 2n) : 1 \leq n \leq 4\},$$

and Kenku-Momose (1988) and Kamienny (1992) proved

$$\begin{aligned}\Phi(2) = \{(1, n) : 1 \leq n \leq 18,\ n \neq 17\} \ &\cup\ \{(2, 2n) : 1 \leq n \leq 6\} \\ &\cup\ \{(3, 3), (3, 6), (4, 4)\}.\end{aligned}$$

For $d > 2$ the set $\Phi(d)$ has yet to be determined (but $d = 3$ is TBA).

Torsion subgroups that occur infinitely often

Let $\Phi^\infty(d)$ be the subset of $\Phi(d)$ arising infinitely often as E and K vary.

Then $\Phi^\infty(d) = \Phi(d)$ for $d = 1, 2$. Jeon-Kim-Schweizer (2004) proved

$$\Phi^\infty(3) = \{(1,n) : 1 \le n \le 20,\ n \ne 17, 19\} \cup \{(2,2n) : 1 \le n \le 7\},$$

and Jeon-Kim-Park (2006) proved

$$\begin{aligned}\Phi^\infty(4) = \{(1,n) : 1 \le n \le 24,\ n \ne 19, 23\} &\cup \{(2,2n) : 1 \le n \le 9\} \\ \cup \{(3,3n) : 1 \le n \le 3\} &\cup \{(4,4), (4,8), (5,5), (6,6)\}.\end{aligned}$$

For $d = 5, 6, 7, 8$ the cylic elements $(1, n) \in \Phi^\infty(d)$ were determined by Derickx-van Hoeij (2013).

New result

Theorem (Derickx-S 2016)

We have

$$\Phi^{\infty}(5) = \{(1,n) : 1 \leq n \leq 25,\ n \neq 23\} \cup \{(2,2n) : 1 \leq n \leq 8\},$$
$$\Phi^{\infty}(6) = \{(1,n) : 1 \leq n \leq 30,\ n \neq 23, 25, 29\} \cup \{(2,2n) : 1 \leq n \leq 10\}$$
$$\cup \{(3,3n) : 1 \leq n \leq 4\} \cup \{(4,4), (4,8), (6,6)\}.$$

Key ingredients of the proof:

- Explicit models of modular curves $X_1(m, mn)$ parametrizing triples (E, P, Q) with P and Q independent points of order m and mn on E.
- $\mathbb{C}$-gonality lower bounds of Abramovich and $\mathbb{F}_p$-gonality lower bounds obtained computationally, combined with a result of Frey.
- New techniques for proving $\mathrm{rk}(J_1(m, mn)(\mathbb{Q}(\zeta_m)) = 0$ using L-ratios.

In principle we can handle $\Phi^{\infty}(7)$ and $\Phi^{\infty}(8)$, but computationally hard.

Explicit models of $X_1(m, mn)$

Example:

$$X_1(2,14) : v^3 - (u^3+u^2+u-1)v^2 - (u^5+3u^4+3u^3+u^2+u)v + u^5+u^4 = 0,$$

with maps

$$q = \frac{v+1}{v-2u+1}$$

$$t = \frac{(v+1)(2u-v+1)(2u(u+1)+v+1)}{v^3+(2u^2+1)v^2-(2u(u^2-u-1)-1)v+u^4+(u+1)^4}$$

defining

$$\begin{aligned} E(q,t): &\quad y^2 = x^3 + (t^2-qt-2)x^2 - (t^2-1)(qt+1)^2 x, \\ P(q,t) &:= (0,0) && \text{(order 2)}, \\ Q(q,t) &:= \big((t+1)(qt+1)\,,\, t(qt+1)(t+1)\big) && \text{(order 14)}. \end{aligned}$$

See `http://math.mit.edu/~drew/X1mn.html` for more ($m^2 n \le 120$).