Torsion subgroups of rational elliptic curves over the compositum of all cubic fields

Andrew V. Sutherland

Massachusetts Institute of Technology

April 7, 2016

joint work with Harris B. Daniels, Álvaro Lozano-Robledo, and Filip Najman

http://arxiv.org/abs/1509.00528

and also with David Zywina.

Elliptic curves

Let E be an elliptic curve over a number field K:

$$E : y^2 = x^3 + Ax + B.$$

For any field extension L/K, the set $E(L)$ forms an abelian group.

Theorem (Mordell-Weil 1920s)

The group $E(K)$ is a finitely generated. Thus $E(K) \simeq E(K)_{\text{tors}} \oplus \mathbb{Z}^r$, where $E(K)_{\text{tors}}$ is a finite abelian group.

Theorem (Merel 1996)

For every $d \geqslant 1$ there is a bound B_d such that $\#E(K)_{\text{tors}} \leqslant B_d$ for all elliptic curves E over any number field K of degree d.

Elliptic curves

Let E be an elliptic curve over a number field K:

$$E : y^2 = x^3 + Ax + B.$$

For any field extension L/K, the set $E(L)$ forms an abelian group.

Theorem (Mordell-Weil 1920s)

The group $E(K)$ is a finitely generated. Thus $E(K) \simeq E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r$, where $E(K)_{\mathrm{tors}}$ is a finite abelian group.

Theorem (Merel 1996)

For every $d \geqslant 1$ there is a bound B_d such that $\#E(K)_{\mathrm{tors}} \leqslant B_d$ for all elliptic curves E over any number field K of degree d.

Remark

The groups $E(\overline{K})$ and $E(\overline{K})_{\mathrm{tors}}$ are not finitely generated.

Torsion subgroups of elliptic curves over number fields

Theorem (Mazur 1977)

Let E be an elliptic curve over $\mathbb{Q}$.

$$E(\mathbb{Q})_{\mathrm{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & 1 \leqslant M \leqslant 10,\ M = 12; \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leqslant M \leqslant 4. \end{cases}$$

Theorem (Kenku,Momose 1988, Kamienny 1992)

Let E be an elliptic curve over a quadratic number field K.

$$E(K)_{\mathrm{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & 1 \leqslant M \leqslant 16,\ M = 18; \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leqslant M \leqslant 6; \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & M = 1, 2\ (K = \mathbb{Q}(\zeta_3)\ \textit{only}); \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & (K = \mathbb{Q}(i)\ \textit{only}). \end{cases}$$

Torsion subgroups of elliptic curves over cubic fields

Theorem (Jeon,Kim,Schweizer 2004)

For cubic $K/\mathbb{Q}$, the groups $T \simeq E(K)_{\mathrm{tors}}$ arising infinitely often are:

$$T \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & 1 \leqslant M \leqslant 16,\ M = 18, 20; \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leqslant M \leqslant 7. \end{cases}$$

Theorem (Najman 2012)

There is an elliptic curve $E/\mathbb{Q}$ for which $E(\mathbb{Q}(\zeta_9)^+)_{\mathrm{tors}} \simeq \mathbb{Z}/21\mathbb{Z}$.

Torsion subgroups of elliptic curves over cubic fields

Theorem (Jeon,Kim,Schweizer 2004)

For cubic $K/\mathbb{Q}$, the groups $T \simeq E(K)_{\text{tors}}$ arising infinitely often are:

$$T \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & 1 \leqslant M \leqslant 16,\ M = 18, 20; \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leqslant M \leqslant 7. \end{cases}$$

Theorem (Najman 2012)

There is an elliptic curve $E/\mathbb{Q}$ for which $E(\mathbb{Q}(\zeta_9)^+)_{\text{tors}} \simeq \mathbb{Z}/21\mathbb{Z}$.

Theorem (Derickx,Etropolski,Morrow,Zureick-Brown, 2016)

Let E be an elliptic curve over a cubic number field K.

$$E(K)_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & 1 \leqslant M \leqslant 16,\ M = 18, 20, 21; \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leqslant M \leqslant 7. \end{cases}$$

Elliptic curves over $\mathbb{Q}(2^\infty)$

Definition

Let $\mathbb{Q}(d^\infty)$ be the compositum of all degree-d extensions $K/\mathbb{Q}$ in $\overline{\mathbb{Q}}$.

Example: $\mathbb{Q}(2^\infty)$ is the maximal elementary 2-abelian extension of $\mathbb{Q}$.

Theorem (Frey,Jarden 1974)

For $E/\mathbb{Q}$ the group $E(\mathbb{Q}(2^\infty))$ is not finitely generated.

Elliptic curves over $\mathbb{Q}(2^\infty)$

Definition

Let $\mathbb{Q}(d^\infty)$ be the compositum of all degree-d extensions $K/\mathbb{Q}$ in $\overline{\mathbb{Q}}$.

Example: $\mathbb{Q}(2^\infty)$ is the maximal elementary 2-abelian extension of $\mathbb{Q}$.

Theorem (Frey,Jarden 1974)

For $E/\mathbb{Q}$ the group $E(\mathbb{Q}(2^\infty))$ is not finitely generated.

Theorem (Laska,Lorenz 1985, Fujita 2004,2005)

For $E/\mathbb{Q}$ the group $E(\mathbb{Q}(2^\infty))_{\text{tors}}$ is finite and

$$E(\mathbb{Q}(2^\infty))_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & M = 1,3,5,7,9,15; \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leqslant M \leqslant 6,\ M = 8; \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4M\mathbb{Z} & 1 \leqslant M \leqslant 4; \\ \mathbb{Z}/2M\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 3 \leqslant M \leqslant 4. \end{cases}$$

Elliptic curves over $\mathbb{Q}(3^\infty)$

Theorem (Daniels,Lozano-Robledo,Najman,S 2015)

For $E/\mathbb{Q}$ the group $E(\mathbb{Q}(3^\infty))_{\text{tors}}$ is finite and

$$E(\mathbb{Q}(3^\infty))_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & M = 1,2,4,5,7,8,13; \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4M\mathbb{Z} & M = 1,2,4,7; \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6M\mathbb{Z} & M = 1,2,3,5,7; \\ \mathbb{Z}/2M\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & M = 4,6,7,9. \end{cases}$$

Of these 20 groups, 16 arise for infinitely many $j(E)$. We give complete lists/parametrizations of the $j(E)$ that arise in each case.

$E/\mathbb{Q}$	$E(\mathbb{Q}(3^\infty))_{\text{tors}}$	$E/\mathbb{Q}$	$E(\mathbb{Q}(3^\infty))_{\text{tors}}$
11a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	338a1	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$
17a3	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	20a1	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
15a5	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	30a1	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$
11a1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$	14a3	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$
26b1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$	50a3	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$
210e1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$	162b1	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z}$
147b1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$	15a1	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$
17a1	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	30a2	$\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$
15a2	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	2450a1	$\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$
210e2	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$	14a1	$\mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$

T	$j(t)$
$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	t
$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	$\frac{(t^2+16t+16)^3}{t(t+16)}$
$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$	$\frac{(t^4-16t^2+16)^3}{t^2(t^2-16)}$
$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$	$\frac{(t^4-12t^3+14t^2+12t+1)^3}{t^5(t^2-11t-1)}$
$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$	$\frac{(t^2+13t+49)(t^2+5t+1)^3}{t}$
$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}$	$\frac{(t^{16}-8t^{14}+12t^{12}+8t^{10}-10t^8+8t^6+12t^4-8t^2+1)^3}{t^{16}(t^4-6t^2+1)(t^2+1)^2(t^2-1)^4}$
$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/26\mathbb{Z}$	$\frac{(t^4-t^3+5t^2+t+1)(t^8-5t^7+7t^6-5t^5+5t^3+7t^2+5t+1)^3}{t^{13}(t^2-3t-1)}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	$\frac{(t^2+192)^3}{(t^2-64)^2}$, $\frac{-16(t^4-14t^2+1)^3}{t^2(t^2+1)^4}$, $\frac{-4(t^2+2t-2)^3(t^2+10t-2)}{t^4}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$	$\frac{16(t^4+4t^3+20t^2+32t+16)^3}{t^4(t+1)^2(t+2)^4}$, $\frac{-4(t^8-60t^6+134t^4-60t^2+1)^3}{t^2(t^2-1)^2(t^2+1)^8}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}$	$\frac{(t^{16}-8t^{14}+12t^{12}+8t^{10}+230t^8+8t^6+12t^4-8t^2+1)^3}{t^8(t^2-1)^8(t^2+1)^4(t^4-6t^2+1)^2}$
$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/28\mathbb{Z}$	$\left\{\frac{351}{4}, \frac{-38575685889}{16384}\right\}$
$\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$	$\frac{(t+27)(t+3)^3}{t}$
$\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$	$\frac{(t^2-3)^3(t^6-9t^4+3t^2-3)^3}{t^4(t^2-9)(t^2-1)^3}$
$\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/18\mathbb{Z}$	$\frac{(t+3)^3(t^3+9t^2+27t+3)^3}{t(t^2+9t+27)}$, $\frac{(t+3)(t^2-3t+9)(t^3+3)^3}{t^3}$
$\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/30\mathbb{Z}$	$\left\{\frac{-121945}{32}, \frac{46969655}{32768}\right\}$
$\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/42\mathbb{Z}$	$\left\{\frac{3375}{2}, \frac{-140625}{8}, \frac{-1159088625}{2097152}, \frac{-189613868625}{128}\right\}$
$\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$	$\frac{(t^8+224t^4+256)^3}{t^4(t^4-16)^4}$
$\mathbb{Z}/12\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$	$\frac{(t^2+3)^3(t^6-15t^4+75t^2+3)^3}{t^2(t^2-9)^2(t^2-1)^6}$, $\left\{\frac{-35937}{4}, \frac{109503}{64}\right\}$
$\mathbb{Z}/14\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$	$\left\{\frac{2268945}{128}\right\}$
$\mathbb{Z}/18\mathbb{Z}\oplus\mathbb{Z}/18\mathbb{Z}$	$\frac{27t^3(8-t^3)^3}{(t^3+1)^3}$, $\frac{432t(t^2-9)(t^2+3)^3(t^3-9t+12)^3(t^3+9t^2+27t+3)^3(5t^3-9t^2-9t-3)^3}{(t^3-3t^2-9t+3)^9(t^3+3t^2-9t-3)^3}$

Characterizing $\mathbb{Q}(3^\infty)$

Definition

A finite group G is of *generalized* S_3-type if it is isomorphic to a subgroup of $S_3 \times \cdots \times S_3$. Example: D_6. Nonexamples: A_4, C_4, $B(2,3)$.

Lemma

G is of generalized S_3-type if and only if (a) G is supersolvable, (b) $\lambda(G)$ divides 6, and (c) every Sylow subgroup of G is abelian.

Corollary

The class of generalized S_3-type groups is closed under products, subgroups, and quotients.

Characterizing $\mathbb{Q}(3^\infty)$

Definition

A finite group G is of *generalized* S_3-type if it is isomorphic to a subgroup of $S_3 \times \cdots \times S_3$. Example: D_6. Nonexamples: A_4, C_4, $B(2,3)$.

Lemma

G is of generalized S_3-type if and only if (a) G is supersolvable, (b) $\lambda(G)$ divides 6, and (c) every Sylow subgroup of G is abelian.

Corollary

The class of generalized S_3-type groups is closed under products, subgroups, and quotients.

Proposition

A number field K lies in $\mathbb{Q}(3^\infty)$ if and only the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is of generalized S_3-type.

Uniform boundedness for base extensions of $E/\mathbb{Q}$

Theorem

Let $F/\mathbb{Q}$ be a Galois extension with finitely many roots of unity. There is a uniform bound B such that $\#E(F)_{\mathrm{tors}} \leqslant B$ for all $E/\mathbb{Q}$.

Uniform boundedness for base extensions of $E/\mathbb{Q}$

Theorem

Let $F/\mathbb{Q}$ be a Galois extension with finitely many roots of unity. There is a uniform bound B such that $\#E(F)_{\mathrm{tors}} \leqslant B$ for all $E/\mathbb{Q}$.

Proof sketch.

Uniform boundedness for base extensions of $E/\mathbb{Q}$

Theorem

Let $F/\mathbb{Q}$ be a Galois extension with finitely many roots of unity. There is a uniform bound B such that $\#E(F)_{\mathrm{tors}} \leqslant B$ for all $E/\mathbb{Q}$.

Proof sketch.

1. $E[n] \not\subseteq E(F)$ for all sufficiently large n.
2. If $E[p^k] \subseteq E(F)$ with $k \leqslant j$ maximal and $p^j | \lambda(E(F)[p^\infty])$, then E admits a $\mathbb{Q}$-rational cyclic p^{j-k}-isogeny.
3. $E/\mathbb{Q}$ cannot admit a $\mathbb{Q}$-rational cyclic p^n-isogeny for $p^n > 163$ (Mazur+Kenku).

Corollary

$E(\mathbb{Q}(3^\infty))_{\mathrm{tors}}$ *is finite. Indeed,* $\#E(\mathbb{Q}(3^\infty))_{\mathrm{tors}}$ *must divide* $2^{10}3^7 5^2 7^3 13$.

Galois representations

Let E be an elliptic curve over $\mathbb{Q}$ and let $N \geqslant 1$ be an integer.

The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the N-torsion subgroup of $E(\overline{\mathbb{Q}})$,

$$E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z},$$

via its action on points (coordinate-wise). This yields a representation

$$\rho_{E,N}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}),$$

whose image we denote $G_E(N)$. Choosing bases compatibly, we can take the inverse limit and obtain a single representation

$$\rho_E\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \varprojlim_N \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

whose image we denote G_E, with projections $G_E \to G_E(N)$ for each N.

Modular curves

Let $F_N \coloneqq \mathbb{Q}(\zeta_n)(X(N))$. Then $F_1 = \mathbb{Q}(j)$ and $F_N/\mathbb{Q}(j)$ is Galois with

$$\mathrm{Gal}(F_N/\mathbb{Q}(j)) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$$

Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a group containing $-I$ with $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Define $X_G/\mathbb{Q}$ to be the smooth projective curve with function field F_N^G. Let $J_G\colon X_G \to X(1) = \mathbb{Q}(j)$ be the map corresponding to $\mathbb{Q}(j) \subseteq F_N^G$.

If $M|N$ and G is the full inverse image of $H \subseteq \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$, then $X_G = X_H$. We call the least such M the *level* of G and X_G.

Better: identify G with $\pi_N^{-1}(G)$, where $\pi_N\colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$; G as an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ containing $-I$ with $\det(G) = \hat{\mathbb{Z}}^\times$.

For any $E/\mathbb{Q}$ with $j(E) \notin \{0, 1728\}$, up to $\mathrm{GL}_2(\hat{\mathbb{Z}})$-conjugacy,

$$G_E \subseteq G \iff j(E) \in J_G(X_G(\mathbb{Q})).$$

Congruence subgroups

For $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of level N as above, let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be the preimage of $\pi_N(G) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Then Γ is a congruence subgroup containing $\Gamma(N)$, and the modular curve $X_\Gamma \coloneqq \Gamma\backslash\mathfrak{h}^*$ is isomorphic to the base change of X_G to $\mathbb{Q}(\zeta_n)$.

The genus g of X_G and X_Γ must coincide, but their levels need not (!); the level M of X_Γ may strictly divide the level N of X_G.

For each $g \geqslant 0$ we have $g(X_\Gamma) = g$ for only finitely many X_Γ; for $g \leqslant 24$ these Γ can be found in the tables of Cummins and Pauli.

But we may have $g(X_G) = g$ for infinitely many X_G (!)

Call $g(X_G)$ the genus of G.

Modular curves with infinitely many rational points

Theorem (S.,Zywina)

There are 248 modular curves X_G of prime power level with $X_G(\mathbb{Q})$ infinite. Of these, 220 have genus 0 and 28 have genus 1.

For each of these 248 groups G we have an explicit $J_G\colon X_G \to X(1)$.

2-adic cases independently addressed by Rouse and Zureick-Brown.

Corollary

For each of these G we can completely describe the set of j-invariants of elliptic curves $E/\mathbb{Q}$ for which $G_E \subseteq G$.

Corollary

There are 1294 non-conjugate open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of prime power level that occur as G_E for infinitely many $E/\mathbb{Q}$ with distinct $j(E)$.

Determining $E(\mathbb{Q}(3^\infty))[p^\infty]$ for $p \in \{2, 3, 5, 7, 13\}$

Lemma

For $j(E) \neq 1728$ the structure of $E(\mathbb{Q}(3^\infty))_{\mathrm{tors}}$ is determined by $j(E)$. For $j(E) = 1728$ we have $E(\mathbb{Q}(3^\infty))_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Now we start computing possible Galois images G in $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ and corresponding modular curves X_G, leaning heavily on results of Rouse–Zureick-Brown and S.-Zywina.

The most annoying case is 27-torsion. We get the genus 4 curve

$$X : x^3y^2 - x^3y - y^3 + 6y^2 - 3y = 1.$$

As shown by Morrow, $\mathrm{Aut}(X_{\mathbb{Q}(\zeta_3)}) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, and the two cyclic quotients are hyperelliptic curves over $\mathbb{Q}(\zeta_3)$ with only three rational points; none of these give a non-cuspidal $\mathbb{Q}$-rational point on X.

Determining $E(\mathbb{Q}(3^\infty))[p^\infty]$ for $p \in \{2, 3, 5, 7, 13\}$

Lemma

For $j(E) \neq 1728$ the structure of $E(\mathbb{Q}(3^\infty))_{\mathrm{tors}}$ is determined by $j(E)$. For $j(E) = 1728$ we have $E(\mathbb{Q}(3^\infty))_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Now we start computing possible Galois images G in $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ and corresponding modular curves X_G, leaning heavily on results of Rouse–Zureick-Brown and S.-Zywina.

The most annoying case is 27-torsion. We get the genus 4 curve

$$X : x^3y^2 - x^3y - y^3 + 6y^2 - 3y = 1.$$

As shown by Morrow, $\mathrm{Aut}(X_{\mathbb{Q}(\zeta_3)}) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, and the two cyclic quotients are hyperelliptic curves over $\mathbb{Q}(\zeta_3)$ with only three rational points; none of these give a non-cuspidal $\mathbb{Q}$-rational point on X.

We eventually find $E(\mathbb{Q}(3^\infty))_{\mathrm{tors}}$ must be isomorphic to a subgroup of

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z}.$$

An algorithm to compute $E(\mathbb{Q}(3^\infty))_{\text{tors}}$

Naive approach is not practical, need to be clever.

- Compute each $E(\mathbb{Q}(3^\infty))[p^\infty]$ separately.
- $\mathbb{Q}(E[p^n]) \subseteq \mathbb{Q}(3^\infty)$ iff $\mathbb{Q}(E[p^n])$ is of generalized S_3-type.
- $\mathbb{Q}(P) \subseteq \mathbb{Q}(3^\infty)$ iff $\mathbb{Q}(P)$ is of generalized S_3-type.
- Use fields defined by division polynomials (+ quadratic ext).
- If the exponent does not divide 6 we can detect this locally.
- Use isogeny kernel polynomials to speed things up.
- Prove theorems to rule out annoying cases.

theorem $\Rightarrow$ algorithm $\Rightarrow$ theorem $\Rightarrow$ algorithm $\Rightarrow$ theorem $\Rightarrow \cdots$

An algorithm to compute $E(\mathbb{Q}(3^\infty))_{\text{tors}}$

Naive approach is not practical, need to be clever.

- Compute each $E(\mathbb{Q}(3^\infty))[p^\infty]$ separately.
- $\mathbb{Q}(E[p^n]) \subseteq \mathbb{Q}(3^\infty)$ iff $\mathbb{Q}(E[p^n])$ is of generalized S_3-type.
- $\mathbb{Q}(P) \subseteq \mathbb{Q}(3^\infty)$ iff $\mathbb{Q}(P)$ is of generalized S_3-type.
- Use fields defined by division polynomials (+ quadratic ext).
- If the exponent does not divide 6 we can detect this locally.
- Use isogeny kernel polynomials to speed things up.
- Prove theorems to rule out annoying cases.

theorem $\Rightarrow$ algorithm $\Rightarrow$ theorem $\Rightarrow$ algorithm $\Rightarrow$ theorem $\Rightarrow \cdots$

Eventually you don't need much of an algorithm.

Ruling out combinations of p-primary parts

Having determined all the minimal and maximal p-primary possibilities leaves 648 possible torsion structures.

- Work top down (divisible by 13, divisible by 7 but not 13, ...).
- Use known isogeny results to narrow the possibilities (rational points on $X_0(15)$ and $X_0(21)$ for example).
- Search for rational points on fiber products built from Z-S curves. (side benefit: gives parameterizations for genus 0 cases).
- Hardest case: ruling out a point of order 36.

Eventually we whittle our way down to 20 torsion structures, all of which we know occur because we have examples.

Constructing a complete set of parameterizations

For each torsion structure T with $\lambda(T) = n$ we enumerate subgroups G of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ that are maximal subject to:

1. $\det\colon G \to (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective.
2. G contains an element γ corresponding to complex conjugation ($\operatorname{tr}\gamma = 0$, $\det\gamma = -1$, γ-action trivial on $\mathbb{Z}/n\mathbb{Z}$ submodule).
3. The submodule of $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ fixed by the minimal $N \triangleleft G$ for which G/N is of generalized S_3-type is isomorphic to T.

Each such G will contain $-I$ and the modular curve X_G will be defined over $\mathbb{Q}$. For $j(E) \neq 0, 1728$ the non-cuspidal points in $X_G(\mathbb{Q})$ give $j(E)$ for which $E(\mathbb{Q}(3^\infty))_{\mathrm{tors}}$ contains a subgroup isomorphic to T.

There are 33 such G for the 20 possible T. In each case either:
(a) X_G has genus 0 and a rational point, (b) X_G has genus 1 and no rational points, (c) X_G is an elliptic curve of rank 0, or (d) $g(X_G) > 1$.

T	$j(t)$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	t
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\frac{(t^2+16t+16)^3}{t(t+16)}$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\frac{(t^4-16t^2+16)^3}{t^2(t^2-16)}$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$	$\frac{(t^4-12t^3+14t^2+12t+1)^3}{t^5(t^2-11t-1)}$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$	$\frac{(t^2+13t+49)(t^2+5t+1)^3}{t}$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$	$\frac{(t^{16}-8t^{14}+12t^{12}+8t^{10}-10t^8+8t^6+12t^4-8t^2+1)^3}{t^{16}(t^4-6t^2+1)(t^2+1)^2(t^2-1)^4}$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$	$\frac{(t^4-t^3+5t^2+t+1)(t^8-5t^7+7t^6-5t^5+5t^3+7t^2+5t+1)^3}{t^{13}(t^2-3t-1)}$
$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\frac{(t^2+192)^3}{(t^2-64)^2}$, $\frac{-16(t^4-14t^2+1)^3}{t^2(t^2+1)^4}$, $\frac{-4(t^2+2t-2)^3(t^2+10t-2)}{t^4}$
$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\frac{16(t^4+4t^3+20t^2+32t+16)^3}{t^4(t+1)^2(t+2)^4}$, $\frac{-4(t^8-60t^6+134t^4-60t^2+1)^3}{t^2(t^2-1)^2(t^2+1)^8}$
$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$	$\frac{(t^{16}-8t^{14}+12t^{12}+8t^{10}+230t^8+8t^6+12t^4-8t^2+1)^3}{t^8(t^2-1)^8(t^2+1)^4(t^4-6t^2+1)^2}$
$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$	$\left\{\frac{351}{4}, \frac{-38575685889}{16384}\right\}$
$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$\frac{(t+27)(t+3)^3}{t}$
$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$	$\frac{(t^2-3)^3(t^6-9t^4+3t^2-3)^3}{t^4(t^2-9)(t^2-1)^3}$
$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$	$\frac{(t+3)^3(t^3+9t^2+27t+3)^3}{t(t^2+9t+27)}$, $\frac{(t+3)(t^2-3t+9)(t^3+3)^3}{t^3}$
$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$	$\left\{\frac{-121945}{32}, \frac{46969655}{32768}\right\}$
$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z}$	$\left\{\frac{3375}{2}, \frac{-140625}{8}, \frac{-1159088625}{2097152}, \frac{-189613868625}{128}\right\}$
$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\frac{(t^8+224t^4+256)^3}{t^4(t^4-16)^4}$
$\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$	$\frac{(t^2+3)^3(t^6-15t^4+75t^2+3)^3}{t^2(t^2-9)^2(t^2-1)^6}$, $\left\{\frac{-35937}{4}, \frac{109503}{64}\right\}$
$\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$	$\left\{\frac{2268945}{128}\right\}$
$\mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$	$\frac{27t^3(8-t^3)^3}{(t^3+1)^3}$, $\frac{432t(t^2-9)(t^2+3)^3(t^3-9t+12)^3(t^3+9t^2+27t+3)^3(5t^3-9t^2-9t-3)^3}{(t^3-3t^2-9t+3)^9(t^3+3t^2-9t-3)^3}$

References

[F15] Y. Fujita, *Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$*, J. Number Theory **114** (2005), 124–134.

[GG14] I. Gal and R. Grizzard, *On the compositum of all degree d extensions of a number field*, J. Théor Nombres Bordeaux **26** (2014), 655–672.

[LL85] M. Laska and M. Lorenz, *Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$*, J. Reine Agnew. Math. **355** (1985), 163–172.

[L13] A. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), 279–305.

[N15] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Lett., to appear.

[RZ15] J. Rouse and D. Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, arXiv:1402.5997.

[S15] A.V. Sutherland, *Computing image of Galois representations attached to elliptic curves*, arXiv:1504.07618.

[SZ15] A.V. Sutherland and D. Zywina, *Modular curves of prime power level with infinitely many rational points*, in preparation.

[Z15] D. Zywina, *Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$*, arXiv:1508.07663.