Mazur's Program B, after Furio–Lombardo

David Zureick-Brown (Amherst College)
Santiago Arango-Piñeros (UMass Amherst)

ChaBONNty, at the Max Plank Institute for Mathematics

July 2, 2026

Slides available at https://dmzb.github.io/

Summary

- We solve the final two 7-adic cases of program B (in progress)
- using Furio–Lombardo's recent work, and
- a "variant" of Kummer's proof of FLT for regular primes

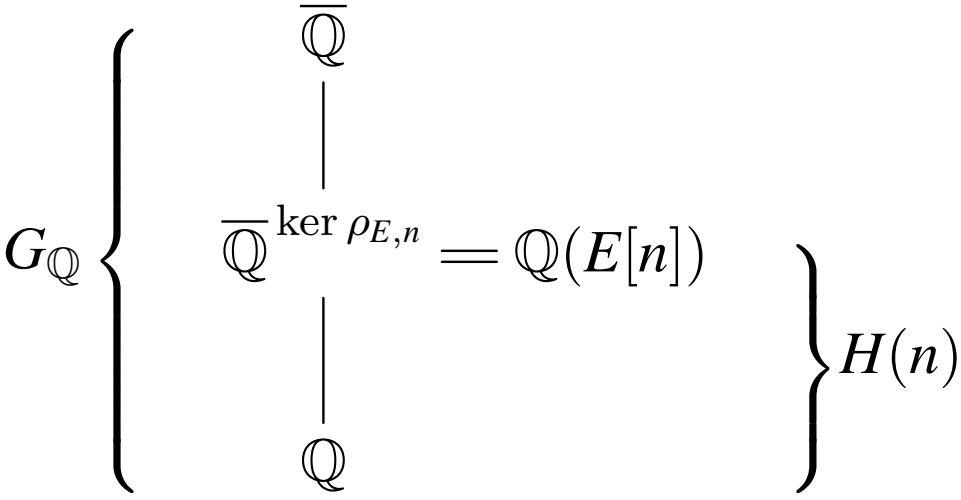
Galois Representations

$$\begin{aligned} \mathbb{Q} &\subset K \subset \overline{\mathbb{Q}} \\ G_K &:= \mathrm{Aut}(\overline{K}/K) \\ E[n](\overline{K}) &\cong (\mathbb{Z}/n\mathbb{Z})^2 \end{aligned}$$

$$\begin{aligned} \rho_{E,n}\colon \quad G_K \to \mathrm{Aut}\, E[n] &\cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ \rho_{E,\ell^\infty}\colon \quad G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell) &= \varprojlim_n \mathrm{GL}_2\left(\mathbb{Z}/\ell^n\mathbb{Z}\right) \\ \rho_E\colon \quad G_K \to \mathrm{GL}_2(\widehat{\mathbb{Z}}) &= \varprojlim_n \mathrm{GL}_2\left(\mathbb{Z}/n\mathbb{Z}\right) \end{aligned}$$

Image of Galois

$$\rho_{E,n} \colon G_{\mathbb{Q}} \twoheadrightarrow H(n) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$



Problem (Mazur's "program B")

Classify all possibilities for $H(n)$.

Mazur's Program B

As presented at Modular functions in one variable V in Bonn

Theorem 1 also fits into a general program:

B. Given a number field K and a subgroup H of $GL_2\hat{\mathbb{Z}} = \prod_p GL_2\mathbb{Z}_p$ classify all elliptic curves $E_{/K}$ whose associated Galois representation on torsion points maps $\mathrm{Gal}(\overline{K}/K)$ into $H \subset GL_2\hat{\mathbb{Z}}$.

Mazur - Rational points on modular curves (1977)

Example - torsion on an elliptic curve

If E has a K-rational **torsion point** $P \in E(K)[n]$ (of exact order n) then:

$$H(n) \subset \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

since for $\sigma \in G_K$ and $Q \in E(\overline{K})[n]$ such that $E(\overline{K})[n] \cong \langle P, Q \rangle$,

$$\begin{aligned} \sigma(P) &= P \\ \sigma(Q) &= a_\sigma P + b_\sigma Q \end{aligned}$$

Example - Isogenies

If E has a K-rational, **cyclic isogeny** $\phi\colon E \to E'$ with $\ker\phi = \langle P \rangle$ then:

$$H(n) \subset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

since for $\sigma \in G_K$ and $Q \in E(\overline{K})[n]$ such that $E(\overline{K})[n] \cong \langle P, Q \rangle$,

$$\begin{aligned} \sigma(P) &= a_\sigma P \\ \sigma(Q) &= b_\sigma P + c_\sigma Q \end{aligned}$$

Example - other maximal subgroups

$\mathbb{F}_{p^2}^*$ acts on $\mathbb{F}_{p^2} \cong \mathbb{F}_p \times \mathbb{F}_p$

Normalizer of a non-split Cartan:

$$C_{\text{ns}} = \text{im}\left(\mathbb{F}_{p^2}^* \to \text{GL}_2(\mathbb{F}_p)\right) \subset N_{\text{ns}}$$

$H(n) \subset N_{\text{ns}}$ and $H(n) \not\subset C_{\text{ns}}$ iff

E admits a “necklace” (Rebolledo, Wuthrich)

Modular curves

Definition

- $X(N)(K) := \{(E/K, P, Q) : E[N] = \langle P, Q\rangle\} \cup \{\text{cusps}\}$
- $X(N)(K) \ni (E/K, P, Q) \Leftrightarrow \rho_{E,N}(G_K) = \{I\}$

Let $\Gamma(N) \subset H \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$. The minimal such N is the **level** of H.

Definition

$X_H := X(N)/H(N)$ (where $H(N)$ is the image of H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$)

$X_H(K) \ni (E/K, \iota) \Leftrightarrow \rho_{E,N}(G_K) \subset H(N)$

Stacky disclaimer

This is only true up to twist; there are some subtleties if

1. $j(E) \in \{0, 12^3\}$ (plus some minor group theoretic conditions), or
2. if $-I \in H$.

Rational Points on modular curves

Mazur's program B

Compute $X_H(\mathbb{Q})$ for all H.

Remark

- *Sometimes $X_H \cong \mathbb{P}^1$ or elliptic with rank $X_H(\mathbb{Q}) > 0$.*
- *Some X_H have **exceptional** points (i.e, non-cusp non-CM points).*
- *Can compute $g(X_H)$ group theoretically (via Riemann–Hurwitz).*

Fact

$$g(X_H), \gamma(X_H) \to \infty \text{ as } \left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : H\right] \to \infty.$$

Let E be an elliptic curve over $\mathbb{Q}$ without CM

Conjecture (Question of Serre)

For $\ell > 37$, $\rho_{E,\ell}$ is surjective.

Conjecture (Zywina)

$$\left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})\right] \leq 2736.$$

Zywina (indices occurring infinitely often, modulo conjectures)

The **index** of $\rho_{E,N}(G_{\mathbb{Q}})$ divides $220, 336, 360, 504, 864, 1152, 1200, 1296$ or 1536.

Remark

$j(E) \in \{-7 \cdot 11^3, -7 \cdot 137^3 \cdot 2083^3\}$ *does occur finitely often*

Definition

A point $(E, \iota) \in X_H(K)$ is exceptional if $X_H(K)$ is finite and $\operatorname{End} E = \mathbb{Z}$.

Let ℓ prime, $E/\mathbb{Q}$ be a non-CM elliptic curve, and $H = \rho_{E,\ell^\infty}(G_{\mathbb{Q}})$.

Theorem (Rouse–Sutherland–ZB 2021)

Exactly one of the following is true:

1. $X_H(\mathbb{Q})$ *is infinite and* H *is listed in* (Sutherland–Zywina 2017)*;*
2. X_H *has a rational exceptional point listed in Table 1;*
3. $H \leq N_{\mathrm{ns}}(3^3), N_{\mathrm{ns}}(5^2), N_{\mathrm{ns}}(7^2), N_{\mathrm{ns}}(11^2)$*, or* $N_{\mathrm{ns}}(\ell)$ *for some* $\ell > 13$*; or*
4. $H \leq G_{\mathrm{sp}}^{\#}(7^2), G_{\mathrm{ns}}^{\#}(7^2)$ *(*`49.179.9.1` *or* `49.196.9.1`*).*

Conjecture

Cases (3) and (4) never occur.

If they do, the exceptional points have **extraordinarily** large heights (e.g. $10^{10^{200}}$ for $X_{\mathrm{ns}}^{+}(11^2)(\mathbb{Q})$).

label	level	notes	j-invariants/models of exceptional points
16.64.2.1	2^4	$N_{\mathrm{ns}}(16)$	$-2^{18}\cdot 3\cdot 5^3\cdot 13^3\cdot 41^3\cdot 107^3/17^{16}$ $-2^{21}\cdot 3^3\cdot 5^3\cdot 7\cdot 13^3\cdot 23^3\cdot 41^3\cdot 179^3\cdot 409^3/79^{16}$
16.96.3.335	2^4	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	$257^3/2^8$
16.96.3.343	2^4	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	$17^3\cdot 241^3/2^4$
16.96.3.346	2^4	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	$2^4\cdot 17^3$
16.96.3.338	2^4	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	2^{11}
32.96.3.230	2^5	$H(4)\subsetneq N_{\mathrm{sp}}(4)$	$-3^3\cdot 5^3\cdot 47^3\cdot 1217^3/(2^8\cdot 31^8)$
32.96.3.82	2^5	$H(8)\subsetneq N_{\mathrm{sp}}(8)$	$3^3\cdot 5^6\cdot 13^3\cdot 23^3\cdot 41^3/(2^{16}\cdot 31^4)$
25.50.2.1	5^2	$H(5)=N_{\mathrm{ns}}(5)$	$2^4\cdot 3^2\cdot 5^7\cdot 23^3$
25.75.2.1	5^2	$H(5)=N_{\mathrm{sp}}(5)$	$2^{12}\cdot 3^3\cdot 5^7\cdot 29^3/7^5$
7.56.1.2	7	$\subsetneq N_{\mathrm{ns}}(7)$	$3^3\cdot 5\cdot 7^5/2^7$
7.112.1.2	7	$-I\notin H$	$y^2+xy+y=x^3-x^2-2680x-50053$ $y^2+xy+y=x^3-x^2-131305x+17430697$
11.60.1.3	11	$\subsetneq B(11)$	$-11\cdot 131^3$
11.120.1.8	11	$-I\notin H$	$y^2+xy+y=x^3+x^2-30x-76$
11.120.1.9	11	$-I\notin H$	$y^2+xy=x^3+x^2-2x-7$
11.60.1.4	11	$\subsetneq B(11)$	-11^2
11.120.1.3	11	$-I\notin H$	$y^2+xy=x^3+x^2-3632x+82757$
11.120.1.4	11	$-I\notin H$	$y^2+xy+y=x^3+x^2-305x+7888$
13.91.3.2	13	$S_4(13)$	$2^4\cdot 5\cdot 13^4\cdot 17^3/3^{13}$, $-2^{12}\cdot 5^3\cdot 11\cdot 13^4/3^{13}$ $2^{18}\cdot 3^3\cdot 13^4\cdot 127^3\cdot 139^3\cdot 157^3\cdot 283^3\cdot 929/(5^{13}\cdot 61^{13})$
17.72.1.2	17	$\subsetneq B(17)$	$-17\cdot 373^3/2^{17}$
17.72.1.4	17	$\subsetneq B(17)$	$-17^2\cdot 101^3/2$
37.114.4.1	37	$\subsetneq B(37)$	$-7\cdot 11^3$
37.114.4.2	37	$\subsetneq B(37)$	$-7\cdot 137^3\cdot 2083^3$

Table 1. All known exceptional groups, j-invariants, and points of prime power level.

Steps of the proof

1. Compute the set $\mathcal{S}$ of **arithmetically maximal** subgroups of ℓ-power level for $\ell \leq 37$ (for all $\ell > 37$ we already know $N_{\mathrm{ns}}(\ell)$ is the only possible exceptional group).

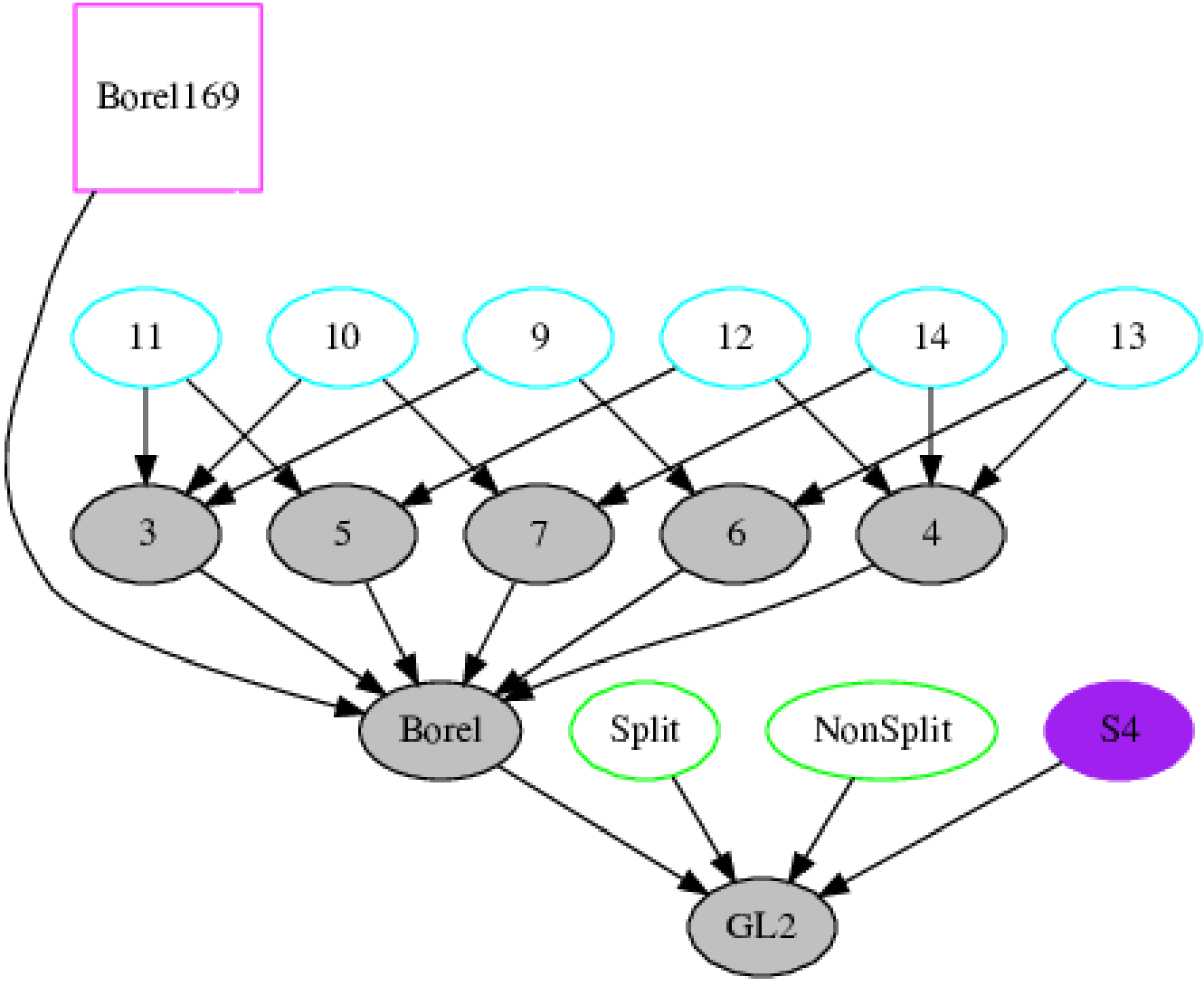
2. For $H \in \mathcal{S}$ check for **local obstructions** and compute the **isogeny decomposition** of the Jacobian of X_H and the analytic ranks of all its simple factors.

3. For $H \in \mathcal{S}$ **compute equations** for X_H and $j_H \colon X_H \to X(1)$ (if needed). In several cases we can prove $X_H(\mathbb{Q})$ is empty without a model for X_H.

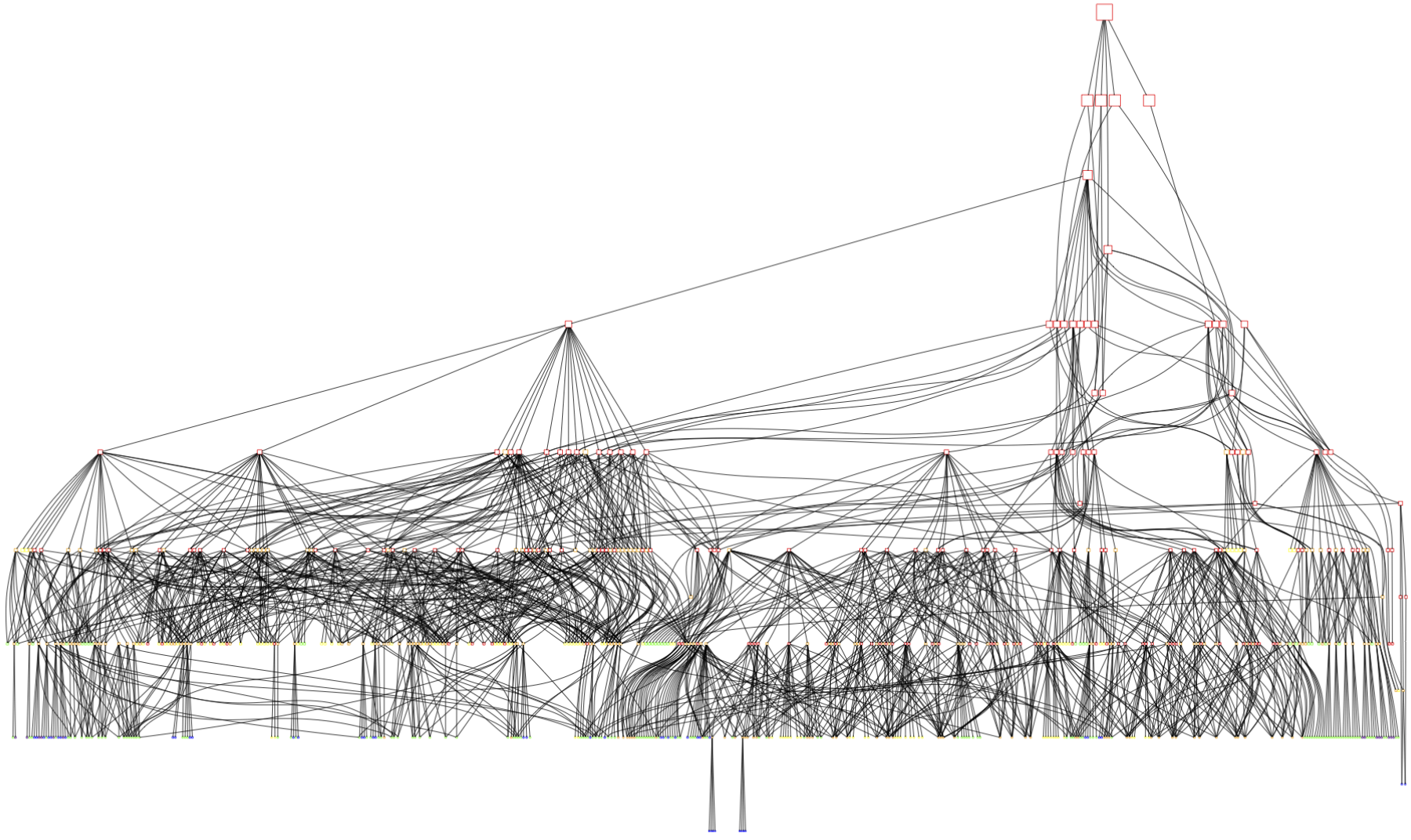
4. For $H \in \mathcal{S}$ with $-I \in H$ **determine the rational points** in $X_H(\mathbb{Q})$ (if possible). In several cases we are able to exploit recent progress by others ($\ell = 13$ for example).

5. For $H \in \mathcal{S}$ with $-I \notin H$ **compute equations** for the universal curve $\mathcal{E} \to U$, where $U \subseteq X_H$ is the locus with $j(P) \neq 0, 1728, \infty$.

Subgroups of $\mathrm{GL}_2(\mathbb{Z}_{13})$



Subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$



UNSOLVED mysteries

Arithmetically maximal level ℓ^n groups with $\ell \leq 13$ with $X_H(\mathbb{Q})$ unknown.

label	level	group	genus
27.243.12.1	3^3	$N_{\mathrm{ns}}(3^3)$	12
25.250.14.1	5^2	$N_{\mathrm{ns}}(5^2)$	14
49.1029.69.1	7^2	$N_{\mathrm{ns}}(7^2)$	69
49.147.9.1	7^2	$G^{\#}_{\mathrm{ns}}(7^2)$	9
49.196.9.1	7^2	$G^{\#}_{\mathrm{sp}}(7^2)$	9
121.6655.511.1	11^2	$N_{\mathrm{ns}}(11^2)$	511

Each has rank $=$ genus, rational CM points, no rational cusps, and no known exceptional points.

Arithmetically maximal level ℓ^n groups with $\ell \leq 13$ with $X_H(\mathbb{Q})$ unknown.

label	level	group	genus
~~27.243.12.1~~[1]	3^3	$N_{\mathrm{ns}}(3^3)$	12
25.250.14.1	5^2	$N_{\mathrm{ns}}(5^2)$	14
~~49.1029.69.1~~[2]	7^2	$N_{\mathrm{ns}}(7^2)$	69
49.147.9.1	7^2	$G^{\#}_{\mathrm{ns}}(7^2)$	9
49.196.9.1	7^2	$G^{\#}_{\mathrm{sp}}(7^2)$	9
121.6655.511.1	11^2	$N_{\mathrm{ns}}(11^2)$	511

Each has rank $=$ genus, rational CM points, no rational cusps, and no known exceptional points.

[1] Balakrishnan–Betts–Hast–Jha–Müller

[2] Furio–Lombardo

Stacks and ramification

The map $X_{\mathrm{ns}}(\ell^n) \to X(1)$ is ramified with degree ℓ^n at each cusp.

Thus $X_{\mathrm{ns}}(\ell^n) \to X_{\mathrm{ns}}(\ell^{n-i})$ is ramified with degree ℓ^i at each cusp.

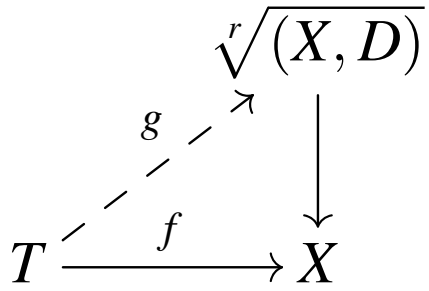
Equivalently, the denominator of $j(E)$ is a perfect ℓ^nth power.

Almost true at the level of polynomials.

Root stacks

Let $D \subseteq X$ be an effective divisor on a scheme and $r \in \mathbb{Z}_{\geq 1}$.

The *rth root stack* $\sqrt[r]{(X, D)}$ of (X, D):



lifting f to g is the same as giving a divisor E on T and a linear equivalence $rE \sim f^*D$.

For curves:

Example

Denominator of the j-map

Furio–Lombardo: Let $E/\mathbb{Q}$ be an elliptic curve without CM.

If $\operatorname{Im}\rho_{E,49} \subseteq C_{\mathrm{ns}}^{+}(49)$, there exist $k \in \{1,8\}$ and pairwise coprime integers $x, y, z \in \mathbb{Z}$ such that

$$x^3 - 7x^2y + 7xy^2 + 7y^3 = k \cdot z^7 \qquad \text{and} \qquad j(E) = j_{\mathrm{ns}}\left(\frac{x}{y}\right).$$

If $\operatorname{Im}\rho_{E,49} \subseteq G_{\mathrm{ns}}^{\#}(49)$, there exist $k \in \{1,8\}$ and pairwise coprime integers $x, y, z \in \mathbb{Z}$ such that

$$x^3 - 7x^2y + 7xy^2 + 7y^3 = 7k \cdot z^7 \qquad \text{and} \qquad j(E) = j_{\mathrm{ns}}\left(\frac{x}{y}\right).$$

If $\operatorname{Im}\rho_{E,49} \subseteq G_{\mathrm{sp}}^{\#}(49)$, there exist $k \in \{1,7\}$ and pairwise coprime integers $x, y, z, w \in \mathbb{Z}$ such that $y = w^7$ and

$$x^3 - 4x^2y + 3xy^2 + y^3 = k \cdot z^7 \qquad \text{and} \qquad j(E) = j_{\mathrm{sp}}\left(\frac{x}{y}\right).$$

Bennett–Dahmen and invariant theory

Darmon and Granville prove that such equations have finitely many primitive solutions. (Because of stacks)

The Poonen–Schaefer–Stoll playbook

Theorem (Furio–Lombardo)

The $(\star)$-solutions of the equation

$$a^2 + 28b^3 = 27c^7 \tag{1}$$

are precisely

$$(\pm 1, -1, -1), \quad (\pm 27, -3, -1), \quad (\pm 2521, -61, -1).$$

Theorem (ZB–Santiago Arango-Piñeros, in progress)

$X_{\mathrm{ns}}^{\#}(49)$ and $X_{\mathrm{sp}}^{\#}(49)$ have no exceptional points

Kummer's proof of Fermat's Last Theorem for Regular primes

A "variant" of Kummer's proof

Suppose that we want to solve

$$x^3 - 4x^2z + 3xz^2 + z^3 = w^7.$$

Kummer's approach gives $u \in \mathcal{O}_L^*/(\mathcal{O}_L^*)^7$ such that

$$x - z\alpha = u\beta^7$$

Extend $\{1, \alpha\}$ to a basis. (α^2 will do fine.) Write

$$\beta = a + b\alpha + c\alpha^2$$

where a, b, c are variables. Then

$$x - z\alpha = \beta^7 = (a + b\alpha + c\alpha^2)^7 = f_0(a,b,c) + f_1(a,b,c)\alpha + f_2(a,b,c)\alpha^2$$

for some homogenous degree 7 polynomials f_i. In particular,

$$\begin{aligned} x &= f_0(a,b,c) \\ -z &= f_1(a,b,c) \\ 0 &= f_2(a,b,c). \end{aligned}$$

This last equation $f_2(a,b,c)$ defines a smooth genus 15 curve C.

$$x - z\alpha = \beta^7 = (a + b\alpha + c\alpha^2)^7 = f_0(a,b,c) + f_1(a,b,c)\alpha + f_2(a,b,c)\alpha^2$$

$f_2(a,b,c)$ defines a smooth genus 15 curve C.

Over $K = \mathbb{Q}(\zeta_7)$ we have computable maps

$$C \to D \to E$$

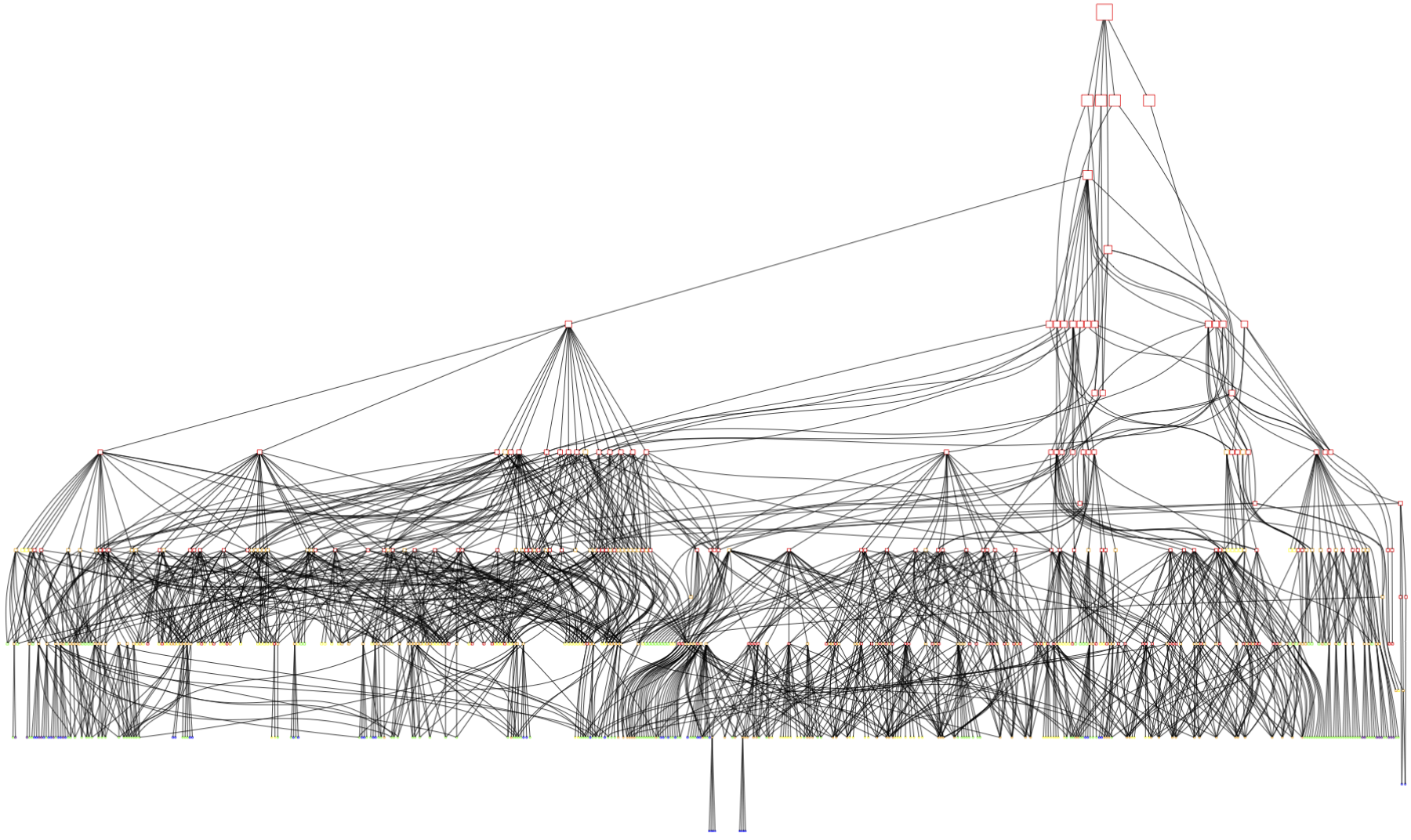
where D is a genus 3 curve and E is an elliptic curve with $\operatorname{rk} E(K) = 0$.

For $u = 1$ this took most of a day, and a longer computation is running now to verify all of the cases.

If we pick a better basis, this works **integrally** and "recovers" Kummer's proof, and generally gives lots of "divisibility" information.

E.g. for $u = 1$, $f_1(a,b,c)$ is a multiple of 7, and so z is too.

Subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$



Agreeable groups

Zywina (indices occurring infinitely often, modulo conjectures)

The **index** of $\rho_{E,N}(G_{\mathbb{Q}})$ divides $220, 336, 360, 504, 864, 1152, 1200, 1296$ or 1536.

Remark

$j(E) \in \{-7 \cdot 11^3, -7 \cdot 137^3 \cdot 2083^3\}$ *does occur finitely often*

Definition

An open $G \leq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is **agreeable** if $\det G = \widehat{\mathbb{Z}}^\times$, contains all scalar matrices, and the levels of G and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ are divisible by the same odd prime divisors.

Zywina computes a finite list of agreeable G such that determining $X_G(\mathbb{Q})$ determines all possibilities for the index.

Agreeable groups

Zywina computes a finite list of agreeable G such that determining $X_G(\mathbb{Q})$ determines all possibilities for the index.

Such G are **arithmetically maximal**, i.e., $X_G(\mathbb{Q})$ is finite and for every H such that $G \leq H$, $X_H(\mathbb{Q})$ is infinite.

If G is normal in H then the map of coarse spaces

$$X_G \to X_H$$

factors through a root stack $\mathcal{X}$ over X_H.

$\mathcal{X}$ is a stacky $\mathbb{P}^1$ or stacky elliptic curve, and is hyperbolic.

One can thus work with (twists of) étale covers of $\mathcal{X}$ (e.g., Belyi covers) and mostly ignore G.

If G is not normal in H, one can look directly at the ramification and might get lucky.