

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 of what's new:

- 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

Condensed Pseudo-Perfectoid Higher ∞ -Stacks and a Derived Hyper-Monoidal Liquid Arithmetic Bhargava–Gauss–Langlands–Scholze–Rota–Witt Correspondence via δ -modularity of ℓ -adic forms on the Rigid Interuniversal Log-Crystalline Site of Non-Teichmüller Motives: A Gentle Introduction¹

David Zureick-Brown (Amherst College)

Santiago Arango-Piñeros (UMass Amherst)

$$\begin{array}{c}
 \begin{array}{ccc}
 \tilde{X}_A & \xleftrightarrow{\alpha_u} & \tilde{X}_A \\
 \downarrow \psi_B & \searrow f & \downarrow \psi_B \\
 \Pi_1(G)^{\sim} \tilde{X}_B & \longrightarrow & X_B
 \end{array}
 \end{array}
 \quad
 \begin{array}{c}
 D^+(R_{\infty}(1/p) \otimes \mathcal{L} \mathcal{LC}^{\bullet}(S) = R\Gamma(\widehat{Y}_{\mathcal{B}}, \widehat{\mathcal{D}}_{\text{LG}} \widehat{T}) \longrightarrow \int \text{graph} \\
 -|x|_{\text{dd}} < e. \implies R\Gamma(\widehat{Y}'_{\mathcal{B}}, \widehat{\mathcal{D}}_{\text{LT}}) \approx R\text{Hom}(S, T) \Big|_{\mathcal{B}}^{\mathcal{B}} \tilde{\Pi}_{\mathcal{B}} = \frac{M}{\mathcal{T}_{\mathcal{E}} n} \\
 \sum_z i\{n \text{ Ext}_1^z(M, N) = [-\mathcal{T}_c \mathcal{J} \cdot \text{Gal}(L/M) \triangleleft \text{GL}_2(\dot{\mathbb{E}})^{L+} \} \\
 \lim_{\alpha \infty} - = E_k^{\mathcal{E}} \quad \tau_n = \text{Tr}_{\mathcal{O}}(\Phi^{\mathcal{E}}_1 V_1) \rightarrow 0 \rightarrow F_{\mathcal{E}} \rightarrow C^{\mathcal{I}} \rightarrow 0 \quad \longleftarrow \circ \longrightarrow \quad \longleftarrow \frac{\widehat{\mathcal{I}}_c + H}{\mathcal{I}_{\mathcal{B}} + H} = \\
 \text{graph} \quad |D_j^a| > \text{RH}^{\Delta}(\widehat{V}_{\psi}, \overline{V}) - H^{\frac{u_a}{\theta}}(X, \overline{Z}_p) = (\widehat{T}_p)^{\frac{n}{2}} \Big\| \text{Mod}_{\Delta} \Leftrightarrow \widehat{D}F\text{-Isoc} \circ.
 \end{array}$$

¹but with Full Proofs

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 of what's new:

- 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

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

$$\begin{aligned}\rho_{E,n}: G_K &\rightarrow \text{Aut } E[n] \cong \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ \rho_{E,\ell^\infty}: G_K &\rightarrow \text{GL}_2(\mathbb{Z}_\ell) = \varprojlim_n \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \\ \rho_E: G_K &\rightarrow \text{GL}_2(\widehat{\mathbb{Z}}) = \varprojlim_n \text{GL}_2(\mathbb{Z}/n\mathbb{Z})\end{aligned}$$

Image of Galois

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

$$\left\{ \begin{array}{c} \overline{\mathbb{Q}} \\ | \\ \overline{\mathbb{Q}}^{\ker \rho_{E,n}} = \mathbb{Q}(E[n]) \\ | \\ \mathbb{Q} \end{array} \right\} H(n)$$

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 $Gal(\bar{K}/K)$ 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** $\phi: E \rightarrow E'$ 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:

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

$H(n) \subset N_{\text{ns}}$ 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 $\Gamma(N) \subset H \subset \text{GL}_2(\widehat{\mathbb{Z}})$. 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 $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$)

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

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. $X_H(\mathbb{Q})$ is finite and E is non-cuspidal and non-CM)
- Can compute $g(X_H)$ group theoretically (via Riemann–Hurwitz).

Fact

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

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

Uniformity 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: the indices occurring infinitely often divide

220, 336, 360, 504, 864, 1152, 1200, 1296 or 1536

Remark

$$1536 < \left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}}) \right] \leq 2736$$

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

Recall

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

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 $H \leq N_{\text{ns}}(3^3), N_{\text{ns}}(5^2), N_{\text{ns}}(7^2), N_{\text{ns}}(11^2)$, or $N_{\text{ns}}(\ell)$ for some $\ell > 13$; or
- ④ $H \leq G_{\text{sp}}^\#(7^2), G_{\text{ns}}^\#(7^2)$ (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 $X_{\text{ns}}^+(11^2)(\mathbb{Q})$).

label	level	notes	j -invariants/models of exceptional points
16.64.2.1	2 ⁴	$N_{\text{ns}}(16)$	$-2^{18} \cdot 3 \cdot 5^3 \cdot 13^3 \cdot 41^3 \cdot 107^3 / 17^{16}$ $-2^{21} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13^3 \cdot 23^3 \cdot 41^3 \cdot 179^3 \cdot 409^3 / 79^{16}$
16.96.3.335	2 ⁴	$H(4) \subsetneq N_{\text{sp}}(4)$	$257^3 / 2^8$
16.96.3.343	2 ⁴	$H(4) \subsetneq N_{\text{sp}}(4)$	$17^3 \cdot 241^3 / 2^4$
16.96.3.346	2 ⁴	$H(4) \subsetneq N_{\text{sp}}(4)$	$2^4 \cdot 17^3$
16.96.3.338	2 ⁴	$H(4) \subsetneq N_{\text{sp}}(4)$	2^{11}
32.96.3.230	2 ⁵	$H(4) \subsetneq N_{\text{sp}}(4)$	$-3^3 \cdot 5^3 \cdot 47^3 \cdot 1217^3 / (2^8 \cdot 31^8)$
32.96.3.82	2 ⁵	$H(8) \subsetneq N_{\text{sp}}(8)$	$3^3 \cdot 5^6 \cdot 13^3 \cdot 23^3 \cdot 41^3 / (2^{16} \cdot 31^4)$
25.50.2.1	5 ²	$H(5) = N_{\text{ns}}(5)$	$2^4 \cdot 3^2 \cdot 5^7 \cdot 23^3$
25.75.2.1	5 ²	$H(5) = N_{\text{sp}}(5)$	$2^{12} \cdot 3^3 \cdot 5^7 \cdot 29^3 / 7^5$
7.56.1.2	7	$\subsetneq N_{\text{ns}}(7)$	$3^3 \cdot 5 \cdot 7^5 / 2^7$
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.

Approach

Compute the set of **arithmetically maximal** subgroups

H is arithmetically maximal if

- $X_H(\mathbb{Q})$ is finite and
- for every G such that $H \leq G$, $X_G(\mathbb{Q})$ is infinite.

For such H **compute equations** for X_H and $j_H: X_H \rightarrow X(1)$

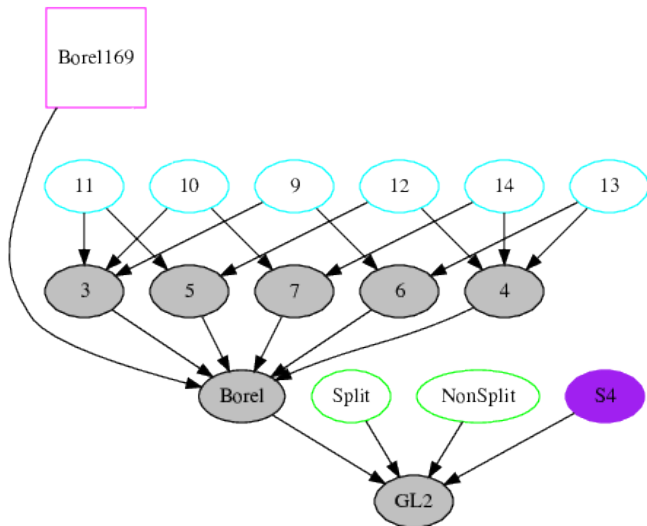
See Rouse's **VaNTAGe talk** for details and examples,

Assaf's **recent paper** and

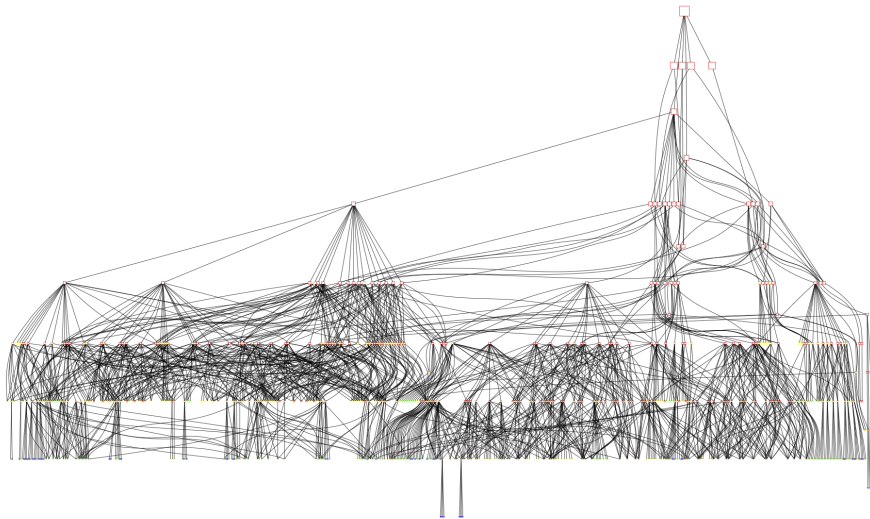
Zywina's **BIRS talk** for newer efficient approaches.

For such H with $-I \in H$ **determine the rational points** in $X_H(\mathbb{Q})$

Subgroups of $GL_2(\mathbb{Z}_{13})$



Subgroups of $GL_2(\mathbb{Z}_2)$



Explicit methods: highlight reel

- Local methods
 - Chabauty and Elliptic Chabauty
 - Mordell–Weil sieve
 - étale descent
 - Pryms
-
- *Equationless étale descent via group theory*
 - *New techniques for computing $\text{Aut } C$*
-
- *Nonabelian Chabauty*
 - **“Equationless” local methods** and **Mordell–Weil sieve**
 - **Greenberg Transforms** (and big computations)
 - **Novel variants of existing techniques** (e.g., Atkin–Lehner sieve)
 - **Modularity of isogeny factors of J_H** (w/ Voight)

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	$N_{\text{ns}}(3^3)$	12
25.250.14.1	5^2	$N_{\text{ns}}(5^2)$	14
49.1029.69.1	7^2	$N_{\text{ns}}(7^2)$	69
49.147.9.1	7^2	$G_{\text{ns}}^{\#}(7^2)$	9
49.196.9.1	7^2	$G_{\text{sp}}^{\#}(7^2)$	9
121.6655.511.1	11^2	$N_{\text{ns}}(11^2)$	511

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

THE SETTLERS OF

CARTAN®



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

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

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

²Balakrishnan–Betts–Hast–Jha–Müller

³Furio–Lombardo

Stacks and ramification

Some related facts:

- The map $X_{\text{ns}}(\ell^n) \rightarrow X(1)$ is ramified with degree ℓ^n at each cusp.
- Thus $X_{\text{ns}}(\ell^n) \rightarrow X_{\text{ns}}(\ell^{n-i})$ is ramified with degree ℓ^i at each cusp.
- The denominator of $j(E)$ is a perfect ℓ^n th power (for E a point on $X_{\text{ns}}(\ell^n)$ and ℓ odd).
- The denominator of the j -map $X_{\text{ns}}(\ell^n) \rightarrow X(1)$ is “often” a perfect ℓ^n th power.

Denominator of j -map

$$j_{\text{ns}}: X_{\text{ns}}(7) \cong \mathbb{P}^1 \rightarrow X(1)$$

is given by

$$j(E) = j_{\text{ns}}(t) = \frac{g(t)^3}{f(t)^7}$$

The denominator of $j_{\text{ns}}: X_{\text{ns}}(7^2) \rightarrow X(1)$ is a 7^2 th power.

So if $j(E)$ is the j -invariant of an exceptional point on $X_{\text{ns}}(7^2)$,
then $f(x, y)^7$ is a 7^2 th power (up to a resultant),
i.e., $f(x, y)$ is a 7th power.
(up to resultants)

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

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

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

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

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

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

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

Darmon–Granville: Faltings' theorem is true for stacky curves.

Certain surfaces have finitely many primitive integral solutions, e.g.,

- $x^3 + y^5 = z^7$,
- $x^3 - 7x^2y + 7xy^2 + 7y^3 = k \cdot z^7$,

since their stack quotients are hyperbolic.

Bennett–Dahmen: Generalized superelliptic equations

If $F(x, y)$ is a homogenous binary cubic, then

$$4H(x, y)^3 + G(x, y)^2 = -27\Delta_F F(x, y)^2.$$

Thus

$$-27\Delta(x^3 - 7x^2y + 7xy^2 + 7y^3)^2 = 4H(x, y)^3 + G(x, y)^2 = -27(k \cdot z^7)^2$$

Theorem (Furio–Lombardo)

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

$$a^2 + 28b^3 = 27c^7$$

are

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

The Poonen–Schaefer–Stoll playbook

- **Frey Curve:** $(a, b, c) \mapsto E_{a,b,c}$
- **Level lowering:** $\exists E$ with $N_E \mid 2^4 \cdot 7^2$ s.t. $E_{a,b,c}[7] \cong E[7]$
- **Moduli:** This corresponds to a point $(E_{a,b,c}[7], \iota) \in X_E(7)(\mathbb{Q})$.
- $X_E(7)$ is a **twist of the Klein quartic**, a genus 3 plane quartic.

$$x^4 + 3x^3y - 3x^2yz - 3x^2z^2 + 6xy^3 - 6xy^2z + 3xyz^2 - 2xz^3 + 4y^4 + 2y^3z - 5yz^3$$

- One can do **Chabauty** and more with this finite list of curves.

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

Assuming GRH, $X_{\text{ns}}^{\#}(49)$ and $X_{\text{sp}}^{\#}(49)$ have no exceptional points

Kummer: Fermat's Last Theorem for Regular primes

Theorem

If $(x, z, w) \in \mathbb{Z}^3$ is a solution to $x^7 + z^7 = w^7$, then 7 divides xzw .

Idea: factor over $L = \mathbb{Q}(\zeta_7)$,

and use the following facts about L and $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \subset \mathbb{R}$:

- 1 $\mathbb{Q}(\zeta_7)$ has class number 1
- 2 $\mathcal{O}_L^\times = \mu_L \mathcal{O}_K^\times$
- 3 for all $\beta \in L$, $\beta^7 = b \pmod{7\mathcal{O}_L}$ for some $b \in \mathbb{Z}$.

Let $L = \mathbb{Q}(\zeta_7)$ and $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \subset \mathbb{R}$. Then

$$x^7 + z^7 = \prod (x - \zeta_7^i z) = w^7$$

Since $\text{cl}(L) = 1$ and $\mathcal{O}_L^\times = \mu_L \mathcal{O}_K^\times$

$$x - \zeta_7 z = (\zeta_7^r u) \beta^7, \quad \text{for } u \in \mathcal{O}_K^\times, \quad \beta \in \mathcal{O}_L.$$

Elementary: $\beta^7 \equiv b \pmod{7\mathcal{O}_L}$ for some $b \in \mathbb{Z}$. Thus

$$x - \zeta_7 z = \zeta_7^r u b$$

Applying complex conjugation gives

$$x - \zeta_7^{-1} z = \zeta_7^{-r} u b$$

Combining

$$\zeta_7^r (x - \zeta_7^{-1} z) \equiv \zeta_7^{-r} (x - \zeta_7 z) \pmod{7\mathcal{O}_L}$$

i.e.,

$$x \cdot 1 - z \cdot \zeta_7 + z \cdot \zeta_7^{2r-1} - x \cdot \zeta_7^{2r} \equiv 0 \pmod{7\mathcal{O}_L}.$$

If the elements $1, \zeta_7, \zeta_7^{2r-1}, \zeta_7^{2r}$ are all distinct, then they are part of a $\mathbb{Z}$ basis for $\mathcal{O}_L = \mathbb{Z}[\zeta_7]$, and so implies that $7 \mid x$ and $7 \mid z$.

A “variant” of Kummer’s proof

Suppose that we want to solve

$$f(x, z) = x^3 - 4x^2z + 3xz^2 + z^3 = w^7.$$

Let $L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ be the splitting field of f .

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

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

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

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

for some homogenous degree 7 polynomials f_i . In particular,

$$x = f_0(a, b, c)$$

$$-z = f_1(a, b, c)$$

$$0 = f_2(a, b, c).$$

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

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

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

Over $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{7^2})$ we have computable maps

$$C \rightarrow D \rightarrow E$$

where D is a genus 3 curve and E is an elliptic curve with

$$\text{rk } E(\mathbb{Q}(\zeta_{7^2})) = 0.$$

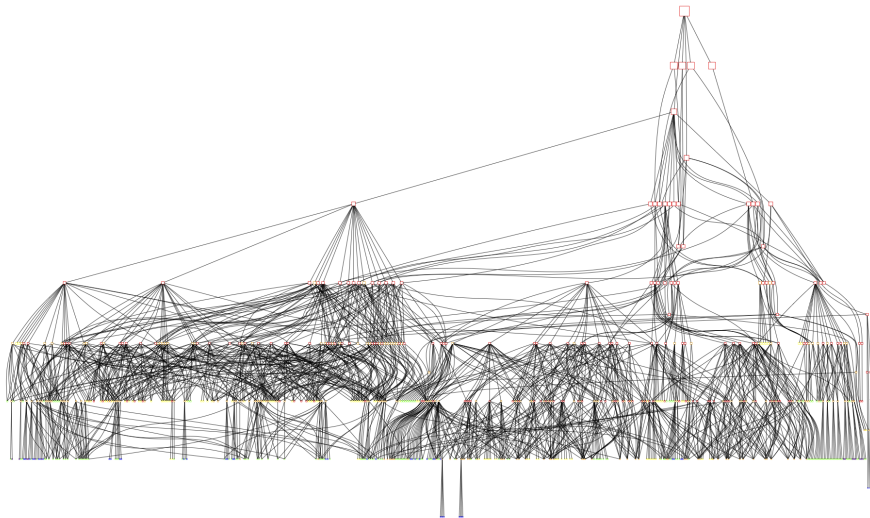
For $u = 1$ this took most of a day.

A longer computation is running now to verify for all units u .

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 $GL_2(\mathbb{Z}_2)$



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

$$X_G \rightarrow X_H$$

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.

Root stacks

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

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

$$\begin{array}{ccc} & \sqrt[r]{(X, D)} & \\ g \nearrow & \downarrow & \\ T & \xrightarrow{f} & X \end{array}$$

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