ℓ-adic Galois representations attached to elliptic curves with CM.

AMS SPRING MEETING

SPECIAL SESSION ON (ANALYTIC METHODS IN) ARITHMETIC GEOMETRY

MARCH 19TH, 2022

ÁLVARO LOZANO-ROBLEDO
UNIVERSITY OF CONNECTICUT

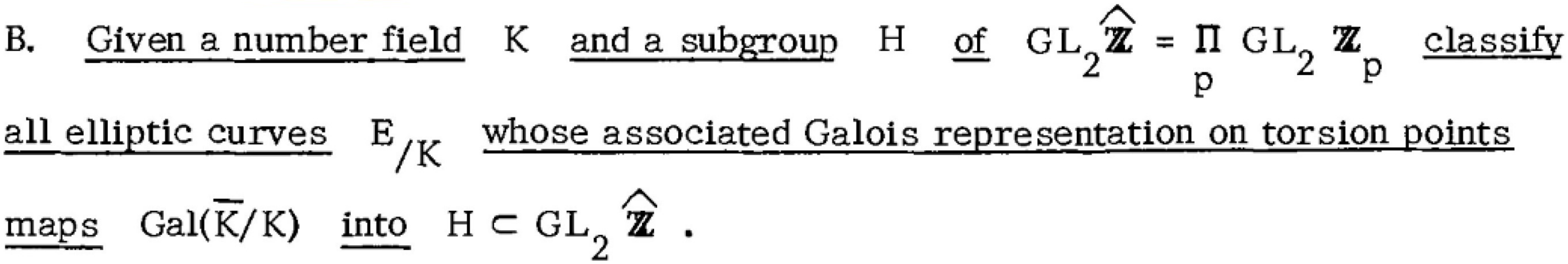
- F a number field
- E/F an elliptic curve over F
- ℓ a prime number
  - $T_\ell(E) = \varprojlim E[\ell^n]$, the ℓ-adic Tate module
  - $T(E) = \varprojlim E[m]$, the adelic Tate module
    - $$\begin{tikzcd} \rho_E : \mathrm{Gal}(\overline{F}/F) \arrow[r] \arrow[dr, bend right, "\rho_{E,\ell^\infty}"'] & \mathrm{Aut}(T(E)) \cong GL(2,\hat{\mathbb{Z}}) \arrow[d] \\ & \mathrm{Aut}(T_\ell(E)) \cong GL(2,\mathbb{Z}_\ell) \end{tikzcd}$$

$$\rho_E : \mathrm{Gal}(\bar{F}/F) \longrightarrow GL(2,\hat{\mathbb{Z}})$$

Question: For a fixed F, what are the possible images (up to conjugation) of ρ_E in $GL(2,\hat{\mathbb{Z}})$?

Mazur's "Program B":

(from "Rational points on modular curves")



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 $\mathrm{Gal}(\bar{K}/K)$ into $H \subset GL_2\hat{\mathbb{Z}}$.

example (Serre)

$E/\mathbb{Q} : y^2 + y = x^3 + x^2$, $\Delta_E = -43.$ LMFDB $(43.a1)$

- $\mathrm{Im}(\rho_{E,\ell^\infty}) = GL(2, \mathbb{Z}_\ell)$ for <u>all</u> primes ℓ.

- $\mathrm{Im}(\rho_{E,86}) \underset{\text{index } 2}{\subsetneq} GL(2, \mathbb{Z}/86\mathbb{Z})$

- $\mathrm{Im}(\rho_E) \underset{\text{index } 2}{\subsetneq} GL(2, \hat{\mathbb{Z}})$

$$\begin{tikzcd}
 & & \mathbb{Q}(E[43]) \arrow[d, dash] \\
\mathbb{Q}(E[2]) \arrow[dr, dash] & & \mathbb{Q}(\zeta_{43}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{-43}) \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Theorem (Serre) If $E/\mathbb{Q}$ does not have CM, then $\mathrm{Im}(\rho_E)$ is open (finite index) in $GL(2,\hat{\mathbb{Z}})$.

Moreover, $[GL(2,\hat{\mathbb{Z}}) : \mathrm{Im}(\rho_E)] \geq 2$. (INDEX IS IN FACT ALWAYS EVEN!)

Serre's Question: If $E/\mathbb{Q}$ does not have CM,

is $\mathrm{Im}(\rho_{E,\ell^\infty}) = GL(2,\mathbb{Z}_\ell)$ for all $p > 37$?

Conjecture. (Zywina) If $E/\mathbb{Q}$ does not have CM, then except for a finite number of exceptions ($j \in J$, w/ $J \subseteq \mathbb{Q}$ finite)

$$[GL(2,\hat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \in \left\{ \begin{array}{l} 2,4,6,8,10,12,16,20,24,30,32,36,40,48,54,60, \\ 72,84,96,108,112,120,144,192,220,240,288, \\ 336,360,384,504,576,768,864,1152,1200,1296,1536 \end{array} \right\}.$$

THE 2-ADIC IMAGE

Theorem (Rouse, Zureick-Brown, 2014)

Let $E/\mathbb{Q}$ be an elliptic curve w/o CM. Then, the image of

$$\rho_{E,2^\infty} : G_{\mathbb{Q}} \to \mathrm{Aut}(T_2(E)) \cong GL(2, \mathbb{Z}_2)$$

is one of 1208 possibilities (up to conjugation).

THE ℓ-ADIC IMAGE

Theorem*(Sutherland, Zywina, 2017, and Rouse, Sutherland, Zureick-Brown, 2021)

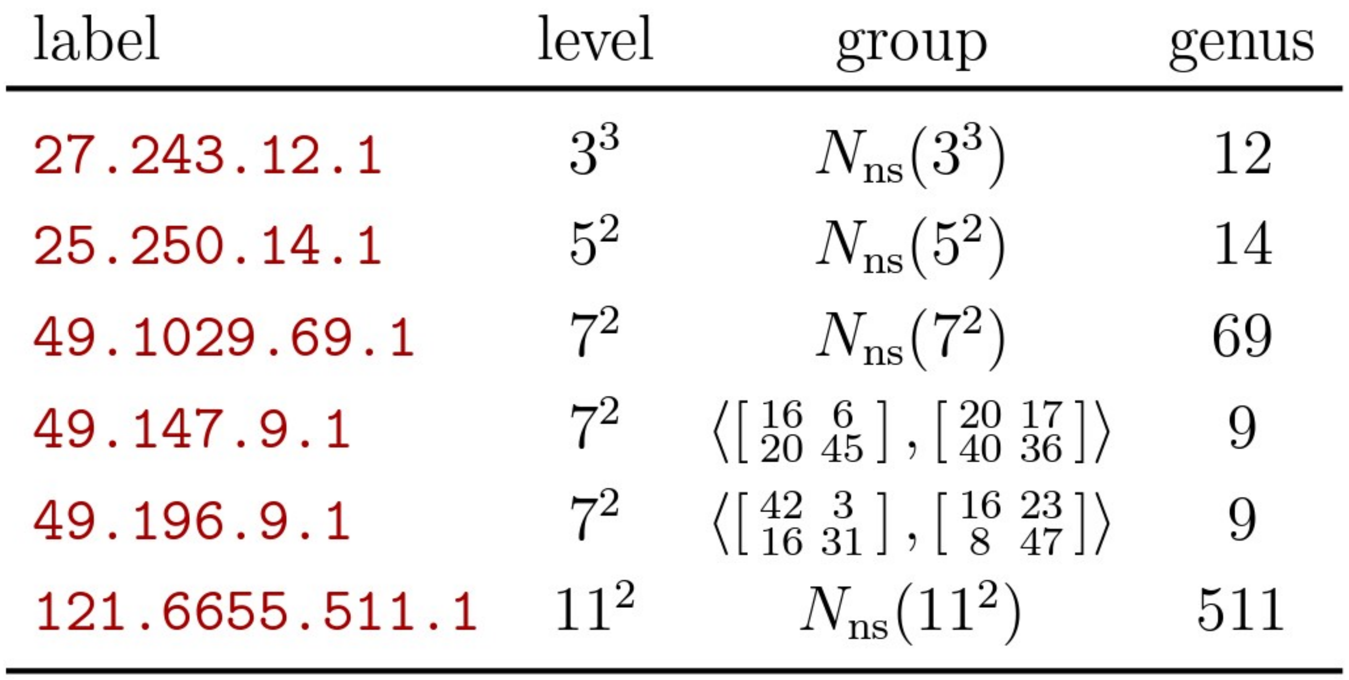
Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ (w/o CM). Then, there are $a(\ell)$ possibilities for $\rho_{E,\ell^\infty}(G_{\mathbb{Q}})$ up to conjugation, where

ℓ	2	3	5	7	11	13	17	37	other
$a(\ell)$	1208	47*	25*	17*	8*	12	3	3*	1*

*: depends on a "ℓ-adic Serre uniformity" conjecture.

* IMAGES :

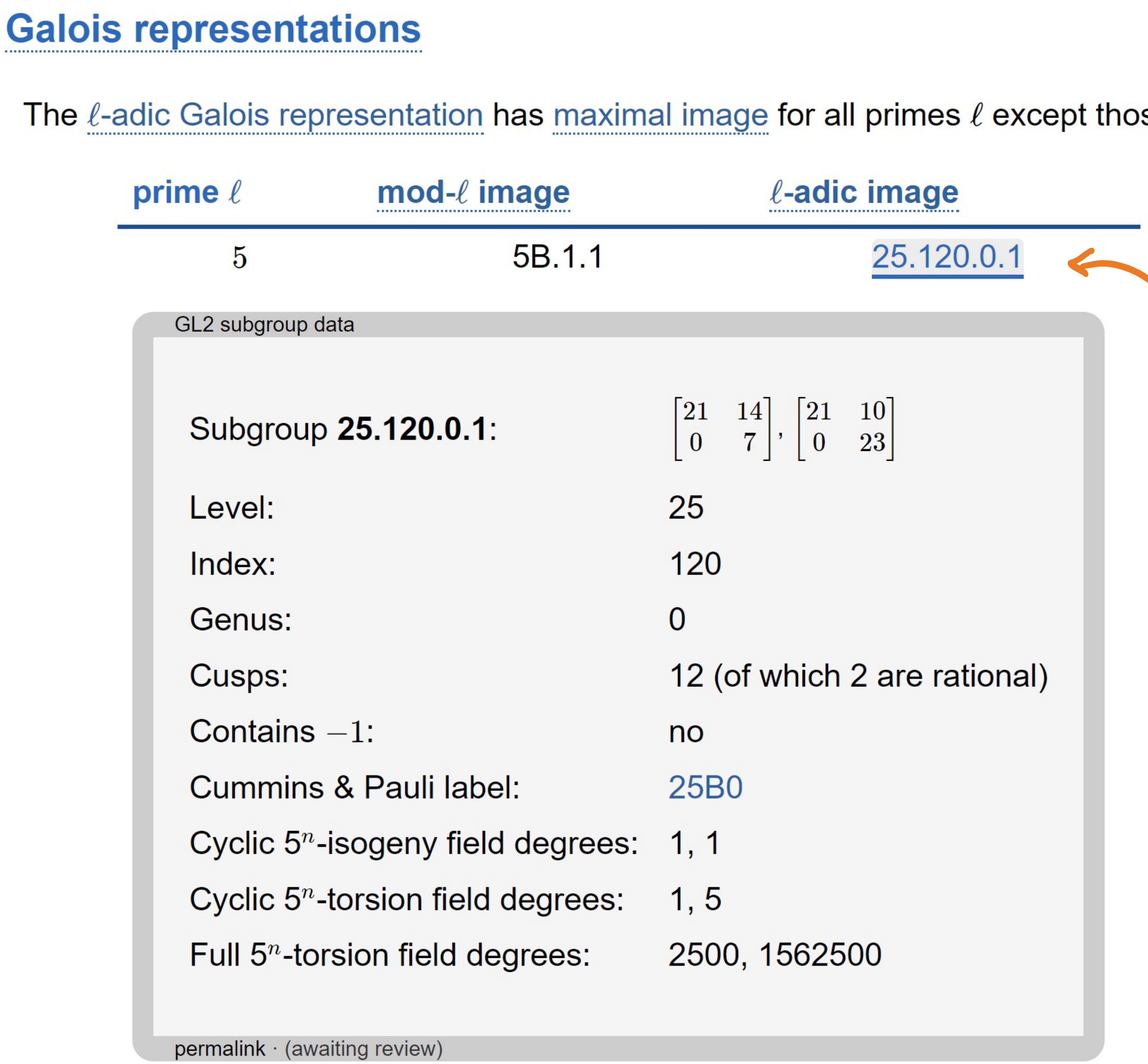
$N_{ns}(\ell)$ for $\ell > 17$ and ...



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	$\langle \left[\begin{smallmatrix} 16 & 6 \\ 20 & 45 \end{smallmatrix}\right], \left[\begin{smallmatrix} 20 & 17 \\ 40 & 36 \end{smallmatrix}\right] \rangle$	9
49.196.9.1	7^2	$\langle \left[\begin{smallmatrix} 42 & 3 \\ 16 & 31 \end{smallmatrix}\right], \left[\begin{smallmatrix} 16 & 23 \\ 8 & 47 \end{smallmatrix}\right] \rangle$	9
121.6655.511.1	11^2	$N_{\mathrm{ns}}(11^2)$	511

TABLE 2. Arithmetically maximal groups of ℓ-power level with $\ell \leq 17$ for which $X_H(\mathbb{Q})$ is unknown; each has rank = genus, rational CM points, no rational cusps, and no known exceptional points.

example $E/\mathbb{Q} : y^2 + y = x^3 - x^2$ (11.a3)



Galois representations

The ℓ-adic Galois representation has maximal image for all primes ℓ except those listed in the table below.

prime ℓ	mod-ℓ image	ℓ-adic image
5	5B.1.1	25.120.0.1

GL2 subgroup data

Subgroup **25.120.0.1**:	$\begin{bmatrix}21 & 14\\ 0 & 7\end{bmatrix}, \begin{bmatrix}21 & 10\\ 0 & 23\end{bmatrix}$
Level:	25
Index:	120
Genus:	0
Cusps:	12 (of which 2 are rational)
Contains -1:	no
Cummins & Pauli label:	25B0
Cyclic 5^n-isogeny field degrees:	1, 1
Cyclic 5^n-torsion field degrees:	1, 5
Full 5^n-torsion field degrees:	2500, 1562500

permalink · (awaiting review)

$$\left\{\begin{pmatrix} \overset{\equiv 1 \bmod 5}{a} & b \\ \underset{\equiv 0 \bmod 25}{c} & d\end{pmatrix}\right\} \subseteq GL(2,\mathbb{Z}_5)$$

Question : What about in the CM case ??

Theorem: Let $E/\mathbb{Q}$ be an elliptic curve WITH CM.

Then, there are $a_{CM}(\ell)$ possibilities for $\rho_{E,\ell^\infty}(G_{\mathbb{Q}})$ up to conjugation, where:

ℓ	2	3	7, 11, 43, 67	19, 163	else $\ell \not\equiv \pm 1 \bmod 9$	else $\ell \equiv \pm 1 \bmod 9$
$a_{CM}(\ell)$	28	17	6	5	2 or 3	1 or 2

example $\ell = 7$: 27.a1, 32.a1, 441.d2, 441.c1, 49.a1, 49.a3

27.a1	32.a1	441.d2	441.c1	49.a1	49.a3
maximal split	maximal non-split	index 3 in maximal split ($j=0$)	maximal "CM Borel"	index 2 in "CM Borel"	

Possibilities for the image by CM order, over $\mathbb{Q}$:

Δ_K	f	2		3		7,11,43,67		19,163		else ℓ $\ell\not\equiv\pm1 \bmod 9$		else ℓ $\ell\equiv\pm1$ (9)	
-3	1	1+1	3	9+3	15	1+1	2	1	1	1+1	2	1	1
	2	1		3		1		1		1		1	
	3	1		3		1		1		1		1	
-4	1	13	18	1	1	1	1	1	1	1	1	1	1
	2	5		1		1		1		1		1	
-7	1	1	2	1	1	4 (if $\ell=7$	4 (else 1)	1	1	1	1	1	1
	2	1		1		4 else 1)		1		1		1	
-8	1	5		1		1		1		1		1	
-11	1	1		1		$\begin{cases}4 & \text{if } \ell=-\Delta_K\\ 1 & \text{if } \ell\neq-\Delta_K\end{cases}$		$\begin{cases}4 & \text{if } \ell=-\Delta_K\\ 1 & \text{if } \ell\neq-\Delta_K\end{cases}$		1		1	
-19	1												
-43	1												
-67	1												
-163	1												

Example

$\Delta_K = -8$

$f = 1$

$\ell = 2$

SUBGROUPS OF $GL(2,\mathbb{Z}_2)$:

- $\left\langle \left\{ \begin{pmatrix} a & b \\ -2b & a \end{pmatrix} : a \in \mathbb{Z}_2^\times, b \in \mathbb{Z}_2 \right\}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$, 2304.h2
- $\left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$, 16.192.5.602 (image mod 16), 256.d1 (LMFDB label of an example E/$\mathbb{Q}$)
- $\left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$, 16.192.5.617, 256.d2
- $\left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$, 16.192.5.607, 256.a2
- $\left\langle \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$, 16.192.5.624, 256.a1

($\ell > 3$, $j \neq 0$)

EXAMPLE

FACT: [If $\Delta_K f^2 \notin (\mathbb{Z}_\ell^\times)^2$ (resp. $\in (\mathbb{Z}_\ell^\times)^2$)

then image is $N_{ns}(\ell^\infty) \subseteq GL_2(\mathbb{Z}_\ell)$ (resp. $N_s(\ell^\infty)$)]

If $\ell \equiv 1 \bmod 9$ and $-1, 2, 3, 7, 11, 19, 43, 67, 163 \notin (\mathbb{Z}_\ell^\times)^2$ (resp $\in (\mathbb{Z}_\ell^\times)^2$)

then *every* $E/\mathbb{Q}$ w/ CM will have image

$$N_{ns}(\ell^\infty) \qquad (\text{resp. } N_s(\ell^\infty))$$

This happens for: $\ell = 13267, 25939, 27091, 46027, \ldots$

(resp. for $\ell = 69337, 100153, 107209, 140977, \ldots$)

THE CM CASE

- $K/\mathbb{Q}$ quad. imag.,
- $\mathcal{O}_K$ ring of integers, discriminant Δ_K,
- $\mathfrak{f} \geq 1$ conductor,
- $\mathcal{O}_{K,\mathfrak{f}} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ order of conductor $\mathfrak{f}$,
- $j_{K,\mathfrak{f}}$ a Galois conjugate of $j(\mathbb{C}/\mathcal{O}_{K,\mathfrak{f}})$

- $E/\mathbb{Q}(j_{K,\mathfrak{f}})$ an elliptic curve defined over $\mathbb{Q}(j_{K,\mathfrak{f}})$ with CM by $\mathcal{O}_{K,\mathfrak{f}}$.

- $E/\mathbb{Q}(j_{K,f})$ an elliptic curve defined over $\mathbb{Q}(j_{K,f})$ with CM by $\mathcal{O}_{K,f}$.

- If $\Delta_K f^2 \equiv 0 \bmod 4$, put $\delta = \frac{\Delta_K f^2}{4}$, $\phi = 0$.

  If $\Delta_K f^2 \not\equiv 0 \bmod 4$, put $\delta = \frac{\Delta_K - 1}{4} \cdot f^2$, $\phi = f$.

- $$C_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a+b\phi & b \\ \delta b & a \end{pmatrix} : a,b \in \mathbb{Z}/N\mathbb{Z} \text{ s.t. } \det \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}$$

- $$N_{\delta,\phi}(N) = \left\langle C_{\delta,\phi}(N), \begin{pmatrix} -1 & 0 \\ f & 1 \end{pmatrix} \right\rangle$$ the "normalizer" of Cartan

- $$N_{\delta,\phi} = \varprojlim N_{\delta,\phi}(N) \subseteq GL(2,\hat{\mathbb{Z}})$$

WARNING!

- $E/\mathbb{Q}(j_{K,f})$ an elliptic curve defined over $\mathbb{Q}(j_{K,f})$ with CM by $\mathcal{O}_{K,f}$.
- If $\Delta_K f^2 \equiv 0 \bmod 4$, put $\delta = \frac{\Delta_K f^2}{4}$, $\phi = 0$.

  If $\Delta_K f^2 \not\equiv 0 \bmod 4$, put $\delta = \frac{\Delta_K - 1}{4} \cdot f^2$, $\phi = f$.
- $C_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a+b\phi & b \\ \delta b & a \end{pmatrix} : a,b \in \mathbb{Z}/N\mathbb{Z} \text{ s.t. } \det \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}$
- $N_{\delta,\phi}(N) = \left\langle C_{\delta,\phi}(N), \begin{pmatrix} -1 & 0 \\ f & 1 \end{pmatrix} \right\rangle$
- $N_{\delta,\phi} = \varprojlim N_{\delta,\phi}(N)$

Theorem:
- $\mathrm{Im}(\rho_E)$ is conjugate to a subgroup $H_E \subseteq N_{\delta,\phi} \subseteq GL(2,\hat{\mathbb{Z}})$.
- $[N_{\delta,\phi} : H_E]$ is a divisor of 4 or 6,

  and if $j_{K,f} \neq 0, 1728$, then a divisor of 2.
- If $\ell \nmid 2\Delta_K f$, $\mathrm{Im}(\rho_{E,\ell^\infty}) = N_{\delta,\phi}(\ell^\infty)$.
- If $\ell > 2$ and $j_{K,f} \neq 0$, then $N_{\delta,\phi}(\ell^\infty)$ is full inverse image of $N_{\delta,\phi}(\ell)$.

  or $\ell > 3$

[* See also Bourdon-Clark, Lombardo.]

Question: What are the possibilities for $H \subseteq N_{\delta,\phi}(\ell^\infty)$ up to conjugation?

FIRST: Possibilities for $N_{\delta,\phi}(\ell^\infty)$ up to conjugation!

- If $\Delta_K f^2 \equiv 0 \bmod 4$: write $\delta = \frac{\Delta_K f^2}{4} = u \cdot \ell^n$ with $u \in \mathbb{Z}_\ell^\times$.
  - $N_{\delta,0}(\ell^\infty)$, up to conj., depends only on $[u] \in \mathbb{Z}_\ell^\times / (\mathbb{Z}_\ell^\times)^2$, and $n \geq 0$.

$$\Rightarrow \begin{cases} \ell \geqslant 3 & \{(\text{split}, n), (\text{non-split}, n) : n \geqslant 0\} \\ \ell = 2 & \{(u, n) : u \equiv \underset{\text{"split"}}{1}, \underbrace{3, 5, 7}_{\text{"non-split's"}} \bmod 8, \ n \geqslant 0\} \end{cases}$$

- If $\Delta_K f^2 \not\equiv 0 \bmod 4$, and $\ell = 2$: $N_{\delta,\phi}(2^\infty)$ only depends on $\begin{cases} \delta \equiv 0 \bmod 2 \\ \delta \equiv 1 \bmod 2 \end{cases}$

  with $\delta = \frac{\Delta_K - 1}{4} \cdot f^2$

Maximal images $N_{\delta,\phi}(\ell^\infty)$ up to conj. over $\mathbb{Q}$?

List of (Δ_K, f) s.t. $j_{K,f} \in \mathbb{Q}$:

$$\{(-3,1), (-3,2), (-3,3), (-4,1), (-4,2), (-7,1), (-7,2), (-8,1), (-11,1), (-19,1), (-43,1), (-67,1), (-163,1)\}$$

$\boxed{\ell = 2}$

- $\Delta_K f^2 \not\equiv 0 \bmod 4$

  $\delta = \frac{\Delta_K - 1}{4} \cdot f^2$

  $\rightarrow$ $\delta \equiv 0 \bmod 2, \phi = 1$, $(-7,1)$, 49.a2

  $\rightarrow$ $\delta \equiv 1 \bmod 2, \phi = 1$, $(-3,1)$, 36.a4

- $\Delta_K f^2 \equiv 0 \bmod 4$

  $\delta = \Delta_K f^2$

$$\begin{cases} \delta \equiv 1 \bmod 8, & (-7,2), \quad 784.f3 \\ \delta \equiv 5 \bmod 8, & (-3,2), \quad 36.a2 \\ \delta \equiv 7 \bmod 8, & (-4,1), \quad 288.a2 \\ \delta \equiv 7 \cdot 2 \bmod 16, & (-8,1), \quad 2304.h2 \\ \delta \equiv 7 \cdot 4 \bmod 32, & (-4,2), \quad 288.d2 \end{cases}$$

* $\delta \equiv 3 \bmod 8$ does not occur $/\mathbb{Q}$

$$\boxed{\ell = 3} \qquad \mathcal{N}_{\delta,0}(\mathbb{Z}_3) \begin{cases} \delta \equiv 1 \bmod 3, & (-8,1), & 2304.\mathrm{h2} \\ \delta \equiv 2 \bmod 3, & (-4,1), & 288.\mathrm{a2} \\ \delta \equiv 2\cdot 3 \bmod 9, & (-3,1), & 144.\mathrm{a3} \\ \delta \equiv 2\cdot 3^3 \bmod 81, & (-3,3), & 432.\mathrm{e1} \end{cases}$$

$$\boxed{\ell = 5} \qquad \begin{cases} \delta \equiv 1 \bmod 5, & (-4,1), & 288.\mathrm{a2} \\ \delta \equiv 2 \bmod 5, & (-3,1), & 144.\mathrm{a3} \end{cases}$$

$$\boxed{\ell = 7} \qquad \begin{cases} \delta \equiv 2 \bmod 7, & (-3,3), & 27.\mathrm{a1} \\ \delta \equiv 3 \bmod 7, & (-4,1), & 32.\mathrm{a1} \\ \delta \equiv 5\cdot 7 \bmod 49, & (-7,1), & 441.\mathrm{c1} \end{cases} \rightsquigarrow \left\{ \begin{pmatrix} a & b \\ 0 & \pm a \end{pmatrix} \right\} \subseteq GL(2, \mathbb{F}_7)$$

"CM Borel" mod p

NEXT: Compute subgroups of $N_{\delta,\phi}(\mathbb{Z}_\ell)$ of index dividing $\mathcal{O}_{K,f}^{\times}$ that are possible images.

- $j_{K,f} = 1728$ → indices 1, 2, 4
- $j_{K,f} = 0$ → indices 1, 2, 3, 6
- $j_{K,f} \neq 0, 1728$ → indices 1 or 2

example:

$\boxed{\ell = 7}$ • When $j=0$, $\ell = 7$ is split → $H \subseteq N_{\delta,0}(\mathbb{Z}_7)$ of index 3

ex: 441.d2

- $N_{5\cdot7,0}(\mathbb{Z}_7)$ has 2 subgps of index 2:

$$\text{mod } 7: \quad \underset{441.c1}{\left\{\begin{pmatrix} a & b \\ 0 & \pm a \end{pmatrix}\right\}} \supseteq \underset{49.a1}{\left\{\begin{pmatrix} a^2 & b \\ 0 & \pm a^2 \end{pmatrix}\right\}}, \underset{49.a3}{\left\{\begin{pmatrix} \pm a^2 & b \\ 0 & a^2 \end{pmatrix}\right\}}$$

A LABEL FOR EACH CM IMAGE

$\ell.n.s-L.i.t$ where: ℓ = prime

$n = v_\ell(\Delta)$ where $\Delta = \Delta_K f^2 = \mathrm{disc}(\mathcal{O}_{K,f})$

s = square class of δ/ℓ^n in $\mathbb{Z}_\ell^\times/(\mathbb{Z}_\ell^\times)^2$

L = level of the image

i = index in the maximal gp $\mathcal{N}_{\delta,\phi}(\mathbb{Z}_\ell)$

t = tie breaker

ex $\ell = 7$ / $\mathbb{Q}$

maximal images
- 7.0.ns-1.1.1
- 7.0.s-1.1.1

7.0.s-7.$\underline{\underline{3}}$.1

index 3

7.1.ns-1.1.1

7.1.ns-7.2.1

7.1.ns-7.2.2

Borel type

THANK YOU !

ex

$\ell = 2$

$\Delta_K = -4$

$f = 2$

2.4.ns7-1.1.1	16.96.3.325	288.d2
2.4.ns7-8.2.1	16.192.3.545	64.a2
2.4.ns7-8.2.2	16.192.3.540	32.a2
2.4.ns7-8.2.3	16.192.3.554	32.a1
2.4.ns7-8.2.4	16.192.3.563	64.a1
CM label	mod 16 gp. image	LMFDB label of an ex. $E/\mathbb{Q}$