

# Regular realizations of $p$ -projective quotients and modular curve-like towers

Part I: Use of conjugacy classes

Part II. Is the RIGP really so hard?

Part III: The RIGP realm using virtually pro- $p$  groups

Part IV. Cusps on curve components ( $r = 4$ )

Part V: Compare modular curve cusps with MT cusps

Part VI. Where is the Main Conjecture with  $r = 4$ ?

---

Part VII. What happens in real MT levels!

Part VIII. Generalizing Serre's OIT and the  $g$ - $p'$  conjecture

App. A: Fried-Serre Formula for Spin-Lift Invariant

App. B: **sh**-incidence Matrix for  $(A_4, \mathbf{C}_{\pm 3^2})$

## The IGP versus the RIGP

The I(nverse)G(alois)P(roblem): Is finite group  $G$  the Galois group of an extension of every number field?

The R(egular)IGP: Is there one Galois extension  $L_G/\mathbb{Q}(z)$  with group  $G$  containing only  $\mathbb{Q}$  for constants? From Hilbert's irreducibility Theorem, RIGP  $\implies$  IGP. Further, beyond the solvable case, the RIGP has provided most all the successes through the *braid monodromy method*.

## Part I: Use of conjugacy classes

We say  $\mathbf{g} \stackrel{\text{def}}{=} (g_1, \dots, g_r) \in G^r$   
*generates with product-one* if

$$\langle g_1, \dots, g_r \rangle = G \text{ and } \prod g_1 \cdots g_r \stackrel{\text{def}}{=} \Pi(\mathbf{g}) = 1. \quad (1)$$

Also,  $\mathbf{g}$  defines a set  $\mathbf{C}$  of conjugacy classes in  $G$ .  
Given  $\mathbf{C}$ ,  $\mathbf{g} \in \mathbf{C}$  means  $\mathbf{g}$  defines  $\mathbf{C}$ . Such  $\mathbf{g}$  form the  
*Nielsen class*  $\text{Ni}(G, \mathbf{C})$  of  $(G, \mathbf{C})$ .

In  $\mathbf{C} = \{C_1, \dots, C_r\}$  some classes may appear  
several times: *multiplicity counts; order does not.*

## Apply Riemann's Existence Theorem

A regular realization  $L_G/\mathbb{Q}(z)$  has  $r \geq 2$  branch points  $\mathcal{Z} = \{z_1, \dots, z_r\}$  ( $z$  over which are less than  $[L_G : \mathbb{Q}(z)]$  places):  $z_i \mapsto$  conjugacy class  $\mathbf{C}_i$  of inertia generator from a clockwise small circle around  $z_i$ .

**RET:**  $G(L_G/\mathbb{Q}(z)) = G \implies$  some  $\mathbf{g} \in \mathbf{C}$  generates  $G$  with product-one.

Since the realization is over  $\mathbb{Q}$ ,  $\mathbf{C}$  is a rational union (its union is closed under putting all elements in it to powers prime to orders of elements in  $\mathbf{C}$ ).

An addition to a Fried-Völklein Thm. 1992:

**Theorem 1 (Branch-Generation Thm.).** *Assume  $G$  centerless and  $\mathbf{C}^*$  a distinct rational union of (nontrivial) classes in  $G$ . An **infinite** set  $I_{G,\mathbf{C}^*}$  indexes distinct absolutely irreducible  $\mathbb{Q}$  varieties*

$\mathcal{R}_{G,\mathbf{C}^*} \stackrel{\text{def}}{=} \mathcal{R}_{G,\mathbf{C}^*,\mathbb{Q}} = \{\mathcal{H}_i\}_{i \in I_{G,\mathbf{C}^*}}$  *satisfying these:*

- $i \in I_{G,\mathbf{C}^*} \mapsto {}_i\mathbf{C}$ , *cardinality  $r_i$  and support in  $\mathbf{C}^*$ .*
- *The RIGP holds for  $G$  with conjugacy classes  $\mathbf{C}$  supported in  $\mathbf{C}^* \Leftrightarrow$   
 $i \in I_{G,\mathbf{C}^*}$  with  $\mathbf{C} = {}_i\mathbf{C}$  and  $\mathcal{H}_i$  has a  $\mathbb{Q}$  point.*

## Using Nielsen classes

Realizations come from augmenting existence of  $\mathcal{R}_{G, \mathbf{C}^*}$  with info on  $\mathcal{H}_i$ ,  $i \in I_{G, \mathbf{C}^*}$ .

The reduced space  $\mathcal{H}_i^{\text{rd}}$ : Equivalence field extensions under change of variables  $z \mapsto \alpha(z)$ ,  $\alpha \in \text{PGL}_2(\mathbb{C})$ . Dimension of  $\mathcal{H}_i^{\text{rd}}$  is  $r_i - 3$ .

## Dihedral and Alternating cases

$G = D_{p^{k+1}}$  with  $p$  odd,  $\mathbf{C}^* = \{C_2\}$  (class of involution):

Then  $i \mapsto \mathbf{C}_{2^{r_i}}$  is one-one and onto  $r_i \geq 4$  even. Also,  $H_i^{\text{rd}}$  identifies with space of cyclic  $p^{k+1}$  covers of hyperelliptic jacobians of genus  $\frac{r_i-2}{2}$ .

(Fried-Serre)  $G = A_n$  with  $\mathbf{C}^* = \{C_3\}$ , class of 3-cycles:

Then  $i \mapsto \mathbf{C}_{3^{r_i}}$  with  $r_i \geq n$  is two-one. Denote indices mapping to  $r$  by  $i_r^\pm$ . Covers in  $\mathcal{H}_{i_r^\pm}$  are Galois closures of degree  $n$  covers  $\varphi : X \rightarrow \mathbb{P}_z^1$  with 3-cycles for local monodromy. Write divisor  $(d\varphi)$  of differential of  $\varphi$  as  $2D_\varphi$ . Then,  $\varphi \in \mathcal{H}_{i_r^+}$  (resp.  $\mathcal{H}_{i_r^-}$ ) if linear system of  $D_\varphi$  has even (resp. odd) dim.; even (resp. odd)  $\theta$  characteristic. For  $r_i = n - 1$ ,  $i \mapsto \mathbf{C}_{3^{r_i}}$  is one-one.

## Part II. Is the RIGP really so hard?

Dividing RIGP techniques into three cases shows how  $i \in I_{G, \mathbf{C}^*}$  on  ${}_i \mathbf{C}$  affects complexity of computation. Yet, it is diophantine reasons more than group theory complexity that makes the RIGP hard.

1. When  $r_i = 3$ ,  $\mathcal{H}_i^{\text{rd}}$  is a finite collection of  $(\mathbb{Q})$  points.
2. When  $r_i = 4$ ,  $\mathcal{H}_i^{\text{rd}}$  is naturally an upper half-plane quotient and a cover of the  $j$ -line, with meaningful cusp types.
3. No matter what is  $r_i$ ,  $\mathcal{H}_i$  is a cover of  $U_{r_i}$ , projective  $r_i$  space minus its discriminant locus; can compare this with the (Galois) Noether cover  $U^{r_i} \rightarrow U_{r_i}$  (with group  $S_{r_i}$ ).

## Using #1:

*Rigidity*, an effective sufficiency test for existence of  $i \in I$  with  $r_i = 3$ , requires only knowing the character table of  $G$  to conclude the RIGP for  $G$ .

**Problem:** Rarely does this hold. Even for Chevalley groups, the method achieved only special rank 1 groups over prime finite fields (Belyi) and some other special simple groups by Matzat and Thompson.

## Using #3:

For many families of simple groups **Thompson and Völklein** found  $\mathbf{C}^*$  and used specific  $i \in I_{G, \mathbf{C}^*}$  (**Thompson-tuples**). For these the  $\mathcal{H}_i \rightarrow U_{r_i}$  covers were *almost* subcovers of  $U^{r_i} \rightarrow U_{r_i}$ . This gave many examples of simple  $G$  satisfying RIGP.

**Problem:** This intricate work required much luck and extensive details about the simple group series to which it applied.

## Virtues of using #2:

- $\mathcal{H}_i^{\text{rd}}$  is a curve with **useful cusps** from the moduli problem to compactify it. Gives precise statements about these spaces.
- More groups (like **all simple groups and all their Frattini covers**) have conjugacy classes producing this case than holds for #1.
- **Combinatorial techniques** allow computing the genus of these spaces, and to *identify the part of the Nielsen class they come from*.

## Part III: The RIGP realm using virtually pro- $p$ groups

Use the *virtually pro- $p$  universal  $p$ -Frattini* cover  ${}_p\tilde{G}$  of  $G$ , for any prime  $p \mid |G|$  (to see how the RIGP generalizes classical results for modular curves).

Assume  $G$  is  *$p$ -perfect* (no  $G \rightarrow \mathbb{Z}/p \rightarrow 1$ ) and *centerless*. Then  ${}_p\tilde{G} = \lim_{\infty \leftarrow k} G_k$ , with

- $G_k$  also  *$p$ -perfect* and *centerless*; and
- $G_k \rightarrow G$  *versal* for all extensions  $\psi : H \rightarrow G$  with  $\ker(\psi)$  a  $p$ -group of exponent at most  $p^k$ .

## Add a restriction on Ramification

From Schur-Zassenhaus, if a conjugacy class is  $p'$ , then it has a unique lift to a  $p'$  class in  $G_k$ . So, if  $\mathbf{C}$  consists of  $p'$  classes, denote those lifted classes to  $G_k$  by the same notation. Here is a *restrict ramification condition* depending on  $r_0 \geq 3$ :

**Ram $_{r_0}$ :** For  $k \geq 0$ , consider just covers in  $\text{Ni}(G_k, \mathbf{C}_k)$  with the cardinality of  $\mathbf{C}_k$  at most  $r_0$ .

**Question 2 (RIGP( $\mathbf{G}, \mathbf{p}, r_0$ ) Question).** Is there an  $r_0$  so all  $G_k$  s satisfy the RIGP from covers in  $\text{Ram}_{r_0}$ ?

## How the Main Conjecture Arises

**Theorem 3 (Fried-Kopeliovic, 1997).** *If the conclusion of Quest. 2 is affirmative (for  $(G, p, r_0)$ ), then there are  $p'$  conjugacy classes  $\mathbf{C}$  (no more than  $r_0$ ) in  $G$ , and a projective system  $\{\mathcal{H}'_k \in \mathcal{R}_{G_k, \mathbf{C}}\}_{k=0}^{\infty}$  each having a  $\mathbb{Q}$  point.*

We call  $\{\mathcal{H}'_k\}_{k=0}^{\infty}$  a *Modular Tower component branch* (over  $\mathbb{Q}$ ).

**Conjecture 4 (Main Conjecture).** Given any MT component branch, and any number field  $K$ , for  $k \gg 0$ ,  $\mathcal{H}'_k^{\text{rd}}(K) = \emptyset$ .

## Part IV. Cusps on curve components ( $r = 4$ )

*Inner Nielsen classes*  $\text{Ni}(G_k, \mathbf{C})^{\text{in}}$  :

$$\{\mathbf{g} = (g_1, \dots, g_4) \in \mathbf{C} \pmod{G_k}\}$$

- $\text{Cond}^1$  – Generation:  $\langle g_1, g_2, g_3, g_4 \rangle = G_0$ ;
- $\text{Cond}^2$  – Product-one:  $g_1 g_2 g_3 g_4 = 1$ .

*Twist action* of  $H_4 = \langle q_1, q_2, q_3 \rangle$  generators on  $\mathbf{g} \in \text{Ni}(G_k, \mathbf{C})^{\text{abs}}$ . Ex.:  $q_2 : \mathbf{g} \mapsto (g_1, g_2 g_3 g_2^{-1}, g_2, g_4)$ .

*Cusps*:  $\text{Cu}_4 \stackrel{\text{def}}{=} \langle q_1 q_3^{-1}, (q_1 q_2 q_3)^2, q_2 \rangle$  orbits.

Let  $\mathcal{Q}'' = \langle q_1 q_3^{-1}, (q_1 q_2 q_3)^2 \rangle$ .

Why  $\bar{M}_4 \stackrel{\text{def}}{=} H_4/Q''$  is  $\text{PSL}_2(\mathbb{Z})$ !

- $q_2 \mapsto \gamma_\infty$ ;
- $q_1q_2q_3$  (shift)  $\mapsto \gamma_1$  (order 2).
- $q_1q_2 \mapsto \gamma_0$  has order 3, from braid relation  $q_1q_2q_1 = q_2q_1q_2 \pmod{\text{Cu}_4}$  and Hurwitz relation  $1 = q_1q_2q_3q_3q_2q_1$ :

$$= q_1q_2q_1q_1q_2q_1 = q_1q_2q_1q_2q_1q_2 = (q_1q_2)^3.$$

## Example of computing component genera

From a component branch, what to compute:

- Nature of cusps and their widths (length of  $Cu_4$  mod  $Q''$  orbits).
- How they fall in  $\bar{M}_4$  orbits and of what genera (Riemann-Hurwitz).

## Part V: Compare modular curve cusps with MT cusps [Fr05c, §3.2]

When  $r = 4$ , MT levels ( $k \geq 0$ ) are  $j$ -line covers.  
Rarely modular curves.

With  $r = 4$ ,  $\mathbf{g} \in \text{Ni}(G, \mathbf{C})^{\text{in}}$ , denote:

$$\langle g_2, g_3 \rangle = H_{2,3}(\mathbf{g}) \text{ and } \langle g_1, g_4 \rangle = H_{1,4}(\mathbf{g}).$$

$(\mathbf{g})\text{Cu}_4$  is a  $g$ - $p'$  cusp:  $H_{2,3}(\mathbf{g})$  and  $H_{1,4}(\mathbf{g})$  are  $p'$  groups.  
Ex: H(arbater)-M(umford) cusps have  $g_2 = g_1^{-1}$ .

$p$  cusps: Those with  $p \mid \text{ord}(g_2 g_3)$ .

$o(nly)-p'$ : Cusps neither  $p$  nor  $g-p'$ .

Modular curve  $X_1(p^{k+1})$  has H-M cusps, many  $p$  cusps of different cusps widths, all growing in width by  $p$  as  $k$  increases, but no  $o-p'$  cusps.

## Apply R-H to MT components

$\text{Ni}'$  is a  $\bar{M}_4$  orbit on a reduced Nielsen class  $\text{Ni}(G, \mathbf{C})^{\text{abs}} / \mathcal{Q}''$  (or  $\text{Ni}(G, \mathbf{C})^{\text{in}} / \mathcal{Q}''$ ). Denote action of  $(\gamma_0, \gamma_1, \gamma_\infty)$  (p. 14) on  $\text{Ni}'$  by  $(\gamma'_0, \gamma'_1, \gamma'_\infty)$ : Branch cycles for a cover  $\bar{\mathcal{H}}' \rightarrow \mathbb{P}_j^1$ ,

R-H gives genus,  $g_{\bar{\mathcal{H}}'}$ :

$$2(\deg(\bar{\mathcal{H}}' / \mathbb{P}_j^1) + g' - 1) = \text{ind}(\gamma'_0) + \text{ind}(\gamma'_1) + \text{ind}(\gamma'_\infty).$$

To compute genera of components in a MT  
answer these questions

- What are the components  $\mathcal{H}'_k$  of  $\mathcal{H}_k$  ( $\bar{M}_4$  orbits  $\text{Ni}'_k$  on  $\text{Ni}_k^{\text{rd}}$ )?
- What are the cusp widths (ramification orders over  $\infty$ ; orbit lengths of  $\gamma'_\infty$  on  $\text{Ni}'_k$ )?
- What points ramify in each component over elliptic points  $j = 0$  or  $1$ ; length 3 (resp. 2) orbits of  $\gamma'_0$  (resp.  $\gamma'_1$ ) on  $\text{Ni}'_k$ ?

## Part VI. Where is the Main Conjecture with $r = 4$ ?

Let  $B' = \{\mathcal{H}'_k\}_{k=0}^{\infty}$  be an infinite component branch. Possible Main Conj. contradictions:

1.  $g_{\bar{\mathcal{H}}'_k} = 0$  for all  $0 \leq k < \infty$   
( $B'$  has genus 0;  $g_{B'}$  consists of 0's); or
2. For  $k$  large,  $g_{\bar{\mathcal{H}}'_k} = 1$   
( $B'$  has genus 1; almost all of  $g_{B'}$  is 1's).

## Reductions from Fried-Luminy 2006:

**Use Frattini Principle 1:** An element  $g \in G_k$  of order divisible by  $p^u$ ,  $u > 0$  has above it in  $G_{k+1}$  only elements of order divisible by  $p^{u+1}$ .

**Conclusions from Reductions:** Each level  $k + 1$  cusp over a  $p$  cusp at level  $k$  is ramified (of order  $p$ ).

**Example use:** From R-H, for  $k \gg 0$ , (2) implies  $\bar{\mathcal{H}}'_{k+1} \rightarrow \bar{\mathcal{H}}'_k$  doesn't ramify. So, FP1 says:  
For no  $k$  does  $\bar{\mathcal{H}}'_k$  have a  $p$  cusp.

## Possible exceptional cases! [Fr05c, §5]

Assume  $\mathbf{p}'_k \in \bar{\mathcal{H}}'_k$  is a  $p$  cusp (some  $k$ ). Denote:  
 $\deg(\bar{\mathcal{H}}'_{k+1}/\bar{\mathcal{H}}'_k) = \nu_k$  and  $|\mathbf{p}'_{k+1} \in \bar{\mathcal{H}}'_{k+1} \text{ over } \mathbf{p}'_k| = u_k$ .

**Theorem 5.** *The Main Conj. is true unless for  $k \gg 0$ ,  $\nu_k = p$ ,  $u_k = 1$  and  $\bar{\mathcal{H}}'_{k+1}/\bar{\mathcal{H}}'_k$  is equivalent (as a cover over  $K$ ) to either:*

1.  $(\mathbf{P}^{\text{oly}}\mathbf{M})$  a degree  $p$  polynomial map; or
2.  $(\mathbf{R}^{\text{edi}}\mathbf{M})$  a degree  $p$  rational function ramified precisely over two  $K$  conjugate points.

**Corollary 6.** *If neither  $(P^{\text{oly}}M)$  nor  $(R^{\text{edi}}M)$  hold for the component branch  $B'$ , then high levels of  $B'$  have no  $K$  points.*

*For  $B'$  with full elliptic ramification (includes when  $B'$  has fine reduced moduli) for  $k \gg 0$ , the Main Conj. holds unless  $(R^{\text{edi}}M)$  holds.*

## Part VII. What happens in real MT levels!

- Main point to finish Main Conjecture for  $r = 4$ :  
Find  $p$  cusps at high levels.
- If the  $\limsup$  of  $\deg(\bar{\mathcal{H}}'_{k+1}/\bar{\mathcal{H}}'_k)$  is *not*  $p$ , one  $p$  cusp guarantees the  $p$  cusp count (at level  $k$ ) is unbounded as  $k \mapsto \infty$ .

The case  $(A_5, \mathbf{C}_{3^4}, p = 2)$  (four 3-cycles):

- Level 0:  $\mathcal{H}(A_5, \mathbf{C}_{3^4})^{\text{in,rd}}$  has one component, and no  $p$  ( $=2$ ) cusps.
- Apply lift invariant for  $\text{Spin}_5 \rightarrow A_5$  (App<sub>2</sub>): Shows all level 1 comps. have  $p$  ( $= 2$ ) cusps [BFr02, Cor. 8.3] (Fr-Se formula).
- Level 1 [BFr02, Prop. 9.14]: Two components ( $\bar{M}_4$  orbits,  $\text{Ni}_{1,\pm}$ ), distinguished by embedding  $G_1(A_5) \leq A_{40}$  giving  $s_{\text{Spin}_{40}}(\mathbf{g}) = \pm 1$  depending on  $\mathbf{g} \in \text{Ni}_{1,\pm}$ .

On compactification  $\bar{\mathcal{H}}_+$  of  $\mathcal{H}_+(G_1(A_5), \mathbf{C}_{34})^{\text{in,rd}}$ :

- Contains all H-M cusps (FP2  $\implies$   ${}_2\tilde{G}$  is a limit group for a comp. branch over it).
- Has genus 12 and degree 16 over the unique component of  $\bar{\mathcal{H}}(A_5, \mathbf{C}_{34})^{\text{in,rd}}$ .
- Has all the real (and so all the  $\mathbb{Q}$ ) points at level 1 [BFr02, §8.6]. On its compactification  $\bar{\mathcal{H}}_+$ ,  $\bar{\mathcal{H}}_+(\mathbb{R})$  is connected. All except the shift of the H-M cusps are 2 cusps.

On compactification  $\bar{\mathcal{H}}_-$  of  $\mathcal{H}_-(G_1(A_5), \mathbf{C}_{34})^{\text{in,rd}}$ :

- Has genus 9, but no real points.
- Because of the lifting invariant, nothing above it at level 2:  ${}_2\tilde{G}(A_5)$  (the whole 2-Frattini cover of  $A_5$ ) is not a limit group.

## Higher ( $A_5, \mathbf{C}_{34}, p = 2$ ) levels: modular curve-like cusp properties

Let  $\{\mathcal{H}'_k\}_{k=0}^{\infty}$  be an H-M comp. branch (FP2).

**Proposition 7.** *On all  $\bar{\mathcal{H}}'_k$ ,  $g$ - $p'$  cusps are H-M. It has no  $o$ - $p'$  cusps [Fr05c, Prop. 3.12]. Number of  $p$  cusps on  $\mathcal{H}'_k \mapsto \infty$ .*

**Uses a General Idea:** Let  $B = \{\mathbf{p}_k\}_{k=0}^{\infty}$  be a  $g$ - $p'$  cusp branch. Assume for each  $k \geq k_0$ ,  $\mathbf{p}_k$  braids to a  $p$  cusp  $\mathbf{p}'_k$  with ramification index exactly divisible by  $p$ . Then, FP1 allows, with  $k = k_0 + u$ , inductively braiding  $\mathbf{p}_k$  to a sequence of cusps  $\mathbf{p}'_k(1), \dots, \mathbf{p}'_k(u)$  with  $\mathbf{p}'_k(t)$  having ramification index exactly divisible by  $p^t$ ,  $u = 1, \dots, t$ .

From their ramification indices over  $j = \infty$ , these give  $u$  different  $p$  cusps at level  $k_0 + u$ .

For  $\text{Ni}(G_k(A_5), \mathbf{C}_{34})$  take  $k_0 = 1$ :  $\mathbf{p}'_k$  is produced as the *near* H-M rep. associated to  $\mathbf{p}_k$  [BFr02, Prop. 6.8].

$A_n$  examples of two braid orbits from lifting inv.

**Example 8 ( $A_n$  and 3-cycles).** For each pair  $(n, r)$  with  $r \geq n$ , there are exactly two braid orbits on  $\text{Ni}(A_n, \mathbf{C}_{3^r})$ . One contains a  $g$ -2' representative and the other is obstructed at level 0. Braid orbit reps for  $n = r = 4$ :

$$\begin{aligned} \mathbf{g}_{4,+} &= ((1\ 3\ 4), (1\ 4\ 3), (1\ 2\ 3), (1\ 3\ 2)), \\ \mathbf{g}_{4,-} &= ((1\ 2\ 3), (1\ 3\ 4), (1\ 2\ 4), (1\ 2\ 4)). \end{aligned}$$

## Nonbraidable, isomorphic $M_{\tilde{g}}$

Suppose two extensions  $M_{g_i} \rightarrow G$ , arise from  $g_i \in \text{Ni}(G, \mathbf{C})$ ,  $i = 1, 2$ . Assume they are isomorphic. Still might not be braidable.

The Nielsen class  $\text{Ni}(G_1(A_4), \mathbf{C}_{\pm 3^2})$  has six braid orbits. Two extensions correspond to the two H-M components called  $\mathcal{H}_1^{+, \beta}$ ,  $\mathcal{H}_1^{+, \beta^{-1}}$ . An *outer* automorphism of  $G_1(A_4)$  takes  $g_1$  to  $g_2$ , giving elements in different braid orbits. These are H-M components, so *FP2* gives isomorphic extensions  $M_{g_i} \rightarrow {}_p\tilde{G}$ ,  $i = 1, 2$  in distinct braid orbits.

## Part VIII. Generalizing Serre's OIT and the $g$ - $p'$ conjecture

Stay with  $r = 4$  to simplify notation.

1. Why you expect a  $\text{PSC}_K$  for some number field  $K$  only if you have a  $g$ - $p'$  cusp.
2. Generalize in  $(G, \mathbf{C}, p)$  to allow many primes. Use **higher rank MTs**: a group  $H$  ( $\mathbf{C}$  are classes in  $H$ ) acting on either a free group or a lattice  $L$ , and for all allowable  $p$  look at  $(L/pL \times^s H, \mathbf{C}, p)$ .

3. Decide when you can inductively find infinitely many points corresponding to “complex multiplication, ” (i.e. prediction of full Galois image for the fiber over  $j_0 \in U_\infty$ ).
4. Where (when?) are the Hecke operators?

Topics (2) and (3) are in [Fr05c, §6], with extensive examples comparing modular curve to the general case. My NSF proposal outline how topics (1) and (4) work. These will be in my RIMS talk in October.

(Lots of evidence for)  $g$ - $p'$  Conjecture: Each  $\text{PSC}_K$  is defined by a cusp sequence called  $g$ - $p'$ . Their **shifts** often resemble sequences of *width*  $p^{k+1}$  *cusps* on  $\{X_0(p^{k+1})\}_{k=0}^{\infty}$ ; moduli interpretation generalizing Tate elliptic curve.

## App. A: Fried-Serre Formula for Spin-Lift Invariant

For  $g \in A_n$  of odd order, let  $w(g)$  be the sum of  $(l^2 - 1)/8 \pmod{2}$  over all disjoint cycle lengths  $l$  in  $g$  ( $l \not\equiv \pm 1 \pmod{8}$  contribute).

**Theorem 9 (Fried-Serre).** *If  $\varphi : X \rightarrow \mathbb{P}^1$  is in Nielsen class  $\text{Ni}(A_n, \mathbf{C}_{3n-1})^{\text{abs}}$ , then  $\deg(\varphi) = n$ ,  $X$  has genus 0, and  $s(\varphi) = (-1)^{n-1}$ .*

*Generally, for any genus 0 Nielsen class of odd order elements, and representing  $\mathbf{g} = (g_1, \dots, g_r)$ ,  $s(\mathbf{g})$  is constant, equal to  $(-1)^{\sum_{i=1}^r w(g_i)}$ .*

**Meaning:** Let  $\hat{X} \rightarrow \mathbb{P}_z^1$  be Galois closure of  $\varphi$ .  
 Then,  $s(\varphi) = 1 \implies \exists \mu : Y \rightarrow \hat{X}$  unramified, so  
 $\varphi \circ \mu$  is Galois with group  $G \times_{A_n} \text{Spin}_n$ .

**Exercise:** Genus 0 assumption doesn't apply to

$$\mathbf{g}_1 = ((1\ 2\ 3)^{(3)}, (1\ 4\ 5)^{(3)}), \text{ or to}$$

$$\mathbf{g}_2 = ((1\ 2\ 3)^{(3)}, (1\ 3\ 4), (1\ 4\ 5), (1\ 5\ 3)),$$

but you can easily compute  $s(\mathbf{g}_i)$ ,  $i = 1, 2$ .

## App. B: **sh**-incidence Matrix for $(A_4, \mathbf{C}_{\pm 3^2})$

**Goal:** There are two components  $\bar{\mathcal{H}}_{\pm}$ . Want their branch cycle description  $(\gamma_0^{\pm}, \gamma_1^{\pm}, \gamma_{\infty}^{\pm})$  as  $j$ -line covers.

Let  $O$  be all the reduced Nielsen class reps. in a cusp orbit. Then  $(O)\mathbf{sh}$  is collection of shifts of all elements in  $O$ . If  $O_1, \dots, O_t$  is a complete list of cusp sets, then the  $(i, j)$  entry of the **sh**-incidence matrix is  $|O_i \cap (O_j)\mathbf{sh}|$ .

## Listing cusp sets and blocks for $(A_4, \mathbf{C}_{\pm 3^2})$

There are six easily computed cusp sets on  $(A_4, \mathbf{C}_{\pm 3^2})^{\text{in,rd}}$  listed in [Fr05c, §6.3.1]:

- $O_{1,1}$ : cusp orbit of an H-M rep.  $g_{1,1}$  with 3rd and 4th entries  $((1\ 3\ 4), (4\ 3\ 1))$ ;
- $O_{3,1}$ : cusp orbit of another H-M rep.,  $(g_{1,1})q_3$ ;
- $O_{1,4}$ : cusp orbit of

$$g_{1,4} = ((1\ 2\ 3), (1\ 2\ 4), (1\ 2\ 3), (1\ 2\ 4)),$$

- $O_{1,5}$ : cusp orbit of  $(g_{1,4})q_3$ , etc.

As cusp orbits and **sh** of them are easy to compute, easily get the  $6 \times 6$  **sh**-incidence matrix blocks.

Orbit	$O_{1,1}$	$O_{1,3}$	$O_{3,1}$
$O_{1,1}$	1	1	2
$O_{1,3}$	1	0	1
$O_{3,1}$	2	1	0
Orbit	$O_{1,4}$	$O_{3,4}$	$O_{3,5}$
$O_{1,4}$	2	1	1
$O_{3,4}$	1	0	0
$O_{3,5}$	1	0	0

**Lemma 10.** *In general, **sh**-incidence matrix is same as matrix from replacing  $\mathbf{sh} = \gamma_1$  by  $\gamma_0$ . Only possible elements fixed by either lie in  $\gamma_\infty$  orbits  $O$  with  $|O \cap (O)\mathbf{sh} \neq 0|$ .*

*On  $\text{Ni}_0^+$  (resp.  $\text{Ni}_0^-$ ),  $\gamma_1$  fixes 1 (resp. no) element(s), while  $\gamma_0$  fixes none.*