Séminaires & Congrès
13, 2006, p. 165–233

THE MAIN CONJECTURE OF MODULAR TOWERS AND ITS HIGHER RANK GENERALIZATION

by

Michael D. Fried

Abstract. — The genus of projective curves discretely separates decidedly different two variable algebraic relations. So, we can focus on the connected moduli $\mathcal{M}_g$ of genus g curves. Yet, modern applications require a data variable (function) on such curves. The resulting spaces are versions, depending on our need from this data variable, of *Hurwitz spaces*. A *Nielsen class* (§1) is a set defined by $r \geq 3$ conjugacy classes $\mathbf{C}$ in the data variable monodromy G. It gives a striking genus analog.

Using Frattini covers of G, every Nielsen class produces a projective system of related Nielsen classes for any prime p dividing $|G|$. A nonempty (infinite) projective system of braid orbits in these Nielsen classes is an infinite $(G, \mathbf{C})$ *component (tree) branch*. These correspond to projective systems of irreducible (dim $r-3$) components from $\{\mathcal{H}(G_{p,k}(G), \mathbf{C})\}_{k=0}^{\infty}$, the $(G, \mathbf{C}, p)$ Modular Tower (**MT**). The classical modular curve towers $\{Y_1(p^{k+1})\}_{k=0}^{\infty}$ (simplest case: G is dihedral, $r = 4$, $\mathbf{C}$ are involution classes) are an avatar.

The (weak) Main Conjecture 1.2 says, if G is *p-perfect*, there are no rational points at high levels of a component branch. When $r = 4$, **MT**s (minus their cusps) are systems of upper half plane quotients covering the j-line. Our topics.

- §3 and §4: Identifying component branches on a **MT** from *g-p′, p and Weigel cusp branches* using the **MT** generalization of *spin structures*.
- §5: Listing cusp branch properties that imply the (weak) Main Conjecture and extracting the small list of towers that could possibly fail the conjecture.
- §6: Formulating a (strong) Main Conjecture for higher rank **MT**s (with examples): almost all primes produce a modular curve-like system.

2000 *Mathematics Subject Classification.* — Primary 11F32, 11G18, 11R58; Secondary 20B05, 20C25, 20D25, 20E18, 20F34.
Key words and phrases. — Moduli spaces of covers, j-line covers, braid group and Hurwitz monodromy group, Frattini and Spin covers, Serre's lifting invariant.

Support from NSF #DMS-99305590, #DMS-0202259 and #DMS-0455266. This contains many advances on my March 12, 2004, Luminy talk (subsumed by overheads in [**Fri05a**]). One of those centers on Weigel cusps and whether they exist. This interchange with Thomas Weigel occurred in Jerusalem and Milan during the long trip including Luminy. Prop. 3.12 is due to Darren Semmen, a constant modular representation consultant. Conversations with Anna Cadoret, Pierre Debes and Kinya Kimura influenced me to be more complete than otherwise I would have been.

***Résumé* (La conjecture principale sur les tours modulaires et sa généralisation en rang supérieur)**

Le genre des courbes projectives est un invariant discret qui permet une première classification des relations algébriques en deux variables. On peut ainsi se concentrer sur les espaces de modules connexes $\mathcal{M}_g$ des courbes de genre g donné. Pourtant de nombreux problèmes nécessitent la donnée supplémentaire d'une fonction sur la courbe. Les espaces de modules correspondants sont les espaces de Hurwitz, dont il existe plusieurs variantes, répondant à des besoins divers. Une classe de Nielsen (§1) est un ensemble, constitué à partir d'un groupe G et d'un ensemble $\mathbf{C}$ de $r \geq 3$ classes de conjugaison de G, qui décrit la monodromie de la fonction. C'est un analogue frappant du genre.

En utilisant les revêtements de Frattini de G, chaque classe de Nielsen fournit un système projectif de classes de Nielsen dérivées, pour tout premier p divisant $|G|$. Un système projectif non vide (infini) d'orbites d'actions de tresses dans ces classes de Nielsen est une branche infinie d'un arbre de composantes. Cela correspond à un système projectif de composantes irréductibles (de dimension $r-3$) de $\{\mathcal{H}(G_{p,k}(G), \mathbf{C})\}_{k=0}^{\infty}$, la tour modulaire. La tour classique des courbes modulaires $\{Y_1(p^{k+1})\}_{k=0}^{\infty}$ (le cas le plus simple où G est le groupe diédral D_{2p}, $r=4$ et $\mathbf{C}$ la classe d'involution répétée 4 fois) en est un avatar.

La conjecture principale (faible) dit que, si G est p-parfait, il n'y a pas de points rationnels au delà d'un niveau suffisamment élevé d'une branche de composantes. Quand $r=4$, les tours modulaires (privées des pointes) sont des systèmes de quotients du demi-plan supérieur au-dessus de la droite projective de paramètre j. Nos thèmes.

- §3 et §4 : Identification des branches de composantes sur une tour modulaire à partir des branches de pointes $g-p'$, p et Weigel, grâce à la généralisation des structures de spin.
- §5 : Énoncé d'un ensemble de propriétés des branches de pointes impliquant la conjecture principale (faible) et réduction à un nombre limité de cas de tours pouvant encore éventuellement la mettre en défaut.
- §6 : Formulation d'une conjecture principale forte pour des tours modulaires de rang supérieur (avec des exemples) : presque tous les premiers conduisent à un système semblable à celui des courbes modulaires.

Contents

Luminy in March 2004 gave me a chance to show the growing maturity of Modular Towers (**MT**s). Documenting its advances, however, uses two other sources: Papers from this conference; and a small selection from the author's work. §C.1 lists the former. While the first two papers in that list have their own agendas, they show the influence of **MT**s. The last two papers aim, respectively, at the arithmetic and group theory of **MT**s. This paper concentrates on (cusp) geometry. As [**Fri07**] is not yet complete, I've listed typos corrected from the print version of [**BF02**] — our basic reference — in the on-line version (§C.2). From it came the serious examples (see partial list of §6.2.3) that graphically demonstrate the theory.

A glance at the Table of Contents shows §4 is the longest and most theoretical in the paper. It will figure in planned later papers. We have done our best in §6 to get serious examples to illustrate everything in §4. (Constraints include assuring we had in print enough on the examples to have them work as we wanted.) So, we suggest referring to §4 after finding motivation from other sections.

Many items in this paper would seem to complicate looking at levels of a **MT**: types of cusps, Schur multipliers of varying groups, component orbits. It behooves us to have an organizing tool to focus, label and display crucial and difficult computations. Further, we find that arithmetic geometers with little group theory background just don't know where to start. What surely helps handle some of these problems is the **sh**-incidence matrix. I suggested to Kay Maagard that the braid package (for computing Nielsen class orbits) would gain greatly if it had a sub-routine for this. He said he would soon put such in [**MSV03**].

We use the **sh**-incidence Matrix on $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$ in §6.4.2 to show what we mean. More elaborate examples for level 1 of this **MT** and also for $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{\mathrm{in,rd}}$ are in [**BF02**, Chaps. 8 and 9]. All these are done without [**Sch95**] or other computer calculation, and they figure in many places in this paper as nontrivial examples of the mathematical arguments that describe the structure of **MT** levels. Still, [**BF02**, §9.2.1 and 9.2.2] list what [**Sch95**] produced for all branch cycles (see §5.2.2 and §6.2.3) for both (j-line covering) components at level 1 in the $(A_5, \mathbf{C}_{3^4}, p = 2)$ **MT**.

1. Questions and topics

In this paper the branch point parameter $r \geq 3$ is usually 4 (or 3). Results (based on §3 and §4) on **MT**s with r arbitrary are in a companion paper [**Fri06a**] that contains proofs of several results from the author's long-ago preprints. For example: It describes all components of Hurwitz spaces attached to $(A_n, \mathbf{C}_{3^r})$, alternating groups with 3-cycle branch cycles running over all $n \geq 3$, $r \geq n-1$.

1.1. The case for investigating MTs. — A group G and r conjugacy classes $\mathbf{C} = \mathrm{C}_1, \dots, \mathrm{C}_r$ from G define a *Nielsen class* (§2.4.1). The Hurwitz monodromy group H_r acts on (we say *braids*) elements in representing Nielsen classes. Components of **MT** levels correspond to H_r orbits. Other geometry, especially related to cusps, corresponds to statements about subgroups of H_r on Nielsen classes.

Sometimes we use the notation $r_{\mathbf{C}}$ for the number r of conjugacy classes. Mostly, however, we concentrate on **MT**s defined by reduced (inner) Nielsen classes $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in,rd}}$ where $r_{\mathbf{C}} = 4$ (sometimes one conjugacy class, repeated four times). Then, the sequence of reduced inner Hurwitz spaces $(\{\mathcal{H}(G_{p,k}(G), \mathbf{C})^{\mathrm{in,rd}}\}_{k=0}^{\infty}$ below) defining their levels are curves. Here H_4, acting on a corresponding projective sequence of Nielsen classes, factors through a mapping class group we denote as $\bar{M}_4$. It is naturally isomorphic to $\mathrm{PSL}_2(\mathbb{Z})$.

In this case, a projective sequence of finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ acting on the upper half-plane, indexed by powers of a prime p, do correspond to these levels. Yet, this sequence appears indirectly in MTs, unlike the classical approach to the special case of modular curve sequences. The closure $\bar{\mathcal{H}}(G_{p,k}(G), \mathbf{C})^{\mathrm{in,rd}}$ is a ramified cover of the j-line (§2.3) that includes *cusps* (lying over $j = \infty$). Each cusp identifies with a *Nielsen class cusp set* (as in (2.5a)).

Like modular curves towers, the usual cusp type is a p cusp. Also, like modular curve towers, special cusp sets correspond to actual cusps with special geometric properties. The technical theme of this paper: **MT**s with *g-p' cusps* (§3.2.1) have a special kinship to modular curves (a subcase). That is because g-p' cusps potentially generalize a classical meaning for those modular curve cusps akin to representing degenerating Tate elliptic curves. This relates to the topic of *tangential base points* (Princ. 4.10 and §6.2). The other kind of cusp type called o-p' has no modular curve analog. We give many examples of these occurring on **MT**s where $p = 2$ and G_0 is an alternating group.

Direct interpretation of cusps and other geometric properties of **MT** levels compensates for how they appear indirectly as upper half-plane quotients. This allows defining **MT**s for $r > 4$. These have many applications, and an indirect relation with Siegel upper half-spaces, though no direct analog with modular curves.

1.1.1. Why investigate **MT***s?*— We express **MT**s as a response to these topics.

- T_1. They answer to commonly arising questions:
  - T_1.a. Why has it taken so long to solve the Inverse Galois Problem?
  - T_1.b. How does the Inverse Galois Problem relate to other deep or important problems?
- T_2. Progress on **MT**s generates new applications:
  - T_2.a. Proving the Main Conjecture shows **MT**s have some properties analogous to those for modular curves.
  - T_2.b. Specific **MT** levels have many recognizable applications.

Here is the answer to T_1.a. in a nutshell. **MT**s shows a significant part of the Inverse Galois Problem includes precise generalizations of many renown statements from modular curves. Like those statements, **MT** results say you can't find very many of certain specific structures over $\mathbb{Q}$.

For example, §6.1.2 cites [**Cad05b**] to say the weak (but not the strong) Main Conjecture of **MT**s follows from the Strong Torsion Conjecture (STC) on abelian varieties. Still, there is more to say: Progress on our Main Conjecture implies specific insight and results on the STC (subtle distinctions on the type of torsion points in question), and relations of it to the Inverse Galois Problem.

1.1.2. Frattini extensions of a finite group G lie behind **MT***s.* — Use the notation $\mathbb{Z}/n$ for congruences $\bmod n$ and $\mathbb{Z}_p$ for the p-adic integers. Denote the profinite completion of $\mathbb{Z}$ by $\tilde{\mathbb{Z}}$ and its automorphisms (invertible profinite integers) by $\tilde{\mathbb{Z}}^*$.

Suppose p is a prime dividing $|G|$. Group theorists interpret p' as an *adjective* applying to sets related to G: A set is p' if p does *not* divide orders of its elements.