M 392C: Open Problems in Topology Presentation - Congruence Subgroup Conjecture

Aaron Benda

February 2026

1 The Motivating Analogy

Recall the definition of the mapping class group $\mathrm{Mod}(S)$ (isotopy classes of self-diffeomorphisms of S, "extended" vs "pure") and the complex of curves (simplicial complex whose vertices are nontrivial simple closed curves with simplices joining mutually disjoint ones).

A lattice in a Lie group is a discrete subgroup of finite covolume under Haar measure. An arithmetic group is a special kind of lattice; for our purposes, just think of $\mathbf{SL}_n(\mathbb{Z}) \leqslant \mathbf{SL}_n(\mathbb{R})$.

Ivanov developed an analogy between mapping class groups and arithmetic groups, which we summarize in the table below.

Theme	Arithmetic Groups	Mapping Class Groups
Geometric Action	Symmetric spaces	Teichmüller space
Combinatorial Action	Tits buildings	Complex of curves
Automorphism Rigidity	Mostow rigidity	Ivanov's theorem
Finite Quotients	Mod an ideal	Finite covers of S

Arithmetic groups act on their symmetric spaces by isometries; any isometry of Teichmüller space (with the Teichmüller metric) comes from the action of the mapping class group. Similarly, arithmetic groups are the automorphism groups of Tits buildings, just as the mapping class group is the automorphism group for the complex of curves (a theorem which Ivanov proved). According to Ivanov, these combinatorial objects play similar roles in the theories of symmetric spaces of noncompact type and Teichmüller theory, respectively. Ivanov also proves that there is a certain subgroup rigidity statement for $\mathrm{Mod}(S)$, closely resembling Mostow rigidity.

Theorem 1.1: Mostow rigidity '68

Let $n \geq 3$. If $\Lambda, \Gamma \leqslant \mathbf{PO}(n,1) = \mathrm{Isom}^+(\mathbb{H}^n)$ are lattices and $\Lambda \cong \Gamma$, then in fact $\exists g \in \mathbf{PO}(n,1)$ so that $g\Lambda g^{-1} = \Gamma$.

In other words, if N, M are complete, finite volume hyperbolic manifolds of dimension ≥ 3 with $\phi : \pi_1(N) \to \pi_1(M)$ an isomorphism; then $\exists!$ isometry $f : N \to M$ so that $\phi \equiv f_*$.

Compare Ivanov's theorem below.

Theorem 1.2: Ivanov '89

Suppose S has genus at least 2 and is not $S^0_{2,0}$. If $\Lambda, \Gamma \leqslant \mathrm{Mod}(S)$ both of finite index, then any isomorphism $\Lambda \to \Gamma$ is obtained by conjugation in $\mathrm{Mod}(S)$. Consequence: $|\mathrm{Out}(\Gamma)| < \infty$.

2 Congruence Subgroups

In arithmetic groups, there is a natural quotient structure, leading to the following definition.

Definition 2.1: Congruence Subgroups in $\mathbf{SL}_n(\mathbb{Z})$

Let $I \leqslant \mathbb{Z}$ be any ideal (i.e. $I = N\mathbb{Z}$), and there is a natural homomorphism $\phi : \mathbf{SL}_n(\mathbb{Z}) \to \mathbf{SL}_n(\mathbb{Z}/I)$. The kernel of this homomorphism $\ker(\phi) \leqslant \mathbf{SL}_n(\mathbb{Z})$ is called a *principal congruence subgroup*. Any subgroup of $\mathbf{SL}_n(\mathbb{Z})$ containing a principal congruence subgroup is called a *congruence subgroup*.

Let G be a group. Recall that the *outer automorphism group* of G is the group $\mathrm{Out(G)} = \mathrm{Aut}(G)/\mathrm{Inn}(G)$, where $\mathrm{Inn}(G)$ is the collection of automorphisms of G by conjugation.

One may view the mapping class group of a closed surface as an outer automorphism group.

Theorem 2.2: Dehn-Nielsen-Baer

Suppose S is a closed surface. The extended mapping class group $\mathrm{Mod}(S)$ is isomorphic to the group $\mathrm{Out}(\pi_1(S))$.

For automorphism groups, there is also a natural notion of congruence subgroup.

Definition 2.3: Congruence Subgroups of Automorphism Groups

Suppose $H \leqslant G$ is a *characteristic subgroup*, meaning that H is invariant under all automorphisms of G. Then there is a natural homomorphism $\psi_H : \mathrm{Out}(G) \to \mathrm{Out}(G/H)$ via the action on left cosets. When H is of finite index in G, we must have that $\ker(\psi_H) \leqslant \mathrm{Out}(G)$ is of finite index as well.

Subgroups of the outer automorphism group arising as $\ker(\psi_H)$ from some characteristic $H \leqslant G$ are called *principal congruence subgroups*. Any subgroup of $\mathrm{Out}(G)$ containing a principal congruence subgroup is called a *congruence subgroup*.

Remark 2.4

Since $\pi_1(S)$ is finitely generated (when S is of finite type), every subgroup of finite index in $\pi_1(S)$ contains a characteristic subgroup of finite index. Thus, $\mathrm{Out}(\pi_1(S))$ has many congruence subgroups arising from the above construction.

Now we can generally formulate the congruence subgroup property.

Definition 2.5: Congruence Subgroup Property (CSP)

A group G is said to have the *congruence subgroup property* (CSP) if every finite index subgroup of G is a congruence subgroup (that is, contains a principal congruence subgroup).

For arithmetic groups, there are classical results regarding whether these groups have the CSP.

Theorem 2.6

$\mathbf{SL}_n(\mathbb{Z})$ has the CSP if $n > 2$. $\mathbf{SL}_2(\mathbb{Z})$ does not have the CSP, and in fact admits many finite index subgroups which are not congruence.

We can now state the conjecture.

Conjecture 2.7: Congruence Subgroup Conjecture

Suppose S is a compact orientable surface. $\mathrm{Mod}(S)$ has the CSP.

3 Connection to Geometric Group Theory, Elliptic Curves

There is a famous conjecture in geometric group theory:

Conjecture 3.1: Residual Finiteness of Hyperbolic Groups

Every hyperbolic group Γ is residually finite, meaning for every $g \in \Gamma$, there is a homomorphism ϕ from Γ to a finite group such that $\phi(g) \neq 1$.

If S is hyperbolic, $\pi_1(S)$ is a hyperbolic group. Harry Wilton proved that the above conjecture implies the congruence subgroup conjecture. Also, there is a related conjecture of Bridson-Reid:

Conjecture 3.2: Bridson-Reid

Let $G, H \leqslant \mathbf{PSL}_2(\mathbb{C})$ be lattices. $\hat{G} \cong \hat{H} \implies G \cong H$ ($\hat{G}$ is the profinite completion of G).

The profinite completion involves taking limits over quotients by finite-index subgroups, hence the connection. Ivanov also said Voevodsky noted to him that the congruence subgroup conjecture implies the following conjecture of Grothendieck (since proven unconditionally):

Theorem 3.3

A smooth algebraic curve over $\mathbb{Q}$ is determined up to isomorphism by its algebraic fundamental group (isomorphic to the profinite completion of $\pi_1(S)$), considered together with the natural action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on it.