

What is the Congruence Subgroup Property?

Dave Witte Morris

University of Lethbridge, Alberta, Canada
 http://people.uleth.ca/~dave.morris
 Dave.Morris@uleth.ca

Abstract. We will present a few different characterizations of the Congruence Subgroup Property, and describe some of its connections with other important topics in the field of arithmetic groups, including superrigidity, subgroup growth, bounded generation, and Algebraic K-Theory.

Summary

- $\Gamma = \text{SL}_3(\mathbb{Z})$ or other arithmetic group
- $\Gamma_{n,H}$ = congruence subgroup = obvious finite-index subgroup of Γ

Theorem (~1964 Bass-Lazard-Serre, Mennicke)

Every fin-ind subgrp of $\text{SL}_k(\mathbb{Z})$ is a cong subgrp if $k \geq 3$.

For short, we say that $\text{SL}_k(\mathbb{Z})$ satisfies the **Congruence Subgroup Property** ("CSP") when $k \geq 3$.

Profinite completion

CSP calculates the **profinite completion** of Γ :

$$\hat{\Gamma} := \varprojlim \frac{\Gamma}{N} \quad \text{where } \Gamma/N \text{ ranges over all the finite quotients of } \Gamma.$$

Example

$$\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p \quad (\mathbb{Z}_p = \text{the ring of } p\text{-adic integers})$$

Remark (for $\Gamma = \text{SL}_3(\mathbb{Z})$)

$$\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}} \Rightarrow \Gamma \hookrightarrow \text{SL}_3(\hat{\mathbb{Z}}) \Rightarrow \hat{\Gamma} \twoheadrightarrow \text{SL}_3(\hat{\mathbb{Z}}).$$

Proposition (assume $\Gamma = \text{SL}_3(\mathbb{Z})$)

$$\text{CSP} \Leftrightarrow \hat{\Gamma} = \text{SL}_3(\hat{\mathbb{Z}}) \quad (= \prod_p \text{SL}_3(\mathbb{Z}_p))$$

Statement of the property

Let $\Gamma = \text{SL}_3(\mathbb{Z}) = \{ 3 \times 3 \text{ integer mats with det } 1 \}$.

Should also consider other **arithmetic groups**:

- $\text{SL}_2(\mathbb{Z}), \text{SL}_2(\mathbb{Z}[\sqrt{5}]), \text{Sp}_4(\mathbb{Z}), \dots$
- the \mathbb{Z} -points of a semisimple algebraic \mathbb{Q} -group G
- a lattice in a semisimple Lie group G with finite center

Congruence Subgroup Property (CSP):

The finite-index subgroups of Γ are all obvious.
 (There are **not very many** finite-index subgrps.)

Theorem

$\text{SL}_2(\mathbb{Z})$ does **not** have the CSP.

Proof.

Let F = finite quotient of $\text{SL}_2(\mathbb{Z}) = \Gamma$.
 CSP: F is quotient of $\text{SL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_p \text{SL}_2(\mathbb{Z}/p^{k_i}\mathbb{Z})$
 (because $\mathbb{Z}/n\mathbb{Z} \cong \bigoplus \mathbb{Z}/p_i^{k_i}\mathbb{Z}$).

So all nonabelian factors in composition series of F are of the form $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

However, $\text{SL}_2(\mathbb{Z}) \cong$ free group (up to finite index).
 So **every** finite simple grp is in a composition series.

→ ← □

Abelian quotients

Proposition

CSP $\Rightarrow \Gamma$ has no infinite abelian quotients.

Proof.

$\Gamma \twoheadrightarrow \mathbb{Z} \Rightarrow \hat{\Gamma} = \prod_p \text{SL}_3(\mathbb{Z}_p) \twoheadrightarrow \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}_p$.
 Lie Theory (p -adic): Lie alg of $\text{SL}_3(\mathbb{Z}_p)$ is simple, so no (continuous) homo to abelian grp. □

Note: Kazhdan's Property T also implies $\Gamma \not\rightarrow \mathbb{Z}$.

Open question

Can Kazhdan's property be used to prove CSP?

CSP: all finite-index subgrps of Γ are obvious

The obvious finite-index subgroups of Γ

Let H be any subgroup of $\text{SL}_3(\mathbb{Z}/n\mathbb{Z})$.

- $\mathbb{Z}/n\mathbb{Z}$ is finite $\Rightarrow \text{SL}_3(\mathbb{Z}/n\mathbb{Z})$ is finite $\Rightarrow H$ has **finite index** in $\text{SL}_3(\mathbb{Z}/n\mathbb{Z})$.
- $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ is a ring homomorphism $\Rightarrow \varphi_n: \text{SL}_3(\mathbb{Z}) \rightarrow \text{SL}_3(\mathbb{Z}/n\mathbb{Z})$ is group homo.

$\Gamma_{n,H} := \varphi_n^{-1}(H)$ is a **subgroup of finite index** in Γ .

Definition

$\Gamma_{n,H}$ is a **congruence subgroup** of Γ .

These are the obvious finite-index subgroups of Γ .

Applications of the CSP

Subgroup growth

Theorem (1995 Lubotzky)

$$\text{CSP} \Leftrightarrow \#\{X < \Gamma \mid |\Gamma : X| \leq n\} < n^{\epsilon \log n} \quad \begin{matrix} \forall \epsilon > 0, \\ \forall \text{ large } n \end{matrix}$$

This generalizes CSP to arbitrary abstract groups.

Theorem (1991 Platonov-Rapinchuk)

$$\text{CSP} \Leftrightarrow \left| \frac{\Gamma}{\langle g^n \mid g \in \Gamma \rangle} \right|^* \text{ bdd by a polynomial in } n$$

* If infinite, replace with largest of its finite quotients.

Superrigidity

Theorem (for $\Gamma = \text{SL}_3(\mathbb{Z})$)

$\rho: \Gamma \rightarrow \text{GL}_k(\mathbb{R})$ (any finite-dim'l representation)
 $\Rightarrow \rho$ **virtually extends** to $\hat{\rho}: \text{SL}_3(\mathbb{R}) \rightarrow \text{GL}_k(\mathbb{R})$.

Sketch of proof.

Assume $\rho: \Gamma \rightarrow \text{SL}_k(\mathbb{Q})$.
 Γ is finitely generated, so $\rho(\Gamma) \subset \text{SL}_k(\mathbb{Z}_p), \exists p$.
 extension $\hat{\rho}: \hat{\Gamma} \rightarrow \text{SL}_k(\mathbb{Z}_p)$.
 CSP tells us $\hat{\rho}: \text{SL}_3(\mathbb{Z}_p) \rightarrow \text{SL}_k(\mathbb{Z}_p)$.
 Lie theory: any such homomorphism is analytic; indeed, it is defined by polynomials.
 Since $\rho(\Gamma) \subset \text{SL}_k(\mathbb{Q})$, the polys have \mathbb{Q} coefficients, so they define homo $\text{SL}_3(\mathbb{R}) \rightarrow \text{SL}_k(\mathbb{R})$. □

Bounded generation

Recall: Γ *finitely generated* if \exists finite set S , every elt of Γ is product of powers of elts of S .

Definition

Γ is *boundedly generated* if \exists finite set S , every elt of Γ is prod of **bdd #** of powers of elts of S .
I.e., $\Gamma = \langle s_1 \rangle \cdot \langle s_2 \rangle \cdots \langle s_n \rangle$.

Conjecture (Rapinchuk)

$CSP \Rightarrow$ *bounded generation*.

Proposition (Lubotzky, Rapinchuk)

Converse is true: bounded generation \Rightarrow CSP.

Key step in proof of CSP: $E(n\mathbb{Z}) = \Gamma_{n, \{e\}}$.
A starting point of *Algebraic K-Theory*.

Definition

$R =$ ring (commutative). $K_1(R) = \lim_{k \rightarrow \infty} \frac{SL_k(R)}{E_k(R)}$.

Exercise

$E_k(\mathbb{Z}^\infty) = SL_k(\mathbb{Z}^\infty)$ ($\mathbb{Z}^\infty = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots$)
 $\Rightarrow SL_k(\mathbb{Z})$ is *boundedly gen'd* (by elem mats).

So methods in pf of CSP apply to prove bdd gen:
• short pf of bdd gen of $SL_3(\mathbb{Z})$ and $SL_3(\mathbb{Z}[\alpha])$
• pf of bdd gen of $SL_2(\mathbb{Z}[\alpha])$ and $SL_2(\mathbb{Z}[1/r])$

(Actually, easier to use *ultrapower* instead of ordinary power.)

Proposition (Lubotzky, Rapinchuk)

Bounded generation \Rightarrow CSP.

Proof.

$\Gamma = \langle x \rangle \cdot \langle y \rangle$
 $\Rightarrow \frac{\Gamma}{\langle \text{nth powers} \rangle} = \{x, x^2, \dots, x^n\} \cdot \{y, \dots, y^n\}$.

So $\left| \frac{\Gamma}{\langle \text{nth powers} \rangle} \right| \leq n^2$ is bdd by polynomial. \square

CSP for other latts in ss Lie groups

Conjecture (Serre)

$\Gamma = G(\mathbb{Z})$ *arithmetic lattice in conn, ss Lie group G .*
(irreducible, G simply conn as alg'ic grp, isotropic at p -adic places)
 \mathbb{R} -rank $G \geq 2 \Rightarrow$ *some finite-index subgrp of Γ has CSP.*

Remark

- True if G/Γ is *not* compact [Raghunathan].
- Open for some latts in $SL_k(\mathbb{R})$ (and others).
- Serre conjectured converse:
CSP fails whenever \mathbb{R} -rank $G = 1$.
But lattices in $Sp(1, n)$ or $F_{4,1}$ may have CSP. (?)

Proof of the CSP for $SL_3(\mathbb{Z})$ (outline)

• $X =$ finite-index subgroup of $\Gamma = SL_3(\mathbb{Z})$.


• $n = \gcd \{x_{ij}, x_{ii} - x_{jj} \mid x \in X\}$, so
 $X \subset \{g \in SL_3(\mathbb{Z}) \mid g \equiv \lambda \text{Id} \pmod{n}\} = \Gamma_{n, \{\lambda \text{Id}\}}$


• $E(n\mathbb{Z}) = \left\langle \begin{bmatrix} 1 & n\mathbb{Z} & n\mathbb{Z} \\ 0 & 1 & n\mathbb{Z} \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & & \\ n\mathbb{Z} & 1 & \\ & n\mathbb{Z} & 1 \end{bmatrix} \right\rangle \subset X$.


Easy: $E(\mathbb{Z}) = \Gamma (= \Gamma_{1, \{e\}})$. *Not easy:* $E(n\mathbb{Z}) = \Gamma_{n, \{e\}}$.


(Actually, normal closure of $E(n\mathbb{Z})$ — assume wolog X normal.)

$\therefore \Gamma_{n, \{e\}} \subset X$. So $X \supset$ is a congruence subgroup. \square

 A. S. Rapinchuk: The congruence subgroup problem, in: *Algebra, K-theory, groups, and education (New York, 1997)*. Amer. Math. Soc., Providence, RI, 1999, pp. 175-188. MR1732047 (2001f:20108)

 B. Sury: *The Congruence Subgroup Problem. An elementary approach aimed at applications*. Hindustan Book Agency, New Delhi, 2003. ISBN 81-85931-38-0, MR1978430 (2005g:20082)

 A. Lubotzky and D. Segal: *Subgroup Growth*. Birkhäuser, Basel, 2003. ISBN 3-7643-6989-2, MR1978431 (2004k:20055)

 D. W. Morris: Bounded generation of $SL(n, A)$ (after D. Carter, G. Keller, and E. Paige). *New York J. Math.* 13 (2007), 383-42. MR2357719 (2008j:20145)