# THE CONGRUENCE SUBGROUP PROPERTY AND BOUNDED GENERATION

DAVE WITTE MORRIS

Abstract. This module will explain what the Congruence Subgroup Property is, and why it is important. Then "Mennicke symbols" (a tool from Algebraic K-Theory) will be used to show that $\mathrm{SL}(3,\mathbb{Z})$ has the property, and a stronger property called "bounded generation."

## Lecture I. Introduction to the Congruence Subgroup Property

### 1. Statement of the Congruence Subgroup Property for $\mathrm{SL}(3,\mathbb{Z})$

Note that $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a ring homomorphism, so

$$\varphi_n \colon \mathrm{SL}(3,\mathbb{Z}) \to \mathrm{SL}(3,\mathbb{Z}/n\mathbb{Z})$$

is a group homomorphism. Since the ring $\mathbb{Z}/n\mathbb{Z}$ is obviously finite, it is clear that the group $\mathrm{SL}(3,\mathbb{Z}/n\mathbb{Z})$ is finite, so the image of $\varphi_n$ is finite. Hence,

$$\Gamma_n := \ker \varphi_n$$

is a (normal) subgroup of finite index in $\Gamma = \mathrm{SL}(3,\mathbb{Z})$.

These subgroups are the most obvious finite-index subgroups of $\Gamma$, and they have a special name:

**Definition.** $\Gamma_n$ is a *principal congruence subgroup* of $\Gamma$.

By definition, $\Gamma_n$ is the inverse image of $\{e\}$, the trivial subgroup. We can generalize the above construction by replacing $\{e\}$ with a more general subgroup:

| |
|---|
| If $X$ is any subgroup of $\mathrm{SL}(3,\mathbb{Z}/n\mathbb{Z})$, then $\varphi_n^{-1}(X)$ is a finite-index subgroup of $\Gamma$. It is a *congruence subgroup* of $\Gamma$. |

Equivalently:

**Definition.** A subgroup $H$ of $\Gamma$ is a *congruence subgroup* if it contains a principal congruence subgroup.

Thus, it is obvious that every congruence subgroup of $\mathrm{SL}(3,\mathbb{Z})$ is a subgroup of finite index. It is not at all obvious that the converse is true:

**Theorem** (Bass-Lazard-Serre (1964), Mennicke (1965))**.** *If $k \geq 3$, then every finite-index subgroup of $\mathrm{SL}(k,\mathbb{Z})$ is a congruence subgroup.*

For short, we say that $\mathrm{SL}(k,\mathbb{Z})$ satisfies the *Congruence Subgroup Property* ("CSP") when $k \geq 3$. We will see later that this is false for $k = 2$.

**Remark.** If $\Gamma$ is the fundamental group of a manifold $M$, then the Congruence Subgroup Property is a quite explicit description of all the finite covers of $M$.

*Date*: Geometric Literacy Seminar, University of Chicago, May 2008.

### 2. CSP for other groups

#### 2.1. Lattices in semisimple Lie groups.

**Conjecture** (Serre)**.** *Let $\Gamma$ be an irreducible, arithmetic lattice in a connected, semisimple Lie group $G$. (And assume $G$ is "algebraically simply connected.") If $\mathbb{R}$-rank $G \geq 2$, then some finite-index subgroup of $\Gamma$ has the CSP.*

**Remark.**

- The conjecture is true whenever $G/\Gamma$ is *not* compact [Raghunathan].
- Many, but not all, additional cases have been verified.
- Serre conjectured, conversely, that CSP fails whenever $\mathbb{R}$-rank $G = 1$, but it seems quite possible that (some? all?) lattices in $\mathrm{Sp}(1,n)$ will turn out to have CSP.
- I think it is known that hyperbolic groups (i.e., lattices in $\mathrm{SO}(1,n)$) do *not* have the Congruence Subgroup Property.

#### 2.2. The automorphism group of a free group.

Note that, for $\Gamma = \mathrm{SL}(3,\mathbb{Z})$, the principal congruence subgroup $\Gamma_n$ consists of the automorphisms of $\mathbb{Z}^3$ that act trivially on the finite quotient $\mathbb{Z}^3/n\mathbb{Z}^3$. This has a natural generalization to the automorphism group of a free group.

**Definition.**

- Let $N$ be a (characteristic) subgroup of finite index in $F_n$, so $\mathrm{Aut}(F_n)$ acts on the finite group $F_n/N$.
- The kernel of this action is a *principal congruence subgroup* of $\mathrm{Aut}(F_n)$.
- Any subgroup that contains a principal congruence subgroup is a *congruence subgroup*.

The following question is attributed to Ihara (see [4, p. 1679]). I learned of it from A. Rapinchuk.

**Wide open problem** (Ihara)**.** *Is every finite-index subgroup of $\mathrm{Aut}(F_n)$ a congruence subgroup?*

**Exercise.** Let $H$ be a subgroup of finite index in $F_n$. Show that

$$\{\, \alpha \in \mathrm{Aut}(F_n) \mid \alpha(xH) = xH, \forall x \in F_n \,\}$$

is a congruence subgroup.

2.3. **Braid groups and mapping class groups.** According to notes [6] from a recent seminar by Jordan Ellenberg at the University of Wisconsin:

> "Braid group has the congruence subgroup property CSP. This was discovered by Thurston last year (2007), but known by algebraic geometers Diaz-Donagi-Harbater, Asada (2001) earlier. This is for any $n$, so we don't get any $\mathrm{SL}_2(\mathbb{Z})$ weirdness. For $\Gamma_g$ (the mapping class group of genus $g$ things) it is suggested to have this property but not known."

## 3. $\mathrm{SL}(2,\mathbb{Z})$ does not have the CSP

Let $F$ be a finite quotient of $\Gamma = \mathrm{SL}(2,\mathbb{Z})$. If $\Gamma$ has the CSP, then $F$ is a quotient of $\Gamma/\Gamma_n$, for some $n$. Since $\mathbb{Z}/n\mathbb{Z} \cong \bigoplus \mathbb{Z}/p_i^{k_i}\mathbb{Z}$, we have

$$\frac{\Gamma}{\Gamma_n} \cong \bigoplus \frac{\Gamma}{\Gamma_{p_i^{k_i}}},$$

so it is easy to see that the only nonabelian factors in a composition series of $F$ are of the form $\mathrm{SL}(2,\mathbb{Z}/p\mathbb{Z})$.

On the other hand, $\mathrm{SL}(2,\mathbb{Z})$ is almost a free group, so its finite quotients include *every* finite simple group in their composition series. This is a contradiction.

## 4. Applications of the CSP

4.1. **Normal subgroups of $\mathbf{SL(3,\mathbb{Z})}$.** The Margulis Normal Subgroups Theorem tells us that every infinite, normal subgroup of $\Gamma = \mathrm{SL}(3,\mathbb{Z})$ has finite index. (It is easy to find all the finite, normal subgroups; in fact, for the case of $\mathrm{SL}(3,\mathbb{Z})$, there are none at all, other than $\{e\}$.) Thus, the Congruence Subgroup Property provides a classification of all the (infinite) normal subgroups of $\Gamma$.

4.2. **Subgroup growth** [3]**.** Let $S_n$ be the number of subgroups of index $\leq n$ in $\Gamma$; i.e.,

$$S_n = \#\{\, H \subset \Gamma \mid |\Gamma : H| \leq n \,\}.$$

$\Gamma$ has the CSP iff

$$S_n = n^{(C \pm \epsilon)\log n / \log\log n}.$$

If $\Gamma$ does not have the CSP, then its subgroup growth is larger:

$$\exists \epsilon > 0, S_n > n^{\epsilon \log n}.$$

4.3. **Abelian quotients.** The estimate on subgroup growth (or other, easier arguments) implies that if $\Gamma$ has the CSP, then it has no infinite, abelian quotients.

**Remark** (Virtual Haken Conjecture)**.** It is believed that hyperbolic groups behave the opposite way: W. Thurston conjectured that if $\Gamma$ is any lattice in $\mathrm{SO}(1,n)$, then some finite-index subgroup of $\Gamma$ has an infinite cyclic quotient.

4.4. **Profinite completion.** Recall $\mathbb{Z}_p$, the ring of $p$-adic integers is:

$$\lim_{\longleftarrow} \frac{\mathbb{Z}}{p^n\mathbb{Z}} = \{\, a_0 + a_1 p + a_2 p^2 + \cdots \mid 0 \leq a_i < p \,\}.$$

**Lemma.** *$\bigoplus_p \mathbb{Z}_p$ is the* profinite completion $\widehat{\mathbb{Z}}$ *of* $\mathbb{Z}$*, i.e.,*

$$\bigoplus_p \mathbb{Z}_p \cong \lim_{\longleftarrow} \frac{\Gamma}{N},$$

*where $\Gamma/N$ ranges over all the finite quotients of $\Gamma$.*

*Proof.* Suppose $\varphi \colon \mathbb{Z} \twoheadrightarrow F$, where $F$ is a finite group. Then

$$F \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \bigoplus \frac{\mathbb{Z}}{p^{k_i}\mathbb{Z}},$$

so $\varphi$ extends to a *unique* $\widehat{\varphi} \colon \bigoplus_p \mathbb{Z}_p \to F$. □

The Congruence Subgroup Property calculates the profinite completion of $\mathrm{SL}(3,\mathbb{Z})$:

$$\widehat{\mathrm{SL}(3,\mathbb{Z})} = \bigoplus_p \mathrm{SL}(3,\mathbb{Z}_p).$$

4.5. **Superrigidity.**

**Theorem** (Bass-Milnor-Serre, Raghunathan)**.** *Let*

- $\Gamma = \mathrm{SL}(3,\mathbb{Z})$*, and*
- $\rho \colon \Gamma \to \mathrm{GL}(n,\mathbb{R})$ *be a finite-dimensional representation of* $\Gamma$*.*

*Then $\rho$ almost extends to a representation $\widetilde{\rho} \colon \mathrm{SL}(3,\mathbb{R}) \to \mathrm{GL}(n,\mathbb{R})$.*

*Sketch of proof.* For simplicity, assume $\rho \colon \Gamma \to \mathrm{SL}(n,\mathbb{Q})$. Since $\Gamma$ is finitely generated, we have $\rho(\Gamma) \subset \mathrm{SL}(n,\mathbb{Z}_p)$, for some $p$. Since $\mathrm{SL}(n,\mathbb{Z}_p)$ is profinite, then $\rho$ extends to $\widehat{\rho} \colon \widehat{\mathrm{SL}(3,\mathbb{Z})} \to \mathrm{SL}(n,\mathbb{Z}_p)$. By the CSP, this amounts to a map $\mathrm{SL}(3,\mathbb{Z}_p) \to \mathrm{SL}(n,\mathbb{Z}_p)$. The theory of ($p$-adic) Lie groups tells us that any such homomorphism is analytic; indeed, it is defined by polynomials. Since $\rho(\Gamma) \subset \mathrm{SL}(n,\mathbb{Q})$, these polynomials have rational coefficients, so they define a homomorphism $\widetilde{\mathrm{SL}}(3,\mathbb{R}) \to \mathrm{SL}(n,\mathbb{R})$. □

## References

[1] H. Bass, M. Lazard, J.-P. Serre: Sous-groupes d'indice fini dans $\mathrm{SL}(n,\mathbb{Z})$, *Bull. Amer. Math. Soc.* 70 (1964) 385–392. MR 0161913 (28 #5117)
[2] H. Bass, J. Milnor, J.-P. Serre: Solution of the congruence subgroup problem for $\mathrm{SL}_n$ ($n \geq 3$) and $\mathrm{Sp}_{2n}$ ($n \geq 2$), *Inst. Hautes Études Sci. Publ. Math.* 33 (1967) 59–137. MR 0244257 (39 #5574)
[3] A. Lubotzky and D. Segal: *Subgroup Growth.* Birkhäuser, Basel, 2003. ISBN 3-7643-6989-2, MR 1978431 (2004k:20055)
[4] B. Sury: Bounded generation does not imply finite presentation, *Comm. Algebra* 25 (1997), no. 5, 1673–1683. MR 1444027 (98b:20046)
[5] B. Sury: *The Congruence Subgroup Problem. An elementary approach aimed at applications.* Hindustan Book Agency, New Delhi, 2003. ISBN 81-85931-38-0, MR 1978430 (2005g:20082)
[6] http://www.math.wisc.edu/∼rhoades/Notes/ellenberg02-18-08.pdf