Lecture 5

Congruence subgroup problem.

Let $\Gamma = SL_d(\mathbb{Z})$

What are finite index subgroups of Γ?

Consider the factor maps: $\pi_n : SL_d(\mathbb{Z}) \to SL_d(\mathbb{Z}/n)$

$\Gamma(n) = \mathrm{Ker}(\pi_n) = \{\gamma \in SL_d(\mathbb{Z}) : \gamma = id \pmod n\}$

$\Gamma(n)$ is called the principle congruence subgroup of level n.

$\Lambda \leq \Gamma$ is called a congruence subgroup if $\Lambda \supset \Gamma(n)$ for some n.

Congruence subgroup problem (naive formulation):
Is every subgroup of finite index in Γ a congruence subgroup?

Klein: no, for $d=2$

Bass-Lazard-Serre, Mennicke: yes, for $d \geq 3$.

Elementary matrices: $e_{ij} = \begin{matrix} \\ \\ i \\ \\ j \end{matrix}\!\!\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$, $i \neq j = 1, \dots d$.

Lemma $SL_d(\mathbb{Z})$ (and $SL_d(\mathbb{Z}/n)$) generated by elementary matrices.

Multiplications by e_{ij} correspond to elementary row/column operations.

Let $\gamma \in SL_d(\mathbb{Z})$. Using induction on $\max\{|\gamma_{i1}| : i = \overline{1,d}\}$ we can reduce γ by elementary column operations

to the form $\begin{pmatrix} 0\cdots 0\ d\ 0\cdots 0 \\ * \end{pmatrix}$ where

$d = \gcd(\gamma_{11}, \dots \gamma_{1d})$. Since $\det\gamma = 1$, $d = \pm 1$.

$$\begin{pmatrix} 0\cdots 0\ \pm 1\ 0\cdots 0 \\ * \end{pmatrix} \sim \begin{pmatrix} 1 0\cdots 0\ \pm 1\ 0\cdots 0 \\ * \end{pmatrix} \sim \begin{pmatrix} 1\ 0\cdots 0 \\ * \end{pmatrix}.$$

Then using column operations, $\sim \left(\begin{array}{c|c} 1 & 0\cdots 0 \\ 0 & \\ \vdots & * \\ 0 & \end{array}\right)$.

Cor. The factor map $SL_d(\mathbb{Z}) \to SL_d(\mathbb{Z}/n)$ is onto.

The restriction to elementary subgroups is onto.

Thm $SL_2(\mathbb{Z})$ contains a free subgroup F_2 of index 12.

$\Lambda = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle$.

1) $\Gamma(2)$ is generated by Λ and $\pm id$.

($|\Gamma : \Gamma(2)| = \#SL_2(\mathbb{Z}/2) = (4-1)\cdot(4-2) = 6$.

Hence, $|\Gamma : \Lambda| = 12$)

$\Gamma(2) \ni \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $c \neq 0$. We have $a = 2q\cdot c + r$

where $|r| \le |c|$

Since a is odd and c is even, we have $0 < |r| < |c|$.

$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-q}\gamma = \begin{pmatrix} r & * \\ c & * \end{pmatrix}$, with $|r| < |c|$.

Continue this process...

After a finite number of steps.

We get $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ or $\begin{pmatrix} 0 & * \\ * & * \end{pmatrix}$.

Since this element is in $\Gamma(2)$, we get $\pm\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Remark: $\left\langle \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \right\rangle$ is an infinite index subgroup of $\Gamma(n)$.

Ping-Pong Lemma: Suppose that a group Γ acts on a set S, and $U, V \subset S$, $a, b \in \Gamma$ such that

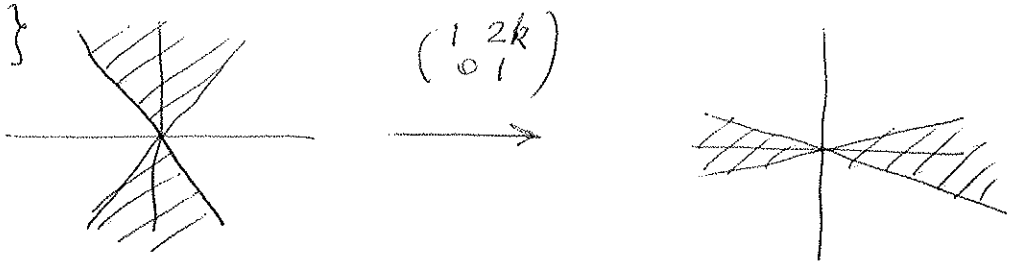
$$a^n \cdot U \subsetneq V, \quad n \neq 0, \qquad b^n \cdot V \subsetneq U, \quad n \neq 0.$$

Then $\langle a, b \rangle$ is freely generated by a and b.

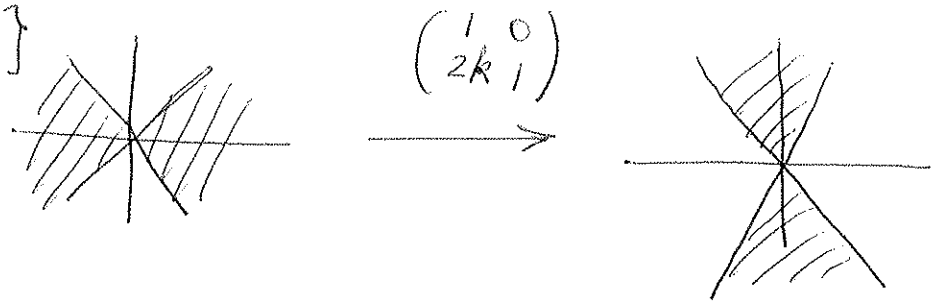
Suppose that $\gamma = a^{n_1} b^{m_1} \dots a^{n_k} b^{m_k}$ be a nontrivial reduced word such that $\gamma = e$. Conjugating we may assume that γ starts with a and ends with b. Then $\gamma \cdot V \subsetneq V$. Hence, $\gamma \neq e$. ∎

2) Λ is freely generated by $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

$U = \{ |y| > |x| \}$



$V = \{ |x| > |y| \}$



Tits alternative If $\Gamma < GL_d(\mathbb{K})$, then either

1) Γ contains a soluable subgroup of finite index.

2) Γ contains a nonabelean free subgroup.

Thm (Klein) $\Gamma = SL_2(\mathbb{Z})$ does not have CSP.

Γ $SL_2(\mathbb{Z})/\Gamma(n) \simeq SL_2(\mathbb{Z}/n) \simeq SL_2(\mathbb{Z}/p_1^{n_1}) \times \dots \times SL_2(\mathbb{Z}/p_s^{n_s})$

$1 \to K_n \to SL_2(\mathbb{Z}/p^n) \to SL_2(\mathbb{Z}/p) \to 1$

K_n: p-group; $SL_2(\mathbb{Z}/p)$: simple group mod $\pm id$. $p \geq 5$

On the other hand, $\Lambda = \langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \rangle$ is free,

so it has many other quotients...

For example, S_m for every $m \geq 1$. $\square$

Thm (Bass-Lazard-Serre 1964, Mennicke)

$\Gamma = SL_d(\mathbb{Z})$ has CSP, $d \neq 3$.

$E(n) = [$the smallest normal subgroup generated by e_{ij}^n.$]$

Lemma 0. Every $\Lambda \leq_{f.i.} \Gamma$ contains some $E(n)$.

$\Delta = \bigcap_{\gamma \in \Gamma/\Lambda} \gamma \Lambda \gamma^{-1}$ is normal subgroup of Γ of finite index.

$\exists n \geq 1$: $e_{ij}^n \in \Delta \Rightarrow E(n) \leq \Delta \subset \Lambda$. $\square$

Main Claim: $\boxed{E(n) = \Gamma(n).}$

$p_n : \Gamma(n) \to \Gamma(n)/E(n)$.

For simplicity, consider $d = 3$.

Lemma 1 $p_n\left(\begin{array}{c|c} SL_2(\mathbb{Z})(n) & 0 \\ \hline 0 & 1 \end{array}\right) = \Gamma(n)/E(n)$.

$$\gamma = \begin{bmatrix} * & * & * \\ * & * & * \\ a & b & c \end{bmatrix} \overset{(1)}{\rightsquigarrow} \begin{bmatrix} * & * & * \\ * & * & * \\ a & b' & c \end{bmatrix} \overset{(2)}{\rightsquigarrow} \begin{bmatrix} * & * \\ n & b' \end{bmatrix} \overset{\times e_{13}^{s}}{\rightsquigarrow} \begin{bmatrix} * & * \\ n & b' \end{bmatrix} \rightsquigarrow \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix} \overset{e_{13}^{s}\times}{\rightsquigarrow}$$

1) Find $b' = b \pmod{na}$ such that $\gcd(b', c) = 1$.
$b' = b + \alpha \cdot na$. Let $p \mid c$, p-prime. Since $c = 1 \pmod n$, $p \nmid n$. and either $p \nmid a$ or $p \nmid b$.

In both cases, $\exists \alpha : p \nmid b'$
We can find b' as required by Chinese Reminder Thm.

2) $\left.\begin{array}{l} \gcd(b', c) = 1 \\ a = 0 \pmod n \end{array}\right| \Rightarrow \alpha n b' + \beta n c = a - n$ for $\alpha, \beta \in \mathbb{Z}$.

3) $b' = 0 \pmod n$
$c' = 1 \pmod n$

$$\rightsquigarrow \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix} \rightsquigarrow \left[\begin{array}{c|c} * & 0 \\ \hline 0 & 1 \end{array}\right].$$

$p_n(e_{13}^{-s} \gamma e_{13}^{s}) \in p_n\left(\begin{array}{c|c} * & c \\ \hline 0 & 1 \end{array}\right)$

$\Downarrow$

$p_n(\gamma) \in p_n\left(\begin{array}{c|c} * & * \\ \hline 0 & 1 \end{array}\right) = p_n\left(\begin{array}{c|c} * & 0 \\ \hline 0 & 1 \end{array}\right)$.

Lemma 2. $p_n\left(\begin{array}{c|c} a\ b \\ c\ d & 1 \end{array}\right) = p_n\left(\begin{array}{c|c} a\ b \\ c'\ d' & 1 \end{array}\right)$

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c' & d' \end{pmatrix}^{-1}\right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d' & -b \\ -c' & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ cd' - dc' & 1 \end{pmatrix} \in E(n).$$

$cd' - dc' = 0 \pmod n$

Mennicke symbol: $\left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right] = p_n\left(\begin{array}{cc|c} a & b & 0 \\ * & * & \\ \hline 0 & & 1 \end{array}\right) \in \Gamma(n)/E(n)$

Need to show that the Mennicke symbol is trivial.

Lemma 3. $\Gamma(n)/E(n)$ is central in $\Gamma/E(n)$.

Since elementary matrices in Γ are conjugate to each other, it suffices to show that for one of them: $[e_{13}, \Gamma(n)] \subset E(n)$.
By Lemma 1, we just need to check that

$$[e_{13}, \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}] \subset E(n)$$

$$\| \quad \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1}$$

$$e_{13}^{-1} \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} e_{13} \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix} = e_{13}^{-1} \left(\begin{array}{cc|c} * & * & 0 \\ * & * & \\ \hline 0 & 0 & 1 \end{array}\right)^{-1} \begin{pmatrix} * & * & 1 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \left(\begin{array}{c|c} E & \begin{matrix} n\mathbb{Z} \\ n\mathbb{Z} \end{matrix} \\ \hline 0 \quad 0 & 1 \end{array}\right)$$

Lemma 4. $\begin{bmatrix} b_1 b_2 \\ a \end{bmatrix} = \begin{bmatrix} b_1 \\ a \end{bmatrix} \cdot \begin{bmatrix} b_2 \\ a \end{bmatrix}$.

$$\begin{bmatrix} b_2 \\ a \end{bmatrix} = \left(\begin{array}{cc|c} a & b_2 & 0 \\ c & d & \\ \hline 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix} \left(\begin{array}{cc|c} a & b_2 & 0 \\ c & d & \\ \hline 0 & 0 & 1 \end{array}\right) \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} d & 0 & -c \\ 0 & 1 & 0 \\ -b_2 & 0 & a \end{pmatrix}.$$

$$\begin{bmatrix} b_1 \\ a \end{bmatrix} \cdot \begin{bmatrix} b_2 \\ a \end{bmatrix} = \left(\begin{array}{cc|c} a & b_1 & 0 \\ * & * & \\ \hline 0 & 0 & 1 \end{array}\right) \begin{pmatrix} d & 0 & -c \\ 0 & 1 & 0 \\ -b_2 & 0 & a \end{pmatrix} = \begin{pmatrix} ad & b_1 & -ac \\ * & * & * \\ -b_2 & 0 & a \end{pmatrix} \xrightarrow{\times c} \sim \begin{pmatrix} 1 & b_1 & 0 \\ * & * & * \\ -b_2 & 0 & a \end{pmatrix}$$

($c \equiv 0 \pmod n$)

$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & b_1 b_2 & a \end{pmatrix} \longrightarrow \begin{pmatrix} a & b_1 b_2 & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{bmatrix} b_1 b_2 \\ a \end{bmatrix}$$

$b_2 \equiv 0 \pmod n$, $b_1 \equiv 0 \pmod n$ — conjugation

Lemma 5. $\begin{bmatrix} b + ta \\ a \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$ for $t \in n\mathbb{Z}$.

$$\begin{bmatrix} b \\ a + tb \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} \text{ for } t \in \mathbb{Z}.$$

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a+b & b \\ * & * \end{pmatrix} = \begin{pmatrix} a+b & b \\ * & * \end{pmatrix}.$$

Lemma 7. If $b = \pm 1 \pmod a$, then $\left[\frac{b}{a}\right] = 1$.

$$\left[\frac{b}{a}\right] = \left[\frac{b-ba}{a}\right] = \left[\frac{(\pm 1 + ka)(1-a)}{a}\right] = \left[\frac{\pm(1-a) + ka(1-a)}{a}\right] = \left[\frac{\pm(1-a)}{a}\right]$$

$$= \left[\frac{\pm(1-a)}{1}\right] = \left[\frac{0}{1}\right] = e$$

Cor. If $b^n = \pm 1 \pmod a$, then $\left[\frac{b}{a}\right]^n = 1$.

Lemma 8. $\left[\frac{b}{a}\right] = 1 \quad (\Rightarrow CSP)$.

Choose a prime p such that $p = a + tb$ (Dirichlet thm on primes in arithmetic progressions).

$p - 1 = 2^e q_1^{e_1} \dots q_\alpha^{e_\alpha}$ – prime decomposition.

Choose primes r_1 and r_2:

$$r_1 = -p \pmod{b, \text{ mod } q_1, \dots \text{ mod } q_\alpha}$$
$$r_2 = -1 \pmod{b, \text{ mod } q_1, \dots \text{ mod } q_\alpha} \qquad (*)$$

Let $a' = r_1 \cdot r_2$. Then $a' = a \pmod b$ and $\left[\frac{b}{a}\right] = \left[\frac{b}{a'}\right]$.

The exponent of $b \pmod p$ divides $p-1 \Rightarrow \left[\frac{b}{a}\right]^{p-1} = 1$.

The exponent of $b \pmod{a'}$ divides $(r_1-1)(r_2-1) \Rightarrow \left[\frac{b}{a}\right]^{(r_1-1)(r_2-1)} = 1$.

$(*) \Rightarrow \gcd\left(p-1, (r_1-1)(r_2-1)\right) = 2^{e'} \Rightarrow \left[\frac{b}{a}\right]^{2^{e'}} = 1$.

- If $b \neq 0 \pmod 4$ or $a = -1 \pmod 4$, we choose $p = -1 \pmod 4$.
  Then $b^{\frac{p-1}{2}} = \pm 1 \pmod p \Rightarrow \left[\frac{b}{a}\right]^{\frac{p-1}{2}} = 1$.
  Since $\frac{p-1}{2}$ is odd, $\left[\frac{b}{a}\right] = 1$.
- If $a = 1 \pmod 4$ and $b = 0 \pmod 4$, then choose prime $p = 1 \pmod 4$ such that $a + tb = -p$, and argue as above.

Profinite and congruence completions.

$\Gamma \leq SL_d(\mathbb{Z})$, – finitely generated.

$\{N_k\}_{k\geq 1}$ = all finite-index $\begin{cases} \text{normal} \\ \text{subgroups} \end{cases}$ of Γ.

Profinite metric: $d(\gamma_1,\gamma_2) := \sum_{k\geq 1} \frac{1}{2^k} \cdot \delta_{\gamma_1 \neq \gamma_2 \,(\mathrm{mod}\, N_k)}$.

Profinite topology: $\Gamma \xrightarrow[\text{diagonally}]{} \prod_{k\geq 1} \Gamma/N_k$ (product topology).

$$\widehat{\Gamma} = \left(\text{closure of } \Gamma \text{ in } \prod_{k\geq 1} \Gamma/N_k\right)$$

is called profinite completions

Similarly, if $\{M_k\}_{k\geq 1}$ is the collection of all congruence subgroups,

we define $\overline{\Gamma} = \left(\text{closure of } \Gamma \text{ in } \prod_{k\geq 1} \Gamma/M_k\right)$

– the congruence completion.

We have projection map:

$$\begin{array}{ccc} \prod_{k\geq 1} \Gamma/N_k & \longrightarrow & \prod_{k\geq 1} \Gamma/M_k \\ \uparrow & & \uparrow \\ \Gamma & \longrightarrow & \Gamma \end{array}$$

Hence, we have $\widehat{\Gamma} \longrightarrow \overline{\Gamma}$. Since Γ is dense in $\overline{\Gamma}$, this map is onto.

Congruence subgroup problem (modern formulation):
Identify the kernel of the map $\widehat{\Gamma} \longrightarrow \overline{\Gamma}$.

ex. 1) $\widehat{\mathbb{Z}} = \left\{ (x_k)_{k\geq 1} : x_k \in \mathbb{Z}/k,\ k_1 \mid k_2 \Rightarrow x_{k_2} = x_{k_1} \,(\mathrm{mod}\, k_1) \right\}$.

By Chineese Remainder Thm, $\mathbb{Z}/k = \prod_{i=1}^{s} \mathbb{Z}/p_i^{\alpha_i}$.

p-adic integers: $\mathbb{Z}_p = \left\{ (x_i)_{i\geq 0} : x_i \in \mathbb{Z}/p^i,\ x_j = x_i \,(\mathrm{mod}\, p^i) \text{ for } j > i \right\}$

$$\widehat{\mathbb{Z}} = \prod_{p\text{-prime}} \mathbb{Z}_p.$$

2) $\overline{SL_d(\mathbb{Z})} = \prod_{p\text{-prime}} SL_d(\mathbb{Z}_p)$.

For $d \geq 3$, the profinite completion of $SL_d(\mathbb{Z})$ coincides with the congruence completion.

Conj. (Serre) Let G be simply connected simple alg. group defined over $\mathbb{Q}$. Then

[the kernel of the map $\widehat{G(\mathbb{Z})} \to \overline{G(\mathbb{Z})}$ is finite] $\iff$ $\mathbb{R}$-rank $(G) \geq 2$.

Thm. (Rigidity) Let $\varphi: SL_d(\mathbb{Z}) \to SL_d(\mathbb{Z})$, $d \geq 3$, be a homeomorphism. Then $\exists$ algebraic homomorphism $\tilde{\varphi}: SL_d(\mathbb{C}) \to SL_d(\mathbb{C})$ such that $\tilde{\varphi} = \varphi$ on a (finite-index) subgroup of $SL_d(\mathbb{Z})$.

(sketch)

$\Gamma = SL_d(\mathbb{Z})$

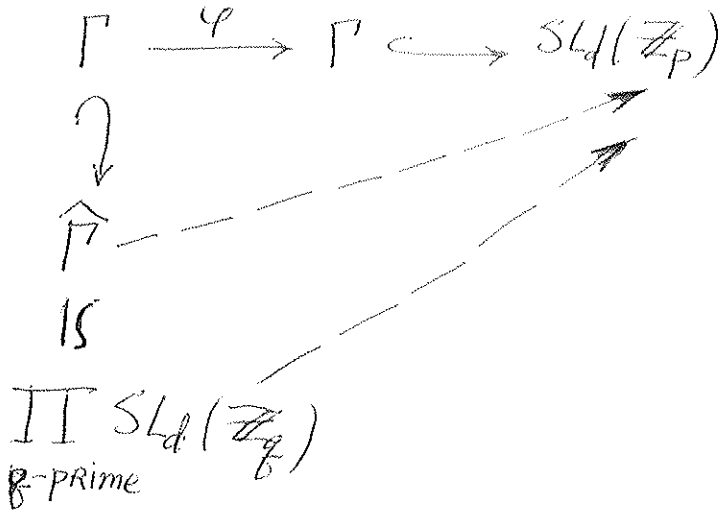
We have a map $\varphi: \Gamma \to SL_d(\mathbb{Z}_p)$

Equip Γ with the profinite metric and $SL_d(\mathbb{Z}_p)$ with the congruence metric. Then φ is uniformly continuous

[Lemma. If X_1 and X_2 are compact metric spaces and $\varphi: Y \to X_2$ a uniformly continuous map with $Y \subseteq_{\text{dense}} X_1$. Then φ extends to X_1, continuously.]

Therefore, φ extends to the map $\hat{\Gamma} \to SL_d(\hat{\mathbb{Z}})$ where $\hat{\Gamma}$ is the profinite completion of Γ.

CSP $\Rightarrow$ $\hat{\Gamma} \simeq \prod_{q\text{-prime}} SL_d(\mathbb{Z}_q)$.



Now it remains to classify continuous homomorphisms

$$SL_d(\mathbb{Z}_q) \longrightarrow SL_d(\mathbb{Z}_p).$$

Theory of (p-adic) Lie groups implies that every such homomorphism is polynomial.