Centrality of the Congruence Subgroup Kernel

T.N.Venkataramana

School of Mathematics,
Tata Institute of Fundamental Research, Mumbai
venky@math.tifr.res.in

ICERM June 14-18, 2021

Congruence Subgroups

$G \subset SL_n$ is a subgroup defined as the set of zeroes of a finite collection of polynomials P in the matrix entries X_{ij}, such that P have coefficients in $\mathbb{Q}$. Then G is said to be an algebraic group defined over $\mathbb{Q}$.

Congruence Subgroups

$G \subset SL_n$ is a subgroup defined as the set of zeroes of a finite collection of polynomials P in the matrix entries X_{ij}, such that P have coefficients in $\mathbb{Q}$. Then G is said to be an algebraic group defined over $\mathbb{Q}$.

For such a group G defined over $\mathbb{Q}$, let $\Gamma = G(\mathbb{Z}) = G \cap SL_n(\mathbb{Z})$. The subgroup of Γ of the form $g \in \Gamma : g \equiv 1(mod\ m)$ for some integer m is called the principal congruence subgroup of level m. It is the kernel to the map $G(\mathbb{Z}) \to G(\mathbb{Z}/m\mathbb{Z})$, and hence has finite index in Γ.

Congruence Subgroup Property

Definition

$\Gamma = G(\mathbb{Z})$ has the **congruence subgroup property** if every finite index subgroup of Γ contains a principal congruence subgroup.

Congruence Subgroup Property

Definition

$\Gamma = G(\mathbb{Z})$ has the **congruence subgroup property** if every finite index subgroup of Γ contains a principal congruence subgroup.

Easy to see: $SL_2(\mathbb{Z})$ does not have the congruence subgroup property. However, Mennicke and Lazard showed that for $n \geq 3$, and $g \geq 2$ the groups $SL_n(\mathbb{Z}), Sp_{2g}(\mathbb{Z})$ do have the congruence subgroup property. There is a slightly more general definition of the congruence subgroup property:

Weak Congruence Subgroup Property

A reformulation of the congruence subgroup property: let $\Gamma = G(\mathbb{Z})$ as before. Denote by $\widehat{\Gamma}$ the profinite completion of Γ. Denote by $\overline{\Gamma}$ the *congruence completion* of Γ, namely the inverse limit $\overline{\Gamma} = \varprojlim_{m \geq 2} \Gamma(\mathbb{Z}/m\mathbb{Z})$. By the universal property of profinite completions, there exists a surjective map $p : \widehat{\Gamma} \to \overline{\Gamma}$. The kernel C of p is called the congruence subgroup kernel. The congruence subgroup property is equivalent to saying that this map p is an isomorphism, i.e. that the congruence kernel is trivial.

Weak Congruence Subgroup Property

A reformulation of the congruence subgroup property: let $\Gamma = G(\mathbb{Z})$ as before. Denote by $\widehat{\Gamma}$ the profinite completion of Γ. Denote by $\overline{\Gamma}$ the *congruence completion* of Γ, namely the inverse limit $\overline{\Gamma} = \varprojlim_{m \geq 2} \Gamma(\mathbb{Z}/m\mathbb{Z})$. By the universal property of profinite completions, there exists a surjective map $p : \widehat{\Gamma} \to \overline{\Gamma}$. The kernel C of p is called the congruence subgroup kernel. The congruence subgroup property is equivalent to saying that this map p is an isomorphism, i.e. that the congruence kernel is trivial.

Definition

The group $\Gamma = G(\mathbb{Z})$ has the **weak congruence subgroup property** (shortened to CSP) if the kernel to the foregoing map $p : \widehat{\Gamma} \to \overline{\Gamma}$ is **finite**, i.e. the congruence subgroup kernel of Γ is finite.

Examples

A theorem of Bass, Milnor and Serre says that if $n \geq 3, g \geq 2$, and K is a totally imaginary number field, then the groups $SL_n(O_K), Sp_{2g}(O_K)$ satisfy the weak congruence subgroup property. They also showed that in this case, the congruence subgroup kernel is isomorphic to the group of roots of unity in the number field K, and is in particular, not trivial. If K is not totally imaginary, and if $n \geq 3$ and $g \geq 2$ (Bass-Milnor-Serre) then the groups $SL_n(O_K)$ and $Sp_{2g}(O_K)$ do have the congruence subgroup property: the congruence subgroup kernel is trivial.

Examples

A theorem of Bass, Milnor and Serre says that if $n \geq 3, g \geq 2$, and K is a totally imaginary number field, then the groups $SL_n(O_K), Sp_{2g}(O_K)$ satisfy the weak congruence subgroup property. They also showed that in this case, the congruence subgroup kernel is isomorphic to the group of roots of unity in the number field K, and is in particular, not trivial. If K is not totally imaginary, and if $n \geq 3$ and $g \geq 2$ (Bass-Milnor-Serre) then the groups $SL_n(O_K)$ and $Sp_{2g}(O_K)$ do have the congruence subgroup property: the congruence subgroup kernel is trivial.

Theorem

(Serre) If $G = SL_2$ over a number field K with infinitely many units, then CSP holds; the congruence subgroup kernel C is trivial unless K is totally imaginary, and when K is totally imaginary, C is isomorphic to the group of roots on unity in K.

Notion of Rank

If $G \subset SL_n$ is a linear algebraic group defined over $\mathbb{Q}$, a connected subgroup of G is called a $\mathbb{Q}$-split torus if T can be conjugated into the diagonals in SL_n by a matrix in $SL_n(\mathbb{Q})$. A maximal $\mathbb{Q}$-split torus in G is a $\mathbb{Q}$-split torus which is maximal with respect to this property; all maximal $\mathbb{Q}$-split tori are conjugate under $G(\mathbb{Q})$ and the dimension of a maximal $\mathbb{Q}$-split torus is called the $\mathbb{Q}$-rank of G.

Notion of Rank

If $G \subset SL_n$ is a linear algebraic group defined over $\mathbb{Q}$, a connected subgroup of G is called a $\mathbb{Q}$-split torus if T can be conjugated into the diagonals in SL_n by a matrix in $SL_n(\mathbb{Q})$. A maximal $\mathbb{Q}$-split torus in G is a $\mathbb{Q}$-split torus which is maximal with respect to this property; all maximal $\mathbb{Q}$-split tori are conjugate under $G(\mathbb{Q})$ and the dimension of a maximal $\mathbb{Q}$-split torus is called the $\mathbb{Q}$-rank of G.
One can similarly define the $\mathbb{R}$-rank of G.

The $\mathbb{Q}$-rank of SL_n is $n-1$; that of Sp_{2g} is g.

Notion of Rank

If $G \subset SL_n$ is a linear algebraic group defined over $\mathbb{Q}$, a connected subgroup of G is called a $\mathbb{Q}$-split torus if T can be conjugated into the diagonals in SL_n by a matrix in $SL_n(\mathbb{Q})$. A maximal $\mathbb{Q}$-split torus in G is a $\mathbb{Q}$-split torus which is maximal with respect to this property; all maximal $\mathbb{Q}$-split tori are conjugate under $G(\mathbb{Q})$ and the dimension of a maximal $\mathbb{Q}$-split torus is called the $\mathbb{Q}$-rank of G.
One can similarly define the $\mathbb{R}$-rank of G.

The $\mathbb{Q}$-rank of SL_n is $n-1$; that of Sp_{2g} is g.
If D is a central division algebra over $\mathbb{Q}$, then the $\mathbb{Q}$-rank of $G = SL_1(D)$ is zero.

Notion of Rank

If $G \subset SL_n$ is a linear algebraic group defined over $\mathbb{Q}$, a connected subgroup of G is called a $\mathbb{Q}$-split torus if T can be conjugated into the diagonals in SL_n by a matrix in $SL_n(\mathbb{Q})$. A maximal $\mathbb{Q}$-split torus in G is a $\mathbb{Q}$-split torus which is maximal with respect to this property; all maximal $\mathbb{Q}$-split tori are conjugate under $G(\mathbb{Q})$ and the dimension of a maximal $\mathbb{Q}$-split torus is called the $\mathbb{Q}$-rank of G.
One can similarly define the $\mathbb{R}$-rank of G.

The $\mathbb{Q}$-rank of SL_n is $n-1$; that of Sp_{2g} is g.
If D is a central division algebra over $\mathbb{Q}$, then the $\mathbb{Q}$-rank of $G = SL_1(D)$ is zero.
If q is a nondegenerate quadratic form with rational coefficients, then the $\mathbb{Q}$ rank of $SO(q)$ is the number r where $q = h \oplus \cdots \oplus h \oplus q'$ where q' does not represent a rational zero.

Serre's Conjecture

Serre's conjecture: if G is a ($\mathbb{Q}$-simple) algebraic group defined over $\mathbb{Q}$ and if $\mathbb{R} - rank(G) \geq 2$, then the congruence subgroup kernel C associated to $G(\mathbb{Z})$ is finite.

Serre's Conjecture

Serre's conjecture: if G is a ($\mathbb{Q}$-simple) algebraic group defined over $\mathbb{Q}$ and if $\mathbb{R} - rank(G) \geq 2$, then the congruence subgroup kernel C associated to $G(\mathbb{Z})$ is finite. That is, the weak congruence subgroup property holds for $G(\mathbb{Z})$.

Serre's Conjecture

Serre's conjecture: if G is a ($\mathbb{Q}$-simple) algebraic group defined over $\mathbb{Q}$ and if $\mathbb{R} - rank(G) \geq 2$, then the congruence subgroup kernel C associated to $G(\mathbb{Z})$ is finite. That is, the weak congruence subgroup property holds for $G(\mathbb{Z})$. For example, if Γ is a lattice in $SL_n(\mathbb{R})$ with $n \geq 3$, then Γ satisfies the weak congruence subgroup property.

Serre's Conjecture

Serre's conjecture: if G is a ($\mathbb{Q}$-simple) algebraic group defined over $\mathbb{Q}$ and if $\mathbb{R}-rank(G) \geq 2$, then the congruence subgroup kernel C associated to $G(\mathbb{Z})$ is finite. That is, the weak congruence subgroup property holds for $G(\mathbb{Z})$. For example, if Γ is a lattice in $SL_n(\mathbb{R})$ with $n \geq 3$, then Γ satisfies the weak congruence subgroup property. Results of Raghunathan and Gopal Prasad say that finiteness is equivalent to the congruence subgroup kernel being *central* in $\widehat{\Gamma}$. From now on , we will discuss the centrality of C.

Serre's Conjecture

Serre's conjecture: if G is a ($\mathbb{Q}$-simple) algebraic group defined over $\mathbb{Q}$ and if $\mathbb{R}-rank(G) \geq 2$, then the congruence subgroup kernel C associated to $G(\mathbb{Z})$ is finite. That is, the weak congruence subgroup property holds for $G(\mathbb{Z})$. For example, if Γ is a lattice in $SL_n(\mathbb{R})$ with $n \geq 3$, then Γ satisfies the weak congruence subgroup property. Results of Raghunathan and Gopal Prasad say that finiteness is equivalent to the congruence subgroup kernel being *central* in $\widehat{\Gamma}$. From now on , we will discuss the centrality of C.

Theorem

(Raghunathan 1976, 1984) Under the assumption of Serre's conjecture, if $G(\mathbb{R})/G(\mathbb{Z})$ is not compact (same as $\mathbb{Q}-rank(G) \geq 1$), then CSP holds.

Serre's Conjecture

Serre's conjecture: if G is a ($\mathbb{Q}$-simple) algebraic group defined over $\mathbb{Q}$ and if $\mathbb{R} - rank(G) \geq 2$, then the congruence subgroup kernel C associated to $G(\mathbb{Z})$ is finite. That is, the weak congruence subgroup property holds for $G(\mathbb{Z})$. For example, if Γ is a lattice in $SL_n(\mathbb{R})$ with $n \geq 3$, then Γ satisfies the weak congruence subgroup property. Results of Raghunathan and Gopal Prasad say that finiteness is equivalent to the congruence subgroup kernel being *central* in $\widehat{\Gamma}$. From now on , we will discuss the centrality of C.

Theorem

(Raghunathan 1976, 1984) Under the assumption of Serre's conjecture, if $G(\mathbb{R})/G(\mathbb{Z})$ is not compact (same as $\mathbb{Q} - rank(G) \geq 1$), then CSP holds.

CSP also known for many cocompact lattices, but not in general; lattices which arise as unit groups of orders in division algebras over $\mathbb{Q}$ of degree 3 are conjectured to have CSP.

Raghunathan proved that the congruence subgroup kernel is **central.** His proof was quite general when $\mathbb{Q} - rank(G) \geq 2$ (1976), but in the case of $\mathbb{Q} - rank$ 1 (1984), there was a quite elaborate case by case check.

Raghunathan proved that the congruence subgroup kernel is **central**. His proof was quite general when $\mathbb{Q}-rank(G) \geq 2$ (1976), but in the case of $\mathbb{Q}-rank$ 1 (1984), there was a quite elaborate case by case check.

I outline here a proof which is completely general (avoiding the case by case check) and does not depend on the $\mathbb{Q}$-rank (of course, $\mathbb{Q}-rank(G) \geq 1$ and $\mathbb{R}-rank(G) \geq 2$).

Raghunathan proved that the congruence subgroup kernel is **central.** His proof was quite general when $\mathbb{Q} - \mathit{rank}(G) \geq 2$ (1976), but in the case of $\mathbb{Q} - \mathit{rank}$ 1 (1984), there was a quite elaborate case by case check.

I outline here a proof which is completely general (avoiding the case by case check) and does not depend on the $\mathbb{Q}$-rank (of course, $\mathbb{Q} - \mathit{rank}(G) \geq 1$ and $\mathbb{R} - \mathit{rank}(G) \geq 2$).

The proof imitates Serre's proof of centrality when $G = SL_2$ over a number field K with infinitely many units (this corresponds to real rank at least two).

Serre's proof for SL_2

$G = SL_2$ over a number field K with infinitely many units, $G(\mathbb{Z})$ corresponds to $SL_2(O_K)$, O_K integers in K. The unit group H of K may be viewed as the group of diagonals $\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$ with u a unit of K.

Serre's proof for SL_2

$G = SL_2$ over a number field K with infinitely many units, $G(\mathbb{Z})$ corresponds to $SL_2(O_K)$, O_K integers in K. The unit group H of K may be viewed as the group of diagonals $\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$ with u a unit of K.

For an integer m, $E(m)$ is the (normal in $SL_2(O_K)$) subgroup generated by the elementary matrices in $U^{\pm}(O_K)$ ($U^{\pm}$ are upper and lower triangular unipotent matrices) which are congruent to identity modulo m, and $\Gamma(m)$ the smallest congruence subgroup containing $E(m)$.

Serre's proof for SL_2

$G = SL_2$ over a number field K with infinitely many units, $G(\mathbb{Z})$ corresponds to $SL_2(O_K)$, O_K integers in K. The unit group H of K may be viewed as the group of diagonals $\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$ with u a unit of K.

For an integer m, $E(m)$ is the (normal in $SL_2(O_K)$) subgroup generated by the elementary matrices in $U^{\pm}(O_K)$ ($U^{\pm}$ are upper and lower triangular unipotent matrices) which are congruent to identity modulo m, and $\Gamma(m)$ the smallest congruence subgroup containing $E(m)$.

The congruence subgroup kernel C is the inverse limit of the groups $G(m)/E(m)$ as m varies. Serre shows that to check centrality of C, it is enough to check that a **fixed** subgroup of finite index in the unit group $H(\mathbb{Z})$ acts trivially on **all the** $\Gamma(m)/E(m)$.

Serre's proof

If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ lies in $\Gamma(m)/E(m)$, then easy to show: conjugation action by the congruence subgroup $H(a)$ fixes g:

$$\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 \\ (u^{-2} - 1)\frac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \frac{b}{a}(u^2 - 1) \\ 0 & 1 \end{pmatrix}$$

Serre's proof

If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ lies in $\Gamma(m)/E(m)$, then easy to show: conjugation action by the congruence subgroup $H(a)$ fixes g:

$$\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 \\ (u^{-2} - 1)\frac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \frac{b}{a}(u^2 - 1) \\ 0 & 1 \end{pmatrix}$$

But can replace g by another matrix by multiplying by an element of $E(m)$:

$$g' = g \begin{pmatrix} 1 & 0 \\ mx & 0 \end{pmatrix} = \begin{pmatrix} a + bmx & b \\ c' & d \end{pmatrix} \equiv g \in \Gamma(m)/E(m),$$

and get: $H(a + bmx)$ also fixes $g \in \Gamma(m)/E(m)$.

(Fact) The group generated by these congruence subgroups $H(a+bmx)$ (as x varies through integers) is a *fixed* congruence subgroup Δ independent of a, b and m and hence Δ acts trivially on C; this implies, by the simplicity of $SL_2(K)$, that all of $SL_2(K)$ acts trivially.

(Fact) The group generated by these congruence subgroups $H(a+bmx)$ (as x varies through integers) is a *fixed* congruence subgroup Δ independent of a, b and m and hence Δ acts trivially on C; this implies, by the simplicity of $SL_2(K)$, that all of $SL_2(K)$ acts trivially.

Serre's proof of the fact uses some number theory (Artin reciprocity).

Serre's proof can be generalised; there is the notion of elementary matrices, namely unipotent elements in two fixed opposing unipotent radicals $U^{\pm}$ of two parabolic subgroups $P^{\pm}$; the torus group H can be replaced by the Levi group H belonging to $P \cap P^{-}$.

general result

The proof in the general case uses the following result (H is analogous to the unit group used by in Serre's proof, but groups other than units are involved):

Theorem

$H \subset SL_n$ is an algebraic group defined over $\mathbb{Q}$, $N \geq 1$ fixed. For each pair a, b of coprime integers, $H_{a,b}$ is the subgroup generated by the congruence groups $H((a+bx)^N)$ as x varies. There is a fixed congruence subgroup Δ of $H(\mathbb{Z})$ such that $\Delta \subset H_{a,b}$ for each a, b.

The proof is an application of Dirichlet's theorem on infinitude of primes in arithmetic progressions.

The proof of the independence (from a, b, m) of the congruence subgroup Δ in $H(\mathbb{Z})$ is "theoretical" but I don't know the precise index of Δ in $H(\mathbb{Z})$. Calculations by hand show that the index is quite small.

The proof of the independence (from a, b, m) of the congruence subgroup Δ in $H(\mathbb{Z})$ is "theoretical" but I don't know the precise index of Δ in $H(\mathbb{Z})$. Calculations by hand show that the index is quite small. The index is related to the following problem (replacing $(a+bX)^N$ by any polynomial):
Given a polynomial $P \in \mathbb{Z}[X]$ of degree N such that the gcd of its coeficients is one, and given coprime integers a, b set (ϕ is Euler's ϕ function)

$$g_P = g.c.d\{\phi(P(x)); x \in \mathbb{Z}\}$$

.
(Problem) Is it true that there exists a constant g dependent only on the degree N such that $g_P \leq g$.

The proof of the independence (from a, b, m) of the congruence subgroup Δ in $H(\mathbb{Z})$ is "theoretical" but I don't know the precise index of Δ in $H(\mathbb{Z})$. Calculations by hand show that the index is quite small. The index is related to the following problem (replacing $(a+bX)^N$ by any polynomial):

Given a polynomial $P \in \mathbb{Z}[X]$ of degree N such that the gcd of its coeficients is one, and given coprime integers a, b set (ϕ is Euler's ϕ function)

$$g_P = g.c.d\{\phi(P(x)); x \in \mathbb{Z}\}$$

.

(Problem) Is it true that there exists a constant g dependent only on the degree N such that $g_P \leq g$.

true if P has degree one (Serre's proof uses this). True for $N = 2$ (recent paper of Soundararajan). Sound shows true in general if a known conjecture in number theory (Schinzel's hypothesis) is assumed.

Thank you for your attention.