Proc. Indian Acad. Sci. (Math. Sci.) Vol. 114, No. 4, November 2004, pp. 299–308.

The congruence subgroup problem*

M S RAGHUNATHAN

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Mumbai 400 005, India
E-mail: msr@math.tifr.res.in

MS received 22 July 2004

Abstract. This is a short survey of the progress on the congruence subgroup problem since the sixties when the first major results on the integral unimodular groups appeared. It is aimed at the non-specialists and avoids technical details.

Keywords. Algebraic groups; arithmetic groups; congruence groups.

The group $SL(2, \mathbb{Z})$ of 2×2 integral matrices of determinant 1 is a group that crops up in different contexts in mathematics. Its structure is understood. The group has a natural family of normal subgroups (of finite index). If $I \subset \mathbb{Z}$ is a proper non-zero ideal, the subgroup $\{g \in SL(2, \mathbb{Z}) | g \equiv 1 (\bmod I)\}$ is a subgroup of finite index which we will denote as $SL(2, I)$.

It is in fact the kernel of the natural homomorphism of $SL(2, \mathbb{Z})$ into the finite group $SL(2, Z/I)$. Towards the end of the 19th century, the question was raised if there were other examples of normal subgroups of finite index; and Fricke–Klein exhibited such subgroups. It turns out that there is a *surjective* homomorphism φ: $SL(2, \mathbb{Z}) \to A_5$ (alternating group on 5 symbols. Let $\Gamma =$ kernel φ.

Claim. The group Γ cannot contain a subgroup of the form $SL(2, I)$.

In what follows (k) will denote $k\mathbb{Z}$. If $I = n\mathbb{Z}, n > 0$ and $n = \prod_p p^{\alpha_p}$ is the prime factorization of $n, SL(2, \mathbb{Z}/n\mathbb{Z}) = \prod_p SL(2, \mathbb{Z}/(p^{\alpha_p}))$. The natural map $SL(2, \mathbb{Z}) \to S(2, \mathbb{Z}/n\mathbb{Z})$ is surjective. So any simple quotient of $SL(2, \mathbb{Z})$ is a quotient of $SL(2, \mathbb{Z}/(p^{\alpha_p}))$ for some prime p. Now the kernel of the map $SL(2, \mathbb{Z}/(p^{\alpha_p})) \to SL(2, \mathbb{Z}/(p))$ is a p-group and $SL(2, \mathbb{Z}/(p))/(\pm Id)$ is simple and non-abelian if $p \neq 2$ or 3. We conclude that any simple quotient of $SL(2, \mathbb{Z})/I$ is of the form $SL(2, \mathbb{Z}/(p))/(\pm Id)$ for some prime $p > 3$.

On the other hand, A_5 is not isomorphic to $SL(2, \mathbb{Z}/(p))$ for any prime p.

The order of $SL(2, \mathbb{Z}/(p)) = (p-1) \cdot p \cdot (p+1)$. So $SL(2, \mathbb{Z}/(p)) \not\simeq A_5$ unless $p = 5$. The two sylow subgroup of $SL(2, \mathbb{Z}/(p))$ is cyclic while that of A_5 is $\mathbb{Z}/2 \times \mathbb{Z}/2$. So kernel φ does not contain any $SL(2, I)$ with I a proper non-zero ideal.

This phenomenon raises the following question. First, a definition.

*This is essentially a transcript of the plenary talk given at the Joint India–AMS Mathematics Meeting held in December 2003 in Bangalore, India.

A subgroup $\Gamma \subset SL(n, \mathbb{Z})$ (n integer ≥ 2) is a *congruence subgroup* iff there is a proper non-zero ideal $I \subset \mathbb{Z}$ such that $\Gamma \supset SL(n, I) = \{g \in SL(n, \mathbb{Z}) | g \equiv 1(\text{mod } I)\}$.

Are there subgroups Γ of finite index (note that $SL(n, I)$ has finite index in $SL(n, \mathbb{Z})$) which are not congruence subgroups?

We saw above that the answer is 'yes' when $n = 2$.

In 1962, Bass–Lazard–Serre and independently Mennicke discovered that $SL(2, \mathbb{Z})$ is exceptional. They proved the following theorem.

Theorem. *If $n > 2$, every subgroup of finite index in $SL(n, \mathbb{Z})$ is a congruence subgroup.*

The problem can be generalized. One can pose it for other groups of integral matrices such as symplectic ones or orthogonal ones (for a quadratic form over $\mathbb{Z}$). One may also replace $\mathbb{Z}$ by integers in a number field or S-integers for a *set S of primes* including all the archimedean primes.

We will now give a very general formulation. Apart from the fact that many naturally arising examples fall within the ambit of this formulation, the formulation suggests techniques for the attack that the special cases may not suggest that readily. For the general formulation we introduce the following notations: k will be a number field; V, a complete set of mutually inequivalent valuations of k; ∞, the set of archimedean valuations; S, a subset of V containing ∞.

For $v \in V \backslash \infty$, k_v is the completion of k at v, $\mathcal{O}_v =$ integers in k_v, $\mathcal{O}_S = \{x \in k | x \in \mathcal{O}_v \text{ for } v \notin S\}$, the ring of S-integers in k, $\mathcal{O} = \mathcal{O}_\infty =$ integers in k (when $k = Q$, $\mathcal{O} = \mathbb{Z}$).

Next we recall the definition of a linear algebraic group defined over k. We regard k as a subfield of $\mathbb{C}$. A linear algebraic group G (defined) over k is a subgroup of $GL(n, \mathbb{C})$ which is also the set of zeros of a (finite) collection of functions on $GL(n, \mathbb{C})$ of the form $P(g_{ij}, \det g^{-1})$ where $g = (g_{ij})_{1 \leq i,j \leq n} \in GL(n, \mathbb{C})$ and P is a polynomial in $(n^2 + 1)$ variables with *coefficients in k*. We will call G a k-algebraic group or simply a k-group. We denote by $G(k)$ the group $G \cap GL(n, k)$.

Examples.

1. $GL(n, \mathbb{C})$ is evidently one (over any k).
2. $SL(n, \mathbb{C}) = \{g \in GL(n, \mathbb{C}) | \det\ g = 1\}$.
3. $D(n) = \{g \in GL(n, \mathbb{C}) | g_{ij} = 0 \quad \text{for } i \neq j\}$.
4. The group of upper triangular matrices in $GL(n)$.
5. The group of upper triangular matrices with all diagonal entries equal to 1.
6. Let F be a symmetric non-singular $n \times n$ matrix over k and
$$O(F) = \{g \in GL(n, \mathbb{C}) | {}^t g F g = F\}.$$
The orthogonal group of F is a k-group.
7. $SO(F) = \{g \in O(F) | \det\ g = 1\}$.
8. In Example 6, if one takes $n = 2$ and $F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, then $a \mapsto \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ gives an isomorphism of $D(1)$ on $SO(F)$.
9. Note that the algebraic group
$$\{g \in GL(n, \mathbb{C}) | g_{ij} - \delta_{ij} = 0 \quad \text{for } i \neq 1, g_{11} = 1\}$$
is isomorphic to $\mathbb{C}^{n-1}$ – again a group over any k.

10. Let D be a division algebra over k and $e_1, e_2, \ldots, e_{d^2}$ a basis of D over k. Then $e_1, e_2, \ldots, e_{d^2}$ is a basis over $\mathbb{C}$ of $D \otimes_k \mathbb{C}$. Let R_i denote the multiplication by e_i on the right

$$R_i \colon D \otimes_k \mathbb{C} \to D \otimes_k \mathbb{C};$$

they are elements of $GL(d^2, \mathbb{C})$. Define $G = \{g \in GL(d^2, \mathbb{C}) | gR_i = R_i g$ for all $i, 1 \leq i \leq d^2\}$. This is an algebraic group over k.

We now make the definition.

DEFINITION 1

A subgroup Γ of $G(k)$ is a S-*congruence* subgroup if it contains a subgroup of the form $G \cap GL(n, I)$ with I a proper non-zero ideal in $\mathcal{O}_S$, as a subgroup of finite index. Note that $\mathcal{O}_S/I$ is finite so that $G \cap GL(n, I)$ has finite index in $G \cap GL(n, \mathcal{O}_S)$; thus $GL(n, I) \cap G$ is an S-arithmetic subgroup (see Definition below).

DEFINITION 2

A subgroup Γ of $G(k)$ is a S-arithmetic subgroup if for some (hence any) S-congruence subgroup Γ' of $G(k)$, $\Gamma \cap \Gamma'$ has finite index in both Γ and Γ'.

We say that subgroups H_1, H_2 of a group H are *commensurable* iff $H_1 \cap H_2$ has finite index in both H_1 and H_2.

A k-morphism of a k-group $G \subset GL(n, \mathbb{C})$ into a k-group G' in $GL(n', \mathbb{C})$ is a group morphism $f \colon G \to G'$ such that for every (i', j'), $1 \leq i', j' \leq n'$, the (i', j')th entry $f_{i'j'}(g)$ of $f(g)$ and $\det f(g)^{-1}$ are polynomials with coefficients in k in the entries g_{ij}, $1 \leq i, j \leq n$ of g and $\det g^{-1}$: $f_{i'j'}(g) = P_{i'j'}(g_{ij}, \det\, g^{-1}) \det\, f(g)^{-1} = D(g_{ij}, \det\, g^{-1})$. Note that these are polynomials in $(g_{ij} - \delta_{ij})$ and $(\det\, g^{-1} - 1)$ as well.

Lemma. The inverse image in $G(k)$ of an S-congruence (*resp. S-arithmetic*) *subgroup of $G'(k)$ under a k-morphism $f \colon G \to G'$ is a S-congruence* (*resp. S-arithmetic*) *subgroup of $G(k)$.*

Note that $f(G(k)) \subset G(k')$.

Let

$$f_{i'j'}(g) = Q_{ij}(g_{ij} - \delta_{ij}, \det\, g^{-1} - 1)$$

and

$$\det\, f(g^{-1}) = D'(g_{ij} - \delta_{ij}, \det\, g^{-1} - 1).$$

Let

$$\{c_i = a_i/b_i | i \in E, a_i \in \mathcal{O}_S, b_i \in \mathcal{O}_S, b_i \neq 0\}$$

be the collection of all the (non-zero) coefficients of Q_{ij} and D'. Let J' be a proper non-zero ideal in $\mathcal{O}_S$ and $J = (\prod_{i \in I} c_i) \cdot J'$. Then one sees immediately that

$$f(G \cap GL(n, J)) \subset G' \cap GL(n, J').$$

Hence the lemma.

Consequence. The notions of S-arithmetic and S-congruence subgroups of $G(k)$ depend only on the k-isomorphism class of G (not on the realisation of G as a k-subgroup of $GL(n, \mathbb{C})$). Then the congruence subgroup problem is:

Question. Is every S-arithmetic subgroup of G a S-congruence subgroup?

The case $k = Q$ and $S = \infty$ is itself sufficiently challenging; so if you are not comfortable with the more general situation, you can make the assumption $k = Q$, $S = \infty$. In this case $\mathcal{O}_S = \mathbb{Z}$. In the other extreme case when $S = V$, $\mathcal{O}_S = k(= Q$ if $k = Q)$. We saw above that the answer is, 'No', for $k = Q$, $S = \infty$ and $G = SL(2, \mathbb{C})$, 'Yes', for $k = Q$, $S = \infty$ and $G = SL(n, \mathbb{C})$, $n > 2$.

Very substantial progress has been made on this general question. To describe the progress, we first describe a way of measuring the failure of an affirmative answer to the above question formulated by Serre. We make the group $G(k)$ into a topological group in two different ways. Let $\mathcal{A}_S$ (resp. $\mathcal{C}_S$) be the collection of all S-arithmetic (resp. S-congruence) subgroups in $G(k)$ and $\mathcal{J}_{a,S}$ (resp. $\mathcal{J}_{c,s}$) the topology of the unique structure of a topological group on $G(k)$ for which $\mathcal{A}_S$ (resp. $\mathcal{C}_S$) is a fundamental system of neighbourhoods of the identity. Let $\widehat{G}_{a,S}$ (resp. $\widehat{G}_{c,S}$) be the completion of $G(k)$ with respect to the natural (left-invariant) uniform structure. Since $\mathcal{J}_{c,S}$ is weaker than $\mathcal{J}_{a,S}$, the identity map as a map of $G(k)$ is uniformly continuous from the topology $\mathcal{J}_{a,S}$ to the topology $\mathcal{J}_{c,S}$. Consequently the identity map extends to a continuous homomorphism of $\widehat{G}_{a,S}$ on $\widehat{G}_{c,S}$. We have a commutative diagram

$$\begin{tikzcd}
\widehat{G}_{a,S} \arrow[rr, "\pi"] & & \widehat{G}_{c,S} \\
& G(k) \arrow[ul, hook] \arrow[ur, hook] &
\end{tikzcd}.$$

It turns out that π is surjective and kernel $\pi := C(S, G)$ is compact and totally disconnected. Evidently $C(S, G)$ provides a measure of the failure of the family of S-arithmetic groups coinciding with the family of S-congruence subgroups.

From the definitions it is not difficult to see that $C(S, G)$ is contained in $\widehat{G}_a(\mathcal{O}_S)$, the closure of $G(\mathcal{O}_S) = G \cap GL(n, \mathcal{O}_S)$ in $\widehat{G}_{a,S}(k)$ and is thus the kernel of $\widehat{G}_a(\mathcal{O}_S) \to \widehat{G}_c(\mathcal{O}_S)$ (= closure of $G(\mathcal{O}_S)$ in $\widehat{G}_{c,S}(k)$). Because of this one is able to conclude that $C(S, G)$ is totally disconnected and compact: $\widehat{G}_a(\mathcal{O}_S)$ is the profinite completion of $G(\mathcal{O}_S)$. We now pose the *congruence subgroup problem*:

$$\text{Determine } C(S, G) \tag{P}$$

for a given G and S.

Observe that $C(S, G)$ is trivial iff every S-arithmetic subgroup is a S-congruence subgroup. Consider the extreme case $S = V$. Here $\mathcal{O}_S = k$; and k has no proper non-zero ideals. So $\mathcal{O}_S = \{G(k)\}$. Thus $C(S, G)$ is trivial if and only if $G(k)$ has no proper (normal) subgroups of finite index. It is not difficult to see that $G = GL(1)$ has lots of subgroups of finite index; so $C(V, G)$ in general is non-trivial. However $C(V, G)$ has been conjectured to be trivial under some natural restrictions on G (Platonov–Margulis conjecture).

The problem for general G can be reduced to G of a special kind using the elaborate structure theory of linear algebraic k-groups.

Observe that $G \mapsto C(S, G)$ is a functor from the category of k-groups into the category of compact totally disconnected ($\equiv$ profinite) groups.

Lemma 1. *If G^o is the connected component of the identity in G, G^o is a k-group and the map $C(S, G^o) \to C(S, G)$ is an isomorphism.*

Lemma 2. *If a k-group G is a semidirect product $(B \cdot N)$ with B and N k-subgroups and N normal in G and $C(S, N)$ is trivial, then the map $C(S, B) \to C(S, G)$ is an isomorphism.*

Lemma 2 combined with the structure theory of k-groups enables one to reduce the problem to the case of *reductive* groups. A (connected) k-group G is *reductive* if it has no connected normal subgroups consisting entirely of unipotent elements (unipotent $\equiv$ all eigenvalues are 1). It is a basic theorem that any k-group G is the semidirect product of a reductive k-group B and the maximum normal unipotent subgroup $R_u G$ (called the unipotent radical of G) which is a k-group.

A unipotent k-group U is a semidirect product $B \cdot U'$ where $\dim U' = \dim U - 1$ and $B \simeq \text{Add} = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| \, x \in \mathbb{C} \right\} \subset GL(2, \mathbb{C})$.

Now $C(S, \text{Add})$ is trivial (an easy exercise).

An induction on dimension shows that $C(S, G)$ is trivial if G is unipotent (i.e. consists entirely of unipotent matrices). Lemma 2 thus reduces our problem to the case of reductive G.

A k-group T is a *torus* if it is connected and can be conjugated into diagonal matrices in $GL(n, \mathbb{C})$.

It is again a basic result that if G is a reductive k-group, G contains a central k-torus T such that G/T has no connected abelian normal subgroups. Information on T and G/T separately can be pieced together to obtain results on G: this is somewhat delicate though. We will now deal with k-tori. These are abelain but they need much more subtle handling than unipotent groups. One has the following:

Theorem (Chevalley). $C(S, G) = \{1\}$ *if S is finite and G is a torus.*

This is false if S is infinite. However one knows the structure of T in sufficient detail to get considerable information on $C(S, G)$ in this case too. Chevalley's theorem as also other information on $C(S, G)$ for S infinite needs some class field theory.

I will now say something on the most important case: G semisimple, i.e. G has no non-trivial connected abelian normal subgroups. We will make two more assumptions viz. that G is simply connected and that G is absolutely almost simple – the latter means that G has no proper connected normal subgroups. This last assumption is not really restrictive but simple connectivity is. However information in the simply connected case can be effectively used to handle the general case. To explain what is expected to be true, I need to introduce some other concepts.

A k-split torus T is k-torus k-isomorphic to the group $D(n)$ of all diagonal matrices in $GL(n)$ for some n.

It is a theorem of Borel–Tits that all maximal k-split tori in a k-group G are mutual conjugates under $G(k)$ and their common dimension is called the k-rank of G. It is again a theorem of Borel–Tits that k-rank $G \geq 1$ iff $G(k)$ has non-trivial unipotent elements.

The S-rank of G is the number $\sum_{v \in S} k_v$-rank G.

One expects the following: Assume S is such that k_v-rank $G > 0$ for all $v \in S \backslash \infty$ and S-rank $G \geq 2$. Then $C(S, G)$ is trivial or isomorphic to the group μ_k of roots of unity in k.

Note that k_v-rank and S-rank $SL(n) \geq 2$ for any v and any S for $n \geq 3$. It is now known that the expectation is indeed true for any G with k-rank $G \geq 1$ (Bass, Lazard, Milnor, Serre, Mennicke, Matsumoto, Deodhar, Vaserstein, Bak, Rehman, Prasad and Raghunathan). The strategy in all this work has been to break the proof into two parts.

(1) Show that

$$1 \to C(S, G) \to \widehat{G}_{a,S}(k) \to \widehat{G}_{c,S}(k) \to 1$$

is a central extension.

This has the consequence that $C(S, G)$ is the Pontrjagin dual of the kernel of the map

$$H^2(\widehat{G}_{c,S}(k), \mathbb{Q}/\mathbb{Z}) \to H^2(G(k), \mathbb{Q}/\mathbb{Z}).$$

The first group is the cohomology group based on continuous co-chains, the second is the usual group cohomology.

(2) Show that the above kernel is μ_k or trivial.

The latter programme has in fact been carried out for all G (Moore, Matsumoto, Deodhar, Prasad, Raghunathan and Rapinchuk).

The centrality of the sequence in (1) above has also been settled in many cases of k-rank 0 (groups of type B_n, C_n, D_n and some exceptional groups) (Kneser, Rapinchuk and Tomanov). The case $S = V$ for anisotropic G is much more delicate than for isotropic G. The first results here are due to Kneser. Anisotropic groups of type A_1 were dealt with by Platonov, Rapinchuk and Margulis. Groups of type B_n, C_n, D_n and some exceptional groups have been dealt with (Ĉernusov, Rapinchuk, Sury and Tomanov). Groups of type A_n pose the greatest challenge. For *inner* forms of A_n and $S = V$, $C(V, G)$ has been determined. One can reformulate this as follows: Let D be a central division algebra over k. Let D^1 = the group of reduced norm 1 elements in D. Let $S_0 = \{v \in V \backslash \infty | D \otimes_k k_v = D_v$ is a division algebra$\}$. Let $D^1 \hookrightarrow \prod_{v \in S_0} D_v^*$ be the diagonal imbedding. The (locally compact) topology on $\prod_{v \in S_0} D_v^*$ induces a topology on D^1. Then any normal subgroup of D^1 is either central (and finite) or is open in the above topology. (This is the result of the work of Platonov, Rapinchuk, Margulis, Segev, Seitz and Raghunathan). In the k-rank ≥ 1 situation the presence of unipotent subgroups holds the key to the problem. In the case of groups of type B_n, C_n, D_n one exploits the presence of *reflections* in these groups.

The cohomology computations were carried out in classical cases by using the work of Moore. The general situation needs some more refined machinery – the Bruhat–Tits theory of buildings associated to groups over local fields.

If one knows the expectation to hold for an S, it will hold for larger S. So the aim would be to handle finite S.

The techniques used to handle the case $S = V$ can be used to handle some kinds of S: for example if K is a finite extension and $S = \{v \in V | K$ does not split completely in $v\}$, then $C(S, G) = 1$ if G is of inner type A_n (and k-rank $G = 0$).

When S-rank $G = 0$, any S-arithmetic group is finite and $C(S, G)$ is trivial.

In the case of S-rank $G = 1$ some partial results are known. One expects that $C(S, G)$ in this case is infinite. And this has been shown to hold in many (classical) cases. One method is to use the following result: if $C(S, G)$ is finite then Γ^{ab} is finite for any S-arithmetic Γ. One exhibits then S-arithmetic Γ in certain G with Γ^{ab} infinite thereby showing $C(S, G)$ is not finite.

Going back to cohomology computations, one has a good understanding of the group $\widehat{G}_{c,S}(k)$. It is a 'restricted direct product' of $G(k_v)$, $v \notin S$. Here $G(k_v)$ is the group of the k_v-points, k_v being the (locally compact) completion of k at v and $G(k_v)$ is the group of k_v-points of G equipped with its natural locally compact topology. This reduces the computations to that of $H^2(G(k_v), \mathbb{Q}/\mathbb{Z})$. Moore carried out the computations in the case when G is split and Deodhar when G is quasi-split. For dealing with the general case one uses the Bruhat–Tits buildings: These are *contractible* simplicial complexes on which $G(k_v)$ acts. One compares the cohomology of $G(k_v)$ with that of an imbedded quasi-split subgroup $H(k_v) \subset G(k_v)$.

Evidently this gets too technical to interest a general audience.

References

I give below a fairly comprehensive list of references dealing with the congruence subgroup problem. In the main body of the paper the precise references are not given – only names of some authors are mentioned. References 59 and 63 below are detailed surveys.

[1] Bak A, Le probléme des sous-groupes de congruences et le probléme metaplectique pour les groupes classiques de rang > 1, *C.R. Acad. Sci. Paris* **292** (1981) 307–310

[2] Bak A and Rehmann U, The congruence subgroup and metaplectic problems for $SL_{n\geq 2}$ of division algebras, *J. Algebra* **78** (1982) 475–547

[3] Bass H, Lazard M and Serre J-P, Sous-groupes d'indices finis dans $SL(n, \mathbb{Z})$, *Bull. Am. Math. Soc.* **70** (1964) 385–392

[4] Bass H, Milnor J and Serre J-P, Solution of the congruence subgroup problem for $SL_n (n \geq 3)$ and $Sp_{2n} (n \geq 2)$, *Pub. Math. IHES* **33** (1967) 59–137; see also **44** (1974) 241–244

[5] Borel A, Introduction aux groupes arithmétiques (Paris: Hermann) (1969)

[6] Borel A and Harish-Chandra, Arithmetic subgroups of algebraic groups, *Ann. Math.* **75** (1962) 485–535

[7] Borel A and Tits J, Groupes Réductifs, *Publ. Math. IHES* **27** (1965) 55–110

[8] Borovoi M V, Abstract simplicity of some simple anisotropic algebraic groups over number fields, *Sov. Math. Dokl.* **32** (1985) 191–193

[9] Birtto J, On defining a subgroup of the special linear group by a congruence, *J. Ind. Math. Soc.* **40** (1976) 235–243

[10] Bruhat F and Tits J, Groups réductifs sur un corps local, I: Données radicielles valuéés, *Publ. Math. IHES* **41** (1972) 5–251; II: Schémas en groupes. Existence d'une donnée radicielles, *Publ. Math. IHES* **60** (1984) 5–184

[11] Ĉernusov V, On the projective simplicity of certain groups of rational points over algebraic number fields, *Math. USSR Izv.* **34** (1990) 409–423

[12] Chevalley C, Sur certains groupes simples, *Tohoku J. Math.* **7(2)** (1955) 14–62

[13] Chevalley C, Deux théorèmes d'arithmétiques, *J. Math. Soc. Japan* **3** (1951) 36–44

[14] Corlette K, Archimedean super-rigidity and hyperbolic geoemetry, *Ann. Math.* **135** (1992) 165–182

[15] Delaroche C and Kirillov A, Sur les relations entrel'espace dual d'un groupe et la structure de ses sous-groupes fermés, Exposé 343, Séminaire Bourbaki (1967–68)

[16] Deligne P, Extensions centrales non résiduellement finis de groupes arithmétiques, *C.R. Acad. Sci. Paris, Ser A-B* **287(4)** (1978) A203–208
[17] Deodhar V V, On central extensions of rational points of algebraic groups, *Am. J. Math.* **100** (1978) 303–386
[18] Dickson L E, Linear group (Leipzig: Teubner) (1901)
[19] Dieudonné J, La géometrie des groupes classiques (Berlin: Springer-Verlag) (1955)
[20] Fricke R and Klein F, Vorlesungen über die Theorie der automorphen Funktionen, Band I: Die gruppentheoretischen Grundlagen, Band II: Die funktionentheoretischen Ausführungen und die Andwendungen (German) (Stuttgart: B.G. Teubner Verlagsgesellschaft) (1965)
[21] Harder G, Minkowskische Reduktionstheorie über Funktionenkörpern, *Invent Math.* **7** (1969) 33–54
[22] Kazhdan D A, On the connection between the dual space of the group with the structure of the closed subgroups, *Funct. Anal. Appl.* **1** (1967) 71–74 (Russian)
[23] Kazhdan D A, Some application of the Weil representation, *J. Analyse Mat.* **32** (1977) 235–248
[24] Kazhdan A A and Bernstein I N, The one-dimensional cohomology of discrete subgroups (Russian), *Funkcional. Anal. i Pril.* **4** (1970) 1–5
[25] Kneser M, Orthogonale Gruppen über algebraischen Zahlkörpern, *Crelles J.* **196** (1956) 213–220
[26] Kneser M, Normalteiler ganzzahliger Spingruppen, *Crelles J.* **311/312** (1979) 191–214
[27] Kostant B, On the existence and irreducibility of certain series of representation, *Bull. Am. Math. Soc.* **75** (1969) 627–642
[28] Li J-S, Non-vanishing theorems for the cohomology of some arithmetic quotients, *J. Reine Angew. Math.* **428** (1992) 111–217
[29] Lubotzky A, Group presentation, p-adic analytic groups and lattices in $SL(2, \mathbb{C})$, *Ann. Math.* **118** (1983) 115–130
[30] Margulis G A, Arithmetic properties of discrete groups, *Russian Math. Surveys* **29** (1974) 107–165
[31] Margulis G A, Arithmeticity of non-uniform lattices in weakly non-compact groups (Russian), *Funkcional Anal. i Prilozen* **9** (1975) 35–44
[32] Margulis G A, Arithmeticity of the irreducible lattices in the semisimple groups of rank greater than 1, *Inv. Math.* **76** (1984) 93–120
[33] Margulis G A, Finiteness of quotient groups of discrete subgroups, *Funct. Anal. Appl.* **13** (1979) 178–187
[34] Margulis G A, On the multiplicative group of a quaternion algebra over a global field, *Soviet Math. Dokl.* **21** (1980) 780–784
[35] Matsumoto H, Sur les groupes arithmétiques des groupes semisimples déployés, *Ann. Sci. Ecole Norm. Sup. (4^e ser.)* **2** (1969) 1–62
[36] Mennicke J, Finite factor groups of the unimodular groups, *Ann. Math.* **81** (1965) 31–37
[37] Mennicke J, Zur Theorie der Siegelschen Modulgruppe, *Math. Annalen.* **159** (1965) 115–129
[38] Millson J, Real vector bundles with discrete structure group, *Topology* **18** (1979) 83–89
[39] Millson J, On the first Betti number of constant negatively curved manifolds, *Ann. Math.* **104** (1976) 235–247

[40] Moore C C, Extensions and low dimensional cohomology theory of locally compact groups I and II, *Trans. Am. Math. Soc.* **113** (1964) 40–86; III, *Trans. Am. Math. Soc.* **221** (1976) 1–38
[41] Moore C C, Group extensions of p-adic and adelic groups, *Publ. Math. IHES* **35** (1969) 5–70
[42] Platonov V P, The problem of strong approximation and the Kneser–Tits conjecture for algebraic groups, *Math. USSR Izv.* **3** (1969) 1139–1147
[43] Platonov V P, Arithmetic and structure problems in linear algebraic groups, *Proc. ICM Vancouver* **1** (1974) 471–476
[44] Platonov V P, The Tannaka–Artin problem, *Sov. Math. Dokl.* **16** (1975) 468–473
[45] Platonov V P and Rapinchuk A S, Algebraic groups and number theory (Academic Press) (1991)
[46] Platonov V P and Rapinchuk A S, On the group of rational points of three dimensional groups, *Sov. Math. Dokl.* **20** (1979) 693–697
[47] Platonov V P and Rapinchuk A S, The multiplicative structure of division algebras over number fields and the Hasse norm principle, *Sov. Math. Dokl.* **26** (1982) 388–390
[48] Prasad G, Strong approximation, *Ann. Math.* **105** (1977) 553–572
[49] Prasad G, A variant of a theorem of Calvin Moore, *C.R. Acad. Sci. (Paris) Ser I* **302** (1982) 405–408
[50] Prasad G and Raghunathan M S, Topological central extensions of semi-simple groups over local fields, *Ann. Math.* **119** (1984) 143–268
[51] Prasad G and Raghunathan M S, On the congruence subgroup problem: Determination of the 'metaplectic kernel', *Inv. Math.* **71** (1983) 21–42
[52] Prasad G and Raghunathan M S, On the Kneser–Tits problem, *Comm. Math. Helv.* **60** (1985) 107–121
[53] Prasad G and Rapinchuk A S, Computation of the metaplectic kernel, *Publ. Math. IHES* **84** (1997) 91–187
[54] Raghunathan M S, On the congruence subgroup problem I, *Publ. Math. IHES* **46** (1976) 107–161
[55] Raghunathan M S, On the congruence subgroup problem II, *Inv. Math.* **85** (1986) 73–117
[56] Raghunathan M S, Torsion in co-compact lattices of spin (2, N), *Math. Ann.* **266** (1984) 403–419
[57] Raghunathan M S, On the group of norm 1 elements in a division algebra, *Math. Ann.* **279** (1988) 457–484
[58] Raghunathan M S, A note on generators for arithmetic subgroups of algebraic groups, *Pac. J. Math.* **152** (1992) 365–373
[59] Raghunathan M S, The congruence subgroup problem, Proceedings of the Hyderabad Conference on Algebraic Groups, Hyderabad, India, Dec. 1989, Manoj Prakashan, India
[60] Rapinchuk A S, On the congruence subgroup problem for algebraic groups, *Dokl. Akad. Nauk. SSSR* **306** (1989) 1304–1307
[61] Rapinchuk A S, Multiplicative arithmetic of division algebras over number fields and the metaplectic problem, *Math. USSR Izv.* **31** (1988) 349–379
[62] Rapinchuk A S, Combinatorial theory of arithmetic groups, Preprint (Acad. of Sciences BSSR) (1990)
[63] Rapinchuk A S, Congruence subgroup problem for algebraic groups, old and new, *Journeés Arithmétiques* (Geneva) (1991), *Astérisque* **209(1)** (1992) 73–84

[64] Rapinchuk A S, Segev Y and Seitz G M, Finite quotients of the multiplicative group of a finite dimensional division algebra are solvable, *J. Am. Math. Soc.* **15(4)** (2002) 929–978 (electronic)

[65] Rapinchuk A S and Segev Y, Valuation-like maps and the congruence subgroup property, *Invent. Math.* **144(3)** (2001) 571–607

[66] Segal D, Congruence topologies in commutative rings, *Bull. London Math. Soc.* **11** (1979) 186–190

[67] Segev Y, On finite homomorphic images of the multiplicative group of a division algebra. *Ann. Math. (2)* **149(1)** (1999) 219–251

[68] Serre J-P, Le problem̀e des groupes de congruence pour SL_2, *Ann. Math.* **92** (1970) 489–527

[69] Serre J-P, Sur les groupes de congruence des variet́eś abelienne, *Izv. Akad. Nauk. SSSR* **28** (1964) 3–18; II, *Akad. Nauk. SSSR* **35** (1971) 731–735

[70] Serre J-P, Le problem̀e des groupes de congruence pour SL_2, *Ann. Math.* **92** (1970) 489–527

[71] Serre J-P, Sur les groupes de congruence des variet́eś abelienne, *Izv. Akad Nauk. SSSR* **28** (1964) 3–18; II, *Akad. Nauk. SSSR* **35** (1971) 731–735

[72] Steinberg R, Geńeérateurs, reĺations et revet̂ements de groupes algeb́riques, Colloque de Bruxelles, CNRB (1962) 113–127

[73] Sury B, Congruence subgroup problem for anisotropic groups over semilocal rings, *Proc. Indian Acad. Sci. (Math. Sci.)* **101** (1991) 87–110

[74] Swan R G, Generators and relations for certain special linear groups, *Adv. Math.* **6** (1971) 1–77

[75] Tits J, Algebraic and abstract simple groups, *Ann. Math.* **80** (1964) 313–329

[76] Tits J, Classification of algebraic semi-simple groups, *Proc. Symp. Pure Math.* **9** (1966) (AMS)

[77] Tits J, Systems geńerateurs de groupes de congruence, *C.R. Acad. Sci. Paris Series A* **283** (1976) 693–695

[78] Toledo D, Projective varieties with non-residually finite fundamental group, *Inst. Hautes Études Sci. Publ. Math.* **77** (1993) 103–119

[79] Tomanov G, On the congruence subgroup problem for some anisotropic algebraic groups over number fields, *Crelles J.* **402** (1989) 138–152

[80] Tomanov G, Projective simplicity of groups of rational points of simply connected algebraic groups defined over number fields, Topics in Algebra Part 2 (Warsaw) (1998) 455–466, (Banach Centre Publications) 26, Part 2, PWN, Warsaw (1990)

[81] Tomanov G, On the group of elements of reduced norm l in a division algebra over a global field (Russian), *Izv. Akad. Nauk. SSSR Ser. Mat.* **55** (1991) 917; translation in *Math. USSR-Izv.* **39** (1992) 895–904

[82] Vaserstein L, The structure of classical arithmetic group of rank greater than one, *Math. USSR Sb.* **20** (1973) 465–492

[83] Venkataramana T N, On super-rigidity and arithmeticity of lattices in semisimple groups, *Invent Math.* **92** (1988) 255–306

[84] Venkataramana T N, On systems of generators of arithmetic subgroups of higher rank groups, *Pac. J. Math.* **166** (1994) 193–212

[85] Wall C T C, On the commutator subgroups of certain unitary groups, *J. Algebra* **27** (1973) 306–310

[86] Wall G E, The structure of a unitary factor group, *Publ. Math. IHES* **1** (1959)

[87] Wang S P, The dual space of a semisimple Lie group, *Am. J. Math.* **91** (1969) 921–937