Astérisque

A. S. RAPINCHUK

Congruence subgroup problem for algebraic groups: old and new

Astérisque, tome 209 (1992), p. 73-84

<http://www.numdam.org/item?id=AST_1992__209__73_0>

CONGRUENCE SUBGROUP PROBLEM FOR ALGEBRAIC GROUPS: OLD AND NEW

A. S. RAPINCHUK*

Let $G \subset \mathrm{GL}_n$ be an algebraic group defined over an algebraic number field K. Let S be a finite subset of the set V^K of all valuations of K, containing the set V_∞^K of archimedean valuations. Denote by $\mathcal{O}(S)$ the ring of S-integers in K and by $G_{\mathcal{O}(S)}$ the group of S-units in G. To any nonzero ideal $\mathfrak{a} \subset \mathcal{O}(S)$ there corresponds the congruence subgroup

$$G_{\mathcal{O}(S)}(\mathfrak{a}) = \{g \in G_{\mathcal{O}(S)} \mid g \equiv E_n \pmod{\mathfrak{a}}\},$$

which is a normal subgroup of finite index in $G_{\mathcal{O}(S)}$. The initial statement of the Congruence Subgroup Problem was:

(1) Does any normal subgroup of finite index in $G_{\mathcal{O}(S)}$ contain a suitable congruence subgroup $G_{\mathcal{O}(S)}(\mathfrak{a})$?

In fact, it was found by F. Klein as far back as 1880 that for the group $\mathrm{SL}_2(\mathbb{Z})$ the answer to question (1) is "no". So a more accurate statement of the problem should be: for which G and S does (1) have an affirmative answer? However, till the mid sixties there were no nontrivial examples of groups for which this is actually true. Only in 1965 did Bass-Lazard-Serre [1] and Mennicke [10] give a positive solution to the congruence subgroup problem for $\mathrm{SL}_n(\mathbb{Z})$ $(n \geq 3)$. In the course of further investigations, it appeared convenient

* The author wishes to thank the Department of Mathematics in Geneva for editing and retyping the manuscript.

to introduce the object measuring deviation from the positive solution of (1) and then to view the congruence subgroup problem as the problem of its computation. This object (called the congruence kernel) was defined by Serre [27] as follows.

Let us introduce on the group G_K of K-rational points two Hausdorff topologies, τ_a and τ_c, called S-arithmetic topology and S-congruence topology, respectively. The complete system of neighbourhoods of unity for τ_a (resp., τ_c) consists of all normal subgroups of finite index (resp., all congruence subgroups) in $G_{\mathcal{O}(S)}$. It is easy to show that these topologies satisfy all the properties that ensure the existence of the corresponding S-arithmetic and S-congruence completions $\widehat{G}$ and $\overline{G}$. Since τ_a is stronger than τ_c, the identity map

$$(G_K, \tau_a) \to (G_K, \tau_c)$$

is continuous. Therefore it can be extended to a continuous homomorphism $\pi\colon \widehat{G} \to \overline{G}$ of the completions. By definition, $C^S(G) = \operatorname{Ker}\pi$ is the *congruence kernel.*

PROPOSITION 1. *The projection π is surjective and $C^S(G)$ is a profinite group. $C^S(G)$ is trivial if and only if the congruence subgroup problem in the form* (1) *has an affirmative solution for $G_{\mathcal{O}(S)}$.*

Thus, in general, the congruence kernel $C^S(G)$ measures deviation from a positive answer to the congruence subgroup problem. So, by the modern statement of the problem we mean the problem of determination of $C^S(G)$. It is well-known (see for example [23]) that this problem can be reduced to the main case of an (absolutely) simple, simply connected algebraic group G. Here we shall be exclusively concerned with that case. As we have already remarked, the first positive result on the congruence subgroup problem for such groups is due to Bass-Lazard-Serre [1] and Mennicke [10], who studied the case of $\mathrm{SL}_n(\mathbb{Z})$ $(n \geq 3)$. Then Bass-Milnor-Serre [2] completed the investigation of SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$ over an arbitrary number field K, after obtaining a description of $C^S(G)$ in the following form:

$$C^S(G) = \begin{cases} 1 & \text{if } \exists\, v \in S \text{ such that } K_v \neq \mathbb{C} \\ E(K) & \text{otherwise,} \end{cases} \tag{2}$$

where $E(K)$ is the group of all roots of unity in K. By further developing the methods of [2], Matsumoto [9] extended (2) to all universal Chevalley groups different from SL_2 (the case of twisted Chevalley groups was considered by Deodhar [4]). In the case $G = \mathrm{SL}_2$, first Mennicke [11] gave a positive solution to the congruence subgroup problem for the group $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$, and then Serre

[27] studied the general situation and showed that, provided Card $S > 1$, the answer is of the form (2). On analysing the obtained results, Serre [27] formulated the following congruence subgroup conjecture, which gives sufficient conditions for $C^S(G)$ to be finite or infinite, in terms of the so-called S-rank:

$$\operatorname{rang}_S G = \sum_{v \in S} \operatorname{rang}_{K_v} G,$$

where $\operatorname{rang}_P G$ denotes the rank of the group G over the field P, i.e., the dimension of a maximal P-split subtorus in G.

CONJECTURE 1. *Let G be simple and simply connected. Then in case $\operatorname{rang}_S G \geq 2$ and G is K_v-isotropic for all $v \in S \setminus V_\infty^K$, the congruence kernel $C^S(G)$ should be finite. In case $\operatorname{rang}_S G = 1$, it should be infinite.*

The case of finite $C^S(G)$ is the most interesting and important for applications. In that case, we shall say that the group $\Gamma = G_{\mathcal{O}(S)}$ has the *congruence subgroup property* (*CSP*). In this paper we are going to describe the class of groups for which (*CSP*) is known to hold and outline some new methods of attacking the congruence subgroup problem, which, as we hope, will enable us to enlarge this class considerably.

Let us first describe the general scheme for calculating the congruence kernel $C = C^S(G)$. It follows from our definitions that C can be determined from the exact sequence:

$$1 \to C \to \widehat{G} \xrightarrow{\pi} \overline{G} \to 1 \tag{3}$$

Let us consider the initial segment of the Hochschild-Serre spectral sequence corresponding to (3):

$$H^1(\overline{G}) \xrightarrow{\varphi} H^1(\widehat{G}) \to H^1(C)^{\overline{G}} \xrightarrow{\psi} H^2(\overline{G}), \tag{4}$$

where $H^i(*)$ denotes the i-th continuous cohomology group with coefficients in the one-dimensional torus $\mathbb{R}/\mathbb{Z}$. The term $H^1(C)^{\overline{G}}$ in (4) is connected with C as follows:

$$H^1(C)^{\overline{G}} = \operatorname{Hom}(C/[C, \hat{G}]\,, \mathbb{R}/\mathbb{Z}).$$

So one can reconstruct C from $H^1(C)^{\overline{G}}$ only under the assumption that C is central, i.e., lies in the centre of $\widehat{G}$. Indeed, in this case $H^1(C)^{\overline{G}}$ coincides with the Pontryagin dual C^* of C. Suppose now that C is central. Then we have the following exact sequence:

$$1 \to \operatorname{Coker} \varphi \to C^* \to \operatorname{Im} \psi \to 1.$$

Ignoring the trivial case $\operatorname{rang}_S G = 0$, in which $G_{\mathcal{O}(S)}$ is finite and consequently $C^S(G) = 1$, we immediately obtain from the strong approximation theorem that the group $\overline{G}$ can be identified with the group $G_{A(S)}$ of S-adeles. Then, using the fact that the sequence (3) splits over the group G_K and is the "universal" sequence with this property, one can show that $\operatorname{Im}\psi$ coincides with the so-called *metaplectic kernel*

$$M(G,S) = \operatorname{Ker}\big(H^2(G_{A(S)}) \to H^2(G_K)\big),$$

where G_K is endowed with the discrete topology. On the other hand

$$\operatorname{Coker}\varphi \cong \overline{[G_K, G_K]}/[G_K, G_K],$$

where the bar denotes closure in G_K for the S-arithmetic topology. Taking into account that $M(G,S)$ is always finite (see [17]) and that $[G_K, G_K]$ has finite index in G_K (see [8]), we arrive at the following

PROPOSITION 2. *If C is central then it is finite. If, moreover,* $\operatorname{Coker}\varphi = 1$ *then $C^* \simeq M(G,S)$.*

In fact, at present it is known that $\operatorname{Coker}\varphi$ is indeed trivial for most cases. This depends on the validity for G_K of the following conjecture, which describes the normal structure. (This conjecture was formulated by Platonov [13] in the form of a local-to-global principle for projective simplicity and then by Margulis [8] in the final form).

CONJECTURE 2. *Let $V_f^K = V^K \setminus V_\infty^K$ be the set of nonarchimedean valuations, and let $T = \{v \in V_f^K \mid G \text{ is } K_v\text{-anisotropic}\}$. Then for any noncentral, normal subgroup $N \subset G_K$ there is an open normal subgroup $W \subset G_T = \prod_{v\in T} G_{K_v}$ such that $N = W \cap G_K$. In other words, any noncentral normal subgroup is open (equivalently, closed) in the T-adic topology.*

If Conjecture 2 is true for G_K then we say that G_K has a *standard description of normal subgroups.* In the situation of Conjecture 1 we have $S \cap T = \varnothing$, and so the triviality of $\operatorname{Coker}\varphi$ is equivalent to saying that Conjecture 2 holds for $N = [G_K, G_K]$. But the latter statement is actually true for all groups, with the possible exception of some anisotropic forms of types ${}^2A_n$, ${}^{3,6}D_4$ and E_6 (see [14]). Thus, in most cases, the calculation of C (provided it is central) reduces to that of $M(G,S)$.

The first computations of the metaplectic kernel had been carried out by Moore [12] and Matsumoto [9]. They obtained the description of $M(G,S)$

for Chevalley groups in the form (2). The case of quasi-split groups was considered by Deodhar [4]. The final result for isotropic groups, due to Prasad-Raghunathan [17], is of the form:

$$M(G,S) = \begin{cases} 1 & \text{if } S \neq V_\infty^K \\ \subset E(K) & \text{otherwise,} \end{cases} \tag{5}$$

where $E(K)$ is the group of all roots of unity in K. The author [20] calculated $M(G,S)$ for a large series of anisotropic groups. Here the description of $M(G,S)$ is of the same nature as (5), but its precise form may differ from (5) by a certain group of exponent 2. The main part of these results is the computation of $M(G,S)$ for the groups of type $\mathrm{SL}_1(D)$. As in the classical case of the group SL_n, we show that any element $x \in M(G,S)$ gives rise to a certain reciprocity law, i.e., to a relation of the form

$$\prod_{w \in V^L} (a,b)_w^{n_w} = 1,$$

where L is a certain maximal subfield in D and $(*,*)_w$ is the norm residue symbol of degree $\mu_w = [E(L_w)]$. But the difference from the classical situation is that this reciprocity law must hold not for all $a, b \in L^*$, but for all a, b of some specific form. Then we prove a certain version of the uniqueness theorem for reciprocity laws of this kind (similar results were obtained by Prasad [16]) and derive from it the desired description of the metaplectic kernel. That is all that is known about the problem of the precise determination of C under the assumption that it is central. Now we shall move on to the methods of proving the centrality of C. This is equivalent (as explained above) to its being finite.

That the congruence kernel is central for the groups SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$, was established by Bass-Milnor-Serre in [2]. The case of split and quasi-split groups was considered by Matsumoto [9] and Deodhar [4] respectively. For $G = \mathrm{SL}_2$, Serre [27] proved that $C^S(G)$ is central in the case where $\mathrm{Card}\, S > 1$. Raghunathan [18], [19] completed the discussion of K-isotropic groups by proving that they satisfy Conjecture 1, i.e. in fact that $C^S(G)$ is central for the case $\mathrm{rang}_S G \geq 2$. The argument in all these papers was based on some manipulations with unipotent elements in G_K, and so no version of it can be applied to anisotropic groups. Until recently, the only result which allowed also anisotropic groups was Kneser's theorem [6] for spinor groups of quadratic forms. But then Rapinchuk [21], [22] and Tomanov [29] extended this theorem to all groups having a nice geometric realization.

THEOREM 1. *Let G be a simple, simply connected K-group of one of the following types B_n $(n \geq 2)$, C_n $(n \geq 2)$, D_n $(n \geq 5)$, G_2 or the special unitary groups, $\mathrm{SU}_m(f)$ $(m \geq 4)$, of a nondegenerate hermitian form f over some quadratic extension L/K belonging to the type ${}^2A_{m-1}$. Assume that $\mathrm{rang}_S G \geq 2$ and, moreover, if G is of type C_3 then either S contains a nonarchimedean valuation or such an archimedean valuation v that $\mathrm{rang}_{K_v} G \geq 2$. Then $C^S(G)$ is central.*

Later Tomanov [30] included into the list of groups in Theorem 1 also the unitary groups over the quaternions.

The proof of Theorem 1 is actually independent of the type of the group. It is based on the following two statements.

PROPOSITION 3. *$C^S(G)$ is central if the group G_K is projectively simple and if there is a K-defined subgroup $H \subset G$ with the following properties:*

1) *the natural map $C^S(H) \to C^S(G)$ is surjective;*
2) *for some nontrivial K-defined automorphism $\sigma \in \mathrm{Aut}\, G$, the restriction $\sigma|_H$ is trivial.*

PROPOSITION 4. *Let G act K-rationally on some affine K-variety X, and let $x \in X_K$. Assume that, for any normal subgroup $N \subset G_{\mathcal{O}(S)}$ of finite index, the orbit Nx is open in $G_{\mathcal{O}(S)}x$ for the S-adelic topology (of the space $X_{A(S)}$). Then, if $G(x)$ denotes the stabilizer of the point x, the natural map $C^S(G(x)) \to C^S(G)$ is surjective.*

We apply these statements to the natural realizations of the groups in Theorem 1 as the automorphism groups of some quadratic, hermitian or skew-hermitian forms. In fact, this method is applicable in many other situations besides those described in Theorem 1. For example, it was shown in [23] how it can be used to establish the centrality of the congruence kernel for the group SL_n $(n \geq 3)$. On the other hand, it is inapplicable to the groups which have no nice geometric presentation, in particular to most exceptional groups. Here the solution of the congruence subgroup problem was obtained by Rapinchuk [22] through another approach, using the intrinsic structure of the group.

THEOREM 2. *Let G be a simple, simply connected K-anisotropic group of one of the following types: E_7, E_8, F_4. Assume that:*

1) *if G is of type E_7 or E_8 then $\mathrm{rang}_S G \geq 2$;*
2) *if G is of type F_4 then there is $v \in S$ such that $\mathrm{rang}_{K_v} G \geq 2$.*

Then $C^S(G)$ is central.

A crucial role in the proof of Theorem 2 is played by the fact that all groups of the enumerated types split over some quadratic extension L/K with a special local behaviour. This result is a consequence of the Hasse principle for the Galois cohomology of simply connected groups and the fact that the centres of these groups have order at most 2.

All these results confirm Serre's conjecture for most types of simple groups. However, there is a very important class of groups, viz. the groups of type $\mathrm{SL}_1(D)$ where D is a division algebra, for which these methods fail to work. Even for the case of a quaternion algebra D, until recently there was not a single example of a group of type $\mathrm{SL}_1(D)$ with property (*CSP*). But a few months ago it appeared that such an example can be obtained on the basis of a new approach to the congruence subgroup problem developed in Minsk.

This approach is based on the use of some abstract algebraic concepts. The first step in its foundation was a purely algebraic proof of centrality for the congruence kernel of the groups SL_n ($n \geq 3$) (in fact, for all Chevalley groups of rank ≥ 2) and of $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ (see [26]). To be more precise, it was shown that the centrality of the congruence kernel for these groups follows directly from commutator relations. It seems plausible that this argument can be extended to all (or most) isotropic groups where commutator relations of the same type hold. On the other hand, it is inapplicable to groups for which no explicit presentation of a convenient form exists (or is known), i.e. to the most interesting case of anisotropic groups. It is clear that the algebraic approach here should be based not on the analysis of particular relations, but on the specification of some abstract properties of arithmetic groups which would imply the finiteness (or centrality) of the congruence kernel. At present, we know a few properties of this kind, the first of which being the property of bounded generation.

DEFINITION. We say that an abstract group Γ has the property of *bounded generation* (*BG*) if there are elements $\gamma_1, \ldots, \gamma_t \in \Gamma$ such that $\Gamma = \langle\gamma_1\rangle \ldots \langle\gamma_t\rangle$, where $\langle\gamma_i\rangle$ is the cyclic subgroup generated by γ_i.

This property is clearly of a combinatorial nature. However, the author failed to find any mention of it in the works on combinatorial group theory. It should be emphasized that this abstract definition was strongly motivated by a result of Carter and Keller [3], according to which any matrix in $\mathrm{SL}_n(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers in an algebraic number field and $n \geq 3$, is a product of a certain bounded number of elementary matrices. In fact, this paper of Carter and Keller was aimed at the solution of a problem from algebraic K-theory, viz. the question of the triviality of the SK_1-functor for so-

called non-standard models of the rings of integers. Their result quoted above is precisely equivalent to this triviality. However, the technique employed in that paper was borrowed from the works on the congruence subgroup problem (Mennicke symbols, etc.). The analysis of that paper, and also of some other facts, induced the author to formulate the following conjecture.

CONJECTURE 3. *Let G be a simple, simply connected algebraic group over an algebraic number field K, and let $S \subset V^K$ be a finite subset containing V_∞^K. Then for the group $\Gamma = G_{\mathcal{O}(S)}$ of S-integral points the properties (CSP) and (BG) are equivalent.*

Some further evidence in favour of this conjecture appeared when Tavgen' [28] established (BG) for arithmetic and S-arithmetic subgroups of all Chevalley groups of rank ≥ 2, both of normal and of most twisted types. (The (CSP) property for these groups was proved by Matsumoto [9] and Deodhar [4].) There are also some examples of the reverse character. For the groups $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{SL}_2(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers in an imaginary quadratic field, both properties (CSP) and (BG) fail to hold. In all these cases, (CSP) and (BG) are proved or disproved independently, and somehow it happens that they simultaneously hold or fail to hold. But the real question was whether there is some direct connection between these two properties in the general situation. The first result which established such a connection was the following theorem, proved by the author [24].

THEOREM 3. *Assume that the group G_K admits a standard description of normal subgroups. If $\Gamma = G_{\mathcal{O}(S)}$ has (BG) then the abelianized congruence kernel $C^{ab} = C/[C, C]$ is finite.*

Subsequently it turned out that the technique invented for the proof of Theorem 3 can be pushed further, so that, for S-arithmetic groups of bounded generation, property (CSP) can be proved in full (see Corollary 1 below). This fact was obtained as a consequence of some more general results (to be described a little later), obtained independently by Platonov-Rapinchuk [15] and A. Lubotzky. It is worth mentioning that this enables us to present new examples of S-arithmetic groups with (CSP). Namely, recently F. Grunewald found by computer some explicit examples of groups with (BG) among the groups of the form $G_{\mathbb{Z}(S)}$, where $G = \mathrm{SL}_1(D)$ for some quaternion algebra D over $\mathbb{Q}$ and $S = \{\infty, p\}$ (p prime). This gives the first examples of quaternionic groups with (CSP). Now I would like to formulate a conjecture, the proof of which would provide a proof of Serre's congruence subgroup conjecture.

CONJECTURE 4. *If G is simple and $\operatorname{rang}_S G \geq 2$ then $\Gamma = G_{\mathcal{O}(S)}$ has bounded generation.*

There is no doubt that groups with (BG) (and especially their profinite analogues) deserve some special treatment. They have interesting structural properties and, under additional assumptions, they satisfy an important property from representation theory – the property of finiteness of the representation type (see [25], [26]). However, at present it is not quite clear how to determine in general whether a particular group has bounded generation or not. For this reason we had undertaken a search of other abstract properties of arithmetic groups, which should also ensure (CSP) but be (or at least look) more constructive than (BG). Now, I am going to describe some results in this direction, which have been obtained by Platonov and Rapinchuk [15]. We shall need some new definitions, bearing not on the S-arithmetic group Γ itself but on its profinite completion $\widehat{\Gamma}$.

DEFINITION. Let Δ be a finitely generated profinite group.

1. Δ has *bounded generation as a profinite group* (property $(BG)_{pf}$) if there exist elements $\delta_1, \ldots, \delta_t \in \Delta$ such that $\Delta = \overline{\langle \delta_1 \rangle} \ldots \overline{\langle \delta_t \rangle}$, where $\overline{\langle \delta_i \rangle}$ denotes the closure of the cyclic subgroup generated by δ_i.
2. The *n-th Burnside factor* Δ_n of Δ is the factor group Δ/Δ^n modulo the closed subgroup Δ^n generated by n-th powers of all elements of Δ. (Note that, according to [31], Δ_n is finite for any n.)
3. Δ has *polynomial growth in the orders of its Burnside factors* (property $(PG)_{pf}$) if there are constants c and k such that $|\Delta_n| \leq cn^k$ for all n.
4. Δ has *property* $(PG)'_{pf}$ if, for any integer $n > 0$ and any prime q, there exist c and k such that $\left|\Delta_{nq^i}\right| \leq cq^{ki}$ for all $i > 0$.

It is easy to show that property (BG) for Γ implies $(BG)_{pf}$ for $\widehat{\Gamma}$. On the other hand, for arbitrary Δ we have

$$(BG)_{pf} \Longrightarrow (PG)_{pf} \Longrightarrow (PG)'_{pf}.$$

No other relations between these properties are known. So it would be interesting to find out whether properties $(BG)_{pf}$ and $(PG)_{pf}$ are equivalent or not. (Our results show that this is certainly true for the profinite completions of S-arithmetic groups; see Corollary 2 below. Moreover, as follows from [5] and [7], for a pro-p-group Δ each of the conditions $(BG)_{pf}$, $(PG)_{pf}$, or $(PG)'_{pf}$ is equivalent to analyticity.)

Now we may formulate:

THEOREM 4. *Assume that G_K admits a standard description of normal subgroups and suppose $S \cap T = \varnothing$. If the profinite completion $\widehat{\Gamma}$ of the group $\Gamma = G_{\mathcal{O}(S)}$ satisfies $(PG)'_{pf}$, then Γ has property (CSP).*

Naturally, for the proof we show that $(PG)'_{pf}$ implies that $C = C^S(G)$ is central. It should also be noted that, after the paper [15] had been prepared for publication, A. Lubotzky informed us that he also managed to establish the centrality of C under the condition $(PG)_{pf}$ for $\widehat{\Gamma}$.

COROLLARY 1. *With the assumptions of Theorem 4, if the group $\widehat{\Gamma}$ has property $(BG)_{pf}$ (in particular, if Γ has property (BG)) then Γ has (CSP).*

Now it should be pointed out that the converse statement to Theorem 4 is true without any additional assumptions on the group G. This follows from

THEOREM 5. *Let G be a simple, simply connected K-group, and let $S \subset V^K$ be a finite subset containing V_∞^K. Then the group $G_{A_S(S)}$ of S-integral S-adeles is a profinite group satisfying $(BG)_{pf}$.*

COROLLARY 2. *If G_K has a standard description of normal subgroups and $S \cap T = \varnothing$ then each of the conditions $(BG)_{pf}$, $(PG)_{pf}$, and $(PG)'_{pf}$ for $\widehat{\Gamma}$, is equivalent to (CSP) for Γ.*

Now, to close this survey, we show that, for example in the case of $\Gamma = \mathrm{SL}_m(\mathbb{Z})$ $(m \geq 3)$, the condition $(PG)'_{pf}$ can be straightforwardly checked by purely algebraic means, while condition (BG) requires some rather delicate arithmetic considerations (cf. [3]). (There is no direct proof of condition $(PG)_{pf}$ for this group either.)

It is well-known that $\Gamma = \mathrm{SL}_m(\mathbb{Z})$ $(m \geq 3)$ is generated by elementary matrices e_{ij} $(i, j = 1, \ldots, m;\ i \neq j)$. These satisfy the following commutator relations

$$[e_{ij}^{\alpha}, e_{jk}^{\beta}] = e_{ik}^{\alpha\beta} \tag{6}$$

for all pairwise distinct subscripts i, j, k. Clearly, the profinite Burnside factor $\widehat{\Gamma}_n$ is the maximal finite factor group of the discrete Burnside factor $\Gamma_n = \Gamma/\Gamma^n$, where Γ^n is generated by n-th powers of all elements of Γ. It is known that any noncentral normal subgroup in Γ is of finite index (see [8]). So Γ_n is finite and $|\widehat{\Gamma}_n| = |\Gamma_n|$ for any n. Denote by E_n the normal subgroup in Γ generated by $\{e_{ij}^n\}$. Evidently, we have $E_n \subset \Gamma^n$; so it suffices to estimate

$|\Gamma/E_n|$. Now we fix an integer $n > 0$ and a prime p, and we estimate $|\Gamma/E_{np^\alpha}|$. Assuming $\alpha > 8$ we have

$$|\Gamma/E_{np^\alpha}| = c\,|E_{np^8}/E_{np^\alpha}|,$$

where $c = [\Gamma : E_{np^8}]$. Consider now the profinite group $\Delta = \varprojlim E_{np^8}/E_{np^\alpha}$, the limit being taken over $\alpha > 8$. Using the relations (6), it is easy to show that for any $\alpha > 8$ the group $E_{np^\alpha}/E_{np^{\alpha+2}}$ is an abelian p-group. Thus Δ is a pro-p-group. On the other hand, we have

$$E_{np^{10}} \subset E_{np^8}^{p^2} \subset E_{np^8}.$$

In particular, $[E_{np^8}, E_{np^8}] \subset E_{np^8}^{p^2}$. Applying Lazard's criterion for analyticity (see [7]), or the results on the so-called powerful pro-p-groups (see [5]), we deduce that Δ is analytic. Then it has each of the properties $(BG)_{pf}$, $(PG)_{pf}$, and $(PG)'_{pf}$. This clearly implies that $|E_{np^8}/E_{np^\alpha}|$ grows polynomially in p^α. Hence the same assertion holds for $|\Gamma/E_{np^\alpha}|$, and we are through.

References

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

[2] H. Bass, J. Milnor & J-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_n ($n \geq 2$), *Publ. Math. IHES*, 33 (1967), 54–137.

[3] D. Carter & G. Keller, Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$, *Amer. J. Math.*, 105 (1983), 673–687.

[4] V. Deodhar, On central extensions of rational points of algebraic groups, *Amer. J. Math.*, 100 (1978), 303–386.

[5] J.D. Dixon, M.P.F. du Sautoy, A. Mann & D. Segal, Analytic pro-p-Groups, *London Math. Soc. Lecture Note Series*, No. 157, Cambridge Univ. Press, 1991.

[6] M. Kneser, Normalteiler ganzzahliger Spingruppen, *J. reine und angew. Math.*, 311/312 (1979), 191–214.

[7] M. Lazard, Groupes analytiques p-adiques, *Publ. Math. IHES*, 26 (1965), 389–603.

[8] G.A. Margulis, Finiteness of factor groups of discrete groups, *Funct. Anal. and Appl.*, 13 (1979), 28–39 (in Russian).

[9] H. Matsumoto, Sur les sous-groupes arithmétiques des groupes semi-simples déployés, *Ann. Sci. Ecole Norm. Sup.*, (4) 2 (1969), 1–62.

[10] J. Mennicke, Finite factor groups of the unimodular group, *Ann. of Math.*, 81 (1965), 31–37.

[11] —, On Ihara's modular group, *Invent. Math.*, 4 (1967), 202–228.

[12] C. Moore, Group extensions of p-adic and adelic groups, *Publ. Math. IHES*, 35 (1968), 5–70.

[13] V.P. Platonov, Arithmetic and structural problems for linear algebraic groups, *Proc. Intern. Congr. Math. Vancouver 1974*, vol. 1 (1975), 471–476 (in Russian).

[14] V.P. Platonov & A.S. Rapinchuk, *Algebraic groups and number theory*, Moscow, Nauka, 1991 (in Russian; English translation is being prepared by Academic Press).

[15] —, —, Abstract characterizations of arithmetic groups with the congruence subgroup property, *Dokl. Akad. Nauk SSSR*, 319 (1991), No. 6 (in Russian).

[16] G. Prasad, A variant of a theorem of Calvin Moore, *C.R. Acad. Sci.*, 302 (1986), 405–408.

[17] G. Prasad & M.S. Raghunathan, On the congruence subgroup problem: Determination of the "Metaplectic kernel", *Invent. Math.*, 71 (1983), 21–42.

[18] M.S. Raghunathan, On the congruence subgroup problem, *Publ. Math. IHES*, 46 (1976), 107–161.

[19] —, On the congruence subgroup problem II, *Invent. Math.*, 85 (1986), 73–117.

[20] A.S. Rapinchuk, Multiplicative arithmetic of division algebras over number fields and metaplectic problem, *Izv. Akad. Nauk SSSR, Ser. Mat.*, 51 (1987), 1033–1064 (in Russian).

[21] —, Congruence subgroup problem for algebraic groups and strong approximation in affine varieties, *Dokl. Akad. Nauk BSSR*, 32 (1988), 581–584 (in Russian).

[22] —, On the congruence subgroup problem for algebraic groups, *Dokl. Akad. Nauk SSSR*, 306 (1989), 1304–1307 (in Russian).

[23] —, The congruence subgroup problem for algebraic groups, *Topics in algebra, Banach center publ.*, vol. 26, part 2 (1990), 399–410.

[24] —, The congruence subgroup problem for arithmetic groups with bounded generation, *Dokl. Akad. Nauk SSSR*, 314 (1990), 1327–1331 (in Russian).

[25] —, Representations of groups with bounded generation, *Dokl. Akad. Nauk SSSR*, 315 (1990), 536–540 (in Russian).

[26] —, *Combinatorial theory of arithmetic groups*, Preprint of the Institute of Mathematics of the Byelorussian Acad. Sci., No. 20 (420) (1990).

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

[28] O.I. Tavgen', Bounded generation of Chevalley groups over the rings of S-integers, *Izv. Akad. Nauk SSSR, Ser. Mat.*, 54 (1990), 97–122 (in Russian).

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

[30] —, Remarques sur la structure des groupes algébriques définis sur des corps de nombres, *C.R. Acad. Sci.*, 310 (1990), 33–36.

[31] E.I. Zel'manov, The solution of the restricted Burnside problem for groups of odd exponent, *Izv. Akad. Nauk SSSR., Ser. Mat.*, 54 (1990) (in Russian).

Andreĭ S. Rapinchuk
Institute of Mathematics
of the
Byelorussian Academy of Sciences
ul. Surganova, 11
MINSK 220072 – Byelorussia