Prasad's work on the congruence subgroup problem

Andrei Rapinchuk

The investigation into the CSP began in the 19th century but there are still important cases where the problem remains open. In this talk I will tell you about some of the available results referring for more details to our survey paper

G. Prasad, A. Rapinchuk, *Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre,* Milnor's Collected Works, vol. 5.

I should point out that in the article, as well as in this talk, we will focus exclusively on the classical case of the CSP for S-arithmetic subgroups of algebraic groups but nowadays the CSP is being actively considered also in the context of the automorphism groups of free groups, mapping class groups and also the automorphism groups of other finitely generated groups.

Speaking about linear groups, given a commutative ring R and its ideal $\mathfrak{a} \subset R$, one can consider the homomorphism

$$\rho_{\mathfrak{a}} \colon \mathrm{GL}_n(R) \longrightarrow \mathrm{GL}_n(R/\mathfrak{a})$$

of reduction modulo $\mathfrak{a}$, the kernel of which is called the *congruence subgroup of level* $\mathfrak{a}$ and denoted $\mathrm{GL}_n(R, \mathfrak{a})$. More generally, for any subgroup $\Gamma \subset \mathrm{GL}_n(R)$ one can define the congruence subgroup

$$\Gamma(\mathfrak{a}) := \Gamma \cap \mathrm{GL}_n(R, \mathfrak{a}),$$

which of course is a normal subgroup of Γ. Moreover, in this talks R will be the ring of S-integers of a global field, and in this case for every nonzero $\mathfrak{a}$, the subgroup $\Gamma(\mathfrak{a})$ is automatically of finite index in Γ (over more general rings, one typically considers only ideals of finite index). Given this supply of finite index normal subgroups $\{\Gamma(\mathfrak{a})\}$ of Γ naturally associated with the ideals of R, one is led to the following question.

Congruence Subgroup Problem. *Does every normal subgroup $N \subset \Gamma$ of finite index contain a suitable congruence subgroup?*

For the first time, this question was considered back in the 19th century for the group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ which was central to the theory of modular functions, and then Fricke and Klein discovered that in this case the answer is *negative* in a very strong sense. The point is that the quotients modulo congruence subgroups have a very distinctive and restricted structure. Namely, we have an isomorphism

$$\mathrm{SL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z}, m) \simeq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}),$$

and furthermore, if $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, then

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \simeq \mathrm{SL}_2(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times \mathrm{SL}_2(\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}),$$

which implies that the quotient has a composition series where the consecutive quotients are either (almost) simple groups $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ or cyclic groups of prime order. On the other hand,

$$\mathrm{SL}_2(\mathbb{Z})/\{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} \quad \text{(free product)},$$

hence can be mapped surjectively onto *many* finite simple groups different from the ones listed above. Then the kernels of these homomorphisms do *not* contain any congruence subgroups, yielding the negative answer to the CSP. While the description of quotients by congruence subgroups extends to $\mathrm{SL}_n(\mathbb{Z})$ ($n \geqslant 3$), the (abstract) structure of even $\mathrm{SL}_3(\mathbb{Z})$ is significantly more complex than that of $\mathrm{SL}_2(\mathbb{Z})$. So, it was not obvious how to map the former onto finite simple groups other than $\mathrm{PSL}_3(\mathbb{Z}/p\mathbb{Z})$, so the CSP remained unanswered at that time. There seems to be no evidence in the literature of attempts to prove the CSP in this case, so most probably the negative answer for $\mathrm{SL}_2(\mathbb{Z})$ had some discouraging, and in fact quite lasting effect.

The interest to the CSP re-developed in the 1960s when Bass, Lazard and Serre (1964) and independently Mennicke (1965) showed that for $\mathrm{SL}_n(\mathbb{Z})$ the CSP has the affirmative answer. Interestingly, the proof is rather elementary and uses no number-theoretic tools other than Dirichlet's Theorem on Primes in Arithmetic Progression (so, potentially, it could have been found back in the 19th century).

A few years later, Bass, Milnor and Serre (1967) investigated the CSP for $\mathrm{SL}_n(R)$ where $n \geqslant 3$ and R is an arbitrary ring of algebraic integers. The results turned out to be quite surprising: while for $\mathrm{SL}_n(\mathbb{Z}[\sqrt{2}])$ the answer to the CSP problem is still affirmative, for $\mathrm{SL}_n(\mathbb{Z}[i])$ it becomes negative. However, the reason the CSP fails for $\mathrm{SL}_3(\mathbb{Z}[i])$ is *different* from the case of $\mathrm{SL}_2(\mathbb{Z})$: one knows for a fact that $\mathrm{SL}_3(\mathbb{Z}[i])$ does *not* have finite quotients that involve finite simple groups other than PSL_3 over appropriate finite fields. So, morally this case is closer to $\mathrm{SL}_3(\mathbb{Z})$ rather than to $\mathrm{SL}_2(\mathbb{Z})$ but nevertheless the answer to the CSP is negative. In order to describe precisely what happens we need the notion of the *congruence kernel* proposed by Serre which we will define next.

First, we need to fix some notations that will be used throughout the talk. We let G denote a linear algebraic group defined over a global field K, let S be a subset (not necessarily finite) of the set V^K of all valuations of K (containing all archimedean valuations if K is a number field, and at least nonempty if K has positive characteristic), and let

$$\mathcal{O}_S = \{a \in K^\times \mid v(a) \geqslant 0 \ \text{ for all } \ v \in V^K \setminus S\} \cup \{0\}$$

be the corresponding ring of S-integers in K. We fix a faithful K-representation $G \hookrightarrow \mathrm{GL}_N$, which allows us to define unambiguously the group

$$\Gamma = G(\mathcal{O}_S) := G \cap \mathrm{GL}_N(\mathcal{O}_S)$$

of S-integral points. Moreover, to every nonzero ideal $\mathfrak{a} \subset \mathcal{O}_S$, one associates the congruence subgroup $\Gamma(\mathfrak{a})$.

Next, we introduce two topologies on Γ:

- τ_a^S, the S-arithmetic topology, with the fundamental system of neighborhoods of the identity consisting of all finite index normal subgroups $N \subset \Gamma$ (= profinite topology);
- τ_c^S, the congruence topology, with the fundamental system of neighborhoods of the identity consisting of all congruence subgroups $\Gamma(\mathfrak{a})$ for all nonzero ideals $\mathfrak{a} \subset \mathcal{O}_S$.

Clearly, $\tau_a^S \succeq \tau_c^S$, and the affirmative answer to the CSP as stated above is equivalent to the fact that these topologies coincide: $\tau_a^S = \tau_c^S$. To measure the difference between these topologies in the general case, one considers the corresponding completions which in the case at hand can be described in terms of inverse limits (instead of Cauchy sequences):

$$\widehat{\Gamma} = \lim_{\leftarrow} \Gamma/N \quad \text{and} \quad \overline{\Gamma} = \lim_{\leftarrow} \Gamma/\Gamma(\mathfrak{a})$$

(arithmetic and congruence completions). Since $\tau_a^S \succeq \tau_c^S$, there is a natural continuous surjective homomorphism of topological groups:

$$\pi^S \colon \widehat{\Gamma} \longrightarrow \overline{\Gamma}$$

The kernel $C(\Gamma) = \operatorname{Ker} \pi^S$ is called the *congruence kernel.* One easily shows that

$$\tau_a^S = \tau_c^S \quad \Leftrightarrow \quad \operatorname{Ker} \pi^S = \{1\},$$

i.e. the affirmative solution to the congruence subgroup problem is equivalent to the fact that $C(\Gamma)$ is trivial. In the general case, the size of $C(\Gamma)$ characterizes the difference between the two topologies, i.e. the deviation from the positive solution. So, according to Serre, by the Congruence Subgroup Problem one should understand the problem of computation of the congruence kernel $C(\Gamma)$.

Here is what the congruence kernel is in the above examples:

(a) $C(\mathrm{SL}_2(\mathbb{Z}))$ is a free profinite group of countable rank;

(b) $C(\mathrm{SL}_n(\mathbb{Z}) = C(\mathrm{SL}_n(\mathbb{Z}[\sqrt{2}])) = \{1\}$ where $n \geqslant 3$;

(c) $C(\mathrm{SL}_n(\mathbb{Z}[i])) \simeq \mathbb{Z}/4\mathbb{Z}$ for $n \geq 3$.

We will now describe a general method for computing the congruence kernel which yields the results in (b) and (c) and many other situations. First, the above topologies τ_a^S and τ_c^S can be extended from $\Gamma = G(\mathcal{O}_S)$ to $G(K)$, and the latter admits the completions $\widehat{G}^S$ and $\overline{G}^S$ with respect to these topologies. As above, there is a continuous surjective group homomorphism $\tilde{\pi}^S \colon \widehat{G}^S \longrightarrow \overline{G}^S$, the kernel $C^S(G) = \operatorname{Ker} \tilde{\pi}^S$ of which coincides with $C(\Gamma)$ (in particular, it is a profinite group). Thus, $C = C^S(G)$ can be determined from the exact sequence

$$1 \to C \longrightarrow \widehat{G}^S \xrightarrow{\tilde{\pi}^S} \overline{G}^S \to 1.$$

The definition of C in terms of $\widehat{G}^S$ and $\overline{G}^S$ rather than in terms of $\widehat{\Gamma}$ and $\overline{\Gamma}$ has several advantages. First, it quickly shows that the congruence kernel is independent of the choice of a faithful K-representation $G \hookrightarrow \mathrm{GL}_N$. Second, we acquire an action of the group $G(K)$ on C, and the available structural information on $G(K)$ can be used to show that this action is trivial, in which case we say that C is *central*, i.e. is contained in the center of $\widehat{G}^S$ (see below). Third, one can identify $\overline{G}^S$. More precisely, the general case in the congruence subgroup can be reduced to the main case where G is absolutely almost simple and simply connected. So, henceforth we will assume that G is such, and besides we can of course assume that $\Gamma = G(\mathcal{O}_S)$ is infinite. Then it follows from the Strong Approximation Theorem that $\overline{G}^S$ can be identified with the group of S-adeles $G(\mathbb{A}_S)$ (the restricted topological product of the groups $G(K_v)$ for $v \in V^K \setminus S$ with respect to the open subgroups $G(\mathcal{O}_v)$). Here I would like to point out that the Strong Approximation Theorem was proved by Kneser and Platonov over number fields, and independently by Prasad and Margulis over global fields of positive characteristic. This brings us to the problem of analyzing topological extensions

$$\text{(C)} \qquad 1 \to C \longrightarrow \widehat{G} \xrightarrow{\pi} G(\mathbb{A}_S) \to 1$$

with a *profinite* kernel C. Another important feature of this sequence is that it splits over $G(K)$, and is in fact the universal extension with these properties. In order to get information about C one uses *duality*; more precisely, one considers the Hochschild-Serre spectral sequence of continuous cohomology with coefficients in $\mathbb{R}/\mathbb{Z}$ with trivial action (thus, $H^i(*) = H^i_{\mathrm{ct}}(*, \mathbb{R}/\mathbb{Z})$):

$$H^1(G(\mathbb{A}_S)) \xrightarrow{\varphi} H^1(\widehat{G}) \longrightarrow H^1(C)^{G(\mathbb{A}_S)} \xrightarrow{\psi} H^2(G(\mathbb{A}_S)).$$

Using the fact that the extension (C) splits over $G(K)$ and is universal, one shows that $\operatorname{Im}\psi$ coincides with the *metaplectic kernel*:

$$M(S, G) := \operatorname{Ker}(H^2(G(\mathbb{A}_S)) \xrightarrow{\text{res}} H^2(G(K))).$$

This brings us to the exact sequence

$$1 \to \operatorname{Coker}\varphi \longrightarrow H^1(C)^{G(\mathbb{A}_S)} \longrightarrow M(S, G) \to 1.$$

On the other hand, $\operatorname{Coker}\varphi$ can be described as

$$\operatorname{Hom}(\overline{[G(K), G(K)]}/[G(K), G(K)], \mathbb{R}/\mathbb{Z}),$$

the dual group for the finite abelian group $\overline{[G(K), G(K)]}/[G(K), G(K)]$ where the bar denotes the closure in the S-arithmetic topology. In many cases it is known that $G(K)$ is an almost simple abstract group (meaning no nontrivial noncentral normal subgroups), and then $G(K) = [G(K), G(K)]$, hence $\operatorname{Coker}\varphi = \{1\}$. In particular, this is always the case if G is K-isotropic, which follows from the truth of the Kneser-Tits Conjecture over global fields. Here I would like to mention Prasad's contributions to the investigation of the Kneser-Tits Conjecture. In a joint paper with M.S. Raghunathan, he reduced the general case of the conjecture to the relative rank one case. This easily implies the truth of it over local fields, and reduces it over global fields to the verification of a small number of cases, one of which (the isotropic triality forms of type D_4) was considered by Prasad himself. Furthermore, according to a conjecture due to Platonov and Margulis, which we call Conjecture (MP), $G(K)$ is expected to be almost simple for all groups of type different from A_n no matter whether it is isotropic or anisotropic, which again has been established in most cases (with the exception of anisotropic triality forms of type D_4 and most anisotropic forms of type E_6). For anisotropic groups of type A_n, it may happen that $G(K) \neq [G(K), G(K)]$ but according to (MP), the commutator subgroup is closed in the S-congruence topology provided that S does not contain any non-archimedean places v such that G is K_v-anisotropic (which we typically assume) - this has been proven for all inner forms and also some outer forms. So, in all those cases, $\operatorname{Coker}\varphi$ is known to be trivial, and conjecturally this is always the case. Then, of course,

$$H^1(C)^{G(\mathbb{A}_S)} \simeq M(S, G).$$

In practically all cases where C is known to be finite, its computation has been carried out in two steps. First, one proves that C is *central*, i.e. is contained in the center of $\widehat{G}$ (in some cases, it is relatively easy, in others it is less easy, but there are still cases where it is unknown). Then the action of $G(\mathbb{A}_S)$ on $H^1(C)$ is trivial, and we obtain that

$$H^1(C) = \mathrm{Hom}(C, \mathbb{R}/\mathrm{Z}),$$

which is the Pontrjagin dual of C, is isomorphic to $M(S, G)$. So, one concludes the computation of C by computing the metaplectic kernel.

While there are cases where the centrality is expected but has not been established yet, the metaplectic kernel has been computed in all cases needed for the CSP. The final result was obtained in our paper

G. Prasad, A. Rapinchuk, *Computation of the metaplectic kernel,* Publ. math. IHES **84**(1996), 91-187.

But it was preceded by a series of papers by Prasad and Raghunathan, in which they have provided complete local computations and also global computations in the isotropic case, as well as the important papers by Matsumoto, Moore and Deodhar.

Theorem 1. *Let G be an absolutely almost simple algebraic group over a global field K, and S be a set of places of K that contains all archimedean places if K is a number field, and nonempty if K is of positive characteristic. Then*

(a) *$M(S, G)$ is isomorphic to a subgroup of the group μ_K of all roots of unity in K. In particular, it is always finite, and hence the congruence kernel is finite once it is central;*

(b) *If S contains a place v_0 which is either nonarchimedean and G is K_{v_0}-isotropic, or is real and $G(K_{v_0})$ is not topologically simply connected, then $M(S, G)$ is trivial*[1].

Thus, if C is central then it is finite. Conversely, if C is finite, and we assume (MP), then C is central. So, the centrality of C is essentially equivalent to its finiteness.

If we assume that S contains no nonarchimedean anisotropic places, then the dichotomy for the congruence kernel can be made even sharper: it is either trivial (precisely in the situation as described in the theorem) or isomorphic to μ_K.

Let us also observe in passing that our results also cover the case where $S = \emptyset$ which is important for the theory of automorphic forms: it turns out that in this case $M(S, G)$ is always isomorphic to μ_K (this depends on one assumption for some outer forms of type A_n).

For illustration purpose, let us show how this theorem explains the previous examples.

Example. Let $G = \mathrm{SL}_n$, $n \geqslant 3$. Then for any K and any S as above, the congruence kernel $C = C^S(G)$ is central (see below).

- For $\Gamma = \mathrm{SL}_n(\mathbb{Z})$, we have $K = \mathbb{Q}$ and $S = \{v_\infty\}$ with v_∞ the real valuation. Since $\pi_1(\mathrm{SL}_n(\mathbb{R})) = \mathbb{Z}/2\mathbb{Z}$ (and, in particular, $\mathrm{SL}_n(\mathbb{R})$ is not topologically simply connected), we obtain $M(S, G) = \{1\}$, and therefore $C^S(G) = \{1\}$, as we stated above.
- For $\Gamma = \mathrm{SL}_n(\mathbb{Z}[\sqrt{2}])$ we have $K = \mathbb{Q}(\sqrt{2})$ and $S = \{v'_\infty, v''_\infty\}$ with v'_∞, v''_∞ being two real valuation. Again, since $\mathrm{SL}_n(\mathbb{R})$ is not topologically simply connected, we conclude that $M(S, G) \simeq C^S(G)$ is trivial.
- For $\Gamma = \mathrm{SL}_n(\mathbb{Z}[i])$, we have $K = \mathbb{Q}(i)$ and $S = \{v_\infty\}$ with v_∞ a single complex valuation. We obtain that $C^S(G) \simeq M(S, G) \simeq \mu_K$ which is a cyclic group of order 4.

[1] This, in particular, means that $M(S, G)$ is always trivial if S is infinite.

The proof of Theorem 1 uses a lot of ingredients and requires a case-by-case analysis. The following theorem summarizes the local computations carried out by Prasad and Raghunathan, the ambiguity in which was later eliminated by Prasad.

Theorem 2. *Let $\mathcal{K}$ be a nonarchimedean local field. For any absolutely almost simple simply connected $\mathcal{K}$-group $\mathcal{G}$, the group $H^2(\mathcal{G}(\mathcal{K}))$ is isomorphic to the group $\mu_{\mathcal{K}}$ of roots of unity in $\mathcal{K}$.*

I would like to conclude the talk with a couple of remarks about the problem of centrality of the congruence kernel. The main efforts here are focused on proving the following

Conjecture (Serre) *Let G be an absolutely almost simple simply connected algebraic group over a global field K, and let S be a set of valuations of K that contains all archimedean valuations if K is a number field and is nonempty if K has positive characteristic. If*

$$\mathrm{rk}_S\, G := \sum_{v \in S} \mathrm{rk}_{K_v}\, G \geqslant 2 \quad \textit{and} \quad \mathrm{rk}_{K_v}\, G > 0 \quad \textit{for all nonarchimedean} \quad v \in S$$

then $C^S(G)$ is finite (equivalently, central).

(In particular, $C^S(G)$ is expected to be trivial whenever S is infinite provided that it does not contain any anisotropic nonarchimedean places for G.)

Serre's conjecture has been proven in quite a few cases using a variety of techniques but it still remains open, for example, for the norm 1 groups associated with division algebras (even quaternion division algebras). I would like to show you our result on centrality that does not require any case-by-case considerations. To put this result in perspective, we recall that the congruence completion $\overline{G}$ can be identified with the group of S-adeles $G(\mathbb{A}_S)$. This implies that for any $v_1, v_2 \in V^K \setminus S$, $v_1 \neq v_2$, the groups $G(K_{v_1})$ and $G(K_{v_2})$ can be naturally embedded into $\overline{G}$ so that the images of these embeddings commute inside $\overline{G}$. The theorem below says that if the arithmetic completion $\widehat{G}$ has a similar structure.

Theorem 3. *Let G, K and S be as above, and assume that (MP) holds for G/K and S contains no nonarchimedean anisotropic places for G. Suppose that for every $v \notin S$, there exists a subgroup $\mathcal{G}_v$ of $\widehat{G}$ so that the following conditions are satisfied:*

(i) *$\pi(\mathcal{G}_v) = G(K_v)$ for all $v \notin S$, where $\pi \colon \widehat{G} \to \overline{G}$ is as above;*

(ii) *$\mathcal{G}_{v_1}$ and $\mathcal{G}_{v_2}$ commute elementwise for all $v_1, v_2 \notin S$, $v_1 \neq v_2$;*

(iii) *the subgroup generated by the $\mathcal{G}_v$ for $v \notin S$ is dense in $\widehat{G}$.*

Then $C^S(G)$ is central in $\widehat{G}$.

(Essentially, this means that the existence of the elementwise commuting lifts of the local groups $G(K_v)$ implies that the congruence kernel is central.)

This theorem enables one to quickly check the centrality for $G = \mathrm{SL}_n$, $n \geqslant 3$. The argument uses only the well-known commutator relations for elementary matrices in conjunction with the fact that for $v_1, v_2 \notin S$ and $a \in K_{v_1}$ and $b \in K_{v_2}$ we have $a \cdot b = 0$ in $\mathbb{A}_S$. We refer to our survey paper for the details. This argument extends to all Chevalley groups of rank > 1, to SL_2 if the group of S-units $\mathcal{O}_S^{\times}$ is infinite, and some other situations.

As we pointed out, Serre's conjecture implies that $C^S(G)$ should be trivial for any infinite S. What we can prove is that it is trivial for *some* infinite S, viz. when S almost contains a generalized arithmetic progression (with one technical restriction on the progression if G is an outer form). Here generalized arithmetic progressions are defined in terms of the Frobenius automorphism of a given finite (but not necessarily commutative Galois extension).

Finally, here is one interesting result in the case where the congruence kernel is infinite. As we mentioned above, for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, the congruence kernel C is the free profinite group of countable rank[2]. However, using some variations of Theorem 3 one shows that as a *normal* subgroup of $\widehat{G}$ it is generated by a *single* element. Similar facts are available for other groups of relative rank one.

[2] In fact, in the situation at hand, we have the following dichotomy: the congruence kernel is either finite or is not finitely generated