The congruence subgroup problem

B. Sury

Abstract | This article is an exposition on the 'congruence subgroup problem'. This subject is at a common ground shared by group theory and number theory. It deals with certain groups defined arithmetically and their subgroup structure. This is a relatively modern subject having taken off in the mid 1960's after Klein's early investigations on the modular group. Apart from interest in its own right, the subject gains importance also because of connections with the theory of automorphic forms which is central to number theory. This exposition is meant to introduce the subject to professional mathematicians working in other areas. At the end, some recent work by the author is mentioned.

1. Introduction

If one views $\mathbf{Z}$ simply as a discrete subgroup of $\mathbf{R}$, many of its number-theoretic properties lie hidden. For instance, to 'see' prime numbers, one needs to use some other topology on $\mathbf{Z}$. This is the so-called *profinite* (or artihmetic) topology. Here, arithmetic progressions form a basis of open sets. The Chinese remainder theorem essentially tells us that the arithmetic topology is 'built out of' various p-adic topologies for all the primes p. More precisely, any subgroup of finite index in $\mathbf{Z}^n$ evidently contains $k\mathbf{Z}^n$ for some natural number k. The congruence subgroup problem is a question which asks whether this property generalises to vastly general groups. As we shall see, an affirmative answer would again amount to the 'topology given by subgroups of finite index being built out of the p-adic topologies'. If one considers a matrix group with integral entries, say, $SL_n(\mathbf{Z})$, for some $n \geq 2$, one natural way of finding a subgroup of finite index is to look at the natural ring homomorphism $\mathbf{Z} \to \mathbf{Z}/k\mathbf{Z}$ for a natural number k and look at the kernel of the corresponding group homomorphism $SL_n(\mathbf{Z}) \to SL_n(\mathbf{Z}/k\mathbf{Z})$. This is known as the principal congruence subgroup of level k, for obvious reasons. Any subgroup of $SL_n(\mathbf{Z})$ which contains a principal congruence subgroup of some level is called a congruence subgroup. Congruence subgroups show up in many situations in number theory. For instance, the main step in Wiles's proof of Fermat's last theorem is to obtain a non-constant meromorphic map from the quotient of the upper half-plane by a suitable congruence subgroup into an elliptic curve defined over $\mathbf{Q}$. In fact, the classical theory of modular forms and Hecke operators which plays such a central role in number theory is a theory which 'lives' on congruence subgroups. Interestingly, this fact that Hecke operators essentially live on subgroups of the modular group already requires the solution of the congruence subgroup problem for the so-called Ihara modular group $SL_2(\mathbf{Z}[1/p])$, as shown by Serre and Thompson. Suffice it to say that

congruence subgroups are important in number theory.

1.1. *A naive form of the congruence subgroup problem*

The first question one may ask is whether all subgroups of finite index in $SL_n(\mathbf{Z})$ are congruence subgroups. Note that the question is meaningful because of the existence of plenty of congruence subgroups in the sense that their intersection consists just of the identity element. Already in the late 19th century, Fricke and Klein showed that the answer to this question is negative if $n = 2$. Indeed, since the free group of rank 2 is the principal congruence subgroup $\Gamma(2)$ of level 2, any 2-generated finite group is a quotient of this group. But there are many finite, simple 2-generated groups (like A_n $(n > 5)$, $PSL_3(\mathbf{Z}/q\mathbf{Z})$ for prime q) which are quotients of $\Gamma(2)$ where the corresponding kernel cannot be a congruence subgroup of $SL_2(\mathbf{Z})$. One way to see this is to use the fact that any simple, non-abelian quotient group of $\Gamma(2)$ by a congruence subgroup must be of the form $PSL_2(\mathbf{F}_p)$ where $\mathbf{F}_p$ is the finite field with p elements and observe that there are 2-generated finite simple groups different from $PSL_2(\mathbf{F}_p)$ for any p. Indeed, for $n > 5$, even the order of A_n cannot be be equal to that of any of these groups. As $PSL_2(\mathbf{F}_p)$ has abelian q-Sylow subgroups for all odd primes q whereas a group like $PSL(3, \mathbf{Z}/q\mathbf{Z})$ has non-abelian q-Sylow subgroups, the latter group is a quotient of $\Gamma(2)$ by a non-congruence subgroup. Thus, $SL_2(\mathbf{Z})$ has non-congruence subgroups, of finite index. In fact, it can be shown that there are many more noncongruence subgroups of finite index in $SL_2(\mathbf{Z})$ than there are congruence subgroups. It was only in 1962 that Bass–Lazard–Serre—and, independently, Mennicke—showed that the answer to the question is affirmative when $n \geq 3$. Later, in 1965, Bass–Milnor–Serre generalised this to the special linear and the symplectic groups over number fields.

Mennicke showed later that subgroups of finite index in $SL_2(\mathbf{Z}[1/p])$ are congruence subgroups and this is the principal reason behind the fact asserted above that the classical Hecke operators for $SL(2, \mathbf{Z})$ live only on congruence subgroups.

2. Arithmetic and congruence groups in algebraic groups

Let us first say how the question can be posed for general (linear) algebraic groups over a number field k. The algebraic groups we consider are all linear (therefore, affine) algebraic groups; the formulation for abelian varieties is quite different. Recall that an algebraic group defined over k (considered as a subfield of $\mathbf{C}$) is a subgroup G of $GL(N, \mathbf{C})$ which is also the set of common zeroes of a finite set of polynomial functions $P(g_{ij}, det(g)^{-1})$ in $N^2 + 1$ variables with coefficients from k. The definition has to be slightly modified if k is a field of positive characteristic. The group $G(k) = G \cap GL(N, k)$ turns out to be defined independent of the choice of embedding $G \subset GL(N, \mathbf{C})$ and, is called the abstract group of k-points of G.

Here are some standard examples of algebraic groups defined over a subfield k of $\mathbf{C}$.

(i) $G = GL(n, \mathbf{C})$.

(ii) $G = SL(n, \mathbf{C}) = Ker(det : GL(n, \mathbf{C}) \to \mathbf{C}^*)$.

(iii) For any symmetric matrix $M \in GL(n, k)$, the orthogonal group

$$O(M) = \{g \in GL(n, \mathbf{C}) : {}^t gMg = M\}.$$

(iv) For any skewsymmetric matrix $\Omega \in GL(2n, k)$, the symplectic group

$$Sp(\Omega) = \{g \in GL(2n, \mathbf{C}) : {}^t g\,\Omega g = \Omega\}.$$

(v) Let D be a division algebra with center k (its dimension as a k-vector space must be n^2 for some n). Let $v_i; 1 \leq i \leq n^2$ be a k-basis of D (then it is also a $\mathbf{C}$-basis (as a vector space) of the algebra $D \otimes_k \mathbf{C}$). The right multiplication by v_i gives a linear transformation R_{v_i} from $D \otimes_k \mathbf{C}$ to itself, and thus, one has elements $R_{v_i} \in GL(n^2, \mathbf{C})$ for $i = 1, 2, \ldots, n^2$.

$$G = \{g \in GL(n^2, \mathbf{C}) : gR_{v_i} = R_{v_i} g \quad \forall\, i = 1, 2, \ldots, n^2\}.$$

This last group has its $G(k) =$ the nonzero elements of D.

Henceforth, k will denote an algebraic number field. Let $G \subset SL_n$ be a k-embedding of a linear algebraic group. If O_k denotes the ring of algebraic integers in k, we denote by $G(O_k)$, the group $G \cap SL_n(O_k)$. For any non-zero ideal I of O_k, one has the normal subgroup $G(I) = \mathrm{Ker}(G(O_k) \to SL_n(O_k/I))$ of finite index in $G(O_k)$. Note that it is of finite index because the ring O_k/I is finite.

Then, one could define a subgroup of $G(O_k)$ to be a congruence subgroup if it contains a subgroup of the form $G(I)$ for some non-zero ideal I. The only problem is that, unlike $G(k)$, the definitions of $G(O_k)$ and $G(I)$ etc. depend on the k-embedding we started with. However, it turns out that for a new k-embedding, the 'new' $G(O_k)$ contains an 'old' $G(I)$ for some $I \neq 0$. Thus, the following definition is independent of the choice of the k-embedding:

A subgroup Γ of $G(O_k)$ is a congruence subgroup if $\Gamma \supset G(I)$ for some $I \neq 0$.

The group $G(O_k)$ can be realised as a discrete subgroup of a product $G(\mathbf{R})^{r_1} \times G(\mathbf{C})^{r_2}$ of Lie groups, where k has r_1 real completions and r_2 non-conjugate complex completions. More generally, let S be any finite set of inequivalent valuations containing all the above archimedean valuations. The nonarchimedean valuations in S correspond to nonzero prime ideals of O_k. One has the bigger ring O_S of S-units of k; these are the elements of k which admit denominators only from primes in S. One may define $G(O_S) = G \cap SL_n(O_S)$; then $G(O_S)$ is a discrete subgroup of the product $\prod_{v \in S} G(k_v)$ of real, complex and p-adic Lie groups, where k_v denotes the completion of k with respect to the valuation v.

One calls a subgroup $\Gamma \subset G(O_S)$ an S-congruence subgroup if and only if it contains $G(I)$ (the elements of $G(O_S)$ which map to the identity element in $G(O_S/I)$) for some nonzero ideal I of O_S. Of course, $G(O_S)$ itself depends on the k-embedding of G chosen.

Hence, the most general definition is the following:

A subgroup $\Gamma \subset G(k)$ is an S-congruence subgroup if, for some (and, therefore, any) k-embedding of G, the group Γ contains $G(I)$ as a subgroup of finite index for some nonzero ideal I of O_S.

One also defines:

A subgroup $\Gamma \subset G(k)$ is an S-arithmetic subgroup if, for some (and, therefore, any) k-embedding, Γ and $G(O_S)$ are commensurable (i.e., $\Gamma \cap G(O_S)$ has finite index in both groups).

3. The congruence kernel

Each of the two families (the S-arithmetic groups and the S-congruence groups) defines a topology on $G(k)$ as follows. For any $g \in G(k)$, one defines a fundamental system of neighbourhoods of g to be the cosets $gG(I)$ as I varies over the nonzero ideals of O_S. This topology T_c is called the S-congruence topology on $G(k)$. If one takes a fundamental system of neighbourhoods of g to be the cosets $g\Gamma$ as Γ varies over S-arithmetic subgroups of $G(k)$, the corresponding topology T_a is called the S-arithmetic topology. As S-congruence subgroups are S-arithmetic subgroups, T_a is finer. Note that T_a just gives the profinite topology on $G(O_S)$. If the resulting completions of (uniform structures on) $G(k)$ are denoted by $\hat{G}_a$ and $\hat{G}_c$, then there is a continuous surjective homomorphism from $\hat{G}_a$ onto $\hat{G}_c$. Obviously, this is an isomorphism if all subgroups of finite index in $G(O_S)$ are S-congruence subgroups. In general, the kernel $C(S, G)$ of the above map, called the *S-congruence kernel*, measures the deviation.

A basic important property is that $C(S, G)$ is a profinite group. In fact, the closures $\widehat{\Gamma}_a$, $\widehat{\Gamma}_c$ of $G(O_S)$ in $\hat{G}_a$ and $\hat{G}_c$ respectively, are profinite groups and $C(S, G) \subset \widehat{\Gamma}_a$. The congruence subgroup problem (CSP) is the problem of determining the group $C(S, G)$ for any S, G.

4. Margulis–Platonov conjecture

There is a conjecture due to Serre which predicts precisely when the group $C(S, G)$ is finite. The finiteness of $C(S, G)$ has many interesting consequences as we shall soon see. Before going into it, we note that when $C(S, G)$ is trivial, all S-arithmetic subgroups are S-congruence subgroups. For any S, the association $G \mapsto C(S, G)$ is a functor from the category of k-algebraic groups to the category of profinite groups. Given G, a general philosophy (which can be made very precise) is that the larger S is, the 'easier' it is to compute $C(S, G)$. In fact, when S consists of all the places of k excepting the (finitely many possible) nonarchimedean places T for which $G(k_v)$ is compact (for the topology induced from k_v), the computation of $C(S, G)$ amounts to a conjecture of Margulis & Platonov which has been proved in most cases. In fact, in most cases T is empty which means that the triviality of $C(S, G)$ (for the S mentioned last) is equivalent to the simplicity of the abstract group $G(k)/center$. One important case where the Margulis–Platonov conjecture has still not been proved is that of the special unitary group of a division algebra with center k and with an involution of the second kind. The following people have contributed to the proof of the MP conjecture for the other cases: Borovoi, Chernousov, Liebeck, Margulis, Platonov, Raghunathan, Rapinchuk, Segev, Seitz, Sury and Tomanov.

5. Necessary conditions for finiteness

First, we briefly indicate how the CSP for a general group reduces to CSP for certain types of groups. The problem easily reduces to connected algebraic groups G and, further, to the reductive group $G/R_u(G)$ using nothing more than the Chinese remainder theorem. Here, the unipotent radical $R_u(G)$ of G is the maximal, normal, connected, unipotent subgroup. A reductive k-group G contains a central k-torus T (an algebraic k-torus is a connected, abelian k-subgroup $\mathbf{C}$-isomorphic to products of k^*) so that G/T is a semisimple group. For tori T, the congruence

kernel $C(S,T)$ is trivial—this is a theorem due to Chevalley and is essentially a consequence of Chebotarev's density theorem in global class field theory. Hence, the problem reduces to that for semisimple groups. For semisimple G, the group $G(O_S)$ (for any embedding) can be identified with a lattice in the group $G_S := \prod_{v\in S} G(k_v)$ under the diagonal embedding of $G(k)$ in G_S. That is, the quotient space $G_S/G(O_S)$ has a finite, G_S-invariant measure.

Finally, it is necessary (as observed by Serre) for the finiteness of $C(S,G)$ that G be simply-connected as an algebraic group—that is, there is no k-algebraic group $\tilde{G}$ admitting a surjective k-map $\pi : \tilde{G} \to G$ with finite nontrivial kernel. This is actually equivalent to $G(\mathbf{C})$ being simply-connected in the usual sense. Further, if one can compute $C(S,\tilde{G})$ for a simply-connected 'cover' $\tilde{G}$ of G, then one can compute $C(S,G)$. Thus, the CSP reduces to the problem for semisimple, simply-connected groups.

If G is simply-connected and the group $\prod_{v\in S} G(k_v)$ is noncompact (equivalently, $G(O_S)$ is not finite), one has the strong approximation property. This means that the closure $\widehat{\Gamma}_c$ of $G(O_S)$ with respect to T_c can be identified with $\prod_{v\notin S} G(O_v)$. Here O_v is the local ring of integers in the p-adic field k_v. Thus, if $C(S,G)$ is trivial, the profinite completion of $G(O_S)$ is also equal to $\prod_{v\notin S} G(O_v)$.

Thus, roughly speaking, when the congruence kernel is trivial the topology given by subgroups of finite index is built out of the p-adic topologies as asserted in the introduction.

For $G(k)$ itself, strong approximation means that G_c can be identified with the 'S-adelic group' $G(A_S)$, the restricted direct product of all $G(k_v)$, $v \notin S$ with respect to the open compact subgroups $G(O_v)$. The reason that G must be simply-connected in order that $C(S,G)$ be finite, is as follows. Let there exist a k-map: $\tilde{G} \to G$ with kernel μ and $\tilde{G}$ simply-connected. Now, the S-congruence completion $\tilde{G}_c$ can be identified with the S-adelic group $\tilde{G}(A_S)$. If π is the homomorphism from the S-arithmetic completion $\tilde{G}_a$ to $\tilde{G}_c = \tilde{G}(A_S)$, then it is easy to see that $C(S,G)$ contains the infinite group $\pi^{-1}(\mu(A_S))/\mu(k)$.

As mentioned at the beginning, subgroups of finite index in $SL(n,\mathbf{Z})$ are congruence subgroups when $n \geq 3$ while this is not so when $n = 2$. What distinguishes these groups qualitatively is their rank.

If $G \subset SL_n$ is a k-embedding, one calls a k-torus T in G to be k-split, if there is some $g \in G(k)$ such that gTg^{-1} is a subgroup of the diagonals in SL_n. The maximum of the dimensions of the various k-split tori (if they exist) is called the k-rank of G. For example, k-rank $SL_n = n-1$ and k-rank $Sp_{2n} = n$. If F is a quadratic form over k, it is an orthogonal sum of an anisotropic form over k and a certain number r of hyperbolic planes (r is called the Witt index of F), by Witt's classical theorem. Then, the group $SO(F)$ is a k-group whose k-rank is this same r.

6. Serre's conjecture

Let us consider a general semisimple, simply-connected k-group G. Assume that G is absolutely almost simple (that is, G has no connected normal algebraic subgroups). For a finite S containing all the archimedean places, Serre formulated the characterisation of the congruence subgroup property (that is, the finiteness of $C(S,G)$) conjecturally as follows. First, it is easy to see that a necessary condition for finiteness of $C(S,G)$ is that for any nonarchimedean place v in S, the group G has k_v-rank > 0 (equivalently, $G(k_v)$ is not profinite by a theorem of Bruhat-Tits-Rousseau). Indeed, otherwise the whole of $G(k_v)$ is a quotient of $C(S,G)$.

Conjecture 1 (Serre). *$C(S,G)$ is finite if, and only if, S-rank$(G) := \sum_{v\in S} k_v - \mathrm{rank}(G) \geq 2$ and $G(k_v)$ is noncompact for each nonarchimedean $v \in S$.*

When $C(S,G)$ is finite, one says that the CSP is solved affirmatively or that the congruence subgroup property holds for the pair (G,S).

As mentioned in the introduction, for $k = \mathbf{Q}$, $S = \{\infty, p\}$ for some prime p and $G = SL_2$, the CSP was solved affirmatively by Mennicke and this fact can be used to show (as was done by Serre and Thompson) that the classical theory of Hecke operators 'lives' only on congruence subgroups of $SL_2(\mathbf{Z})$.

It should be noted that the finitness of $C(S,G)$ as against its being actually trivial, already has strong consequences. One, pointed by Serre, is super-rigidity; this means:

If $C(S,G)$ is finite, then any abstract homomorphism from $G(O_S)$ to $GL_n(\mathbf{C})$ is essentially algebraic. In other words, there is a k-algebraic group homomorphism from G to GL_n which agrees with the homomorphism we started with, at least on a subgroup of finite index in $G(O_S)$. In particular, $\Gamma/[\Gamma,\Gamma]$ is finite for every subgroup of finite index in $G(O_S)$.

This last fact has already been used to prove in some cases that $C(S,G)$ is NOT finite, by producing a Γ of finite index which surjects onto $\mathbf{Z}$.

7. Relation with cohomology

Consider the exact sequence defining $C(S,G)$. Recall that the strong approximation theorem for $G(k)$ means G_c can be identified with the 'S-adelic

group' $G(A_S)$, the restricted direct product of all $G(k_v), v \notin S$ with respect to the open compact subgroups $G(O_v)$. Thus, we have the exact sequence

$$1 \to C(S,G) \to \hat{G_a} \to G(A_S) \to 1$$

which defines $C(S,G)$. By looking at continuous group cohomology H^i with the universal coefficients $\mathbf{R}/\mathbf{Z}$, one has the corresponding Hochschild–Serre spectral sequence which gives the exact sequence

$$H^1(G(A_S)) \to H^1(\hat{G_a}) \to H^1(C(S,G))^{G(A_S)} \to H^2(G(A_S)).$$

Now, the congruence sequence above splits over $G(k)$, the last map actually goes into the kernel of the restriction map from $H^2(G(A_S))$ to $H^2(G(k))$. So, if α denotes the first map, then we have an exact sequence

$$1 \to \text{Coker}\alpha \to H^1(C(S,G))^{G(A_S)} \to Ker(H^2(G(A_S) \to H^2(G(k))).$$

Here $G(k)$ is considered with the discrete topology. The last kernel is called the S-metaplectic kernel and it is a finite group. It had been computed for several cases by Gopal Prasad and Raghunathan and now, it has been computed in all cases by Gopal Prasad and Rapinchuk. The cokernel of α is nothing but the S-arithmetic closure of $[G(k), G(k)]$; hence it is also a finite group since $[G(k), G(k)]$ has finite index in $G(k)$. In fact, one expects the cokernel to be trivial, and this is known in most cases. Therefore, the middle term $H^1(C(S,G))^{G(A_S)}$ is finite. But, this shows that the the quotient $C(S,G)/[C(S,G), \hat{G_a}]$ is finite. In fact, we have:

$C(S,G)$ is finite if, and only if, it is contained in the center of $\hat{G_a}$.

The centrality of $C(S,G)$ has been proved for all cases of S-rank at least 2 other than the important case of groups of type A_n which have k-rank 0.

Several people like Clozel, Labesse, J-S Li, Lubotzky, Millson, Gopal Prasad, Raghunathan, Schwermer & Venkataramana have proved vanishing results for cohomology of lattices in Lie groups and the techniques of the CSP can often be applied. For instance, Raghunathan and Venkataramana established the existence of cocompact arithmetic lattices Δ in $SO(n,1)$ $(n \geq 5, n \neq 7)$ for which $H^1(\Delta, \mathbf{C}) \neq 0$. It is relevant to recall a famous old conjecture of Thurston to the effect that any compact (real) hyperbolic manifold admits a finite covering with non-vanishing first Betti number. The various results mentioned here prove it except for 3-manifolds. The connection with CSP arises in the approach of Raghunathan and Venkataramana (and in later work by Venkataramana) as follows. Embed the real hyperbolic manifold in a suitable complex hyperbolic manifold. That the latter admits a 'congruence' covering with non-vanishing first Betti number is a result of Kazhdan using his property T. More precisely, (the later refinement of Venkataramana asserts):

If $H \subset G$ are Q-simple and $H(R) = SO(n,1)$ and $G(R) = SU(n,1)$, and Γ is a congruence subgroup of $G(Q)$, then the restriction of $H^1(\Gamma, C)$ to the product of $H^1(g\Gamma g^{-1} \cap H, C)$ over all $g \in G(Q)$, is injective.

The idea is to prove that the translates of $C(S,H)$ under the group $(AutG)(Q)$ topologically generate a subgroup of finite index in $C(S,G)$.

There are other connections with cohomology in the form of Kazhdan's property T, and Selberg's property for minimal eigenvalue of Laplacian etc. where Alex Lubotzky is one of the principal contributors. For instance, Thurston's famous conjecture on the first Betti number is solved for a number of cases by Lubotzky using these techniques.

8. Profinite group theory

Since $C(S,G)$ is a profinite group, it is conceivable that one can use general results on profinite groups profitably. This is indeed the case. In fact, one can characterise the centrality by means of purely profinite-group-theoretic conditions. Platonov & Rapinchuk proved that $C(S,G)$ is finite if, and only if, the profinite group $\widehat{\Gamma_a}$ has bounded generation. In other words, there are elements $x_1, \cdots, x_r$ (not necessarily distinct) in Γ so that the set $\overline{<x_1>} \cdots \overline{<x_r>}$ coincides with the whole group $\widehat{\Gamma_a}$. The fore-runner of this result (which was used by them crucially) is the theorem of Lazard to the effect that among pro-p groups (for any prime p), the Lie groups are characterised as those admitting bounded generation as above. After the solution of the restricted Burnside problem, one also has other characterisations for analyticity of pro-p groups like the number of subgroups of any given index being a polynomial function of the index. These can also be adapted to characterise the finiteness of $C(S,G)$ in terms of *polynomial index growth* for $\widehat{\Gamma_a}$.

Another characterisation was conjectured by Lubotzky and proved by Platonov and Sury. The following general result turns out to be true: *a (topologically) finitely generated profinite group Δ which can be continuously embedded in the S-adelic group $\prod_p SL(n, \mathbf{Z}_p)$ for some n, has bounded generation.* A special case of this, proved by Platonov

and Sury, was sufficient to prove Lubotzky's conjecture that $C(S,G)$ is finite if, and only if, $G(O_S)$ can be continuously embedded in the S-adelic group $\prod_p SL(n,\mathbf{Z}_p)$ for some n.

Aspects of subgroup growth have turned out to have deep relations with the CSP. Many such have emerged from the works of Alex Lubotzky and collaborators. For instance, apart from revealing finer structural facts like the number of noncongruence subgroups being a higher order function (in a more precisely known form) than the number of congruence subgroups (when CSP does not hold), the methods allow an analogue of the CSP to be asked for lattices (even nonarithmetic ones!) in semisimple Lie groups, viz.,

If Γ is a lattice in a semisimple Lie group over a local field (of characteristic 0), is the subgroup growth type of Γ strictly less than $n^{\log n}$?

Such results as well as others like polynomial subgroup growth etc. are described in the recent book [LS] where a number of open problems are also mentioned.

An unexpected connection of the CSP with cohomology of finite simple groups is revealed by some recent work of Alex Lubotzky. For a finite group A, denote by $h(A)$, the supremum of the number $\frac{dim H^2(A,M)}{dim M}$ over all primes p and all simple $\mathbf{F}_p[G]$-modules M. Derek Holt had proved that for any finite simple group A, there is a bound $h(A) = O(log|A|)$; he conjectured that there is a constant $c > 0$ such that $h(A) \leq c$ for all finite simple groups A. Partial results can be obtained from the methods of the CSP. For instance, if G is a fixed simple Chevalley scheme, then there is a constant $c > 0$ such that $h(G(\mathbf{F}_p)/center) \leq c$ for all primes p. The idea is to obtain the finite groups $G(\mathbf{F}_p)$ as quotients of the congruence completion of $G(Z)$.

9. Status of finiteness of $C(S,G)$

For the classical case of $SL_n(\mathbf{Z})$ with $n \geq 3$, centrality can be proved with the help of elementary matrices and reduction to SL_{n-1}. The key fact here is that any unimodular integral vector c which satisfies $c \equiv e_n \bmod r$ must be in the orbit of $E_n(r)$, the normal subgroup generated by those elementary matrices which are in the principal congruence subgroup $\Gamma(r)$ of level r. For general G whose k-rank is nonzero, there are unipotent elements in $G(k)$ which play the role of the elementary matrices and which allow for similar (although much harder) proofs. For the groups of k-rank 0, there are no unipotents and one needs to work with concrete descriptions of them as unitary groups of hermitian forms etc. Apart from the list mentioned in the discussion of MP conjecture, Bak, Rehmann and Kneser have made crucial contributons.

The proofs have been shortened and simplified by Gopal Prasad and Rapinchuk recently. Their arguments bring out the essential feature that centrality hinges on locating subgroups G_v in the S-arithmetic completion $\widehat{G}_a$, for each place $v \notin S$ which pairwise commute and map onto $G(k_v)$.

Most of what we discussed earlier for number fields is also valid for global fields of positive characteristic; these are finite extensions of $F_q(t)$. Note that in the positive characteristic case, every valuation of k is nonarchimedean. One must remember though that lattices may not be finitely generated and that the congruence subgroup property fails for unipotent groups.

The centrality/finiteness of $C(S,G)$ (for the cases where it is conjectured to be finite) is still open for two very important cases where new ideas may be required but these cases have a lot of relevance to the theory of automorphic forms. These two cases are: (i) $G = SL(1,D)$ for a division algebra with center k, and (ii) $G = SU(1,D)$ where D is a division algebra with a center K which is a quadratic extension of k and D has a K/k-involution.

10. Structure of $C(S,G)$ when it is infinite

One theme which has been exploited in proving finiteness of $C(S,G)$ is: *If $C(S,G)$ is not finite, it has to be really huge.*

This can be used to show that if $C(S,G)$ is infinite, it is infinitely generated as a profinite group. Melnikov used results on profinite groups to prove that, for $SL_2(\mathbf{Z})$, one has $C(\{\infty\}, SL_2) \cong \hat{F}_\omega$, the free profinite group of countably infinite rank. This proof uses the existence of a central element of order 2 in $SL_2(\mathbf{Z})$ and a general result about free profinite groups. We note that although the profinite completion of a free group of finite rank r is the free profinite group of rank r, the profinite completion of a free group of countably infinite rank is not the group $\hat{F}_\omega$ appearing here. The profinite completion is much larger and, the group $\hat{F}_\omega$ can be constructed from a countably infinite set X by looking at the free group $F(X)$ and at only those normal subgroups of finite index in $F(X)$ which contain all but finitely many elements of X.

One further distinction between the case of free profinite groups and those of (discrete) free groups is that closed subgroups of free profinite groups may not be free profinite. For instance, $\mathbf{Z}_p$ is a closed subgroup of $\hat{\mathbf{Z}}$.

This result of Melnikov is an isolated one and does not give a general method. We assume now that

k_v-rank $(G) = 1$ for some nonarchimedean place $v \in S$ and that $G(k_w)$ is compact (equivalently, k_w-rank $(G) = 0$) for all $w \in S - \{v\}$. Then, the S-rank of G (the sum of the local ranks for the places in S) is 1 and $C(S, G)$ should be infinite. The projection Γ of $G(O_S) \subset \prod_{w \in S} G(k_w)$ into $G(k_v)$ is a lattice in it. In other words, for any choice of left Haar measure for the locally compact group $G(k_v)$, the corresponding quotient space $G(k_v)/\Gamma$ has finite $G(k_v)$-invariant measure. The group $G(k_v)$ acts simplicially on a tree, known as its Bruhat–Tits tree (for groups of rank r over k_v, the corresponding object is a rank r building). Hence, one can use the Bass-Serre theory of groups acting on trees to try to study the structure of lattices in $G(k_v)$.

First, a basic theorem of Bass-Serre theory tells us that when a group Γ acts on a tree X, there is a graph of groups (Γ, Y) associated with the quotient graph Y such that Γ is the fundamental group of this graph of groups. The main advantage of this is that one can obtain a presentation for Γ. For instance, this is an easy and natural way of proving that $PSL_2(\mathbf{Z})$ is a free product of $\mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/3\mathbf{Z}$. In fact, the notion of fundamental group of a graph of groups generalises free groups and free products with amalgamation. Here, a graph of groups (Γ, Y) simply means that Y is a connected graph, and there are groups Γ_v (vertex stabilisers) and Γ_e (edge stabilisers) corresponding to each vertex v and each edge e of Y along with inclusions of Γ_e in the vertex stabilisers for both the origin vertex and the terminus vertex.

Classically, one has symmetric spaces associated to semisimple Lie groups and for an arithmetic subgroup of a $\mathbf{Q}$-group G the construction of a fundamental domain for its action on the symmetric space provided a presentation. Garland and Raghunathan had constructed fundamental domains for $\mathbf{R}$-rank 1 groups and Raghunathan also constructed fundamental domains in rank 1 groups in positive characteristic. Then, one has:

Let G, k, S be as above and let X denote the associated Bruhat-Tits tree. Then, the quotient graph X/Γ is a union of a finite graph with finitely many infinite rays.

If characteristic of k is zero (that is k is a finite extension of $\mathbf{Q}_p$), it is a fact that lattices in $G(k_v)$ must be cocompact. Note this departure from the case of real and complex groups where one has both uniform (another name for cocompact) and nonuniform lattices. The reason for this is that one can find large open compact subgroups of $G(k_v)$ which are torsion-free. For example, the subgroup of $SL_n(\boldsymbol{Q}_p)$ consisting of matrices A with entries in $\mathbf{Z}_p$ such that $a_{ii} \in 1 + p\mathbf{Z}_p$, $a_{ij} \in p\mathbf{Z}_p$ for $i \neq j$ is such a group when p is odd.

On the other hand, when characteristic of k is positive, there could exist nonuniform lattices. An example is the group $SL_2(\mathbf{F}_p((t)))$ in which $SL_2(\mathbf{F}_p[t^{-1}])$ is a nonuniform lattice.

Lubotzky used Raghunathan's results and proved a structure theorem for the quotient graph of groups (Γ, Y) where Γ is a lattice in $G(k_v)$ for G of rank 1 over a nonarchimedean local field k_v, and Y is the quotient graph of the Bruhat-Tits tree of $G(k_v)$ by Γ. From this, he deduced a structure theorem for the lattice and concluded that when Γ is arithmetic, then a subgroup of finite index in Γ maps onto $\mathbf{Z}$. This already implies that Γ does not satisfy the congruence subgroup property as we noted earlier.

In joint work with Alec Mason, Alexander Premet and Pavel Zalesskii, we completely determine the structure of $C(S, G)$ when G, S are as above—that is, so that $G(O_S)$ can be identified with a lattice in $G(k_v)$ for some nonarchimedean completion k_v. We use group actions on trees and profinite analogues as well as a detailed analysis of unipotent radicals in every rank 1 group over a local field of positive characteristic, to deduce the following structure theorem:

Theorem 1 (Ref. [29]). *Let G, k, S be as above, with S-rank $(G) = 1$. Then,*

(i) if $G(O_S)$ is cocompact in $G(k_v)$ (in particular, if char. $k = 0$), then $C(S, G) \cong \hat{F_\omega}$, and

(ii) if $G(O_S)$ is nonuniform (therefore, necessarily char. $k = p > 0$), then $C(S, G) \cong \hat{F_\omega} \sqcup T$, a free profinite product of a free profinite group of countably infinite rank and of the torsion factor T which is a free profinite product of groups, each of which is isomorphic to the direct product of $2^{\aleph_0}$ copies of $\mathbf{Z}/p\mathbf{Z}$.

A surprising consequence of the theorem is that $C(S, G)$ depends only on the characteristic of k when $G(\mathcal{O}_S)$ is a lattice in a rank 1 group over a nonarchimedean local field.

As a by-product of the above result, we also obtain the following result which is of independent interest:

Theorem 2. *Let U be the unipotent radical of a minimal k_v-parabolic subgroup of G where G is as in (ii) above, then either U is abelian or is automatically defined over k.*

We recall what a free profinite product is and also some important facts about profinite groups which we need.

The free profinite product $G_1 \sqcup \cdots \sqcup G_n$ of profinite groups $G_1, \ldots, G_n$ can be defined by an obvious universal property but it can also be

constructed as the completion of the free product $G_1 * \cdots * G_n$ with respect to the topology given by the collection of all normal subgroups N of finite index in the free product such that $N \cap G_i$ is open in G_i for each i.

One has the profinite counterpart of Schreier's formula:

Let H be an open subnormal subgroup of a free profinite group $\hat{F}_r$ of rank r. Then, H is a free profinite group of rank $1 + (r-1)[\hat{F}_r : H]$.

In general, one says that a profinite group Δ satisfies Schreier's formula if the following holds. Let $d(\Delta)$ denote the smallest cardinality of a set of generators of Δ converging to 1. Here, a subset X of a profinite group Δ is said to be a set of generators converging to 1 if every open subgroup of Δ contains all but finitely many elements in X and $< X >$ is dense in Δ. Then, Δ is said to satisfy Schreier's formula if, for every open normal subgroup H, one has

$$d(H) = 1 + (d(\Delta) - 1)[\Delta : H].$$

Free profinite groups satisfy Schreier's formula. One also uses the following results:

Let Δ be a finitely generated pro-p group, for some prime p. Then, Δ is free pro-p if, and only if, it satisfies Schreier's formula.

On the other hand, a free pronilpotent group Δ with $d(\Delta) \geq 2$ never satisfies Schreier's formula. Note that this is not true if $d(\Delta) = 1$. In fact, any direct product $\Delta = \Delta_1 \times \Delta_2$ with $d(\Delta) \geq 2$ does not satisfy Schreier's formula. This is one of the key (although simple to prove) facts we use in our proof.

Let $\hat{F}_r$ be the free profinite group of finite rank $r \geq 2$. Let H be a closed normal subgroup of $\hat{F}_r$ of infinite index. If $\hat{F}_r / H$ does not satisfy Schreier's formula, then H is a free profinite group of countably infinite rank.

The analogue of Kurosh subgroup theorem holds for open subgroups of free profinite products but not for closed subgroups. For closed normal subgroups of free profinite products, one has a similar statement which involves projective profinite groups in place of free profinite groups. Projective profinite groups are closed subgroups of free profinite groups. We use the following result:

Let F be a free profinite group of infinite rank and let P be a projective profinite group with $d(P) \leq d(F)$. Then the free profinite product $F \sqcup P \cong F$.

Note that the above result also shows that free factors of a free profinite group need not be free profinite groups.

Another fact we use is:

Let F be a free profinite group of rank r (any cardinal number) ≥ 2. Then, a closed normal subgroup H of infinite index with $d(F/H) < r$ must be a free profinite group and it has rank $\max(r, \aleph_0)$.

Some of these facts that we use are proved using the notion of a profinite graph of profinite groups and a notion of the fundamental group of such a profinite graph of groups.

To finish with, we recall the two problems which may be termed outstanding here. The first is the finiteness of the $C(S, G)$ in Serre's conjecture is still very much open for the groups of type A_n with k-rank 0. Solving them would lead to applications to the theory of automorphic forms. These G, S are described as follows:

(i) Let D be a division algebra with center k and the k-group G is $SL(1, D)$. For S with S-rank$(G) \geq 2$, is $C(S, G)$ finite?

(ii) Let D be a division algebra with center K which is a quadratic extension of k and suppose D admits an involution of the 2nd kind whose fixed field is k. Then the k-group G is $SU(1, D)$. For S so that S-rank$(G) \geq 2$, is $C(S, G)$ finite?

The second question is when k is a number field, S consists only of the archimedean places, and G is a k-group such that S-rank of G is 1, then what is the structure of $C(S, G)$? Recently, it has been proved by Lubotzky that $C(S, G)$ is finitely generated as a normal subgroup of $\widehat{G(\mathcal{O}_S)}$. However, the structure is unknown as yet. This is unknown excepting the case of $SL(2, \mathbf{Z})$; our theorem above deals with all the cases where S contains a nonarchimedean place.

Received 24 October 2007; revised 27 October 2007.

References

1. M. Abert, N. Nikolov & B. Saegedy, Congruence subgroup growth of arithmetic groups in positive characteristic, *Duke J. Math.* **117** (2003) 367–383.
2. A. Bak, Le Probleme des sous-groupes de congruence et le probleme metaplectique pour les groupes classiques de rang > 1, *C. R. Acad. Sci. Paris* **292** (1981) 307–310.
3. A. Bak & U. Rehmann, The congruence subgroup and metaplectic problems for $SL_{n\geq 2}$ of division algebras, *Jour. Algebra* **78** (1982) 475–547.
4. H. Bass, M. Lazard and J-P. Serre, Sous-groupes d'indice fini dans SL(n,**Z**), *Bull. Amer. Math. Soc.* **70** (1964) 59–137.
5. H. Bass, J. Milnor and J-P. Serre, Solution of The Congruence Subgroup Problem, *Publ. Math. I.H.E.S.*, **33** (1967) 59–137.
6. J. L. Brenner, The linear homogeneous group III, *Ann. of Math.* **71** (1960) 210–233.
7. J. Britto, On defining a subgroup of the special linear group by a congruence, *J. Indian Math. Soc.* **69** (1981) 298–304.
8. D. Carter & G. Keller, Bounded elementary generation of $SL(n, \mathcal{O})$, *Amer. J. Math.* **105** (1983) 673–687.
9. J. W. S. Cassels & A. Frohlich (editors), *Algebraic Number Theory*, Acad. Press, London 1967.

10. C. Chevalley, Deux Théorémes d'arithmétique, *J. Math. Soc. Japan*, **3** (1951), 36–44.
11. V. Deodhar, On central extensions of rational points of algebraic groups, *Amer. J. Math.* **100** (1978) 303–386.
12. 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.
13. J. D. Dixon, M. P. F. du Sautoy, A. Mann & D. Segal, Counting congruence subgroups in arithmetic groups, *Bull. London Math. Soc.* **26** (1994) 255–262.
14. D. Goldfeld, A. Lubotzky, N. Nikolov & L. Pyber, Counting primes, groups, and manifolds, *Proc. Natl. Acad. Sci. of USA*, **101**, (37) (2004) 13428–13430.
15. D. Goldfeld, A. Lubotzky & L. Pyber, Counting congruence subgroups, *Acta Math.* 193 (2004) 73–104.
16. F. Grunewald & J. Schwermer, Free nonabelian quotients of $SL(2)$ over orders of imaginary quadratic number fields, *Jour. Algebra* **69** (1981) 298–304.
17. J. Humphreys, Arithmetic groups, *LNM* **789**, Springer, 1980.
18. G. Janusz, *Algebraic Number Fields*, Academic Press 1973.
19. D. Kazhdan, A certain characterisation of congruence subgroups of the group $SL(2, \mathbf{Z})$, *Func. Analysis & its applcns.* **4** (1970) 89–90.
20. M. Kneser, Normalteiler ganzzahliger spingruppen, *Crelle's J.* **311** (1979) 191–214.
21. A. Lubotzky, Free quotients and the congruence kernels of $SL(2)$, *Jour. Algebra* **77** (1982) 411–418.
22. A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.* **119** (1995) 267–295.
23. A. Lubotzky, Eigenvalues of the Laplacian, the first Betti number and the congruence subgroup problem, *Ann. of Math.* **144** (1996) 441–452.
24. A. Lubotzky & B. Martin, Polynomial representation growth and the congruence subgroup problem, *Israel J. Math.* **144** (2004) 293–316.
25. A. Lubotzky & D. Segal, Subgroup growth, *Progress in Mathematics* vol. **212**, Birkhauser 2003.
26. A. Mason, Free quotients of congruence subgroups of SL_2 over a co-ordinate ring, *Math. Zeit.* **198** (1988) 39–51.
27. A. Mason, Congruence hulls in $SL(n)$, *J. Pure Appl. Alg.* **89** (1993) 255–272.
28. A. Mason, Quotients of the congruence kernels of SL_2 over Dedekind domains, *Israel J. Math.* **91** (1995) 77–91.
29. A. W. Mason, A. A. Premet, B. Sury & P. Zalesski, The congruence kernel of an arithmetic lattice in a rank one algebraic group over a local field, *Crelle's Journal*, To Appear.
30. M. Matsumoto, Sur les sous-groupes arithmetiques des groupes semisimple deployes, *Ann. Sci. Ecole Norm. Sup.* **2** (1969) 1–62.
31. J. Mennicke, Finite factor groups of the modular group, *Ann. Math.* **81** (1965) 31–37.
32. J. Mennicke, On Ihara's modular group, *Invent. Math.* **4** (1967) 202–228.
33. J. Milnor, *Introduction to K-theory*, Princeton Univ. Press 1971.
34. C. C. Moore, Group extensions of p-adic and adelic linear groups, *Publ. Math. IHES* **35** (1968) 5–70.
35. M. Newman, *Integral Matrices*, Academic Press, New York 1972.
36. New horizons in pro-p groups, Edited by M. du Sautoy, D. Segal & A. Shalev, *Progress Math.* vol 184, Birkhauser, Boston 2000.
37. V. Platonov & A. Rapinchuk, Abstract properties of S-arithmetic groups and the congruence subgroup problem, *Russian Acad. Sci. Izv.* **56** (1992) 483–508.
38. V. Platonov & A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, San Diego 1994.
39. V. Platonov & B. Sury, Adelic profinite groups, *Jour. Algebra* **193** (1997) 757–763.
40. G. Prasad & M. S. Raghunathan, On the congruence subgroup problem determination of the metaplectic kernel, *Invent. Math.* **71** (1983) 21–42.
41. G. Prasad & A. Rapinchuk, Computation of the metaplectic kernel, *Math. IHES* **84** (1996) 91–187.
42. M. S. Raghunathan, On the congruence subgroup problem, *Publ. Math. IHES* **46** (1976) 107–161.
43. M. S. Raghunathan, On the congruence subgroup problem II, *Invent. Math.* **85** (1986) 73–117.
44. M. S. Raghunathan, *The Congruence Subgroup Problem, Proceedings of the Hyderabad Conference on Algebraic Groups, (Hyderabad 1989)*, 465–494, Manoj Prakashan, Madras 1991.
45. A. Rapinchuk, On the congruence subgroup problem for algebraic groups, *Soviet Math. Dokl. Akad.* **39** (1989) 618–621.
46. A. Rapinchuk, The congruence subgroup problem, *Contemp. Math.* **243** (1999) 175–188.
47. D. Segal, Congruence topologies in commutative rings, *Bull. London Math. Soc.* **11** (1979) 186–190.
48. D. Segal, Le probleme des groupes de congruence pour $SL(2)$, *Ann. Math.* **92** (1970) 489–527.
49. D. Segal, *Groupes de Congruence*, Seminaire Bourbaki, Expose 330, 1967.
50. R. Steinberg, Some consequences of the elementary relations in $SL(n)$, *Contemp. Math.* **45** (1985) 335–350.
51. B. Sury , *The Congruence subgroup problem - an elementary approach aimed at applications*, Hindustan Book Agency, TRIM Series, vol. 24, 2003.
52. B. Sury, Congruence subgroup problem for anisotropic groups over semi-local rings, *Proc. Indian Acad. Sci.* **101** (1991) 87–110.
53. B. Sury, Central extensions of p-adic groups; a theorem of Tate, *Comm. Algebra* **21** (1993) 1203–1213.
54. B. Sury & T. N. Venkataramana, Generators for principal congruence subgroups for $SL(n, \mathbf{Z})$ with $n \geq 3$, *Proc. Amer. Math. Soc.* **122** (1994) 355–358.
55. J. Thompson, *Hecke Operators and Noncongruence Subgroups*, Group theory, Singapore, de Gruyter, Berlin–New York 1989.
56. J. Tits, Systemes generateurs de groupes de congruence, *C. R. Acad. Sci. Paris* **283** (1976) 693–695.
57. G. Tomanov, On the congruence subgroup problem for some anisotropic algebraic groups over number fields, *Crelle's J.* **402** (1989) 138–152.
58. L. N. Vaserstein, Structure of the classical arithmetic groups of rank greater than 1, *Math. USSR Sbornik* **20** (1973) 465–492.
59. L. N. Vaserstein, On the congruence topology, *Comm. Algebra* **16** (1988) 2103–2120.

B. Sury got his Ph.D. degree from the Tata Institute of Fundamental Research, Bombay in 1991 having worked under the supervision of Professor M. S. Raghunathan. His interests are in group theory and number theory. He has written 2 books—one on the Congruence Subgroup Problem and, one on selected problems in group theory. Having always been interested in teaching, he moved from TIFR to the Indian Statistical Institute in Bangalore in 1999 motivated by the starting of an undergraduate mathematics honours programme. Apart from formal teaching, he has tried to keep his interest in education alive in other ways like being an editor for 'Resonance', a journal of Science Education and, being a regional co-ordinator for the mathematical olympiad programme. His other interests include ping-pong (managed to lose to J.-P. Serre once after leading 20-15), soccer (broke a toe in a friendly match on this Teachers' Day), cricket (where he had the good fortune to play against some Ranji players at the club level decades back), Indian classical music (Hindustani) and punning (for which he gets his daily lesson from Vishwambhar Pati during coffee time).