isib/ms/2005/5
February 18th, 2005
http://www.isibang.ac.in/~ statmath/eprints

The congruence kernel of an arithmetic lattice in a rank one algebraic group over a local field

A. W. Mason, B. Sury, and P. A. Zalesskii

Indian Statistical Institute, Bangalore Centre
8th Mile Mysore Road–560 059, India

The congruence kernel of an arithmetic lattice in a rank one algebraic group over a local field

A. W. Mason[1], B. Sury[2, *], P. A. Zalesskii[3, †]

[1] Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland UK (e-mail: awm@maths.gla.ac.uk)
2 Statistics-Mathematics Unit, Indian Statistical Institute, Bangalore 560 059, India (e-mail: sury@isibang.ac.in)
[3] Department of Mathematics, University of Brasilia, 70.910 Brasilia DF, Brazil (e-mail: pz@mat.unb.br)

Abstract

Let k be a global field and let k_v be the completion of k with respect to v, a non-archimedean place of k. Let $\mathbf{G}$ be a connected, simply-connected algebraic group over k, which is absolutely almost simple of k_v-rank 1. Let $G = \mathbf{G}(k_v)$. Let Γ be an *arithmetic lattice* in G and let $C = C(\Gamma)$ be its *congruence kernel*. We determine the structure of C, providing a complete solution of the *congruence subgroup problem* for Γ. It is shown that C is a free profinite product, one of whose factors is $\hat{F}_\omega$, the free profinite group on countably many generators. This result is already known for a number of special cases. These include the important (*non-uniform*) example $\Gamma = SL_2(\mathcal{O}(S))$, where $\mathcal{O}(S)$ is the *the ring of S-integers in k*, with $S = \{v\}$, which plays a central role in the theory of Drinfeld modules. The proof makes use of a decomposition theorem of Lubotzky, arising from the action of Γ on the *Bruhat-Tits tree* associated with G.

2000 Mathematics Subject Classification : 20G30, 11F06, 20E08, 20E18.

*Partially supported by an EPSRC Visiting Fellowship GR/N32211/01.
†Partially supported by the Edinburgh Mathematical Society Research Support Fund and the Glasgow Mathematical Journal Trust Fund.

Introduction

Let k be a global field and let $\mathbf{G}$ be a connected, simply-connected algebraic group over k, which is absolutely almost simple. For each non-empty, finite set S of places of k, containing all the archimedean places, let $\mathcal{O}(S)$ denote the corresponding *ring of S-integers in k*. The problem of determining whether or not a finite index subgroup of the arithmetic group, $\mathbf{G}(\mathcal{O}(S))$, contains a principal congruence subgroup (modulo some non-zero $\mathcal{O}(S)$-ideal), the so-called *congruence subgroup problem* or CSP, has attracted a great deal of attention since the 19th century. As a measure of the extent of those finite index subgroups of $\mathbf{G}(\mathcal{O}(S))$ which are not congruence, its so-called *non-congruence subgroups*, Serre [S1] has introduced a profinite group, $C(S, \mathbf{G})$, called the *(S-)congruence kernel* of $\mathbf{G}$. In his terminology [S1] the CSP for this group has an *affirmative* answer if this kernel is finite. Otherwise the CSP has an *essentially negative* answer. The principal result in [S1] is that, for the case $\mathbf{G} = \mathbf{SL}_2$, the congruence kernel $C(S, \mathbf{G})$ is *finite* if and only if card$S \geq 2$. Moreover Serre has formulated the famous *congruence subgroup conjecture* [PR, p.556], which states that the answer to the CSP is determined entirely by the *S-rank* of $\mathbf{G}$, $\mathrm{rank}_{\mathrm{S}}\mathbf{G}$. (See [Mar, p.258].) It is known [Mar, (2.16) Theorem, p.269] that $C(S, \mathbf{G})$ is finite (cyclic), when $\mathbf{G}$ is *k-isotropic* and $\mathrm{rank}_S\mathbf{G} \geq \mathbf{2}$. It is also known that $C(S, \mathbf{G})$ is infinite for many "rank one" $\mathbf{G}$ (for example, $\mathbf{G} = \mathbf{SL_2}$). The conjecture however remains open for some of these cases. (See, for example, [L3].) The congruence kernel $C(S, H)$ can be defined in a similar way for every subgroup H of $\mathbf{G}(k)$ which is commensurable with $\mathbf{G}(\mathcal{O}(\mathcal{S}))$. (From this definition it is clear that $C(S, H)$ is finite if and only if $C(S, \mathbf{G})$ is finite.)

The books of Margulis [Mar, p.268] and Platonov/Rapinchuk [PR, Section 9.5] emphasise the importance of determining the *structure* of the congruence kernel. (Lubotzky refers to this as the *complete* solution of the CSP.) In this paper we are concerned with the structure of infinite congruence kernels. The first result of this type is due to Mel'nikov [Me], who shows that, for the case where $\mathbf{G} = \mathbf{SL}_2$, $k = \mathbb{Q}$ and $S = \{\infty\}$, (i.e. $\mathbf{G}(\mathcal{O}(S)) = SL_2(\mathbb{Z})$, the classical *modular group*), the congruence kernel is isomorphic to $\hat{F}_\omega$, the free profinite group on countably many generators. Lubotzky [L1] has proved that, when $\mathbf{G} = \mathbf{SL_2}$ and card $S = 1$, the congruence kernel of $SL_2(\mathcal{O}(\mathcal{S}))$ has a closed subgroup isomorphic to $\hat{F}_\omega$, reproving Mel'nikov's result in the process. (When char $k = 0$ and card $S = 1$, it is known that $k = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$, with $S = \{\infty\}$, where d is a square-free positive rational integer.) In [Mas2] it is shown that, when $\mathbf{G} = \mathbf{SL}_2$ and card $S = 1$, the congruence kernel maps onto every free profinite group of finite rank.

In this paper we extend these results by determining the structure of the congruence kernel of an arithmetic lattice in a rank one algebraic group over a local field, providing a complete solution of the CSP for this case. With the above notation let V_k be the set of places of k and let (the local field) k_v be the completion of k with respect to v. In addition to the above hypotheses we assume that $\mathbf{G}$ has k_v-rank 1. We denote the set of k_v-rational points, $\mathbf{G}(k_v)$, by G. Let Γ be a *lattice* in G, i.e. a discrete subgroup of (the locally compact group) G for which $\mu(G/\Gamma)$ is *finite*, where μ is a Haar measure on G. As usual Γ is said to be *cocompact* (resp. *non-uniform*) if G/Γ is compact (resp. not compact). We assume further that Γ is $(S-)$*arithmetic*, i.e. Γ is commensurable with $\mathbf{G}(\mathcal{O})$, where $\mathcal{O} = \mathcal{O}(\mathcal{S})$ is as above.

Example. When $\operatorname{char} k > 0$, $S = \{v\}$ and $\mathbf{G} = \mathbf{SL}_2$, the group $\Gamma = SL_2(\mathcal{O})$ is a (non-uniform) arithmetic lattice (in $SL_2(k_v)$). This lattice, which plays a central role in the theory of Drinfeld modules, is the principal focus of attention in Chapter II of Serre's book [S2].

We now fix a linear representation of G (of degree n, say). For each $\mathcal{O}$-ideal $\mathfrak{q}$ we put

$$\Gamma(\mathfrak{q}) = \{X \in \Gamma : X \equiv I_n \pmod{\mathfrak{q}}\},$$

the *principal congruence subgroup of level* $\mathfrak{q}$. Let Λ be a subgroup of finite index in Γ. The S-*arithmetic* and S-*congruence* subgroups of G (via the finite index subgroups and the subgroups $\Gamma(\mathfrak{q})$ of Γ, resp.) define topologies on Λ which give rise to profinite completions of Λ denoted by $\hat{\Lambda}$ and $\bar{\Lambda}$, resp.
Since every S-congruence subgroup is S-arithmetic, there is an exact sequence

$$1 \to C(\Gamma) \to \hat{\Gamma} \to \overline{\Gamma} \to 1.$$

The (profinite) group $C(\Gamma)(= C(S, \Gamma))$ is called the *congruence kernel* of Γ. Our principal results are the following.

Theorem A. *If* Γ *is cocompact, then*

$$C(\Gamma) \cong \hat{F}_\omega.$$

It is well-known that Γ is cocompact when, for example, char $k = 0$. For examples of this type see [S2, p.84]. This result however is not a straightforward generalization of Mel'nikov's theorem [Me]. On the one hand $SL_2(\mathbb{Z})$ is *not* a lattice in $SL_2(\mathbb{Q}_p)$, where

$\mathbb{Q}_p$ is the p-adic completion of $\mathbb{Q}$ with respect to any rational prime p. On the other hand $SL_2(\mathbb{Z})$ is a *non-uniform* lattice in $SL_2(\mathbb{R})$. (See [Mar, p.295].) Moreover the third author [Za2] has proved that the congruence kernel of every arithmetic lattice in $SL_2(\mathbb{R})$ is isomorphic to $\hat{F}_\omega$.

Theorem B. *If* Γ *is non-uniform and* $p = \mathrm{char}\ k$*, then*

$$C(\Gamma) \cong \hat{F}_\omega \amalg N(\Gamma),$$

the free profinite product of $\hat{F}_\omega$ *and* $N(\Gamma)$*, where* $N(\Gamma)$ *is a free profinite product of nilpotent pro-p groups, each of class at most* 2 *and each generated by torsion elements of p-power order.*

The proof is based on the action of G, and hence Γ, on the associated Bruhat-Tits tree T. For the non-uniform case it makes use of a decomposition theorem for Γ due to Lubotzky [L2]. This extends a number of existing results. The third author [Za1, Theorem 4.3] has proved Theorem B for the special case $\mathbf{G} = \mathbf{SL}_2$ and $S = \{v\}$. Lubotzky [L1] has proved that, for this case, $C(\Gamma)$ has a closed subgroup isomorphic to $\hat{F}_\omega$. Lubotzky has also shown [L2, Theorem 7.5] that $C(\Gamma)$ is *infinite* when Γ is non-uniform.

For $\mathbf{G}, k$ as above and any S a cohomological formulation of the S-congruence kernel, $C(S, \mathbf{G})$, has been defined (originally by Moore) called the *S-metaplectic kernel*, $M(S, \mathbf{G})$. (See, for example, [Mar, p.269].) The structure of $M(S, \mathbf{G})$ has been determined for many cases. See [PRap].

1 Arithmetic lattices

This section is devoted to a number of properties of arithmetic lattices which are needed to establish our principal results. We begin with a general property of lattices.

Lemma 1.1. *If* Γ *is any lattice, then* Γ *is not virtually solvable.*

Proof. It is known that Γ is *Zariski-dense* in $\mathbf{G}$. (See [Mar, (4.4) Corollary, p.93] and [Mar, (2.3) Lemma, p.84].) It follows that $[\Gamma, \Gamma]$ is Zariski-dense in $[\mathbf{G}, \mathbf{G}] = \mathbf{G}$, by [B, Proposition, p.59] and [B, Proposition, p.181]. If Γ is virtually solvable then $\mathbf{G}$ is finite, which contradicts the fact that it has k_v-rank 1. $\square$

For each non-archimedean $v \in V_k$, we denote the completion of $\mathcal{O}$ with respect to v by $\mathcal{O}_v$. This is a local ring with a finite residue field.
We define [PR, p.161] the *restricted topological product*

$$\mathbf{G}(\hat{\mathcal{O}}) = \prod_{v \notin S} \mathbf{G}(\mathcal{O}_v).$$

By definition the group $\mathbf{G}(\hat{\mathcal{O}})$ is a topological group with a base of neighbourhoods of the identity consisting of all subgroups of the form

$$\prod_{v \notin S} M_v, \qquad (*)$$

where each M_v is an open subgroup of $\mathbf{G}(\mathcal{O}_v)$ and $M_v = \mathbf{G}(\mathcal{O}_v)$, for all but finitely many $v \notin S$. Let $\mathfrak{m}$ denote the maximal ideal of the (local) ring $\mathcal{O}_v$. Then the "principal congruence subgroups", $\mathbf{G}(\mathfrak{m}^t)$, where $t \geq 1$, provide a base of neighbourhoods of the identity in $\mathbf{G}(\mathcal{O}_v)$. (See [PR, p.134].) The group $\mathbf{G}(\mathcal{O})$ embeds, via the "diagonal map", in $\mathbf{G}(\hat{\mathcal{O}})$. Let $\overline{\mathbf{G}}(\mathcal{O})$ denote the "congruence completion" of $\mathbf{G}(\mathcal{O})$ determined by its S-congruence subgroups. The hypotheses on $\mathbf{G}$ ensure that the following holds.

Lemma 1.2. *"The Strong Approximation Property"*

$$\overline{\mathbf{G}}(\mathcal{O}) \cong \mathbf{G}(\hat{\mathcal{O}}).$$

Proof. By [PR, Theorem 7.12, p.427] it suffices to verify that

$$G_S := \prod_{v \in S} \mathbf{G}(\mathcal{O}_v)$$

is not compact. Now by [Mar, (3.2.5), p.63] the group $\mathbf{G}(\mathcal{O})$ is a lattice in G_S. If G_S is compact then $\mathbf{G}(\mathcal{O})$ and hence Γ are finite, which contradicts Lemma 1.1. $\square$

We record another well-known property of Γ.

Lemma 1.3. *With the above notation,*

$$C(\Gamma) = \bigcap_{\mathfrak{q} \neq \{0\}} \hat{\Gamma}(\mathfrak{q}).$$

It follows that, for all $\mathfrak{q} \neq \{0\}$, there is an exact sequence

$$1 \to C(\Gamma) \to \hat{\Gamma}(\mathfrak{q}) \to \overline{\Gamma}(\mathfrak{q}) \to 1.$$

We may assume that Γ and, hence all its subgroups, act on the Bruhat-Tits tree T associated with G *without inversion.* As usual let the vertex and edge sets of a graph X be denoted by $V(T)$ and $E(T)$, resp. For each subgroup H of Γ and each $w \in V(T) \cup E(T)$, we denote the *stabilizer* of w in H by

$$H_w = \{g \in H : g(w) = w\}.$$

Since Γ is discrete it follows that H_w is always *finite.*
From now on we deal with the cocompact and non-uniform cases separately.

2 Cocompact arithmetic lattices

For each positive integer s, let F_s denote the free group of rank s.

Lemma 2.1. *If Γ is cocompact, then, for all but finitely many $\mathfrak{q}$,*

$$\Gamma(\mathfrak{q}) \cong F_r,$$

where $r = r(\mathfrak{q}) \geq 2$. Moreover $r(\mathfrak{q})$ is unbounded in the following sense.
If $r(\mathfrak{q}) \geq 2$ and

$$\mathfrak{q} = \mathfrak{q}_1 \gneqq \mathfrak{q}_2 \gneqq \mathfrak{q}_3 \cdots$$

is an infinite properly descending chain of $\mathcal{O}$-ideals, then

$$r(\mathfrak{q}_i) \to \infty, \textit{ as } i \to \infty.$$

Proof. It is well-known that the quotient graph

$$\Gamma \backslash T \text{ is } finite.$$

Let $v_1, \cdots, v_t$ denote the vertices (in $V(T)$) of a *lift* $j : \Gamma\backslash T \to T$. We put

$$\Gamma_i = \Gamma_{v_i} \quad (1 \leq i \leq t).$$

It is clear that, for all but finitely many $\mathfrak{q}$,

$$\Gamma(\mathfrak{q}) \cap \Gamma_i = \{I_n\} \quad (1 \leq i \leq t),$$

since each Γ_i is finite.
For such a $\mathfrak{q}$ all the stabilizers in $\Gamma(\mathfrak{q})$ of the vertices of T are trivial, since $\Gamma(\mathfrak{q})$ is normal in Γ. Further $|\Gamma : \Gamma(\mathfrak{q})|$ is finite and so

$$\Gamma(\mathfrak{q})\backslash T \text{ is finite.}$$

It follows that

$$\Gamma(\mathfrak{q}) \cong F_r,$$

for some r. (See [S2, Theorem 4, p.27].) By Lemma 1 it is clear that $r \geq 2$.
If $r(\mathfrak{q}) \geq 2$ and

$$\mathfrak{q} = \mathfrak{q}_1 \gneqq \mathfrak{q}_2 \gneqq \mathfrak{q}_3 \cdots.$$

By the well-known Schreier formula,

$$r(\mathfrak{q}_i) - 1 = |\Gamma(\mathfrak{q}) : \Gamma(\mathfrak{q}_i)|(r(\mathfrak{q}) - 1).$$

The result follows since $|\Gamma(\mathfrak{q}) : \Gamma(\mathfrak{q}_i)| \to \infty$, as $i \to \infty$. □

Theorem 2.2. *If* Γ *is cocompact, then*

$$C(\Gamma) \cong \hat{F}_\omega.$$

Proof. Fix any $\mathfrak{q}$ for which Lemma 2.1 holds. Let $C = C(\Gamma)$. Then, by the exact sequence after Lemma 1.3,

$$\hat{F}_r/C \cong \overline{\Gamma}(\mathfrak{q}).$$

Now $|\mathbf{G}(\mathcal{O}) : \Gamma(\mathfrak{q})|$ is finite and so (by Lemma 1.2) $\overline{\Gamma}(\mathfrak{q})$ embeds as an *open* subgroup of $\mathbf{G}(\hat{\mathcal{O}})$ and hence contains an open subgroup O of $\mathbf{G}(\hat{\mathcal{O}})$ of type (*).
Since Γ is cocompact, $\Gamma(\mathfrak{q})$ is finitely generated. It follows that $\overline{\mathbf{G}}(\mathcal{O}), \overline{\Gamma}(\mathfrak{q})$ and O are all *finitely generated* profinite groups. Consequently the group O does not "satisfy Schreier's formula". (See [RZ, Lemma 8.4.5, p.320].) Hence $\overline{\Gamma}(\mathfrak{q})$ does not satisfy Schreier's formula, since $|\overline{\Gamma}(\mathfrak{q}) : O|$ is finite. The result follows from [RZ, Corollary 8.4.4, p.320]. □

3 Non-uniform arithmetic lattices: discrete results

Here we assume that G/Γ is *not* compact, in which case k is a function field. We put char $k = p$.

It is well-known that an element X of Γ has finite order if and only if $X \in \Gamma_v$, for some $v \in V(T)$.

In order to describe the structure of $\Gamma\backslash T$ we make the following.

Definitions. Let R be a *ray* in $\Gamma\backslash T$, i.e. an infinite path without backtracking and let $j : R \to T$ be a *lift*. Let $V(j(R)) = \{v_1, v_2, \cdots\}$. We say that j is *stabilizer ascending*, if

$$\Gamma_{v_i} \leq \Gamma_{v_{i+1}} \quad (i \geq 1).$$

We put

$$\Gamma(R)\ (=\Gamma(R,j)) := \langle \Gamma_v : v \in V(j(R))\rangle.$$

Using results of Raghunathan [R], Lubotzky [L2, Theorem 6.1] has determined the structure of $\Gamma\backslash T$. This extends an earlier result of Serre [S, Theorem 9, p.106] for the special case $\mathbf{G} = \mathbf{SL}_2$, $\Gamma = SL_2(\mathcal{O})$ and $S = \{v\}$. Baumgartner [Ba] has provided a more detailed and extended version of Lubotzky's proof.

Theorem 3.1. *With the above notation,*

$$\Gamma\backslash T = Y \cup R_1 \cup \cdots \cup R_m,$$

where Y is a finite subgraph and $R_1, \cdots, R_m$ $(m \geq 1)$ are rays.

In addition,

(a) $\mathrm{card}\{V(Y) \cap V(R_i)\} = 1 \quad (1 \leq i \leq m)$,

(b) $E(Y) \cap E(R_i) = \phi \quad (1 \leq i \leq m)$,

(c) $R_i \cap R_\ell = \phi \quad (i \neq \ell)$.

Moreover there exists a lift $j : \Gamma\backslash T \to T$ such that

$$j : R_i \to T \ \textit{ is stabilizer ascending } \ (1 \leq i \leq m).$$

Lemma 3.2. *Let R be a ray in $\Gamma\backslash T$ and let $j : R \to T$ be a lift. Then $\Gamma(R)$ is contained in a minimal parabolic k_v-subgroup of $\mathbf{G}$, whose unipotent radical is nilpotent of class at most* 2.

Proof. The group $\Gamma(R)$ stabilizes the *end* of T corresponding to $j(R)$ and hence is a subgroup of a minimal parabolic k_v-subgroup of $\mathbf{G}$. Since the k_v-rank of $\mathbf{G}$ is 1, the unipotent radical of the latter is nilpotent of class at most 2 , by [BT, 4.7 Proposition]. (The authors are indebted to to Professor Gopal Prasad for providing them with this reference.) □

It is known that in this context "2" is best possible. (See, for example, [PRag].) On the other hand, if G has a 2-dimensional representation, then the unipotent radical is abelian (i.e. has class 1). (This happens, of course, when $\mathbf{G} = \mathbf{SL}_2$.) We now use Theorem 3.1 to provide a useful free decomposition for $\Gamma(\mathfrak{q})$.

Lemma 3.3. *Let $\mathfrak{q}$ be a proper $\mathcal{O}$-ideal. Then every element of finite order of $\Gamma(\mathfrak{q})$ is unipotent of p-power order.*

Proof. Let k_0 be the (full) field of constants of (the function field) k. Let $g \in \Gamma(\mathfrak{q})$ have finite order and let $\chi_g(t)$ denote its characteristic polynomial over k. Then

$$\chi_g(t) \equiv (t-1)^n \pmod{\mathfrak{q}}.$$

Now each zero of $\chi_g(t)$ is a root of unity and so each coefficient of $\chi_g(t)$ lies in the algebraic closure of k_0 in k, which is k_0 itself. Since $k_0 \leq \mathcal{O}$ it follows that

$$\chi_g(t) = (t-1)^n.$$

$\square$

Lemma 3.4. *Let R be a ray in $\Gamma\backslash T$ and $j : R \to T$ a stabilizer ascending lift. For each proper $\mathcal{O}$-ideal $\mathfrak{q}$, the subgroup*

$$\Gamma(\mathfrak{q}) \cap \Gamma(R)$$

consists of unipotent matrices and (hence) is nilpotent of class at most 2, generated by elements of p-power order.

Proof. By definition $\Gamma(R) \cap \Gamma(\mathfrak{q})$ consists of elements of finite order in $\Gamma(\mathfrak{q})$. By Lemma 3.3 therefore it consists of unipotent matrices. It follows that it is contained in the unipotent radical of the parabolic subgroup referred to in Lemma 3.2. $\square$

Theorem 3.5. *For all but finitely many $\mathfrak{q}$,*

$$\Gamma(\mathfrak{q}) \cong F_r * \Lambda(\mathfrak{q}),$$

where $\Lambda(\mathfrak{q})$ is a free product of finitely many unipotent groups, each nilpotent of class at most 2 and each generated by unipotent elements of p-power order.

In addition,

$$r = r(\mathfrak{q}) = \mathrm{r}k_{\mathbb{Z}}(\Gamma(\mathfrak{q})) = \dim_{\mathbb{Q}} H^1(\Gamma(\mathfrak{q}), \mathbb{Q}),$$

the (finite) free abelian rank of $\Gamma(\mathfrak{q})$.

Proof. By the fundamental theorem of the theory of groups acting on trees [S2, Theorem 13, p.55] Γ is the fundamental group of the graph of groups given by the lift $j : \Gamma\backslash T \to T$ as described in Theorem 3.1.

For all but finitely many $\mathfrak{q}$,

$$\Gamma(\mathfrak{q}) \cap \Gamma_v = \{I_n\},$$

for all $v \in V(j(Y))$.
We fix such a $\mathfrak{q}$. Now $\Gamma(\mathfrak{q})$ is a *normal* subgroup of finite index in Γ. From standard results on the decomposition of a normal subgroup of a fundamental group of a graph of groups, $\Gamma(\mathfrak{q})$ is a free product of a free group F_r and a finite number of subgroups, each of which is a conjugate of $\Gamma(\mathfrak{q}) \cap \Gamma(R_i)$, for some i. The rest follows from Lemma 3.4. □

For the case $\mathbf{G} = \mathbf{SL}_2$, $S = \{v\}$ and $\Gamma = SL_2(\mathcal{O})$, Theorem 3.5 is already known [Mas2, Theorem 2.5].

Corollary 3.6. *Let $U(\mathfrak{q})$ denote the (normal) subgroup of $\Gamma(\mathfrak{q})$ generated by its unipotent matrices. Then, for all but finitely many $\mathfrak{q}$,*

$$\Gamma(\mathfrak{q})/U(\mathfrak{q}) \cong F_r,$$

where $r = r(\mathfrak{q}) = \mathrm{r}k_{\mathbb{Z}}(\Gamma(\mathfrak{q}))$.

Proof. We fix an ideal $\mathfrak{q}$ for which Theorem 3.5 holds. Let $\Lambda(\mathfrak{q})^*$ denote the normal subgroup of $\Gamma(\mathfrak{q})$ generated by $\Lambda(\mathfrak{q})$. Now every unipotent element of $\Gamma(\mathfrak{q})$ is of finite order and so lies in a conjugate of some $\Gamma(\mathfrak{q}) \cap \Gamma(R_i)$, by Theorem 3.5. It follows that $\Lambda(\mathfrak{q})^* = U(\mathfrak{q})$. □

We now show that $r(\mathfrak{q})$ is not bounded.

Lemma 3.7. *With the above notation, for infinitely many $\mathfrak{q}$,*

$$r(\mathfrak{q}) \geq 2.$$

If $r(\mathfrak{q}') \geq 2$ and

$$\mathfrak{q}' = \mathfrak{q}_1 \gneqq \mathfrak{q}_2 \gneqq \mathfrak{q}_3 \gneqq \cdots$$

is an infinite properly descending chain of $\mathcal{O}$-ideals, then

$$r(\mathfrak{q}_i) \to \infty, \quad as \;\; i \to \infty.$$

Proof. We note that, if

$$\Gamma(\mathfrak{q}) = F_s * H,$$

where H is a subgroup of $\Gamma(\mathfrak{q})$, then

$$r(\mathfrak{q}) \geq s.$$

By Theorem 3.1 together with [S, Theorem 13, p.55] it follows that

$$\Gamma = A *_W B,$$

where

(i) $B = \Gamma(R)$, for some ray R and a lift $j : R \to T$;

(ii) $W = \Gamma_v$, for some $v \in V(T)$.

Now B is infinite (since Γ is *non-uniform*) and W is finite.

If $A = W$, then $\Gamma(\mathfrak{q})$ is nilpotent by Lemma 3.4, for any proper $\mathfrak{q}$. This contradicts Lemma 1.1. We conclude that $W \neq A$.

It is well-known that, for any $\mathfrak{q}$,

$$r(\mathfrak{q}) \geq 1 + |\Gamma : W \,.\, \Gamma(\mathfrak{q})| - |\Gamma : A \,.\, \Gamma(\mathfrak{q})| - |\Gamma : B \,.\, \Gamma(\mathfrak{q})|.$$

We now restrict our attention to the (all but finitely many) $\mathfrak{q}$ for which

$$W \cap \Gamma(\mathfrak{q}) = \{I_n\}.$$

Among these are infinitely many $\mathfrak{q}'$ for which

$$|A \cdot \Gamma(\mathfrak{q}') : \Gamma(\mathfrak{q}')| > |W \cdot \Gamma(\mathfrak{q}') : \Gamma(\mathfrak{q}')| \ \text{ and } \ |B \cdot \Gamma(\mathfrak{q}') : \Gamma(\mathfrak{q}')| > 2|W \cdot \Gamma(\mathfrak{q}') : \Gamma(\mathfrak{q}')|.$$

It follows that

$$r(\mathfrak{q}') \geq 2.$$

For the second part, it is clear that

$$r(\mathfrak{q}_{i+1}) \geq r(\mathfrak{q}_i) \geq 2 \quad (i \geq 1).$$

Fix i. Then, by Theorem 3.5,

$$\Gamma(\mathfrak{q}_i) = F_{r'} * H,$$

say, where $r' = r(\mathfrak{q}_i)$. For any $t > i$, it follows from the Kurosh subgroup theorem and the Schreier formula that

$$r(\mathfrak{q}_t) > r',$$

unless $\Gamma(\mathfrak{q}_t) \cap F_{r'} = F_{r'}$ *and* $\Gamma(\mathfrak{q}_i) = \Gamma(\mathfrak{q}_t) \cdot F_{r'}$. We choose t so that $\Gamma(\mathfrak{q}_i) \neq \Gamma(\mathfrak{q}_t)$. □

Lemma 3.7 is already known for the case $\mathbf{G} = \mathbf{SL}_2,\ S = \{v\}$ and $\Gamma = SL_2(\mathcal{O})$. See the proof of [Mas1, Theorem 3.6].

4 Non-uniform arithmetic lattices: profinite results

Let A and B be *free pro$-\mathcal{C}$ groups*, where $\mathcal{C}$ is a (suitable) class of finite groups. See [RZ, p.90]. (The most important examples are the classes of all finite groups and all finite p-groups.) We will denote by

$$A \amalg B$$

the free profinite product (or, more precisely, *the free pro$-\mathcal{C}$ product) of A and B*. See [RZ, p.361].
Let $\hat{F}_s$ denote *the free profinite group of rank s*, where $s \geq 1$, (i.e. the "full" profinite completion of the free group F_s).

Lemma 4.1. *With the above notation, for all but finitely many $\mathfrak{q}$,*

$$\hat{\Gamma}(\mathfrak{q}) \cong \hat{F}_r \amalg \hat{\Lambda}(\mathfrak{q}),$$

where

(a) $\hat{\Lambda}(\mathfrak{q})$ is a free profinite product of nilpotent pro-p groups, each of class at most 2 and each generated by torsion elements of p-power order;

(b) the normal subgroup of $\hat{\Gamma}(\mathfrak{q})$ generated by $\hat{\Lambda}(\mathfrak{q})$ is $\hat{U}(\mathfrak{q})$;

(c) $r = r(\mathfrak{q})$ is not bounded.

Moreover,

$$\hat{\Gamma}(\mathfrak{q})/\hat{U}(\mathfrak{q}) \cong \hat{F}_r.$$

Proof. Follows from Theorem 3.5 and Lemma 3.7. □

A *projective* group is, by definition, a closed subgroup of a free profinite group.

Lemma 4.2. *Let N be a normal, closed, non-open subgroup of $\hat{\Gamma}(\mathfrak{q})$. Then, for all but finitely many $\mathfrak{q}$,*

$$N \cong P \amalg N(\mathfrak{q}),$$

where

(a) $N(\mathfrak{q})$ is a closed subgroup of $\hat{U}(\mathfrak{q})$ and a free profinite product of nilpotent pro-p groups, each of class at most 2 and each generated by torsion elements of p-power order;

(b) P is a projective group, all of whose proper, open subgroups are isomorphic to $\hat{F}_\omega$.

Proof. This follows from a result of the third author [Za1, Theorem 2.1]. (See also [Za1, Theorem 4.1, Lemma 4.2].) $\square$

An immediate consequence of Lemma 4.2 and Lemma 1.3 is the following.

Lemma 4.3. *With the above notation,*

$$C(\Gamma) \cong P \amalg N(\Gamma),$$

where

(a) $N(\Gamma)$ *is a closed subgroup of all* $\hat{U}(\mathfrak{q})$ *and a free profinite product of nilpotent pro-p groups, each of class at most* 2 *and each generated by torsion elements of p-power order;*

(b) P *is a projective group, all of whose proper, open subgroups are isomorphic to* $\hat{F}_\omega$.

Our principal aim in this paper is to replace P with $\hat{F}_\omega$ in Lemma 4.3. We will refer to this as the *principal result*

.

Lemma 4.4. *Let* A *and* B *be free pro-* $\mathcal{C}$ *groups and let* M *be a normal, closed subgroup of*

$$A \amalg B.$$

Then $M \cap A$ *is a factor in the free profinite decomposition of* M.

Proof. Follows from [Za1, Theorem 2.1]. $\square$

Lemma 4.5. *Let* P *be as in Lemma 4.3 and* F *be isomorphic to* $\hat{F}_\omega$. *Then*

$$P \amalg F \cong \hat{F}_\omega.$$

Proof. See [RZ, Proposition 9.1.11, p. 370]. $\square$

Our next two lemmas deal with a special case for which the principal result holds.

Lemma 4.6. *Suppose that the set of positive integers t for which there exists a (continuous) epimorphism*

$$C(\Gamma) \longrightarrow \hat{F}_t$$

is not bounded. Then the principal result holds.

Proof. This follows from the proof of [Za1, Lemma 4.6]. $\square$

An immediate application is the following.

Lemma 4.7. *Suppose that, for all $\mathfrak{q}$, the closure of $U(\mathfrak{q})$ in $\overline{\Gamma}$, $\overline{U}(\mathfrak{q})$, is open in $\overline{\Gamma}$. Then the principal result holds.*

Proof. The hypothesis ensures that $|\overline{\Gamma}(\mathfrak{q}) : \overline{U}(\mathfrak{q})|$ is finite. We confine our attention to those (all but finitely many) $\mathfrak{q}$ for which Theorem 3.5 and Lemma 4.1 hold. Let $C(\Gamma) = C$. Now $C \cdot \hat{U}(\mathfrak{q})$ is of finite index in $C \cdot \hat{\Gamma}(\mathfrak{q}) = \hat{\Gamma}(\mathfrak{q})$. It follows that

$$C/C \cap \hat{U}(\mathfrak{q}) \cong C \cdot \hat{U}(\mathfrak{q})/\hat{U}(\mathfrak{q})$$

is an open subgroup of

$$\hat{\Gamma}(\mathfrak{q})/\hat{U}(\mathfrak{q}) \cong \hat{F}_r.$$

By [RZ, Corollary 3.6.4, p.119] C maps *onto* $\hat{F}_{r'}$, for some $r' \geq r = r(\mathfrak{q})$. The result follows from Lemmas 3.7 and 4.6. $\square$

Lemma 4.6 applies, for example, to the case $\mathbf{G} = \mathbf{SL}_2$, $S = \{v\}$ and $\Gamma = SL_2(\mathcal{O})$ (as demonstrated in [Za1]). It is known [Mas1, Theorem 3.1] that, when $\Gamma = SL_2(\mathcal{O})$, the "smallest congruence subgroup" of Γ containing $U(\mathfrak{q})$.

$$\bigcap_{\mathfrak{q}' \neq \{0\}} U(\mathfrak{q}) \cdot \Gamma(\mathfrak{q}') = \Gamma(\mathfrak{q}),$$

for all $\mathfrak{q}$. It follows that in this case $\overline{\Gamma}(\mathfrak{q}) = \overline{U}(\mathfrak{q})$, for all $\mathfrak{q}$.

We now make use of the Strong Approximation Property for $\mathbf{G}$. We will identify $\overline{\mathbf{G}}(\mathcal{O})$ with the restricted topological product

$$\mathbf{G}(\hat{\mathcal{O}}) = \prod_{v \notin S} \mathbf{G}(\mathcal{O}_v).$$

We record a well-known property.

Lemma 4.8. *For all $v \notin S$, $\mathbf{G}(\mathcal{O}_v)$ is virtually a pro-p group.*

Proof. In the notation of Section 1, the subgroup $\mathbf{G}(\mathfrak{m})$ is of finite index in $\mathbf{G}(\mathcal{O}_v)$ and is a pro-p group. (See, for example, [PR, Lemma 3.8, p.138].) $\square$

It is convenient at this point to simplify our notation. We put

$$C = C(\Gamma) \text{ and } \Lambda = \Gamma(\mathfrak{q}).$$

It will always be assumed that Theorem 3.5 applies to $\mathfrak{q}$ and (by Lemma 3.7) that $r(\mathfrak{q}) \geq 2$. We identify $\overline{\Lambda}$ with its embedding in $\mathbf{G}(\hat{\mathcal{O}})$, (via the "diagonal" embedding of Λ). We also identify each $\mathbf{G}(\mathcal{O}_v)$ with its embedding as a normal subgroup of $\mathbf{G}(\hat{\mathcal{O}}_v)$. Let

$$\phi : \hat{\Lambda} \longrightarrow \overline{\Lambda}$$

denote the natural epimorphism.

Definition. For each $v \notin S$, we put

$$N_v = \phi^{-1}(\overline{\Lambda} \cap \mathbf{G}(\mathcal{O}_v)).$$

Lemma 4.9. *For all $v \notin S$, N_v is a closed, normal subgroup of $\hat{\Lambda}$ containing C. Moreover*

$$N_v \cong P_v \amalg N_v(p),$$

where

(i) *P_v is a projective group, all of whose proper, open subgroups are isomorphic to $\hat{F}_\omega$;*

(ii) *$N_v(p)$ is a closed subgroup of $\hat{U}(\mathfrak{q})$ and is a free profinite product of nilpotent pro-p groups, each of class at most 2 and each generated by torsion elements of p-power order.*

Proof. Follows from Lemma 4.2. $\square$

Our next lemmas will be used to establish another condition under which the principal result holds.

Lemma 4.10. *Let $\mid \mathbf{G}(\mathcal{O}) : \Lambda \mid = n$ and let*

$$\pi(\overline{\Lambda}) = \prod_{v \notin S} (\overline{\Lambda} \cap \mathbf{G}(\mathcal{O}_v)).$$

Then, for all $g \in \mathbf{G}(\hat{\mathcal{O}})$,

$$g^{n!} \in \pi(\overline{\Lambda}).$$

Proof. We note that

$$\mid \mathbf{G}(\mathcal{O}_v) : \overline{\Lambda} \cap \mathbf{G}(\mathcal{O}_v) \mid = \mid \overline{\Lambda} \cdot \mathbf{G}(\mathcal{O}_v) : \overline{\Lambda} \mid \leq \mid \mathbf{G}(\hat{\mathcal{O}}) : \overline{\Lambda} \mid \leq n.$$

$\square$

Lemma 4.11. *With the above notation,*

$$\mid \mathbf{G}(\hat{\mathcal{O}}) : \pi(\overline{\Lambda}) \,.\, \overline{U}(\mathfrak{q}) \mid < \infty.$$

Proof. Let

$$\Lambda^* = \overline{\Lambda}/(\pi(\overline{\Lambda}) \,.\, \overline{U}(\mathfrak{q})).$$

Then the (compact, Hausdorff) group Λ^* is finitely generated by Lemma 4.1 and periodic by Lemma 4.10. It follows from Zel'manov's celebrated result [Ze] that Λ^* is finite. □

We are now able to prove the principal result.

Theorem 4.12. *If* Γ *is non-uniform, then*

$$C(\Gamma) \cong \hat{F}_\omega \amalg N(\Gamma),$$

where $N(\Gamma)$ *is a free profinite product of nilpotent pro-p groups, each of class at most* 2 *and each generated by torsion elements of p-power order.*

Proof. There are two possibilities, the first of which can be readily dealt with.

Case A: *For all* $\mathfrak{q}$, *and all* $v \notin S$, $P_v \leq C$.

For all $\mathfrak{q}$ and all $v \notin S$, it follows from Lemma 4.9 that

$$\pi(\overline{\Lambda}) \leq \overline{U}(\mathfrak{q}).$$

The principal result then follows from Lemmas 4.7 and 4.11. We consider the remaining case.

Case B: *There exists* $\mathfrak{q}$ *and* $v \notin S$ *such that* $P_v \nleq C$.

For such a v there exists an open, normal subgroup L of N_v, containing C, such that

$$L \cap P_v \neq P_v.$$

It follows from Lemma 4.4 that

$$L \cong \hat{F}_\omega \amalg \cdots.$$

Restricting ϕ to L, there are again two possibilities. If $\phi(\hat{F}_\omega)$ is trivial, then $C \cap \hat{F}_\omega = \hat{F}_\omega$. Now C is a closed normal subgroup of L. The principal result follows from Lemmas 4.4 and 4.5.

We may assume from now on therefore that $\phi(\hat{F}_\omega)$ is non-trivial. We note that, for all $n \geq 2$,

$$L \cong \hat{F}_n \amalg \cdots .$$

Again restricting ϕ to L there are two cases.

Case (i): *$\phi(\hat{F}_n)$ is finite, for all $n \geq 2$.*

It follows that, for all $n \geq 2$,

$$C \cap \hat{F}_n \cong \hat{F}_{n'},$$

for some $n' \geq n$, by [RZ, Theorem 3.6.2, p.118]. Then, as C is a closed, normal subgroup of L,

$$C \cong \hat{F}_{n'} \amalg \cdots ,$$

by Lemma 4.4. Thus C maps onto $\hat{F}_{n'}$. The principal result follows from Lemma 4.6.

Case (ii): *There exists $n \geq 2$ such that $\phi(\hat{F}_n)$ is infinite.*

We consider $\phi(\hat{F}_n)$ as a subgroup of $\mathbf{G}(\mathcal{O}_v)$. Let $M = \mathbf{G}(\mathfrak{m})$, as defined in the proof of Lemma 4.8. Then

$$(\phi^{-1}(M \cap \phi(\hat{F}_n))) \cap \hat{F}_n \cong \hat{F}_{n'},$$

for some $n' \geq n$, by [RZ, Theorem 3.6.2, p.118], and, under suitable identifications,

$$C \cap \hat{F}_n = C \cap \hat{F}_{n'}.$$

Suppose that $M \cap \phi(\hat{F}_n)$ is non-abelian. Then by [BL] and Lemma 4.8 this group is not free pro-p and hence does not *satisfy Schreier's formula* ([RZ, p.320]), by [RZ, Theorem 8.4.7, p.321]. It follows that $\hat{F}_n / C \cap \hat{F}_n$ does not satisfy Schreier's formula and so

$$C \cap \hat{F}_n \cong \hat{F}_\omega,$$

by [RZ, Corollary 8.4.4, p.320]. The principal result follows from Lemmas 4.4 and 4.5.

There remains the possibility that $M \cap \phi(\hat{F}_n)$ is (finitely generated, infinite and) abelian. Then by [RZ, Lemma 8.4.5, p.320] this group does not satisfy the Schreier formula (in which case the principal result holds as above) *unless* it is infinite cyclic. In the latter case we can use [RZ, Theorem 8.4.3, p.319] to conclude that again

$$C \cap \hat{F}_n \cong \hat{F}_\omega,$$

from which the principal result follows, as above. $\square$

5 Concluding remarks

If the unipotent subgroups which are the factors of $\Lambda(\mathfrak{q})$ in Theorem 3.5 are actually abelian, then $N(\Gamma)$ is a free profinite product of groups , each of which is isomorphic to the direct product of $2^{\aleph_0}$ copies of $\mathbb{Z}/p\mathbb{Z}$. In this case the structure of $C(\Gamma)$ depends *only* on the characteristic of k. This holds, for example, when $\mathbf{G}(\mathcal{O})$ has a two-dimensional representation which applies in particular to the case $\mathbf{G} = \mathbf{SL}_2$, $S = \{v\}$ and $\Gamma = SL_2(\mathcal{O})$. (See [Za1, Theorem 4.3].) From the Tits Classification this also applies to the case where $\mathbf{G}$ is of *type* $\mathbf{C}_2$. See [PRag].

References

[Ba] Udo Baumgartner, Cusps of lattices in rank 1 Lie groups over local fields, Geom. Ded. 99 (2003), 17-46.

[Bo] A. Borel, *Linear Algebraic Groups (Second Enlarged Edition)*, Springer, 1991.

[BL] Y. Barnea and M. Larsen, A non-abelian free pro-p group is not linear over a local field, J. Algebra 214 (1999), 338-341.

[BT] Armand Borel and Jacques Tits, Homomorphismes "abstrait" de groupes algebriques simples, Ann. of Math. (2) 97 (1973), 499-571.

[L1] A. Lubotzky, Free quotients and the congruence kernel of SL_2, J. Algebra 77 (1982), 411-418.

[L2] A. Lubotzky, Lattices in rank one Lie groups over local fields, Geom. Funct. Anal. 1 (1991), 405-431.

[L3] A. Lubotzky, Eigenvalues of the Laplacian, the first Betti number and the congruence subgroup problem, Ann. of Math. 144 (1996), 441-452.

[Mar] G.A. Margulis, *Discrete Subgroups of Semisimple Lie Groups*, Springer, 1991.

[Mas1] A. W. Mason, Congruence hulls in SL_n, J. Pure Appl. Algebra 89 (1993), 255-272.

[Mas2] A.W. Mason, Quotients of the congruence kernels of SL_2 over arithmetic Dedekind domain, Israel J. Math. 91 (1995), 77-91.

[Me] O. V. Mel'nikov, The congruence kernel of the group $SL_2(\mathbb{Z})$, (Russian) Dokl. Akad. Nauk. 228 (1976), 1034-1036. (Translation) Soviet Math. Dokl. 17 (1976), 867-870.

[PR] V. P. Platonov and A. S. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, 1994.

[PRag] G.Prasad and M. S. Raghunathan, Tame subgroup of a semi-simple group over a local field, Amer. J. Math. 105 (1983), 1023-1048.

[PRap] G. Prasad and A. S. Rapinchuk, Computation of the metaplectic kernel, Inst. Hautes Études Sci. Publ. Math. 84 (1996), 91-187.

[R] M.S. Raghunathan, Discrete subgroups of algebraic groups over local fields of positive characteristics, Proc. Indian Acad. Sci. (Math. Sci.) 99 (1989), 127-146.

[RZ] L. Ribes and P.A. Zalesskii, *Profinite Groups*, Springer, 2000.

[S1] J-P. Serre, Le problème des groupes de congruence pour $\mathbf{SL}_2$, Ann. of Math. 92 (1970), 489-527.

[S2] J-P. Serre, *Trees*, Springer, 1980.

[Za1] P.A. Zalesskii, Normal subgroups of free constructions of profinite groups and the congruence kernel in the case of positive characteristic, (Russian) Izv. Ross. Akad. Nauk Ser. Mat. 59 (1995), 59-76. (Translation) Izv. Math 59 (1995), 499-516.

[Za2] P. A. Zalesskii, Profinite surface groups and the congruence kernel of arithmetic lattices in $SL_2(\mathbb{R})$. To appear in the Israel Journal of Mathematics.

[Ze] E. I. Zel'manov, On periodic compact groups, Israel J. Math. 77 (1992), 83-95.