A remark on the congruence subgroup problem

(dedicated to H.Helling for his 60th birthday)

J.Mennicke

Abstract

In the theory of congruence subgroups, one usually shows that, under suitable assumptions, the normal closure of the mth power of an elementary unipotent matrix coincides with the full congruence subgroup $\mod m$.
For applications, it is sometimes useful to study the subgroup generated by the mth powers of the elementary unipotent elements. We give an elementary proof for the fact that in $SL_n(\mathbb{Z})$ for $n \geqslant 3$, this subgroup is normal.

During a visit to Bielefeld, Professor A. Janner raised the following question, in the context of an investigation in cristallography:

Consider the two quadratic forms

$$\begin{aligned} f = &\ 6x^2 - 6xy - 3y^2 - 16z^2 \\ g = &\ -6x^2 + 6xy + 3y^2 - 16z^2, \end{aligned}$$

and the groups of units

$$U = SO_3(f, \mathbb{Z}), V = SO_3(g, \mathbb{Z}).$$

Put $H = \langle U, V \rangle < SL_3(\mathbb{Z})$.

Can one characterise H as a subgroup of $SL_3(\mathbb{Z})$. Is it, in particular, true that

$$|SL_3(\mathbb{Z}) : H| < \infty\,?$$

I have studied this particular problem. It involves some aspects of the theory of congruence subgroups which are not yet in the literature. Therefore, I present these aspects in this note.

Here are the basic definitions:

$$\begin{array}{ll} G = SL_n(\mathbb{Z}), & n \geq 3 \\ m \in \mathbb{N} & \\ E_m = \langle I + me_{ij} \rangle, & \text{subgroup generated by } I + me_{ij}, \forall 1 \leq i \neq j \leq n\,. \\ G_m = \left\{ X \in (a_{ij}) \in G, \right. & \left. \begin{array}{l} a_{ij} \equiv 0 \bmod m \text{ for } i \neq j \\ a_{ii} - 1 = 0 \bmod m^2 \end{array} \right\} \end{array}$$

The standard theory of congruence subgroups proceeds a little differently. One defines

$$\bar{E}_m = NCl_G(E_m), \quad \bar{G}_m = \left\{ X = (a_{ij}) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \bmod m \right\},$$

and one proves $\bar{G}_m = \bar{E}_m$, involving some number theory.

This is not quite good enough for our purposes, since it may be difficult to obtain full contrôle about a normal closure.

The basic theorems for E_m, G_m are:

Theorem 1 $E_m \lhd G_m$.

Theorem 2 $E_m = G_m$.

The proof involves old ideas of L.N. Vaserstein, and of the lecturer. Here are some technical tools:

Lemma 1 *Let $m \mid m'$. Then $G_m = G_{m'} \cdot E_m$.*

Proof: Let $X \in G_m$ be given. We construct a matrix

$$\bar{X} \in E_m$$

such that

$$\begin{aligned} \bar{X} &\equiv X \bmod m' \\ \bar{a}_{ii} &\equiv a_{ii} \bmod m'^2 . \end{aligned}$$

Then

$$X \cdot \bar{X}^{-1} = Y \in G_{m'},$$

and the Lemma holds.

Put $X = (a_{ij}) \in G_m$.

Put $(a_{12}, a_{13}, \ldots, a_{1n}) = c$, the greatest common divisor. Then

$$(c, a_{11}) = 1 .$$

Consider

$$X \begin{pmatrix} 1 & & 0 \\ mt_2 & 1 & \\ \vdots & \ddots & \\ mt_n & c & 1 \end{pmatrix} = X' .$$

We obtain

$$a'_{11} = a_{11} + m(t_2 a_{12} = \cdots + t_n a_{1n}) .$$

c is an integral linear combination of $a_{12}, \ldots, a_{1n}$, hence we obtain for a suitable choice of $t_2, \ldots, t_n$:

$$a'_{11} = a_{11} + mtc .$$