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

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

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 $t_2, \ldots, t_n$:

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

Because of $(a_{11}, c) = 1$ and $(a_{11}, m) = 1$, we can use the Dirichlet Theorem on primes in arithmetic progression to produce

$$a'_{11} = p, a \text{ prime}, \text{ and } (p, m') = 1,\ (p, a_{1n}) = 1\,. \tag{1}$$

Hence we may assume from the beginning $a_{n_1} = p$, and (1) holds.

Consider

$$X \cdot (I + tme_{1n}) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} + t_m a_{11} \\ & & ** & \end{pmatrix}$$

Put $a_{1n} = ma^*_{1n}$, obtaining

$$a'_{1n} = m(a^*_{1n} + ta_{11})$$

Because of $(a_{11}, a_{1n}) = 1$, we can invoke Dirichlet's Theorem, obtaining

$$a'_{1n} = mq\,,$$

q a prime number, $(q, m') = 1$.

Consider $X \cdot (I + t_m a_{n1})$, obtaining

$$a'_{11} = a_{11} + mta_{1n} = a_{11} + m^2 tq\,.$$

Solve the congruence

$$a'_{11} = 1 \bmod m'^2\,. \tag{2}$$

Let $m' = md$. Because of $a_{11} = 1 + m^2 a^*_{11}$, we have $a'_{11} = 1 + m^2 a^*_{11} + m^2 tq$, hence the congruence (2) reads

$$a^*_{11} + tq \equiv 0 \bmod d^2\,.$$

Because of $(q, m') = 1$, we have $(q, d) = 1$, and hence the congruence (2) can be solved.

For $2 \leq j \leq n$, consider $X(I + t_m e_{1j})$, obtaining

$$a'_{1j} = a_{1j} + t_m a_{11}\,.$$

One can solve the congruence $a_{1j} + tma_{11} \equiv 0 \bmod m'$, obtaining

$$X = (a_{ij})\,,$$
$$a_{11} = 1 \bmod m'^2, a_{1j} \equiv 0 \bmod m', 2 \leq j \leq n$$

Consider for $2 \leq j \leq n$: $(I + tme_{j1}) \cdot X$, obtaining

$$a'_{j1} = a_{j1} + tma_{11}$$

One can solve the congruence $a_{j1} + tma_{11} \equiv 0 \bmod m'$, $2 \le j \le n$, obtaining

$$\begin{gathered} X = (a_{ij}) \\ a_{11} \equiv 1 \bmod m'^2 \\ a_{1j} \equiv a_{j1} \equiv 0 \bmod m', \quad 2 \le j \le n\,. \end{gathered}$$

Repeat the argument, obtaining

$$\begin{gathered} X = (a_{ij}) \\ a_{ii} \equiv 1 \bmod m'^2 \\ a_{ij} \equiv a_{ji} \equiv 0 \bmod m', i \neq j \;\, 1 \le i, j \le n\,, \end{gathered}$$

and hence we have for the originally given $X \in G_n$:

$$\begin{gathered} E_1 \dots E_k \cdot X \cdot E_{k+1} \cdots E_r \in G_{m'}\,, \\ E_j \in E_m\,. \end{gathered}$$

Put $E_k^{-1} \dots E_1^{-1} \cdot E_r^{-1} \dots E_{k+1}^{-1} = \bar{X} \in E_m$, obtaining $\bar{X} \equiv X \bmod m', \bar{a}_{ii} \equiv a_{ii} \bmod m'^2$, and hence

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

The proof of Lemma 1 is complete.

The cornerstone of the argument is

Lemma 2 *Let $m \neq 0$ and $g \in SL_n(\mathbb{Q})$ be given and assume $n \ge 3$.*
$\Rightarrow$ *There exists an $m' \neq 0$ such that*

$$X^{-1} g X g^{-1} \in E_m \textit{ for all } X \in G_{m'}\,.$$

Historical remark: An analogue of Lemma 2, for the group SL_2 over maximal orders in algebraic number fields with infinitely many units, was first proved by L.N. Vaserstein.

Our Lemma 2 is a modification of Vaserstein's Lemma. The ring $\mathbb{Z}$ has only the units ± 1. In order to balance this deficiency, we work in SL_n for $n \ge 3$. For $SL_2(\mathbb{Z})$, the Lemma 2 does not hold.

We show how Lemma 2 implies Theorem 1.

Proof of Theorem 1: Let $X \in G_m$ be given, and choose $g = I + me_{ij}, i \neq j$. For these given data m, g, Lemma 2 gives the existence of $m' \neq 0$ such that

$$Y^{-1} g Y g^{-1} \in E_m \quad \text{for all} \quad Y \in G_{m'}\,.$$

Let $(m, m') = d$. Then $m'' = \frac{mm''}{d} = [m, m']$ is the smallest common multiple of m, m'.

Choose $Y \in G_{m'}$ such that it satisfies further congruences:

$$Y \in G_{m''} \, .$$

Then $m \mid m''$, and one can use Lemma 1 to find $E \in E_m$ such that

$$Y = XE \; , \quad E \in E_m \, .$$

We obtain

$$E^{-1} \cdot X^{-1} \cdot g \cdot XE \cdot g^{-1} \in E_m, \quad \text{and hence}$$
$$X^{-1} g X \in E_m \, .$$

Since this holds for all $X \in G_m$, we have proved Theorem 1, modulo Lemma 2.

The proof of Lemma 2 will be broken up into several steps.

Lemma 3 *Let $m \neq 0$ and $g \in GL_n(\mathbb{Q})$ be given.*
$\Rightarrow$ *There exists $m'' \neq 0$ such that*

$$E_{m''} < g E_m g^{-1} \, .$$

Proof: We distinguish several cases:

1. Consider

$$g = \begin{pmatrix} x_1 & & & 0 \\ & x_2 & & \\ 0 & & \ddots & \\ & & & x_n \end{pmatrix}, x_i = \frac{u_i}{v_i}, \; u_i, v_i \in \mathbb{Z} \, .$$

We have:

$$g \cdot (I + m e_{ij}) g^{-1} = I + m x_i x_j^{-1} e_{ij} \, .$$

Choose

$$m'' = m u_1 \dots u_n v_1 \dots v_n \, .$$

Let

$$N = u_j^2 v_i^2 \prod_{l \neq i,j} u_l \cdot \prod_{l \neq i,j} v_l \, .$$

We obtain

$$(I + m x_i x_j^{-1} l_{ij})^N = I + m'' l_{ij} \, .$$

Hence we have

$$I + m'' e_{ij} < g \cdot E_m \cdot g^{-1} \;\; \text{for all } i \neq j, \text{ and hence}$$
$$E_{m''} < g E_m g^{-1} \, .$$

2. Consider

$$g = I + e_{12} = \begin{pmatrix} 1 & 1 & & 0 \\ & 1 & & \\ & & \ddots & \\ & 0 & & 1 \end{pmatrix}$$

For $i, j \neq 1, 2$, the elements g and $I + me_{ij}$ commute:

$$\begin{gathered} I + me_{ij} \leftrightarrows g, \quad \text{and hence} \\ I + me_{ij} \in gE_m g^{-1}, \qquad i, j \neq 1, 2 \end{gathered}$$

Also, $I + me_{1j} \leftrightarrows g$ and hence

$$I + me_{1j} \in gE_m g^{-1}$$

For $j > 2$, we have

$$\begin{gathered} g^{-1}(I + me_{2j})g = (I + me_{ij})(I - me_{1j}), \text{ and hence} \\ I + me_{2j} \in gE_m g^{-1} \text{ for } j > 2\,. \end{gathered}$$

We have

$$g^{-1}(I + me_{j1})g = (I + me_{j1})(I + me_{j2}) \text{ for } j > 2\,,$$

and hence

$$I + me_{j1} \in gE_m g^{-1} \quad \text{for } j > 2\,.$$

We have

$$\begin{gathered} I + me_{j2} \leftrightarrows g, \quad \text{and hence} \\ I + me_{j2} \in gE_m g^{-1}\,. \end{gathered}$$

Hence it remains to consider $I + ke_{21}$.

We have

$$I + m^2 e_{21} = (I + me_{23})(I + me_{31})(I - me_{23})(I - me_{31})$$

This implies:

$$\begin{aligned} I + m^2 e_{21} &= g \cdot g^{-1}(I + me_{23})g \cdot g^{-1}(I + me_{31})g \\ &\quad \cdot g^{-1}(I - me_{23})g \cdot g^{-1}(I - me_{31})g \cdot g^{-1} \\ &= g \cdot (I - me_{13})(I + me_{23})(I + me_{31})(I + me_{32})(I + me_{13}) \\ &\quad \cdot (I - me_{23})(I - me_{31})(I + me_{32}) \cdot g^{-1}\,. \end{aligned}$$

Hence we have

$$Em'' < gE_m g^{-1} \quad \text{for } m'' = m^2\,.$$

3. Let g be a permutation matrix, i.e. a matrix which has precisely one entry $+1$ in each row and column, and 0 otherwise. Because of

$$g(I+me_{ij})g^{-1}=I+me_{kl}, \quad \text{we have}$$
$$Em'' < gE_m g^{-1} \quad \text{for } m''=m\,.$$

4. An arbitrary element $g \in GL_n(\mathbb{Q})$ is a product of matrices of types 1), 2), 3). Apply repeatedly the arguments given under 1), 2), 3), completing the proof of Lemma 3.

Lemma 4 *The elements $g \in GL_n(\mathbb{Q})$ for which Lemma 2 holds true form a subgroup $W < GL_n(\mathbb{Q})$. W is even a normal subgroup in $GL_n(\mathbb{Q})$.*

$$W \lhd GL_n(\mathbb{Q})\,.$$

Proof: The elements $g \in GL_n(\mathbb{Q})$ for which Lemma 2 holds true are precisely these elements for which there is a function

$$m \to m' \quad \text{for all} \;\; m \in \mathbb{N}$$

such that $X^{-1}gXg^{-1} \in E_m$ for all $X \in G_{m'}$.

Let g, g_1 be two elements for which Lemma 2 holds true. For g, m, use Lemma 3 to determine m'' such that

$$E_{m''} < gE_m g^{-1}\,.$$

Because Lemma 2 holds true for g, g_1 start out from m'', and determine m^*, m^{**} for m'' and g, g_1, respectively such that

$$\begin{array}{rcll} X^{-1}gXg^{-1} & \in & E_{m''} & \text{for all } X \in G_{m^*} \\ Y^{-1}\cdot g_1 Y \cdot g_1^{-1} & \in & E_{m''} & \text{for all } Y \in G_{m^{**}}\,. \end{array}$$

Conclude for $m^+ = m^* \cdot m^{**}$:

$$\left.\begin{array}{rcl} X^{-1}\cdot g\cdot X\cdot g^{-1} & \in & E_{m''} \\ X^{-1}\cdot g_1\cdot X\cdot g_1^{-1} & \in & E_{m''} \end{array}\right. \quad \text{for all } X \in G_{m^+}\,.$$

This implies

$$\begin{array}{ll} g\cdot X^{-1}\cdot g^{-1}X\cdot X^{-1}g_1Xg_1^{-1} \in E_{m''}\,, & \text{and hence} \\ g\cdot X^{-1}\cdot g^{-1}g_1X\cdot g_1^{-1} \in E_{m''} & \text{for all } X \in G_{m^+}\,. \end{array}$$

This implies

$$X^{-1}\cdot g^{-1}g_1X\cdot g_1^{-1}g \in g^{-1}E_{m''}g < E_m \text{ for all } X \in G_{m^+}\,.$$

Hence we have constructed a function

$$m \longrightarrow m^+$$

for the element $g^{-1}g_1$. Hence Lemma 2 holds for $g^{-1}g_1$. Hence the elements for which Lemma 2 holds true form a subgroup

$$W < GL_n(\mathbb{Q})\,.$$

Next we prove that the subgroup W is normal in $GL_n(\mathbb{Q})$.

Let $g \in W$ and $g_1 \in GL_n(\mathbb{Q})$.

Use Lemma 3 to determine for g_1^{-1} and m an element $m'' \neq 0$ such that

$$E_{m''} < g_1^{-1} E_m g_1\,.$$

For m'', g, determine m^* such that

$$X^{-1} g X g^{-1} \in E_{m''} \quad \text{for all } X \in G_{m^*}\,.$$

Hence we obtain

$$g_1 \cdot X^{-1} g X g^{-1} g_1^{-1} \in g_1 E_{m''} g_1^{-1} < E_m \quad \text{for all } X \in G_{m^*}\,.$$

Rewrite this equation obtaining

$$(g_1 X g_1^{-1})^{-1} \cdot g_1 g g_1^{-1} (g_1 X g_1^{-1}) \cdot (g_1 g g_1^{-1})^{-1} \in E_m \text{ for all } X \in G_{m^*}\,.$$

Put $Y := g_1 X g^{-1},\ X = g_1^{-1} Y g_1$. Because $g_1 \in GL_n(\mathbb{Q})$, there is $N \in \mathbb{N}$ such that

$$g_1 = \frac{1}{N} g_2,\ g_2 \in M_n(\mathbb{Z}),\ \det g_2 = M \in \mathbb{Z}\,.$$

Choose $M \in \mathbb{N}$ minimal with this property. We obtain

$$\begin{array}{ll} g_2 = N g_1,\ g_2^{-1} = N^{-1} g_1^{-1}, & \text{and hence} \\ g_1^{-1} Y g_1 = N \cdot g_2^{-1} Y \frac{1}{N} g_2 = g_2^{-1} Y g_2\,. & \end{array}$$

The inverse of g_2:

$$g_2^{-1} = \frac{1}{M} g_3,\ g_3 \in M_n(\mathbb{Z})\,.$$

Hence we have

$$g_3 \cdot g_2 = M \cdot I\,.$$

Choose $M' = M m^{*2}$, obtaining for $Y \in G_{M'}$:

$$g_1^{-1} Y g_1 = g_2^{-1} Y g_2 = \frac{1}{M} g_3 Y g_2\,.$$

The matrix $g_3 Y g_2 \in M_n(\mathbb{Z})$ has integral entries, and we can compute congruences $\bmod M'$, $M' = M m^{*2}$, obtaining

$$M g_1^{-1} Y g_1 \equiv g_3 Y g_2 \equiv g_3 \cdot I g_2 \equiv g_3 g_2 \equiv M I \bmod M m^{*2}\,.$$

Dividing all entries by M, we find

$$g_1^{-1} Y g \in M_n(\mathbb{Z}) \,,$$

and moreover: $g_1^{-1} Y g_1 \equiv I \bmod m^{*2}$.

Hence we have, in particular

$$g_1^{-1} Y g_1 = X \in G_{m^*} \quad \text{for all } Y \in G_{M'} \,.$$

Hence we conclude

$$Y^{-1} \cdot g_1 g g_1^{-1} \cdot Y (g_1 g g_1^{-1})^{-1} \in E_m \text{ for all } Y \in G_{M'} \,.$$

Hence we have constructed a function

$$m \longrightarrow M'$$

such that

$$Y^{-1} \cdot g_1 g g_1^{-1} \cdot Y \cdot (g_1 g g_1^{-1})^{-1} \in E_m \text{ for all } Y \in G_{M'} \,.$$

Hence $g_1 g g_1^{-1} \in W$ for all $g \in W$ and all $g_1 \in GL_n(\mathbb{Q})$.

Hence $W \lhd GL_n(\mathbb{Q})$ is a normal subgroup.

We have completed the proof of Lemma 4.

Remember that the group $GL_n(\mathbb{Q})$ has no normal non-central subgroups not containing $SL_n(\mathbb{Q})$. Hence in order to prove Lemma 2, it suffices to produce a non-central element $g \in SL_n(\mathbb{Q})$ for which Lemma 2 holds true.

Lemma 5 *For*

$$g = \begin{pmatrix} b & & & & 0 \\ & b & & & \\ & & b^{-2} & & \\ & 0 & & 1 & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix} , \quad \begin{array}{l} b \in \mathbb{Z} \,, \\ b^2 \neq 1 \,, \end{array}$$

and for the function

$$m \longrightarrow m' = b^3 m \,,$$

Lemma 2 holds true.

Proof: Let $X \in G_{m'},\ X = (a_{ij})$. Consider

$$X \begin{pmatrix} 1 & & & \\ 0 & 1 & & 0 \\ t_3 m' & & 1 & \\ \vdots & & & \ddots \\ & & & 0 \\ t_n m' & & & 1 \end{pmatrix} \cdot \begin{pmatrix} & * & & \\ & & & \\ & & & \\ a'_{n1} a_{n2} & & & a_{nn} \end{pmatrix} \text{ obtaining}$$

$$a'_{n1} = a_{n1} + t_3 m' a_{n2} + \cdots + t_n m' a_{nm}$$

Put $a_{n1} = m' a^*_{n1}$,

$$d = (a_{n3}, \ldots, a_{nn}), \quad a_{nj} = d a'_{nj}, \quad 3 \le j \le n\,,$$

obtaining

$$a'_{n1} = n' a^*_{n1} + m' d(t_3 a'_{n3} + \cdots + t_n a'_{nm})\,.$$

If $p \mid d$ and $p \mid a_{n2}$, then $p \nmid m'$ and $p \nmid a_{n1}$, hence $p \nmid a^*_{n1}$.
If $p \mid d$ and $p \mid a_{n1}$, then $p \nmid m'$ and $p \nmid a_{n2}$.

Choose $t_3, \ldots t_n$ such that

$$\begin{aligned} t_3 a'_{n3} + \cdots + t_n a'_{nn} &= 1 && \text{for } n \ge 4, \text{ and} \\ a'_{n1} &= m'(a^*_{n1} + t a'_{33}) && \text{for } n = 3, \text{ such that} \\ (a'_{31}, a_{32}) &= m'\,. \end{aligned}$$

In both cases we have

$$(a'_{n1}, a_{n2}) = m'\,.$$

Consider

$$X \cdot (I + t m' e_{1n} + r m' e_{2n}) = \begin{pmatrix} & * & \\ a_{n1} \cdots & & a_{nn-1} a'_{nn} \end{pmatrix}\,,$$

obtaining

$$a'_{nn} = a_{nn} + t m' a_{n1} + r m' a_{n2}\,.$$

¿From $a_{n1} = m' a'_{n1}, a_{n2} = m' a'_{n2}, (a'_{n1}, a'_{n2}) = 1$ we conclude

$$a'_{nn} = a_{nn} + m'^2 (t a'_{n1} + r a'_{n2})\,.$$

Because of $a_{nn} \equiv 1 \bmod m'^2$ we can choose $t, r \in \mathbb{Z}$ such that

$$a'_{nn} = 1\,.$$

Consider

$$X \begin{pmatrix} 1 & & & \\ & 1 & & \\ & \ddots & & \\ & & 1 & \\ t_2 m' & t_2 m' & t_{n-1} m' & 1 \end{pmatrix} = \begin{pmatrix} & * & & \\ & & & \\ a_{n1} + t_1 m' & a_{n2} + t_2 m' \ldots a_{nn-1} + t_{n-1} m' & & 1 \end{pmatrix}.$$

Choose $t_i \in \mathbb{Z}$ such that

$$X = \begin{pmatrix} & * & \\ 0\ 0 & \dots & 0\ 1 \end{pmatrix} .$$

Consider

$$\begin{pmatrix} 1 & & & & m'u_1 \\ & 1 & & & m'u_2 \\ & & \ddots & & \\ & & & 1 & m'u_{n-1} \\ & & & & 1 \end{pmatrix} X = \begin{pmatrix} * & & & 0 \\ & & & 0 \\ & & & \vdots \\ & & & 0 \\ 0\ 0 & & \dots 0 & 1 \end{pmatrix} .$$

Define

$$\begin{aligned} K_n = \ & \langle \ \ I + m'e_{nj},\ j = 1, \dots, n-1 \\ & \quad\ \ I + m'e_{j1},\ j = 3, \dots, n \\ & \quad\ \ I + m'e_{1n}, I + m'e_{2n} \rangle \\ \\ H_n = \ & \langle \ \ I + m'e_{jn},\ j = 1, \dots, n-1 \rangle . \end{aligned}$$

We have shown that

$$\begin{aligned} & X = E_n \cdot X_{n-1} \cdot F_n , \\ & E_n \in H_n, F_n \in K_n . \end{aligned}$$

Define

$$\begin{aligned} K_{n-i} = \ & \langle \ \ I + m'e_{n-i,j},\ j = 1, \dots, n-i-1 \\ & \quad\ \ I + m'e_{j1},\ j = 3, \dots, n-i \\ & \quad\ \ I + m'e_{1n-i},\ I + m'e_{2,n-i} \rangle \\ \\ H_n = \ & \langle \ \ I + m'e_{j,n-i},\ j = 1, \dots, n-i-1 \rangle , \end{aligned}$$

for $i = 0, 1, 2, \dots, n-3$.

The above argument yields a decomposition

$$X = E_n E_{n-1} \dots E_3 \cdot Y \cdot F_3 \dots F_{n-1} F_n ,$$

$$Y = \begin{pmatrix} b_{11} & b_{12} & & 0 \dots \\ b_{21} & b_{22} & & \\ & & 1 & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

$$\begin{matrix} E_{n-i} & \in & H_{n-i} \\ F_{n-i} & \in & K_{n-i} \end{matrix} \quad i = 0, 1, \dots, n-3 .$$

The assertion of Lemma 2 can be written this way:

$$F_n^{-1} \dots F_3^{-1} Y^{-1} E_3^{-1} \dots E_n^{-1} g \cdot E_{11} \dots E_3 Y F_3 \dots F_n g^{-1} \in E_n .$$

Because of $m \mid m'$, the assertion reduces to

$$Y^{-1} E_3^{-1} \dots E_n^{-1} \cdot g \cdot E_n \dots E_3 \cdot Y \cdot F_3 \dots F_n g^{-1} \in E_m .$$

We have

$$I + m'e_{nj} \leftrightarrows g \qquad \text{for } j \geq 4$$

$$\begin{array}{rcll} g(I+m'te_{n1})g^{-1} &=& I+b^{-1}m'te_{n1} & \\ g(I+m'te_{n2})g^{-1} &=& I+b^{-1}m'te_{n2} & \text{for } n \geq 4 \\ g(I+m'te_{n3})g^{-1} &=& I+m'tb^2e_{n3} & \end{array}$$

$$\begin{array}{rcl} g(I+m'te_{31})g^{-1} &=& I+b^{-3}m'te_{31} \\ g(I+m'te_{32})g^{-1} &=& I+b^{-3}m'te_{32} \end{array}$$

$$g(I+m'te_{j1})g^{-1} = I+b^{-1}m'te_{j1} \qquad \text{for } j > 3$$

$$\begin{array}{rcll} g(I+m'te_{1n})g^{-1} &=& I+bm'te_{1n} & \\ g(I+m'te_{2n})g^{-1} &=& I+bm'te_{2n} & \text{for } n \geq 4 \end{array}$$

$$\begin{array}{rcl} g(I+m'te_{13})g^{-1} &=& I+m'b^3te_{13} \\ g(I+m'te_{23})g^{-1} &=& I+m'b^3te_{23}\,. \end{array}$$

Hence one can shift the elements of K_n across g, reducing the assertion to

$$Y^{-1}\cdot E_3^{-1}\dots E_n^{-1}\cdot g\cdot E_n\dots E_3\cdot Y\cdot F_3\dots F_{n-1}g^{-1}\in E_m\,.$$

For the elements of K_{n-i}, one needs the formulas

$$I + m'e_{\mu,\nu} \leftrightarrows g \qquad \text{for } \mu,\nu \geq 4$$

$$\begin{array}{rcll} g(I+m'te_{n-i,1})g^{-1} &=& I+m'tb^{-1}e_{n-i,1} & \\ g(I+m'te_{n-i,2})g^{-1} &=& I+m'tb^{-1}e_{n-i,2} & \text{for } n-i \geq 4 \\ g(I+m'te_{n-i,3})g^{-1} &=& I+m'tb^2e_{n-i,3} & \end{array}$$

$$g(I+m'te_{j1})g^{-1} = I+m'tb^{-1}e_{j1}$$

$$\begin{array}{rcll} g(I+m'te_{1n-i})g^{-1} &=& I+bm'te_{1n-i} & \text{for } n-i \geq 4 \\ g(I+m'te_{2,n-i})g^{-1} &=& I+bm'te_{2n-i} & \end{array}$$

These formulas permit to shift the factors $F_3,\dots,F_n$ across g, reducing the assertion to

$$Y^{-1}E_3^{-1}\dots E_n^{-1}gE_n\dots E_3Yg^{-1}\in E_m\,.$$

The elements Y, g commute:

$$Y \leftrightarrows g\,,$$

reducing the assertion to

$$Y^{-1}\cdot E_3^{-1}\dots E_n^{-1}gE_n\dots E_3\cdot g^{-1}\cdot Y\in E_m$$

We have

$$\begin{array}{ll} I+m'e_{j,n-i} \leftrightarrows g & \text{for } j \geq 4, n-i \geq 4 \\ I+m'e_{j,n-i} \leftrightarrows Y & \text{for } j \geq 3, n-i \geq 3 \end{array}$$

For $n-i=3$ and $j=1,2$, we have

$$g(I+m'te_{j3})g^{-1}=I+m'b^3te_{j3}\,.$$

Hence one can shift all elements E_{n-i} across g, possibly changing exponents.

For $n-i=3, j=1,2$ we use the fact that these elements are normalized by Y.

The same argument holds for $j=1,2$ and $n-i\geq 4$.

Hence we have proved that for

$$g=\begin{pmatrix} b & & & & & 0\\ & b & & & & \\ & & b^{-2} & & & \\ & & & 1 & & \\ & & & & \ddots & \\ 0 & & & & & 1 \end{pmatrix}, b\in\mathbb{Z}, b^2\neq 1$$

and $m'=b^3m$ the Lemma 2 holds true. We have completed the proof of Lemma 5. We have also completed the proof of Theorem 1:

$$E_m \lhd G_m\,.$$

Lemma 6 *For*

$$X=\begin{pmatrix} a & b & a\\ c & d & a\\ 0 & 0 & 1\end{pmatrix}\in G_m,\quad Y=\begin{pmatrix} a & b' & 0\\ c' & d' & 0\\ 0 & 0 & 1\end{pmatrix}\in G_m\,,$$

we have

$$X\cdot Y\equiv\begin{pmatrix} a & bb' & 0\\ c'' & d'' & 0\\ 0 & 0 & 1\end{pmatrix}\bmod E_m\,.$$

Proof: By Lemma 2, for m and

$$g_1=\begin{pmatrix} 0 & 0 & 1\\ -1 & 0 & 0\\ 0 & -1 & 0\end{pmatrix},$$

we can find $m'\neq 0$ such that

$$U^{-1}g_1Ug_1^{-1}\in E_m \text{ for all } U\in G_{m'}\,.$$

We may enlarge m' by adding further congruence conditions, achieving $m \mid m'$.

By Lemma 1, we can decompose Y:

$$Y=UE,\ U\in G_{m'},\ E\in E_m\,,$$

obtaining $U = YE^{-1}$ and

$$\begin{array}{l} EY^{-1}g_1YE^{-1}g_1^{-1} \in E_m \text{ and hence} \\ Y^{-1}g_1Yg_1^{-1} \cdot g_1E^{-1}g_1^{-1} \in E_m\,. \end{array}$$

Because g_1 is a generalized permutation matrix, it normalises E_m:

$$g_1 \cdot E_m \cdot g_1^{-1} = E_m\,.$$

Hence we obtain

$$Y^{-1}g_1Yg_1^{-1} \in E_m\,.$$

Hence we have

$$Y \equiv g_1Yg_1^{-1} \bmod E_m \text{ for all } Y \in G_m\,.$$

The same argument, applied to

$$g_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \text{yields}$$

$$Y \equiv g_2Yg_2^{-1} \bmod E_m \text{ for all } Y \in G_m\,.$$

The following matrix computation is standard in the theory of congruence subgroups:

$$Y_1 = g_1Yg_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b' \\ a & c' & d' \end{pmatrix} \equiv Y \bmod E_m$$

$$XY_1 = \begin{pmatrix} a & ab & bb' \\ c & ad & b'd \\ 0 & c' & d' \end{pmatrix}$$

$$U_1 = XY_1 \begin{pmatrix} 1 & -b & \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} a & 0 & bb' \\ c & 1 & b'd \\ 0 & c' & d' \end{pmatrix}$$

$$U_2 = U_1 \begin{pmatrix} 1 & 0 & 0 \\ -c & 1 & -b'd \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 & bb' \\ 0 & 1 & 0 \\ c'' & c' & d'' \end{pmatrix}$$

$$U_3 = \begin{pmatrix} 1 & & \\ & 1 & \\ & -c' & 1 \end{pmatrix} U_2 = \begin{pmatrix} a & 0 & bb' \\ 0 & 1 & 0 \\ c'' & 0 & d'' \end{pmatrix}$$

$$U_4 = g_2^{-1}U_3g_2 = \begin{pmatrix} a & bb' & 0 \\ c'' & d'' & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We have shown that

$$U_4 \equiv XY \bmod E_m \,.$$

We have completed the proof of Lemma 6. We shall now prove Theorem 2. By Lemma 6, the map

$$Y = \begin{pmatrix} a & b & & 0 \\ c & d & & \\ & & 1 & \\ & & & \ddots & \\ & 0 & & & 1 \end{pmatrix} \bmod E_m, \;\; Y \in G_m$$

$$\to \begin{bmatrix} b \\ a \end{bmatrix} = E_m \begin{pmatrix} a & b & & a \\ c & d & & \\ & & 1 & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}$$

defines a group symbol.

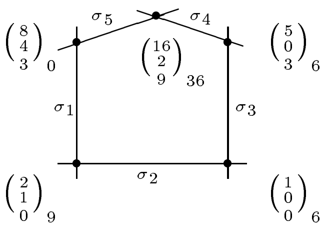
A group symbol on $\mathbb{Z}$ is known to be trivial. Hence we conclude $G_m/E_m = 1$, i.e. $G_m = E_m$. We have completed the proof of Theorem 2.

We now come to the question posed by Professor Janner.

It is a routine matter to compute the groups of units of the forms f and g, respectively see e.g. [2] for more details. We describe the results

$$f = 6x^2 - 6xy - 3y^2 - 16z^2 \,.$$

A fundamental domain is a pentagon with four right angles and one angle 0.



We list the hyperbolic lines bounding the fundamental domain:

$$\begin{aligned} \sigma_1 &= (1\ 1\ 0)_{-3} \\ \sigma_2 &= (0\ 0\ 1)_{-16} \\ \sigma_3 &= (1,\ 2,\ 0)_{-18} \\ \sigma_4 &= (8\ 0\ 5)_{-16} \\ \sigma_5 &= (6,\ 3,\ 2)_{-12} \end{aligned}$$

The reflection in the lines σ_i are units. The indices denote the various spinor normes. Here are the reflections in σ_i:

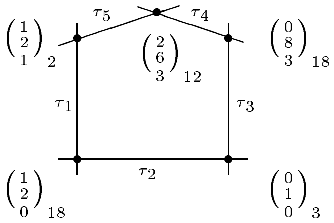
$$X_1 = \begin{pmatrix} -3 & 4 & 0 \\ -2 & 3 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad X_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad X_3 = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

$$X_4 = \begin{pmatrix} 49 & 24 & 80 \\ 0 & -1 & 0 \\ -30 & 15 & 49 \end{pmatrix}, \quad X_5 = \begin{pmatrix} -31 & 24 & 48 \\ -10 & 7 & 16 \\ -15 & 12 & 23 \end{pmatrix}$$

$$U = \langle X_1, X_2, X_3, X_4, X_5 \rangle = SO_3(f, \mathbb{Z})$$

$$g = -6x^2 + 6xy + 3y^2 - 16z^2$$

The fundamental domain is a pentagon with five right angles.



$$\begin{aligned} \tau_1 &= (1\ 0\ 0)_{-6} \\ \tau_2 &= (0,\ 0,\ 1)_{-16} \\ \tau_3 &= (1, -1, 0)_{-9} \\ \tau_4 &= (0, 2, 1)_{-4} \\ \tau_5 &= (8, 16, 9)_{-144} \end{aligned}$$

The reflection in the lines are units:

$$Y_1 = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad Y_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad Y_3 = \begin{pmatrix} 1 & 0 & 0 \\ -2 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$Y_4 = \begin{pmatrix} -1 & 0 & 0 \\ -6 & -7 & 16 \\ -3 & -3 & 7 \end{pmatrix}, \quad Y_5 = \begin{pmatrix} -1 & -8 & 16 \\ 0 & -17 & 32 \\ 0 & -9 & 17 \end{pmatrix}$$

$$V = \langle Y_1, Y_2, Y_3, Y_4, Y_5 \rangle = SO_3(g, \mathbb{Z})$$

Let $H = \langle U, V \rangle$. We shall show that

Theorem 3 $\qquad |SL_3(\mathbb{Z}) : H| < \infty.$

Proof: We must try to produce sufficiently many elementary unipotent elements in H.

We note some computations:

$$X_2X_5X_2Y_4 = \begin{pmatrix} 31 & -24 & 48 \\ 16 & -1 & 0 \\ -12 & 15 & -31 \end{pmatrix}$$

$$(X_2X_5X_2Y_4)^{2n} = \begin{pmatrix} 1 & 0 & 0 \\ 480n & 1-384n & 768n \\ 240n & -192n & 1+384n \end{pmatrix}, \ n \in \mathbb{Z}$$

$$W_1 = Y_3 \cdot (X_2X_5X_2Y_4)^{2n} \cdot Y_3^{-1} \cdot (X_2X_5X_2Y_4)^{-2n} = \begin{pmatrix} 1 & 0 & 0 \\ -1728n & 1 & 0 \\ -864n & 0 & 1 \end{pmatrix}$$

$$Y_2 \cdot W_1 \cdot Y_2^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -1728n & 1 & 0 \\ -864n & 0 & 1 \end{pmatrix}$$

$$W_{31} = Y_2W_1Y_2^{-1}W_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -864n & 0 & 1 \end{pmatrix}$$

$$W_{21} = W_1^{-2}W_{31}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 3456n & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$W_{32} = (Y_1W_{31})^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1728n & 1 \end{pmatrix}$$

Take W_1 for $n = 1$, obtaining

$$W_2 = W_1^5 (X_2 X_5 X_2 Y_4)^{36} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -6911 & 13824 \\ 0 & -3456 & 6913 \end{pmatrix}$$

$$W_3 = Y_1 W_2 Y_1^{-1} W_2^{-1} = \begin{pmatrix} 1 & -6912 & 13824 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$W_{12} = (Y_2 W_3)^2 = \begin{pmatrix} 1 & -13824 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$W_{13} = Y_2 W_3 Y_2^{-1} W_3^{-1} = \begin{pmatrix} 1 & 0 & -27648 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$W_{23} = Y_3 W_{13} Y_3^{-1} W_{13}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -55296 \\ 0 & 0 & 1 \end{pmatrix}$$

Hence we have

$$I + m e_{ij} \in H,\ \ i,j = 1,2,3,\ \ i \neq j \ \ \text{for } m = 55296 = 2^{11} \cdot 3^3\,.$$

Using Theorem 2, we conclude

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

It is a routine computation to produce the precise index. One has to examine the image of $< x_1, \ldots y_5 >$ in the finite group $SL_3(\mathbb{Z}|m\mathbb{Z})$ for $m = 2^{11}3^3$.

Of course, the method which we have deployed carries over to $SL_n(\mathcal{O})$ for maximal orders in number fields, $n \geq 3$.

References

[1] Vaserstein, L.N.: On the group SL_2 over Dedekind rings of arithmetical type, Mat. Sbornik 89 (131), 1972

[2] Fricke, R. und Klein, F.: Vorlesungen "uber die Theorie der automorphe Funktionen, Bd.1 (XIV +634 S.), 1897, Bd.2 (VIII +668 S.), Lieferung 1, 1901, Lieferung 2, 1911, Lieferung 3, 1912, Leipzig, Teubner.