A REMARK ON THE CONGRUENCE SUBGROUP PROBLEM

J. MENNICKE

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

Abstract

In the theory of congruence subgroups, one usually shows that, under suitable assumptions, the normal closure of the $m$th 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 $m$th powers of the elementary unipotent elements. We give an elementary proof for the fact that in $\text{SL}_n(\mathbb{Z})$ for $n \geq 3$, this subgroup is normal in a suitably defined congruence subgroup of $\text{SL}_n(\mathbb{Z})$. Moreover, the two subgroups coincide.

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

Consider the two quadratic forms

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

and the groups of units

\[ U = \text{SO}_3(f, \mathbb{Z}), V = \text{SO}_3(g, \mathbb{Z}). \]

Put $H = \langle U, V \rangle < \text{SL}_3(\mathbb{Z})$.

Can one characterise $H$ as a subgroup of $\text{SL}_3(\mathbb{Z})$. Is it, in particular, true that

\[ |\text{SL}_3(\mathbb{Z}) : H| < \infty ? \]

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:

---

Received August 12, 1997.
A REMARK ON THE CONGRUENCE SUBGROUP PROBLEM

\[ G = \text{SL}_n(\mathbb{Z}), \quad n \geq 3 \]

\[ m \in \mathbb{N} \]

\[ E_m = \langle I + me_{ij} \rangle, \]

subgroup generated by \( I + me_{ij}, \forall 1 \leq i \neq j \leq n \).

\[ G_m = \left\{ X \in \begin{pmatrix} a_{ij} \end{pmatrix} \in G, \begin{array}{l} a_{ij} \equiv 0 \mod m \text{ for } i \neq j \vspace{0.5em} \quad \forall 1 \leq i \leq n \text{ and } 1 \leq j \leq n \end{array} \right\} \]

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

\[ \bar{E}_m = N\text{Cl}_G(E_m), \quad \bar{G}_m = \left\{ X \equiv (a_{ij}) = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \mod m \right\}, \]

and one proves \( \bar{G}_m = \bar{E}_m \), involving some number theory (see [1], and more generally [2]).

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

The basic theorems for \( E_m, G_m \) are:

**Theorem 1.** \( E_m = G_m \).

One of the main ingredients of the proof of Theorem 1 is

**Theorem 2.** \( E_m \triangleleft G_m \).

**Remark.** Going through the subsequent proof, it is not difficult to see that Theorem 2 holds much more generally. In fact, a minor modification of our arguments shows that the theorem holds true for Dedekind rings of arithmetical type, in particular for maximal orders in algebraic number fields. Also Theorem 1 generalises. For more details, see [2].

The proofs of Theorem 1 and 2 involve old ideas of L. N. Vaserstein, and of the present author.

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

\[ \tilde{X} \in E_m \]

such that

\[ \tilde{X} \equiv X \mod m' \]

\[ \tilde{a}_{ii} \equiv a_{ii} \mod m'^2 . \]

Then

\[ X \cdot \tilde{X}^{-1} = Y \in G_{m'} \]
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

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

We obtain

\[
a'_{11} = a_{11} + mt(t_2a_{12} + \cdots + t_na_{1n}).
\]

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 progressions to produce

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

Hence we may assume from the beginning \( a_{11} = p \), and (1) holds.

Consider

\[
X \cdot (I + tme_{1n}) = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} + tma_{11} \\
\end{pmatrix}
\]

Put \( a_{1n} = ma_{1n}' \), obtaining

\[
da'_{1n} = m(a_{1n}' + ta_{11})
\]

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

\[
da'_{1n} = mq,
\]

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

Consider \( X \cdot (I + tm_e_{n1}) \), obtaining

\[
da'_{11} = a_{11} + mta'_{1n} = a_{11} + m^2tq.
\]

Solve the congruence

\[
(2) \quad a'_{11} \equiv 1 \mod m'^2.
\]
Let $m' = md$. Because of $a_{11} = 1 + m^2 a_{11}$, we have $d_{11}' = 1 + m^2 a_{11} + m^2 t q$, hence the congruence (2) reads

$$d_{11}' + t q \equiv 0 \mod d^2.$$ 

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

$$d_{1j}' = a_{1j} + t m a_{11}.$$ 

One can solve the congruence $a_{1j} + t m a_{11} \equiv 0 \mod m'$, obtaining

$$X = (a_{1j})$$

$$a_{11} \equiv 1 \mod m^2, a_{1j} \equiv 0 \mod m', 2 \leq j \leq n$$

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

$$d_{1j}' = a_{1j} + t m a_{11}$$ 

One can solve the congruence $a_{1j} + t m a_{11} \equiv 0 \mod m'$, $2 \leq j \leq n$, obtaining

$$X = (a_{1j})$$

$$a_{11} \equiv 1 \mod m^2$$

$$a_{1j} \equiv a_{1j} \equiv 0 \mod m', 2 \leq j \leq n.$$ 

Repeat the argument, obtaining

$$X = (a_{1j})$$

$$a_{11} \equiv 1 \mod m^2$$

$$a_{ij} \equiv a_{ij} \equiv 0 \mod m', i \neq j 1 \leq i, j \leq n,$$

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

$$E_1 \ldots E_k \cdot X \cdot E_{k+1} \ldots E_r \in G_{m'},$$

$$E_j \in E_m.$$ 

Put $E_1^{-1} \ldots E_1^{-1} \cdot E_{r+1}^{-1} \ldots E_{k+1}^{-1} = \tilde{X} \in E_m$, obtaining $\tilde{X} \equiv X \mod m', \alpha_{ii} \equiv a_{ii} \mod m^2$, and hence

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

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 $n \geq 3$.

$\Rightarrow$ There exists an $m' \neq 0$ such that

$$X^{-1} g X g^{-1} \in E_m$$ for all $X \in G_{m'}$. 
Historical remark. An analogue of Lemma 2, for the group $\text{SL}_2$ over maximal orders in algebraic number fields with infinitely many units, was first proved by L. N. Vaserstein (see [3]).

Our Lemma 2 is a modification of Vaserstein’s Lemma. The ring $\mathbb{Z}$ has only the units $\pm 1$. In order to balance this deficiency, we work in $\text{SL}_n$ for $n \geq 3$. For $\text{SL}_2(\mathbb{Z})$ and $\mathbb{Q}$, the Lemma 2 does not hold.

We show how Lemma 2 implies Theorem 2.

Proof of Theorem 2. 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

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

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 $m | m''$, 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 2, modulo Lemma 2.

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

Lemma 3. Let $m \neq 0$ and $g \in \text{GL}_n(\mathbb{Q})$ be given.

⇒ There exists $m'' \neq 0$ such that

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

Proof. We distinguish several cases:

Case 1. Consider

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

We have:
A REMARK ON THE CONGRUENCE SUBGROUP PROBLEM

\[ g \cdot (I + me_{ij})g^{-1} = I + m\alpha_i x_j^{-1}e_{ij}. \]

Choose

\[ m'' = mu_1 \ldots u_nv_1 \ldots v_n. \]

Let

\[ N = u_j^2v_j^2 \prod_{l \neq i,j} u_l \cdot \prod_{l \neq i,j} v_l. \]

We obtain

\[ (I + m\alpha_i x_j^{-1}e_{ij})^N = I + m''e_{ij}. \]

Hence we have

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

**Case 2.** Consider

\[ g = I + e_{12} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & \ddots & \vdots \\ 0 & \ldots & 1 \end{pmatrix} \]

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

\[ I + me_{ij} \cong g, \quad \text{and hence} \]
\[ I + me_{ij} \in gE_mg^{-1}, \quad i, j \neq 1,2 \]

Also, \( I + me_{1j} \cong g \) and hence

\[ I + me_{1j} \in gE_mg^{-1} \]

For \( j > 2 \), we have

\[ g^{-1}(I + me_{2j})g = (I + me_{2j})(I - me_{1j}), \text{ and hence} \]
\[ I + me_{2j} \in gE_mg^{-1} \text{ for } j > 2. \]

We have

\[ g^{-1}(I + me_{1j})g = (I + me_{1j})(I + me_{2j}) \text{ for } j > 2, \]

and hence

\[ I + me_{1j} \in gE_mg^{-1} \quad \text{for } j > 2. \]
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:

$$I + m^2 e_{21} = g \cdot g^{-1}(I + me_{23})g \cdot g^{-1}(I + me_{31})g$$

$$\cdot g^{-1}(I - me_{23})g \cdot g^{-1}(I - me_{31})g \cdot g^{-1}$$

$$= g \cdot (I - me_{13})(I + me_{23})(I + me_{31})(I + me_{32})(I + me_{13})$$

$$\cdot (I - me_{23})(I - me_{31})(I + me_{32}) \cdot g^{-1}.$$
A REMARK ON THE CONGRUENCE SUBGROUP PROBLEM

\[
X^{-1}gXg^{-1} \in E_{m^*} \quad \text{for all } X \in G_{m^*}.
\]
\[
Y^{-1} \cdot g_1 Y \cdot g_1^{-1} \in E_{m^*} \quad \text{for all } Y \in G_{m^*}.
\]

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

\[
X^{-1} \cdot g \cdot X \cdot g^{-1} \in E_{m^*} \quad \text{for all } X \in G_{m^*}.
\]
\[
X^{-1} \cdot g_1 \cdot X \cdot g_1^{-1} \in E_{m^*} \quad \text{for all } X \in G_{m^*}.
\]

This implies

\[
g \cdot X^{-1} \cdot g \cdot X \cdot X^{-1}g_1Xg_1^{-1} \in E_{m^*}, \text{ and hence}
\]
\[
g \cdot X^{-1} \cdot g_1^{-1}X \cdot g_1^{-1} \in E_{m^*} \quad \text{for all } X \in G_{m^*}.
\]

This implies

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

Hence we have constructed a function

\[
m \rightarrow m^+
\]

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

\[
W < \text{GL}_n(Q).
\]

Next we prove that the subgroup \(W\) is normal in \(\text{GL}_n(Q)\).

Let \(g \in W\) and \(g_1 \in \text{GL}_n(Q)\).

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

\[
E_{m''} < g_1^{-1}E_{m_2}g_1.
\]

For \(m'', g\), determine \(m^*\) such that

\[
X^{-1}gXg^{-1} \in E_{m''} \quad \text{for all } X \in G_{m''}.
\]

Hence we obtain

\[
g_1 \cdot X^{-1}gXg^{-1}c_1^{-1} \in g_1E_{m''}g_1^{-1} < E_m \quad \text{for all } X \in G_{m''}.
\]

Rewrite this equation obtaining

\[
(g_1Xg_1^{-1})^{-1} \cdot g_1gg_1^{-1}(g_1Xg_1^{-1}) \cdot (g_1gg_1^{-1})^{-1} \in E_m \quad \text{for all } X \in G_{m''}.
\]

Put \(Y := g_1Xg_1^{-1}, X = g_1^{-1}Yg_1\). Because \(g_1 \in \text{GL}_n(Q)\), there is \(N \in \mathbb{N}\) such that

\[
g_1 = \frac{1}{N}g_2, \quad g_2 \in M_n(\mathbb{Z}), \quad \det g_2 = M \in \mathbb{Z}.
\]
Choose $M \in \mathbb{N}$ minimal with this property. We obtain
\[ g_2 = Ng_1, \quad g_2^{-1} = N^{-1}g_1^{-1}, \quad \text{and hence} \]
\[ g_1^{-1} Yg_1 = N \cdot g_2^{-1} Y \frac{1}{N} g_2 = g_2^{-1} Yg_2. \]
The inverse of $g_2$:
\[ g_2^{-1} = \frac{1}{M} g_3, \quad g_3 \in M_n(\mathbb{Z}). \]
Hence we have
\[ g_3 \cdot g_2 = M \cdot I. \]
Choose $M' = Mm^2$, obtaining for $Y \in G_{M'}$:
\[ g_1^{-1} Yg_1 = g_2^{-1} Yg_2 = \frac{1}{M} g_3 Yg_2. \]
The matrix $g_3 Yg_2 \in M_n(\mathbb{Z})$ has integral entries, and we can compute congruences mod $M'$, $M' = Mm^2$, obtaining
\[ Mg_1^{-1} Yg_1 \equiv g_3 Yg_2 \equiv g_3 \cdot I g_2 \equiv g_3 g_2 \equiv M I \text{ mod } Mm^2. \]
Dividing all entries by $M$, we find
\[ g_1^{-1} Yg_1 \in M_n(\mathbb{Z}), \]
and moreover: $g_1^{-1} Yg_1 \equiv I \text{ mod } m^2$.
Hence we have, in particular
\[ g_1^{-1} Yg_1 = X \in G_{m'}, \quad \text{for all } Y \in G_{M'}. \]
Hence we conclude
\[ Y^{-1} \cdot g_1 Yg_1^{-1} \cdot Y \cdot (g_1 Yg_1^{-1})^{-1} \in E_m \text{ for all } Y \in G_{M'}. \]
Hence we have constructed a function
\[ m \rightarrow M' \]
such that
\[ Y^{-1} \cdot g_1 Yg_1^{-1} \cdot Y \cdot (g_1 Yg_1^{-1})^{-1} \in E_m \text{ for all } Y \in G_{M'}. \]
Hence $g_1 Yg_1^{-1} \in W$ for all $g \in W$ and all $g_1 \in \text{GL}_n(\mathbb{Q})$.
Hence $W \triangleleft \text{GL}_n(\mathbb{Q})$ is a normal subgroup.
We have completed the proof of Lemma 4.

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

**Lemma 5.** For

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

and for the function

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

Lemma 2 holds true.

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

$$X = \begin{pmatrix} 1 & 0 & \cdots & \cdots \\ 0 & 1 & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots \\ t_n m' & \cdots & \cdots & 1 \end{pmatrix} = \begin{pmatrix} * \\ * \\ * \\ * \end{pmatrix}$$

obtaining

$$d'_{n1} = a_{n1} + t_3 m' a_{n3} + \cdots + t_n m' a_{nn}.$$ 

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

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

obtaining

$$d'_{n1} = m' a_{n1}^* + m' d(t_3 d'_{n3} + \cdots + t_n d'_{nn}).$$

If $p \mid d$ and $p \nmid a_{n2}$, 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

$$t_3 d'_{n3} + \cdots + t_n d'_{nn} = 1 \quad \text{for } n \geq 4, \text{ and }$$

$$d'_{n1} = m'(a_{n1}^* + td'_3) \quad \text{for } n = 3, \text{ such that }$$

$$(a'_{31}, a_{32}) = m'.$$

In both cases we have
\[(d'_{n1}, a_{n2}) = m'.\]

Consider
\[
X \cdot (I + tm'e_{1n} + rm'e_{2n}) = \begin{pmatrix} * & \cdots & a_{n-1} & d'_{nn} \\ a_{n1} & \cdots & & \end{pmatrix},
\]

obtaining
\[
d'_{nn} = a_{nn} + tm'a_{n1} + rm'a_{n2}.
\]

From \(a_{n1} = m'd'_{n1}, a_{n2} = m'd'_{n2}, (d'_{n1}, d'_{n2}) = 1\) we conclude
\[
d'_{nn} = a_{nn} + m^2(td'_{n1} + rd'_{n2}).
\]

Because of \(a_{nn} \equiv 1 \mod m^2\) we can choose \(t, r \in \mathbb{Z}\) such that
\[
d'_{nn} = 1.
\]

Consider
\[
\begin{pmatrix} 1 \\ 1 \\ \vdots \\ t_1m' \\ t_2m' \\ \cdots \\ t_{n-1}m' \\ 1 \end{pmatrix}
\]

Choose \(t_i \in \mathbb{Z}\) such that
\[
X = \begin{pmatrix} * & \cdots & 0 \\ 0 & \cdots & 0 \end{pmatrix}.
\]

Consider
\[
\begin{pmatrix} 1 & m'u_1 \\ \vdots & \vdots \\ m'u_{n-1} & 1 \end{pmatrix} \begin{pmatrix} m'u_1 \\ m'u_2 \\ \vdots \\ m'u_{n-1} \end{pmatrix} = \begin{pmatrix} * & 0 \\ 0 & \cdots \\ 0 & \cdots \\ 0 & 1 \end{pmatrix}.
\]

Define
\[
K_n = \langle I + m'e_{nj}, j = 1, \ldots, n - 1 \rangle
\]
\[
I + m'e_{j1}, j = 3, \ldots, n
\]
\[
I + m'e_{1n}, I + m'e_{2n}
\]
\[
H_n = \langle I + m'e_{jn}, j = 1, \ldots, n - 1 \rangle.
\]

We have shown that
A REMARK ON THE CONGRUENCE SUBGROUP PROBLEM

\[ X = E_n \cdot X_{n-1} \cdot F_n, \]
\[ E_n \in H_n, F_n \in K_n. \]

Define

\[ K_{n-i} = \langle I + m'e_{n-i,j}, j = 1, \ldots, n - i - 1 \]
\[ I + m'e_{n-1}, j = 3, \ldots, n - i \]
\[ I + m'e_{1,n-i}, I + m'e_{2,n-i} \rangle \]
\[ H_{n-i} = \langle I + m'e_{j,n-i}, j = 1, \ldots, n - i - 1 \rangle, \]

for \( i = 0, 1, 2, \ldots, n - 3. \)

The above argument yields a decomposition

\[ X = E_nE_{n-1} \cdots E_3 \cdot Y \cdot F_3 \cdots F_{n-1}F_n, \]
\[ Y = \begin{pmatrix} b_{11} & b_{12} & 0 \\ b_{21} & b_{22} & 1 \\ & \ddots & \ddots \\ & & 0 & 1 \end{pmatrix} \]
\[ E_{n-i} \in H_{n-i} \]
\[ F_{n-i} \in K_{n-i} \]

The assertion of Lemma 2 can be written this way:

\[ F_n^{-1} \cdots F_3^{-1} Y^{-1} E_3^{-1} \cdots E_n^{-1} g \cdot E_n \cdots E_3 Y F_3 \cdots F_n g^{-1} \in E_m. \]

Because of \( m | m', \) the assertion reduces to

\[ Y^{-1} E_3^{-1} \cdots E_n^{-1} \cdot g \cdot E_n \cdots E_3 \cdot Y \cdot F_3 \cdots F_n g^{-1} \in E_m. \]

We have

\[ I + m'e_{nj} \leftrightarrow g \quad \text{for} \quad j \geq 4 \]
\[ g(I + m'te_{n1})g^{-1} = I + b^{-1}m'te_{n1} \]
\[ g(I + m'te_{n2})g^{-1} = I + b^{-1}m'te_{n2} \quad \text{for} \quad n \geq 4 \]
\[ g(I + m'te_{n3})g^{-1} = I + m'tb^2e_{n3} \]
\[ g(I + m'te_{31})g^{-1} = I + b^{-3}m'te_{31} \]
\[ g(I + m'te_{32})g^{-1} = I + b^{-3}m'te_{32} \]
\[ g(I + m'te_{j1})g^{-1} = I + b^{-1}m'te_{j1} \quad \text{for} \quad j > 3 \]
\[ g(I + m'te_{1n})g^{-1} = I + bm'te_{1n} \]
\[ g(I + m'te_{2n})g^{-1} = I + bm'te_{2n} \quad \text{for} \quad n \geq 4 \]
\[ g(I + m'te_{13})g^{-1} = I + m'b^3te_{13} \]
\[ g(I + m'te_{23})g^{-1} = I + m'b^3te_{23}. \]
Hence one can shift the elements of $K_n$ across $g$, reducing the assertion to
\[ Y^{-1} \cdot E_3^{-1} \ldots E_n^{-1} \cdot g \cdot E_n \ldots E_3 \cdot Y \cdot F_3 \ldots F_{n-1}g^{-1} \in E_m. \]

For the elements of $K_{n-i}$, one needs the formulas
\[
I + m't e_{\mu,\nu} \rightleftarrows g \quad \text{for } \mu, \nu \geq 4
\]
\[
g(I + m't e_{n-i,1})g^{-1} = I + m'tb^{-1}e_{n-i,1} \quad \text{for } n - i \geq 4
\]
\[
g(I + m't e_{n-i,2})g^{-1} = I + m'tb^{-1}e_{n-i,2} \quad \text{for } n - i \geq 4
\]
\[
g(I + m't e_{n-i,3})g^{-1} = I + m'tb^2e_{n-i,3}
\]
\[
g(I + m't e_{j,1})g^{-1} = I + m'tb^{-1}e_{j,1} \quad \text{for } n - i \geq 4
\]
\[
g(I + m't e_{j,2})g^{-1} = I + m'tb e_{j,2} \quad \text{for } n - i \geq 4
\]
\[
g(I + m't e_{j,3})g^{-1} = I + m'tb^2 e_{j,3}
\]

These formulas permit to shift the factors $F_3, \ldots, F_n$ across $g$, reducing the assertion to
\[ Y^{-1}E_3^{-1} \ldots E_n^{-1}gE_n \ldots E_3 Yg^{-1} \in E_m. \]

The elements $Y, g$ commute:
\[ Y \rightleftarrows g, \]
reducing the assertion to
\[ Y^{-1} \cdot E_3^{-1} \ldots E_n^{-1} \cdot g \cdot E_n \ldots E_3 \cdot g^{-1} \cdot Y \in E_m. \]

We have
\[
I + m't e_{j,n-i} \rightleftarrows g \quad \text{for } j \geq 4, n - i \geq 4
\]
\[
I + m't e_{j,n-i} \rightleftarrows Y \quad \text{for } j \geq 3, n - i \geq 3
\]

For $n - i = 3$ and $j = 1, 2$, we have
\[ g(I + m't e_{j,3})g^{-1} = I + m'tb^3 e_{j,3}. \]

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
A REMARK ON THE CONGRUENCE SUBGROUP PROBLEM

\[
g = \begin{pmatrix}
    b & 0 \\
    b^{-2} & 1 \\
    b & 1 \\
    1 & 0
\end{pmatrix}, \quad b \in \mathbb{N}, b^2 \neq 1
\]

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 2:

\[E_m \triangleleft G_m.\]

**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

\[X \cdot Y \equiv \begin{pmatrix}
    a & bb' & 0 \\
    c'' & d'' & 0 \\
    0 & 0 & 1
\end{pmatrix} \mod E_m.\]

The Lemma holds in much greater generality, and is a consequence of known facts, see in particular Lemmas 8 and 10 of [6].

Lemma 6 obviously implies Theorem 1, see [1]. We have established Theorem 1.

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. [4] 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:

\[
\sigma_1 = (1, 1, 0)_{-3} \\
\sigma_2 = (0, 0, 1)_{-16} \\
\sigma_3 = (1, 2, 0)_{-18} \\
\sigma_4 = (8, 0, 5)_{-16} \\
\sigma_5 = (6, 2, 3)_{-12}
\]
The reflection in the lines $\sigma_i$ are units. The indices denote the various spinor normes. Here are the reflections in $\sigma_i$:

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

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

\[
U = \langle X_1, X_2, X_3, X_4, X_5 \rangle = \text{SO}_3(f, \mathbb{Z})
\]

\[
g = -6x^2 + 6xy + 3y^2 - 16z^2
\]

The fundamental domain is a pentagon with five right angles.

\[
\begin{align*}
\tau_1 &= (1 \ 0 \ 0)_{-6} \\
\tau_2 &= (0 \ 0 \ 1)_{-16} \\
\tau_3 &= (1 \ -1 \ 0)_{-9} \\
\tau_4 &= (0 \ 2 \ 1)_{-4} \\
\tau_5 &= (8 \ 16 \ 9)_{-144}
\end{align*}
\]

The reflection in the lines are units:

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

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

\[
V = \langle Y_1, Y_2, Y_3, Y_4, Y_5 \rangle = \text{SO}_3(g, \mathbb{Z})
\]

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

**Theorem 3.** \( |\text{SL}_3(\mathbb{Z}) : H | < \infty \).

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

We note some computations:
A REMARK ON THE CONGRUENCE SUBGROUP PROBLEM

\[ X_2X_5X_2 Y_4 = \begin{pmatrix} 31 & -24 & 48 \\ 16 & -1 & 0 \\ -12 & 15 & -31 \end{pmatrix} \]

\[(X_2X_5X_2 Y_4)^{2n} = \begin{pmatrix} 1 & 0 & 0 \\ 480n & 1 - 384n & 768n \\ 240n & -192n & 1 + 384n \end{pmatrix}, \ n \in \mathbb{Z} \]

\[ W_1 = Y_3 \cdot (X_2X_5X_2 Y_4)^{2n} \cdot Y_3^{-1} \cdot (X_2X_5X_2 Y_4)^{-2n} = \begin{pmatrix} 1 & 0 & 0 \\ -1728n & 1 & 0 \\ -864n & 0 & 1 \end{pmatrix} \]

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

\[ W_{31} = Y_2 W_1 Y_2^{-1} W_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -864n & 0 & 1 \end{pmatrix} \]

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

\[ W_{32} = ( Y_1 W_{31} )^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1728n & 1 \end{pmatrix} \]

Take \( W_1 \) for \( n = 1 \), obtaining

\[ W_2 = W_1^5 (X_2X_5X_2 Y_4)^{36} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -6911 & 13824 \\ 0 & -3456 & 6913 \end{pmatrix} \]

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

\[ W_{12} = ( Y_2 W_3 )^2 = \begin{pmatrix} 1 & -13824 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \]
Using Theorem 1, we conclude

\[ |\text{SL}_3(\mathbb{Z}) : H| < \infty. \]

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 \( \text{SL}_3(\mathbb{Z}/m^2\mathbb{Z}) \) for \( m = 2^{11} \cdot 3^3 \).

Thanks go to the referee for useful comments and references.

It is also understood that Vaserstein’s idea and its generalization such as presented in this paper lend themselves to a broad generalization, both to different types of discrete subgroups of simple Lie groups and to linear groups over more general rings where the elementary number theory used in this paper can be mimicked.

REFERENCES