LIE REGULAR GENERATORS OF GENERAL LINEAR GROUP $GL(4, \mathbb{Z}_n)$

SWATI MAHESHWARI AND R. K. SHARMA

Abstract. In this article, we discuss the existence of Lie regular matrices in $\mathcal{M}(4, \mathbb{Z}_n)$. It is shown that the linear group $GL(4, \mathbb{Z}_n)$ is generated by Lie regular matrices for all $n > 1$.

1. Introduction

Special linear group $SL(n, \mathbb{Z})$ is the multiplicative group of all $n \times n$ matrices with integer entries having determinant 1. It is well known that $SL(n, \mathbb{Z})$ is generated by transvections, the matrices T_{ij} ($1 \leq i, j \leq n, i \neq j$) with 1's on the diagonal and in the (i, j)-th position and 0's elsewhere. Generators of unimodular group, the linear group $GL(n, \mathbb{Z})$ of all $n \times n$ matrices with integer entries having determinant ± 1, has been discussed in [1, p.85], [5]. In 2012, Sharma et al. introduced Lie regular elements and Lie regular units for non commutative rings (see [2, 3]). They have given generators of linear group $GL(2, \mathbb{Z}_n)$, for some $n > 1$ in terms of Lie regular units. They proposed an open problem to determine rings that have Lie regular units and whether it is possible to generate the whole unit group of such rings using Lie regular units. We are considering this problem with the ring $\mathcal{M}(4, \mathbb{Z}_n)$. In this article, we will discuss the existence of Lie regular units in the ring $\mathcal{M}(4, \mathbb{Z}_n)$ and will show that Lie regular units generate $GL(4, \mathbb{Z}_n)$ for $n > 1$.

Throughout this article, ϕ denotes the Euler's totient function and $\mathcal{U}(\mathbf{R})$ denotes the unit group of the ring $\mathbf{R}$. $|A|$ denotes the cardinality of the set A. Suppose G is a group then $o(G)$ denotes the order of G and $o(g)$ denotes the order of an element g of G.

2. Preliminaries

We shall frequently use the following well known results to prove our main results.

2010 *Mathematics Subject Classification.* Primary 20H25; 16U60; 20F05.
Key words and phrases. Linear Group; Lie regular elements.

Lemma 2.1. *The linear group $SL(n,\mathbb{Z})$ is generated by transvections, the matrices T_{ij} $(1 \leq i \neq j \leq n)$ with 1's on the diagonal and in the (i,j)-th position and 0's elsewhere.*

Lemma 2.2. [4, p.21] *The natural map from $SL(n,\mathbb{Z}) \to SL(n,\mathbb{Z}_m)$ is onto.*

Note that we denote image of a transvection T_{ij} by T_{ij} itself.

Corollary 2.1. *Transvections generate $SL(n,\mathbb{Z}_m)$.*

Lemma 2.3. *Suppose m and n are two positive integers such that $(m,n) = 1$. Then $\mathcal{U}(\mathbb{Z}_{mn}) \cong \mathcal{U}(\mathbb{Z}_m) \times \mathcal{U}(\mathbb{Z}_n)$.*

Definition 2.1. [3] *An element 'a' of a ring $\mathbf{R}$ is said to be Lie regular if $a = [e,u] = eu - ue$, where e is an idempotent in $\mathbf{R}$ and u is a unit in $\mathbf{R}$. Further, a unit in $\mathbf{R}$ is said to be Lie regular unit if it is Lie regular as an element of $\mathbf{R}$.*

Proposition 2.1. [3, Proposition 2.6] *Let $\mathbf{F}$ be a field then the inverse of a Lie regular unit in $\mathcal{M}(2,\mathbf{F})$ is again Lie regular.*

Proposition 2.2. [3, Proposition 2.14] *If $\mathbf{R}$ is a commutative ring then any element in $\mathcal{M}(2,\mathbf{R})$ of the form*

$$\begin{pmatrix} \lambda y & x \\ -y & -\lambda y \end{pmatrix}, \begin{pmatrix} -\lambda y & -y \\ x & \lambda y \end{pmatrix}, \begin{pmatrix} -\lambda y & y \\ -x & \lambda y \end{pmatrix}, \begin{pmatrix} \lambda y & -x \\ y & -\lambda y \end{pmatrix},$$

where λ, x and y belong to $\mathbf{R}$ and xy is invertible in $\mathbf{R}$, is a Lie regular element.

3. Lie regular elements in $\mathcal{M}(4,\mathbb{Z}_m)$

Proposition 3.1. *If $\mathbf{R}$ is a commutative ring with unity and A, B are Lie regular elements (units) in $\mathcal{M}(2,\mathbf{R})$, that is, $A = [e,u]$ and $B = [e_1,u_1]$. Then the block matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ is also a Lie regular element (unit) in $\mathcal{M}(4,\mathbf{R})$.*

Proof. Observe that,

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \left[\begin{pmatrix} e & 0 \\ 0 & e_1 \end{pmatrix}, \begin{pmatrix} u & 0 \\ 0 & u_1 \end{pmatrix} \right].$$

This completes the proof. □

Note that if $\mathbf{R}$ is a field then the inverse of $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ is also a Lie regular unit in $\mathcal{M}(4,\mathbf{R})$.

Proposition 3.2. *If* $\mathbf{R}$ *is a commutative ring with unity and* A, B *are Lie regular elements (units) in* $\mathcal{M}(2,\mathbf{R})$ *such that* $A = [e, u]$ *and* $B = [e, u_1]$. *Then the block matrix* $\begin{pmatrix} 0 & A \\ B & 0 \end{pmatrix}$ *is also a Lie regular element (unit) in* $\mathcal{M}(4,\mathbf{R})$.

Proof. Observe that,

$$\begin{pmatrix} 0 & A \\ B & 0 \end{pmatrix} = \left[\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}, \begin{pmatrix} 0 & u \\ u_1 & 0 \end{pmatrix} \right].$$

This completes the proof. □

For example take $A, B \in \mathcal{M}(2,\mathbb{Z}_m)$ such that

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right]$$

and

$$B = \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix} = \left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -\alpha & 0 \end{pmatrix} \right],$$

where $\alpha \in \mathcal{U}(\mathbb{Z}_m)$. Then $\begin{pmatrix} 0 & A \\ B & 0 \end{pmatrix}$ is a Lie regular unit in $\mathcal{M}(4,\mathbb{Z}_m)$.

Note that If $\mathbf{R}$ is a field then the inverse of $\begin{pmatrix} 0 & A \\ B & 0 \end{pmatrix}$ is also a Lie regular unit in $\mathcal{M}(4,\mathbf{R})$.

Proposition 3.3. *Suppose* $A = \begin{pmatrix} 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & e & 0 & f \\ g & 0 & 0 & 0 \end{pmatrix}$ *and* $B = \begin{pmatrix} 0 & a & b & 0 \\ c & 0 & 0 & d \\ e & 0 & 0 & f \\ 0 & g & 0 & 0 \end{pmatrix}$ *are elements in* $GL(4,\mathbf{R})$. *Then* A, B *are Lie regular in* $GL(4,\mathbf{R})$. *Further the element* $C = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ *is also a Lie regular element in* $GL(4,\mathbf{R})$.

Proof. It follows once we observe that

$$A = \left[\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -a & 0 & -b \\ c & 0 & d & 0 \\ 0 & -e & 0 & -f \\ g & 0 & 0 & 0 \end{pmatrix} \right].$$

$$B = \left[\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & a & b & 0 \\ -c & 0 & 0 & -d \\ -e & 0 & 0 & -f \\ 0 & g & 0 & 0 \end{pmatrix} \right].$$

$$C = \left[\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \right].$$

□

Proposition 3.4. *Suppose $A \in GL(2, \mathbf{R})$. Then the block matrix $\begin{pmatrix} A & A \\ -A & -A \end{pmatrix}$ is a Lie regular element in $GL(4, \mathbf{R})$.*

Proof. Observe that

$$\begin{pmatrix} A & A \\ -A & -A \end{pmatrix} = \left[\begin{pmatrix} I_d & I_d \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & A \\ A & 0 \end{pmatrix} \right].$$

This completes the proof. □

Lemma 3.1. *The order of the linear group $SL(4, \mathbb{Z}_m)$ is $\frac{o(GL(4,\mathbb{Z}_m))}{\phi(m)}$.*

Proof. Consider a group homomorphism $\theta : GL(4, \mathbb{Z}_m) \to \mathcal{U}(\mathbb{Z}_m)$ by

$$\theta(A) = determinant(A).$$

The map is surjective, thus result holds. □

4. Generators of Linear Groups

Lemma 4.1. *For each invertible element $\alpha \in \mathbb{Z}_m$, the number of matrices in $\mathcal{M}(4, \mathbb{Z}_m)$ having determinant α is equal to the order of $SL(4, \mathbb{Z}_m)$.*

Proof. Let α be an invertible element in $\mathbb{Z}_m$ and $N_\alpha(4, \mathbb{Z}_m)$ is the set of all 4×4 matrices having determinant α. Define a map

$$\eta : SL(4, \mathbb{Z}_m) \to N_\alpha(4, \mathbb{Z}_m)$$

by

$$\eta \left[\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix} \right] = \begin{pmatrix} \alpha a & \alpha b & \alpha c & \alpha d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix}.$$

We see that η is one-one. Thus $|N(4, \mathbb{Z}_m)| \geq |SL(4, \mathbb{Z}_m)|$, which gives $|\cup_{\alpha \in \mathcal{U}(\mathbb{Z}_m)} N_\alpha(4, \mathbb{Z}_m)| \geq \phi(m)|SL(4, \mathbb{Z}_m)|$. The result follows from the Lemma 3.1. □

Proposition 4.1. *Let p be a prime. Then the order of the linear group $GL(4,\mathbb{Z}_{p^n})$ is $p^{3(4n-2)}(p+1)^2(p^2+1)(p^2+p+1)(\phi(p^n))^4$.*

Proof. This is well known that the natural homomorphism

$$f : GL(4,\mathbb{Z}_{p^n}) \to GL(4,\mathbb{Z}_p)$$

is onto. Observe that $|ker(f)| = (p^{n-1})^{16}$. By using first isomorphism theorem, we get

$$\begin{aligned} o(GL(4,\mathbb{Z}_{p^n})) &= o(GL(4,\mathbb{Z}_p))|ker(f)| \\ &= p^{3(4n-2)}(p+1)^2(p^2+1)(p^2+p+1)(\phi(p^n))^4. \end{aligned}$$

□

Proposition 4.2. *Suppose $m > 1$ is a positive integer such that $m = \prod_{i=1}^{k} p_i^{r_i}$, where p_i's are distinct primes. Then*

$$o(GL(4,\mathbb{Z}_m) = \prod_{i=1}^{k} o(GL(4,\mathbb{Z}_{{p_i}^{r_i}})).$$

Proof. Since $\mathbb{Z}_{p_1^{r_1}\cdots p_k^{r_k}} \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$. Thus

$$o(GL(4,\mathbb{Z}_{p_1^{r_1}\cdots p_k^{r_k}})) = \prod_{i=1}^{k} o(GL(4,\mathbb{Z}_{{p_i}^{r_i}})).$$

□

Lemma 4.2. *Any transvection T_{ij} $(1 \le i \le 4)$ in $\mathcal{M}(4,\mathbb{Z}_m)$ can be written as a combination of a, b and c, where*

$$a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \text{ and } c = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Proof. The proof is based on the following well known result

$$[T_{ij}, T_{jk}] = T_{ij}T_{jk}T_{ij}^{-1}T_{jk}^{-1} = T_{ik},$$

whenever i, j, k are distinct and $1 \le i, j, k \le 4$. Observe that

T_{ij}	combination in a, b, c	T_{ij}	combination in a, b, c
T_{43}	ab	T_{21}	ba
T_{14}	$c^{-1}(ab)^{-1}c$	T_{32}	$c^{-1}bac$
T_{13}	$T_{14}T_{43}T_{14}^{-1}T_{43}^{-1}$	T_{12}	$T_{13}T_{32}T_{13}^{-1}T_{32}^{-1}$
T_{23}	$T_{21}T_{13}T_{21}^{-1}T_{13}^{-1}$	T_{24}	$T_{21}T_{14}T_{21}^{-1}T_{14}^{-1}$
T_{31}	$T_{32}T_{21}T_{32}^{-1}T_{21}^{-1}$	T_{34}	$T_{32}T_{24}T_{32}^{-1}T_{24}^{-1}$
T_{41}	$T_{43}T_{31}T_{43}^{-1}T_{31}^{-1}$	T_{42}	$T_{43}T_{32}T_{43}^{-1}T_{32}^{-1}$

This completes the proof. □

Lemma 4.3. *For $m > 1$, $SL(4, \mathbb{Z}_m)$ is generated by Lie regular elements a, b and c, where*

$$a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \text{ and } c = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Proof. First, observe that a, b and $c \in SL(4, \mathbb{Z}_m)$. Suppose H is a subgroup of $SL(4, \mathbb{Z}_m)$ generated by a, b, c. Let K denotes a subgroup generated by transvections T_{ij}. Then by above lemma, we have

$$K \leq H \leq SL(4, \mathbb{Z}_m).$$

By using Corollary 2.1, $K = SL(4, \mathbb{Z}_m)$ and result follows. □

Let $n = \prod_{i=1}^{k} p_i^{r_i}$ be an odd positive integer. Then an element $\alpha \in \mathcal{U}(\mathbb{Z}_n)$ is called a *primitive element modulo* $p_i^{r_i}$ in $\mathbb{Z}_n$ if order of α modulo n is $\phi(p_i^{r_i})$.
For the forthcoming results, m denotes an odd positive integer such that $m = \prod_{i=1}^{k} p_i^{r_i}$, where p_i's are distinct primes and $r_i \geq 0$.

Theorem 4.1. *Let $\alpha_i \in \mathcal{U}(\mathbb{Z}_{2m})$ be a primitive element modulo $p_i^{r_i}$ in $\mathbb{Z}_{2m}$ for each i and $\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv 1 \; mod \; 2m$, $0 \leq j_i < \phi(p_i{}^{r_i})$, where $j_1, j_2 \ldots j_k$ are not simultaneously zero. Then the linear group $GL(4, \mathbb{Z}_{2m})$ is generated by Lie regular units a, b, c, d and e_i, where $1 \leq i \leq k$,*

$$a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; c = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$d = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \; e_i = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \alpha_i & 0 & 0 & 0 \end{pmatrix}.$$

Proof. By using Lemma 2.3, for each i there exists an element $\alpha_i \in \mathcal{U}(\mathbb{Z}_{2m})$ such that $o(\alpha_i) = \phi(p_i^{r_i})$ and $\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv 1 \bmod 2m$ for $0 \leq j_i < \phi(p_i{}^{r_i})$. First, observe that a, b, c, d and $e_i \in GL(4, \mathbb{Z}_{2m})$. Let G be a subgroup of $GL(4, \mathbb{Z}_{2m})$ generated by a, b, c, d and e_i. Set $x_i = e_i d = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \alpha_i \end{pmatrix}$. Then the order of x_i is $\phi(p_i^{r_i})$. Consider a

group

$$H = \langle x_1, x_2, \ldots, x_k |\ x_i^{\phi(p_i^{r_i})}, x_i x_j = x_j x_i, 1 \leq i, j \leq k \rangle.$$

Then H is a subgroup of G. Since $\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv 1 \bmod 2m$, clearly $\prod_{i=1}^{k} x_i^{j_i} \not\equiv 1 \bmod 2m$. Thus the canonical form of H is given by

$$\langle \prod_{i=1}^{k} x_i^{j_i} |\ 0 \leq j_i < \phi(p_i^{r_i}) \rangle$$

and the order of H is $\prod_{i=1}^{k} \phi(p_i^{r_i})$. We can see that an arbitrary element of H is of the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$$

with determinant β, where $\beta = \prod_{i=1}^{k} \alpha_i^{j_i}$. We also have that a, b, c generate $SL(4, \mathbb{Z}_{2m})$ (by Lemma 4.3). Observe that

$$H \cap SL(4, \mathbb{Z}_{2m}) = \{I_4\}.$$

Now we have

$$o(HSL(4, \mathbb{Z}_{2m})) = \prod_{i=1}^{k} \phi(p_i^{r_i}) o(SL(4, \mathbb{Z}_{2m})).$$

Since $HSL(4, \mathbb{Z}_{2m}) \subseteq G \leq GL(4, \mathbb{Z}_{2m})$ and by using Lemma 3.1,

$$o(GL(4, \mathbb{Z}_{2m})) = \prod_{i=1}^{k} \phi(p_i^{r_i}) o(SL(4, \mathbb{Z}_{2m})).$$

Therefore $HSL(4, \mathbb{Z}_{2m}) = GL(4, \mathbb{Z}_{2m})$. Hence result follows. □

Theorem 4.2. *Let $m > 1$ and $\alpha_i \in \mathcal{U}(\mathbb{Z}_m)$ be a primitive element modulo $p_i^{r_i}$ in $\mathbb{Z}_m$ for each i and $\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv 1$ mod m, $0 \leq j_i < \phi({p_i}^{r_i})$, where $j_1, j_2 \ldots j_k$ are not simultaneously zero. Then the linear group $GL(4, \mathbb{Z}_m)$ is generated by Lie regular units a, b, c, d and e_i, where $1 \leq i \leq k$,*

$$a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},\ b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},\ c = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$d = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},\ e_i = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \alpha_i & 0 & 0 & 0 \end{pmatrix}.$$

Proof. Proof of this theorem is similar to the previous theorem. □

Theorem 4.3. *Let $\alpha_i \in \mathcal{U}(\mathbb{Z}_{4m})$ be a primitive element modulo $p_i^{r_i}$ in $\mathbb{Z}_{4m}$ for each i and $\beta \in \mathcal{U}(\mathbb{Z}_{4m})$ with $o(\beta) = 2$ such that $\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv \beta^j \bmod 4m$, $0 \leq j_i < \phi(p_i^{r_i})$ and $j = 0, 1$, where $j, j_1, j_2 \ldots j_k$ are not simultaneously zero. Then the linear group $GL(4, \mathbb{Z}_{4m})$ is generated by a, b, c, d, e_i and f, where $1 \leq i \leq k$,*

$$a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; c = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$d = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \; e_i = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \alpha_i & 0 & 0 & 0 \end{pmatrix}, \; f = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \beta & 0 & 0 & 0 \end{pmatrix}.$$

Proof. By using Lemma 2.3, for $1 \leq i \leq k$, we have $\alpha_i, \beta \in \mathcal{U}(\mathbb{Z}_{4m})$ such that $\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv \beta \bmod 4m$, where $0 \leq j_i < \phi(p_i^{r_i})$. First, observe that a, b, c, d, e_i and $f \in GL(4, \mathbb{Z}_{4m})$. Let G be a subgroup of $GL(4, \mathbb{Z}_{4m})$ generated by a, b, c, d, e_i and f.

Set $x_i = e_i d = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \alpha_i \end{pmatrix}$ and $y = fd = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$. Then the order of x_i is $\phi(p_i^{r_i})$ and order of y is 2. Consider a group

$$H = \langle x_1, x_2, \ldots, x_k, y |\; x_i^{\phi(p_i^{r_i})}, y^2, yx_i = x_i y, x_i x_j = x_j x_i, 1 \leq i, j \leq k \rangle.$$

Then H is a subgroup of G. Since $\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv \beta^j \bmod 4m$. Thus the canonical form of H is given by

$$\langle y^j x_1^{j_1} \ldots x_k^{j_k} |\; j = 0, 1, \; 0 \leq j_i < \phi(p_i^{r_i}) \rangle$$

and the order of H is $2\phi(m)$. We can see that an arbitrary element of H is of the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix}$$

with determinant γ, where

$$\gamma = (\prod_{i=1}^{k} \alpha_i^{j_i}) \beta^j.$$

We also have that a, b, c generate $SL(4, \mathbb{Z}_{4m})$ (by Lemma 4.3). Observe that $H \cap SL(4, \mathbb{Z}_{4m}) = \{I_4\}$. Now we have

$$o(HSL(4, \mathbb{Z}_{4m})) = 2 \prod_{i=1}^{k} \phi(p_i^{r_i}) o(SL(4, \mathbb{Z}_{4m})).$$

Since $HSL(4, \mathbb{Z}_{4m}) \subseteq G \leq GL(4, \mathbb{Z}_{4m})$ and by using Lemma 3.1

$$o(GL(4, \mathbb{Z}_{4m})) = 2\phi(m) o(SL(4, \mathbb{Z}_{4m})).$$

Therefore $HSL(4, \mathbb{Z}_{4m}) = GL(4, \mathbb{Z}_{4m})$. Hence result follows. □

Proposition 4.3. *Consider the group $\mathcal{U}(\mathbb{Z}_{2^n})$. For $n > 2$ the order of 3 is 2^{n-2}.*

Proof. For $n = 3$, we can directly see that $o(3) = 2$. To prove the result, we shall show that $3^{2^{n-3}} \equiv 1 + 2^{n-1} (mod\ 2^n)$. Observe that $3^2 \equiv 1 + 2^3 (mod\ 2^4)$. Suppose result holds for any positive integer less than n. $3^{2^{n-4}} \equiv 1 + 2^{n-2} (mod\ 2^{n-1})$. Hence there exist an integer r so that

$$\begin{aligned} 3^{2^{n-4}} &= 1 + 2^{n-2} + r2^{n-1} \\ 3^{2^{n-3}} &= (1 + 2^{n-2} + r2^{n-1})^2 \\ 3^{2^{n-3}} &\equiv 1 + 2^{n-1} (mod\ 2^n) \not\equiv 1 (mod\ 2^n) \end{aligned}$$

Hence we get $o(3) \geq 2^{n-2}$ and result follows, since $\mathcal{U}(\mathbb{Z}_{2^n})$ is not cyclic. □

Theorem 4.4. *Let $n > 2$ and $\alpha_i, \beta \in \mathcal{U}(\mathbb{Z}_{2^n m})$, such that $o(\beta) = 2^{n-2}$ and α_i is a primitive element modulo $p_i^{r_i}$ in $\mathbb{Z}_{2^n m}$ for each i with $(\prod_{i=1}^{k} \alpha_i^{j_i})\beta^j \not\equiv \pm 1$ mod $2^n m$, $0 \leq j_i < \phi(p_i^{r_i})$ and $0 \leq j < 2^{n-2}$, where $j_i, j_2 \ldots j_k, j$ are not simultaneously zero. Then the linear group $GL(4, \mathbb{Z}_{2^n m})$ is generated by Lie regular units a, b, c, d, e_i, f and g, where $1 \leq i \leq k$,*

$$a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; c = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$d = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \; e_i = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \alpha_i & 0 & 0 & 0 \end{pmatrix}, \; f = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \beta & 0 & 0 & 0 \end{pmatrix},$$

$$g = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Proof. By using Lemma 2.3 and Proposition 4.3, we have elements $\beta, \alpha_i \in \mathcal{U}(\mathbb{Z}_{2^n m})$ such that $o(\beta) = 2^{n-2}$ and $o(\alpha_i) = \phi(p_i^{r_i})$ with $(\prod_{i=1}^{k} \alpha_i^{j_i})\alpha^j \not\equiv \pm 1 \bmod 2^n m$. Let G be a subgroup of $GL(4, \mathbb{Z}_{2^n m})$ generated by a, b, c, d, e_i, f and g.

Set $x_i = e_i d = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \alpha_i \end{pmatrix}$, $y = fd = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ and $z = gd = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$. Then the order of x_i is $\phi(p_i^{r_i})$, order of y is 2^{n-2} and order of z is 2. Consider the group

$$H = \langle x_1, x_2, \ldots, x_k, y, z |\ x_i^{\phi(p_i^{r_i})}, y^{2^{n-2}}, z^2, yx_i = x_i y, x_i x_j = x_j x_i, zy = yz, zx_i = x_i z, 1 \le i, j \le k \rangle.$$

Then H is a subgroup of G. Since $(\prod_{i=1}^{k} \alpha_i^{j_i})\beta \not\equiv \pm 1 \bmod 2^n m$. Thus the canonical form of H is given by

$$\langle x_1^{j_1} \ldots x_k^{j_k}, y^j, z^l \mid 0 \le j_i < \phi(p_i^{r_i}), 0 \le j < 2^{n-2}, l = 0, 1 \rangle$$

and the order of H is $2^{n-1}\phi(m)$. We can see that an arbitrary element of H is of the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix}$$

with determinant γ, where

$$\gamma = \pm(\prod_{i=1}^{k} \alpha_i^{j_i})\beta^j.$$

We also have that a, b, c generate $SL(4, \mathbb{Z}_{2^n m})$ (by Lemma 4.3). Observe that $H \cap SL(4, \mathbb{Z}_{2^n m}) = \{I_4\}$. Now we have

$$o(HSL(4, \mathbb{Z}_{2^n m})) = 2 \prod_{i=1}^{k} \phi(p_i^{r_i}) o(SL(4, \mathbb{Z}_{2^n m})).$$

Since $HSL(4, \mathbb{Z}_{2^n m}) \subseteq G \le GL(4, \mathbb{Z}_{2^n m})$ and by using Lemma 3.1

$$o(GL(4, \mathbb{Z}_{2^n m})) = 2\phi(m) o(SL(4, \mathbb{Z}_{2^n m})).$$

Therefore $HSL(4, \mathbb{Z}_{2^n m}) = GL(4, \mathbb{Z}_{2^n m})$. Hence result follows. □

References

[1] H. S. M. Coxeter and W. O. J. Moser. *Generators and Relations for Discrete Groups*. Springer-Verlag Berlin Heidelberg, New York, 1972.

[2] P. Kanwar, R. K. Sharma, and P. Yadav. Lie regular generators of general linear groups. *Int. Electron. J. Algebra*, 13(91-108), 2013.

[3] R. K. Sharma, P. Yadav, and P. Kanwar. Lie regular generators of general linear groups. *Comm. Algebra*, 40(4)(1304-1315), 2012.

[4] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Princeton university press, New Jersey, 1971.

[5] S. M. Trott. A pair of generators for the unimodular group. *Canad. Math. Bull.*, 5(3), 1962.

Department of Mathematics
Indian Institute of Technology Delhi
Delhi - 110016 India
E-mail address: swatimahesh88@gmail.com

Department of Mathematics
Indian Institute of Technology Delhi
Delhi - 110016 India
E-mail address: rksharmaiitd@gmail.com