Serdica
Mathematical Journal
Сердика
Математическо списание

For further information on
Serdica Mathematical Journal
which is the new series of
Serdica Bulgaricae Mathematicae Publicationes
visit the website of the journal http://www.math.bas.bg/~serdica
or contact: Editorial Office
Serdica Mathematical Journal
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: serdica@math.bas.bg

Serdica Math. J. **42** (2016), 211–220

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

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

Swati Maheshwari, R. K. Sharma

Communicated by V. Drensky

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

1. Introduction. The 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 the unimodular group, the general 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, Yadav, and Kanwar introduced Lie regular elements and Lie regular units for non-commutative rings (see [2, 3]). They have given generators of the general linear group $GL(2, \mathbb{Z}_m)$ for some $m > 1$ in terms of Lie regular units. They proposed an open problem to describe the

2010 *Mathematics Subject Classification:* Primary 20H25, 16U60, 20F05.
Key words: linear group, Lie regular elements.

rings that have Lie regular units and whether it is possible to generate the whole unit group of such rings using Lie regular units. In this article we are considering this problem for the ring $\mathcal{M}(4, \mathbb{Z}_m)$. We will discuss the existence of Lie regular units in the ring $\mathcal{M}(4, \mathbb{Z}_m)$ and will show that Lie regular units generate $GL(4, \mathbb{Z}_m)$ for $m > 1$.

Throughout this article, ϕ denotes the Euler 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 $o(g)$ is the order of an element g of G.

The authors are thankful to the referee for the useful comments and suggestions for improving of the exposition.

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

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 $SL(n, \mathbb{Z}) \to SL(n, \mathbb{Z}_m)$ is onto.*

In the sequel we preserve the notation T_{ij} for the image of the transvection.

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])**.** *If $\mathbf{F}$ is 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. *Let $\mathbf{R}$ be a commutative ring with unity and let A, B be Lie regular elements (units) in $\mathcal{M}(2, \mathbf{R})$, i.e., $A = [e, u]$ 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 $\mathcal{M}(4, \mathbf{R})$.*

P r o o f. 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 $\mathcal{M}(4, \mathbf{R})$.*

P r o o f. 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* $GL(4, \mathbf{R})$.

P r o o f. It follows once we observe that

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

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

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

□

Lemma 3.1. *Let* $\alpha_{\in}\mathcal{U}(\mathbb{Z}_m)$, $1 \le i \le k$, *generate the group* $\mathcal{U}(\mathbb{Z}_m)$. *Then any subgroup of* $GL(4, \mathbb{Z}_m)$ *containing* $SL(4, \mathbb{Z}_m)$ *and the matrices*

$$e_i = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \alpha_i & 0 & 0 & 0 \end{pmatrix}, \quad 1 \le i \le k,$$

coincides with the whole $GL(4, \mathbb{Z}_m)$.

P r o o f. Since the elements α_i, $1 \le i \le k$, generate the group $\mathcal{U}(\mathbb{Z}_m)$, every element $\gamma \in \mathcal{U}(\mathbb{Z}_m)$ can be expressed by them. Hence the matrices

$$h_\gamma = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \gamma & 0 & 0 & 0 \end{pmatrix}, \quad \gamma \in \mathcal{U}(\mathbb{Z}_m),$$

belong to the subgroup of $GL(4,\mathbb{Z}_m)$ generated by e_i, $1 \le i \le k$. The matrices h_γ, $\gamma \in \mathcal{U}(\mathbb{Z}_m)$ are coset representatives of $SL(4,\mathbb{Z}_m)$ in $GL(4,\mathbb{Z}_m)$ and every matrix in $GL(4,\mathbb{Z}_m)$ is a product of a matrix h_γ and a matrix from $SL(4,\mathbb{Z}_m)$. In this way any subgroup of $GL(4,\mathbb{Z}_m)$ containing $SL(4,\mathbb{Z}_m)$ and e_i, $1 \le i \le k$, coincides with $GL(4,\mathbb{Z}_m)$. □

4. Generators of general linear groups.

Lemma 4.1. *Any transvection T_{ij} $(1 \le i \ne j \le 4)$ in $\mathcal{M}(4,\mathbb{Z}_m)$ can be written as a product of a, b, c and their inverses, where*

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

P r o o f. 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 4.2. *For $m > 1$, $SL(4, \mathbb{Z}_m)$ is generated by the Lie regular elements a, b, and c, where*

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

Proof. First, observe that $a, b, c \in SL(4, \mathbb{Z}_m)$. By Lemma 4.1 all transvections T_{ij} belong to the subgroup of $SL(4, \mathbb{Z}_m)$ generated by a, b, c. By Corollary 2.1, this implies that a, b, c generate $SL(4, \mathbb{Z}_m)$ 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 the 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 the p_i's are distinct primes and $r_i > 0$.

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*

$$\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv 1 \pmod{2m}, \quad 0 \le j_i < \phi({p_i}^{r_i}),$$

where $j_1, j_2, \ldots, j_k$ are not simultaneously zero. Then the general linear group $GL(4, \mathbb{Z}_{2m})$ is generated by the Lie regular units a, b, c, d and e_i, where $1 \le i \le k$,

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

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

P r o o f. Since p_i is an odd prime, the multiplicative group $\mathcal{U}(\mathbb{Z}_{p_i^{k_i}})$ is cyclic, and by Lemma 2.3, the elements α_i, $1 \le i \le k$, from the statement of the theorem do exist in $\mathcal{U}(\mathbb{Z}_{2m})$ and generate $\mathcal{U}(\mathbb{Z}_{2m})$.

Set $x_i = e_i d = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \alpha_i \end{pmatrix}$. For every element $\gamma \in \mathcal{U}(\mathbb{Z}_{2m})$ the matrix

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

belongs to the subgroup of $GL(4,\mathbb{Z}_{2m})$ generated by x_i, $1 \le i \le k$. By Lemma 4.2 we have that a, b, c generate $SL(4,\mathbb{Z}_{2m})$. Hence, by Lemma 3.1, the matrices a, b, c, d, and e_i, $1 \le i \le k$, generate $GL(4,\mathbb{Z}_{2m})$ and the 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*

$$\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv 1 \pmod{m}, \quad 0 \le j_i < \phi({p_i}^{r_i}),$$

where $j_1, j_2, \ldots, j_k$ are not simultaneously zero. Then the general linear group $GL(4,\mathbb{Z}_m)$ is generated by Lie regular units a, b, c, d and e_i, where $1 \le i \le k$,

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

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

P r o o f. The 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*

$$\prod_{i=1}^{k} \alpha_i^{j_i} \not\equiv \beta^j \pmod{4m}, \quad 0 \le j_i < \phi(p_i^{r_i}) \text{ and } j = 0, 1,$$

where $j, j_1, j_2, \ldots, j_k$ are not simultaneously zero. Then the general linear group $GL(4, \mathbb{Z}_{4m})$ is generated by a, b, c, d, e_i and f, where $1 \le i \le k$,

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

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

P r o o f. Since the multiplicative group $\mathcal{U}(\mathbb{Z}_4)$ is cyclic of order 2, as in the proof of Theorem 4.1, the elements α_i, $1 \le i \le k$, and β from the statement of the theorem do exist in $\mathcal{U}(\mathbb{Z}_{4m})$ and generate it. Also, observe that a, b, c, d, e_i and $f \in GL(4, \mathbb{Z}_{4m})$. 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 $y = fd = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$. As in the proof of Theorem 4.1 again, a, b, c generate $SL(4, \mathbb{Z}_{4m})$ by Lemma 4.2 and the proof is complete by Lemma 3.1. □

It is well known that the group $\mathcal{U}(\mathbb{Z}_{2^n})$, $n > 2$, is a direct product of two cyclic groups $C_{2^{n-2}}$ and C_2 of order 2^{n-2} and 2, respectively. It is also well known that we may choose 5 and -1 for generators of the two cyclic factors of $\mathcal{U}(\mathbb{Z}_{2^n})$.

Theorem 4.4. *Let $n > 2$ and let $\alpha_i, \beta \in \mathcal{U}(\mathbb{Z}_{2^n m})$ be 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. Let*

$$\left(\prod_{i=1}^{k} \alpha_i^{j_i} \right) \beta^j \not\equiv \pm 1 \pmod{2^n m}, \quad 0 \le j_i < \phi(p_i^{r_i}) \text{ and } 0 \le j < 2^{n-2},$$

where $j_i, j_2, \ldots, j_k, j$ are not simultaneously zero. Then the general linear group

$GL(4,\mathbb{Z}_{2^n m})$ is generated by the Lie regular units a,b,c,d,e_i,f, and g, $1 \le i \le k$, where

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

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

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

P r o o f. If $m=\prod_{i=1}^{k} p_i^{r_i}$, then the multiplicative group $\mathcal{U}(\mathbb{Z}_{2^n m})$ has the form

$$\mathcal{U}(\mathbb{Z}_{2^n m}) \cong \mathcal{U}(\mathbb{Z}_{p_1^{r_1}}) \times \cdots \times \mathcal{U}(\mathbb{Z}_{p_k^{r_k}}) \times \mathcal{U}(\mathbb{Z}_{2^n}), \quad \mathcal{U}(\mathbb{Z}_{2^n}) \cong C_{2^{n-2}} \times C_2.$$

This guarantees that the elements α_i,$1 \le i \le k$, and β from the statement of the theorem exist and generate the group $\mathcal{U}(\mathbb{Z}_{2^n m})$.

Set

$$x_i = e_i d = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&\alpha_i\end{pmatrix}, \quad y = fd = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&\beta\end{pmatrix}$$

and $z = gd = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}$. As in Theorem 4.1 the matrices a,b,c generate

$SL(4, \mathbb{Z}_{2^n m})$ by Lemma 4.2. Now the proof is completed by Lemma 3.1 because every diagonal matrix

$$h_\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix}, \quad \gamma \in \mathcal{U}(\mathbb{Z}_{2^n m}),$$

belongs to the subgroup of $GL(4, \mathbb{Z}_{2m})$ generated by x_i, $1 \leq i \leq k$, y, z. □

REFERENCES

[1] H. S. M. Coxeter, W. O. J. Moser. Generators and Relations for Discrete Groups. 3rd edition. New York-Heidelberg, Springer-Verlag, 1972.

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

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

[4] G. Shimura. Introduction to the Arithmetic Theory of Automorphic Functions. Princeton, N.J., Princeton University Press, 1971.

[5] S. M. Trott. A pair of generators for the unimodular group. *Canad. Math. Bull.* **5**, *3* (1962), 245–252.

Department of Mathematics
Indian Institute of Technology Delhi
Delhi – 110016 India
e-mail: swatimahesh88@gmail.com *(Swati Maheshwari)*
e-mail: rksharmaiitd@gmail.com *(R. K. Sharma)*

Received June 10, 2015
Revised February 1, 2017