Divulgaciones Matemáticas Vol. 14 No. 2(2006), pp. 107–120

Órdenes de algunos Grupos Lineales Modulares

Orders of some Modular Linear Groups

Roy Quintero (rquinter@ula.ve)
Departamento de Física y Matemáticas
Núcleo Rafael Rangel - Universidad de Los Andes
Trujillo, Venezuela.

Resumen

En este artículo damos las definiciones y calculamos los órdenes de algunos subgrupos de $\mathbf{GL}(m, \mathbb{Z}_n)$ similares a los subgrupos lineales clásicos del grupo lineal gene- ral sobre un cuerpo cualquiera. Específicamente, el grupo lineal modular especial $\mathbf{SL}(m, \mathbb{Z}_n)$, el grupo modular ortogonal $\mathbf{O}(m, \mathbb{Z}_n)$, el grupo modular ortogonal especial $\mathbf{SO}(m, \mathbb{Z}_n)$ y finalmente el grupo modular simpléctico $\mathbf{Sp}(2m, \mathbb{Z}_n)$. La técnica utilizada consiste en reducir el problema al caso primo y luego emplear la descomposición prima de n, para ello aplicamos algunos resultados básicos sobre isomorfismos de grupos y de aritmética modular.
Palabras y frases clave: matrices sobre anillos especiales, unidades, grupos de unidades, otros grupos de matrices sobre anillos.

Abstract

In this paper we give the definitions and calculate the orders of some subgroups of $\mathbf{GL}(m, \mathbb{Z}_n)$ similar to the classical linear subgroups of the general linear group over any field. Specifically, the special modular linear group $\mathbf{SL}(m, \mathbb{Z}_n)$, the orthogonal modular group $\mathbf{O}(m, \mathbb{Z}_n)$, the special orthogonal modular group $\mathbf{SO}(m, \mathbb{Z}_n)$ and finally the symplectic modular group $\mathbf{Sp}(2m, \mathbb{Z}_n)$. The technique used consists in reducing the problem to the prime case and then employ the prime decomposition of n, for this we apply some basic results about group isomorphisms and from modular arithmetic.
Key words and phrases: matrices over special rings, units, groups of units, other matrix groups over rings.

Recibido 10/03/06. Revisado 15/11/2006. Aceptado 12/12/2006.
MSC (2000): Primary 15A33, 20H25; Secondary 16U60.

1 Introducción

El grupo lineal general de rango $m > 1$ sobre $\mathbb{Z}_n$, el anillo de los enteros modulares con módulo n, lo denotaremos $\mathbf{GL}(m, \mathbb{Z}_n)$. Este grupo lineal modular surge frecuentemente de ciertas aplicaciones de la Teoría de Enteros Modulares, Teoría de Grupos Finitos y Algebra Lineal en el estudio o creación de sistemas criptográficos tanto simétricos como de clave pública. Ejemplos del primer tipo son "*Vigenère cipher*" y "*Hill cipher*", los cuales se estudian en [1]. Hace pocos años, la joven científica irlandesa Sara Flannery [3] creó el sistema de clave pública "*Cayley-Purser algorithm*" o simplemente "*CP*". En el caso particular del sistema *CP* se requirió conocer el orden de $\mathbf{GL}(2, \mathbb{Z}_{pq})$ (p, q primos). Es por ello, que el objetivo de este artículo es conocer los órdenes de ciertos subgrupos modulares que pudieran emplearse en futuros sistemas criptográficos que usen algebra matricial modular. A continuación damos las definiciones de algunos subgrupos de $\mathbf{GL}(m, \mathbb{Z}_n)$, similares a los subgrupos clásicos de $\mathbf{GL}(m, F)$ cuando F es un cuerpo cualquiera, y calculamos sus órdenes.

2 Definición de algunos subgrupos de $\mathbf{GL}(m, \mathbb{Z}_n)$

Iniciamos esta sección recordando que el grupo lineal general $\mathbf{GL}(m, \mathbb{Z}_n)$ está constituido por las matrices $m \times m$ invertibles con entradas en $\mathbb{Z}_n$; es decir:

$$\mathbf{GL}(m, \mathbb{Z}_n) = \{A = [\overline{a_{ij}}] \in \mathbb{Z}_n^{m \times m} : \det(A) \in \mathcal{U}(\mathbb{Z}_n)\}$$

donde $\mathcal{U}(\mathbb{Z}_n) = \{\overline{u} \in \mathbb{Z}_n : \operatorname{mcd}(u, n) = 1\}$ es el grupo de unidades de $\mathbb{Z}_n$ y cuyo orden es $\varphi(n)$; es decir, el valor de la función-φ de Euler en n.

En [2] pueden verse las definiciones de los grupos lineales clásicos siguientes: grupo lineal especial, grupo ortogonal, grupo ortogonal especial y grupo simpléctico, todos de rango general y con entradas en un cuerpo.

Definición 2.1. *Los grupos modulares especial, ortogonal y ortogonal especial de rango m sobre $\mathbb{Z}_n$, denotados $\mathbf{SL}(m, \mathbb{Z}_n)$, $\mathbf{O}(m, \mathbb{Z}_n)$ y $\mathbf{SO}(m, \mathbb{Z}_n)$ y simpléctico de rango $2m$ sobre $\mathbb{Z}_n$, $\mathbf{Sp}(2m, \mathbb{Z}_n)$, son definidos a continuación:*

$$\mathbf{SL}(m, \mathbb{Z}_n) := \{A \in \mathbf{GL}(m, \mathbb{Z}_n) : \det(A) = \overline{1}\},$$

$$\mathbf{O}(m, \mathbb{Z}_n) := \{A \in \mathbf{GL}(m, \mathbb{Z}_n) : A^T \cdot A = I_m\},$$

$$\mathbf{SO}(m, \mathbb{Z}_n) := \{A \in \mathbf{O}(m, \mathbb{Z}_n) : \det(A) = \overline{1}\ \}$$

y

$$\mathbf{Sp}(2m, \mathbb{Z}_n) := \{S \in \mathbf{GL}(2m, \mathbb{Z}_n) : S^T J_n \; S = J_n\},$$

donde $J_n = \left[\begin{array}{c:c} O_m & I_m \\ \hdashline -I_m & O_m \end{array}\right]$ *(O_m y I_m son las matrices nula e identidad de* $\mathbb{Z}_n^{m\times m}$*).*

3 Órdenes de los subgrupos de $\mathbf{GL}(m, \mathbb{Z}_n)$

3.1 Orden de $\mathbf{SL}(m, \mathbb{Z}_n)$

El orden del grupo lineal modular viene dado por la fórmula (ver [6])

$$|\mathbf{GL}(m, \mathbb{Z}_n)| = n^{m^2} \prod_{i=1}^{k} \prod_{j=1}^{m} (1 - p_i^{-j}),$$

siendo $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ la descomposición prima de n.

Teorema 3.1. *El orden del grupo lineal modular especial de rango m sobre $\mathbb{Z}_n$ es (ver [5]):*

$$|\mathbf{SL}(m, \mathbb{Z}_n)| = n^{m^2-1} \prod_{i=1}^{k} \prod_{j=2}^{m} (1 - p_i^{-j}).$$

Demostración: Es bien conocido que la aplicación $\Delta\colon \mathbf{GL}(m, \mathbb{Z}_n) \longrightarrow \mathcal{U}(\mathbb{Z}_n)$ definida por $A \longmapsto \det(A)$ es un epimorfismo de grupos. Además, tenemos que

$$\mathrm{Ker}(\Delta) = \{A \in \mathbf{GL}(m, \mathbb{Z}_n) : \Delta(A) = \overline{1}\ \} = \mathbf{SL}(m, \mathbb{Z}_n).$$

Aplicando el primer teorema de isomorfismo de grupos obtenemos que

$$\begin{aligned} |\mathbf{SL}(m, \mathbb{Z}_n)| &= \frac{|\mathbf{GL}(m, \mathbb{Z}_n)|}{|\mathcal{U}(\mathbb{Z}_n)|} = \frac{n^{m^2} \prod_{i=1}^{k} \prod_{j=1}^{m} (1 - p_i^{-j})}{\varphi(n)} \\ &= \frac{n^{m^2} \prod_{i=1}^{k} \prod_{j=1}^{m} (1 - p_i^{-j})}{n \prod_{i=1}^{k} (1 - p_i^{-1})} = n^{m^2-1} \prod_{i=1}^{k} \prod_{j=2}^{m} (1 - p_i^{-j}). \end{aligned}$$

□

3.2 Orden de $\mathbf{O}(m, \mathbb{Z}_n)$

Para calcular el orden del grupo ortogonal de rango m sobre $\mathbb{Z}_n$ primero demostramos algunos resultados.

Lema 3.1. *Sean $\alpha \geq 2$ un entero, $p \geq 2$ un primo y $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ la descomposición prima de n. Entonces*

1. *La aplicación $Red_\alpha \colon \mathbf{GL}(m, \mathbb{Z}_{p^\alpha}) \longrightarrow \mathbf{GL}(m, \mathbb{Z}_{p^{\alpha-1}})$ definida mediante la asignación $A = [\overline{a_{ij}}] \longmapsto Red_\alpha(A) = [\overline{\overline{a_{ij}}}]$, donde $\overline{a_{ij}}$ y $\overline{\overline{a_{ij}}}$ son las clases de congruencia de a_{ij} módulo p^α y $p^{\alpha-1}$, es un epimorfismo de grupos.*

2. *La aplicación $Prod \colon \mathbf{GL}(m, \mathbb{Z}_n) \longrightarrow \mathbf{GL}(m, \mathbb{Z}_{p_1^{\alpha_1}}) \times \cdots \times \mathbf{GL}(m, \mathbb{Z}_{p_k^{\alpha_k}})$ definida mediante la asignación $A = [\overline{a_{ij}}] \longmapsto Prod(A) = (A_{(1)}, \dots, A_{(k)})$, donde $A_{(h)} = [\overline{a_{ij}}^{(h)}]$ y $\overline{a_{ij}}^{(h)}$ es la clase de congruencia de a_{ij} módulo $p_h^{\alpha_h}$ para $h = 1, \dots, k$, es un isomorfismo de grupos.*

Demostración: 1. Claramente $Red_\alpha(A)$ es independiente de la escogencia de los representantes de las clases que son entradas de A. Por otra parte, como $\operatorname{mcd}(\det([a_{ij}]), p^\alpha) = 1 \Longrightarrow \operatorname{mcd}\left(\det([a_{ij}]), p^{\alpha-1}\right) = 1$, tenemos que la aplicación está bien definida. Más aún, para todo par de matrices A y B en $\mathbf{GL}(m, \mathbb{Z}_{p^\alpha})$ se cumple que $Red_\alpha(A \cdot B) = Red_\alpha(A) \cdot Red_\alpha(B)$ y así resulta que Red_α es un homomorfismo. Claramente es sobreyectivo.

2. Es evidente que cada componente de $Prod(A)$ es independiente de la escogencia de los representantes de las clases que son entradas de A y pertenece al correspondiente grupo factor. Por otra parte, como $\operatorname{mcd}(\det([a_{ij}]), n) = 1 \Longrightarrow \operatorname{mcd}(\det([a_{ij}]), p_h^{\alpha_h}) = 1$ para $h = 1, \dots, k$ tenemos que la aplicación está bien definida. Más aún, para todo par de matrices A y B en $\mathbf{GL}(m, \mathbb{Z}_n)$ se cumple que $Prod(A \cdot B) = Prod(A) \cdot Prod(B)$ y así resulta que $Prod$ es un homomorfismo.

Ahora probaremos que $Prod$ es una aplicación sobreyectiva. En efecto, dada una k-upla cualquiera $(B_1, \dots, B_k)$ en el grupo $\mathbf{GL}(m, \mathbb{Z}_{p_1^{\alpha_1}}) \times \cdots \times \mathbf{GL}(m, \mathbb{Z}_{p_k^{\alpha_k}})$, debemos encontrar $X = [\overline{x_{ij}}] \in \mathbf{GL}(m, \mathbb{Z}_n)$ tal que $X_{(h)} = B_h$ para cada h. Supongamos que $B_h = \left[\overline{b_{ij,h}}^{(h)}\right]$, entonces $\overline{x_{ij}} = \overline{b_{ij,h}}^{(h)}$ para $h = 1, \dots, k$ y $i, j = 1, \dots, n$. Por tanto, para cada par (i, j) debemos encontrar un entero x_{ij} que satisfaga el siguiente sistema de ecuaciones modulares

$$\begin{cases} x_{ij} & \equiv & b_{ij,1} \ (\text{mód } p_1^{\alpha_1}) \\ & \vdots & \\ x_{ij} & \equiv & b_{ij,k} \ (\text{mód } p_k^{\alpha_k}), \end{cases}$$

pero el teorema del resto chino garantiza su existencia. Así que $Prod$ es sobre.

Para concluir tenemos que demostrar que $Prod$ es inyectiva. En efecto,

$$\begin{aligned} A = [\overline{a_{ij}}] \in \mathrm{Ker}(Prod) &\iff A_{(h)} = I_{m(h)}, \quad h = 1, \ldots, k \\ &\iff \overline{a_{ij}}^{(h)} = \begin{cases} \overline{0}^{(h)} & \text{if } i \neq j \\ \overline{1}^{(h)} & \text{if } i = j \end{cases}, \quad h = 1, \ldots, k \\ &\iff \overline{a_{ij}} \in \begin{cases} \overline{0} & \text{if } i \neq j \\ \overline{1} & \text{if } i = j. \end{cases} \\ &\iff A = I_m. \end{aligned}$$

Por tanto, $Prod$ es un isomorfismo. □

Lema 3.2. *Sean $\alpha \geq 2$ entero y $p > 2$ primo. Entonces*

1.

$$|\mathbf{O}(m, \mathbb{Z}_{p^\alpha})| = p^{\frac{m^2-m}{2}} \cdot |\mathbf{O}(m, \mathbb{Z}_{p^{\alpha-1}})|. \tag{1}$$

2.

$$|\mathbf{O}(m, \mathbb{Z}_{2^\alpha})| = 2^{\frac{m^2+m}{2}} \cdot |\mathbf{O}(m, \mathbb{Z}_{2^{\alpha-1}})|. \tag{2}$$

Demostración: 1. Sea f la aplicación restricción de Red_α a $\mathbf{O}(m, \mathbb{Z}_{p^\alpha})$; es decir, $f = Red_\alpha \mid_{\mathbf{O}(m,\mathbb{Z}_{p^\alpha})}$. Observemos que, para toda matriz $A \in \mathbf{O}(m, \mathbb{Z}_{p^\alpha})$ se cumple $(Red_\alpha(A))^T \cdot Red_\alpha(A) = Red_\alpha(A^T \cdot A) = Red_\alpha(I_m) = I'_m$, ($I'_m$ es la identidad en $\mathbb{Z}_{p^{\alpha-1}}^{m\times m}$) así que f es un epimorfismo de $\mathbf{O}(m, \mathbb{Z}_{p^\alpha})$ en $\mathbf{O}(m, \mathbb{Z}_{p^\alpha - 1})$.

Ahora procedemos a encontrar su kernel. En efecto, sean $C \subset \mathbb{Z}$ y $U, V \subset \mathbb{Z}_{p^\alpha}$ los conjuntos siguientes $C = \{k \in \mathbb{Z} : 0 \leq k \leq p-1\}$, $U = \{\overline{kp^{\alpha-1}} : k \in C\}$ y $V = \{\overline{kp^{\alpha-1}+1} : k \in C\}$ entonces, $\overline{\overline{u}} = \overline{\overline{0}} \iff \overline{u} \in U$ y $\overline{\overline{v}} = \overline{\overline{1}} \iff \overline{v} \in V$. Luego,

$$\begin{aligned} A = [\overline{a_{ij}}] \in \mathrm{Ker}(f) &\iff \overline{\overline{a_{ij}}} = \begin{cases} \overline{\overline{0}} & \text{if } i \neq j \\ \overline{\overline{1}} & \text{if } i = j \end{cases} \text{ y } A^T \cdot A = I_m \\ &\iff \overline{a_{ij}} \in \begin{cases} U & \text{if } i \neq j \\ V & \text{if } i = j. \end{cases} \text{ y } A^T \cdot A = I_m \\ &\iff A = \overline{p^{\alpha-1}}\ [\overline{t_{ij}}] + I_m \ \text{ donde } t_{ij} \in C \\ &\qquad \text{y } A^T \cdot A = I_m. \end{aligned}$$

Así que,

$$\mathrm{Ker}(f) = \left\{ A = \overline{p^{\alpha-1}}\ [\overline{t_{ij}}] + I_m : (t_{11}, \ldots, t_{mm}) \in C^{m^2} \text{ y } A^T \cdot A = I_m \right\}. \tag{3}$$

Determinemos con precisión todos los elementos del kernel. En efecto,

$$\begin{aligned}
& (\overline{p^{\alpha-1}}\ \overline{[t_{ij}]} + I_m)^T(\overline{p^{\alpha-1}}\ \overline{[t_{ij}]} + I_m) = I_m \\
\iff\ & (\overline{p^{\alpha-1}}\ \overline{[t_{ij}]}^T + I_m)(\overline{p^{\alpha-1}}\ \overline{[t_{ij}]} + I_m) = I_m \\
\iff\ & \overline{p^{\alpha-1}}\big(\overline{[t_{ij}+t_{ji}]}\big) + I_m = I_m \\
\iff\ & p \mid t_{ii}, t_{ij}+t_{ji} \text{ (si } i \neq j) \\
\iff\ & t_{ii} = 0 \text{ y } t_{ij}+t_{ji} = 0 \text{ ó } p \text{ (si } i \neq j).
\end{aligned}$$

Por tanto,

$$\mathrm{Ker}(f) =$$

$$\big\{\overline{p^{\alpha-1}}\ \overline{[t_{ij}]} + I_m : t_{ii} = 0 \text{ y } (t_{ij}, t_{ji}) \in \{(0,0),(1,p-1),\ldots,(p-1,1)\} \text{ si } i < j\big\},$$

y su orden es $p^{\frac{m^2-m}{2}}$, luego la ecuación (1) se cumple.

2. Observemos que todo lo hecho en la parte 1 hasta la ecuación (3), es válido si reemplazamos p por 2; es decir,

$$\mathrm{Ker}(f) = \left\{A = \overline{2^{\alpha-1}}\overline{[t_{ij}]} + I_m : (t_{11},\ldots,t_{mm}) \in C^{m^2} \text{ y } A^T \cdot A = I_m\right\},$$

pero,

$$\begin{aligned}
& (\overline{2^{\alpha-1}}\ \overline{[t_{ij}]} + I_m)^T(\overline{2^{\alpha-1}}\ \overline{[t_{ij}]} + I_m) = I_m \\
\iff\ & (\overline{2^{\alpha-1}}\ \overline{[t_{ij}]}^T + I_m)(\overline{2^{\alpha-1}}\ \overline{[t_{ij}]} + I_m) = I_m \\
\iff\ & \overline{2^{\alpha-1}}\big(\overline{[t_{ij}+t_{ji}]}\big) + I_m = I_m \\
\iff\ & 2 \mid t_{ij}+t_{ji} \text{ (si } i \neq j) \\
\iff\ & t_{ij}+t_{ji} = 0 \text{ ó } 2 \text{ (si } i \neq j).
\end{aligned}$$

Por tanto,

$$\mathrm{Ker}(f) = \left\{\overline{2^{\alpha-1}}\overline{[t_{ij}]} + I_m : t_{ii} \in C \text{ y } (t_{ij}, t_{ji}) \in \{(0,0),(1,1)\} \text{ si } i < j\right\},$$

y su orden es $2^{\frac{m^2+m}{2}}$, luego la ecuación (2) también se cumple. □

Corolario 3.1. *Sean $\alpha \geq 2$ un entero y $p > 2$ primo. Entonces*

1.

$$|\mathbf{O}(m, \mathbb{Z}_{p^\alpha})| = p^{\left(\frac{m^2-m}{2}\right)(\alpha-1)} \cdot |\mathbf{O}(m, \mathbb{Z}_p)|.$$

2.

$$|\mathbf{O}(m,\mathbb{Z}_{2^\alpha})| = 2^{\left(\frac{m^2+m}{2}\right)(\alpha-1)} \cdot |\mathbf{O}(m,\mathbb{Z}_2)|.$$

En [4, pags. 158 y 163] se encuentra el siguiente lema.

Lema 3.3. *Si $p > 2$ es primo y $r \geq 1$ es entero, entonces:*

1. $|\mathbf{O}(2r+1,\mathbb{Z}_2)| = 2^{r^2}\prod_{t=1}^{r}(2^{2t}-1)$.

2. $|\mathbf{O}(2r+1,\mathbb{Z}_p)| = 2p^{r^2}\prod_{t=1}^{r}(p^{2t}-1)$.

3. $|\mathbf{O}(2r,\mathbb{Z}_2)| = \begin{cases} 2 & si\ r=1 \\ 2^{r^2}\prod_{t=1}^{r-1}(2^{2t}-1) & si\ r\geq 2 \end{cases}$

4. $|\mathbf{O}(2r,\mathbb{Z}_p)| = \begin{cases} 2(p-1) & si\ r=1\ y\ p\equiv 1 \pmod 4 \\ 2(p+1) & si\ r=1\ y\ p\equiv 3 \pmod 4 \\ 2p^{r^2-r}(p^r-1)\prod_{t=1}^{r-1}(p^{2t}-1) & si\ r\geq 2\ y\ p\equiv 1 \pmod 4 \\ 2p^{r^2-r}(p^r-(-1)^r)\prod_{t=1}^{r-1}(p^{2t}-1) & \\ & si\ r\geq 2\ y\ p\equiv 3 \pmod 4 \end{cases}$

Definición 3.1. *Diremos que un primo p es del tipo 1, si $p \equiv 1 \pmod 4$, y del tipo 2, si $p \equiv 3 \pmod 4$.*

Teorema 3.2. *. Sea $n = 2^\alpha p_1^{\alpha_1}\dots p_k^{\alpha_k} q_1^{\beta_1}\dots q_l^{\beta_l}$ donde $\alpha \geq 1$, $p_1,\dots,p_k$ son primos distintos dos a dos del tipo 1 y $\alpha_1,\dots,\alpha_k$ son enteros positivos, y $q_1,\dots,q_l$ son primos distintos dos a dos del tipo 2 y $\beta_1,\dots,\beta_l$ son enteros positivos. Entonces,*

1. *Los grupos $\mathbf{O}(m,\mathbb{Z}_n)$ y $\mathbf{O}(m,\mathbb{Z}_{2^\alpha})\times\prod_{i=1}^{k}\mathbf{O}(m,\mathbb{Z}_{p_i^{\alpha_i}})\times\prod_{j=1}^{l}\mathbf{O}(m,\mathbb{Z}_{q_j^{\beta_j}})$ son isomorfos; es decir,*

$$\mathbf{O}(m,\mathbb{Z}_n) \cong \mathbf{O}(m,\mathbb{Z}_{2^\alpha}) \times \prod_{i=1}^{k}\mathbf{O}(m,\mathbb{Z}_{p_i^{\alpha_i}}) \times \prod_{j=1}^{l}\mathbf{O}(m,\mathbb{Z}_{q_j^{\beta_j}}). \quad (4)$$

2. El orden del grupo $\mathbf{O}(m,\mathbb{Z}_n)$ *se expresa mediante la siguiente fórmula:*

$$|\mathbf{O}(m,\mathbb{Z}_n)| = \begin{cases} C(2)\prod_{i=1}^{k}(1-p_i^{-1})\prod_{j=1}^{l}(1+q_j^{-1}) \\ C(m)\prod_{t=1}^{\frac{m-1}{2}}\left[\prod_{i=1}^{k}(1-p_i^{-2t})\prod_{j=1}^{l}(1-q_j^{-2t})\right] \\ C(m)\prod_{t=1}^{\frac{m}{2}-1}\left[(1-2^{-2t})\prod_{i=1}^{k}(1-p_i^{-\frac{m}{2}})(1-p_i^{-2t})\times \right. \\ \left. \prod_{j=1}^{l}(1-(-q_j)^{-\frac{m}{2}})(1-q_j^{-2t})\right] \end{cases} \tag{5}$$

si $m=2$, $m\geq 3$ *es impar y* $m\geq 4$ *es par, respectivamente, siendo* $C(s)=n^{\frac{s^2-s}{2}}2^{s(\alpha-1)+k+l}$.

Demostración: 1. Por el Lema 3.1, *Prod* es un isomorfismo de grupos. Además

$$\begin{aligned} A \in & \mathbf{O}(m,\mathbb{Z}_n) \Longleftrightarrow A\in \mathbf{GL}(m,\mathbb{Z}_n) \text{ y } A^T\cdot A = I_m \\ & \Longleftrightarrow (A_{(h)})_{h=0}^{k+l} \in \mathbf{GL}(m,\mathbb{Z}_{2^\alpha})\times\prod_{i=1}^{k}\mathbf{GL}(m,\mathbb{Z}_{p_i^{\alpha_i}})\times\prod_{j=1}^{l}\mathbf{GL}(m,\mathbb{Z}_{q_j^{\beta_j}}) \\ & \qquad \text{y } A_{(h)}^T\cdot A_{(h)} = I_{m(h)}, \quad h=0,1,\ldots,k+l \\ & \Longleftrightarrow Prod(A)\in \mathbf{O}(m,\mathbb{Z}_{2^\alpha})\times\prod_{i=1}^{k}\mathbf{O}(m,\mathbb{Z}_{p_i^{\alpha_i}})\times\prod_{j=1}^{l}\mathbf{O}(m,\mathbb{Z}_{q_j^{\beta_j}}), \end{aligned}$$

lo cual demuestra que la función *Prod* restringida al grupo $\mathbf{O}(m,\mathbb{Z}_n)$ (i.e., $Prod|_{\mathbf{O}(m,\mathbb{Z}_n)}$), es el isomorfismo buscado; es decir, la ecuación (4) se cumple.

2. Probaremos sólo la tercera ecuación; es decir, cuando $m\geq 4$ es par. Los otros dos casos se prueban similarmente.

En efecto, asumamos que $m\geq 4$ es par. Combinando la ecuación (4) con

el Corolario 3.1 y el Lema 3.3 tenemos que

$$\begin{aligned}
|\mathbf{O}(m,\mathbb{Z}_n)| &= |\mathbf{O}(m,\mathbb{Z}_{2^\alpha})| \prod_{i=1}^{k} |\mathbf{O}(m,\mathbb{Z}_{p_i^{\alpha_i}})| \prod_{j=1}^{l} |\mathbf{O}(m,\mathbb{Z}_{q_j^{\beta_j}})| \\
&= 2^{\left(\frac{m^2+m}{2}\right)(\alpha-1)} 2^{(\frac{m}{2})^2} \prod_{t=1}^{\frac{m}{2}-1} (2^{2t}-1) \times \\
&\quad \prod_{i=1}^{k} \left[p_i^{\left(\frac{m^2-m}{2}\right)(\alpha_i-1)} 2 p_i^{(\frac{m}{2})^2-\frac{m}{2}} (p_i^{\frac{m}{2}}-1) \prod_{t=1}^{\frac{m}{2}-1} (p_i^{2t}-1) \right] \times \\
&\quad \prod_{j=1}^{l} \left[q_j^{\left(\frac{m^2-m}{2}\right)(\beta_j-1)} 2 q_j^{(\frac{m}{2})^2-\frac{m}{2}} (q_j^{\frac{m}{2}}-(-1)^{\frac{m}{2}}) \prod_{t=1}^{\frac{m}{2}-1} (q_j^{2t}-1) \right] \\
&= (2^\alpha)^{\frac{m^2-m}{2}} 2^{m(\alpha-1)} \prod_{t=1}^{\frac{m}{2}-1} (1-2^{-2t}) \times \\
&\quad 2^k \left(\prod_{i=1}^{k} p_i^{\alpha_i} \right)^{\frac{m^2-m}{2}} \prod_{i=1}^{k} (1-p_i^{-\frac{m}{2}}) \prod_{t=1}^{\frac{m}{2}-1} (1-p_i^{-2t}) \times \\
&\quad 2^l \left(\prod_{j=1}^{l} q_j^{\beta_j} \right)^{\frac{m^2-m}{2}} \prod_{j=1}^{l} (1-(-q_j)^{-\frac{m}{2}}) \prod_{t=1}^{\frac{m}{2}-1} (1-q_j^{-2t}) \\
&= C(m) \prod_{t=1}^{\frac{m}{2}-1} \Big[(1-2^{-2t}) \prod_{i=1}^{k} (1-p_i^{-\frac{m}{2}})(1-p_i^{-2t}) \times \\
&\quad \prod_{j=1}^{l} (1-(-q_j)^{-\frac{m}{2}})(1-q_j^{-2t}) \Big].
\end{aligned}$$

□

3.3 Orden de $\mathbf{SO}(m,\mathbb{Z}_n)$

Para calcular el orden del grupo modular ortogonal especial de rango m sobre $\mathbb{Z}_n$ consideramos el homomorfismo de grupos determinante, Δ (Teorema 3.1), restringido al grupo modular ortogonal correspondiente; es decir, $\Delta|_{\mathbf{O}(m,\mathbb{Z}_n)}$.

Teorema 3.3. *El orden del grupo lineal especial de rango m sobre $\mathbb{Z}_n$ es:*

$$|\mathbf{SO}(m,\mathbb{Z}_n)| = \frac{|\mathbf{O}(m,\mathbb{Z}_n)|}{2}. \tag{6}$$

Demostración: Dado el homomorfismo $\Delta|_{\mathbf{O}(m,\mathbb{Z}_n)}$, observemos que su rango o imagen es el grupo multiplicativo $\{\pm\overline{1}\}$ y su kernel es exactamente $\mathbf{SO}(m,\mathbb{Z}_n)$. Entonces, por el primer teorema de isomorfismo de grupos tenemos que:

$$|\mathbf{O}(m,\mathbb{Z}_n)| \quad = \quad |\operatorname{Ker}(\Delta|_{\mathbf{O}(m,\mathbb{Z}_n)})||\operatorname{Im}(\Delta|_{\mathbf{O}(m,\mathbb{Z}_n)})| = 2|\mathbf{SO}(m,\mathbb{Z}_n)|,$$

luego, la ecuación (6) se cumple. □

Corolario 3.2. *Sea $n = 2^{\alpha}p_1^{\alpha_1}\dots p_k^{\alpha_k}q_1^{\beta_1}\dots q_l^{\beta_l}$ donde $\alpha \geq 1$, $p_1,\dots,p_k$ son primos distintos dos a dos del tipo 1 y $\alpha_1,\dots,\alpha_k$ son enteros positivos, y $q_1,\dots,q_l$ son primos distintos dos a dos del tipo 2 y $\beta_1,\dots,\beta_l$ son enteros positivos. Entonces,*

1. *Los grupos*

$$\mathbf{SO}(m,\mathbb{Z}_n) \text{ y } \mathbf{SO}(m,\mathbb{Z}_{2^{\alpha}}) \times \prod_{i=1}^{k}\mathbf{SO}(m,\mathbb{Z}_{p_i^{\alpha_i}}) \times \prod_{j=1}^{l}\mathbf{SO}(m,\mathbb{Z}_{q_j^{\beta_j}})$$

son isomorfos, es decir,

$$\mathbf{SO}(m,\mathbb{Z}_n) \cong \mathbf{SO}(m,\mathbb{Z}_{2^{\alpha}}) \times \prod_{i=1}^{k}\mathbf{SO}(m,\mathbb{Z}_{p_i^{\alpha_i}}) \times \prod_{j=1}^{l}\mathbf{SO}(m,\mathbb{Z}_{q_j^{\beta_j}}). \quad (7)$$

2. *El orden del grupo $\mathbf{SO}(m,\mathbb{Z}_n)$ se expresa mediante la siguiente fórmula:*

$$|\mathbf{SO}(m,\mathbb{Z}_n)| = \begin{cases} \frac{1}{2}C(2)\prod_{i=1}^{k}(1-p_i^{-1})\prod_{j=1}^{l}(1+q_j^{-1}) \\ \frac{1}{2}C(m)\prod_{t=1}^{\frac{m-1}{2}}\left[\prod_{i=1}^{k}(1-p_i^{-2t})\prod_{j=1}^{l}(1-q_j^{-2t})\right] \\ \frac{1}{2}C(m)\prod_{t=1}^{\frac{m}{2}-1}\Big[(1-2^{-2t})\prod_{i=1}^{k}(1-p_i^{-\frac{m}{2}})(1-p_i^{-2t}) \\ \times\prod_{j=1}^{l}(1-(-q_j)^{-\frac{m}{2}})(1-q_j^{-2t})\Big] \end{cases} \quad (8)$$

si $m = 2$, $m \geq 3$ es impar y $m \geq 4$ es par, respectivamente.

Demostración: 1. Sea *Prod* como en el Lema 3.1. Además

$$\begin{aligned} A \in & \mathbf{SO}(m,\mathbb{Z}_n) \iff A \in \mathbf{O}(m,\mathbb{Z}_n) \text{ y } \det(A) = \overline{1} \\ & \iff (A_{(h)})_{h=0}^{k+l} \in \mathbf{O}(m,\mathbb{Z}_{2^\alpha}) \times \prod_{i=1}^{k} \mathbf{O}(m,\mathbb{Z}_{p_i^{\alpha_i}}) \times \prod_{j=1}^{l} \mathbf{O}(m,\mathbb{Z}_{q_j^{\beta_j}}) \\ & \qquad \text{y } \det(A_{(h)}) = \overline{1}^{(h)}, \quad h = 0,1,\ldots,k+l \\ & \iff Prod(A) \in \mathbf{SO}(m,\mathbb{Z}_{2^\alpha}) \times \prod_{i=1}^{k} \mathbf{SO}(m,\mathbb{Z}_{p_i^{\alpha_i}}) \times \prod_{j=1}^{l} \mathbf{SO}(m,\mathbb{Z}_{q_j^{\beta_j}}), \end{aligned}$$

lo cual demuestra que la función *Prod* restringida al grupo $\mathbf{SO}(m,\mathbb{Z}_n)$ (i.e., $Prod|_{\mathbf{SO}(m,\mathbb{Z}_n)}$) es el isomorfismo buscado, es decir, la ecuación (7) se cumple.

2. La ecuación (8) se sigue de las ecuaciones (5) y (7). □

3.4 Orden de $\mathbf{Sp}(2m,\mathbb{Z}_n)$

Para calcular el orden del grupo modular simpléctico de rango $2m$ sobre $\mathbb{Z}_n$ necesitamos algunos resultados previos.

Lema 3.4. *Sean $p \geq 2$ primo y $\alpha \geq 2$ entero. Entonces*

1.
$$|\mathbf{Sp}(2m,\mathbb{Z}_{p^\alpha})| = p^{2m^2+m}|\mathbf{Sp}(2m,\mathbb{Z}_{p^{\alpha-1}})|. \tag{9}$$

2.
$$|\mathbf{Sp}(2m,\mathbb{Z}_{p^\alpha})| = p^{(2m^2+m)(\alpha-1)}|\mathbf{Sp}(2m,\mathbb{Z}_p)|. \tag{10}$$

Demostración: 1. Sea g la aplicación restricción de Red_α a $\mathbf{Sp}(2m,\mathbb{Z}_{p^\alpha})$; es decir, $g = Red_\alpha\ |_{\mathbf{Sp}(2m,\mathbb{Z}_{p^\alpha})}$. Observemos que, para toda matriz $A \in \mathbf{O}(m,\mathbb{Z}_{p^\alpha})$ se cumple $Red_\alpha(S)^T J_{p^{\alpha-1}} Red_\alpha(S) = Red_\alpha(S^T J_{p^\alpha} S) = Red_\alpha(J_{p^\alpha}) = J_{p^{\alpha-1}}$, luego g es un epimorfismo de $\mathbf{Sp}(2m,\mathbb{Z}_{p^\alpha})$ en $\mathbf{Sp}(2m,\mathbb{Z}_{p^{\alpha-1}})$.

Ahora procedemos a encontrar su kernel. En efecto, sean $C \subset \mathbb{Z}$ y $U, V \subset \mathbb{Z}_{p^\alpha}$ los conjuntos siguientes $C = \{k \in \mathbb{Z} : 0 \leq k \leq p-1\}$, $U = \{\overline{kp^{\alpha-1}} : k \in C\}$ y $V = \{\overline{kp^{\alpha-1}+1} : k \in C\}$ entonces, $\overline{\overline{u}} = \overline{\overline{0}} \iff \overline{u} \in U$ y $\overline{\overline{v}} = \overline{\overline{1}} \iff \overline{v} \in V$. Luego,

$$S = [\overline{s_{ij}}] \in \mathrm{Ker}(g) \iff \overline{\overline{s_{ij}}} = \begin{cases} \overline{\overline{1}} \text{ si } i = j \\ \overline{\overline{0}} \text{ si } i \neq j \end{cases} \quad \text{y} \quad S^T J_{p^\alpha} S = J_{p^\alpha}$$

$$\iff S = \overline{p^{\alpha-1}}\ [\overline{t_{ij}}] + I_{2m} \text{ donde } t_{ij} \in C \text{ y } S^T J_{p^\alpha} S = J_{p^\alpha}.$$

Por tanto,

$$\mathrm{Ker}(g) = \left\{ S = \overline{p^{\alpha-1}}\,[\overline{t_{ij}}] + I_{2m} : (t_{11}, \ldots, t_{2m,2m}) \in C^{4m^2} \text{ y } S^T J_{p^\alpha} S = J_{p^\alpha} \right\}.$$

Ahora determinaremos con precisión todos los elementos del kernel, pero primero observemos que cualquier elemento de $\mathrm{Ker}(g)$ se puede expresar como sigue:

$$\overline{p^{\alpha-1}}\,[\overline{t_{ij}}] + I_{2m} \quad = \quad \left[\begin{array}{c|c} \overline{p^{\alpha-1}}A + I_m & \overline{p^{\alpha-1}}B \\ \hline \overline{p^{\alpha-1}}C & \overline{p^{\alpha-1}}D + I_m \end{array}\right],$$

donde $A = [\overline{a_{ij}}]$, $B = [\overline{b_{ij}}]$, $C = [\overline{c_{ij}}]$ y $D = [\overline{d_{ij}}] \in \mathbb{Z}_{p^\alpha}^{m\times m}$ y

$$\left\{\begin{array}{l} \overline{a_{ij}} = \overline{t_{ij}} \\ \overline{b_{ij}} = \overline{t_{i(m+j)}} \\ \overline{c_{ij}} = \overline{t_{(m+i)j}} \\ \overline{d_{ij}} = \overline{t_{(m+i)(m+j)}} \end{array}\right. \quad i = 1, \ldots, m; \quad j = 1, \ldots, m.$$

Luego,

$$\left[\begin{array}{c|c} \overline{p^{\alpha-1}}A + I_m & \overline{p^{\alpha-1}}B \\ \hline \overline{p^{\alpha-1}}C & \overline{p^{\alpha-1}}D + I_m \end{array}\right]^T J_{p^\alpha} \left[\begin{array}{c|c} \overline{p^{\alpha-1}}A + I_m & \overline{p^{\alpha-1}}B \\ \hline \overline{p^{\alpha-1}}C & \overline{p^{\alpha-1}}D + I_m \end{array}\right] = J_{p^\alpha}$$

$$\iff \quad \left[\begin{array}{c|c} \overline{p^{\alpha-1}}(C - C^T) & \overline{p^{\alpha-1}}(A^T + D) + I_m \\ \hline -\overline{p^{\alpha-1}}(A + D^T) - I_m & \overline{p^{\alpha-1}}(B^T - B) \end{array}\right] = \left[\begin{array}{c|c} O_m & I_m \\ \hline -I_m & O_m \end{array}\right]$$

$$\iff \quad \left\{\begin{array}{l} \overline{p^{\alpha-1}}(C - C^T) = O_m \\ \overline{p^{\alpha-1}}(A^T + D) = O_m \\ \overline{p^{\alpha-1}}(A + D^T) = O_m \\ \overline{p^{\alpha-1}}(B^T - B) = O_m \end{array}\right.$$

$$\iff \quad \left\{\begin{array}{l} p \mid b_{ij} - b_{ji}, c_{ij} - c_{ji} \text{ (si } i \neq j) \\ p \mid a_{ij} + d_{ji} \end{array}\right.$$

Así que,

$$\mathrm{Ker}(g) = \left\{ \left[\begin{array}{c|c} \overline{p^{\alpha-1}}A + I_m & \overline{p^{\alpha-1}}B \\ \hline \overline{p^{\alpha-1}}C & \overline{p^{\alpha-1}}D + I_m \end{array}\right] : (A, D) \in M \text{ y } B, C \in N \right\}$$

donde M es

$$\left\{\left([\overline{x_{ij}}],[\overline{y_{ij}}]\right) \in \mathbb{Z}_{p^\alpha}^{m\times m}\times\mathbb{Z}_{p^\alpha}^{m\times m} : (x_{ij},y_{ij}) \in \{(0,0),(1,p-1),\ldots,(p-1,1)\}\right\}$$

y $N = \left\{[\overline{z_{ij}}] \in \mathbb{Z}_{p^\alpha}^{m\times m} : \overline{z_{ij}} = \overline{z_{ji}} \text{ si } i<j \text{ y } z_{ij}\in\{0,1,\ldots,p-1\}\right\}$.

En consecuencia,

$$|\operatorname{Ker}(g)| = \#(M)\times\#(N)\times\#(N) = p^{m^2}p^{\frac{m^2+m}{2}}p^{\frac{m^2+m}{2}} = p^{2m^2+m}.$$

Por tanto, se cumple la fórmula (9).

2. La fórmula (10) se sigue fácilmente de la parte anterior. □

Un resultado bastante conocido es dado en [2, Proposition 4.4] y expresa que el orden del grupo simpléctico de rango $2m$ sobre $\mathbb{Z}_p$ es:

$$|\mathbf{Sp}(2m,\mathbb{Z}_p)| = p^{m^2}\prod_{j=1}^{m}(p^{2j}-1). \tag{11}$$

Así que el corolario siguiente se sigue inmediatamente.

Corolario 3.3. *Sean $p\geq 2$ primo y $\alpha\geq 2$ entero. Entonces*

$$|\mathbf{Sp}(2m,\mathbb{Z}_{p^\alpha})| = (p^\alpha)^{2m^2+m}\prod_{j=1}^{m}(1-p^{-2j}).$$

Demostración: De las ecuaciones (10) y (11) tenemos que

$$|\mathbf{Sp}(2m,\mathbb{Z}_{p^\alpha})| = p^{(2m^2+m)(\alpha-1)}p^{m^2}\prod_{j=1}^{m}(p^{2j}-1) = (p^\alpha)^{2m^2+m}\prod_{j=1}^{m}(1-p^{-2j}).$$

□

Teorema 3.4. *Sea $n = p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ la descomposición prima de n. Entonces,*

1. *Los grupos $\mathbf{Sp}(2m,\mathbb{Z}_n)$ y $\mathbf{Sp}(2m,\mathbb{Z}_{p_1^{\alpha_1}})\times\ldots\times\mathbf{Sp}(2m,\mathbb{Z}_{p_k^{\alpha_k}})$ son isomorfos; es decir,*

$$\mathbf{Sp}(2m,\mathbb{Z}_n) \cong \mathbf{Sp}(2m,\mathbb{Z}_{p_1^{\alpha_1}})\times\ldots\times\mathbf{Sp}(2m,\mathbb{Z}_{p_k^{\alpha_k}}). \tag{12}$$

2. *El orden del grupo $\mathbf{Sp}(2m,\mathbb{Z}_n)$ se expresa mediante la siguiente fórmula,*

$$|\mathbf{Sp}(2m,\mathbb{Z}_n)| = n^{2m^2+m}\prod_{i=1}^{k}\prod_{j=1}^{m}(1-p_i^{-2j}). \tag{13}$$

Demostración: 1. Nuevamente consideremos el isomorfismo $Prod$. Entonces

$$\begin{aligned} A \in & \mathbf{Sp}(2m, \mathbb{Z}_n) \iff A \in \mathbf{GL}(2m, \mathbb{Z}_n) \text{ y } A^T J_n A = J_n \\ & \iff A_{(h)} \in \mathbf{GL}(2m, \mathbb{Z}_{p_h^{\alpha_h}}) \text{ y } A_{(h)}^T J_{p_h^{\alpha_h}} A_{(h)} = J_{p_h^{\alpha_h}}, \quad h = 1, \ldots, k \\ & \iff Prod(A) \in \mathbf{Sp}(2m, \mathbb{Z}_{p_1^{\alpha_1}}) \times \ldots \times \mathbf{Sp}(2m, \mathbb{Z}_{p_k^{\alpha_k}}), \end{aligned}$$

lo cual demuestra que la función $Prod$ restringida al grupo $\mathbf{Sp}(2m, \mathbb{Z}_n)$ (i.e., $Prod|_{\mathbf{Sp}(2m,\mathbb{Z}_n)}$), es el isomorfismo buscado; es decir, la ecuación (12) se cumple.

2. Combinando la ecuación (12) con el Corolario 3.3 tenemos que

$$\begin{aligned} |\mathbf{Sp}(2m, \mathbb{Z}_n)| &= \prod_{i=1}^{k} |Sp(2m, \mathbb{Z}_{p_i^{\alpha_i}})| = \prod_{i=1}^{k} [(p_i^{\alpha_i})^{2m^2+m} \prod_{j=1}^{m} (1 - p_i^{-2j})] \\ &= \left(\prod_{i=1}^{k} p_i^{\alpha_i} \right)^{2m^2+m} \prod_{i=1}^{k} \prod_{j=1}^{m} (1 - p_i^{-2j}) = n^{2m^2+m} \prod_{i=1}^{k} \prod_{j=1}^{m} (1 - p_i^{-2j}). \end{aligned}$$

y por tanto la ecuación (13) también es válida. □

Referencias

[1] Buchmann, J., *Introduction to Cryptography*, Springer-Verlag, New York, 2000.

[2] Cameron, P., *Notes on Classical Groups*, 2000, Disponible en: http://www.maths.qmul.ac.uk/ ∼pjc/class_gps/

[3] Flannery, S. y Flannery, D., *In Code*, Workman Publishing, New York, 2001.

[4] MacWilliams, J., *Orthogonal matrices over finite fields*, Amer. Math. Monthly, **76**(1969), 152–164.

[5] B. McDonald. *Linear Algebra over Conmutative Rings*, Marcel Dekker, New York, 1984.

[6] Roby, N., *Sur le cardinal du groupe $Gl(n, A)$ ou A est un anneau fini*, An. Acad. Brasil. Ci., **49**(1977), no. 1, 15–18.