MATRICES NILPOTENTES SOBRE Z_m

por

D. Bollman y H. Ramírez-López

Una matriz A, de orden k, sobre un anillo R, se dice que es nilpotente si existe un entero positivo h tal que $A^h = 0$. En este trabajo desarrollamos una fórmula para el número de matrices nilpotentes sobre el anillo Z_m de los enteros módulo un entero positivo $m \geqslant 2$.

Dado un entero positivo k y un anillo finito R, sea $N(k, R)$ el número de matrices $k \times k$ nilpotentes sobre R. Observamos que si R es un cuerpo, entonces $N(k, R)$ es, efectivamente, el número de matrices X, de orden k sobre R, que satisfacen a la ecuación $X^k = 0$. En particular, si R es Z_p, siendo p primo, entonces

$$N(k, Z_p) = g(k) \sum_{\pi} p^{-a(\pi)} \prod_{j=1}^{k} g(k_j)^{-1}$$

donde

$$g(t) = \prod_{i=0}^{t-1} (p^t - p^i), \quad t \geqslant 1$$

es el número de matrices $t \times t$ no singulares sobre Z_p, $g(0) = 1$, y, además,

$$a(\pi) = \sum_{u=1}^{k} \left[\binom{k_u}{2} (u - 1) + 2u\, k_u \sum_{v=u+1}^{k} k_v \right]$$

$$\left(\sum_{v=k+1}^{k} k_v \text{ se define como } 0 \right),$$

donde la sumación se efectua sobre todas las particiones π de k definidas por

$$k = \sum_{j=1}^{k} j\, k_j.$$

Esta fórmula es un caso particular de la fórmula dada en [2] para el número de matrices $k \times k$ sobre un cuerpo finito GF(q), que satisfacen a un polinomio mónico dado sobre GF(q).

Ahora bien, sea $A = [a_{ij}]$ cualquier matriz $k \times k$, sobre el anillo de los enteros, con la propiedad $0 \leqslant a_{ij} \leqslant p^{\alpha+1}$ para todos los elementos a_{ij} de A, donde p es primo y α es un entero positivo. Entonces existen matrices únicas $B = [b_{ij}]$ y $K = [k_{ij}]$, de orden k, con $0 \leqslant b_{ij} < p^{\alpha}$ y $0 \leqslant k_{ij} < p$ para tdos los elementos b_{ij} y k_{ij} de B y K, respectivamente, y tales que

$$A = B + p^{\alpha} K.$$

Lema: A es nilpotente módulo $p^{\alpha+1}$ (es decir, existe un entero positivo h tal que $A^h = 0 \bmod p$), si y sólo si B es nilpotente módulo p^{α}.

Demostración: Supongamos que A es nilpotente módulo $p^{\alpha+1}$. Entonces existe un entero positivo h tal $A^h \equiv 0 \bmod. p^{\alpha+1}$. Por tanto, $A^h \equiv \equiv 0 \bmod. p^{\alpha}$. Pero $A \equiv B \bmod. p^{\alpha}$; luego $B^h = 0 \bmod. p^{\alpha}$, o sea B es nilpotente módulo p^{α}.

Recíprocamente, supongamos que B es nilpotente módulo p^{α}. Entonces existe un entero positivo h tal que $B^h \equiv 0 \bmod. p^{\alpha}$.

Ahora bien, $A^r \equiv B^r + p^{\alpha} (B^{r-1} K + B^{r-2} KB + B^{r-3} KB^2 + + \ldots + KB^{r-1}) \bmod. p^{\alpha+1}$ para todo entero positivo r. En particular, $A^{2h} \equiv B^{2h} + p^{\alpha} (B^{2h-1} K + \ldots + B^h KB^{h-1} + B^{h-1} KB^h + \ldots + + KB^{2h-1}) \bmod. p^{\alpha+1}$.

Pero como $B^h \equiv 0 \bmod. p^{\alpha}$, tenemos que $B^{2h} = 0 \bmod. p^{\alpha+1}$.

Así, pues, $A^{2h} \equiv 0 \bmod. p^{\alpha+1}$ y, por tanto, A es nilpotente módulo $p^{\alpha+1}$.

Por inducción en α, podemos demostrar fácilmente el siguiente Corolario: $N(k, Z_{p\alpha}) = p^{(\alpha-1)k^2} N(k, Z_p)$.

Finalmente, desarrollamos una fórmula para $N(k, Z_m)$, cuando m es un entero positivo arbitrario $\geqslant 2$. Para ello utilizaremos la bien conocida descomposición de Z_m en una suma directa de subanillos de Z_m.

Supongamos que $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ es una factorización de m en potencias de primos distintos. Para cada $i = 1, 2, \ldots, r$, sea $\overline{p_i}$ el entero positivo único, tal que $m = p_i^{\alpha_i} \overline{p_i}$. Entonces existen enteros $x_1, x_2, \ldots, x_r$, tales que

$$x_1\overline{p_1} + x_2\overline{p_2} + \ldots + x_r\overline{p_r} \equiv 1 \bmod. m$$

Para cada $i = 1, 2, \ldots, r$, sea $e_i \equiv x_i\overline{p_i}$.

Entonces, $e_1 + e_2 + \ldots + e_r \equiv 1 \bmod. m$.

y

$$e_i e_j = \begin{cases} 0 \bmod. m, & i \neq j \\ e_i \bmod. m, & i = j, \end{cases}$$

es decir, $1 \in Z_m$ puede descomponerse en idempotentes mutuamente ortogonales.

Por tanto,

$$Z_m = M_1 \Theta M_2 \Theta \ldots \Theta M_g,$$

donde

$$M_i = \{\overline{a_i} \equiv a_{ei} = \text{mod. } m \mid a \in Z_m\}.$$

Ademas, cada M_i, $i = 1, 2, \ldots, r$ es isomórfico a $Z_{pi\,\alpha i}$ respecto de la correspondencia

$$f(\overline{a_i}) \equiv a \text{ mod. } p_i\, \alpha i, \text{ siendo } \overline{a_i} = ae_i$$

Teorema:

$$N(k, Z_m) = \left[\frac{m}{p_1 p_2 \ldots p_r}\right]^{k^2} \prod_{i=1}^{r} N(k, Z_{pi}),$$

donde $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p^{r\alpha_r}$ es una factorización de m en potencias de primos distintos.

Demostración: Cualquier matriz $k \times k$ sobre Z_m puede expresarse en la forma única

$A \equiv A_1 + A_2 + \ldots + A_r$ mod. m, donde cada A_i es una matriz $k \times k$ sobre M_i.

Además,

$A^h \equiv 0$ mod. m, sí y sólo sí $A_i^h \equiv 0$ módulo m para cada $i = 1, 2, \ldots, r$.

Luego,

$$N(k, Z_m) = \prod_{i=1}^{r} N(k, M_i)$$

Pero $M_i \cong Z_{pi\,\alpha_i}$ y, en consecuencia,

$$N(k, M_i) = N(k, Z_{pi\,\alpha_i})$$

para cada $i = 1, 2, \ldots, r$.

Por tanto,

$$N(k, Z_m) = \prod_{i=1}^{r} N(k, Z_{p_i^{\alpha_i}}) =$$

$$= \prod_{i=1}^{r} N(k, Z_{p_i}) p_i^{(\alpha_i - 1)k^2} =$$

$$= \left[\frac{m}{p_1 p_2 \ldots p_r}\right]^{k^2} \prod_{i=1}^{r} N(k, Z_{p_i})$$

BIBLIOGRAFIA

1. H. Hasse, Zahlentheorie, Berlin, Akademie-Verlag, 1949.
2. J. H. Hodges, «Scalar Polynomial Equations for Matrices over a Finite Field», *Duke Mathematical Journal*. Tomo 25. Núm. 2, Páginas 291-296, junio 1958.