

Combinatoria

Práctica 5

1. i) Sea p un primo y sea $a \in \mathbb{Z}$ tal que $p \nmid a$. Probar que $a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$ para todo $k \in \mathbb{N}$

ii) Recordemos que denotamos por $\Phi(n)$ a la cantidad de números naturales menores o iguales que n que son coprimos con n y que habíamos probado que

$$\Phi(n) = n \cdot \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

donde $p_1, p_2, \dots, p_r$ son los primos que dividen a n .

Usando esta identidad, probar que si $n = p_1^{k_1} \cdot p_2^{k_2} \dots p_r^{k_r}$ es la factorización de n entonces

$$\Phi(n) = \prod_{i=1}^r \left((p_i - 1) \cdot p_i^{k_i - 1} \right)$$

iii) Probar que si a es un entero es coprimo con n entonces $a^{\Phi(n)} \equiv 1 \pmod{n}$

2. Supongamos que la clave pública de Pedro es $(n, e) = (2173, 51)$. A partir de la factorización de n hallar su clave privada (p, q, d) .

3. Probar que la métrica de Hamming es una distancia en F^n , es decir, para todo $v, w \in F^n$ valen

i) $d(v, w) \geq 0$ y $d(v, w) = 0$ sii $v = w$

ii) $d(v, w) = d(w, v)$

iii) $d(v, w) \leq d(v, u) + d(u, w) \quad \forall u \in F^n$

4. Dado un vector binario u de longitud n , denotemos por $w(u)$ a la cantidad de unos que contiene u .

i) Probar que $w(u + v) = w(u) + w(v) - 2u \cdot v$, donde $u + v$ es la suma en $\mathbb{Z}_2^n$ y $u \cdot v$ es el producto escalar de u y v (considerados como vectores de coordenadas reales).

ii) Probar que, si identificamos un string de ceros y unos con el correspondiente vector binario, $d(u, v) = w(u + v)$

5. Si v es un string de ceros y unos, denotamos por $\bar{v}$ al string que se obtiene cambiando cada 1 de v por un 0 y cada 0 por un 1.

Probar que si u y v son strings de ceros y unos de longitud n entonces $d(u, \bar{v}) = n - d(u, v)$

6. Construir el código de Hamming $A \subseteq F^{15}$ que corrige un error. Supongamos que $v \in A$ es transmitido y durante la transmisión a lo sumo un bit es alterado. Determine v sabiendo que el string que fue recibido es $v' = 101000000000000$.

7. Sea $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$ y sea

$$C = \{B \cup \{8\} / B \in C_1\} \cup C_2$$

donde C_1 y C_2 los conjuntos de bloques de los diseños construidos en los ejemplos 1 y 2 respectivamente.

Probar que (S, C) es un diseño de parámetros

i) 3-(8, 4, 1)

ii) 2-(8, 4, 3)

iii) 1-(8, 4, 7)

8. Sea $S = \{0, 1, 2, \dots, 20\}$ y sea $U = \{3, 6, 7, 12, 14\}$. Para cada h entre 0 y 20 definimos un bloque B_h en la forma

$$B_h = \{r_{21}(u + h) / u \in U\}$$

i) Verificar que para cada r entre 1 y 20 existe un único $u \in U$ tal que $r_{21}(u + r) \in U$.

ii) Sean $i, j \in S$, $i < j$, y sea u el único elemento de U tal que $r_{21}(u + j - i) \in U$. Probar que $\{i, j\} \subseteq B_h$ si y sólo si $h = r_{21}(i - u)$.

iii) Probar que $(S, \{B_h / 0 \leq h \leq 20\})$ es un diseño cuadrado de parámetros $(21, 5, 1)$.

9. Sea (S, C) un diseño cuadrado de parámetros (ν, k, λ) . Probar que $k(k - 1) = \lambda(\nu - 1)$. Sugerencia: Fijado $v \in S$, contar de dos maneras la cantidad de pares (u, B) tales que $u \in S$, $u \neq v$ y B es un bloque que contiene a u y a v .

10. Sea D la matriz de incidencia de un diseño cuadrado de parámetros (ν, k, λ) .

i) Probar que $\det(D^t \cdot D) = k^2(k - \lambda)^{\nu-1}$

ii) Deducir de i) que D es inversible.

11. Sea (S, C) un diseño cuadrado de parámetros (ν, k, λ) . Sea D su matriz de incidencia y sea D' la matriz que se obtiene cambiando cada 1 de D por un 0 y cada 0 por un 1.

Probar que si $C' = \{S - B / B \in C\}$ entonces (S, C') es un diseño cuadrado de parámetros $(\nu, \nu - k, \nu - 2k + \lambda)$ (llamado el complemento de (S, C)) y su matriz de incidencia es D' .

12. Sea M la matriz cuya fila 1 es 1 1 0 1 0 0 0 0 0 1 0 0 0 y cuyas restantes filas se obtienen por permutaciones cíclicas de la fila 1 (la fila 2 será 0 1 1 0 1 0 0 0 0 0 1 0 0, la fila 3 será 0 0 1 1 0 1 0 0 0 0 0 1 0, etc).

Mostrar que M es la matriz de incidencia de un diseño cuadrado de parámetros $(13, 4, 1)$.

13. Probar que las matrices H_m definidas en el ejemplo 7 satisfacen

$$H_m^t \cdot H_m = H_m \cdot H_m^t = 2^{m+1} I$$

14. Sea D la matriz de incidencia del diseño cuadrado construido en el ejercicio 8 y sea D' la de su complemento. Construir un código $A \subseteq F^{21}$ de cardinal 42 que corrige 3 errores, utilizando las filas de D y D' .

15. Sea $(G, *)$ un grupo finito de n elementos, $G = \{g_1, g_2, \dots, g_n\}$. Probar que si definimos $a_{ij} = k$ si y sólo si $g_i * g_j = g_k$ entonces $\|a_{ij}\|$ es un cuadrado latino de orden n .

16. Sea $n = p^r$ (p primo, $r \in \mathbb{N}$) y sea K un cuerpo de n elementos, $K = \{f_0, f_1, \dots, f_{n-1}\}$ donde $f_0 = 0$. Sean $L_1, L_2, \dots, L_{n-1}$ las matrices de $n \times n$ definidas por $L_m(i, j) = f_m f_i + f_j$ ($0 \leq i, j \leq n-1$) (donde las operaciones son la suma y el producto en K)

i) Probar que L_j es un cuadrado latino de orden n para todo $1 \leq j \leq n-1$

ii) Probar que para todo $i \neq j$ los cuadrados latinos L_i y L_j son ortogonales (es decir, $L_1, L_2, \dots, L_{n-1}$ es un sistema completo para n).