Ejercicio Hill 3x3

C = TAKKFMBEZ

Tamaño bloque = 3

Llave = polygraso

- Llave valida?

$$K = \begin{pmatrix} p & e & l \\ i & g & r \\ a & s & o \end{pmatrix} = \begin{pmatrix} 16 & 4 & 11 \\ 8 & 6 & 18 \\ 15 & 14 & 15 \end{pmatrix}$$

$$|K| = \left(\begin{array}{ccc|cc} 16 & 4 & 11 & 16 & 4 \\ 8 & 6 & 18 & 8 & 6 \\ 15 & 14 & 15 & 15 & 14 \end{array}\right) = (16 \times 6 \times 15) + (4 \times 18 \times 15) + (11 \times 8 \times 14) - [(11 \times 6 \times 15) + (16 \times 18 \times 14) + (4 \times 8 \times 15)] = 4192 - 6942$$

$$\Rightarrow -2750 \bmod 27 = -23 \bmod 27 = 4 \bmod 27 = \underline{4}$$

$27 = 4(6) + 3$

$4 = 3(1) + \underline{1}$ $\qquad$ MCD$(4, 27) = \underline{1}$

$3 = 1(3) + 0$ $\qquad$ = Llave valida, gcd(det(K), n) = $\underline{1}$

Buscando K^{-1}

$$\left(\begin{array}{ccc|ccc} 16 & 4 & 11 & 1 & 0 & 0 \\ 8 & 6 & 18 & 0 & 1 & 0 \\ 15 & 14 & 15 & 0 & 0 & 1 \end{array}\right) \Leftrightarrow \frac{1}{16}F_1 \left(\begin{array}{ccc|ccc} 1 & 1/4 & 11/16 & 1/16 & 0 & 0 \\ 8 & 6 & 18 & 0 & 1 & 0 \\ 15 & 14 & 15 & 0 & 0 & 1 \end{array}\right) \Leftrightarrow \begin{array}{l} F_2 - 8F_1 \\ F_3 - 15F_1 \end{array}$$

$$\left(\begin{array}{ccc|ccc} 1 & 1/4 & 11/16 & 1/16 & 0 & 0 \\ 0 & 4 & 25/2 & -1/2 & 1 & 0 \\ 0 & 61/4 & 75/16 & -15/16 & 0 & 1 \end{array}\right) \Leftrightarrow \frac{1}{4}F_2 \left(\begin{array}{ccc|ccc} 1 & 1/4 & 11/16 & 1/16 & 0 & 0 \\ 0 & 1 & 25/8 & -1/8 & 1/4 & 0 \\ 0 & 61/4 & 75/16 & -15/16 & 0 & 1 \end{array}\right) \Leftrightarrow \begin{array}{l} F_1 - \frac{1}{4}F_2 \\ F_3 - \frac{61}{4}F_2 \end{array}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & -3/32 & 3/32 & -1/16 & 0 \\ 0 & 1 & 25/8 & -1/8 & 1/4 & 0 \\ 0 & 0 & -1375/32 & 31/32 & -61/16 & 1 \end{array}\right) \underset{-\frac{32}{1375}F_3}{\Longleftrightarrow} \left(\begin{array}{ccc|ccc} 1 & 0 & -3/32 & 3/32 & -1/16 & 0 \\ 0 & 1 & 25/8 & -1/8 & 1/4 & 0 \\ 0 & 0 & 1 & -\frac{31}{1375} & \frac{122}{1375} & -\frac{32}{1375} \end{array}\right)$$

$$\underset{F_2-\frac{25}{8}F_3}{\overset{F_1+\frac{3}{32}F_3}{\Longleftrightarrow}} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{126}{1375} & -\frac{149}{2750} & -\frac{3}{1375} \\ 0 & 1 & 0 & -3/55 & -\frac{3}{110} & 4/55 \\ 0 & 0 & 1 & -\frac{31}{1375} & \frac{122}{1375} & -\frac{32}{1375} \end{array}\right)$$

$$K^{-1} = \begin{pmatrix} \frac{126}{1375} & -\frac{149}{2750} & -\frac{3}{1375} \\ -\frac{3}{55} & -\frac{3}{110} & \frac{4}{55} \\ -\frac{31}{1375} & \frac{122}{1375} & -\frac{32}{1375} \end{pmatrix} \bmod 27 = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

① $126 \cdot 1375^{-1} \bmod 27$

$1375^{-1} \bmod 27 = 25^{-1} \bmod 27 = 13$ $\checkmark$

$27 = 25(1)+2$ $\qquad 2 = 27 - 25(1)$

$25 = 2(12)+1$ $\qquad 1 = 25 - 12(2)$

$2 = 1(2)+0$ $\qquad 1 = 25 - 12(2)$

$1 = 25 - 12(27) + 25(12)$ $\qquad 1 = 25 - 12(27 - 25(1))$

$1 = 25(13) - 12(27) = 25(13) + 27(-12)$

$1 = ax + by$ $\qquad$ Comprobar

$a^{-1} \bmod b = x$ $\qquad 13 \cdot 25^{-1} \bmod 27 = 1$ $\checkmark$

$25^{-1} \bmod 27 = 13$

$126 \bmod 27 = 18$ $\qquad$ ① $18 \cdot 13 \bmod 27 = 234 \bmod 27$

$a = 18$ $\checkmark$

b) $-149 \cdot 2750^{-1} \bmod 27$

$2750^{-1} \bmod 27 = 23^{-1} \bmod 27$

$27 = 23(1) + 4$ $\quad 4 = 27 - 23(1)$

$23 = 4(5) + 3$ $\quad 3 = 23 - 4(5)$

$4 = 3(1) + 1$ $\quad 1 = 4 - 3(1)$

$3 = 3(1) + 0$

$\Rightarrow 23^{-1} \bmod 27 = 20$

Comprobación

$23^{-1} \cdot 20 \bmod 27 = 1$

$1 = 4 - 3(1)$

$1 = 4 - 23 + 4(5)$

$1 = 4(6) - 23$

$1 = (27 - 23)(6) - 23$

$1 = 27(6) - 7(23)$

$1 = ax + by$

$1 = 23(-7) + 27(6)$

$a^{-1} \bmod b = x$

$23 \bmod 27 = -7 \bmod 27$

$= -149 \bmod 27 = -14 \bmod 27 = 13$

$b = 13 \cdot 20 \bmod 27 = 260 \bmod 27 = 17$

$b = 17$

c) $-3 \cdot 1375^{-1} \bmod 27 = 24 \cdot 13 \bmod 27 = 312 \bmod 27 = 15$

$-3 \bmod 27 = 24$

$c = 15$

$1 = 27 - 2(13)$

$1 = 2(-13) + 27$

$2^{-1} \bmod 27 = -13 \bmod 27$

$2^{-1} \bmod 27 = 14$

Comprobación

$2^{-1} \cdot 14 \bmod 27 = 1$

d) $-3 \cdot 55^{-1} \bmod 27$

$55^{-1} \bmod 27 = 1^{-1} \bmod 27 = 1$

$-3 \bmod 27 = 24$

$24 \cdot 1 \bmod 27 = 24$

$d = 24$

e) $-3 \cdot 110^{-1} \bmod 27 = 24 \cdot 110^{-1} \bmod 27$

$110^{-1} \bmod 27 = 2^{-1} \bmod 27 = 14$

$27 = 2(13) + 1$

$2 = 1(2) + 0$

$-3 \bmod 27 = 24$

$24 \cdot 14 \bmod 27 = 336 \bmod 27 = 12$

$c = 12$

f) $4 \cdot 55^{-1} \bmod 27 = 4 \cdot 1 \bmod 27 = 4$

$f = 4$

g) $-31 \cdot 1375^{-1} \bmod 27 = 23 \cdot 13 \bmod 27 = 299 \bmod 27 = 2$

$-31 \bmod 27 = -4 \bmod 27 = 23 \bmod 27$

$g = 2$

h) $122 \cdot 1375^{-1} \bmod 27 = 14 \cdot 13 \bmod 27 = 182 \bmod 27 = 20$

$122 \bmod 27 = 14$

$h = 20$

i) $-32 \cdot 1375^{-1} \bmod 27 = 22 \cdot 13 \bmod 27 = 286 \bmod 27 = 16$

$-32 \bmod 27 = -5 \bmod 27 = 22$

$i = \frac{16}{27}$

$$K^{-1} = \begin{pmatrix} 18 & 17 & 15 \\ 24 & 12 & 4 \\ 2 & 20 & 16 \end{pmatrix}$$

$e = 18 + 4 \cdot 24 + 26 \cdot 2 = 166$

$f = 17 + 4 \cdot 12 + 26 \cdot 20 = 585$

$g = 15 + 16 + 26 \cdot 16 = 447$

$$C = \begin{pmatrix} T & A & K \\ K & F & M \\ B & E & Z \end{pmatrix} = \begin{pmatrix} 20 & 0 & 10 \\ 10 & 5 & 12 \\ 1 & 4 & 26 \end{pmatrix}$$

$$m = CK^{-1} = \begin{pmatrix} 20 & 0 & 10 \\ 10 & 5 & 12 \\ 1 & 4 & 26 \end{pmatrix} \begin{pmatrix} 18 & 17 & 15 \\ 24 & 12 & 4 \\ 2 & 20 & 16 \end{pmatrix} = \begin{pmatrix} 380 & 540 & 460 \\ 324 & 470 & 362 \\ 166 & 585 & 447 \end{pmatrix} \bmod 27$$

$a = 20 \cdot 18 + 0 + 20 = 380$

$b = 20 \cdot 17 + 0 + 200 = 540$

$c = 20 \cdot 15 + 0 + 160 = 460$

$d = 10 \cdot 18 + 5 \cdot 24 + 12 \cdot 2 = 324$

$e = 10 \cdot 17 + 5 \cdot 12 + 12 \cdot 20 = 470$

$d = 10 \cdot 15 + 5 \cdot 4 + 12 \cdot 16 = 362$

$$m = \begin{pmatrix} 380 & 540 & 460 \\ 324 & 470 & 362 \\ 166 & 585 & 447 \end{pmatrix} \bmod 27 = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 11 & 11 \\ 4 & 18 & 15 \end{pmatrix} = \begin{pmatrix} c & a & b \\ a & l & l \\ e & r & o \end{pmatrix}$$

$m = \text{caballero}$