

Algoritmo de la división

$$a = 58, n = 7$$

$$q = 8 < \frac{58}{7} < 9$$

$$\begin{aligned} r &= a - (q)n \\ &= 58 - (8)7 \\ &= 58 - 56 \\ &= 2 \end{aligned} \quad 58 = (8)7 + 2$$

$$a = -96, n = 12$$

$$q = -8 < \frac{-96}{12} < -7$$

$$\begin{aligned} r &= -96 - (-8)12 \\ &= -96 + 96 \\ &= 0 \end{aligned} \quad -96 = (-8)12$$

$$a = 84, n = 12$$

$$q = 7 < 84/12 < 8$$

$$\begin{aligned} r &= a - (q)n \\ &= 84 - (7)12 \\ &= 84 - 84 \\ &= 0 \end{aligned} \quad 8 = (7)12$$

$$a = 100, n = 9$$

$$q = 11 < \frac{100}{9} < 12$$

$$\begin{aligned} r &= 100 - (11)9 \\ &= 100 - 99 \\ &= 1 \end{aligned} \quad 100 = (11)9 + 1$$

$$a = -4, n = 5$$

$$q = -1 < -4/5 < 0$$

$$\begin{aligned} r &= -4 - (-1)5 \\ &= -4 + 5 \\ &= 1 \end{aligned} \quad -4 = (-1)5 + 1$$

Algoritmo Euclides

93, 27

$$93 = (3) 27 + 12$$

$$27 = (2) 12 + 3$$

$$12 = (4) 3 + 0$$

$$\text{mcd} = 3$$

209, 78

$$209 = (2) 78 + 53$$

$$78 = (1) 53 + 15$$

$$53 = (3) 15 + 8$$

$$15 = (1) 8 + 7$$

$$8 = (1) 7 + 1$$

$$7 = (1) 1 + 0$$

$$\text{mcd} = 1$$

138, 61

$$138 = (2) 61 + 16$$

$$61 = (3) 16 + 13$$

$$16 = (1) 13 + 3$$

$$13 = (4) 3 + 1$$

$$3 = (3) 1 + 0$$

$$\text{mcd} = 1$$

231, 49

$$231 = (4) 49 + 35$$

$$49 = (-1) 35 + 14$$

$$35 = (2) 14 + 7$$

$$14 = (2) 7 + 0$$

$$\text{mcd} = 7$$

Coeficiente de Bézout

• $-112, -91$

$$-112 = (2) \cdot 91 + 70$$

$$-91 = (-2) \cdot 70 + 49$$

$$70 = (1) \cdot 49 + 21$$

$$49 = (2) \cdot 21 + 7$$

$$21 = (3) \cdot 7 + 0$$

$$7 = 49 - (2) \cdot 21$$

$$= (2) [70 - 49] = (3) \cdot 49 - (2) \cdot 70$$

$$= (3) [-91 + (2) \cdot 70] - (2) [-112 + (2) \cdot 91]$$

$$= (3) \cdot -91 + (4) \cdot -91 + (-2) \cdot (-112) + (6) \cdot 70$$

$$= (7) \cdot -91 + (-2) \cdot -112 + 6 [-112 + (2) \cdot 91]$$

$$= (-5) \cdot -91 + (4) \cdot -112$$

$$7 = (4) \cdot -112 + (-5) \cdot -91$$

• $-105, 39$ $[\text{mcd}(105, 39) = \text{mcd}(-105, 39)]$

$$105 = (2) \cdot 39 + 27$$

$$= (1) \cdot 27 + 12$$

$$= (2) \cdot 12 + 3$$

$$= (4) \cdot 3 + 0$$

$$3 = 27 - (2) \cdot 12$$

$$= 27 - (2) [39 - 27] = (3) \cdot 27 - (2) \cdot 39$$

$$= (3) [-105 + (-6) \cdot 39 - (-2) \cdot 39]$$

$$= (-3) \cdot -105 + (-6) \cdot 39 - (-2) \cdot 39$$

$$= (-3) \cdot -105 + (-3) \cdot 39$$

Residuo mínimo

$$\bullet r \bmod 10$$

- $50 \bmod 10$
 $5 \leq 50/10 < 6$
 $r = 50 - (5)10$
 $r = 0$

- $-38 \bmod 10$
 $-4 < -38/10 < -3$
 $r = -33 - (-4)10$
 $r = 2$

- $6 \bmod 10$
 $0 < 6/10 < 1$
 $r = 6 - (0)10$
 $r = 6$

- $17 \bmod 10$
 $1 < 17/10 < 2$
 $r = 17 - (1)10$
 $r = 7$

- $-1 \bmod 10$
 $-1 < -1/10 < 0$
 $r = -1 - (-1)10$

$$\bullet r \bmod 3$$

- $17 \bmod 3$
 $5 < 17/3 < 6$
 $r = 17 - (5)3$
 $r = 2$

- $9 \bmod 3$
 $3 \leq 9/3 < 4$
 $r = 9 - (3)(3)$
 $r = 0$

- $-2 \bmod 3$
 $-1 \leq -2/3 < 0$
 $r = -2 - (-1)3$
 $r = 1$

- $3 \bmod 3$
 $1 \leq 3/3 < 2$
 $r = 3 - (1)3$
 $r = 0$

- $-10 \bmod 3$
 $-4 < -10/3 < -3$
 $r = -10 - (-4)3$
 $r = 2$

¿Qué día de la semana va a ser dentro de 1000 días?
⇒ Jueves

$$7 \text{ días a la semana } \{ 1004 = 1000 + 4 = \text{(jueves)} \uparrow$$

$$1004 \bmod 7 \equiv (700 + 280 + 24) \% 7$$

$$\equiv 24 \bmod 7$$

$$r = 3 \text{ (3}^{\text{er}} \text{ día de la semana)}$$

Sería Miércoles

Aritmética modular

min $r \mod 6$

$$\begin{aligned} & \star 7+3 \mod 6 \\ & 10 \mod 6 \\ & r = 4 \end{aligned}$$

$$\begin{aligned} & \bullet 7-3 \mod 6 \\ & 4 \mod 6 \\ & r = 4 \end{aligned}$$

$$\begin{aligned} & \bullet 67+68 \mod 6 \\ & (67+68) \equiv (7+8) \mod 6 \\ & \equiv 15 \mod 6 \end{aligned}$$

$$r = 3$$

$$\begin{aligned} & \bullet 601-601 \mod 6 \\ & \equiv 1-1 \mod 6 \\ & \equiv 0 \mod 6 \end{aligned}$$

$$r = 0$$

$$\begin{aligned} & \bullet -3-19 \mod 6 \\ & -22 \mod 6 \\ & r = 2 \end{aligned}$$

Aritmética modular

min. $r \bmod 10$

$$\begin{aligned} & \bullet 14 - 7 \bmod 10 \\ & \quad 7 \bmod 10 \\ & \quad r = 7 \end{aligned}$$

$$\begin{aligned} & \bullet 10 - 11 - 1 \bmod 10 \\ & \equiv 0 - 1 - 1 \bmod 10 \\ & \equiv -2 \bmod 10 \\ & \quad r = 8 \end{aligned}$$

$$\begin{aligned} & \bullet 6 + 4 \bmod 10 \\ & \quad 10 \bmod 10 \\ & \quad r = 0 \end{aligned}$$

$$\begin{aligned} & \bullet 101 + 11 + 1 \bmod 10 \\ & \equiv 1 + 1 + 1 \bmod 10 \\ & \equiv 3 \bmod 10 \end{aligned}$$

$$r = 3$$

$$\begin{aligned} & \bullet 21 - 17 \bmod 10 \\ & \equiv 4 + 3 \bmod 10 \\ & \equiv 12 \bmod 10 \\ & \quad r = 2 \end{aligned}$$

$$\begin{aligned} & \bullet 13 - 15 \bmod 10 \\ & \equiv 3 - 5 \bmod 10 \\ & \equiv -2 \bmod 10 \\ & \quad r = 8 \end{aligned}$$

