## Práctico 3: Algoritmo de Euclides y ec. diofánticas

**Algoritmo Extendido de Euclides:** para hallar $mcd(a,b)$ y una c. lineal $ax+by = mcd$.

$a \leq b$

$M \leftarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Mientras $b \neq 0$

- $q \leftarrow coc(a,b)$
- $r \leftarrow res(a,b)$
- $M_i = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$
- $M = M_i \times M$
- $a \leftarrow b$
- $b \leftarrow r$

$g \leftarrow a$

$x \leftarrow M_{11}$

$y \leftarrow M_{12}$

Devolver $g, x, y$.

**Ec. Diofánticas:** $ax + by = c \qquad a,b,c \in \mathbb{Z}$

**Teorema:** (1) $ax+by=c$ tiene sol $x,y \in \mathbb{Z}$ si y sólo si $mcd(a,b) \mid c$

(2) Si tiene una solución, entonces tiene $\infty$ sols, y están dadas por

$$\left(x_0 + \frac{b}{mcd(a,b)} k \,,\, y_0 - \frac{a}{mcd(a,b)} k\right)$$

con $(x_0, y_0)$ sol. particular.

**Ejercicio 1.** En cada caso usar el Algoritmo de Euclides para calcular $d = \mathrm{mcd}(a,b)$ y determinar una expresión de $d$ como combinación lineal de $a$ y de $b$.

**a.** $a = 63$, $b = 15$. **b.** $a = 455$, $b = 1235$. **c.** $a = 2366$, $b = 273$.

(a) $a=63 \quad b=15$

$a = b \cdot q + r \rightsquigarrow mcd(a,b) = mcd(b, \underbrace{a-bq}_{r}) = mcd(b,r)$

$$63 = \underset{q}{4} \cdot 15 + \underset{r}{3}$$

$$\text{mcd}(63,15) = \text{mcd}(15,3) = 3.$$

(b) $a = 455$ $\quad b = 1235$

| $i$ | $B_i = \begin{pmatrix} b \\ a \end{pmatrix}$ | $M_i$ | $M$ | Division |
|---|---|---|---|---|
| 0 | $\begin{pmatrix} 1235 \\ 455 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | $1235 = 2 \cdot 455 + 325$ |
| 1 | $\begin{pmatrix} 455 \\ 325 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$ | $455 = 1 \cdot 325 + 130$ |
| 2 | $\begin{pmatrix} 325 \\ 130 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$ | $\begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix}$ | $325 = 2 \cdot 130 + 65$ |
| 3 | $\begin{pmatrix} 130 \\ 65 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$ | $\begin{pmatrix} -1 & 3 \\ 3 & -8 \end{pmatrix}$ | $130 = 2 \cdot 65 + 0 =$ |
| 4 | $\begin{pmatrix} 65 \\ 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$ | $\begin{pmatrix} 3 & -8 \\ x & x \end{pmatrix}$ | |

$$\text{mcd}(1235, 455) = 65$$

$x = 3 \qquad y = -8$

$$1235 \cdot 3 - 455 \cdot 8 = 65$$

**Ejercicio 3.** Un hombre va a una ferretería a comprar un trozo de burlete de goma de $x$ metros con $y$ centímetros. Pero el ferretero confunde los metros con centímetros y viceversa, cortando una cantidad distinta de la que el cliente había pedido. Sin percatarse de ello, el cliente toma su paquete y se marcha. Cuando llega a su casa, corta 68 centímetros de burlete y, para su sorpresa, descubre que le queda el doble de lo que él pensaba que había comprado.

¿Cuál es la menor cantidad de burlete (en metros y centímetros) que pudo haber pedido dicho cliente?

El hombre pide $x$ metros con $y$ cm $\rightarrow (\overset{y}{x} \cdot 100 + \overset{x}{y})$ cm

recibe 68cm + $2 \cdot$ ($x$ metros con $y$ cm) $\rightarrow \boxed{68 + 2(x \cdot 100 + y) = (y \cdot 100 + x) \text{cm}}$

$$68 + 2(x \cdot 100 + y) = (y \cdot 100 + x)$$

Pide: 8 metros 15 cm $\rightarrow 8 \cdot 100 + 15 = 815$

Le dan: 15 metros 8 cm $\rightarrow 15 \cdot 100 + 8 = 1508$

$$1508 \text{ cm} - 68 \text{ cm} = 2 \cdot 815$$

$$68 + 200x + 2y = 100y + x \qquad ax+by=c$$

$$\boxed{-199x + 98y = +68}$$

$\text{mcd}(98, 199) = 1 \mid 68 \Rightarrow$ Existe sol.

Podemos hallar $x'$ e $y'$ tales que $199x' + 98y' = 1$ y multiplicar por $(\pm 68)$

| $i$ | $B_i = \begin{pmatrix} b \\ a \end{pmatrix}$ | $M_i = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$ | $M$ | División |
|---|---|---|---|---|
| 0 | $\begin{pmatrix} 199 \\ 98 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | $199 = 2 \cdot 98 + 3$ |
| 1 | $\begin{pmatrix} 98 \\ 3 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$ | $98 = 32 \cdot 3 + 2$ |
| 2 | $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & -32 \end{pmatrix}$ | $\begin{pmatrix} 1 & -2 \\ -32 & 65 \end{pmatrix}$ | $3 = 1 \cdot 2 + 1$ |
| 3 | $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$ | $\begin{pmatrix} -32 & 65 \\ 33 & -67 \end{pmatrix}$ | $2 = 2 \cdot 1 + 0$ |
| 4 | $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ | ... | $\begin{pmatrix} 33 & -67 \\ * & * \end{pmatrix}$ | ... |
| | | $M_4 \cdot M$ | | |
| | | $M = M_3 \cdot M_2 \cdot M_1$ | | |

$\text{mcd}(199, 98) = 1$

$x' = 33 \qquad y' = -67$

$199 \cdot 33 + 98 \cdot -67 = 1$

$-199(-33 \cdot 68) - 98 \cdot 67 \cdot 68 = 68$

$-199(\underline{-2244}) + 98 \cdot (\underline{-4556}) = 68$

tienen que ser $>0$.

$$M = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -32 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$$

$$ax + by, \quad \underbrace{-199}_{a}x + \underbrace{98}_{b}y = 68$$

Todas las soluciones son de la forma: $\left(x_0 + \frac{b}{\text{mcd}}k, \; y_0 - \frac{a}{\text{mcd}}k\right)$

$$(x,y) = \Big(\underbrace{-2244}_{x_0} + \underbrace{98}_{b} \cdot k, \; \underbrace{-4556}_{y_0} + \underbrace{199}_{a} k\Big)$$

Debemos hallar el $k$ más chico t.q. $x, y > 0$

$$\left.\begin{array}{l} -2244 + 98k \geq 0, \; y \\ -4556 + 199k \geq 0 \end{array}\right\} \text{ simultáneamente.}$$

$$\Leftrightarrow \left.\begin{array}{l} 98k \geq 2244 \\ 199k \geq 4556 \end{array}\right\} \rightsquigarrow \boxed{k \geq 23}$$

$k = 23 \qquad x = -2244 + 98 \cdot 23 = 10$

$y = -4556 + 199 \cdot 23 = 21$

Verificamos: $2(10 \cdot 100 + 21) + 68 = (21 \cdot 100 + 10)$

$1021 \cdot 2 + 68 = 2110$

$\Leftrightarrow 2042 + 68 = 2110$ ✓