Máximo común divisor

Calcular el máximo común divisor de dos números, escribiendo el conjunto de sus divisores, puede ser muy moroso, Entonces necesitamos adquirir un método para calcular de manera menos moroso.

Hemos visto que (12,30)=6, resulta que se puede escribir el 6 como combinación lineal de 12 y 30.

$$6=12(-2) + 30(1) \quad \text{y} \quad 6=12(8)+30(-3)$$

Es posible hallar otros enteros u y v tales que $\boxed{6=12u + 30v.}$

Teorema Sea a y b enteros, no ambos 0, y sea d el máximo común divisor. Entonces existe (no necesariamente único) enteros u y v tales que d= au+bv.

El recíproco de este teorema es falso.

Ejm. Calcule el $(24,78)$ y luego escriba como combinación lineal.

Sol. divisores $24 = \{1, 2, 3, 4, 6, 8, 12, 24\}$

divisores $78 = \{1, 2, 3, 6, 13, 26, 39, 78\}$

Así $(24,78) = 6$

$$6 = 24(-3) + 78(1)$$

Teorema El máximo común divisor de dos números, no ambos ceros, es unico.

Algoritmo de Euclides Consideremos dos enteros positivos a y b. Sea $a > b$

Entonces, por el algoritmo de la división, existen q_1 y r_1 tales que

$$a = q_1 b + r_1 \quad , \quad 0 \le r_1 < b$$

$b, r_1 \rightarrow$
$$b = q_2 r_1 + r_2 \quad , \quad 0 \le r_2 < r_1$$

r_1 y $r_2 \rightarrow$
$$r_1 = q_3 r_2 + r_3$$

$$\vdots$$

$$r_{k-2} = q_k r_{k-1} + r_k \quad , \quad 0 \le r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1} r_k + \boxed{0}$$

Así $\quad r_k = (a,b)$

Ejm Encuentra $(72, 86)$

Sea $a = 86$ y $b = 72$

Entonces por el alg. de la división.

$$86 = (1)\cdot 72 + 14 \qquad 0 \leq 14 < 72$$

$$72 = (5)\cdot 14 + 2 \qquad 0 \leq 2 < 14$$

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

Así $\quad (86, 72) = 2$

Ej. Calcula $(10672, 4147)$

Sol.

$$10672 = (2)\,4147 + 2378 \qquad 6$$

$$4147 = (1)\cdot 2378 + 1769 \qquad 5$$

$$2378 = (1)\,1769 + 609 \qquad 4$$

$$1769 = (2)\cdot 609 + 551 \qquad 3$$

$$609 = (1)\,551 + 58 \qquad 2$$

$$551 = (9)\cdot 58 + 29 \qquad 1$$

$$58 = (2)\cdot 29 + 0$$

$$\begin{array}{r} 10672 \\ -\ 8294 \\ \hline 2378 \end{array} \qquad \begin{array}{r} 4147 \\ -\ 2378 \\ \hline 1769 \end{array}$$

$\therefore \quad (10672, 4147) = 29$

$$29 = 10672 \cdot (\overset{?}{\ \ }) + 4147(\overset{?}{\ \ })$$

El algoritmo de Euclides puede ser usado para escribir el (a,b) como una combinación lineal de a y b.

Ejm. Expresar $(10672, 4147)$ como una combinación lineal de 10672 y 4147.

$$29 = 10672x + 4147y$$

$10672 = (2)4147 + 2378$	6	$2378 = 10672 + (-2)4147$	✓
$4147 = (1)\cdot 2378 + 1769$	5	$1769 = 4147 + (-1)2378$	✓
$2378 = (1)1769 + 609$	4	$609 = 2378 + (-1)1769$	✓
$1769 = (2)\cdot 609 + 551$	3	$551 = 1769 + (-2)609$	✓
$609 = (1)551 + 58$ ✓	2	$58 = 609 + (-1)551$	✓
$551 = (9)\cdot 58 + 29$ ✓	1	$29 = 551 + (-9)58$	✓

Luego

$$29 = 551 + (-9)\cdot 58$$
$$29 = 551 + (-9)\cdot(609 + (-1)551)$$
$$= 551 + (-9)609 + (9)551$$
$$29 = (10)551 + (-9)609$$

$$29 = (10)\left(1769 + (-2)609\right) + (-9)609$$

$$29 = (10)\cdot 1769 + (-20)609 + (-9)609$$
$$29 = (10)1769 + (-29)609$$

$$29 = (10)\underline{1769} + (-29)\left(2378 + (-1)\underline{1769}\right)$$

$$29 = (39)\cdot 1769 + (-29)2378$$

$$29 = (39)\left(4147 + (-1)\underline{2378}\right) + (-29)\underline{2378}$$

$$29 = (39)4147 + (-68)2378$$

$$29 = (39)\underline{\underline{4147}} + (-68)\cdot\left(10672 + (-2)\underline{\underline{4147}}\right)$$

$$29 = (\underline{175})4147 + (-\underline{68})10672$$

$$\therefore\ 29 = 10672(-68) + 4147(175)$$

Inducción Matemática

1° Verificar para $n=1$

2° Suponer cierto para $n=k$, entonces dem. para $n=k+1$

3° Concluir que la prop. es V, $\forall n \in \mathbb{N}$.

Divisible. $a \mid b \iff b = a \cdot t \ , \ \exists t \in \mathbb{Z}$

$3 \nmid 5 \iff 5 = 3 \cdot (\ ?\ )$

Ejm. Demuestra que. $2^{2n} - 1$ es múltiplo de 3, $\forall n \in \mathbb{N}$.

Dem. Demostramos por inducción mat.

$$2^{2n} - 1 = 3 \cdot t \ , \ t \in \mathbb{Z} \ ?$$

1°. $n = 1$

$$\begin{aligned} 2^{2\cdot 1} - 1 &= 2^2 - 1 \\ &= 4 - 1 \\ &= 3 \cdot (1) \ , \quad 1 \in \mathbb{Z} \end{aligned}$$

2° Supongamos cierta para $n = k$

$$\boxed{2^{2k} - 1 = 3t} \quad \exists t \in \mathbb{Z} \qquad [\text{Hip.}]$$

entonces para $n = k+1$

$$2^{2(k+1)} - 1 = 3 \cdot r \ , \ \exists r \in \mathbb{Z} \ ?$$

Dem.

$$\begin{aligned} 2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\ &= 2^{2k} \cdot 2^2 - 1 \\ &= 4 \cdot 2^{2k} - 1 \\ &= (1+3)\, 2^{2k} - 1 \\ &= 2^{2k} + 3 \cdot 2^{2k} - 1 \end{aligned}$$

$a^n \cdot a^m = a^{n+m}$

$a^n \cdot b^n = (a \cdot b)^n$

$$- \underbrace{2^{2k} - 1} + 3 \cdot 2^{2k}$$

$$= 3 \cdot t + 3 \cdot 2^{2k}$$

$$= 3 \left(\underbrace{t + 2^{2k}}_{r} \right)$$

$$= 3 r. \qquad r \in \mathbb{Z}$$

3° $\therefore$ $2^{2n} - 1$ es múltiplo de 3, $\forall n \in \mathbb{N}$

Ej. Dem. que. $10^{n+1} - 9n - 10$ es múltiplo de 81.

Dem. $10^{n+1} - 9n - 10 = 81 \cdot t \quad , \quad t \in \mathbb{Z}$

1° $n = 1$: $10^{1+1} - 9 \cdot 1 - 10 = 10^2 - 9 - 10$

$$= 100 - 19$$

$$= 81 \cdot (1) \qquad \checkmark$$

2° Sup. cierto para $n = k$.

$$\boxed{10^{k+1} - 9 \cdot k - 10 = 81 \cdot t} \quad , \quad \exists\, t \in \mathbb{Z} \quad (\text{Hip.})$$

entonces, veamos $n = k+1$

$$10^{k+2} - 9(k+1) - 10 = 81 \cdot r \quad , \quad \exists\, r \in \mathbb{Z} \;?$$

Dem.

$$10^{k+2} - 9(k+1) - 10 = 10^{k+1+1} - 9k - 9 - 10$$

$$= \underline{10^{k+1}} \cdot 10^1 - \underline{9k} - 9 \underline{-10}$$

$$= (1+9)\, 10^{k+1} - 9k - 10 - 9$$

$$= \underline{10^{k+1}} + 9 \cdot 10^{k+1} - \underline{9k} - \underline{10} - 9.$$

?