Matemática Discreta I
Clase 13 - Máximo común divisor (2)

FAMAF / UNC

29 de abril de 2021

Algoritmo de Euclides

Para calcular el mcd de enteros a y b, con $b > 0$, definimos q_i y r_i recursivamente de la siguiente manera: $r_0 = a$, $r_1 = b$, y

$$
\begin{array}{lcl}
(e_1) & r_0 = r_1 q_1 + r_2 & (0 < r_2 < r_1) \\
(e_2) & r_1 = r_2 q_2 + r_3 & (0 < r_3 < r_2) \\
(e_3) & r_2 = r_3 q_3 + r_4 & (0 < r_4 < r_3) \\
\dots & & \\
(e_i) & r_{i-1} = r_i q_i + r_{i+1} & (0 < r_{i+1} < r_i) \\
\dots & & \\
(e_{k-1}) & r_{k-2} = r_{k-1} q_{k-1} + r_k & (0 < r_k < r_{k-1}) \\
(e_k) & r_{k-1} = r_k q_k + 0, &
\end{array}
$$

Entonces $r_k = \mathrm{mcd}(a, b)$ (Se usa en filmina 6)

- El proceso se detiene en el primer resto r_i igual a 0.

- El proceso debe detenerse, porque cada resto no nulo es positivo y estrictamente menor que el anterior.

- Este procedimiento es conocido como el *algoritmo de Euclides*.

Teorema

Sean a y b enteros con $b > 0$, entonces el máximo común divisor es el último resto no nulo obtenido en el algoritmo de Euclides (r_k de la filmina anterior).

Idea de la demostración

$r_{i-1} = r_i q_i + r_{i+1} \Rightarrow \operatorname{mcd}(r_{i-1}, r_i) = \operatorname{mcd}(r_i, r_{i+1})$. Luego,

$$\begin{aligned}\operatorname{mcd}(a, b) = \operatorname{mcd}(r_0, r_1) = \operatorname{mcd}(r_1, r_2) = \cdots \\ \cdots = \operatorname{mcd}(r_{k-1}, r_k) = \operatorname{mcd}(r_k, 0) = r_k. \quad \square\end{aligned}$$

Ejemplifiquemos el algoritmo de Euclides.

Ejemplo

Encuentre el mcd de 2406 y 654.

Solución

Tenemos

$$
\begin{array}{rll}
2406 = 654 \cdot 3 + 444, & \text{entonces} & (2406, 654) = (654, 444) \\
654 = 444 \cdot 1 + 210, & \text{entonces} & (654, 444) = (444, 210) \\
444 = 210 \cdot 2 + 24, & \text{entonces} & (444, 210) = (210, 24) \\
210 = 24 \cdot 8 + 18, & \text{entonces} & (210, 24) = (24, 18) \\
24 = 18 \cdot 1 + 6, & \text{entonces} & (24, 18) = (18, 6) \\
18 = 6 \cdot 3 + 0 & \text{entonces} & (18, 6) = (6, 0) = 6
\end{array}
$$

Por lo tanto $(2406, 654) = 6$.

- El algoritmo de Euclides es fácilmente implementable en un lenguaje de programación.

- A continuación una versión del mismo en pseudocódigo (estilo Python).

Algoritmo de Euclides

```
# pre: a y b son números positivos
# post: obtenemos d = mcd(a,b)
i, j = a, b
while j != 0:
    # invariante: mcd(a, b) = mcd(i, j)
    resto = i % j  # i = q * j + resto
    i, j = j, resto
d = i
```

Sean $a, b \in \mathbb{Z}$, uno de ellos no nulo, entonces

$$d = sa + tb.$$

Calculemos s y t. En el caso que $b > 0$, la ecuación (e_i) de la filmina 2 es:

$$r_{i-1} = r_i q_i + r_{i+1}$$

Esto implica que

$$r_{i+1} = r_{i-1} - r_i q_i.$$

Lo cual nos dice que r_i puede ser calculado usando r_{i-1} y r_{i-2}.

$$\begin{array}{rl} r_k & \text{puede ser calculado con } r_{k-1} \text{ y } r_{k-2} \\ r_{k-1} & \text{puede ser calculado con } r_{k-2} \text{ y } r_{k-3} \\ \dots & \dots \\ r_3 & \text{puede ser calculado con } r_2 \text{ y } r_1 \\ r_2 & \text{puede ser calculado con } r_1 = b \text{ y } r_0 = a \end{array}$$

Ejemplo

Encuentre d, el mcd de 174 y 72 y escribir $d = s \cdot 174 + t \cdot 72$.

Solución

$$
\begin{aligned}
174 &= 72 \cdot 2 + 30, &\Rightarrow\quad 30 &= 174 - 72 \cdot 2 &(1)\\
72 &= 30 \cdot 2 + 12, &\Rightarrow\quad 12 &= 72 - 30 \cdot 2 &(2)\\
30 &= 12 \cdot 2 + 6, &\Rightarrow\quad 6 &= 30 - 12 \cdot 2 &(3)\\
12 &= 6 \cdot 2 + 0.
\end{aligned}
$$

Por lo tanto, $(174, 72) = 6$ y,

$$
\begin{aligned}
6 &\overset{(3)}{=} 30 - 12 \cdot 2 \\
&\overset{(2)}{=} 30 - (72 - 30 \cdot 2) \cdot 2 \\
&= 5 \cdot 30 + (-2) \cdot 72 \\
&\overset{(1)}{=} 5 \cdot (174 - 72 \cdot 2) + (-2) \cdot 72 \\
&= 5 \cdot 174 + (-12) \cdot 72
\end{aligned}
$$

Concluyendo:

- $(174, 72) = 6$ y,
- $6 = 5 \cdot 174 + (-12) \cdot 72$.

$\square$

Ejemplo

Encuentre d, el mcd de 470 y 55 y escribir $d = s \cdot 470 + t \cdot 55$.

Solución

Por el algoritmo de Euclides obtenemos

$$\begin{aligned}
470 &= 55 \cdot 8 + 30 &\Rightarrow\quad & 30 = 470 + (-8) \cdot 55 &\quad (1)\\
55 &= 30 \cdot 1 + 25 &\Rightarrow\quad & 25 = 55 + (-1) \cdot 30 &\quad (2)\\
30 &= 25 \cdot 1 + 5 &\Rightarrow\quad & 5 = 30 + (-1) \cdot 25 &\quad (3)\\
25 &= 5 \cdot 5 + 0.
\end{aligned}$$

Luego

$$\begin{aligned}
5 &\stackrel{(3)}{=} 30 + (-1) \cdot 25\\
&\stackrel{(2)}{=} 30 + (-1) \cdot (55 + (-1) \cdot 30) = 2 \cdot 30 + (-1) \cdot 55\\
&\stackrel{(1)}{=} 2 \cdot (470 + (-8) \cdot 55) + (-1) \cdot 55 = 2 \cdot 470 + (-17) \cdot 55 \qquad \square
\end{aligned}$$

Mínimo común múltiplo

Definición

Si a y b son enteros decimos que un entero no negativo m es el *mínimo común múltiplo*, o *mcm*, de a y b si

a) $a|m$ y $b|m$;

b) si $a|n$ y $b|n$ entonces $m|n$.

- La condición (a) nos dice que m es múltiplo común de a y b.
- La condición (b) nos dice que cualquier otro múltiplo de a y b también debe ser múltiplo de m.

Ejemplo

Hallemos el mínimo común múltiplo entre 8 y 14.

Solución

Escribamos los múltiplos de ambos números y busquemos el menor común a ambos.

Los primeros múltiplos de 8 son: $8, 16, 24, 32, 40, 48, 56, \ldots$.

Los primeros múltiplos de 14 son: $14, 28, 42, 56, 72, \ldots$.

Luego se tiene $\text{mcm}(8, 14) = 56$. Nos faltaría comprobar que cualquier múltiplo de 8 y 14 es múltiplo de 56, pero eso se deduce fácilmente de los resultados que veremos a continuación.

Teorema

Sean a y b enteros no nulos, entonces

$$\mathrm{mcm}(a, b) = \frac{ab}{\mathrm{mcd}(a, b)}.$$

En particular este resultado implica que si a y b son enteros coprimos, entonces $\mathrm{mcm}(a, b) = ab$.

Ejemplo

Encontrar el mcm de 8 y 14.

Solución

Es claro que $2 = \mathrm{mcd}(8, 14)$, luego $\mathrm{mcm}(8, 14) = 8 \cdot 14/2 = 56$.

Ejercicio

Demostrar que si a, b y n son enteros no nulos, entonces $\operatorname{mcd}(na, nb) = n \operatorname{mcd}(a, b)$.

Solución

Sea $d = (a, b)$, debemos probar que $nd = (na, nb)$.

a) $d|a$ y $d|b$;

b) si $c|a$ y $c|b$ entonces $c|d$.

$$\Downarrow$$

a') $nd|na$ y $nd|nb$;

b') si $c|na$ y $c|nb$ entonces $c|nd$.

a')
Por a), $a = d \cdot q_1$, $b = d \cdot q_2$, luego

$$na = d \cdot nq_1, \quad nb = d \cdot nq_2,$$

es decir

$$nd | na, \quad nd | nb.$$

b')
Sea c tal que $c | na$ y $c | nb$.

Ahora bien

$$d = ra + sb \Rightarrow nd = s(na) + t(nb),$$

Luego,

$$c | na, c | nb \Rightarrow c | s(na) + t(nb) = nd.$$

Esto prueba b'). $\square$