MATEMÁTICA DISCRETA

Máximo Común Divisor (MCD). Algoritmo de Euclides

- Propiedades de los números enteros.
- Máximo Común Divisor (MCD). Algoritmo de Euclides.

Propiedades de los números enteros.

Ejercicio

Sean $a, b \in \mathbb{Z}^+$. Demuestra que si $b \mid a$ y $b \mid (a+2)$, entonces $b = 1$ ó $b = 2$.

Solución:

Si $b \mid a$, entonces $b \mid -a$, y como $b \mid (a+2)$, entonces:

$b \mid [-a + (a+2)] \ \to b \mid 2$. Por tanto, $b = 1$ ó $b = 2$ debido a que $b \in \mathbb{Z}^+$.

Ejercicio

Sean $p, q \in \mathbb{Z}^+$ números primos. Demuestra que si $p \mid q$, entonces $p = q$.

Solución:

Como q es primo y p es un divisor de q, entonces $p = 1$ ó $p = q$.

Como p es primo, entonces $p > 1$. Por tanto $p = q$.

Ejercicio

Expresa el número 13874945 en base hexadecimal.

Solución:

16 | 13,874,945	
16 | 867,184	1
16 | 54,199	0
16 | 3,387	7
16 | 211	11 (=B)
16 | 13	3
0	13 (=D)

Por tanto, $13874945 = D3B701_{16}$.

Máximo Común Divisor (MCD). Algoritmo de Euclides.

Definición

Sean $a,b \in \mathbb{Z}$ tal que o bien $a \neq 0$ ó $b \neq 0$. Se dice que $c \in \mathbb{Z}^+$ es el *máximo común divisor* de a y b, y se denota $c = mcd(a,b)$ ó $c = MCD(a,b)$, si:

(i) $c \mid a$ y $c \mid b$ (i.e., c es un divisor común de a y b).

(ii) cualquier otro divisor común de a y b también es un divisor de c.

Teorema

Para todo $a,b \in \mathbb{Z}^+$, siempre existe un único $c \in \mathbb{Z}^+$ que es el máximo común divisor de a y b.

Definición

Sean $a,b \in \mathbb{Z}$. Se dice que a y b son *primos relativos* si:

- $mcd(a,b) = 1$ (i.e., existen $x,y \in \mathbb{Z}$ tal que $ax + by = 1$).

Ejemplo

Para cada declaración, diga si es V o F.

- Si dos números son primos relativos, entonces son primos. F
- Si dos números son primos, entonces son primos relativos. V

Ejemplo

Calcula $mcd(42,70)$.

Solución: Los divisores comunes de 42 y 70 son: $1,2,7$ y 14. Por tanto $mcd(42,70) = 14$.

Cálculo de $mcd(a,b)$ por el método de fuerza bruta.

- Descomponer en factores primos a y b.
- Seleccionar los factores primos comunes.

Este método no es computacionalmente eficiente.

Ejemplo

Calcula $mcd(50,125)$.

Solución:

$50 = 2 \cdot 5^2$. $\qquad 125 = 5^3$.

Por tanto, $mcd(50,125) = 5^2 = 25$.

Propiedad fundamental

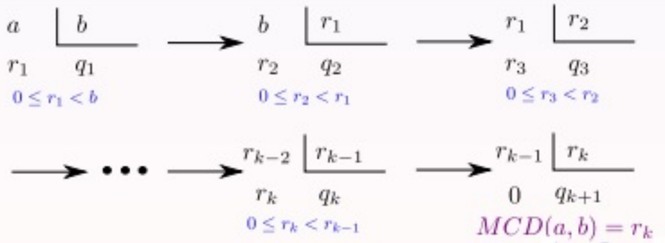
Sean $a, b \in \mathbb{Z}$, $|a| \geq |b|$, y sea r el resto de dividir a entre b ($a = b \cdot q + r$), entonces:

- Los divisores comunes de a y de b también lo son de r.
- Los divisores comunes de b y de r también lo son de a.

Por tanto $MCD(a, b) = MCD(b, r)$.

Algoritmo de Euclides

Se aplica reiteradamente la propiedad anterior hasta obtener un resto 0.



Ejemplo

Calcula $mcd(111,250)$.

Solución:

$$
\begin{aligned}
250 &= 2(111)+28 &\quad 0<28<111.\\
111 &= 3(28)+27 &\quad 0<27<28.\\
28 &= 1(27)+1 &\quad 0<1<27.\\
27 &= 1(27)+0.
\end{aligned}
$$

Por tanto, $mcd(111,250)=1$.

Ejemplo

Sea $n \in \mathbb{Z}^+$. Demuestra que los enteros positivos $5n+2$ y $8n+3$ son primos relativos.

Solución:

$5n+2$ y $8n+3$ son primos relativos si y solo si $mcd(5n+2, 8n+3) = 1$.

$$
\begin{aligned}
8n+3 &= 1(5n+2)+(3n+1), && 0 < 3n+1 < 5n+2.\\
5n+2 &= 1(3n+1)+(2n+1), && 0 < 2n+1 < 3n+1.\\
3n+1 &= 1(2n+1)+n, && 0 < n < 2n+1.\\
2n+1 &= 2(n)+1, && 0 < 1 < n.\\
n &= n(1)+0.
\end{aligned}
$$

Por tanto, $mcd(5n+2, 8n+3) = 1$.