Máximo común divisor

Definición

Sean $a, b \in \mathbb{Z}$. *Un número* d *se llama divisor común de* a *y* b *si*

$$d \mid a \text{ y } d \mid b.$$

Ejemplo

El conjunto de divisores de 24 es

$$\{-24, -12, -8, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 8, 12, 24\}$$

mientras que el conjunto de divisores de 36 es

$$\{-36, -18, -12, -9, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 9, 12, 18, 36\}.$$

El conjunto de divisores comunes de 24 y 36 es

$$\{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}.$$

Nótese que el máximo de los divisores comunes es 12.

Definición

Sean $a, b \in \mathbb{Z}$. El máximo común divisor de a y b se denota con $\gcd(a, b)$.

Ejemplo

$\gcd(24, 36) = 12$.

Es evidente que, para cualesquiera enteros a, b se cumple $\gcd(a, b) = \gcd(b, a)$. También que sólo necesitamos de los divisores positivos.

Ejemplo

¿Cuál el el máximo común divisor de 17 y 22?

Sol.

El conjunto de divisores positivos de 17 es:

$$\{1, 17\}$$

y los divisores positivos de 22 son

$$\{1, 2, 11, 22\}$$

entonces el conjunto divisores positivos comunes es: $\{1\}$, cuyo máximo es 1. Por lo tanto

$$\gcd(17, 22) = 1.$$

Definición

Sean $a, b \in \mathbb{Z}$. *Se dice que* a *es coprimo con* b *si* $\gcd(a, b) = 1$.

Ejemplo

Los números 17 *y* 22 *son coprimos, también* 2 *y* 3 *son coprimos.*

Lema

Si $a \in \mathbb{Z}$, *entonces* $\gcd(a, 0) = |a|$.

Demostración.

Podemos poner como divisores positivos de a a

$$D = \{1, \ldots, |a|\}.$$

Mientras que los divisores positivos de 0 son todos los naturales no cero: $\mathbb{N}^*$. Luego, el conjunto de divisores comunes es $D \cap \mathbb{N}^* = D$ cuyo máximo es $|a|$. $\square$

Calcular el máximo común divisor usando sólo la definición como lo hemos estado haciendo es ineficiente. Es mejor usar el *algoritmo de Euclides* para el cálculo de gcd. Por ejemplo, digamos que queremos calcular $\gcd(91, 287)$. Deberíamos encontrar todos los d divisores comunes de 91 y 287, i.e.,

$$d \in \mathbb{Z} \text{ tales que } d \mid 91 \text{ y } d \mid 287.$$

En lugar de escribir la lista de tales, le aplicamos el algoritmo de la división a 91 y 287:

$$287 = 3 * 91 + 14.$$

Esto es útil porque entonces se obtiene que los divisores comunes de 91 y 287 son los mismos que los divisores comunes de 91 y el residuo 14. En efecto: si $d \mid 91$ y $d \mid 287$ entonces $d \mid \underbrace{287 - 3 * 91}_{14}$ y $d \mid 91$. Recíprocamente, si $d \mid 14$ y $d \mid 91$ entonces, del Corolario **??** obtenemos que $d \mid \underbrace{(3 * 91 + 14)}_{287}$ y $d \mid 91$.

Por lo anterior podemos poner

$$\gcd(287, 91) = \gcd(91, 14).$$

Hemos reducido el problema a calcular $\gcd(91, 14)$. Repetimos el mismo argumento ahora para 91 y 14. Le aplicamos el algoritmo de la división a 91 y 14:

$$91 = 6 * 14 + 7.$$

Entonces los divisores comunes de 91 y 14 son los mismos divisores comunes que los de 7 y 14. En efecto, si $d \mid 91$ y $d \mid 14$ entonces $d \mid \underbrace{91 - 6 * 14}_{7}$ y $d \mid 14$. Recíprocamente, si $d \mid 7$ y $d \mid 14$ entonces $d \mid \underbrace{(6 * 14 + 7)}_{91}$ y $d \mid 14$.

Por lo tanto $\gcd(91, 14) = \gcd(14, 7)$. Ahora aplicamos el algoritmo de la división a 14 y 7:

$$14 = 2 * 7 + 0,$$

y procedemos como antes, para obtener que $\gcd(14, 7) = \gcd(7, 0)$. Pero sabemos del Lema 1 que $\gcd(7, 0) = 7$ y ya terminamos.

En resumen, obtuvimos la siguiente cadena de igualdades:

$$\begin{aligned}\gcd(287, 91) &= \gcd(91, 14)\\ &= \gcd(14, 7)\\ &= \gcd(7, 0)\\ &= 7.\end{aligned}$$

Nótese que finalmente el máximo común divisor se obtuvo del residuo antes de obtener residuo cero.
El procedimiento anterior es esencialmente el algoritmo de Euclides que hace uso repetitivo del siguiente hecho.

Lema

Sean a, b, q, r enteros tales que

$$a = qb + r.$$

Entonces

$$\gcd(a, b) = \gcd(b, r).$$

Demostración. Sea D_1 el conjunto de divisores comunes de a y b. Sea D_2 el conjunto de divisores comunes de b y r. Probaremos primero que $D_1 = D_2$ por contenciones. En efecto:

$D_1 \subseteq D_2$: si $d \in D_1$ entonces $d \mid a$ y $d \mid b$, luego por el Corolario **??**, $d \mid \underbrace{a - qb}_{r}$ y $d \mid b$, esto es d es un divisor común de b y r, lo que indica $d \in D_2$.

$D_2 \subseteq D_1$: si $d \in D_2$ entonces $d \mid b$ y $d \mid r$ y de nuevo obtenemos que $d \mid \underbrace{qb + r}_{a}$ y $d \mid b$. Lo que significa que d es

divisor común de a y b, i.e., $d \in D_1$.
Por lo tanto

$$\begin{aligned} \gcd(a,b) &= \max D_1, && \text{por definición de gcd,} \\ &= \max D_2 \\ &= \gcd(b,r). \end{aligned}$$

Ejemplo

Encontrar el máximo común divisor de 414 y 662.

Sol. Usamos el algoritmo de Euclides:

$$
\begin{array}{rr}
 & 1 \\
414 & \overline{)662} \\
 & 248
\end{array}
$$

$$
\begin{array}{rr}
 & 1 \\
248 & \overline{)414} \\
 & 166
\end{array}
$$

$$
\begin{array}{rr}
 & 1 \\
166 & \overline{)248} \\
 & 82
\end{array}
$$

$$
\begin{array}{rr}
 & 2 \\
82 & \overline{)166} \\
 & 2
\end{array}
$$

$$\begin{array}{rl} & 41 \\ 2 & \overline{)82} \\ & 0 \end{array}$$

Por lo tanto

$$\gcd(414, 662) = 2.$$

Tarea

1. *¿A cuáles de los siguientes* 17 *divide?* $68, 84, 357, 1001$.
2. *Sean* a, b, c, d *enteros.*
   - 2.1 *Muestre que si* $a \mid b$ *y* $b \mid a$ *entonces* $a = b$ *ó* $a = -b$.
   - 2.2 *Muestre que si* $a \mid b$ *y* $c \mid d$ *entonces* $ac \mid bd$.
   - 2.3 *Muestre que si* $ac \mid bc$ *y* $c \neq 0$ *entonces* $a \mid b$.
3. *Cuáles son el cociente y el residuo cuando*
   - 3.1 44 *is dividido por* 88*?*
   - 3.2 -123 *es dividido por* 19*?*
   - 3.3 -1 *es dividido por* 23*?*
   - 3.4 0 *es dividido por* 17*?*

Tarea

1. *Evaluar*
   1.1 $-17 \mod 2$
   1.2 $144 \mod 7$
   1.3 $-101 \mod 13$
2. *Determine cuáles de los siguientes números es primo:* $19, 27, 93, 101, 107, 113$
3. *Encuentre la factorización en primos de cada uno de los siguientes:* $88, 126, 729, 1001, 1111$
4. *Encuentre la factorización en primos de* $10!$