EL ALGORITMO DE EUCLIDES Y ALGUNAS APLICACIONES

1. El máximo común divisor de dos números

Como sabes, el máximo común divisor de dos números no nulos $a, b \in \mathbb{Z}$ es el más grande de sus divisores comunes. Por ejemplo, en el caso $a = -60$, $b = 24$, las dos listas de divisores son

$$\operatorname{div}(-60) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60\}$$
$$\operatorname{div}(24) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$$

por lo que

$$\operatorname{div}(-60) \cap \operatorname{div}(24) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

así que se tiene $\operatorname{mcd}(-60, 24) = 12$.

Observa que el máximo común divisor es, por definición, positivo, y observa también que $\operatorname{mcd}(a, b) = \operatorname{mcd}(-a, b) = \operatorname{mcd}(a, -b) = \operatorname{mcd}(-a, -b)$.

En la escuela primaria se aprende a calcular el máximo común divisor mediante el siguiente procedimiento:

(1) Se descomponen ambos números como producto de factores primos.
(2) Se calcula el máximo común divisor como el producto de los números primos comunes a ambas factorizaciones, elevados al menor de los dos exponentes que tienen en las dos factorizaciones.

Por ejemplo, para $a = -60$ y $b = 24$:

(1) $-60 = -2^2 \cdot 3 \cdot 5, \quad 24 = -2^3 \cdot 3$
(2) $\operatorname{mcd}(-60, 24) = 2^2 \cdot 3 = 12$

Sin embargo, encontrar la factorización de un número como producto de números primos es una tarea enormemente costosa desde el punto de vista computacional. Es por eso por lo que el método que aprendiste en primaria es en general muy poco eficiente.

En su lugar, es posible calcular $\operatorname{mcd}(a, b)$ de otro modo, mediante un procedimiento conocido como algoritmo de Euclides, consistente en una sucesión de divisiones entre números enteros (divisiones euclídeas). Antes de describirlo, conviene formalizar qué entendemos por división euclídea (o división entera) entre dos números enteros:

2. La división euclídea en el anillo $\mathbb{Z}$ de los números enteros

Una propiedad que se enseña en la escuela para números a, b naturales, pero que en realidad funciona igual con enteros, es:

> **Teorema (de la división euclídea en $\mathbb{Z}$)**
> Dados dos números enteros $a, b \in \mathbb{Z}$ con $b \neq 0$ existe un único par de números enteros $q, r \in \mathbb{Z}$ tales que $a = q \cdot b + r$, sujetos a la condición $0 \leq r < |b|$.

Se conoce a q y a r como el cociente y el resto, respectivamente, de la división euclidea o división entera de a entre b.

Por ejemplo $70 = (-7) \cdot (-9) + 7$, así que la división de 70 entre -9 da cociente -7 y resto 7 (observa que $7 < |-9| = 9$).

3. Descripción del algoritmo de Euclides

Para calcular texto mcd(a, b) se realiza la siguiente serie de divisiones:

$$a = q_1 b + r_1 \text{ con } 0 \leq r_1 < |b| \text{ (división entera de } a \text{ entre } b\text{, resto } r_1)$$

Si $r_1 > 0$ se sigue con

$$b = q_2 r_1 + r_2 \text{ con } 0 \leq r_2 < r_1 < |b| \text{ (división entera de } b \text{ entre } r_1\text{, resto } r_2)$$

Si $r_2 > 0$ se sigue con

$$r_1 = q_3 r_2 + r_3 \text{ con } 0 \leq r_3 < r_2 < r_1 < |b| \text{ (división entera de } r_1 \text{ entre } r_2\text{, resto } r_3)$$

$$\vdots$$

Como la sucesión de restos no negativos $r_1 > r_2 > \cdots \geq 0$ es estrictamente decreciente, en una cantidad finita de pasos se llega a la situación siquiente:

$$\vdots$$

$r_{k-2} = q_k r_{k-1} + r_k$ con $0 \leq r_k < \cdots < r_2 < r_1 < |b|$ (división entera de r_{k-2} entre r_{k-1}, resto r_k no nulo)
pero

$$r_{k-1} = q_{k+1} r_k \text{ (división entera de } r_{k-1} \text{ entre } r_k \text{ ya da resto nulo)}$$

Entonces r_k, el último resto no nulo del algoritmo, resulta ser el mcd(a, b) (se ocuparán de demostrarte esto con rigor en la asignatura de Conjuntos y Números en breve, si no lo han hecho ya).

En resumen:

Algoritmo de Euclides:

Tras la serie de divisiones euclídeas

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ &\vdots \\ r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k \end{aligned}$$

en las que r_k es el último resto no nulo, $\mathrm{mcd}(a, b) = r_k$.

4. La identidad de Bézout

Un resultado famoso de aritmética elemental es el siguiente:

Teorema.- Si d es el máximo común divisor de dos números enteros a y b entonces existen $x, y \in \mathbb{Z}$ tales que $ax + by = d$.

Se conoce a esta igualdad como identidad de Bézout.

Un método sistemático que permite encontrar dos valores concretos x, y que realicen la identidad de Bézout para a y b dados consiste en darle la siguiente vuelta de tuerca al algoritmo de Euclides:

5. El algoritmo de Euclides extendido

Supongamos que el algoritmo de Euclides produce las siguientes identidades hasta llegar al resto $r_k = \mathrm{mcd}(a, b)$:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ &\vdots \\ r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k \end{aligned}$$

Ahora, podemos usar esta sucesión de igualdades para ir expresando, en cada paso, el correspondiente resto como combinación lineal de a y b:

- $a = q_1 b + r_1 \Rightarrow r_1 = a \cdot 1 + b \cdot (-q_1)$, es decir
$$r_1 = ax_1 + by_1 \quad \text{con } x_1 = 1 \text{ e } y_1 = -q_1$$
- $b = q_2 r_1 + r_2 \Rightarrow r_2 = -q_2 r_1 + b = (0 - q_2 x_1)a + (1 - q_2 y_1)b$, es decir
$$r_2 = ax_2 + by_2 \quad \text{con } x_2 = (0 - q_2 x_1) \text{ e } y_2 = (1 - q_2 y_1)$$
- $r_1 = q_3 r_2 + r_3 \Rightarrow r_3 = -q_3 r_2 + r_1 = -q_3(ax_2 + by_2) + (ax_1 + by_1) = (x_1 - q_3 x_2)a + (y_1 - q_3 y_2)b$, es decir
$$r_3 = ax_3 + by_3 \quad \text{con } x_3 = ((x_1 - q_3 x_2) \text{ e } y_3 = (y_1 - q_3 y_2)$$
- $r_2 = q_4 r_3 + r_4 \Rightarrow r_4 = -q_4 r_3 + r_2 = -q_4(ax_3 + by_4) + (ax_2 + by_2) = (x_2 - q_4 x_3)a + (y_2 - q_4 y_3)b$, es decir
$$r_4 = ax_4 + by_4 \quad \text{con } x_4 = ((x_2 - q_4 x_3) \text{ e } y_4 = (y_2 - q_4 y_3)$$

Si se continua este proceso, eventualmente se llega a

$$r_k = ax_k + by_k \quad \text{con } x_k = x_{k-2} - q_k x_{k-1},\ y_k = y_{k-2} - q_k y_{k-1}$$

y como $r_k = \text{mcd}(a, b)$ los valores $x = x_k$, $y = y_k$ realizan la identidad de Bézout $\text{mcd}(a, b) = ax + by$.

En resumen, ¿qué se necesita para producir los valores finales x_k, y_k?

Método 1 (para una realización concreta de la identidad de Bézout):

- Se calcula la sucesión de cocientes $q_1, q_2, \ldots, q_k$ del algoritmo de Euclides.
- Se define un proceso iterativo para ir generando los sucesivos x's e y's. Si te fijas, cada uno depende de los dos anteriores vía las identidades
$$x_j = x_{j-2} - q_j x_{j-1}, \quad y_j = y_{j-2} - q_j y_{j-1}$$
y para echar a andar la iteración basta definir $x_0 = 0$, $x_1 = 1$, $y_0 = 1$, $y_1 = -q_1$. Observa que esa aparentemente extraña definición de x_0 e y_0 hace que la regla iterativa que acabamos de dar produzca para x_2 e y_2 los valores correctos descritos arriba (y, a partir de ahí, los consiguientes para $k > 2$).

6. Resolución de ecuaciones diofánticas lineales

Se conoce como ecuaciones diofánticas a aquellas ecuaciones que sólo involucran números enteros, y para las que se buscan soluciones que sean números enteros.

Por ejemplo, la ecuación diofántica de dos variables $2x + 3y = 1$ admite como solución a $x = -1$, $y = 2$.

Sin embargo, no existen dos números enteros x, y para los que se cumpla la igualdad $-60x+24y = 13$. La razón es que el miembro de la izquierda es necesariamente un múltiplo de $\text{mcd}(-60, 24) = 12$, y el miembro de la derecha no lo es.

En general, se tiene el siguiente:

Teorema.- La ecuación diofántica lineal $ax + by = c$ tiene solución si y sólo si $d = \text{mcd}(a, b)$ divide a c.

Cuando existen soluciones, una estrategia para encontrar una solución particular a la ecuación $ax + by = c$ es la siguiente:

(1) Si $d = \text{mcd}(a, b)$, denotemos $a = a'd$, $b = b'd$, $c = c'd$, de modo que $a'x + b'y = c'$ es la ecuación resultante de dividir ambos miembros de la ecuación original entre d.
(2) Como a' y b' ya no tienen divisores comunes, $\text{mcd}(a', b') = 1$. Por la identidad de Bézout, existen enteros x', y' tales que $a'x' + b'y' = 1$.
(3) Se deduce que $a'(x'c') + b'(y'c') = c'$, y ahora multiplicando por d, se concluye que $a(x'c') + b(y'c') = c$.
(4) Es decir, $x_0 = x'c'$, $y_0 = y'c'$ es solución de la ecuación original $ax + by = c$.

En resumen:

Método 2 (para obtener una solución particular de una ecuación diofántica lineal):

Si denotamos $a' = \dfrac{a}{\text{mcd}(a, b)}$, $b' = \dfrac{b}{\text{mcd}(a, b)}$, encontramos x', y' tales que $a'x' + b'y' = 1$, y tomamos $x_0 = x'c'$, $y_0 = y'c'$ con $c' = \dfrac{c}{\text{mcd}(a, b)}$, habremos encontrado una solución particular $(x, y) = (x_0, y_0)$ de la ecuación diofántica lineal $ax + by = c$.

Recuerda que se puede obtener el par (x', y') mediante el método 1 descrito arriba.

Cómo podemos encontrar todas las soluciones, no solo una solución particular?

Observa que restando las dos identidades

$$\begin{aligned} ax + by &= c \\ ax_0 + by_0 &= c \end{aligned}$$

llegamos a

$$a(x - x_0) + b(y - y_0) = 0$$

así que, dividiendo entre $\mathrm{mcd}(a,b)$ y denotando, como antes, $a' = \dfrac{a}{\mathrm{mcd}(a,b)}$, $b' = \dfrac{b}{\mathrm{mcd}(a,b)}$, se llega a

$$a'(x - x_0) + b'(y - y_0) = 0$$

Como a' y b' no tienen factores comunes, se deduce que $(x - x_0)$ debe ser múltiplo de b' y que $(y - y_0)$ debe ser múltiplo de a'. Pero sustituyendo en la ecuación anterior $(x - x_0) = nb'$ e $(y - y_0) = ma'$ se llega a $m = -n$.

En resumen:

Método 3 (para obtener el conjunto de todas las soluciones de una ecuación diofántica lineal):

El conjunto de todas las soluciones de una ecuación diofántica lineal $ax + by = c$ en la que $\mathrm{mcd}(a,b)$ divide a c está dado por

$$\left\{(x,y) = \left(x_0 + n\frac{b}{d}, y_0 - n\frac{a}{d}\right) \mid n \in \mathbb{Z}\right\},$$

donde $d = \mathrm{mcd}(a,b)$ y (x_0, y_0) es una solución particular de la citada ecuación.

Recuerda que la solución particular (x_0, y_0) puede ser calculada por el método 2 descrito arriba.