El Algoritmo de Eulides

elescritoriodeenrique.com

Enrique Ferres

Bienvenidas al Escritorio de Enrique. En este artículo (bastante más teórico que otros) vamos a tratar un tema muy relacionado con mi anterior post Congruencias. Las matemáticas de la semana: la divisibilidad de números enteros, y como tema central se estudiará el Algoritmo de Euclides (aunque realmente es anterior a Euclides) como herramienta de división de números enteros.

Dado un número entero a, decimos que un entero d es divisor de a, o divide a a si existe otro entero b tal que $a = bd$, y se escribe $d|a$. Por ejemplo, un divisor de 12 es 6, porque $12 = 2 \cdot 6$, pues hemos encontrado un entero (2). Llamamos máximo común divisor de dos enteros $a,\ b$, al mayor divisor de entre todos los divisores comunes a a y b, y se denota por $\text{mcd}(a,\ b)$. Por ejemplo, $\text{mcd}(24,\ 18) = 6$. Los divisores de 24 son $1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 12,\ 24$ (y sus respectivos negativos), y los de 18 son $1,\ 2,\ 3,\ 6,\ 9,\ 18$ (y sus respectivos negativos). Los divisores comunes a ambos son $1,\ 2,\ 3,\ 6$ (y sus respectivos negativos), y el mayor de todos ellos es 6, por lo que es el máximo común divisor.

Una forma de encontrar $\text{mcd}(a,\ b)$ es calcular "a mano" todos los divisores, como en el párrafo anterior, y quedarnos con el mayor de los comunes a ambos, pero es un método muy largo y trabajoso (hay que pensar siempre en grande, cuando tenemos números enormes). Euclides en sus Elementos expuso un algoritmo para calcular el máximo común divisor basado en la fórmula que ya comenté en el artículo que he enlazado en la introducción de dividendo = divisor $\cdot$ cociente + resto. Antes de explicarlo, vamos a realizar unas observaciones.

1. Si $d|ab$ y $\text{mcd}(d,\ a) = 1$, entonces $d|b$. Además, si $d|a$, entonces $d|ab$, para cualquier entero b. Por ejemplo, como $5|5$, 5 divide a cualquier múltiplo de 5 ($5k,\ \forall k \in \mathbb{Z}$).

   El máximo común divisor de dos números es único. Esto quiere decir que no hay dos máximo común divisor diferentes. En matemáticas nada se deja a la imaginación, todo exige demostración; al fin y al cabo, a priori nada nos garantiza que esto tenga por qué ser así. La prueba es un argumento por reducción al absurdo suponiendo que existe otro máximo común divisor. Veámoslo. Sea d máximo común divisor de

a y de b (ninguno de ellos es 0), y sea c otro máximo común divisor. Como d es máximo común divisor de a y b, y como c es, en particular, divisor de ellos, también tiene que dividir a su máximo común divisor d. Por tanto, como lo divide es porque es, como mucho, tan grande como él: $c \leq d$. Por otra parte, podemos hacer el mismo argumento cambiando los papeles de c y d, obteniendo que $d \leq c$. De las dos desigualdades obtenemos que $c = d$. Esto constituye un absurdo, porque habíamos supuesto que eran distintos, así que concluimos que no lo son.

2. Otra observación que debemos hacer es que, si $a = b + c$ y $d|a,\ d|b$, entonces $d|c$. La razón es que si $d|a,\ d|b$, existen dos números $k_1,\ k_2$ tales que $a = dk_1,\ b = dk_2$. Si pasamos b al otro lado de la desigualdad restando, sustituimos a y b por sus nuevas expresiones y sacamos factor común d, nos queda que

$$a - b = dk_1 - dk_2 = d(k_1 - k_2) = d.$$

Como $k_1 - k_2$ es un número entero k, concluimos que $c = dk$. De esta forma, hemos encontrado un entero k que hace que al multiplicarlo por d nos dé c. Por tanto, $d|c$.

3. Esta última observación se puede generalizar al caso en que $a = bm + c$ y $d|a,\ d|bm$. Así que, si dividimos a entre b, con la fórmula

$$\text{dividendo} = \text{divisor} \cdot \text{cociente} + \text{resto}$$

denotando por c al cociente y r al resto, la fórmula es $a = bc + r$. Por lo que hemos descubierto hasta ahora, como $d = \text{mcd}(a,\ b)$, en particular es un divisor de ambos, es decir, $d|a,\ d|b$ (luego $d|bc$). De esta forma, $d|r$.

En matemáticas no hay una definición precisa de algoritmo, pero se podría definir como un proceso que, dados unos datos de entrada y realizando unas operaciones sistemáticas, se devuelven unos resultados de salida. El algoritmo de Euclides recibe como datos de entrada los enteros que se dividen $a,\ b$ y devuelve como salida el máximo común divisor. La clave de todo, que luego vamos a entender, es que $\text{mcd}(a,\ b) = \text{mcd}(b,\ r)$. Veamos la forma del algoritmo:

Supongamos que $a \geq b$ (si no, intercambiamos los papeles de a y b). El primer paso consiste en hacer la división de a entre b y escribirla en forma de $a = bc + r$, pero vamos a llamar al cociente c_1 y al resto r_1. Recordemos que el resto es siempre mayor o igual que 0 y menor que el divisor.

El siguiente paso es ver si el resto es 0. Si lo es, entonces $a = bc_1$ y b sería $\text{mcd}(a,\ b)$ (porque b sería divisor de a y no hay mayor divisor de b que b). Si $r_1 \neq 0$, dividimos b entre r_1 y lo escribimos como $b = r_1c_2 + r_2$. Este proceso se repite hasta encontrar un $r_n = 0$, y el máximo común divisor será r_{n-1}. Veámoslo bien escrito (suponiendo $a \geq b$):

$$a = bc_1 + r_1\ (0 \leq r_1 < b)$$

$$b = r_1c_2 + r_2\ (0 \leq r_2 < r_1)$$

$$r_1 = r_2c_3 + r_3\ (0 \leq r_3 < r_2)$$

$$\vdots$$

$$r_{n-3} = r_{n-2}c_{n-1} + r_{n-1}\ (0 \leq r_{n-2} < r_{n-1}).$$
$$r_{n-2} = r_{n-1}c_n\ (r_n = 0)$$

Para comprobar que este algoritmo es correcto hay que comprobar dos cosas: que va a terminar en algún momento y que $r_{n-1} = \text{mcd}(a,\ b)$. Pero antes vamos a ver un ejemplo.

Veamos quién es mcd(36, 174). Tal y como están dispuestos los números, 36 jugaría el papel de a y 174 el de b, pero como $36 < 174$, vamos a cambiar el orden, es decir, vamos a encontrar el mcd(174, 36) (que, obviamente, es igual).

$$174 = 36 \cdot 4 + 30\ (c_1 = 4,\ r_1 = 30).$$

Como $r_1 \neq 0$,

$$36 = 30 \cdot 1 + 6\ (c_2 = 1,\ r_2 = 6).$$

Como $r_2 \neq 0$,

$$30 = 6 \cdot 5\ (c_3 = 5,\ r_3 = 0).$$

$r_3 = 0$, luego

$$\text{mcd}(36,\ 174) = mcd(174,\ 36) = r_2 = 6.$$

La justificación de la terminación del algoritmo radica en que cada $r_{i+1} < r_i$ y en que todos los $r_i \geq 0$. Por lo que en cada iteración del algoritmo los restos se van haciendo cada vez más pequeños, hasta que no les queda otra que anularse.

Ver que $r_{n-1} = \text{mcd}(a,\ b)$ es un pelín más costoso. Por una parte hay que demostrar que r_{n-1} es divisor de a y b, y por otra hay que demostrar que si c es otro divisor común de a y b, entonces es más pequeño que r_{n-1}.

Para ver que r_{n-1} es divisor de a y b, comencemos por el final del algoritmo.

$r_{n-2} = r_{n-1}c_n$. Esto, junto con el hecho de que $r_{n-1} < r_{n-2}$, implica que $r_{n-1}|r_{n-2}$.

Ahora vamos al paso justo anterior del algoritmo sabiendo que $r_{n-1}|r_{n-2}$.

$r_{n-3} = r_{n-2}c_{n-1} + r_{n-1}$. Como r_{n-1} divide a ambos sumandos del lado derecho de la fórmula, existe $k_1 \in \mathbb{Z}$ tal que $r_{n-3} = r_{n-1}k_1$. Por tanto, $r_{n-1}|r_{n-3}$.

Si repetimos este proceso de abajo hacia arriba del algoritmo, en el primer paso del algoritmo tendríamos que r_{n-1} divide a r_1 y a b, luego divide a a. En conclusión: es divisor común de a y b.

Ahora, si suponemos que d es otro divisor común de a y b, por el primer paso del algoritmo, también va a ser divisor de r_1. En el segundo paso del algoritmo obtenemos que d es divisor de r_2 (por serlo de b y r_1). Reiterando el argumento hasta llegar al penúltimo paso, obtendríamos que d es divisor de r_{n-1}, lo que implica que $d < r_{n-1}$ y $r_{n-1} = \text{mcd}(a,\ b)$.

Como colofón para las más teóricas vamos a demostrar el Teorema Fundamental de la Aritmética, que dice que todo número entero se descompone como producto de números primos (de manera única). Por ejemplo, $12 = 2^2 \cdot 3$ (el primo 2 aparece elevado al cuadrado porque se está multiplicando dos veces, luego no deja de ser un producto de números

primos). La demostración es por inducción sobre el número.

Si $n = 2$, 2 ya es un número primo.

Sea $n > 2$. Si n es primo, ya habríamos terminado, porque la descomposición es ese mismo número. Si no es primo, entonces tiene algún divisor primo p de forma que $n = kp$. Por hipótesis de inducción, como $k < n,\ k$ se descompone en producto de números primos, $k = p_1 p_2 \cdots p_i$, luego $n = p_1 p_2 \cdots p_i p$.

Como véis, el algoritmo de Euclides es muy útil para calcular de forma eficiente el máximo común divisor. Espero que os haya gustado. Si es así, dejádmelo en los comentarios. ¡Hasta la próxima!