TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

2.4 El Algoritmo de Euclides

Se puede hallar el máximo común divisor de dos enteros alistando todos sus divisores positivos y eligiendo el mayor común a los dos; pero esto es engorroso para números grandes. En el séptimo libro de los *Elementos* se da un proceso más eficaz, involucrando la aplicación repetida del Algoritmo de División. Aunque hay evidencia histórica de que este método es anterior a Euclides, hoy se le conoce como el Algoritmo de Euclides.

El Algoritmos de Euclides se puede describirse de la siguiente manera: Sean a y b dos enteros cuyo máximo común divisor es deseado. Como $\text{mcd}(|a|, |b|) = \text{mcd}(a, b)$, no hay nada de malo en suponer que $a \geq b \geq 0$. El primer paso es aplicar el algoritmo de división a a y b y obtener

$$a = q_1 b + r_1 \text{ con } 0 \leq r_1 < b$$

Si pasa que $r_1 = 0$ entonces $b|a$ y $\text{mcd}(a, b) = b$. Cuando $r_1 \neq 0$, divide b por r_1 para producer enteros q_2 y r_2 tales que

$$b = q_2 r_1 + r_2 \text{ con } 0 \leq r_2 < r_1$$

Si $r_2 = 0$, entonces paramos; si no, procedemos como antes para obtener

$$r_1 = q_3 r_2 + r_3 \text{ con } 0 \leq r_3 < r_2$$

Este proceso de división continua hasta que un resto de cero aparece; digamos al paso $n + 1$ en donde r_{n-1} es dividido por r_n (un resto de cero ocurre tarde o temprano porque la sucesión decreciente $b > r_1 > r_2 > \cdots \geq 0$ no puede contener más que b enteros).

El resultado es el siguiente sistema de ecuaciones:

$$\begin{aligned}
a &= q_1 b + r_1 && 0 < r_1 < b \\
b &= q_2 r_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Argumentamos que r_n, el último resto no cero que aparece de esta manera, es igual a $\text{mcd}(a, b)$. Nuestra demostración esta basada en el lema siguiente.

Lema. Si $a = bq + r$, entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración: Si $d - \text{mcd}(a, b)$, entonces las relaciones $d|a$ y $d|b$ juntos implican que $d|(a - qb)$, o $d|r$. Por lo tanto, d es un divisor común de b y r. Por otro lado, si c es un divisor común arbitrario de b y r, entonces $c|(qb + r)$, y entonces $c|a$. Esto convierte al c un divisor común de a y b, de modo que $c \leq d$. Ahora resulta de la definición de $\text{mcd}(a, b)$ que $d = \text{mcd}(b, r)$.

Utilizando el resultado del lema, simplemente trabajamos el sistema de ecuaciones mostrado, obteniendo

$$\text{mcd}(a, b) = \text{mcd}(b, r_1) = \cdots = \text{mcd}(r_{n-1}, r_n) = \text{mcd}(r_n, 0) = r_n$$

como se afirma.

Teorema 2.3 afirma que $\text{mcd}(a, b)$ se puede expresar en la forma $ax + by$, pero la demostración de este teorema no da ninguna pista sobre cómo determinar los enteros x e y. Para esto, recurrimos al Algoritmo de Euclides. Empezando con la penultima ecuación que surge del algoritmo, escribimos

$$r_n = r_{n-2} - q_n r_{n-1}$$

Ahora resuelve la ecuación anterior para r_{n-1} y sustituye para obtener

$$\begin{aligned} r_n &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= (1 + q_n q_{n-1})r_{n-2} + (-q_n)r_{n-3} \end{aligned}$$

Esto representa r_n como una combinación lineal de r_{n-2} y r_{n-3}. Continuando hacia atrás a través del sistema de ecuaciones, eliminamos sucesivamente los restos $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$ hasta llegar a una etapa donde $r_n = \text{mcd}(a, b)$ se expresa como combinación lineal de a y b.

Ejemplo 2.3. Veamos como funciona el Algoritmo de Euclides en un caso concreto calculando, digamos, $\text{mcd}(12378, 3054)$. Las aplicaciones apropiadas del Algoritmo de División producen las ecuaciones

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0 \end{aligned}$$

Nuestra discusión anterior nos dice que el último resto no cero que aparece en estas ecuaciones, es decir el entero 6, es el máximo común divisor de 12378 y 3054:

$$6 = \text{mcd}(12378, 3054)$$

Para representar 6 como combinación lineal de los enteros 12378 y 3054, empezamos con la penultima de las ecuaciones mostradas y eliminamos sucesivamente los restos 18, 24, 138, y 162:

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 = (138 - 5 \cdot 24) \\ &= 6 \cdot 24 - 138 \\ &= 6(162 - 138) - 138 \\ &= 6 \cdot 162 - 7 \cdot 138 \\ &= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \\ &= 132 \cdot 162 - 7 \cdot 3054 \\ &= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \\ &= 132 \cdot 12378 + (-535)3054 \end{aligned}$$

Entonces tenemos

$$6 = \text{mcd}(12378, 3054) = 12378x + 3054y$$

en donde $x = 132$ e $y = -535$. Nota que esto no es el único modo de expresar el entero 6 como combinación lineal de 12378 y 3054; entre otras posibilidades, podríamos sumar y restar $3054 \cdot 12378$ para obtener

$$\begin{aligned} 6 &= (132 + 3054)12378 + (-535 - 12378)3054 \\ &= 3186 \cdot 12378 + (-12913)3054 \end{aligned}$$

El matemático francés Gabriel Lamé (1795-1870) demostró que el número de pasos requeridos en el Algoritmo de Euclides es como máximo cinco veces el número de dígitos en el entero menor. En Ejemplo 2.3, por ejemplo, el entero menor (es decir, 3054) tiene cuatro dígitos, de modo que el número total de divisiones no puede ser mayor que 20; en realidad solo se necesitaban seis divisiones. Otra observación de interés es que para cada $n > 0$, es posible hallar enteros a_n y b_n tales que se necesiten exactamente n divisiones para computar $\text{mcd}(a_n, b_n)$ por el Algoritmo de Euclides. Demostraremos este hecho en Capítulo 14.

Es necesario un comentario más. El número de pasos en el Algoritmo de Euclides se puede reducir a menudo seleccionando restos r_{k+1} tal que $|r_{k+1}| < r_k/2$, es decir, trabajando con mínimos restos absolutos en las divisiones. Entonces, repitiendo el Ejemplo 2.3, es más eficaz escribir

$$\begin{aligned} 12378 &= 4 \cdot 2054 + 162 \\ 3054 &= 19 \cdot 162 - 24 \\ 162 &= 7 \cdot 24 - 6 \\ 24 &= (-4)(-6) + 0 \end{aligned}$$

Como mostrado por este conjunto de ecuaciones, este schema es apto producir el negativo del valor del máximo común divisor de dos enteros (el último resto no cero siendo -6) en lugar el máximo común divisor si mismo.

Una consecuencia importante el Algoritmo de Euclides es el siguiente teorema:

Teorema 2.7. Si $k > 0$, entonces $\text{mcd}(ka, kb) = k\text{mcd}(a, b)$.

Demostración: Si cada una de las ecuaciones que aparecen en el Algoritmo de Euclides por a y b (ver página 1) es multiplicado por k, obtenemos

$$\begin{aligned} ak &= q_1(bk) + r_1k & 0 < r_1k < bk \\ bk &= q_2(r_1k) + r_2k & 0 < r_2k < r_1k \\ &\vdots \\ r_{n-2}k &= q_n(r_{n-1}k) + r_nk & 0 < r_nk < r_{n-1}k \\ r_{n-1}k &= q_{n+1}(r_nk) + 0 \end{aligned}$$

Pero esto es claramente el Algoritmo de Euclides aplicado a los enteros ak y bk, de modo que su máximo común divisor es el último resto no cero r_nK; es decir,

$$\text{mcd}(ka, kb) = r_nk = k\text{mcd}(a, b)$$

como afirmado en el teorema.

Corolario. Por cualquier entero $k \neq 0$, $\text{mcd}(ka, kb) = |k|\text{mcd}(a, b)$.

Demostración: Es suficiente considerar el caso en que $k < 0$. Entonces $-k = |k| > 0$ y, por Teorema 2.7,

$$\begin{aligned} \text{mcd}(ak, bk) &= \text{mcd}(-ak, -bk) \\ &= \text{mcd}(a|k|, b|k|) \\ &= |k|\text{mcd}(a, b) \end{aligned}$$

Una demostración alternativa del Teorema 2.7 corre muy rápidamente como sigue: $\text{mcd}(ak, bk)$ es el mínimo entero positivo de la forma $(ak)x + (bk)y$, lo cual

es, en torno, igual a k veces el mínimo entero positivo de la forma $ax + by$; el último valor iguala a $k\text{mcd}(a, b)$.

A modo de ilustración de la Teorema 2.7, veamos que

$$\text{mcd}(12, 30) = 3\text{mcd}(4, 10) = 3 \cdot 2\text{mcd}(2, 5) = 6 \cdot 1 = 6$$

Hay un concepto paralelo al del máximo común divisor de dos enteros, conocido como el mínimo común multiple; pero no tendremos muchas ocasiones de aprovecharlo. Un entero c es un *multiple común* de dos enteros no cero a y b siempre que $a|b$ y $a|c$. Evidentemente, cero es un multiple común de a y b. Para ver que existen multiples comunes que no son triviales, notamos que los productos ab y $-(ab)$ son multiples comunes de a y b, y uno es positivo. Por el Principio del Buen Orden, el conjunto de enteros positivos de a y b debe contener a un elemento mínimo; lo llamamos el mínimo común multiple de a y b.

Para que conste, aquí está la definición oficial.

Definición 2.4. El *mínimo común multiple* de dos enteros no cero a y b, denotado por $\text{mcm}(a, b)$, es el entero positivo que satisface lo siguiente:

a) $a|m$ y $b|m$.

b) Si $a|c$ y $b|c$, con $c > 0$, entonces $m \leq c$.

Como ejemplo, los multiples comunes positivos de los enteros -12 y 30 son $60, 120, 180, \ldots$; por lo tanto, $\text{mcm}(-12, 30) = 60$.

La siguiente observación se desprende claramente de nuestra discusión: dado enteros no cero a y b, $\text{mcm}(a, b)$ siempre existe y $\text{lcm}(a, b) \leq |ab|$.

Nos falta una relación entre las ideas de máximo común divisor y mínimo común multiple. Este vacío se llena con el Teorema 2.8.

Teorema 2.8. Para los enteros positivos a y b

$$\text{mcd}(a, b)\text{mcm}(a, b) = ab$$

Demostración: Para empezar, pon $d = \text{mcd}(a, b)$ y escribe $a = dr$, $b = ds$ para enteros r y s. Si $m = ab/d$, entonces $m = as = rb$, cuyo efecto es hacer m un divisor común (y positivo) de a y b.

Ahora sea r cualquier entero positivo que es un múltiple positivo de a y b; digamos $c = au = bv$. Como sabemos, existen enteros x e y tales que $d = ax + by$. En consecuencia,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \left(\frac{c}{b}\right) x + \left(\frac{c}{a}\right) y = vx + uy$$

Esta ecuación afirma que $m|c$, permitiéndonos concluir que $m \leq c$. Por lo tanto, de acuerdo con la Definición 2.4, $m = \text{mcm}(a, b)$; es decir,

$$\text{mcm}(a, b) = \frac{ab}{d} = \frac{ab}{\text{mcd}(a, b)}$$

que es lo que empezamos a demostrar.

La Teorema 2.8 tiene un corolario que merece una mención aparte.

Corolario. Para cualquier elección de enteros positivos a y b, $\text{mcm}(a, b) = ab$ si y solo si $\text{mcd}(a, b) = 1$.

Quizás la principal virtud de la Teorema 2.8 es que se hace el cálculo del mínimo común multiple de dos enteros dependiente del valor de su máximo común divisor - que, a su vez, se puede calcular a partir del Algoritmo de Euclides. Cuando consideramos los enteros positivos 3054 y 12378, por ejemplo, encontramos que $\text{mcd}(3054, 12378) = 6$; entonces

$$\text{mcm}(3054, 12378) = \frac{3054 \cdot 12378}{6} = 6300402$$

Antes de pasar a otros asuntos, observemos que la noción de máximo común divisor se puede extender a más que dos enteros en una forma obvia. En el caso de tres enteros, a, b, c, no todos cero, $\text{mcd}(a, b, c)$ se define como el entero positivo d con las siguientes propiedades:

a) d es un divisor de cada uno de a, b, c

b) Si e divide los enteros a, b, c, entonces $c \leq d$.

Citamos dos ejemplos:

$$\text{mcd}(39, 42, 54) = 3 \text{ y } \text{mcd}(49, 210, 350) = 7$$

Se advierte al lector que es posible que tres enteros sean coprimos como un triple (es decir, $\text{mcd}(a, b, c) = 1$), pero no coprimos en pares, como se muestra con los enteros 6, 10, y 15.

PROBLEMAS 2.4

1. Hallar $\text{mcd}(143, 227)$, $\text{mcd}(306, 657)$, y $\text{mcd}(272, 1479)$.

2. Utilizar el Algoritmo de Euclides para obtener enteros x e y satisfaciendo lo siguiente:
a) $\text{mcd}(56, 72) = 56x + 72y$.
b) $\text{mcd}(24, 138) = 24x + 138y$.
c) $\text{mcd}(119, 272) = 119x + 272y$.
d) $\text{mcd}(1769, 2378) = 1769x + 2378y$.

3. Demostrar que si d es un divisor común de a y b, entonces $d = \text{mcd}(a, b)$ si y solo si $\text{mcd}(a/d, b/d) = 1$.
[Consejo: Utilizar la Teorema 2.7.]

4. Suponiendo que $\text{mcd}(a, b) = 1$, demostrar lo siguiente:

a) $\text{mcd}(a+b, a-b) = 1$ o 2.
[Consejo: Sea $d = \text{mcd}(a+b, a-b)$ y demostrar que $d|2a$, $d|2b$, y por lo tanto que $d \leq \text{mcd}(2a, 2b) = 2\text{mcd}(a, b)$.]
b) $\text{mcd}(2a+b, a+2b) = 1$ o 3.
c) $\text{mcd}(a+b, a^2+b^2) = 1$ o 2.
[Consejo: $a^2+b^2 = (a+b)(a-b)+2b^2$.]
d) $\text{mcd}(a+b, a-b) = 1$ o 2.
[Consejo: $a^2-ab+b^2 = (a+b)^2-3ab$.]

5. Para $n \geq 1$ y enteros positivos a y b, demostrar lo siguiente:
a) Si $\text{mcd}(a, b) = 1$, entonces $\text{mcd}(a^n, b^n) = 1$.
[Consejo: Ver Problema 20a), Sección 2.2.]
b) La relación $a^n|b^n$ implica que $a|b$.
[Consejo: Poner $d = \text{mcd}(a, b)$ y escribir $a = rd$, $b = sd$, en donde $\text{mcd}(r, s) = 1$. Por parte a), $\text{mcd}(r^n, s^n) = 1$. Demostrar que $r = 1$, y entonces $a = d$.]

6. Demostrar que si $\text{mcd}(a, b) = 1$, entonces $\text{mcd}(a+b, ab) = 1$.

7. Para enteros no cero a y b, verificar que las siguientes condiciones son equivalentes:
a) $a|b$.
b) $\text{mcd}(a, b) = |a|$.
c) $\text{mcm}(a, b) = |b|$.

8. Hallar $\text{lcm}(143, 227)$, $\text{lcm}(306, 657)$, y $\text{lcm}(272, 1479)$.

9. Demostrar que el máximo común divisor de dos enteros positivos divide a su mínimo común multiple.

10. Dado enteros no cero a y b, establecer los siguientes hechos relativos al $\text{mcm}(a, b)$:
a) $\text{mcd}(a, b) = \text{mcm}(a, b)$ si y solo si $a = \pm b$.
b) Si $k > 0$, entonces $\text{mcm}(ka, kb) = k\text{mcm}(a, b)$.
c) Si m es un multiple común de a y b, entonces $\text{mcm}(a, b)|m$.
[Consejo: Poner $t = \text{mcm}(a, b)$ y utilizar el Algoritmo de División para escribir $m = qt + r$, en donde $0 \leq r < t$. Demostrar que m es un multiple común de a y b.]

11. Sean a, b, c enteros, no hay dos de los cuales son cero, y $d = \text{mcd}(a, b, c)$. Demostrar que

$$d = \text{mcd}(\text{mcd}(a, b), c) = \text{mcd}(a, \text{mcd}(b, c)) = \text{mcd}(\text{mcd}(a, c), b)$$

12. Hallar enteros x, y, z satisfaciendo

$$\text{mcd}(198, 288, 512) = 198x + 288y + 512z$$

[Consejo: Poner $d = \text{mcd}(198, 228)$. Como $\text{mcd}(198, 288, 512) = \text{mcd}(d, 512)$, primero hallar enteros u y v tales que $\text{mcd}(d, 512) = du + 512v$.]