TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

2.3 El Máximo Común Divisor

De significado especial es en el caso en que el resto en el Algoritmo de División resulta ser cero. Analicemos esta situación ahora.

Definición 2.1. Un entero b es llamado *divisible* por un entero $a \neq 0$ (escrito $a|b$), si existe algún entero c tal que $b = ac$. Escribimos $a \nmid b$ para indicar que b no es divisible por a.

Entonces, por ejemplo, -12 es divisible por 4, porque $-12 = 4(-3)$. Sin embargo, 10 no es divisible por 3, como no hay entero c que hace que el anunciado $10 = 3c$ es verdadero.

Hay otro modo para expresar la relación de divisibilidad $a|b$. Podriamos decir que a es un *divisor* de b, o que a es un *factor* de b, o que b es un multiple de a. Nota que en Definición 2.1 hay una restricción en el divisor a: cada vez que se utiliza la notación $a|b$, se entiende que a es distinto de cero.

Si a es un divisor de b, entonces b también es divisible por $-a$ (en efecto, $b = ac$ implica que $b = (-a)(-c)$), y entonces los divisores de en entero siempre ocurren en pares. Para encontrar todos los divisores de un entero dado, es suficiente obtener los divisores positivos y después adjuntar los enteros negativos correspondientes. Por esta razón, normalmente nos limitamos a considerar los divisores positivos.

Sería útil alistar unas consecuencias inmediatas de la Definición 2.1. (Se recuerda nuevamente al lector que, aunque no se indica, supongamos que los divisores no son cero.)

Teorema 2.2. Para enteros a, b, y c, se mantiene lo siguiente:
a) $a|0$, $1|a$, y $a|a$.
b) $a|1$ si y solo si $a = \pm 1$.
c) Si $a|b$ y $c|d$, entonces $ac|bd$.
d) Si $a|b$ y $b|c$, entonces $a|c$.
e) $a|b$ y $b|a$ si y solo si $a = \pm b$.
f) Si $a|b$ y $b \neq 0$, entonces $|a| \leq |b|$.
g) Si $a|b$ y $a|c$, entonces $a|(bx + cy)$ para cualquier enteros x e y.

Demostración: Demostraremos afirmaciones f) y g), dejando los otros partes como ejercicios. Si $a|b$, entonces existe un entero c tal que $b = ac$; también, $b \neq 0$

indica que $c \neq 0$. Al tomar valores absolutos, tenemos $|b| = |ac| = |a||c|$. Como $c \neq 0$, se deduce que $|c| \geq 1$, y entonces $|b| = |a||c| \geq |a|$.

Con respecto a g), las relaciones $a|b$ y $a|c$ aseguran que $b = ar$ y $c = as$ por algunos enteros apropiados r y s. Pero entonces cualquier sea la elección de x e y,

$$bx + cy = arx + asy = a(rx + sy)$$

Como $rx + sy$ es un entero, esto dice que $a|(bx + cy)$, como se desee.

Vale la pena notar que propiedad g) del Teorema 2.2 se extiende por inducción a las sumas de más que dos términos. Es decir, si $a|b_k$ para $k = 1, 2, \ldots, n$, entonces

$$a|(b_1x_1 + b_2x_2 + \ldots b_nx_n)$$

para todos los enteros $x_1, x_2, \ldots, x_n$. Los pocos detalles requeridos son tan directos que los omitimos.

Si a y b son enteros arbitrarios, entonces un en entero d se llama un *divisor común* de a y b si $d|a$ y $d|b$. Como 1 es un divisor de cada entero, 1 es un divisor común de a y b; entonces su conjunto de divisores positivos comunes es no vacío. Ahora, cada entero divide a cero, y entonces si $a = b = 0$, entonces cada entero se sirve como divisor común de a y b. En esta instancia, el conjunto de divisores comunes es infinito. Sin embargo, cuando por lo menos uno de a o b es distinta de cero, hay solo un número finito de divisores positivos comunes. Entre estos, hay un máximo, llamada el máximo común divisor de a y b. Enmarcamos esto como Definición 2.2.

Definición 2.2. Sean a y b dos enteros dados, con por lo menos un distinto de cero. El *máximo común divisor* de a y b, denotado por $\text{mcd}(a, b)$, es el entero positivo d que satisface lo siguinte:

a) $d|a|$ y $d|b$,

b) Si $c|a$ y $c|b$, entonces $c \leq d$.

Ejemplo 2.2. Los divisores positivos de -12 son $1, 2, 3, 4, 6, 12$, mientras los de 30 son $1, 2, 3, 5, 6, 10, 15, 30$; entonces los divisores positivos comunes de -12 y 30 son $1, 2, 3, 6$. Como 6 es el mayor de estos enteros, resulta que $\text{mcd}(-12, 30) = 6$. Del mismo modo, podemos demostrar que

$$\text{mcd}(-5, 5) \text{ y } \text{mcd}(8, 17) = 1 \text{ y } \text{mcd}(-8, -36) = 4$$

El proximo teorema indica que $\text{mcd}(a, b)$ se puede representar como una combinación lineal de a y b. (Por combinación lineal nos referimos a una expresión de la forma $ax + by$, en donde x e y son enteros.) Esto se ilustra por, digamos,

$$\text{mcd}(-12, 30) = 6 = (-12)2 + 30 \cdot 1$$

o

$$\text{mcd}(-8, -36) = 4 = (-8)4 + (-36)(-1)$$

Ahora el teorema.

Teorema 2.3. Dado enteros a, y b, no ambos cero, existen enteros x e y tales que

$$\text{mcd}(x, y) = ax + by$$

Demostración: Consideramos el conjunto S de las combinaciones lineales positivas de a y b:

$$S = \{au + bv | au + bv > 0; u, v \text{ enteros}\}$$

Nota primero que S no es vacío. Por ejemplo, si $a \neq 0$, entonces el entero $|a| = au + b \cdot 0$ queda en S, en donde elegimos $u = 1$ o $u = -1$ según que a es positivo o negativo. Por el Principio del Buen Orden, S deber contener en elemento mínimo d. Entonces, de la definición de S, existen enteros x e y tales que $d = ax + by$. Afirmamos que $d = \text{mcd}(a, b)$.

Haciendo balance del Algoritmo de División, podremos obtener enteros q y r tales que $a = qd + r$, en donde $0 \leq r < d$. Entonces r se puede escribir en la forma

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$$

Si r fuera positivo, entonces esta representación implicaría que r es un miembro de S, contradiciendo el hecho que d es el entero mínimo en S (recordar que $r < d$). Por lo tanto, $r = 0$, y entonces $a = qd$, o equivalentemente $d|a$. Por un razonamiento similar, $d|b$, y entonces d es un divisor común de a y b.

Ahora, si c es un divisor común positiva cualquier de los enteros a y b, entonces parte g) del Teorema 2.2 nos permite concluir que $c|(ax + by)$, es decir, $c|d$. Por parte f) del mismo teorema, $c = |c| \leq |d| = d$, y entonces d es mayor que cada divisor común positivo de a y b. Uniendo los pedazos de información, veamos que $d = \text{mcd}(a, b)$.

Cabe señalar que el argumento anterior es solo una demostración de "existencia" y no provee un método practica para hallar los valores de x e y. Esto vendrá después.

Una lectura cuidadosa de la demostración del Teorema 2.3 revela que el máximo común divisor de a y b puede describirse como el mínimo entero positivo de la forma $ax + by$. Consideramos el caso en que $a = 6$ y $b = 15$. Aquí, el conjunto se convierte en

$$S = \{6(-2) + 15 \cdot 1, 6(-1) + 15 \cdot 1, 6 \cdot 1 + 15 \cdot 0, \dots\} = \{3, 9, 6, \dots\}$$

Observemos que 3 es el mínimo entero en S, y entonces $3 = \text{mcd}(6, 15)$.

El carácter de los miembros de S en esta ilustración sugiere otro resultado, que damos en el próximo corolario.

Corolario. Si a y b son enteros dados, no ambos cero, entonces el conjunto

$$T = \{ax + by | x, y, \text{ son enteros}\}$$

es precisamente el conjunto de todos los multiples de $d = \text{mcd}(a, b)$.

Demostración: Como $d|a$ y $d|b$, sabemos que $d|(ax+by)$ para todos enteros x, y. Entonces cada miembro de T es un multiple de d. Reciprocamente, d se puede escribir como $d = ax_0 + by_0$ por enteros apropiados x_0 e y_0, de modo que cualquier multiple nd de d es de la forma

$$nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0)$$

Entonces, nd es una combinación lineal de a y b, y, por definición, queda en T.

Puede suceder que 1 y -1 son los únicos divisores comunes de un par dado de enteros a y b, y por consiguiente $\text{mcd}(a, b) = 1$. Por ejemplo:

$$\text{mcd}(2, 5) = \text{mcd}(-9, 16) = \text{mcd}(-27, -35) = 1$$

Esta situación ocurre con suficiente frecuencia como para dar lugar a una definición.

Definición 2.3. Dos enteros a y b, no ambos cero, son llamados *coprimos* cada vez que $\text{mcd}(a, b) = 1$.

El siguiente teorema se caracteriza enteros coprimos en términos de combinaciones lineales.

Teorema 2.4 Sean a y b enteros, no ambos cero. Entonces a y b son coprimos si y solo si existen enteros x e y tales que $1 = ax + by$.

Demostración: Si a y b son coprimos de modo que $\text{mcd}(a, b) = 1$, entonces el Teorema 2.3 garantiza la existencia de enteros x e y tales que $1 = ax + by$. Por el reciproco, supongamos que $1 = ax + by$ por alguna elección de x e y, y que $d = \text{mcd}(a, b)$. Como $d|a$ y $d|b$, Teorema 2.2 nos da $d|(ax + by)$, o $d|1$. Ya que d es un entero positivo, esta última condición de divisibilidad obliga que d iguala a 1 (parte b) de Teorema 2.2 juega un papel aquí), y la conclusión deseada sigue.

Este resultado conduce a una observación que es útil en determinadas situaciones, a saber,

Corolario 1. Si $\text{mcd}(a, b) = d$, entonces $\text{mcd}(a/d, b/d) = 1$.

Demostración: Antes de empezar con la demostración, deberíamos observar que aunque a/d y b/d tiene el aspecto de fracciones, en realidad son enteros porque d es un divisor de a y b. Ahora, sabiendo que $\text{mcd}(a, b) = d$, es posible hallar enteros x e y tales que $d = ax+by$. Al dividir cada lado de esta ecuación por d, obtenemos

$$1 = \left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y$$

Como a/d y b/d son enteros, un llamamiento al teorema es legítima. La conclusión es que a/d y b/d son coprimos.

Por una ilustración del último corolario, observemos que $\text{mcd}(-12, 30) = 6$ y

$$\text{mcd}(-12/6, 30/6) = \text{mcd}(-2, 5) = 1$$

como debería ser.

No es verdad, sin añadir una condición extra, que $a|c$ y $b|c$ juntos dan $ab|c$. Por ejemplo, $6|24$ y $8|24$ pero $6 \cdot 8 \nmid 24$. Si 6 y 8 fueron coprimos, por supuesto, esta situación no se daría. Esto nos lleva al Corolario 2.

Corolario 2. Si $a|c$ y $b|c$, con $\text{mcd}(a, b) = 1$, entonces $ab|c$.

Demostración: Como $a|c$ y $b|c$, enteros r y s pueden ser encontrados tales que $c = ar = bs$. Ahora la relación $\text{mcd}(a, b) = 1$ nos permite escribir $1 = ax + by$ por alguna elección de enteros x e y. Multiplicando la última ecuación por c, parece que

$$c = c \cdot 1 = c(ax + by) = acx + bcy$$

Si hacemos las sustituciones apropiadas en el lado derecho, entonces

$$c = a(bs)x + b(ar)y = ab(sx + ry)$$

o, como un enunciado de divisibilidad, $ab|c$.

Nuestro próxima resultado parece bastante leve, pero es de importancia fundamental.

Teorema 2.5 El Lema de Euclides. Si $a|bc$, con $\text{mcd}(a, b) = 1$, entonces $a|c$.

Demostración: Otra vez, empezamos desde Teorema 2.3, escribiendo $1 = ax+by$, en donde x e y son enteros. Multiplicación de esta ecuación por c produce

$$c = c \cdot 1 = c(ax + by) = acx + bcy$$

Como $a|ac$ y $a|bc$, resulta que $a|(acx + bcy)$, que puede reformularse como $a|c$.

Si a y b no son coprimos, entonces la conclusión del Lema de Euclides puede no ser válida. Aquí hay un ejemplo especifico: $12|9 \cdot 8$, pero $12 \nmid 9$ y $12 \nmid 8$.

El teorema subsecuente a menudo sirve como una definición de $\text{mcd}(a, b)$. La ventaja de utilizarlo como una definición es que la relación de orden no está involucrada. Por lo tanto, se puede utilizarlo en sistemas algebraicas que no tiene ningún relación de orden.

Teorema 2.6. Sean a y b enteros, no ambos cero. Para un entero positivo d, $d = \text{mcd}(a, b)$ si y solo si

a) $d|a$ y $d|b$

b) Cada vez que $c|a$ y $c|d$, entonces $c|d$.

Demostración: Para empezar, supongamos que $d = \text{mcd}(a, b)$. Es cierto que $d|a$ y $d|b$, de modo que a) se mantiene. A la luz de Teorema 2.3, d se puede expresar

como $d = ax + by$ por algunos enteros x, y. Por lo tanto, si $c|a$ y $c|b$, entonces $c|(ax + by)$ o $c|d$. Recíprocamente, sea d cualquier entero positivo que satisface las condiciones indicadas. Dado cualquier divisor común c de a y b, tenemos $c|d$ de hipótesis b). La implicación es que $d \geq c$, y de consecuencia d es el máximo común divisor de a y b.

PROBLEMAS 2.3

1. Si $a|b$, demostrar que $(-a)|b$, $a|(-b)$, y $(-a)|(-b)$.

2. Dado enteros a, b, c, d, verificar lo siguiente:
a) Si $a|b$, entonces $a|bc$.
b) Si $a|b$ y $a|c$, entonces $a^2|bc$.
c) $a|b$ si y solo si $ac|bc$, en donde $c \neq 0$.
d) Si $a|b$ y $c|d$, entonces $ac|bd$.

3. Probar o refutar: Si $a|(b + c)$, entonces o $a|b$ o $a|c$.

4. Para $n \geq 1$, utilizar la inducción matemática para establecer cada uno de los siguientes enunciados de divisibilidad.
a) $8|5^{2n+7}$.
[Consejo: $5^{2(k+1)} + 7 = 5^2(5^{2k} + 7) + (7 - 5^2 \cdot 7)$.]
b) $15|2^{4n} - 1$.
c) $5|3^{3n+1} + 2^{n+1}$.
d) $21|4^{n+1} + 5^{2n-1}$.
e) $24|2 \cdot 7^n + 3 \cdot 5^n - 5$.

5. Demostrar que para cada entero a, uno de los enteros $a, a + 2, a + 4$ es divisible por 3.

6. Para un entero arbitrario a, verificar lo siguiente:
a) $2|a(a + 1)$, y $3|(a(a + 1)(a + 2)$.
b) $3|a(2a^2 + 7)$
c) Si a es impar, entonces $32|(a^2 + 3)(a^2 + 7)$.

7. Demostrar que si a y b son enteros impares, entonces $16|a^4 + b^4 + 2$.

8. Demostrar lo siguiente:
a) La suma de los cuadrados de dos enteros impares no puede ser un cuadrado perfecto.
b) El producto de cuatro enteros consecutivos es una menos que un cuadrado perfecto.

9. Establecer que la diferencia entre dos cubos consecutivos nunca es divisible por 2.

10. Por un entero a no cero, demostrar que $\text{mcd}(a, 0) = |a|$, $\text{mcd}(a, a) = |a|$, y $\text{mcd}(a, 1) = 1$.

11. Si a y b son enteros, no ambos cero, verificar que

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

12. Demostrar que, para un entero positivo n y cualquier entero a, $\text{mcd}(a, a + n)$ divide a n; entonces $\text{mcd}(a, a + 1) = 1$.

13. Dado enteros a y b, demostrar lo siguiente:
a) Existen enteros x e y tales que $c = ax + by$ si y solo si $\text{mcd}(a, b)|c$.
b) Si existen enteros x e y tales que $ax+by = \text{mcd}(a, b)$, entonces $\text{mcd}(x, y) = 1$.

14. Para cualquier entero a, demostrar lo siguiente:
a) $\text{mcd}(2a + 1, 9a + 4) = 1$
b) $\text{mcd}(5a + 2, 7a + 3) = 1$
c) Si a es impar, entonces $\text{mcd}(3a, 3a + 2) = 1$

15. Si a y b son enteros, no ambos cero, demostrar que $\text{mcd}(2a - 3b, 4a - 5b)$ divide a b; por lo tanto $\text{mcd}(2a - 3, 4a - 5) = 1$.

16. Dado un entero impar a, establecer que

$$a^2 + (a + 2)^2 + (a + 4)^2 + 1$$

es divisible por 12.

17. Demostrar que la expresión $(3n)!/(3!)^n$ es un entero para cada $n \geq 0$.

18. Demostrar: el producto de cualquier tres enteros consecutivos es divisible por 6; el producto de cualquier cuatro enteros consecutivos es divisible por 24; el producto de cualquier cinco enteros consecutivos es divisible por 120.
[Consejo: ver Corolario 2 a Teorema 2.4.]

19. Establecer cada uno de las siguientes afirmaciones:
a) Si a es un entero arbitrario, entonces $6|a(a^2 + 11)$.
b) Si a es un entero impar, entonces $24|a(a^2 - 1)$.
[Consejo: El cuadrado de un entero impar es de la forma $8k + 1$.]
c) Si a y b son enteros impares, entonces $8|(a^2 - b^2)$.
d) Si a es un entero no divisible por 2 o 3, entonces, $24|a^2 + 23$.
e) Si a es un entero arbitrario, entonces $360|a^2(a^2 - 1)(a^2 - 4)$.

20. Confirmar las siguientes propiedades del máximo común divisor:
a) Si $\text{mcd}(a, b) = 1$ y $\text{mcd}(a, c) = 1$, entonces $\text{mcd}(a, bc) = 1$.
[Consejo: Como $1 = ax + by = au + cv$ por algunos x, y, u, v, entonces

$1 = (ax + by)(au + cv) = a(aux + cvx + byu) + bc(yv)$.]
b) Si $\text{mcd}(a, b) = 1$ y $c|a$, entonces $\text{mcd}(b, c) = 1$.
c) Si $\text{mcd}(a, b) = 1$, entonces $\text{mcd}(ac, b) = \text{mcd}(c, b)$.
d) Si $\text{mcd}(a, b) = 1$ y $c|a + b$, entonces $\text{mcd}(a, c) = \text{mcd}(b, c) = 1$.
[Consejo: Sea $d = \text{mcd}(a, c)$. Entonces $d|a$, $d|c$ implica que $d|(a + b) - a$, o $d|b$.]
e) Si $\text{mcd}(a, b) = 1$, $d|ac$, y $d|bc$, entonces $d|c$.
f) Si $\text{mcd}(a, b) = 1$, entonces $\text{mcd}(a^2, b^2) = 1$.
[Consejo: Primero mostrar que $\text{mcd}(a, b^2) = \text{mcd}(a^2, b) = 1$.]

21. a) Demostrar que si $d|n$, entonces $2^d - 1|2^n - 1$.
[Consejo: Utilizar la identidad

$$x^k = 1 = (x - 1)(x^{k-1} + x^{k-2} + \cdots + x + 1).]$$

b) Verificar que $2^{35} - 1$ es divisible por 31 y 127.

22. Sea t_n el enésimo número triangular. Para cuales valores de n divide t_n la suma $t_1 + t_2 + \ldots t_n$?
[Consejo: Ver Problema 1c), sección 1.1.]

23. Si $a|bc$, demostrar que $a|\text{mcd}(a, b)\text{mcd}(a, c)$.