Sobre el máximo común divisor de dos enteros

OSCAR FERNANDO SOTO AGREDA

PRESENTACION

La matemática se retroalimenta de sus propias teorías, pero además muchos de los resultados en algunas de sus ramas suele atravesar los dominios de otras; por ejemplo, muchos de los resultados del análisis en variable real se consiguen como aplicaciones del estudio del análisis en variable compleja. En este orden de ideas, el artículo presenta sin demostración formal sino más bien como una justificación lógica, un resultado de la teoría de números que se consigue como un parto elemental de la teoría de grupos: es una hermosa identidad en la que solo intervienen *máximos común divisores* y que asombra por su "inutilidad".

Acaso algún lector acusioso, logre encontrar para la identidad objeto de estudio y que se muestra a continuación algún fin práctico de carácter algorítmico que hasta el momento no he encontrado. La identidad que se persigue se puede escribir como:

$$\frac{(n(a,b),ab)}{(n,a)(n,b)} = \frac{(a,b)}{(n,(a,b))}$$

donde n,a,b son números naturales y (a,b) denota el máximo común divisor de a y b con igual significado para las demás expresiones de la identidad.

De hecho, a y b pueden ser números enteros, por el contrario n se obliga a ser un número natural. Se hace necesario recordar algunos hechos fundamentales como los que se desglosan en seguida.

1. MAXIMO COMUN DIVISOR

Al dividir un entero a por un entero b no nulo, el proceso no termina hasta encontrar un resto r más pequeño que el divisor b; este algoritmo se resume en el siguiente teorema.

TEOREMA. Si $a \in Z$ y $b \in Z^+$, siempre existen enteros q y r tales que $a = bq + r$ donde además $0 \leq r < b$.

Es preciso anotar que en este artículo se omiten las demostraciones pero en varias ocasiones se brindan sugerencias para efectuarlas o se invita a leerlas en algunos textos técnicos. Por ejemplo, para demostrar el teorema formulado puede emplearse el hecho de que todo entero no múltiplo de b está comprendido entre dos múltiplos consecutivos de él.

Este teorema brinda como primera utilidad un algoritmo para calcular el *máximo común divisor de dos enteros.*

DEFINICION. Si a y b son dos enteros donde al menos uno de ellos es diferente de cero, existe un único entero d que es el mayor entre todos los divisores comunes a a y b y que se denota como $d = (a,b)$ y se llama el *máximo común divisor de a y b.* Si b fuese cero, se define $(a,0) = a$.

Ejemplo 1.

$(8, 4) = 4$; $(12, 9) = 3$; $(7, 8) = 1$

Cuando el máximo común divisor de los enteros a y b es uno, se dice que ellos son primos relativos o primos entre sí.

Ejemplo 2.

8 y 9 son primos relativos; 25 y 36 son primos relativos. Dos números enteros consecutivos son primos entre sí, dos impares consecutivos también son primos entre sí.

Ejemplo 3.

Para hallar el (1830, 750) es posible ver que:

$$\begin{aligned}
1830 &= 750(2) + 330 \quad \text{y por ello} \quad (1830, 750) = (750, 330) \\
750 &= 330(2) + 90 \quad \text{y por ello} \quad (1830, 750) = (330, 90) \\
330 &= 90(3) + 60 \quad \text{y por ello} \quad (1830, 750) = (90, 60) \\
90 &= 60(1) + 30 \quad \text{y por ello} \quad (1830, 750) = (60, 30) \\
60 &= 30(2) + 0 \quad \text{y en definitiva} \quad (1830, 750) = (30, 0) = 30
\end{aligned}$$

Este proceso de hallar el máximo común divisor está expuesto en LOS ELEMENTOS de Euclides y por supuesto, en forma geométrica.

El algoritmo se generaliza así:

Para a y b enteros arbitrarios y no nulos, por divisiones sucesivas se escribe:

$$\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < b \\
b &= r_1 q_2 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && 0 < r_3 < r_2 \\
r_2 &= r_3 q_4 + r_4 && 0 < r_4 < r_3 \qquad (1) \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0
\end{aligned}$$

Lo que indica como (a,b) es igual al último resto mayor que cero en la sucesión de residuos $r_1 > r_2 > r_3 > \cdots > r_n > 0$ y viendo que $(a,0) = a$, cualquiera que sea a en $\mathbb{Z}$, se tiene que

$$(a,b) = (b,r_1) = (r_1,r_2) = \cdots = (r_{n-1},r_n) = (r_n,0) = r_n.$$

De las expresiones (1) se deduce que si $d=(a,b)$, existen dos enteros α y β tales que $d=a\alpha+b\beta$.

En efecto, si (a,b) fuese igual a r_1, la primera igualdad de (1) asegura que $r_1=a+b(-q_1)$; luego $d=a\alpha+b\beta$ donde $\alpha=1$ y $\beta=-q_1$.

Si (a,b) fuese igual a r_2 se consigue:

$$r_2=b-r_1q_2=b-(a+b(-q_1))q_2=a(-q_2)+b(1+q_1q_2)$$

y nuevamente $d=a\alpha+b\beta$ donde $\alpha=-q_2$ y $\beta=1+q_1$. El proceso se reitera para los restos sucesivos $r_3, r_4, \ldots, r_n$.

Para el ejemplo 3 se encuentra que

$$(1830, 750)=1830(-9)+750(22).$$

Es usual decir que el máximo común divisor de a y b se escribe como "combinación lineal" de a y b.

2. FRACCIONES CONTINUAS Y MAXIMO COMUN DIVISOR

El algoritmo de Euclides conduce a un importante método para representar el cociente de dos enteros mediante una fracción compuesta. Basta considerar el grupo de igualdades (1):

La primera igualdad se escribe como $\frac{a}{b}=q_1+\frac{r_1}{b}=q_1+\frac{1}{\frac{b}{r_1}}$, pero de la segunda igualdad del mismo sistema es claro que:

$\frac{b}{r_1}=q_2+\frac{r_2}{r_1}=q_2+\frac{1}{\frac{r_1}{r_2}}$ y por lo tanto: $\frac{a}{b}=q_1+\cfrac{1}{q_2+\frac{1}{\frac{r_1}{r_2}}}$,

de la tercera igualdad se tiene $\frac{r_1}{r_2}=q_3+\frac{r_3}{r_3}=q_3+\frac{1}{\frac{r_2}{r_3}}$ y por ello:

$$\frac{a}{b}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\frac{1}{\frac{r_2}{r_3}}}}$$

Llevando este proceso hasta el fin se consigue

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{\vdots}{+\cfrac{1}{q_n + 1}}}} \qquad (2)$$

Esta expresión es el desarrollo del racional $\frac{a}{b}$ en fracción continua. Para evitar este tipo de designación demasiado voluminosa para esta fracción continua se usan varias notaciones convencionales entre las cuales resalta por su sencillez la estructura:

$$\frac{a}{b} = [q_1; q_2, q_3, \ldots, q_n + 1],$$

notación en la que el punto y coma resalta la parte entera de la fracción.

Ejemplo 4.

De acuerdo a la convención de escritura, para la expresión (2) se escribe:

$$\frac{17}{9} = [1; 1, 8], \quad \frac{37}{11} = [3; 2, 1, 3], \quad -\frac{61}{37} = [-3; 1, 2, 1, 6]$$

Se observa que para desarrollar $\frac{a}{b}$ en una fracción continua se aplica a los números a y b el algoritmo de Euclides, los cocientes obtenidos en las divisiones sucesivas, son los elementos y en ese orden de la fracción continua. Para el ejemplo 3 se obtiene que $\frac{1830}{750} = [2; 2, 3, 1, 2]$.

Un bonito resultado que conecta aún más el máximo común divisor de los números a y b con las fracciones continuas y de carácter algorítmico, se demuestra en uno de los excelentes folletos de divulgación llamados "lecciones populares de matemáticas"; el resultado algorítmico se describe así: Si

$$\frac{a}{b} = [q_1; q_2, q_3, \ldots, q_n + 1]$$

entonces la fracción continua

$$[q_1; q_2, q_3, \ldots, q_n] = \frac{u}{v}$$

consigue que $av - bu = \pm(a,b)$.

Ejemplo 5.

Paara el ya tan mencionado ejemplo 3 se tiene que

$$\frac{1830}{750} = [2;\ 2,\ 3\ ,\ 1\ ,\ 2]$$

mientras que la fracción $[2;\ 2,\ 3,\ 1,\ 2] = \frac{22}{9}$ de donde se encuentra $1830(9) - 750(22) = -30$.

Para dos enteros consecutivos se tiene que $\frac{n+1}{n} = [1;\ 1]$ y como $[1] = \frac{1}{1}$ se tiene que $(n+1)(1) - n(1) = 1$ lo que asegura que dos enteros consecutivos son primos entre sí, como se afirmó antes. Para dos enteros impares consecutivos se tiene: $\frac{2n+1}{2n-1} = [1;\ n-1,2]$ y la fracción continua $[1;\ n-1] = \frac{n}{n-1}$ de donde se tiene que $(2n+1)(n-1) - (2n-1) = -1$ y por ello dos enteros impares consecutivos siempre son primos entre sí. Para dos números pares consecutivos $2n+2$ y $2n$ se encuentra que $(2n+2, 2n) = 2$.

La última parte del ejemplo 5 es solo un caso particular de la propiedad general para el máximo común divisor: $(\alpha a, \alpha b) = \alpha(a,b)$. Para el caso

$$(2n+2, 2n) = (2(n+1), 2n) = 2(n+1, n) = 2 \cdot 1 = 2$$

3. UNA REVISION DEL GRUPO CICLICO $(Z_n, +)$

Aquí se mencionan algunos resultados de la teoría de grupos que se requieren para establecer la identidad objeto de estudio.

3.1 El grupo $(Z, +)$ es cíclico de orden infinito generado por 1 o por -1. Debe recordarse que todo grupo cíclico es abeliano.

Cada grupo $(Z, +)$ está generado al menos por la clase residual 1 y posee orden n. El grupo puede poseer más generadores y en efecto, cada clase a de Z_n tal que $(a,n) = 1$ es un generador del grupo. Una demostración de este hecho se sustenta en que la clase 1 pertenece al subgrupo cíclico generado por a y que se denota por $\langle a \rangle$.

3.2 Todo subgrupo de un grupo cíclico es cíclico; por ejemplo los subgrupos de $(Z, +)$ y cualquier entero n genera el subgrupo cíclico $(nZ, +) = \langle n \rangle$.

Z_n posee orden n, hecho que se denota $\sigma(Z_n) = n$, y cada elemento genera un subgrupo cíclico. Esto significa que Z_n posee un número finito de subgrupos cíclicos. Para el grupo $(Z_n, +)$ se conoce el siguiente teorema sobre órdenes.

TEOREMA. Si $s \in Z_n$, s genera un subgrupo cíclico de Z_n cuyo orden es $\frac{n}{d}$ donde $d = (n,s)$. En símbolos esto significa que $\sigma(\langle s \rangle) = \frac{n}{(n,s)}$. De modo que si $(n,s) = 1$ se tiene que $\sigma(\langle s \rangle) = n$ y por ello $\langle s \rangle = Z_n$ que es ina conclusión del parágrafo 3.1.

Ejemplo 6.

Para Z_{15}, la clase residual 9 genera un subgrupo cuyo orden es $\sigma(\langle 9 \rangle) = \frac{15}{(15,9)} = 5$. En efecto $\langle 9 \rangle = \{9, 3, 12, 6, 0\}$.

3.3 Para el grupo Z_n el producto de dos subgrupos cíclicos $\langle a \rangle$ y $\langle b \rangle$ se define como $\langle a \rangle \cdot \langle b \rangle = \{a\alpha + b\beta \,/\, \alpha \in Z,\ \beta \in Z\}$ según aritmética modular. Puede verse entonces que $(a,b) \in \langle a \rangle \cdot \langle b \rangle$. Debido a que $\langle a \rangle \cdot \langle b \rangle = \langle b \rangle \cdot \langle a \rangle$ se concluye que este producto es un subgrupo cíclico de Z_n y para él no puede existir otro generador diferente a (a,b) es decir $\langle a \rangle \cdot \langle b \rangle = \langle\langle (a,b) \rangle\rangle$ hecho que se prueba por la misma definición de producto de subgrupos.

Así mismo $\langle a \rangle \cap \langle b \rangle$ es un subgrupo cíclico de Z_n y puede demostrarse con facilidad que $\langle a \rangle \cap \langle b \rangle = \left\langle \frac{ab}{(a,b)} \right\rangle$.

3.4 Es necesario tener aquí a disposición el siguiente resultado sobre el orden de los subgrupos:

TEOREMA. Si H y K son subgrupos finitos de un grupo G de órdenes $\sigma(H)$ y $\sigma(K)$ respectivamente, entonces:

$$\sigma(\mathrm{HK}) = \frac{\sigma(H) \cdot \sigma(K)}{\sigma(H \cap K)}$$

4. LA IDENTIDAD

Se está ahora en libertad de escribir de manera deductiva el resultado objeto de estudio en el presente artículo.

Suponga que $\langle a \rangle$ y $\langle b \rangle$ son dos subgrupos cíclicos de Z_n; por el parágrafo 3.2, se tiene que $\sigma(\langle a \rangle) = \frac{n}{(n,b)}$.

El parágrafo 3.3 asegura que $\langle a \rangle \cap \langle b \rangle = \left\langle \frac{ab}{(a,b)} \right\rangle$ y por lo tanto:

$$\sigma(\langle a \rangle \cap \langle b \rangle) = \frac{n}{\left(n, \frac{ab}{(a,b)}\right)} = \frac{n(a,b)}{(n(a,b),ab)} \tag{2}$$

Del teorema 3.4 se deduce, utilizando (2) que:

$$\sigma(\langle a \rangle \cdot \langle b \rangle) = \frac{n(n(a,b),ab)}{(n,a)(n,b)(a,b)} \tag{3}$$

Y como $\langle a \rangle \cdot \langle b \rangle = \langle (a,b) \rangle$ se encuentra que

$$\sigma\left(\left\langle (a,b) \right\rangle\right) = \frac{n}{(n,(a,b))} \tag{4}$$

Conjugando las expresiones (3) y (4) que son iguales se concluye en definitiva que:

$$\frac{(n(a,b),ab)}{(n,a)(n,b)} = \frac{(a,b)}{(n,(a,b))}$$

Esta identidad que puede entenderse como una proporción se puede escribir de diferentes maneras e intentar encontrar sobre ellas un beneficio algorítmico práctico. La belleza de la identidad se encuentra en que solo entrelaza máximos comunes divisores.

BIBLIOGRAFIA

[1] BELSKI A. A. y otro. *División Inexacta.* Editorial Mir. Moscú. 1980.

[2] VOROBIOV N. N. *Números de Fibonacci.* Editorial Mir. Moscú. 1974.

[3] BESKIN N. *Fracciones Maravillosas.* Editorial Mir. Moscú. 1987.

[4] COURANT Richard y Otro. *Qué es la Matemática?* Ediciones Aguilar. Madrid. 1964.

UNIVERSIDAD DE NARIÑO
PROGRAMA DE MATEMATICAS Y ESTADISTICA
SAN JUAN DE PASTO