AMPLIACIÓN DE MATEMÁTICAS

EL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA.

El siguiente resultado es él que nos asegura que todo número entero puede descomponerse. En la prueba está implícito el como hacerlo, aunque de una forma poco eficiente.

Teorema 1. (***Fundamental de la Aritmética.***) *Todo número natural mayor que 1 puede expresarse de forma única como un producto de números primos (puede que algunos se repitan).*

Observación 1. *Un teorema similar también lo veremos para polinomios más adelante.*

Demostración: Sea un número natural $n > 1$. Sabemos que existe un número primo p que le divide $(p|n)$. Con lo anterior, procedamos por inducción. Si $n = 2$, claro $2 = 1 \times 2$. Y el 2 es primo. Supuesto que para todo $m \leq n$, se tiene que m se puede expresar como un producto de primos, veamos que le acorre a $n + 1$. Existe un primo p que lo divide, así $n + 1 = p \times k$ y seguro que $k < n + 1$ (salvo que $n + 1$ sea primo y entonces no hay nada que probar; caso trivial). Entonces por el principio de inducción, k es un producto de primos, cuyos factores junto a p nos dan el producto que determima $n + 1$.

Veamos ahora la **unicidad**. Supongamos que n se puede escribir de dos formas

$$n = p_1 p_2 ......p_r = q_1 q_2 .....q_s$$

donde los p_i y los q_j son primos. Así $p_1|n$ y por tanto existe un q_j (que le llamamos ahora q_1) de modo que $p_1|q_1$. Por la definición de primo, tenemos que $p_1 = q_1$. Luego $p_2 p_3 ...p_r = q_2 q_3 ...q_s$. Ahora siguiendo por recurrencia, $p_2|q_2 q_3 ...q_s$ ....etc, se llega a ver que $p_i = q_i$ para todo i y donde $r = s\square$

Corolario 1. *Si n es un número natural mayor que 1 se puede escribir de forma única como potencias de primos. Es decir existe $p_1, p_2, ..., p_k$ números primos distintos y $r_1, r_2, ..., r_k$ enteros positivos de modo que*

$$n = p_1^{r_1} p_2^{r_2} .....p_k^{r_k}.$$

Corolario 2. *Si $a, b \in \mathbb{N}\backslash\{0\}$ de modo que $a = p_1^{r_1} p_2^{r_2} .....p_k^{r_k}$ y $b = p_1^{s_1} p_2^{s_2} .....p_k^{s_k}$, entonces*

- $m.c.d.(a, b) = p_1^{\min\{r_1,s_1\}} p_2^{\min\{r_2,s_2\}} .....p_k^{\min\{r_k,s_k\}}$.
- $m.c.m.(a, b) = p_1^{\max\{r_1,s_1\}} p_2^{\max\{r_2,s_2\}} .....p_k^{\max\{r_k,s_k\}}$.

Observación 2. *Lo anterior nos da un procedimiento para a hallar el máximo común divisor de dos números (¡el procedimiento del cole!), aunque no es muy eficiente. Es mejor usar el algoritmo de Euclides como veremos.*

Demostración: $p_1, ..., p_k$ son todos los divisores primos de a y b (comunes o no, por tanto algunos r_i o s_j pueden ser cero).

Sea $d = p_1^{\min\{r_1,s_1\}} p_2^{\min\{r_2,s_2\}} .....p_k^{\min\{r_k,s_k\}}$, es claro que d divide tanto a a como a b. Si c es otro divisor común de a y b y c se escribe como $c = q_1 q_2 ...q_m$, cada primo q_n divide a a y b, luego tendra que ser algún p_i. Así $c|d$, lo que prueba que d es el máximo común divisor.

Sea $m = p_1^{\max\{r_1,s_1\}} p_2^{\max\{r_2,s_2\}} .....p_k^{\max\{r_k,s_k\}}$. Es claro que $a|m$ y $b|m$. Si c es otro múltiplo común de a y b, entonces $p_i^{\max\{r_i,s_i\}}|c$ para cada $i = 1, 2..., k$. Así $m|c$. Lo que prueba que $m = m.c.m.(a, b)$□

Corolario 3. *Para cada $a, b \in \mathbb{N}\backslash\{0\}$ se tiene que*

$$ab = m.c.d.(a, b)m.c.m.(a, b)$$

Corolario 4. *Para cada $a, b \in \mathbb{N}\backslash\{0\}$ se tiene que*

$$m.c.m.(a, b) = \min\{c \in \mathbb{N}\backslash\{0\} \ : \ a|c \ y \ b|c\}.$$

Demostración: Primero

$$ab \in \{c \in \mathbb{N}\backslash\{0\} \ : \ a|c \text{ y } b|c\}.$$

Luego el conjunto anterior es no vacío y por tanto tiene un mínimo, sea este m. Por la definición de mínimo común múltiplo se tiene que $m.c.m.(a, b)|m$ y así $m.c.m.(a, b) \leq m$. Por otro lado

$$m.c.m.(a, b) \in \{c \in \mathbb{N}\backslash\{0\} \ : \ a|c \text{ y } b|c\},$$

luego por la definición de m, $m \leq m.c.m.(a,b)$. Ambas desigualdades nos dicen que $m = m.c.m.(a,b)\square$

Ejemplo 1. *Si* $a, b \in \mathbb{N}\backslash\{0\}$ *hay que ver que* $m.c.d.(a,b)|(na+mb)$ *para todo* $n, m \in \mathbb{Z}$.

Sea $d = m.c.d.(a,b)$. d divide tanto a a como a b. Así $a = q_1 d$ y $b = q_2 d$, por lo tanto

$$na + mb = nq_1 d + mq_2 d = (nq_1 + mq_2)d.$$

Así $d|na + mb\square$

Ejemplo 2. $m.c.d.(n, n+1) = 1$.

Según la prueba del Lema de Bezout

$$m.c.d.(n, n+1) = \text{mín}\{x \in \mathbb{N}\backslash\{0\} \ : \ x = ua + vb \text{ donde } u, v \in \mathbb{Z}\}.$$

Para $u = -1$ y $v = 1$ se tiene que $1 = -n + (n+1)$, lo que dice que $1 = m.c.d.(a,b)$.

Ejemplo 3. *¿* $m.c.d.(n, n+2)$*?*

Si $d = m.c.d.(n, n+2)$, entonces $d|n$ y $d|n+2$; por tanto $d|2$. Así d puede ser 1 o 2. Por ejemplo

$$m.c.d.(17, 19) = 1, \quad \text{sin embargo } m.c.d.(18, 20) = 2\square$$

Ejemplo 4. *¿* $m.c.d.(n, n+6)$*?*

Si $d = m.c.d.(n, n+6)$, entonces $d|n$ y $d|n+6$; por tanto $d|6$. Así d puede ser $1, 2, 3$ o 6. Por ejemplo

$$m.c.d.(5, 11) = 1, \ \ m.c.d.(2, 8) = 2, m.c.d.(3, 9) = 3 \text{ y } \ m.c.d.(6, 12) = 6\square$$

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es