Sobre un teorema de la teoría elemental de números

Pedro Alvarado Robis.

Universidad Autónoma

Le recomendamos seguir el razonamiento que nos llevará a redescubrir el Teorema, leyendo al mismo tiempo el ejemplo numérico que hay después del enunciado del mismo.

Sean $m \in IN$ un número natural y $A_m = \{1,2,3,\cdots,m\}$
Para cada $x \in A_m$, el máximo común divisor (x,m), satisface $(x,m)=1$ o $(x,m)>1$ (se trata de una dicotomía).

Para cada d, divisor de m, definimos:

$$I_d = \left\{ sd \,/\, s \in IN,\, sd \le m \ y \left(s, \frac{m}{d} \right) = 1 \right\}$$

Afirmación: $I_d \cap I_{d'} = \phi$ si $d \neq d'$, con d y d' divisores de m.

Demostración: Sea d el divisor más pequeño de m tal que exista un d' con $I_d \cap I_{d'} \neq \phi$ y $d \neq d'$.

Existen, entonces, s y t, enteros positivos, tales que $sd = td'$, donde $\left(s, \frac{m}{d} \right) = 1 = \left(t, \frac{m}{d'} \right)$.

Por la elección de d, $d' > d$.

De $sd = td'$, deducimos que d'/sd, entonces $(s,d) = a > 1$, si no d'/d, lo que imposible puesto que $d' > d$.

De la definición de máximo común divisor tenemos: a/d', y como d'/m, entonces a/m.

Como $m = \frac{m}{d} \cdot d$ y $\left(a, \frac{m}{d} \right) = 1$ (porque $\left(s, \frac{m}{d} \right) = 1$), se tiene: a/d.

Entonces, como $sd = td'$, $d = ua$ y $d' = wa$: $sd_1 = td_1^{'}$, con $d_1 = \frac{d}{a} \in Z$ y $d_1^{'} = \frac{d'}{a} \in Z$; es decir $I_{d1} \cap I_{d_1^{'}} \neq \phi$.

Y como $d_1 < d$, se contradice la minimalidad en la elección del divisor *d*. Lo que prueba la afirmación.

Afirmación: $A_m = \bigcup_{d/m} I_d$

Demostración: Claramente $I_d \subset A_m \quad \forall d / m.$

Si $a \in A_m$, entonces $a = cd$, donde $d = (a, m)$ y $\left(c, \dfrac{m}{d}\right) = 1$, entonces $a \in I_d$.

¿Cuántos elementos hay en conjunto I_d ?

Hay tantos como números naturales s tales que: $1 \le s \le \dfrac{m}{d}$ y $\left(s, \dfrac{m}{d}\right) = 1$; es decir, $card(I_d) = \varphi\left(\dfrac{m}{d}\right)$, donde $\varphi(a)$, para $a \in IN$, indica el número de números naturales menores que *a* y primos con *a* (función de Euler).

Por ejemplo:

1. Si $a = 6$, $\varphi(6) = 2$ ya que del conjunto $\{1,2,3,4,5\}$ solo el 1 y el 5 son primos con 6.
2. Si $a = 12$, $\varphi(12) = 4$ ya que del conjunto $\{1,2,3,4,5,6,7,8,9,10,11\}$ solo el 1, 5, 7 y 11 son primos con 12.

Así hemos demostrado el siguiente

Teorema: Sea $m \in IN$. Entonces se cumple $\sum_{d/m} \varphi\left(\dfrac{m}{d}\right) = m$, donde la suma se toma sobre todos los divisores *d* de *m*.

Ejemplo numérico:

Sea $m = 18$.

$A_{18} = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17\}$

1, 2, 3, 6, 9 y 18 divisores de $m = 18$.

$I_1 = \{1,5,7,11,13,17\}$ $\qquad \varphi\left(\dfrac{18}{1}\right) = \varphi(18) = 6$

$I_2 = \{2,4,8,10,14,16\}$ $\qquad \varphi\left(\dfrac{18}{2}\right) = \varphi(9) = 6$

$I_3 = \{3,15\}$ $\qquad \varphi\left(\dfrac{18}{3}\right) = \varphi(6) = 2$

$I_6 = \{6,12\}$

$I_9 = \{9\}$

$I_{18} = \{18\}$

$\varphi\left(\frac{18}{6}\right) = \varphi(3) = 2$

$\varphi\left(\frac{18}{9}\right) = \varphi(2) = 1$

$\varphi\left(\frac{18}{18}\right) = \varphi(1) = 1$

Observar que:

- $\varphi\left(\frac{18}{1}\right) + \varphi\left(\frac{18}{2}\right) + \varphi\left(\frac{18}{3}\right) + \varphi\left(\frac{18}{6}\right) + \varphi\left(\frac{18}{9}\right) + \varphi\left(\frac{18}{18}\right) = 6 + 6 + 2 + 2 + 1 + 1 = 18$
- $I_1 \cup I_2 \cup I_3 \cup I_6 \cup I_9 \cup I_{18} = A_{18}$