AMPLIACIÓN DE MATEMÁTICAS

LA FUNCIÓN DE EULER.

Definición 1. *La* ***función de Euler*** *se define por*

$$\begin{array}{rcccl} \phi & : & \mathbb{N}\backslash\{0\} & \to & \mathbb{N}\backslash\{0\} \\ & & n & \to & \phi(n) = Card\{k \in \mathbb{N}\backslash\{0\} \ : \ k < n \ \ y \ \ m.c.d.(k,n) = 1\}. \end{array}$$

También a ϕ se la conoce como Totalizador o función Indicador.

Observación 1. **A:**

$$\begin{aligned} \phi(n) &= Card\{[k] \in \mathbb{Z}_n \ : \ m.c.d.(k,n) = 1\} \\ &= Card\{[k] \in \mathbb{Z}_n \ : \ existe \ [k]^{-1}\}. \end{aligned}$$

B: *Si p es un número primo, entonces $\phi(p) = p - 1$.*

C: *La función de Euler tiene aplicaciones en* ***Critografía****, como veremos al final del tema de Teoría de Grupos (* ***algoritmo R.S.A.****).*

Los siguientes resultados permiten calcular la función de Euler.

Proposición 1. *Si p es primo, entonces $\phi(p^n) = p^n(1 - \frac{1}{p})$.*

Demostración: Es claro que $m.c.d.(k, p^n) = 1$ si y solo si $p \nmid k$. Existen p^{n-1} números entre 1 y p^n que son divisibles por p, estos son:

$$1p, 2p, 3p, ..., p^{n-1}p.$$

Por tanto

$$\phi(p^n) = p^n - p^{n-1} = p^n(1 - \frac{1}{p}).$$

Proposición 2. *Si $m.c.d.(n, m) = 1$, entonces $\phi(nm) = \phi(n)\phi(m)$.*

Demostración: Al estudiar las operaciones "rápidas" vimos que la aplicación

$$\begin{array}{rcccl} T & : & \mathbb{Z}_{nm} & \to & \mathbb{Z}_n \times \mathbb{Z}_m \\ & & [x]_{nm} & \to & T([x]_{nm}) = ([x]_n, [x]_m) \end{array}$$

es una aplicación biyectiva (gracias al Teorema Chino del Resto) y que además verifica que $T(x+y) = T(x) + T(y)$ y $T(xy) = T(x)T(y)$.

De lo anterior se sigue que $x \in \mathbb{Z}_{nm}$ tiene inverso si y solo si $x \in \mathbb{Z}_n$ y $x \in \mathbb{Z}_m$ tienen inversos. Veamoslo.

- Sean $[x]_{nm} \in \mathbb{Z}_{nm}$ y $[y]_{nm}$ su inverso. Entonces

$$\begin{aligned}(1,1) = T(1) = T(xy) = T(x)T(y) &= ([x]_n, [x]_m)([y]_n, [y]_m]) \\ &= ([x]_n[y]_n, [x]_m[y]_m),\end{aligned}$$

  por tanto $1 = [x]_n[y]_n$ y $1 = [x]_m[y]_m$.
- Sea $([a]_n, [b]_m) \in \mathbb{Z}_n \times \mathbb{Z}_m$ con inverso, lo cuál quiere decir por la definición de multiplicación en $\mathbb{Z}_n \times \mathbb{Z}_m$ que existen $[a]_n^{-1} \in \mathbb{Z}_n$ y $[b]_m^{-1} \in \mathbb{Z}_m$. Por ser T biyectiva existe un único x de modo que $T(x) = ([a]_n, [b]_m)$ y existe un único y de modo que $T(y) = ([a]_n^{-1}, [b]_m^{-1})$. Ahora es claro que $x, y \in \mathbb{Z}_{nm}$ y que y es el inverso de x $(T(xy) = T(x)T(y) = (1,1) \Rightarrow xy = 1)$.

Con lo anterior se tiene que

$$\begin{aligned}\phi(nm) &= Card\{k \in \mathbb{Z}_{nm} \ : \ \text{existe } k^{-1}\} \\ &= Card\{T(k) \in \mathbb{Z}_n \times \mathbb{Z}_m \ : \ \text{existe } T(k)^{-1}\} \\ &= Card\left(\{a \in \mathbb{Z}_n \ : \ \text{existe } a^{-1}\} \times \{b \in \mathbb{Z}_m \ : \ \text{existe } b^{-1}\}\right) \\ &= Card\{a \in \mathbb{Z}_n \ : \ \text{existe } a^{-1}\} \times Card\{b \in \mathbb{Z}_m \ : \ \text{existe } b^{-1}\} \\ &= \phi(n)\phi(m)\square\end{aligned}$$

El siguiente teorema nos dice como calcular la función de Euler en general.

Teorema 1. *Para todo $n \in \mathbb{N}\backslash\{0\}$*

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}).....(1 - \frac{1}{p_k})$$

donde p_i, $i = 0, 1, 2, ..., k$, son todos los primos que deviden a n.

Demostración: Consideremos la descomposición (única) de n como producto de potencias de primos

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

Los factores de este producto son todos primos entre si, luego por los resultados anteriores

$$\phi(n) = \phi(p_1^{r_1} p_2^{r_2} .... p_k^{r_k})$$
$$\phi(p_1^{r_1})\phi(p_2^{r_2})....\phi(p_k^{r_k})$$
$$= p_1^{r_1}(1 - \frac{1}{p_1})p_2^{r_2}(1 - \frac{1}{p_2})....p_k^{r_k}(1 - \frac{1}{p_k})$$
$$= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}).....(1 - \frac{1}{p_k})\square$$

Proposición 3. *Para todo $n \in \mathbb{N}\backslash\{0\}$ se verifica que*

$$\sum_{d|n} \phi(d) = n.$$

Demostración: Haremos la demostración por inducción.

- Para $n = 1$, $\sum_{d|1} \phi(d) = \phi(1) = 1$.
- Para $n = 2$, $\sum_{d|2} \phi(d) = \phi(1) + \phi(2) = 2$.
- Para $n = p$, primo , $\sum_{d|p} \phi(d) = \phi(1) + \phi(p) = 1 + (p - 1) = p$.
- Para $n = p^r$, potencia de un primo,

$$\sum_{d|p^r} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + ... + \phi(p^r)$$

$$= 1 + (p - 1) + p^2(1 - \frac{1}{p}) + p^3(1 - \frac{1}{p}) + ... + p^r(1 - \frac{1}{p}) = p^r$$

- Tomemos n y supongamos que la propiedad es cierta para todo $k < n$. Existe un primo p que divide a n; tomamos el mayor exponente r de modo que $p^r | n$. Así

$$n = p^r k \text{ de modo que } m.c.d.(p^r, k) = 1.$$

Así

$$\sum_{d|n} \phi(d) = \sum_{d|k} \left(\sum_{i=0}^{r} \phi(dp^i) \right),$$

observemos que para $d = 1$ salen los divisores p^i de n. Y para $i = 0$ los divisores d exclusivos de k. Seguimos desarrollando la fórmula

$$= \sum_{d|k} \phi(d) \left(\sum_{i=0}^{r} \phi(p^i) \right) = p^r \sum_{d|k} \phi(d) = p^r k = n,$$

donde en la penúltima igualdad hemos utilizado la hipótesis de inducción$\square$

Para nosotros la propiedad más importante de la función de Euler es la que sigue. Con ella podremos dar el algoritmo R.S.A., aunque aún no estamos en condiciones de probarla. Necesitamos para ello la **Teoría de Grupos** que veremos en el próximo tema. Entender este resultado es uno de los motivos de estudiar la teoría de Grupo.

Teorema 2. ***(de Euler o Teorema Pequeño de Fermat)***. *Si* $m.c.d.(a,n)=1$, *entonces*

$$a^{\phi(n)} \equiv 1 \ \ mód \ n.$$

Demostración: En $\mathbb{Z}_n$ consideramos el subconjunto

$$\mathbb{Z}_n^* = \{[j] \in \mathbb{Z}_n \ : \ \exists [j]^{-1}\}.$$

$(\mathbb{Z}_n^*, \times)$ es un grupo conmutativo, ya que todos sus elementos tienen inversos. Observemos que el cardinal de $(\mathbb{Z}_n^*, \times)$ es prescisamente $\phi(n)$. Además si $m.c.d.(n,a) = 1$ se tiene que $[a] \in \mathbb{Z}_n^*$. Ahora, **a partir de aquí es teoría de Grupos**, el subgrupo cíclico generado por $[a]$ en $(\mathbb{Z}_n^*, \times)$ tendrá un orden k_0. Por el teorema de Lagrange, que veremos más adelante, k_0 divide al orden del grupo. Esto quiere decir que $k_0 | \phi(n)$. Por tanto

$$[a]_n^{k_0} = [a^{k_0}] \equiv 1 \ \text{ mód } n,$$

como $\phi(n) = kk_0$, se sigue que

$$[a]_n^{\Phi(n)} = [a^{\phi(n)}]_n = [(a^{k_0})^k]_n = [1]_n \square$$

Ejemplo 1. *Tenemos que calcular* $[2^{23}]_{25}$

Observemos que $m.c.d.(2,25) = 1$ y que $\phi(5^2) = 5^2(1 - \frac{1}{5}) = 20$. Así

$$[2^{23}]_{25} = [2^{20+3}] = [2]^{20}[2]^3 = [8]_{25}.$$

Ejemplo 2. *Queremos conocer la última cifra del número* 2^{333}.

Este problema no es más que determinar $x \in \mathbb{Z}_{10}$ de modo que $2^{333} \equiv x$ mód. 10. Como $\mathbb{Z}_{10}$ es igual algebraicamente hablando a $\mathbb{Z}_2 \times \mathbb{Z}_5$, el problema anterior es equivalente a deternimar $([2^{333}]_2, [2^{333}]_5) \in \mathbb{Z}_2 \times \mathbb{Z}_5$. Ahora, como $m.c.d.(2,5) = 1$ y $\phi(5) = 5 - 1 = 4$, se tiene que $2^{\phi(5)} \equiv 1$ mód 5 (por el Teorema de Euler). Además $\begin{array}{cc} 333 & |\underline{4} \\ 1 & 83 \end{array}$ por tanto

$$([2^{333}]_2, [2^{333}]_5) = ([0]_2, [2^{4\times 83} \times 2]_5) = ([0]_2, [2]_5).$$

Luego la x que buscamos será

$$x \equiv 0 \qquad \text{mód} 2$$
$$x \equiv 2 \qquad \text{mód} 5.$$

En este caso tan sencillo no hace falta usar el **Teorema Chino del Resto** para resolver el sistema de congruencias. Se ve que $x = 2 \in \mathbb{Z}_{10}$.

Problema. Un profesor contento con sus alumnos les invitó a comer en un restaurante con tres estrellas Michellin. La cuenta ascendió a 2^{784} euros. La cuál pagó con gusto el profesor usando billetes de cien euros. No recogió el cambio. ¿Cuánta propina dejó?

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

Email address: Cesar_Ruiz@mat.ucm.es