AMPLIACIÓN DE MATEMÁTICAS

EL TEOREMA DE EULER.

Los siguientes resultados, corolarios del Teorema de Lagrange, son esenciales en el cálculo con congruencias de enteros. También son parte de la base teórica de la encriptación con clave pública (**algoritmo R.S.A.**).

Recordemos que un elemento de un grupo finito, $g \in \mathbb{G}$, tiene un orden $Ord(g) = k$ (este es el menor entero positivo de modo que $g^k = e$). Además, $Ord(g) = | < g > | \leq |\mathbb{G}|$.

Teorema 1. *(**Pequeño de Fermat**). Dado un elemento de un grupo finito, $g \in \mathbb{G}$, entonces $g^{|\mathbb{G}|} = e$.*

Demostración: Sea $k = Ord(g) = | < g > |$. Como $\mathbb{G}$ es finito, k existe y además por el Teorema de Lagrange $k \,|\, |\mathbb{G}|$. Luego podemos escribir $|\mathbb{G}| = kn$ para cierto entero positivo n. Por tanto

$$g^{|\mathbb{G}|} = g^{kn} = (g^k)^n = e^n = e \ \square$$

Teorema 2. *(**de Euler**). Sean $a \in \mathbb{Z}$ y $n \in \mathbb{N}\backslash\{0\}$ de modo que $m.c.d.(a, n) = 1$, entonces*

A:

$$a^{\phi(n)} \equiv 1 \qquad mód\ n$$

*(donde ϕ es la **función de Euler**).*

B: *Si, además, $n = p$ es un número primo, entonces*

$$a^{p-1} \equiv 1 \qquad mód\ p$$

o equivalentemente

$$a^p \equiv a \qquad mód\ p.$$

Demostración:

A: Si $m.c.d.(a,n)=1$ eso quiere decir que $[a]\in(\mathbb{Z}_n^*,\times)$ (es decir que existe $[a]^{-1}\in\mathbb{Z}_n$). Como

$$Card(\mathbb{Z}_n^*)=\phi(n),$$

así por el Teorema Pequeño de Fermat

$$1=[a]^{\phi(n)}=[a^{\phi(n)}] \qquad \Leftrightarrow \qquad a^{\phi(n)}\equiv 1 \qquad \text{mód } n.$$

B: $\phi(p)=p-1$ por ser p primo $\square$

Ejemplo 1. *¿*$[2^{333}]_5=$ *? Como* 5 *es primo y* $\phi(5)=4$*, tenemos que*

$$[2^{333}]_5=[2^{4\times 83+1}]_5=[(2^4)^{84}\times 2]_5=([2]_5^4)^{83}\times[2]_5=[2]_5.$$

Referencias

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