ARITMÉTICA MODULAR

Teorema de Euler.

"Si y es inversible en Z_m, entonces $y^{\phi(m)} \equiv 1 \ (\text{mód } m)$"

Proof:

Sea U_m el conjunto de los enteros positivos menores que m y coprimos con m. Es decir el conjunto de los elementos inversibles de Z_m. Se cumplirá, entonces, $|U_m| = \phi(m)$

$$U_m = \{p_1, p_2, \dots, p_{\phi(m)}\}$$

Por ser elementos inversibles, se verificará:

$$\left.\begin{array}{l} \alpha y \equiv 1 \ (\text{mód } m) \\ \alpha_i p_i \equiv 1 \ (\text{mód } m) \end{array}\right\} \text{ con } \alpha, \alpha_i \in Z; \ i = 1, \dots, \phi(m)$$

Sea $u = p_1 p_2 \cdots p_{\phi(m)} = \prod_{i=1}^{\phi(m)} p_i$, que será inversible (y, por lo tanto, congruente con alguno de los p_i), puesto que

$$\prod_{i=1}^{\phi(m)} (\alpha_i p_i) \equiv 1 \ (\text{mód } m)$$

Además, $y p_i$ también es inversible porque $(\alpha \alpha_i)(y p_i) \equiv$ $\equiv 1 \ (\text{mód } m)$, y, para cada $i \neq j$, $y p_i$ será distinto de $y p_j$ (no congruentes), porque, si lo fueran: $y p_i \equiv y p_j \ (\text{mód } m)$ $\Rightarrow p_i \equiv p_j \ (\text{mód } m)$ (en contradicción con la hipótesis).

También se verifica que si $y \not\equiv 1 \ (\text{mód } m) \Rightarrow y p_i \not\equiv p_i \ (\text{mód } m)$

La conclusión es que el conjunto $P = \{yp_1, yp_2, \dots, yp_{\phi(m)}\}$ es el mismo (en $\mathbb{Z}_m$) que U_m; pero la lista de $\phi(m)$ elementos $p_1; p_2; \dots; p_{\phi(m)}$ es una permutación distinta a la $yp_1; yp_2; \dots; yp_{\phi(m)}$. Luego:

$$\prod_{i=1}^{\phi(m)} (y p_i) \equiv \prod_{i=1}^{\phi(m)} p_i \pmod{m} \Rightarrow$$

$$y^{\phi(m)} \cdot u \equiv u \pmod{m} \Rightarrow$$

$$y^{\phi(m)} \equiv 1 \pmod{m}$$

COROLARIOS

1) Teorema pequeño de Fermat: "Si p es primo e $y \not\equiv 0 \pmod{m}$ $\Rightarrow$ $y^{p-1} \equiv 1 \pmod{m}$"

2) "Si p es primo $\Rightarrow$ $y^p \equiv y \pmod{m}$; $\forall y \in \mathbb{Z}$"

ARITMÉTICA MODULAR

Teorema

"Si m y n son coprimos, entonces $\emptyset(mn) = \emptyset(m)\emptyset(n)$"

Proof: Considérese la siguiente tabla numérica:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \cdots & 3n \\ \vdots & \vdots & \vdots & & \vdots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \cdots & mn \end{array}$$

tabla formada por m filas y n columnas (mn elementos).

En la primera fila hay $\emptyset(n)$ coprimos con n. Además $\forall k=1,\dots,n$ si k es coprimo con n, todos los elementos de su columna también serán coprimos con n (si k no es coprimo con n, tampoco lo serán los elementos de su columna) $\Rightarrow$ En esta tabla hay $\emptyset(n)$ columnas formadas por números coprimos con n (el resto de las columnas no lo será).

Bastará, ahora, con demostrar que si k es coprimo con n, hay exactamente $\emptyset(m)$ coprimos con m del conjunto de elementos de la columna k, que son:

$$k\,;\ n+k\,;\ 2n+k\,;\ \dots\,;\ (m-1)n+k$$

Veamos, ahora, que toda pareja de elementos de esa columna son incongruentes (mód m):

Sean i, j $(i<j)$; $0 \leq i, j \leq m-1$; y sean $k+in$ y $k+jn$ dos elementos cualesquiera de la columna k-ésima.

Supongamos que $k+in \equiv k+jn \pmod{m} \Rightarrow$

$\Rightarrow in \equiv jn \pmod{m}$ y como $\operatorname{mcd}(m,n)=1 \Rightarrow i \equiv j \pmod{m}$

lo cual implica que la única posibilidad de congruencia es consigo mismo.

Como los elementos de la columna k-ésima son incongruentes dos a dos $\Rightarrow$ cada uno de ellos será congruente con alguno de los valores $1, 2, \dots, m-1$ (las clases de equivalencia mód m).

Luego $k\,;(n+k)\,;(2n+k)\,;\dots\,;(m-1)n+k$ será congruente con alguna permutación de $1, 2, \dots, m-1$, donde sólo hay $\phi(m)$ elementos inversibles en $\mathbb{Z}_m$. Por lo tanto:

$$\phi(mn) = \phi(m)\,\phi(n)$$