Apellidos y nombre

AMPLIACIÓN DE MATEMÁTICAS
TRABAJO PRÁCTICO 12: Exponenciación en anillos finitos

El **Pequeño Teorema de Fermat** dice que, si p es un entero primo y a es primo con p ($\text{mcd}(p, a) = 1$), entonces:

$$a^{p-1} \equiv 1(\text{mód } p)$$

Demuestra que para todo entero b, $b^p \equiv b(\text{mód } p)$.

$\text{mcd}(p,b) = 1 \Rightarrow b^p = b^{p-1} \cdot b \overset{PTF}{\equiv} 1 \cdot b \text{ mód } p$ ✓

$\text{mcd}(p,b) \neq 1 \underset{p \text{ primo}}{\Rightarrow} p \mid b \Rightarrow b \equiv 0 \text{ mód } p$ y $b^p \equiv 0 \text{ mód } p \Rightarrow b^p \equiv b \text{ mód } p$

Utiliza el Pequeño Teorema de Fermat para calcular el resto de la división por 13 de los números: 5^{13}, 3^{62}, 32^{361}, 90^{735}, y 125^{2424}.

$5^{13} \equiv_{13} 5$

$62 = 12 \cdot 5 + 2 \Rightarrow 3^{62} \equiv 3^2 \equiv 9$

$361 = 12 \cdot 30 + 1 \Rightarrow 32^{361} \equiv_{13} 32^1 \equiv_{13} 6$

$735 = 12 \cdot 61 + 3 \Rightarrow 90^{735} \equiv_{13} 90^3 \equiv_{13} 12^3 \equiv_{13} 12$

$2424 = 12 \cdot 202 \Rightarrow 125^{2424} \equiv_{13} 1$

La **función ϕ de Euler** es aquella que a cada número entero n le asocia el número de elementos de $\mathbb{Z}_n^*$. Calcula $\phi(p)$, cuando $p > 0$ es un número primo.

$p - 1$

Se sabe que, si p es un número primo, $\phi(p^k) = (p-1)p^{k-1}$ y que, si m y n son primos entre sí, $\phi(mn) = \phi(m)\phi(n)$. Calcula: $\phi(125)$, $\phi(490)$, $\phi(300)$, y $\phi(1260)$.

$125 = 5^3 \Rightarrow \varphi(125) = 4 \cdot 5^2 = 100$

$490 = 7^2 \cdot 5 \cdot 2 \Rightarrow \varphi(490) = 6 \cdot 7 \cdot 4 \cdot 1 = 168$

$300 = 3 \cdot 2^2 \cdot 5^2 \Rightarrow \varphi(300) = 2 \cdot 2 \cdot 1 \cdot 5 \cdot 4 = 80$

$$\begin{array}{r|l} 1260 & 2 \\ 630 & 2 \\ 315 & 3 \\ 105 & 3 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

$\Rightarrow 1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \Rightarrow \varphi(1260) = 2 \cdot 1 \cdot 3 \cdot 2 \cdot 4 \cdot 6 =$

$= 288$

53
53
159
265
2709

El **Teorema de Euler** asegura que, si $\mathrm{mcd}(a,n) = 1$, entonces $a^{\phi(n)} \equiv 1 (\text{mód } n)$. Utiliza el Teorema de Euler para hallar las dos últimas cifras de 53^{4085}

$100 = 2^2 \cdot 5^2 \Rightarrow \varphi(100) = 2 \cdot 1 \cdot 5 \cdot 4 = 40$

$\Rightarrow 53^{40} \equiv_{100} 1$ ~~//~~ $4085 = 40 \cdot 102 + 5 \Rightarrow$

$\Rightarrow 53^{4085} \equiv_{100} 53^5 \equiv_{100} 9 \cdot 9 \cdot 53 \equiv 81 \cdot 53 \equiv_{100} 93$

81
53
243
405
4293

Calcula 2^{6124} en $\mathbb{Z}_{77}$.

$77 = 7 \cdot 11 \Rightarrow \varphi(77) = 6 \cdot 10 = 60$

$6124 = 60 \cdot 102 + 4 \Rightarrow 2^{6124} \equiv_{77} 2^4 = 16$

Considera el anillo $\mathbb{F} = \mathbb{Z}_3[x]/(x^3 + x^2 + 2)$. Demuestra que es un cuerpo y utiliza el Teorema de Lagrange para calcular $[2x+1]^{2860}$ en $\mathbb{F}$. Halla un generador de $\mathbb{F}^*$

$f(x) = x^3 + x^2 + 2$; $f(0) = 2$, $f(1) = 1$, $f(2) = 2$

$\Rightarrow f$ irred. $\Rightarrow \mathbb{F}$ cuerpo.

$|\mathbb{F}^*| = |\mathbb{F}| - 1 = 3^3 - 1 = 26$

$\Rightarrow [2x+1]^{26} = [1]$

$2860 = 26 \cdot 110 \Rightarrow [2x+1]^{2860} = [1]$