FDFDαH

Apellidos y nombre

AMPLIACIÓN DE MATEMÁTICAS 2019-2020
TRABAJO PRÁCTICO 11: Exponenciación en anillos finitos

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

$$a^{p-1} \equiv 1 (\text{mód } p)$$

Demuestra que **para todo entero** b es $b^p \equiv b (\text{mód } p)$. Distinguimos dos casos:

- Si $\text{mcd}(p,b)=1 \Rightarrow b^p \equiv b^{p-1} b \underset{PTF}{\equiv} b (\text{mód. } p)$
- Si $\text{mcd}(p,b) \neq 1 \underset{\text{por ser } p \text{ primo}}{\Rightarrow} p \mid b \Rightarrow b \equiv 0 (\text{mód. } p)$, $\Rightarrow b^p \equiv 0 (\text{mód. } p)$ $\Rightarrow b^p \equiv b (\text{mód. } p)$ ■

Utiliza el **Pequeño Teorema de Fermat** para calcular el resto de la división por 17 de los números: 5^{17}, 3^{83}, 23^{897}, 5^{580} y 987^{15440}.

$5^{17} \equiv 5 \cdot 5^{16} \underset{P.T.F.}{\equiv} 5 (\text{mód. } 17)$

$3^{83} \equiv 3^3 \cdot 3^{5 \cdot 16} \underset{PTF}{\equiv} 27 \equiv 10 (\text{mód. } 17)$

$23^{897} \equiv 23 \cdot 23^{56 \cdot 16} \underset{PTF}{\equiv} 23 \equiv 6 (\text{mód. } 17)$

$5^{580} \equiv 5^4 5^{36 \cdot 16} \underset{PTF}{\equiv} 5^4 \equiv 13 (\text{mód. } 17)$

$987^{15440} \equiv 987^{965 \cdot 16} \underset{PTF}{\equiv} 1 (\text{mód. } 17)$

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

$\mathbb{Z}_p^* = \{1, 2, \dots, p-1\} \Rightarrow \phi(p) = |\mathbb{Z}_p^*| = p-1$ (enteros positivos menores a p coprimos con el primo p)

Se sabe que, si p es un número primo, entonces $\phi(p^k) = (p-1)p^{k-1}$ y que, si m y n son coprimos, entonces $\phi(mn) = \phi(m)\phi(n)$. Calcula: $\phi(1234)$, $\phi(853)$, $\phi(9258)$ y $\phi(58042)$.

$\phi(\underbrace{1234}_{2 \cdot 617}) = \phi(2) \cdot \phi(617) = 616$

$\phi(853) = 852$

$\phi(\underbrace{9258}_{2 \cdot 3 \cdot 1543}) = \phi(2) \cdot \phi(3) \cdot \phi(1543) = 3084$

$\phi(\underbrace{58042}_{2 \cdot 29021}) = \phi(2) \cdot \phi(29021) = 29020$.

El **Teorema de Euler** asegura que, si a y n son coprimos, entonces $a^{\phi(n)} \equiv 1(\text{mód } n)$. Utiliza este resultado para hallar las dos últimas cifras de 91^{27923}.

↳ reducir módulo 100 $\phi(100) = \phi(2^2)\cdot\phi(5^2) =$

$= (2-1)\cdot 2^{2-1}\cdot(5-1)\cdot 5^{2-1} = 2^2 5^2$

$= \boxed{40} \rightsquigarrow a^{40} \equiv 1 \ (\text{mód. } 100),\ \forall a \in \mathbb{Z}$

Luego: $91^{27923} \equiv 91^3 \cdot 91^{698\cdot 40} \equiv 91^3 \equiv$

$\equiv 71 \ (\text{mód. } 100)$

↳ las últimas dos cifras son 7 y 1

Calcula $2^{1507097}$ en $\mathbb{Z}_{726}$.

$\phi(\underbrace{726}_{2\cdot 3\cdot 11^2}) = \phi(2)\cdot\phi(3)\cdot\phi(11^2) =$

$= (2-1)\cdot(3-1)\cdot(11-1)\cdot 11^{2-1} =$

$= \boxed{220} \rightsquigarrow a^{220} \equiv 1 \ (\text{mód. } 726),\ \forall a \in \mathbb{Z}$

$2^{1507097} \equiv 2^{685\cdot 220}\cdot 2^{97} \equiv 2^{97} \equiv (2^{10})^9 \cdot 2^7 \equiv (298^3)^3 \cdot 2^7 \equiv$

Considera el anillo $\mathbb{F} = \mathbb{Z}_3[x]/(x^3 - x + 1)$. Demuestra que este es un cuerpo, determina su cardinal y utiliza el **Teorema de Lagrange** para calcular $[x^2 + x - 1]^{2000}$ en $\mathbb{F}$. Halla un generador de $\mathbb{F}^*$.

$\equiv 166^3 \cdot 2^7 \equiv 496 \cdot 2^7 \equiv 326 \ (\text{mód. } 726)$

Como $\mathbb{Z}_3$ es cuerpo $\Longleftrightarrow$ $\mathbb{Z}_3[x]$ es DE.

Al ser $x^3 - x + 1 \in \mathbb{Z}_3[x]$ de grado 3 trivialmente, basta ver si no tiene raíces para tener si es o no irreducible.

Claramente $\left\{\begin{array}{l} 0^3 - 0 + 1 \neq 0 \\ 1^3 - 1 + 1 \neq 0 \\ 2^3 - 2 + 1 \neq 0 \end{array}\right\}$ luego este es irreducible.

Por consiguiente $\mathbb{F}$ es cuerpo. Además $|\mathbb{F}| = 3^3 = 27$.
Se sabe que $\mathbb{F}^*$ es un grupo cíclico de orden $26 = 2\cdot 13$
Luego, por el Teorema de Lagrange: $[a]^{26} \equiv [1]$ $\forall a \in \mathbb{F}^*$
Como $2000 = 26\cdot 77 - 2$; tenemos que

$[x^2+x-1]^{2000} \equiv (\underbrace{[x^2+x-1]^{-1}}_{\text{vamos a calcular el inverso de } x^2+x-1 \text{ en } \mathbb{F}})^2 \equiv [2x^2]^2 \equiv [x^2+2x] \neq [1]$ en $\mathbb{F}$

↳ utilizando el algoritmo de Euclides sale que este es $2x^2$.

Finalmente, para hallar un generador, vamos a tomar un elemento de orden 2 (el $[2]$ por ejemplo) y otro elemento de orden mayor que 2 (el $[2x^2]$ como se acaba de ver $\Rightarrow$ $[x^2]$ tiene orden 26 (generador)