

Teoría de números - I

Problemas de Criptología - Hoja 6

Curso 07-08

- 1 **Sistemas de congruencias.** Resuelve las siguientes congruencias:
 - (a) $a \equiv 0 \pmod{3}, a \equiv 1 \pmod{5}, a \equiv 2 \pmod{7}$.
 - (b) $a \equiv 0 \pmod{4}, a \equiv 2 \pmod{5}, a \equiv 4 \pmod{7}$.
 - (c) $a \equiv 2 \pmod{2}, a \equiv 5 \pmod{19}, a \equiv 15 \pmod{23}$.
- 2 **La ecuación** $x^2 \equiv 1 \pmod{p}$. Sea p un primo mayor que 3. Resuelve la ecuación $x^2 \equiv 1 \pmod{p}$.
- 3 **Resolución de una ecuación cuadrática.** Resuelve $x^2 \equiv 9 \pmod{23}$.
- 4 **Exponenciación modular.** Calcula las siguientes potencias usando el algoritmo de potencias cuadradas sucesivas.
 - (a) $38^{75} \pmod{103}$.
 - (b) $12^{1729} \pmod{19}$.
- 5 **El teorema de Fermat.** Comprueba con los siguientes números el teorema de Fermat: $p = 29, a = 19$ y $p = 53, a = 27$.
- 6 **La ecuación** $a^p \equiv a \pmod{p}$. Sea p un número primo. Prueba en 10 segundos que $a^p \equiv a \pmod{p}$. Tiempo...¡ya!
- 7 **Últimos dígitos.** ¿Cuáles son los tres últimos dígitos de 7^{803} ?
- 8 **Órdenes de elementos.** Determina el orden de 5 mod 1367 y de 13 mod 2547.
- 9 **Cálculos de potencias.** Calcula los siguientes valores:
 - (a) $23^{80} \pmod{109}$.
 - (b) $2^{1000000} \pmod{77}$.
- 10 **La función de Euler.** Calcula los siguientes valores de $\phi(n)$: $\phi(51), \phi(3^9), \phi(1.007), \phi(10^9)$.
- 11 **Raíces primitivas.** Hallar las raíces primitivas de $\mathbb{Z}_{11}$ y $\mathbb{Z}_{13}$.