

- (1) (a) Si  $(a, m) = 1$ , calcular la solución (única módulo  $m$ ) de la congruencia lineal

$$ax \equiv b \pmod{m}.$$

(b) Resolver la congruencia  $5x \equiv 3 \pmod{24}$ .

(c) Resolver la congruencia lineal  $25x \equiv 15 \pmod{120}$ .

- (2) Sea  $p$  un primo y  $f(x) = c_0 + c_1x + \dots + c_nx^n \in \mathbb{Z}[x]$ . Demostrar los siguientes resultados:

(a) **Teorema (Lagrange):** Si  $p \nmid c_n$ , entonces la congruencia polinómica  $f(x) \equiv 0 \pmod{p}$  tiene como mucho  $n$  soluciones.

(b) Si  $f(x) \equiv 0 \pmod{p}$  tiene más de  $n$  soluciones, entonces  $c_i \equiv 0 \pmod{p}$ ,  $i = 0, \dots, n$ .

**Observación:** El Teorema de Lagrange no es cierto si  $p$  no es primo. Por ejemplo, la congruencia  $x^2 \equiv 1 \pmod{8}$  tiene 4 soluciones.

- (3) Probar que  $5n^3 + 7n^5 \equiv 0 \pmod{12}$ , para todo entero  $n$ .

- (4) Encontrar todos los enteros positivos  $n$  para los que:

(a)  $n^{13} \equiv n \pmod{1365}$ ,

(b)  $n^{17} \equiv n \pmod{4080}$ .

- (5) Calcular:

$$\left(\frac{5}{3593}\right), \left(\frac{5}{3889}\right), \left(\frac{14}{137}\right), \left(\frac{55}{179}\right), \left(\frac{299}{397}\right), \left(\frac{37603}{48611}\right).$$

- (6) Demostrar que  $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$  para cualquier primo impar  $p$ .

- (7) (a) Sea  $q$  un primo impar tal que  $q \equiv 1 \pmod{4}$ , entonces  $q$  es un residuo cuadrático módulo  $p$  si y sólo si  $p \equiv r \pmod{q}$ , donde  $r$  es un residuo cuadrático módulo  $q$ .

(b) Calcular  $\left(\frac{5}{p}\right)$ .

- (8) Sea  $p$  un primo, demostrar que el número de soluciones de

$$x^2 + y^2 \equiv 1 \pmod{p},$$

con  $0 \leq x, y < p$ , es par.

- (9) **El Símbolo de Jacobi**

Sea  $m$  un entero positivo impar. Podemos escribir  $m = p_1 \dots p_s$  donde  $p_i$  son primos impares, no necesariamente distintos. Se define el símbolo de Jacobi como:

$$\left(\frac{a}{m}\right) = \prod_{i=1}^s \left(\frac{a}{p_i}\right).$$

Si  $m$  y  $m'$  son enteros positivos impares, demostrar

(a)  $\left(\frac{a}{mm'}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{m'}\right)$ .

$$(b) \left(\frac{aa'}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{a'}{m}\right).$$

$$(c) \left(\frac{a}{m}\right) = \left(\frac{a'}{m}\right) \text{ si } a \equiv a' \pmod{m}.$$

(10) Si  $m$  es un entero positivo impar, demostrar

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}.$$

(11) Si  $m$  es un entero positivo impar,  $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$ .

(12) **Ley de reciprocidad cuadrática para el símbolo de Jacobi** Sean  $m$  y  $n$  enteros positivos impares tales que  $(m, n) = 1$ . Demostrar

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}.$$

El símbolo de Jacobi se puede generalizar aún mas, y es lo que se llama el **Símbolo de Kronecker**. Sea  $a = (-1)^nb$  y  $b, n$  enteros positivos, definimos

$$\left(\frac{a}{-1}\right) = (-1)^n = \text{signo}(a) \quad \text{y} \quad \left(\frac{a}{2}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \pmod{2}, \\ \left(\frac{2}{a}\right) & \text{si } a \equiv 1 \pmod{2}. \end{cases}$$

Así para un entero cualquiera  $n = (-1)^r 2^c m$  con  $(2, m) = 1$  definimos

$$\left(\frac{a}{n}\right) = (-1)^r \left(\frac{a}{2}\right)^c \left(\frac{a}{m}\right)$$

donde  $\left(\frac{a}{2}\right)$  se define como antes, y  $\left(\frac{a}{m}\right)$  es el símbolo de Jacobi.

(13) Si  $p$  es un primo impar, demostrar que el menor entero positivo que no es residuo cuadrático es menor que  $\sqrt{p} + 1$ .

(14) Demostrar que  $x^4 \equiv 25 \pmod{1013}$  no tiene solución.

(15) Demostrar que  $x^4 \equiv 25 \pmod{p}$  no tiene solución si  $p$  es un primo congruente a 13 ó 17 (mod 20).

(16) Si  $p$  es un primo congruente a 13 ó 17 (mod 20), demostrar que  $x^4 + py^4 = 25z^4$  no tiene soluciones enteras no triviales.