Práctico 5: Congruencias

Ejercicio 2. Sea m un entero fijo y suponga que $a \equiv b \pmod{m}$. Probar las siguientes propiedades:

i) $\lambda a \equiv \lambda b \pmod{m}$ para todo $\lambda \in \mathbb{Z}$ y $\boxed{a^n \equiv b^n} \pmod{m}$ para todo $n \in \mathbb{N}$;

ii) si $p(x)$ es un polinomio con coeficientes enteros entonces $p(a) \equiv p(b) \pmod{m}$.

$$\begin{array}{ll} a \equiv b \pmod{m} & \Rightarrow \; ac \equiv bd \pmod{m} \\ c \equiv d \pmod{m} & \quad\;\; a+c \equiv b+d \pmod{m} \end{array}$$

$\exists r_i$ tq $a \equiv r_i \pmod{m}$ y $0 \leq r_i < m$.

Ec: $ax \equiv b \pmod{m}$ tiene sol. sii $\text{mcd}(a,m) \mid b$, si tiene una sol. módulo m

$\Rightarrow$ tiene exactamente $d = \text{mcd}(a,m)$.

Ejercicio 8.

a. Demostrar que $10^n \equiv (-1)^n \pmod{11}$. $\forall n \geq 0$.

b. Enunciar y probar un criterio de divisibilidad entre 11.

c. Hallar el dígito d, de modo que el número $2d653874$ sea múltiplo de 11.

(a) Sabemos por el ej 2.: Si $a \equiv b \pmod{m}$ entonces $a^n \equiv b^n$ $\forall n \geq 0$.

$\Rightarrow$ Bastaría ver que $10 \equiv -1 \pmod{11}$

$11 \mid 10+1$ ✓

(b) Dado n, queremos ver si $11 \mid n$ o no, por (a) sabemos la clase de congruencia de las potencias de 10.

$$n = a_k a_{k-1} \dots a_1 a_0$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \qquad \text{con } a_i \in \{0, \dots, 9\}$$

Queremos ver la congruencia módulo 11

$$\longrightarrow n \equiv \sum_{i=0}^{k} a_i (-1)^i \equiv a_0(-1)^0 + a_1(-1)^1 + a_2(-1)^2 + \dots + (a_k)(-1)^k \pmod{11}$$

$$\equiv a_0 - a_1 + a_2 + \dots + (-1)^k a_k \pmod{11}$$

$$n \equiv 0 \pmod{11} \iff a_0 - a_1 + a_2 - a_3 + \dots + (-1)^k a_k \equiv 0 \pmod{11}$$

$$\iff 11 \mid (a_0 - a_1 + a_2 + \dots + (-1)^k a_k).$$

"n es múltiplo de 11 si y sólo si la suma alternada de sus dígitos lo es"

(c) d tal que 2d653874 es múltiplo de 11.

d t.q. $2-d+6-5+3-8+7-4 \equiv 0 \pmod{11}$

$d \equiv 2+6+7+3-5-4-8 \pmod{11}$

$\equiv 1 \pmod{11}$

Como $0 \leq d \leq 9 \Rightarrow d = 1$.

Ejercicio 9.

a. Probar que 2 es invertible módulo n si y solamente si n es impar. En tal caso, hallar el inverso.

b. Resolver la ecuación $2x + 1 \equiv 0 \pmod{69}$.

(a) a y b son inversos módulo n si $ab \equiv 1 \pmod{n}$, tenemos que ver que $\exists b$ tq $2b \equiv 1 \pmod{n} \Leftrightarrow n$ es impar.

$\exists b$ tq. $n \mid (2b-1)$ sii $\exists k, b$ t.q. $2b-1 = nk$

sii $\exists k, b$ tq $\boxed{2b - nk = 1}$

sii $mcd(2,n) = 1$

$mcd(a,b) = m \Rightarrow \exists c, d$ tales que $ac + bd = m$

$mcd(a,b) = 1 \Leftrightarrow \exists c, d$ tales que $ac + bd = 1$

n impar: $\exists q$ t.q $n = 2q+1$, queremos b, k tales que

b tq $2b \equiv 1$ $\Leftrightarrow$ $2b - nk = 1$

$2b - (2qk + k) = 1$

$k = 1$ $b = q + 1$

$\cancel{2q} + 2 - \cancel{2q} - 1 = 1$

El inverso es $b = q + 1$ donde $q = coc(n, 2)$

Hallemos el inverso de 2 módulo 69.

$69 = 34 \cdot 2 + 1 \Rightarrow q = 34 \Rightarrow \boxed{b = 35}$

(b) $2x + 1 \equiv 0 \pmod{69}$

$2x \equiv -1 \pmod{69} \Leftrightarrow \exists k, x$ tq $2x - nk = -1$

$\boxed{x = 9}$ -34 $k = 1$

Ejercicio 10.

a. Determinar el último dígito de 3^{55}. $\to$ usar $3^2 \equiv -1$

b. Hallar el resto de la división de 12^{1257} entre 5. usamos $12 \equiv 2$
$2^2 \equiv -1 \Rightarrow 2^4 \equiv 1$

c. Hallar 71^{10} (mód 141) $\to$ usar $71 \cdot 2 \equiv 1$
$\Rightarrow 71 = (2^{-1})$

(a) $3^{55} = a_k a_{k-1} \dots a_1 a_0$, queremos hallar a_0.

$\Rightarrow$ El último dígito (a_0) satisface: $\left.\begin{cases} 3^{55} \equiv a_0 \pmod{10} \\ 0 \leq a_0 \leq 9. \end{cases}\right\}$ queda det. de forma única.

Sabemos que $9 \equiv -1 \pmod{10}$

$$3^{55} = 3^{54} \cdot 3 = (3^2)^{27} \cdot 3 = 9^{27} \cdot 3 \equiv (-1)^{27} \cdot 3 \equiv (-1) \cdot 3 \equiv 7 \pmod{10}$$

$$\begin{cases} 3^{55} \equiv 7 \pmod{10} \\ 0 \leq 7 \leq 9 \end{cases}$$

(b) $12^{1257} \pmod 5$

Para simplificar podemos usar $12 \equiv 2 \pmod 5$

$$12^{1257} \equiv 2^{1257} \equiv 2^{1256} \cdot 2 \equiv (2^{4k}) \cdot 2 \equiv 2 \pmod 5$$

$2 \equiv 2$

$2^2 \equiv 4$ $(\equiv -1)$

$2^4 \equiv 1$

(c) $71^{10} \pmod{141}$

$71 \equiv (2^{-1}) \pmod{141}$

$$71 \equiv (2)^{-10} \equiv (2^{10})^{-1} \equiv (1024)^{-1} \equiv (37)^{-1} \pmod{141}$$

usar Algoritmo Extendido de Euclides para ver que $37^{-1} \bmod 141 = 61$