Ejercicio 2. Suponga que $a \equiv b \pmod{m}$, para cierto entero m fijo. Probar las siguientes propiedades:

a. $\lambda a \equiv \lambda b \pmod{m}$, para todo $\lambda \in \mathbb{Z}$.

b. $a^n \equiv b^n \pmod{m}$ para todo $n \in \mathbb{N}$.

c. Si $a \equiv 3 \pmod{5}$, hallar el resto de dividir $4a^3$ entre 5.

d. Usando las propiedades anteriores, probar que si $p(x) = \lambda_n x^n + \lambda_{n-1}x^{n-1} + \ldots + \lambda_1 x + \lambda_0$, es un polinomio con coeficientes enteros λ_i, entonces $p(a) \equiv p(b) \pmod{m}$, para todo $a, b \in \mathbb{Z}$.

e. Si $a \equiv 3 \pmod{5}$, hallar el resto de dividir $33a^3 + 3a^2 - 197a + 2$ por 5.

c) $a \equiv 3 \pmod 5$

queremos $4a^3 \equiv r \pmod 5$ con $0 \le r \le 4$

$a \equiv 3 \pmod 5 \Rightarrow a^3 \equiv 3^3 \pmod 5$

$\Rightarrow a^3 \equiv 27 \pmod 5$

$\Rightarrow a^3 \equiv 2 \pmod 5$

$\Rightarrow 4a^3 \equiv 4 \cdot 2 \pmod 5$

$\Rightarrow 4a^3 \equiv 8 \pmod 5$

$\Rightarrow 4a^3 \equiv 3 \pmod 5$

entonces el resto es 3

d) $p(x) = \lambda_n x^n + \lambda_{n-1} x^{n-1} + \ldots + \lambda_1 x + \lambda_0$ con λ_i entero

queremos ver que $a \equiv b \pmod m \Rightarrow p(a) \equiv p(b) \pmod m$

$a \equiv b \pmod m$

$\Rightarrow a^i \equiv b^i \pmod m$ para todo $0 \le i \le n$

$\Rightarrow \lambda_i a^i \equiv \lambda_i b^i \pmod m$

entonces $\lambda_n a^n \equiv \lambda_n b^n \pmod m$

$\lambda_{n-1} a^{n-1} \equiv \lambda_{n-1} b^{n-1} \pmod m$

$\vdots$

$\lambda_1 a \equiv \lambda_1 b \pmod m$

$\lambda_0 \equiv \lambda_0 \pmod m$

$\Rightarrow \lambda_n a^n + \lambda_{n-1} a^{n-1} + \ldots + \lambda_1 a + \lambda_0 \equiv \lambda_n b^n + \lambda_{n-1} b^{n-1} + \ldots + \lambda_1 b + \lambda_0 \pmod m$

$p(a) \equiv p(b) \pmod m$

e) $a \equiv 3 \pmod 5$

$33a^3 + 3a^2 - 197a + 2 \equiv r \pmod 5$ con $0 \leq r \leq 4$

$p(x) = 33x^3 + 3x^2 - 197x + 2$

$-197 \equiv -197 + \overbrace{200}^{\equiv 0 \pmod 5} \pmod 5$

$\equiv 3 \pmod 5$

$-197 = -200 + 3$

$a \equiv 3 \pmod 5$

$\Rightarrow p(a) \equiv p(3) \pmod 5$

$\equiv 33 \cdot 3^3 + 3 \cdot 3^2 - 197 \cdot 3 + 2 \pmod 5$

$\equiv 33 \cdot 27 + 27 - 197 \cdot 3 + 2 \pmod 5$

$\equiv 3 \cdot 2 + 2 + 3 \cdot 3 + 2 \pmod 5$

$\equiv 6 + 2 + 9 + 2 \pmod 5$

$\equiv 19 \pmod 5$

$\equiv 4 \pmod 5$

↑ resto

123

Ejercicio 5.

a. Determinar el último dígito de 3^{55} en base 10. Sugerencia: probar que $3^{55} \equiv a_0 \pmod{10}$; donde a_0 es el dígito buscado.

b. Hallar el resto de la división de 12^{1257} entre 5.

a) último dígito de 3^{55} en base 10

buscamos el resto de dividir 3^{55} entre 10

$3^{55} \equiv r \pmod{10}$ con $0 \leq r \leq 9$

$3^1 \equiv 3 \pmod{10}$

$3^2 \equiv 9 \pmod{10}$ $\quad 9 \equiv 9 - 10 \pmod{10}$

$\boxed{3^2 \equiv -1 \pmod{10}}$ $\quad 9 \equiv -1 \pmod{10}$

$(3^2)^m \equiv (-1)^m \pmod{10}$

$55 = 2 \cdot 27 + 1$

$3^{55} = 3^{2 \cdot 27 + 1} = 3^{2 \cdot 27} \cdot 3 = (3^2)^{27} \cdot 3$

$3^{55} \equiv (3^2)^{27} \cdot 3 \pmod{10}$

$\equiv (-1)^{27} \cdot 3 \pmod{10}$

$\equiv -3 \pmod{10}$

$\equiv 7 \pmod{10}$

$3^{55} \equiv 7 \pmod{10}$ $\Rightarrow$ el último dígito de 3^{55} en base 10 es 7.

b) resto al dividir 12^{1257} entre 5

buscamos $12^{1257} \equiv r \pmod 5$ con $0 \leq r \leq 4$

$12 \equiv 2 \pmod 5$

$\Rightarrow 12^{1257} \equiv 2^{1257} \pmod 5$

entonces buscamos $2^{1257} \equiv r \pmod 5$ con $0 \leq r \leq 4$

$2^2 \equiv 4 \pmod 5 \rightarrow 2^2 \equiv -1 \pmod 5$

$2^4 \equiv 16 \pmod 5 \rightarrow \boxed{2^4 \equiv 1 \pmod 5}$

$1257 = 4 \cdot 314 + 1$

$2^{1257} = 2^{4 \cdot 314 + 1} = 2^{4 \cdot 314} \cdot 2 = (2^4)^{314} \cdot 2$

$2^{1257} \equiv (2^4)^{314} \cdot 2 \pmod 5$

$\equiv 1^{314} \cdot 2 \pmod 5$

$\equiv 2 \pmod 5$

entonces el resto de dividir 12^{1257} entre 5 es 2.

Ejercicio 6.

a. Hallar el inverso de 2 módulo 141.

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

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

queremos resolver $2x + 1 \equiv 0 \pmod{69} \rightsquigarrow 2x \equiv -1 \pmod{69}$

si tuviéramos

$2x + 1 = 0 \iff 2x = -1 \iff \frac{1}{2} 2x = \frac{1}{2}(-1)$

↑ inverso de 2 en $\mathbb{R}$

Forma 1:

$2x \equiv -1 \pmod{69} \iff 2x \equiv 68 \pmod{69}$

(2 coprimo con 69)

$\iff 2x \equiv 2 \cdot 34 \pmod{69}$

$\iff x \equiv 34 \pmod{69}$

(porque 2 y 69 son coprimos)

* en el ejercicio 2 vimos:

$a \equiv b \pmod{m} \Rightarrow \lambda a \equiv \lambda b \pmod{m}$

en general el recíproco no vale

pero si λ y m son coprimos

$\lambda a \equiv \lambda b \pmod{m} \Rightarrow a \equiv b \pmod{m}$

* en general:

$$\lambda a \equiv \lambda b \pmod{m} \Rightarrow a \equiv b \left(\mod \frac{m}{mcd(m,\lambda)}\right)$$

Forma 2: $2x \equiv -1 \pmod{69}$

decimos que y es inverso de 2 modulo 69 si

$$2y \equiv 1 \pmod{69}$$

$$2x \equiv -1 \pmod{69} \iff \overbrace{y2}^{\equiv 1 \pmod{69}} x \equiv y(-1) \pmod{69}$$

$$\iff x \equiv y(-1) \pmod{69}$$

→ vamos a buscar el inverso de 2 módulo 69

2 y 69 son coprimos

tenemos la igualdad de Bezout:

$$2 \cdot 35 - 69 = 1$$

entonces $2 \cdot 35 - 69 \equiv 1 \pmod{69}$

$$2 \cdot 35 \equiv 1 \pmod{69}$$

(35 inverso de 2 modulo 69)

→ volvemos a $2x \equiv -1 \pmod{69}$

$2x \equiv -1 \pmod{69} \iff \underbrace{35 \cdot 2x}_{\equiv 1 \pmod{69}} \equiv 35(-1) \pmod{69}$

$\iff x \equiv -35 \pmod{69}$

$\iff x \equiv 34 \pmod{69}$

Ejercicio 7

d. $6x - 1 \equiv 5$ (mód 12).

$6x - 1 \equiv 5 \pmod{12}$

$6x \equiv 6 \pmod{12}$

6 y 12 no son coprimos $\Rightarrow$ 6 no tiene inverso modulo 12

$6x \equiv 6 \pmod{12}$

$6 \cdot x \equiv 6 \cdot 1 \pmod{12} \iff x \equiv 1 \left(\mod \frac{12}{\text{mcd}(12,6)} \right)$

$\iff x \equiv 1 \pmod{2}$

$6x \equiv 6 \pmod{12} \iff 12 \mid 6x - 6$

$\iff 6x - 6 = 12q$

$\iff x - 1 = 2q$

$\iff 2 \mid x - 1$

$\iff x \equiv 1 \pmod{2}$