Congruencias

definición: Sea $n \in \mathbb{Z}$ fijo

Dados a y $b \in \mathbb{Z}$, decimos que a es congruente con b modulo n o que a y b son congruentes módulo n si $n \mid a-b$

escribimos: $a \equiv b \pmod{n}$

* $a \equiv b \pmod{n} \iff a$ y b tienen el mismo resto al dividir entre n

* dado a existe un unico $r \in \{0, 1, .., n-1\}$ tal que $a \equiv r \pmod{n}$
  $\Rightarrow$ r es el resto al dividir entre n

* $$\left.\begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array}\right\} \Rightarrow a+c \equiv b+d \pmod{n} \text{ y } ac \equiv bd \pmod{n}$$

① $a+c \equiv b+d \pmod{n} \iff n \mid (a+c)-(b+d)$

$$\left.\begin{array}{l} a \equiv b \pmod{n} \Rightarrow n \mid a-b \\ c \equiv d \pmod{n} \Rightarrow n \mid c-d \end{array}\right] \Rightarrow n \mid \underbrace{(a-b)+(c-d)}_{a-b+c-d \,=\, (a+c)-(b+d)}$$

$\Rightarrow n \mid (a+c)-(b+d)$

$\Rightarrow a+c \equiv (b+d) \pmod{n}$

② $ac \equiv bd \pmod{n} \iff n \mid ac-bd$

$a \equiv b \pmod{n} \Rightarrow n \mid a-b \Rightarrow n \mid c(a-b) \Rightarrow n \mid ac-bc$

$c \equiv d \pmod{n} \Rightarrow n \mid c-d \Rightarrow n \mid b(c-d) \Rightarrow n \mid bc-bd$

$$\left.\begin{array}{l} n \mid ac-bc \\ n \mid bc-bd \end{array}\right\} \Rightarrow n \mid ac-\cancel{bc}+\cancel{bc}-bd \Rightarrow n \mid ac-bd$$

$\Rightarrow ac \equiv bd \pmod{n}$

Ejercicio 1.

a. Si $a \equiv 22 \pmod{14}$, hallar el resto de dividir a por 2, por 7 y por 14.

b. Verifique que se cumplen las siguientes congruencias: $5! \equiv 12 \pmod{36}$; $i! \equiv 0 \pmod{36}$, $\forall\, i \geq 6$.

c. Hallar, para cada $n \in \mathbb{N}$, el resto de dividir $S_n = \sum_{i=1}^{n} (-1)^i \cdot i!$ por 36.

a) $a \equiv 22 \pmod{14}$

* buscamos $a = 2Q + r$ con $0 \leq r \leq 1$

$a \equiv 22 \pmod{14} \Rightarrow 14 \mid a - 22$

$\Rightarrow a - 22 = 14q$ para algún $q \in \mathbb{Z}$

$\Rightarrow a = 14q + 22$

$= 2 \cdot 7q + 2 \cdot 11$

$= 2(7q + 11)$

$\Rightarrow$ el resto de dividir a entre 2 es 0

* $a \equiv 22 \pmod{14}$

resto de dividir a entre 14?

<u>forma 1</u>: $a \equiv 22 \pmod{14} \Rightarrow 14 \mid a - 22$

$\Rightarrow a - 22 = 14q$ para algún $q \in \mathbb{Z}$

$\Rightarrow a = 14q + 22$

$= 14q + 14 + 8$

$= 14(q+1) + \underbrace{8}_{\uparrow}$

$\Rightarrow$ el resto es 8

<u>forma 2</u>: $a \equiv 22 \pmod{14} \Rightarrow a$ y 22 tienen el mismo resto al dividir entre 14

$\Rightarrow$ el resto de dividir a entre 14 es 8

$a \equiv 22 \pmod{14}$

$0 \equiv -14 \pmod{14}$

$a \equiv 22 - 14 \pmod{14}$

b) * $5! \equiv 12 \pmod{36}$?

$5! = 2 \cdot 3 \cdot 4 \cdot 5 = 120$

$5! \equiv 120 \pmod{36}$

$+ \quad 0 \equiv -36 \cdot 3 \pmod{36}$

$5! \equiv 120 - 108 \pmod{36}$

$5! \equiv 12 \pmod{36}$

$5! \equiv 120 \pmod{36}$

$120 = 36 \cdot 3 + 12$

$120 \equiv 12 \pmod{36}$

$\Rightarrow 5! \equiv 12 \pmod{36}$

* $i! \equiv 0 \pmod{36}$ para todo $i \geq 6$

$i \geq 6 \Rightarrow i! = \underbrace{2 \cdot 3}\cdot 4 \cdot 5 \cdot \underbrace{6} \cdots (i-1) i$

$= 2 \cdot 3 \cdot 6 \cdot 4 \cdot 5 \cdot 7 \cdots (i-1) i$

$= 36 \cdot 4 \cdot 5 \cdot 7 \cdots (i-1) i$

$\Rightarrow i!$ es multiplo de 36

$\Rightarrow$ el resto de dividir $i!$ entre 36 es 0

$\Rightarrow i! \equiv 0 \pmod{36}$

c) $n \in \mathbb{N}$

buscamos el resto de dividir $S_n = \sum_{i=1}^{n} (-1)^i i!$ entre 36

$\Rightarrow S_n \equiv r_n \pmod{36}$ con $0 \leq r_n \leq 35$

* $\underline{n=1}$: $S_1 = (-1)^1 1! = -1$

$S_1 \equiv -1 \pmod{36}$

$S_1 \equiv -1 + 36 \pmod{36}$

$\boxed{S_1 \equiv 35 \pmod{36}}$ $\Rightarrow$ resto 35

$* \; n=2: \quad S_2 = \sum_{i=1}^{2} (-1)^i i! = -1+2 = 1$

$\boxed{S_2 \equiv 1 \pmod{36}} \Rightarrow$ resto 1

$* \; n=3: \quad S_3 = \sum_{i=1}^{3} (-1)^i i! = -1+2-3! = -1+2-6 = -5$

$S_3 \equiv -5 \pmod{36}$

$\boxed{S_3 \equiv 31 \pmod{36}} \Rightarrow$ resto 31

$* \; n=4: \quad S_4 = \sum_{i=1}^{4} (-1)^i i! = S_3 + (-1)^4 4! = -5+4! = -5+24 = 19$

$\boxed{S_4 \equiv 19 \pmod{36}} \Rightarrow$ resto 19

$* \; n=5: \quad S_5 = \sum_{i=1}^{5} (-1)^i i! = 19-5! = 19-120 = -101$

$S_5 \equiv -101 \pmod{36}$

$S_5 \equiv \underbrace{-101+3 \cdot 36}_{7} \pmod{36}$

$\boxed{S_5 \equiv 7 \pmod{36}} \Rightarrow$ resto 7

$* \; n=6: \quad S_6 = \sum_{i=1}^{6} (-1)^i i! = S_5 + 6!$

$S_6 \equiv S_5 + 6! \pmod{36} \qquad 6! \equiv 0 \pmod{36}$

$S_6 \equiv 7+0 \pmod{36}$

$\boxed{S_6 \equiv 7 \pmod{36}} \Rightarrow$ resto 7

$* \; n=7: \quad S_7 = \sum_{i=1}^{7} (-1)^i i! = \overbrace{\sum_{i=1}^{5} (-1)^i i!}^{S_5} + \overline{6!} - \overline{7!}$

$S_7 \equiv S_5 + 6! - 7! \pmod{36}$

$S_7 \equiv 7+0-0 \pmod{36}$

$$\boxed{S_7 \equiv 7 \pmod{36}} \rightsquigarrow \text{resto } 7$$

$* \; n \geq 6$ $\quad S_n = \sum_{i=1}^{n} (-1)^i i! = \sum_{i=1}^{5} (-1)^i i! + \sum_{i=6}^{n} (-1)^i i!$

$$= S_5 + \sum_{i=6}^{n} (-1)^i i!$$

$$S_n \equiv S_5 + \sum_{i=6}^{n} (-1)^i \underbrace{i!}_{\equiv 0 \pmod{36}} \pmod{36}$$

$$S_n \equiv S_5 \pmod{36}$$

$$\boxed{S_n \equiv 7 \pmod{36}} \rightsquigarrow \text{resto } 7$$

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 $n \in \mathbb{N}$. Sugerencia: usar el teorema del binomio.

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.

m fijo

$a \equiv b \pmod{m}$

a) si $\lambda \in \mathbb{Z}$, $\lambda a \equiv \lambda b \pmod{m} \iff m \mid \overbrace{\lambda a - \lambda b}^{\lambda(a-b)}$

$$a \equiv b \pmod{m} \Rightarrow m \mid a-b$$
$$\Rightarrow m \mid \lambda(a-b)$$
$$\Rightarrow m \mid \lambda a - \lambda b$$
$$\Rightarrow \lambda a \equiv \lambda b \pmod{m}$$

recíproco? $\underbrace{\lambda a \equiv \lambda b \pmod{m}}_{m \mid \lambda(a-b)} \Rightarrow \underbrace{a \equiv b \pmod{m}}_{m \mid a-b}$?

no es cierto

$m \mid \lambda(a-b) \xrightarrow[\text{cuando } mcd(m,\lambda)=1]{} m \mid a-b$

por ejemplo:

$$3\cdot 4 \equiv 0 \pmod 6$$
$$3\cdot 2 \equiv 0 \pmod 6$$

entonces $3\cdot 4 \equiv 3\cdot 2 \pmod 6$ pero $4 \not\equiv 2 \pmod 6$

b) $\underbrace{a \equiv b \pmod m}_{m \mid a-b} \Rightarrow a^n \equiv b^n \pmod m \iff m \mid a^n - b^n$

con el binomio de Newton: $(x+y)^n = (x+y)(x+y)\cdots(x+y)$

$$a^n - b^n = (b + (a-b))^n - b^n$$
$$= \cancel{b^n} + \binom{n}{1} b^{n-1}(a-b) + \binom{n}{2} b^{n-2}(a-b)^2 + \dots + (a-b)^n - \cancel{b^n}$$
$$= \binom{n}{1} b^{n-1}\underline{(a-b)} + \binom{n}{2} b^{n-2}\underline{(a-b)^2} + \dots + \underline{(a-b)^n}$$

$$a \equiv b \pmod m \Rightarrow m \mid a-b$$
$$\Rightarrow m \mid \binom{n}{1} b^{n-1}(a-b) + \dots + (a-b)^n$$
$$\Rightarrow m \mid a^n - b^n$$
$$\Rightarrow a^n \equiv b^n \pmod m$$

Otra forma de probarlo:

$$\left[\left.\begin{array}{l} a \equiv b \pmod m \\ c \equiv d \pmod m \end{array}\right\} \Rightarrow ac \equiv bd \pmod m\right]$$

$$\left.\begin{array}{l} \left.\begin{array}{l} a \equiv b \pmod m \\ a \equiv b \pmod m \end{array}\right\} \Rightarrow a^2 \equiv b^2 \pmod m \\ \qquad\qquad\qquad\qquad\qquad a \equiv b \pmod m \end{array}\right\} \Rightarrow a^3 \equiv b^3 \pmod m$$

paso inductivo: Suponemos $a^{n-1} \equiv b^{n-1} \pmod m$

y queremos probar $a^n \equiv b^n \pmod m$

$$\left.\begin{array}{l} a^{n-1} \equiv b^{n-1} \pmod m \\ a \equiv b \pmod m \end{array}\right\} \Rightarrow a^n \equiv b^n \pmod m$$

c) tenemos $a \equiv 3 \pmod 5 \leftrightarrow a-3 = 5q$

buscamos el resto de dividir $4a^3$ entre 5

$a \equiv 3 \pmod 5$

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

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

$4a^3 \equiv 4 \cdot 27 \pmod 5$ $\qquad 27 \equiv 2 \pmod 5$

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

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