Congruencias

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

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

notación: $a \equiv b \pmod{n}$

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

* dado a existe un unico $r \in \{0, 1, \dots, n-1\}$ tal que $a \equiv r \pmod{n}$
  $\rightarrow$ r es el resto al dividir a entre 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) $a \equiv 22 \pmod{14}$ $\quad 22 = 14 + 8 \rightsquigarrow 22 \equiv 8 \pmod{14}$

$a \equiv 22 \pmod{14}$

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

$a \equiv 8 \pmod{14}$

* resto de dividir a entre 2?

$a \equiv 8 \pmod{14} \Rightarrow 14 \mid a - 8$

$\Rightarrow a - 8 = 14q$ para algún $q \in \mathbb{Z}$

$\Rightarrow a = 14q + 8$

$a = 14q + 8 = 2 \cdot 7q + 2 \cdot 4 = 2(7q + 4) + 0$

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

* resto de dividir a entre 7?

$a = 14q + 8 = \underbrace{14q + 7}\, + 1 = 7(2q + 1) + 1$

$\Rightarrow$ el resto de dividir a entre 7 es 1

* resto al dividir a entre 14?

$a \equiv 22 \pmod{14} \Rightarrow a$ y 22 tienen el mismo resto al dividir entre 14

$\Rightarrow$ el resto al dividir a entre 14 es 8.

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

resto al dividir $5!$ entre 36?

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

$120 = 3 \cdot 36 + 12$

$120 \equiv 12 \pmod{36}$

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

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

para ver que $i! \equiv 0 \pmod{36}$ vamos a ver que $i!$ es multiplo de 36 y por lo tanto tiene resto 0 al dividir entre 36

$$i! = i(i-1) \cdots 7 \cdot \underset{\uparrow}{6} \cdot 5 \cdot 4 \cdot \underset{\uparrow}{\underline{3 \cdot 2}}$$

$$= \underbrace{6 \cdot 3 \cdot 2}_{36}\, i(i-1) \cdots 7 \cdot 5 \cdot 4$$

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

$\Rightarrow i!$ es multiplo de 36

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

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

buscamos

$$S_n \equiv \underset{\substack{\uparrow \\ \text{resto}}}{r_n} \pmod{36} \quad \text{con} \quad 0 \leq r_n \leq 35$$

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

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

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

$S_1 \equiv 35 \pmod{36} \Rightarrow r_1 = 35$

* $\underline{n=2}$: $S_2 = \underbrace{(-1)^1 1!}_{S_1} + (-1)^2 2! = -1 + 2 = 1$

$S_2 \equiv 1 \pmod{36} \Rightarrow r_2 = 1$

* $\underline{n=3}$: $S_3 = \underbrace{(-1)^1 1! + (-1)^2 2!}_{S_2} + (-1)^3 3! = 1 - 6 = -5$

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

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

$S_3 \equiv 31 \pmod{36} \Rightarrow r_3 = 31$

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

$S_4 \equiv 19 \pmod{36} \Rightarrow r_4 = 19$

* $\underline{n=5}$: $S_5 = S_4 + (-1)^5 5! = S_4 - 5!$

$S_5 \equiv S_4 - 5! \pmod{36}$

$S_5 \equiv 19 - 12 \pmod{36}$

$S_5 \equiv 7 \pmod{36} \Rightarrow r_5 = 7$

* $\underline{n=6}$: $S_6 = S_5 + (-1)^6 6!$

$S_6 \equiv S_5 + (-1)^6 6! \pmod{36}$ $\quad 6! \equiv 0 \pmod{36}$

$S_6 \equiv S_5 \pmod{36}$

$S_6 \equiv 7 \pmod{36} \Rightarrow r_6 = 7$

* $\underline{n \geq 6}$:

$$S_n = \sum_{i=1}^{n} (-1)^i \, i!$$

$$= \underbrace{\sum_{i=1}^{5} (-1)^i \, i!}_{S_5} + \sum_{i=6}^{n} (-1)^i \, \underbrace{i!}_{\equiv 0 \pmod{36}}$$

$$S_n \equiv \underbrace{S_5}_{\equiv 7 \pmod{36}} + \underbrace{\sum_{i=6}^{n} (-1)^i \, i!}_{\equiv 0 \pmod{36}} \pmod{36}$$

$$\Rightarrow S_n \equiv 7 \pmod{36} \qquad \Rightarrow r_n = 7$$

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 $n \in \mathbb{N}$.

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 $p(a) \equiv p(b) \pmod{m}$.

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

Tenemos $a \equiv b \pmod{m}$

a) queremos ver que $\overbrace{\lambda a \equiv \lambda b \pmod{m}}^{m \mid \lambda a - \lambda b}$

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ \lambda \equiv \lambda \pmod{m} \end{array}\right\} \Rightarrow \lambda a \equiv \lambda b \pmod{m}$$

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

$\Rightarrow a - b = mq$ para algún $q \in \mathbb{Z}$

$\Rightarrow \lambda(a-b) = \lambda m q$

$\Rightarrow \lambda a - \lambda b = m \lambda q$

$\Rightarrow m \mid \lambda a - \lambda b$

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

$\underline{\text{Recíproco}}$? $\lambda a \equiv \lambda b \pmod{m} \Rightarrow a \equiv b \pmod{m}$?

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

$\Rightarrow m \mid \lambda(a-b)$

$\Rightarrow m \mid a-b$ si m y λ son coprimos

Contraejemplo:

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

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

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

b) Suponemos $a \equiv b \pmod m$

querenos ver que $a^n \equiv b^n \pmod m$

Forma 1:

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

Vamos a probar que $a^n \equiv b^n \pmod m$ por inducción

caso base: $n = 1$: $a \equiv b \pmod m$ ✓

$n = 2$: $\left.\begin{array}{l} a \equiv b \pmod m \\ a \equiv b \pmod m \end{array}\right\} \Rightarrow a^2 \equiv b^2 \pmod m$

paso inductivo

Suponemos que $a^n \equiv b^n \pmod m$ y queremos ver que $a^{n+1} \equiv b^{n+1} \pmod m$

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

Forma 2: con el binomio de Newton

$$(x+y)^n = x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \dots + \binom{n}{n-1} x y^{n-1} + y^n$$

$$(x+y)(x+y)(x+y) \cdots (x+y)$$

queremos ver que $\underbrace{a \equiv b \pmod m}_{m \mid a-b} \Rightarrow \underbrace{a^n \equiv b^n \pmod m}_{m \mid a^n - b^n}$

$$a^n - b^n = (\overbrace{b}^{x} + \overbrace{(a-b)}^{y})^n - b^n$$

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

$$\Rightarrow a^n - b^n = \binom{n}{1} b^{n-1} \underbrace{(a-b)}_{\text{divisible ehre } m} + \binom{n}{2} b^{n-2} \underbrace{(a-b)^2}_{\text{divisible ehre } m} + \dots + \underbrace{(a-b)^n}_{\text{divisible ehre } m}$$

$$\Rightarrow m \mid a^n - b^n$$

$$\Rightarrow a^n \equiv b^n \pmod{m}$$