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

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

(i) $\lambda \in \mathbb{Z}$ y $a \equiv b \pmod m \Rightarrow \lambda a \equiv \lambda b \pmod m$

$m \mid (a-b)$

· Hay que ver que $m \mid (\lambda a - \lambda b) = \lambda(a-b) \rightsquigarrow m \mid (a-b) \mid \lambda(a-b)$ ✓

· $m \mid (a-b)$, queremos ver que $m \mid a^n - b^n$

· Opciones: ① Si $\boxed{a-b \mid a^n - b^n}$, tenemos que $m \mid a^n - b^n$ por transitividad.

② Inducción: $\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \Rightarrow a \cdot c \equiv bd \pmod m$

Usar lo anterior y que $a^2 \equiv b^2 \pmod m$

③ Binomio de Newton: $a \equiv b \pmod m \Rightarrow a = m.k + b$

$\Rightarrow a^n = (mk+b)^n = b^n + \dot{m}$

① $a^n - b^n = (a-b) \cdot (a^{n-1} + b \cdot a^{n-2} + b^2 a^{n-3} + \ldots + a \cdot b^{n-2} + b^{n-1}) = (a-b) \cdot \boxed{\sum_{i=0}^{n-1} a^i b^{n-i-1}}$

$a^n - b a^{n-1} + b^2 a^{n-2} \ldots$

(ii) Sea $p(x) = \lambda_0 + \lambda_1 x + \lambda_2 \cdot x^2 + \ldots + \lambda_k x^2$

Ppd: $\begin{cases} a \equiv b \pmod n \\ c \equiv d \pmod n \end{cases} \Rightarrow a + c \equiv b + d \pmod n$

Si $\begin{cases} \lambda_i \cdot b^i \equiv \lambda_i \cdot a^i \ (n) \\ \lambda_j \cdot b^j \equiv \lambda_j \cdot a^j \ (n) \end{cases} \Rightarrow \lambda_i a^i + \lambda_j a^j \equiv \lambda_i b^i + \lambda_j b^j$

· Es decir, si $\boxed{\lambda_i a^i \equiv \lambda_i b^i \pmod n}$ $\forall i: 0 \leq i \leq k \Rightarrow p(a) \equiv p(b) \pmod n$

· $\begin{cases} \lambda_0 \equiv \lambda_0 \ (n) \\ \lambda_1 \cdot a \equiv \lambda_1 \cdot b \ (n) \quad \text{por la parte (i)} \\ a^i \equiv b^i \quad '' \\ \lambda_i \cdot a^i \equiv \lambda_i b^i \quad '' \end{cases}$

Basta ver que $\begin{cases} \lambda_0 \equiv \lambda_0 \quad (n) \\ \lambda_1 a \equiv \lambda_1 b \quad (n) \quad \text{ppd anterior} \\ \vdots \\ \lambda_k a^k \equiv \lambda_k b^k \, (n) \end{cases}$

$a^k \equiv b^k \quad (n)$ ppd previa

$\downarrow$

$\lambda \cdot a^k \equiv \lambda b^k \quad (n)$ ppd previa

Ejercicio 5.

a. Probar que si a y b son enteros y p un número primo entonces $\boxed{(a+b)^p \equiv a^p + b^p \pmod{p}}$
¿Vale el resultado si p no es primo?

b. Probar (por inducción) el Teorema de Fermat: $a^p \equiv a \pmod{p}$, para todo a entero y todo primo p.

$a^{p-1} \equiv 1 \pmod{p}$

(a) $p \mid (a+b)^p - a^p - b^p$

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = b^p + a^p + \boxed{\sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}}$$

Hay que ver que $\displaystyle\sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-1} \equiv 0 \pmod{p}$

$\left(\text{i.e.} \quad p \mid \sum_{1}^{p-1} \binom{p}{i} a^i b^{p-i}\right)$

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$$

Como $0<i<p \Rightarrow \begin{cases} i! \text{ no es divisible entre } p: \ i! = i(i-1)\dots(2)(1) \\ (p-i)! \text{ no es divisible entre } p: \ (p-i)(p-i-1)\dots \end{cases}$

$$\binom{p}{i} = p \cdot \frac{(p-1)!}{i!\,(p-i)!} \equiv 0 \pmod{p}$$

$$\Rightarrow \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} \equiv 0 \pmod{p} \quad \text{como queríamos}$$

Contraejemplo: $(1+1)^4 = 2^4 = 16 \equiv 0 \pmod{4}$

$1^4 + 1^4 = 2 \equiv 2 \pmod{4}$

($i = 2$ en el binomio $\Rightarrow i!(p-i)!$ es múltiplo de 4)

(b) Paso base: $0^p \equiv 0 \pmod{p}$, $1^p \equiv 1 \pmod{p}$

Paso ind: $a^p \equiv a \pmod{p}$, queremos ver $(a+1)^p \equiv (a+1) \pmod{p}$

$$\Rightarrow (a+1)^p \equiv \underbrace{a^p + 1^p}_{\text{parte anterior con } b=1} \equiv a^p + 1 \pmod{p} \underset{\text{paso ind + paso base}}{\equiv} a+1 \pmod{p}$$

Ejercicio 7. Sea $n \in \mathbb{N}$ cuya representación en base 10 es $\underbrace{a_k a_{k-1} \cdots a_2}a_1 a_0$.

a. Probar que $n \equiv 2a_1 + a_0 \pmod 4$.

b. Probar que $n \equiv 4a_2 + 2a_1 + a_0 \pmod 8$.

c. Enunciar y demostrar un resultado similar a los anteriores para 2^i, $i < k$.

→ Práctico 1.

Ejercicio 10. Sea $n \in \mathbb{N}$ cuya representación en base 10 es $a_k a_{k-1} a_{k-2} \cdots a_4 a_3 a_2 a_1 a_0$. Demostrar que:

a. $2|n$ si y sólo si $2|a_0$.

b. $4|n$ si y sólo si $4|a_1 a_0$.

c. $8|n$ si y sólo si $8|a_2 a_1 a_0$.

d. Establecer el resultado general sugerido por los casos anteriores.

e. Investigar si 32 divide a 1.273.460.

(a) $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots$

$= a_0 + a_1 \cdot 10 + \dot{4}$

$\Rightarrow n \equiv a_0 + a_1 \cdot 10 \pmod 4$

$10 \equiv 2 \pmod 4$

$\Rightarrow n \equiv a_0 + a_1 \cdot 2 \pmod 4$

$= \sum_{i=0}^{k} a_i \cdot 10^i$

$= a_0 + a_1 \cdot 10 + \sum_{i=2}^{k} a_i \cdot 10^i$

$= a_0 + a_1 \cdot 10 + 10^2 \cdot \sum_{i=0}^{k} a_i \cdot 10^{2-i}$

$= a_0 + a_1 \cdot 10 + 4 \cdot (25 \sum \dots)$

$n = a_0 + a_1 (2 \cdot 4 + 2) + 4 \cdot (25 \cdot \sum \dots)$

$= a_0 + a_1 \cdot 2 + 4 \cdot (\underbrace{2a_1 + 25 \sum \dots})$

$n \equiv a_0 + a_1 \cdot 2 \pmod 4$

(b) $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \dots$

$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + 10^3 \cdot A$

$n \equiv a_0 + a_1 \cdot 2 + a_2 \cdot 4 + 0 \pmod 8$

Ppd: $a \equiv b \ (m)$, $c \equiv d$

$a + c \equiv b + d \ (m)$

(c) $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots = \sum_{i=0}^{k} a_i \cdot 10^i$

$2^k | 10^k \Rightarrow 2^k | 10^j \ \forall j \geq k$

$n \equiv a_0 + a_1 \cdot 10 + \dots + a_{j-1} \cdot 10^{j-1} \pmod{2^j}$

$+ \underbrace{a_j \cdot 10^j + \dots}_{\dot{(2^j)}}$

⇒ Ahora cambiar 10^i por el resto de dividir 10^i entre 2^j

$a \equiv r \pmod n$ donde r es el resto de dividir a entre n.

⇒ Puedo elegir $0 \leq r < 10$ tq $10^i \equiv r \mod 2^i$

$\boxed{\text{Caso } 2^k}$

$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3$

r_i resto de dividir 10^i entre 2^k

$n \equiv a_0 + a_1 \cdot r_1 + a_2 \cdot r_2 + a_3 \cdot r_3 \dots \pmod{2^k}$

$n = a_0 + a_1 \cdot \underset{2}{\overset{\shortparallel}{r_1}} + a_2 \cdot \underset{0}{\overset{\shortparallel}{r_2}}$

Observación: $r_i = 0$ si $i \geq k$

$n \equiv (a_0 + a_1 \cdot r_1 + \dots + a_{k-1} r_{k-1}) + a_k \cdot 0 + \dots \pmod{2^k}$