Cosas básicas de congruencias

Si $x \equiv x' \pmod{m}$

$y \equiv y' \pmod{m}$

entonces $x + y \equiv x' + y' \pmod{m}$

$xy \equiv x'y' \pmod{m}$

si $n \in \mathbb{N}$ $x^n \equiv (x')^n \pmod{m}$

Si $a \equiv 13 \pmod 5$

calcular el resto al dividir

$33a^3 + 3a^2 - 197a + 2$ entre 5

Ideas: números "más chicos" son más fáciles de manejar

Como las operaciones básicas y los polinomios se pueden hacer mód 5, cambio los elementos que pueda por otros más chicos con la misma congruencia

$33 = 30 + 3 = 6 \cdot 5 + 3$

$33 \equiv 3 \pmod 5$

Facundo: reducir los coeficientes.

continuamos esta idea →

Benjamín: expresar y reducir a

Idea: Tengo un polinomio evaluado en a

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

$a \equiv 13 \pmod 5 \equiv 3 \pmod 5$

mejor hacer $p(3)$ que $p(13)$

$\Rightarrow p(a) \equiv p(13) \pmod 5 \equiv p(3) \pmod 5$

Puedo calcular $33 \cdot 3^3 + 3 \cdot 3^2 - 197 \cdot 3 + 2$ y dividir entre 5 ✓

$33a^3 + 3a^2 - 197a + 2$ (mód 5) juntando

$33 \equiv 3 \pmod 5$ $\quad 33a^3 \equ 3 \cdot 2 \pmod 5$

$3 \equiv 3 \pmod 5$ $\quad + 3a^2 \equ 3 \cdot 4 \pmod 5$

$197 \equiv 2 \pmod 5$ $\quad - 197a \equ 2 \cdot 3 \pmod 5$

$2 \equiv 2 \pmod 5$ $\quad + 2 \equ 2 \pmod 5$

$p(a) \equ 3 \cdot 2 + 3 \cdot 4 - 2 \cdot 3 + 2 \pmod 5$

$\equ 1 + 2 - 1 + 2 \pmod 5$

$\equ 4 \pmod 5$

$a \equ 3 \pmod 5$

$a^2 \equ 3^2 \pmod 5 \equ 9 \pmod 5 \equ 4 \pmod 5$

$a^3 \equ 3^3 \pmod 5 \equ 27 \pmod 5 \equ 2 \pmod 5$

también pueb. así

$-197 \equiv -2 \ (5)$

$\equiv 3 \ (5)$

Hallar todos los x tales que

$$x + 3 \equiv 2 \pmod 8$$

$$x + 3 = 8k + 2 \longrightarrow x + 3 - 3 = 8k + 2 - 3$$

$$x = 8k + 2 - 3 = 8k - 1$$

$$x \equiv -1 \pmod 8 \equiv 7 \pmod 8$$

¿Se puede "pasar restando"? (¿Qué era eso?)

¿Se puede "pasar restando" módulo m?

$$x + 3 \equiv 2 \pmod 8$$

$$x + 3 - 3 \equiv 2 - 3 \pmod 8 \equiv -1 \pmod 8$$

$$x \equiv -1 \pmod 8 \text{ sii } x = -1 + 8k, \ k \in \mathbb{Z}$$

$x^2 - 1 \equiv 0 \pmod{35}$

$x^2 \equiv 1 \pmod{35}$

Lo peor que me puede pasar es tener que elevar al cuadrado 35 números (buscar todas las x a mano)

Si escribimos $35 = 5 \cdot 7$, por el Teo Chino del Resto

$$x^2 \equiv 1 \pmod{35} \iff \begin{cases} x^2 \equiv 1 \pmod{5} \\ x^2 \equiv 1 \pmod{7} \end{cases}$$

(a cada uno le ajusto a 1)

8 3 1

↳ la solución del sistema es única

$x^2 \equiv 1 \pmod 5$ pruebo 5 números:

x	x^2		¿cuáles son $\equiv 1 \pmod 5$?
0	0	0	X
1	1	1	✓
2	4	4	X
3	9	4	X
4	16	1	✓

$x \equiv 1 \pmod 5$

o $x \equiv 4 \pmod 5$

$x^2 \equiv 1 \pmod 7$ 7 números

x	x^2		
0	0	0	x
1	1	1	✓
2	4	4	x
3	9	2	x
4	16	2	x
5	25	4	x
6	36	1	✓

$x \equiv 1 \pmod 7$

o $x \equiv 6 \pmod 7$

Hay que ver las 4 posibilidades

$x \equiv 104 \pmod 5$, $x \equiv 166 \pmod 7$

① $x \equiv 1 \pmod 5$, $x \equiv 1 \pmod 7$

$x \equiv 1 \pmod{35}$ ⟼ es único (T. Ch. del R.)

② $x \equiv 1 \pmod 5$, $x \equiv 6 \pmod 7$

7 posibilidades

1
6
11
16
21
26
31

6
13
20
27
34

$x \equiv 6 \pmod{35}$ verifica

ya probamos que los otros no, pero si lo encontrate, sé que es único por el T. Ch. del R.

(3) $x \equiv 4 \pmod 5$, $x \equiv 1 \pmod 7$

4
9
14
19
24
29 ✓
34

1
8
15
22
29 ✓

$x \equiv 29 \pmod{35}$

(4) $x \equiv 4 \pmod 5$, $x \equiv 6 \pmod 7$

$x \equiv 34 \pmod{35}$

6
13
20
27
34

Las soluciones son $x = 1, 6, 29 \circ 34 + 35k$

con $k \in \mathbb{Z}$

Idea

$x^2 - 1 = (x+1)(x-1)$

2 casos

- $x+1 \equiv 0 \pmod 5$
- $x-1 \equiv 0 \pmod 5$

2 casos

- $x+1 \equiv 0 \pmod 7$
- $x-1 \equiv 0 \pmod 7$

$x+1 \equiv 0 \pmod m \Rightarrow (x+1)(x-1) \equiv 0 \pmod m$

ó $x-1 \equiv 0 \pmod m$

$\Leftarrow$ Sólo es válido

$a \equiv 0 \pmod m \Rightarrow ab \equiv 0 \pmod m$ Si m es primo.

ó $b \equiv 0 \pmod m$ $\Leftarrow$

$3x \equiv 7 \pmod{16}$

$\Updownarrow$ (porque son invertibles)

$3x(-5) \equiv 7(-5) \pmod{16}$

$-15x \equiv -35 \pmod{16}$, $-15 \equiv 1 \pmod{16}$

$x \equiv -35 \pmod{16}$ $\qquad 35 = 32 + 3$

$\equiv -3 \pmod{16}$

$\equiv 13 \pmod{16}$