

QUÈ HEM FET FINS ARA?

El darrer que hem treballat és el l'estudi de les equacions diofàntiques i el començament del tema de les congruències.

CLASSE D'AVUI 11/12/2020

Avui continuem amb tema de les congruències definint formalment les operacions després de la introducció de les operacions amb un exemple.

Recordem la taula de la suma i de la multiplicació a $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ del darrer exemple:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

•	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Però en aquesta definició s'ha d'anar amb molta cura amb el següent: si hem de fer $\bar{2} + \bar{3}$ a \mathbb{Z}_4 sabem que $\bar{2} = \bar{6}$, $\bar{3} = \bar{-1}$ podríem fer l'operació de diverses maneres, com per exemple $\bar{2} + \bar{3} = \bar{5} = \bar{1}$ que també la podem calcular com $\bar{6} + \bar{-1} = \bar{5} = \bar{1}$ que dona el mateix. La possible problemàtica és si el resultat serà el mateix si fem servir uns representants o uns altres per les classes d'equivalència. Per exemple si fem la multiplicació $\bar{2} \cdot \bar{3} = \bar{2}$ i també $\bar{6} \cdot \bar{-1} = \bar{-6} = \bar{2}$.

Sempre dona el mateix resultat malgrat que canviem els representants escollits per fer l'operació? Sí.

PROP.: Si $a \equiv a' \pmod{m}$ i $b \equiv b' \pmod{m}$ llavors $a + b \equiv a' + b' \pmod{m}$ i $ab \equiv a'b' \pmod{m}$.

DEM.: Per hipòtesi $a \equiv a' \pmod{m}$ i $b \equiv b' \pmod{m}$ o sigui que

$$\left. \begin{array}{l} a = a' + k_1m \\ b = b' + k_2m \end{array} \right\} \Rightarrow a + b = a' + k_1m + b' + k_2m = a' + b' + (k_1 + k_2)m \Rightarrow \\ \Rightarrow a + b \equiv a' + b' \pmod{m}$$

I amb el producte passa el mateix:

$$ab = (a' + k_1m)(b' + k_2m) = a'b' + a'k_2m + k_1mb' + k_1mk_2m = \\ = a'b' + (a'k_2 + k_1b' + k_1k_2m)m \Rightarrow ab \equiv a'b' \pmod{m}$$

I aquesta propietat justifica que es pot introduir una suma i una multiplicació a \mathbb{Z}_m que està ben definida.

DEF.: En el conjunt $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$ es defineixen dues operacions de la manera següent:

$$\bar{a} + \bar{b} = \overline{a+b}, \bar{a} \cdot \bar{b} = \overline{a \cdot b} \text{ per a tot } \bar{a}, \bar{b} \in \mathbb{Z}_m.$$

Aquestes operacions estan ben definides:

PROP.: La suma i el producte estan ben definits.

DEM.: Cal veure que la suma i el producte tenen un resultat únic i que sempre es pot calcular. Això és cert perquè al final es redueix a una suma o una multiplicació a \mathbb{Z} i a més no depèn del representant que s'agafi per fer l'operació, és a dir: si $a \equiv a' \pmod{m}$ i $b \equiv b' \pmod{m}$ llavors $\bar{a} + \bar{b} = \overline{a' + b'}$ i $\bar{a} \cdot \bar{b} = \overline{a' \cdot b'}$, cosa certa per la darrera proposició.

A més aquestes operacions tenen les propietats importants de la suma i la multiplicació de nombres enters:

PROP.: La suma i el producte definits a les classes modulars tenen les propietats següents:

SUMA

Commutativa: Per a tot $\bar{a}, \bar{b} \in \mathbb{Z}_m$ tenim que $\bar{a} + \bar{b} = \bar{b} + \bar{a}$

Associativa: Per a tot $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ tenim que $\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$

Existència element neutre: Existeix $\bar{0} \in \mathbb{Z}_m$ tal que per a tot $\bar{a} \in \mathbb{Z}_m$ tenim que $\bar{a} + \bar{0} = \bar{a}$

Existència element invers (oposat): Per a tot $\bar{a} \in \mathbb{Z}_m$ existeix $\neg\bar{a} \in \mathbb{Z}_m$ tal que $\bar{a} + \neg\bar{a} = \bar{0}$

"Suma repetida": Per a tot $n \geq 1$ tenim que $\bar{a} + \overset{veg}{n} \cdot \bar{a} = n\bar{a} = \overline{n\bar{a}}$

PRODUCTE

Commutativa: Per a tot $\bar{a}, \bar{b} \in \mathbb{Z}_m$ tenim que $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$

Associativa: Per a tot $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ tenim que $\bar{a} \cdot (\bar{b} \cdot \bar{c}) = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$

Existència element neutre: Existeix $\bar{1} \in \mathbb{Z}_m$ tal que per a tot $\bar{a} \in \mathbb{Z}_m$ tenim que $\bar{a} \cdot \bar{1} = \bar{a}$

"Producte repetit": Per a tot $n \geq 1$ tenim que $\bar{a} \cdot \overset{veg}{n} \cdot \bar{a} = \bar{a}^n = \overline{a^n}$

DISTRIBUTIVA DEL PRODUCTE RESPECTE DE LA SUMA: Per a tot $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ tenim que $\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$

DEM.: Totes aquestes propietats surten de la corresponent propietat en els nombres enters. Per exemple: en els nombres enters tenim que

$$a + b = b + a \Rightarrow \overline{a + b} = \overline{b + a} \Rightarrow \bar{a} + \bar{b} = \bar{b} + \bar{a}.$$

O per exemple: $a \cdot 1 = a \Rightarrow \overline{a \cdot 1} = \bar{a} \Rightarrow \bar{a} \cdot \bar{1} = \bar{a}.$

Les propietats d'aquestes dues operacions (exceptuant les de "repetició" de suma i de producte) se satisfan en molts altres conjunts i operacions per la qual reben un nom global: es diu que és un anell amb la suma i el producte. Així podem dir que \mathbb{Z}_m és un anell amb la suma i el producte. Per exemple, és el mateix que passa amb els polinomis a coeficients reals amb la suma i la multiplicació.

Ara practiquem aquestes operacions en el conjunt de les classes modulars:

EX.: Quin és el residu de dividir $58 \cdot 79$ mòdul 11?

En lloc d'utilitzar el factor 58 utilitzem el factor 3 que és congruent amb 58 però que facilitarà els càlculs. Això es diu reduir el nombre mòdul 11 (sumant o restant múltiples de 11, o calculant el residu de la divisió per 11, fins arribar a un nombre en el rang $0, 1, 2, 3, \dots, m-1$). Fem el mateix amb el segon factor: $79 \equiv 2 \pmod{11}$. Llavors:

$$58 \cdot 79 \equiv 3 \cdot 2 = 6 \pmod{11}$$

EX.: Calculeu les dues últimes xifres de $4^{1000000}$ a mà (no necessitem calculadora).

Les dues últimes xifres s'obtenen calculant $4^{1000000}$ mòdul 100. Calculem les primeres potències de 4:

$$4^1 \pmod{100} = 4$$

$$4^2 \pmod{100} = 16$$

$$4^3 \pmod{100} = 64 = -36$$

$$4^4 \pmod{100} = 56 = -44$$

$$4^5 \pmod{100} = 24$$

$$4^6 \pmod{100} = 96 = -4$$

$$4^7 \pmod{100} = 84 = -16$$

$$4^8 \pmod{100} = 36$$

$$4^9 \pmod{100} = 44$$

$$4^{10} \pmod{100} = 76 = -24$$

$$4^{11} \pmod{100} = 4$$

i a partir d'aquí es repeteixen els resultats. Ara mirem quants 11s hi ha en 1000000 fent la divisió entera:

1000000	11
1	90909

 $\rightarrow 1000000 = 11 \cdot 90909 + 1$

Per tant:

$$4^{1000000} = 4^{11 \cdot 90909 + 1} = (4^{11})^{90909} 4^1 \equiv 4^{90909} 4 = 4^{90910}$$

Ara fem el mateix amb l'exponent

90910	11
6	8264

 $\rightarrow 90910 = 11 \cdot 8264 + 6$

Aleshores:

$$4^{90910} = 4^{11 \cdot 8264 + 6} = (4^{11})^{8264} 4^6 \equiv 4^{8264} 4^6 = 4^{8270}$$

Repetim el mateix amb l'exponent

8270	11
9	751

 $\rightarrow 8270 = 11 \cdot 751 + 9$

Llavors:

$$4^{8270} = 4^{11 \cdot 751 + 9} = (4^{11})^{751} 4^9 \equiv 4^{751} 4^9 = 4^{760}$$

Repetim el mateix amb l'exponent

760	11
1	69

 $\rightarrow 760 = 11 \cdot 69 + 1$

Aleshores:

$$4^{760} = 4^{11 \cdot 69 + 1} = (4^{11})^{69} 4^1 \equiv 4^{69} 4^1 = 4^{70}$$

Finalment fem el mateix amb el darrer exponent

70	11
4	6

 $\rightarrow 70 = 11 \cdot 6 + 4$

Llavors:

$$4^{70} = 4^{11 \cdot 6 + 4} = (4^{11})^6 4^4 \equiv 4^6 4^4 = 4^{10} = 76$$

Per tant les dues darreres xifres són 76.