QUÈ HEM FET FINS ARA?

El darrer dia vam continuar amb el tema de les congruències, resolent equacions, trobant inversos i finalment començant els sistemes d'equacions.

CLASSE D'AVUI 17/12/2020

Avui continuem amb els sistemes d'equacions i els resultats teòrics.

Fem un altre exemple de com fer els sistemes d'equacions abans de mirar en general si es poden fer sempre com a l'exemple que vam fer el darrer dia.

EX.: (45) Una banda de 13 pirates s'apodera d'una caixa de monedes d'or. Si es repartissin equitativament, en sobrarien 8. Moren 2 pirates. Si es repartissin ara en sobrarien 3. Desapareixen 3 pirates més. En la repartició, ara en sobrarien 5. Quin és el mínim nombre de monedes d'or?

La interpretació de les dades que ens donen en el problema ens porten a plantejar un sistema de congruències. Diem $x =$"nombre de monedes d'or" llavors:

$$\left.\begin{array}{c} x \equiv 8 \pmod{13} \\ x \equiv 3 \pmod{11} \\ x \equiv 5 \pmod{8} \end{array}\right\}$$

Resolem primer el sistema determinat per les dues primeres equacions:

$$\left.\begin{array}{c} x \equiv 8 \pmod{13} \\ x \equiv 3 \pmod{11} \end{array}\right\} \Leftrightarrow \left.\begin{array}{c} x = 8 + 13a \\ x = 3 + 11b \end{array}\right\} \Rightarrow 8 + 13a = 3 + 11b \Rightarrow 13a - 11b = -5$$

Aquesta equació diofàntica té solució ja que $mcd(13, 11) = 1|5$. Una identitat de Bézout per 13 i 11 és molt fàcil de trobar:

1	0	1	−5
0	1	−1	6
	1	5	2
13	11	2	1
2	1	0	

Aleshores:

$$13 \cdot (-5) + 11 \cdot (6) = 1 \Rightarrow 13 \cdot (25) + 11 \cdot (-30) = -5 \Rightarrow 13 \cdot (25) - 11 \cdot (30) = -5$$

Per tant les solucions de l'equació diofàntica són $a = 25 + 11t, b = 30 + 13t$ i d'aquí:
$x = 8 + 13a = 8 + 13(25 + 11t) = 333 + 143t$

o sigui $x \equiv 333 \pmod{143}$ que és el mateix que dir $x \equiv 47 \pmod{143}$. Observem que no hem fet servir per res el resultat obtingut de la b.

I ara fem el mateix amb aquesta congruència i la tercera (i darrera del sistema):

$$\left.\begin{array}{r} x \equiv 47 (\operatorname{mod} 143) \\ x \equiv 5 (\operatorname{mod} 8) \end{array}\right\} \Leftrightarrow \left.\begin{array}{r} x = 47 + 143a \\ x = 5 + 8b \end{array}\right\} \Rightarrow 47 + 143a = 5 + 8b \Rightarrow 143a - 8b = -42$$

Aquesta equació diofàntica té solució ja que $mcd(143, 8) = 1|{-42}$. Una identitat de Bézout per 143 i 8 és també molt fàcil de calcular:

1	0	1	−1
0	1	−17	18
	17	1	7
143	8	7	1
7	1	0	

Llavors:
$143 \cdot (-1) + 8 \cdot (18) = 1 \Rightarrow 143 \cdot (42) + 8 \cdot (-756) = -42 \Rightarrow$
$\Rightarrow 143 \cdot (42) - 8 \cdot (756) = -42$

Per tant les solucions de l'equació són $a = 42 + 8t, b = 756 + 143t$ i d'aquí la
$x = 47 + 143a = 47 + 143(42 + 8t) = 6053 + 1144t$

o sigui $x \equiv 6053 (\operatorname{mod} 1144)$ que és el mateix que dir $x \equiv 333 (\operatorname{mod} 1144)$. Per tant el mínim número de monedes d'or del tresor és 333.

Aquesta manera de procedir dona la solució en general del problema de resoldre un sistema del tipus

$$\left.\begin{array}{c} x \equiv a_1 (\operatorname{mod} m_1) \\ x \equiv a_2 (\operatorname{mod} m_2) \\ \ldots \\ x \equiv a_n (\operatorname{mod} m_n) \end{array}\right\}$$

El resultat general que estudia aquests sistemes (molt usuals en aplicacions tecnològiques com a la criptografia i comunicacions en general) s'anomena el teorema xinès dels residus (però no el farem). Per trobar aquests resultats generals necessitem la propietat següent de les congruències que ens ajudarà:

PROP.:
$a \equiv b (\operatorname{mod} m_1), a \equiv b (\operatorname{mod} m_2), \ldots, a \equiv b (\operatorname{mod} m_n) \Leftrightarrow a \equiv b (\operatorname{mod} mcm(m_1, m_2, \ldots, m_n))$.

DEM.: Aquesta propietat és certa perquè:
$a \equiv b (\operatorname{mod} m_1), a \equiv b (\operatorname{mod} m_2), \ldots, a \equiv b (\operatorname{mod} m_n) \Leftrightarrow m_1|a - b, m_2|a - b, \ldots, m_n|a - b \Leftrightarrow$
$\Leftrightarrow mcm(m_1, m_2, \ldots, m_n)|a - b \Leftrightarrow a \equiv b (\operatorname{mod} mcm(m_1, m_2, \ldots, m_n))$

El primer resultat general que donarem és que si tenim una solució del sistema llavors sabem determinar-les totes:

PROP.: Si coneixem x_0 una solució particular del sistema

$$\left.\begin{array}{l} x \equiv a_1(\operatorname{mod} m_1) \\ x \equiv a_2(\operatorname{mod} m_2) \\ \quad\ldots \\ x \equiv a_n(\operatorname{mod} m_n) \end{array}\right\}$$

aleshores totes les solucions del sistema són $x \equiv x_0(\operatorname{mod} mcm(m_1, m_2, \ldots, m_n))$.

DEM.: Si x és una solució del sistema llavors $x \equiv a_i(\operatorname{mod} m_i)$ per $i = 1, 2, \ldots, n$ però també sabem que $x_0 \equiv a_i(\operatorname{mod} m_i)$ per $i = 1, 2, \ldots, n$ per la qual cosa $x \equiv x_0(\operatorname{mod} m_i)$ per $i = 1, 2, \ldots, n$ i això hem vist abans que és equivalent a dir que $x \equiv x_0(\operatorname{mod} mcm(m_1, m_2, \ldots, m_n))$. Ara és fàcil veure que tot nombre de la forma $x = x_0 + t \bullet mcm(m_1, m_2, \ldots, m_n)$ és solució del sistema.

EX.: Sigui el sistema

$$\left.\begin{array}{l} x \equiv 0(\operatorname{mod} 3) \\ x \equiv 1(\operatorname{mod} 4) \\ x \equiv 2(\operatorname{mod} 5) \end{array}\right\}$$

Verifiqueu que -3 és una solució i trobeu totes les solucions.

És molt fàcil comprovar que és solució del sistema: $-3 \operatorname{mod} 3 = 0$, $-3 \operatorname{mod} 4 = 1$, $-3 \operatorname{mod} 5 = 2$ per tant és una solució. Aplicant l'anterior teorema les solucions són $x \equiv -3(\operatorname{mod} mcm(3,4,5)) \ \equiv -3(\operatorname{mod} 60)$ és a dir $x = -3 + 60t$ per a tot t enter.

I com es veu si un sistema d'aquest tipus té solució o no? Veurem només el cas de dues equacions:

$$\left.\begin{array}{l} x \equiv a_1(\operatorname{mod} m_1) \\ x \equiv a_2(\operatorname{mod} m_2) \end{array}\right\} \Leftrightarrow \left.\begin{array}{l} x = a_1 + m_1 a \\ x = a_2 + m_2 b \end{array}\right\} \Rightarrow a_1 + m_1 a = a_2 + m_2 b \Rightarrow m_1 a - m_2 b = a_2 - a_1$$

per tant tindrà solució si i només si $mcd(m_1, m_2) | a_2 - a_1$.

PROP.: El sistema $\left.\begin{array}{l} x \equiv a_1(\operatorname{mod} m_1) \\ x \equiv a_2(\operatorname{mod} m_2) \end{array}\right\}$ té solució $\Leftrightarrow$ $mcd(m_1, m_2) | a_2 - a_1$

DEM.: OK.

Es poden donar resultats més generals però no els estudiarem (teorema xinès dels residus).

També ens podem plantejar sistemes amb diverses variables i totes les congruències amb el mateix mòdul. Aquests sistemes es fan igual que es procedeix a $\mathbb{R}$ sempre que el mòdul sigui primer. Si el mòdul no és primer s'ha d'anar amb més cura amb els raonaments.

EX.: (26) Resoleu el sistema $\overline{3}\overline{x} + \overline{5}\overline{y} = \overline{0}, \overline{2}\overline{x} - \overline{y} = \overline{1}$ a $\mathbb{Z}_7$.

Fem-lo per Gauss: ($\overline{3}^{-1} = \overline{5}, \overline{5}^{-1} = \overline{3}$)

$$\left(\begin{array}{cc|c} \overline{3} & \overline{5} & \overline{0} \\ \overline{2} & -\overline{1} & \overline{1} \end{array}\right) \to \left(\begin{array}{cc|c} \overline{1} & \overline{4} & \overline{0} \\ \overline{2} & -\overline{1} & \overline{1} \end{array}\right) \to \left(\begin{array}{cc|c} \overline{1} & \overline{4} & \overline{0} \\ \overline{0} & \overline{5} & \overline{1} \end{array}\right) \to \left.\begin{array}{c} \overline{y} = \overline{3} \\ \overline{x} = \overline{2} \end{array}\right\}$$

I ens queda només un teorema potent en el curs: el petit teorema de Fermat.

PROP.: (petit teorema de Fermat) Si p és primer i $\overline{a} \neq \overline{0}$ a $\mathbb{Z}_p$ llavors: $\overline{a}^{p-1} = \overline{1}$ (o si es prefereix $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$).

DEM.: Si fem el producte dels nombres $1, 2, 3, \ldots, (p-1)$ obtenim un resultat diferent de zero ja que tots són no nuls. Si ara multipliquem cada nombre per a obtenim els nombres $1a, 2a, 3a, \ldots, (p-1)a$ que són els mateixos que els anteriors (però desordenats) ja que dos a dos són diferents (si dos fossin iguals tindríem $ia \equiv ja \Rightarrow i \equiv j$, però com que $i, j = 1, 2, 3, \ldots, p-1$ tindrem $i = j$). Per tant els dos productes seran iguals:

$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv 1a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a (\mathrm{mod}\, p) \Leftrightarrow$

$\Leftrightarrow 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) a^{p-1} (\mathrm{mod}\, p) \Leftrightarrow 1 \equiv a^{p-1} (\mathrm{mod}\, p)$

perquè el nombre $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ és no nul.

EX.: (26) . Calculem el residu de 43^{3221} mòdul 13.

En pirmer lloc simplifiquem els càlculs: $43^{3221} \equiv 4^{3221}\ (\mathrm{mod}\, 13)$. Aplicant el petit teorema de Fermat sabem que $4^{12} \equiv 1 (\mathrm{mod}\, 13)$. Aleshores fem la divisió entera de 3221 entre 12 (per quants 12s hi ha dintre de 3221):

3221	12
5	268

$\to 3221 = 268 \cdot 12 + 5$

Llavors: $43^{3221} = 4^{268 \cdot 12 + 5} = (4^{12})^{268} 4^5 \equiv 1^{268} 4^5 \equiv 4^5 \equiv 4^2 4^2 4^1 \equiv 9 \cdot 4 \equiv 10 (\mathrm{mod}\, 13)$.