QUÈ HEM FET FINS ARA?

El darrer dia vam continuar amb el tema de les congruències definint formalment les operacions, les seves propietats, etc.

CLASSE D'AVUI 14/12/2020

Avui continuem amb el tema de les congruències, resolent equacions, trobant inversos i finalment començant els sistemes d'equacions.

Tenim un segon bloc de propietats de les congruències que parlen fonamentalment de com simpolifiar expressions a l'hora de fer càlculs o fer equacions:

PROP.:

1. Si $a \equiv b(\mathrm{mod}\, m)$ i $d|m$ llavors $a \equiv b(\mathrm{mod}\, d)$.

2. Si $k \neq 0$ llavors: $ka \equiv kb(\mathrm{mod}\, km) \Leftrightarrow a \equiv b(\mathrm{mod}\, m)$.

3. Si $mcd(k,m) = 1$ llavors: $ka \equiv kb(\mathrm{mod}\, m) \Leftrightarrow a \equiv b(\mathrm{mod}\, m)$

DEM.:

1. Si $a \equiv b(\mathrm{mod}\, m)$ i $d|m$ llavors $a - b = km, m = k'd$ per certs enters k, k', per tant $a - b = kk'd \Rightarrow a \equiv b(\mathrm{mod}\, d)$.

2. Si $k \neq 0$ i tenim $ka \equiv kb(\mathrm{mod}\, km) \Leftrightarrow ka - kb = k'km$ per cert $k' \Leftrightarrow ka - kb = k'km$ per cert $k' \Leftrightarrow a - b = k'm$ per cert $k' \Leftrightarrow a \equiv b(\mathrm{mod}\, m)$.

3. Si $mcd(k,m) = 1$ i tenim $ka \equiv kb(\mathrm{mod}\, m)$ o sigui $ka - kb = k'm$ per cert $k' \Leftrightarrow k(a-b) = k'm$ per cert k', aleshores $k|k'$ (pel Lema de Gauss) i per tant $k' = kk''$ per cert $k'' \Rightarrow k(a-b) = kk''m \Rightarrow a - b = k''m \Leftrightarrow a \equiv b(\mathrm{mod}\, m)$

La implicació cap a l'altre cantó és trivial $a \equiv b(\mathrm{mod}\, m) \Rightarrow ka \equiv kb(\mathrm{mod}\, m)$.

Veiem com s'utilitzen aquest resultats per resoldre equacions:

EX.: Resoleu les congruències indicant quina de les propietats anteriors utilitzeu:

a) $5x \equiv 10(\mathrm{mod}\, 9)$

b) $3x \equiv 6(\mathrm{mod}\, 9)$

c) $15x \equiv 30(\mathrm{mod}\, 9)$

d) $8x \equiv 28(\mathrm{mod}\, 6)$

a) $5x \equiv 10(\mathrm{mod}\, 9) \Leftrightarrow_{3)} x \equiv 2(\mathrm{mod}\, 9) \Leftrightarrow x = 2 + 9t$ per tot enter t

a´) $5x \equiv 4(\mathrm{mod}\, 9) \Leftrightarrow 5x \equiv -5(\mathrm{mod}\, 9) \Leftrightarrow_{3)} x \equiv -1(\mathrm{mod}\, 9) \Leftrightarrow_{3)} x \equiv 8(\mathrm{mod}\, 9)$

b) $3x \equiv 6(\mathrm{mod}\, 9) \Leftrightarrow_{2)} x \equiv 2(\mathrm{mod}\, 3)$

c) $15x \equiv 30(\mathrm{mod}\, 9) \Leftrightarrow_{2)} 5x \equiv 10(\mathrm{mod}\, 3) \Leftrightarrow_{3)} x \equiv 2(\mathrm{mod}\, 3)$

d) $8x \equiv 28(\mathrm{mod}\, 6) \Leftrightarrow_{2)} 4x \equiv 14(\mathrm{mod}\, 3) \Leftrightarrow x \equiv 2(\mathrm{mod}\, 3)$

Observeu que de vegades val la pena simplificar (reduir mòdul 6 o 3) però de

vegades no. Per exemple si es redueix a l'inici aquesta equació obtenim $2x \equiv 4 (\mathrm{mod}\, 6) \Leftrightarrow x \equiv 2 (\mathrm{mod}\, 3)$; però per exemple $2x \equiv 7 (\mathrm{mod}\, 3) \Leftrightarrow 2x \equiv 1 (\mathrm{mod}\, 3)$ no facilitaria els càlculs. Ara podeu repassar les cinc congruències a veure si fent simplificacions a l'inici es fan més fàcilment.

EX.: (1) Demostreu que per a tot $n \geq 0$, $2^4 \cdot 7^{n+1} + (6 \cdot 9^n)^2$ és múltiple de 148 usant congruències.

És a dir, ens demanen demostrar que $2^4 \cdot 7^{n+1} + (6 \cdot 9^n)^2 \equiv^{???} 0 \bmod 148$. Podem veure que hi ha factors comuns a tot arreu:

$4(2^2 \cdot 7^{n+1} + 3^2 9^{2n}) \equiv^{???} 0 \bmod 2^2 37 \Leftrightarrow 2^2 \cdot 7^{n+1} + 3^2 9^{2n} \equiv^{???} 0 \bmod 37$

També podem simplificar: $9^2 \bmod 37 = 81 \bmod 37 = 7$ i llavors ens queda un càlcul molt simple:

$2^2 \cdot 7^{n+1} + 3^2 9^{2n} \equiv 2^2 \cdot 7^{n+1} + 3^2 7^n = 7^n (2^2 \cdot 7^1 + 3^2) = 7^n (37) \equiv 0 \bmod 37$

Just el que es volia demostrar.

EX.: (10) Demostreu que no hi ha cap enter n tal que $7n + 2$ sigui un cub.

Volem veure que no té solució l'equació $x^3 = 7n + 2 \equiv 2 \bmod 7$. Si existís un enter x tal que $\bar{x}^3 = \bar{2}$ a $\mathbb{Z}_7$ llavors aquest x seria una arrel cúbica de 2. Però si observem els cubs en $\mathbb{Z}_7$ veurem que és impossible:

x	$x^3 \bmod 7$
0	0
1	1
2	1
3	6
4	-6
5	-1
6	-1

Per tant no tindrà mai solució perquè els cubs a $\mathbb{Z}_7$ no donen mai $\bar{2}$.

EX.: (11) Quina xifra s'ha de posar en el lloc de z perquè el nombre $9z86$ en dividir-lo per 11 tingui residu 5?

Ens demanen trobar z tal que

$9z86 \equiv 5 \bmod 11 \Leftrightarrow 6 + 8 \cdot 10 + z \cdot 10^2 + 9 \cdot 10^3 \equiv 5 \bmod 11 \Leftrightarrow$

$\Leftrightarrow 6 + 8 \cdot (-1) + z \cdot 1 + 9 \cdot (-1) \equiv 5 \bmod 11 \Leftrightarrow z \equiv 5 \bmod 11 \Leftrightarrow z = 5 + 11t$ per t enter

Per $t = 0$ ens dona $z = 5$ l'única solució (els altres valors de t no dona un resultat entre 0 i 9).

EX.: (12) Demostreu el criteri de divisibilitat següent: n és múltiple de 4 sii el nombre

format pels dos últims dígits de n és múltiple de 4.

$n = a_k a_{k-1} \ldots a_1 a_{0(10}$ és múltiple de

$4 \Leftrightarrow a_0 + a_1 10 + a_2 10^2 + \ldots + a_{k-1} 10^{k-1} + a_k 10^k \equiv 0 \bmod 4 \Leftrightarrow$

$\Leftrightarrow a_0 + a_1 10 + a_2 0 + \ldots + a_{k-1} 0 + a_k 0 \equiv 0 \bmod 4 \Leftrightarrow a_0 + a_1 10 \equiv 0 \bmod 4 \Leftrightarrow a_1 a_{0(10}$ és múltiple de 4

És molt més usual la formulació equivalent següent:

$n = a_k a_{k-1} \ldots a_1 a_{0(10}$ és múltiple de $4 \Leftrightarrow a_0 + 2a_1 \equiv 0 \bmod 4$

EX.: Tenim una ALU que utilitza nombres de k xifres escrits en hexadecimal emmagatzemats en els seus registres. Demostreu el criteri de divisibilitat següent pels nombres que utilitza aquesta màquina: n és múltiple de 17 sii la suma de les xifres en possició parella menys les de posició senar dona múltiple de 17.

Seguint el mateix raonament que a l'exercici anterior:

n és múltiple de $17 \Leftrightarrow a_0 + a_1 16 + a_2 16^2 + \ldots + a_{k-1} 16^{k-1} + a_k 16^k \equiv 0 \bmod 17 \Leftrightarrow$

$\Leftrightarrow a_0 + a_1 (-1) + a_2 + \ldots + a_{n-1} (-1)^{n-1} + a_n (-1)^n \equiv 0 \bmod 17$

Quan hem mirat les propietats que complia la suma i el producte hem trobat a faltar de vegades l'existència d'invers per la multiplicació (per exemple ho vam veure a la taula de la multiplicació a $\mathbb{Z}_4$ que uns elements en tenien i uns altres no). Mirem un exemple abans d'examinar què passa en general:

EX.: A $\mathbb{Z}_{452}$ determineu els inversos (si existeixen) de $a = \overline{2}$ i de $a = \overline{201}$.

Fins ara havíem trobat l'invers mirant la taula de la multiplicació com a l'exemple de $\mathbb{Z}_4$ però a $\mathbb{Z}_{452}$ no és factible.

- Pel cas de trobar l'invers de $a = \overline{2}$ cal resoldre l'equació en la qual busquem $x \in \mathbb{Z}$:

  $2x \equiv 1 \bmod 452 \Leftrightarrow$existeix y tal que $2x - 1 = 452y$

  per tant és equivalent a resoldre l'equació diofàntica $2x - 452y = 1$. Ara podem aplicar tot el que sabem d'aquestes equacions i veiem que no té cap solució ja que $mcd(2,452) = 2$ que no divideix a 1. Per tant no té invers.
- I pel segon cas: per trobar l'invers de $a = \overline{201}$ cal resoldre l'equació en la qual busquem $x \in \mathbb{Z}$:

  $201x \equiv 1 \bmod 452 \Leftrightarrow$existeix y tal que $201x - 1 = 452y$

  per tant és equivalent a resoldre l'equació diofàntica $201x - 452y = 1$. Per tant haurem de trobar el $mcd(201,452)$ i veure si divideix a 1 o no; si divideix haurem de resoldre l'equació i trobar x (la y no ens interessa), per tant en aquest cas caldrà completar la taula de l'algorisme d'Euclides extés:

1	0	1	–2	9
0	1	0	1	–4
	0	2	4	50
201	452	201	50	1
201	50	1	0	

Ara amb una identitat de Bézout obtenim una solució:

$9 \cdot 201 - 4 \cdot 452 = 1 \Rightarrow \bar{9} \cdot \overline{201} = \bar{1} \Rightarrow \overline{201}^{-1} = \bar{9}$

S'observa que només cal fer una de les files de l'algorisme extés perquè només s'utilitza un coeficient:

1	0	1	–2	9
	0	2	4	50
201	452	201	50	1
201	50	1	0	

Amb aquest exemple tan simple es veu quin pot ser el resultat per esbrinar si un nombre té invers i a més justifiquem que amb una identitat de Bezout podem trobar l'invers (és com es fa a la pràctica) a més d'un altre resultat interessant:

PROP.: Sigui $\bar{a} \in \mathbb{Z}_m$, aleshores:

a) $\bar{a}$ té invers a $\mathbb{Z}_m \Leftrightarrow mcd(a,m) = 1$

b) Si $mcd(a,m) \neq 1$ llavors existeix un $\bar{x} \neq \bar{0}$ tal que $\bar{a} \cdot \bar{x} = \bar{0}$

DEM.:

a)

$\Leftarrow$: Si té invers tenim que existeix un $\bar{x}$ tal que $\bar{a} \cdot \bar{x} = \bar{1} \Leftrightarrow ax \equiv 1 \bmod m \Leftrightarrow ax - 1 = km \Leftrightarrow ax - km = 1$

si $d = mcd(a,m)$ llavors $d|a, d|m \Rightarrow d|ax - km = 1 \Rightarrow d|1 \Leftrightarrow d = 1 \Leftrightarrow mcd(a,m) = 1$

$\Rightarrow$: Agafem una identitat de Bézout: $xa + ym = 1 \Rightarrow \bar{x}\bar{a} + \bar{y}\bar{0} = \bar{1} \Rightarrow \bar{x}\bar{a} = \bar{1} \Rightarrow \bar{a}^{-1} = \bar{x}$ que dona la recepta que hem dit abans: a partir d'una identitat de Bézout es troba l'invers.

b) Si $mcd(a,m) = d \neq 1$ llavors $d|m, d|a \Rightarrow m = kd, a = k'd$ i d'aquí es veu que:

$\bar{a} \cdot \bar{k} = \overline{k'd} \cdot \bar{k} = \overline{k'm} = \bar{0}$

i k no és zero ja que $0 < k < m$.

EX.: A $\mathbb{Z}_{10}$ digueu quins nombres tenen invers, quin és l'invers i pels que no en tenen determineu un element $\bar{x} \neq \bar{0}$ tal que multiplicat per aquest element doni $\bar{0}$.

x	$\bar{x}^{-1}$	$\bar{y} \neq \bar{0}$ tal que $\bar{y}\bar{x} = \bar{0}$
1	1	
2		5
3	7	
4		5
5		2
6		5
7	3	
8		5
9	9	

Per tant el que està clar és que només en el cas que m sigui un nombre primer tots els elements tindran invers (llevat del $\bar{0}$). I en aquest cas podrem afirmar l'existència d'invers per tot element no nul. Quan en un anell tenim invers per tots els elements no nuls (com li passa a $\mathbb{R}$, $\mathbb{C}$, etc.; però no li passa a $\mathbb{Z}$ ni al conjunt dels polinomis a coeficients reals) es diu que és un cos. Per tant podem afirmar:

PROP.: $\mathbb{Z}_m$ és un cos $\Leftrightarrow$ m és un nombre primer.

DEM.: $\mathbb{Z}_m$ és un cos$\Leftrightarrow$ tot $\bar{a} \in \mathbb{Z}_m$ no nul té invers$\Leftrightarrow$

$\Leftrightarrow$per a tot $a = 1,2,3,\ldots,m-1$ tenim $mcd(a,m) = 1 \Leftrightarrow$ m és un nombre primer

Practiquem l'aritmètica en aquests anells i cossos:

EX.: A $\mathbb{Z}_9$ resoleu les dues equacions següents: $\bar{2}\bar{x} = \bar{2}$, $\bar{3}\bar{x} = \bar{3}$.

- $\bar{2}\bar{x} = \bar{2} \Leftrightarrow \bar{x} = \overline{1} \Leftrightarrow x = 1 + 9t$ ja que existeix l'invers per ser $mcd(2,9) = 1$; a $\mathbb{Z}_9$ la solucio sortiria: $\bar{x} = \bar{1}$
- $\bar{3}\bar{x} = \bar{3} \Leftrightarrow 3x \equiv 3 \cdot 1 \bmod 3 \cdot 3 \Leftrightarrow x \equiv 1 \bmod 3 \Leftrightarrow x = 1 + 3t$ que a $\mathbb{Z}_9$ sortiria: $\bar{x} = \bar{1}, \bar{4}, \bar{7}$.

EX.: (25) Resoleu l'equació $\bar{5}\bar{x} - \bar{3} = \overline{29}$ a $\mathbb{Z}_{13}$.

$\bar{5}\bar{x} - \bar{3} = \bar{3} \Leftrightarrow \bar{5}\bar{x} = \bar{6} \Leftrightarrow \bar{5}\bar{x} = \bar{6} \Leftrightarrow \bar{8} \cdot \bar{5}\bar{x} = \bar{8} \cdot \bar{6} \Leftrightarrow \bar{x} = \bar{9}$

EX.: (27) Resoleu les congruències següents:

a) $3x \equiv 5(\bmod 10)$.

b) $2x \equiv 4(\bmod 10)$.

c) $6x \equiv 4(\bmod 10)$.

d) $2x \equiv 7(\bmod 10)$.

a) $3x \equiv 5(\bmod 10)$, com que l'invers de 3 modul 10 és 7 tenim:

$7 \cdot 3x \equiv 7 \cdot 5(\bmod 10) \Leftrightarrow x \equiv 5(\bmod 10)$

b) $2x \equiv 4(\bmod 10)$, com que l'invers de 2 modul 10 no existeix utilitzem la propietat explicada per simplificar: $2x \equiv 4(\bmod 10) \Leftrightarrow x \equiv 2(\bmod 5)$

c) $6x \equiv 4(\bmod 10)$, com a l'anterior:

$6x \equiv 4(\bmod 10) \Leftrightarrow 3x \equiv 2(\bmod 5) \Leftrightarrow 2 \cdot 3x \equiv 2 \cdot 2(\bmod 5) \Leftrightarrow x \equiv 4(\bmod 5)$

d) $2x \equiv 7(\bmod 10)$, com que 2 no té invers i no podem fer servir cap de les propietats

de simplificació anteriors multiplicarem pel nombre 5 que verifica que $2 \cdot 5 \equiv 0 \bmod 10$:

$2x \equiv 7(\bmod 10) \Rightarrow 5 \cdot 2x \equiv 5 \cdot 7(\bmod 10) \Leftrightarrow 0x \equiv 5(\bmod 10)$

expressió que no la satisfà cap valor de x, per tant l'equació no té solució. Un latra manera de fer-la seria passar a l'equació diofànti que surt: $2x - 7 = 10y \Leftrightarrow 2x - 10y = 7$ que no té cap solució.

EX.: Resoleu el sistema

$$\left.\begin{array}{r} x \equiv 0(\bmod 2) \\ x \equiv 2(\bmod 3) \\ x \equiv 4(\bmod 10) \end{array}\right\}$$

de la manera següent: en primer lloc resoleu el sistema de les dues primeres equacions expressant en forma d'equació diofàntica; a continuació resoleu el sistema que queda amb la solució trobada i la darrera equació de la mateixa manera (treballant l'equació diofàntica que s'obté).

Resolem primer el sistema determinat per les dues primeres equacions:

$$\left.\begin{array}{l} x \equiv 0(\bmod 2) \\ x \equiv 2(\bmod 3) \end{array}\right\} \Leftrightarrow \left.\begin{array}{l} x = 0 + 2a \\ x \equiv 2 + 3b \end{array}\right\} \Rightarrow 0 + 2a = 2 + 3b \Rightarrow 2a - 3b = 2$$

Aquesta equació diofàntica té solució ja que $mcd(2,3) = 1|2$. La identitat de Bézout per 2 i 3 és molt fàcil: $-1 \cdot 2 + 1 \cdot 3 = 1 \Rightarrow -2 \cdot 2 + 2 \cdot 3 = 2 \Rightarrow (-2) \cdot 2 - (-2) \cdot 3 = 2$

Per tant les solucions de l'equació són $a = -2 + 3t, b = -2 + 2t$ i d'aquí la $x = 0 + 2a = -4 + 6t$ o sigui $x \equiv -4(\bmod 6)$. 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:

$$\left.\begin{array}{l} x \equiv -4(\bmod 6) \\ x \equiv 4(\bmod 10) \end{array}\right\} \Leftrightarrow \left.\begin{array}{l} x = -4 + 6a \\ x \equiv 4 + 10b \end{array}\right\} \Rightarrow -4 + 6a = 4 + 10b \Rightarrow 6a - 10b = 8 \Rightarrow 3a - 5b =$$

Aquesta equació diofàntica té solució ja que $mcd(3,5) = 1|4$. La identitat de Bézout per 3 i 5 és també molt fàcil: $2 \cdot 3 + (-1) \cdot 5 = 1 \Rightarrow 8 \cdot 3 + (-4) \cdot 5 = 4 \Rightarrow 8 \cdot 3 - 4 \cdot 5 = 4$

Per tant les solucions de l'equació són $a = 8 + 5t, b = 4 + 3t$ i d'aquí la $x = -4 + 6a = -4 + 6(8 + 5t) = 44 + 30t$ o sigui $x \equiv 14(\bmod 30)$.