QUÈ HEM FET FINS ARA?

El darrer que hem treballat és formalment el tema de la divisió entera, l'algorisme d'Euclides extés, les identitats de Bézout i aplicacions d'aquestes identitats.

CLASSE D'AVUI 07/12/2020

Avui continuem amb un exercici que un estudiant ha demanat de fer i a continuació l'estudi de les equacions diofàntiques i el començament de les congruències.

(7) Demostreu que si $x|y$ i $y|2x$ llavors o bé $|x| = |y|$ o bé $|y| = 2|x|$.

A partir de les hipòtesis tenim: $y = kx, 2x = k'y$ per certs enters k, k'. Llavors:

$$\left.\begin{array}{r} y = kx \\ 2x = k'y \end{array}\right\} \Rightarrow \left.\begin{array}{r} y = kx \\ 2x = k'kx \end{array}\right\}$$

- Si $x = 0$ llavors $y = 0, 0 = k'y \Rightarrow y = 0, 0 = 0$ per tant $x = 0, y = 0$ que

  verifiquen la conclusió: $|x| = |y|$ o bé $|x| = 2|y|$.
- Si $x \neq 0$ llavors $2 = k'k$. Ara tenim dos casos:
  - Primer cas: $2|k \Rightarrow k = 2k''$ per cert $k'' \Rightarrow 2 = k'2k'' \Rightarrow 1 = k'k''$; per tant $k' = k'' = \pm 1 \Rightarrow k = \pm 2 \Rightarrow y = \pm 2x, 2x = \pm 1 \cdot (\pm 2)x$ aleshores $y = \pm 2x$ i llavors $|y| = 2|x|$.
  - Segon cas: $2|k' \Rightarrow k' = 2k''$ per cert $k'' \Rightarrow 2 = 2k''k \Rightarrow 1 = k''k$; per tant $k = k'' = \pm 1 \Rightarrow k' = \pm 2 \Rightarrow y = \pm 1x, 2x = \pm 2 \cdot (\pm 1)x$ per tant $y = \pm x$ i llavors $|y| = |x|$.

Equacions diofàntiques

Les equacions diofàntiques són equacions en les quals intervenen nombres enters i de les quals nommés busquem solucions enteres. Nosaltres en concentrarem en les equacions diofàntiques lineals amb dues incògnites:

$$ax + by = c$$

EX.: Doneu solucions de l'equació diofàntica $3x + 5y = 2$.
$(x, y) = (-1, 1)$

EX.: Doneu solucions de l'equació diofàntica $3x + 15y = -12$.
$(x, y) = (1, -1)$

Veiem un darrer exemple introductori:

EX.: Doneu solucions de l'equació diofàntica $9x + 18y = 2$.

No té cap solució perquè si tingués una solució (x, y), llavors veiem que $3|9, 3|18$ i per tant per linealitat $3|9x + 18y = 2$ i aleshores 3 hauria de dividir a 2 cosa que és impossible: $3 \nmid 2$. Per tant no pot haver-hi cap solució. Aquest raonament també le podríem haver fet amb el nombre 9. En general podrem repetir el raonament amb qualsevol divisor comú de 9 i 18 i per tant sembla que el nombre amb el que serà més fàcil veure si no és possible que tingui una solució serà el $mcd(9, 18)$ perquè és el divisor comú més gran.

Amb aquests exemples s'intueix el resultat següent:

PROP.: L'equació diofàntica $ax + by = c$ té solució si només si $mcd(a,b)|c$.

DEM.: Anomenem $d = mcd(a,b)$.

$\Rightarrow$: Si té solució vol dir que existeixen x,y tals que $ax + by = c$ i per tant com que $d|a, d|b \Rightarrow d|ax + by = c \Rightarrow d|c$ o sigui $mcd(a,b)|c$.

$\Leftarrow$: Com que $d = mcd(a,b)$ sabem que existeixen x,y tals que $ax + by = d$ (identitat de Bézout) i per tant

$$ax + by = d \Rightarrow \tfrac{a}{d}x + \tfrac{b}{d}y = 1 \Rightarrow a\tfrac{c}{d}x + b\tfrac{c}{d}y = c$$

per tant tenim que existeix una solució (solució particular) $\left(\frac{c}{d}x, \frac{c}{d}y\right)$. Recordem que sabem que $d|c$.

EX.: Comproveu que l'equació diofàntica $14.001x + 279y = 21$ té solució. Determineu una solució.

Fem l'algorisme d'Euclides extès:

1	0	1	–5	11
0	1	–50	251	–552
	50	5	2	8
14001	279	51	24	3
51	24	3	0	

$\rightarrow mcd(14001, 279) = 3|21 \Rightarrow$té solució

$11 \cdot \mathbf{14001} + (-552) \cdot \mathbf{279} = 3 \Rightarrow 77 \cdot \mathbf{14001} + (-3864) \cdot \mathbf{279} = 21 \Rightarrow$ és solució $(x_0, y_0) = (77, -3864)$

A partir d'una solució particular (x_0, y_0) de l'equació diofàntica $ax + by = c$ podem obtenir les altres solucions (x,y) fixant-nos que:

$$\left.\begin{array}{r} ax_0 + by_0 = c \\ ax + by = c \end{array}\right\} \Rightarrow a(x - x_0) + b(y - y_0) = 0 \Rightarrow a(x - x_0) = -b(y - y_0) \Rightarrow$$
$$\Rightarrow \tfrac{a}{d}(x - x_0) = -\tfrac{b}{d}(y - y_0)$$

sent $d = mcd(a,b)$. Sabem que $mcd(\frac{a}{d}, \frac{b}{d}) = 1$ i $\frac{a}{d}|-\frac{b}{d}(y - y_0)$ llavors pel Lema de Gauss tenim que $\frac{a}{d}|y - y_0$ per la qual cosa $y - y_0 = \frac{a}{d}t$ per cert t enter. Per tant $y = y_0 + \frac{a}{d}t$ i per la x obtenim:

$$a(x - x_0) + b\left(y_0 + \tfrac{a}{d}t - y_0\right) = 0 \Leftrightarrow a(x - x_0) + b\tfrac{a}{d}t = 0 \Leftrightarrow x - x_0 + b\tfrac{1}{d}t = 0 \Leftrightarrow$$
$$\Leftrightarrow x = x_0 - \tfrac{b}{d}t$$

o sigui que $x = x_0 - \frac{b}{d}t, y = y_0 + \frac{a}{d}t$. I tot parell de nombres amb aquesta forma són solució? Sí:

$$a\left(x_0 - \tfrac{b}{d}t\right) + b\left(y_0 + \tfrac{a}{d}t\right) = ax_0 - a\tfrac{b}{d}t + by_0 + b\tfrac{a}{d}t = ax_0 + by_0 = c$$

Per tant la recepta que obtenim és trobar una solució particular (x_0, y_0) de l'equació diofàntica $ax + by = c$ i utilitzar les fórmules $x = x_0 - \frac{b}{d}t, y = y_0 + \frac{a}{d}t$.

EX.: Determineu totes les solucions de l'equació diofàntica $14.001x + 279y = 21$.

Sabem que és solució particular $(x_0, y_0) = (77, -3864)$, $d = 3$ llavors totes les solucions són:

$x = x_0 - \frac{b}{d}t = 77 - 93t, y = y_0 + \frac{a}{d}t = -3864 + 4667t$

Resumim el resultat que hem obtingut en forma de proposició i resolem la pregunta següent: si ens donen unes fórmules de la forma $x = x_0 + \lambda t, y = y_0 + \mu t$, com veiem que ens donen totes les solucions de l'equació diofàntica?

PROP.: Sigui l'equació diofàntica $ax + by = c$ amb $mcd(a,b)|c$ i sigui (x_0, y_0) una solució particular. Aleshores:

a) $x = x_0 - \frac{b}{d}t, y = y_0 + \frac{a}{d}t$ per a tot $t \in \mathbb{Z}$ ens proporciona totes les solucions de l'equació diofàntica;

b) $x = x_0 + \lambda t, y = y_0 + \mu t$ per a tot $t \in \mathbb{Z}$ ens proporciona totes les solucions de l'equació diofàntica si i només si

- $x = x_0 + \lambda t, y = y_0 + \mu t$ per a tot $t \in \mathbb{Z}$ són solució de l'equació
- $mcd(\lambda, \mu) = 1$

DEM.:

a)Ja està demostrat.

b)

$\Leftarrow$: Evident.

$\Rightarrow$: (81) Com que sabem que $mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ i que $x = x_0 - \frac{b}{d}, y = y_0 + \frac{a}{d}$ és una solució, llavors aquesta solució s'ha d'obtenir amb un valor t col.locat a les fórmules $x = x_0 + \lambda t, y = y_0 + \mu t$ o sigui que:

$$\left.\begin{aligned} x_0 + \lambda t &= x_0 - \tfrac{b}{d} \\ y_0 + \mu t &= y_0 + \tfrac{a}{d} \end{aligned}\right\} \Rightarrow \left.\begin{aligned} \lambda t &= -\tfrac{b}{d} \\ \mu t &= \tfrac{a}{d} \end{aligned}\right\} \Rightarrow t|\tfrac{b}{d}, t|\tfrac{a}{d} \Rightarrow t|mcd\left(\tfrac{a}{d}, \tfrac{b}{d}\right) = 1 \Rightarrow t = \pm 1$$

per tant $\lambda = -\frac{b}{d}, \mu = \frac{a}{d}$ o bé $\lambda = \frac{b}{d}, \mu = -\frac{a}{d}$ llavors $mcd(\lambda, \mu) = mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. A més podríem dir que si unes fórmules d'aquesta forma donen totes les solucions les dues úniques possibilitats seran:

$$\left.\begin{aligned} x &= x_0 - \tfrac{b}{d}t \\ y &= y_0 + \tfrac{a}{d}t \end{aligned}\right\} \text{ o bé } \left.\begin{aligned} x &= x_0 + \tfrac{b}{d}t \\ y &= y_0 - \tfrac{a}{d}t \end{aligned}\right\}$$

Una altra formulació d'aquesta proposició és posant en lloc de la solució particular (x_0, y_0) una altra solució particular (x_1, y_1) i llavors la fórmula pot prendre una altra forma.

EX.: Li demaneu a un amic que mulpliqui el dia que va néixer per 12 i el número del mes per 31 i que us digui el resultat de la suma d'aquestes quantitats. El resultat és 244 (l'alumne és en David). Esbrineu la data del seu aniversari.

Diem $x =$el dia del mes de l'aniversari del David, $y =$el mes de l'aniversari del David, per tant al resoldre l'equació:

$12x + 31y = 244$

Fem l'algorisme extès pels nombres 12 i 31 (observeu com el propi algorisme gira l'ordre dels dos nombres):

1	0	1	−2	3	−5	13
0	1	0	1	−1	2	−5
	0	2	1	1	2	2
12	31	12	7	5	2	1
12	7	5	2	1	0	

$\mathbf{12} \cdot (13) + \mathbf{31} \cdot (-5) = 1 \Rightarrow \mathbf{12} \cdot (13 \cdot 244) + \mathbf{31} \cdot (-5 \cdot 244) = 244 \Rightarrow (x_0, y_0) = (13 \cdot 244, -5 \cdot 244) = (3172, -1220)$ és una solució particular; per tant totes les solucions:

$x = x_0 - \frac{b}{d}t = 3172 - 31t, y = y_0 + \frac{a}{d}t = -1220 + 12t$

La solució al nostre problema:

$1 \leq 3172 - 31t \leq 31 \Leftrightarrow -3171 \leq -31t \leq -3141 \Leftrightarrow \frac{-3171}{-31} \geq t \geq \frac{-3141}{-31} \Leftrightarrow$

$\Leftrightarrow 102,2\ldots \geq t \geq 101,3\ldots \Rightarrow t = 102$ i llavors la solució serà: $x = 3172 - 31 \cdot 102 = 10, y = -1220 + 12 \cdot 102 = 4$

per tant el 10 d'abril.

Ara farem un repàs del mínim comú múltiple i de les seves propietats començant per la definició:

DEF.: Pels nombres $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ anomenem $mcm(a_1, a_2, \ldots, a_n) = 0$ si algun $a_i = 0$ i serà $mcm(a_1, a_2, \ldots, a_n) = m$ l'unic nombre enter amb les propietats següents:

- $m > 0$ i $a_i | m$ per a cada $i = 1, 2, \ldots, n$
- si $m' > 0$ i $a_i | m'$ per a cada $i = 1, 2, \ldots, n$ aleshores $m \leq m'$.

Per la definició és immediat que $mcm(a_1, a_2, \ldots, a_n) \geq 0$ i que $mcm(a_1, a_2, \ldots, a_n) = 0$ només en el cas que algun dels nombres sigui 0.

Com a propietats importants del mínim comú múltiple tenim:

PROP.: Siguin $a, b \in \mathbb{Z}$.

1. Si $a|b$ llavors $mcm(a, b) = |b|$.

2. El mínim comú múltiple no depèn del signe: $mcm(a, b) = mcm(a, -b) = mcm(-a, b) = mcm(-a, -b)$.

DEM.:

1. Per la hipòtesi, si $a = 0$ llavors $b = 0$ i per tant $mcm(a, b) = 0, |b| = 0$. El mateix passa si $b = 0$ i $a \neq 0$. El cas important és el següent: si $a \neq 0$ i $b \neq 0$ llavors $|b|$ és un multiple de b i de a i a més el múltiple més petit no nul positiu de b és $|b|$.

2. El mínim comú múltiple no depèn del signe ja que la divisibilitat no depèn del signe.

El segon bloc de propietats utilitza la factorització pels càlculs i demostracions:
PROP.: Siguin $a, b, c \in \mathbb{Z}$.

1. Si expressem els nombres $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ amb $\varepsilon_1, \varepsilon_2 = \pm 1$, cada p_i primer i cada $e_i \geq 0$ llavors

$$mcm(a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \dots p_k^{\max(e_k,f_k)}.$$

2. $mcd(a,b)mcm(a,b) = |ab|$

3. Un enter és múltiple comú de dos nombres si i només si és múltiple del mínim comú múltiple, o sigui:

$$a|c, b|c \Leftrightarrow mcm(a,b)|c$$

4. $mcm(mcm(a,b),c) = mcm(a, mcm(b,c)) = mcm(a,b,c)$

DEM.: fem les demostracions per nombres no nuls (pels nuls són fàcils de veure les propietats).

1. Per la definició del mínim comú múltiple.

2. Com que $mcm(a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \dots p_k^{\max(e_k,f_k)}$ i $mcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \dots p_k^{\min(e_k,f_k)}$ llavors $mcd(a,b)mcm(a,b) = |ab|$ perquè $\max(e_i,f_i) + \min(e_i,f_i) = e_i + f_i$.

3. Si $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$, $c = \varepsilon_3 p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$, la propietat es redueix al fet que:

$$a|c, b|c \Leftrightarrow e_i \leq g_i, f_i \leq g_i \text{ per a tot } i \Leftrightarrow \max(e_i,f_i) \leq g_i \text{ per a tot } i$$

4. De la mateixa manera que l'anterior es redueix a utilitzar el fet que:

$$\max(\max(e_i,f_i),g_i) = \max(e_i, \max(f_i,g_i)) = \max(e_i,f_i,g_i)$$

EX.: (90) Suposem que p és primer. Demostreu que són equivalents:
a) $p|a$.
b) $mcm(p,a) = |a|$.
c) $p|a^2$
d) $p^2|a^3$.

Veiem cadascuna de les implicacions:
a)⇒b): feta abans
b)⇒c): sabem que per hipòtesi $mcm(p,a) = |a|$ llavors $p| |a| \Rightarrow |a| = kp \Rightarrow a = \pm kp \Rightarrow a^2 = (k^2 p) \cdot p \Rightarrow p|a^2$
c)⇒d): sabem que $p|a^2$ llavors $p|a^2 = a \cdot a \Rightarrow p|a$ o $p|a$ i per tant $a = kp \Rightarrow a^3 = k^3 p^3 = (k^3 p)p^2 \Rightarrow p^2|a^3$
d)⇒a): sabem en aquest cas que $a^3 = kp^2$ d'aquí tenim que $p|a^3 = a \cdot a^2 \Rightarrow p|a$ o $p|a^2$. ne le primer cas ja estaria i en el segon tornem a repetir l'aplicació del lema d'Euclides.

EX.: (91) Demostreu que si $a_1, a_2, \dots, a_n$ són primers entre si dos a dos, llavors

$mcm(a_1,a_2,\ldots,a_n) = |a_1a_2\ldots a_n|$.

Com que són primers dos a dos, no podran tenir cap factor en comú per tant podem suposar que tenen nombres primers diferents a la descomposició factorial:

$a_1 = \varepsilon_1 p_{11}^{e_{11}} p_{12}^{e_{12}} \ldots p_{1k_1}^{e_{1k_1}}$, $a_2 = \varepsilon_2 p_{21}^{e_{21}} p_{22}^{e_{22}} \ldots p_{2k_2}^{e_{2k_2}}$,..., $a_n = \varepsilon_2 p_{n1}^{e_{n1}} p_{n2}^{e_{n2}} \ldots p_{nk_n}^{e_{nk_n}}$ amb $e_{ij} \geq 0$

amb $p_{11},p_{12},\ldots,p_{1k_1},p_{21},p_{22},\ldots,p_{2k_2},\ldots,p_{n1},p_{n2},\ldots,p_{nk_n}$ nombres primers diferents. Per tant el mínim comú múltiple serà molt fàcil de calcular per ser tots primers diferents:

$mcm(a_1,a_2,\ldots,a_n) = p_{11}^{e_{11}} p_{12}^{e_{12}} \ldots p_{1k_1}^{e_{1k_1}} p_{21}^{e_{21}} p_{22}^{e_{22}} \ldots p_{2k_2}^{e_{2k_2}} \ldots p_{n1}^{e_{n1}} p_{n2}^{e_{n2}} \ldots p_{nk_n}^{e_{nk_n}} = |a_1a_2\ldots a_n|$

EX.: (92) Demostreu que $mcm(ca,cb) = |c|mcm(a,b)$.

Suposem que $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k}$, $c = \varepsilon_3 p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k}$ amb $e_i,f_i,g_i \geq 0$. Llavors:

- $|c|mcm(a,b) = p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k} mcm(\varepsilon_1 p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}, \varepsilon_2 p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k}) =$
  $= p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k} p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \ldots p_k^{\max(e_k,f_k)} = p_1^{g_1+\max(e_1,f_1)} p_2^{g_2+\max(e_2,f_2)} \ldots p_k^{g_k+\max(e_k,f_k)}$
- $mcm(ca,cb) = mcm(\varepsilon_3 p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k} \varepsilon_1 p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}, \varepsilon_3 p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k} \varepsilon_2 p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k}) =$
  $= mcm(\varepsilon_1\varepsilon_3 p_1^{g_1+e_1} p_2^{g_2+e_2} \ldots p_k^{g_k+e_k}, \varepsilon_2\varepsilon_3 p_1^{g_1+f_1} p_2^{g_2+f_2} \ldots p_k^{g_k+f_k}) =$
  $= p_1^{\max(g_1+e_1,g_1+f_1)} p_2^{\max(g_2+e_2,g_2+f_2)} \ldots p_k^{\max(g_k+e_k,g_k+f_k)}$

Per tant només caldrà veure si $g_i + \max(e_i,f_i) = \max(g_i+e_i,g_i+f_i)$ cosa evident perquè és el mateix fer el màxim abans de sumar un número a tots dos que fer les sumes i després el màxim.

6. CONGRUÈNCIES

En el darrer capítol del curs estudiarem la relació d'equivalència "ser congruent mòdul m" per un m natural no nul que ja vam estudiar en algun exemple particular de m a l'apartat de relacions d'equivalència. Aquesta relació d'equivalència és molt útil. Primer definim-les formalment:

DEF.: En el conjunt dels nombres enters $\mathbb{Z}$ sigui $m \geq 1$ i considerem la relació

$$a \equiv b(\mathrm{mod}\, m) \Leftrightarrow m|a-b$$

(es diu que a és congruent amb b módul m)

Aquesta relació té unes propietats importants:

PROP.: Siguin $a,b,m \in \mathbb{Z}$, $m \geq 1$.

1. La relació de congruència mòdul m és una relació d'equivalència.
2. Aquesta relació admet aquestes formes equivalents:

   $a \equiv b(\mathrm{mod}\, m) \Leftrightarrow m|a-b \Leftrightarrow b = a+km$ per cert enter $k \Leftrightarrow a$ i b tenen el mateix residu al dividir per m

DEM.:

1. La relació és reflexiva, simètrica i transitiva:

   REFLEXIVA: $a \equiv a(\mathrm{mod}\, m) \Leftrightarrow m|a-a = 0$ cosa evident

   SIMÈTRICA:

$a \equiv b(\mathrm{mod}\, m) \Leftrightarrow m|a-b \Rightarrow a-b = km \Rightarrow b-a = -km \Rightarrow b \equiv a(\mathrm{mod}\, m)$

TRANSITIVA:

$$\left.\begin{array}{l} a \equiv b(\mathrm{mod}\, m) \\ b \equiv c(\mathrm{mod}\, m) \end{array}\right\} \Rightarrow \left.\begin{array}{l} m|a-b \\ m|b-c \end{array}\right\} \Rightarrow m|a-b+b-c = a-c$$

2. La primera equivalència és evident per la definició de divisibilitat:

$a \equiv b(\mathrm{mod}\, m) \Leftrightarrow m|a-b \Leftrightarrow$existeix un enter k tal que $a-b = km \Leftrightarrow a = b+km$

Si fem la divisió entera de b entre m obtenim q, r tals que $b = qm+r$ i $0 \leq r < |m|$ i com que

$$a = b+km = qm+r+km = (b+k)m+r$$

amb $0 \leq r < |m|$ però com que el quocient i el residu són únics tenim que el residu de la divisió de a entre m té també residu r (i quocient $b+k$).

EX.: Determineu les classes d'equivalència i el conjunt quocient per la relació de congruència mòdul $m = 5$.

Sabem que al dividir per $m = 5$ els possbles residus són $0, 1, 2, 3, 4$, llavors:

$\overline{0} = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}$
$\overline{1} = \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\}$
$\overline{2} = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$
$\overline{3} = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$
$\overline{4} = \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}$
$\mathbb{Z}/\equiv\, = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

DEF.: Per la relació de congruència mòdul m denotarem les classes d'equivalència per $\overline{a}$ i al conjunt quocient per $\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\}$.

S'observa que com tenim m residus possibles $0, 1, 2, \ldots, m-1$ de la divisió d'un nombre per m tindrem que $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

Una de les propietats més importants del conjunt $\mathbb{Z}_m$ és que es pot definir una suma i una multiplicació. Veiem un exemple primer:

EX.: Si definim a $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ les operacions $\overline{a}+\overline{b} = \overline{a+b}$, $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ determineu la taula de la suma i de la multiplicació.

La taula de la suma i de la multiplicació queda:

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

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$