1.2. ARITMÈTICA MODULAR

Les nocions de divisibilitat que hem vist en $\mathbb{N}$ i $\mathbb{Z}$ ens permeten introduir les següents nocions i estructures.

DEFINICIÓ:

Siguin $x, y \in \mathbb{Z}$ i $m \in \mathbb{N}$, $m > 0$.

Diem que x és congruent amb y mòdul m, i ho escribim per

$$x \equiv y \mod m$$

si $x - y$ és divisible per m.

OBS:

La relació $\equiv$ en $\mathbb{Z}$ és una relació d'equivalència, verifica per exemple propietats reflexives i de simetria:

$$\begin{cases} x \equiv y \ ; \ y \equiv z \Rightarrow x \equiv z \\ x \equiv y \Rightarrow y \equiv x \end{cases}$$

DEFINICIÓ:

Definim la classe de congruència de x mòdul m per

$$\overline{x} := \{a \in \mathbb{Z} \mid x \equiv a \mod m\}$$ (també s'anomena classe d'equivalència)

Denotem per $\mathbb{Z}_{(m)}$ al conjunt de classes de congruència mòdul m.

EXEMPLE:

$7 \equiv 1 \mod (2)$ $\quad 12 \equiv 2 \mod 5$ $\quad 9 \equiv 0 \mod 3$ $\quad 21 \equiv 1 \mod 5$

OBS:

(a) $x \equiv 0 \mod m$ si i només si $x = p \cdot m$, i.e. x és multiple de m o $m \mid x$.

(b) $\overline{x} = \overline{y}$ si $x \equiv y \mod m$.

(c) De vegades les classes d'equivalència també es denoten per $[x] = \overline{x}$

EXEMPLE:

$4 \in \overline{0}$ a $\mathbb{Z}_{/2}$ $\qquad 17 \in \overline{3}$ a $\mathbb{Z}_{/7}$

$10 \in \overline{1}$ a $\mathbb{Z}_{/3}$ $\qquad 10 \in \overline{0}$ a $\mathbb{Z}_{/5}$

PROPOSICIÓ:

Donats $x \in \mathbb{Z}$ i $m \in \mathbb{N}$, $m \neq 0$, existeix un únic $r \in \mathbb{N}$, $0 \leq r < |m|$ tal que

$$x \equiv r \mod m.$$

DEMO: En efecte, per la divisió entera, $\exists\, q$ tal que $x = q \cdot m + r$ on $0 \leq r < |m|$

Per tant $x - r$ és divisible per m i per tant $x \equiv r \mod m$.

En vista a aquest resultat,

$$\mathbb{Z}/(m) = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$$ és un conjunt finit de m classes.

A $\mathbb{Z}/(m)$ es defineix una suma i un producte.

DEFINICIÓ:

A $\mathbb{Z}/(m)$ es defineix la suma i el producte de classes com segueix:

$$\overline{x} + \overline{y} := \overline{x+y}$$

$$\overline{x} \cdot \overline{y} := \overline{x \cdot y}$$

Observem que $\overline{0}$ és l'element neutre de la suma i $\overline{1}$ és l'element neutre del producte.

Això vol dir que $\forall\, \overline{x} \in \mathbb{Z}/(m)$

$$\overline{x} + \overline{0} = \overline{x} \quad ; \quad \overline{x} \cdot \overline{1} = \overline{x}$$

EXEMPLE ⓐ A $\mathbb{Z}/4$, $\overline{2} + \overline{6} = \overline{2} + \overline{2} = \overline{0}$

$$\overline{3} \cdot \overline{2} = \overline{6} = \overline{2}$$

ⓑ A $\mathbb{Z}/11$ $\quad \overline{5} + \overline{10} = \overline{15} = \overline{4}$

$$\overline{5} \cdot \overline{4} = \overline{9}$$

ⓒ Taula de sumar i multiplicar a $\mathbb{Z}/3$

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

·	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

OBSERVACIÓ: En general és FALS que $\overline{x} \cdot \overline{y} = \overline{z} \cdot \overline{y}$ impliqui $\overline{x} = \overline{z}$

Exemple: A $\mathbb{Z}/4$, $\overline{2} \cdot \overline{2} = \overline{2} \cdot \overline{0} = \overline{0}$; $\overline{2} \neq \overline{0}$

NOTE BOOK En alguns casos és cert. Penseu quan.

OBS: Formalment només definim la suma però observem que

$$\overline{x} + \overline{-x} = \overline{x-x} = \overline{0}$$

Per tant $\overline{x} = -\overline{(-x)}$ i per tant $\overline{x} - \overline{y} = \overline{x} + \overline{(-y)} = \overline{x-y}$

L'altre observació important és que a $\mathbb{Z}/(m)$ treballem amb les classes $\overline{0}, \ldots, \overline{m-1}$.

Si per exemple estem a $\mathbb{Z}/7$, qui és $\overline{-4}$. Una forma de pensar-ho és dir, a $\mathbb{Z}/7$,

$$\overline{-4} = \overline{7} + \overline{(-4)} = \overline{7-4} = \overline{3}$$

Penseu com es calcula la classe de $\overline{-x}$ a $\mathbb{Z}/(m)$ en general.

DEFINICIÓ:
Un element $\overline{x} \in \mathbb{Z}/(m)$ és <u>invertible</u> si $\exists\, \overline{y} \in \mathbb{Z}/(m)$ tal que

$$\overline{x} \cdot \overline{y} = \overline{1}$$

En aquest cas es diu que $\overline{y}$ és l'invers de $\overline{x}$: es denota per $\overline{x}^{-1}$.

NOTACIÓ:
Per abús de notació, si pel context sabem que treballem a $\mathbb{Z}/(m)$ de vegades no escrivim $\overline{x}$ sinó només x però tenint present que a $\mathbb{Z}/(m)$ tot són classes.

DEFINICIÓ:
Un element $\overline{x} \in \mathbb{Z}/(m)$ és <u>divisor de zero</u> si $\exists\, \overline{y} \in \mathbb{Z}/m$ tal que $\overline{x} \cdot \overline{y} = \overline{0}$.

EXEMPLE:

(a) A $\mathbb{Z}/(4)$ $\overline{3}$ és invertible i $\overline{3}$ és el seu invers donat que

$$\overline{3} \cdot \overline{3} = \overline{9} = \overline{1} \quad \Rightarrow \overline{3}^{-1} = \overline{3}$$

(b) A $\mathbb{Z}/(5)$ $\overline{3}$ és invertible: el seu invers és $\overline{2}$ donat que

$$\overline{3} \cdot \overline{2} = \overline{6} = \overline{1}.$$

PROPOSICIÓ:

$\overline{x}$ és invertible a $\mathbb{Z}/(m)$ si i només si $\mathrm{mcd}(x, m) = 1$

En particular si p és primer, a $\mathbb{Z}/(p)$ tota classe $\overline{x}$, $\overline{x} \neq \overline{0}$ és invertible i a $\mathbb{Z}/p$, p primer, l'únic divisor de $\overline{0}$ és $\overline{0}$.

OBSERVACIÓ (IMP).

El resultat anterior i la identitat de Bézout ens dóna un mètode efectiu per calcular l'invers de $\overline{x} \in \mathbb{Z}/(m)$ si és que existeix.

Com calcular $\overline{x}^{-1}$ a $\mathbb{Z}/(m)$ quan existeix:

- Com $\overline{x}$ és invertible $\Rightarrow \text{mcd}(x, m) = 1$. La identitat de Bézout ens diu que $\exists$ $p, q \in \mathbb{Z}$ tals que

$$1 = p \cdot x + q \cdot m$$

Agafant classes:

$$\overline{1} = \overline{px + qm} = \overline{p} \cdot \overline{x} + \overline{q} \cdot \overline{m} = \overline{p} \cdot \overline{x}$$

($\overline{m} = 0$ a $\mathbb{Z}/m$)

$\Rightarrow \overline{p} = \overline{x}^{-1}$.

L.

Alguns problemes ens plantegen sistemes d'equacions amb congruències. Per exemple:

EXEMPLE:

13 amics es troben una caixa plena de monedes d'or. Si es repartissen en parts iguals en sobren 8. 2 dels amics no volen problemes i surten del repartiment. Els 11 restants les repartissen en parts iguals i en sobren 3. Finalment 3 altres amics es desentenen del repartiment i si se les repartissen els altres 8 amics que queden en parts iguals en sobren 5. Com a mínim quantes monedes hi havia a la caixa?

- Si ho traduïm en termes de congruències, si x és aquest nº mínim de monedes, tenim:

$$x \equiv 8 \mod (13)$$
$$x \equiv 3 \mod (11)$$
$$x \equiv 5 \mod (8)$$

Volem determinar el menor $x \geq 0$ que verifica aquestes 3 congruències alhora. El següent teorema ens dóna resposta a aquest tipus de problemes en determinades circumstàncies.

TEOREMA (XINÈS DEL RESTA)

Siguin $a_i, m_i \in \mathbb{Z}$, $1 \le i \le k$ enters tals que $\text{mcd}(m_i, m_j) = 1$ per tot $i \neq j$.

El sistema de congruències

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

té les mateixes solucions que la congruència

$$x \equiv x_0 \mod m_1 \cdot m_2 \cdots m_k$$

on $x_0 = a_1 N_1 y_1 + a_2 N_2 y_2 + \cdots + a_k N_k y_k$ amb $N_i := \dfrac{m_1 \cdots m_k}{m_i} = m_1 \cdots \hat{m_i} \cdots m_k$

$$y_i \cdot N_i \equiv 1 \mod m_i$$

EXEMPLE:

Intentem resoldre el problema dels amics. Busquem el menor $x > 0$ tq

$$\begin{aligned} x &\equiv 8 \mod (13) \\ x &\equiv 3 \mod (11) \\ x &\equiv 5 \mod (8) \end{aligned}$$

En primer lloc es verifiquen les hipòtesi de $\text{mcd}(13,11) = \text{mcd}(13,8) = \text{mcd}(11,8) = 1$.

Per definició $N_1 = m_2 \cdot m_3 = 11 \cdot 8 = 88$

$N_2 = m_1 \cdot m_3 = 13 \cdot 8 = 104$

$N_3 = m_1 \cdot m_2 = 13 \cdot 11 = 143$

Ara, y_1 és l'invers de N_1 a $\mathbb{Z}/(13)$. Com $\text{mcd}(13, 88) = 1$, l'algoritme de Euclides ens dóna:

$$\begin{aligned} 88 &= 13 \cdot 6 + 10 \\ 13 &= 1 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned} \Rightarrow \quad 1 = 4 \cdot 88 - 27 \cdot 13 \quad \Rightarrow \quad y_1 = \overline{4}$$

↳ operant

De la mateixa forma calculem $y_2 = -2$ i $y_3 = -1$. Per tant

$$x_0 = 8 \cdot 88 \cdot 4 + 3 \cdot 104 \cdot (-2) + 5 \cdot 143 \cdot (-1) = 1477$$

Així, $x \equiv 1477 \mod 13 \cdot 11 \cdot 8$ $\quad (13 \cdot 11 \cdot 8 = 1144)$

$1477 = 1 \cdot 1144 + 333 \quad \Rightarrow \quad \boxed{x \equiv 333}$