ARITHMETIQUE ET MATRICE :

Congruence

Table des matières

Première partie: Arithmétique

Chapitre V :CONGRUENCE

I. Introduction

Le modulo est le nom d'une opération mathématique qui, pour 2 nombres a et b, calcule le reste r de la division euclidienne a/b. Mathématiquement le calcul modulaire s'écrit a ≡ r modb

Exemple 1 :

Un tas de a=123 billes se divise en b=10 tas de 12 billes et il reste r=3 billes. Donc 123modulo 10 est égal à 3, soit 123≡3mod10

Les calculs modulaires sont parfois imagés avec un cercle, comme sur une horloge où les calculs d'heures se font modulo 12 (ou 24) pour les heures et modulo 60 pour les minutes.

Exemple 2 :

Il est 3h00, dans 25 heures il sera 4h00, revient au calcul 3+25≡4mod12 ou mod 24

L'aiguille des minutes est sur 15, dans 90 minutes, elle sera sur 45, car 15+90≡45mod60

II. Définition

Soit n un entier naturel non nul, a et b deux entiers relatifs.

On dit que a est congru à b modulo n si a−b est un multiple de n.

On écrit : a ≡ b (n) ; a ≡ b (modulo n); a ≡ b(mod n) ou parfois a ≡ b [n].

Exemples :

1. **56 ≡ 6 (mod10)**; car: 56−6=50=5×10. Cela se lit 56 est congru avec 6 modulo 10 car 56-6 est un multiple de 10.
2. **77 ≡ 0(mod7)**; car :77−0=77=11×7.

3. **$-5 \equiv 3 \pmod 8$**; car :$-5-3=-8=-1\times 8$.

III. Propriété de la congruence

a, b, c et d sont des entiers naturels, $k \in \mathbb{Z}$, $p \in \mathbb{N}^*$

Si $a \equiv b\ [n]$ alors $ka \equiv kb\ [n]$

$a^p \equiv b^p\ [n]$

Si $a \equiv b\ [n]$, $c \equiv d\ [n]$

Alors, $a = c \equiv b = d\ [n]$

$ac \equiv bd\ [n]$

On dit que la congruence est compatible avec l'addition et la multiplication.

Exemple :

-Vérifier que $5^2 \equiv 8\ [17]$

- En déduire que $5^4 \equiv -4\ [17]$ puisque $5^8 \equiv -1\ [17]$

- Quel est le reste de la division euclidienne par 17 ? de 5^{16} ? 5^{500}

Vérification : $5^2 \equiv 8\ [17]$

$5^2 = 25 = 17 \times 1 + 8$

$5^2 \equiv 8\ [17]$

Déduisons que $5^4 \equiv 8\ [17]$

$5^2 \equiv 8\ [17]$

$(5^2)^2 \equiv 8^2\ [17]$

$5^4 \equiv 64\ [17]$

$64 - (-4) = 64+4$

$=68 = 17 \times 4$

$\Rightarrow 64 \equiv -4\ [17]$ c'est-à-dire **$\underline{5^4 \equiv -4\ [17]}$**

$5^8 \equiv -1\ [17]$

Donc $(5^4)^2 \equiv (-4)^2\ [17]$

$5^8 \equiv 16\ [17]$

Et 16 – (-1) = 16 + 1 = 17

Donc 16 **≡** -1 [17]

$5^8 \equiv -1$ [17]

5^{16} **≡ ?** [17]

$(5^8)2 \equiv (-1)^2$ [17]

$5^{16} \equiv 1$ [17]

5^{500} **≡ ?** [17]

500 = 16 x 31 +4

$5^{500} = 5^{16 \times 31 + 4}$

$= 5^{16 \times 31} \times 5^4$

$= (5^{16})^{31} \times 5^4$

$5^{500} \equiv 1^{31} \times (-4)$ [17]

$5^{500} \equiv 13$ [17]

1. Petit théorème de FERMAT

Soit p un nombre premier et a un entier relatif.

(1) $a^p \equiv a \pmod p$;

(2) si de plus a et p sont premiers entre eux alors : $a^{p-1} \equiv 1 \pmod p$.

Remarque : Ce théorème peut s'énoncer en disant que $a^p - a$ est multiple de p et que si a est n'est pas multiple de p alors $a^{p-1} - 1$ est multiple de p.

Exemple : p= 3 a= 8

$8^{3-1} = 8^2 = 64$

$8^{3-1} - 1 = 63 \equiv 0$ [3]

2. Relation d'équivalence

Soit $n \geq 2$, $n \in \mathbb{N}$.

Pour tout entier naturel a, on a : a ≡ a [n].

En effet, a – a = 0 et 0 = n x 0

On dit que la relation d'équivalence est réflexive. Si a ≡ b [n] alors b ≡ a [n].

Si a – b = nk alors b – a = - (a -b) = - nk = k (-n)

Donc b ≡ a [n]

On dit que la relation de congruence est symétrique.

Si a ≡ b [n et b ≡ c [n] alors, a ≡ c [n]

On dit que la relation de congruence est transitive.

Une relation binaire qui est réflexive, symétrique et transitive est dite relation d'équivalence, la relation de congruence est donc une relation d'équivalence.

Si x ∈ ℕ, on appelle classe d'équivalence de x modulo n l'ensemble noté e^p défini par :

$\dot{x}$ = { a ∈ ℕ / x ≡ a [n]}

Exemple :

Si x=5

$\dot{3}$ = { 5k + 3 / k ∈ ℕ }

$\dot{2}$ = { 5k + 2 / k ∈ ℕ }

Si x = 2

$\dot{2}$ = $\dot{0}$ { 2k / k ∈ ℕ }

L'ensemble de tous les classes d'équivalence modulo n noté ℤ / nℤ (appelé ensemble quotient modulo n) est l'ensemble défini par :

ℤ / nℤ = { $\dot{0}$; $\dot{1}$; $\dot{2}$; … ; n-1}

Exemple :

ℤ / 2ℤ = { $\dot{0}$; $\dot{1}$ }

ℤ / 5ℤ = { $\dot{0}$; $\dot{1}$; $\dot{2}$; $\dot{3}$; $\dot{4}$}

On définit sur $\mathbb{Z}$ / n$\mathbb{Z}$ les deux opérations suivantes :

$\dot{x}$ **+** $\dot{y} = x \dot{+} y$

$\dot{x}$ **x** $\dot{y} = x\dot{y}$

Tableau d'addition et multiplication de $\mathbb{Z}$ / n$\mathbb{Z}$

+	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

x	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$