Exposé 10 :
Congruence dans $\mathbb{Z}$. Anneau $\mathbb{Z}/m\mathbb{Z}$

0- Pré Requis

- Notion de division euclidienne dans $\mathbb{Z}$
- Anneau
- PGCD
- Thm de Bezout, Gauss.

I Congruence dans $\mathbb{Z}$:

1) Définition :

Def : $x, y \in \mathbb{Z}$, $m \in \mathbb{N}$. On dit que x est congru à y modulo m si $x - y \in m\mathbb{Z}$

Notation : $x \equiv y [m]$

Rq : - Si $x \equiv 0 [m] \Leftrightarrow m | x$

- Si $m = 0$ $x \equiv y [0]$ se réduit à $x = y$
- $x \equiv y [m] \Leftrightarrow x$ et y ont le même reste dans la division euclidienne par m.

Thm : La relation de congruence est une relation d'équivalence.

Prop : $x, y, x', y' \in \mathbb{Z}$, $m \in \mathbb{N}$ Si $x \equiv x' [m]$ et $y \equiv y' [m]$ alors

i) $x + y \equiv x' + y' [m]$

ii) $xy \equiv x'y' [m]$

[$x - x' \in m\mathbb{Z}$ et $y - y' \in m\mathbb{Z}$

i) $x + y - (x' + y') = (x - x') + (y - y') \in m\mathbb{Z}$

ii) $xy - x'y' = (x - x')y \quad + x'y - x'y' = (x - x')y + x'(y - y') \in m\mathbb{Z}$]

Conséquences :

i) $\forall p \in \mathbb{Z}$, Si $x \equiv y [m]$, $px \equiv py [m]$

ii) $\forall k \in \mathbb{N}^*$, Si $x \equiv y [m]$, $x^k \equiv y^k [m]$

iii) Si $ka \equiv kb [m]$, $k \wedge m = 1$ alors $a \equiv b [m]$.

II Anneau $\mathbb{Z}/m\mathbb{Z}$:

1) Classes d'équivalences :

Def : On appelle classe d'équivalence de x ($x \in \mathbb{Z}$) modulo m, noté $\bar{x}$ l'ensemble $\{ y \in \mathbb{Z} \mid x \equiv y [m] \} = x + m\mathbb{Z}$

Rq : $x \equiv y [m] \Leftrightarrow \bar{x} = \bar{y}$

Thm : Chaque classe d'équivalence contient un unique représentant x tq $0 \leq x < m$.

[Existence :
$y \in \bar{x}$, $y = qm + r$ $\quad 0 \leq r < m$

$y \equiv r\ [m]$ et $0 \leq r < m$

Unicité :
soit $s \in \bar{x}$ $\quad 0 \leq s < m \Rightarrow y \equiv s\ [m]$

$r \in \bar{x}$ $\quad 0 \leq r < m \quad y \equiv r\ [m]$

$\Rightarrow r \equiv s\ [m] \Leftrightarrow r - s \in m\mathbb{Z}$ or $|r - s| < m$

$\Rightarrow r - s = 0$ ie $r = s$]

2) Ensemble quotient :

Def : L'ensemble des m classes associées à la congruence modulo m est appelé l'ensemble des entiers modulo m

On le note $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$

Thm : On peut définir deux lois internes dans $\mathbb{Z}/m\mathbb{Z}$:

$\forall x, y \in \mathbb{Z}$ i) $\bar{x} + \bar{y} = \overline{x+y}$

ii) $\bar{x}\bar{y} = \overline{xy}$

$(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire d'element d'unité $\bar{1}$

[Il suffit de montrer que $\dot{x} + \dot{y}$ et le produit $\dot{x} . \dot{y}$ ne depend pas du representant x et y choisis.

Ensuite les vérifications ne posent pas de problème]

Rq : $\mathbb{Z}/m\mathbb{Z}$ n'est pas forcement un anneau intègre.

Ex : $\mathbb{Z}/6\mathbb{Z}$ $\quad \bar{2} \times \bar{3} = \bar{0}$

3) Elements inversibles :

Def : $\bar{x} \in \mathbb{Z}/m\mathbb{Z}$ inversible si il existe $\bar{y} \in \mathbb{Z}/m\mathbb{Z}$ tq $\bar{x}\bar{y} = 1$

Thm : $\bar{x} \in \mathbb{Z}/m\mathbb{Z}$, $\bar{x} \neq \bar{0}$ $\quad \bar{x}$ inversible $\Leftrightarrow x \wedge m = 1$

[$\dot{x}$ inversible $\Leftrightarrow \exists \dot{y} \in \mathbb{Z}/m\mathbb{Z}$ tq $\dot{x}\dot{y} = \dot{1} \Leftrightarrow \exists y \in \mathbb{Z}, \exists u \in \mathbb{Z}$

$xy + um = 1$

$\Leftrightarrow$ pgcd $(x, m) = 1$]

Notation : $(\mathbb{Z}/m\mathbb{Z})^\times$

Corollaire : $\mathbb{Z}/p\mathbb{Z}$ corps $\Leftrightarrow$ p premier.

III Applications :

1) Problème de date.

2004 , 11 novembre jeudi

11 novembre 1918 ?

↳ 86 ans, 22 années bissextiles.

$86 \times 365 + 22 = 31412 \equiv 3 [7]$

Donc on était lundi (car entre 2004 et 1918 on recule donc jeudi → lundi

2) <u>Application à l'arithmétique:</u>

10^{2005} diviser par 7 ? le reste ?

$10 \equiv 3 \; [7]$

$10^2 \equiv 3^2 \; [7]$ ie $10^2 \equiv 2 \; [7]$

$10^3 \equiv 2 \times 10 \; [7]$ ie $10^3 \equiv 6 \; [7]$

$10^4 \equiv 4 \; [7]$

$10^5 \equiv 5 \; [7] \Rightarrow 10^6 \equiv 1 \; [7]$

ie $2005 = 6 \times 334 + 1$

$10^{2005} \equiv 3 \; [7]$

3) <u>Critère de divisibilité par 9:</u>

Soit $n \in \mathbb{N}$

$n = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$

on a $10 \equiv 1 \; [9]$ donc $\forall k \in \mathbb{N} \; 10^k \equiv 1 \; [9]$

donc $n \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \; [9]$

Donc un entier naturel est donc divisible par 9 ssi la somme de tous ses chiffres est divisible par 9.