103 Anneaux $\mathbb{Z}/n\mathbb{Z}$ Application

I. Congruence

$n \in \mathbb{N}^*$

- Déf 1. $(a;b) \in \mathbb{Z}^2$.
  On dit que a est congru à b modulo n si $n | (a-b)$
  et on note $a \equiv b \, [n]$
  On a la congruence modulo 0
- Prop 2. Si $a \in \mathbb{Z}$, il existe un unique entier $r \in \{0; \dots n-1\}$ tq $a \equiv r \, [n]$
- Théo 3 : dans $\mathbb{Z}$, la relation $a \equiv b \, [n]$ est une relation d'équivalence
  $\mathbb{Z}/n\mathbb{Z}$ = ensemble des classes d'équivalence
  Si $\bar{a}$ classe d'équivalence de $a \in \mathbb{Z}$
  on a : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \dots; \overline{n-1}\}$
- Théo 4 : a' et b' entiers tqs $a \equiv a' \, [n]$
  $b \equiv b' \, [n]$
  alors : $a + b \equiv a' + b' \, [n]$
  $ab \equiv a'b' \, [n]$
  $\forall p \in \mathbb{N}^* : a^p \equiv a'^p \, [n]$

(Cnl. (nbre divisible par 3))

- Prop 5 : * si $a \equiv b \, [n]$ et $d | n$ alors $a \equiv b \, [d]$
  * si $P \in \mathbb{Z}[X]$ et $a \equiv b \, [n]$
  alors $P(a) \equiv P(b) \, [n]$

II Anneau $\mathbb{Z}/n\mathbb{Z}$.

- Théo 7 . ~~anneau~~ $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition des classes
  $(\mathbb{Z}/n\mathbb{Z}; +)$ groupe commutatif
  + addition des classes
- Théo 8 : $(\mathbb{Z}/n\mathbb{Z}; +; \times)$ anneau commutatif ~~intègre~~
  neutre : $\bar{0}$ unité : $\bar{1}$
- Prop 9. $x \in \mathbb{Z}$. On a équivalence entre
  i) $\bar{x}$ inversible dans $\mathbb{Z}/n\mathbb{Z}$
  ii) ~~x et n premiers entre eux~~ $x \wedge n = 1$
  iii) $\bar{x}$ engendre le gp $\mathbb{Z}/n\mathbb{Z}$
- Rem : $U(\mathbb{Z}/n\mathbb{Z})$: ens. des inversibles de $\mathbb{Z}/n\mathbb{Z}$
- Théo 10 : on a équivalence entre :
  i) n premier
  ii) $(\mathbb{Z}/n\mathbb{Z}; +; \times)$ est un corps
  iii) $(\mathbb{Z}/n\mathbb{Z}; +; \times)$ est intègre

III Application

1/ Indicatrice d'Euler

- Déf 11 : $\varphi : \mathbb{N}^* \to \mathbb{N}^*$
  $n \mapsto \begin{cases} 1 & \text{si } n = 1 \\ \text{Card}(U(\mathbb{Z}/n\mathbb{Z})) & \text{sinon} \end{cases}$
  est la fonction indicatrice d'Euler

Encad. $\varphi(n)$ / Nbre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, \times)$

- Théo 12 : Euler

$\forall a \in \mathbb{N} \wedge (a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \ [n]$

- Théo 13 : p premier $\Rightarrow \varphi(p) = p - 1$

$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

$\forall \alpha \in \mathbb{N}^*$

- ~~p_1 et p_2 nbres premiers distincts~~ ~~et α_1, α_2 entiers~~
- Si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (décomp. en fact. premiers)

alors $\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$

$n = \sum_{d \mid n} \varphi(d)$

4) Théo. de Fermat :

- Théo 14 : $a \in \mathbb{Z}$ et p premier, alors $a^p \equiv a \ [p]$

si $p \nmid a$: $a^{p-1} \equiv 1 \ [p]$

5) Théo de Wilson :

- Théo 15 : $p \in \mathbb{N}^*, p \geq 2$

p premier ssi $(p-1)! \equiv -1 \ [p]$

6) Théo Chinois :

- Théo 16 : ~~Structure~~ $m, n \in \mathbb{N}^*$

si $m \wedge n = 1$ alors l'anneau $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

- Ex : Résolution du système $\begin{cases} x \equiv 4 \ [5] \\ x \equiv 2 \ [7] \end{cases}$

7) Critère d'Eisenstein :

- Théo : $A = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$

si $p \mid a_i \ \forall i \in [\![0; n-1]\!]$

et $p^2 \nmid a_0$

alors A est irréductible dans $\mathbb{Z}[X]$

- Ex : $5X^4 + 15X^2 + 10$ est irréductible dans $\mathbb{Z}[X]$

15 minutes

ESSAI

22/5