109

Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

I) Construction et 1ères propriétés

- $x \mathcal{R} y \Leftrightarrow x - y \in n\mathbb{Z}$ déf une rel d'équiv sur $\mathbb{Z}$.
Déf : $\mathbb{Z}/n\mathbb{Z}$.
- Muni de $\bar{a} + \bar{5} = \overline{a+5}$ et $\bar{a}\bar{5} = \overline{a5}$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau comm
- $\mathbb{Z}/n\mathbb{Z}$ est intègre $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ n est 1er
- Lemme chinois
$\rightarrow$ Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.

II) Etude de $(\mathbb{Z}/n\mathbb{Z})^*$

1) Cas général

- $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z} \mid k \wedge n = 1\} = \{\text{générateurs de } (\mathbb{Z}/n\mathbb{Z}, +)\}$
Ep, $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$
- $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.
Ep, $|\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$
- Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, $(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$.

Ep, $\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

2) Cas où $n = p$ est 1er > 2 $(\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z})$

- $\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$
$\Rightarrow$ Détermine les gpes d'ordre pq avec $p < q$ 1ers.

- $|(\mathbb{F}_p^*)^2| = \frac{p-1}{2}$
- $\bar{x} \in (\mathbb{F}_p^*)^2 \iff \bar{x}^{\frac{p-1}{2}} = \bar{1}$

$\Rightarrow -\bar{1}$ est un carré ds $\mathbb{F}_p \iff p \equiv 1 \bmod 4$

$\Rightarrow \exists$ ∞té de nbres 1ers de la forme $1+4n$, $n \in \mathbb{N}$.

III) Identités de congruence

1) Th d'Euler

$\rightarrow$ Th de Fermat

$\Rightarrow$ Système de codage RSA

2) Th de Wilson

IV) Utilisation de $\mathbb{Z}/n\mathbb{Z}$.

1) Symboles de Legendre

Déf : symb de Leg.

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- Loi de réciprocité quad.

$\Rightarrow \exists$ ∞té de nbres 1ers de la forme $1+6n$, $n \in \mathbb{N}$

2) Sommes de carrés

- Un entier est somme de 2 carrés d'entiers ssi ts ses fact 1ers de la forme $4m+3$ ont un exp pair ds la décomp en fact 1ers.
- Un entier est somme de 4 carrés d'entiers.

3) Critère de réd mod p

$\Rightarrow X^3 + 462X^2 + 2433X - 67691$ est irréd ds $\mathbb{Z}[X]$
$\Rightarrow X^9 - X - 1$ est irréd ds $\mathbb{Z}[X]$.

4) Critère de divisibilité par 9

5) Critère de factorisabilité des nbres de Mersennes

6) Résolution de $x^2 + y^2 = z^2$ ds $(\mathbb{N}^*)^3$