Leçon 120- Anneaux Z/nZ. Applications.

I. L'anneau $\mathbb{Z}/n\mathbb{Z}$

1. Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ [1] p94

— Prop : Il est fini de cardinal n
— $\mathbb{Z}/n\mathbb{Z}$ est cyclique
— Prop : Sous groupe de $\mathbb{Z}/n\mathbb{Z}$. Il y en a $\varphi(n)$
— Exemple : Quels sont les sous groupe de $\mathbb{Z}/6\mathbb{Z}$
— Prop : Générateur de $\mathbb{Z}/n\mathbb{Z}$

2. Les inversibles de l'anneau ($\mathbb{Z}/n\mathbb{Z}$,+,.) [2]p.13

— Déf : On note ($\mathbb{Z}/n\mathbb{Z})^*$ le groupe multiplicatif des éléments inversibles de l'anneau
— Prop : Il n'est pas stable par +, mais il est abélien.
— Prop : $pgcd(a,n) = 1 \Leftrightarrow \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow \overline{a}$ engendre ($\mathbb{Z}/n\mathbb{Z}$,+)
— Corollaire : $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow n = p \in \mathscr{P}$
— $(\mathbb{Z}/n\mathbb{Z})^* \cong Aut(\mathbb{Z}/n\mathbb{Z})$
— Notation : $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ avec p premier
— Prop : $|\mathbb{F}_p^*| = \varphi(p) = p-1$
— Thm : $\sum_{d|n} \varphi(d) = n$

3. Résultats d'arithmétique [2]p.15

— Thm d'Euler : $a^{\varphi(n)} \equiv 1[n]$
— Petit thm de Fermat
— Thm de Wilson : $(p-1)! \equiv -1[p]$

II. Théorème chinois et applications [2]p16

1. Théorème

— Thm Chninois + son corollaire
— Exemple

2. Applications

— $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/m_1\mathbb{Z})^* \times (\mathbb{Z}/m_2\mathbb{Z})^*$
— **Dev 1 : Automorphisme de Z / p alpha Z**
— Prop : Multiplicativité de φ

III. Applications

1. Nombres premiers [3]

— Déf : Polynômes cyclotomique
— **Dev 2 : Thm de Dirichlet Faible**

2. Equations diophantiennes [4]

— Prop : Solution de l'équation $ax + by = c$
— Exemple

Bibliographie :

— 1- Calais : Elements de théorie des groupes
— 2- Risler-Boyer : Algèbre pour la L3
— 3-Perrin : Cours d'algèbre
— 4- De Konick et Mercier :Introduction à la théorie des nombres