# 109 – Anneau $\mathbb{Z}/n\mathbb{Z}$. A.

*« On appelle cette projection Pi parce que… euh… ça fait grec. »*

*Un petit commentaire avant de commencer : J'ai prié toute la nuit précédant l'oral pour ne pas tomber sur cette leçon. Je n'ai pas développement adapté à cette leçon !*

Le plan :

I) Anneau $\mathbb{Z}/n\mathbb{Z}$.
Construction avec la division euclidienne. Bézout et Gauss. Indépendance par rapport au représentant pour l'addition. Structure de groupe. Générateurs. Loi x. Structure d'anneau. Structure des groupes abéliens finis. Etude des inversibles. Cas où n est premier. Lemme chinois et sa réciproque. Application : résolution d'un système de congruences.

II) Groupe $(\mathbb{Z}/n\mathbb{Z})^*$ et applications.
Indicatrice d'Euler. Propriétés. Théorème de Fermat, de Wilson, de Fermat-Euler. Application au système de cryptage RSA, exemple. App : tests de primalité.

III) Lien avec $\mathbb{U}_n$ et applications.
Lien avec $\mathbb{U}_n$, polynômes cyclotomiques. Loi de réciprocité quadratique avec le symbole de Legendre. Théorème de Frobenius-Zolotarev. Progression arithmétique de Dirichlet. Somme de deux carrés entiers.

Les développements :

A16 : Frobenius-Zolotarev
A20 : Théorème des deux carrés

La bibliographie :

[Mer]-[Per]-[CaA]-[Per]-[BMP]-[Duv]-[Del]-[HaW]-[Cmb]