121. Nombres premiers. Applications.

1 Les nombres premiers : briques élémentaires de l'anneau $\mathbb{Z}$

1.1 L'anneau factoriel $\mathbb{Z}$

Définitions. Propriétés élémentaires. Nombres premiers entre eux. PGCD/PPCM.Théorème d'arithmétiques. Alogorithme d'Euclide.

1.2 Répartition des nombres entiers.

Existence d'une infinité de nombres entiers. (Conjecture pour les jumeaux)

$\sum \frac{1}{p}$ diverge.

Théorème des nombres premiers (admis). Théorème de Dirichlet faible et fort(admis pour le fort).

Lien avec la fonction ζ

1.3 Premiers critères de primalité.

Tests des éléments plus petits que $\sqrt{n}$. Crible d'ératosthène.

Petit théorème de Fermat. Témoins de Fermat. Nombres de Carmichael. Critère de Miller-Rabin et témoins de Miller (comparaisons avec Fermat).

2 Corps finis

2.1 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Théorème chinois

$\mathbb{Z}/n\mathbb{Z}$ éléments inversible, calcul de l'inverse, Indicatrice d'Euler.

Corps $\mathbb{Z}/p\mathbb{Z}$, caractéristique.

Construction de corps fini (Frobenius)

Nombres de Fermat

Gauss Wantzel **[Développement]**

2.2 Carrés dans $\mathbb{F}_p$

Nombre de carrés.

$x^{\frac{p-1}{2}} = \pm 1$, symbole de Legendre. Loi de réciprocité quadratique **[Développement]**. Exemple de résolution d'équation.

2.3 Polynômes irréductibles

Eisenstein. Réduction modulaire. Application.