

121 : Nombres premiers. Applications.

I) Généralités

A) Définitions, propriétés

Définition, exemples. Nombre infini de nombres premiers. Théorème fondamental de l'arithmétique, exemple. PGCD, PPCM, nombres premiers dans leur ensemble, deux à deux. Lien entre les deux. Théorème de BEZOUT, de GAUSS, exemples.

B) Tests de primalité

Caractérisation d'un premier avec l'anneau $\mathbb{Z}/n\mathbb{Z}$. Théorème de FERMAT, de WILSON, applications. Nombres de MERSENNE, de FERMAT.

II) Application aux polynômes

Critère d'EISENSTEIN, applications. Théorème de réduction modulo p . Faux dans $A[X]$, réciproque fausse. Polynôme cyclotomique, irréductibilité, exemples.

III) Application aux groupes

A) Les p -SYLOW

Définitions : p -groupe, p -SYLOW. Exemple de $GL_n(\mathbb{F}_p)$. Les théorèmes de SYLOW. Application aux groupes d'ordre pq . Exemples.

B) Automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Caractérisation des générateurs de $\mathbb{Z}/n\mathbb{Z}$. Structure de $Aut(\mathbb{Z}/n\mathbb{Z})$. Inversibles de $\mathbb{Z}/p\mathbb{Z}$. DEV 2 : CYCLICITÉ DE $(\mathbb{Z}/n\mathbb{Z})^*$. Application.

IV) Application aux corps finis

Caractéristique d'un corps, structure des corps finis. $(\mathbb{F}_q)^*$ cyclique. Carrés de $(\mathbb{F}_q)^*$, application. Construction d'un corps fini, exemples. Symbole de LEGENDRE DEV 2 : LOI DE RÉCIPROCITÉ QUADRATIQUE. Application.

Références :

- GOURDON
- PERRIN
- CALDERO