

Leçon 121 : Nombres premiers. Applications.

I Ensemble des nombres premiers

1 Introduction aux nombres premiers

- Lemme d'Euclide/Gauss
- Décomposition en produit de facteurs premiers
- Application au calcul de pgcd/ppcm
- Théorème de Wilson
- p premier ssi $\mathbb{Z}/p\mathbb{Z}$ est intègre/un corps

2 Répartition des nombres premiers

- n non premier $\implies \exists p \leq \sqrt{n}$ premier tel que $p|n$, on en déduit un test de primalité
- Crible d'Eratosthène
- Théorème des nombres premiers
- Théorème de Bertrand

3 Fonctions arithmétiques

- Fonction indicatrice d'Euler et propriétés
- Fonction de Möbius et propriétés

II Utilisation des nombres premiers

1 Irréductibilité des polynômes

- $\bar{P}$ irréductible sur $\mathbb{Z}/p\mathbb{Z} \implies P$ irréductible sur $\mathbb{Z}$
- DEV 1 : Lemme des contenus + Critère d'Eisenstein + ϕ_p irréductible sur $\mathbb{Q}$ + $[\mathbb{R} : \mathbb{Q}] = +\infty$

2 Théorie des corps finis

- Caractéristique d'un corps
- $\mathbb{K}$ fini $\implies \text{car}(\mathbb{K}) = p^n$
- Existence et unicité des corps finis
- DEV 2 : Carrés de $\mathbb{F}_q^*$ + Théorème des 2 carrés

3 Théorie des groupes

- Théorème de Cauchy
- p-groupes
- Le centre d'un p-groupe est non trivial
- Application : $|G| = p^2 \implies G$ est abélien