

Leçon 121 : Nombres premiers. Applications.

I) Généralités sur les nombres premiers

1) Définitions et propriétés [ROM, BER]

(possibilité de commencer par quelques résultats permettant de démontrer le thm fdtal de l'algèbre)

- Définition nombre premier
- Décomposition en facteurs premiers
- Définition valuation p-adique et propriétés
- Ecriture pgcd et ppem

2) Indicatrice d'Euler [SAUX1]

- Indicatrice d'Euler
- Application au calcul de $|(\mathbb{Z}/n\mathbb{Z})^\times|$
- $\varphi(n)$ à l'aide de la décompo en facteurs premiers

3) Répartition des nombres premiers [ROM]

- Il existe une infinité de nombres premiers
- Théorème de Hadamard et de la Vallée Poussin
- Inégalité de Tchebychev
- Application à la convergence de séries

4) Critères de primalité [ROM]

- Tout nombre n non premier possède un diviseur $\leq \sqrt{n}$
- Crible d'Erathostène
- Théorème de Fermat
- Réciproque fausse $\rightarrow$ nombres de Carmichael
- Théorème de Wilson

II) Applications

1) Théorie des groupes [BER]

- Définition p-groupe
- Equation p-groupe
- Le centre d'un p-groupe n'est pas trivial
- Classification des groupes d'ordre p^2
- Pour chaque diviseur du cardinal d'un p -groupe, il existe un sg de ce card
- Théorème de Cauchy
- Cyclicité de $(\mathbb{Z}/n\mathbb{Z})^\times$

2) Théorie des corps finis [GOZ, ULM]

- La caractéristique d'un corps fini est un nombre premier
- Morphisme de Frobenius
- Existence et unicité des corps finis
- $\mathbb{F}_q^\times$ est cyclique

3) Théorème des deux carrés de Fermat

4) RSA [ROM, ZEMOR]

- Théorème des restes chinois
- Principe du RSA
- Complexité

Idée : Possibilité de rajouter une partie irréductibilité des polynômes et carrés dans $\mathbb{F}_p$