(121) Nombres premiers. Applications.

Demazure, Combes
FGNalg 1, Perrin

I/ Généralités (Combes)

- Déf, ex
- Algorithme d'Euclide ; décomposition en facteurs premiers : pgcd / ppcm. (Bézout + éq diophan)
- $\mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow$ n premier (Combes)
  - Appl: Caractéristique d'un anneau intègre
    Thm de Fermat, de Wilson
  - Inversibles de $\mathbb{Z}/n\mathbb{Z}$: fonction d'Euler, $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \dots$, lemme chinois.
  - Corps finis : morphismes de Frobenius
    Carrés dans $\mathbb{F}_p$, symbole de Legendre.

II/ Tests de primalité (Demazure)

- Eratosthène
- Fermat, Wilson
  ↝ critères de non primalité
  Nombres de Carmichael.
- Critère de Lehmer
- Test de Miller-Rabin

III/ Familles de nombres premiers et répartition des nombres premiers

- Fermat, Mersenne
- Répartition : infinité de nombres premiers
  - inf — $4n+1$ (Perrin, cas des carrés de $\mathbb{F}_p$)
  - (FGN) — $(4n+1)_n$, infini
  - $\sum \frac{1}{p}$ diverge (Combes)
  - → Cultivé : Hadamard-de la Vallée-Poussin (FGN)

IV/ Applications

- Critère d'Eisenstein (Combes)
- Facteurs invariants d'un groupe abélien
- Théorie des groupes : Cauchy (tout groupe tq $p \mid |G|$ a un élt d'ordre p)
  p-groupes, p-Sylow → gpes d'ordre pq
  A_5 simple
- Cryptographie RSA (Demazure)
- Construction règle / compas