

110 : NOMBRES PREMIERS – App

I. Premiers résultats [CaA] – [Com] – [Dih]

1. Théorème fondamental de l'arithmétique
Th fond – def valuation, expression pgcd, ppcm – Th Euclide ($\infty^{\text{té}}$)
2. Premières propriétés
ptt th de Fermat – Fermat-Euler – Wilson
3. Application : le cryptage RSA
th – app : méthode de cryptage/décryptage

II. Applications en arithmétique [Zem] – [Duv] – [Pe]

1. Indicatrice d'Euler
 $= \#\{\text{inversibles}\}$, mult – $\varphi(p, p^r, n) - \sum \varphi(d) = n$
2. Symbole de Legendre
def carrés ds F_p , symb de Legendre – loi de réciprocité quadratique
3. Somme de 2 carrés
def, prop $Z[i]$ – Th : somme de 2 carrés pour p 1er et n entier

III. Localisation [Com][HW][Zem]

1. Répartition
Th : Dirichlet faible – Euler ($\sum_{p \leq x} \frac{1}{p} = \infty$) – Tchebychev ($\pi(x) = \theta(x/\ln(x))$)
2. Nombres remarquables
Nb de Fermat – de Mersenne
3. Tests de primalité
Test de Fermat, nb de Carmichael – test de Lucas-Lehmer

IV. Applications diverses [Pe]

1. Théorie des groupes
groupes cycliques, th de Sylow, p-groupes
2. Corps finis
ss-corps premiers, existence et unicité des F_p
3. Réduction des polynômes
Critère d'Eisenstein, réduction mod p

Biblio :

Calais (anneaux)
Combes
Delahaye
Zemor
Duvernay
Hardy Wright
Perrin

Développements :

11 – Théorème de Dirichlet faible
15 – Entiers de Gauss
33 – Loi de réciprocité quadratique
(18 – Théorème de Tchebychev)