M0

Nbres premiers. Appl

I) 1ères propriétés

Déf: nbre 1er
- Th fond de l'arithmétique
- Th de Fermat
  ⇒ Syst de codage RSA
- Th de Wilson

II) Nbres de Fermat et nbres de Mersenne

- Si 2^n+1 est 1er, n est une puissance de 2

Déf: nbres de Fermat F_n
- Les F_n st 1ers entre eux 2 à 2
  ⇒ ∃ infté de nbres 1ers
- Si a^n-1 est 1er, $a=2$ et n est 1er

Déf: nbres de Mersenne M_p
- Critère de factorisabilité des nbres de Mersenne
  ⇒ M_p n'est pas 1er pour $p = 11, 23, 83, 131, 191, 239, 251$

Déf: nbre parfait
- Les nbres parfaits pairs st les $2^{p-1}M_p$ avec M_p 1er.

III) Progression

- $\sum_{p \in \mathcal{P}} \frac{1}{p}$ diverge

- Th de Tchebycheff
- Th de la Vallée-Poussin - Hadamard

IV) Appl

1) Symboles de Legendre

Déf : symb de Leg.
- $\left(\frac{-1}{p}\right) = (-1)^{p-1/2}$
- Loi de réciprocité quad
  $\Rightarrow \exists$ infté de nbres 1ers de la forme $1+6n$, $n \in \mathbb{N}$

2) Sommes de carrés

- Un entier est somme de 2 carrés d'entiers ssi ses fact 1ers de la forme $4m+3$ ont un exp pair ds la décomp en fact 1ers.
- Un entier est somme de 4 carrés.

3) Critères d'irréd

- Critère d'Eisenstein
  $\Rightarrow \Phi_p = X^{p-1} + \dots + X + 1$ est irréd ds $\mathbb{Z}[X]$ pour p 1er
  $\Rightarrow \Phi_8 = X^4 + 1$ est irréd ds $\mathbb{Z}[X]$
- Th de réd mod p
  $\Rightarrow X^3 + 462X^2 + 2433X - 67691$ est irréd ds $\mathbb{Z}[X]$
  $\Rightarrow X^p - X - 1$ est irréd ds $\mathbb{Z}[X]$.