

PLAN

1 Généralités [Gou] [AF87] ...

1.1 Nombre premiers

- définition
- prop classique
- existence d'un diviseur premier

1.2 Decomposition en facteur premier

- Thm
- exemple : $641 \mid 2^5$
- app au pgcd et au ppcm
- app a l'indicatrice d'euler
- exemple (s?)

1.3 $\mathbb{Z}/p\mathbb{Z}$

- thm : $\mathbb{Z}/p\mathbb{Z}$ est integre equiv est un corp equi est n premier
- petit thm de Fermat
- exemple
- contre exemple 341
- Thm de Wilson
- inversible de $\mathbb{Z}/p\mathbb{Z}$ [Per]

2 Primalité et répartition

2.1 Quelques exemple de nombre premiers

- Nombre de Mersenne[Gou]
- Contre exemple
- nombre de Fermat [Gou]
- prop : lien avec les polygone constructible [Car01]

2.2 Primalité [Dem97] [PR02]

- Retour sur les nombre de Carmichael

- L'algo de Rabin Miller
- L'algo de Lucas

2.3 Primalité [Dem97] [PR02]

- nombres congru à 1 mod 4
- nombres congru à -1 mod 4
- Diriclet Faible [FGS01] **DVP**
- Thm des nombres premiers

3 Applications

3.1 En arithmetiques

- $ax + by = d$ [Gou]
- fermat pour $n = 2$ version arithmétique [Gou]?
- $y^2 = x^3 + 7$
- nombre de Fermat [Gou]
- critère d'eisenstein et divisibilité ..

3.2 p -groupes [Hal59] [Cal84][Per]

- centre et groupe distingué
- Quelque mot sur les thm de Sylow et la classification
- Thm de la Base de Burnside [Hal59] **DVP**

3.3 corps finis [Per] ...

- carctéristique
- Frobinus
- existence des corps fin
- Loi de Réciprocité quadratique [Tau99] **DVP**
- exemples

BIBLIOGRAPHIE

Références

- [AF87] J. M. Arnaudiès and H. Fraysse, *Cours de mathématiques*, vol. Algèbre 1, Dunod, 1987, 51.12 ARN.
- [Cal84] J. Calais, *Élément de théorie des groupes*, PUF, 1984, 512.1 CAL.
- [Car01] J. C. Carrega, *Théorie des corps-la règle et le compas*, Hermann, 2001, 512.1 CAR.
- [Dem97] M. Demazure, *Cours d'algèbre*, Cassini, 1997, 512.1 DEM.
- [FGS01] S. Francinou, H. Gianella, and S. Serge, *oraux X-ENS, Algèbre 1*, Cassini, 2001.
- [Gou] Xavier Gourdon, *Les maths en tête algèbre*, Ellipse.
- [Hal59] M. Hall, *The theory of groups*, Macmillan, 1959.
- [Per] Daniel Perrin, *Cours d'algèbre*, Ellipse.
- [PR02] P. Sau Picart and E. Rannou, *Cours de calcul formel*, Ellipse, 2002, 512.1 SAU.
- [Tau99] P. Tauvel, *cours d'algèbre*, dunod, 1999, 512.1 TAU.

DEVELOPPEMENT

- Loi de Réciprocité quadratique [Tau99] **DVP**
- Thm de la Base de Burnside [Hal59] **DVP**
- Diriclet Faible [FGS01] **DVP**