Lecon 109 : L'anneau $\mathbb{Z}/n\mathbb{Z}$. Application

Plan

1 Congruence dans $\mathbb{Z}$. L'anneau $\mathbb{Z}/n\mathbb{Z}$

1.1 Idéaux de $\mathbb{Z}$[AF87] [Gou][Tau99]

- def de $n\mathbb{Z}$ de $\mathbb{Z}/n\mathbb{Z}$
- Exemple de calcul [Gou][exo]

1.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$[Goz97]

- Thm de structure des inversible
- cas ou c'est un corp
- Fermat et exo [Gou]
- Wilson

1.3 Indicatrice d'euler [Goz97]

- Def
- Prop multi
- formule de Gauss
- Application au groupe fini

2 Probleme de primalité[PR02] [Dem97]

- System RSA
- Pt thm de Ferma et nbr de Carmichael
- Methode de Rabin Miller **DVP**[Dem97]
- Nbr de Mersenne. Test de Lucas.
- Diriclet Faible [FGS01]**DVP**

3 Application

3.1 equation diophantiennes

- exo [Gou]
- Fermat $n = 2, 4$ **DVP** [HW79]

3.2 Groupe abelien fini

- $\mathbb{Z}$ module [Cal84]
- thm de structure [Cal84] [BR79] [Gob96]

3.3 Corps finis[Per]

- K^* est cyclique
- Eisenstiein
- LRQ [Tau99] **DVP**

Bibliographie

Références

[AF87] J. M. Arnaudiès and H. Fraysse, *Cours de mathématiques*, vol. Algèbre 1, Dunod, 1987, 51.12 ARN.

[BR79] A. Bouvier and D. Richard, *Groupes*, Herman, 1979.

[Cal84] J. Calais, *Élément de théorie des groupes*, PUF, 1984, 512.1 CAL.

[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.

[Gob96] R. Goblot, *Algèbre commutative*, Masson, 1996, 512.1 GOB.

[Gou] Xavier Gourdon, *Les maths en tête algèbre*, Ellipse.

[Goz97] I. Gozard, *Théorie de galois*, Elipse, 1997, 512.1 GOZ.

[HW79] G.H. Hardy and E. M. Wright, *An introduction to the theory of number*, Oxford Press, 1979, 512.2 HAR.

[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

- Methode de Rabin Miller **DVP**[Dem97]
- Diriclet Faible [FGS01]**DVP**
- Fermat $n = 2, 4$ **DVP** [HW79]
- LRQ [Tau99] **DVP**