Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

1 Présentation

- Définitions, notations [4]
- Structure des groupes abéliens finis [1]
- Théorème chinois, applicatoins aux systèmes de conguences [4]

2 Le groupes des inversibles

- – Définitions, caractérisations des inversibles [4]
  - Théorèmes classiques, Wilson, Fermat, Euler, [4] Algorithme de Berlekamp [2, 9]
  - Théorèmes de structure [7]
- Autour de $\varphi(n)$
  - Formule explicite. RSA. [4]
  - Application aux corps finis [7]
  - Inversion de Möbius [7, 4]
    - Probabilités que deux nombres soit premier entre eux [3]
    - Nombres de polynômes irréductibles [6, 3, 7]

3 Lien avec les racines $n^{\text{ème}}$ de l'unité.

- isomorphisme, racine primitives $n^{\text{ème}}$ de l'unité, lien avec les polynômes cyclotomiques [7]
- Théorème de Dirichlet faible [5]
- Loi de réciprocité quadratique, symbole de legendre [8], Théorème de Frobenius Zolotarev [9]

Références

[1] F. Combes. *Algèbre et géométrie*. Breal, 2000.

[2] M. Demazure. *Cours d'algèbre : Primalité. Divsibilitée. Codes.* Cassini, 1997.

[3] Nicolas Francinou, Gianella. *Oraux X-ENS : algèbre I.* Cassini, 2001.

[4] X. Gourdon. *Les maths en tête : algèbre*. Ellipses, 1994.

[5] I. Gozard. *Théorie de Galois*. Ellipses, 1997.

[6] P. Ortiz. *Exercices d'algèbres*. Ellipses, 2004.

[7] D. Perrin. *Cours d'algèbre*. Ellipses, 1996.

[8] J.-P. Serre. *Cours d'arithmetique*. PUF, 1970.

[9] G. Peyré V. Beck, J. Malick. *Objectif agrégation*. HK, 2è edition, 2005.