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

Jonathan Loupia jonas001@free.fr http://jonas001.free.fr/agreg/index2.htm

Plan :

1) Anneaux $\mathbb{Z}/n\mathbb{Z}$
- définitions et premières propriétés
- le groupe $(\mathbb{Z}/n\mathbb{Z},+)$
- le théorème chinois
- le groupe $(\mathbb{Z}/n\mathbb{Z}\ ^*, .)$

2) Applications
- cryptographie : le système RSA
- critères de primalité
- symbole de Legendre, carré mod p
- cas particuliers du théorème de Dirichlet
- irréductibilité des polynômes

Développements :

- Einsenstein [G1] p 58
- Berlekamp

Bibliographie

- Schwarz : algèbre
- Fresnel "Anneaux" [F4]
- Gozard "Théorie de Galois" [Goz]
- Gourdon "Algèbre" [G1]