Nombres premiers. Applications

Gabriel Peyré

1 - Généralités, premières applications :

. Définition, premières propriétés[**?**]

. Quelques tests de primalité [*insister sur l'utilisation des résidus quadratiques*]

. Application : crypto système RSA

2 - Corps finis et applications aux les codes correcteurs :

. Généralités sur les corps finis

. Factorisation de polynômes sur les corps finis [*algorithme de Berlekamp. Faire le parallèle factorisation sur les corps finis / dans* $\mathbb{Z}$]

. Présentation des codes cycliques

. Codes BCH : présentation, décodage

. code QR : propriété, groupe d'automorphisme du code complété

3 - Théorie analytique des nombres :

. La fonction ζ [*formule d'Euler, prolongement*]

. Un théorème taubérien [*expliquer la formulation en terme de séries de Dirichlet*]

. Le théorème sur les nombres premiers

21	Algorithme de Berlekamp	***
23	Codes correcteurs linéaires cycliques [*cyclotomie, décodage des codes BCH*]	***