

Arithmétique – Applications aux codes correcteurs et à la cryptographie

Auteur : Pierre Wassef

Partie I – Arithmétique élémentaire

1. Divisibilité dans \mathbb{Z}
2. PGCD et algorithme d'Euclide
3. Nombres premiers
4. Congruences et arithmétique modulaire
5. Théorème de Bézout
6. Théorème de Gauss
7. Théorème fondamental de l'arithmétique

Partie II – Arithmétique modulaire approfondie

8. Groupes multiplicatifs modulo n
9. Petit théorème de Fermat
10. Théorème d'Euler
11. Fonctions arithmétiques (fonction ϕ d'Euler)
12. Systèmes de congruences
13. Théorème des restes chinois

Partie III – Applications aux codes correcteurs

14. Corps finis
15. Polynômes sur un corps fini
16. Codes linéaires

17. Distance de Hamming

18. Codes de Hamming

19. Codes cycliques

Partie IV – Applications à la cryptographie

20. Principes de cryptographie

21. Chiffrement affine et de Hill

22. Systèmes à clé publique

23. Cryptosystème RSA

24. Sécurité et factorisation

Exercices corrigés (122 exercices classés par chapitre)