Mathématiques Discrètes 1

(Théorie des ensembles et Arithmétique)

1 Introduction à la théorie des ensembles

- I. Rappels de théorie des ensembles (Notion première d'ensemble, règles de fonctionnement sous-ensembles, ensemble des parties représentation graphique)
- II. Opérations sur les ensembles (Égalité de deux ensembles réunion, intersection, complémentaire, produit cartésien)

2 Relations binaires entre ensembles

- I. Relations
- II. Relations d'ordre (réflexivité, anti-symétrie, transitivité, relation d'ordre, ordre partiel, ordre total éléments maximaux)
- III. Relations d'équivalence (Classes d'équivalence, ensemble-quotient)
- IV. Compatibilité entre une opération et une relation binaire

3 Application d'un ensemble dans un autre

- I. Application et relation fonctionnelle
- II. Image et antécédent d'un élément
- III. Applications injectives
- IV. Applications surjectives
- V. Image d'un ensemble par une application
- VI. Applications bijectives

5 Ensembles de nombres entiers

- I. Nombres entiers naturels (N) (Définition de N, Opérations, et relation d'ordre dans N, Nombres premiers, Relation de divisibilité, Entiers relatifs)
- II. Division euclidienne dans Z et applications (Définition, Représentation des nombres entiers,Arithmétique modulo n Division « entière » informatique et division euclidienne, Arithmétique modulo 2^n dans les ordinateurs
- III. Algorithmes d'Euclide et applications (PGCD de deux entiers Algorithme d'Euclide, Théorème de Bézout Algorithme d'Euclide généralisé)

6 Représentation des nombres réels en machine

- I. Introduction
- II. Les formats IEEE (La norme IEEE 754, Format«single», Format«double», Format«extended», D'une manière générale, Format«extended»des microprocesseurs, Réels représentables et précision)

7 Cryptologie et arithmétique

- I. Méthodes decryptage «à clé publique (Principe, Utilisation de l'indicatrice d'Euler)
- II. Choix d'un nombre n (Nombres premiers Décomposition en facteurs premiers)

8 Tests de primalité

- I. Théorème de Fermat
- II. Test de Miller-Rabin
- III. Tests de Lucas, Selfridge et Pocklington

9 Décomposition en facteurs premiers

- I. Divisions successives

- II. Algorithme de Monte-Carlo(1975) (Présentation, L'algorithme Discussion)
- III. Algorithme du crible quadratique QS de Pomerance
- IV. Algorithme (p−1) de Pollard
- V. Algorithme de Lenstra (courbes elliptiques) (Introduction aux courbes elliptiques, Algorithme de Lenstra)