Arithmétique modulaire et cryptologie

Pierre MEUNIER

Arithmétique modulaire et cryptologie Pierre MEUNIER

Arithmétique modulaire et cryptologie

Pierre MEUNIER

Arithmétique modulaire et cryptologie Pierre MEUNIER

190 pages

Présentation de l'éditeur

La cryptologie, science des écritures secrètes, peut schématiquement être configurée de manière duale à l aide du couple : cryptographie cryptanalyse :

- la cryptographie ayant pour objet la création de procédés techniques de codage les plus sûrs possibles,
- la cryptanalyse, au contraire, cherchant à élaborer des protocoles mathématiques permettant de casser les cryptosystèmes.

La plupart de ces objectifs sont atteints grâce à la subtilité et l élégance de l arithmétique modulaire. Cet ouvrage est issu d un enseignement en mathématiques Spéciales MP* résultant à la fois d un approfondissement en algèbre destiné aux candidats des ENS et d une adaptation des mathématiques disponibles en Spé MP* aux techniques de codage et de décodage numériques.

Introduction

L arithmétique modulaire est, avant tout, la discipline mathématique dont l objet est l étude des anneaux ou des corps - le plus souvent finis -- obtenus par "réduction" à partir d un idéal I d un anneau commutatif A; l idéal I définit alors ce qu on appelle le modulo (ou parfois le modulus) à l aune duquel sont "regardés" les éléments de l an¬neau A; l ensemble ainsi "réduit", toujours noté A/I, porte le nom d ensemble quotient (algébrique) de l anneau A par son idéal I.

En pratique, ou bien A = E et I est du type nZ, ou bien A = [X], étant un corps (le plus souvent fini) et éventuellement, mais plus rarement, A = A'[X] où A' est un anneau fini, l idéal I étant toujours du type (P), c est-à-dire l idéal de A engendré par le polynôme P. A partir d un ensemble produit de l arithmétique modulaire usuelle, anneau E/(n) ou corps fini, on peut créer des sous-ensembles algébriquement très faciles à identifier, organisés en groupes cycliques, qui, à ce titre, relèvent également du concept modulaire (courbes elliptiques, surfaces de Frobénius, groupe des inversibles de Z/(n) lorsque n = pl, p premier...).

L intérêt de l arithmétique modulaire, telle qu elle vient d être exposée dans cette introduction, réside essentiellement dans le fait qu elle dispose et crée des ensembles finis, algébriquement très riches, pourvus de modes opératoires n ayant aucun ordre prévisible et, de ce fait, susceptibles de favoriser la création de mécanismes mathématiques de secret si nécessaires en cryptologie.

C est la raison pour laquelle sont réunies dans le même ouvrage l arithmétique mo¬dulaire et la cryptologie, étant entendu que cette discipline mathématique est abordée de façon élémentaire afin qu un taupin ou candidat aux concours (CAPES, Agrégation) puisse "y trouver son compte".

Table des matières :

Lire Arithmétique modulaire et cryptologie par Pierre MEUNIER pour ebook en ligneArithmétique modulaire et cryptologie par Pierre MEUNIER Téléchargement gratuit de PDF, livres audio, livres à lire, bons livres à lire, livres bon marché, bons livres, livres en ligne, livres en ligne, revues de livres epub, lecture de livres en ligne, livres à lire en ligne, bibliothèque en ligne, bons livres à lire, PDF Les meilleurs livres à lire, les meilleurs livres pour lire les livres Arithmétique modulaire et cryptologie par Pierre MEUNIER à lire en ligne.Online Arithmétique modulaire et cryptologie par Pierre MEUNIER ebook Téléchargement PDFArithmétique modulaire et cryptologie par Pierre MEUNIER DocArithmétique modulaire et cryptologie par Pierre MEUNIER MobipocketArithmétique modulaire et cryptologie par Pierre MEUNIER EPub
UYIJAEO4MH6UYIJAEO4MH6UYIJAEO4MH6