Mathématiques pour l'Informatique : Introduction et Fondements Mathématiques

Hervé Talé Kalachi

1 Objectifs du cours

Ce cours vise à fournir les fondements mathématiques essentiels pour aborder ultérieurement des notions de cryptographie. À l'issue de ce cours, l'étudiant devra :

— Comprendre le rôle des mathématiques dans la cryptographie.
— Maîtriser les méthodes de raisonnement et de preuve.
— Se familiariser avec des exemples historiques et des applications illustratives.

2 Le rôle des Mathématiques en Cryptographie

Les mathématiques constituent le socle de la cryptographie moderne. Elles permettent notamment de :

— Formaliser et démontrer la sécurité des algorithmes.
— Analyser la complexité des problèmes sous-jacents (par exemple, la factorisation utilisée en RSA).
— Garantir l'intégrité et la confidentialité des échanges d'informations.

Exemple : L'algorithme RSA repose sur la difficulté de factoriser un nombre composé en ses facteurs premiers.

3 Histoire et Motivation

La cryptographie a évolué depuis des systèmes simples de l'Antiquité jusqu'aux techniques de pointe actuelles :

— **Antiquité :** Chiffres simples (exemple, le chiffre de César).
— **Époque Moderne :** Développement de machines de chiffrement (exemple, Enigma pendant la Seconde Guerre mondiale).
— **Ère Numérique :** Apparition des systèmes asymétriques et des protocoles complexes.

4 Méthodes de Raisonnement et de Preuve

Pour développer une pensée rigoureuse, nous aborderons deux méthodes de preuve importantes.

4.1 Preuve par Induction

La preuve par induction est utilisée pour démontrer qu'une propriété $P(n)$ est vraie pour tout entier n à partir d'une base et d'une étape inductive.

1. **Étape de base :** Vérifier que $P(1)$ est vraie.
2. **Étape inductive :** Supposer que $P(n)$ est vraie pour un n quelconque et montrer que $P(n+1)$ est vraie.

Exemple : Montrer que la somme des n premiers entiers est donnée par :

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

4.2 Preuve par Contradiction

La preuve par contradiction consiste à supposer que la proposition à démontrer est fausse, puis à montrer que cette hypothèse conduit à une contradiction.

1. Supposer que la proposition P est fausse.
2. Déduire une contradiction.
3. Conclure que P doit être vraie.

Exemple : Démontrer qu'il existe une infinité de nombres premiers.

5 Solutions des Exemples

5.1 Exemple 1 : Preuve par Induction de la Somme des Entiers

Énoncé : Montrer que pour tout $n \geq 1$,

$$S(n) = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Preuve :

1. **Base :** Pour $n = 1$, $S(1) = 1 = \frac{1(1+1)}{2} = 1$.
2. **Induction :** Supposons que pour un $n \geq 1$,

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Alors, pour $n+1$,

$$1 + 2 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}.$$

La propriété est ainsi démontrée par induction.

5.2 Exemple 2 : Preuve par Contradiction de l'Infinité des Nombres Premiers

Énoncé : Prouver qu'il existe une infinité de nombres premiers.

Preuve : Supposons, par l'absurde, qu'il n'existe qu'un nombre fini de nombres premiers $p_1, p_2, \ldots, p_k$. Considérons alors le nombre

$$N = p_1 \cdot p_2 \cdots p_k + 1.$$

Pour tout $i \in \{1, \ldots, k\}$, le reste de la division de N par p_i est 1. Ainsi, N n'est divisible par aucun p_i et est soit premier, soit divisible par un nombre premier extérieur à la liste, ce qui contredit l'hypothèse initiale.

6 Exercices d'Application

Exercice 1 :

Démontrer par induction que pour tout $n \geq 1$,

$$2^n \geq n + 1.$$

Indice : Vérifiez la base pour $n = 1$ puis effectuez l'étape inductive.

Exercice 2 :

Utilisez la méthode de contradiction pour démontrer que $\sqrt{2}$ est irrationnel.

Exercice 3 :

Soit $A = \{x \in \mathbb{R} \mid x^2 < 2\}$.

1. Déterminez si A est borné.
2. Trouvez une borne supérieure et une borne inférieure pour A.

Solution Indicative pour l'Exercice 3 : A est borné, avec par exemple $\sqrt{2}$ comme borne supérieure et $-\sqrt{2}$ comme borne inférieure.

Références

[1] Velleman, Daniel J. *How to Prove It : A Structured Approach*. Cambridge University Press, 2006.

[2] Rosen, Kenneth H. *Discrete Mathematics and Its Applications*. McGraw-Hill, 7ème édition, 2011.

[3] Hoffstein, J., Pipher, J. et Silverman, J. H. *An Introduction to Mathematical Cryptography*. Springer, 2008.