

Dédicace

*Je dédie ce travail à mes chers parents, qu'ils trouvent
ici le témoignage de ma profonde gratitude pour leur amour,
leur encourage et leur soutien tout au long de mes études, que ALLAH les bénisse.*

Et mes chers frères

*A mon mari **mokhtari elhachemi.***

A tous mes amies.

A tous mes collègues de promotion.

A tous ceux que j'aime.

Avec l'expression de tous mes sentiments de respect,

Je dédie ce mémoire.

Remerciements

Je remercie tout d'abord mon Dieu qui m'a donné la force pour terminer ce modeste travail.

*Je tiens à remercier mon encadreur : **Mr. N. Ghadbane** pour
la confiance qu'il m'a témoignée en me proposant ce sujet, ses
encouragements et sa patience.*

*Les discussions scientifiques qu'il a su générer, ses remarques et ses
suggestions qui m'ont permis de finaliser ce modeste travail. Je
souhaite lui transmettre ma reconnaissance et ma plus profonde
gratitude.*

*Je remercie aussi tous les membres du Jury pour l'honneur qu'ils m'ont
fait, en acceptant de juger ce travail.*

*Je ne peux pas clôturer mes remerciements sans se retourner vers les
êtres qui me sont les plus chers, ma famille qui ont eu un rôle essentiel
et continu dans ma réussite.*

Merci

Table des matières

Notations	1
Introduction	2
1 Notions élémentaires sur l'arithmétique	3
1.1 Ensembles des entiers naturels et des entiers relatifs	4
1.2 Les opérations fondamentales sur l'arithmétique	5
1.3 Nombre premier et décomposition en facteurs premiers	12
1.4 Plus grand commun diviseur et plus petit commun multiple	14
1.5 Structures algébriques (groupes, anneaux, corps)	18
2 L'addition et la multiplication de Nim	22
2.1 L'addition de Nim et quelques propriétés	23
2.2 La multiplication de Nim et quelques propriétés	29
2.3 Les puissances de Fermat avec les opérations de Nim	34
3 Structures algébriques avec les opérations de Nim	36
3.1 Groupes	37
3.2 Anneaux	39
3.3 Corps	39
3.4 Les codes binaires	40
Conclusion	44
Bibliographie	45

Notations

$\emptyset$: Ensemble vide.

$\mathbb{N}$: Ensemble des entiers naturels (positifs ou nuls).

$\mathbb{N}^*$: Ensemble des entiers naturels strictement positifs.

$\mathbb{Z}$: Ensemble des entiers relatifs.

$a|b$: a divise b .

$PGCD$: Plus grand commun diviseur.

$PPCM$: Plus petit commun multiple.

$s(n)$: Successeur de n .

$\oplus$: L'addition de Nim.

$\otimes$: La multiplication de Nim.

$\{a'\}$: L'ensemble des nombres plus petit que a .

Introduction

L'arithmétique consiste, en résumé, à étudier les entiers relatifs, i.e, les éléments de $\mathbb{Z}$, l'arithmétique a aussi un côté et beaucoup plus puissant, à savoir la théorie des nombres, qui consiste à étudier l'arithmétique d'entiers plus généraux comme par exemple $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\} \subset \mathbb{C}$ où $i^2 = -1$. L'un des intérêts de l'arithmétique sont ses applications ludiques et concrètes, citons par exemple :

- La résolution d'équation diophantienne, le développement décimal de $1/p$, des applications des courbes elliptiques.
- Le jeu de Nim.
- Critères de primalité, factorisation des entiers.
- Les problèmes de transmissions, plus particulièrement, la cryptographie et des codes correcteurs d'erreurs.

L'objectif de ce mémoire est d'étudier deux opérations sur les entiers plutôt inhabituelles tels que l'addition et la multiplication de Nim qui permettent d'obtenir l'arithmétique de Nim et ainsi que certaines de leurs propriétés.

Ce travail est composé de 3 chapitres.

Le premier chapitre consiste en un rappel des notions et notations utilisées par la suite : la divisibilité, la division euclidienne, le plus grand commun diviseur et le plus petit commun multiple, les nombres premiers, les structures algébriques (groupes, anneaux, corps).

Dans le second chapitre, on fait une étude sur l'addition et la multiplication de Nim ainsi que certaines de leurs propriétés.

Dans le troisième chapitre nous avons présenté les structures algébriques (groupes, anneaux, corps) avec les opérations de Nim et quelques exemples. D'autre part on donne quelques notions sur les codes binaires.

Chapitre 1

Notions élémentaires sur l'arithmétique

Introduction

Ce chapitre, comme son nom l'indique, présente le concept de base de l'arithmétique, à savoir la divisibilité. On introduit ensuite les nombres premiers ce qui permet d'énoncer le théorème fondamental de l'arithmétique (c'est-à-dire la décomposition en facteurs premiers) dans lequel les nombres premiers, on introduit ensuite le plus grand commun diviseur et plus petit commun multiple et finalement les structures algébriques (groupes, anneaux, corps).

Contenu

- 1.1. Ensembles des entiers naturels et des entiers relatifs.
- 1.2. Les opérations fondamentales sur l'arithmétique.
- 1.3. Nombre premier et décomposition en facteurs premiers
- 1.4. Plus grand commun diviseur et plus petit commun multiple
- 1.5. Structures algébriques (groupes, anneaux, corps)

1.1 Ensembles des entiers naturels et des entiers relatifs

Définition 1.1.1 L'ensemble des entiers naturels $\mathbb{N}$ peut être défini comme un ensemble vérifiant les axiomes de Peano :

- $\mathbb{N}$ contient un élément appelé 0.
- Tout entier n de $\mathbb{N}$ a un successeur unique, noté $s(n)$.
- 0 n'est pas un successeur d'un entier.
- Deux entiers naturels ayant même successeur sont égaux.
- Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments, alors cet ensemble est égal à $\mathbb{N}$.

L'ensemble $\mathbb{N}^*$ est l'ensemble des entiers naturels non nuls, i.e, $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Définition 1.1.2. Dans $\mathbb{N}$, certaines équations du type $x + b = a$ (avec b non nul) n'ont pas de solution. On cherche à construire un nouvel ensemble de nombres notée $\mathbb{Z}$ contenant $\mathbb{N}$ des entiers relatifs dans le but de pouvoir résoudre ce type d'équation. L'ensemble $\mathbb{Z}$ est défini comme la symétrie de $\mathbb{N}$.

Théorème 1.1.3 (Principe de récurrence)

Soit P une proposition dépendant de $n \in \mathbb{N}$. On suppose :

- 1- $P(0)$ est vraie (initialisation).
- 2- Pour tout $n \in \mathbb{N}$, $P(n)$ implique $P(n + 1)$ (on dit alors que “ la propriété est héréditaire”).

Alors $P(n)$ est vraie pour tout entier $n \in \mathbb{N}$.

Preuve On considère l'ensemble $A = \{n \in \mathbb{N} : P(n) \text{ n'est pas vraie}\}$. On veut montrer que $A = \emptyset$. Par l'absurde, on suppose que $A \neq \emptyset$ et $A \subset \mathbb{N}$ donc il existe n_0 le plus petit élément de A . Puisque $P(0)$ est vraie, $n_0 \neq 0$. Mais $n_0 - 1 \notin A$ donc $P(n_0 - 1)$ est vraie, donc, par hypothèse sur P , $P(n_0)$ est vraie, d'où une contradiction avec le fait que $n_0 \in A$. Alors A est vide.

1.2 Les opérations fondamentales sur l'arithmétique

Dans cette section, nous allons définir les opérations fondamentales sur $\mathbb{N}$ et $\mathbb{Z}$, comme l'addition et la multiplication.

Définition 1.2.1 On définit par récurrence sur l'ensemble $\mathbb{N}$ des entiers naturels, une loi de composition interne appelée addition et notée $+$, comme suit :

- $\forall n \in \mathbb{N} : n + 0 = n.$
- $\forall n, p \in \mathbb{N} : n + s(p) = s(n + p).$

Exemples 1.2.2

1- $\forall n \in \mathbb{N}, n + 2$ désigne le successeur du successeur de n , on a donc

$$\begin{aligned}n + 2 &= n + s(1) \\&= s(n + 1) \\&= s(n + s(0)) \\&= s(s(n)) \\&= s^2(n).\end{aligned}$$

2-

$$\begin{aligned}2 + 3 &= 2 + s(2) = s(2 + 2) \\&= s(2 + s(1)) = s(s(1 + 2)) \\&= s(s(s(0) + 2)) = s(s(s(2))) \\&= s(s(3)) = s(4) \\&= 5.\end{aligned}$$

Propriétés 1.2.3

- 1- La loi $+$ est commutative.
- 2- La loi $+$ est associative.
- 3- La loi $+$ possède un élément neutre.

Preuve Montrons par récurrence sur l'entier n .

1- Commutativité de $+$:

- Pour $n = 0, \forall m \in \mathbb{N} : 0 + m = m + 0 = m$ (d'après la définition).
- Supposons la propriété vraie pour un entier $n \geq 0$ et nous prouvons sa vérité pour $s(n)$, on a :

$$\forall m \in \mathbb{N}, s(n) + m = s(n + m) = s(m + n) = m + s(n).$$

2- Associativité de $+$:

- Pour $n = 0, \forall m, p \in \mathbb{N} : 0 + (m + p) = (0 + m) + p = m + p$.
- Supposons propriété vraie pour un entier $n \geq 0$ et nous prouvons sa vérité pour $s(n)$, $\forall m, p \in \mathbb{N}$, on a :

$$\begin{aligned}(s(n) + m) + p &= s(n + m) + p = (n + m) + s(p) \\ &= n + (m + s(p)) \\ &= n + s(m + p) \\ &= s(n) + (m + p).\end{aligned}$$

3- L'élément neutre : D'après la définition de l'addition l'élément neutre est 0.

Nous définissons maintenant la multiplication des entiers.

Définition 1.2.4 On définit par récurrence sur l'ensemble $\mathbb{N}$ des entiers naturels, une loi de composition interne appelée multiplication et notée $\times$, comme suit :

- $\forall n \in \mathbb{N} : 0 \times n = 0$.
- $\forall n, p \in \mathbb{N} : s(p) \times n = (p \times n) + n$.

Exemple 1.2.5 On calcul 2×2 :

$$\begin{aligned}2 \times 2 &= s(1) \times 2 = 1 \times 2 + 2 = s(0) \times 2 + 2 \\ &= 0 \times 2 + 2 + 2 = 0 + 2 + 2 = s(1) + 2 \\ &= s(1 + 2) = s(s(0) + 2) = s(s(0 + 2)) \\ &= s(s(2)) = 4.\end{aligned}$$

Propriétés 1.2.6

1- La multiplication est distributive par rapport à l'addition, i.e,

$$\forall a, b, c \in \mathbb{N} : a \times (b + c) = (a \times b) + (a \times c) \text{ et } (a + b) \times c = (a \times c) + (b \times c).$$

2- La multiplication est commutative : $\forall a, b \in \mathbb{N}, a \times b = b \times a$.

3- La multiplication est associative : $\forall a, b, c \in \mathbb{N}, a \times (b \times c) = (a \times b) \times c$.

4- L'entier naturel 1 est un élément neutre pour la multiplication, i.e, $\forall n \in \mathbb{N} : n \times 1 = n$.

Preuve

1- **Distributivité de $\times$** : Montrons par récurrence sur c .

- Pour $c = 0$ on a $(a + b) \times 0 = 0$ et $a \times 0 + b \times 0 = 0$ pour tous $a, b \in \mathbb{N}$, donc $(a + b) \times 0 = a \times 0 + b \times 0 = 0$.

- Supposons que l'égalité est satisfaite pour c et calculons $(a + b) \times s(c)$ et

$a \times s(c) + b \times s(c)$, $\forall a, b, c \in \mathbb{N}$. En appliquant l'hypothèse de récurrence, on obtient :

$$(a + b) \times s(c) = (a + b) \times c + (a + b) = (a \times c) + (b \times c) + (a + b) \quad (1)$$

et

$$a \times s(c) + b \times s(c) = (a \times c) + a + (b \times c) + b = (a \times c) + (b \times c) + (a + b) \quad (2)$$

De (1) et (2) la multiplication est distributive.

2- **Commutativité de $\times$** : Montrons par récurrence sur b .

- Pour $b = 0$, $\forall a \in \mathbb{N} : a \times 0 = 0 \times a = 0$ (d'après la définition).

- Supposons que $a \times b = b \times a$ et nous prouvons l'égalité est vraie pour $s(b)$, on a :

$$\forall a, b \in \mathbb{N}, a \times s(b) = (a \times b) + a \quad (1)$$

et

$$\forall a, b \in \mathbb{N}, s(b) \times a = (b + 1) \times a = (b \times a) + (1 \times a) = (b \times a) + a = (a \times b) + a \quad (2)$$

De (1) et (2) la multiplication est commutative.

3- Associativité de $\times$: Montrons par récurrence sur c .

- Pour $c = 0$, on a $(a \times b) \times 0 = 0$ et $a \times (b \times 0) = a \times 0 = 0$ pour tous $a, b \in \mathbb{N}$ donc $(a \times b) \times 0 = a \times (b \times 0) = 0$.

- Supposons que l'égalité est satisfaite pour c et calculons $(a \times b) \times s(c)$ et $a \times (b \times s(c))$ pour tous a, b, c trois entières naturels. En appliquant l'hypothèse de récurrence, on obtient :

$$(a \times b) \times s(c) = ((a \times b) \times c) + (a \times b) = (a \times (b \times c)) + (a \times b) \quad (1)$$

et

$$a \times (b \times s(c)) = a \times ((b \times c) + b) = ((b \times c) + b) \times a = (a \times (b \times c)) + (a \times b) \quad (2)$$

De (1) et (2) la multiplication est associative.

4- Élément neutre : $\forall n \in \mathbb{N}, n \times 1 = n \times s(0) = (n \times 0) + n = 0 + n = n$.

Définition 1.2.7 (Divisibilité dans $\mathbb{Z}$) Soit $a, b \in \mathbb{Z}$, on dit que a divise b et le note $a|b$, s'il existe un entier relative q tel que : $b = a \times q$.

Exemples 1.2.8

1- $3|6$ car $6 = 3 \times 2$.

2- $\forall n \in \mathbb{Z}, 2|n \times (n + 1)$ en effet :

- Si n est pair, $n = 2 \times p$, pour $p \in \mathbb{Z}$ et donc :

$$n \times (n + 1) = 2 \times p \times (n + 1) \Rightarrow 2|n \times (n + 1).$$

- Si n est impair, alors $n = 2 \times p + 1$ pour $p \in \mathbb{Z}$ et donc :

$$n \times (n + 1) = n \times (2 \times p + 2) = n \times (2 \times (p + 1)) = (n \times 2) \times (p + 1) \Rightarrow 2|n \times (n + 1).$$

Remarque 1.2.9 Autres formulations, $a|b$ signifié :

- b est un multiple de a .
- a est un diviseur de b .

Propriété 1.2.10 Soient a, b et c désignent des entiers relatifs.

- 1- (Réflexivité), $\forall n \in \mathbb{Z}, n|n$.
- 2- (Transitivité), $\begin{cases} a|b \\ b|c \end{cases} \Rightarrow a|c$.
- 3- Tout entier n admet au moins quatre diviseurs sont : $1, -1, n, -n$.
- 4- Pour tout entier $k : a|b \Rightarrow (ka)|(kb)$.

Preuve

- 1- $\forall n \in \mathbb{Z}, n|n$ car $n = n \times 1$.
- 2- On traduit les hypothèses : Il existe p et q deux entier tel que :
$$\begin{cases} b = a \times p \\ c = b \times q \end{cases} \Rightarrow c = (a \times p) \times q = a \times (p \times q).$$
- 3- Soit $n \in \mathbb{Z}, n = n \times 1 = 1 \times n$ et $n = (-n) \times (-1) = (-1) \times (-n) \Rightarrow -1, 1, n$ et $-n$ sont diviseurs de n .
- 4- Il existe un entier p et q tel que $b = a \times p$, donc $k \times b = (k \times a) \times p \Rightarrow (ka)|(kb)$.

Théorème 1.2.11 (Division Euclidienne)

Soient a et b deux éléments de $\mathbb{Z}$, avec $b \neq 0$. Il existe un couple unique $(q, r) \in \mathbb{Z}^2$ vérifiant :

$$\begin{cases} a = b \times q + r \\ 0 \leq r < b \end{cases}$$

On dit que q est le quotient et r le reste de la division euclidienne de a par b .

Preuve Il ya deux parties à démontrer dans ce théorème : L'existence du couple (q, r) , puis son unicité.

1- Existence de q et r :

- Premier cas : Si $0 \leq a < b$ alors le couple $(q, r) = (0, a)$ convient.
- Second cas : Si $a = b$ alors le couple $(1, 0)$ convient.

• Troisième cas : Supposons que $a > b$. En particulier, a et b sont donc tous strictement positifs. Soit $E = \{p \in \mathbb{N} | a < pb\}$, $E \neq \emptyset$ donc E admet un plus petit élément p_0 . Si $q = p_0 - 1$, on a alors $a < p_0 b = (q + 1)b$ et $q \notin E$, d'où l'encadrement $qb \leq a < (q + 1)b = qb + b$. Soit $r = a - bq$ on obtient $a = bq + r < bq + b$ donc $r < b$.

2- Unicité de couple (q, r) :

Supposons qu'il existe deux couples (q, r) et (q', r') tel que : $a = bq + r$ et $a = bq' + r'$, avec $0 \leq r < b$ et $0 \leq r' < b$. Comme $a = bq + r = bq' + r'$ alors $b(q - q') = r - r'$ avec $q - q'$ entier, $r - r'$ est multiple de b . Comme $0 \leq r < b$ alors $-b < -r \leq 0$ et, en additionnant avec la relation $0 \leq r' < b$, on obtient : $-b < r' - r < b$.

Or $r' - r$ est aussi multiple de b . Le seul multiple de b compris strictement entre $-b$ et b est 0. Par conséquent : $r' - r = 0$ et $r' = r$. En reportant dans $a = bq + r = bq' + r'$, on obtient alors $bq + r = bq' + r$ puis $bq = bq'$, d'où $q = q'$ car $b \neq 0$, donc le couple (q, r) est unique.

Exemple 1.2.12 La division euclidienne de $(n + 3)^2$ par $(n + 4)$

$$\begin{aligned} (n + 3)^2 &= n^2 + 9 + 6n \\ &= n(n + 4) + 2n + 9 \\ &= n(n + 4) + 8 + 1 + 2n \\ &= n(n + 4) + 2(4 + n) + 1 \\ &= (n + 2)(n + 4) + 1. \end{aligned}$$

Donc le reste de division $(n + 3)^2$ par $(n + 4)$ est 1, $0 \leq 1 < n + 4$ pour tout $n \in \mathbb{N}$.

Définition 1.2.13 (Congruence dans $\mathbb{Z}$)

Soit a et b des entiers relatifs et $n > 1$ un entier strictement positif. On dit que a est congru à b modulo n lorsque $a - b$ est un multiple de n .

Notation : Lorsque a est congru à b modulo n , on note :

$$a \equiv b[n] \text{ ou } a \equiv b(\text{mod } n).$$

Propriétés 1.2.14 On a pour tous $a, b, c, n \in \mathbb{Z}$.

- 1- $\forall a \in \mathbb{Z}, a$ est divisible par $n \Leftrightarrow a \equiv 0[n]$.
- 2- $\forall a \in \mathbb{Z}, a \equiv a[n]$ (la relation de congruence est réflexive).
- 3- Si $a \equiv b[n]$ et si $b \equiv c[n]$, alors $a \equiv c[n]$ (la relation de congruence est transitive).
- 4- Si $a \equiv b[n]$, alors $b \equiv a[n]$ (la relation de congruence est symétrique).

Preuve On a pour tous $a, b, c, n \in \mathbb{Z}$.

- 1- Si a est divisible par n alors il existe $k \in \mathbb{Z}$ tel que :

$$a = nk \Rightarrow a - 0 = nk \Rightarrow a \equiv 0[n].$$

- 2- On a $n|(a - a)$ alors $a - a = nk, k \in \mathbb{Z}$, donc $a \equiv a[n]$.

- 3- Si $a \equiv b[n]$ alors $a = b + nk, k \in \mathbb{Z}$ et on a si $b \equiv c[n]$ alors $b = c + nk', k' \in \mathbb{Z}$, donc :

$$\begin{aligned} a &= b + nk = c + nk' + nk \\ &= c + n(k + k') \\ &= c + nk'', k'' = (k + k') \in \mathbb{Z}. \end{aligned}$$

- 4- Si $a \equiv b[n]$, alors $n|a - b$, on déduit que $n|b - a$ (dans $\mathbb{Z}$) et donc $b \equiv a[n]$.

Proposition 1.2.15 Soient $a, b, c, n \in \mathbb{Z}$ et $n > 1$. Alors :

- Si $a \equiv b[n]$ alors $a + c \equiv b + c[n]$ (la relation de congruence est compatible avec l'addition).
- Si $a \equiv b[n]$ alors $a \times c \equiv b \times c[n]$ (la relation de congruence est compatible avec la multiplication).

Preuve On a $a \equiv b[n] \Rightarrow a = b + nk, k \in \mathbb{Z}$, donc :

- $\forall a, b, c, n \in \mathbb{Z}, a + c = (b + nk) + c = (b + c) + nk/k \in \mathbb{Z} \Rightarrow a + c \equiv b + c[n]$.
- $\forall a, b, c, n \in \mathbb{Z}, a \times c = (b + nk) \times c = (b \times c) + n \times k \times c = (b \times c) + n \times k'/k' = (c \times k) \in \mathbb{Z} \Rightarrow a \times c \equiv b \times c[n]$.

Exemples 1.2.16

1- $57 \equiv 15[7]$ car : $57 - 15 = 42$ est un multiple de 7.

2- Si $x \equiv 0[2]$, alors x est pair et si $x \equiv 1[2]$, x est impair.

Définition 1.2.17 (Principe de la numération de position).

Il consiste à choisir une base b de numération, et b symboles qui constitueront les chiffres dans la représentation d'un entier positif en base b . Celle-ci s'écrira alors :

$$n = n_p b^p + n_{p-1} b^{p-1} + \dots + n_1 b^1 + n_0.$$

Notation : Cette écriture est abrégée en $\overline{(n_p n_{p-1} \dots n_0)_b}$.

Obtention de cette représentation : L'algorithme pour obtenir la représentation en base b d'un entier est :

- Effectuer la division euclidienne de cet entier par b , division qui donne un premier quotient et un premier reste.
- Le quotient est à son tour divisé par b pour donner un second quotient et un second reste, et ainsi de suite jusqu'à obtenir un quotient nul.
- Les restes successifs (tous strictement inférieurs à b), et en commençant par le dernier, constituent la représentation en base b de l'entier donné.

Exemples 1.2.18

1- Le nombre 14 en base 2 est 1110.

2- Le nombre 120 en base 2 est 1111000.

1.3 Nombre premier et décomposition en facteurs premiers

Définition 1.3.1 Un nombre premier est un entier naturel qui admet exactement deux diviseurs : 1 et lui-même.

Théorème 1.3.2 (Critère d'arête)

- Tout entier naturel $n, n \geq 2$ admet un diviseur premier.
- Si n n'est pas premier, alors il admet un diviseur premier p tel que :

$$2 \leq p \leq \sqrt{n}.$$

Preuve

- Si n est premier, il admet donc un diviseur premier : lui-même.
- Sinon, on suppose D l'ensemble des diviseurs de n , tel que D n'est pas vide (il contient 1). Il admet donc un plus petit élément p . Si p n'était pas premier, il admettrait un diviseur d' tel que : $2 \leq d' < p$, qui diviserait n . Ceci contredirait la définition de p . Donc p est premier. Et on a $n = p \times q$ avec $p \leq q$. En multipliant cette inégalité par p , on obtient :

$$p^2 \leq pq \Rightarrow p^2 \leq n \Leftrightarrow p \leq \sqrt{n}.$$

Exemple 1.3.3 (Comment montre que 109 est un nombre premier)

- On a $10 < \sqrt{109} < 11$, on teste donc 2, 3, 5 et 7 tous les nombres premiers strictement inférieurs à 11.
- Des règles de divisibilité, on déduit 109 n'est divisible ni par 2, ni par 3, ni par 5.
- Soit, on se rappelle le critère de divisibilité par 7, soit on effectue la division euclidienne de 109 par 7, on obtient :

$$109 = 7 \times 15 + 4.$$

Donc 109 n'est pas divisible par 7, comme 109 n'est pas divisible par 2, 3, 5, 7 et $(11)^2 > 109$ il est premier.

Définition 1.3.4 L'écriture d'un entier sous la forme $n = a^\alpha b^\beta c^\gamma \dots$, où $a, b, c, \dots$, sont les diviseurs premiers distincts de n et où les exposants $\alpha, \beta, \gamma, \dots$, sont tels que, par exemple, n est divisible par a^α mais pas par $a^{\alpha+1}$. S'appelle la décomposition en facteurs

premiers de n . On dit que les exposants α , β , et γ sont les ordres de multiplicité des diviseurs a, b, c .

Corollaire 1.3.5 Soit p un nombre premier. Si p divise un produit $p_1 p_2 \dots p_n$ de n nombres premiers, il existe un indice $i \in \{1, 2, 3, \dots, n\}$ tel que :

$$p = p_i.$$

Exemple 1.3.6 Décomposons 120 en nombres premier

$$\begin{array}{rcl} 120 & : & 2 \\ 60 & : & 2 \\ 30 & : & 2 \\ 15 & : & 3 \\ 5 & : & 5 \\ 1 & & fin \end{array}$$

On présente la décomposition avec une barre verticale ou l'on écrit à gauche le quotient des diviseurs premiers pris dans l'ordre croissant :

$$120 = 2^3 \times 3 \times 5.$$

On a $(3 + 1)(1 + 1)(1 + 1) = 4 \times 2 \times 2 = 16$, 120 possède donc 16 diviseurs.

1.4 Plus grand commun diviseur et plus petit commun multiple

Notation : Etant donné deux entiers $a, b \in \mathbb{Z}$ on note $D(\{a, b\})$ (respectivement $M(\{a, b\})$) l'ensemble des diviseurs (respectivement multiples) communs de a et de b .

Définition 1.4.1

- On appelle *PGCD* de a et b tout entier p tel que :

$$p \in D(\{a, b\}) \text{ et pour tout } d \in D(\{a, b\}), d|p.$$

- On appelle *PPCM* de a et b tout entier q tel que :

$$q \in M(\{a, b\}) \text{ et pour tout } m \in M(\{a, b\}), m|q.$$

Définition 1.4.2 (Nombres premiers entre eux) Deux entiers a et b sont premiers entre eux si et seulement si :

$$PGCD(a, b) = 1.$$

Exemples 1.4.3

1- $PGCD(120, 32) = 8$; $PPCM(120, 32) = 480$.

2- 36 et 35 sont premiers entre eux, 16 et 18 ne le sont pas car ils sont tous deux pairs.

Théorème 1.4.4 (Égalité de Bézout)

Soit a et b deux entiers non nuls et $d = PGCD(a, b)$. Il existe alors un couple (u, v) d'entiers relatifs tel que :

$$au + bv = d.$$

Preuve Considérons G l'ensemble formé par les entiers naturels strictement positifs de la forme $ma + nb$ où m et n sont des entiers relatifs. G admet donc un plus petit élément $d = au + bv$. Il ne reste plus qu'à montrer que $d = PGCD(a, b)$. On le fait par double inégalité. Posons $D = PGCD(a, b)$. Comme D divise a et b , il divise aussi $au + bv = d$. Donc $D \leq d$. Montrons que d divise a et b . La division euclidienne de a par d s'écrit $a = dq + r$ avec $0 \leq r < d$. D'où,

$$\begin{aligned} r &= a - dq \\ &= a - (au + bv)q \\ &= a(1 - uq) + b(-vq). \end{aligned}$$

Donc $r \in G$ et $r < d$. Cette condition ne peut être remplie sans contredire la définition de d que si $r = 0$, i.e, $d|a$. Par le même raisonnement, on montrerait que $d|b$. Le nombre d est donc un diviseur de a et b . Il est plus petit que D : $d \leq D$. Donc $d = D$.

Théorème 1.4.5 (Théorème de Bézout)

Deux entiers relatifs a et b sont premiers entre eux si et seulement si, il existe deux entiers relatifs u et v tel que :

$$au + bv = 1.$$

Preuve

$\Rightarrow$) Si $PGCD(a, b) = 1$, c'est immédiat grâce à l'égalité de Bézout.

$\Leftarrow$) Réciproquement, supposons qu'il existe deux entiers u et v tel que : $au + bv = 1$.

On a $PGCD(a, b)$ divise a et b par définition donc divise aussi $au + bv = 1$. Donc :

$$PGCD(a, b) = 1.$$

Théorème 1.4.6 ((lemme de Gauss)(Carl Frindrich Gauss, 1777–1855))

Soient a , b et c trois entiers, si a divise le produit bc et si a est premier avec b , alors a divise c , i.e,

$$a|bc \text{ et } PGCD(a, b) = 1 \text{ donc } a|c.$$

Preuve Avec le théorème de Bézout, la démonstration est simple. On traduit l'énoncé et on observe :

Comme $a|bc$, il existe $k \in \mathbb{Z}$ tel que :

$$bc = ka.$$

Comme a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tel que :

$$au + bv = 1.$$

En multipliant par c , on a :

$$acu + (bc)v = c \Leftrightarrow a(cu + kv) = c.$$

Donc a divise c .

Proposition 1.4.7 Entre le $PGCD(a, b)$ et $PPCM(a, b)$, on a la relation suivant :

$$PPCM(a, b) = \frac{a \times b}{PGCD(a, b)}.$$

Preuve Tout d'abord, si a est nul et b non nul, l'égalité est vérifiée car $d = b$ et $m = 0$. De même pour $b = 0$ et $a \neq 0$. Supposons maintenant que a et b soient non nuls, posons $d = PGCD(a, b)$ et soient a' et b' des entiers premiers entre eux tels que $a = da'$ et $b = db'$. Soit μ un multiple commun de a et b , i.e,

$$\begin{aligned}\exists(k, k') \in Z^2 \text{ tel que } \mu = ka & \quad \text{et} \quad \mu = k'b \\ & = kda' \quad \quad \quad = k'db'.\end{aligned}$$

D'où, $kda' = k'db'$ et par simplification par $d \leq 0, ka' = k'b'$. Conséquence, a' divise $k'b'$. Or a' et b' sont premiers entre eux. D'après le théorème de Gauss, a'/k' . Il existe ainsi un entier q tel que $k' = qa'$, i.e, $\mu = qda'b'$. Ainsi, tout multiple commun μ à a et b est un multiple de $da'b'$. Or, par définition, le plus petit de ces multiples est $PPCM(a, b)$ et l'égalité est atteinte pour $q = 1$, i.e, $PPCM(a, b) = da'b'$. On alors :

$$PPCM(a, b) \times PGCD(a, b) = (da'b') \times d = (da') \times (db') = ab.$$

Exemples 1.4.8

$$\mathbf{1-} \quad PGCD(28, 77) = 7; PPCM(28, 77) = \frac{28 \times 77}{7} = 308.$$

$$\mathbf{2-} \quad PGCD(18, 42) = 6; PPCM(28, 77) = \frac{18 \times 42}{6} = 126.$$

Théorème 1.4.9 Soit a et b deux naturels non nuls tels que b ne divise pas a . La suite des divisions euclidiennes suivantes finit par s'arrêter. Le dernier reste non nul est alors le $pgcd(a, b)$.

$$a \text{ par } b \quad \quad a = b \times q_0 + r_0 \quad \quad \text{avec} \quad \quad b > r_0 > 0$$

$$b \text{ par } r_0 \quad \quad b = r_0 \times q_1 + r_1 \quad \quad \text{avec} \quad \quad r_0 > r_1 > 0$$

$$r_0 \text{ par } r_1 \quad \quad r_0 = r_1 \times q_2 + r_2 \quad \quad \text{avec} \quad \quad r_1 > r_2 > 0$$

...

...

$$r_{n-2} \text{ par } r_{n-1} \quad r_{n-2} = r_{n-1} \times q_n + r_n \quad \quad \text{avec} \quad \quad r_{n-1} > r_n > 0$$

$$r_{n-1} \text{ par } r_n \quad \quad r_{n-1} = r \times q_{n+1} + 0.$$

On a alors $PGCD(a, b) = r_n$.

Preuve La suite des restes : $r_0, r_1, r_2, \dots, r_n$ est une suite strictement décroissante dans $\mathbb{N}$ car $r_0 > r_1 > r_2 > \dots > r_n$. Cette suite est donc finie. Il existe alors n tel que $r_{n+1} = 0$.

Montrons que $PGCD(a, b) = PGCD(b, r_0)$.

Soit $D = PGCD(a, b)$ et $d = PGCD(b, r_0)$. D divise a et b donc D divise $a - bq_0 = r_0$, donc D divise b et r_0 donc : $D \leq d$, d divise b et r_0 donc d divise $bq_0 + r_0 = a$, donc d divise a et b donc : $d \leq D$. De (1) et (2) alors $D = d$, c'est-à-dire $PGCD(a, b) = PGCD(b, r_0)$.

De proche en proche, on en déduit que :

$$PGCD(a, b) = PGCD(b, r_0) = \dots = PGCD(r_{n-2}, r_{n-1}) = PGCD(r_{n-1}, r_n).$$

Or r_n divise r_{n-1} , donc $PGCD(r_{n-1}, r_n) = r_n$. Donc $PGCD(a, b) = r_n$. Le dernier reste non nul est le pgcd.

Exemple 1.4.10 On calcule $PGCD(1600, 229)$ par l'algorithme d'Euclide :

$$1600 = 229 \times 6 + 226,$$

$$229 = 226 \times 1 + 3,$$

$$226 = 3 \times 75 + 1,$$

$$3 = 1 \times 3 + 0.$$

Donc $PGCD(1600, 229) = 1$,

1.5 Structures algébriques (groupes, anneaux, corps)

Définition 1.5.1 Un groupe est la donnée d'un ensemble G et d'une loi interne notée $*$

$$G * G \longrightarrow G.$$

$$(x, y) \longmapsto x * y$$

telle que $(G, *)$ vérifie les trois propriétés suivantes :

- 1- (Elément neutre) Il existe $e \in G$, $\forall x \in G : e * x = x * e = x$.
- 2- (Associativité) Pour tous $x, y, z \in G : (x * y) * z = x * (y * z)$.
- 3- (Elément inverse) $\forall x \in G, \exists x' \in G : x * x' = x' * x = e$.

Si de plus $\forall x, y \in G, x * y = y * x$, on dit que $*$ est commutative et que $(G, *)$ est un groupe commutatif ou abélien.

Notation : Les notations les plus utilisées sont la notation additive avec 0 pour élément neutre, $-x$ pour le symétrique (dit aussi opposé) et la notation multiplicative où l'élément neutre est noté 1, x^{-1} pour le symétrique (dit aussi inverse).

Proposition 1.5.2

- 1- Dans un groupe l'élément neutre est unique.
- 2- Dans un groupe l'inverse x' d'un élément x est unique.
- 3- L'inverse de l'inverse de x est x , i.e, $\forall x, x' \in G : (x')' = x$.
- 4- $\forall x, y \in G : (x * y)' = y' * x'$.

Preuve

- 1- On suppose que il existe deux élément neutre $\acute{e}, e \in G$ tel que $\acute{e} * x = x, e * x = x$ donc par conséquence $\acute{e} = e$.
- 2- Soit $x', x'' \in G$ et on a $x' * x = e, x'' * x = e$ donc $x'' * x * x' = e * x' = x'$ donc par conséquence $x'' = x'$.
- 3- Pour tous $x, x' \in G$, on a $x * x' = x' * x = e$ donc x est l'inverse de x' , d'après 2. On a $x = (x')'$.
- 4- $\forall x, y \in G$, on a $(x * y) * (y' * x') = x * y * y' * x' = x * e * x' = e$ donc $(x * y)' = y' * x'$.

Exemples 1.5.3

- 1- $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ sont des groupes additifs commutatifs.
- 2- $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe multiplicative commutative, avec $(\mathbb{Z}/p\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \dots, \overline{(p-1)}\}$, p premier.

Définition 1.5.4 Un anneau est la donnée d'un ensemble A et de loi interne de composition $+$ (addition) et $\times$ (multiplication) telles que :

- 1- $(A, +)$ est un groupe commutatif (dont on note l'élément neutre $0 = 0_A$).
- 2- La loi $\times$ est associative.
- 3- La loi $\times$ possède un élément neutre (qu'on notera $1 = 1_A$).
- 4- La loi $\times$ est distributive par rapport à l'addition, i.e,

$$\forall x, y, z \in A, x \times (y + z) = (x \times y) + (x \times z) \text{ et } (y + z) \times x = (y \times x) + (z \times x).$$

Si de plus la loi $\times$ est commutative, on dit que l'anneau A est commutatif.

Définition 1.5.5 (Sous anneaux)

Soit $(A, +, *)$ un anneaux et B une partie de A . On dit que B est un sous anneaux de l'anneaux $(A, +, *)$ si :

- 1- $1_A \in B$.
- 2- $\forall a, b \in B, a - b \in B$.
- 3- $\forall a, b \in B, ab \in B$.

Exemples 1.5.6

- 1- $(\mathbb{Z}, +, \times)$ est un anneau commutatif.
- 2- $(\mathbb{R}^n, +, \times)$ est un anneau commutatif pour les lois internes suivantes :

$$\begin{aligned} (x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) &= (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n), \\ (x_1, x_2, \dots, x_n) \times (y_1, y_2, \dots, y_n) &= (x_1 \times y_1, x_2 \times y_2, \dots, x_n \times y_n). \end{aligned}$$

Définition 1.5.7 $\mathbf{K} = (\mathbf{A}, +, *)$ est un corps si et seulement si :

- 1- $K = (A, +, *)$ est un anneau.
- 2- Chaque élément non nul de A possède un inverse pour l'opération $(*)$.

Définition 1.5.8 Un corps fini est un corps qui possède un nombre fini q d'éléments, et on le note par F_q .

Propriétés 1.5.9

- 1- Tout corps fini est commutatif.
- 2- La cardinalité d'un corps fini F_q est une puissance d'un nombre premier, i.e, $q = p^m$, avec p est premier et $m > 0$.

Définition 1.5.10 (Sous corps)

Soit $(K, +, *)$ un corps et K' un sous anneaux de $(K, +, *)$ on dit qu'une partie K' est un sous corps du corps de $(K, +, *)$ si $(K', +, *)$ est un corps.

Exemples 1.5.11

- 1- $F_2 = \{0, 1\}$ est le corps binaire, c'est le plus petit corps fini.
- 2- $\mathbb{Z}/p\mathbb{Z}$ avec p premier sont des corps finis de cardinal p .

Chapitre 2

L'addition et la multiplication de Nim

Introduction

Dans ce chapitre, on donne les notions et les propriétés de l'addition et la multiplication de Nim.

Contenu

- 2.1. L'addition de Nim et quelques propriétés.
- 2.2. La multiplication de Nim et quelques propriétés.
- 2.3. Les puissances de Fermat avec les opérations de Nim.

2.1 L'addition de Nim et quelques propriétés

Définition 2.1.1 Pour X un sous ensemble de $\mathbb{N}$, $X \neq \mathbb{N}$, on a :

$$\text{mex}(X) = \min(\mathbb{N}/X).$$

Exemples 2.1.2

1- $\text{mex}(\{1, 2, 3, 4, 5\}) = \min(\mathbb{N}/\{1, 2, 3, 4, 5\}) = 0.$

2- $\text{mex}(\{0, 1, 2, 3, 5, 6, 7\}) = \min(\mathbb{N}/\{0, 1, 2, 3, 5, 6, 7\}) = 4.$

3- $\text{mex}(\{n = 2k, k \in \mathbb{N}\}) = \min(\mathbb{N}/\{n = 2k, k \in \mathbb{N}\}) = 1.$

Notation :

- On notera $\oplus$ et $\otimes$ les symboles d'addition et de multiplication de Nim respectivement.
- Les symboles utilisés pour l'addition et la multiplication habituelle sur les entiers seront ceux généralement utilisés, c'est à dire $+$ ou $\times$.
- Les relations d'inégalité seront toujours utilisées suivant leur sens usuel (c'est à dire que l'ordre qu'elles définissent est l'ordre usuel des entiers).

Définition 2.1.3 Pour tous $a, b \in \mathbb{N}$, $a \oplus b$ est le plus petit entier naturel qui n'est pas de la forme $a' \oplus b$ pour $a' < a$ ni $a \oplus b'$ pour $b' < b$.

Symboliquement,

$$a \oplus b = \text{mex}(\{a' \oplus b : 0 \leq a' < a\} \cup \{a \oplus b' : 0 \leq b' < b\}).$$

Définition 2.1.4 Soient $a, b \in \mathbb{N}$, soient $a_2, b_2 \in F_2^n$ leurs représentations en base 2, avec n le nombre de chiffres nécessaires pour écrire le plus grand des nombres a_2 et b_2 . On définit alors $\oplus$ comme l'addition composante par composante des vecteurs a_2 et b_2 .

De manière équivalente, cela se formule en disant que $\oplus$ est l'addition sans retenue (ou encore le « ou exclusif » xor) sur les chaînes de n bits représentant a et b .

Remarques 2.1.5

- 1- L'addition de Nim est définie d'une manière récursive.
- 2- Les ensembles $\{a' \oplus b\}$ et $\{a \oplus b'\}$ peuvent être vus comme des suites indexées par les $\{0, 1, 2, \dots, a-1\}$ et les $\{0, 1, 2, \dots, b-1\}$,

3- Si $a = 0$ ou $b = 0$, l'ensemble $\{i|i < a\}$ ou l'ensemble $\{i|i < b\}$ à considérer est vide.

Exemple 2.1.6 Une opération encore plus simple, l'addition binaire sans retenue :

$$\begin{aligned} 42 &= (101010)_2 \text{ et } 38 = (100110)_2 \\ (101010)_2 + (100110)_2 &= (001100)_2 = 12. \\ \text{Donc } 42 \oplus 38 &= 12. \end{aligned}$$

Exemple 2.1.7

$$\begin{aligned} 1 &= (001)_2 \text{ et } 3 = (011)_2 \\ (001)_2 + (011)_2 &= (010)_2 = 2 \\ \text{Donc } 1 \oplus 3 &= 2. \end{aligned}$$

Propriétés 2.1.8

- 1-** $\forall a \in \mathbb{N} : a \oplus 0 = a.$
- 2-** $\forall a \in \mathbb{N} : a \oplus a = 0.$

Preuve

1- On montre que par récurrence sur a .

- Pour $a = 0$, on a $0 \oplus 0 = \text{mex} \{a' \oplus 0, 0 \oplus b' | a' < 0, b' < 0\}, \{a' \oplus 0\} = \phi, \{0 \oplus b'\} = \phi$, et on a $\text{mex } \phi = 0$ donc $0 \oplus 0 = 0$.
- Si on suppose que $a' \oplus 0 = a', \forall a' < a$, et nous prouvons le propriété est vraie pour a , on a alors :

$$\begin{aligned} a \oplus 0 &= \text{mex} (\{a \oplus b', b' < 0\} \cup \{a' \oplus 0, a' < a\}) \\ &= \text{mex} \{0, 1, 2, 3, \dots, a'\} = a, \{a \oplus b', b' < 0\} = \phi. \end{aligned}$$

2- On montre que par récurrence sur a .

- Si $a = 0$ le résultat est vérifié $0 \oplus 0 = 0$, d'après la démonstration précédente.
- Si $a \neq 0$, alors $a \oplus a' \neq 0, \forall a' < a$, puisque $a' \oplus a' = 0, \forall a' \in \mathbb{N}$, si on suppose qu'il existe a' tel que $a \oplus a' = 0$, on a $a' \oplus a' = 0$, ce qui implique $a \oplus a' = a' \oplus a' \Rightarrow a = a'$,

$$\begin{aligned} a \oplus a &= \text{mex} \{a \oplus a', a' \oplus a\}, \text{ donc } 0 \notin \{a \oplus a', a' \oplus a\}, \\ &= \min(\mathbb{N} / \{a \oplus a', a' \oplus a\}) \\ &= 0. \end{aligned}$$

Exemple 2.1.9

$$1 \oplus 3 = \text{mex} \{1 \oplus 3', 1' \oplus 3\} \text{ avec } 3' \in \{0, 1, 2\} \text{ et } 1' \in \{0\}$$

$$\{1 \oplus 3'\} = \{1 \oplus 0, 1 \oplus 1, 1 \oplus 2\}, 1 \oplus 0 = 1, 1 \oplus 1 = 0$$

$$1 \oplus 2 = \text{mex} \{1 \oplus 2', 1' \oplus 2\}$$

$$\{1 \oplus 2'\} = \{1 \oplus 0, 1 \oplus 1\} = \{1, 0\}$$

$$\{1' \oplus 2\} = \{0 \oplus 2\} = \{2\}$$

$$1 \oplus 2 = \text{mex} \{0, 1, 2\} = 3$$

$$\{1 \oplus 3'\} = \{1, 0, 3\}$$

$$\{1' \oplus 3\} = \{0 \oplus 3\} = \{3\}$$

$$1 \oplus 3 = \text{mex} \{0, 1, 3\} = 2.$$

Proposition 2.1.10 Soient $\alpha_1 > \alpha_2 > \alpha_3 > \dots > \alpha_n$ des entiers naturels, alors la somme usuelle $2^{\alpha_1} + 2^{\alpha_2} + 2^{\alpha_3} + \dots + 2^{\alpha_n}$ des puissances de 2 correspondantes coïncide avec la somme de Nim $2^{\alpha_1} \oplus 2^{\alpha_2} \oplus 2^{\alpha_3} \oplus \dots \oplus 2^{\alpha_n}$.

Preuve Voir [12].

Proposition 2.1.11 Pour tous $a, b, c \in \mathbb{N}$, si $a \oplus b = a \oplus b'$, alors $b = b'$.

Preuve Si ce n'est pas le cas, supposons sans perte de généralité que $b' < b$. Alors $a \oplus b$ est le mex d'un ensemble contenant $b \oplus b'$, donc il ne peut pas lui être égal, d'où une contradiction.

Propriété 2.1.12

1- Si a est pair, alors $a \oplus 1 = a + 1$.

2- Si a est impair, alors $a \oplus 1 = a - 1$.

Preuve On montre par récurrence sur a

On a $0 \oplus 1 = 1$ et $1 \oplus 1 = 0$. On peut aussi facilement vérifier que $2 \oplus 1 = 3$ et $3 \oplus 1 = 2$.

Supposons que la propriété est vraie pour les a' , c'est-à-dire $a' \oplus 1 = a' + 1$.

1- Si a est pair : On a $a \oplus 1 = \text{mex} \{a \oplus 0, a' \oplus 1\}, \forall a, a' \in \mathbb{N}, a' < a$ donc :

$$\{a' \oplus 1\} = \{a' + 1\} = \{1, 0, 3, 2, \dots, a - 3, a - 1, a - 2\} = \{0, 1, \dots, a - 1\},$$

puisque $a - 1$ est impair, on a $a \oplus 1 = \text{mex} \{a, 0, 1, \dots, a - 1\} = a + 1$.

2- Si a est impair : On a $a \oplus 1 = \text{mex} \{a \oplus 0, a' \oplus 1\}, \forall a, a' \in \mathbb{N}, a' < a$ donc :

$$\{a' \oplus 1\} = \{a' + 1\} = \{1, 0, 3, 2, \dots, a - 2, a - 3, a\} = \{0, 1, \dots, a - 3, a - 2, a\},$$

alors $a \oplus 1 = \text{mex} \{0, 1, \dots, a - 3, a - 2, a\} = a - 1$.

Propriété 2.1.13 Soient $a, b \in \mathbb{N}$, on a :

$$a \oplus b = 0 \Leftrightarrow a = b.$$

Preuve On a $a \oplus b = \text{mex} \{a \oplus b', a' \oplus b | a' < a, b' < b\} = 0 \Leftrightarrow 0 \notin \{a \oplus b', a' \oplus b\}$, pour tous a, a', b, b' des entiers de $\mathbb{N}$, alors $a \oplus b' \neq 0, a' \oplus b \neq 0$. Comme $a \oplus a = 0, \forall a \in \mathbb{N}$, on a donc :

$$\left\{ \begin{array}{l} a \neq b' \Rightarrow a \leq b \text{ ou } b \leq a \\ \text{et} \\ b \neq a' \Rightarrow b \leq a \text{ ou } a \leq b \end{array} \right. . \text{ Ce qui implique } b \leq a \text{ et } a \leq b \text{ donc } a = b.$$

Propriété 2.1.14 Soient a, b et n sont des entiers naturels et $b = 2^n$

$$\forall a < b, a \oplus 2^n = a + 2^n.$$

Preuve On montre par récurrence sur a

- Pour $a = 0$ et $a = 1$, on a $0 \oplus 2^n = 2^n$ et $1 \oplus 2^n = 1 + 2^n$, d'après la propriété 2.1.8 et la propriété 2.1.12.
- Supposons que $a' \oplus 2^n = a' + 2^n, \forall a' \in \mathbb{N}, \forall a' < a, \forall (2^n)' < (2^n)$ et nous prouvons la propriété pour $a < (2^n)$. On a :

$$\begin{aligned} a \oplus 2^n &= \text{mex} \{a \oplus (2^n)', a' \oplus 2^n\} = \text{mex} \{a \oplus (2^n)', a' + 2^n\}, \\ \{a' + 2^n\} &= \{2^n, 1 + 2^n, 2 + 2^n, \dots, (a - 1) + 2^n\}, \\ \{a \oplus (2^n)'\} &= \{a \oplus 0, a \oplus 1, a \oplus 2, \dots, a \oplus (2^n - 1)\}. \end{aligned}$$

$$\text{Donc } a \oplus 2^n = \text{mex} \{a \oplus 0, a \oplus 1, \dots, a \oplus (2^n - 1), 2^n, 1 + 2^n, \dots, (a - 1) + 2^n\} = a + 2^n.$$

Propriété 2.1.15 Soient $m, n \in \mathbb{N}$, on a :

$$(2^m \oplus 2^n = 2^m + 2^n) \Leftrightarrow (m \neq n) \text{ et } (2^m \oplus 2^n = 0) \Leftrightarrow (m = n).$$

Preuve

1- Soient $m, n \in \mathbb{N} : (2^m \oplus 2^n = 2^m + 2^n) \Leftrightarrow (m \neq n)$.

$\Leftarrow$) Si $m \neq n$, on suppose que $m < n$, c'est-à-dire $2^m < 2^n$, on a $2^m \oplus 2^n = 2^m + 2^n$, en utilisant la propriété 2.1.14.

$\Rightarrow$) On suppose que $2^m \oplus 2^n = 2^m + 2^n$ et $m = n$, donc $2^m + 2^n = 0$ (contradiction).

2- Soient $m, n \in \mathbb{N} : (2^m \oplus 2^n = 0) \Leftrightarrow (m = n)$.

$\Leftarrow$) Si $m = n$, on a $2^m \oplus 2^n = 0$, en utilisant la propriété 2.1.8.

$\Rightarrow$) Si $2^m \oplus 2^n = 0 \Rightarrow 2^m = 2^n \Rightarrow m = n$, en utilisant la propriété 2.1.8.

Propriété 2.1.16 L'addition de Nim est commutative.

Preuve On montre par récurrence double sur a et b , $\forall a, b \in \mathbb{N}$.

Pour $a = 0 : 0 \oplus b = b \oplus 0 = b$ et pour $b = 0 : a \oplus 0 = 0 \oplus a = a$.

Supposons que $\forall a' < a, \forall a'' \leq a : a'' \oplus a' = a' \oplus a''$.

Supposons que $\forall b' < b, \forall b'' \leq b : b'' \oplus b' = b' \oplus b''$.

Supposons que $a > b$. On a alors :

$$\begin{aligned} a \oplus b &= \text{mex} \{a \oplus b', b' \oplus a\} \\ &= \text{mex} \{b' \oplus a, a \oplus b'\} \\ &= b \oplus a. \end{aligned}$$

Propriété 2.1.17 L'addition de Nim est associative.

Preuve On suppose qu'il existe $\xi \in \mathbb{N} : \xi < (\alpha_1 \oplus \alpha_2) \oplus \alpha_3$ et on montre que

$\xi \neq \alpha_1 \oplus (\alpha_2 \oplus \alpha_3)$. Soit $\xi = \gamma \oplus \alpha_3$, avec $\gamma < (\alpha_1 \oplus \alpha_2)$ qui peut lui-même s'écrire :

$$\left\{ \begin{array}{l} \gamma = \beta_1 \oplus \alpha_2, \beta_1 < \alpha_1 \\ \text{ou bien} \\ \gamma = \alpha_1 \oplus \beta_2, \beta_2 < \alpha_2 \end{array} \right.$$

Et comme $\xi < (\alpha_1 \oplus \alpha_2) \oplus \alpha_3$ ce qui implique $\xi = (\alpha_1 \oplus \alpha_2) \oplus \alpha'_3, \alpha'_3 < \alpha_3$, et on a $\xi = \gamma \oplus \alpha_3$, donc $\xi = (\beta_1 \oplus \alpha_2) \oplus \alpha_3 = (\alpha_1 \oplus \beta_2) \oplus \alpha_3$ et d'après proposition ceci est différent $\alpha_1 \oplus (\alpha_2 \oplus \alpha_3)$ donc $\xi \neq \alpha_1 \oplus (\alpha_2 \oplus \alpha_3)$.

Propriété 2.1.18 Pour tout $m, n \in \mathbb{N}$ et $n, m < 2^p$ on a :

$$n \oplus (2^p \oplus m) = n \oplus (2^p + m) = (n \oplus m) + 2^p.$$

Preuve D'après la propriété 2.1.14, on a : $n \oplus (2^p \oplus m) = n \oplus (2^p + m)$, $\forall n, m < 2^p$, et comme $n \oplus (2^p \oplus m) = n \oplus (m \oplus 2^p)$, $\forall (m, n) \in \mathbb{N}^2$ ($\oplus$ est commutative) et $n \oplus (m \oplus 2^p) = (n \oplus m) \oplus 2^p$ ($\oplus$ est associative) alors :

$$n \oplus (2^p \oplus m) = (n \oplus m) \oplus 2^p = (n \oplus m) + 2^p \text{ car } (n \oplus m) < 2^p.$$

Propriété.2.1.19 Pour tous $m, n \in \mathbb{N}$ on a :

$$a \oplus b \leq a + b.$$

Preuve On a toujours $\text{mex} X \leq \text{card}(X)$ et comme on a évidemment $\text{card}(\{a \oplus b'\}) \leq b$, $\text{card}(\{a' \oplus b\}) \leq a$ et $\text{card}(\{a \oplus b', a' \oplus b\}) \leq \text{card}(\{a \oplus b'\}) + \text{card}(\{a' \oplus b\})$ donc :

$$\begin{aligned} a \oplus b &= \text{mex}(\{a \oplus b', a' \oplus b\}) \leq \text{card}(\{a \oplus b', a' \oplus b\}) \\ &\leq \text{card}(\{a \oplus b'\}) + \text{card}(\{a' \oplus b\}) \leq a + b. \end{aligned}$$

Donc :

$$a \oplus b \leq a + b.$$

Table de opération $\oplus$

Pour comprendre cette définition, le mieux est de calculer quelques valeurs. Voici le tableau des $n_1 \oplus n_2$ pour $n_1 < 16$ et $n_2 < 16$:

$\oplus$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

2.2 La multiplication de Nim et quelques propriétés

Définition 2.2.1 Pour tous $a, b \in \mathbb{N}$, $a \otimes b$ est le plus petit entier naturel qui n'est pas de la forme $(a' \otimes b) \oplus (a \otimes b') \oplus (a' \otimes b')$ pour $a' < a$ et $b' < b$

Symboliquement,

$$a \otimes b = \text{mex} \{ (a' \otimes b) \oplus (a \otimes b') \oplus (a' \otimes b') : 0 \leq a' < a, 0 \leq b' < b \}.$$

Propriétés 2.2.2

1- $\forall a \in \mathbb{N} : 0 \otimes a = 0.$

2- $\forall a \in \mathbb{N} : 1 \otimes a = a.$

Preuve

1- Aucun nombre ne peut être de la forme $b' \otimes a \oplus 0 \otimes a' \oplus b' \otimes a'$ avec $b' < 0$, donc l'ensemble des nombres de cette forme est vide, et son *mex* est par conséquent 0.

2- On raisonne par récurrence sur a .

- On a pour $a = 0, 1 \otimes 0 = 0$ (d'après 1)
- Supposons que la propriété est vraie pour tout $a' \in \mathbb{N}$, i.e, $1 \otimes a' = a', \forall a' < a$ et nous prouvons sa vérité pour $a \in \mathbb{N}$, donc :

$$\begin{aligned} 1 \otimes a &= \text{mex} \{1' \otimes a \oplus 1 \otimes a' \oplus 1' \otimes a'\} \\ &= \text{mex} \{0 \otimes a \oplus 1 \otimes a' \oplus 0 \otimes a' | a' < a\} \\ &= \text{mex} \{a' | a' < a\}, \{1'\} = \{0\}. \end{aligned}$$

Donc le *mex* de l'ensemble des nombres de cette forme est a .

Exemple 2.2.3 Pour tous $a', b' \in \mathbb{N}$ on a :

$2 \otimes 2 = \text{mex} \{2 \otimes 2' \oplus 2' \otimes 2 \oplus 2' \otimes 2'\}$ avec $2' \in \{0, 1\}$, donc $(0, 0)(0, 1)(1, 0)(1, 1)$ sont des solutions.

Pour $(a', b') = (0, 0)$, avec $2 \otimes 0 = 0, 0 \otimes 2 = 0$ on a :

$$\{2 \otimes 2' \oplus 2' \otimes 2 \oplus 2' \otimes 2'\} = \{2 \otimes 0 \oplus 0 \otimes 2 \oplus 0 \otimes 0\} = \{0 \oplus 0 \oplus 0\} = \{0\}.$$

Pour $(a', b') = (0, 1)$ ou bien $(a', b') = (1, 0)$, avec $1 \otimes 2 = 2, 0 \otimes 1 = 0$ on a :

$$\{2 \otimes 2' \oplus 2' \otimes 2 \oplus 2' \otimes 2'\} = \{2 \otimes 0 \oplus 1 \otimes 2 \oplus 0 \otimes 1\} = \{0 \oplus 2 \oplus 0\} = \{2\}.$$

Pour $(a', b') = (1, 1)$, avec $2 \oplus 2 = 0, 0 \oplus 1 = 1, 2 \otimes 1 = 2$ on a :

$$\{2 \otimes 2' \oplus 2' \otimes 2 \oplus 2' \otimes 2'\} = \{2 \otimes 1 \oplus 1 \otimes 2 \oplus 1 \otimes 1\} = \{2 \oplus 2 \oplus 1\} = \{1\}.$$

Donc $2 \otimes 2 = \text{mex} \{0, 1, 2\} = \min(\mathbb{N} - \{0, 1, 2\}) = 3$.

Propriété 2.2.4 Pour tous $a, b \in \mathbb{N}$ on a :

$$a \otimes b = a \Rightarrow b = 1.$$

Preuve $\forall a, a', b, b' \in \mathbb{N}, a \otimes b = a \Leftrightarrow \{0, 1, \dots, a-1\} \in \{a \otimes b' \oplus a' \otimes b \oplus a' \otimes b'\}$ et $a \notin \{a \otimes b' \oplus a' \otimes b \oplus a' \otimes b'\}$.

Comme $a \otimes 1 = \text{mex} \{a \otimes 1' \oplus a' \otimes 1 \oplus a' \otimes 1' \mid a' < a, 1' < 1\} = a$, la seconde condition ci-dessus implique que $1 \notin \{b'\}$ et donc que $b = 0$ ou bien $b = 1$. Le seul choix possible pour vérifier la première condition est alors $b = 1$.

Propriété 2.2.5 La multiplication de Nim est commutative.

Preuve On raisonne par récurrence double sur a et b . On a : $0 \otimes 1 = 1 \otimes 0 = 0$.

Supposons que : $\forall a' < a, \forall a'' \leq a, a'' \otimes a' = a' \otimes a''$.

Supposons que : $\forall b' < b, \forall b'' \leq b, b'' \otimes b' = b' \otimes b''$.

Supposons que $a > b$.

On a alors $\forall a, b \in \mathbb{N}$:

$$\begin{aligned} a \otimes b &= \text{mex} \{a' \otimes b \oplus a \otimes b' \oplus a' \otimes b'\} \\ &= \text{mex} \{b \otimes a' \oplus b' \otimes a \oplus b' \otimes a'\} \\ &= b \otimes a. \end{aligned}$$

Propriété 2.2.6 La multiplication de Nim est distributive sur $\oplus$.

Preuve On montre par récurrence sur les triplets $(a, b, c) \in \mathbb{N}^3$.

Supposons que : $\forall (a', b', c') < (a, b, c) : a' \otimes (b' \oplus c') = a' \otimes b' \oplus a' \otimes c'$, et on note $d = b \oplus c$.

On a alors :

$$\begin{aligned} a \otimes (b \oplus c) &= \text{mex} \{a' \otimes (b \oplus c) \oplus d' \otimes a \oplus a' \otimes d'\} \\ &= \text{mex} \{a' \otimes b \oplus a' \otimes c \oplus d' \otimes a \oplus a' \otimes d'\}. \end{aligned}$$

Comme $d = b \oplus c = \text{mex} \{b \oplus c', b' \oplus c\}$, alors $d' \in \{b \oplus c', b' \oplus c\}, \forall d' < d$. Donc

$$\{a \otimes d'\} = \begin{cases} a \otimes (b \oplus c') = a \otimes b \oplus a \otimes c' \\ \text{ou bien} \\ a \otimes (b' \oplus c) = a \otimes b' \oplus a \otimes c \end{cases}, \{a' \otimes d'\} = \begin{cases} a' \otimes (b \oplus c') = a' \otimes b \oplus a' \otimes c' \\ \text{ou bien} \\ a' \otimes (b' \oplus c) = a' \otimes b' \oplus a' \otimes c \end{cases}$$

Donc :

$$a \otimes (b \oplus c) = \text{mex} \{a' \otimes b \oplus a' \otimes c \oplus (a \otimes b \oplus a \otimes c') \oplus (a' \otimes b \oplus a' \otimes c')\}.$$

Ou bien

$$a \otimes (b \oplus c) = \text{mex} \{a' \otimes b \oplus a' \otimes c \oplus (a \otimes b \oplus a \otimes c') \oplus (a' \otimes b' \oplus a' \otimes c)\}.$$

Ou bien

$$a \otimes (b \oplus c) = \text{mex} \{a' \otimes b \oplus a' \otimes c \oplus (a \otimes b' \oplus a \otimes c) \oplus (a' \otimes b \oplus a' \otimes c')\}.$$

Ou bien

$$a \otimes (b \oplus c) = \text{mex} \{a' \otimes b \oplus a' \otimes c \oplus (a \otimes b' \oplus a \otimes c) \oplus (a' \otimes b' \oplus a' \otimes c)\}.$$

Et on a aussi

$$k = a \otimes b = \text{mex} \{a' \otimes b \oplus a \otimes b' \oplus a' \otimes b'\} \Rightarrow k' \in \{a' \otimes b \oplus a \otimes b' \oplus a' \otimes b'\},$$

$$l = a \otimes c = \text{mex} \{a' \otimes c \oplus a \otimes c' \oplus a' \otimes c'\} \Rightarrow l' \in \{a' \otimes c \oplus a \otimes c' \oplus a' \otimes c'\},$$

$$k \oplus l = a \otimes b \oplus a \otimes c = \text{mex} \{k' \oplus l, k \oplus l'\}.$$

Donc :

$$a \otimes b \oplus a \otimes c = \text{mex} \{a' \otimes b \oplus a \otimes b' \oplus a' \otimes b' \oplus a \otimes c, a \otimes b \oplus a' \otimes c \oplus a \otimes c' \oplus a' \otimes c'\}.$$

Propriété 2.2.7 La multiplication de Nim est associative.

Preuve On montre que par récurrence sur les triplets $(a, b, c) \in \mathbb{N}^3$.

Supposons que : $\forall (a', b', c') < (a, b, c) : a' \otimes (b' \otimes c') = a' \otimes b' \otimes c'$. On note $d = b \otimes c$.

On a alors : $a \otimes (b \otimes c) = \text{mex} \{a \otimes d' \oplus a' \otimes (b \otimes c) \oplus a' \otimes d'\}.$

Comme $d = b \otimes c = \text{mex} \{b' \otimes c \oplus b \otimes c' \oplus b' \otimes c'\} \Rightarrow d' \in \{b' \otimes c \oplus b \otimes c' \oplus b' \otimes c'\},$

$\forall d' < d$. Donc :

$$\begin{aligned} \{a \otimes d'\} &= \{a \otimes (b' \otimes c \oplus b \otimes c' \oplus b' \otimes c')\} \\ &= \{a \otimes (b' \otimes c) \oplus a \otimes (b \otimes c') \oplus a \otimes (b' \otimes c')\} \\ &= \{(a \otimes b') \otimes c \oplus (a \otimes b) \otimes c' \oplus (a \otimes b') \otimes c'\}. \end{aligned}$$

$$\begin{aligned}
\{a' \otimes d'\} &= \{a' \otimes (b' \otimes c \oplus b \otimes c' \oplus b' \otimes c')\} \\
&= \{a' \otimes (b' \otimes c) \oplus a' \otimes (b \otimes c') \oplus a' \otimes (b' \otimes c')\} \\
&= \{(a' \otimes b') \otimes c \oplus (a' \otimes b) \otimes c' \oplus (a' \otimes b') \otimes c'\}.
\end{aligned}$$

Donc :

$$a \otimes (b \otimes c) = mex \left\{ \begin{array}{l} (a \otimes b') \otimes c \oplus (a \otimes b) \otimes c' \oplus (a \otimes b') \otimes c' \oplus a' \otimes (b \otimes c) \\ \oplus (a' \otimes b') \otimes c \oplus (a' \otimes b) \otimes c' \oplus (a' \otimes b') \otimes c' \end{array} \right\} \dots\dots(i)$$

Et on a aussi : $(a \otimes b) \otimes c = mex \{m' \otimes c \oplus (a \otimes b) \otimes c' \oplus m' \otimes c'\}.$

Comme $m = (a \otimes b) = mex \{a' \otimes b \oplus a \otimes b' \oplus a' \otimes b'\} \Rightarrow m' \in \{a' \otimes b \oplus a \otimes b' \oplus a' \otimes b'\},$

$\forall m' < m.$ Donc :

$$\begin{aligned}
\{m' \otimes c\} &= \{(a' \otimes b \oplus a \otimes b' \oplus a' \otimes b') \otimes c\} \\
&= \{(a' \otimes b) \otimes c \oplus (a \otimes b') \otimes c \oplus (a' \otimes b') \otimes c\}.
\end{aligned}$$

$$\begin{aligned}
\{m' \otimes c'\} &= \{(a' \otimes b \oplus a \otimes b' \oplus a' \otimes b') \otimes c'\} \\
&= \{(a' \otimes b) \otimes c' \oplus (a \otimes b') \otimes c' \oplus (a' \otimes b') \otimes c'\}.
\end{aligned}$$

Donc :

$$(a \otimes b) \otimes c = mex \left\{ \begin{array}{l} (a' \otimes b) \otimes c \oplus (a \otimes b') \otimes c \oplus (a' \otimes b') \otimes c \oplus (a \otimes b) \otimes c' \\ \oplus (a' \otimes b) \otimes c' \oplus (a \otimes b') \otimes c' \oplus (a' \otimes b') \otimes c' \end{array} \right\} \dots\dots(ii)$$

De (i) et (ii) La multiplication de Nim est associative.

Table de opération $\otimes$

Pour comprendre cette définition, le mieux est de calculer quelques valeurs. Voici le tableau des $n_1 \otimes n_2$ pour $n_1 < 16$ et $n_2 < 16$:

$\otimes$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	3	1	8	10	11	9	12	14	15	13	4	6	7	5
3	0	3	1	2	12	15	13	14	4	7	5	6	8	11	9	10
4	0	4	8	12	6	2	14	10	11	15	3	7	13	9	5	1
5	0	5	10	15	2	7	8	13	3	6	9	12	1	4	11	14
6	0	6	11	13	14	8	5	3	7	1	12	10	9	15	2	4
7	0	7	9	14	10	13	3	4	15	8	6	1	5	2	12	11
8	0	8	12	4	11	3	7	15	13	5	1	9	6	14	10	2
9	0	9	14	7	15	6	1	8	5	12	11	2	10	3	4	13
10	0	10	15	5	3	9	12	6	1	11	14	4	2	8	13	7
11	0	11	13	6	7	12	10	1	9	2	4	15	14	5	3	8
12	0	12	4	8	13	1	9	5	6	10	2	14	11	7	15	3
13	0	13	6	11	9	4	15	2	14	3	8	5	7	10	1	12
14	0	14	7	9	5	11	2	12	10	4	13	3	15	1	8	6
15	0	15	5	10	1	14	4	11	2	13	7	8	3	12	6	9

2.3 Les puissances de Fermat avec les opérations de Nim

Définition 2.3.1 On nomme puissance de Fermat un nombre s'écrivant sous la forme 2^{2^n} avec $n \in \mathbb{N}$.

Proposition 2.3.2 Le produit de Nim de deux puissances de Fermat distinctes est leur produit usuel, et le carré de Nim d'une puissance de Fermat est égal à cette même puissance de Fermat multipliée par $\frac{3}{2}$. Les produits d'autres nombres peuvent être obtenus en utilisant des propriétés d'associativité et de distributivité sur l'addition de Nim.

Exemple 2.3.3 Les nombres $2 = 2^{2^0}$, $4 = 2^{2^1}$, $16 = 2^{2^2}$, $256 = 2^{2^3}$ et $66536 = 2^{2^4}$ sont des puissances de Fermat.

Propriétés 2.3.4

1- $\forall (u, v) \in \mathbb{N}^2 : 2^{2^u} \otimes 2^{2^v} = 2^{2^u + 2^v}$ si $u \neq v$ (c'est aussi $2^{2^u} \times 2^{2^v}$).

2- $\forall n \in \mathbb{N}^2 : 2^{2^n} \otimes 2^{2^n} = \frac{3}{2} \times 2^{2^n}$.

Exemple 2.3.5 On a $2 = 2^{2^0}$ est une puissance de Fermat, donc le carré de Nim d'une puissance de Fermat est :

$$2 \otimes 2 = 2^{2^0} \otimes 2^{2^0} = \frac{3}{2} \times 2^{2^0} = 3.$$

Exemple 2.3.6

$$10 \otimes 7$$

$$10 = 2^3 \oplus 2^1 = 2^{2+1} \oplus 2^1 = 2^2 \otimes 2 \oplus 2 = 2^{2^1} \otimes 2^{2^0} \oplus 2^{2^0}$$

$$7 = 2^2 \oplus 2 \oplus 1 = 2^{2^1} \oplus 2^{2^0} \oplus 1$$

$$10 \otimes 7 = (4 \otimes 2 \oplus 2) \otimes (4 \oplus 2 \oplus 1)$$

$$= 4 \otimes 4 \otimes 2 \oplus 4 \otimes 2 \otimes 2 \oplus 4 \otimes 2 \oplus 2 \otimes 4 \oplus 2 \otimes 2 \oplus 2$$

$$= 4 \otimes 4 \otimes 2 \oplus 4 \otimes 2 \otimes 2 \oplus 2 \otimes 2 \oplus 2$$

$$= 6 \otimes 2 \oplus 4 \otimes 3 \oplus 3 \oplus 2$$

$$6 = 4 \oplus 2 \implies 6 \otimes 2 = (4 \oplus 2) \otimes 2 = 8 \oplus 3 = 11$$

$$3 = 2 \oplus 1 \implies 3 \otimes 4 = (2 \oplus 1) \otimes 4 = 8 \oplus 4 = 12$$

$$10 \otimes 7 = 11 \oplus 12 \oplus 1 = 8 \oplus 8 \oplus 3 \oplus 4 \oplus 1 = 6.$$

Remarque 2.3.7 Si $i \in \mathbb{N}$ et $i < 2^{2^n}$, alors $i \otimes 2^{2^n} = i \times 2^{2^n}$.

Exemples 2.3.8

1- $4 \otimes 3 = 4 \times 3 = 12$.

2- $16 \otimes 13 = 16 \times 13 = 208$.

Chapitre 3

Structures algébriques avec les opérations de Nim

Introduction

Dans ce chapitre, en utilisant les opérations de Nim, nous allons faire une étude sur les structures algébriques (groupes, anneaux, corps). D'autre part on donne quelques notions sur les codes binaires.

Contenu

- 3.1. Groupes.
- 3.2. Anneaux.
- 3.3. Corps.
- 3.4. Les codes binaires.

3.1 Groupes

Théorème 3.1.1 Pour tout $n \in \mathbb{N}$, $2^n = \{i \in \mathbb{N}, i < 2^n\}$, $(2^n, \oplus)$ est un groupe commutatif.

Preuve On raisonne par récurrence sur les puissances de 2, pour plus de détaille voir [5].

Exemples 3.1.2 On a pour tout $n \in \mathbb{N}$, $2^n = \{i \in \mathbb{N}, i < 2^n\}$

- 1- Si $n = 1$, l'ensemble $\{0, 1\}$ muni de l'opération $\oplus$ définie dans le tableau ci-après est un groupe abélien

$\oplus$	0	1
0	0	1
1	1	0

- 2- Si $n = 2$, l'ensemble $\{0, 1, 2, 3\}$ muni de l'opération $\oplus$ définie dans le tableau ci-après est un groupe abélien

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

- 3- Si $n = 3$, l'ensemble $\{0, 1, 2, 3, 4, 5, 6, 7\}$ muni de l'opération $\oplus$ définie dans le tableau ci-après est un groupe abélien

$\oplus$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

Théorème 3.1.3 Pour tout n un entier naturel, $(2^{2^n}, \otimes)$ est un groupe abélien.

Preuve Voir [5].

Exemples 3.1.4 On a pour tout $n \in \mathbb{N}$, $2^{2^n} = \{i \in \mathbb{N}, i < 2^{2^n}\}$

- 1- Si $n = 1$, $2^{2^1} = \{0, 1, 2, 3\}$, l'ensemble $\{0, 1, 2, 3\}$ muni de l'opération $\otimes$ définie dans le tableau ci-après est un groupe abélien

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

- 2- Si $n = 2$, $2^{2^2} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$, $(2^{2^2}, \otimes)$ est un groupe abélien.

Théorème 3.1.5 $(\mathbb{N}, \oplus)$ est un groupe abélien.

Preuve Soient $x, y, z \in \mathbb{N}$, on a :

- La loi interne $\oplus$ est associative : $\forall x, y, z \in \mathbb{N}, x \oplus (y \oplus z) = (x \oplus y) \oplus z$.
- La loi interne $\oplus$ possède un élément neutre noté 0 : $\forall x \in \mathbb{N}, 0 \oplus x = x$.
- Tout élément x de $\mathbb{N}$ possède un symétrique unique $x' = x$: $\forall x \in \mathbb{N}, x \oplus x = 0$.
- $\forall x, y \in \mathbb{N} : x \oplus y = y \oplus x$, la loi $\oplus$ est commutative.

Donc $(\mathbb{N}, \oplus)$ est un groupe abélien.

Théorème 3.1.6 $(\mathbb{N}, \otimes)$ est un groupe abélien

Preuve Soient $x, y, z \in \mathbb{N}$, on a :

- La loi interne $\otimes$ est associative : $\forall x, y, z \in \mathbb{N}, x \otimes (y \otimes z) = (x \otimes y) \otimes z$.
- La loi interne $\otimes$ possède un élément neutre noté 1 : $\forall x \in \mathbb{N}, 1 \otimes x = x$.
- Tout élément x de $\mathbb{N}$ possède un symétrique unique $x' = x$: $\forall x \in \mathbb{N}, x \otimes x = 1$.
- $\forall x, y \in \mathbb{N} : x \otimes y = y \otimes x$, la loi $\otimes$ est commutative.

Donc $(\mathbb{N}, \otimes)$ est un groupe abélien.

3.2 Anneaux

Théorème 3.2.1 $(\mathbb{N}, \oplus, \otimes)$ est un anneau commutatif unitaire.

Preuve Soient $x, y, z \in \mathbb{N}$ on a :

- 1- $(\mathbb{N}, \oplus)$ est un groupe commutatif.
- 2- La loi interne $\otimes$ est associative.
- 3- La loi interne $\otimes$ possède un élément neutre.
- 4- La loi interne $\otimes$ est distributive par rapport à l'addition de Nim :

$$\forall x, y, z \in A, x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \text{ et } (y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x).$$

- 5- La loi interne $\otimes$ est commutative.

Donc $(\mathbb{N}, \oplus, \otimes)$ est un anneau commutatif unitaire.

Théorème 3.2.2 $(\mathbb{N}, \oplus, \otimes)$ est quadratiquement clôt. C'est-à-dire tout polynôme de degré 2 à coefficients dans $\mathbb{N}$ a une racine dans $\mathbb{N}$.

Preuve Voir [6].

3.3 Corps

Théorème 3.3.1 $(\mathbb{N}, \oplus, \otimes)$ est un corps commutatif.

Preuve $K = (\mathbb{N}, \oplus, \otimes)$ est un corps car :

- 1- $K = (\mathbb{N}, \oplus, \otimes)$ est un anneau.
- 2- Chaque élément non nul de $\mathbb{N}$ possède un inverse pour l'opération " $\otimes$ ".
- 3- la loi interne $\otimes$ est commutative.

Théorème 3.3.2. $\forall n \in \mathbb{N}, (2^{2^n}, \oplus, \otimes)$ est un corps commutatif.

Proposition 3.3.3 On obtient un corps infini de caractéristique 2. Ce corps est la clôture quadratique de F_2 .

Proposition 3.3.4 Les sous corps finis de $(\mathbb{N}, \oplus, \otimes)$ sont les $F_{2^{2^n}}$.

Exemples 3.3.5

- 1- $(\{0, 1\}, \oplus, \otimes)$ est un corps commutatif, la table d'addition $\oplus$ et la multiplication $\otimes$ de $(\{0, 1\}, \oplus, \otimes)$ sont :

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

- 2- $(\{0, 1, 2, 3\}, \oplus, \otimes)$ est un corps commutatif, la table d'addition $\oplus$ et la multiplication $\otimes$ de $(\{0, 1, 2, 3\}, \oplus, \otimes)$ sont :

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

3.4 Les codes binaires

Définition 3.4.1 (Codes, mots de code)

Soit $A = \{a_1, a_2, \dots, a_q\}$ un ensemble fini que nous appellerons un alphabet de code et soit A^n l'ensemble de toutes les chaînes de longueur n sur A . Nous dirons que chaque sous-ensemble $C \subset A^n$ s'appelle un code. Chacune des chaînes c de C est appelée mot du code. Et on note $|C| = M$ la cardinalité de code C . La dimension n de A^n est appelée la longueur du code. Un code de longueur n contenant M mots sera appelé un (n, M) -code.

Définition 3.4.2 (Codes, mots de code)

Soit S et T deux ensembles finis. Un code C est une fonction injective $C : S \rightarrow T^*$. Pour chaque symbole $s \in S$, la chaîne $C(s) \in T^*$ est appelée le mot de code pour s . L'ensemble de tous les mots de code est :

$$C = \{C(s) | s \in S\}.$$

Est également appelé le code. Si $|T| = 2$ le code est dit binaire, $|T| = 3$ c'est ternaire, et en général Si $|T| = n$, c'est n-aire.

Définition 3.4.3 (Code de parité ou VRC : Vertical Redundancy Check)

Le code de parité consiste tout simplement ajouter un bit supplémentaire (appelé bit de parité) à un certain nombre de bits de données, et définit comme :

$$(x_1, x_2, \dots, x_n) \mapsto (x_1, \dots, x_n, x_{n+1}),$$

avec $x_{n+1} = \bigoplus_{i=1}^n x_i$.

Exemple 3.4.4 Il consiste à ajouter un bit supplémentaire à un certain nombre de bits de données tel que le nombre total de bits à 1 soit pair.

- Le nombre de bits de données à 1 est pair, le bit de parité est donc positionné à 0.

le bit de parité ↓ 0	1	1	0	0	1	1	0
----------------------------	---	---	---	---	---	---	---

- Le nombre de bits de données à 1 est impair, le bit de parité est donc positionné à 1.

le bit de parité ↓ 1	1	0	0	0	1	1	0
----------------------------	---	---	---	---	---	---	---

Définition 3.4.5 (Code de répétition)

Le code de répétition consiste tout simplement à répéter chaque bit du message un certain nombre de fois. C'est un code $[n, 1, n]$, de dimension 1, de longueur n et de distance n . Pour n impair, ce code est parfait et optimal lorsque l'on protège un seul bit de donnée, i.e,

$$(x_1) \mapsto \underbrace{(x_1, x_1, \dots, x_1)}_{n \text{ fois}}.$$

Exemple 3.4.6 Dans le code C chaque bit est répété 3 fois et le message source $s \in C$ suivant :

$$s = 0010110$$

Sera encodé en

$$t = 000000111000111111000.$$

Définition 3.4.7 (Code linéaire)

Un code linéaire de longueur n est un sous-espace vectoriel $C \subset F_2^n$. La lettre k désignera toujours la dimension de C avec 2^k est le nombre de mots du ce code.

Exemple 3.4.8 On pose $S = \{x, y, z\}, T = \{0, 1\}$ et on a :

$$c(x) = 0, c(y) = 10, c(z) = 11.$$

C'est un code binaire et l'ensemble des mots de code est $C = \{0, 10, 11\}$.

Définition 3.4.9 (Matrice de contrôle)

Soit C un code linéaire, une matrice de contrôle de C est la matrice d'un système d'équations linéaires homogènes indépendantes dont l'espaces des solutions est C . Autrement dit, une matrice de contrôle H est de taille $(n - k) \times n$ et de rang $n - k$, et $C = \{x \in F_2^n | H^t x = 0\}$.

Définition 3.4.10 (Code de Hamming)

Soit r un entier positive et soit H une matrice de m ligne et $2^m - 1$ colonnes non nulles distinctes. Alors le code ayant H comme matrice de contrôle est appelé un code de Hamming binaire et est noté $H_2(r)$.

Exemple 3.4.11 Le code de Hamming de longueur 7 est donné par la matrice de contrôle

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

la matrice H est de rang 3. Donc la dimension du code est 4.

Définition 3.4.12 (Distance de Hamming, le poids de Hamming)

La distance de Hamming entre de mots binaires $x = (x_1, x_2, x_3, \dots, x_n)$ et $y = (y_1, y_2, y_3, \dots, y_n)$ est définie par :

$$d(x, y) = |\{i | x_i \neq y_i\}|.$$

Le poids de Hamming de $x = (x_1, x_2, x_3, \dots, x_n)$ est le nombre de symboles différents de 0 que contient x . Et est noté $w(x)$:

$$w(x) = d(x, 0).$$

Il est immédiat de vérifier que :

$$d(x, y) = w(x - y).$$

Remarque 3.4.13 La distance de Hamming entre deux mots binaires x et y de taille n est le poids de $x \oplus y$.

$$d(x, y) = w(x \oplus y).$$

Exemple 3.4.14

$$\begin{aligned} d(111001111000, 101000111001) &= w(111001111000 \oplus 101000111001) \\ &= w(010001000001) \\ &= 3 \end{aligned}$$

Définition 3.4.15 (La distance minimale)

Soit $C \subset F_2^n$, la distance minimale de C noté d est définie par :

$$d(C) = \min_{x, y \in C, x \neq y} d(x, y).$$

Exemples 3.4.16 Soient $x = (0, 0, 1, 0, 1, 0, 1)$ et $y = (1, 0, 1, 0, 0, 1, 1)$.

1- La distance de Hamming entre de mots $x = (0010101)$ et $y = (1010011)$ est :

$$d(x, y) = |\{i | x_i \neq y_i\}| = 3.$$

2- Le poids de Hamming de $x = (0, 0, 1, 0, 1, 0, 1)$ est $w(x) = d(x, 0) = 3$.

3- la distance minimale de $C = \{0000, 0100, 1001, 1100\}$, avec C un code de longueur 4 est $d(C) = 1$.

Remarque 3.4.17 On regroupe les trois paramètre n, k et d d'un code linéaire C non nul, en disant que C est de type (n, k, d) . On a toujours $d + k \leq n + 1$.

Conclusion

Dans ce mémoire, on a fait une étude de deux opérations sur les entiers plutôt inhabituelles tels que l'addition et la multiplication de Nim qui permettent d'obtenir l'arithmétique de Nim et ainsi que certaines de leurs propriétés. D'autre part nous avons présenté les structures algébriques (groupes, anneaux, corps) avec les opérations de Nim et quelques exemples.

Bibliographie

- [1] N. Biggs, " Codes An introduction to Information communication and cryptography", Departement of Mathematics, London School of Economics, 2008.
- [2] D. Bruno, " Arithmétique des entiers", Université d'Eleuthéria-Polites, 2015.
- [3] L. Christine, " Axiomatique des nombres", Université Joseph Fourier, Grenoble, 2014.
- [4] M. Coste, A. Paugam, R. Quarez, " Codes correcteurs", 2002.
- [5] A. Daniel, " Jeu de Marienbard, Codage, Cryptographie et stéganographie élémentaires", Inria Sacaly-Île de France et École polytechnique, 2010.
- [6] M. David A, " Le jeu de Nim : Thème et variations", Télécom Paris Tech, 2017.
- [7] M. David A, " Théories des jeux (notes de cors)", MITRo 206, 2017.
- [8] P. Delhayé, " Arithmétique", MPSI Prytanée National Militaire, 2017.
- [9] P. Fabien, " Cours de Mathématiques", 2015.
- [10] C. Jean-françois, G. Christophe, " Mathématiques pour l'informatique", 2010.
- [11] A. Labourel, " Codes détecteurs correcteurs", Université de Provence, 2011.
- [12] B. Mayag, " Contrôle des erreurs", Université Paris Dauphine, 2012.
- [13] H. D. Oussama, " Arithmétique finie et réciprocity quadratique", 2017.
- [14] D. Piau, B. Ycart, " Arithmétique", 2013.

- [15] K. Pierre, " Arithmétique de Nim", 2008.
- [16] D. Raphaël, H. Rejeb, J. Stéphane, L. Eva, P. Jacques, S. Stéphane, " Cours arithmétique et groupes-licence première année, premier semestre", 2007.
- [17] P. Vincent, " Cours de spécialité mathématiques en T^{ale}S", 2010.