

110. Base de numération d'entiers. Applications.

Prérequis : division euclidienne dans \mathbb{N} .

Congruences dans $\mathbb{Z} / n\mathbb{Z}$

I Base de numération

1) Théorème : Soit $a > 1$ un nombre entier. Soit $p \in \mathbb{N}$.

Alors il existe un unique nombre entier n_0 et une suite d'entiers x_i tous inférieurs à a , tels

que $x_{n_0} \neq 0$ et :

$$p = \sum_{i=0}^{n_0} x_i \cdot a^i .$$

C'est la décomposition de l'entier p dans le système de numération à base a .

Notation :

$$p = \overline{x_{n_0} x_{n_0-1} \dots x_1 x_0}_a$$

Démonstration :

En général, les démonstrations fournissent un résultat quant à l'existence d'un objet mais ne révèlent en rien la façon pratique de l'obtenir.

Cette démonstration est intéressante puisqu'elle fournit un procédé d'obtention l'écriture en base a .

Existence :

- 1^{er} pas : on écrit la division euclidienne de p par a :

Il existe un unique couple $(q_0, r_0) \in \mathbb{N} \times \mathbb{N}$ tel que :

$$p = aq_0 + r_0 \text{ et } r_0 < a$$

Si $q_0 < a$ alors on pose $n_0 = 1, x_0 = r_0$ et $x_1 = q_0$.

- 2^e pas : Si $q_0 \geq a$, on renouvelle le procédé en écrivant la division euclidienne de q_0 par a :

Il existe un unique couple $(q_1, r_1) \in \mathbb{N} \times \mathbb{N}$ tel que :

$$q_0 = aq_1 + r_1 \text{ et } r_1 < a$$

....

La suite (q_0, q_1, \dots) ainsi obtenue est décroissante puisque $a > 1$.

Il existe donc un entier p_0 tel que $q_{p_0-1} \geq a$ et $q_{p_0} < a$.

On écrit la suite des divisions euclidiennes obtenues :

$$\begin{aligned}
 p &= aq_0 + r_0 \\
 q_0 &= aq_1 + r_1 \\
 q_1 &= aq_2 + r_2 \\
 &\dots \\
 q_{p_0-2} &= aq_{p_0-1} + r_{p_0-1} \\
 q_{p_0-1} &= aq_{p_0} + r_{p_0}
 \end{aligned}$$

On multiplie la deuxième égalité par a , la troisième par a^2 , ... et la dernière par a^{p_0} :

$$\begin{aligned}
 p &= aq_0 + r_0 \\
 aq_0 &= a^2q_1 + ar_1 \\
 a^2q_1 &= a^3q_2 + a^2r_2 \\
 &\dots \\
 a^{p_0-1}q_{p_0-2} &= a^{p_0}q_{p_0-1} + a^{p_0-1}r_{p_0-1} \\
 a^{p_0}q_{p_0-1} &= a^{p_0+1}q_{p_0} + a^{p_0}r_{p_0}
 \end{aligned}$$

On effectue la somme des égalités membre à membre :

$$p = r_0 + r_1a + r_2a^2 + \dots + r_{p_0}a^{p_0} + q_{p_0}a^{p_0+1}$$

où q_{p_0} et chaque r_i est strictement inférieur à a par définition.

Soit le résultat attendu, en posant

- $n_0 = p_0$ si $q_{p_0} = 0$, $x_i = r_i$ pour $i = 0..n_0$
- $n_0 = p_0 + 1$ si $q_{p_0} \neq 0$, $x_i = r_i$ pour $i = 0..n_0 - 1$ et $x_{n_0} = q_{p_0}$.

Donc
$$p = \sum_{i=0}^{n_0} x_i \cdot a^i$$

Unicité :

L'unicité provient de l'unicité de la division euclidienne, donc de la suite des entiers (q_i, r_i) .

Remarque : on utilise les chiffres usuels de 0 à $a - 1$ pour les écritures en base $a < 11$ et ensuite on utilise des lettres.

Exemple : les chiffres pour la numération à base 16 (hexadécimale) sont 0, 1, ..., 9, A, B, C, D, E, F.

Exemples :

- Montrer que $\overline{407}^{10} = \overline{1515}^6$, $\overline{255}^{10} = \overline{FF}^{16}$
- En informatique et électronique les écritures binaires (en base 2) et hexadécimales sont les plus souvent utilisées. Les informations sont traitées sous la forme d'octets (suites de huit « chiffres » binaires, qu'on exprime souvent à l'aide de deux « chiffres » hexadécimaux).

Par exemple, $\overline{123}^{10} = \overline{01111011}^2$. On sépare l'écriture binaire en

deux : $\overline{0111}^2 = \overline{7}^{16}$ et $\overline{1011}^2 = \overline{B}^{16}$: l'octet 123 s'écrira donc $7B$

2) Mise en œuvre de l'algorithme à l'aide de l'outil informatique :

Comme tous les algorithmes simples, la décomposition d'un entier en base a est très facile à mettre en œuvre à l'aide d'un tableau par exemple

	A	B	C	D	E	F
1	base :	2	entier :	123		puissance de a
2						
3	quotient		61	reste :	1	0
4			30		1	1
5			15		0	2
6			7		1	3
7			3		1	4
8			1		1	5
9			0		1	6
10			0		0	7
11						

3) Propriétés

Soit $a > 1$:

- $\overline{0}^{10} = \overline{0}^a$
- $\overline{1}^{10} = \overline{1}^a$
- $\overline{a}^{10} = \overline{1}^a$
- Quel que soit $n \in \mathbb{N}$, $\overline{a^n}^{10} = \underbrace{\overline{10\dots0}}_{n \text{ zéros}}^a$

Démonstration : évidente

II Applications

1) Critères de divisibilité en base a

Théorème : Soit $a > 1$ et $p = \sum_{i=0}^{n_0} x_i \cdot a^i$ l'écriture de p en base a .

i) Soit $k \geq 1$: p est divisible par $a^k \Leftrightarrow x_0 = x_1 = \dots x_{k-1} = 0$.

ii) p est divisible par $a - 1 \Leftrightarrow \sum_{i=0}^{n_0} x_i$ est divisible par $a - 1$.

iii) p est divisible par $a + 1 \Leftrightarrow \sum_{i=0}^{n_0} (-1)^i x_i$ est divisible par $a + 1$.

Démonstration :

i) p est divisible par a^k si et seulement si le reste de la division euclidienne de p par a^k est nul.

$$\Leftrightarrow 0 = \sum_{i=0}^{k-1} x_i \cdot a^i$$

$\Leftrightarrow x_0 = x_1 = \dots x_{k-1} = 0$ puisque c'est l'unique décomposition de 0 en base a .

ii) $p = \sum_{i=0}^{n_0} x_i \cdot a^i$ donc $p \equiv \sum_{i=0}^{n_0} x_i \cdot a^i [a-1]$.

Or, $a \equiv 1[a-1]$ puisque $a = 1 + (a-1)$.

On déduit des propriétés usuelles des congruences que $a^i \equiv 1[a-1]$ quel que soit l'entier i .

Donc $p \equiv \sum_{i=0}^{n_0} x_i [a-1]$.

Le résultat est alors immédiat.

iii) Le raisonnement est analogue : $p = \sum_{i=0}^{n_0} x_i \cdot a^i$ donc $p \equiv \sum_{i=0}^{n_0} x_i \cdot a^i [a+1]$.

Or, $a \equiv -1[a+1]$ puisque $a = -1 + (a+1)$.

On déduit des propriétés usuelles des congruences que $\begin{cases} a^{2k} \equiv 1[a+1] \\ a^{2k+1} \equiv -1[a+1] \end{cases}$ quel que soit l'entier k .

Donc $p \equiv \sum_{i=0}^{n_0} (-1)^i x_i [a+1]$.

Le résultat est alors immédiat.

Remarque : On retrouve les critères de divisibilité par 10^n , 9 et 11 dans l'écriture décimale d'un entier.

2) Exemple « monétaire »

On suppose que la banque centrale européenne émette des billets de valeur numéraire des puissances de 3 : 1 €, 3 €, 9 €, 27 €, 81 €

Alors, pour payer un achat (d'une somme entière) inférieure ou égale à 81 €, il suffit que chacune des deux parties ait exactement un billet de chaque sorte.

Démonstration :

Elle est basé sur l'égalité, vraie quel que soit l'entier k , $2 \times 3^k = 1 \times 3^{k+1} - 1 \times 3^k$.

Soit S la somme due : on écrit S en base 3 : Soit $S = \sum_{i=0}^4 x_i \cdot 3^i$

- Si $x_0 = 0$ alors les deux parties n'échangent pas de billet de 1 €
- Si $x_0 = 1$ alors l'acheteur donne un billet de 1 € au vendeur.
- Si $x_0 = 2$: l'acheteur ne peut donner deux billets de 1 € au vendeur : il ne lui en donne aucun et il augmente x_1 de une unité (modulo 3, en répercutant éventuellement sur x_2, x_3, x_4 si ces valeurs deviennent supérieures à 2)

L'acheteur devra donc donner un billet de 3 € supplémentaire au vendeur qui lui rendra un billet de 1 €

On recommence pour les billets de 3 €, 9 €, 27 € et 81 €

Exemple : On effectue un achat de 62 €. On écrit 62 en base 3 : $\overline{62}^{10} = \overline{2022}^3$.

L'acheteur devrait donner 2 billets de 1 € au vendeur : il ne lui en donne pas et augmente x_1 de 1 unité modulo 3, le vendeur devra lui rendre un billet de 1 €. x_1 devient égal à 3 donc on pose $x_1 = 0$ et $x_2 = 1$.

De la même façon, l'acheteur devrait donner deux billets de 27 € au vendeur : il ne lui en donnera aucun, lui donnera un billet de 81 € en recevant en retour un billet de 27 €

En résumé : l'acheteur donne un billet de 9 € et un billet de 81 €, soit 90 €

Le vendeur rend un billet de 1 € et un billet de 27 €, soit 28 €

3) Jeu de Nim :

On dispose au départ d'un certain nombre de tas T_j , ($j = 1..p$), chaque tas étant constitué de jetons, d'allumettes... Soit n_j le nombre d'objets du tas T_j . Ne considérant pas de tas vide, on a $n_j \geq 1$.

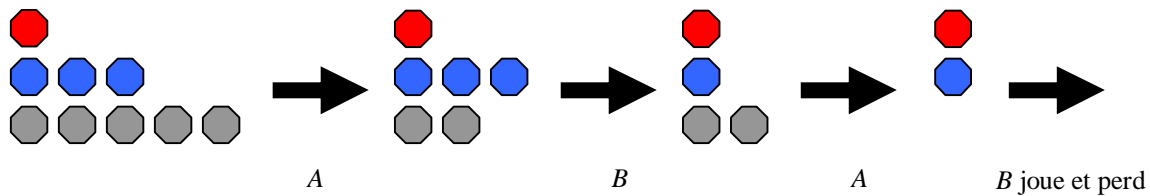
Le jeu de Nim se joue à deux joueurs, A et B . Les joueurs jouent alternativement et à chaque étape, celui dont c'est le tour prend autant de jetons qu'il le souhaite, mais dans un seul tas.

Le joueur qui prend le dernier jeton est gagnant.

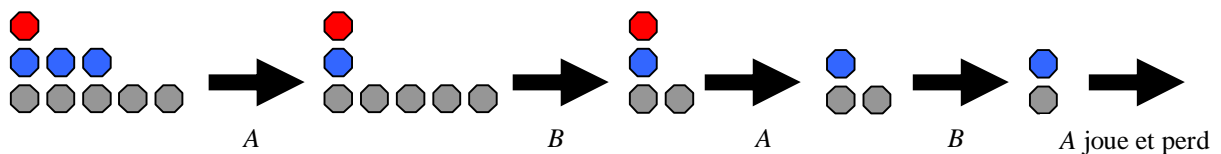
Exemple :

On part avec trois tas T_1 , T_2 et T_3 avec $n_1 = 1$, $n_2 = 3$ et $n_3 = 5$.

Le joueur A commence et prend 3 jetons dans T_3 , puis B prend 2 jetons dans T_2 , A prend 2 jetons dans T_3 puis B joue et A gagne.



Avec la même configuration de départ, si A prend 2 jetons dans T_2 , puis B en prend 3 dans T_3 , A en prend 1 dans T_1 , B en prend 1 dans T_3 puis A joue et B gagne.



Il y a forcément un vainqueur puisque à chaque étape, le nombre de jetons diminue strictement. Nous dirons qu'une situation est gagnante pour A si c'est une configuration obtenue après un coup de A et telle que A gagne quoique fasse B . C'est par exemple le cas si, après que A ait joué, il ne reste qu'un nombre pair de tas non vides n'ayant chacun qu'un seul jeton. Ou bien si, après un coup de A , il ne reste que 2 tas non vides ayant chacun 2 jetons.

Une stratégie pour gagner :

A une configuration de jeu, on associe une matrice de 0 et de 1 de la façon suivante : on écrit chaque n_j en base deux et on met, au besoin, des 0 devant pour que toutes les écritures soient de la même longueur q : on obtient une matrice à p lignes et q colonnes, la ligne j contenant l'écriture binaire de n_j .

Par exemple, la situation de jeu initiale de l'exemple correspond à la matrice :

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

A chaque coup de jeu, on obtient une nouvelle matrice : les matrices suivantes correspondent aux trois premiers coups de l'exemple :

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

On dit qu'une configuration est correcte si, dans la matrice qui lui est associée, chaque colonne contient un nombre pair de 1. Dans l'exemple précédent, les configurations associées aux matrices 2 et 4 sont correctes, les autres ne le sont pas.

Lemme 1 : *Tout mouvement à partir d'une configuration correcte conduit à une configuration qui ne l'est pas.*

Démonstration : Si la configuration est correcte, dans chaque colonne il y a un nombre pair de 1. Le joueur dont c'est le tour de jouer prend des jetons dans un tas T_j où il y en a encore, ce qui correspond à une ligne où il n'y a pas que des 0. Ce faisant, il remplace n_j par un entier strictement plus petit, dont l'écriture en base deux diffère de celle de n_j en au moins une place. Alors la nouvelle colonne correspondant en cette place contient un nombre impair de 1.

Lemme 2 : A partir d'une configuration incorrecte, il existe toujours un mouvement conduisant à une configuration correcte.

Démonstration : Si la configuration est incorrecte, il existe au moins une colonne de la matrice correspondante qui contient un nombre impair de 1 : soit C_{j_0} la colonne la plus à gauche de la matrice contenant un nombre impair de 1. On choisit une ligne contenant un 1 dans cette colonne, soit L_{i_0} . $L_{i_0} = (a_1, a_2, \dots, a_{j_0-1}, 1, a_{j_0+1}, \dots, a_q)$. On prend dans le tas T_{i_0} correspondant un nombre de jetons de façon à obtenir une ligne $L'_{i_0} = (a'_1, a'_2, \dots, a'_{j_0-1}, 0, a'_{j_0+1}, \dots, a'_q)$ avec $a'_i = a_i$ si la colonne i contient un nombre pair de 1, et $a'_i \neq a_i$ sinon. Les autres lignes restent inchangées. Dans cette nouvelle matrice, toutes les colonnes ont un nombre pair de 1, et correspondent donc à une configuration correcte.

Exemple :

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \longrightarrow \quad \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

La situation est incorrecte, le tas T_2 contient 15 jetons. En prenant 14 jetons dans ce tas, le joueur ramène le jeu à une configuration correcte.

Proposition : Les configurations correctes sont les configurations gagnantes.

Démonstration :

Dans une configuration correcte où tous les tas ne sont pas vides, il y a au moins des jetons dans deux tas différents. Donc un joueur héritant d'une telle configuration ne peut pas gagner en un coup.

Supposons qu'après que A ait joué, la configuration soit correcte. Le joueur B , en jouant son coup, produit une configuration incorrecte d'après le lemme 1. D'après le lemme 2, le joueur A ramène le jeu à une configuration correcte. B ne peut donc pas gagner en un coup...

En clair, B ne peut donc pas gagner tant que A le laisse dans une configuration correcte. Comme la partie se termine, c'est évidemment A qui gagne.

En conclusion, le joueur connaissant ces résultats est sûr de gagner dès que son adversaire lui laisse une position incorrecte.