Une approche globale des systèmes de numération.

L'article sur la découverte des chiffres romains dans la ville de Caen m'a amené à dépoussiérer un exposé préparé pour l'oral du CAPES de mathématiques (années 1975).
Commençons par citer un extrait des éléments d'histoire des mathématiques de N. Bourbaki (p.64).

> L'histoire et l'archéologie nous font connaître un grand nombre de systèmes de numération ; leur but initial est d'attacher à chaque entier individuel (jusqu'à une limite qui dépend des besoins de la pratique) un nom et une représentation écrite, formés de combinaisons d'un nombre restreint de signes, s'effectuant suivant des lois plus ou moins régulières. Le procédé de beaucoup le plus fréquent consiste à décomposer les entiers en sommes d' « unités successives »$u_1, u_2, u_n, \dots$ dont chacune est un multiple entier de la précédente ; et si en général $\dfrac{u_n}{u_{n-1}}$ est pris égal à un même nombre b (la « base »du système, le plus souvent 10), on observe mainte exception à cette règle comme chez les Babyloniens, où $\dfrac{u_n}{u_{n-1}}$ est tantôt égal à 10, tantôt à 6, dans le système chronologique des Mayas, où $\dfrac{u_n}{u_{n-1}}$ est égal à 20 sauf pour $n = 2$, et où $\dfrac{u_2}{u_1} = 18$, et dans le système romain où $\dfrac{u_n}{u_{n-1}}$ est tantôt égal à 5, tantôt à 2. Quant à l'écriture correspondante, elle doit indiquer le nombre d' « unités »u_i de chaque ordre i ; dans beaucoup de systèmes (comme chez les Égyptiens, les Grecs et les Romains), les multiples successifs $k.u_i$, (où k varie de 1 à $\dfrac{u_{i+1}}{u_i} - 1$) sont désignés par des symboles qui dépendent à la fois de k et de i. Un premier et important progrès consiste à désigner tous les nombres $k.u_i$ (pour la même valeur de k) par le même signe : c'est le principe de la « numération de position », où l'indice i est indiqué par le fait que le symbole représentant $k.u_i$, apparaît à la i-ème place dans la succession des « tranches »constituant le nombre représenté. Le premier système de cette nature se rencontre chez les Babyloniens, qui, sans doute dès 2 000 avant J.-C., notent par un même signe tous les multiples $k.60^{\pm i}$ correspondant à des valeurs quelconques de l'exposant i .

La présentation du système b-adique (qui généralise la numération décimale de position et où b est un entier supérieur ou égal à 2) se trouve fréquemment détaillée dans les ouvrages de mathématiques élémentaires. Nous nous proposons d'examiner ici une présentation moins courante, qui généralise le système b-adique en formalisant les situations « uni et multi-base » évoquées dans l'extrait précédent. Sautons donc joyeusement dans le formalisme « bourbakien »

Représentation générale d'un entier

On se donne une suite d'entiers **non nuls** $(b_i)_{i \in I}$ avec soit $I = [\![1, l]\!]$ où $l \in \mathbb{N}^*$(cas fini), soit $I = \mathbb{N}^*$(cas infini). Pour chaque $i \in I$, on considère un sous-ensemble d'entiers S_i fixé et constitué de b_i représentants pour la congruence modulo b_i. S_i peut être $(0, 1, ..., b_i - 1)$ mais aussi tout autre système de représentants, même négatifs.
soit m un entier rationnel.

On appelle développement de m dans le système $(S_i, b_i)_{i \in I}$ toute suite finie d'entiers $(a_j)_{0 \le j \le k}$ $(a_0, a_1, \dots, a_k)$ telle que

- $0 \le k \le l$ dans le cas fini, $k \ge 0$ sinon
- Si $0 \le j \le k - 1$ alors $a_j \in S_{j+1}$ et si $k + 1 \in I$ alors $a_k \in S_{k+1}$ (a_k est un entier quelconque lorsque S_{k+1} n'est pas défini)
- $k \ne 0$ entraîne $a_k \ne 0$
- $m = a_0 + a_1 b_1 + a_2 b_1 b_2 + a_3 b_1 b_2 b_3 + \cdots + a_k b_1 b_2 \cdots b_k$

Exemples

Système de « Cro-Magnon » La suite $(b_i)_{i \in \mathbb{N}^*}$ est la suite constante valant 1. $S_1 = \{0\}$ et $S_i = \{1\}$ pour $i \ge 2$. Tout entier m positif admet le développement (0,1,1,1,. . ., 1) ; c'est une liste de longueur $m + 1$ et $k = m$.

Système « horaire » I est fini, $l = 3$. Nous fixons les valeurs suivantes : $b_1 = b_2 = 60$, $b_3 = 24$, $S_1 = S_2 = \{r \in \mathbb{Z}/0 \leq r < 60\}$ et et $S_3 = \{r \in \mathbb{Z}/0 \leq r < 24\}$. Toute durée exprimée en secondes peut s'exprimer en jours, heures, minutes et secondes. Par exemple m=4617087 se décompose selon le développement(27,31,10,53) soit 53 jours, 10 heures 31 minutes et 27 secondes. Ici $k = 3$ et $m = \mathbf{27} + \mathbf{31} \times 60 + \mathbf{10} \times 60 \times 60 + \mathbf{53} \times 60 \times 60 \times 24$. Comme S_4 n'est pas défini $a_3 = 53$ n'a pas de contrainte à satisfaire.

Système « décimal » La suite $(b_i)_{i\in\mathbb{N}^*}$ est la suite constante valant 10. $S_i = \{r \in \mathbb{Z}/0 \leq r < 10\} = \{0, 1, 2, \ldots, 8, 9\}$ pour tout $i \in \mathbb{N}^*$. $m = \overline{12379}^{10} = \mathbf{9} + \mathbf{7} \times 10 + \mathbf{3} \times 10^2 + \mathbf{2} \times 10^3 + \mathbf{1} \times 10^4$.

Système « Romain limité » I est fini, $l = 6$. On choisit la suite $(b_i)_{1\leq i\leq 6}$ telle que $b_i = 5$ pour i impair et $b_i = 2$ pour i pair. $S_i = \{-1, 0, 1, 2, 3\}$ pour i impair et $S_i = \{0, 1\}$ pour i pair.
$m = 3773 = \underline{3}+\underline{0}\times5+\underline{2}\times5\times2+\underline{1}\times5\times2\times5+\underline{2}\times5\times2\times5\times2+\underline{1}\times5\times2\times5\times2\times5+\underline{3}\times5\times2\times5\times2\times5\times2$
Le développement de m est (3,0,2,1,2,1,3). $k = 6$ et $a_6 = 3$.
En utilisant les sept symboles (I,V,X,L,C,D,M) pour chaque tranche d'unités on en déduit l'écriture de type additif $m =$ **MMMDCCLXXIII**. $a_1 = 0$ se traduit par l'absence du symbole V dans l'écriture. Pour $m = 14$ nous avons $14 = \mathbf{-1} + \mathbf{1} \times 5 + \mathbf{1} \times 5 \times 2$ qui donne $m =$ **XIV** avec la convention d'écriture soustractive classique. Ici $a_0 = -1, a_1 = 1, a_2 = 1$. Pour $m = 99$ le développement est donné par (-1,0,0,0,1) qui produit l'écriture $m =$**IC**. Cette représentation ne respecte pas la convention « pas de soustraction d'une lettre plus de dix fois supérieure » et on écrit plutôt $m =$**XCIX** qui ne cadre pas avec notre type de décomposition (l'entité X est à la fois ajoutée et retranchée). Ces règles sont restées assez floues jusqu'au Moyen-Âge, et pas toujours appliquées d'ailleurs.

Système « Romain généralisé » I est $\mathbb{N}^*$. On choisit la suite $(b_i)_{i\in I}$ telle que $b_i = 5$ pour i impair et $b_i = 2$ pour i pair. $S_i = \{-1, 0, 1, 2, 3\}$ pour i impair et $S_i = \{0, 1\}$ pour i pair.
Ce système ne présente pas d'intérêt pratique car avec le principe additif de l'écriture symbolique, il nous faudrait un ensemble infini de symboles pour écrire tous les entiers.

Examinons maintenant l'existence et l'unicité de la décomposition des entiers dans ces systèmes $(S_i, b_i)_{i\in I}$.

Théorème 1

Tout entier m a un développement unique dans tout système $(S_i, b_i)_{i\in I}$ fini, $I = \llbracket 1, l \rrbracket$.

Une remarque préliminaire : Soit $(a_0, a_1, \ldots, a_k)$ un développement de m dans $(S_i, b_i)_{i\in I}$. Nous avons $a_0 \equiv m[b_1]$ et $m - a_0 = b_1 m_1$. Nous en déduisons $m_1 = a_1 + a_2 b_2 + a_3 b_2 b_3 + \cdots + a_k b_2 \cdots b_k$ où les a_i satisfont aux conditions d'un développement dans le système $(S_i, b_i)_{i\in I\setminus 1}$; $(a_1, a_2, \ldots, a_k)$ est un développement de m_1 dans $(S_i, b_i)_{2\leq i\leq l}$.
Réciproquement, soit m un entier et $a_0 \in S_1$ tel que $m \equiv a_0[b_1]$. Posons $m_1 = \frac{m-a_0}{b_1}$. Si $(a_1, a_2, \ldots, a_k)$ est un développement de m_1 dans $(S_i, b_i)_{2\leq i\leq l}$ alors $(a_0, a_1, \ldots, a_k)$ est un développement de m dans $(S_i, b_i)_{i\in I}$.

Nous prouvons alors par récurrence sur la longueur l du système $(S_i, b_i)_{i\in I}$ que tout entier a un développement unique dans tout système de longueur l.

- Pour $l = 1$, $m = a_0 + a_1 b_1$ où a_0 est le représentant de S_1 congru à m modulo b_1 et $a_1 = \frac{m-a_0}{b_1}$. D'où l'existence et l'unicité de la décomposition de tout entier dans ce cas.
- D'après la remarque préliminaire, l'existence de la décomposition est une propriété héréditaire à partir de $l = 1$. Montrons que l'unicité de la décomposition l'est aussi :
  Nous posons $k = l + 1$ et envisageons deux décompositions.
  $m = a_0 + a_1 b_1 + a_2 b_1 b_2 + a_3 b_1 b_2 b_3 + \cdots + a_k b_1 b_2 \cdots b_k$ et
  $m = \alpha_0 + \alpha_1 b_1 + \alpha_2 b_1 b_2 + \alpha_3 b_1 b_2 b_3 + \cdots + \alpha_k b_1 b_2 \cdots b_k$.
  Ces décompositions entraînent $a_0 - \alpha_0 \equiv 0[b_1]$ d'où $a_0 = \alpha_0$ puisque a_0 et α_0 sont dans S_1. Nous avons alors $a_1 + a_2 b_2 + a_3 b_2 b_3 + \cdots + a_k b_2 \cdots b_k = \alpha_1 + \alpha_2 b_2 + \alpha_3 b_2 b_3 + \cdots + \alpha_k b_2 \cdots b_k$ et l'unicité pour la longueur l (hypothèse de récurrence) entraîne l'égalité $a_i = \alpha_i$ pour tout $i \in \llbracket 0, l + 1 \rrbracket$.

Nous concluons selon le principe de récurrence que tout entier m a une décomposition unique pour tout système fini de longueur l, quel que soit l'entier l non nul.

Abordons maintenant le cas infini où $I = \mathbb{N}^*$.

Théorème 2

Avec les hypothèses plus restrictives suivantes :
Pour tout i de $\mathbb{N}^*$, $\quad b_i > 1$ et $S_i \subset \{r \in \mathbb{Z} / -b_i < 2r < 2b_i\}$
nous pouvons affirmer que tout entier m strictement positif admet un développement unique dans le système $(S_i)_{i\in I}$. C'est aussi le développement dans le système fini $(S_i, b_i)_{1\leq i\leq m}$. De plus le développement de $m = 0$ ne peut être que $(0)(k = 0$ et $a_0 = 0)$. Celui-ci existe ssi $0 \in S_1$.

Preuve

Étape 1 Pour $m \geq 0$, nous prouvons que dans tout système fini extrait de $(S_i)_{i\in I}$ en se limitant à $1 \leq i \leq l$ $(l \geq 1)$, le dernier élément du développement a_k vérifie $a_k \geq 0$.
$m = a_0 + a_1b_1 + a_2b_1b_2 + a_3b_1b_2b_3 + \cdots + a_kb_1b_2\cdots b_k$. Or pour $i < k$, $a_i \in S_{i+1}$ entraîne $a_i < b_{i+1}$ ou $a_i \leq b_{i+1} - 1$. Il vient alors par majoration
$m \leq (b_1 - 1) + (b_2 - 1)b_1 + (b_3 - 1)b_1b_2 + (b_4 - 1)b_1b_2b_3 + \cdots + (b_{k-1} - 1)b_1b_2\cdots b_{k-1} + a_kb_1b_2\cdots b_k$
et en développant et simplifiant $m \leq -1+b_1b_2\cdots b_k+a_kb_1b_2\cdots b_k$, d'où $m \leq -1+(a_k+1)(b_1b_2\cdots b_k)$.
Finalement $m < (a_k + 1)(b_1b_2\cdots b_k)$ ce qui pour $m \geq 0$ permet de conclure $a_k \geq 0$.
Si $a_k = 0$, on a $k = 0$ et $m = a_0 = a_k = 0$. Donc ce cas ne présente pas lorsque $m > 0$ ou $k \neq m$.

Étape 2 Nous prouvons que $a_k > 0$ entraîne $m > k$.
$2m = 2a_0 + 2a_1b_1 + 2a_2b_1b_2 + 2a_3b_1b_2b_3 + \cdots + 2a_kb_1b_2\cdots b_k$. Pour $0 \leq i < k \quad 2a_i > -b_{i+1}$, ce qui équivaut à $2a_i \geq -b_{i+1} + 1$. Nous déduisons que
$2m \geq 1 - b_1 + (1 - b_2)b_1 + (1 - b_3)b_1b_2 + (1 - b_4)b_1b_2b_3 + \cdots + (1 - b_k)b_1b_2\cdots b_{k-1} + 2a_kb_1b_2\cdots b_k$. En simplifiant après calculs, il nous reste $2m \geq 1 + (2a_k - 1)b_1b_2\cdots b_k$. Comme $a_k > 0$, $2a_k - 1 \geq 1$ d'où $2m \geq 1 + b_1b_2\cdots b_k > b_1b_2\cdots b_k$. Sachant que $b_i \geq 2$ nous en tirons $2m > 2^k \geq 2k$ ce qui implique $m > k$. Cela montre que le développement de m est alors le même dans le système $(S_i)_{1\leq i\leq m}$.

Étape 3 Pour $m > 0$ choisissons $l = m$. m admet un développement dans le système fini (théorème 1) extrait de $(S_i)_{1\leq i\leq m}$ et nous avons $k < m$. Cela fournit donc aussi ($a_k \in S_{k+1}$ car $k + 1 \leq m$) un développement dans le système infini $(S_i)_{i\in I}$. Ainsi m possède un développement.

L'unicité découle aussi du théorème 1 car deux développements de m dans le système infini $(S_i)_{i\in I}$ sont aussi des développements dans des systèmes finis extraits donc aussi dans $(S_i)_{1\leq i\leq m}$ dans lequel ils sont nécessairement identiques.

Pour $m = 0$, nous avons nécessairement $a_k = 0$ pour tout développement, puisque $a_k > 0$ entraîne $m > k \geq 0$. Dès lors $m = a_0 = 0$. Ce développement existe ssi $0 \in S_1$.

Corollaires

les hypothèses du théorème 2 étant remplies :

Système b-adique ($b \geq 2$) Tout entier $m \geq 0$ a un développement unique :
$m = a_0 + a_1b + a_2b^2 + \cdots + a_kb^k$. Les a_i sont dans $S = \{r \in \mathbb{Z}/0 \leq r < b\}$.

Système romain généralisé Tout entier $m > 0$ a un développement unique :
$m = a_0 + a_1 \times 5 + a_2 \times 10 + a_3 \times 50 + \cdots + a_k \times u_k$ où $u_k = 10^{k/2}$ si k pair et $u_k = 5 \times 10^{(k-1)/2}$ si k est impair. Les (a_i) sont dans $S = \{-1, 0, 1, 2, 3\}$ pour i pair et dans $S = \{0, 1\}$ pour i impair.

Éric Trotoux