Qu'est-ce que les nombres p-adiques ?

Alain M. Robert[1]

Différentes sortes de nombres

Les nombres entiers naturels 1,2,3,... sont les premiers qui se présentent à l'esprit. On découvre rapidement l'importance du nombre 0 qu'il s'agit d'ajouter aux précédents pour obtenir le fameux ensemble N sur lequel se basent les mathématiques de Kronecker (1823-1891, banquier et mathématicien!). Peano en donne une axiomatique en 1889.

On reconnaît aussi rapidement la nécessité d'introduire des nombres négatifs (chiffres rouges!) et de considérer les couples "actif-passif" pour les décrire. Cette exigence de pouvoir toujours soustraire des entiers peut être reportée sur la division et c'est dans ce but que l'ensemble des nombres rationnels (les fractions) est introduit. Les notations canoniques pour ces ensembles sont les suivantes

$$\mathbf{Z} = \{0, \pm 1, \pm 2, ...\}, \quad \mathbf{Q} = \{m/n \ : m \text{ et } n \in \mathbf{Z} \text{ et } n \geq 1\}.$$

Le théorème fondamental de l'arithmétique dit alors que tout nombre rationnel peut être écrit d'une et d'une seule façon comme produit de nombres premiers, certains apparaissant au dénominateur, donc avec des exposants négatifs

$$m/n = \pm 2^a 3^b 5^c ... \quad (a, b, c, ... \in \mathbf{Z}).$$

En particulier, si la fraction *m/n* n'est pas réduite, un nombre premier p peut apparaître au numérateur et au dénominateur et l'exposant qui figure dans la décomposition précédente est la différence des exposants de ce nombre premier apparaissant au numérateur et au dénominateur. Le carré du nombre rationnel *m/n* est ainsi

$$(m/n)^2 = +2^{2a} 3^{2b} 5^{2c} ...$$

Il en résulte que les carrés des nombres rationnels sont exactement les nombres rationnels positifs ayant des exposants tous pairs dans leur décomposition comme produit de facteurs premiers. Par conséquent, les nombres suivants

$$2, 3, 2/3, 15 = 3 \cdot 5, 2/9, 27 = 3^3, 27/4 = 2^{-2} \cdot 3^3, ...$$

ne sont pas des carrés de nombres rationnels. Pour pouvoir dire que la diagonale du carré unité est un nombre, il faut encore étendre la notion de nombre pour y inclure $\sqrt{2}$. C'est ainsi qu'on considère l'ensemble des nombres réels **R** que l'on se représente par les points d'une droite (sur laquelle on a choisi une origine, le 0, et une unité, le 1). Ces nombres représentent traditionnellement le continu. Ils permettent une bonne description du temps, dans son passé et son futur, dans son écoulement sans saccade.

Il faut ensuite mentionner les nombres complexes **C** qui représentent une extension très utile des nombres réels. Sans entrer dans les détails de la polémique créée par leur introduction, rappelons que le symbole $i = \sqrt{-1}$ a été introduit par Euler en 1777, précisément comme abréviation d'une unité imaginaire.

[1] Institut de mathématiques de l'université de Neuchâtel. L'article reprend un exposé fait le 14 novembre 1995 dans le cadre du Mois de la Science organisé par la SENS. Il a été remis en page en janvier 2008.

Par la suite, Hamilton a encore introduit un corps de quaternions **H** (non commutatif), Cayley a défini des octaves (qui forment un domaine non associatif). Ainsi le concept de nombre a-t-il connu toute une suite d'extensions.

Kurt Hensel (1861-1941) découvre une alternative. Partant des nombres rationnels, il envisage en effet vers 1897 des nombres nouveaux, indépendants des nombres réels. Le corps **Q** des nombres rationnels est ainsi à l'origine de plusieurs extensions *indépendantes*

$$\mathbf{Q}_2, \mathbf{Q}_3, \mathbf{Q}_5, \ldots \quad (\text{et } \mathbf{R}).$$

Chacune d'elle peut être ensuite plongée dans un corps universel

$$\mathbf{C}_2, \mathbf{C}_3, \mathbf{C}_5, \ldots \quad (\text{et } \mathbf{C}).$$

Ces corps universels sont miraculeusement isomorphes algébriquement bien que leur construction et leur aspect topologique soient totalement différents (les corps **C***p* sont totalement discontinus, tandis que le corps complexe **C** est connexe). Pour introduire ces nombres p-adiques, nous allons nous inspirer de l'article de R. Cuculière (référence en fin de ce texte) et commencer par les nombres automorphes.

Les nombres automorphes de Gergonne et Lucas

Nous nous intéressons aux nombres n qui dans le système décimal ont la propriété d'écriture

$$n^2 \text{ se termine par } n.$$

Par exemple, on peut citer

$$6 \times 6 = 36 \text{ se termine par } 6,$$
$$76 \times 76 = 5776 \text{ se termine par } 76,$$
$$376 \times 376 = 171376 \text{ se termine par } 376, \text{ etc.}$$

ou bien

$$5 \times 5 = 25 \text{ se termine par } 5,$$
$$25 \times 25 = 625 \text{ se termine par } 25,$$
$$625 \times 625 = 390625 \text{ se termine par } 625, \text{ etc.}$$

On peut montrer (bon exercice !) que les deux séries de nombres précédentes peuvent être continuées indéfiniment de façon unique, d'où l'idée de considérer les développements illimités à gauche

$$\ldots 109376 = s, \quad \ldots 890625 = t$$

comme des "nombres" d'un type nouveau. Ces développements seront appelés *nombres décadiques ou* mieux *nombres 10-adiques.* La terminaison vient de la racine *-adis* latine ou *-ados* grecque (la décade est une période de dix jours, utilisée par exemple dans le calendrier républicain après la révolution française; on réserve plutôt le terme de décennie pour une période de dix ans). Les règles usuelles de *retenues* permettent d'additionner et multiplier ces nombres décadiques. On obtient ainsi un anneau commutatif que l'on représente par $\mathbf{Z}_{10}$. Les entiers naturels sont considérés comme des nombres décadiques simplement en convenant que leur développement commence par une infinité de zéros. Par exemple voici une somme

$$\ldots 999990 + \ldots 000010 = \ldots 000000 \ (= 0).$$

Ceci nous permet de dire que le nombre décadique ...999990 est inverse pour l'addition de 10, et donc que ...999990 = -10. Donc notre anneau $\mathbf{Z}_{10}$ contient des nombres négatifs (cette particularité de représentation de nombres négatifs par des nombres commençant par une suite de chiffres 9 est utilisée dans les ordinateurs).

Si on continue notre expérimentation des nombres automorphes, on trouve que par construction

$$s^2 = ...109376 \text{ x } ...109376 = ...109376 = s,$$

$$t^2 = ...890625 \text{ x } ...890625 = ...890625 = t.$$

(Mieux : $s = s^2 = s^3 = ...$ et de même pour t !) On trouve aussi

$$s + t = 1 \text{ (mais oui !) et } st = 0.$$

Cet anneau est un peu étrange à première vue. Puisque le produit de deux éléments non nul peut y être nul, on dit qu'il n'est *pas intègre.*

Tout ce qui vient d'être fait dépend naturellement du choix de la base 10 pour représenter les nombres. On pourrait faire de même avec les bases 2, 3, 5, ... Par exemple, $\mathbf{Z}_5$ dénote l'anneau des nombres ayant une écriture illimitée à gauche en base 5. Le sens de l'écriture étant inversé, on doit considérer que les chiffres placés de plus en plus à gauche ont de moins en moins d'importance (et dénotent par conséquent des contributions de plus en plus *petites* dans un sens à préciser...). Pour chaque nombre premier p, l'anneau des nombres p-adiques est ainsi l'anneau $\mathbf{Z}_p$ consistant en les développements illimités

$$... a_3a_2a_1a_0 = a_0 + a_1p + a_1p^2 + a_1p^3 + ...$$

Une façon de présenter cet anneau consiste à poser par définition

$$\mathbf{Z}_p = \mathbf{Z}[[X]]/(X - p)$$

donc à identifier les nombres p-adiques aux séries formelles en une indéterminée X que l'on remplace par le nombre p en fin de compte.

Revenons aux nombres 10-adiques. On observe que $s = ...109376$ a un reste de division par 5 égal à 1, ce qui est traditionnellement dénoté par

$$s \equiv 1 \bmod 5.$$

Le reste de la division de s par 25 est aussi 1 et plus généralement

$$s = ...109376 \equiv 1 \bmod 5^n.$$

Cela signifie que si on essaie de développer ce nombre en base 5, on trouve

$$s = 1 + 0\cdot5 + 0\cdot5^2 + 0\cdot5^3 + ...$$

Ce même nombre s est divisible par 2, 4, ... et satisfait

$$s \equiv 0 \bmod 2^n$$

qui disent que son développement illimité en base 2 est trivial

$$s = 0 + 0\cdot2 + 0\cdot2^2 + 0\cdot2^3 + ...$$

Loin de nous décourager, ces faits nous conduisent à remarquer que l'application qui à un nombre décadique associe ses développements en base 5 et en base 2, disons

$$f : \mathbf{Z}_{10} \to \mathbf{Z}_5 \times \mathbf{Z}_2$$

est telle que $f(s) = (1,0)$ et $f(t) = (0,1)$. On peut aussi expliciter cette application f sous la forme suivante

$$x \mapsto (sx, tx)$$

Elle est inversible par $(a, b) \mapsto a + b$ car en effet

$$x = 1 \cdot x = (s + t)x = sx + tx.$$

Cette application f fournit un *isomorphisme* entre $\mathbf{Z}_{10}$ et $\mathbf{Z}_5 \times \mathbf{Z}_2$. Il est plus facile d'étudier les anneaux p-adiques (p premier) que l'anneau 10-adique. On peut montrer en effet que lorsque p est un nombre premier, l'anneau $\mathbf{Z}_p$ est *intègre.* Ce sont ces nombres p-adiques qui ont été découverts par Hensel (1861-1941) et qu'il introduit par des considérations algébriques dans *Theorie des algebraischen Funktionen einer Variabeln* (1902).

Il ajoute par la suite le corps des fractions $\mathbf{Q}_p$ de l'anneau $\mathbf{Z}_p$ dans *Theorie des algebraischen Zahlen* (1908).

On peut se représenter les nombres rationnels p-adiques comme étant ceux qui en base p ont un nombre fini de décimales: ils correspondent ainsi à un nombre fini de termes $a_i p^i$ avec i négatif (on rencontre des séries analogues en développant des fonctions rationnelles en série de Laurent).

Quelques commentaires encore concernant les nombres décadiques. Le nombre s engendre un idéal principal $(s) = I = s\mathbf{Z}_{10} \subset \mathbf{Z}_{10}$ et la multiplication par s dans l'anneau décadique est un projecteur de cet anneau sur cet idéal. Il en est de même pour la multiplication par t qui projette l'anneau $\mathbf{Z}$ sur l'idéal principl $(t) = J$. Comme $s + t = 1$, on en déduit que l'anneau décadique est isomorphe à la somme directe de ces deux idéaux. L'équation $x^2 - x = 0$ a en fait quatre solutions dans $\mathbf{Z}_{10}$, à savoir 0, 1, s et t. Il et clair que si x en est une solution, $1-x$ en est aussi une puisque

$$(1 - x)^2 = 1 - 2x + x^2 = 1 - 2x + x = 1 - x.$$

Les deux solutions complémentaires x et $1-x$ satisfont encore

$$x(1 - x) = x - x^2 = 0$$

qui représente une forme d'orthogonalité. Ainsi les solutions de $x^2 = x$ apparaissent par paires. Par exemple 0 et 1 forment une paire, tout comme s et t.

Visualisation des anneaux p-adiques

Puisqu'on considère que les premiers chiffres apparaissant dans un développement illimité à gauche ont de moins en moins d'importance, on peut essayer de construire une *valeur absolue* sur $\mathbf{Z}_p$ pour laquelle $|p| > 1$ et donc pour laquelle

$$\ldots |p^3| = |p|^3 < |p^2| = |p|^2 < |p| < 1.$$

Ceci peut être fait et la valeur absolue correspondante a une propriété intéressante

$$|x| > |y| \Rightarrow |x + y| = |x| \quad \text{(le plus fort l'emporte !)}$$

Nous ne poursuivrons pas ce point de vue important ici. Néanmoins, une idée simple s'impose. Ne faut-il pas voir un développement illimité à gauche $x \in \mathbf{Z}_{10}$ tout simplement comme un développement décimal illimité à droite, de la forme

$$x = 0, \ldots \in [0, 1] \, ?$$

Plus généralement, pourquoi ne pas simplement retourner les développements et considérer l'application

$$\mathbf{Z}_p \to [0, 1] : \ldots a_2 a_1 a_0 \mapsto 0, a_0 a_1 a_2 \ldots = a_0/p + a_1/p^2 + \ldots \, ?$$

On a choisi la numération en base p - par cohérence - aussi pour les nombres réels entre 0 et 1. Deux inconvénients surgissent. Le premier est que cette correspondance ne respecte pas les règles de retenues: les retenues sont reportées à gauche dans la source, tout comme dans l'image alors que la symétrie retourne gauche et droite. Le deuxième est la non injectivité de cette symétrie. En effet, les deux nombres 10-adiques distincts ...9990 = -10 et ...0001 = 1 ont même image 0,1 = 0,0999... (Le même phénomène apparaît bien sûr dans tous les $\mathbf{Z}_p$).

Il est plus raisonnable de se représenter l'ensemble des suites de 0 et 1 par les branches d'un arbre qui présente une structure dichotomique régulière. Une suite binaire illimitée peut soit être interprétée comme branche (trajet) illimitée ou comme extrémité de la branche. Le dessin de la figure 1 montre cette façon de représenter $\mathbf{Z}_2$ La correspondance avec les nombres réels entre 0 et 1 est bien illustrée par ce modèle: la coïncidence de deux numérations peut être rendue par un choix d'échelle convenable.

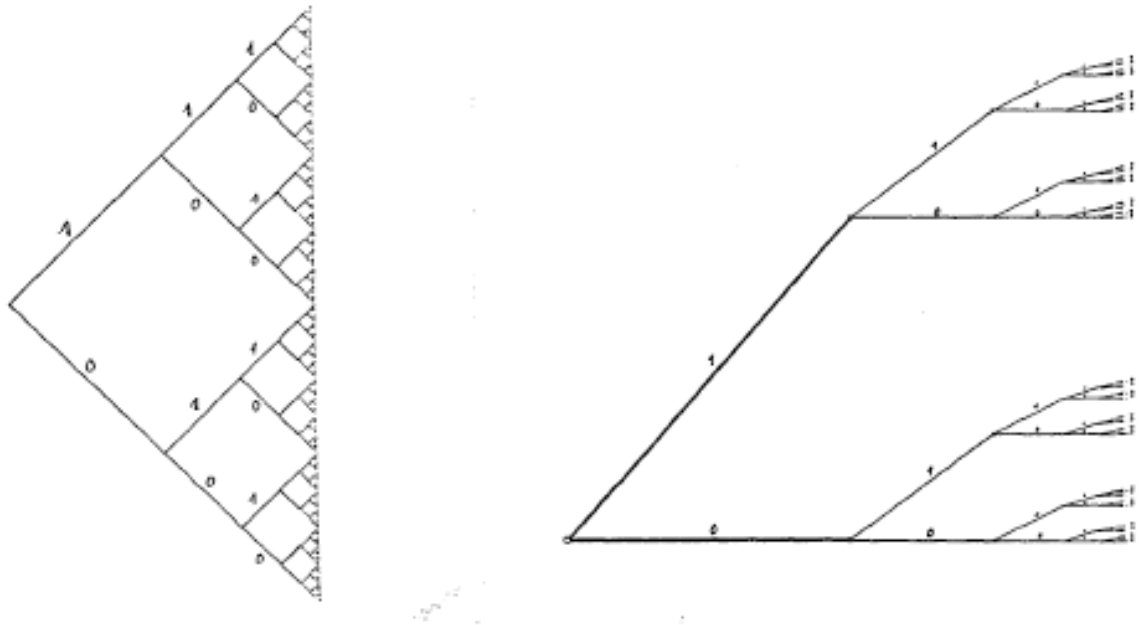

fig 1. Représentation de $\mathbf{Z}_2$

Le dessin montre aussi comment pallier cet inconvénient: il suffit de séparer les branches par exemple en les faisant aboutir dans l'*ensemble de Cantor.* Rappelons que ce dernier ensemble est obtenu en retranchant le tiers médian de l'intervalle [0,1], puis celui des intervalles restants, etc. Cette procédure s'explique facilement en base 3. Les nombres 0, a_0 ... qui ont un premier chiffre après la virgule différent de 1 en base 3 (donc $a_0 = 0$ ou 2) sont précisément ceux qui évitent le tiers médian. Les nombres qui tombent dans l'ensemble de Cantor sont précisément ceux qui en base 3 s'écrivent avec des chiffres a_i tous différents de l ($a_i = 0$ ou 2). Une bonne correspondance entre $\mathbf{Z}_2$ et une partie de [0,1] est donnée par

$$\varphi : ...a_2a_1a_0 \mapsto 0, b_0b_1b_2 ... = 2a_0/3 + 2a_1/3^2 + ...$$

où donc $a_i = 0$ ou 1 implique $b_i = 2a_i = 0$ ou 2. Cette application nous donne une bonne idée de la morphologie *de* $\mathbf{Z}_2$ (mais ne rend pas compte de la structure algébrique de cet anneau). On peut procéder de même pour $\mathbf{Z}_3$, $\mathbf{Z}_5$, ...

Modèles euclidiens des anneaux p-adiques

Suivons l'idée donnée au paragraphe précédent en la généralisant. Pour cela, introduisons un espace euclidien V (espace vectoriel réel de dimension finie avec un produit scalaire). Choisissons une famille de vecteurs

$$k \mapsto v(k) \in V \ (0 \leq k \leq p - 1)$$

paramétrée par les chiffres qui interviennent dans les développements p-adiques. Alors, on peut fabriquer des applications $\mathbf{Z}_p \rightarrow V$

$$\Phi_q \ : \ \sum_{i\geq 0} a_i p^i \ \mapsto \ c \sum_{i\geq 0} v(a_i)/q^{i+1}$$

(où c est une constante de normalisation et $q > 1$ assure la convergence de la série). Selon les valeurs de q, on va voir que Φ_q est injective. Même lorsque ce n'est pas le cas, l'image est un fractal paramétré naturellement par $\mathbf{Z}_p$. Posons

$$\Sigma = \{v(0), v(1), ..., v(p - 1)\}$$

$$F_q = Im(\Phi_q) = \Phi_q(\mathbf{Z}_p) \subset V.$$

Par définition même

$$F_q = \bigcup_{v\in\Sigma} c\,(v + F_q/q)$$

réunion de p morceaux self-similaires au tout. Si q est assez grand, ces morceaux sont disjoints, Φ_q est injective et la dimension de self- similarité de cette image est le nombre d tel que l'homothétie de rapport q produit q^d morceaux semblables à l'original. On doit donc avoir

$$q^d = p, \ \ d = \log p / \log q \ .$$

Les cas particuliers suivants illustrent les images obtenues avec plusieurs applications Φ_q du type précédent.

Avec $p = 3$, on peut obtenir un modèle de $\mathbf{Z}_3$ qui paramètre naturellement le napperon (connexe) de Sierpinski (figure 2).

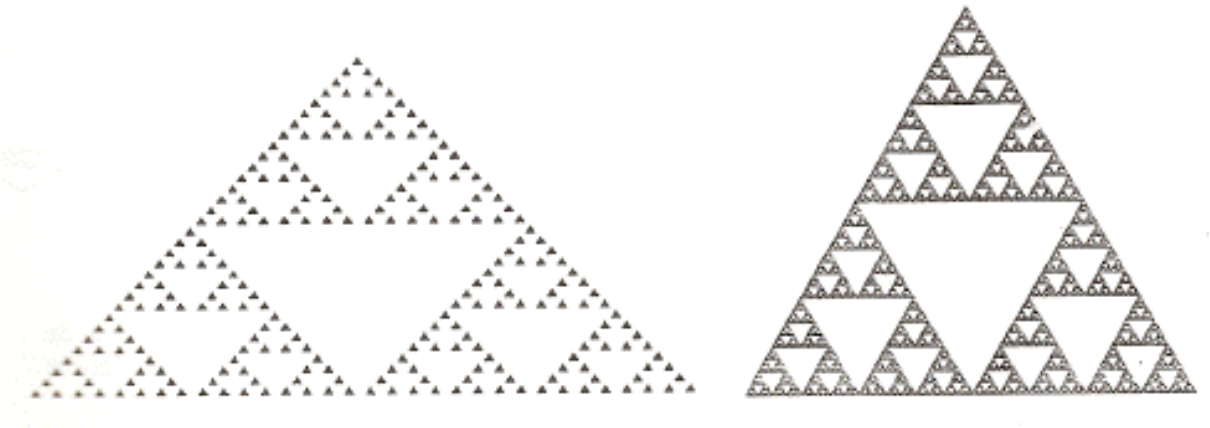

fig 2. Représentation de $\mathbf{Z}_3$

Avec $p = 5$, on peut construire un modèle plan de $\mathbf{Z}_5$ qui paramètre naturellement un fractal connexe bien connu (figure 3).

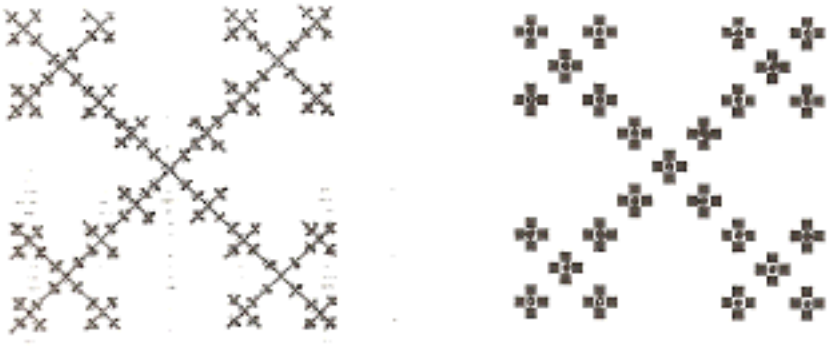

fig 3. Représentation de $\mathbf{Z}_5$

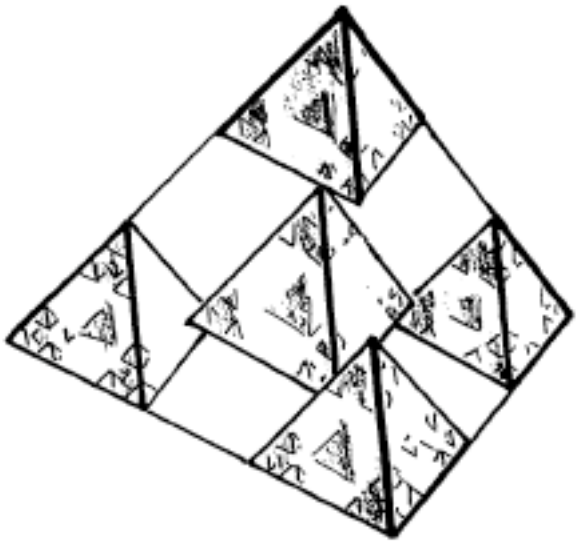

fig 4. Représentation de $\mathbf{Z}_5$

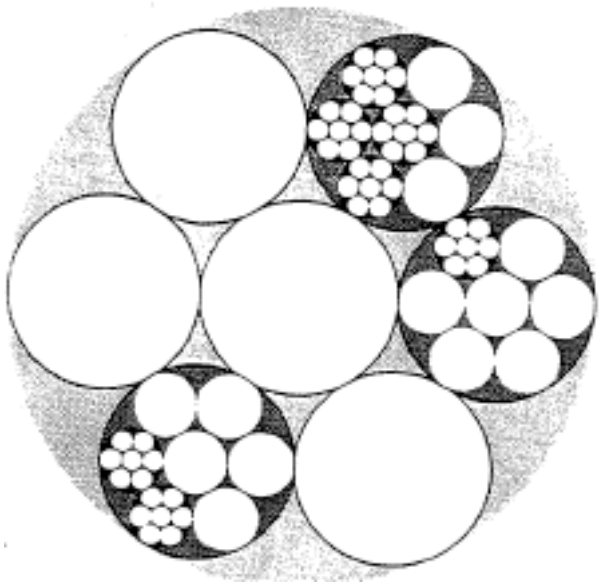

fig 5. Représentation de $\mathbf{Z}_7$

On peut aussi choisir des vecteurs v(k) dans l'espace de dimension trois et obtenir une famille d'applications de $\mathbf{Z}_5$ dans cet espace dont des modèles situés à l'intérieur d'un tétraèdre. On en

observera en particulier les faces (qui donnent des modèles de $\mathbf{Z}_3$) ainsi que les arêtes (qui donnent des modèles de $\mathbf{Z}_2$) (figure 4).

Finalement, pour $p = 7$, une image donnée dans le livre de Schikhof (figure 5) peut être insérée dans ce contexte. Il est même possible de la relever dans l'espace de dimension trois en fixant les 7 images v(k) ($0 \leq k \leq 6$) en les sommets d'un octaèdre (régulier) et en son centre (figure 6).

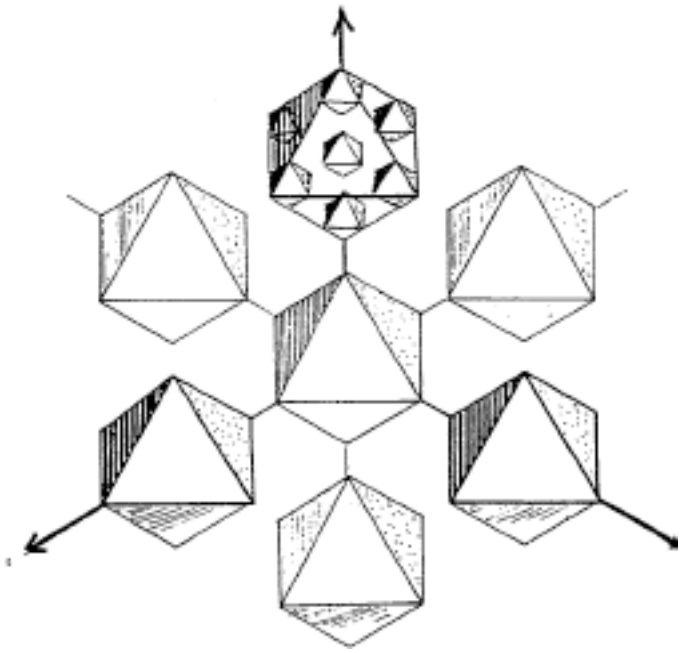

fig 6. Représentation de $\mathbf{Z}_7$

Références

Barsky D., Christol G. Les Nombres p-adiques. *La Recherche* **26** (1995), 766-771.

Cuculière R. A l'horizon de l'arithmétique décimale: les nombres 10-adiques issus des nombres automorphes de Gergonne et Lucas. *Pour la Science* (Juin 1986), 10-15.

Schikhof W. H. *Ultrametric Calculus: An introduction to p-adic Analysis.* Cambridge : University Press 1984, ISBN: 0- 521- 24234-7.

NDLR : L'auteur a publié ultérieurement à cet article un important ouvrage sur l'analyse p–adique

Robert Alain M. *A Course in p-adic Analysis*. Berlin : Springer-Verlag, Graduate Texts in Mathematics,198 (2000). ISBN 0-387-98669-3.