ARITHMÉTIQUE ET LOGIQUE

René CORI
MCF retraité, Université Paris Cité
IMJ-PRG / IREM
cori@math.univ-paris-diderot.fr

Résumé
La logique, c'est l'étude du langage et du raisonnement, base de toute activité mathématique. Elle est donc omniprésente dans notre enseignement.
Nous suivons ici sa trace en arithmétique où, comme ailleurs, elle est parfois bien visible mais souvent soigneusement cachée, comme on le constate dans tous les manuels scolaires. Le raisonnement par récurrence est un exemple emblématique. Nous nous intéressons aussi à l'énoncé du théorème de Bézout et aux questions de langage qu'il soulève. Mais la logique est avant tout présente dans les fondements de l'arithmétique, sujet dont les élèves (voire les professeurs !) n'entendent pratiquement jamais parler. Nous présentons donc ici les axiomes de Peano et nous évoquons les modèles de l'arithmétique. Nous terminons par un résultat très troublant qui mêle inextricablement arithmétique et logique : le théorème de Goodstein.

DÉDICACE

Je dédie cet exposé à la mémoire de Pierre Audin, décédé le 28 mai dernier, et à celle de ses parents, Josette et Maurice Audin. Pierre était un formidable promoteur des mathématiques. Il les a fait découvrir sous leur meilleur jour à des milliers de jeunes au Palais de la Découverte, où il a été pendant plus de vingt ans responsable de la médiation pour notre discipline.

Pierre Audin sous un portrait de son père Maurice

Mais Pierre a aussi agi sans relâche pour perpétuer la mémoire de Maurice Audin, enlevé, torturé et tué à Alger par l'armée française en 1957 alors que Pierre avait à peine plus d'un mois. Maurice Audin était un jeune mathématicien qui luttait pour l'indépendance de l'Algérie aux côtés de Josette, également professeure de mathématiques, disparue en 2019. Pierre a été avec sa mère au premier rang d'un long combat pour que soit dite toute la vérité sur le sort réservé à Maurice Audin. Le 18 septembre 2018, le président de la République s'est déplacé au domicile de Josette Audin pour reconnaître officiellement la responsabilité de l'État dans la disparition de Maurice Audin et dans l'instauration d'un système de torture pendant la guerre d'Algérie. Ce geste solennel d'Emmanuel Macron a été une étape décisive dans cette lutte pour la vérité, mais de nombreuses interrogations demeurent.

[https://www.association-audin.fr/6]

I - PROLOGUE : QU'EST-CE QU'UN NOMBRE PAIR ?

À cette question, une amie professeure des écoles a répondu : « C'est un nombre qui se termine par 0, 2, 4, 6 ou 8 », en s'étonnant de cette question, à laquelle elle n'imaginait pas d'autre réponse. J'ai voulu en savoir plus. J'ai obtenu la même réponse auprès de plusieurs autres professeures des écoles. Des collègues de l'IREM spécialisées dans l'enseignement primaire m'ont confirmé que c'était généralement cette définition qui était utilisée. Je suis alors allé consulter les textes officiels et les manuels scolaires. Le résultat est édifiant.

Dans l'ensemble des documents publiés par le ministère de l'Éducation nationale [voir l'annexe I] (programmes, attendus, outils d'évaluation, documents d'accompagnement), on trouve au total 55 occurrences de la chaîne de caractères « p a i r ». Mais pour 41 d'entre elles (soit 74,5%), le mot dans lequel elles figurent est pris dans un sens non mathématique (« présentation des travaux à ses pairs », « une paire de chaussettes » …). Je note incidemment que j'ai eu l'idée de dénombrer les occurrences des mots « compétences » et « connaissances » dans le programme du socle commun. Résultats respectifs : 46 et 58.

Dans les 14 manuels de l'enseignement primaire que j'ai consultés, la situation est radicalement différente. « pair » pris dans le sens « alter-ego » apparaît très peu, alors que les textes officiels en font un usage immodéré. Ici, sur 77 occurrences de « pair », 60 correspondent à la signification mathématique de ce mot. MAIS je n'ai RIEN trouvé qui puisse être considéré comme une définition de la notion de nombre pair !

Comment interpréter cela ?

Les enseignantes, et notamment les autrices de manuels scolaires, ont évidemment besoin de parler de la notion de nombre pair. Or elles ne trouvent rien dans les textes officiels qui puisse les guider, et rien dans les manuels qui soit une définition de cette notion. Elles se disent qu'un nombre pair, tout le monde finit par savoir ce que c'est ! Elles en parlent donc sans ambages, convaincues que, de même qu'Alphonse Allais n'avait pas besoin de caractères pour reconnaître un chou-fleur [voir l'annexe II], nous n'avons pas besoin de définition pour reconnaître un nombre pair.

Mais en maths, on aimerait bien quand même disposer d'une définition… Et heureusement, il y en a une !

« n est pair »

est synonyme de

« il existe au moins un entier k tel que $n = 2k$ »

ou encore (n'ayons pas peur !) de

$$(\exists k \in \mathbb{N}) \qquad n = 2k.$$

Comment passer d'une connaissance intuitive, installée très tôt, à la possibilité de formuler une telle définition ? C'est une question qui me semble fondamentale, mais à laquelle je ne prétends pas apporter de réponse.

II - RÉCURRENCE

1. Un théorème bien connu : ($\forall n \in \mathbb{N}$) ($n = 0$ ou $n = 1$)

J'appelle $P[n]$ la propriété ($n = 0$ ou $n = 1$), définie pour chaque entier naturel n, et je vais démontrer par récurrence la propriété ($\forall n \in \mathbb{N}$) $P[n]$.

Pour ce faire, consultons la notice :

Propriété **Principe de récurrence**
Si une propriété est vraie pour l'entier naturel n_0 et s'il est prouvé que lorsqu'elle est vraie pour un entier naturel p supérieur ou égal à n_0, elle est vraie aussi pour l'entier naturel $p+1$, alors elle est vraie pour tous les entiers naturels supérieurs ou égaux à n_0.

Une démonstration utilisant ce principe comporte **deux étapes**.
P(n) désigne une propriété qui dépend d'un entier naturel n et n_0 désigne un entier naturel. Pour démontrer que pour tout entier naturel $n \geqslant n_0$, P(n) est vraie, on procède comme ci-dessous.

- **Première étape :** on vérifie que P(n_0) est vraie, c'est l'**initialisation** de la récurrence.
- **Deuxième étape : l'hérédité.** On suppose ensuite qu'il existe un entier p tel que P(p) soit vraie, c'est l'hypothèse de récurrence et on démontre alors que P$(p+1)$ est vraie.

Éditions Bordas, collection Indice, TS programme 2012

Et suivons-la pas à pas :

Première étape (initialisation) : ici, $n_0 = 0$, et $P[n_0]$ est donc la propriété : ($0 = 0$ ou $0 = 1$). On doit pouvoir démontrer qu'elle est vraie… La première manche est gagnée !

Deuxième étape (hérédité) : La notice dit : « On suppose qu'il existe un entier p tel que $P[p]$ soit vraie ». Est-ce le cas ? On dirait que oui : il suffit de prendre $p = 0$. Mais alors $p + 1 = 1$ et on dirait bien que $P[1]$ est également vraie : ($1 = 0$ ou $1 = 1$).

Il en résulte que ($\forall n \in \mathbb{N}$) ($n = 0$ ou $n = 1$).

Victoire en deux manches !

2. Digression

On considère un polynôme Q à coefficients réels. Essayons de traduire dans un langage symbolique la propriété qui s'énonce de façon informelle comme suit :

« Si le polynôme Q a une racine réelle, alors elle est positive ou nulle. »

La tentation est grande d'écrire :

$$(\exists x \in \mathbb{R}) \ \ Q[x] = 0 \quad \Rightarrow \quad x \geq 0.$$

Mais on voit bien que cela ne va pas : la variable x est muette dans l'expression à gauche du symbole d'implication (elle est liée par le quantificateur existentiel), tandis qu'elle est libre à droite. La proposition ainsi écrite équivaut à $(\exists y \in \mathbb{R}) \ \ Q[y] = 0 \quad \Rightarrow \quad x$ ▯ 0. Contrairement à ce qu'on pourrait croire, la propriété que l'on voulait traduire formellement est une proposition universelle :

$$(\forall x \in \mathbb{R}) \ \ (Q[x] = 0 \ \Rightarrow \ x \geq 0).$$

La situation est tout à fait analogue à ce que nous venons de voir pour la récurrence. En effet la formulation adoptée pour l'hérédité dans le manuel cité conduit tout naturellement à écrire :

$$(\exists p \in \mathbb{N}) \ \ P[p] \quad \Rightarrow \quad P[p+1],$$

alors que la formulation correcte est :

$$(\forall p \in \mathbb{N}) \ \ (P[p] \ \Rightarrow \ P[p+1]).$$

Nous pouvons ainsi pointer ce qui ne va pas dans notre manuel :

Propriété **Principe de récurrence**
Si une propriété est vraie pour l'entier naturel n_0 et s'il est prouvé que lorsqu'elle est vraie pour un entier naturel p supérieur ou égal à n_0, elle est vraie aussi pour l'entier naturel $p+1$, alors elle est vraie pour tous les entiers naturels supérieurs ou égaux à n_0.

Une démonstration utilisant ce principe comporte **deux étapes**.
$\mathrm{P}(n)$ désigne une propriété qui dépend d'un entier naturel n et n_0 désigne un entier naturel. Pour démontrer que pour tout entier naturel $n \geqslant n_0$, $\mathrm{P}(n)$ est vraie, on procède comme ci-dessous.

- **Première étape :** on vérifie que $\mathrm{P}(n_0)$ est vraie, c'est l'**initialisation** de la récurrence.
- **Deuxième étape : l'hérédité.** On suppose ensuite qu'il existe un entier p tel que $\mathrm{P}(p)$ soit vraie, c'est l'hypothèse de récurrence et on démontre alors que $\mathrm{P}(p+1)$ est vraie.

3. Le principe de récurrence

Il s'exprime par la proposition suivante, qui est vraie :

$$(P[0] \quad \text{et} \quad (\forall k \in \mathbb{N}) \ (P[k] \ \Rightarrow \ P[k+1])) \quad \Rightarrow \quad (\forall n \in \mathbb{N}) \ \ P[n]$$

Bien entendu, il n'est pas question d'asséner cette formule à nos élèves[1] ! Nous voulons simplement faire observer qu'elle comporte deux quantificateurs universels et deux implications, ce qui explique peut-être les difficultés rencontrées par plusieurs élèves pour rédiger une preuve par récurrence…

[1]On peut par exemple leur dire que, pour démontrer qu'une propriété $P[n]$ est vraie pour tout entier n, il suffit, d'une part (initialisation) de démontrer que $P[0]$ est vraie, et d'autre part (hérédité) de démontrer que, **pour tout entier *k***, si $P[k]$ est vraie, alors $P[k+1]$ est également vraie.

III - À PROPOS DU THÉORÈME DE BÉZOUT

L'expression suivante nous est familière :

« n peut s'écrire sous la forme $au + bv$, avec u et v dans $\mathbb{Z}$. »

Les variables qui ont au moins une occurrence dans cette proposition sont n, a, u, b et v.

Mais de quels objets la proposition « parle »-t-elle ? De n, de a et de b. Mais ni de u, ni de v.

n, a et b y sont *libres* (ou *parlantes*). u et v y sont *liées* (ou *muettes*).

Pourquoi u et v sont-elles muettes ? Qui leur « coupe la parole » ? Il n'y a pas de symbole de quantificateur, ni de sommation ou d'intégration (ni d'autres signes qui ont pour effet de rendre des variables muettes).

Mais il y a une quantification existentielle implicite, et c'est le mot « avec » qui en témoigne. Pour expliciter la quantification, il conviendrait de formuler la proposition de la manière suivante :

« Il existe des entiers relatifs u et v tels que $n = au + bv$. »

Le discours mathématique fait un usage intensif du mot « avec ». Il cache la plupart du temps une quantification existentielle. Mais il peut y avoir des exceptions. Ainsi on peut rencontrer la phrase suivante : « On a $\ln(x^2) = 2\ln x$, avec $x \in \mathbb{R}$ et $x > 0$ », où il s'agit manifestement d'une quantification universelle implicite. Mais je ne recommande vraiment pas ce genre de formulation.

La proposition considérée nous parle donc des objets n, a et b. Lorsque des variables apparaissent dans une proposition, cette proposition exprime une propriété des objets désignés par celles des variables qui y sont LIBRES.

Le théorème de Bézout peut être énoncé de la manière suivante :

> Pour tout entier n, n est un multiple du pgcd de a et b si et seulement si n peut s'écrire sous la forme $au + bv$ avec u et v dans $\mathbb{Z}$.

Cette proposition nous parle uniquement des objets a et b. Qu'est-il arrivé à la variable n ? Elle a été rendue muette par la quantification universelle (« pour tout entier n »). On dit qu'elle a été *mutifiée*.

Voici une autre manière de dire la même chose (en précisant que la variable n est *astreinte*[2] à $\mathbb{N}$ et que les variables a, b, k, u et v sont astreintes à $\mathbb{Z}$) :

[2]On dit qu'une variable x est *astreinte* à un ensemble E lorsqu'elle est appelée à *prendre ses valeurs* dans E. Il y a une différence majeure entre « $x \in E$ » et « x est astreinte à E ». La première phrase nous parle d'un objet mathématique, nommé x (et nous dit que cet objet appartient à l'ensemble E), la deuxième nous parle d'un symbole du langage appelé à désigner des objets mathématiques. Il est important de faire la distinction entre un objet et le nom de cet objet. On retrouve ici la dualité classique signifié / signifiant. Le *signifié* est l'objet dont on parle, le *signifiant* est le nom qu'on lui donne. Le nom de l'objet relève de la syntaxe. L'objet lui-même relève de la sémantique. On connaît la devinette : *SANS MOI, PARIS SERAIT PRIS. QUI SUIS-JE* ?

$$\forall n \quad \left(\exists k \quad n = k \text{ pgcd}(a,b) \iff \exists u \; \exists v \quad n = au + bv\right)$$

Là aussi apparaît nettement la complexité de la structure de cette proposition, où il y a six variables et quatre quantificateurs (sur l'emplacement desquels il ne faut pas se tromper !), mais qui ne parle en fait que de deux objets (*a* et *b*). Mettons-nous à la place d'un élève de Terminale ! On me dira que justement, comme c'est compliqué, il vaut mieux ne pas expliciter tous les quantificateurs et dire les choses « avec les mots de tous les jours ». Je m'inscris évidemment en faux contre ce point de vue : cacher une difficulté ne peut pas faciliter la compréhension, bien au contraire. Attention ! Je ne dis pas qu'il faille donner la formule ci-dessus aux élèves ! Mais qu'une enseignante ait conscience de sa structure me semble vraiment utile.

Pour clore cette section, je reproduis un extrait d'un manuel du début des années 2010. Je n'en ai pas retrouvé la référence mais j'en garantis l'authenticité.

Propriétés

(1) a et b **sont** deux entiers naturels. **Si** a divise b, **alors** $\text{PGCD}(a; b) = a$.

(2) **Propriété fondamentale** : **Soit** a non nul tel que $a = bk + r$ **où** k est un entier. Alors $D(a) \cap D(b) = D(b) \cap D(r)$ et $\text{PGCD}(a; b) = \text{PGCD}(b; a - bk)$.

Les mots en bleu ont été soulignés par mes soins. Ils vous invitent à méditer sur le statuts des 4 variables qui apparaissent dans ce texte, sur les sorts respectifs réservés à *k* et à *r*, et à deviner où se nichent des quantifications. Le « Si …, alors ... » de la propriété (1) suggère évidemment une quantification universelle sur *a* et *b*. Hélas, la phrase précédente (on admirera qu'elle soit présentée par le titre comme une *propriété* !) indiquerait plutôt que *a* et *b* sont deux objets particuliers. Dans (2), le mot « Soit » est censé faire comprendre aux lectrices que ce qui va suivre vaut pour tout élément *a*. Mais l'autrice ne juge pas utile de nous renseigner sur *b* ! Si le mot « où » témoigne d'une quantification existentielle implicite sur la variable *k*, en revanche rien n'est dit, ni même suggéré, à propos de *r*.

IV - LES AXIOMES DE PEANO

Avec les axiomes de Peano et les deux sections suivantes, respectivement consacrées aux ensembles bien ordonnés et aux ordinaux, nous quittons les mathématiques de l'enseignement secondaire pour aborder des notions plus abstraites, qui ne font pas partie de la formation de base des enseignantes et enseignants de mathématiques. Nous nous permettons de le faire pour deux raisons. La première est que ces notions interviennent dans la septième et dernière section, où est présenté le théorème de Goodstein. Cet énoncé et les objets qui y interviennent sont plutôt élémentaires, puisqu'il s'agit de définir et d'étudier une suite de nombres entiers. Le résultat est très spectaculaire et est accessible à des élèves de Terminale. C'est la démonstration du théorème qui nécessite de faire un détour par la théorie des ordinaux. Et il faut avoir une idée de ce qu'est une théorie axiomatique pour comprendre le statut très spécial du théorème de Goodstein. La deuxième raison pour laquelle nous avons voulu présenter ces notions plus avancées, c'est qu'elles nous semblent dignes de figurer dans le bagage culturel de toute personne qui enseigne les mathématiques ou réfléchit à leur enseignement. Quoi de plus basique en effet que les nombres entiers et les

Pour trouver la bonne réponse (la lettre « A »), il faut renoncer à l'interprétation spontanée (*Sans moi, la ville de Paris serait prise*) et considérer que PARIS est ici le nom de la ville (le signifiant) et non la ville elle-même (le signifié).

fondements des mathématiques ? Si vous avez des réticences à aborder directement les considérations abstraites qui suivent, vous pouvez commencer par aller découvrir à la section VII le théorème de Goodstein. Il est probable qu'il vous fascinera et vous donnera envie de revenir en arrière pour en savoir plus.

Pour un exposé des notions abordées ici, on peut consulter [2] *et* [3].

1. Le langage de l'arithmétique et les axiomes de Peano

Les axiomes de Peano sont des propositions, écrites dans un langage en respectant des règles syntaxiques simples (ce n'est pas le lieu de les expliciter ici), et qui sont vérifiées dans l'ensemble $\mathbb{N}$ des entiers naturels qui nous est familier, celui dont nous avons une connaissance intuitive, sans laquelle il n'est pas possible de faire des mathématiques. L'idée serait d'avoir un ensemble d'axiomes duquel on puisse déduire *toutes* les propriétés vraies dans $\mathbb{N}$. Hélas il faudra renoncer à cet objectif. Nous reviendrons sur ce point.

Le *langage de l'arithmétique* est constitué, d'une part de symboles dits *logiques* (variables, connecteurs, quantificateurs, parenthèses), et d'autre part des symboles spécifiques suivants :

- le symbole d'égalité : =
- un **symbole de fonction unaire** : S (pour la fonction successeur)
- deux **symboles de fonction binaires** : + et × (pour l'addition et la multiplication)
- un symbole de constante : 0 (pour le nombre 0)

L'*arithmétique du premier ordre* est la théorie constituée des axiomes suivants (de Peano) :

- $\forall x\ \forall y\ \ (Sx = Sy \Longrightarrow x = y)$
- $\forall x\ \ x + 0 = x$
- $\forall x\ \ x \times 0 = 0$
- $\forall x\ \ (x \neq 0 \Longleftrightarrow \exists y\ x = Sy)$
- $\forall x\ \forall y\ \ x + Sy = S(x + y)$
- $\forall x\ \forall y\ \ x \times Sy = (x \times y) + x$
- $\left\{ \Big(F[0] \text{ et } \forall x\ (F[x] \Longrightarrow F[Sx])\Big) \Longrightarrow \forall x\ F[x] \ \Big|\ F \text{ est une proposition} \right\}$

Remarquez que le dernier item n'est pas un axiome unique mais un ensemble (infini) d'axiomes : il y en a un pour chaque proposition F écrite dans le langage. On appelle cet ensemble le *schéma de récurrence*.

2. Les modèles de l'arithmétique

Un modèle de l'arithmétique, c'est un ensemble M muni d'une fonction unaire S, de deux fonctions binaires + et × et d'un élément distingué 0 qui vérifie les axiomes de Peano.

Notre ensemble $\mathbb{N}$ avec sa structure habituelle est un modèle de ces axiomes, mais ce n'est sûrement pas le seul. Il y a en effet des théorèmes de logique qui garantissent l'existence de bien d'autres modèles de l'arithmétique de Peano, non isomorphes à $\mathbb{N}$, y compris des modèles non dénombrables !

L'existence d'un modèle fait que l'arithmétique de Peano est une *théorie cohérente*. (Le mot « théorie » désigne simplement un ensemble de propositions sans variables libres.)

De plus, l'arithmétique de Peano est une théorie incomplète. Cela signifie qu'il existe des propositions (du langage) qui ne peuvent être ni démontrées ni réfutées à partir de ces axiomes. De telles propositions sont vraies dans certains des modèles et fausses dans les autres. Il y a en particulier des propositions qui sont vraies dans $\mathbb{N}$ mais qui ne peuvent pas être démontrées à partir des axiomes de Peano. C'est en exhibant une telle proposition que Kurt Gödel a démontré vers 1930 que l'arithmétique est incomplète. Mais la proposition qui a servi à Gödel a un défaut majeur : même si elle est relative aux nombres entiers, elle est très éloignée de l'intuition qui nous guide lorsque nous faisons de l'arithmétique et il est vraiment difficile de l'appréhender. À tel point que certaines personnes y voient un objet pathologique, étranger au « vrai monde » des mathématiques. Cette objection tombe avec le théorème de Goodstein : il s'agit d'une proposition arithmétique qui parle en des termes usuels d'objets familiers. Elle n'est pas prouvable à partir des axiomes de Peano mais elle est vraie dans $\mathbb{N}$. Nous reviendrons à la section VII sur cette affirmation, mais pour en mieux comprendre la signification, il faut renoncer à l'idée qu'il n'y aurait qu'un unique modèle de la théorie de Peano et faire connaissance avec les modèles non-standard, que nous présentons maintenant.

Dans tout modèle de l'arithmétique de Peano, il y a des éléments (des entiers, donc) qui représentent nos entiers à nous, ceux avec lesquels nous faisons des mathématiques, appelons-les entiers intuitifs. Il s'agit de l'élément 0, de son image par la fonction successeur (c'est-à-dire par la fonction qui est l'interprétation du symbole S), du successeur de 0, etc. :

$$0,\ S(0)\ (\text{noté } 1),\ S(S(0)) = S^2(0)\ (\text{noté } 2),\ S^3(0)\ (\text{noté } 3),\ \ldots,\ S^n(0)\ (\text{noté } n),\ \ldots$$

[*La notation* $S^n(0)$ *est définie par récurrence :* $S^0(0) = 0$ *et, pour tout entier (intuitif !)* k, $S^{k+1}(0) = S(S^k(0))$.]

Mais attention à ce « etc. » et à ces points de suspension : les entiers utilisés ici (comme exposants de la fonction S) sont nos entiers intuitifs, et rien ne nous garantit que les images itérées de 0 par la fonction successeur vont constituer tous les éléments du modèle. Il y a même un théorème qui affirme qu'il existe des modèles contenant des éléments autres que ces successeurs itérés de 0. Les successeurs itérés de 0, nous les appelons *entiers standard*. L'itération, nous la faisons avec nos entiers intuitifs. Si elle ne suffit pas à épuiser le modèle, c'est qu'il contient d'autres éléments : les entiers non-standard.

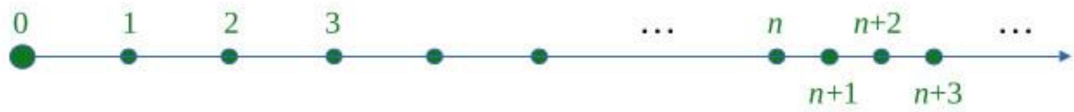
Les modèles où il y a des entiers non-standard sont appelés modèles non-standard. Notre ensemble $\mathbb{N}$ des entiers intuitifs, muni des opérations usuelles S, +, x, 0, est un modèle standard, et même LE modèle standard, car il est unique à isomorphisme près. (Deux modèles sont isomorphes s'il existe entre eux une bijection compatible avec les interprétations respectives des symboles S, +, x, 0.) En revanche, il y a beaucoup de modèles non-standard, et il y en a dans toutes les cardinalités infinies.

V - ENSEMBLES BIEN ORDONNÉS

Pour cette section et la suivante (ordinaux), on peut se référer à [2], [3] et [7].

Un ensemble E muni d'une relation d'ordre $\leqslant$ est bien ordonné si toute partie non vide de E admet un plus petit élément pour l'ordre $\leqslant$.

L'exemple emblématique de bon ordre est fourni par l'ensemble $\mathbb{N}$ des entiers naturels avec son ordre usuel :

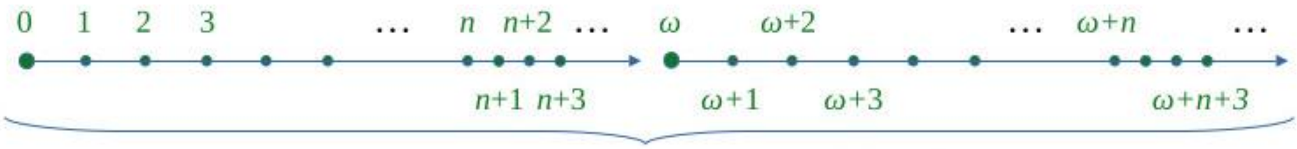


On a encore un ensemble bien ordonné en adjoignant aux entiers un élément qui soit plus grand que tous les autres :

… ou plusieurs :

Donnons des noms à ces nouveaux éléments :

On peut aussi mettre bout à bout deux exemplaires de l'ensemble des entiers :



$\omega + \omega = \omega \times 2$ (ω répété 2 fois)

… ou trois :

$\omega+\omega+\omega = \omega\times 3$ (ω répété 3 fois)

… ou un grand nombre :

$\omega \times \omega$ (ω répété ω fois)

Propriété fondamentale des ensembles bien ordonnés :

> *Étant donné deux ensembles bien ordonnés quelconques, il y en a toujours au moins un des deux qui est isomorphe à un segment initial de l'autre.*

On peut esquisser une démonstration. Soit A et B deux ensembles bien ordonnés. Si l'un d'eux est vide, il est lui-même un segment initial de l'autre. S'ils sont tous les deux non vides, chacun est une partie non vide de lui-même et a donc à ce titre un plus petit élément, disons a_0 pou A et b_0 pour B. Si A n'a pas d'autre élément que a_0, l'application qui envoie a_0 sur b_0 est un isomorphisme de A sur un segment initial de B. Situation symétrique si c'est B qui a un seul élément. Si ni A ni B ne sont réduits à un élément, leurs sous-ensembles obtenus en ôtant a_0 de A et b_0 de B sont non vides, et ont donc chacun un plus petit élément, disons a_1 pou A et b_1 pour B. Si A n'a pas d'autre élément que a_0 et a_1, l'application qui envoie a_0 sur b_0 et a_1 sur b_1 est un isomorphisme de A sur un segment initial de B. Situation symétrique si c'est B qui n'a que deux éléments. On continue ainsi tant qu'il reste à la fois des éléments dans A et dans B, et on finira bien par épuiser les éléments de l'un ou de l'autre de ces ensembles. Cette dernière phrase est évidemment une escroquerie : rien ne permet d'affirmer que l'on arrivera à passer en revue tous les éléments de l'un des deux ensembles. Déjà, si on parvenait à le faire, cela signifierait que l'ensemble en question (disons que ce soit A) est dénombrable (on aurait énuméré ses éléments sous la forme d'une suite a_0, a_1 , …, a_k, …). Le raisonnement ne tient donc pas si A et B sont tous les deux infinis et non dénombrables. Mais il ne tient pas non plus lorsque l'un des deux est dénombrable : supposons en effet que A soit l'ensemble $\omega + \omega$ (obtenu en mettant bout à bout deux exemplaires de l'ensemble des entiers naturels) ; on ne pourra jamais atteindre avec notre procédé les éléments du deuxième exemplaire. La démonstration n'est donc pas aussi simple que ça, mais le résultat est bien vrai (à condition d'admettre l'axiome du choix ; mais nous n'en dirons pas plus à ce sujet).

Il en résulte que les *classes d'isomorphisme* des ensembles bien ordonnés sont deux à deux comparables. Il y a un ordre total sur ces classes. Et cet ordre est même un bon ordre !

VI - LES ORDINAUX

1. Présentation et premières propriétés

Nous ne donnerons pas de définition des ordinaux : cela relève de la théorie des ensembles et sortirait du cadre de cet exposé. Contentons-nous de dire que les ordinaux sont des représentants particuliers des classes d'isomorphisme d'ensembles bien ordonnés dont nous venons de parler.

Il y a d'abord les ordinaux finis, que l'on identifie aux entiers naturels. Certains d'entre eux (mais pas forcément tous ! il y peut y avoir des ordinaux finis non-standard) s'obtiennent de la façon suivante :

$$
\begin{aligned}
&\varnothing = 0\\
&\{\varnothing\} = 1\\
&\{\varnothing, \{\varnothing\}\} = \{0, 1\} = 2\\
&\Big\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\Big\} = \{0, 1, 2\} = 3\\
&\qquad\qquad \vdots
\end{aligned}
$$

Le premier ordinal est donc l'ensemble vide (identifié à l'entier 0).

Chaque ordinal est égal à l'ensemble de ceux qui le précèdent.

Pour tout ordinal a, l'ensemble $a \cup \{a\}$ est aussi un ordinal, appelé successeur de α et noté $S(a)$ ou $a + 1$.

Voici quelques propriétés des ordinaux :

Tous les éléments d'un ordinal sont des ordinaux.

Quels que soient les ordinaux α et β, si $\beta \in \alpha$, alors tous les éléments de β appartiennent aussi à α.

Il y a trois sortes d'ordinaux :

- 0 (l'ensemble vide) ;
- les ordinaux successeurs (un ordinal α est successeur s'il existe un ordinal β tel que $\alpha = \beta \cup \{\beta\}$) ;
- les ordinaux limites (ce sont tous les autres).

L'ordre sur les ordinaux est très simple :

Quels que soient les ordinaux α et β, on a

- $\alpha < \beta$ si et seulement si $\alpha \in \beta$ (l'ordre strict est l'appartenance) ;
- $\alpha \leqslant \beta$ si et seulement si $\alpha \subseteq \beta$ (l'ordre large est l'inclusion).

L'ordinal ω est le premier ordinal non fini.

ω est l'ensemble des ordinaux finis.

C'est aussi le premier ordinal limite.

- Chaque ordinal est un ensemble bien ordonné.
- La classe de tous les ordinaux est bien ordonnée.
- Toute classe non vide d'ordinaux a un plus petit élément.

► Il n'existe pas de suite d'ordinaux strictement décroissante.

Cette dernière propriété est cruciale. Nous y reviendrons.

2. Arithmétique ordinale

On définit trois opérations binaires sur les ordinaux : l'*addition*, la *multiplication* et l'*exponentiation*. Elles correspondent à des opérations sur les ensembles bien ordonnés, qui « passent au quotient », c'est-à-dire sont compatibles avec la relation d'isomorphisme entre ensembles bien ordonnés.

Étant donné deux ordinaux α et β, nous allons définir la somme $\alpha + \beta$, le produit $\alpha \times \beta$ et l'exponentielle α^{β}.

2.1. Addition

$\alpha + \beta$ est l'ordinal représentant l'ensemble bien ordonné obtenu en mettant « bout à bout » l'ensemble bien ordonné α suivi de l'ensemble bien ordonné β.

Formellement, on prend l'ensemble $(\{0\} \times \alpha) \cup (\{1\} \times \beta)$, avec l'ordre lexicographique.

On constate immédiatement que cette addition n'est pas commutative. Par exemple, $\omega + 1$ est l'ordinal successeur de ω, tandis que $1 + \omega$ est égal à ω.

En revanche, l'addition des ordinaux est associative.

2.2. Multiplication

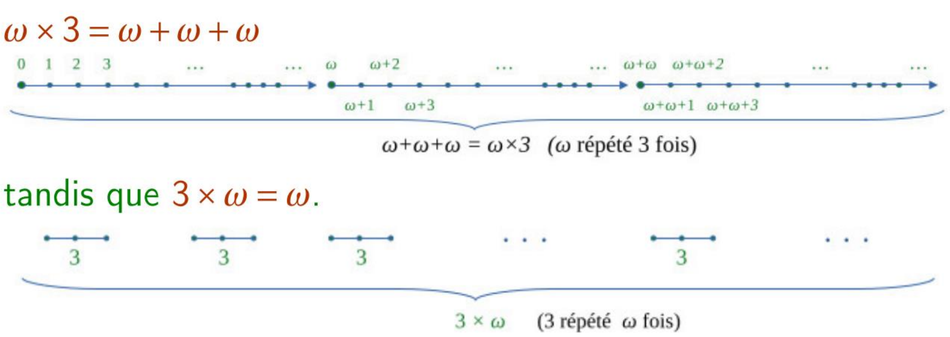
$\alpha \times \beta$ est l'ordinal représentant l'ensemble bien ordonné obtenu en munissant le produit cartésien $\alpha \times \beta$ de l'ordre anti-lexicographique :

$$(\gamma, \delta) \leqslant (\mu, \nu) \text{ si et seulement si } [\delta < \nu \text{ ou } (\delta = \nu \text{ et } \gamma \leqslant \mu)].$$

(On peut aussi prendre le produit cartésien $\beta \times \alpha$ avec l'ordre lexicographique.)

Intuitivement, $\alpha \times \beta$, c'est l'ordinal α « répété β fois ».

Là encore, il n'y a clairement pas commutativité :



Mais, comme l'addition, la multiplication des ordinaux est associative.

Nous nous permettrons, comme cela se fait toujours pour les multiplications usuelles, de noter indifféremment « $\alpha \times \beta$ » ou « $\alpha.\beta$ ».

2.3. *Exponentiation*

Pour définir l'ordinal α^β, on considère l'ensemble $\alpha^{(\beta)}$ des applications de β dans α dont le *support* est fini. Le support d'une application f de β dans α est l'ensemble des éléments de β en lesquels f ne prend pas la valeur 0. Sur cet ensemble $\alpha^{(\beta)}$, on définit l'ordre suivant :

> f est strictement inférieure à g s'il existe un ordinal $\gamma \in \beta$ tel que $f(\gamma) < g(\gamma)$ et, pour tout ordinal $\delta > \gamma$ dans β, $f(\delta) = g(\delta)$.

On obtient ainsi un ensemble bien ordonné dont l'ordinal est, par définition, α^β.

Pour tout ordinal $\alpha \neq 0$, il existe un nombre fini d'entiers non nuls k_1, k_2, …, k_n, et un même nombre d'ordinaux α_1, α_2, …, α_n vérifiant

Attention : l'exponentiation des ordinaux n'a rien à voir avec celle des cardinaux. Ainsi, l'ordinal 2^ω est dénombrable. Et il est tellement dénombrable qu'il est égal à ω…

2.4. *Fort heureusement...*

Appliquées aux seuls ordinaux finis, les trois opérations que nous venons de définir ne produisent que des ordinaux finis, et elles coïncident parfaitement avec celles de l'arithmétique de notre enfance : addition, multiplication et exponentiation des entiers.

3. Théorème de la forme normale de Cantor

Pour tout ordinal $\alpha \neq 0$, il existe un nombre fini d'entiers non nuls k_1, k_2, …, k_n, et un même nombre d'ordinaux α_1, α_2, …, α_n vérifiant

$$\alpha_1 > \alpha_2 > \ldots > \alpha_n,$$

tels que

$$\alpha = \omega^{\alpha_1}.k_1 + \omega^{\alpha_2}.k_2 + \ldots + \omega^{\alpha_n}.k_n.$$

Cette décomposition est unique et s'appelle la forme normale de Cantor de l'ordinal α.

Nous ne démontrons pas ce résultat. Voir [3] *pour plus de détails.*

On pourrait appeler cette décomposition l'*écriture de l'ordinal α en base ω*, par analogie avec l'écriture des entiers non nuls dans une base donnée.

VII - LE THÉORÈME DE GOODSTEIN

1. Écritures d'un entier naturel non nul en base 2 et en base 2 étendue

Partons de votre entier préféré : 89. Comme tous ses confrères, il s'écrit comme somme de puissances de 2 :

$$89 = 64+16+8+1 = 2^6\cdot 1+2^5\cdot 0+2^4\cdot 1+2^3\cdot 1+2^2\cdot 0+2^1\cdot 0+2^0\cdot 1$$

Cette décomposition est unique et on le représente donc ainsi dans cette base : $89 = \overline{1011001}_{[2]}$.

Mais les exposants, eux, sont écrits en base 10.

Écrivons-les à leur tour en base 2 puis itérons ce procédé tant que c'est nécessaire, pour ne plus avoir que des puissances de 2.

On obtient ainsi l'écriture de l'entier 89 **en base 2 étendue** :

$$89 = 2^{2^1+2^{2^1}}\cdot 1+2^{2^0+2^{2^1}}\cdot 0+2^{2^{2^1}}\cdot 1+2^{2^0+2^1}\cdot 1+2^{2^1}\cdot 0+2^1\cdot 0+2^0\cdot 1$$

[*Remplacer les* 1 *par* 2^0 *ne changerait rien pour ce qu'on va faire ensuite*.]

2. Écriture d'un entier non nul en base *k* étendue et changement de base

On définit évidemment de la même manière, pour tout entier $n \geq 1$ et tout entier $k \geq 2$, le développement de n en base k étendue.

Soit p et q deux entiers naturels strictement supérieurs à 1. Pour tout entier naturel n, on appelle $T_{p,q}(n)$ l'entier obtenu en remplaçant toutes les occurrences de p par q dans l'écriture de n en base p étendue.

Ainsi, de l'écriture de 89 en base 2 étendue, on déduit que :

$$T_{2,3}(89) = 3^{3^1+3^{3^1}}\cdot 1+3^{3^0+3^{3^1}}\cdot 0+3^{3^{3^1}}\cdot 1+3^{3^0+3^1}\cdot 1+3^{3^1}\cdot 0+3^1\cdot 0+3^0\cdot 1$$

(*base* 3 *étendue*)

Le calcul donne :

$$T_{2,3}(89) = 213\ 516\ 729\ 579\ 718$$

3. Définition des suites de Goodstein

L'algorithme suivant définit la suite de Goodstein associée à un entier $n \geq 1$:

Voici l'algorithme qui définit la **suite de Goodstein associée à un entier** n :

- Le premier terme est $G_0 = n$. Dans notre exemple, $G_0 = 89$.
- On écrit le développement de G_0 en base 2 étendue.

  $89 = 2^{2^1+2^{2^1}} \cdot 1 + 2^{2^0+2^{2^1}} \cdot 0 + 2^{2^{2^1}} \cdot 1 + 2^{2^0+2^1} \cdot 1 + 2^{2^1} \cdot 0 + 2^1 \cdot 0 + 2^0 \cdot 1$
- On lui applique la fonction $T_{2,3}$.

  $T_{2,3}(G_0) = 3^{3^1+3^{3^1}} \cdot 1 + 3^{3^0+3^{3^1}} \cdot 0 + 3^{3^{3^1}} \cdot 1 + 3^{3^0+3^1} \cdot 1 + 3^{3^1} \cdot 0 + 3^1 \cdot 0 + 3^0 \cdot 1$
- **On soustrait 1 au résultat obtenu**, ce qui fournit le deuxième terme de la suite : $G_1 = T_{2,3}(G_0) - 1 = 213\,516\,729\,579\,717$.
- On écrit le développement de G_1 en base 3 étendue.

  $G_1 = 3^{3^1+3^{3^1}} \cdot 1 + 3^{3^0+3^{3^1}} \cdot 0 + 3^{3^{3^1}} \cdot 1 + 3^{3^0+3^1} \cdot 1 + 3^{3^1} \cdot 0 + 3^1 \cdot 0 + 3^0 \cdot 0$
- On lui applique la fonction $T_{3,4}$.

  $T_{3,4}(G_1) = 4^{4^1+4^{4^1}} \cdot 1 + 4^{4^0+4^{4^1}} \cdot 0 + 4^{4^{4^1}} \cdot 1 + 4^{4^0+4^1} \cdot 1 + 4^{4^1} \cdot 0 + 4^1 \cdot 0 + 4^0 \cdot 0$
- **On soustrait 1 au résultat obtenu**, ce qui fournit le terme suivant de la suite : $G_2 = T_{3,4}(G_1) - 1$.
- On écrit le développement de G_2 en base 4 étendue.
- $G_2 = 4^{4^1+4^{4^1}} \cdot 1 + 4^{4^0+4^{4^1}} \cdot 0 + 4^{4^{4^1}} \cdot 1 + 4^{4^1} \cdot 3 + 4^3 \cdot 3 + 4^2 \cdot 3 + 4^1 \cdot 3 + 4^0 \cdot 3$
- *et on continue* ***tant que*** G_k ***n'est pas nul***.

Voici donc les tout premiers termes de la suite de Goodstein partant de 89 :

$$
\begin{aligned}
G_0 &= \boxed{89} \\
&= 2^{2^1+2^{2^1}} \cdot 1 + 2^{2^0+2^{2^1}} \cdot 0 + 2^{2^{2^1}} \cdot 1 + 2^{2^0+2^1} \cdot 1 + 2^{2^1} \cdot 0 + 2^1 \cdot 0 + 2^0 \cdot 1 \\
T_{2,3}(89) &= 3^{3^1+3^{3^1}} \cdot 1 + 3^{3^0+3^{3^1}} \cdot 0 + 3^{3^{3^1}} \cdot 1 + 3^{3^0+3^1} \cdot 1 + 3^{3^1} \cdot 0 + 3^1 \cdot 0 + 3^0 \cdot 1 \\
&= 213\,516\,729\,579\,718 \\
G_1 &= T_{2,3}(89) - 1 = \boxed{213\,516\,729\,579\,717} \\
T_{3,4}(G_1) &= 4^{4^1+4^{4^1}} \cdot 1 + 4^{4^0+4^{4^1}} \cdot 0 + 4^{4^{4^1}} \cdot 1 + 4^{4^0+4^1} \cdot 1 + 4^{4^1} \cdot 0 + 4^1 \cdot 0 + 4^0 \cdot 0 \\
G_2 &= T_{3,4}(G_1) - 1 \\
&= 3445806637995247454590524424538902454762197015 8 \\
&\quad 9224509807495529103649335572890157303808169462 8 \\
&\quad 8941809163381875539269150694147478826702684762 3 \\
&\quad 3447794563613695
\end{aligned}
$$

C'est un nombre à 157 chiffres : $10^{156} \leqslant G_2 < 10^{157}$

Donnons la définition générale, par récurrence, de la suite de Goodstein $(G_k)_{k \in \mathbb{N}}$ associée à un entier n ≥ 1

$$
\begin{aligned}
&G_0 = n,\\
&G_1 = T_{2,3}(n) - 1,\\
&\text{et pour tout } k \in \mathbb{N},\\
&G_{k+1} = \begin{cases} T_{k+2,k+3}(G_k) - 1 & \text{si } G_k \neq 0 \\ 0 & \text{si } G_k = 0 \end{cases}
\end{aligned}
$$

Et donc, pour $n = 89$, on obtient :

$$
\begin{aligned}
&G_0 = 89,\\
&G_1 = T_{2,3}(89) - 1 = 205\,891\,132\,094\,757,\\
&G_2 = T_{3,4}(205\,891\,132\,094\,757) - 1,\\
&\dots
\end{aligned}
$$

On s'attend à ce que ces suites aient une croissance vertigineuse et tendent vers l'infini. Et pourtant…

4. Théorème de Goodstein

Toute suite de Goodstein stationne à la valeur 0.

Le logicien britannique *Reuben Louis Goodstein* a démontré cet étonnant résultat en 1944. Comment lui est venue l'idée d'étudier une suite aussi étrange ? Mystère ! [5]

La démonstration (voir [3]) utilise la théorie des ordinaux, et se fait donc dans le cadre de la théorie des ensembles, qui est strictement plus forte que l'arithmétique de Peano[3]. Or l'énoncé du théorème se ramène à une proposition du langage de l'arithmétique. En 1982, les logiciens *Jeff Paris* et *Laurence Kirby* ont prouvé ([6]) que cette proposition arithmétique n'est pas démontrable avec les seuls axiomes de Peano. On a ainsi un exemple de proposition « ordinaire » qui est vraie dans certains modèles de l'arithmétique (notamment dans notre modèle standard des entiers naturels) et fausse dans d'autres modèles[4]. C'est dans ce type de situation qu'on parle de propositions « vraies mais non démontrables ».

Nous allons donner pour terminer une idée de la preuve du théorème.

[3]Ce qui signifie que toute proposition arithmétique prouvable dans Peano l'est aussi dans la théorie des ensembles, mais qu'il existe des propositions arithmétiques prouvables dans la théorie des ensembles mais pas dans Peano.

[4]Mais décrire des modèles où elle est fausse est une tout autre histoire !

Soit p un entier strictement supérieur à 1. Pour tout entier naturel $n \geq 1$, on appelle $T_{p,\omega}(n)$ l'ordinal obtenu en remplaçant toutes les occurrences de p par ω dans l'écriture de n en base p étendue. La fonction $T_{p,\omega}$ est donc une application de $\mathbb{N}$ dans la classe des ordinaux.

Ainsi,

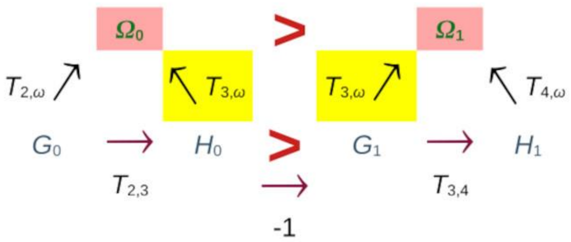
$$T_{2,\omega}(89) = \omega^{\omega^1+\omega^{\omega^1}}\cdot 1+\omega^{\omega^0+\omega^{\omega^1}}\cdot 0+\omega^{\omega^{\omega^1}}\cdot 1+\omega^{\omega^0+\omega^1}\cdot 1+\omega^{\omega^1}\cdot 0+\omega^1\cdot 0+\omega^0\cdot 1$$

Remarque importante : Quels que soient les entiers $p > 1$ et $q > 1$, $T_{p,\omega} = T_{q,\omega} \circ T_{p,q}$, c'est-à-dire que, pour tout entier $n \geq 1$, $T_{p,\omega}(n) = T_{q,\omega}(T_{p,q}(n))$. Autrement dit, il revient au même de remplacer toutes les occurrences de p par q, puis toutes celles de q par ω, que de remplacer directement toutes les occurrences de p par ω.

Nous admettons le résultat suivant (voir [3], 4.2.5, page 81) :

Lemme : *Pour tout entier $p > 1$, la fonction $T_{p,\omega}$ est strictement croissante.*

Posons, pour chaque entier naturel k, $H_k = T_{k+2,k+3}(G_k)$ et $\Omega_k = T_{k+2,\omega}(G_k)$.



Comme la fonction $T_{3,\omega}$ est strictement croissante, on a

$$\Omega_0 = T_{2,\omega}(G_0) = T_{3,\omega}(T_{2,3}(G_0)) = T_{3,\omega}(H_0) > T_{3,\omega}(H_0-1) = T_{3,\omega}(G_1) = \Omega_1$$

De même,

$$\Omega_1 = T_{4,\omega}(T_{3,4}(G_1)) = T_{4,\omega}(H_1) > T_{4,\omega}(H_1-1) = T_{4,\omega}(G_2) =$$
$$\Omega_2 = T_{5,\omega}(T_{4,5}(G_2)) = T_{5,\omega}(H_2) > T_{5,\omega}(H_2-1) = T_{5,\omega}(G_3) = \Omega_3 \ \dots$$

Tant que l'entier G_k n'est pas nul, on peut définir l'**ordinal** Ω_k.

Si aucun des G_k n'était nul, on aurait une suite infinie strictement décroissante d'ordinaux : $(\Omega_k)_{k\in\mathbb{N}}$. Cela est impossible.

La suite de Goodstein finira donc nécessairement par s'annuler.

(*Sur le théorème de Goodstein, on trouve d'excellents exposés destinés à un large public dans l'article* [1], *et la vidéo* [4].)

VIII - BIBLIOGRAPHIE

[1] Artigue, M., Arzarello, F. et Epp, S. *Les suites de Goodstein ou la puissance du détour par l'infini*, Projet Klein, 2012.
http://blog.kleinproject.org/?p=722&lang=fr

[2] Cori, R. et Lascar, D. *Logique mathématique, cours et exercices* (2 tomes). Masson, collection Axiomes, 1992, Dunod, 2004.

[3] Dehornoy, P. *La théorie des ensembles*. Calvage et Mounet, collection Tableau noir, 2017, 2e éd. 2018.

[4] Dehornoy, P. *Georg Cantor et les infinis*. Société mathématique de France, Cycle de conférences « *Un texte un mathématicien* », 2009.
https://www.youtube.com/watch?v=cf15qYStKbA

[5] Goodstein, R. L. On the restricted ordinal theorem. *The Journal of Symbolic Logic*, 9, 33-41, 1944.

[6] Kirby, L.A.S. et Paris, J. B. Accessible Independant Results for Peano's Arithmetic. *Bulletin of the London Mathematical Society*, 14, 285–293, 1982.

[7] Krivine, J.-L. *Théorie des ensembles*, Cassini, 1998/2007.

ANNEXE 1 : DANS LES TEXTES OFFICIELS

La chaîne de caractères pair dans les documents du ministère de l'Éducation nationale.

Document	Nb occ	Math	Autre
Programme du cycle 2	19	**0**	19
Pour enseigner les nombres, le calcul et la résolution de problèmes au CP	4	2	2
Le calcul aux cycles 2 et 3	0	0	0
Le calcul en ligne au cycle 2	0	0	0
Doubles et moitiés	0	0	0
Programme du cycle 3	0	**0**	0
Résolution de problèmes - Cours moyen	6	1	5
Résolution de problèmes - Collège	15	6	9
Programme du cycle 4	6	**0**	6
Attendus de fin d'année 5ème	3	3	0
Attendus de fin d'année 4ème	2	2	0
Attendus de fin d'année 3ème	0	0	0
Socle commun	0	**0**	0
Évaluation des niveaux de maîtrise du socle (21 fiches pour Nombres et calculs)	0	0	0
	55	14	41

ANNEXE 2 : UN TEXTE D'ALPHONSE ALLAIS (1854-1905)

Extrait du conte Pour se donner une contenance (*Littoralement*, Éditions Arcanes, 1952)

Un jour, j'arrive à l'école – rara avis – pour passer un examen.

Parmi les examinateurs, j'aperçois qui ? Vous avez deviné : le vieux petit monsieur grincheux, chargé de sonder mes connaissances botaniques.

Oh ! combien rudimentaires, mes notions.

Le vieux petit monsieur grincheux m'offrit une plante médicinale, me demandant sur un ton d'où était bannie toute urbanité :

- Qu'est-ce que c'est que ça ?

– C'est du chou-fleur, monsieur.

– Le nom latin ?

– Je ne me rappelle pas, monsieur, mais je puis vous dire le nom anglais : cauliflower.

– Gardez votre anglais pour vous…
Et à quels caractères avez-vous reconnu cette plante ?

– *Mais, monsieur, je n'ai pas besoin de caractères pour reconnaître du chou-fleur.*

– Ça suffit... merci, monsieur.

Le vieux petit monsieur grincheux se vengea spirituellement de mes plaisanteries en me priant de repasser à une autre session.