Stage olympique de Saint-Malo

Cours – Stratégies de base

Lundi 28 juillet 2003

par

Xavier Caruso

Table des matières

Ce document n'est pas à proprement parler un cours, il s'agit plus d'un recueil de méthodes et d'exemples. Loin d'être exhaustif, le choix des sujets traités reprend évidemment les fameux incontournables (par exemple la récurrence) mais essaie également d'insister sur d'autres points, disons plus « originaux »[1], ceci, quelque part, dans le but de ne pas *trop* faire redite avec le cours du stage de l'an dernier.

Ce document, bien que sans doute *self-contained*[2], gagnera à être complété par un vrai cours de « stratégies de base ». Il est possible d'en trouver par exemple sur la page d'Animath : `http://www.animath.fr/`.

1 Les tiroirs

1.1 Le principe

Il s'agit d'une idée fort simple et fort naturelle mais dont les conséquences sont tout à fait impressionnantes. La situation est la suivante : supposons que l'on ait à ranger 23 chaussettes[3] et que l'on dispose pour cela de 5 tiroirs. Il y aura alors forcément au moins 5 chaussettes dans un tiroir. En effet, s'il y avait au plus 4 chaussettes par tiroir, il n'y aurait pas plus de 20 chaussettes en tout.

Évidemment, la formulation générale n'est pas aussi précise, mais il n'y a de fait rien de plus à comprendre.

Propriété 1

Si n balles sont placées dans k tiroirs, au moins un tiroir contiendra $\frac{n}{k}$ balles ou plus.

Déjà, il faut dire que si $\frac{n}{k}$ n'est pas un entier, contenir au moins $\frac{n}{k}$ balles voudra dire en contenir au moins le premier entier supérieur à $\frac{n}{k}$, entier que l'on notera par la suite $\lceil \frac{n}{k} \rceil$.

Ce n'est pas tant la propriété précédente qui est intéressante en elle, mais plutôt les conséquences qu'elle peut avoir et la façon dont on l'utilise pour prouver ces conséquences.

Une première conséquence simple est de prouver qu'il y a au moins deux parisiens qui ont le même nombre de cheveux sur la tête. Évidemment, il faut des données numériques pour traiter le problème : disons que la population de Paris est d'environ 20 millions d'habitants et que les gens n'ont jamais plus d'un million de cheveux sur la tête. Dans ces conditions, si l'on veut appliquer le principe tel qu'énoncé précédemment, il faut construire de gigantesques tiroirs, tiroirs que l'on va numéroter avec les nombres compris entre 0 et 1 000 000. On va ensuite répartir les parisiens dans chacun de ces tiroirs, et ce en fonction du nombre de cheveux qu'il possède. Comme il y a strictement plus de parisiens que de tiroirs, au moins un tiroir contiendra deux parisiens, et ces deux bons hommes auront donc le même nombre de cheveux sur le crane.

Évidemment, on peut raffiner le résultat précédent. D'après le principe, et en reprenant les données précédentes (qui sont sûrement fausses) on pourra toujours un tiroir contenant $\lceil \frac{20\,000\,000}{1\,000\,001} \rceil = 20$ parisiens. Il y a donc au moins un groupe de 20 parisiens qui ont le même

[1] Originaux pour un stage olympique ; les sujets évoqués restent somme toute assez classiques.
[2] Ne demandant que peu des prérequis.
[3] Oui, apparemment, elles ne vont pas toutes par deux.

nombre de cheveux. Après le club très fermé des « 130 de Q.I. »[4], on peut former le club encore plus fermé des « 145 876 cheveux sur le crane ».

1.2 Plusieurs façons d'utiliser ce principe

Dans un premier temps, il s'agit de dire que le principe des tiroirs apporte souvent un secours inespéré lorsque l'on a un grand nombre d'entités du même objet et que l'on cherche à en isoler certains qui auraient des propriétés sympathiques. L'exemple des parisiens chevelus est en ce sens frappant. La difficulté dans ce cas sera de trouver quels seront ces objets et comment les répartir judicieusement dans les tiroirs, l'énoncé ne suggérant pas toujours si fortement la solution que dans l'exemple précédent.

Il est à noter que cette situation apparaît assez souvent en arithmétique, l'exemple de base étant le suivant. On se donne un entier n, et $n+1$ entiers $a_0, \ldots, a_n$. Il faut prouver qu'il existe deux indices distincts i et j tels que $a_i - a_j$ soit un multiple de n.

On procède comme suit. On considère donc n tiroirs que l'on numérote avec les nombres compris entre 0 et $n-1$. Maintenant, on va placer les a_i dans ces tiroirs. Plus précisément, pour tout indice i, on calcule le reste de la division de a_i par n, et si l'on appelle r ce reste, on place le nombre a_i dans le tiroir étiqueté r. D'après le principe des tiroirs, il est bien clair qu'ainsi au moins deux nombres seront placés dans le même tiroir. Cela signifiera qu'il existe un entier r et deux indices distincts i et j tels que :

$$\begin{aligned} a_i &= q_i n + r \\ a_j &= q_j n + r \end{aligned}$$

les nombres q_i et q_j étant alors les quotients des divisions faites. Mais on fait alors la différence des deux égalités données ci-dessus et on remarque que $a_i - a_j$ est un multiple de n, les restes r se simplifiant. Cela répond donc à la question.

Donnons finalement sous forme d'exercice deux nouveaux exemples illustrant de nouvelles applications de cette situation. Un peu comme dans le cas précédent, ici, la difficulté consiste à considérer les bons tiroirs.

Exercice : Sur une table rectangulaire de dimension 2m × 1m sont réparties 500 miettes de pain. Prouver que l'on peut trouver trois miettes qui déterminent un triangle d'aire inférieure à 50cm^2.

Solution :
► Apparemment, on a déjà trouvé nos objets que l'on va devoir ranger dans nos tiroirs ; il s'agit des miettes de pain. Il faut donc encore trouver les tiroirs.

L'astuce, ici, consiste à découper la table en 200 petits carrés de côté 10cm. D'après le principe des tiroirs, dans au moins un de ces carrés, il y aura trois miettes, et ces miettes vont déterminer un triangle dont l'aire sera inférieure à la moitié de la surface du carré en question. Après calcul, on aboutit bien à 50cm^2. ◄

Exercice (OIM 1984) : On fait une partition de l'ensemble des points du plan orienté en un nombre fini de parties représentées par autant de couleurs. On fixe deux points distincts O et A de ce plan. À tout point X du plan, distinct de O, on fait correspondre :

a) la mesure en radians $\alpha(X)$ de l'angle $(\widehat{OA, OX})$ prise dans $[0, 2\pi[$;

[4] cf. un sketch de Desproges.

b) le cercle $\mathcal{C}(X)$ de centre O et de rayon $OX + \frac{\alpha(X)}{OX}$

Démontrer qu'il existe un point Y du plan avec $\alpha(Y) > 0$, tel qu'il existe un point de $\mathcal{C}(Y)$ de la même couleur que Y.

Solution :

► Comme on l'a dit la difficulté ici consiste à trouver à quels objets appliquer le principe des tiroirs, car avec un peu d'entrainement il est passablement clair que c'est ce principe qu'il va falloir utiliser.

Il ne faut en fait ici pas se focaliser sur les points, mais plutôt sur les cercles de centre 0. À tout cercle, on peut associer l'ensemble des couleurs qui apparaîssent sur ce cercle ; ils sont là nos tiroirs. Un dénombrement simple nous dit qu'il y a $2^n - 1$ tiroirs, il nous suffira donc de choisir 2^n cercles. En fait, si l'on réfléchit un peu au problème, on se rend facilement compte qu'il faudra choisir ces cercles relativement proches les uns des autres. On choisit donc au final 2^n cercles parmi ceux de rayons strictement inférieurs à $\sqrt{2\pi}$. Parmi ces cercles, il va y en avoir deux qui auront le même ensemble de couleurs associé.

Il s'agit maintenant de jouer sur l'angle. Plus précisément si R_1 et R_2 sont les rayons des deux cercles choisis, avec par exemple $R_1 < R_2$, il faut trouver Y sur R_1 tel que $\alpha(Y)$ vérifie l'équation suivante :

$$R_2 = R_1 + \frac{\alpha(Y)}{R_1}$$

équation dont on vérifie facilement qu'elle admet une solution dans l'intervalle $]0, 2\pi[$.

Le cercle $\mathcal{C}(Y)$ est alors le cercle de centre O et de rayon R_2 ; la conclusion s'ensuit. ◄

Toutefois, ce n'est pas le seul cas dans lequel il peut être utile ; il apparaît souvent au détour d'un raisonnement et c'est alors encore moins évident de le mettre en évidence. Pour tout commentaire, nous proposons l'exercice suivant :

Exercice (OIM 1997) : Une matrice carrée à n lignes et n colonnes, à éléments dans l'ensemble $S = \{1, 2, \ldots, 2n-1\}$, est appelée une matrice d'*argent* si, pour tout $i = 1, \ldots, n$, la réunion de la i-ième ligne et de la i-ième colonne contient tous les éléments de S. Montrer qu'il n'existe pas de matrice d'argent pour $n = 1997$.

Solution :

► On reconnaît, ici, bien évidemment la situation donnée dans le test de bienvenue[5].

Donnons-nous un entier a compris entre 1 et $2n-1$. Si cet entier apparaît à la position (i, j), alors il apparaît à la fois dans la i-ième croix[6] et dans la j-ième croix. Comme maintenant a doit apparaître une et une seule fois dans chaque croix, on peut faire la chose suivante : on écrit les uns à la suite des autres les nombres de 1 et 1997, et on barre au fur et à mesure les numéros des croix dans lesquelles a apparaît. À la fin, toutes les croix devront être barrées.

On se rend compte que si a n'apparaît pas sur la diagonale, on va barrer les nombres deux par deux. Mais cela n'est pas possible puisque 1997 est un nombre impair. Il reste donc à prouver qu'il existe un entier a qui n'apparaît pas sur la diagonale.

C'est la qu'intervient le principe des tiroirs. Il y a 3993 nombres en tout et seulement 1997 places sur la diagonale ; il y a donc au moins un nombre qui ne peut pas apparaître (en fait, il y en a au moins 1996, mais bon). ◄

[5] Cela vous touche, je le sais !

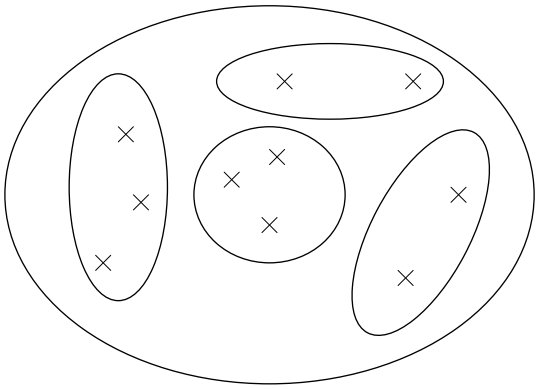
[6] On appelle *i-ième croix* la réunion de la i-ième ligne et de la i-ième colonne.

2 Les invariants

2.1 La situation

Supposons que l'on ait un gros ensemble regroupant un certain nombre de configurations. Supposons en outre que l'on se soit dicté des règles permettant de passer d'une configuration à une autre. Ainsi on va regrouper entre elles les configurations qui peuvent être atteintes l'une de l'autre par application de ces règles.

Schématiquement, on a la chose suivante :



La grosse patate représente l'ensemble des configurations et on a regroupé dans les petites patates les configurations que l'on pouvait déduire l'une de l'autre par les transformations autorisées[7].

La situation que l'on va étudier est la suivante : on se donne deux configurations et on se demande si elles sont ou non dans la même patate, c'est-à-dire s'il y a moyen de passer de l'une à l'autre par une suite d'opérations autorisées.

Nous allons peut-être d'ores et déjà donner un exemple qui va clarifier les choses. L'ensemble des configurations va être ici l'ensemble des mots (qui ont un sens ou pas) écrits avec les seules lettres x, y, z et t. On s'autorise les trois transformations suivantes :

i) $xy \to yyx$ et $yyx \to xy$

ii) $xt \to ttx$ et $ttx \to xt$

iii) $yt \to ty$ et $ty \to yt$

La première condition signifie par exemple que lorsque l'on a un mot dans lequel apparaît les deux lettres x et y *juste à côté*, alors on s'autorise à remplacer ceux deux lettres par les trois lettres y, y et x. On s'autorise également à revenir en arrière ; c'est la deuxième condition du i).

Ainsi les mots $xxyy$ et $xyyyyx$ vont être *equivalents*, grâce à la suite de transformations suivantes :

$$xxyy = x\ xy\ y \to x\ yyx\ y = xyy\ xy \to xyy\ yyx = xyyyyx$$

Dans le schéma précédent, ces deux-mots là appartiendraient donc à la même petite patate. On voit que pour prouver que deux mots sont dans la même petite patate, il « suffit » d'exhiber une suite de transformations permettant de passer de l'un à l'autre. Mais comment prouver que deux mots n'appartiennent pas à la même petite patate ? C'est là qu'intervient la théorie des *invariants*.

[7] Les transformations sont supposées symétriques, ce qui fait que les petites patates seront supposées disjointes.

De façon générale, l'idée consiste à associer à chaque configuration un objet (généralement un entier, ou une propriété) que l'on va appeler son *invariant*. Cet invariant devra au moins avoir les deux propriétés sympathiques suivantes :

1. le calcul de l'invariant devra pouvoir se faire de manière simple et systématique
2. deux configurations équivalentes (*ie* dans la même patate) devront avoir même invariant

Ainsi, pour prouver que deux configurations ne sont pas équivalentes, on calcule les invariants associés à chacune d'elles : si ces invariants sont différents, on peut conclure. Attention, on ne peut pas conclure si les invariants sont égaux !

On voit maintenant qu'une troisième propriété qui serait sympathique pour un invariant serait de prendre des valeurs assez diversifiées : un invariant qui a toute position associe par exemple le nombre 0 est certes facile à calculer, mais ne donnera au final que peu d'informations. Au mieux un invariant permet de distinguer deux ensembles de configurations, au plus on dira qu'il est *fin*. Construire des invariants fins est en général un problème difficile ; toutefois, on verra par la suite que souvent des invariants très grossiers permettent d'arriver à des résultats déjà intéressants.

Revenons à notre exemple et posons-nous la question suivante : les mots $xytx$ et $txyt$ sont-ils équivalents ? Pour résoudre cette question, on remarque que les transformations permises ne modifient jamais le nombre d'occurrences de la lettre x dans le mot. Si l'on veut reprendre le langage introduit précédent, on dira que si l'on associe à un mot le nombre d'apparitions de la lettre x dans ce mot, on obtient un invariant.

Maintenant, l'invariant du mot $xytx$ vaut 2 et celui du mot $txyt$ vaut 1 ; cela prouve que ces mots ne sont pas équivalents.

L'invariant que l'on vient de construire permet de distinguer quantité de mots, mais il est incapable de donner une réponse pour les mots xy et xt. En fait, on peut prouver que ces deux mots ne sont pas équivalents. Voyez-vous comment ?

2.2 Invariant de parité

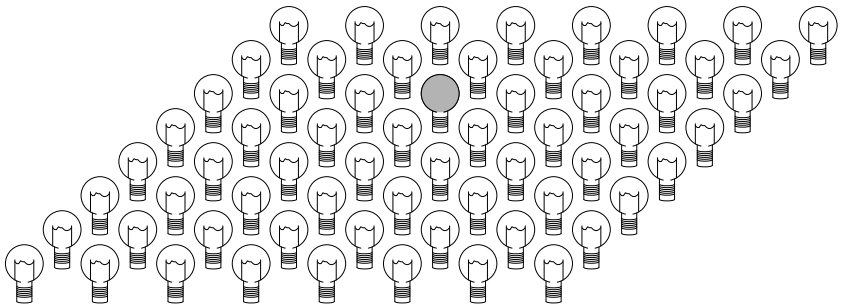
Un invariant *a priori* grossier, mais qui permet souvent d'arriver au résultat, est ce que l'on appelle un *invariant de parité* : à une configuration donnée, on va associer soit *pair*, soit *impair*, le problème étant bien sûr souvent de savoir ce qu'il faut compter.

Donnons un exemple qui illustre cela. Supposons que l'on dispose d'une table carrée sur laquelle sont disposées 64 ampoules dans un carré 8×8. Au bout de chaque ligne et de chaque colonne, il y a un interrupteur. Lorsque celui-ci est actionné, il inverse l'état[8] de chacune des ampoules de la ligne ou de la colonne à laquelle il correspond.

Au début, toutes les ampoules sont éteintes. Est-il possible d'arriver dans la configuration dans laquelle seule l'ampoule marquée est allumée (voir dessin page suivante) ?

Pour répondre à cette question on utilise un invariant de parité : on constate que lorsque l'on appuie sur un interrupteur la parité du nombre d'ampoules allumés ne change pas. En effet, si avant sur la ligne ou la colonne affectée par l'opération, il y avait a ampoules allumées et b ampoules éteintes, il y aura après l'opération b ampoules allumées et a ampoules éteintes. Ce qu'il faut voir c'est que a et b sont forcément de même parité puisque $a + b = 8$.

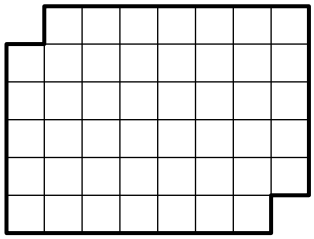
[8] Cela signifie que si l'ampoule était allumée, elle s'eteint et si elle était éteinte, elle s'allume.



Formellement, on associe à une configuration l'invariant *pair* si le nombre d'ampoules allumées est pair et l'invariant *impair* sinon. On vient de voir que cet invariant n'est bien pas modifié lors d'une transformation autorisée. Au début, toutes les ampoules sont éteintes, l'imvariant est donc *pair*. À la fin, on souhaite qu'il n'y ait qu'une ampoule allumée et donc un invariant *impair*. C'est impossible !

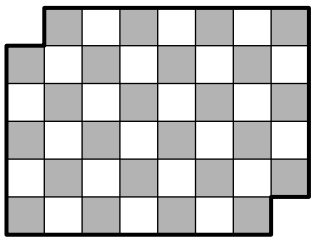
2.3 Invariants et coloriage

Le problème à résoudre ce coup-ci est le suivant. On considère le plateau de jeu représenté ci-dessous :



jeu que l'on souhaite paver avec des dominos de la forme suivante :  , dominos que l'on peut disposer soit horizontalement, soit verticalement.

En fait, cela est impossible et la méthode pour prouver ce fait est la suivante. On commence par colorier les cases du plateau de jeu de la façon suivante :



On remarque alors que si l'on pose un domino sur le plateau de jeu, il recouvrira forcément une case blanche et une case noire. On conclut en comptant les cases : il y a 24 cases noires et 22 cases blanches seulement. Un pavage est par le fait impossible.

Cette dernière démonstration est en fait une illustration de la théorie des invariants. Bien que cela ne soit pas fondamental, nous allons expliquer en quoi.

L'ensemble des configurations sera l'ensemble des ensembles de cases. Cela signifie qu'une configuration sera le choix d'un certain nombre de cases, ces cases étant choisies

de façon totalement quelconque ; en particulier, ce choix ne correspond pas forcément à un pavage par des dominos.

Les transformations autorisées seront celles qui consistent à enlever ou à ajouter deux cases adjacentes, correspondant donc à l'enlèvement ou à l'ajout d'un domino. Il faut maintenant définir l'invariant : étant donné une configuration (*ie* un choix de certaines cases), on compte le nombre de cases noires et de cases blanches parmi les cases choisies et on soustrait ces deux nombres, le résultat pouvant être positif ou négatif.

Il est clair que l'on définit ainsi un invariant : rajouter un domino rajoute à la fois une case blanche et une case noire et donc ne modifie pas la différence ; enlever un domino supprime à la fois une case noire et une case blanche et donc ne modifie pas la différence non plus. Maintenant l'invariant associé à la position d'origine (celle où l'on choisit toutes les cases) est $24 - 22 = 2$. Pour la position d'arrivée par contre (celle où l'on ne choisit aucune case), c'est 0.

Cela prouve donc l'impossibilité.

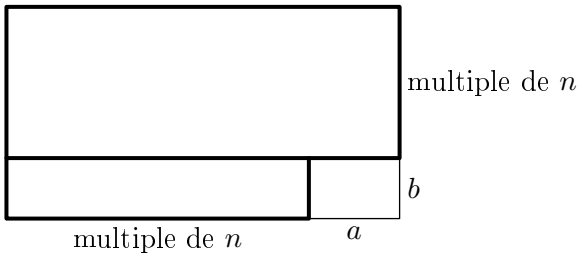
2.4 Colorier avec plusieurs couleurs

Lorsque l'on ne pave plus avec des dominos mais avec des pièces plus grandes ou plus difformes, il peut parfois être utile d'utiliser un coloriage plus perfectionné. Le premier exemple à traiter est probablement le suivant.

On considère un rectangle de dimension $a \times b$ que l'on veut paver avec des n-ominos de taille $1 \times n$. On se demande à quelle condition portant sur les dimensions du rectangle a et b, un tel pavage est réalisable.

On colorie comme précédemment les petites cases du rectangle, mais ce coup-ci en utilisant n couleurs, l'idée étant toujours la même : lorsque l'on va poser un n-omino, il va recouvrir une case de chacune des couleurs. Ainsi, s'il n'y a pas autant de cases de chaque couleur, le pavage ne sera pas possible. Pour cela, on commence par ordonner de façon arbitraire les couleurs : il y donc la première, la deuxième, etc. Sur la première ligne, on dispose les couleurs dans l'ordre et on recommence lorsque l'on a épuisé notre palette. On fait de même sur la seconde ligne sauf que l'on procède à un décalage d'une couleur (*ie* on commence à la deuxième couleur). On continue et termine alors de la même façon, décalant d'une couleur (toujours dans le même sens) à chaque nouvelle ligne.

Essayons donc de compter le nombre de cases de chaque couleur. Déjà, on remarque que tout rectangle de taille $n \times x$ portera exactement x cases de chaque couleur. Ainsi pour faire notre décompte, on peut commencer par retirer deux rectangles de sorte que les dimensions a et b soient toutes les deux strictement plus petites que n. Quitte à faire pivoter le rectangle obtenu, on peut supposer en outre que $a \geqslant b$.



La a-ième couleur est celle qui apparaît le plus à droite sur la première ligne du petit rectangle en bas à droite. Cette couleur apparaît donc sur toutes les lignes. Par contre la n-ième couleur, elle, ne peut évidemment apparaître plus d'une fois par ligne, mais n'apparaît pas non plus sur la première. Finalement, elle apparaît moins que la a-ième et le rectangle n'est pas pavable. Bien évidemment le raisonnement précédent ne tient pas si a ou b est nul ; dans ces cas, il n'y a plus de rectangle en bas.

On vient ainsi de donner une première réponse à la question que l'on s'était posée : si une des dimensions a ou b n'est pas un multiple de n, alors le rectangle n'est pas pavable. D'autre part, il est clair que si l'une des dimensions est un multiple de n alors le rectangle est pavable. On vient donc de répondre totalement à la question.

Là encore, ce problème que l'on vient de traiter avec des coloriages peut être vu comme une application de la théorie des invariants. Comme dans le cas du paragraphe précédent, une configuration sera le choix d'un certain nombre de cases de notre rectangle $a \times b$. Les n couleurs vont ce coup-ci être remplacées par des nombres $x_1, \ldots, x_n$ vérifiant la condition $x_1 + \ldots + x_n = 0$.

L'invariant associé à une configuration sera la somme des nombres associés aux cases retenues pour la configuration en question. Lorsque l'on passe d'une configuration à une autre en ajoutant n cases alignées horizontalement ou verticalement, on ne change pas l'invariant, justement en vertu de la condition $x_1 + \ldots + x_n = 0$.

Certains choix de valeurs pour les x_k simplifient grandement les calculs, le plus simple étant probablement de prendre :

$$x_k = \exp\left(\frac{2i\,(k-1)\,\pi}{n}\right)$$

i étant le « $\sqrt{-1}$ » des nombres complexes et exp désignant l'exponentielle complexe[9].

Dans ces conditions, un simple calcul[10] permet de déterminer l'invariant du rectangle $a \times b$. On trouve :

$$\frac{\left[\exp\left(\frac{2ia\pi}{n}\right)-1\right]\left[\exp\left(\frac{2ib\pi}{n}\right)-1\right]}{\left[\exp\left(\frac{2i\pi}{n}\right)-1\right]^2}$$

et l'on sait que si ce nombre n'est pas nul, alors le rectangle n'est pas pavable. Or un produit de facteurs est nul si et seulement si un des facteurs est nul et les exponentielles égalent 1 si et seulement si leur argument est un multiple de $2i\pi$. Cela permet d'arriver de même que précédemment à la conclusion.

Il est remarquable de noter que cette dernière méthode se généralise directement au cas continu. Le problème est alors le suivant. Les nombres a et b sont cette fois-ci des réels et on veut paver un rectangle de taille $a \times b$ par des lattes de dimensions $1 \times x$, la valeur de x pouvant varier d'une latte à l'autre.

Une configuration sera alors une partie (mesurable) A du rectangle et l'invariant associée sera :

$$\int_A \exp\left(2i\,(x+y)\,\pi\right)\mathrm{d}x\mathrm{d}y$$

Comme précédemment, on montre que si cette quantité est non nulle, alors le rectangle n'est pas pavable. De cela on déduit que le rectangle est pavable si et seulement si une des dimensions a ou b est un nombre entier.

[9] Le lecteur qui n'est pas familier avec ces notions peut passer directement au chapitre suivant.
[10] Si l'on connait la formule de sommation d'une série géométrique.

3 Le raisonnement par l'absurde

3.1 La situation

Supposons que l'on ait à démontrer une certaine phrase mathématique. Une façon d'aborder le problème est de commencer par supposer que cette phrase est fausse. On regarde ensuite ce qui découle de cette nouvelle hypothèse, le but étant de parvenir à une contradiction. Si l'on y arrive, cela voudra dire que notre supposition de départ ne pouvait être valable et ainsi on aura bien démontré notre propriété.

La grande force du raisonnement par l'absurde est d'introduire une hypothèse supplémentaire, ce qui est fort utile lorsque l'on n'a rien ou pas grand-chose pour partir. En outre, le raisonnement par l'absurde est particulièrement efficace lorsqu'il s'agit de montrer une propriété négative (« Montrer que telle chose n'a *pas* telle propriété »). Dans ce cas, on suppose que cette chose a la propriété en question et on regarde ce qu'il en découle.

Le raisonnement par l'absurde se révèle à la fois efficace et naturel pour tout ce qui fait partie des problèmes de logique grand public[11], dirions-nous. En voici un exemple :

Le gentil héros se retrouve face à la confrontation finale. Il est dans une salle au fond de laquelle se trouvent trois portes donnant sur trois prisons gardées par trois vaillants logiciens. Le héros s'approche et les logiciens parlent tour à tour :

Le gardien de la première porte dit : « Derrière ma porte, il y a la princesse ».
Le gardien de la deuxième porte dit : « Il y a un et un seul menteur parmi nous et derrière *ma* porte, il y a la princesse ».
Le gardien de la troisième porte dit : « Nous sommes tous des menteurs ».

La question est bien entendu de savoir où se cache la princesse, sachant que parmi les trois gardiens, certains disent *toujours* la vérité et les autres mentent *toujours*.

N'ayant que peu d'informations au début, pour résoudre ces questions, on est souvent amené à faire des hypothèses successives et à les tester. C'est exactement le principe du raisonnement par l'absude.

Commençons par analyser la phrase prononcée par le troisième gardien. Supposons que ce gardien dise toujours la vérité. Dans ce cas, ce serait un menteur, comme il le dit. C'est absurde ! Le troisième gardien est donc un menteur et on sait en outre maintenant qu'au moins un des deux autres gardiens a dit la vérité. Une autre façon de voir les choses est de dire que le troisième gardien se contredit lui-même ; c'est donc forcément un menteur.

Maintenant que l'on sait cela, focalisons-nous sur le deuxième gardien et supposons qu'il dise la vérité. Alors, dans un premier temps, il y aurait un et un seul menteur parmi les trois gardiens, comme il le dit. Mais on l'a déjà trouvé ce menteur, c'est le troisième. Cela voudrait donc dire que les deux premiers gardiens ont dit la vérité. Mais cela n'est pas possible puisque chacun affirme que la princesse se trouve dans la prison qu'il garde, et qu'évidemment il n'y a qu'une princesse. Encore, on arrive à une contradiction et le second gardien est aussi un menteur.

Dès lors, le premier dit forcément la vérité puisque l'on sait qu'ils ne sont pas tous les trois des menteurs : la princesse est donc retenue dans la première cellule !

[11] Le démineur en est encore un exemple : si vous jouez couramment à ce jeu, vous faites sans doute nombre de démonstrations par l'absurde sans même le savoir.

Bien sûr, dans ce cas simple, une étude exhaustive fonctionnera tout aussi bien : il y a 8 possibilités en tout, chaque gardien pouvant soit mentir soit dire la vérité. Il faut alors éliminer les cas un par un quand ceux-ci deviennent contradictoires. C'est encore exactement une application du raisonnement par l'absurde, mais de façon moins subtile que celle présentée juste avant.

3.2 L'irrationalité de $\sqrt{2}$

Un nombre rationnel est un nombre qui peut s'écrire comme le quotient de deux entiers, donc une fraction $\frac{p}{q}$. On souhaite ici prouver que $\sqrt{2}$, donc le nombre qui multiplié par lui-même fait 2, n'est pas rationnel.

C'est un exemple typique où l'on souhaite obtenir une propriété « négative », et donc un raisonnement par l'absurde va nous permettre de pouvoir partir. On suppose donc, sans pitié, qu'il existe des entiers a et b tels que :

$$\sqrt{2} = \frac{a}{b}$$

le dénominateur b étant non nul. Il s'agit maintenant de trifouiller tout cela pour aboutir à une contradiction.

La seule information dont on dispose sur le nombre $\sqrt{2}$ porte sur son carré ; il est donc naturel d'élever l'égalité précédente au carré. On obtient ainsi après avoir chassé les dénominateurs $a^2 = 2b^2$. Il s'agit maintenant de comprendre pourquoi cette équation ne peut pas avoir de solutions, a et b devant être des entiers.

Pour cela, il faut se rappeler un peu d'arithmétique et principalement la décomposition en facteurs premiers, propriété que nous rappelons ci-dessous.

Propriété 2

Soit $n \geqslant 2$ un entier naturel. Alors il existe des nombres premiers $p_1, \ldots, p_k$ deux à deux distincts et des entiers strictement positifs $\alpha_1, \ldots, \alpha_k$, le tout tel que :

$$n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

En outre cette écriture est unique à l'ordre d'écriture près.

On rappelle que par définition, un nombre *premier* est un nombre qui n'admet pas de diviseurs propres, c'est-à-dire qui n'est divisible que par 1 et lui-même. On rappelle en outre que par convention, 1 n'est pas considéré comme étant premier.

Il est une façon, peut-être plus agréable pour certains, de réénoncer la propriété précédente :

Propriété 3

Soit n un entier naturel non nul. Alors il existe une unique suite d'entiers positifs ou nuls (α_p) indexée par les nombres premiers et telle que :

1. *l'entier α_p est nul pour p suffisamment grand*
2. $n = \prod_{p \text{ premier}} p^{\alpha_p}$

L'entier α_p s'appelle la valuation p-adique *de n ; il est souvent noté $v_p(n)$.*

Il est sans doute nécessaire de faire quelques remarques. Déjà le signe « $\prod$ » signifie que l'on fait le produit des tous les termes p^{α_p} lorsque p parcourt l'ensemble des nombres premiers. La première condition assure que ce produit est en fait fini : $p^0 = 1$ pour tout entier non nul p et multiplier par 1 ne modifie pas le résultat.

Finalement, la valuation p-adique de l'entier n peut se définir directement. Il s'agit du plus grand entier α_p tel que p^{α_p} divise n. On voit alors que pour p suffisamment grand (par exemple $p > n$), α_p va être nul.

Une dernière remarque, facile à prouver et laissée au lecteur, dit que si a et b sont des entiers strictement positifs, alors :

$$v_p(ab) = v_p(a) + v_p(b)$$

Revenons à nos moutons. On rappelle que l'on était arrivé à l'équation $a^2 = 2b^2$ et qu'il s'agissait de trouver une absurdité. L'idée consiste donc à passer aux valuations 2-adiques ; on obtient, en vertu de la remarque précédente :

$$2v_p(a) = 1 + 2v_p(b)$$

mais cela est absurde car le membre de gauche de l'égalité précédente est manifestement un nombre pair, alors que celui de droite est manifestement impair. Ils ne peuvent donc pas être égaux[12].

On déduit de cela que notre hypothèse de départ ne pouvait être vraie : $\sqrt{2}$ est bien un nombre irrationnel.

4 Le raisonnement par récurrence

En guise d'introduction, on se propose de démontrer la partie « existence » de la propriété 2. On prend donc un entier n strictement positif et on souhaite écrire n comme un produit de nombres premiers.

Il y a deux cas à distinguer : soit n est déjà premier, soit il ne l'est pas. Dans le premier cas, il n'y a rien à faire : n est déjà écrit comme un produit de nombres premiers (un seul nombre en l'occurrence).

Maintenant si n n'est pas premier, c'est qu'il existe des entiers a et b strictement plus petits que n tels que $n = ab$. C'est le premier pas de notre décomposition et on n'a plus qu'à continuer ainsi. Si a est premier, c'est très bien, sinon on l'écrit comme produit de deux nombres et ainsi de suite. Bien sûr on fait pareil avec b.

4.1 Le principe

Voyons comment l'on peut écrire proprement le raisonnement précédent. L'idée consiste à prouver la propriété 2 pour les entiers les uns après les autres. On sait faire pour 2, c'est

[12] Le lecteur un peu embrouillé par l'introduction des valuations pourra décomposer a et b en facteurs premiers et remplacer dans l'égalité $a^2 = 2b^2$, a et b par leur décomposition respective. Il ne restera plus alors qu'à comparer les exposants de 2 qui interviennent pour aboutir à la même contradiction.

déjà un nombre premier. On peut débuter à 1 si l'on préfère ; il faut alors se convaincre que 1 s'écrit comme le produit d'*aucun* nombre premier.

Ensuite, on sait faire pour 3, c'est encore un nombre premier. 4 n'est pas premier mais il s'écrit 2×2 et on sait dejà faire pour 2. Et on continue ainsi de suite.

Rigoureusement le « ainsi de suite » qui précède correspond au principe de récurrence qui s'énonce comme suit :

Propriété 4

Considérons une famille d'énoncés mathématiques qui dépendent d'un paramètre entier n. Notons P_n le n-ième énoncé[13].

Si d'une part, l'on sait démontrer P_0 et que d'autre part, on arrive à prouver que P_{n+1} est une conséquence des énoncés $P_0, \ldots, P_n$, alors tous les énoncés P_n sont vrais.

Faisons tout de suite des remarques. Dans un premier temps, on n'est évidemment pas obligé de débuter à 0, on peut commencer à n'importe quel entier : si l'on commence à l'entier k, il faudra prouver que l'énoncé P_k est vrai et que pour tout $n \geqslant k$, l'énoncé P_{n+1} est une conséquence des énoncés $P_k, \ldots, P_n$.

Remarquons également que très souvent P_{n+1} est simplement une conséquence de l'énoncé P_n, voire des énoncés P_n et P_{n-1}, mais pas vraiment de tous les précédents. Bref.

Pour faire une démonstration par récurrence, il y a toujours deux étapes :
- L'*initialisation* qui consiste à prouver la propriété P_0
- L'*hérédité* qui consiste à prouver que P_{n+1} est conséquence des propriétés $P_0, \ldots, P_n$

Dans un raisonnement classique par syllogismes, on tente de prouver un résultat général d'un seul coup pour toutes les valeurs de n indépendamment. Ce qui fait la spécificité du raisonnement par récurrence est de disposer d'une hypothèse supplémentaire (« l'hypothèse de récurrence ») qui, lors de l'hérédité, nous donne une information utilisable sur l'entier n sur lequel on raisonne. Si l'on est capable de conclure sans utiliser cette information, c'est qu'en fait on n'a pas utilisé un raisonnement par récurrence. Inversement, cela nous donne aussi une indication sur la méthode à suivre pour mener un tel raisonnement, ou comment gérer l'hérédité : la clé consiste à se mettre en situation d'utiliser cette donnée supplémentaire.

4.2 Notre premier exemple

Voyons comment cela fonctionne avec notre premier exemple. Comme on l'a déjà dit, l'énoncé P_n va être « l'entier n peut s'écrire comme un produit de nombres premiers ». On ne commence ici pas à l'entier 0 mais plutôt à 1.

L'étape d'initialisation consiste à prouver P_1, c'est-à-dire que 1 peut s'écrire comme un produit de nombres premiers. On a déjà dit que c'était le cas puisque 1 est le produit d'aucun nombre premier. Encore une fois si cela ne vous plait pas, vous pouvez commencer à 2.

[13] Dans l'exemple précédent, P_n était donc l'énoncé : « l'entier n peut s'écrire comme un produit de nombres premiers ».

Considérons maintenant un entier n. On souhaite démontrer P_{n+1}, mais en ayant le droit de supposer $P_1, \ldots, P_n$. Autrement dit, on sait déjà que tous les entiers inférieurs ou égaux à n peuvent s'écrire comme produit de nombres premiers, et on veut montrer qu'il en est de même de $n+1$.

Si $n+1$ est un nombre premier, alors on a gagné. Si par contre ce n'est pas le cas, il existe des entiers a et b, tous les deux strictement inférieurs à $n+1$ (et donc inférieurs ou égaux à n) tels que $n+1 = ab$. Mais pour a et b on sait faire ; on sait par hypothèse de récurrence comme on dit, qu'il existe des nombres premiers $a_1, \ldots, a_k$ et $b_1, \ldots, b_l$ tels que :

$$a = a_1 \ldots a_k \quad \text{et} \quad b = b_1 \ldots b_l$$

Mais alors, $n+1 = ab = a_1 \ldots a_k b_1 \ldots b_l$ et donc $n+1$ s'écrit bien comme produit de nombres premiers.

Tout cela permet de conclure.

Moralement il y a deux façons de voir la récurrence : soit en partant d'« en haut », soit en partant d'« en bas ». La première est celle que nous avons ébauchée dans l'introduction du chapitre : on veut écrire n comme produit de nombres premiers, alors on commence par écrire n comme produit de deux nombres et on continue jusqu'à n'obtenir que des nombres premiers. Le problème avec cette stratégie est qu'il faut prouver que la suite d'opérations prend nécessairement fin[14]. La méthode par « le bas », quant à elle, bien que parfois moins naturelle a l'avantage d'être sans surprise et de permettre des rédactions plus simples et souvent plus compréhensibles, ce qui nous ne le dirons jamais assez aide autant le lecteur que l'élève.

4.3 Digression sur l'intérêt des formules

L'exercice à résoudre est maintenant le suivant : on se donne un réel non nul x tel que le nombre $x + \frac{1}{x}$ soit un entier. Il s'agit de montrer que pour tout entier n, le nombre $x^n + \frac{1}{x^n}$ est également un entier.

Voyons ce qu'il se passe pour $n = 2$. On sait que $x + \frac{1}{x}$ est un entier et on veut prouver que $x^2 + \frac{1}{x^2}$ en est aussi un. Il nous faut donc trouver un moyen de relier ces deux nombres. Mais on a la formule suivante :

$$\left(x + \frac{1}{x}\right)^2 = x^2 + 2 + \frac{1}{x^2} = \left(x^2 + \frac{1}{x^2}\right) + 2$$

et on voit qu'elle permet de conclure directement : le nombre dont on veut voir qu'il est entier s'écrit comme le carré d'un nombre entier auquel on a enlevé 2.

Comment faire maintenant pour $n = 3$? Ben de la même façon ; on utilise la formule :

$$\left(x^2 + \frac{1}{x^2}\right)\left(x + \frac{1}{x}\right) = x^3 + x + \frac{1}{x} + \frac{1}{x^3} = \left(x + \frac{1}{x}\right) + \left(x^3 + \frac{1}{x^3}\right)$$

Comme précédemment, on sait déjà que le membre de gauche de l'égalité précédente est un entier. Il en est de même par hypothèse de la quantité $x + \frac{1}{x}$. On en déduit donc bien ce que l'on veut.

[14] Ce qui repose en général toujours sur le fait qu'il n'existe pas de suite strictement décroissante d'entiers, principe d'ailleurs équivalent à l'énoncé de récurrence.

De façon générale, on utilise une récurrence pour prouver le résultat général. L'initialisation correspond au cas $n = 1$ et est donnée par hypothèse. Supposons donc que chacun des nombres $x + \frac{1}{x}, \ldots, x^n + \frac{1}{x^n}$ soit un entier et essayons de prouver qu'il en est de même de $x^{n+1} + \frac{1}{x^{n+1}}$. Pour cela, on utilise comme précédemment la formule :

$$\left(x^n + \frac{1}{x^n}\right)\left(x + \frac{1}{x}\right) = x^{n+1} + x^{n-1} + \frac{1}{x^{n-1}} + \frac{1}{x^{n+1}} = \left(x^{n+1} + \frac{1}{x^{n+1}}\right) + \left(x^{n-1} + \frac{1}{x^{n-1}}\right)$$

et on conclut comme les autres fois.

On constate qu'ici nous n'avons utilisé l'hypothèse de récurrence que pour les rangs n et $n-1$. Il faut toutefois faire attention au fait que ces deux valeurs font bien partie de celles pour lesquelles on a le droit de supposer quelque chose. Ce n'est d'ailleurs ici pas le cas pour $n + 1 = 2$: $n - 1$ vaut alors 0 et on a commencé notre récurrence à 1. Pour terminer notre preuve, il faut donc traiter le cas $n = 2$ à part.

Souvent, des identités purement algébriques comme les précédentes résultent simplement de formules qu'il s'agit de déterminer. Pour illustrer ce propos, nous donnons les deux exercices suivants :

Exercice : On suppose que les entiers n et m s'écrivent tous deux comme somme de deux carrés. Montrer qu'il en est de même du produit nm.

Solution :
► Les hypothèses nous disent qu'il existe quatre entiers a, b, c et d tels que $n = a^2 + b^2$ et $m = c^2 + d^2$. Il s'agit donc d'écrire le produit $\left(a^2 + b^2\right)\left(c^2 + d^2\right)$ comme une somme de deux carrés et cela se fait « simplement » à l'aide de la formule suivante :

$$\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac + bd)^2 + (ad - bc)^2$$

◄

Remarquons qu'il existe des formules analogues pour les sommes de quatre et de huit carrés. Elles sont :

$$\begin{aligned}&\left(a^2 + b^2 + c^2 + d^2\right)\left(e^2 + f^2 + g^2 + h^2\right) = \\ &\quad (ae - bf - cg - dh)^2 + (af + be + ch - dg)^2 + (ce + ag - bh + df)^2 + (ah + de + bg - cf)^2\end{aligned}$$

et

$$\begin{aligned}&\left(x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2\right)\left(y_0^2 + y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2\right) = \\ &\qquad (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7)^2 \\ &\quad + (x_0y_1 + x_1y_0 + x_2y_4 + x_3y_7 - x_4y_2 + x_5y_6 - x_6y_5 - x_7y_3)^2 \\ &\quad + (x_0y_2 - x_1y_4 + x_2y_0 + x_3y_5 + x_4y_1 - x_5y_3 + x_6y_7 - x_7y_6)^2 \\ &\quad + (x_0y_3 - x_1y_7 - x_2y_5 + x_3y_0 + x_4y_6 + x_5y_2 - x_6y_4 + x_7y_1)^2 \\ &\quad + (x_0y_4 + x_1y_2 - x_2y_1 - x_3y_6 + x_4y_0 + x_5y_7 + x_6y_3 - x_7y_5)^2 \\ &\quad + (x_0y_5 - x_1y_6 + x_2y_3 - x_3y_2 - x_4y_7 + x_5y_0 + x_6y_1 + x_7y_4)^2 \\ &\quad + (x_0y_6 + x_1y_5 - x_2y_7 + x_3y_4 - x_4y_3 - x_5y_1 + x_6y_0 + x_7y_2)^2 \\ &\quad + (x_0y_7 + x_1y_3 + x_2y_6 - x_3y_1 + x_4y_5 - x_5y_4 - x_6y_2 + x_7y_0)^2\end{aligned}$$

Pour information 2, 4 ou 8 sont les seuls entiers pour lesquels on dispose de telles formules.

De la même façon, la formule suivante nous assure par exemple que tout rationnel s'écrit comme la somme de trois cubes de nombres rationnels :

$$r = \left(\frac{r^6 + 45r^4 - 81r^2 + 27}{6r\left(r^2 + 3\right)^2}\right)^3 + \left(\frac{-r^4 + 30r^2 - 9}{6r\left(r^2 + 3\right)}\right)^3 + \left(\frac{-6r^3 + 18r}{\left(r^2 + 3\right)^2}\right)^3$$

Exercice : Soient x, y et z trois nombres réels vérifiant $x+y+z=0$ et $x^2+y^2+z^2=2003$. Calculer $x^4+y^4+z^4$.

Solution :
▶ Cela se fait directement à partir des trois formules suivantes :

$$\begin{aligned}(x+y+z)^2 &= x^2+y^2+z^2+2(xy+yz+xz)\\ (xy+yz+xz)^2 &= x^2y^2+y^2z^2+x^2z^2+2xyz(x+y+z)\\ \left(x^2+y^2+z^2\right)^2 &= x^4+y^4+z^4+2\left(x^2y^2+y^2z^2+x^2z^2\right)\end{aligned}$$

La première formule conduit à :

$$xy+yz+xz=-\frac{2003}{2}$$

La seconde implique alors :

$$x^2y^2+y^2z^2+x^2z^2=\frac{2003^2}{4}$$

et finalement :

$$x^4+y^4+z^4=2003^2-2\cdot\frac{2003^2}{4}=\frac{1}{2}\cdot 2003^2$$

Bien évidemment, le lecteur ayant une âme de frimeur pourra combiner les trois formules précédentes pour n'en n'utiliser qu'une bien plus impressionnante. ◀

5 Récurrence et suites

Une suite récurrente est une suite dont le n-ième terme, u_n donc, est défini en fonction des précédents : $u_0,\ldots,u_{n-1}$. On conçoit facilement que le principe de récurrence va être particulièrement utile pour montrer de nombreuses propriétés sur de telles suites.

Bien que l'on puisse montrer de nombreuses sortes de propriétés différentes, nous allons nous cantonner par la suite à donner des formules explicites pour calculer u_n, la suite (u_n) étant *a priori* définie de façon récurrente.

5.1 Les suites arithmético-géométriques

On considère a et b deux réels. On suppose que la suite u_n vérifie la relation de récurrence $u_{n+1}=au_n+b$ pour tout entier $n\geqslant 1$. Bien entendu, cette seule relation ne définit par complètement u_n, il reste encore à choisir une valeur pour u_0[15], mais disons simplement que u_0 vaut u, un certain réel fixé à l'avance.

On se propose de prouver que pour tout entier n, le terme u_n est donné par la formule :

$$u_n=a^nu+b\cdot\frac{a^n-1}{a-1}$$

[15]Pour faire un parallèle avec le raisonnement par récurrence, on a donné ici l'équivalent de l'étape d'hérédité, il reste à se soucier de l'initialisation.

On fait naturellement cela par récurrence. Pour $n = 0$, la formule donne $u_0 = u$, ce qui est vrai par hypothèse. Supposons maintenant cette formule établie pour tout entier inférieur ou égal à n et prouvons-là pour l'entier $n+1$. On a successivement :

$$\begin{aligned} u_{n+1} &= au_n + b = a\left(a^n u + b \cdot \frac{a^n - 1}{a-1}\right) + b \\ &= a^{n+1}u + b\left(\frac{a^{n+1} - a}{a-1} + 1\right) = a^{n+1}u + b \cdot \frac{a^{n+1} - 1}{a-1} \end{aligned}$$

ce qui est bien ce que l'on désirait. On remarque en outre que dans ce cas, on a utilisé l'hypothèse de récurrence seulement pour le rang n ; ceci est somme toute assez normal puisque u_{n+1} était défini seulement en fonction de u_n.

Avant de passer à la suite, faisons plusieurs remarques. Tout d'abord, on a peut-être déjà remarqué que la formule démontrée est seulement valable dans le cas $a \neq 1$, n'ayant aucun sens sinon. Toutefois, il doit être possible de donner une formule, différente certes, pour le cas $a = 1$. Dans ces conditions, la relation de récurrence devient simplement $u_{n+1} = u_n + b$ et on peut imaginer directement qu'alors :

$$u_n = u_0 + nb$$

Il faut sans doute souligner le fait que cette dernière formule est en fait bien un « cas particulier » de la formule générale. On peut donner un sens très précis à l'affirmation suivante, mais ce qu'il faut remarquer ici, c'est que lorsque a se rapproche de 1, la fraction $\frac{a^n-1}{a-1}$ se rapproche, elle, de n, comme on le constate efficacement en regardant des valeurs numériques. La formule générale redonne ainsi la formule précédente pour le cas particulier $a = 1$.

Une dernière remarque pour finir ce paragraphe. En fait, l'étape difficile dans une démonstration par récurrence n'est souvent ni l'initialisation, ni l'hérédité mais plutôt la détermination exacte de la formule P_n que l'on va devoir manier. L'exemple précédent aurait été bien plus délicat à traiter si la formule à prouver n'était pas donnée *a priori*, et pourtant c'est souvent le cas et il faudra alors la deviner.

Voyons que même ici cela n'est pas insurmontable. Pour essayer de deviner quelque chose, on commence toujours par voir ce qu'il se passe pour les premiers termes. Ici, on a :

$$\begin{aligned} u_0 &= u \\ u_1 &= au + b \\ u_2 &= a^2u + ab + b = a^2u + b(a+1) \\ u_3 &= a^3u + ab(a+1) + b = a^3u + b\left(a^2 + a + 1\right) \\ u_4 &= a^4u + ab\left(a^2 + a + 1\right) + b = a^4u + b\left(a^3 + a^2 + a + 1\right) \end{aligned}$$

Ainsi, on imagine sans trop de mal que la formule générale doit être :

$$u_n = a^n u + b\left(a^{n-1} + \ldots + 1\right)$$

Il ne reste plus qu'à calculer la somme $S = 1 + \ldots + a^{n-1}$. Pour cela, on calcule $aS = a + \ldots + a^n$ et on fait la différence ; on obtient $aS - S = a^n - 1$. Finalement :

$$S = 1 + \ldots + a^{n-1} = \frac{a^n - 1}{a-1}$$

et on obtient bien la formule voulue. Il s'agit quand même de faire attention : ce qui précède n'a rien d'une démonstration rigoureuse et implacable, c'est juste un préambule à faire au brouillon. La vraie démonstration est bien celle que l'on a faite par récurrence juste avant.

5.2 Les suites homographiques

Il s'agit des suites définies par la formule de récurrence suivante :

$$u_{n+1} = \frac{au_n + b}{cu_n + d}$$

les nombres a, b, c et d étant des réels fixés. Là encore, il faut fixer une valeur pour u_0 pour déterminer complètement la suite ; disons que, comme tout à l'heure, $u_0 = u$ un certain réel fixé également.

On se propose une fois de plus de déterminer une formule explicite donnant directement la valeur de u_n. Nous allons en fait présenter la méthode *via* l'exercice suivant :

Exercice : On considère donc la suite (u_n) définie précédemment. On définit en outre la fonction $f : x \mapsto \frac{ax+b}{cx+d}$. On se souciera peu[16] de la valeur interdite $\frac{-d}{c}$ mais on retiendra que $u_{n+1} = f(u_n)$.

a) Prouver que l'équation $f(l) = l$ admet 0, 1 ou 2 solutions selon les valeurs choisies pour a, b, c et d.

On supposera dans la suite que l'équation $f(l) = l$ admet deux solutions distinctes que l'on appelera l_1 et l_2.

b) On définit la suite v_n par la formule :

$$v_n = \frac{u_n - l_1}{u_n - l_2}$$

Prouver que v_n vérifie une relation de récurrence simple. (On pourra pour cela commencer par calculer et simplifier $f(x) - f(y)$, x et y étant des réels quelconques).

c) En déduire une formule explicite pour v_n puis pour u_n.

Solution :

► **a)** L'équation $f(l) = l$ conduit directement à $cl^2 + (d-a)l - b = 0$. Il s'agit d'une équation de degré 2 (sauf dans le cas où $c = 0$; on remarque que ce cas a d'ailleurs déjà été traité dans le paragraphe précédent) qui admet 0, 1 ou 2 solutions selon le signe du discriminant $\Delta = (d-a)^2 + 4bc$.

b) Comme indiqué par l'énoncé, on commence par calculer :

$$\begin{aligned} f(x) - f(y) &= \frac{ax+b}{cx+d} - \frac{ay+b}{cy+d} = \frac{(ax+b)(cy+d) - (cx+d)(ay+b)}{(cx+d)(cy+d)} \\ &= \frac{acxy + adx + bcy + bd - acxy - bcx - ady - bd}{(cx+d)(cy+d)} \\ &= \frac{(ad-bc)(x-y)}{(cx+d)(cy+d)} \end{aligned}$$

Et maintenant :

$$\begin{aligned} v_{n+1} &= \frac{u_{n-1} - l_1}{u_{n-1} - l_2} = \frac{f(u_n) - f(l_1)}{f(u_n) - f(l_2)} \\ &= \frac{(ad-bc)(u_n - l_1)}{(cu_n + d)(cl_1 + d)} \times \frac{(cu_n + d)(cl_2 + d)}{(ad-bc)(u_n - l_2)} \\ &= \frac{cl_2 + d}{cl_1 + d} \times v_n \end{aligned}$$

[16] Normalement, il faudrait mais bon c'est un problème assez délicat qui n'apporte finalement pas grand-chose...

ce qui est effectivement satisfaisant pour une relation de récurrence simple : si on pose en outre $k = \frac{cl_2+d}{cl_1+d}$, on obtient $v_{n+1} = kv_n$, chose que l'on sait déjà traiter.

c) En utilisant les formules du paragraphe précédent, on obtient

$$v_n = k^n v_0 = k^n \cdot \frac{u - l_1}{u - l_2}$$

Maintenant il n'est plus bien difficile de trouver u_n. De la relation $v_n = \frac{u_n - l_1}{u_n - l_2}$ définissant v_n, on tire :

$$u_n = \frac{l_2 v_n - l_1}{v_n - 1} = \frac{l_2 k^n (u - l_1) - l_1 (u - l_2)}{k^n (u - l_1) - (u - l_2)}$$

ce qui n'est certes pas une formule très agréable, mais bon... ◀

5.3 La suite de Fibonacci

La suite de Fibonacci est celle qui est définie de la façon suivante :

$$\begin{cases} F_1 = F_2 = 1 \\ F_n = F_{n-1} + F_{n-2} \quad \text{pour } n \geqslant 3 \end{cases}$$

Le but est encore de calculer explicitement la valeur de F_n. En fait, nous n'allons pas le faire. Nous laissons au lecteur le plaisir immense de prouver par récurrence que :

$$F_n = \frac{\sqrt{5}}{5} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right]$$

Remarquons toutefois qu'une fois cette démonstration faite, elle prouvera *ipso facto* que le nombre défini par la formule précédente est un entier pour toute valeur de n, ce qui n'est pas évident *a priori*.

Remarquons également que la suite de Fibonacci apparaît dans divers contextes où on ne l'attend pas toujours. Un exemple est l'exercice suivant : on se demande de combien de façons on peut monter un escalier de n marches sachant que l'on monte les marches soit par une soit par deux, bien entendu en pouvant changer d'avis autant de fois qu'on le veut au cours de l'ascension.

Comme donner des noms aux choses permet souvent de mieux les apprivoiser, on appelle u_n ce nombre recherché. Pour des petits escaliers, on sait résoudre le problème. Si l'escalier a une marche, il n'y a qu'une façon de le gravir ; ainsi $u_1 = 1$. Si l'escalier a deux marches, il y a deux façons : soit on monte les deux marches à la fois, soit on y va pépère ; ainsi $u_2 = 2$.

Mettons-nous maintenant devant un escalier de n marches, avec $n \geqslant 3$. Au bas de l'escalier, on a deux possibilités : soit on monte une marche, soit deux. Si on a monté une marche, il nous restera évidemment $n - 1$ marches à gravir, sinon il nous en restera $n - 2$. De cela, on déduit la relation :

$$u_n = u_{n-1} + u_{n-2}$$

oh ! miracle, on retrouve la relation de Fibonacci. Ainsi on voit facilement que :

$$u_n = F_{n+1} = \frac{\sqrt{5}}{5} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{n+1} \right]$$

5.4 Le triangle de Pascal

On va se concentrer ici sur les suites $(u_{n,k})$ indexées à la fois par les indices n et k, eux deux parcourant $\mathbb{N}$. En fait, on va voir plus précisément comment on peut définir une telle suite de façon récurrente. Commençons tout de suite par un exemple. Soit donc la suite $(u_{n,k})$ définie par les relations suivantes :

$$\begin{cases} u_{n,0} = 1 & \text{pour tout } n \\ u_{0,k} = 0 & \text{pour tout } k \geqslant 1 \\ u_{n,k} = u_{n-1,k} + u_{n-1,k-1} & \text{pour } n > 0 \text{ et } k > 0 \end{cases}$$

Commençons par calculer les valeurs des « premiers » termes de la suites. On les reporte dans le tableau suivant :

n \ k	**0**	**1**	**2**	**3**	**4**	**5**
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

Disons en premier lieu que le tableau que l'on obtient ainsi s'appelle le *triangle de Pascal*. Les nombres qui apparaîssent dans ce tableau sont ce que l'on appelle les *coefficients binomiaux*, cette dernière terminologie s'expliquant avec la formule de binôme que nous allons voir par la suite. La quantité $u_{n,k}$ se note traditionnellement C_n^k

On remarque que les conditions données permettent de remplir toutes les cases du tableau : on commence par exemple par remplir la première ligne, on peut dès lors calculer les valeurs à mettre sur la seconde et ainsi de suite. Il faut peut-être dire que les cases non remplies dans le tableau correspondent à des 0.

Comme pour les autres cas traités, il est ici encore possible de donner une formule explicite pour C_n^k. Précisément, on a :

$$\begin{cases} \mathrm{C}_n^k = \dfrac{n!}{k!\,(n-k)!} & \text{si } k \leqslant n \\ \mathrm{C}_n^k = 0 & \text{sinon} \end{cases}$$

où $i!$ (lire *factorielle* i) désigne par définition le produit $1 \times 2 \times \ldots \times i$ et où par convention $0! = 1$.

La démonstration de cette dernière affirmation se fait à nouveau par récurrence. Toutefois, comme ce coup-ci, on a deux indices, il faut faire un peu plus attention à ce que l'on fait. Ici, ce ne sera pas compliqué : la récurrence ne va concerner que l'indice n. Précisément, l'énoncé P_n que l'on va considérer sera : « pour tout entier $k \geqslant 0$, le coefficient binômial C_n^k est donné par la formule ci-dessus ».

L'initialisation est simple : pour $n = 0$, on vérifie directement que la formule donnée redonne les mêmes valeurs que la définition. On suppose donc maintenant que tous les énoncés P_i sont vrais pour $i \leqslant n$ et on cherche à démontrer P_{n+1}.

Pour cela, il va bien sûr falloir distinguer plusieurs cas. En premier lieu, si $k = 0$, la formule $\frac{(n+1)!}{k!(n+1-k)!}$ vaut bien 1 comme le veut la définition de C_{n+1}^0.

Si maintenant k est compris entre 1 et n, il s'agit de prouver l'identité suivante :

$$\frac{(n+1)!}{k!\,(n+1-k)!} = \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!}$$

ce qui résulte de manipulations élémentaires que nous laissons au lecteur[17].

Finalement, pour les k strictement supérieur à n, il s'agit d'additionner des 0 entre eux, un 1 venant éventuellement jouer les trouble-fêtes. C'est tout à fait immédiat.

Tout cela prouve l'hérédité et démontre donc la formule annoncée.

Les coefficients binômiaux ont un intérêt immense en mathématiques et principalement en combinatoire. Ils apparaîssent en outre dans la formule du binôme de Newton qui donne le développement de $(a+b)^n$. Cette formule s'écrit ainsi :

$$(a+b)^n = \sum_{k=0}^{n} \mathrm{C}_n^k a^{n-k} b^k$$

le signe « $\sum$ » voulant dire que l'on fait varier k entre 0 et n, que pour chacun de ces k on évalue le terme écrit à côté du signe, et que l'on somme tous les termes obtenus (il y en a donc $n+1$). Par exemple si on l'applique pour $n = 5$, on trouve :

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

Il ne nous reste plus qu'à prouver cette formule. Bien sûr, cela va se faire une fois de plus par récurrence. Pour $n = 1$, la formule donne $a+b = a+b$, ce qui est effectivement une vérité incontestable. On suppose maintenant que la formule est vraie pour tout exposant inférieur ou égal à n et on peut prouver qu'elle reste vraie pour l'exposant $n+1$. On entreprend pour ce faire le calcul suivant :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)\,(a+b)^n = (a+b)\left(\sum_{k=0}^{n} \mathrm{C}_n^k a^{n-k} b^k\right) \\
&= \left(\sum_{k=0}^{n} \mathrm{C}_n^k a^{n-k+1} b^k\right) + \left(\sum_{k=0}^{n} \mathrm{C}_n^k a^{n-k} b^{k+1}\right) \\
&= a^{n+1} + \left(\sum_{k=1}^{n} \mathrm{C}_n^k a^{n-k+1} b^k\right) + \left(\sum_{k=0}^{n-1} \mathrm{C}_n^k a^{n-k} b^{k+1}\right) + b^{n+1} \\
&= a^{n+1} + \left(\sum_{k=1}^{n} \mathrm{C}_n^k a^{n+1-k} b^k\right) + \left(\sum_{k=1}^{n} \mathrm{C}_n^k a^{n+1-k} b^k\right) + b^{n+1} \\
&= a^{n+1} + \left(\sum_{k=1}^{n} \left(\mathrm{C}_n^k + \mathrm{C}_n^{k-1}\right) a^{n+1-k} b^k\right) + b^{n+1} \\
&= \sum_{k=0}^{n+1} \mathrm{C}_n^{k+1} a^{n+1-k} b^k
\end{aligned}$$

[17] Hé, hé !

Et ceci achève la démonstration. On remarque en outre que si l'on ne connaissait pas à l'avance les coefficients binômiaux C_n^k, le calcul précédent permet de trouver la relation de récurrence qui les définit. Bien sûr, accéder à la formule explicite est une autre paire de manches, mais dans d'autres situations il n'y aura pas forcément de formules explicites et connaître une relation de récurrence simple peut déjà aider énormément.

La chose à laquelle il faut prendre garde avec ces suites à multi-indices, c'est que le calcul de proche en proche ne se fait pas forcément ligne par ligne. Parfois, c'est plus compliqué et il faut donc adapter la façon de faire les récurrences ; il est par exemple possible que le tableau se construise en « diagonale », auquel cas, il faudra privilégier les récurrences sur la somme $n + k$.

5.5 L'opération « eXclusive OR »

Présentation de la suite

Voyons un autre exemple de suite récurrente ayant plusieurs indices. La définition par récurrence peut paraître ce coup-ci surprenante ; la voici :

$$u_{n,k} = \operatorname{mex}\left(\left\{u_{n',k},\ n' < n\right\} \cup \left\{u_{n,k'},\ k' < k\right\}\right) \tag{1}$$

où $\operatorname{mex} A$ est le plus petit entier naturel qui n'appartient pas à l'ensemble A. On remarque qu'un tel entier existe toujours dans les cas précédents puisque tous les ensembles considérés sont finis.

Afin de comprendre comment cela fonctionne, le plus simple est sans doute d'essayer de calculer les premiers termes. Regroupons les résultats dans le tableau suivant :

n \ k	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	0	3	2	5	4
2	2	3	0	1	6	7
3	3	2	1	0	7	6
4	4	5	6	7	0	1
5	5	4	7	6	1	0

Expliquons donc comment on parvient à un tel résultat. La formule nous dit que l'entier qui doit être écrit dans la case de coordonnées (n, k) doit être le plus petit qui n'est ni écrit à gauche ni au-dessus de ladite case. Ainsi, on remplit le tableau de gauche à droite et de haut en bas.

Pour la case $(0, 0)$, il n'y a aucune case qui lui soit située à gauche ou en haut. Il s'agit donc de prendre le plus petit entier ; c'est 0. Pour sa voisine de droite, il faut prendre le plus petit entier qui n'est pas 0, c'est donc 1. De même pour la voisine du dessous. Maintenant pour la case de coordonnées $(0, 2)$, il faudra prendre le plus petit entier qui n'est ni 0, ni 1 ; c'est donc bien 2. Ainsi de suite...

Cet exemple est une mine d'or si l'on veut s'entraîner à faire des récurrences simples : on s'amuse à repérer des propriétés sur la tableau et on essaie de les démontrer.

Par exemple, commençons par prouver que $u_{n,0} = n$ pour tout entier n. L'initialisation a déjà été faite : on a déjà calculé $u_{0,0} = 0$. Maintenant on suppose que $u_{n',0} = n'$ pour tout $n' \leqslant n$ et on veut calculer $u_{n+1,0}$. Par définition, étant donné qu'il n'y a pas d'entier strictement inférieur à 0, c'est le plus petit entier ne s'écrivant pas $u_{n',0}$ pour $n' < n+1$, c'est-à-dire $n' \leqslant n$. Mais on les connait ces entiers justement : $u_{n+1,0}$ est donc le plus petit entier qui n'est ni 0, ni 1, ..., ni n : c'est bien $n+1$. Ceci achève donc l'étape d'hérédité et la démonstration.

Une deuxième chose que l'on peut remarquer et prouver, peut-être un poil plus difficile, est que pour tout entier n, $u_{n,n} = 0$. Allons-y. L'initialisation est déjà connue. Passons directement à l'hérédité : on suppose donc que pour tout $n' \leqslant n$, $u_{n',n'} = 0$ et il s'agit de calculer $u_{n+1,n+1}$. C'est par définition le plus petit nombre qui ne s'écrit ni $u_{n',n+1}$, ni $u_{n+1,n'}$ pour $n' \leqslant n$. Le problème est qu'apparemment on ne connaît rien sur ces nombres.

Toutefois, ce que l'on souhaite, c'est arriver à la conclusion selon laquelle $u_{n+1,n+1} = 0$. Il suffit donc de prouver que 0 n'apparaît pas parmi les $u_{n',n+1}$ et les $u_{n+1,n'}$, n' étant toujours inférieur ou égal à n. Voyons donc comment est défini $u_{n',n+1}$: c'est le plus petit entier qui ne s'écrit ni sous la forme $u_{p,n+1}$ pour $p < n'$ ni sous la forme $u_{n',q}$ pour $q \leqslant n$. Mais parmi ces entiers, il y a $u_{n',n'}$ qui est nul par hypothèse de récurrence, ce qui assure la non-nullité de $u_{n',n+1}$. De la même façon, on prouve la non-nullité de $u_{n+1,n'}$ et la conclusion en découle.

Prouvons un dernier fait : pour tous entiers n et k, $u_{n,k} = u_{k,n}$. Ce coup-ci, on a deux indices et il faut choisir comment faire la récurrence. En fait, à peu près toutes les choses auxquelles on peut penser fonctionnent. Nous allons pour le plaisir[18] faire une récurrence sur la somme $n+k$, ce qui n'est pas forcément le plus simple, mais pas forcément le plus compliqué non plus.

Notre énoncé de récurrence va dépendre d'un nouveau paramètre s et sera le suivant : « pour tout couple d'entiers (n,k) tels que $n+k=s$, on a $u_{n,k} = u_{k,n}$ ». Si l'on veut voir comment les choses se passent « géométriquement », il faut constater que l'on prouve non pas le résultat ligne par ligne ou colonne par colonne mais en se déplaçant en diagonale dans le tableau.

Voyons comment la récurrence fonctionne. L'étape d'initialisation est simple. Le seul couple d'entier (n,k) pour lequel $n+k=0$ est le couple $(0,0)$ et il est incontestable que $u_{0,0} = u_{0,0}$. Montrer l'hérédité revient à supposer que pour tous les couples (n,k) tels que $n+k \leqslant s$, on a $u_{n,k} = u_{k,n}$ et à montrer que la conclusion demeure pour les couples (n,k) tels que $n+k = s+1$. Prenons donc n et k vérifiant $n+k = s+1$ et voyons ce que valent respectivement $u_{n,k}$ et $u_{k,n}$.

Le premier est défini comme étant le plus petit entier ne s'écrivant ni sous la forme $u_{n',k}$ pour $n' < n$, ni sous la forme $u_{n,k'}$ pour $k' < k$. Le second, quant à lui, est défini comme étant le plus petit entier ne s'écrivant ni sous la forme $u_{k,n'}$ pour $n' < n$, ni sous la forme $u_{k',n}$ pour $k' < k$. Mais si $k' < k$, $k' + n < s+1$ ou encore $k' + n \leqslant s$ et donc le couple (k',n) relève de l'hypothèse de récurrence, ce qui assure $u_{k',n} = u_{n,k'}$. De la même façon $u_{n',k} = u_{k,n'}$. Les deux entiers que l'on veut comparer sont donc définis de la même façon ; ils sont par le fait égaux. Cela conclut.

Bien entendu, évoquer un argument de symétrie eût conduit à une démonstration plus simple. Une façon d'exploiter cette idée est de développer l'argument suivant. On a vu que

[18] En fait, surtout pour montrer ce que peut donner ce genre de raisonnements.

la relation (1) suffit à elle seule à définir la double suite $(u_{n,k})$. Ainsi si $(v_{n,k})$ désigne une autre suite et que l'on arrive à prouver que cette suite vérifie la même relation (1), on aura prouvé que pour tous entiers n et k, $u_{n,k} = v_{n,k}$.

Cette dernière remarque s'applique à notre situation en prenant $v_{n,k} = u_{k,n}$. La conclusion est alors immédiate.

Une méthode de calcul

Il est encore possible de donner une « formule » explicite pour le calcul de $u_{n,k}$. Pour expliquer cette formule, il va nous falloir dans un premier temps expliquer la base 2. On fait remarquer que « la base 2 » n'est pas quelque chose d'anecdotique et permet de résoudre nombreux problèmes et de comprendre nombreuses théories.

L'idée est fort simple : on décrète qu'à partir de maintenant, on ne comptera plus qu'avec deux chiffres, en l'occurrence `0` et `1`. Pour compter, on utilise toujours la même méthode : on commence à `0` ; on incrémente ensuite tant que l'on peut le chiffre des unités, lorsque l'on ne peut plus, on le remet à `0` et on incrémente le chiffre des dizaines[19] ; si l'on ne peut plus incrémenter ce chiffre, on le remet à `0` à son tour et on incrémente celui des centaines et ainsi de suite.

Après application de cet algorithme, on obtient la liste des premiers nombres écrits en base 2 :

`0`, `1`, `10`, `11`, `100`, `101`, `110`, `111`, `1000`, `1001`, `1010`, `1011`, etc.

Le n-ième nombre ainsi listé (on commence à compter à 0) est ce que l'on appelle l'*écriture en base* 2 de l'entier n. Ainsi l'écriture en base 2 de 1 est `1`, celle de 9 est `1001`. Il serait sans doute bon d'expliquer maintenant comment on retrouve un nombre à partir de son écriture en base 2 et réciproquement.

Plusieurs remarques simples vont permettre de nous donner de précieux indices. Tout d'abord dans la liste des nombres, il apparaît évidemment en premier lieu les nombres à un seul chiffre, puis ceux de deux chiffres et ainsi de suite. D'autre part, il y a exactement 2^n nombres qui s'écrivent avec moins de n chiffres : pour chaque emplacement on a le choix entre `0` et `1` et bien sûr toutes les suites possibles de chiffres apparaîssent. De cela, on déduit que le premier nombre à $n+1$ chiffres (*ie* `1` suivi de n `0`) sera le 2^n-ième de la liste[20].

Mais si maintenant, on regarde ce qui vient après ce premier nombre à $n+1$ chiffres, on constate que c'est exactement la liste prise du début mais avec ce `1` en plus ; évidemment, c'est la même construction. Dans un langage plus mathématique, on vient de dire que la position du nombre $\texttt{1}x_{n-1}x_{n-2}\dots x_0$ (où les x_i sont des chiffres pris parmi `0` et `1` est celle du nombre $x_{n-1}x_{n-2}\dots x_0$ augmentée de 2^n. Finalement[21], on trouve que la position du nombre $x_n \dots x_0$ est :

$$x_n 2^n + x_{n-1}2^{n-1} + \dots + x_0$$

Maintenant que l'on sait convertir de la base 2 en base 10 (*ie* trouver la position connaissant le nombre), on voudrait s'intéresser à l'opération inverse. Prenons par exemple l'entier 217 et essayons de trouver quel nombre doit être écrit à la 217-ième place. D'après

[19] Il ne faut sans doute plus dire « dizaines » pour parler du deuxième chiffre en partant de la droite lorsque l'on compte en base 2, mais bon...

[20] Remarquez que cela fonctionne aussi pour $n = 0$.

[21] Le lecteur pas vraiment convaincu pourra prouver le résultat par récurrence lui-même.

ce qui précède, il s'agit d'écrire 217 comme une somme de puissances de 2. Quelles sont donc les puissances de 2 ? Il y a dans l'ordre : 1, 2, 4, 8, 16, 32, 64, 128, 256, etc. Je m'arrête à 256 car il est clair que lui et les suivants ne pourront pas intervenir pour donner un résultat aussi minable que 217.

Il y a maintenant deux façons de voir les choses : soit on commence par le haut, soit un commence par le bas. Commençons par le haut dans un premier temps. On a dit qu'il ne fallait pas prendre 256 mais 128 on peut, mais en fait c'est même obligatoire car la somme des autres puissances arrivent à peine à 127. On prend donc 128, il nous reste $217-128 = 89$ à faire. On fait pareil : on prend la puissance de 2 immédiatement inférieure à 89, c'est ici 64. Il reste ensuite 25, on prend donc 16. Au final, on obtient :

$$217 = 128 + 64 + 16 + 8 + 1$$

et donc le 217-ième nombre listé sera `11011001`.

Si on commence par le bas, maintenant, comment faut-il procéder ? On remarque que toutes les puissances de 2 sont paires, à l'exception de $2^0 = 1$. Et 217 est impair, il faut donc obligatoirement prendre ce 1. Il nous reste maintenant 216 à faire et on ne doit prendre que des puissances de 2 paires ; il nous reste donc $\frac{216}{2} = 108$ à faire avec toutes les puissances de 2. Ce coup-ci 108 est pair, il ne faut donc pas prendre le 1, c'est-à-dire qu'il ne faut pas prendre le 2 pour 217. On divise encore par 2 et regarde à nouveau la parité et ainsi de suite.

Fort de savoir écrire les nombres en base 2, on va pouvoir définir ce que l'on appelle le *ou exclusif* (*eXclusive OR* en anglais) que l'on note souvent XOR et que l'on notera nous #. La méthode de calcul est la suivante. On part de deux entiers, par exemple 1548 et 217. On écrit ces nombres en base 2 et on pose l'opération suivante :

$$\begin{array}{rr} & \texttt{11000001100} \\ \# & \texttt{11011001} \\ \hline & \texttt{11011010101} \end{array}$$

qui est une addition sans retenue. Ainsi lorsque deux chiffres différents sont écrits l'un en dessous de l'autre, le résultat sera `1`, sinon il sera `0`. Sur notre exemple, on obtient $1548 \# 217 = 1749$.

Nous allons maintenant prouver que $u_{n,k} = n \# k$. Et pour cela, nous allons simplement démontrer que $(n, k) \mapsto n \# k$ vérifie la relation (1). On prend donc n et k deux entiers et on veut montrer deux choses :

1. $n \# k \neq n' \# k$ pour tout $n' < n$ et $n \# k \neq n \# k'$ pour tout $k' < k$
2. tout entier $a < n \# k$ s'écrit soit sous la forme $n' \# k$ pour un $n' < n$, soit sous la forme $n \# k'$ pour un $k' < k$

La première chose est plutôt simple à voir. Il s'agit d'une propriété « négative », on raisonne donc par l'absurde. Que se passerait-il donc si on avait $n \# k = n' \# k$ avec $n' < n$? Il est pas bien difficile, en regardant comme on a défini l'opération # de se convaincre que l'égalité $n \# k = n' \# k$ va entraîner $n = n'$, ce qui est absurde.

Une façon plus rigoureuse d'obtenir la dernière implication est de « composer par $\# k$ des deux côtés ». Précisément si $n \# k$ et $n' \# k$ sont égaux alors il en est de même de $(n \# k) \# k$ et $(n' \# k) \# k$ mais ces deux dernières quantités sont respectivement égales à n et à n'. On en déduit bien ce que l'on voulait.

Passons donc à la seconde propriété. On considère un entier a strictement inférieur à $n \# k$. Dans ces conditions, l'écriture en base 2 de ces deux entiers sera forcément de la forme suivante :

$$\begin{aligned} a &: a_1 \dots a_p \mathtt{0} \dots \\ n \# k &: a_1 \dots a_p \mathtt{1} \dots \end{aligned}$$

Ainsi, n et k s'écrivent par exemple :

$$\begin{aligned} n &: n_1 \dots n_p \mathtt{1} \dots \\ k &: k_1 \dots k_p \mathtt{0} \dots \end{aligned}$$

Bien sûr le `1` et le `0` peuvent être intervertis, mais il y a forcément deux chiffres différents à cette position puisque leur *ou exclusif* vaut `1`. On traite ce cas pour l'instant, l'autre se faisant en fait de façon tout à fait similaire.

En outre, on n'oublie pas que l'on a la relation $n_i \# k_i = a_i$, qui implique $a_i \# k_i = n_i$. Finalement $a \# k$ s'écrit :

$$n' = a \# k \quad : \quad n_1 \dots n_p \mathtt{0} \dots$$

Ce nombre est donc strictement plus petit que n et il vérifie en outre $n' \# k = a$, ce qui est exactement ce que l'on voulait.

Ceci termine donc la preuve et la relation de récurrence (1) définit une suite dont le terme général est :

$$u_{n,k} = n \# k$$

ce que l'on peut s'amuser à vérifier sur les premières valeurs calculées dans le tableau.

5.6 Digression sur l'intérêt de la base 2

L'écriture en base 2 est particulièrement intéressante lorsque l'on a affaire à des suites récurrentes pour lesquelles u_{2n} et u_{2n+1} sont tous les deux définis en fonction de u_n. La raison en est que si n s'écrit $n_p \dots n_0$ en base 2, alors $2n$ va s'écrire $n_p \dots n_0 \mathtt{0}$ et $2n+1$ s'écrira $n_p \dots n_0 \mathtt{1}$. Ainsi très souvent, les propriétés de ces suites se lisent sur leur écriture en base 2.

Bien entendu, si ce sont les nombres u_{3n}, u_{3n+1} et u_{3n+2} qui sont définis en fonction de u_n, il sera judicieux de compter en base 3 et ainsi de suite.

Pour illustrer ces idées, proposons l'exercice suivant :

Exercice (OIM 1988) : On désigne par f l'application de l'ensemble des entiers strictement positifs dans lui-même définie par les conditions suivantes :

$$f(1) = 1, \quad f(3) = 3$$

et pour tout entier n strictement positif :

$$\begin{aligned} f(2n) &= f(n) \\ f(4n+1) &= 2f(2n+1) - f(n) \\ f(4n+3) &= 3f(2n+1) - 2f(n) \end{aligned}$$

Déterminer le nombre des entiers n, $1 \leqslant n \leqslant 1988$ pour lesquels $f(n) = n$.

Solution :
► Étant donnée la définition de f, il est sans doute souhaitable de regarder le comportement de cette fonction sur les nombres écrits en base 4 ou 2. Commençons par 2, ça ne peut pas faire de mal.

Comme on voit pas très bien *a priori*, ce que f pourrait vouloir faire avec les chiffres de l'écriture en base 2, on calcule les premières valeurs :

1	$\mapsto$	1	1	$\mapsto$	1
2	$\mapsto$	1	10	$\mapsto$	01
3	$\mapsto$	3	11	$\mapsto$	11
4	$\mapsto$	1	100	$\mapsto$	001
5	$\mapsto$	5	101	$\mapsto$	101
6	$\mapsto$	3	110	$\mapsto$	011
7	$\mapsto$	7	111	$\mapsto$	111
8	$\mapsto$	1	1000	$\mapsto$	0001
9	$\mapsto$	9	1001	$\mapsto$	1001
10	$\mapsto$	5	1010	$\mapsto$	0101
11	$\mapsto$	13	1011	$\mapsto$	1101
12	$\mapsto$	3	1100	$\mapsto$	0011
13	$\mapsto$	11	1101	$\mapsto$	1011

Rapidement ou non, on constate finalement que f semble inverser l'écriture en base 2. Plus précisément si a s'écrit en base 2, $a_p \dots a_0$ où a_p est 1, il semblerait que $f(x)$ soit le nombre qui s'écrive $a_0 \dots a_p$ en base 2

Essayons de prouver ce fait. On raisonne évidemment par récurrence. On ne sait pas trop que faire pour l'étape d'initialisation puisque l'on a une valeur pour $f(1)$ et une pour $f(3)$; disons que l'on vérifie jusqu'à 4, ce qui de toute façon a déjà été fait.

Il reste à prouver l'hérédité. Supposons donc que f fasse bien ce que l'on veut d'elle sur les entiers $1, \dots, n$ et prouvons le pour l'entier $n+1$. Il y a alors trois cas à distinguer.

• Tout d'abord si $n+1$ est pair, alors il s'écrit $2k$ pour un certain entier k. Supposons que k s'écrive $k_p \dots k_0$ en base 2 où k_p vaut 1. Alors $2k$ s'écrit :

$$2k \quad : \quad k_p \dots k_0 0$$

et par hypothèse de récurrence, $f(k)$ s'écrit :

$$f(k) \quad : \quad k_0 \dots k_p$$

ce qui correspond bien à l'écriture renversée. L'hérédité est donc prouvée dans ce cas.

• Maintenant si $n+1$ s'écrit $4k+1$ pour un certain entier k. Écrivons encore k en base 2 : $k_p \dots k_0$. Alors $4k+1$ s'écrit :

$$4k+1 \quad : \quad k_p \dots k_0 01$$

et en utilisant l'hypothèse de récurrence on peut poser l'opération suivante :

$$\begin{array}{rrcr} & 2f(2k+1) & : & 1k_0 \dots k_p 0 \\ - & f(k) & : & k_0 \dots k_p \\ \hline & & & 10k_0 \dots k_p \end{array}$$

ce qui est bien ce que l'on veut encore une fois.

• Finalement si $n+1$ s'écrit $4k+3$ pour un certain entier k. Écrivons encore k en base 2 : $k_p \dots k_0$. Alors $4k+3$ s'écrit :

$$4k+3 \quad : \quad k_p \dots k_0 \texttt{11}$$

et en utilisant l'hypothèse de récurrence on peut poser l'opération suivante :

$$\begin{array}{rrcr} & 2f\left(2k+1\right) & : & \texttt{1}k_0 \dots k_p\texttt{0} \\ + & f\left(2k+1\right) & : & \texttt{1}k_0 \dots k_p \\ - & 2f\left(k\right) & : & k_0 \dots k_p\texttt{0} \\ \hline & & & \texttt{11}k_0 \dots k_p \end{array}$$

la première et la troisième ligne se simplifiant bien. Cela conclut l'hérédité.

Il ne reste plus qu'à compter le nombre d'entiers « symétriques en base 2 » et inférieurs à 1988. Commençons peut-être par écrire ce nombre en base 2 : c'est `11111000100`. Ce nombre s'écrit avec 11 chiffres, on n'aura donc pas encore trop de problèmes pour dénombrer le nombre de solutions de moins de 10 chiffres.

Avec un seul chiffre, il n'y a qu'une solution ; c'est `1`. Avec deux chiffres, il n'y a aussi qu'une seule solution ; c'est `11`. Avec trois chiffres, maintenant, le premier est forcément fixé à `1` et par conséquent le dernier aussi, mais on a libre choix sur celui du milieu, il y a donc deux solutions.

De la même façon pour p valant 5, 7 ou 9, il va y avoir $2^{\frac{p-1}{2}}$ solutions de p chiffres. Pour les p pairs, donc valant 4, 6, 8 ou 10, il y aura $2^{\frac{p-2}{2}}$ solutions. Ainsi parmi les nombres qui ont moins de 10 chiffres, on dénombre $1+1+2+2+4+4+8+8+16+16 = 62$ solutions.

Voyons les nombres de 11 chiffres maintenant. Une solution éventuelle doit s'écrire en base 2 sous la forme suivante :

`1_____1`

les cinq premiers « `_` » représentant *a priori* des chiffres arbitraires, et les quatre derniers étant déterminés par le choix des premiers. Toutefois pour que ce nombre reste inférieur à `11111000100`, il faut imposer que les quatre premiers « `_` » ne soient pas simultanément des `1`, et c'est en fait la seule contrainte. On dénombre alors $\left(2^4-1\right) \times 2 = 30$ solutions dans cette situation.

Au final l'équation proposée admet 92 solutions. ◄

5.7 Parité des coefficients binômiaux

On se demande dans ce chapitre à quelles conditions sur les entiers n et k, le coefficient binômial C_n^k est pair. La réponse n'est pas forcément évidente mais est assez élégante. On commence par écrire n et k en base 2 ; on obtient par exemple :

$$\begin{array}{rcl} n & : & n_p \dots n_0 \\ k & : & k_p \dots k_0 \end{array}$$

Dans ces conditions, C_n^k est un nombre pair si et seulement si il existe un indice i compris entre 0 et p pour lequel à la fois $n_i = 0$ et $k_i = 1$. (On dira alors que le couple (n,k) vérifie le critère (C)).

Encore une fois, nous allons prouver ce résultat par récurrence sur n. L'initialisation est facile. Si $n = 0$, n s'écrit en base 2 simplement avec des chiffres `0`, donc dès qu'il arrive un `1` dans l'écriture en base 2, c'est-à-dire dès que k est non nul, la condition que l'on a donnée ne va pas être vérifiée. D'autre part, le seul k qui soit tel que C_0^k soit non nul est $k = 0$, et alors $\mathrm{C}_0^0 = 1$. Ainsi, C_0^k est pair si et seulement si k est non nul. En mettant les deux choses précédentes ensemble, on peut conclure pour l'initialisation.

Voyons maintenant l'hérédité. Prenons un entier n et supposons que pour tous les $n' \leqslant n$, l'équivalence donnée précédemment soit vérifiée. Il s'agit de la montrer pour $n+1$. Il faut traiter le cas $k = 0$ à part, puisque la définition de C_n^k traite ce cas à part. On a alors $\mathrm{C}_n^0 = 1$ qui est un nombre impair. En outre, il n'apparaît dans l'écriture en base 2 de k que des `0` de sorte qu'il n'existe aucun indice i pouvant vérifier la condition. On a donc bien l'équivalence dans ce cas.

On suppose désormais $k > 0$, et l'on peut ainsi écrire :

$$\mathrm{C}_{n+1}^k = \mathrm{C}_n^k + \mathrm{C}_n^{k-1}$$

La stratégie consiste alors à étudier la parité de chacun de deux termes de la somme précédente, ceci bien entendu en fonction du critère donné, et à en déduire celle de C_{n+1}^k. Commençons donc par écrire n et $k-1$ en base 2 :

$$\begin{aligned} n &: n_p \dots n_{N+1}\texttt{01}\dots\texttt{1} \\ k-1 &: k_p \dots k_{K+1}\texttt{01}\dots\texttt{1} \end{aligned}$$

où donc les indices N (resp. K) désigne la position du dernier `0` de l'écriture en base 2 de n (resp. $k-1$). Cela permet évidemment de savoir comment vont s'écrire $n+1$ et k en base 2. Plus précisément, on aura :

$$\begin{aligned} n+1 &: n_p \dots n_{N+1}\texttt{10}\dots\texttt{0} \\ k &: k_p \dots k_{K+1}\texttt{10}\dots\texttt{0} \end{aligned}$$

Il y a maintenant trois cas à distinguer selon les positions relatives de N et de K.

• Commençons par le plus simple, celui où $N = K$. Dans ces conditions, d'après l'hypothèse de récurrence, C_n^k sera forcément pair, puisqu'en position $N = K$, il y aura respectivement un `0` dans n et un `1` dans k.

On distingue maintenant deux sous-cas selon la parité de C_n^{k-1}. Toujours d'après l'hypothèse de récurrence, si C_n^{k-1} est pair, alors il va exister un indice i pour lequel $n_i = 0$ et $k_i = 1$, mais cela ne peut arriver pour les indices $i \leqslant N = K$. Ainsi, il va exister un indice i tel que $n_i = 0$, $k_i = 1$ et $N + 1 \leqslant i \leqslant p$, et donc le couple $(n+1, k)$ va vérifier le critère (C). En outre, C_{n+1}^k va être un nombre pair, comme somme de deux nombres pairs. On a bien l'équivalence dans ce cas.

On traite de la même façon le cas où C_n^{k-1} est impair.

• Si $N < K$, alors en regardant en position N et en utilisant l'hypothèse de récurrence, on voit que C_n^{k-1} est un nombre pair.

Comme tout à l'heure, on commence par regarder ce qu'il se passe si C_n^k est pair. Dans ce cas, soit $n_K = 0$, soit il existe un indice $i \geqslant K+1$ tel que $n_i = 0$ et $k_i = 1$. On constate alors que quoi qu'il en soit le couple $(n+1, k)$ vérifie le critère (C). De plus, C_{n+1}^k est pair, comme somme de deux nombres pairs, ce qui conclut.

On traite l'autre cas de façon analogue.

• Finalement, si $N > K$, alors en regardant en position K, on voit que le couple $(n+1, k)$ vérifie toujours le critère (C). Il s'agit donc de montrer que les nombres C_n^k et C_n^{k-1} sont de même parité.

Si C_n^k est pair, c'est soit que k_N est pair, soit qu'il existe un indice $i \geqslant N+1$ tel que $n_i = 0$ et $k_i = 1$. On voit que cela implique que le couple $(n, k-1)$ vérifie le critère (C) et donc que C_n^{k-1} est pair. Youpi.

On fait de même si C_n^k est impair.

Ceci extermine[22] l'hérédité et la récurrence.

Là encore, on peut se demander comment l'on peut penser à un tel critère. Il ne tombe pas du ciel encore une fois et quelques expérimentations simples permettent de le deviner. Nous allons essayer de les exposer. Tout d'abord, redessinons le tableau de Pascal en remplaçant les nombres pairs par des 0 et les impairs par des 1. On obtient :

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	10	11	12	13	14	15	16
0	1																
1	1	1															
2	1	0	1														
3	1	1	1	1													
4	1	0	0	0	1												
5	1	1	0	0	1	1											
6	1	0	1	0	1	0	1										
7	1	1	1	1	1	1	1	1									
8	1	0	0	0	0	0	0	0	1								
9	1	1	0	0	0	0	0	0	1	1							
10	1	0	1	0	0	0	0	0	1	0	1						
11	1	1	1	1	0	0	0	0	1	1	1	1					
12	1	0	0	0	1	0	0	0	1	0	0	0	1				
13	1	1	0	0	1	1	0	0	1	1	0	0	1	1			
14	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1		
15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
16	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

La première remarque à faire consiste à dire que pour construire le tableau précédent, on n'est pas du tout obligé de regarder la parité des coefficients qui apparaîssent dans le tableau de Pascal. Il suffit plutôt de remarquer que la somme de deux nombres pairs ou de deux nombres impairs donne un résultat pair, alors que la somme d'un nombre pair et d'un nombre impair donne un résultat impair. On utilise ensuite la définition par récurrence.

Plus précisément, on construit le tableau comme on construisait le tableau de Pascal, sauf que lorsque l'on a à faire « $1+1$ », on écrit 0 et pas 2.

Maintenant, il faut observer, contempler et conjecturer. Ce que l'on peut remarquer, c'est que les lignes 2, 4, 8 et 16, c'est-à-dire les lignes puissances de 2, sont d'une forme bien particulière : elles semblent commencer et se terminer par un 1 (mais cela est obligatoire et évident) mais ne contenir que des 0 sinon. Que l'on sache ou non montrer cela[23], prenons-le pour acquis.

Une conséquence majeure va alors apparaître. Par exemple, les lignes de 8 à 15 vont forcément être deux copies mises côte-à-côté des lignes 0 à 7, comme la méthode de construction du tableau le prouve directement. De la même façon les lignes de 2^n à $2^{n-1}-1$ vont être deux copies mises côte à côte des lignes de 0 à $2^n - 1$.

[22] Une variante de « achève ». Un délire de sup, vous ne pouvez sans doute pas comprendre ce qui peut m'amuser là-dedans.

[23] Ce résultat est bien entendu une conséquence du critère précédemment énoncé, mais on peut le montrer directement de manière relativement simple.

Et lorsque l'on essaie de comprendre ce que peut entraîner tout cela, on pense à écrire les nombres n et k en base 2 et on obtient finalement le critère énoncé au début du paragraphe.

Il est intéressant finalement de griser les cases impaires et de regarder le dessin obtenu.

Il est intéressant finalement de généraliser le résultat précédent en remplaçant 2 par un nombre premier quelconque. Le théorème est alors le suivant :

Théorème 5

Soit p un nombre premier. Soient n et k deux entiers dont l'écriture en base p est donnée par les formules suivantes :

$$\begin{aligned} n &= n_d p^d + n_{d-1} p^{d-1} + \ldots + n_1 p + n_0 \\ k &= k_d p^d + k_{d-1} p^{d-1} + \ldots + k_1 p + k_0 \end{aligned}$$

les n_i et les k_i étant donc des entiers compris entre 0 et $p-1$. Alors on a la congruence suivante :

$$C_n^k \equiv C_{n_d}^{k_d} \cdot C_{n_{d-1}}^{k_{d-1}} \cdot \ldots \cdot C_{n_1}^{k_1} \cdot C_{n_0}^{k_0} \pmod{p}$$

cette dernière écriture signifiant que la différence des deux termes écrits de part et d'autre du signe « $\equiv$ » est un multiple de p.

Ce dernier résultat implique donc que s'il existe un indice i tel que $k_i > n_i$ alors le nombre C_n^k est un multiple de p. C'est exactement cela le critère que l'on avait annoncé dans le cas $p = 2$.

6 Constructions

Nous allons voir dans ce chapitre que parfois il ne faut pas hésiter à mettre les choses comme on veut qu'elles le soient.

6.1 Nombres univers et nombres normaux

Un *nombre univers* (en base 10) est un nombre réel pour lequel on peut trouver n'importe quelle suite de chiffres dans son développement décimal. Ainsi dans un tel nombre, on trouvera après la virgule un 3 quelque part, mais aussi un 4, et aussi un 12, et aussi un 154876 et tout ce que l'on veut ainsi.

Ce que l'on peut remarquer d'ores et déjà, c'est que dans un nombre univers, il va apparaître non seulement un 3, mais en fait une infinité de 3 après la virgule. En effet, il devra apparaître $30, 31, \ldots, 39$, ce qui fait déjà pas moins de dix 3 (évidemment, ce ne sera pas les mêmes : un 3 qui est suivi d'un 0 n'est pas suivi d'un 1). Mais il devra apparaître aussi $300, \ldots, 399$, ce qui amène déjà le nombre de 3 à cent. En considérant les nombres à quatre chiffres, on trouve mille 3 distincts, et ainsi de suite.

Trouver des nombres qui ne sont pas univers est quelque chose de facile. Pour prendre un exemple bête, les entiers ne sont pas des univers : après la virgule, on ne trouve rien d'autre que des 0. La fraction $\frac{1}{3}$ n'est pas non plus un nombre univers ; ce coup-ci il n'y a que des 3.

La question est maintenant d'en exhiber un, de nombre univers. On peut penser aux fractions mais cela ne marche pas (voir plus loin). On peut ensuite penser à des constantes plus farfelues comme $\sqrt{2}$ ou π... Ces nombres sont selon toute probabilité univers mais personne aujourd'hui ne sait encore le prouver. On n'est donc guère plus avancé.

Pourtant obtenir un nombre univers est tout ce qu'il y a de plus facile, il suffit d'écrire ce que l'on veut. Et ce que l'on veut c'est le nombre suivant :

0 , 0 1 2 3 4 5 6 7 8 9 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 . . .

On voit bien comment ce spécimen est fabriqué : on commence par écrire « 0, » et on ajoute derrière successivement les chiffres un par un jusqu'à épuisement, puis les suites de deux chiffres jusqu'à épuisement, on mettra ensuite les suites de trois chiffres et ainsi de suite. On obtient à l'évidence un nombre univers.

Venons-en maintenant aux nombres normaux. Un *nombre normal* (en base 10) est un nombre pour lequel les 0 apparaîssent avec une fréquence de $\frac{1}{10}$ (cela signifie que si on appelle $z(n)$ le nombre de zéros rencontrés avant la n-ième décimale, on a $\lim_{n\to\infty} \frac{z(n)}{n} = \frac{1}{10}$[24]), les 1 apparaîssent avec une fréquence de $\frac{1}{10}$, les 10 avec une fréquence de $\frac{1}{100}$, les 1847 avec une fréquence de $\frac{1}{10000}$ et de même pour toute suite finie de chiffres.

De façon évidente, tout nombre normal est aussi un normal univers. Le contraire, par contre, demande un peu plus de réflexion. Existe-t-il des nombres univers qui ne sont pas normaux ? Le nombre que l'on a construit ci-dessus est-il normal ? Ces deux dernières questions ne sont *a priori* pas évidentes. Nous allons toutefois répondre à la première : la réponse est positive et de fait il est facile comme précédemment de construire un tel

[24] Je reste et je resterai volontairement flou sur les limites et les problèmes que cela entraîne, ce genre de questions très intéressantes au demeurant ne rentrant pas vraiment dans les choses que je veux présenter. Je ne me soucierai jamais par exemple du problème de la non-existence de ladite limite.

nombre. On souhaite que toutes les suites finies de chiffres soient représentées mais on souhaite également par exemple que le chiffre 0 soit sur-représenté[25]. Qu'à cela ne tienne, on prend simplement :

$$0\,,\ 0\,0\,1\,0\,2\,0\,3\,0\,4\,0\,5\,0\,6\,0\,7\,0\,8\,0\,9\,0\,00\,00\,01\,00\,02\,00\,03\,00\,04\,00\,05\,00\,06\,00\,07\,00\ \ldots$$

Entre deux suites consécutives que l'on veut voir apparaître dans notre nombre univers, on ajoute autant de 0 que nécessaire pour être sûr qu'au final ils auront une proportion supérieure à $\frac{1}{2}$ et donc ne pouvant pas égaler $\frac{1}{10}$.

On a construit un nombre univers qui n'était pas normal, mais peut-on quand même construire un nombre normal. Évidemment et si l'on excepte les détails techniques ennuyeux, les idées sont très similaires aux précédentes. On écrit tout d'abord « 0, » et on s'occupe dans un premier temps des suites d'un seul chiffre : pour cela, on répète suffisamment de fois la séquence 0 1 2 3 4 5 6 7 8 9 pour que la proportion de 0, de 1, etc. se stabilise (à quelque chose de petit près), donc à $\frac{1}{10}$. On s'occupe ensuite des suites de deux chiffres et pour cela on répète la séquence 00 01 02 ... 99, encore jusqu'à avoir une stabilisation suffisante.

Bon, ce qui précède n'est que l'idée ; il y a énormément de détails techniques à régler... nous souhaitons bon courage au lecteur qui veut écrire cela proprement.

6.2 Nombres rationnels et périodicité

On a déjà donné un exemple explicite de nombre irrationnel, en l'occurrence $\sqrt{2}$, mais il est remarquable de se rendre compte que les méthodes utilisées précédemment permettent également d'aboutir à un tel nombre.

Pour cela, nous allons essayer de comprendre comment se comporte la suite des décimales d'un nombre rationnel. Prenons donc par exemple $\frac{1}{7}$ et posons la division. On a :

1	7
10	0 , 142 857 1
30	
20	
60	
40	
50	
10	
3	

La séquence 142 857 va se répéter infiniment. Évidemment, on est retombé sur un reste déjà rencontré et donc on va répéter les mêmes opérations (et de fait, normalement, retrouver les mêmes résultats) jusqu'à ce que mort s'ensuive.

Mais cela n'est pas spécifique à la division de 1 par 7. Dès que l'on divise un entier par un autre, le nombre de restes possibles est fini et on sera ainsi forcé de tomber deux fois sur le même lorsque l'on effectue la division. Ainsi toute fraction est un nombre dont la partie décimale est *périodique* (*ie* au final, une certaine séquence de chiffres se répète, ce caractère répétitif ne commençant pas forcément dès la première décimale, loin de là).

[25] Oui, il est plus facile de rajouter pour sur-représenter que d'enlever pour sous-représenter.

La réciproque est également vraie : tout nombre dont le développement décimal se répète au bout d'un moment est en fait une fraction. Voyons comment on prouve cela sur un exemple. On se donne le nombre $0\,,\,410\,784\,153\,153\,\overline{153}$ (la partie surlignée étant celle qui se répètera) et on cherche une fraction qui lui soit égale. Si l'on appelle x ce nombre, l'astuce consiste à calculer $1000x$. En faisant ensuite la différence, la partie répétitive va s'éliminer. Bref, on a :

$$\begin{array}{rrcr} & 1000x & = & 410\,,\,784\,153\,153\,\overline{153} \\ - & x & = & 0\,,\,410\,784\,153\,\overline{153} \\ \hline & 999x & = & 410\,,\,373\,216 \end{array}$$

De la dernière égalité écrite, on déduit :

$$x = \frac{410\,,\,373\,216}{999} = \frac{410\,373\,216}{999\,000\,000} = \frac{34\,197\,773}{83\,250\,000}$$

trouvant ainsi une fraction égale à notre nombre de départ. Bien évidemment, on comprend comment cette méthode se généralise à tout nombre périodique.

Ainsi pour construire un nombre non rationnel, il suffit de construire une partie décimale qui ne soit pas périodique. Pour cela, on peut faire la construction suivante :

$$0\,,\,1\,0\,1\,00\,1\,000\,1\,0000\,1\,00000\,1\,000000\,1\,0000000\,1\,00000000\,1\,000000000\ldots$$

Après le « 0, », on met un 1 puis un 0, puis encore un 1 puis deux 0, puis encore un 1 puis trois 0, puis encore un 1 puis quatre 0 et ainsi de suite. J'affirme que cette suite ainsi construite n'est pas périodique.

On a une propriété « négative » à prouver ; faisons un raisonnement par l'absurde. Supposons donc que ce nombre soit périodique, il s'écrirait donc $0,ABBBB...$ où A et B sont deux suites de chiffres. En premier lieu, on constate que B ne peut pas être constante égale à 0 : il y a des 1 aussi loin que l'on veut dans notre nombre. Mais alors, le nombre $0,ABBBB...$ ne pourra pas contenir plus de $\lg(A)+\lg(B)$ zéros à la suite ($\lg(X)$ désigne le nombre de chiffres de la suite de chiffres X), ce qui n'est pas le cas de notre nombre. Voici notre contradiction ! Et la conclusion s'ensuit : notre nombre est irrationnel.

On remarque que pour les mêmes raisons que celles exposées dans le raisonnement par l'absurde précédent, le nombre univers que l'on a construit au tout début est forcément irrationnel. Plus généralement d'ailleurs un nombre univers ne peut pas être rationnel.

Finalement c'est avec une construction tout à fait analogue à la précédente que Liouville a exhibé un nombre transcendant. Un nombre *transcendant* est un nombre qui n'est racine d'aucun polynôme à coefficients entiers. On montre en fait que de telles racines sont soit rationnelles, soit mal approchées (dans un sens à définir) par les nombres rationnels ; il suffit donc d'imposer que le nombre transcendant que l'on veut construire ne soit pas périodique, mais pourtant très proche (encore dans un sens à définir) d'un nombre périodique. On ne connaissait avant Liouville aucun exemple explicite de nombre transcendant. On sait aujourd'hui que π et e en sont, mais les preuves sont franchement complexes comparées à celle de Liouville.

6.3 Une fonction pour le moins étrange

Le but de ce paragraphe est de construire une fonction $f : \mathbb{Q} \to \mathbb{Q}$ qui soit telle que l'image de tout intervalle ouvert $]a,b[$ (avec $a < b$) soit $\mathbb{Q}$ tout entier. On rappelle, à tout hasard, que $\mathbb{Q}$ désigne l'ensemble des nombres rationnels.

On voit qu'une telle fonction doit osciller, et on connaît sans doute des fonctions qui ont ce genre de propriétés. On pense peut-être dans un premier temps à $\sin\left(\frac{1}{x}\right)$ qui oscille beaucoup en 0. On pourrait se dire qu'en recollant des fonctions de ce genre un peu partout, on devrait s'en sortir. Ce n'est sans doute effectivement pas désespéré, mais ce n'est probablement pas la meilleure façon d'aborder le problème, d'autant plus que cela va impliquer un nouveau problème bien plus difficile à résoudre : la fonction que l'on doit construire doit prendre ses valeurs dans $\mathbb{Q}$, et on sait que les sinus de nombres rationnels n'en sont en général pas.

La réponse est encore une fois d'y aller franchement et de définir exactement ce que l'on veut. Que veut-on, donc ? On veut par exemple que le rationnel 1 ait un antécédent dans chaque intervalle ouvert. Qu'à cela ne tienne, mettons-le. On choisit donc un point dans chaque intervalle ouvert et on définit f sur ces points en imposant à sa valeur d'égaler 1.

Bien évidemment, dit de la façon précédente, on ne comprend pas bien ce qu'il faut faire. Plutôt que de choisir un point dans chaque intervalle ouvert[26], on va exhiber un sous-ensemble de $\mathbb{Q}$ qui rencontre manifestement chaque intervalle ouvert. Bien sûr, on pourrait prendre $\mathbb{Q}$ lui-même, mais il n'y aurait alors plus de place pour continuer et la fonction serait constante égale à 1, ce qui n'est pas ce que l'on souhaite. Il faut donc trouver plus petit ; et on peut prendre :

$$A_1 = \left\{ \frac{p}{2^n},\ p \text{ impair}, n \in \mathbb{N}^\star \right\}$$

le fait que p soit impair n'est pas primordial maintenant, il assure simplement que la fraction écrite ne peut pas se simplifier. Cette condition nous sera utile par la suite.

On pose ensuite, comme annoncé, $f(x) = 1$ pour tout $x \in A_1$ et on a déjà résolu le problème pour la valeur 1.

Et maintenant, on continue et on traite la valeur 2. On considère un ensemble A_2 intersectant encore tout intervalle ouvert et disjoint de A_1, on peut prendre :

$$A_2 = \left\{ \frac{p}{3^n},\ p \text{ non multiple de } 3, n \in \mathbb{N}^\star \right\}$$

une puissance non nulle de 2 n'étant jamais une puissance non nulle de 3, et les fractions ne pouvant se simplifier. On définit ensuite f sur A_2 en posant $f(x) = 2$ pour tout $x \in A_2$.

Et maintenant, on passe à 3. Il faut trouver un ensemble A_3 disjoint de A_1 et A_2 et intersectant à nouveau tout intervalle ouvert. On prend :

$$A_3 = \left\{ \frac{p}{5^n},\ p \text{ non multiple de } 5, n \in \mathbb{N}^\star \right\}$$

il faut faire attention au nombre 4 pour le dénominateur, les puissances de 4 étant malheureusement des puissances de 2 particulières. On voit un premier problème, mais il est facile à régler, il va suffit d'interdire pour le dénominateur les nombres qui sont déjà des puissances ; si l'on ne veut vraiment pas se tourmenter, on peut ne faire apparaître dans les dénominateurs que les nombres premiers.

Notons donc p_k le k-ième nombre premier et définissons de façon générale :

$$A_k = \left\{ \frac{p}{p_k^n},\ p \text{ non multiple de } p_k, n \in \mathbb{N}^\star \right\}$$

[26] Ce genre de constructions est pourtant tout à fait possible et se révèle souvent très efficace ; ces idées seront quelque peu exposées dans le paragraphe suivant.

On a ainsi toute une ribambelle d'ensembles qui intersectent tout intervalle ouvert, et qui plus est disjoints deux à deux. Il ne reste donc plus qu'à définir f comme précédemment.

Le problème qui se pose est maintenant le suivant : si on décide de poser $f(x) = k$ pour tout $x \in A_k$, f ne va prendre que des valeurs entières (strictement positives qui plus est) et donc pas toutes les valeurs rationnelles. Il faut donc s'arranger pour lister tous les nombres rtionnels, on définira alors pour $x \in A_k$, $f(x)$ comme la k-ième fraction de la liste.

Voyons donc comment l'on peut établir une telle liste. On se cantonne pour débuter aux rationnels compris entre 0 et 1, disons. On voit alors ce que l'on peut faire : on met d'abord les rationnels qui ont pour dénominateur 1, puis ceux qui ont pour dénominateur 2 et ainsi de suite. Ainsi la liste obtenue commencera par :

$$0,\, 1,\, \frac{0}{2},\, \frac{1}{2},\, \frac{2}{2},\, \frac{0}{3},\, \frac{1}{3},\, \frac{2}{3},\, \frac{3}{3},\, \frac{0}{4},\, \frac{1}{4},\, \frac{2}{4},\, \frac{3}{4},\, \frac{4}{4},\, \frac{0}{5},\, \dots$$

Bien sûr dans la liste précédente, un même rationnel apparaît de nombreuses fois, on peut s'amuser à éliminer les doublons si cela nous amuse. Le problème, c'est que l'on ne veut pas seulement les rationnels compris entre 0 et 1 mais bien tous les rationnels. Qu'à cela ne tienne, on met d'abord ceux qui sont compris entre -1 et 1 et qui ont un dénominateur égal à 1, puis ceux qui sont compris entre -2 et 2 et qui ont un dénominateur égal à 2, et ainsi de suite. Au final :

$$-1,\, 0,\, 1,\, -\frac{4}{2},\, -\frac{3}{2},\, -\frac{2}{2},\, -\frac{1}{2},\, \frac{0}{2},\, \frac{1}{2},\, \frac{2}{2},\, \frac{3}{2},\, \frac{4}{2},\, -\frac{9}{3},\, -\frac{8}{3},\, \dots$$

Quelle que soit la façon retenue, appelons x_k le k-ième rationnel. On peut maintenant définir notre fonction f en posant :

$$\begin{cases} f(x) = x_k & \text{si } x \in A_k \\ f(x) = 0 & \text{sinon} \end{cases}$$

Elle convient évidemment.

6.4 Le principe du va-et-vient

Nous allons expliquer dans ce paragraphe, sur un exemple pas forcément simple, comment il est possible de combiner les idées précédentes avec la puissance du raisonnement par récurrence.

Fixons-nous donc un problème. On désigne par $\mathbb{Q}\left(\sqrt{2}\right)$ l'ensemble suivant :

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2},\, a, b \in \mathbb{Q}\right\}$$

C'est un sous-ensemble de $\mathbb{R}$. La question consiste à construire une fonction $f : \mathbb{R} \to \mathbb{R}$ strictement croissante envoyant $\mathbb{Q}$ exactement sur $\mathbb{Q}\left(\sqrt{2}\right)$.

Là encore, essayer de trifouiller une formule ne va certainement pas faire apparaître miraculeusement la solution. Il faut littéralement construire cette fonction à la main. On veut envoyer $\mathbb{Q}$ sur $\mathbb{Q}\left(\sqrt{2}\right)$, faisons-le. On a vu précédemment que l'on pouvait numéroter les rationnels, nous n'allons pas nous en priver. Appelons x_k le k-ième nombre rationnel (on commence à $k = 0$ à partir de maintenant, allez hop), pour une liste que l'on s'est fixée à l'avance.

Il va nous falloir en outre, numéroter les éléments de $\mathbb{Q}\left(\sqrt{2}\right)$ si l'on veut continuer. On écrit pour ce faire la liste suivante :

$$x_0 + x_0\sqrt{2},\ x_0 + x_1\sqrt{2},\ x_1 + x_0\sqrt{2},\ x_0 + x_2\sqrt{2},\ x_1 + x_1\sqrt{2},\ x_2 + x_0\sqrt{2},\ x_0 + x_3\sqrt{2},\ \ldots$$

On met d'abord les $x_i + x_j\sqrt{2}$ pour $i + j = 0$, puis ensuite ceux pour $i + j = 1$ et ainsi de suite. Comme cela, on les obtient bien tous. Dans la liste précédente, il n'y a pas de doublons ; c'est une conséquence de l'irrationalité de $\sqrt{2}$. Cela dit, qu'il y en est ou pas, n'est pas le problème, on peut décréter qu'on les élimine. Bref, appelons y_k le k-ième item de cette liste.

On a donc d'une part une liste des éléments de $\mathbb{Q}$ et d'autre part une liste des éléments de $\mathbb{Q}\left(\sqrt{2}\right)$. Il est tentant de débuter la définition de f en posant $f(x_k) = y_k$. Cependant, cela ne va pas marcher : rien n'est là pour assurer la croissance. Il faut donc faire plus attention et c'est là qu'intervient la récurrence.

Nous n'allons pas écrire la démonstration rigoureuse et implacable, mais plutôt donner les idées principales suffisamment détaillées toutefois et laisser au lecteur le soin de mettre tout cela au propre s'il souhaite le faire.

On commence par x_0, on veut lui trouver une image. Il n'y a pour l'instant aucune contrainte, on prend donc naturellement y_0.

On passe à x_1. Il y a cette fois-ci deux cas : soit il est plus grand, soit il est plus petit que x_0. S'il est plus grand, il faut choisir un y_n parmi ceux qui sont plus grands que y_0 ; s'il est plus petit, il faudra en choisir un parmi les plus petits. De toute évidence, de tels y_n existent puisque $\mathbb{Q}\left(\sqrt{2}\right)$ « va jusqu'à l'infini » des deux côtés. Disons, pour fixer les idées, que l'on choisit le plus petit indice n tel que y_n soit comme on le veut.

Au suivant ! C'est x_2. Il y a maintenant trois cas : soit il est plus petit que le plus petit de x_0 et x_1, soit il est plus grand que le plus grand, soit il est compris entre les deux. Bref, il est situé quelque part par rapport aux autres : x_0 et x_1. Pour chacun de ces cas, il y a un y_n correspondant et encore, pour fixer les choses, on choisit le plus petit indice n convenable.

On continue ainsi. Si on a défini les images de $x_0, \ldots, x_n$, on regarde où se situe x_{n+1} entre tous ces nombres et on lui associe le y_n qui va bien.

C'est tout beau, tout mignon, mais ça ne marche pas. Rien n'assure que l'on va tomber ainsi sur tous les y_n et rien ne dit qu'au final, on ne se retrouve pas avec la fonction identité. Il faut bien quelque chose pour tenir compte de ces y_n. L'idée est alors de faire la construction dans les deux sens (d'où le nom de *va-et-vient*).

Reprenons donc. On commence toujours par x_0 et on lui associe toujours y_0. On continue par x_1 comme c'était déjà le cas dans la construction précédente.

Mais maintenant on ne considère pas x_2 mais plutôt y_1 et on lui cherche un antécédent s'il n'en a pas déjà. Le nombre y_1 se situe d'une certaine façon par rapport aux éléments qui sont déjà dans l'image de f, on lui choisit son antécédent en conséquence.

Seulement maintenant, on s'occupe de x_2. Soit il a déjà été choisi à l'étape précédente, et on passe. Soit ce n'est pas le cas, et on le situe non pas par rapport à x_0 et x_1 mais par rapport aux éléments qui ont déjà une image par f, c'est-à-dire x_0, x_1 et éventuellement un antécédent de y_1 choisi précédemment. Une fois cela fait, on choisit une image pour x_2.

Ensuite, on s'occupe de y_2, puis de x_3, de y_3, de x_4, et ainsi de suite. Tout cela nous donne une fonction $f : \mathbb{Q} \to \mathbb{Q}\left(\sqrt{2}\right)$ surjective[27] et strictement croissante. Il reste à prolonger ce début de fonction à $\mathbb{R}$ tout entier.

Mais, si l'on regarde un petit moment dans les yeux la fonction que l'on vient de construire, on voit qu'on n'a pas le choix. Soit x un réel, disons irrationnel. Par croissance, pour tout rationnel $r < x$, on doit avoir $f(r) < f(x)$, et pour tout rationnel $r > x$, on doit avoir $f(r) > f(x)$. Mais l'ensemble de tous les $f(r)$ est $\mathbb{Q}\left(\sqrt{2}\right)$ donc les conditions précédentes déterminent au plus un réel et en fait exactement un réel. C'est ainsi que l'on achève notre construction.

Bien entendu, $\mathbb{Q}$ et $\mathbb{Q}\left(\sqrt{2}\right)$ étaient des exemples arbitraires, on aurait en fait pu les remplacer par n'importe quel partie A de $\mathbb{R}$ dense (*ie* entre deux réels quelconques, il y a toujours un élément de A), dénombrable (*ie* on peut numéroter les éléments) et « allant à l'infini » ou plutôt *sans extrémités* comme on préfère dire (*ie* pout tout réel positif M, il y a dans A un élément plus grand que M et un plus petit que $-M$). La démonstration précédente s'appliquait alors point par point.

Ainsi, on aurait pu remplacer $\mathbb{Q}\left(\sqrt{2}\right)$ par l'ensemble des nombres algébriques[28], ce qui doit paraître peut-être encore plus étonnant.

[27] Cela signifie que tout élément de $\mathbb{Q}\ \sqrt{2}$ admet au moins un antécédent par f.
[28] *Ie* racine d'un polynôme à coefficients entiers – voir paragraphe 6.2.