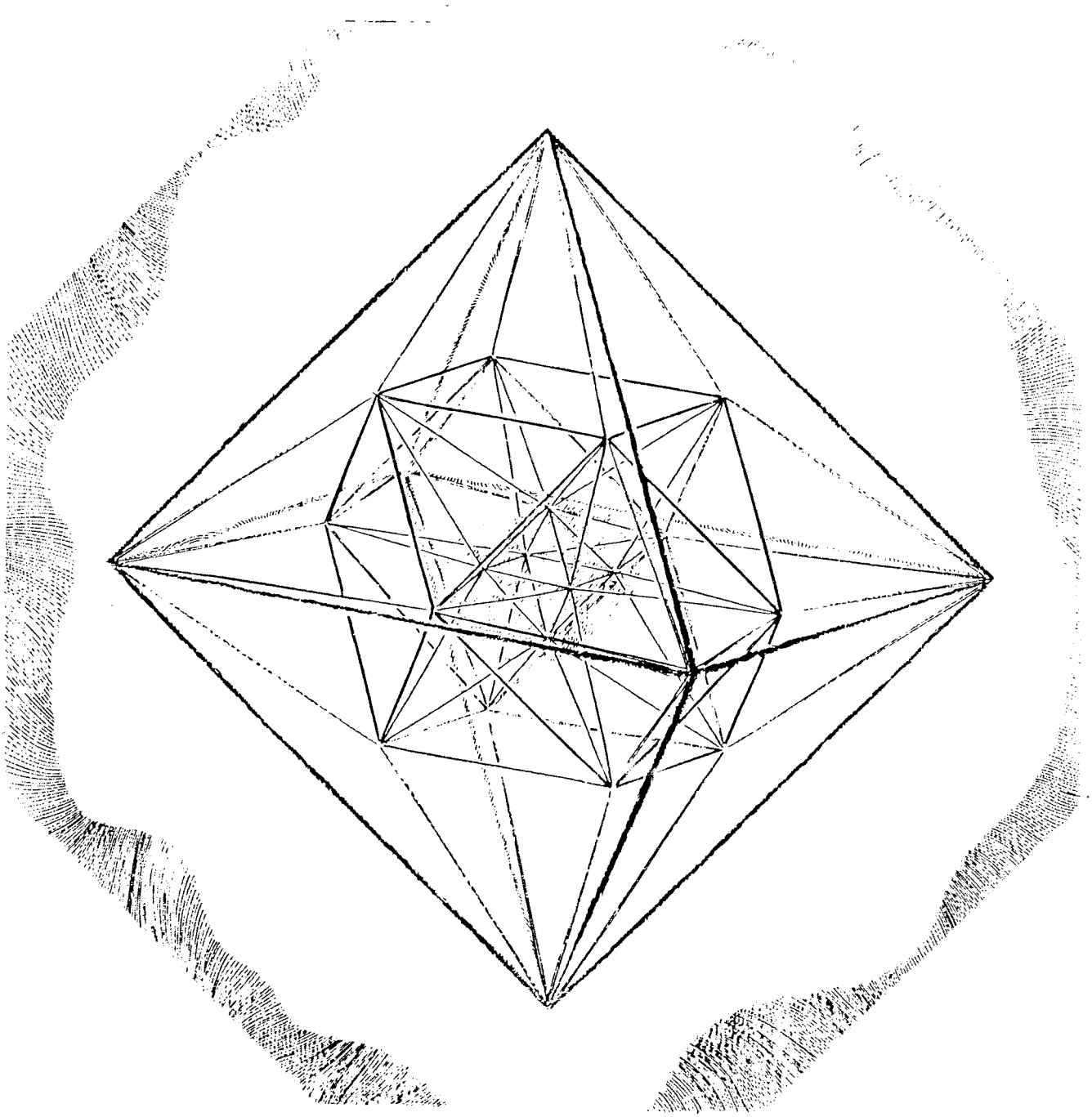
L'OUVERT

JOURNAL DE L'A.P.M.E.P. D'ALSACE ET DE L'I.R.E.M. DE STRASBOURG
n° 69 – DÉCEMBRE 1992 I.S.S.N. 0290 - 0068



NOTRE COUVERTURE : GRAVURE

Reproduction d'une gravure de Patrice JEENER (tirée de "Espaces gravés" chez Cédic - 1986), intitulée C_{24}. Cette gravure est la projection sur $\mathbb{R}^2$, selon une perspective classique, d'un polytope régulier de $\mathbb{R}^4$.

On appelle polytope, la généralisation dans $\mathbb{R}^n$ des polygônes de $\mathbb{R}^2$ et des polyèdres de $\mathbb{R}^3$. Il y a six polytopes réguliers dans $\mathbb{R}^4$ (3 seulement pour $n > 4$).

C_{24} n'a pas vraiment d'analogue dans $\mathbb{R}^3$. Ce polytope qui est son propre dual est formé de 24 sommets, 96 arêtes, 96 faces triangulaires et 24 cellules octaèdriques (d'où son nom C_{24}). De chaque sommet partent 6 cellules et 8 arêtes. Chaque arête appartient à 3 cellules.

JEUNE, BEAU ET RICHE

Chaque année, une information sur les carrières est donnée aux lycéens. A Colmar elle a eu lieu au Parc-Expo les 24, 25 et 26 septembre. A cette occasion, un document a été distribué à tous les lycéens pour qu'ils préparent leur visite. Pour mieux cibler leur objectif professionnel, ils devaient remplir une grille en notant de 0 à 10 l'importance qu'ils attribuaient à 12 critères dont :
- faire un travail intéressant,
- avoir un statut élevé,
- avoir des initiatives,
- avoir du temps libre,
- avoir la sécurité de l'emploi,
- GAGNER BEAUCOUP D'ARGENT.

Peut-on répondre 0 à ces questions? Avec quelques collègues nous constations que ce n'était jamais ce qu'on nous demandait lorsque nous étions jeunes, preuve s'il en est de l'évolution de la société. Pour ne s'en tenir qu'à un seul aspect, il est vrai que la notion d'argent envahit l'école : introduction de l'économie, programmes d'histoire et de géographie résolument orientés vers l'économie, jusqu'à l'introduction notoire des statistiques et des probabilités en mathématiques dans toutes les sections ce qui se comprend quand on sait que les prix Nobel d'économie vont à des mathématiciens ou que les cours de la bourse sont régis par des équations issues de mouvement brownien. Voilà pourquoi se multiplient les ventes de ceci ou celà pour financer tel voyage ... que se développent les filières commerciales ... et peut-être que se diversifient les catégories de professeurs pour mieux les tenir par l'argent qu'ils gagnent ou qu'ils peuvent envisager de gagner.

Ne peut-on craindre de voir l'école y perdre son âme, y perdre les références à d'autres types de valeurs que sont la solidarité, le respect d'autrui, le don ... ce qui a justement permis à l'école d'être le ciment de la société? Si le seul mot d'ordre est : "Enrichissez-vous" alors les affaires qui envahissent la classe politique risquent de se banaliser. Mais l'école n'est pas la seule responsable de notre type de société et j'ai été heureux d'apprendre qu'un élève d'une STS "Force de vente" a refusé le travail : "Comment vendre une moto de 750 cc à une grand-mère de 80 ans" et ce, malgré le risque de sanction qui l'attendait.

J. LEFORT.

SOMMAIRE

N° 69 – DÉCEMBRE 1992

◇ *Notre couverture : Gravure* I

◇ *Editorial : Jeune, riche et beau* II

◇ *Le calcul des nombres $\zeta(2k)$ au moyen des séries formelles*, par M. GUINOT ... 1

◇ *Une preuve lumineuse de la relation* $1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \cdots = 2(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots)^2$, par D. DUMONT 17

◇ *Réflexions préalables à une étude des obstacles*, par G. GLAESER 21

◇ *Le crible d'Eratosthène*, par R. SEROUL 29

◇ *A vos stylos*, par *'L'Ouvert'* 42

L'OUVERT

ISSN 0290 – 0068

◇ *Responsable de la publication* : Jean LEFORT

◇ *Correspondance à adresser à :*
Université Louis Pasteur
Bibliothèque de l'I.R.E.M.
10, rue du Général Zimmer
67084 STRASBOURG CEDEX
Tél. : 88-41-64-40

◇ *Abonnement (pour 4 numéros annuels)*
50 F (95 F/2 ans) pour les membres A.P.M. d'Alsace
90 F (170 F/2 ans) pour l'Alsace
120 F (220 F/2 ans) pour la France ou l'Étranger.
Chèque à l'ordre de Monsieur l'Agent Comptable de l'U.L.P. (IREM)

◇ *Prix du numéro* : 25.– F

LE CALCUL DES NOMBRES $\zeta(2k)$ AU MOYEN DES SÉRIES FORMELLES

Marc GUINOT

Le groupe mathématique de Saumur et le mathématicien Bernhard Riemann ne sont pas des inconnus pour les lecteurs de *'L'Ouvert'*. Les travaux du premier sur les quaternions, les octonions et la géométrie ont fait l'objet d'un article publié en deux parties par *'L'Ouvert'* en 1990-1991 (n° 61 et 62), article qui a été lu jusqu'au Portugal. Le second est connu pour un célèbre mémoire d'habilitation, présenté à Göttingen en 1854, dans lequel il pose les fondements de la topologie et de la géométrie riemannienne. Il est aussi l'auteur d'un court article sur "le nombre de nombres premiers inférieurs à une quantité donnée" dans lequel se trouve énoncée ce qu'on appelle maintenant l'*hypothèse de Riemann* sur la répartition des zéros de la fonction zêta.

Riemann mourut prématurément d'une maladie pulmonaire en 1866, à l'âge de 40 ans et, selon l'*Encyclopaedia Universalis*, il repose dans un petit cimetière près du lac Majeur, en Italie.

Le groupe mathématique de Saumur a failli être emporté à son tour l'hiver dernier. Pourtant, le 22 mai 1992, s'est tenue au lycée technique Sadi-Carnot une réunion inattendue, consacrée à "certaines valeurs de la fonction zêta", et plus précisément au calcul des sommes $1 + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \frac{1}{4^{2k}} + \cdots$ Le compte-rendu de cette séance exceptionnelle ayant séduit le comité de rédaction de l'organe officiel de l'IREM de Strasbourg, je me permets d'en présenter ici une version plus étendue.

L'histoire (ou la préhistoire) de la fonction zêta commence en 1650 lorsqu'un certain Mengoli s'interrogea sur la possibilité de déterminer explicitement la somme $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$ des inverses de tous les carrés parfaits. Le problème résista aux mathématiciens les plus chevronnés de l'époque, parmi lesquels Leibniz et un nombre indéterminé de Bernoulli, et c'est seulement en 1735 qu'Euler, alors dans sa vingt-neuvième année, découvrit la réponse : selon ses propres termes, le résultat dépend de la "quadrature du cercle", c'est-à-dire du nombre π ! Mais Euler ne s'arrêta pas à si peu et, dans le même temps, il obtint des résultats analogues et tout aussi étonnants pour les sommes $1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \frac{1}{5^n} + \cdots$ avec $n = 4$, 6, 8 et 12 – ce que nous noterions aujourd'hui $\zeta(4), \zeta(6), \zeta(8)$ et $\zeta(12)$. C'est ainsi qu'il trouva la valeur de $\zeta(12)$ qui est, bien sûr, $\frac{691\pi^{12}}{638\ 512\ 875} \cdots$

Le raisonnement d'Euler manquait de rigueur et pour répondre aux interrogations de ses contemporains (et sans doute des siennes propres), il revint plusieurs fois sur le problème à l'aide de méthodes variées qui, tout en donnant les mêmes résultats, sacrifiaient encore par trop à la mode des calculs purement formels qui sévissaient

en analyse à cette époque. De nos jours, où la rigueur règne sans entraves dans le moindre manuel, les résultats d'Euler sont présentés comme des applications de théories plus ou moins rébarbatives, en rapport avec les fonctions holomorphes ou les séries de Fourier. Pourtant, les raisonnements d'Euler peuvent être rendus impeccables sans trop d'efforts, avec très peu d'analyse, en faisant appel à la notion moderne, simple et algébrique de séries formelles.

Auparavant, pour expliquer la terminologie contemporaine tout en rendant à Riemann l'hommage qui lui est dû, il n'est peut-être pas mauvais de rappeler que la fonction ζ de Riemann est une fonction d'une variable qui peut être définie soit par la condition

$$\zeta(\alpha) = 1 + \frac{1}{2^\alpha} + \frac{1}{3^\alpha} + \frac{1}{4^\alpha} + \cdots$$

où le second membre (*série de Riemann*) est une série convergente si $\alpha > 1$, soit par la décomposition en produit (due à Euler)

$$\zeta(\alpha) = \Pi_{p \text{ premier}} \frac{1}{1 - \frac{1}{p^\alpha}}$$

le produit (infini) du second membre étant étendu à la totalité des nombres premiers (et étant encore convergent si $\alpha > 1$). C'est cette relation entre la série de Riemann et le produit ci-dessus qui fait l'importance de la fonction zêta, importance qui est apparue en pleine lumière lorsque Riemann eut montré l'intérêt qu'il y avait à choisir α complexe dans les formules précédentes et à étendre la fonction ζ ainsi obtenue au plan complexe tout entier de façon à en faire une fonction "méromorphe", avec un pôle unique (où la fonction n'est en réalité pas définie) correspondant à $\alpha = 1$. Riemann mit en évidence le lien qui existe alors entre le problème (déjà soulevé par Euler) de la répartition des nombres premiers et celui (apparemment sans rapport) de la localisation des nombres complexes α tels que $\zeta(\alpha) = 0$ ("zéros" de la fonction zêta). Le mieux en la matière serait de démontrer l'hypothèse de Riemann qui veut que, en dehors de cas dûment répertoriés sur la partie négative de l'axe des réels, tous ces zéros sont, en fait, placés sur une même droite "verticale", formée des nombres complexes dont la partie réelle est 1/2. Jusqu'à présent, malgré de très nombreuses vérifications à l'ordinateur (plus de 1 milliard!), cette conjecture est restée en suspens.

Après ces considérations hautement culturelles, nous allons revenir à notre véritable propos, qui est le calcul (sans larmes) des nombres $\zeta(2k)$. Pour mettre en appétit, on dira d'abord un mot du cas de $\zeta(2)$, c'est-à-dire du calcul de la somme $\sum_{n=1}^{+\infty} \frac{1}{n^2}$.

1. Le calcul de $\zeta(2)$

Il y a plusieurs façons de procéder. La plus simple me paraît être celle dont je ne donne ici que le canevas en demandant au lecteur de bien vouloir le compléter à sa guise. Elle consiste à utiliser des considérations trigonométriques élémentaires

permettant d'affirmer que

$$\cot^2 \frac{\pi}{2n+1} + \cot^2 \frac{2\pi}{2n+1} + \cdots + \cot^2 \frac{n\pi}{2n+1} = \frac{n(2n-1)}{3}$$

pour tout $n \geq 1$.

Pour établir cette relation, on développe $\sin(2n+1)\theta$ à l'aide de la formule de de Moivre, on met $\sin^{2n+1}\theta$ en facteur et on en déduit que les nombres $\cot^2 \frac{k\pi}{2n+1}$ sont (pour $1 \leq k \leq n$) les racines du polynôme

$$C^1_{2n+1} x^n - C^3_{2n+1}\, x^{n-1} + \cdots + (-1)^n.$$

D'où la formule ci-dessus en considérant la somme desdites racines. En s'appuyant alors sur le fait que $\cot^2\theta < \frac{1}{\theta^2} < 1 + \cot^2\theta$ lorsque $0 < \theta < \frac{\pi}{2}$ (relation qui se déduit sans peine du fait bien connu que $\sin\theta < \theta < \tan\theta$ dans les mêmes conditions), on est capable de prouver que

$$\frac{n(2n-1)\pi^2}{3(2n+1)^2} < 1 + \frac{1}{2} + \cdots + \frac{1}{n^2} < \frac{n(2n+2)\pi^2}{3(2n+1)^2}.$$

Comme les deux expressions encadrantes tendent vers une même limite, égale à $\frac{\pi^2}{6}$, on en déduit qu'il en est de même de la somme du milieu; c'est le résultat d'Euler :

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots = \frac{\pi^2}{6}.$$

Pour aller plus loin, nous aurons besoin de développer quelques notions relatives aux séries formelles.

2. Séries formelles en une indéterminée

La notion de série formelle ne pose pas de problème conceptuels majeurs si on veut bien considérer qu'une série de ce genre n'est rien d'autre, au fond, qu'une suite illimitée $(a_n)_{n\geq 0} = (a_0, a_1, a_2, a_3, \ldots, a_n, \ldots)$ dont tous les termes sont choisis dans un même anneau commutatif A. Si on note S_A provisoirement l'ensemble de ces suites, on définit dans cet ensemble deux lois de composition (addition et multiplication) en posant

$$(a_n) + (b_n) = (a_n + b_n) \text{ et } (a_n)(b_n) = (a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0)$$

lois de composition que l'on complète en leur adjoignant une "loi d'action" permettant de "multiplier" par un élément c quelconque de A un élément arbitraire de S_A, et ce grâce à la condition

$$c(a_n) = (ca_n).$$

Pour la première loi, les termes successifs du résultat sont donc $a_0 + b_0, a_1 + b_1, a_2 + b_2$, etc.; pour la seconde loi, ce sont $a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0$, etc. et pour la loi "externe" : ca_0, ca_1, ca_2, et ainsi de suite.

Cela étant, à ces données de base s'ajoute une convention notatoire de pure forme qui consiste à écrire $\Sigma_{n=0}^{+\infty} a_n X^n$ au lieu de $(a_n)_{n\geq 0}$ ou $a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \ldots$ au lieu de $(a_0, a_1, a_2, a_3, \ldots)$, moyennant quoi les opérations précédentes peuvent être considérées comme définies par les conditions :

$$(1) \qquad (a_0 + a_1 X + a_2 X^2 + \ldots) + (b_0 + b_1 X + b_2 X^2 + \ldots) = (a_0 + b_0) + (a_1 + b_1) X + (a_2 + b_2) X^2 + \cdots$$

$$(2) \qquad (a_0 + a_1 X + a_2 X^2 + \cdots)(b_0 + b_1 X + b_2 X^2 + \cdots) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + \cdots$$

$$(3) \qquad c(a_0 + a_1 X + a_2 X^2 + \cdots) = c a_0 + c a_1 X + c a_2 X^2 + \cdots$$

Le choix de ces notations tient à deux raisons principales auxquelles s'ajoute une troisième explication, de nature topologique, que nous passerons sous silence ici. La première provient du rapprochement que l'on peut faire entre les relations (1), (2) et (3) et des relations analogues concernant les polynômes en X et à coefficients dans l'anneau A. De façon plus précise, ce rapprochement permet d'identifier tout polynôme de ce genre avec un élément de S_A, à condition de convenir qu'un polynôme $a_0 + a_1 X + \cdots + a_n X^n$ correspond à la suite $a_0, a_1, \ldots a_n, 0, 0, \ldots$ des coefficients de ce polynôme (suite qui, on le sait, ne comporte que des termes nuls au delà d'un certain rang). Cette identification faite, les éléments de S_A seront appelés désormais *séries formelles en X et à coefficients dans A* et on utilisera à leur propos, toutes les fois où ce sera possible, le vocabulaire propre aux polynômes : *terme constant, coefficients, terme de degré n* (ou en X^n), etc. On notera cependant qu'une série formelle qui n'est pas un polynôme n'a pas de "terme de plus haut degré", donc pas de degré, mais il y a un *ordre* qui est par définition le degré du terme de plus bas degré. On adoptera aussi des conventions d'écriture analogues à celles en usage pour les polynômes lorsqu'il y a des coefficients qui autorisent certaines simplifications. C'est ainsi que l'écriture $\Sigma_{n=0}^{+\infty} X^n$, ou $1 + X + X^2 + X^3 + \cdots$, représente une série bien précise (dite *série géométrique formelle*) dont tous les coefficients valent 1 (donc correspondant à la suite $(a_n)_{n\geq 0}$ pour laquelle $a_n = 1$ pour tout n); cette série est à coefficients dans un anneau A quelconque. De la même façon, l'écriture $\Sigma_{n=0}^{+\infty} \frac{X^n}{n!}$, ou $1 + \frac{X}{1!} + \frac{X^2}{2!} + \frac{X^3}{3!} + \cdots$, représente une autre série, à coefficients dans le corps $\mathbb{Q}$ cette fois, dont les coefficients successifs sont $1, \frac{1}{1!}, \frac{1}{2!}, \frac{1}{3!}$, etc. On appelle cette série l'*exponentielle formelle* et on la notera, par pure convention, e^X. Cette série nous sera utile plus loin, de même que le *sinus formel* et le *cosinus formel* respectivement définis par les conditions $\sin X = X - \frac{X^3}{3!} + \frac{X^5}{5!} - \frac{X^7}{7!} + \cdots$ et $\cos X = 1 - \frac{X^2}{2!} + \frac{X^4}{4!} - \frac{X^6}{6!} + \cdots$ dont les coefficients successifs sont, respectivement, $0, \frac{1}{1!}, 0, -\frac{1}{3!}, 0, \frac{1}{5!}, 0, \ldots$ et $1, 0, -\frac{1}{2!}, 0, \frac{1}{4!}, 0, \ldots$

Comme l'ensemble des polynômes en X et à coefficients dans un anneau commutatif A se note $A[X]$, on notera $A[[X]]$ l'ensemble des séries formelles du même genre.

La seconde raison qui explique toutes ces conventions d'écriture est l'espèce de

distributivité généralisée qu'exprime la relation suivante :

$$(4) \qquad X^k(c_0 + c_1X + c_2X^2 + \cdots) = c_0X^k + c_1X^{k+1} + c_2xX^{k+2} + \cdots$$

valable pour tout entier naturel k et toute série formelle $\Sigma_{n=0}^{\infty} c_n X^n$. Celle-ci se démontre sans difficultés en partant de la relation (2) ci-dessus, avec $a_n = 0$ si $n \neq k$, $a_n = 1$ si $n = k$ et $b_n = c_n$ quel que soit n.

De toute façon, les propriétés de l'ensemble $A[[X]]$, muni des lois (1), (2), (3), sont sans surprises et conduisent à l'énoncé du théorème suivant :

Théorème 1.– Muni des lois (1) et (2), l'ensemble $A[[X]]$ est un anneau commutatif contenant $A[X]$ comme sous-anneau. De plus, les lois (1) et (2) sont liées à la "multiplication" (3) par les règles

$$c(s+t) = cs + ct,\ (c+d)s = cs + ds,\ c(ds) = (cd)s,\ 1s = s$$
$$c(st) = (cs)t = s(ct)$$

où $c, d \in A$ et $s, t \in A[[X]]$.

On résume parfois tout cela en disant que $A[[X]]$ est une algèbre commutative (et associative) sur l'anneau A.

Les détails de la démonstration sont laissés au lecteur. Le seul point un peu délicat à vérifier est l'associativité de la multiplication. Après avoir noté que $(\Sigma_{n=0}^{+\infty} a_n X^n)(\Sigma_{n=0}^{+\infty} b_n X^n) = \Sigma_{n=0}^{+\infty}(\Sigma_{i+j=n} a_i b_j)X^n$, on vérifie séparément que dans l'anneau A, on a

$$\sum_{q+k=n} (\sum_{i+j=q} a_i b_j)c_k = \sum_{i+j+k=n} a_i b_j c_k \text{ et } \sum_{i+r=n} a_i (\sum_{j+k=r} b_j c_k) = \sum_{i+j+k=n} a_i b_j c_k.$$

Comme dans tout anneau, il y a dans $A[[X]]$ des éléments inversibles, mais ils sont plus nombreux que dans $A[X]$ comme le montre le cas de $1-X$ et $1+X+X^2+\cdots$, inverses l'un de l'autre car

$$(1-X)(1+X+X^2+\cdots) = (1+X+X^2+\cdots) - (X+X^2+X^3+\cdots) = 1.$$

Le résultat général est très simple :

Théorème 2.– Pour qu'une série formelle $a_0 + a_1X + a_2X^2 + \cdots$ à coefficients dans un anneau commutatif A soit inversible (dans $A[[X]]$), il faut et il suffit que son terme constant a_0 soit inversible dans A.

En effet, pour qu'une série quelconque $b_0 + b_1X + b_2X^2 + \cdots$ soit inverse de la série $a_0 + a_1X + a_2X^2 + \cdots$ il faut et il suffit que $a_0b_0 = 1$ et que $a_0b_n + a_1b_{n-1} + \cdots + a_nb_0 = 0$ pour tout $n \geq 1$. La première relation montre effectivement que a_0 doit être inversible dans A. Réciproquement, si cette condition

est vérifiée on a $a_0 b_0 = 1$ si on prend $b_0 = a_0^{-1}, a_0 b_1 + a_1 b_0 = 0$ si on prend $b_1 = a_0^{-1}(-a_1 b_0), a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$ si $b_2 = a_0^{-1}(-a_1 b_1 - a_2 b_0)$ et ainsi de suite. On calcule ainsi les éléments b_n de proche en proche en utilisant la seule inversibilité de a_0.

Nous invitons le lecteur à mettre en œuvre cette méthode dans le cas de la série exponentielle e^X, évidemment inversible : avec $a_0 = 1, a_1 = \frac{1}{1!}, a_2 = \frac{1}{2!}, a_3 = \frac{1}{3!}$, etc., il devrait trouver $b_0 = 1, b_1 = -1, b_2 = \frac{1}{2}, b_3 = -\frac{1}{6}, b_4 = \frac{1}{24}, b_5 = -\frac{1}{120}, \cdots$ De là à penser que l'inverse de e^X est $1 - \frac{X}{1!} + \frac{X^2}{2!} - \frac{X^3}{3!} + \frac{X^4}{4!} - \frac{X^5}{5!} + \cdots$, il n'y a qu'un pas, à franchir par une petite récurrence ... Nous reverrons cela plus bas, dans un contexte plus général.

Plus difficile est le calcul de $(\cos X)^{-1}$. Le résultat commence, sauf erreur, par $1 + \frac{1}{2}X^2 + \frac{5}{24}X^4 + \frac{61}{720}X^6 + \frac{277}{8064}X^8 \ldots$ Comprenne qui pourra!

A noter que la série $\sin X$, elle, n'est pas inversible dans $\mathbb{Q}[[X]]$ puisque son terme constant qui est nul n'est pas inversible dans $\mathbb{Q}$.

Dans le cas général où l'anneau A est un corps, le théorème 2 se traduit immédiatement de la façon suivante :

> **Théorème 3.**– Pour qu'une série formelle $a_0 + a_1 X + a_2 X^2 + \cdots$ à coefficients dans un corps commutatif K soit inversible (dans l'anneau $K[[X]]$), il faut et il suffit que son terme constant ne soit pas nul.

Cela conduit à quelques conséquences intéressantes :

> **Corollaire 1.**– Toute série formelle non nulle $s \in K[[X]]$ peut se mettre sous la forme d'un produit $X^m s_0$ où m est un entier naturel et s_0 une série formelle inversible.

Si on pose $s = a_0 + a_1 X + a_2 X^2 + \cdots$, il suffit en effet de considérer le plus petit entier m tel que $a_m \neq 0$: on a alors $s = a_m X^m + a_{n+1} X^{m+1} + a_{m+2} X^{m+2} + \cdots = X^m s_0$ avec $s_0 = a_m + a_{m+1} X + a_{m+2} X^2 + \cdots$

> **Corollaire 2.**– Le produit de deux séries non nulles $s, t \in K[[X]]$ est une série non nulle.

Il suffit d'écrire (avec des notations évidentes) $s = X^m s_0$ et $t = X^n t_0$ pour voir que dans $st = X^{m+n} s_0 t_0$ le coefficient du terme de degré $m + n$ n'est pas nul.

Ce dernier résultat montre que si K est un corps, l'anneau $K[[X]]$ est intègre. Comme tout anneau intègre, on peut alors le plonger dans un corps, notamment son corps des fractions.

> **Théorème 4.**– Le corps des fractions de l'anneau $K[[X]]$ est formé d'éléments de la forme $\frac{u}{X^k}$ où $u \in K[[X]]$ et où k est un entier naturel quelconque.

En effet, par principe, tout élément du corps des fractions de $K[[X]]$ est de la forme $\frac{s}{t}$ où $s, t \in K[[X]]$ et où $t \neq 0$. D'après le cor. 1 du th. 3 ci-dessus, t peut s'écrire $X^k t_0$ où t_0 est une série inversible de $K[[X]]$. D'où $\frac{s}{t} = \frac{s}{X^k t_0} = \frac{st_0^{-1}}{X^k}$ où le numérateur $u = st_0^{-1}$ représente un élément $u \in K[[X]]$.

On peut dire aussi que les éléments du corps des fractions de $K[[X]]$ sont des séries "généralisées" de la forme $a_h X^h + a_{h+1} X^{h+2} + a_{h+2} X^{h+2} + \cdots$ où h est un entier de signe quelconque et où $a_h, a_{h+1}, a_{h+2}, \ldots$ sont des éléments quelconques du corps K.

Habituellement, on note $K((X))$ le corps des fractions de $K[[X]]$ (ou *corps des séries formelles généralisées* à coefficients dans K) en parallèle avec la notation $K(X)$ pour le corps des fractions de l'anneau $K[X]$ (ou *corps des fractions rationnelles* sur K). On notera au passage que $K(X)$ s'identifie à un sous-corps de $K((X))$.

Un exemple (qui nous servira plus loin) de série formelle généralisée est la "fraction" $\frac{\cos X}{\sin X}$ que l'on appellera la *cotangente formelle* et que l'on notera $\cot X$. Comme $\sin X = X(1 - \frac{X^2}{3!} + \frac{X^4}{5!} - \cdots)$, on voit que $\cot X$ est égal à

$$\frac{(1 - \frac{X^2}{2!} + \frac{X^4}{4!} - \cdots)(1 - \frac{X^2}{3!} + \frac{X^4}{5!} - \cdots)^{-1}}{X},$$

donc une série de la forme $\frac{1}{X} + a_0 + a_1 X + a_2 X^2 + \cdots$ dont le lecteur aura à cœur de calculer les premiers coefficients (on trouve au début $a_0 = 0, a_1 = -\frac{1}{3}, a_2 = 0, a_3 = -\frac{1}{45}, a_4 = 0, a_5 = -\frac{1}{945}$). On notera au passage que bien que la "fraction" $\frac{\sin X}{\cos X} = \tan X$ (*tangente formelle*) soit une série "ordinaire" (je veux dire un élément de l'anneau $\mathbb{Q}[[X]]$) il n'est guère facile d'en calculer les coefficients – sauf ceux d'indices pairs, naturellement. Naturellement ?

Les propriétés purement algébriques dont il nous reste maintenant à parler sont très simples et concernent la notion de dérivée (formelle), celle de dérivée logarithmique et un petit problème lié à la question plus vaste du remplacement de X par autre chose dans une série. Sur ce dernier point, nous nous limiterons ici au cas où l'on désire remplacer, dans une série s donnée, X par cX où c est un élément donné de l'anneau A dans lequel sont pris les coefficients. Si la série s s'écrit $a_0 + a_1 X + a_2 X^2 + \cdots$, ce remplacement de X par cX consiste simplement (et par définition) à remplacer s par la série $a_0 + a_1 cX + a_2 c^2 X^2 + \cdots$, c'est-à-dire par $\Sigma_{n=0}^{+\infty} a_n c^n X^n$. Si on note $s(cX)$ la nouvelle série, on démontre aussitôt le résultat suivant :

> **Théorème 5.**– Si s et t sont des séries formelles, à coefficients dans un anneau A quelconque, et si c est un élément de A, on a $(s + t)(cX) = s(cX) + t(cX)$ et $(st)(cX) = s(cX)t(cX)$.

Le lecteur remarquera, avec satisfaction, que $s = s(X)$ (où X est mis pour $1X \ldots$).

Lorsque s est l'une des séries $e^X, \sin X, \cos X$, on adoptera par convention les notations e^{cX}, $\sin cX$ et $\cos cX$ pour $s(cX)$ – ou mieux, car c'est plus joli comme cela, $e^{aX}, \sin aX$ et $\cos aX$ pour $s(aX)$.

On a ainsi, entre autres, $e^{aX} = 1 + \frac{aX}{1!} + \frac{a^2X^2}{2!} + \frac{a^3X^3}{3!} + \cdots$

Si on prend en particulier pour a le nombre i (ce qui suppose que l'on raisonne dans $\mathbb{C}$, ou plutôt dans $\mathbb{C}[[X]]$, on trouve comme par miracle

$$e^{iX} = 1 + \frac{iX}{1!} - \frac{X^2}{2!} - \frac{iX^3}{3!} + \frac{X^4}{4!} + \frac{iX^6}{6!} - \cdots = \cos X + i \sin X.$$

Comme la substitution de a par $-i$ donne de même $e^{-iX} = \cos X - i \sin X$, on tire de là les formules d'Euler (formelles!) :

$$\cos X = \frac{e^{iX} + e^{-iX}}{2} \text{ et } \sin X = \frac{e^{iX} - e^{-iX}}{2i} \tag{5}$$

valables dans l'anneau $\mathbb{C}[[X]]$.

On complètera ces propriétés de l'exponentielle formelle en établissant formellement que

$$e^{aX} e^{bX} = e^{(a+b)X} \tag{6}$$

quels que soient a, b (réels ou complexes).

Il est facile de voir que le coefficient du terme en X^n du produit $e^{aX}e^{bX}$ est $1\frac{b^n}{n!} + \frac{a}{1!}\frac{b^{n-1}}{(n-1)!} + \frac{a^2}{2!}\frac{b^{n-2}}{(n-2)!} + \cdots + \frac{a^n}{n!}1$, autrement dit une somme dont le terme général est $\frac{a^k b^{n-k}}{k!(n-k)!}$. Comme $C_n^k = \frac{n!}{k!(n-k)!}$, on reconnaît dans ce terme général $\frac{1}{n!}C_n^k a^k b^{n-k}$; d'où pour la somme complète $\frac{1}{n!}(a+b)^n$, ce qui est justement le coefficient du terme en X^n du second membre de l'égalité (6). CQFD.

En prenant $a = 1$ et $b = -1$, on trouve $e^X e^{-X} = 1$, ce qui se passe de commentaires.

La *dérivée formelle* d'une série s est par définition la série s', égale à $a_1 + 2a_2X + 3a_3X^2 + \cdots$, si $s = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots$ Ici, l'anneau A est quelconque. On a en particulier $(X^n)' = nX^{n-1}$ si $n \geq 1$ et $(a)' = 0$.

Théorème 6.– Si s et t sont des séries formelles quelconques, on a $(s+t)' = s' + t', (st)' = s't + st', (cs)' = cs'$ et $[s(cX)]' = cs'(cX)$ pour tout élément c de A.

Contentons-nous de vérifier la seconde et la quatrième égalité. Si on écrit $s = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots$ et $t = b_0 + b_1X + b_2X^2 + b_3X^3 + \cdots$ on a

$$\begin{aligned}(st)' =& [a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 \\ &+ (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)X^3 + \ldots]' \\ =& a_0b_1 + a_1b_0 + 2(a_0b_2 + a_1b_1 + a_2b_0)X \\ &+ 3(a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)X^2 + \ldots\end{aligned}$$

alors que

$$\begin{aligned} s't &= (a_1 + 2a_2X + 3a_3X^2 + \cdots)(b_0 + b_1X + b_2X^2 + \cdots) \\ &= a_1b_0 + (a_1b_1 + 2a_2b_0)X + ((a_1b_2 + 2a_2b_1 + 3a_3b_0)X^2 + \cdots \end{aligned}$$

et

$$\begin{aligned} st' &= (a_0 + a_1X + a_2X^2 + \cdots)(b_1 + 2b_2X + 3b_3X^2 + \cdots) \\ &= a_0b_1 + (2a_0b_2 + a_1b_1)X + (3a_0b_3 + 2a_1b_2 + a_2b_1)X^2 + \cdots \end{aligned}$$

On constate alors que l'addition de $s't$ et de st' donne $(st)'$. Que demander de plus ?

On a aussi $[s(cX)]' = (a_0 + a_1cX + a_2c^2X^2 + a_3c^3X^3 + \cdots)' = a_1c + 2a_2c^2X + 3a_3c^3X^2 + \cdots = c(a_1 + 2a_2cX + 3a_3c^2X^2 + \cdots) = cs'(cX)$.

Corollaire.– Si $s \in A[[X]]$ et si n est un entier $\geq 1, (s^n)' = ns^{n-1}s'$.

La démonstration est laissée au lecteur...

Si on applique la définition précédente à e^X, on trouve aisément, et comme par hasard, e^X. On vérifie de même sans problème que $(\sin X)' = \cos X$ et $(\cos X)' = -\sin X$. Mais nous n'aurons pas besoin de ces résultats. Passons plutôt à la définition et à l'étude de la notion de *dérivée logarithmique* $\lambda(s)$ d'une série s. Nous supposerons $s \neq 0$ et à coefficients dans un corps K. Moyennant quoi, nous poserons $\lambda(s) = \frac{s'}{s}$, le calcul s'effectuant dans le corps des fractions de $K[[X]]$. On a ainsi par exemple $\lambda(\sin X) = \frac{\cos X}{\sin X} = \cot X$.

Théorème 7.– Si s et t sont des séries formelles non nulles, on a $\lambda(st) = \lambda(s) + \lambda(t)$.

C'est immédiat car $\lambda(st) = \frac{(st)'}{st} = \frac{s't+st'}{st} = \frac{s'}{s} + \frac{t'}{t} = \lambda(s) + \lambda(t)$. On notera cependant l'intervention discrète du cor. 2 du th. 3.

Corollaire 1.– Si $c \in K$ et si $s \in k[[X]], \lambda(cs) = \lambda(s)$.

Cela vient de ce que $\lambda(c) = 0$.

Corolaire 2.– Si $s_1, \ldots, s_n$ est une suite de séries, $\lambda(\Pi_{i=1}^n s_i) = \Sigma_{i=1}^n \lambda(s_i)$.

Une récurrence s'impose!

A tout cela, enfin, on ajoutera la possibilité de définir une notion de convergence dite "*terme à terme*", pour les séries à coefficients réels ou complexes, qui consiste à dire qu'une suite (s_n) de séries de ce genre converge vers une série s si pour tout entier $k \geq 0$ (représentant un degré fixé), le coefficient $a_k^{(n)}$ du terme en X^k de s_n tend vers le coefficient a_k analogue de s lorsque n augmente indéfiniment. Donnons tout de suite un exemple spectaculaire :

Théorème 8.– Lorsque n tend vers $+\infty$, le polynôme $(1+\frac{X}{n})^n$ tend terme à terme vers la série exponentielle e^X.

Si on développe l'expression $(1+\frac{X}{n})^n$ par la formule du binôme, on sait que l'on obtient une somme dont le terme général est $C_n^k \frac{X^k}{n^k}$.

Quitte à définir le coefficient binomial C_n^k comme étant le nombre $\frac{n(n-1)\ldots(n-k+1)}{k!}$ (ce qui donne 0 si $k > n$), on peut dire que le coefficient de X^k dans la "série" $(1+\frac{X}{n})^n$ est $\frac{C_n^k}{n^k}$. Si k est fixé, ce coefficient est une fraction rationnelle en n, égale à $\frac{n(n-1)\ldots(n-k+1)}{k!n^k}$, qui tend donc vers $\frac{1}{k!}$ lorsque n tend vers $+\infty$. D'où le résultat cherché, compte tenu de ce que représente la notion de convergence terme à terme.

En plus de cet exemple, on retiendra les quatre règles contenues dans le théorème suivant :

Théorème 9.– Si (s_n) et (t_n) sont deux suites de séries formelles convergeant respectivement terme à terme vers s et t, alors (s_n+t_n) et (s_nt_n) convergent terme à terme vers $s+t$ pour la première et vers st pour la seconde. En outre, si c est un réel ou un complexe quelconque, la suite (cs_n) (resp. $(s_n(cX))$) converge terme à terme vers cs (resp. vers $s(cX)$).

Limitons la démonstration au cas le plus significatif. Supposons que $s_n = a_0^{(n)} + a_1^{(n)}X + a_2^{(n)}X^2 + \cdots$ et $t_n = b_0^{(n)} + b_1^{(n)}X + b_2^{(n)}X^2 + \cdots$ et que parallèlement $s = a_0 + a_1X + a_2X^2 + \cdots$ et $t = b_0 + b_1X + b_2X^2 + \cdots$ Alors le coefficient du terme en X^k de s_nt_n est, comme on sait, $a_0^{(n)}b_k^{(n)} + a_1^{(n)}b_{k-1}^{(n)} + \cdots + a_k^{(n)}b_0^{(n)}$. Comme $a_i^{(n)}$ tend vers a_i et que $b_j^{(n)}$ tend vers b_j (pour i et j fixés), on en déduit que le coefficient précédent tend vers $a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$, ce qui est le coefficient de X^k dans st.

Corolaire.– Lorsque n tend vers $+\infty$, $(1+\frac{iX}{n})^n$ (resp. $(1-\frac{iX}{n})^n$) tend terme à terme vers e^{iX} (resp. e^{-iX}).

On a des résultats semblables donnant, à la limite, $\cos X$ et $\sin X$.

Eh bien, après tout ça, on peut enfin passer au plat de résistance!

3. Calcul de $\zeta(4)$, $\zeta(6)$ et tutti quanti

Chacun sait, bien sûr, que pour n donné ≥ 1, les racines n-ièmes de l'unité dans $\mathbb{C}$ (c'est-à-dire les racines complexes du polynôme $X^n - 1$) sont les nombres $e^{2ik\pi/n} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ où k varie, au choix, de 0 à $n-1$, de 1 à n, ou d'un entier a donné à l'entier $a+n-1$.

Si on prend en particulier n impair, égal à $2m+1$, on peut faire varier ainsi k de $-m$ à m, ce qui donne la factorisation suivante pour le polynôme $X^n - 1$:

$$X^n - 1 = \Pi_{k=-m}^{m}(X - e^{2ik\pi/n}) = (X-1)\Pi_{k=1}^{m}(X - e^{2ik\pi/n})(x - e^{-2ik\pi/n})$$

la seconde expression s'obtenant en isolant $k = 0$ et en regroupant deux par deux

les facteurs restants. On en déduit une décomposition à coefficients réels :

$$X^n - 1 = (X-1)\Pi_{k=1}^{m}(X^2 - 2\cos\frac{2k\pi}{n}X + 1)$$

puis en remplaçant X par $\frac{X}{Y}$ et en multipliant par Y^n, la factorisation analogue :

$$X^n - Y^n = (X-Y)\Pi_{k=1}^{m}(X^2 - 2\cos\frac{2k\pi}{n}XY + Y^2)$$

et enfin, par une ultime substitution

$$\begin{aligned}(1+\frac{iX}{n})^n - (1-\frac{iX}{n})^n =& \frac{2iX}{n}\Pi_{k=1}^{m}[(1+\frac{iX}{n})^2 - 2\cos\frac{2k\pi}{n}(1+\frac{iX}{n}) \\ & (1-\frac{iX}{n}) + (1-\frac{iX}{n})^2] \\ =& \frac{2iX}{n}\Pi_{k=1}^{m}[(2-2\cos\frac{2k\pi}{n}) - (2+2\cos\frac{2k\pi}{n})\frac{X^2}{n^2}] \\ =& \frac{2iX}{n}\Pi_{k=1}^{m}(4\sin^2\frac{k\pi}{n} - 4\cos^2\frac{k\pi}{n}\frac{X^2}{n^2})\end{aligned}$$

en terminant le calcul par un peu de trigonométrie : $2 - 2\cos 2\theta = 2 - 2(\cos^2\theta - \sin^2\theta) = 2 - 2(1 - 2\sin^2\theta) = 4\sin^2\theta$ et $2 + 2\cos 2\theta = 2 + 2(\cos^2\theta - \sin^2\theta) = 2 + 2(2\cos^2\theta - 1) = 4\cos^2\theta$.

La dérivée logarithmique du premier membre donne alors, grâce au théorème 6 ci-dessus (et à son corollaire) :

$$\frac{n(1+\frac{iX}{n})^{n-1}(\frac{i}{n}) - n(1-\frac{iX}{n})^{n-1}(-\frac{i}{n})}{(1+\frac{iX}{n})^n - (1-\frac{iX}{n})^n} = i\frac{(1+\frac{iX}{n})^{n-1} + (1-\frac{iX}{n})^{n-1}}{(1+\frac{iX}{n})^n - (1-\frac{iX}{n})^n}$$

alors que celle du second membre est (cf. le th. 7 et ses corollaires) :

$$\frac{1}{X} + \sum_{k=1}^{m}\frac{-8\cos^2\frac{k\pi}{n}\cdot\frac{X}{n^2}}{4\sin^2\frac{k\pi}{n} - 4\cos^2\frac{k\pi}{n}\cdot\frac{X^2}{n^2}} = \frac{1}{X} + \sum_{k=1}^{m}\frac{-2\cot^2\frac{k\pi}{n}\cdot\frac{X}{n^2}}{1 - \cot^2\frac{k\pi}{n}\cdot\frac{X^2}{n^2}}$$

en divisant numérateur et dénominateur par $4\sin^2\frac{k\pi}{n}$ (ce qui est possible car $\sin\frac{k\pi}{n} \neq 0$ vu que $0 < \frac{k\pi}{n} \leq \frac{m\pi}{n} < \frac{\pi}{2}$: on rappelle que $n = 2m+1$).

Le terme général de la somme finale est une fraction rationnelle qu'il est possible de transformer en une série formelle car on vérifie facilement que

$$\frac{1}{1 - \cot^2\frac{k\pi}{n}\frac{X^2}{n^2}} = 1 + \cot^2\frac{k\pi}{n}\frac{X^2}{n^2} + \cot^4\frac{k\pi}{n}\frac{X^4}{n^4} + \cot^6\frac{k\pi}{n}\frac{X^6}{n^6} + \cdots$$

C'est le même principe que pour l'égalité $\frac{1}{1-X} = 1 + X + X^2 + X^3 + \cdots$ vue (en substance) dans le précédent paragraphe.

D'où pour ce terme général l'expression

$$-2\cot^2\frac{k\pi}{n}\cdot\frac{X}{n^2}-2\cot^4\frac{k\pi}{n}\cdot\frac{X^3}{n^4}-2\cot^6\frac{k\pi}{n}\cdot\frac{X^5}{n^6}-2\cot^8\frac{k\pi}{n}\cdot\frac{X^7}{n^8}-\cdots$$

Si on additionne ces séries terme à terme (pour k variant de 1 à m) et si on reprend le premier membre du début, on obtient l'égalité

$$i\frac{(1+\frac{iX}{n})^{n-1}+(1-\frac{iX}{n})^{n-1}}{(1+\frac{iX}{n})^n-(1-\frac{iX}{n})^n}=\frac{1}{X}-2\frac{\sigma_2(n)}{n^2}X-2\frac{\sigma_4(n)}{n^4}X^3-2\frac{\sigma_6(n)}{n^6}X^5-2\frac{\sigma_8(n)}{n^8}X^7-\cdots$$

où l'on a posé

$$\sigma_2(n)=\sum_{k=1}^{m}\cot^2\frac{k\pi}{n},\ \sigma_4(n)=\sum_{k=1}^{m}\cot^4\frac{k\pi}{n},$$
$$\sigma_6(n)=\sum_{k=1}^{m}\cot^6\frac{k\pi}{n},\ \sigma_8(n)=\sum_{k=1}^{m}\cot^8\frac{k\pi}{n},$$

etc. (rappelons que m dépend directement de n puisque $n=2m+1$). Quitte à éliminer les dénominateurs par une multiplication convenable, cela peut s'écrire aussi :

$$iX[(1+\tfrac{iX}{n})^{n-1}+(1-\tfrac{iX}{n})^{n-1}] \tag{7}$$
$$=[(1+\tfrac{iX}{n})^n-(1-\tfrac{iX}{n})^n][1-2\tfrac{\sigma_2^{(n)}}{n^2}X^2-2\tfrac{\sigma_4(n)}{n^4}X^4-2\tfrac{\sigma_6(n)}{n^6}X^6-\cdots].$$

Examinons alors ce qui se passe lorsqu'on fait tendre n vers $+\infty$ (tout en le gardant impair). Il n'y a pas de problème pour $(1+\frac{iX}{n})^n$ et pour $(1-\frac{iX}{n})^n$ puisqu'on a vu en corollaire du théorème 9 que les limites respectives sont e^{iX} et e^{-iX}. On en déduit que la différence tend (terme à terme, ne l'oublions pas!) vers $2i\sin X$. Pour ce qui est de $(1+\frac{iX}{n})^{n-1}$, il est facile de vérifier que

$$(1+\frac{iX}{n})^{n-1}=(1+\frac{iX}{n})^n\frac{1}{1+\frac{iX}{n}}=(1+\frac{iX}{n})^n[1-\frac{iX}{n}+\frac{i^2X^2}{n^2}-\frac{i^3X^3}{n^3}+\cdots]$$

C'est encore une variante de la formule $\frac{1}{1-X}=1+X+X^2+X^3\cdots$

Comme $\frac{ik}{n^k}$, tend vers 0 lorsque n augmente indéfiniment, on en déduit que l'expression entre crochets ci-dessus tend terme à terme vers 1. En raisonnant de même pour $(1-\frac{iX}{n})^{n-1}$ on en déduit que le premier membre de (7) tend vers $2i\cos X$.

Reste à chercher la limite de $\frac{\sigma_2(n)}{n^2}$, de $\frac{\sigma_4(n)}{n^4}$, de $\frac{\sigma_6(n)}{n^6}$, etc.

La première peut s'obtenir en réutilisant la relation vue dans le premier paragraphe : $\cot^2\theta<\frac{1}{\theta^2}<1+\cot^2\theta$ qu'on va réécrire ici $\frac{1}{\theta^2}<1+\cot^2\theta<1+\frac{1}{\theta^2}$. En prenant $\theta=\frac{\pi}{n},\frac{2\pi}{n},\cdots,\frac{m\pi}{n}$ et en ajoutant membre à membre, on obtient $\frac{n^2}{\pi^2}(1+\frac{1}{2^2}+\cdots+\frac{1}{m^2})<m+\sigma_2(n)<m+\frac{n^2}{\pi^2}(1+\frac{1}{2^2}+\cdots+\frac{1}{m^2})$. Si on divise tout par n^2 et si on fait tendre $n=2m+1$ vers $+\infty$, on constate que les

expressions extrêmes ont toutes deux pour limites $\frac{\zeta(2)}{\pi^2}$ (car $\frac{m}{n^2} = \frac{n-1}{2n^2}$ tend vers 0).Il en est donc de même de $\frac{m}{n^2} + \frac{\sigma_2(n)}{n^2}$, donc finalement de $\frac{\sigma_2(n)}{n^2}$.

Pour $\frac{\sigma_4(n)}{n^4}$, on part de l'encadrement $\frac{1}{\theta^4} < 1 + 2\cot^2\theta + \cot^4\theta < 1 + \frac{2}{\theta^2} + \frac{1}{\theta^4}$ qui donne, avec $\theta = \frac{\pi}{n}, \frac{2\pi}{n}, \cdots \frac{m\pi}{n}$ et par addition, $\frac{n^4}{\pi^4}(1 + \frac{1}{2^4} + \cdots + \frac{1}{m^4}) < m + 2\sigma_2(n) + \sigma_4(n) < m + \frac{2n^2}{\pi^2}(1 + \frac{1}{2^2} + \cdots + \frac{1}{m^2}) + \frac{n^4}{\pi^4}(1 + \frac{1}{2^4} + \cdots + \frac{1}{m^4})$. Si on divise par n^4 et si on fait tendre n vers $+\infty$, on voit encore que les expressions encadrantes ont la même limite, $\frac{\zeta(4)}{\pi^4}$ (car $\frac{m}{n^4}$ et $\frac{2}{\pi^2 n^2}(1 + \frac{1}{2^2} + \cdots + \frac{1}{m^2})$ ont toutes deux pour limite 0). Il en est donc de même de l'expression du milieu $\frac{m}{n^4} + 2\frac{\sigma_2(n)}{n^4} + \frac{\sigma_4(n)}{n^4}$, donc finalement de $\frac{\sigma_4(n)}{n^4}$ (on observera que d'après le cas précédent $\frac{2\sigma_2(n)}{n^4}$ tend vers 0). Le cas général qui demande une petite récurrence (que dis-je? une récurrence soignée!) et l'usage de la formule du binôme se traite de même. Moyennant quoi, le passage à la limite terme à terme dans (7) donne finalement la relation

$$2iX\cos X = 2i\sin X(1 - 2\frac{\zeta(2)}{\pi^2}X^2 - 2\frac{\zeta(4)}{\pi^4}X^4 - 2\frac{\zeta(6)}{\pi^6}X^6 - \cdots)$$

ou si on préfère, le développement en série formelle de la cotangente formelle, sous la forme

$$X\cot X = 1 - 2\frac{\zeta(2)}{\pi^2}X^2 - 2\frac{\zeta(4)}{\pi^4}X^4 - 2\frac{\zeta(6)}{\pi^6}X^6 - \cdots \tag{8}$$

Cela ne donne pas encore, certes, la valeur de $\zeta(2k)$, mais permet d'affirmer qu'en général le quotient $\frac{\zeta(2k)}{\pi^{2k}}$ est un nombre rationnel : il est clair en effet que la série $X\cot X = \frac{X\cos X}{\sin X}$ est à coefficients dans $\mathbb{Q}$. Pour les connaisseurs, cela implique que $\zeta(2k)$ est un nombre transcendant et en particulier un irrationnel ...

Pour calculer la valeur du quotient qui nous manque, on va chercher à atteindre $X\cot X$ à l'aide des formules d'Euler, en raisonnant plus ou moins dans le corps $\mathbb{C}((X))$ et en utilisant (6). Cela donne

$$\begin{aligned} X\cot X = X\frac{\cos X}{\sin X} &= X\frac{(e^{iX} + e^{-iX})/2}{(e^{iX} - e^{-iX})/2i} \\ &= iX\frac{e^{-iX}(e^{2iX} + 1)}{e^{-iX}(e^{2iX} - 1)} = iX\frac{e^{2iX} - 1 + 2}{e^{2iX} - 1} = iX + \frac{2iX}{e^{2iX} - 1}. \end{aligned}$$

On remarque alors que la série $\frac{2iX}{e^{2iX}-1}$ est l'inverse de la série $\frac{e^{2iX}-1}{2iX}$, laquelle s'écrit $\frac{1}{2iX}(1 + \frac{2iX}{1!} + \frac{(2iX)^2}{2!} + \frac{(2iX)^3}{3!} + \cdots - 1) = \frac{1}{1!} + \frac{2iX}{2!} + \frac{(2iX)^2}{3!} + \cdots$ ou si on aime mieux $\Sigma_{n=0}^{+\infty}\alpha_n X^n$ avec $\alpha_n = \frac{(2i)^n}{(n+1)!}$.

La série $\frac{2iX}{e^{2iX}-1}$ cherchée s'écrit donc $\Sigma_{n=0}^{+\infty}\beta_n X^n$ où les coefficients β_n peuvent être calculés de proche en proche au moyen des relations

$$\begin{gathered} \alpha_0\beta_0 = 1,\ \alpha_0\beta_1 + \alpha_1\beta_0 = 0,\ \alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0 = 0, \\ \alpha_0\beta_3 + \alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_3\beta_0 = 0, \ldots \end{gathered} \tag{9}$$

(l'usage de lettres grecques, ici, est destiné à éviter toute confusion avec les nombres de Bernoulli dont on dira un mot plus loin).

Le rapprochement de (8) et de l'égalité $X\cot X = iX + \frac{2iX}{e^{2iX}-1} = \beta_0 + (\beta_1 + i)X + \Sigma_{n=2}^{+\infty}\beta_n X^n$ montre que $\zeta(2) = -\frac{\beta_2}{2}\pi^2$, $\zeta(4) = -\frac{\beta_4}{2}\pi^4$, $\zeta(6) = -\frac{\beta_6}{2}\pi^6$, etc. Le lecteur avisé verra sans doute d'avance que $\beta_1 + i = 0$, $\beta_3 = 0$, $\beta_5 = 0$, etc. Quoi qu'il en soit, les relations (9) donnent successivement (et de plus en plus péniblement) :

$\alpha_0 = 1$	$\beta_0 = 1$		$\alpha_5 = \frac{2i}{45}$	$\beta_5 = 0$	
$\alpha_1 = i$	$\beta_1 = -i$		$\alpha_6 = -\frac{4}{315}$	$\beta_6 = -\frac{2}{945}$	d'où $\zeta(6) = \frac{\pi^6}{945}$
$\alpha_2 = -\frac{2}{3}$	$\beta_2 = -\frac{1}{3}$	d'où $\zeta(2) = \frac{\pi^2}{6}$	$\alpha_7 = -\frac{i}{315}$	$\beta_7 = 0$	
$\alpha_3 = -\frac{i}{3}$	$\beta_3 = 0$		$\alpha_8 = \frac{2}{2835}$	$\beta_8 = -\frac{1}{4725}$	d'où $\zeta(8) = \frac{\pi^8}{9450}$
$\alpha_4 = \frac{2}{15}$	$\beta_4 = -\frac{1}{45}$	d'où $\zeta(4) = \frac{\pi^4}{90}$	$\alpha_9 = \frac{2i}{14175}$	$\beta_9 = 0$	

4. Epilogue : les nombres de Bernoulli

On peut trouver gênant que le calcul des nombres β_n dépende d'une série dont certains coefficients soient des nombres imaginaires. Le mal vient évidemment de la série $\frac{2iX}{e^{2iX}-1}$. C'est pourquoi on présente souvent les résultats précédents au moyen de la série $\frac{X}{e^X-1}$ qui n'a pas les mêmes inconvénients et pour des raisons variées on en profite pour multiplier le coefficient du terme en X^n par $n!$. Le résultat obtenu se note souvent b_n (cf. N. Bourbaki, Fonctions d'une variable réelle, chap. VI, p.8, 1976) et s'appelle le n-ième *nombre de Bernoulli*. De façon précise, les nombres b_n sont définis par le "développement de Taylor"

$$\frac{X}{e^X-1} = b_0 + \frac{b_1}{1!}X + \frac{b_2}{2!}X^2 + \frac{b_3}{3!}X^3 + \cdots = \sum_{n=0}^{+\infty}\frac{b_n}{n!}X^n.$$

Comme il s'agit d'inverser la série $\frac{e^X-1}{X} = \frac{1}{1!} + \frac{X}{2!} + \frac{X^2}{3!} + \cdots = \Sigma_{n=0}^{+\infty}\frac{X^n}{(n+1)!}$, on doit avoir $b_0 = 1$ et $\frac{1}{1!}\frac{b_n}{n!} + \frac{1}{2!}\frac{b_{n-1}}{(n-1)!} + \cdots + \frac{1}{(n+1)!}b_0 = 0$ pour tout $n \geq 1$. En multipliant les deux membres de cette relation par $(n+1)!$, on obtient des coefficients binômiaux C_{n+1}^k et donc la relation, assez commode pour les calculs :

$$C_{n+1}^1 b_n + C_{n+1}^2 b_{n-1} + \ldots + C_{n+1}^{n+1} b_0 = 0 \tag{10}$$

c'est-à-dire concrètement $2b_1 + b_0 = 0$, $3b_2 + 3b_1 + b_0 = 0$, $4b_3 + 6b_2 + 4b_1 + b_0 = 0$, $5b_4 + 10b_3 + 10b_2 + 5b_1 + b_0 = 0$, $6b_5 + 15b_4 + 20b_3 + 15b_2 + 6b_1 + b_0 = 0$, etc. On trouve ainsi sans trop de difficultés $b_1 = -\frac{1}{2}, b_2 = \frac{1}{6}, b_3 = 0, b_4 = -\frac{1}{30}, b_5 = 0$. Des considérations de parité relatives à la série $\frac{X}{e^X-1} + \frac{1}{2}X$ permettent de montrer que $b_{2n+1} = 0$ si $n \geq 1$. Il reste donc à trouver b_{2n} pour $n \geq 3$, ce qui est laissé au lecteur, disons jusqu'à $2n = 30$.

De la définition des nombres b_n résulte que $\frac{2iX}{e^{2iX}-1} = \Sigma_{n=0}^{+\infty} \frac{b_n}{n!}(2iX)^n$. De là, on tire le développement de $X \cot X = iX + \frac{2iX}{e^{2iX}-1}$ en fonction des nombres de Bernoulli :

$$X \cot X = 1 - 4\frac{b_2}{2!}X^2 + 16\frac{b_4}{4!}X^4 - 64\frac{b_6}{6!}X^6 + \cdots = 1 + \sum_{k=1}^{+\infty}(-1)^k 2^{2k}\frac{b_{2k}}{(2k)!}X^{2k}$$

et l'expression usuelle des nombres $\zeta(2k)$:

$$\zeta(2k) = (-1)^{k-1}\frac{(2\pi)^{2k}b_2 k}{2(2k)!}. \tag{11}$$

Cela permet de voir que les nombres b_{2k} sont alternativement positifs et négatifs (ce qui n'était pas du tout évident au départ) et de donner à partir des inégalités $1 \leq \zeta(2k) \leq \zeta(2) = \frac{\pi^2}{6}$ l'encadrement suivant pour b_{2k} :

$$\frac{2(2k)!}{(2\pi)^{2k}} \leq |b_{2k}| \leq \frac{(2k)!}{3.2^{2k}\pi^{2k-2}}$$

de sorte que l'on a $b_{30} \geq 601\ 580\ 873$, $b_{40} \geq 1,92 \times 10^{16}$, $b_{50} \geq 7,5 \times 10^{24}$, etc. Je recopie sans réfléchir des calculs que j'ai fait l'an dernier et que j'ai la flemme de vérifier. Le lecteur s'en chargera!

Les nombres de Bernoulli interviennent dans plusieurs autres formules. Citons

$$\tan X = \sum_{k=1}^{+\infty}(-1)^{k-1}2^{2k}(2^{2k}-1)b_{2k}\frac{x^{2k-1}}{(2k)!}$$

$$\frac{1}{\sin X} = \frac{1}{X} + \sum_{k=1}^{+\infty}(-1)^{k-1}2(2^{2k-1}-1)b_{2k}\frac{X^{2k-1}}{(2k)!}.$$

Là, je recopie Bourbaki (FVR, chap. VI, p. 22, ex. 1 du § 22) en remplaçant n par k et z par X : c'est assez facile.

Avis aux amateurs : y a-t-il quelque chose de semblable pour $\frac{1}{\cos X}$?

Plus intéressante est l'identité :

$$1^k + 2^k + \cdots + n^k = \frac{n^{k+1}}{k+1} + \frac{1}{2}n^k + \frac{1}{k+1}\sum_{i=2}^{k} C_{k+1}^i b_i n^{k+1-i}$$

qui est en fait à l'origine des nombres b_n et qui a été découverte par Jacques Bernoulli vers la fin du XVII$^{\text{e}}$ siècle (l'appellation même de "nombres de Bernoulli", popularisée par Euler, est due à de Moivre).

Mais ce qui est fascinant (du moins pour moi qui n'y comprends rien) est le fait que les numérateurs des nombres b_{2n} jouent un rôle capital dans la résolution

(encore inachevée) de l'équation de Fermat $x^m + y^m = z^m$. Je ne sais si, un jour, le groupe de Saumur aura l'occasion d'aborder ces difficiles questions ... Pour la saison 92-93, il a déjà prévu à son programme les fractions continues et l'équation de Pell. Du gâteau!

Post-scriptum

Je m'aperçois en relisant que je n'ai rien dit des nombres $\zeta(2k+1)$. C'est que la situation est très simple : jusqu'en 1979 (je mets ici la date de parution de l'article explicatif dans la revue "*Astérisque*"), on ne savait rien d'important à leur sujet. Depuis cette date, on sait, grâce à Roger Apéry, que $\zeta(3)$ est irrationnel. C'est tout.

Bien entendu, cela n'empêche pas de calculer $\zeta(3), \zeta(5)$, etc., avec le plus de décimales possibles. Euler avait déjà commencé, dans les années 1740, en donnant $\zeta(3)$ avec 15 décimales, grâce à la formule dite d'Euler-Maclaurin qui, j'y pense tout à coup, dépend aussi des nombres de Bernoulli. Ils sont vraiment partout!

AIGUILLES A TRICOTER

On trouvait page 21 de '*L'Ouvert*' n° 66 le problème de la conversion des mesures françaises (métriques) en mesures anglo-saxonnes pour la taille des aiguilles à tricoter.

Notons "f" la mesure française qui n'est autre que le diamètre en millimètres et "a" la mesure anglaise.

Différentes fonctions peuvent être proposées reliant f et a, étant donnée la précision très relative de l'appareil. Comme f et a varient en sens inverse l'un de l'autre on peut chercher une relation de la forme $(\alpha f + \beta)(\alpha' a + \beta') = \gamma$.

Dans ce cas, la réponse :

$$(5f + 22)(a + 16) = 1000$$

est satisfaisante et permet de travailler avec des entiers. On peut proposer d'autres types de réponses, mais la rédaction de '*L'Ouvert*' n'a rien reçu sur le sujet.

UNE PREUVE LUMINEUSE DE LA RELATION

$$1+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\cdots=2(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots)^2$$

Dominique DUMONT

On sait qu'Euler a calculé la somme des inverses des carrés des entiers naturels et trouvé

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots=\frac{\pi^2}{6}$$

par plusieurs méthodes dont aucune ne constitue une preuve rigoureuse au sens où on l'entend depuis le siècle dernier. Dans ce qui suit nous proposons une nouvelle preuve *à la manière d'Euler* de ce résultat, mais comme cette manière n'est plus guère appréciée de nos jours, nous laisserons aux lecteurs le soin de "justifier" cette preuve, ou le ferons ultérieurement.

Il existe de nombreuses démonstrations de l'identité d'Euler, elles consistent le plus souvent à utiliser un développement en série de Fourier (souvent tiré lui aussi des œuvres d'Euler) dont on donne une démonstration certes rigoureuse mais jamais vraiment élémentaire. La preuve "lumineuse" qu'on propose ici ne requiert que très peu d'Analyse, et consiste en manipulations de séries.

Remarquons tout d'abord que la partie paire de la série d'Euler représente le quart du total, donc la partie impaire représente les trois quarts du total, par conséquent l'identité d'Euler est équivalente à

$$1+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\cdots=\frac{\pi^2}{8}.$$

Or on connaît bien la somme, plus élémentaire, de la série de Leibniz

$$1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots=\frac{\pi}{4}.$$

Rappelons-en la démonstration. On a pour tout x réel

$$\frac{1}{1+x^2}=1-x^2+x^4-\cdots+(-1)^{n-1}x^{2n-2}+\frac{(-1)^n x^{2n}}{1+x^2}$$

d'où en intégrant entre 0 et 1

$$\operatorname{Arctg} 1=1-\frac{1}{3}+\frac{1}{5}-\cdots+(-1)^{n-1}\frac{1}{2n-1}+R_n$$

avec

$$|R_n| = |\int_0^1 \frac{(-1)^n x^{2n}}{1+x^2} dx| \leq \int_0^1 x^{2n} dx = \frac{1}{2n+1}$$

d'où

$$\lim_{n\to\infty}(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots \frac{(-1)^{n-1}}{2n-1}) = \text{Arctg } 1 = \frac{\pi}{4}\cdot$$

Dans ces conditions le résultat d'Euler est équivalent à

$$1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \cdots = 2(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots)^2,$$

et c'est cette identité-là que nous nous proposons de démontrer directement en prenant le carré de la série de Leibniz :

$$\Big(\sum_{p=1}^{\infty} \frac{(-1)^{p+1}}{(2p-1)}\Big)\Big(\sum_{q=1}^{\infty} \frac{(-1)^{q+1}}{(2q-1)}\Big) = \sum_{(p,q)} \frac{(-1)^{p+q}}{(2p-1)(2q-1)} = \frac{\pi^2}{16}.$$

Dans le premier quadrant, nous dessinons le réseau $\Re$ des points dont les coordonnées sont des entiers naturels impairs, et au point de coordonnées $(2p-1, 2q-1)$ nous portons le nombre $\frac{(-1)^{p+q}}{(2p-1)(2q-1)}$.

Dans tout ce qui suit nous allons considérer la somme de la série-double restreinte à tel ou tel sous-ensemble du réseau $\Re$, nous conviendrons d'utiliser une majuscule E pour désigner le sous-ensemble en question, et la minuscule correspondante e pour désigner la somme de la série-double restreinte à ce sous-ensemble.

Etant donné un entier $n > 0$, nous notons R_n le *rayon lumineux* incliné à 45 degrés qui se reflète sur les axes de coordonnées aux points $(0, 2n)$ et $(2n, 0)$. Ce rayon R_n est constitué
— de la demi-droite D_n qui passe par les points $(1, 2n+1), (3, 2n+3), (5, 2n+5), \ldots$
— du segment S_n qui passe par les n points $(1, 2n-1), (3, 2n-3), \ldots (2n-1, 1), \ldots$
— de la demi-droite $\overline{D}_n$ qui passe par les points $(2n+1, 1), (2n+3, 3), (2n+5, 5), \ldots$

Lemme fondamental. *Pour tout $n \geq 0$, la somme r_n des termes de la série-double situés sur le rayon lumineux R_n est nulle.*

Montrons cela dans un cas particulier, par exemple sur le rayon R_3. Pour calculer la somme sur D_3, nous utilisons l'identité $\frac{1}{ab} = \frac{1}{b-a}(\frac{1}{a} - \frac{1}{b})$, et obtenons :

$$\begin{aligned} d_3 &= -(\frac{1}{1.7} + \frac{1}{3.9} + \frac{1}{5.11} + \frac{1}{7.13} + \cdots) \\ &= -\frac{1}{6}\Big((1 - \frac{1}{7}) + (\frac{1}{3} - \frac{1}{9}) + (\frac{1}{5} - \frac{1}{11}) + (\frac{1}{7} - \frac{1}{13}) + \cdots\Big) \\ &= -\frac{1}{6}(1 + \frac{1}{3} + \frac{1}{5}). \end{aligned}$$

Pour calculer la somme sur S_3, nous utilisons l'identité $\frac{1}{ab} = \frac{1}{a+b}(\frac{1}{a}+\frac{1}{b})$, et obtenons :

$$s_3 = \frac{1}{1.5}+\frac{1}{3.3}+\frac{1}{5.1} = \frac{1}{6}(1+\frac{1}{5}+\frac{1}{3}+\frac{1}{3}+\frac{1}{5}+1) = \frac{1}{3}(1+\frac{1}{3}+\frac{1}{5}).$$

Comme par raison de symétrie la somme sur $\overline{D}_3$ vaut celle sur D_3, on trouve bien que la somme sur le rayon R_3 est nulle.

Plus généralement, le lecteur se convaincra aisément qu'on a sur le segment S_n la somme

$$s_n = (-1)^{n+1}\sum_{p+q=n+1}\frac{1}{(2p-1)(2q-1)} = (-1)^{n+1}\frac{1}{n}(1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n-1})$$

et que les sommes d_n et $\overline{d}_n$ sont chacune égale à la moitié de cette quantité avec le signe opposé, d'où le résultat général.

Si nous prenons la réunion des R_n pour $n = 1,2,3,\ldots$, nous voyons que nous passons deux fois sur chaque point du réseau (une fois sur une demi-droite, une fois sur un segment), à l'exception des points de la diagonale principale Δ sur lesquels nous ne passons qu'une fois (sur un segment). Nous décidons donc d'ajouter la diagonale principale Δ parcourue *une seule fois*, de sorte qu'en prenant la réunion des rayons R_n et de Δ, nous passons exactement deux fois sur chaque point du réseau $\Re$. Par conséquent

$$\delta = \delta + r_1 + r_2 + r_3 + \ldots = 2\sum_{\Re},$$

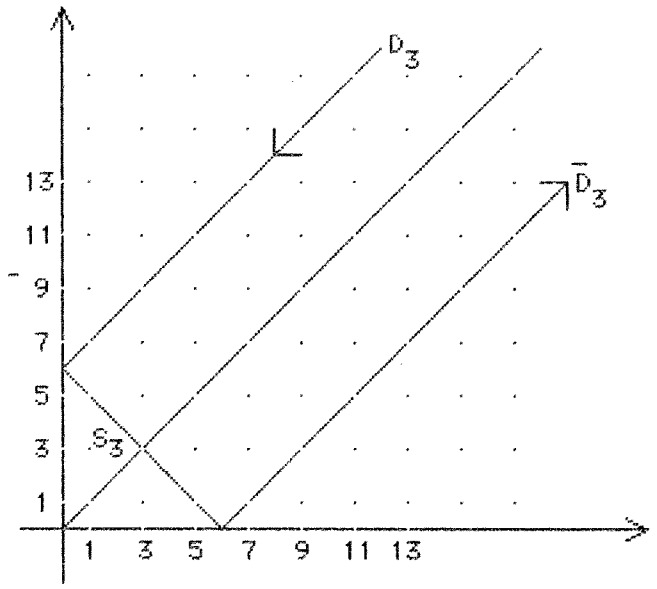
d'où le résultat annoncé :

$$\sum_p \frac{1}{(2p-1)^2} = 2\sum_{p,q\geq 1}\frac{(-1)^{p+q}}{(2p-1)(2q-1)} = 2\Big(\sum_{p=1}^{\infty}\frac{(-1)^{p+1}}{(2p-1)}\Big)^2.$$

Si cette démonstration aurait probablement convenu à Euler, elle manque terriblement de rigueur. La série-double que nous considérons ne constitue pas une *famille sommable*. L'écriture de la somme

$$\sum_{p,q\geq 1}\frac{(-1)^{p+q}}{(2p-1)(2q-1)}$$

n'a pas de sens précis, et nous courons le risque d'obtenir des limites distinctes selon la manière dont nous faisons tendre le domaine de sommation vers le réseau tout entier. Nous laissons aux lecteurs le soin de remédier à ce défaut, et sinon nous tenterons de le faire dans un article ultérieur.



Le rayon lumineux R_3

RÉFLEXIONS PRÉLABLES À UNE ÉTUDE DES OBSTACLES

Georges GLAESER

I. Science ou systèmes idéologiques

La didactique expérimentale des mathématiques (D.E.M.) se nourrit de l'étude des **difficultés** d'apprentissage et des **erreurs des élèves**. Avant d'en aborder l'étude, elle peut prendre le temps de jeter un regard sur l'histoire des sciences qui se sont trouvées devant des tâches analogues.

Pendant des millénaires, la médecine empirique rêvait d'une **théorie générale des maladies** et d'une **belle typologie des symptômes**.

De même, la pré-physique s'est lancée, tête baissée, dans une classification des substances parmi lesquelles elle distinguait les "éléments".

Pour Empédocle, V^{e} siècle avant J.-C., c'étaient "la terre, l'eau, l'air, le feu", d'où d'autres penseurs ont déduit "le chaud et le froid, le sec et l'humide" ou encore "le vide et le plein", "la couleur", "l'âme", etc...

L'humanité a chèrement payé ces anticipations hâtives, puisqu'au XVIII^{e} siècle des "physiques" laissent encore des séquelles même dans l'esprit de grands savants (relisez attentivement Bachelard (BA)).

Or, si de nos jours, la science étudie encore, dans des chapitres séparés certaines de ces notions, elle n'en retient **aucune** comme élément premier.

> **L'impatience théorique a souvent constitué un frein puissant qui contraria les progrès ultérieurs.**

Pour la didactique, la tentation est grande de brosser à grands traits une **théorie des obstacles** autour de laquelle nos connaissances s'organiseraient harmonieusement. Il est certainement indispensable de placer nos recherches futures en perspectives, et d'imaginer par prémonition les progrès futurs.

Mais de grâce, chers amis, **n'oubliez pas Empédocle!** Ne prenons pas pour argent comptant des supputations hâtives. Ne vous laissez pas séduire par le verbe, ou par l'analogie facile.

Notre didactique doit opposer radicalement les deux attitudes suivantes :

> **A) Examen scrupuleux de quelques situations en rapport avec la génèse des concepts, des connaissances ou des habitudes qui interviennent au cours des apprentissages mathématiques. Le traitement de ces phénomènes se soumet aux exigences de l'esprit scientifique.**

Article publié dans le "Séminaire de didactique des mathématiques et de l'informatique" de l'I.M.A.G. (Grenoble) n° 56 (1984) et publié avec l'aimable autorisation de l'auteur et de l'I.M.A.G.

B) Dissertation littéraire qui ne s'appuie que sur des opinions a priori, sans distinguer le rêve et la réalité, ni la constatation factuelle de l'anticipation prophétique.

Tous les didacticiens (y compris moi-même) prennent tour à tour les deux attitudes. Ils se distinguent entre eux, par le degré de foi qu'ils attachent aux conclusions tirées de l'attitude B).

Cette remarque s'applique particulièrement à Jean Piaget, précurseur de notre science. Il a découvert beaucoup de phénomènes importants grâce à l'attitude A). Mais, ce philosophe succomba plus d'une fois au démon des généralisations hâtives. Une tâche urgente qui incombe à notre D.E.M. est de procéder à un réexamen de l'héritage piagétien, pour distinguer ce qui s'appuie sur l'expérience de ce qui dérive d'une idéologie suspecte a priori.

II. Quelques dichotomies plausibles

En ce qui concerne les erreurs et les difficultés, nous sommes confrontés à **un chaos de constatations disparates**. Parmi les faits qui nous sont proposés, certains sont des fictions inventées de toute pièce, ou des annecdotes plus ou moins significatives.

D'autres sont rapportés avec trop peu de précision. Par exemple, on nous relate des exemples d'erreurs commises, sans que nous ayons des renseignements suffisants sur le sort ultérieur de l'incident : (on aurait envie de distinguer une infirmité rapidement guérie, de celles qui persistent en dépit de tous les traitements).

Certaines affirmations sont fréquemment confirmées par une masse de témoignages indépendants, ce qui leur confèrent un label de sérieux : cependant, il est des témoignages collectifs qui ne conduisent pas nécessairement à des certitudes (pensez aux O.V.N.I.).

Enfin, nous connaissons des faits qui ont été observés avec une minutie pastorienne, en prenant toutes les précautions expérimentales qui s'imposent.

Il s'agit de décider, **a priori**, mais **provisoirement**, ce que nous rejetons hors de notre domaine d'étude. Puis, dans le fatras restant, on opèrera des distinctions : considérons nous que la terre et le feu sont des "éléments" de même nature?

Dans ce qui suit, je me contente de poser beaucoup de questions, puis d'examiner des éléments de réponses plausibles, en opposant le pour et le contre.

Le seul point sur lequel je serai affirmatif est, qu'en **l'état actuel, nous n'avons pas les moyens de trancher!**

III. Le fortuit et le significatif

Parmi les faits qui nous sont proposés, quels sont ceux dont la didactique n'a pas à se préoccuper provisoirement?

La question a surgit, lorsque j'ai lu le travail de Jean Tonnelle "Le monde clos de la factorisation" (I.R.E.M. de Marseille, 1979). Il s'agit d'une réflexion qui s'appuie

essentiellement, sur un seul fait curieux, observé sur deux élèves :
"*Ayant à factoriser* $2a - 2x$, *une collégienne propose*

$$2a - 2x = (\sqrt{2a} - \sqrt{2x})(\sqrt{2a} + \sqrt{2x})''.$$

Ce fait présente-t-il assez d'importance pour mériter une étude didactique? J'avoue qu'à première vue, j'ai pensé que depuis que j'enseigne (1935), je ne me souviens pas d'avoir rencontré la même "déviation".

Puis, un événement personnel m'est revenu en mémoire. Lorsque j'étais en seconde, je m'étais beaucoup ennuyé à rédiger un devoir insipide où l'on posait, entre autre, la question : "Compléter le carré suivant...: $x^2 + 8x...$"

Après avoir donné la réponse attendue, je me suis permis à titre de canular de faire la remarque de mauvaise foi : "Les carrés suivants répondent aussi à la question : $(x + \sqrt{8x})^2$ ou $(\sqrt{8x} + \frac{x^2}{2\sqrt{8x}})^2$.

Mon cher professeur, Albert Momal, manqua d'humour en cette occasion et me réprimanda vertement. On dirait aujourd'hui que j'avais transgressé le contrat didactique.

J'aurais tendance à considérer que le cas signalé n'est qu'une curiosité... Mais soyons méfiants : il existe des phénomènes rares (comme les gaz et les terres du même nom) dont la découverte a constitué un pas scientifique important.

IV. Symptômes et causes

La science moderne recherche souvent des interprétations cachées, à des phénomènes directement perceptibles. Jean Perrin nous invite à expliquer "**du visible compliqué par de l'invisible simple**" ("Les atomes", 1939).

Cette attitude, parfaitement légitime, nous incite à chercher derrière les fautes commises par nos "étudiants" des explications cachées, auxquelles on donnerait le nom d'**obstacle**. Mais c'est là que le problème commence à se poser : des explications cachées, on en trouve toujours! Mais est-on sûr que ces explications sont les bonnes?

La "théorie" (?) atomique des anciens a inspiré un des plus beaux monuments de la littérature latine (Le "De natura rerum" de Lucrèce). Mais qu'a-t-elle apporté à la science depuis Démocrite (5^e siècle avant J.-C.) jusqu'à Dalton (1766-1844)? On trouvera dans "Les atomes" (déjà cité) les éléments d'une réflexion sur ce qui manque à un système idéologique chimérique pour devenir une théorie scientifique.

Je voudrais poser le problème de la recherche de l'explication cachée, en l'illustrant d'une de mes expériences personnelles, douloureuse.

Tous mes amis connaissent mon orthographe déplorable. Mon père, fin lettré et polyglotte de haut niveau, souffrait d'avoir donné le jour à un fils incapable d'écrire une page sans commettre des dizaines de lapsus.

Il m'infligeait des dictées, enragaient d'y trouver des fautes puériles qu'il me faisait souligner. Il m'ordonnait ensuite de recopier la dictée : je produisais alors un texte

d'où les dix fautes initiales avaient disparues aussitôt relayées par quinze fautes nouvelles ! Ces séances se terminaient dans les cris et les larmes !

Il essaya de me faire donner des leçons. On m'enseigna la grammaire, que je connaissais aussi bien qu'un autre. La règle d'accord des participes n'a jamais eu de secret pour moi ... L'ennui, c'est que j'oubliais de l'appliquer aux moments les plus imprévisibles.

J'en suis arrivé à la conclusion que mon infirmité ne peut s'expliquer en terme de mauvaises connaissances. Elle doit avoir des causes cachées d'une autre nature. Voilà cinquante ans que je cherche désespérément à comprendre. Certes, il doit y avoir **un** *ou plutôt* **des obstacles**, *mais lesquels ?*

Des charlatans essaient de nous faire croire qu'ils sont compétents : leur seul apport a consisté à forger un néologisme : la **dysorthographie** *qui, à mon avis, ne fait que cacher leur ignorance.*

Ils prétendent voir un lien avec des défauts de latéralisation (et en effet, je suis un gaucher contrarié) mais nul n'a apporté, à ma connaissance, la preuve d'une corrélation entre l'infirmité signalée et la latéralisation (cf. Michel Lobrot "Trouble de la langue écrite et ses remèdes", ESF, 1977, pp. 58).

Ce genre de phénomènes se rencontre souvent en mathématiques. J'ai observé beaucoup d'élèves qui connaissaient bien, une à une, les règles du calcul algébrique (aussi bien que moi en ce qui concerne les marques du pluriel).

Ils transgressent les règles qu'ils connaissent bien d'une façon qui paraît aléatoire. Les enseignants, désarmés devant ce phénomène massif, s'en tirent en disant que ces élèves sont **distraits, qu'ils ne font pas attention**.

Cela ne m'explique toujours pas pourquoi je serais distrait lorsqu'il s'agit de ne pas écrire un conditionnel présent comme un futur et que je ne le serais pas pour multiplier deux polynômes.

En tout cas, vous reconnaîtrez que cette énigme pédagogique mérite autant l'attention que d'autres types d'erreurs et qu'il est insensé de décider que comme il ne s'agit pas d'un **obstacle** au sens de Pierre ou de Paul, il doit être éliminé du domaine de la didactique.

Une autre question doit aussi être posée. S'il est légitime de chercher des causes derrière des symptômes, doit-on accepter d'étudier des symptômes, en s'en tenant à la surface des choses? (Autrement dit, toute erreur qui ne s'expliquerait pas par des obstacles cachés sort-elle du champ de la didactique?).

Je pense qu'il convient de distinguer : si un élève se trompe dans une opération et qu'il apparaît qu'il n'a pas bien appris ses tables de multiplications, il n'y a pas de mystères. Et la didactique n'a guère besoin d'intervenir.

Mais, il existe beaucoup d'erreurs apparentes qui s'expliquent parfaitement par des faits apparents compliqués sans qu'il soit nécessaire d'aller chercher de "l'invisible simple".

Exemple : Il a été remarqué, que lorsqu'on doit exécuter une opération qui comporte plusieurs sous-opérations, et que l'on commence par les sous-opérations difficiles, on oublie souvent les sous-opérations faciles, (ou bien l'on commet des erreurs à leur propos).

C'est pourquoi par exemple, on peut recommander à un élève qui calcule la dérivée d'un quotient $\frac{U}{V}$ de commencer par écrire $\frac{(\quad)-(\quad)}{V^2}$ avant d'aborder le calcul du numérateur.

De même, pour factoriser une différence de carré compliquée on écrira : $\{(\quad)+(\quad)\}\times\{(\quad)-(\quad)\}$ avant de remplir les parenthèses intérieures.

Les raisons de cette faute ne sont pas mystérieuses. A la suite de la tension d'esprit que constitue l'exécution d'une tâche délicate, la fatigue provoque une défaillance de l'attention.

Il est tout à fait possible de confirmer expérimentalement cette remarque, et, en ce cas, d'inclure ce résultat dans la formation des enseignants. Et pourtant, il n'y a pas d'obstacles cachés là dedans.

V. L'instable et le persistant

Il est raisonnable de distinguer radicalement les erreurs qui cèdent immédiatement et définitivement à un enseignement approprié de celles qui persistent, en dépit d'efforts pédagogiques réitérés. Les premières sont souvent causées par une **ignorance** qu'il suffit de réparer.

Exemple : L'anecdote, citée par Josette Adda, concernant une fillette à qui on demande d'écrire, en toutes lettres les nombres suivants : 12, 30, 89 et qui répond sur son cahier : **treize, trente et un, quatre vingt dix**.

L'objectif qui était d'apprendre l'orthographe des adjectifs numéraux cardinaux est manifestement atteint.

Peut-être est-ce une méprise sur le sens du mot "suivant" qui déclenche le gag! Ou bien, s'agit-il d'un défaut de segmentation dans la lecture orale : on oublie de faire une pause entre "nombres suivants" et le mot "12". Mais dès que ce point aura été clarifié, la victime du malentendu sera la première à s'amuser de cet incident.

Les secondes, bien plus importantes pour le didacticien, sont des erreurs qui désarment le pédagogue le plus persévérant : le maître aura beau expliquer et réexpliquer. Il trouvera encore des copies où il lira :

$$0\times a=a \qquad x^2=4\Longrightarrow x=2 \qquad \text{ou encore} \quad \sqrt{a+b}=\sqrt{a}+\sqrt{b}$$

C'est aux sources d'erreurs de ce type qu'il semble raisonnable d'attribuer le nom **d'obstacle** (qui offre de la résistance à la compréhension).

Cependant ces cas d'erreurs persistantes sont parfois de natures très différentes. La didactique expérimentale explore en profondeur toutes ces nuances. Elle n'imite pas ces médecines pré-scientifiques qui mettaient dans le même sac toutes les "fièvres", sans savoir en guérir aucune.

C'est d'ailleurs dans la bonne voie que s'était d'abord engagé G. Brousseau lorsqu'il commença à distinguer des obstacles épistémologiques, des obstacles didactiques, ontogénétiques ...(auxquels il aurait pû ajouter d'autres catégories) et qu'il observait méticuleusement divers cas d'échecs électifs en mathématique. Mais le démon des généralisations hâtives l'a entraîné dans une impasse.

VI. Croyances, archétypes et connaissances

Surestimant une remarque isolée parmi tant d'autres dans l'ouvrage de Bachelard "La formation de l'esprit scientifique" (1938), il restreint l'idée d'obstacle épistémologique, à l'influence de connaissances antérieures et caduques, qui s'oppose au progrès de l'apprentissage. En fait, dans la célèbre citation "On connaît **contre** une connaissance antérieure ..." (p. 14). L'idée cruciale s'exprime dans le mot **contre**. Elle ne fait presque pas intervenir les connaissances.

Pour pouvoir examiner si des "connaissances mal faites" sont encore des sources d'erreurs, il faudrait commencer par préciser ce qu'est une connaissance. Si ce mot désigne n'importe quoi on ne pourra rien en tirer de sérieux.

Je me bornerai à exiger, ici, que l'on oppose **connaissance** à **croyance**, et que l'on fasse quelques distinctions parmi les connaissances.

Une **connaissance ne s'acquiert qu'après un effort intellectuel de réflexion.** En passant aux antonymes, l'**ignorance** s'oppose à l'**irréflexion**. On peut ignorer la réponse à une question à laquelle on a longuement réfléchi. Mais il existe une autre forme d'absence de connaissance, dûe à l'absence totale d'intérêt pour le problème posé.

Exemple : L'engouement pour beaucoup de nos contemporains pour l'**astrologie**, véhiculé par l'idéologie ambiante, relève de croyances irréfléchies. Lorsqu'exceptionnellement une personne curieuse consacre beaucoup d'efforts à consulter les ouvrages de "sciences occultes", elle acquiert des connaissances hélas "malfaites".

Dans l'enseignement des mathématiques nous nous heurtons souvent à beaucoup de préjugés, ancrés dans les esprits sous l'influence de ce qu'on entend dire, sans y prendre garde.

L'"évidence" de la platitude de la terre que j'ai maintes fois observée chez les contemporains, ou au contraire la certitude de la rotondité de la terre, sont souvent des croyances.

La compréhension de la théorie des probabilités est souvent gênée par des croyances fantaisistes sur la guigne, la déveine, le mauvais sort et sur une prétendue "loi des séries" chère aux présentateurs de télévision.

Laurence Viennot signale beaucoup de croyances analogues génératrices d'erreurs.

Il convient de distinguer les **connaissances structurées** qui constituent des systèmes, des **connaissances isolées ou mosaïques** qui ne sont que des informations juxtaposées.

Exemple : La mécanique newtonnienne, corps très cohérent de doctrines, a longtemps opposé des obstacles à ceux qui voulaient comprendre la **relativité.**

Mais il y a des informations isolées, qui finissent par s'ancrer dans l'esprit, et à s'opposer ainsi à des informations plus avancées.

Ainsi, après avoir longtemps compris qu'une sphère de $\mathbb{R}^n$ *est un ensemble compact, on généralise abusivement cette conviction à* $\mathbb{C}^n$

A ces préjugés, que transmet la société, on peut ajouter les fameux **archétypes** qui interviennent dans les théories platonisantes de René Thom. On sait que la théorie des réminiscences de Platon décrit l'apprentissage comme une résurgence de connaissances "inconscientes" apparue avant même la naissance.

L'originalité de l'apport de Thom est dans l'explication de ces "connaissances initiales". Les principales morphologies-archétypes correspondent dans le nuage des sensations que l'enfant reçoit aux **singularités stables** qui se rencontrent dans tous les phénomènes qui apparaissent sur des modèles représentés par des variétés différentiables. C'est ainsi que **l'émission, l'absorption, la fuite, la capture** etc ... sont des phénomènes, que le nourisson cotoie, non seulement à sa naissance, mais au cours de la vie intra-utérine, dans toutes les civilisations.

L'optimisme de Platon-Thom ajoute, en outre, que ces archétypes sont nécessairement générateurs de "bonnes connaissances". A mon avis, cette dernière opinion est complètement fausse.

Par exemple, l'attrait des modèles linéaires, $f(a+b) = f(a) + f(b)$ apparaît spontanément chez beaucoup d'individus. Et c'est pour cela qu'il faudra contrarier énergiquement la tendance à admettre que $(a+b)^2$ est égal à a^2+b^2, et que $\sqrt{a+b}$ vaut $\sqrt{a}+\sqrt{b}$. Dans ce cas là, l'esclave du "Ménon" de Platon, devra non pas se souvenir, mais oublier des évidences erronées.

Exemple : *J'ai rencontré un bûcheron illetré qui devait me livrer du bois, en stères, dans une cave étroite. Avec la meilleure bonne foi, il se mit à construire un empilement où le raccourcissement de 20 cm en largeur (1 m - 0,20 m en largeur) devait être compensé par un agrandissement de 20 cm en hauteur (1 m + 20 cm). Il était persuadé qu'il obtenait ainsi un stère.*

Cette croyance à la compensation était un **obstacle** à la compréhension. Mais il ne s'agissait certainement pas de connaissance scolaire antérieure (car notre homme n'était guère allé à l'école).

Bien entendu, il existe **aussi** beaucoup d'incompréhension induite par des connaissances "mal faites". Ainsi, après avoir longuement manipulé le calcul des entiers supérieurs à 1, l'élève acquiert la conviction que l'élévation au carré agrandi un nombre. Et il faudra ultérieurement lutter contre cette conviction. De même les extentions successives de l'idée de nombre vont véhiculer leur cortège d'obstacles. C'est bien une situation que la didactique doit étudier avec soin, lorsqu'elle prétend échafauder une théorie des erreurs : **ce n'est pas la seule.**

VII. Une autre voie

Pour poursuivre ces pistes de recherches, il existe bien d'autres possibilités. Je voudrais maintenant signaler une autre manière fructueuse d'envisager l'explication des "obstacles". C'est une suggestion de François Pluvinage, qui y réfléchis depuis plus de sept ans (puisqu'on trouve cette idée en germe déjà dans sa thèse). S'il ne la développe pas encore, c'est précisément parce que, plus que moi, il répugne aux généralisations hâtives, aux anticipations pré-scientifiques. Cependant, depuis qu'il y songe, les faits semblent confirmer son intuition.

Il s'appuie sur ce qu'il appelle le modèle du **double contrôle**. Ce modèle distingue dans l'activité d'un "étudiant" en situation d'apprentissage une **fonction algorithmique**, assumée par un schèma de traitement, et une **fonction heuristique** dévolue au schéma de contrôle.

L'activité du sujet s'effectue donc à deux niveaux : sur l'un d'eux, il exécute des tâches, et sur l'autre il apprécie la tâche exécutée, à la lumière des finalités et des objectifs.

Sur un grand nombre de situations signalées par François Pluvinage, ces deux niveaux sont apparents, bien qu'il soit très difficile de les définir en toute généralité.

Qu'il me suffise de dire, que dans ces conditions, un obstacle serait un disfonctionnement où l'ancien schéma de contrôle ne serait plus compatible avec un nouveau schéma de traitement.

Il se peut que mon infirmité orthographique ait quelque chose à voir avec ces notions. Pendant l'exécution de "l'algorithmique" qui consiste à traduire mes pensées en écriture, le contrôle de l'orthographe reste en panne.

VIII. Conclusion

Je souhaite que dans les années qui viennent, des échanges fréquents s'établissent entre didacticiens sur leurs constructions théoriques. Mais, dans l'état actuel, une suggestion publiée dans une revue sérieuse risque d'être prise pour argent comptant. Et il serait bon qu'à l'avenir on évite d'écrire que "les travaux de Jacques ou de Jojo ont démontrées que ..." lorsque l'on n'est pas certain qu'une preuve a été apportée, ni même qu'il s'agisse de "travaux" ...

LE CRIBLE D'ÉRATHOSTÈNE

Raymond SEROUL

1. Description de l'algorithme

Pour déterminer tous les nombres premiers compris entre 2 et N, on pratique, dans les petites classes, un algorithme connu sous le nom de *crible d'Érathostène*. Rappelons en quoi consiste cet algorithme. On écrit tous les entiers de l'intervalle $[2\,..\,N]$, puis on barre les multiples stricts de 2 (ici $N = 50$) :

		2	3	.	5	.	7	.	9	.
	11	.	13	.	15	.	17	.	19	.
(T_2)	21	.	23	.	25	.	27	.	29	.
	31	.	33	.	35	.	37	.	39	.
	41	.	43	.	45	.	47	.	49	.

Le premier entier non barré après 2 étant 3, on barre les multiples de 3 :

		2	3	.	5	.	7	.	.	.
	11	.	13	.	.	.	17	.	19	.
(T_3)	.	.	23	.	25	.	.	.	29	.
	31	.	.	.	35	.	37	.	.	.
	41	.	43	.	.	.	47	.	49	.

Le premier entier non barré après 3 étant 5, on barre les multiples de 5 :

		2	3	.	5	.	7	.	.	.
	11	.	13	.	.	.	17	.	19	.
(T_4)	.	.	23	.	.	.	.	.	29	.
	31	.	.	.	.	.	37	.	.	.
	41	.	43	.	.	.	47	.	49	.

Le premier entier non barré après 5 étant 7, on barre les multiples de 7 :

		2	3	.	5	.	7	.	.	.
	11	.	13	.	.	.	17	.	19	.
(T_5)	.	.	23	.	.	.	.	.	29	.
	31	.	.	.	.	.	37	.	.	.
	41	.	43	.	.	.	47	.	.	.

Le processus s'arrête ici car il n'y a plus rien à barrer. Les entiers qui restent sont les nombres premiers recherchés.

2. Le crible d'Érathostène (version classique)

3. Mise en forme de l'algorithme. — Nous obtiendrons très naturellement un programme si nous traduisons les opérations précédentes à l'aide d'une ou plusieurs suites récurrentes. Une première suite est naturellement :

$$T_t = \text{ensemble des entiers non barrés à l'instant } t.$$

Par convention, $T_1 = [2\,..\,N]$. Les ensembles $T_2, \ldots, T_5$ sont ceux du paragraphe précédent.

Mais cette suite ne suffit pas; pour déduire T_{t+1} de T_t, nous avons besoin d'une information supplémentaire : la suite (p_t) des "premiers non barrés" :

$$p_{t+1} = \min\{n \in T_t \mid n > p_t\}, \quad p_1 = 2.$$

On a donc $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$ *etc.*

En désignant par Mult_Stricts(p) l'ensemble des multiples stricts de p (c'est-à-dire l'ensemble des kp avec $k > 1$), nous avons :

$$T_{t+1} = T_t \setminus \text{Mult}(p_t).$$

Une première description algorithmique du crible d'Érathostène pourrait être :

$t := 1$; $T_1 := [2\,..\,N]$; $p_1 := 2$;
while $T_t \cap]p_t, N] \neq \emptyset$ **do begin**
  $T_{t+1} = T_t \setminus \text{Mult\_Stricts}(p_t)$;
  $p_{t+1} = \min\{T_{t+1} \cap]p_t, N]\}$;
  $t := t + 1$
end

Crible d'Érathostène (version incorrecte).

Le test de sortie de boucle $T_t \cap]p_t, N] \neq \emptyset$ est une tentative de traduction de l'énoncé imprécis : "on barre tant que c'est possible".

Présenté ainsi, cet algorithme présente deux défauts :

- Le test de sortie de la boucle est particulièrement déplaisant :

$$T_t \cap]p_t, N] \neq \emptyset.$$

Devrons-nous parcourir l'intervalle $]p_t, N]$ pour y rechercher un élément de T_t ? Ce n'est pas très efficace! D'autre part, il n'est pas possible de remplacer ce test par la condition $p_t < N$, car $N = 28$ et $p_8 = 23$ fournissent un contre-exemple.

• Plus grave encore, cet algorithme se termine immanquablement par un plantage! Lorsque p_t est le plus grand nombre premier $\leq N$, l'algorithme — qui n'est pas au courant — continue en essayant de trouver le plus petit élément de l'ensemble vide $T_{t+1} \cap]p_t, N]\ldots$

Nous allons améliorer considérablement le test de sortie de boucle en nous inspirant d'un résultat bien connu : un entier p est premier s'il n'est divisible par aucun entier de l'intervalle $2 \leq d \leq \sqrt{p}$.

Avant de continuer, rappelons un résultat — dont la démonstration est assez technique[1] — de la théorie des nombres, résultat connu sous le nom de *postulat de Bertand.* Cet énoncé (qui n'a été que conjecturé par BERTRAND en 1845) a été démontré par TCHEBYCHEFF dès 1850 :

THÉORÈME (postulat de Bertrand). — *Soit (p_t) la suite des nombres premiers : $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Alors, pour tout $t \geq 1$, on a*

$$p_{t+1} < 2p_t.$$

Sachant que pour $n \geq 2$ on a $2n \leq n^2$, on obtient tout de suite le :

COROLLAIRE. — *Soit p un nombre premier. On peut toujours trouver un nombre premier q qui satisfait les inégalités :*

$$p < q < p^2.$$

Nous pouvons maintenant améliorer le test d'arrêt :

$t := 1$; $T_1 := [2\,..\,N]$; $p_1 := 2$;
while $p_t^2 \leq N$ **do begin**
  $T_{t+1} = T_t \setminus \text{Mult\_Stricts}(p_t)$;
  $p_{t+1} = \min\{T_{t+1} \cap]p_t, N]\}$;
  $t := t + 1$
end

Crible d'Érathostène (version correcte).

Démonstration. — Pour démontrer que cet algorithme est exact, nous devons nous assurer :

• que l'algorithme ne va pas boucler indéfiniment (i.e. que l'on sort toujours de la boucle while au bout d'un temps fini);

[1] Une démonstration élémentaire figure dans *An Introduction to the Theory of Numers*, Hardy and Wright, pages 343–344.

• que l'algorithme ne plante pas (i.e. que p_{t+1} est bien défini ou, ce qui revient au même, que l'ensemble $T_{t+1} \cap]p_t, N]$ n'est jamais vide);

• que le dernier ensemble T_t obtenu contient tous les nombres premiers $\leq N$ et rien d'autre.

Considérons l'hypothèse de récurrence :

$$(\mathcal{H}_t) \quad \begin{cases} \text{(i) tous les nombres premiers} \leq N \text{ appartiennent à } T_t ; \\ \text{(ii) les } t \text{ premiers nombres premiers sont } p_1, \ldots, p_t ; \\ \text{(iii) } T_t \text{ ne contient aucun multiple strict des nombres} \\ p_1, \ldots, p_{t-1}. \end{cases}$$

Montrons que l'hypothèse $(\mathcal{H}_t)$ est vraie *chaque fois que l'on se présente à l'entrée de la boucle* (les informaticiens appellent $(\mathcal{H})$ un *invariant* de la boucle).

Il est clair que $(\mathcal{H}_1)$ est vérifiée. Supposons alors $(\mathcal{H}_t)$ vraie à l'entrée dans la boucle et supposons $p_t^2 \leq N$, ce qui nous permet d'entrer de nouveau dans celle-ci.

Nous savons que p_t appartient à T_t d'après $(\text{i})_t$ et $(\text{ii})_t$. Soit q le premier nombre premier que l'on rencontre après p_t. Le corollaire du postulat de Bertrand nous apprend que l'on a $p_t < q < p_t^2$. La condition $(\text{i})_t$ montre alors que q appartient à T_t, d'où il résulte que $T_{t+1} \cap]p_t, N]$ n'est jamais l'ensemble vide. Par conséquent, p_{t+1} existe à chaque passage dans la boucle.

Prouvons alors que $(\mathcal{H}_{t+1})$ est vérifiée lorsque l'on sort de la boucle et que l'on se présente de nouveau à l'entrée :

• L'ensemble T_{t+1} est obtenu en ne supprimant dans T_t que les multiples tricts de p_t : les conditions $(\text{i})_{t+1}$ et $(\text{iii})_{t+1}$ sont satisfaites.

• Supposons que $(\text{ii})_{t+1}$ soit fausse, i.e. que p_{t+1} ne soit pas le plus petit nombre premier $> p_t$. Avec les notations précédentes, on aurait $p_t < q < p_{t+1}$, ce qui contredit la définition de p_{t+1}.

Nous savons maintenant que l'algorithme ne plante jamais. Comme la suite des nombres p_t est strictement croissante et qu'elle est majorée par N, cela nous apprend que l'algorithme ne peut pas boucler indéfiniment.

Il reste une dernière formalité : montrer que l'ensemble T_t, au moment de l'arrêt, contient tous les nombres premiers $\leq N$ et rien d'autre. La condition $(\text{i})_t$ montre que tous les nombres premiers $\leq N$ appartiennent à T_t. Supposons que T_t contient un entier n composé. Le plus petit diviseur premier q de n vérifie $n = qn'$ et $q^2 \leq n \leq N$. Les conditions $(\text{ii})_t$ et $(\text{iii})_t$ nous apprennent que $q > p_{t-1}$. De $(\text{ii})_t$, on tire $q \geq p_t$. Comme nous nous plaçons à la sortie de la boucle, nous savons que $p_t^2 > N$, d'où la contradiction $q^2 \geq p_t^2 > N$. □

4. Passage au programme

La description de l'algorithme est une description mathématique, ce qui inclut la gestion de l'indice t (l'instruction $t := t + 1$). Pour obtenir un "vrai" algorithme (c'est-à-dire un programme), il suffit de se débarrasser du temps t. Pour cela, on utilise la correspondance suivante : on interprète x_t comme le *contenu* de la mémoire x à l'instant t. De cette manière, la relation de récurrence $x_{t+1} = f(x_t)$ se trandforme en l'affectation $x := f(x)$ et nous obtenons le programme :

$T := [2\,..\,N]$; $p := 2$;
while $p^2 \leq N$ **do begin**
  $T := T \setminus \text{Mult\_Stricts}(p)$;
  $p := \min\{T \cap]p, N]\}$;
end

Crible d'Érathostène (version classique).

Mais cette description est encore trop mathématique; la représentation des ensembles T_t dans la machine n'est pas précisée. Une solution naturelle consiste à choisir un tableau de booléens que nous appellerons est_barre :

$$\text{est\_barre}[n] = \begin{cases} \textit{true} & \text{si } n \text{ est barré,} \\ \textit{false} & \text{sinon.} \end{cases}$$

Nous choisirons aussi de travailler sur place, c'est-à-dire dans le même tableau. L'ensemble T_t est donc l'*état* du tableau est_barre à l'instant t.

Les déclarations PASCAL sont donc :

```
const max = 50 ;
type tableau = array[2 .. max] of boolean ;
var est_barre : tableau ; p : integer ;
```

Nous supposerons que nous disposons :

- de la procédure barrer_mult_stricts(p, T) qui barre, dans le tableau T, les multiples stricts de p;
- de la fonction premier_non_barre(p, T) qui retourne le plus petit entier $q \in T$ vérifiant la condition $q > p$.

Ceci précisé, le corps principal du programme PASCAL est :

```
begin
  for p := 2 to max do est_barre[p] := false ; p := 2 ;
  while p * p <= max do begin
      barrer_mult_stricts(p, est_barre) ;
      p := premier_non_barre(p, est_barre)
    end
end.
```

Pour barrer les multiples stricts de p, il est préférable d'utiliser des additions répétées ($x := p + p$ et $x := x + p$), car une addition est au moins dix fois plus rapide qu'une multiplication :

```
procedure barrer_mult_stricts(p : integer ; var est_barre : tableau) ;
var x : integer ;
begin
| x := p + p ;
| while x <= max do begin est_barre[x] := true ; x := x + p end ;
end ;
```

Écrire la fonction premier_non_barre ne présente pas de difficulté particulière. Remarquez simplement la déclaration 'var' qui évite une recopie inutile en mémoire du tableau est_barre (cela ne présente aucun danger puisque l'on ne modifie pas le tableau) :

```
function premier_non_barre(var est_barre : tableau) : integer ;
var x : integer ;
begin
| x := p + 1 ;
| while est_barre[x] do x := x + 1 ;
| premier_non_barre := x
end ;
```

Remarque. — On peut améliorer les performances de ce programme :

- Il est maladroit de partir de l'intervalle $[2\,..\,N]$ pour supprimer tous les entiers pairs à l'instruction suivante.
- On peut remplacer les appels

barrer_mult_stricts$(p, \text{est_barre})$ er premier_non_barre$(p, \text{est_barre})$

par les codes correspondants. Cela évite au programme de perdre du temps lorsqu'il se branche sur le code de la procédure ou de la fonction.

- Les multiples stricts de p sont $2p$, $3p$, $4p$, $5p$, $6p\ldots$ Si p est impair, nous savons que les multiples pairs de p ont déjà été barrés. On accélère notablement le processus en ne barrant que les multiples $3p$, $5p$, $7p\ldots$, ce qui s'obtient en répétant l'instruction $q := q + r$, avec $r := p + p$.

Ces transformations fournissent un algorithme rapide, mais plus difficile à comprendre (voir figure).

```
T := [2..N] \ {4,6,8,...} ; p := 3 ;
while p² ≤ N do begin
    r := p + p ; q := p + r ;
    while q ≤ N do begin T := T \ {q} ; q := q + r end ;
    p := p + 2 ; while p ∉ T do p := p + 2
end
```

Crible d'Érathostène (version rapide et illisible).

5. Un algorithme très intelligent

6. Critique de l'algorithme classique. — L'algorithme que nous venons de développer est inefficace car un entier composé est barré autant de fois qu'il possède de diviseurs premiers distincts. Puisque 30 est divisible par 2, 3 et 5, il est barré trois fois. Le travail superflu n'est pas négligeable :

• Pour $N = 100$, l'algorithme barre 113 entiers et trouve 25 nombres premiers : il effectue donc $113 - (99 - 25) = 39$ suppressions inutiles.

• Pour $N = 1\,000$, l'algorithme barre 1 549 entiers et trouve 168 nombres premiers, ce qui fait 718 suppressions inutiles.

• Et la situation s'aggrave lorsque N augmente, car les nombres premiers se raréfient. Ainsi, pour $N = 10\,000$, il y a 9 221 suppressions inutiles et pour $N = 100\,000$, cela passe à 111 747 !

Il est donc très tentant de rechercher un algorithme qui ne barrerait qu'une seule fois chaque entier composé. Mais, lorsqu'on supprime les multiples stricts de 3, comment savoir qu'il est inutile de barrer 6 alors qu'il faut barrer 9 ? La réponse consiste à calculer le *plus petit diviseur* de ces deux nombres : $\mathrm{ppd}(6) = 2$ et $\mathrm{ppd}(9) = 3$ (le ppd est un nombre premier). Cette remarque nous amène à classifier les nombres composés à l'aide de leur ppd :

PROPOSITION. — *Soient $n > 1$ un entier composé et $p = \mathrm{ppd}(n)$ son plus petit diviseur. Alors n s'écrit de manière unique $n = p^\ell m$ si ℓ et m vérifient les conditions:*

$$\text{(C)} \qquad \ell \geq 1, \quad m = p \text{ ou } \mathrm{ppd}(m) > p.$$

Démonstration. — Écrivons $n = p^\ell m$ avec $\ell \geq 1$ et p ne divisant pas m. Deux cas se présentent :

• Si $m = 1$, on a $n = p^\ell$ avec $\ell \geq 2$ puisque n est composé. L'écriture cherchée est alors $n = p^{\ell-1} \times p$.

• Si $m > 1$, l'écriture cherchée est $n = p^\ell \times m$.

L'unicité de cette écriture est évidente. □

NOTATION. — Nous utiliserons l'écriture $((p, m, \ell))$ pour désigner un triplet (p, m, ℓ) qui vérifie la condition (C).

7. Un ordre nouveau. — Soit $N > 2$ un nombre entier et posons :

$$S_N = \textit{ensemble des entiers composés } n \textit{ tels que } 2 \leq n \leq N.$$

Nous identifierons un entier composé $n \in S_N$ avec le triplet $((p, m, \ell))$ qui lui est associé; autrement dit, nous pratiquerons l'abus d'écriture $n = ((p, m, \ell))$.

Notons $\lessdot$ l'ordre lexicographique sur $\mathbb{N}^3$:

$$(a, b, c) \lessdot (u, v, w) \quad \text{si} \quad (a < u) \text{ ou } (a = u \text{ et } b < v) \text{ ou } (a = u \text{ et } b = v \text{ et } c < w).$$

Il s'agit d'un ordre total.

Puisque nous identifions les éléments de S_N avec des triplets, nous pouvons munir S_N de l'ordre lexicographique, ce qui fournit un ordre total que nous notons encore $\lessdot$.

Exemple. — Les éléments de S_{21}, décomposé en triplets, sont :

$4 = ((2, 2, 1))$	$10 = ((2, 5, 1))$	$16 = ((2, 2, 3))$
$6 = ((2, 3, 1))$	$12 = ((2, 3, 2))$	$18 = ((2, 9, 1))$
$8 = ((2, 2, 2))$	$14 = ((2, 7, 1))$	$20 = ((2, 5, 2))$
$9 = ((3, 3, 1))$	$15 = ((3, 5, 1))$	$21 = ((3, 7, 1))$.

L'ordre total $\lessdot$ sur l'ensemble S_{21} est donc :

$$4 \lessdot 8 \lessdot 16 \lessdot 6 \lessdot 12 \lessdot 10 \lessdot 20 \lessdot 14 \lessdot 18 \lessdot 9 \lessdot 15 \lessdot 21.$$

On voit d'abord apparaître les multiples de 2, puis les multiples de 3. En effet, dans l'ordre lexicographique, la première coodonnée est la 'plus importante'; autrement dit, on a l'implication :

$$\text{ppd}(n) < \text{ppd}(n') \implies n \lessdot n'.$$

8. La fonction successeur dans S_N

Le charme de l'ordre lexicographique est qu'il se programme très simplement. Si $E = E_1 \times E_2 \times E_3$ est un ensemble de triplets (u, v, w), on parcourt linéairement E dans l'ordre lexicographique croissant à l'aide de trois boucles emboîtées :

for $u \in E_1$ **do**
  for $v \in E_2$ **do**
    for $w \in E_3$ **do** ...

Pour parcourir l'ensemble S_N, nous utiliserons donc trois boucles emboîtées :

for $p := 2, 3, 5, 7, \ldots$ **do**
  for $m := m_1, m_2, \ldots$ **do**
    for $\ell := 1, 2, 3, 4, \ldots$ **do** ...

Mais une difficulté surgit : S_N n'est pas un produit de trois intervalles; on a seulement une inclusion $S_N \subset E_1 \times E_2 \times E_3$. Comme les variables p, m et ℓ n'appartiennent pas à un intervalle fixe, le calcul des valeurs successives de p, m et ℓ se complique passablement :

THÉORÈME. — *Soient* $n = ((p, m, \ell)) \in S_N$ *un entier composé* $\leq N$ *et* T *l'intervalle* $[2\,..\,N]$ *privé des entiers composés* $\leq n$. *On munit* S_N *de l'ordre lexicographique et* T *de l'ordre ordinaire; ces deux ordres définissent des fonctions successeur que nous noterons* succ(, S_N) *et* succ(, T). *Dans ces conditions, la deuxième composante* m *de* n *appartient à* T *et l'on a :*

(i) *Si* $pn \leq N$, *on a* $\mathrm{succ}(n, S_N) = pn$.

(ii) *Si* $pn > N$, *alors* $m' = \mathrm{succ}(m, T)$ *existe.*

(iii) *Si* $pn > N$ *et si* $pm' \leq N$, *on a* $\mathrm{succ}(n, S_N) = pm'$.

(iv) *Si* $pn > N$ *et si* $pm' > N$, *l'ensemble* T *ne contient aucun multiple de* p *et* m' *est un nombre premier que nous noterons* p'.

(v) *Si* $pn > N$, *si* $pm' > N$ *et si* $p'^2 \leq N$, *on a* $p'^2 = \mathrm{succ}(n, S_N)$.

(vi) *Si* $pn > N$, *si* $pm' > N$ *et si* $p'^2 > N$, *l'entier* n *n'a pas de successeur dans* S_N *et* T *est l'ensemble de tous les nombres premiers* $\leq N$.

Cet énoncé étant très technique, familiarisons-nous d'abord avec celui-ci à l'aide de l'ensemble S_{50}.

La partie (i) de l'énoncé est la plus intuitive; pour obtenir les successeurs des entiers 4, 8, 16, 6, 12, 24, 10, 20, 14, 18, 22, 9 et 15, on multiplie chacun de ces entiers par son ppd.

La partie (iii) s'applique quand le successeur de n a même ppd que n mais lorsque ℓ a une valeur maximum; il faut alors changer de valeur de m. C'est le cas lorsque $n = 32$ puisque $32 = ((2, 2, 4))$ et $2 \times 32 > 50$. Dans cette situation, on a $T = \{2, 3, 5, \ldots\}$. Par conséquent, le successeur de 32 dans S_{50} est $2 \times \mathrm{succ}(2, T) = 2 \times 3 = 6$.

$n = p^\ell m$	p	m	ℓ	$n = p^\ell m$	p	m	ℓ
4, 8, 16, 32	2	2	1, 2, 3, 4	46	2	23	1
6, 12, 24, 48	2	3	1, 2, 3, 4	50	2	25	1
10, 20, 40	2	5	1, 2, 3	9, 27	3	3	1, 2
14, 28	2	7	1, 2	15, 45	3	5	1
18, 36	2	9	1, 2	21	3	7	1
22, 44	2	11	1, 2	33	3	11	1
26	2	13	1	39	3	13	1
30	2	15	1	25	5	5	1
34	2	17	1	35	5	7	1
38	2	19	1	49	7	7	1.
42	2	21	1				

L'ensemble S_{50} ordonné lexicographiquement.

La partie (v) intervient lorsque l'on a épuisé tous les entiers composés ayant un même ppd. Par exemple, le dernier entier pair de S_{50} est $n = 50$; on a $50 = ((2, 25, 1))$, $p = 2$, $m = 25$ et

$$T = \{2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, \ldots\}.$$

Les successeurs dans T de $m = 25$ et de $p = 2$ sont respectivement $m' = 27$ et $p' = 3$. Comme pm' est trop grand, le successeur de 50 est donc $p'^2 = 9$.

9. Un algorithme sophistiqué. — La détermination explicite du successeur dans l'ensemble S_N suggère un algorithme très intelligent, qui barre une fois et une seule chaque entiers composé de l'intervalle $[2\,..\,N]$. Nous reconnaissons les trois boucles emboîtées qui permettent le parcours linéaire de S_N et les tests qui permettent de sortir de chaque boucle.

Le Théorème de la partie 3.3 montre que cet algorithme est correct. (Le lecteur intéressé et consciencieux est invité à écrire les invariants associés aux trois boucles.)

10. Démonstration du Théorème. — Ce résultat n'est pas très difficle à obtenir; il faut seulement prendre soin de ne pas se perdre dans l'arborescence des démonstrations. Commençons par quelques remarques :

Par hypothèse, on a $m = p$ ou $\mathrm{ppd}(m) > p$, d'où $m \geq p$.

L'ensemble T contient tous les nombres premiers $p \leq N$ puisque on ne supprime que des entiers composés dans l'intervalle $[2\,..\,N]$.

Les entiers composés w qui sont supprimés satisfont $w \leq n$, donc aussi $\mathrm{ppd}(w) \leq n$. Montrons que $m \in T$. Si $m = p$ est premier, c'est terminé; si $m > p$, on a $\mathrm{ppd}(m) > p$ ce qui prouve $m > n$.

```
T := [2..N] ; p := 2 ;
while p^2 ≤ N do begin
    q := p ;
    while pq ≤ N do begin
        x := pq ;
        while x ≤ N do begin
            barrer(x, T) ;
            x := px
        end ;
        q := succ(q, T)
    end ;
    p := succ(p, T)
end
```

Crible d'Érathostène (version très intelligente).

Plus généralement, pour tout entier composé $((\pi, \mu, \lambda))$ appartenant à T, on a $p \leq \pi$, $\pi \in T$ et $\mu \in T$. Pour π, c'est évident. Si μ est premier, on a $\mu \in T$; si μ n'est pas premier, $\mathrm{ppd}(\mu) > \pi$ montre que $n \lessdot \mu$.

Passons à la démonstration proprement dite.

(i) Les inégalités $((p, m, \ell)) \lessdot ((p, m, \ell + 1)) = pn \leq N$ montrent que n a un successeur dans S_N. De $((p, m, \ell)) \lessdot ((\pi, \mu, \lambda)) \lessdot ((p, m, \ell + 1))$, on déduit $\pi = p$, puis $\mu = m$ et $\ell < \lambda < \ell + 1$. Donc pn est bien le successeur de n dans S_N.

(ii) Montrons que $T \cap]m, N]$ n'est pas vide. Le postulat de Bertrand affirme que l'on peut trouver un nombre premier q dans l'intervalle $]m, 2m[$. De $q < 2m \leq p^\ell m = n \leq N$, on déduit que $T \cap]m, N]$ contient q.

Terminons cette partie par deux remarques :

L'inégalité $((p, m, \ell)) \lessdot ((p, m, \lambda))$ exige $\ell < \lambda$. Par conséquent, on a $N < pn = p^{\ell+1} m \leq p^\lambda m$.

Le triplet $(p, m', 1)$ vérifie la condition (C), ce qui nous permet de parler du triplet $((p, m', 1))$. Si $\mathrm{ppd}(m') > p$, c'est terminé. Si $\mathrm{ppd}(m') = p$, il faut montrer que $m' = p$. Si ce n'est pas le cas, m' est composé et l'on peut écrire $m' = ((\pi, \mu, \lambda))$ avec $((p, m, \ell)) \lessdot ((\pi, \mu, \lambda))$ puisque $m' \in T$. Cette inégalité, jointe à l'hypothèse $\mathrm{ppd}(m') = \pi = p$, exige $m < \mu$ ou $m = \mu$ et $\ell < \lambda$. Or $\mu \in T$ et $\mu \leq \pi^\lambda \mu = m'$ et $m' = \mathrm{succ}(m, T)$ montrent que seule la condition $m = \mu$ et $\ell < \lambda$ est possible, d'où $m' = ((p, m, \lambda))$. Nous avons alors une contradiction d'après la première remarque de la partie précédente.

(iii) La majoration $n \lessdot ((p, m', 1))$ montre que n a un successeur dans S_N. Supposons que $((p, m', 1))$ ne soit pas ce successeur. La double inégalité

$((p,m,\ell)) \lessdot ((\pi,\mu,\lambda)) \lessdot ((p,m',1))$ exige $\pi = p$ et $m \leq \mu < m'$. Puisque $\mu \in T$, la minimalité de m' exige $m = \mu$ puis $\ell < \lambda$ ce qui est impossible, d'après (ii).

(iv) Si T contient encore un multiple ν de p, on a $\mathrm{ppd}(\nu) = p$ car $\mathrm{ppd}(\nu) < p$ implique ν barré. Par conséquent $\nu = ((p,\mu,\lambda))$ et $((p,m,\ell)) \lessdot ((p,\mu,\lambda))$. Si $m = \mu$ et $\ell < \lambda$, on a $N < pn = p^{\ell+1}m \leq p^{\lambda}\mu = \nu$, ce qui est impossible. Si $m < \mu$, et sachant que $\mu \in T$, la minimalité de m' exige $\mu \geq m'$, d'où l'on tire $p^{\lambda}\mu \geq p\mu \geq pm' > N$: nouvelle contradiction.

De $p \leq m < m'$ et $m' \in T$ on déduit que $p' = \mathrm{succ}(p,T)$ existe. Supposons alors p' composé. Comme T ne contient plus de multiples de p, nous pouvons d'écrire $p' = ((\pi,\mu,\lambda))$ avec $\pi > p$ et $\pi \in T$. Les inégalités $p < \pi < \pi^{\lambda}\mu = p'$ contredisent alors la minimalité de p'.

(v) L'inégalité $n = ((p,m,\ell)) \lessdot ((p',p',1)) = p'^2$ prouve que n possède un successeur dans S_N. Si p'^2 n'est pas ce successeur, on aurait $((p,m,\ell)) \lessdot ((\pi,\mu,\lambda)) \lessdot ((p',p',1))$. Cela exige $p = \pi$ ou $\pi = p'$. Le premier cas ne peut pas se produire, car T ne contient pas de multiples de p. Quant au deuxième cas, il exige $\pi = p' \leq \mu < p'$.

(vi) Supposons que n possède un successeur dans S_N. On aurait $((p,m,\ell)) \lessdot ((\pi,\mu,\lambda))$. Le cas $p = \pi$, $m = \mu$ et $\ell < \lambda$ ne peut pas se présenter car il exige $p^{\lambda}m > N$ d'après une remarque de (ii). Le cas $p = \pi$ et $m < \mu$ exige $m' \leq \mu$ (minimalité de m') ; la minoration $\pi^{\lambda}\mu \geq pm' > N$ montre que ce n'est pas possible. Reste le cas $\pi > p$. La minimalité de p' exige $\pi \geq p'$. De $\mu \geq \pi$, on déduit alors $\pi^{\lambda}\mu \geq p'^2 > N$, ce qui est absurde. □

11. Conclusion

Les performances sont-elles au rendez-vous? Absolument pas! (voir figure) ; le nouvel algorithme est environ *dix fois plus lent* que l'algorithme classique!

N	crible classique	crible très intelligent
5 000	1	13
10 000	2	26
20 000	4	52
30 000	6	79

Temps obtenus avec un Macintosh ; unité de temps = 1/60 de seconde.

La déception est grande... et l'explication facile à trouver : l'algorithme classique n'utilise que des additions, alors que l'algorithme intelligent n'utilise que des

multiplications, ce qui le pénalise très lourdement (un petit test confirme qu'une multiplication est de 10 à 20 fois plus lente qu'une addition selon la taille des entiers).

Moralité : en informatique aussi, le mieux est souvent l'ennemi du bien...

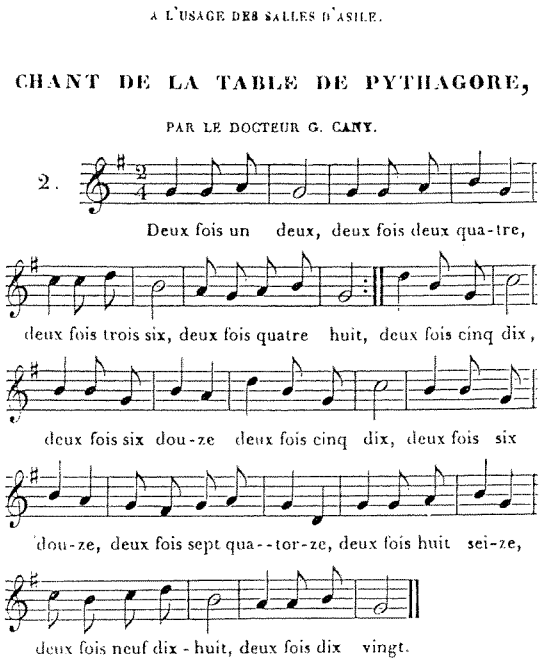
Post-scriptum. — Cette conclusion est volontairement provocatrice. La version très intelligente sert réellement à quelque chose. :

Tout d'abord, elle est très esthétique, ce qui suffit déjà à la justifier.

Mais il y a mieux : en utilisant des structures de données intelligentes qui permettent d'obtenir en un temps constant le premier élément non barré du tableau T, on peut démontrer que l'algorithme classique est un algorithme en $O(n \log n)$ alors que le deuxième algorithme est en $O(n)$. (Les temps expérimentaux sont cohérents avec ces résultats.) Mais ces résultats théoriques ne tiennent pas compte des vitesses respectives de l'addition et de la multiplication. (Bien entendu, il existe aussi des résultats théoriques faisant intervenir les complexités respectives de l'addition et de la multiplication.)

Références

GRIES (D.) and MISRA (J.). — *A Linear Sieve Algorithm for Finding Prime Numbers*, Comm. A.C.M., t. 21, 1978, p. 999–1003.



A L'USAGE DES SALLES D'ASILE.

CHANT DE LA TABLE DE PYTHAGORE,

PAR LE DOCTEUR G. CANY.

2.

Deux fois un deux, deux fois deux qua-tre,

deux fois trois six, deux fois quatre huit, deux fois cinq dix,

deux fois six dou-ze deux fois cinq dix, deux fois six

dou-ze, deux fois sept qua--tor-ze, deux fois huit sei-ze,

deux fois neuf dix - huit, deux fois dix vingt.

A VOS STYLOS

RETOUR SUR LE PROBLÈME 19

Monsieur E. EHRHART propose la conjecture suivante : "Soit $\mathcal{C}$ un ensemble convexe, fermé de l'espace. On peut construire un parallélépipède P inclus dans $\mathcal{C}$ tel que le volume de P soit supérieur ou égal aux 4/9 du volume de $\mathcal{C}$".

Cette conjecture étend à l'espace le problème n° 19 relatif au plan où il s'agissait d'inclure un parallélogramme P d'aire supérieure ou égale à la moitié de l'aire du convexe plan $\mathcal{C}$. On pourrait aussi conjecturer qu'en dimension 3 la meilleure constante est 1/3, obtenue en inscrivant dans un tétraèdre un parallélépipède ayant un sommet et trois faces en commun avec le tétraèdre.

PROBLÈME 21

Énoncé (proposé par D. DUMONT)

Soient $2n$ écolières qui partent en promenade quotidienne en rang deux par deux et souhaitent changer de voisine chaque jour. Trouver un algorithme qui fasse en sorte qu'en $2n-1$ jours chacune ait eu pour voisine chacune des autres une fois et une seule. (Ce problème s'apparente au problème dit "des écolières de Kirkmann".)

Solution

Nous avons reçu deux solutions. La première est de F. Pluvinage :

Puisqu'il s'agit de former des couples, le registre naturel à utiliser est celui des tableaux. On considère un tableau de taille $(2n-1)\times(2n-1)$. Ce tableau, rempli convenablement par les entiers de 1 à $(2n-1)$, désignant les numéros des journées, fournira la matrice des rencontres. Les permutations circulaires de $\{1,2,\ldots,2n-1\}$ conduisent à une matrice symétrique dont chaque ligne et chaque colonne contient tous les entiers de 1 à $(2n-1)$. En termes de rencontres, on y lit par exemple que les individus 2 et 3 seront voisins le jour 4. Les défauts de cette matrice sont au nombre de 2 : l'individu $(2n)$ y est "oublié" et une date est assignée à des "auto-rencontres", comme celle de 2 avec 2 le jour 3. Comme chacun sait, deux défauts ont parfois le bon goût de se compenser : c'est précisément le cas ici, puisqu'il suffit de substituer les rencontres avec l'individu "oublié" aux "auto-rencontres" intempestives. Les nombres de la diagonale principale de la matrice désignent finalement les dates des rencontres avec $(2n)$ et tout le monde est satisfait.

	1	2	3	...	2n - 3	2n - 2	2n - 1
1	*1*	2	3	...	2n - 3	2n - 2	2n - 1
2	2	*3*	4	...	2n - 2	2n - 1	1
3	3	4	*5*	...	2n - 1	1	2
...	...						...
2n - 3	2n - 3	2n - 2	2n - 1	...	*2n - 6*	2n - 5	2n - 4
2n - 2	2n - 2	2n - 1	1	...	2n - 5	*2n - 4*	2n - 3
2n - 1	2n - 1	1	2	...	2n - 4	2n - 3	*2n - 2*

Matrice des dates de rencontres (en italiques : dates des rencontres avec $2n$)

La seconde solution nous a été envoyée indépendamment par C. Pagano et X. Yadol :

Une écolière A se place au centre d'un cercle sur lequel les $2n-1$ autres écolières occupent les sommets d'un polygone régulier. On établit un couplage de la manière suivante : l'écolière A se joint à une écolière quelconque X et les écolières situées aux extrémités d'une corde perpendiculaire au rayon AX se joignent. Le lendemain, on fait pivoter toutes les arêtes de $360°/(2n-1)$. En $2n-1$ jours, tous les couplages possibles ont été effectués.

Un instant de réflexion montre que ces deux algorithmes sont en fait identiques, la personne placée par Pluvinage au centre du cercle étant l'écolière numéro $2n$.

C. Pagano nous signale que cet algorithme est décrit – dans un autre langage – par Oystein Ore dans "les graphes et leurs applications", pages 51 à 54 (Dunod, collection sigma).

Il remarque aussi que, si l'on désigne par B, C, D, etc. les écolières qui donnent la main à l'écolière A les 1er, 2e, 3e jour, etc., il n'y a qu'un calendrier possible pour quatre écolières et exactement six calendriers différents pour six écolières.

PROBLÈME 22

Énoncé

Existe-t-il une fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$ indéfiniment dérivable, telle que, pour tout x rationnel, la dérivée $n^{\text{ième}}$ $f^{(n)}(x)$ soit un rationnel pour n pair et un irrationnel pour n impair ?

Indication

La réponse est oui.

PROBLÈME 23

Énoncé (proposé par J.-M. Nagel)

Dans un jeu de 52 cartes battu, quelle est la probabilité pour qu'une dame et un roi soient voisins immédiats?

PROBLÈME 24

Énoncé

Un faisceau de droites parallèles fournit un exemple de partition du plan en droites.

a) Existe-t-il une partition du plan en cercles (non dégénérés, c'est-à-dire de rayon ni nul ni infini)?

b) Existe-t-il une partition du plan en figures formées chacune de deux cercles (distincts et non dégénérés) tangents intérieurement ou extérieurement?