e.f.

Mathématique et Pédagogie

Sommaire

N° 119 Novembre – Décembre 1998

Éditorial

J. Navez,

Plusieurs membres du conseil d'administration de notre société ont reçu une lettre d'un membre qui exprime ses réserves quant au contenu de *Mathématique et Pédagogie* et au programme scientifique du Congrès de Floreffe. Ce lecteur nous livre aussi quelques considérations personnelles sur l'enseignement des mathématiques.

Les deux Vice-Présidents, Guy Noël et Claude Villers, ainsi que le directeur de la revue, Jacques Bair, ont répondu par lettre aux critiques soulevées par ce membre.

J'aimerais dégager cependant quelques points constructifs. Il est évident que le contenu de la revue ne peut pas plaire à tout le monde. Le directeur de la revue ne peut par ailleurs faire paraître que ce que les "rédacteurs" lui proposent. Si un sujet ou une expérience pédagogique vous touche particulièrement, envoyez-nous un article ou demandez à vos collègues de le faire. Nous sommes également tout à fait disposés à ouvrir les colonnes de la revue à un "Courrier du Lecteur" dans lequel les membres pourraient signaler des faits qui méritent des commentaires.

En ce qui concerne le Congrès, le problème est le même, nous sommes évidemment tributaires des propositions qui nous sont faites. Là aussi, nous sommes ouverts pour créer un espace éventuel où des professeurs pourraient parler de leur expérience en classe, des difficultés qu'ils ont eues et des solutions qu'ils proposent.

Enfin, le souci exprimé par ce membre d'enseigner une "mathématique du citoyen" est un sujet qui rejoint nos préoccupations actuelles et sur lequel nous reviendrons certainement dans le futur.

Jacques NAVEZ

Si π m'était conté...

J. Mawhin, *UCL* [1]

1. Introduction

Il était une fois... C'est ainsi que commencent les contes. Celui qui nous occupe devrait plutôt commencer par "Il était un rapport", puisque l'histoire du nombre qui sera appelé π au XVIIIe siècle seulement, commence par l'étude du rapport qui existe entre la longueur L de la courbe la plus simple qui soit, le cercle, et son diamètre D.

1. Conférence faite à Namur le 9 mai 1998, à la remise des prix des Olympiades mathématiques

Faire-part de naissance

3, sa partie entière,
4, son supérieur immédiat,
22/7, sa bonne approximation,
355/113, sa meilleure approximation,
10, son carré (ou presque),
e, son complice réel,
i, son complice imaginaire,

ont l'incommensurable joie de vous annoncer l'arrivée de

π

né du rapport entre une (quelconque) circonférence et son diamètre.

Le petit irrationnel sera baptisé par sa Transcendance le Pape Pie 3,14,
en la basilique Saint Circulaire le Rond.

2. Civilisation préhellénistiques

L'étude de ce rapport préoccupait déjà les Babyloniens il y a environ 4000 ans, et une tablette cunéiforme de l'époque propose, sans explication et, bien entendu, sans notation algébrique, la formule

$$L = \left(3 + \frac{1}{8}\right) D,$$

c'est-à-dire

$$\frac{L}{D} = 3,125.$$

C'est le premier calcul de π avec **une décimale exacte.**

Un peu plus tard, aux environs de l'an 1800 avant notre ère, le célèbre papyrus Rhind fournit, pour l'aire du disque de diamètre D, la règle

$$A = \left(D - \frac{D}{9}\right)^2,$$

c'est-à-dire

$$\frac{A}{D^2} = \left(1 - \frac{1}{9}\right)^2 = 0,790\ldots = \frac{3,160\ldots}{4}.$$

On ne sait pas comment les Egyptiens sont arrivés à cette formule. Une explication plausible est la suivante : si l'on inscrit le disque dans un carré de côté D, que l'on divise en 9 carrés égaux par trisection des côtés, et que l'on considère l'octogone (irrégulier) obtenu en laissant tomber la moitié des petits carrés situés aux quatre coins, on obtient une figure peu différente du disque, d'aire égale à

$$5\left(\frac{D}{3}\right)^2 + 4\,\frac{1}{2}\left(\frac{D}{3}\right)^2 = \frac{7}{9}\,D^2.$$

D'autre part, $\frac{7}{9} = \frac{63}{9^2}$, et le carré le plus proche de 63 est 8^2. En conséquence, l'aire de l'octogone, et donc du disque, est approximativement égale à $\left(\frac{8}{9}\right)^2 D^2 = \left(D - \frac{D}{9}\right)^2$.

L'Ancien Testament (Premier Livre des Rois 2.4) donne une formule plus simple mais moins exacte puisque qu'on y trouve, au sujet de la construction d'un bassin, l'information suivante :

> "Il fit la Mer en métal fondu, de dix coudées de bord à bord, à pourtour circulaire (...) ; un fil de trente coudées en mesurait le tour",

ce qui équivaut à la formule

$$L = 3D.$$

Ces civilisations sont donc bien conscientes du fait que, pour un cercle de diamètre D, les rapports A/D^2 et L/D sont constants.

3. Archimède

Il faut attendre la civilisation grecque pour que ces recettes plus ou moins empiriques se transforment en assertions démontrées. Les *Eléments* d'Euclide, qui datent du 3e siècle avant J.C., nous apprennent déjà, comme simple conséquence des propriétés des triangles semblables, que

> *Les périmètres de deux polygones réguliers d'un même nombre de côtés, inscrits ou circonscrits à deux cercles, sont entre eux comme le rapport des diamètres de ces cercles, tandis que les*

aires correspondantes sont entre elles comme le carré de ce rapport.

En outre, pour tout polygone régulier circonscrit à un cercle de diamètre D, on a $\frac{L}{D} = 4\frac{A}{D^2}$, et l'un des deux rapports détermine l'autre. Pour obtenir, par exemple, le rapport entre la longueur du cercle et son diamètre, les savants grecs ont alors l'idée de coincer le cercle entre des polygones réguliers inscrits et circonscrits (ils savent en mesurer le périmètre), dont le nombre de côtés est de plus en plus grand. ARCHIMÈDE, au 2e siècle avant J.C., est le premier à faire de cette idée une méthode effective d'approximation du rapport souhaité. Pour mesurer la valeur de sa découverte, n'oublions pas qu'Archimède ne disposait ni de nos chiffres, ni de notre algèbre, ni de notre trigonométrie.

Si l'on part d'un triangle isocèle inscrit au cercle de diamètre D, et si l'on désigne par θ_n l'angle sous-tendu par le polygone régulier de $3 \cdot 2^n$ côtés obtenu en doublant successivement n fois le nombre de côtés, par l_n son périmètre et par L_n celui du polygone circonscrit correspondant, un calcul trigonométrique élémentaire montre que

$$l_n = 3 \cdot 2^n D \sin\frac{\theta_n}{2}, \quad L_n = 3 \cdot 2^n D \tan\frac{\theta_n}{2}.$$

En prenant $n = 5$ (soit un polygone à 96 côtés), Archimède arrive à l'estimation

$$\frac{223}{71} = 3\,\frac{10}{71} < \frac{L}{D} < 3\,\frac{1}{7} = \frac{22}{7},$$

c'est-à-dire, en notations décimales,

$$3,14084\ldots < \frac{L}{D} < 3,142857\ldots.$$

C'est le **premier calcul de π avec estimation de l'erreur.** Il donne **deux décimales exactes.** Notons encore que, puisque $\theta_{n+1} = \frac{\theta_n}{2}$, un peu de trigonométrie montre que

$$L_{n+1} = \frac{2L_n l_n}{L_n + l_n}, \quad l_{n+1} = \sqrt{L_{n+1} l_n}, \tag{1}$$

ce qui permet le calcul itératif de L_n et l_n pour chaque n à partir des valeurs de départ (pour le triangle)

$$l_0 = \frac{3\sqrt{3}D}{2}, \quad L_0 = 3\sqrt{3}D.$$

4. Les successeurs d'Archimède

Les Romains, comme on le sait, préfèrent la guerre et les techniques aux sciences et, puisque rien ne se passe à cette époque dans le développement de π, contentons-nous d'une petite respiration que, pour les courageux, j'accompagnerai toujours d'un projet.

π-romanes romains

Rétablir l'égalité (ou presque) en déplaçant une seule allumette :

$$II = \frac{XXII}{VIII}$$

Projet : Arrêter de fumer.

On sait le rôle joué par les Arabes dans le développement et la transmission du savoir grec, et l'un d'eux, Al Kashi, en 1429, est le premier à donner plus de **dix décimales exactes** de π. Il en obtient 16, que voici :

$$\frac{L}{D} = 3,1415926535898732\ldots.$$

Pour ce faire, il utilise la méthode d'Archimède avec $n = 28$ (c'est-à-dire des $3 \cdot 2^{28}$-gones !). Ces décimales commencent à être difficiles à retenir, et l'on n'aura de cesse d'inventer, dans toutes les langues, des moyens mnémotechniques, comme ceux donnés dans la respiration suivante.

Co-π-ons

29 décimales exactes de π en comptant les lettres de chaque mot du poème :

Que j'aime à faire apprendre un nombre utile aux sages.
Glorieux Archimède, artiste, ingénieur,
Toi de qui Syracuse aime encore la gloire,
Soit ton nom conservé par de savants grimoires.

Existe aussi en *anglais* (31 décimales), pour les physiciens :

How I want a drink, alcoholic of course,
after the tough lectures involving quantum mechanics,
but we did estimate some digits by making very bad,
not accurate, but so greatly efficient tools.

Version *néerlandaise* plus romantique mais nettement moins précise (11 décimales) :

Eva o lief, o zoete hartedief, uw blauwe oogen zyn wreed bedrogen.

Projet : Ecrire un poème en wallon liégeois donnant 42.001 décimales de π.

Signalons pour les chauvins, s'il en reste, que le record du calcul des décimales de π fut détenu pendant quelques années par un savant belge, Adrianus ROMANUS (Adrien ROMAIN pour les francophones et Adriaan VAN ROOMEN pour les néerlandophones), professeur à l'Université de Louvain. En 1593, il obtint 17 décimales à partir d'un polygone de 2^{30} côtés. Il sera battu par l'Allemand Ludolph VAN CEULEN, avec 32 décimales, qu'il fera graver sur sa tombe, dans l'église Saint-Pierre à Leyden (les Allemands appellent encore π le *nombre de Ludolph*). Un tel souhait serait difficilement réalisable pour l'actuel recordman !

5. Des formules aussi belles qu'inutiles

Les temps modernes voient le développement des notations et du calcul algébrique, et il n'est pas étonnant que le Français François Viète, le fondateur de l'algèbre, traduise, en 1593, la méthode d'Archimède en une formule "algébrique" pour π :

$$\pi = \frac{2}{\sqrt{\frac{1}{2}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}}\cdots}.$$

L'Anglais John Wallis donne, en 1655, la formule

$$\pi = 2\frac{2\cdot 2}{1\cdot 3}\cdot\frac{4\cdot 4}{3\cdot 5}\cdot\frac{6\cdot 6}{5\cdot 7}\cdots,$$

immédiatement suivie en 1657 par celle de son compatriote Lord Brouncker

$$\pi = 4\frac{1}{1+\cfrac{1}{2+\cfrac{3^2}{2+\cfrac{5^2}{2+\cfrac{7^2}{2+\cdots}}}}}.$$

Ces formules n'accélèrent pas le calcul des décimales de π, par rapport à la méthode d'Archimède, et tous ces auteurs ignorent qu'ils ont été précédés, dans cet art, par des mathématiciens indiens du XIV^e ou XV^e siècle (Madhava (1340 ?-1425 ?), Nilakantha) qui ont obtenu la formule

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots. \tag{2}$$

Retrouvée indépendamment par James Gregory en 1671 et Gottfried W. Leibniz en 1673, cette jolie expression s'obtient comme suit. Par une identité algébrique bien connue, on a, pour $y \neq 1$,

$$\frac{1-y^{n+1}}{1-y} = 1 + y + y^2 + \ldots + y^n,$$

et dès lors

$$\frac{1}{1-y} = 1 + y + y^2 + \ldots + y^n + \frac{y^{n+1}}{1-y}.$$

En y remplaçant y par $-x^2$, cela donne

$$\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + \ldots + (-1)^n x^{2n} + \frac{(-1)^{n+1}x^{2n+2}}{1+x^2}.$$

Comme la dérivée de arctg x vaut $\frac{1}{1+x^2}$, on en déduit

$$\begin{aligned}\text{arctg } u \;&=\; \int_0^u \frac{dx}{1+x^2} = u - \frac{u^3}{3} + \frac{u^5}{5} - \frac{u^7}{7} \\ &\quad + \ldots + \frac{(-1)^n u^{2n+1}}{2n+1} + \int_0^u \frac{(-1)^{n+1} x^{2n+2}}{1+x^2}\, dx.\end{aligned}$$

Maintenant, si $0 < u \leqslant 1$,

$$\left| \int_0^u \frac{(-1)^{n+1} x^{2n+2}}{1+x^2}\, dx \right| \leqslant \int_0^u x^{2n+2}\, dx = \frac{u^{2n+3}}{2n+3} \leqslant \frac{1}{2n+3},$$

et dès lors

$$\left| \text{arctg } u - \left(u - \frac{u^3}{3} + \frac{u^5}{5} - \frac{u^7}{7} + \ldots + \frac{(-1)^n u^{2n+1}}{2n+1} \right) \right| \leqslant \frac{1}{2n+3}.$$

Ainsi, l'expression entre parenthèses peut être rendue aussi proche que l'on veut de arctg u en prenant n suffisamment grand, c'est-à-dire suffisamment de termes. Cela s'écrit, dans le langage des séries,

$$\text{arctg } u = u - \frac{u^3}{3} + \frac{u^5}{5} - \frac{u^7}{7} + \ldots + \frac{(-1)^n u^{2n+1}}{2n+1} + \ldots = \sum_{n=0}^{\infty} (-1)^n \frac{u^{2n+1}}{2n+1}. \quad (3)$$

En particulier, pour $u = 1$, on retrouve (2).

Malheureusement, cette belle formule (2) converge très lentement et n'apporte pas de progrès dans le calcul numérique de π. Une astuce aussi simple qu'ingénieuse va pourtant faire de (3) une redoutable calculatrice de décimales de π.

6. La formule de Machin et autres trucs

En 1706, l'astronome anglais John Machin découvre la formule

$$\frac{\pi}{4} = 4 \,\text{arctg } \frac{1}{5} - \text{arctg } \frac{1}{239}. \quad (4)$$

Il suffit d'un peu de trigonométrie pour la démontrer. Posons $\theta = \text{Arctg } \frac{1}{5}$, de telle sorte que $\operatorname{tg} \theta = \frac{1}{5}$. Dès lors

$$\operatorname{tg} 2\theta = \frac{2 \operatorname{tg} \theta}{1 - \operatorname{tg}^2 \theta} = \frac{5}{12},$$

$$\operatorname{tg} 4\theta = \frac{2\operatorname{tg} 2\theta}{1-\operatorname{tg}^2 2\theta} = \frac{120}{119} = 1 + \frac{1}{119},$$

$$\operatorname{tg}\left(\frac{\pi}{4} - 4\theta\right) = \frac{\operatorname{tg}\frac{\pi}{4} - \operatorname{tg} 4\theta}{1 + \operatorname{tg}\frac{\pi}{4}\operatorname{tg} 4\theta} = \frac{1-\operatorname{tg} 4\theta}{1+\operatorname{tg} 4\theta} = -\frac{1}{239}.$$

En conséquence,

$$\frac{\pi}{4} = 4\theta - \operatorname{Arctg}\frac{1}{239} = 4\ \operatorname{Arctg}\frac{1}{5} - \operatorname{Arctg}\frac{1}{239}.$$

En calculant chaque terme du second membre de (4) à partir de la formule (3) (la convergence est beaucoup plus rapide puisque 1 est remplacé par $\frac{1}{5}$ et par $\frac{1}{239}$), Machin a été le premier à calculer plus de **cent décimales** de π.

1706 est une année faste pour π puisque c'est aussi celle de son baptême. En effet, dans son ouvrage *Synopsis Palmariorum Matheseos* ou *A new introduction to the mathematics,* William Jones écrit :

> *In the circle, the diameter is to the circumference as 1 to* $3,141159\&c = \ \pi$.

Leonard Euler en répand l'usage dans son *Introductio in analysis infinitorum* (1748), après avoir utilisé, dans d'autres travaux, la lettre p, et même, suivant Jean Bernoulli, la lettre c. Si ce dernier usage avait triomphé, on peut se demander comment se présenterait la célèbre formule d'Einstein liant la masse et l'énergie.

La même approche, où l'on remplace éventuellement la formule de Machin par une autre formule du même genre donnée dans le tableau ci-dessous,

QUELQUES FORMULES EN ARCTANGENTE		
année	**auteur**	**formule pour $\pi/4$**
1706	Machin	$4\ \mathrm{Arctg}\,\frac{1}{5} - \mathrm{Arctg}\,\frac{1}{239}$
1730	Klingenstierna	$8\ \mathrm{Arctg}\,\frac{1}{10} - \mathrm{Arctg}\,\frac{1}{239} - 4\ \mathrm{Arctg}\,\frac{1}{515}$
1755	Euler	$5\ \mathrm{Arctg}\,\frac{1}{7} + 2\ \mathrm{Arctg}\,\frac{3}{79}$
1764	Euler	$4\ \mathrm{Arctg}\,\frac{1}{5} - \mathrm{Arctg}\,\frac{1}{70} + \mathrm{Arctg}\,\frac{1}{99}$
1776	Hutton	$\mathrm{Arctg}\,\frac{1}{2} + \mathrm{Arctg}\,\frac{1}{3}$
1776	Hutton	$2\ \mathrm{Arctg}\,\frac{1}{3} + \mathrm{Arctg}\,\frac{1}{7}$
1844	Strassnitzky	$\mathrm{Arctg}\,\frac{1}{2} + \mathrm{Arctg}\,\frac{1}{5} + \mathrm{Arctg}\,\frac{1}{8}$
1863	Gauss	$12\,\mathrm{Arctg}\,\frac{1}{18} + 8\,\mathrm{Arctg}\,\frac{1}{57} - 5\,\mathrm{Arctg}\,\frac{1}{239}$
1893	Loney	$3\ \mathrm{Arctg}\,\frac{1}{4} + \mathrm{Arctg}\,\frac{1}{20} + \mathrm{Arctg}\,\frac{1}{1985}$
1896	Störmer	$6\ \mathrm{Arctg}\,\frac{1}{8} + 2\ \mathrm{Arctg}\,\frac{1}{57} + \mathrm{Arctg}\,\frac{1}{239}$

est restée la meilleure méthode de calcul des décimales de π jusqu'en 1973 !

Même avec une excellente méthode, on peut se tromper, comme le montre la respiration suivante.

π-toyable

Au *Palais de la Découverte,* construit à Paris en 1937, une galerie circulaire affiche, en lettres de bois, les 707 décimales de π calculées par SHANKS en 1874.
En 1945, FERGUSON découvre que les 180 dernières décimales de SHANKS sont *fausses.*
Funeste erreur qui force le Palais de la Découverte à une (coûteuse) correction.

Projet : Faire un voyage d'étude à Paris : *Palais de la Découverte* l'après-midi (cercle) et *Crazy Horse Saloon* le soir (sphères).

1947 est l'année du **premier calcul de π utilisant une calculatrice mécanique,** toujours à partir de la méthode de Machin. L'Américain D. FERGUSON obtient ainsi 710 décimales. C'est par la même technique que les Américains SMITH et WRENCH sont les premiers, en 1949, à calculer plus de **mille décimales** de π.

1949 voit une autre première d'importance, à savoir le **premier calcul de π utilisant un ordinateur.** Le célèbre mathématicien américain John VON NEUMANN propose d'utiliser l'ENIAC *(Electronic Numerical Integrator and Computer)*, pour calculer, toujours par la méthode de l'arc tangente, autant de décimales de π que l'on peut, afin d'étudier le caractère aléatoire de leur distribution. Le calcul de 2037 décimales de π est complété, à partir de la formule de Machin, durant le week-end du Labor Day (pour ne pas retarder les calculs de bombes nucléaires !), grâce aux efforts combinés de Clyde V. HAUFF (qui vérifie les programmes), Miss Homé S. MCALLISTER, W. Barkley FRITZ et George W. REITWIESNER, qui se relaient par tours de huit heures durant ce week-end bien nommé.

Le développement des ordinateurs permet alors une accélération foudroyante du calcul des décimales sans que l'on modifie le principe de la méthode : les **dix mille décimales** sont dépassées en 1958 par GENUYS et son IBM 704 et les **cent mille décimales** sont dépassées en 1961 par SHANKS et WRENCH sur leur IBM 7090, mais ces Américains doivent laisser la palme aux Français GUILLOUD et BOUYER pour atteindre, en 1973, le **million de décimales** sur leur CDC 7600.

7. La revanche d'Archimède

La méthode de Machin s'est peu à peu essoufflée et s'est vue supplantée, dans les années 80, par des approches parentes de la méthode d'Archimède, mais à convergence beaucoup plus rapide, résumées dans le tableau suivant.

QUELQUES METHODES AGM			
année	**auteur**	**formule**	**convergence**
1976	SALAMIN, BRENT	$\pi = \lim_{n\to\infty} p_n,$ $a_0 = 1,\ b_0 = \frac{1}{\sqrt{2}},\ s_0 = \frac{1}{2},$ $a_{n+1} = \frac{a_n+b_n}{2},\ b_{n+1} = \sqrt{a_n b_n},\ c_n = a_n^2 - b_n^2$ $s_{n+1} = s_n - 2^{n+1}c_n,\ p_n = \frac{2a_n^2}{s_n}.$	quadratique
1981	J. et P. BORWEIN	$\pi = \lim_{n\to\infty} p_n,$ $a_0 = \frac{1}{3},\ s_0 = \frac{\sqrt{3}-1}{2},$ $r_{n+1} = \frac{3}{1+2(1-s_n^3)^{1/3}},\ s_{n+1} = \frac{r_{n+1}-1}{2},$ $a_{n+1} = r_{n+1}^2 a_n - 3^n(r_{n+1}^2 - 1),\ p_n = \frac{1}{a_n}.$	cubique
1985	J. et P. BORWEIN	$\pi = \lim_{n\to\infty} a_n$ $a_0 = 6 - 4\sqrt{2},\ y_0 = \sqrt{2} - 1$ $y_{n+1} = \frac{1-(1-y_n^4)^{1/4}}{1+(1-y_n^4)^{1/4}}$ $a_{n+1} = a_n(1 + y_{n+1})^4$ $-2^{2n+3}y_{n+1}(1 + y_{n+1} + y_{n+1}^2)$	quartique

C'est évidemment la vitesse de convergence supérieure de ces méthodes qui permet le progrès. La convergence est *d'ordre* m (linéaire si $m = 1$, quadratique si $m = 2$, ...) si l'on a, entre les approximations successives p_n, une estimation du type

$$|p_{n+1} - p_n| \leqslant L|p_n - p_{n-1}|^m$$

pour tout n et une certaine constante L. Ainsi, pour la convergence quadratique, le nombre de décimales, grosso modo, double en passant de p_n à p_{n+1}.

Le nom de ces méthodes (AGM) vient de leur relation ou de leur analogie avec la célèbre *moyenne arithmético-géométrique* de deux nombres a et b que le mathématicien allemand GAUSS a définie au XIX^e siècle par les relations

$$a_0 = a, \quad b_0 = b, \quad a_{n+1} = \frac{a_n + b_n}{2}, \quad b_{n+1} = \sqrt{a_n b_n}.$$

Les méthodes AGM ont permis aux Japonais KANADA, TAMURA et YOSHINO de dépasser les **dix millions de décimales** de π en 1982 sur leur HITAC M-280H, les **cent millions** étant dépassés en 1987 par KANADA, TAMURA et KOBO sur une NEC SX2.

Le dépassement du **milliard de décimales** échappe à cette équipe et aux méthodes AGM puisqu'il est l'oeuvre, en 1989, des frères ukrainiens CHUDNOVSKY, à partir d'une autre formule obtenue en 1910 par le mathématicien indien RAMANUJAN (un étrange génie autodidacte découvert par l'anglais HARDY au début du siècle)

$$\pi = \frac{9801}{\sqrt{8}} \left(\sum_{n=0}^{\infty} \frac{(4n)!(1103 + 26390\,n)}{(n!)^4\, 396^{4n}} \right)^{-1}.$$

Une variante de cette formule est due aux frères Chudnowsky (1994)

$$\pi = \left(12 \sum_{n=0}^{\infty} \frac{(-1)^n (6n)!(13591409 + 545140134\,n)}{(3n!)(n!)^3\, 640320^{3n+3/2}} \right)^{-1}.$$

L'année passée, les **dix milliards de décimales** ont été dépassés par KANADA, sur un HITAC S820/80, en utilisant une méthode de type AGM. Ce record (environ 50 milliards de décimales) tient toujours, de même qu'un autre, à couper le souffle, mais qu'une respiration nous fait quand même découvrir.

Jeux olym-π-ques

Depuis 1995, Hiroyuki GOTO détient le record mondial de *mémorisation* de décimales de π : 42.000.
Le précédent record (15.151) appartenait à Hideaki TOMOYORI.

Projet : Faire mieux pour qu'ils rient jaune (de dé-π).

8. π en binaire

On peut évidemment écrire π en une base autre que 10. Ainsi, les 29 premières "décimales" de l'expression binaire de π sont

$$11,00100100001111110110101010001\ldots.$$

Cette occupation peut paraître bien futile, mais, tout récemment, l'attention a été attirée sur ce développement, grâce à une formule découverte le 19 septembre 1995, à 0 h. 29 par le Canadien Simon Plouffe

$$\pi = \sum_{n=0}^{\infty} \frac{1}{16^n} \left(\frac{4}{8n+1} - \frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} \right). \tag{5}$$

La précision de l'instant de la découverte vient de ce que la formule a été trouvée de manière empirique à l'aide de l'ordinateur. La démonstration élémentaire que nous donnons ici est postérieure.

Posons

$$I = \int_0^{\frac{1}{\sqrt{2}}} \left(\frac{4\sqrt{2} - 8x^3 - 4\sqrt{2}x^4 - 8x^5}{1 - x^8} \right) dx,$$

$$J_k = \int_0^{\frac{1}{\sqrt{2}}} \frac{x^{k-1}}{1 - x^8}\, dx, \quad k = 1, 2, \ldots.$$

Comme, pour tout entier $n \geqslant 1$ et tout $x \neq 1$, on a

$$\frac{1 - x^{8(n+1)}}{1 - x^8} = 1 + x^8 + x^{16} + \ldots + x^{8n},$$

et donc

$$\frac{1}{1 - x^8} = 1 + x^8 + x^{16} + \ldots + x^{8n} + \frac{x^{8(n+1)}}{1 - x^8},$$

on a

$$\frac{x^{k-1}}{1 - x^8} = \sum_{j=0}^{n} x^{8j+k-1} + \frac{x^{8(n+1)+k-1}}{1 - x^8},$$

et dès lors

$$J_k = \frac{1}{\sqrt{2}^k} \sum_{j=0}^{n} \frac{1}{16^j (8j + k)} + \int_0^{\frac{1}{\sqrt{2}}} \frac{x^{8(n+1)+k-1}}{1 - x^8}\, dx.$$

Mais, pour $0 \leqslant x \leqslant \frac{1}{\sqrt{2}}$, on a

$$x^{8(n+1)+k-1} \leqslant \frac{x^{8(n+1)+k-1}}{1 - x^8} \leqslant \frac{16}{15} x^{8(n+1)+k-1},$$

et dès lors,

$$\begin{aligned} \frac{1}{\sqrt{2}^k} \frac{1}{2^{4(n+1)}[8(n+1)+k]} &\leqslant \int_0^{\frac{1}{\sqrt{2}}} \frac{x^{8(n+1)+k-1}}{1 - x^8}\, dx \\ &\leqslant \frac{16}{15} \frac{1}{\sqrt{2}^k} \frac{1}{2^{4(n+1)}[8(n+1)+k]}. \end{aligned}$$

Donc,

$$J_k = \frac{1}{\sqrt{2}^k} \sum_{j=0}^{\infty} \frac{1}{16^j(8j+k)},$$

et,

$$\begin{aligned} I &= 4\sqrt{2}J_1 - 8J_4 - 4\sqrt{2}J_5 - 8J_6 \\ &= \sum_{j=0}^{\infty} \frac{1}{16^j} \left(\frac{4}{8j+1} - \frac{2}{8j+4} - \frac{1}{8j+5} - \frac{1}{8j+6} \right). \end{aligned}$$

Calculons maintenant l'intégrale I. En posant $y = \sqrt{2}x$, on trouve

$$I = \int_0^1 \frac{16(y^5 + y^4 + 2y^3 - 4)}{y^8 - 16}\, dy.$$

Les zéros de $y^8 - 16$ sont

$$\sqrt{2}, -\sqrt{2}, 1+i, 1-i, i\sqrt{2}, -i\sqrt{2}, -1+i, -1-i,$$

et dès lors

$$y^8 - 16 = (y^2-2)[(y-1)^2+1](y^2+2)[(y+1)^2+1].$$

D'ailleurs, $y^5 + y^4 + 2y^3 - 4$ admet évidemment la racine 1, et

$$y^5 + y^4 + 2y^3 - 4 = (y-1)(y^4 + 2y^3 + 4y^2 + 4y + 4),$$

tandis que

$$y^4 + 2y^3 + 4y^2 + 4y + 4 = (y^2+2)[(y+1)^2+1].$$

En conséquence,

$$\frac{16(y^5 + y^4 + 2y^3 - 4)}{y^8 - 16} = \frac{16(y-1)}{(y^2-2)(y^2-2y+2)} = \frac{4y}{y^2-2} - \frac{4(y-2)}{y^2-2y+2}.$$

On en déduit facilement que

$$\begin{aligned} I &= 2\int_0^1 \frac{d(y^2-2)}{y^2-2} - 2\int_0^1 \frac{d(y^2-2y+2)}{y^2-2y+2} + 4\int_0^1 \frac{dy}{(y-1)^2+1} \\ &= 4\int_0^1 \frac{du}{u^2+1} = \pi. \end{aligned}$$

L'intérêt de (5) est d'avoir permis pour la première fois, en 1996, le calcul d'une "décimale" de rang donné dans le développement en base 2 de π, sans devoir calculer toutes celles qui précèdent. PLOUFFE et les frères BORWEIN ont ainsi calculé la 40 milliardième "décimale" du développement de π en base 2, et Fabrice BELLARD a obtenu la 400 milliardième !

Malheureusement, il n'existe toujours pas de méthode semblable efficace en base 10.

9. π ailleurs

Le nombre π n'apparaît pas seulement en géométrie et en analyse. Il hante également le *calcul des probabilités* et la *statistique.* Par exemple, l'aire située sous la fameuse *courbe en cloche* de Gauss, d'équation $y = e^{-x^2}$, est égale à $\sqrt{\pi}$.

Le calcul des probabilités fournit même des moyens expérimentaux – peu efficaces à vrai dire – pour calculer π. Par exemple, si on lance au hasard une *aiguille* de longueur $2b$ sur un *parquet* formé de lames de largeur $2a$ ($b \leqslant a$), le naturaliste français BUFFON a calculé en 1777 que la *probabilité* pour que l'aiguille coupe l'une des raies du parquet est égale à

$$\frac{2b}{\pi a}.$$

Par ailleurs, si l'on jette en l'air une *pièce de monnaie* $2n$ fois, et si $P(n)$ désigne la probabilité d'obtenir *autant de piles que de faces,* alors

$$\lim_{n\to\infty} \sqrt{\pi n} P(n) = 1.$$

Ce résultat est une conséquence d'une autre intéressante expression de π obtenue par Euler en 1736 :

$$\frac{\pi^2}{6} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \dots.$$

π apparaît aussi dans de nombreuses formules de physique. Sa présence dans la formule donnant la période d'oscillation d'un pendule a été récemment chantée avec lyrisme par Umberto ECO dans les premières lignes du roman *Le pendule de Foucault,* rappelées dans la respiration qui suit.

π-sticisme

C'est alors que je vis le pendule.
La sphère, mobile à l'extrémité d'un long fil fixé à la voûte du choeur,
décrivait ses amples oscillations avec une isochrone majesté.
Je savais – mais quiconque aurait dû s'en rendre compte
sous le charme de cette paisible respiration – que la période
était réglée par la relation entre la racine carrée de la longueur du fil
et ce nombre π qui, irrationnel aux esprits sublunaires, par divine raison
lie nécessairement la circonférence au diamètre de tous les cercles possibles
– si bien que le temps de l'errance de cette sphère d'un pôle à l'autre
était l'effet d'une mystérieuse conspiration
entre les plus intemporelles des mesures, l'unité du point de suspension,
la dualité d'une dimension abstraite, la nature ternaire de π,
le tétragone secret de la racine, la perfection du cercle.

Projet : Analyser les allusions à π dans la série télévisée *Dallas*
(exemple : son univers im-π-toyable).

D'ailleurs π n'inspire pas seulement les écrivains mais aussi, on s'en étonnera moins, les nombreux adeptes de la *numérologie.*

π-zarre, j'ai dit π-zarre ? Comme c'est π-zarre

Soit $\Phi = \frac{1+\sqrt{5}}{2}$ *(nombre d'or).* Alors,
$\frac{4}{\sqrt{\Phi}} = 3,14460551\ldots, \quad \frac{6}{5}\Phi^2 = 3,14164078...$

Soit $e = 2,71828182\ldots$. Alors
$(2\,e^3 + e^8)^{1/7} = 3,141716\ldots, \quad (\pi^4 + \pi^5)^{1/6} = 2,718281809\ldots$

L'astronome Piazzi-Smith attribue à la pyramide de Chéops (à base carrée)
les dimensions originelles $H = 148,208\ m.,\ B = 232,805\ m.$
Cela donne $\frac{2B}{H} = 3,1415982.$

A-π-calypse now

La somme des 144 ($= 12^2$) premières décimales de π égale 666.

Projet : Retrouver π dans la Tour de l'Yser.

10. Faut-il interdire la chasse aux décimales ?

La chasse aux décimales de π ne répond pas à un souhait des utilisateurs, puisque 39 décimales de π suffisent pour calculer, avec une précision de l'ordre du rayon de l'*atome d'hydrogène,* la longueur de la circonférence d'un cercle entourant l'*univers* connu.

Elle ne répond pas non plus au souhait des hommes politiques ou des législateurs, qui furent même tentés de fixer la valeur de π par une loi, ainsi que le montre la respiration suivante.

π-litiquement correct

En 1897, l'état de l'Indiana (USA) faillit voter une
loi fixant des formules de calcul de surface et de longueur
qui revenaient à décider *simultanément* que
$\pi = 4,\ \pi = 3,1604,\ \pi = 3,2$ et $\pi = 3,232$.
Elle ne fut refusée que sous le prétexte qu'une loi
ne peut intervenir dans le domaine scientifique.

Projet : Fédéraliser π en Belgique.

Le calcul des décimales de π fut d'abord motivé par la recherche d'une éventuelle périodicité suggérant que π est rationnel (quotient de deux entiers). Mais, en 1761, le mathématicien alsacien Johann Heinrich Lambert a donné la première démonstration de l'**irrationalité** de π. π ne peut donc être racine d'une équation du premier degré $ax = b$ à coefficients entiers.

En voici une preuve très simple, due à Ivan Niven (1947). Supposons que $\pi = \frac{a}{b}$, où a et b sont des entiers positifs. Soit

$$p(x) = \frac{x^n(a - bx)^n}{n!}, \quad P(x) = p(x) - p''(x) + p^{(4)}(x) - \ldots + (-1)^n p^{(2n)}(x).$$

Comme $n!p(x)$ a ses coefficients entiers et que ses termes en x commencent au degré n, $p(x)$ et ses dérivées ont des valeurs entières en $x = 0$ (nulles jusqu'à l'ordre $n - 1$). D'ailleurs, $p(x) = p\left(\frac{a}{b} - x\right)$ et on a donc la même conclusion en $x = \frac{a}{b} - \pi$. D'autre part,

$$\frac{d}{dx}\left[P'(x)\sin x - P(x)\cos x\right] = P''(x)\sin x + P(x)\sin x = p(x)\sin x.$$

D'où

$$\int_0^\pi p(x)\sin x\,dx = P(\pi) + P(0),$$

et le deuxième membre est entier puisque les $p^{(j)}(\pi)$ et les $p^{(j)}(0)$ le sont. Or, pour $0 < x < \pi$, on a

$$0 < p(x)\sin x < \frac{\pi^n a^n}{n!},$$

et donc

$$0 < \int_0^\pi p(x)\sin x\,dx < \frac{\pi^{n+1} a^n}{n!},$$

d'où

$$0 < P(\pi) + P(0) < \frac{a}{b}\frac{\left(\frac{a^2}{b}\right)^n}{n!}$$

quel que soit n, ce qui est contradictoire puisque le second membre tend vers zéro lorsque $n \to \infty$.

Ceux que cette démonstration rebute lui préféreront peut-être les arguments buccoliques contenus dans la respiration suivante.

Bourba-π-sme

Posons VACHE = $\beta\pi$, OISEAU = βL
CHE VA L = VA CHE L (commutativité)
CHEVAL/OISEAU = $\beta\pi L/\beta L = \pi$
CHEVAL et OISEAU n'ayant aucun rapport entre eux, π est irrationnel.

Projet : Donner une version *végétarienne* de cette preuve.

Peu de temps après le travail de Lambert (1794), le mathématicien français Adrien-Marie Legendre prouva que π^2 est également **irrationnel.** Il ne peut donc être racine d'une équation du second degré à coefficients entiers. Il faudra attendre près de cent ans pour que le mathématicien allemand Ferdinand von Lindemann prouve en 1882 que π ne peut être racine d'une équation algébrique d'un degré quelconque à coefficients entiers. On dit qu'il est **transcendant,** par opposition aux nombres **algébriques** qui sont racines d'une telle équation. Bien sûr, tout nombre transcendant est irrationnel, mais la réciproque est fausse. Le résultat de Lindemann ruina

définitivement les espoirs des "quadrateurs de cercles" qui tentaient, depuis l'antiquité grecque, la construction, à la règle et au compas, d'un carré ayant la même aire qu'un cercle donné.

Mais il reste bien des questions sans réponse liées à la transcendance et à l'irrationalité pour les plus célèbres constantes des mathématiques. Quelques années avant Lindemann, le mathématicien français HERMITE avait démontré la transcendance de e, base des logarithmes népériens. Même si A. GELFOND et TH. SCHNEIDER ont prouvé indépendamment, en 1935, que e^π est transcendant, on ne sait pas, à ce jour, si $e+\pi$, $e-\pi$, $e\cdot\pi$, π/e et π^e sont irrationnels !

Le calcul de milliards de décimales de π a peu de chances d'aider à résoudre ces questions, mais constitue un excellent test de qualité pour la construction d'un ordinateur ou l'élaboration d'un logiciel. Car, même si une seule erreur survient dans le calcul, il est quasi certain que le résultat final en sera affecté. En 1986, un programme pour calculer π a permis de détecter des problèmes bien cachés dans le hardware des super-ordinateurs Cray 2.

Les mathématiciens, qui savent que π est transcendant, voudraient savoir s'il est **normal,** une notion introduite en 1909 par le mathématicien français Emile BOREL pour formaliser la notion de nombre réel pris au hasard. Un nombre est *normal en base b* si, dans sa représentation dans cette base, tous les chiffres pris un à un, tous les couples de deux chiffres, tous les triplets de trois chiffres, etc. apparaissent avec la même fréquence. Un nombre est *normal* s'il est normal en chaque base. Donc, si π est normal en base 10, on doit constater que, dans son développement décimal, chacun des dix chiffres $0, 1, 2, \ldots, 9$ est présent dans la proportion de $\frac{1}{10}$, chacun des cent couples $00, 01, \ldots, 99$ est présent dans la proportion $\frac{1}{100}$, et ainsi de suite. L'examen des décimales connues de π en base 10 semble montrer qu'il est proche de la normalité, mais ce n'est pas démontré. KANADA et TAKAHASHI ont découvert que la première apparition de la suite finie 0123456789 dans les décimales de π n'arrive qu'à la 17.387.594.880 décimale.

S'il était normal, π serait un *nombre univers,* c'est-à-dire que la suite de ses décimales contiendrait toutes les suites finies possibles. S'il est facile de construire un exemple de nombre-univers en base 10 (le *nombre de* CHAMPERNOWNE $0,123456789101112\ldots$ en est un), il est autrement plus difficile de décider si un nombre donné est ou non un nombre univers.

11. E-π-logue

J'espère vous avoir convaincu, à travers cette esquisse de l'épopée du nombre π, de la vitalité et de l'unité des mathématiques, et de ses incessants progrès. Comme dans les autres sciences, toute question résolue en soulève d'autres et il en sera toujours ainsi. J'espère aussi vous avoir convaincu, mais vous le saviez déjà, que faire des mathématiques n'est jamais triste et toujours passionnant.

Si le malheur voulait que π soit un jour définitivement enterré (six π-eds sous terre diront les aigre-fins), avec, peut-être, comme é-π-taphe :

Ci-gît π, *roulé en boule,*

on peut être sûr que toute la mathématique, et probablement toute la civilisation, l'auront accompagné.

π*-es irae,* π*-es illa.*

12. π-bliographie sommaire

— P. Beckmann, *A history of* π*,* St. Martin Press, New York, 1971
— L. Berggren, J. Borwein and P. Borwein, *Pi : A source book,* Springer, New York, 1997
— J. and P. Borwein, *Pi and the AGM,* Wiley Interscience, New York, 1987
— J.P. Delahaye, *Le fascinant nombre* π*,* Pour la Science, Belin, Paris, 1997
— E. Hobson, *Squaring the circle : a History of the Problem,* Cambridge, 1913. Chelsea, New York, 1953
— F. Klein, *Leçons sur certaines questions de géométrie élémentaire,* Vuibert, Paris, 1931
— J. Montucla, *Histoire des recherches sur la quadrature du cercle,* Paris, 1754
— H. Petit, *A propos du nombre* π, Mémoire de licence en mathématique, UCL, Louvain-la-Neuve, 1981
— *Numéro Special* π, Supplément au Petit Archimède No. 64-65, Mai 1980

APPROXIMATIONS ALGEBRIQUES DE π			
année	**auteur**	**approximation**	**erreur**
-2000	Ahmès	$\left(\frac{4}{3}\right)^4$	$< 2 \cdot 10^{-2}$
-250	Archimède	$\frac{22}{7}$	$< 2 \cdot 10^{-3}$
125	Chang Hing	$\sqrt{10}$	$< 3 \cdot 10^{-2}$
460	Tsu Chung Chih	$\frac{355}{113}$	$< 3 \cdot 10^{-7}$
		$\frac{333}{106}$	$< 9 \cdot 10^{-5}$
		$\sqrt{2}+\sqrt{3}$	$< 5 \cdot 10^{-3}$
1440	Nicolas de Cues	$\frac{3}{4}(\sqrt{3}+\sqrt{6})$	$< 6 \cdot 10^{-3}$
1685	Kochansky	$\sqrt{4+\left(3-\frac{1}{\sqrt{3}}\right)^2}$	$< 6 \cdot 10^{-5}$
1750	Euler	$\frac{103993}{33102}$	$< 10^{-9}$
1828	Specht	$\frac{13}{50}\sqrt{146}$	$< 7 \cdot 10^{-7}$
1879	Chase	$\sqrt{9+\left(1-\frac{27}{4000}\right)^2}$	$< 8 \cdot 10^{-6}$
1913	Hobson	$\frac{9}{5}+\sqrt{\frac{9}{5}}$	$< 5 \cdot 10^{-5}$

QUELQUES FORMULES POUR π		
année	**auteur**	**formule**
1593	Viète	$\pi = \dfrac{2}{\sqrt{\frac{1}{2}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}}\cdots}$
1655	Wallis	$\pi = 2\frac{2\cdot 2}{1\cdot 3}\cdot\frac{4\cdot 4}{3\cdot 5}\cdot\frac{6\cdot 6}{5\cdot 7}\cdots$
1657	Brouncker	$\pi = 4\cfrac{1}{1+\cfrac{1}{2+\cfrac{9}{2+\cfrac{25}{2+\cfrac{49}{2+\cdots}}}}}$
1671	Gregory	$\pi = 4\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots\right)$
1666	Newton	$\pi = \frac{3\sqrt{3}}{4}+24\left(\frac{1}{12}-\frac{1}{5\cdot 2^5}-\frac{1}{28\cdot 2^7}-\frac{1}{72\cdot 2^9}-\cdots\right)$
1700	Sharp	$\pi = \frac{6}{\sqrt{3}}\left(1-\frac{1}{3\cdot 3}+\frac{1}{3^2\cdot 5}-\frac{1}{3^3\cdot 7}+\cdots\right)$
1730	Stirling	$\sqrt{2\pi} = \lim_{n\to\infty}\frac{n!\exp n}{n^{n-\frac{1}{2}}}$
1736	Euler	$\frac{\pi^2}{6} = 1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\frac{1}{25}+\cdots$
1910 1987	Ramanujan J. et P. Borwein	$\pi = \frac{9801}{\sqrt{8}}\left(\sum_{n=0}^{\infty}\frac{(4n)!(1103+26390\,n)}{(n!)^4\,396^{4n}}\right)^{-1}$
1994	G. et D. Chudnowsky	$\pi = \left(12\sum_{n=0}^{\infty}\frac{(-1)^n(6n)!(13591409+545140134\,n)}{(3n!)(n!)^3\,640320^{3n+3/2}}\right)^{-1}$
1995	Plouffe	$\pi = \sum_{n=0}^{\infty}\frac{1}{16^n}\left(\frac{4}{8n+1}-\frac{2}{8n+4}-\frac{1}{8n+5}-\frac{1}{8n+6}\right)$

RECORDS DE DECIMALES DE π				
déc.	**année**	**auteur**	**calcul**	**méthode**
1	-2000	*Tablette de Suse*	main	hexagone
1	-2000	*Papyrus Rhind*	main	octogone
10	1429	Al Kashi	main	3.2^{28}-gone
10^2	1706	Machin	main	Machin-Gregory
10^3	1949	Smith-Wrench	calculatrice	Machin-Gregory
10^4	1958	Genuys	IBM 704	Machin-Gregory
10^5	1961	Shanks-Wrench	IBM 7090	Störmer-Gregory
10^6	1973	Guilloud-Bouyer	CDC 7600	Gauss-Gregory
10^7	1982	Kanada-Tamura-Yoshino	HITAC M-280H	AGM
10^8	1987	Kanada-Tamura-Kobo et al.	NEC SX2	AGM
10^9	1989	Chudnovsky-Chudnovsky		Ramanujan
10^{10}	1997	Kanada	HITAC S820/80	AGM

Sur l'équation du second degré chez Simon Stevin et sur son utilisation des méthodes géométriques

H. Capoen, G. Delcroix, S. Glotz, B. Palmieri, S. Soquette,
Université de Mons-Hainaut

Mots-clé : équation du second degré ; méthode géométrique ; Simon Stevin.

Résumé :

Nous montrons que dans l'oeuvre de Simon Stevin sur l'équation du second degré, en même temps que celui-ci donne aux nombres négatifs un statut analogue à celui des nombres positifs [3], il justifie qu'une équation admette plusieurs solutions.

Nous commentons son utilisation des méthodes géométriques du livre II d'Euclide.

1.1. Introduction

Dans son article [3], Monsieur M. Lartillier indique que dans son étude des équations du second degré, Simon Stevin remarque que soustraire un nombre positif a revient à ajouter le nombre négatif $(-a)$. Cette remarque lui permet de diminuer le nombre de cas d'équations à résoudre. Nous notons ici que dans le même contexte, Stevin argumente l'acceptation du fait qu'une équation du second degré puisse admettre deux racines. Nous commentons l'usage auquel souscrit Stevin de justifier les procédés de résolutions d'équations par les méthodes géométriques du Livre II d'Euclide.

1.2. Dans ce texte, nous utilisons une terminologie et des notations contemporaines : nous parlerons donc de "*résoudre l'équation*" là où dans son ouvrage "*L'arithmétique de Simon Stevin de Bruges*", paru en 1585, [4], Stevin dit "*trouver le quatriefme terme proportionnel*" ; nous écrirons "$x^2 = ax - b$" là où Stevin écrit "*troisiefme difference de second terme* ①−⓪". Pour cette même équation, nous écrirons des formules en a et b là où Stevin indique une méthode, que l'on comprend générale, sur un cas particulier.

2. Un endroit où Stevin justifie l'existence de deux solutions est la résolution de l'équation $x^2 = ax - b$, où a et b sont (des nombres rationnels) positifs ([4] Iib, pp 603-611). Selon son habitude, Stevin présente la théorie comme ceci :

1. *Explication du donné* : il énonce l'équation à résoudre, ici $x^2 = 6x - 5$;
2. *Explication du requis* : il dit qu'il faut résoudre l'équation ;
3. *Construction* : il décrit sur cet exemple numérique son procédé de résolution ;
4. *Démonstration arithmétique* : il justifie son procédé par des arguments arithmétiques ;
5. *Autre démonstration géométrique* : le procédé est justifié par des méthodes géométriques du Livre II d'Euclide.
6. Il donne des commentaires dans des Nota ;
7. De l'origine de la construction du précédent problème.

2.1. Détaillons cela : dans la *construction*, Stevin donne tout d'abord la solution :

$$\frac{a}{2} + \sqrt{\left(\frac{a}{2}\right)^2 - b}$$

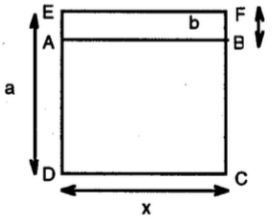
puis, il ajoute : "*ou autrement*" :

$$\frac{a}{2} - \sqrt{\left(\frac{a}{2}\right)^2 - b}$$

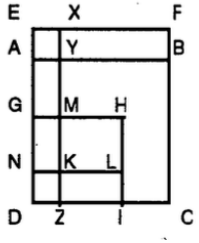
et conclut par l'affirmation : $\frac{a}{2} + \sqrt{\left(\frac{a}{2}\right)^2 - b}$ et $\frac{a}{2} - \sqrt{\left(\frac{a}{2}\right)^2 - b}$ est la solution (pour l'équation $x^2 = 6x - 5$, la conclusion de Stevin est "*Je di que et* 5 *et* 1 *est la quatriefme terme proportionnel requis*").

Remarque : Dans cet exemple, il pratique l'astuce citée par Monsieur Lartillier ([3], p 57) où soustraire 5 revient à ajouter -5.

Dans la *Démonstration arithmétique*, il vérifie que ces nombres sont des solutions. *L'autre Démonstration géométrique* se base sur la méthode des gnomons ([3], pp 47 et 48). Il cherche un rectangle de base x et de hauteur a tel qu'après lui avoir ôté le carré construit sur x, le rectangle qui reste ait pour aire b :



Il considère les segments GD et DN comme ci-dessous, de longueurs respectives $\frac{a}{2}$ et $\sqrt{\left(\frac{a}{2}\right)^2 - b}$, puis la figure complétée



où $ABCD$ et $GHID$ sont des carrés. Il constate que le gnomon $GMKLIDG$ égale le rectangle $EFBA$. Il en déduit que le rectangle $EFCD$ égale la somme du carré $ABCD$ et du rectangle $EFBA$. On a donc d'une part $x = AD = GD + AG = \frac{a}{2} + \sqrt{\left(\frac{a}{2}\right)^2 - b}$ et d'autre part $ax = x^2 + b$.

Puis, il ajoute qu'il y a une autre solution : $DN = y$ est une solution. En effet, le rectangle $EFBA$ égale le rectangle $EXKN$, donc la somme du carré $DZKN$ et de ce dernier rectangle est le rectangle $EXZD$, et donc $y^2 + b = ay$.

Remarque : Dans cette construction, il considère des grandeurs *géométriques* négatives : pour soustraire un morceau du plan b, il ajoute $-b$.

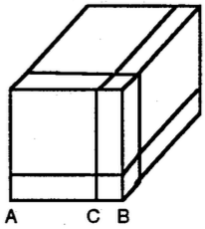
Dans la Nota 2, Stevin montre qu'il n'y a rien de surprenant à ce qu'un problème possède deux solutions. L'exemple qu'il choisit est le système d'équations $6 = x + y,\ 8 = xy$. On peut prendre $x = 2$ et $y = 4$, ou bien $x = 4$ et $y = 2$.

3. Appendice

En l'absence d'un calcul algébrique solidement fondé, la justification systématique par les méthodes géométriques se comprend. Mais il nous semble que parfois l'utilisation de ces méthodes, ou simplement du langage géométrique, s'apparente à une sort de rite. C'est frappant dans le cas de l'équation du troisième degré dont Stevin commence l'étude par le théorème ([4], p 612) qu'il attribue à Tartaglia et qu'il a repris de l'*Ars Magna* de Cardan :

Théorème : Si on coupe une ligne droite en un lieu quelconque, le cube de toute la ligne sera égal aux deux cubes des parties et trois fois le solide rectangle, contenu sous les deux parties et toute la ligne.

On reconnaît l'énoncé $(a+b)^3 = a^3 + b^3 + 3ab(a+b)$. La preuve se base sur une décomposition du cube :



Puis, il vérifie numériquement l'énoncé sur le cas où $AB = 10$, $AC = 8$ et $BC = 2$. Puis, il énonce cinq corollaires. Les deux premiers sont des énoncés portant sur des décompositions d'une face du cube (donnés sans preuve et dont nous nous demandons pourquoi ils sont présentés comme conséquence du Théorème de Tartaglia). Voici ([4], IIb, p 614) le *Corollaire IIII* : *Il est évident que le nombre du cube de la ligne AB est égal au nombre du cube de AC et de* 6 *quarrez de AC et de* 12 *lignes et du cube de CB.*

Traduction : $(a+b)^3 = a^3 + 6a^2 + 12a + b^3$.

Recopions la preuve de Stevin :

“ Car le nombre du cube AB (posant pour AB 10 et pour CB 2, comme dessus) est	1000
Qui sera égal au nombre du cube de AC	512
et de 6 quarrez de AC	384
et de 12 lignes AC	96
et du cube de CB	8
Desquels la somme est aussi	1000”

Il a donc vérifié l'énoncé sur le cas particuler énoncé dans le corollaire III (que nous n'avons pas repris parce qu'il aurait alourdi inutilement ce texte en ajoutant beaucoup de données). Dans cet énoncé, Stevin dit “veu que nous posons AC 8”.

Donc une interprétation de la présence de ce corollaire IIII qui permette de ne pas écrire que Stevin pouvait écrire n'importe quoi, est qu'ayant besoin de l'égalité numérique

$$8^3 + 6.8^2 + 12.8 + 2^3 = 10^3,$$

il trouve nécessaire de l'écrire sous la forme d'un énoncé géométrique dont il omet de préciser qu'il n'est pas général (nous avons retrouvé des endroits du texte de Stevin où l'énoncé numérique correspondant au corollaire III est utilisé, en se référant au corollaire III, mais pas de référence au corollaire IIII).

Nous n'avons trouvé aucune remarque sur ces deux corollaires dans les études sur l'oeuvre de Stevin mentionnées dans la bibliographie (probablement parce qu'il ne semble pas que Stevin puisse être crédité d'apports majeurs à la théorie de l'équation du troisième degré et donc que l'on ne voit pas l'intérêt de commentaires détaillés de cette partie de son traité).

4. Ce texte provient d'un travail rédigé durant l'année académique 1996-1997 dans le cadre du cours “Etudes d'objets de la mathématique élémentaire” de la licence en sciences mathématiques à l'UMH, lorsque les auteurs y étaient étudiant(e)s. Le point 2 est dû au premier et au troisième auteur, le point 3 aux deuxième, quatrième et cinquième auteurs.

Bibliographie

[1] **Bosmans H.**, Notes sur L'Arithmétique de Simon Stevin, *Ann. Soc. Sci. Bruxelles*, 1910-1911, 35, 293-313.

[2] **Depauw R.**, *Simon Stevin*, Bruxelles, Collection Nationale, office de Publicité, 1942, 127 pages.

[3] **Lartillier M.**, Les tribulations de l'équation du second degré, *Mathématique et Pédagogie*, 1997, 115, 43-58.

[4] *The Principal works of Simon Stevin*, Mathematics, II (deux tomes), ed. By D.J. Struik, Amsterdam, C.V. Swets Zeitlinger, 1958, 976 p.

Adresse de l'auteur :

Université de Mons-Hainaut
Institut de Mathématique et d'Informatique
Le Pentagone
Avenue du Champ de Mars
7000 MONS

Quelques cryptosystèmes usuels

P. Paquay et M. Rigo, *Université de Liège*

Mots-clé : cryptosystème, clé publique, one-time pad, RSA.

1. Introduction

La *cryptographie*, science qui étudie les différentes manières de communiquer secrètement, n'est pas une science nouvelle. Ainsi, Jules César y avait déjà recours pour coder certains de ses messages. Cependant, il y a peu de temps encore, les techniques de codage n'intéressaient principalement que les militaires ou les entreprises soucieuses de se prémunir contre l'espionnage industriel.

Depuis quelques années, l'avènement d'Internet nous fournit un nouveau champ d'applications à la cryptographie. Imaginez que vous désiriez envoyer des données critiques sur Internet, par exemple, votre numéro de carte VISA. Il paraît naturel de coder votre message, c'est-à-dire rendre celui-ci secret, et que seul votre destinataire soit en mesure de le décoder.

On peut distinguer deux catégories de codage : les *codages à clé secrète* et les *codages à clé publique*. Pour le codage à clé secrète, l'expéditeur et le destinataire choisissent tous deux une même clé qui servira au codage et au décodage des messages. Dans cet article, nous décrirons le *cryptosystème linéaire* et le *cryptosystème "one-time pad"* qui entrent tous deux dans cette catégorie. Les systèmes de codage à clé publique se présentent comme suit. Le destinataire du message possède une paire de clés (c, d). La clé c est connue de tous et sert à coder les messages que l'on veut envoyer au destinataire. La clé d, quant à elle, n'est connue que du destinataire et sert au décodage des messages codés avec c. La connaissance de c n'implique pas, dans ce cas, la connaissance de d. Le codage à clé publique présente un avantage certain : expéditeur et destinataire ne doivent pas avoir d'accord préalable sur une clé de codage commune. Dans cet article, nous décrirons en détail le *système RSA*.

Traditionnellement, nous appelerons l'expéditeur du message Alice (A), le destinataire Bob (B) et l'espion éventuel tentant d'intercepter le message, Oscar (O).

2. Quelques rappels

Il nous paraît utile, et ce afin d'uniformiser notre propos, de rappeler quelques définitions de base d'algèbre générale.

Définition 2.1 On définit l'anneau $(\mathbb{Z}_n, +, 0, \cdot, 1)$ des *entiers modulo* n, où $n \in \mathbb{N}\backslash\{0,1\}$, comme l'ensemble des restes possibles de la division euclidienne par n, c'est-à-dire

$$\{0, \cdots, n-1\},$$

muni de l'addition et la multiplication modulo n. A titre d'exemple, considérons les tables d'addition et de multiplication dans $\mathbb{Z}_4$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$.$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Définition 2.2 Soit $(A, +, 0, \cdot, 1)$ un anneau ; on définit *l'ensemble des invertibles* $U(A)$ *de* $(A, +, 0, \cdot, 1)$ par l'ensemble des $x \in A$ pour lesquels il existe $y \in A$ tel que

$$x \cdot y = y \cdot x = 1;$$

en général, on remplace y par x^{-1} qu'on appelle l'*inverse* de x. Ainsi 1 est toujours invertible et 0 ne l'est que si $0 = 1$.

Bien sûr, si $x, y \in U(A)$, alors $x^{-1} \in U(A)$, puisque $(x^{-1})^{-1} = x$; et de plus, $x \cdot y \in U(A)$ puisque $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. De la sorte, la structure $(U(A), \cdot, 1)$ est un groupe.

Définition 2.3 La fonction d'Euler φ est définie de la façon suivante, pour $n \geq 2$,

$$\varphi(n) = |U(\mathbb{Z}_n)|.$$

où $|X|$ est le cardinal de l'ensemble X.

3. Principes de base

Pour qu'Oscar ne puisse comprendre le message M, appelé *message clair*, envoyé par Alice, il faut le rendre illisible pour lui mais pas pour Bob. Dans ce cas, comment procéder ?

Nous voulons transformer le message M en un message M', appelé *message secret*, qui soit incompréhensible pour O. Le réflexe naturel est d'utiliser une fonction

$$c : \mathcal{M} \to \mathcal{M}',$$

c'est-à-dire, une fonction définie sur l'espace $\mathcal{M}$ des textes clairs à valeurs dans l'espace $\mathcal{M}'$ des textes secrets ; que nous appelerons par la suite *fonction de codage*, et de définir M' par

$$M' = c(M).$$

Pour que B puisse décoder le message M', il est nécessaire que la fonction c soit bijective. Il reste alors à B à calculer la fonction $d = c^{-1}$ que nous appelerons *fonction de décodage*, pour obtenir le texte clair M.

Une question vient cependant de suite à l'esprit : "Si B, pour obtenir M, n'a qu'à inverser la fonction c, pourquoi O ne ferait-il pas de même pour lire le message clair ?".

Introduisons le contexte mathématique dans lequel nous allons évoluer à l'avenir. Les messages à envoyer étant écrits dans un langage naturel, c'est-à-dire dans notre cas le français, nous n'allons utiliser qu'un nombre fini de caractères (lettres et signes de ponctuation). Notons Σ l'alphabet utilisé, qui représente l'ensemble de tous les signes employés pour écrire un message, et Σ^* l'ensemble des suites finies d'éléments de Σ. Un message M n'est alors rien d'autre qu'un élément de Σ^*. L'alphabet Σ étant fini, il paraît naturel de l'identifier à l'anneau $\mathbb{Z}_n$ où $n = |\Sigma|$, cette identification étant souvent appelée *codage standard*. Le codage standard de l'alphabet $\{A, \cdots, Z\}$ est donné par la bijection suivante,

$$[.] : \Sigma \to \mathbb{Z}_{26}$$

[A] =0	[H] = 7	[O] =14	[V] =21
[B] =1	[I] = 8	[P] =15	[W] =22
[C] =2	[J] = 9	[Q] =16	[X] =23
[D] =3	[K] =10	[R] =17	[Y] =24
[E] =4	[L] =11	[S] =18	[Z] =25.
[F] =5	[M] =12	[T] =19	
[G] =6	[N] =13	[U] =20	

Ainsi, une étape préliminaire au codage proprement dit est la transformation du message M de longueur p en un p-uple d'éléments de $\mathbb{Z}_{26}$.

Une *fonction de codage lettre par lettre*, est une fonction

$$c' : \Sigma^* \to \Sigma^*$$

obtenue à partir d'une fonction de codage de caractères

$$c : \Sigma \to \Sigma$$

de la façon suivante : si $M = m_1 m_2 \cdots m_p$ où les $m_i \in \Sigma$ $(i \leq p)$ représentent les caractères utilisés dans le message, alors

$$c'(M) = c(m_1)\, c(m_2)\, \cdots\, c(m_p).$$

Etant donné qu'une fonction de codage est une bijection, la fonction de décodage

$$d' = (c')^{-1} : \Sigma^* \to \Sigma^*$$

est elle aussi obtenue à partir d' une fonction

$$d = c^{-1} : \Sigma \to \Sigma$$

de décodage lettre par lettre.

4. Cryptosystème linéaire

Un *cryptosystème linéaire* est un *cryptosystème*, c'est-à-dire une famille $\mathcal{F}$ de codages $c : \mathcal{M} \to \mathcal{M}'$, dont la fonction de codage est du type

$$c : \mathbb{Z}_n \to \mathbb{Z}_n : x \mapsto ax + b.$$

Remarquons de suite que la fonction de codage est bijective si et seulement si $a \in U(\mathbb{Z}_n)$; rappelons (voir annexe) que

$$U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n : \text{pgcd}(a, n) = 1\}.$$

Pour que ce codage soit utilisable en pratique, A doit fournir à B les paramètres (a, b) qui sont appelés *la clé secrète* du cryptosystème. Il apparaît ainsi qu'à chaque clé (a, b) correspond une fonction de codage différente $c(x) = ax + b$.

Pour éclaircir notre propos, considérons un exemple.

Exemple 4.1 Alice et Bob ont choisi d'un commun accord la clé $(3, 4)$. Alice désire envoyer le message "BYE". Nous allons donc coder linéairement ce message lettre par lettre à l'aide de la fonction de codage,

$$c : \mathbb{Z}_{26} \to \mathbb{Z}_{26} : x \mapsto 3x + 4.$$

Nous obtenons ainsi, avec le codage standard sur $\mathbb{Z}_{26}$,

$$BYE \to (1, 24, 4) \xrightarrow{c} (7, 24, 16) \to HYC,$$

car

$$\begin{aligned} c(1) &= (3 + 4) \,|2|\, 6 = 7 \\ c(24) &= (72 + 4) \,|2|\, 6 = 24 \\ c(4) &= (12 + 4) \,|2|\, 6 = 16. \end{aligned}$$

Alice envoie donc le message secret "HYQ".

Bob reçoit alors ce message ; et étant donné qu'il connaît la clé $(3, 4)$, il lui est dès lors facile de trouver la fonction de décodage,

$$d : \mathbb{Z}_{26} \to \mathbb{Z}_{26} : x \mapsto 3^{-1}(x - 4).$$

On voit ainsi clairement que $3^{-1} = 9 \,|2|\, 6$ puisque $3 \times 9 = 27 \,|2|\, 6 = 1$. Nous obtenons alors,

$$HYC \to (7, 24, 16) \xrightarrow{d} (1, 24, 4) \to BYE.$$

Remarquons pour terminer que si la clé de codage avait été $(2, 4)$, il aurait été impossible de décoder le message puisque $2 \notin U(\mathbb{Z}_{26})$.

Nous comprenons maintenant que O ne peut inverser facilement la fonction c, car, en principe, il ne connaît pas la clé de codage. Cependant, les codages linéaires lettre par lettre sont facilement "cassés" par l'analyse statistique du message. De plus, nous pouvons remarquer que le nombre de clés possibles pour le décodage est $26|U(\mathbb{Z}_{26})|$. Ainsi en procédant exhaustivement, il serait possible de décoder le message. C'est pourquoi, en pratique, on a souvent recours au codage bloc par bloc.

Exemple 4.2 Le message est cette fois décomposé en blocs de k lettres,

$$M = (m_1 \cdots m_k)\,(m_{k+1} \cdots m_{2k}) \cdots,$$

la fonction de codage c' est cette fois obtenue à partir d'une fonction de codage de blocs de k lettres

$$c : \Sigma^k \to \Sigma^k,$$

ainsi

$$c'(M) = c(m_1 \cdots m_k)\, c(m_{k+1} \cdots m_{2k}) \cdots$$

Le codage linéaire devient alors

$$c : (\mathbb{Z}_n)^k \to (\mathbb{Z}_n)^k : x \mapsto Ax + b,$$

où A est ici une matrice de dimension $k \times k$ et b un vecteur de $\mathbb{Z}_n^k$. Précisons toutefois que cette fonction ne définit un codage que si A est invertible ; il est possible de montrer que cela revient à dire que $\det A$ doit être invertible dans $\mathbb{Z}_n$ [**2**].

5. Cryptosystème "one-time pad"

Le *cryptosystème "one-time pad"* n'est rien d'autre qu'un cryptosystème linéaire bloc par bloc dont la fonction de codage est

$$c : (\mathbb{Z}_n)^k \to (\mathbb{Z}_n)^k : x \mapsto x + b,$$

il présente toutefois la particularité suivante : la clé secrète du message, ici représentée par b, est aussi longue que le message et ne peut être utilisée qu'une seule fois.

Exemple 5.1 Codons le mot "YOU" avec le codage standard sur $\mathbb{Z}_{26}$; on obtient

$$YOU \to (24, 14, 20).$$

Si nous prenons comme clé $b = (11, 8, 4)$; le message codé est alors

$$\begin{aligned} c(24, 14, 20) &= (24, 14, 20) + (11, 8, 4) \\ &= (9, 22, 24); \end{aligned}$$

le message qu'Alice va envoyer à Bob est donc "JWY".

Toutefois, par convention, nous n'utilisons pas le codage standard sur $\mathbb{Z}_{|\Sigma|}$ pour le cryptosystème "one-time pad", mais plutôt un codage sur $\mathbb{Z}_2$.

L'utilisation de $\mathbb{Z}_2$ à la place de $\mathbb{Z}_{|\Sigma|}$ se justifie notamment par le fait que les ordinateurs codent les caractères en binaire (codage ASCII).

Considérons l'exemple suivant comportant un extrait du codage ASCII.

Exemple 5.2 Le codage ASCII permet de coder jusqu'à 256 symboles. L'alphabet utilisé comporte donc d'autres lettres que $A, \cdots, Z$. Nous ne reprenons ici que le codage des lettres utiles à notre exemple.

Lettre	code	en base 2
*	42	01001010
D	68	01000100
G	71	01000111
K	75	01001011
O	79	01001111
v	118	01110110
z	122	01111010

codage de "GOOD"	01000111 01001111 01001111 01000100
clé de codage	00001101 00111001 00000100 00111110
addition dans $\mathbb{Z}_2$	01001010 01110110 01001011 01111010

Par conséquent, le codage de "GOOD" est "*vKz".

Ce cryptosystème est totalement sûr. La clé étant aussi longue que le message, la connaissance de la traduction d'une partie du message n'augmente en rien la probabilité de décryptage d'une autre partie. Il convient de remarquer que la clé ne peut être utilisée qu'une seule fois, puisque si message clair et message secret sont connus, il en est de même pour la clé. On évite ce problème en générant une nouvelle clé à chaque nouveau message.

Il existe cependant deux inconvénients. Il faut produire une nouvelle clé à chaque message, ce qui peut être une tâche considérable si le texte clair compte dix millions de caractères ! Il faut de plus transmettre la clé au destinataire, ce qui procède des mêmes risques que la transmission du message lui-même. Cependant, il est possible de pallier à ces inconvénients. Il est vital pour la sécurité du système que la clé ne puisse être devinée, une bonne façon de procéder serait de générer une suite de nombres aléatoires. Par exemple, on pourrait jeter une pièce de monnaie et prendre 1 si pile apparaît et 0 si c'est face.

Bien sûr, les deux inconvénients majeurs du cryptosystème demeurent, c'est pourquoi, en pratique, au lieu d'utiliser des suites de nombres aléatoires, on utilise des suites appelées *pseudo-aléatoires*. Cette façon de procéder présente le double avantage que ces suites sont "presque" aléatoires (en fait, les éléments d'une telle suite sont bien distribués, non-corrélés et imprévisibles) et donc conviennent bien pour être la clé de ce cryptosystème. De plus, ces suites sont facilement transmissibles car le destinataire ne doit connaître qu'un nombre restreint de paramètres pour reproduire la suite.

Nous allons maintenant donner une méthode pour générer des nombres pseudo-aléatoires. Ce générateur pseudo-aléatoire est basé sur le principe du système RSA dont nous discuterons dans la section suivante.

Définition 5.3 Soient p et q deux nombres premiers distincts et suffisamment éloignés l'un de l'autre, et soit $n = pq$. Considérons b tel que

$$\text{pgcd}(b, \varphi(n)) = 1$$

où φ est la *fonction d'Euler* et vaut dans ce cas (voir annexe)

$$\varphi(n) = (p-1)(q-1).$$

Une *semence* s_0 est un élément de $U(\mathbb{Z}_n)$; pour $i \geq 1$, on définit

$$s_{i+1} = s_i^b \,|n|\,,$$

puis

$$f(s_0) = (z_1, z_2, \cdots, z_l)$$

où

$$z_i = s_i \,|2|$$

et $1 \leq i \leq l$. La fonction f est appelée un (k, l)-*générateur RSA*.

Exemple 5.4 Soient $p = 263$, $q = 347$ et $b = 1547$. On a $n = 91261$ et si $s_0 = 75364$, on obtient

i	s_i	$z_i \bmod 11413$
0	75634	
1	31483	1
2	31238	0
3	51968	0
4	39796	0
5	28716	0
6	14089	1
7	5923	1
8	44891	1
9	62284	0
10	11889	1
11	43467	1
12	71215	1
13	10401	1
14	77444	0
15	56794	0
16	78147	1
17	72137	1
18	89592	0
19	29022	0
20	13356	0
⋮	⋮	⋮

La chaîne pseudo-aléatoire engendrée est donc

$$10000111011110011000\ldots$$

Pour générer une telle suite, il suffit de transmettre les paramètres p, q, b et s_0.

6. Le cryptosystème RSA

Le défaut des cryptosystèmes étudiés jusqu'à présent est qu'ils nécessitent la communication préalable de la clé entre Alice et Bob. L'objectif des systèmes à clé publique est de rendre la connaissance de la fonction d "impossible" même si on connaît la fonction c. Le système RSA, du nom de ses auteurs Rivest, Shamir et Adleman, date de 1977 et est le premier cryptosystème à clé publique. Pour construire un tel système, nous devons

choisir une fonction de codage c à sens unique, c'est-à-dire une fonction nécessairement injective mais qui possède la propriété d'être "difficile" à inverser. Rappelons que c est connu de tous même d'Oscar. Ce dernier ne doit donc pas pouvoir inverser facilement c. Le destinataire, Bob, doit quant à lui pouvoir calculer aisément d. Cela est rendu possible car seul Bob connaît des informations supplémentaires sur la fonction de codage c.

Une des caractéristiques du cryptosystème RSA est qu'il permet à plusieurs utilisateurs de communiquer secrètement. Pour comprendre le fonctionnement du RSA, développons son protocole. Chaque utilisateur choisit secrètement deux grands nombres premiers distincts p et q (de l'ordre de 10^{100}). Posons $n = p.q$; nous savons (voir annexe) que la valeur de la fonction d'Euler en n est $\varphi(n) = (p-1)(q-1)$. L'utilisateur choisit ensuite b invertible dans $\mathbb{Z}_{\varphi(n)}$. Posons $a = b^{-1} \bmod \varphi(n)$. Les fonctions de codage et de décodage sont données par

$$c : \mathbb{Z}_n \to \mathbb{Z}_n : x \mapsto x^b \bmod n$$

$$d : \mathbb{Z}_n \to \mathbb{Z}_n : x \mapsto x^a \bmod n.$$

On démontre en annexe que $d = c^{-1}$. Les nombres n et b sont suffisants au codage et constituent la clé rendue publique. De cette manière, tout utilisateur A peut envoyer secrètement un message M à un autre utilisateur B, tout simplement en envoyant le message codé $c_B(M)$ (on utilise l'indice B pour spécifier que le codage est réalisé avec la paire (n, b) propre à l'utilisateur B). Les nombres p, q et a sont eux conservés secrètement par l'utilisateur concerné. Pour pouvoir effectuer le décodage, il est nécessaire de connaître a. Le nombre b étant public, le calcul de a peut être réalisé si on a sa disposition $\varphi(n)$ ou le couple (p, q). On peut montrer qu'il est aussi "difficile" d'obtenir $\varphi(n)$ que de factoriser n en $p.q$.

Le nombre n étant public, essayons de nous convaincre que n est difficilement factorisable, la sécurité du RSA reposant uniquement sur ce fait. Pour rechercher un des facteurs de n, une méthode rudimentaire appelée *crible d'Eratosthène* consiste à tester la divisibilité de n par tous les nombres impairs de 3 jusqu'à $[\sqrt{n}]$ (la partie entière de $\sqrt{n}$). De cette manière on trouvera inévitablement le plus petit des deux facteurs composant n. Le nombre n comportant pas moins de deux cents chiffres en base 10, $\sqrt{n} \sim 10^{100}$ et si on admet de manière optimiste qu'un ordinateur est capable de réaliser 10^{10} divisions par seconde, il faudra à cet ordinateur pas moins de cinq fois l'âge de l'univers avant de factoriser n ! Il existe bien évidemment d'autres algorithmes plus "performants" mais aucun ne peut factoriser un nombre n suffisamment grand en des temps raisonnables.

Nous ne développerons pas ici comment trouver deux grands nombres premiers p et q (en pratique, on génère deux nombres aléatoires et on leur applique un test efficace de primalité). Considérons à présent une application numérique du RSA avec deux petits nombres premiers. Dans cet exemple, nous montrons comment obtenir l'inverse modulo $\varphi(n)$ et un exposant modulo n.

Exemple 6.1 Soient $p = 101$ et $q = 113$. On a $\varphi(n) = 100 \times 112 = 11200$ et $n = 101 \times 113 = 11413$. Nous devons choisir comme exposant de codage un élément b appartenant à $U(\mathbb{Z}_{\varphi(n)})$. Or $11200 = 2^6 \times 5^2 \times 7$; on peut donc prendre pour b tout nombre n'étant pas divisible par 2, 5 et 7 ; $b = 3533$ convient. On peut vérifier que $\text{pgcd}(b, \varphi(n)) = 1$ au moyen de l'*algorithme d'Euclide* :

$$\begin{aligned}
11200 &= 3533 \times 3 + 601 \\
3533 &= 601 \times 5 + 528 \\
601 &= 528 \times 1 + 73 \\
528 &= 73 \times 7 + 17 \\
73 &= 17 \times 4 + 5 \\
17 &= 5 \times 3 + 2 \\
5 &= 2 \times 2 + 1 \\
2 &= 1 \times 2 + 0
\end{aligned}$$

Le pgcd de 11200 et 3533 est bien 1 et grâce à ce développement, nous pouvons calculer $a = b^{-1} \bmod \varphi(n)$

$$\begin{aligned}
1 &= 5 - 2 \times 2 = 5 - 2 \times (17 - 5 \times 3) \\
&= -2 \times 17 + 7 \times 5 = -2 \times 17 + 7 \times (73 - 4 \times 17) \\
&= 7 \times 73 - 30 \times 17 = 7 \times 73 - 30 \times (528 - 7 \times 73) \\
&= -30 \times 528 + 217 \times 73 = -30 \times 528 + 217 \times (601 - 528) \\
&= 217 \times 601 - 247 \times 528 = 217 \times 601 - 247 \times (3533 - 5 \times 601) \\
&= -247 \times 3533 + 1452 \times 601 = -247 \times 3533 + 1452 \times (11200 - 3 \times 3533) \\
&= -4603 \times 3533 + 1452 \times 11200.
\end{aligned}$$

Donc modulo 11200, on a $1 = -4603 \times 3533$; par conséquent, $a = -4603 = 6597 \bmod 11200$. Bob rend public $n = 11413$ et $b = 3533$. Il garde secret $\varphi(n)$, $a = 6597$ ainsi que p et q. Sans entrer pour l'instant dans le détail du

codage standard, imaginons qu'Alice souhaite envoyer le nombre 9726 à Bob. Elle doit calculer $9726^{3533} \bmod 11413$; pour ce faire, donnons la méthode d'exponentiation modulaire *square-and-multiply* qui présente l'avantage de pouvoir être réalisée rapidement. Voici l'algorithme général du calcul de $x^c \bmod n$:

1. décomposer c en base 2, $c = \sum_{i=0}^{l-1} c_i\, 2^i$.
2. $z \leftarrow 1$
3. pour i allant de $l-1$ jusqu'à 0 faire

$$z \leftarrow z^2$$
si $c_i = 1$ alors $z \leftarrow z.x \bmod n$

Reprenons le calcul de $9726^{3533} \bmod 11413$.

$$\begin{aligned} 3533 \;=\; & \mathbf{1} \times 2048 + \mathbf{1} \times 1024 + \mathbf{0} \times 512 + \mathbf{1} \times 256 + \mathbf{1} \times 128 + \mathbf{1} \times 64 \\ & + \mathbf{0} \times 32 + \mathbf{0} \times 16 + \mathbf{1} \times 8 + \mathbf{1} \times 4 + 0 \times 2 + \mathbf{1} \times 1. \end{aligned}$$

Appliquons l'algorithme,

i	c_i	$z \bmod 11413$
11	1	$1^2 = 1$
		$1 \times 9726 = 9726$
10	1	$9726^2 = 4132$
		$4132 \times 9726 = 2659$
9	0	$2659^2 = 5634$
8	1	$5634^2 = 2403$
		$2403 \times 9726 = 9167$
7	1	$9167^2 = 11383$
		$11383 \times 9726 = 4958$
6	1	$4958^2 = 9575$
		$9575 \times 9726 = 7783$
5	0	$7783^2 = 6298$
4	0	$6298^2 = 4629$
3	1	$4629^2 = 5440$
		$5440 \times 9726 = 10185$
2	1	$10185^2 = 1468$
		$1468 \times 9726 = 105$
1	0	$105^2 = 11025$
0	1	$11025^2 = 2175$
		$2175 \times 9726 = 5761$

donc $c(9726) = 9726^{3533} \bmod 11413 = 5761$. Alice envoie donc à Bob le nombre 5761. Pour le décodage, Bob calcule $5761^{6597} \bmod 11413$ et retrouve 9726.

Nous espérons que le lecteur est à présent convaincu que la mise en oeuvre du RSA s'effectue en un temps raisonnable (générer deux nombres premiers, calcul d'inverse et exponentiation) alors que l'attaque du RSA (équivalente à la factorisation de n) nécessite un temps prohibitif.

Il nous reste à éclaircir un dernier point. Les fonctions c et d sont définies dans $\mathbb{Z}_n$ avec n suffisamment grand. Pour garantir la sécurité du RSA, puisque n est largement supérieur à la taille de l'alphabet utilisé, on va dès lors pouvoir réaliser le codage d'un bloc de lettres par un nombre inférieur à n en complétant le codage standard. La taille des blocs est déterminée par n.

Pour fixer les idées, supposons que l'on travaille sur l'alphabet $\{A, \cdots, Z\}$ de 26 lettres. Il existe $k \in \mathbb{N}$ tel que

$$26^k \leq n < 26^{k+1}. \qquad (*)$$

On peut se convaincre que les nombres exprimés en base 26 et comportant k chiffres sont inférieurs à 26^k, donc à n (par exemple, en base 10, les nombres de trois chiffres sont inférieurs à 10^3). Rappelons que les "chiffres" de la base 26 vont de 0 à 25. Nous allons donc considérer des blocs de k lettres (k vérifiant $(*)$). On applique le codage standard à chacune des k lettres du bloc pour obtenir les k chiffres de la représentation en base 26 d'un nombre inférieur à n. C'est à ce nombre que l'on applique la fonction de codage c. On procède en sens inverse pour le décodage. Par exemple, si $n = 707$, alors $26^2 \leq 707 < 26^3$ et on code par des blocs de deux lettres. Ainsi,

$$(L, A) \to (11, 0) \to 11 \times 26 + 0 \times 1 = 286,$$

$$(Z, Z) \to (25, 25) \to 25 \times 26 + 25 \times 1 = 675 < 700.$$

Inversement,

$$56 \to 56 = 2 \times 26 + 4 \to (2, 4) \to (C, E),$$

$$413 \to 413 = 15 \times 26 + 23 \to (15, 23) \to (P, X).$$

Pour conclure avec les cryptosystèmes à clés publiques, nous voudrions signaler le protocole du message signé. Imaginons qu'Alice désire converser

avec Bob par courrier électronique. Comment Bob peut-il être certain que le message qu'il reçoit provient bien d'Alice et pas d'Oscar ayant simplement signé son message Alice ? Une procédure simple basée sur le principe même des cryptosystèmes à clé publique peut être employée. Soient c_A et c_B les clés publiques de codage d'Alice et de Bob respectivement. Soient d_A et d_B les clés de décodage connues uniquement d'Alice pour d_A et de Bob pour d_B. Alice procède de la manière suivante, voulant envoyer le message M, elle code celui-ci avec d_A et ensuite avec c_B. Elle envoie donc à Bob le message $c_B(d_A(M))$. Bob utilise sa fonction de décodage pour obtenir le texte $d_A(M)$. La fonction c_A étant publique il peut l'appliquer au message pour retrouver M ; car rappelons que c_A et d_A sont inverses l'une de l'autre. Remarquons que seule Alice est capable de générer le texte $d_A(M)$ puisque la fonction d_A n'est connue que d'elle seule. Ceci garantit donc l'authenticité du message. Alice ne doit pas envoyer à Bob le message $d_A(M)$ car celui-ci pourraît être décodé par n'importe qui. C'est pour cette raison qu'elle utilise ensuite c_B.

7. Annexe

Les propriétés suivantes constituent un complément théorique destiné au lecteur intéressé.

Proposition 7.1 *Si $n \geq 2$, alors*

$$U(\mathbb{Z}_n) = \{m \in \mathbb{Z}_n : \text{pgcd}(m, n) = 1\}.$$

Démonstration. Nous savons, par le théorème de Bezout, que $\text{pgcd}(m, n) = 1$ pour $m \in \mathbb{Z}_n$, équivaut au fait qu'il existe $\alpha, \beta \in \mathbb{Z}$ tels que

$$\alpha \cdot m + \beta \cdot n = 1,$$

c'est-à-dire, qu'il existe $\alpha \in \mathbb{Z}$ tel que

$$\alpha \cdot m = 1 \,|n|\,.$$

Ainsi, d'une part, si $0 < \alpha < n$, $\alpha = m^{-1}\,|n|$ convient. D'autre part, si $\alpha > n$, on peut écrire

$$\alpha = \alpha' + kn$$

avec $\alpha' < n$ et $k \in \mathbb{N}_0$. On obtient alors,

$$\begin{aligned} \alpha \cdot m &= \alpha' \cdot m + (k \cdot m)n \\ &= \alpha' \cdot m \, |n| \, , \end{aligned}$$

et $\alpha' = m^{-1} \, |n|$ convient. Pour le cas où $\alpha < 0$, il suffit de considérer $k \in \mathbb{N}_0$ tel que $0 < \alpha + kn < n$, la conclusion s'ensuit aussitôt.

Proposition 7.2 *Si p et q sont deux nombres premiers distincts, alors*

$$\varphi(pq) = (p-1)(q-1).$$

Démonstration. On a

$$\varphi(n) = |U(\mathbb{Z}_n)| = |\{x \in \mathbb{Z}_n : \operatorname{pgcd}(x, n) = 1\}|.$$

Montrons d'abord que $\varphi(pq) = \varphi(p)\varphi(q)$. Nous savons que $\mathbb{Z}_{pq}$ est isomorphe à $\mathbb{Z}_p \times \mathbb{Z}_q$; ainsi, $U(\mathbb{Z}_{pq})$ est aussi isomorphe à $U(\mathbb{Z}_p) \times U(\mathbb{Z}_q)$. Ces deux ensembles possèdent dès lors le même cardinal ; ce qui revient à dire

$$\varphi(pq) = \varphi(p)\varphi(q).$$

Puisque p est premier, il est premier avec $1, \cdots, p-1$, et ainsi

$$\varphi(p) = p - 1,$$

un raisonnement analogue sur q permet de conclure aisément.

Pour prouver la justesse du protocole RSA, il faut montrer que la fonction de codage est bijective. Les deux propositions suivantes prouvent ce fait.

Théorème 7.3 *Soient $r = p_1 \cdots p_k$ où les p_i, $1 \leq i \leq k$, sont premiers et distincts ; et*

$$s = \operatorname{ppcm}(p_1 - 1, \cdots, p_k - 1).$$

Dans ce cas,

$$\alpha = 1 \, |s| \Rightarrow m^\alpha = m \, |r| \, .$$

En particulier, si $n = pq$, où p et q sont deux nombres premiers, alors

$$\alpha = 1 \, |\varphi| \, (n) \Rightarrow m^\alpha = m \, |n| \, .$$

Démonstration. Nous savons que Z_r est isomorphe à $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$; donc, à un $m \in \mathbb{Z}_r$, on associe univoquement un k-uple $(m_1, \cdots, m_k)$ avec $m_i \in \mathbb{Z}_{p_i}$, $1 \leq i \leq k$. Si $\alpha = 1 \,|s|$, alors

$$\alpha = 1 + k' \,\mathrm{ppcm}(p_1 - 1, \cdots, p_k - 1)$$

où $k \in \mathbb{N}$. Donc,

$$\alpha = 1 \,|(|\, p_i - 1)$$

pour tout $i = 1, \cdots, k$. Il suffit alors de montrer que

$$m_i^{\alpha} = m_i \,|p|_i \,.$$

Soit $i \in \{1, \cdots, k\}$, deux cas se présentent.

i) On a $m_i = 0 \,|p|_i$, la conclusion s'ensuit trivialement.

ii) On a $m_i \neq 0 \,|p|_i$, dans ce cas,

$$\begin{aligned} m_i^{\alpha} &= m_i^{1+\beta(p_i-1)} \\ &= m_i (m_i^{(p_i-1)})^{\beta}, \end{aligned}$$

or, par le petit théorème de Fermat, $m_i^{(p_i-1)} = 1 \,|p|_i$. Cela étant,

$$m_i^{\alpha} = m_i \,|p|_i \,.$$

Corollaire 7.4 *L'application $c : \mathbb{Z}_n \to \mathbb{Z}_n : m \mapsto m^b$ est une bijection.*

Démonstration. Puisque $ab = 1 \,|\varphi|\,(n)$, la fonction $d : \mathbb{Z}_n \to \mathbb{Z}_n : m \mapsto m^a$ est bien l'inverse de la fonction c.

8. Quelques adresses Internet

Les personnes disposant d'un accès Internet trouveront ci-dessous quelques adresses intéressantes traitant de cryptographie.

http ://www.ftech.net/˜monark/crypto/main.hts

introduction élémentaire à la cryptographie

http ://rschp2.anu.edu.au :8080/crypt.html

fichiers sources et information à propos du logiciel PGP

http ://crypto.swdev.co.nz/

cryptosystème à clé publique RPK

http ://www.rsa.com/

société commercialisant le RSA

http ://itrc.on.ca/CryptoWeb/

liste de liens sur la cryptographie

http ://www.math.jussieu.fr/˜fermigie/elliptic.html.en

informations sur les courbes elliptiques

http ://www.elementrix.co.il/

cryptosystème basé sur le one-time pad

Bibliographie

[1] *For all practical purposes, introduction to contempory mathematics*, Freeman, New-York, 1997.

[2] G. Hansoul, *Structures discrètes*, cours de licence en sciences mathématiques, Université de Liège, 1993.

[3] B. Schneier, *Cryptographie appliquée*, International Thomson Publishing France, Paris, 1997.

[4] D. Stinson, *Cryptographie - Théorie et pratique*, International Thomson Publishing France, Paris, 1996.

Pierre Paquay et **Michel Rigo**
Faculté d'Economie, de Gestion, de Sciences sociales
Bld. du Rectorat 7, Bat. B31
4000 Liège

Échos de congrès – CIEAEM 50

J. Bair,

Fondée en 1950, la Commission Internationale pour l'Etude et l'Amélioration de l'Enseignement des Mathématiques (CIEAEM) a pour objectifs d'*étudier les conditions actuelles dans lesquelles se déroule l'enseignement des mathématiques et ses possibilités de développement afin de favoriser son amélioration.* Pour cela, elle organise chaque année des conférences regroupant des enseignants et des chercheurs venus du monde entier.

Cette année 1998 avait lieu, du 1er au 8 août à Neuchâtel (en Suisse), la cinquantième rencontre, baptisée CIEAEM 50, sur le thème général suivant : *Les liens entre la pratique de la classe et la recherche en didactique des mathématiques*, avec cinq sous-thèmes, à savoir : *Finalités de l'enseignement des mathématiques, Communication et collaboration entre praticiens et chercheurs, Recherche en didactique des mathématiques et formations des maîtres, Spécificités de la recherche en didactique des mathématiques, La prise en compte de résultats de la recherche dans les moyens et les outils pour l'enseignement.* Plus de 300 participants, issus d'une trentaine de pays, ont travaillé à Neuchâtel selon un rythme de travail assez soutenu (chaque jour, plus de 6 heures de conférences, ateliers ou travaux de groupe), le tout selon un horaire très strict (qui confirmait bien la ponctualité des Suisses). Une douzaine de compatriotes participaient à la rencontre, dont notre président J. Navez, notre ancien trésorier R. Scrève ...et six psycho-pédagogues universitaires.

Le niveau des exposés m'a paru fort inégal : le meilleur côtoyait ...le moins bon. Plutôt que de relater en détail ce qui a été dit à Neuchâtel (les personnes intéressées pourront lire les actes de la rencontre), je voudrais relever deux points qui m'ont profondément marqué ...et qui, de façon générale, m'inquiètent fortement en ce qui concerne l'enseignement des mathématiques.

Il y avait en Suisse de très nombreux psycho-pédagogues pour présenter leurs "recherches". Malheureusement, j'ai constaté qu'ils ne connaissent pas toujours très bien les mathématiques et n'ont aucune expérience de l'enseignement de notre discipline. Toutefois, il se considèrent comme étant des "spécialistes" de la didactique des mathématiques et se permettent de juger, et même de critiquer, les professeurs de mathématiques. J'ai notamment entendu un "chercheur-pédagogue" relater une expérience sur l'apprentissage de l'algèbre (l'algèbre étant, pour lui ...et beaucoup d'autres

psycho-pédagogues, les “calculs avec des lettres”, car, quand il n'y a pas de lettres, c'est de l'arithmétique) auprès de jeunes de 12-13 ans au sein de la Communauté française de Belgique. Il a prétendu, notamment, qu'une des caractéristiques de notre enseignement est la “Culture de l'échec”, que les professeurs de mathématiques cotaient, quelle que soit la valeur des élèves, de manière à “avoir une courbe de Gauss”, qu'il n'y avait en Communauté aucun manuel à la disposition des professeurs, que les professeurs insistent le plus sur ce que leur enquête a révélé être le moins bien assimilé et, qu'en conséquence, les professeurs devaient “changer leurs pratiques”. Bien sûr, nous sommes conscients que notre enseignement est loin d'être parfait et qu'il doit être sans cesse amélioré ; nous serons d'ailleurs toujours contents de recevoir des conseils : encore faut-il que ceux-ci soient pertinents et constructifs. Il va sans dire que les membres du Comité de la Société qui ont entendu pareilles affirmations fausses et malveillantes sont intervenus, énergiquement et à de nombreuses reprises, pour infirmer ce qui avait été dit pendant cette conférence : nous ne pouvions tolérer que des psycho-pédagogues donnent, aux étrangers présents dans la salle, une image aussi négative et pas du tout réaliste de notre enseignement.

Si j'ai relaté cet épisode, c'est parce que cela dépasse, me semble-t-il, et de loin, la simple anecdote : de nombreux non-mathématiciens se disent spécialistes de l'enseignement des mathématiques et ont des avis sur la question alors qu'ils sont parfois très mal informés et incompétents. Il me paraît dangereux, pour nous professeurs de mathématiques, mais aussi et surtout pour la formation intellectuelle de nos jeunes, que de tels “chercheurs” s'occupent de l'enseignement des mathématiques en “prenant même le pouvoir” (car ils sont nombreux et “parlent” beaucoup, avec facilité et “sans complexe”), allant jusqu'à influencer (par exemple, au niveau de la confection des programmes) de façon néfaste les mondes éducatif et politique. Il me semble que nous, les mathématiciens, devons rester vigilants, critiquer et combattre de telles pratiques !

Un autre danger pour l'enseignement des mathématiques est causé par des mathématiciens-didacticiens et réside dans la nature de certaines de leurs recherches. Je pense, par exemple, à cette expérience réalisée par cinq italiennes d'une université. Elles ont réalisé une vaste enquête (en interrogeant plus de 600 personnes, de tous âges) sur le concept de limite. Partant de l'hypothèse (peu plausible, selon moi) que des concepts mathématiques, tels que la notion de limite, étaient mal compris pour des raisons essentiellement linguistiques, parce que le sens du mot en question est mal connu, elles ont demandé à leurs sujets de leur décrire, en général, le sens du mot

"limite". Elles ont reçu des réponses de ce type : *c'est une borne, ça n'a pas de fin*, ou encore *c'est un obstacle*, selon une handicapée, ...Dans une deuxième phase de leur recherche, elles ont demandé à de nombreuses personnes, dont des élèves des beaux-arts sans connaissance mathématique, de réaliser un dessin illustrant le concept de limite ; elles se sont alors efforcées d'interpréter les dessins en fonction des "définitions" reçues, de manière à classer ces dernières ; elles en concluent que le mot "limite" évoque le plus souvent une borne soit physique, soit morale. Ensuite, elles ont considéré le concept mathématique en proposant trois fonctions, définies analytiquement et représentées par un graphe, pour lesquelles les personnes interrogées devaient dire laquelle des assertions suivantes est vraie lorsque la variable x tend vers l'infini : a) la fonction possède une limite finie, b) la fonction possède une limite infinie, c) la fonction ne possède pas de limite ; ces trois fonctions étaient, dans l'ordre, $\cos x$, une fonction homographique (du type $\frac{ax+b}{cx+d}$) et une fonction du type $ax^2 + b$ (les deux derniers cas étant donnés pour des valeurs numériques des paramètres) ; elles ont constaté (fallait-il une enquête pour cela ?) que le premier cas avait été, de loin, le moins bien réussi (ce qui avait l'air de les surprendre fortement !) et elles expliquaient cela par un seul motif (pas faux, du reste, mais, à mon avis, ce n'est sûrement pas la seule explication pertinente à donner), à savoir que dans les deux derniers cas, les élèves pouvaient effectivement calculer numériquement la limite, ce qui était (et pour cause !) impossible dans le premier cas.

Bien que ces chercheurs aient annoncé qu'elles espèrent prolonger et approfondir leur étude, je me demande si de tels travaux font réellement progresser l'enseignement des mathématiques ; ces enquêtes auraient d'ailleurs pu être réalisées au dix-huitième siècle et ne tiennent aucunement compte des progrès réalisés depuis cette époque ! Il me semble que, pour rester crédibles et ne pas être critiqués, les mathématiciens-didacticiens doivent soigneusement sélectionner les sujets de leurs recherches en tenant compte des dernières découvertes scientifiques et en exploitant les technologies les plus récentes, en restant rigoureux dans leur approche et ne transformant pas leurs travaux en de vagues enquêtes sociologiques ou psychologiques.

Ces réflexions (un peu "provocatrices", je le concède) ont été rédigées "à chaud" et n'engagent évidemment que moi. Je serais toutefois heureux et intéressé d'obtenir les réactions des lecteurs de la revue. D'avance Merci.

J. BAIR

Revue des revues

C. Villers,

Bulletin de l'APMEP, *n*°414, février-mars 1998.

Cette livraison de bulletin de l'Association des Professeurs de Mathématique de l'Enseignement Public (France) est "accompagnée" d'un livret intitulé "BAC Mathématique - Horizon 2000" qui est une contribution du groupe de travail de l'APMEP, "Prospective Bac".

Ce livret contient des éléments de réflexion sur la problématique du Bac et propose une analyse de trois sujets après une interrogation sur les apports spécifiques de l'enseignement mathématique.

Le bulletin proprement dit comporte, outre les rubriques habituelles ...

- l'*éditorial* : Que fait l'APMEP pour les lycées professionnels ?
- Un dossier baccalauréat composé de 2 articles :
  - l'un : *quelques réactions à propos des sujets du baccalauréat 1997* par **Jean Capron** qui réalise une synthèse de réponses reçues à une "enquête" sur les sujets proposés. Ceux-ci n'étant pas rappelés, il est très malaisé de bien percevoir la signification des avis émis !
  - l'autre : *Brouillons pour des sujets de bac du troisième millénaire* par **Daniel Reisz**.
    L'auteur y propose 4 énoncés d'exercices plus ouverts, en souhaitant que ses propositions alimentent un débat nécessaire sur la vision des mathématiques, sur la conception de son apprentissage et sur le rôle de l'école dans ce domaine.
- **Karine Saada** traite du travail en groupe utilisé dans le but de remédier à l'hétérogénéité de la classe : A partir de quoi ? Quand ? Comment ? sont les questions auxquelles l'auteur apporte ses réponses !
- **Georges Lion**, auteur du texte "*Régionnement du plan par les bissectrices*" établit, par l'utilisation de la géométrie élémentaire, les relations caractérisant l'appartenance d'un point à chacune des parties du plan déterminées par les bissectrices de 2 droites sécantes.
- **Daniel Mansion** traite de la "*Résolution graphique des équations algébriques du 3e et 4e degré* et montre que ce problème peut être l'occasion d'un bon travail "sans calculatrice".
- Dans "*Démocratie et Mathématique*", **Yves Husset** montre comment des difficultés surgissent lors de l'adoption de la règle majo-

ritaire pour l'adoption d'une décision collective. Il y rappelle l'effet Condorcet, bien connu, dans ce domaine.
- Dans la rubrique "*Mathématiques et Société*", **Patrick Trabal** traite du sujet "*De la violence envers les mathématiques*". Il souhaite conduire les enseignants à réfléchir sur la discipline et sur leurs pratiques.

Suivent alors une copieuse partie consacrée aux rubriques olympiades, bibliographie et vie de l'association.

Bulletin de l'APMEP, *n*°415, avril-mai 1998.

- Dans l'*éditorial* de ce numéro, des représentants du bureau de l'association réagissent au fait que les enseignants soient "montrés du doigt" par leur Ministre, par les médias et par certaines associations de parents. Cette réaction a pris la forme d'une "lettre ouverte d'un prof à son Ministre". Il s'agit bien légitimement de remettre certaines vérités à leur juste place et à répondre à ce que les auteurs considèrent comme des propos injustifiés pour ne pas dire insultants ! De nombreux arguments en faveur des mathématiques sont ici développés et des revendications avancées. Citons, en particulier, celle de disposer du temps suffisant pour enseigner avec profit.
- Un dossier "calculatrices" comporte deux articles fort intéressants.
  Le premier est intitulé : A propos de : "*La dernière partie de l'iceberg est la plus grosse*". Son auteur, **Agnès Barthes**, y défend l'idée que si l'objectif principal des élèves est d'obtenir de bonnes notes, il leur faudra comprendre que l'objectif de l'enseignement est de rendre ces élèves capables de se servir de leur savoir.
  Le deuxième article a pour titre : "*Erreurs d'arrondis et calculatrices*". **Christian Vassard** et **Didier Trotoux** montrent que dans certains calculs, les erreurs d'arrondis peuvent devenir si importantes qu'elles enlèvent tout sens aux résultats obtenus.
- La géométrie au Collège au travers des niveaux de P. M. Van Hiele par **Annette Michoux-Braconne** présente les résultats d'une recherche en didactique sur le problème de l'enseignement de la démonstration en géométrie en 4e année (2e année en Belgique).
- La règle, un instrument de géométrie projective (par **Rudolph Bkouche**) traite des rapports entre l'usage des instruments géométriques et les propriétés géométriques mises en jeu.

– **Dany-Jack Mercier** est l'auteur de "*L'algèbre dans la correction des erreurs*". Il y traite des problèmes des codes correcteurs d'erreurs. De nombreux codes sont ainsi passés en revue.
– Dans la rubrique "*Mathématiques et Société*", **Gérard Kuntz** présente un article intitulé : "*Point de vue sur l'enseignement des mathématiques*". L'auteur traite de divers thèmes qui ont retenu son attention lors d'un congrès sur la didactique des mathématiques tenus en 1997 au Canada.
Ces thèmes sont :
  - La crise des programmes et des contenus des mathématiques
  - L'enseignement des mathématiques en résolvant des problèmes (très) consistants
  - L'enseignement des mathématiques : une réalité complexe, de nature systémique.

Cette livraison du bulletin de l'APMEP comporte enfin les rubriques traditionnelles et certainement très instructives
  - Les problèmes de l'APMEP
  - Les avis de recherche
  - Les nouvelles brèves
  - Les matériaux pour une documentation
  - la vie de l'association

Bulletin de l'APMEP, $n°416$.

Ce bulletin est entièrement consacré aux journées nationales 1997 de l'Association, à Marseille.

On y trouve le compte-rendu de la séance d'ouverture, les résumés de 4 conférences et des synthèses de certains ateliers.

Les conférences sont :

- *La formule de Black et Scholes* par **Etienne Pardoux**
- *Quelques modèles peu connus* par **Pierre Julien**
- *Mathématiques et informatique graphique* par **Jean-Louis Mahtret**
- *Approche mathématique de la notion de complexité* par **Gerard Ranzi**

16 compte-rendus d'activités en ateliers terminent ce numéro particulier.

Bulletin de l'APMEP, $n°417$, juin-juillet 1998.

Au sommaire de ce numéro, nous avons noté

- *Au ras des pâquerettes* par **Guy Chaty**
  L'auteur y rédige un plaidoyer en faveur de l'initiation à l'algorithmique et montre que l'établissement des liens entre les formulations des algorithmes et leur preuve mathématique aide à la compréhension simultanée du processus algorithmique et du support mathématique. De nombreux exemples sont donnés.
- Le calcul de π en cinquième, avec une bassine, une caisse carrée et des boulettes de papier par *Michel Rousselet*.
  C'est la relation d'une activité de type probabiliste.
- **Claude Matz** présente dans "*Fiche d'évaluation*" une fiche d'évaluation permettant de mieux maîtriser la formation des élèves et de bien cerner leur évolution.
- **Roger Cuppeur** a écrit "*Faire de la géométrie en jouant avec Cabri-géomètre : la cas de l'orthocentre*".
  Il y illustre l'intérêt et l'utilité des nouveaux outils fournis par Cabri II.
- **J. P. Brevan** présente une synthèse des solutions reçues en réponse à un avis de recherche paru dans le bulletin n° 403 au sujet du problème que voici : le carré de tout nombre premier différent de 2 et de 5 est somme de 3 carrés non nuls.
- Dans "*Pourquoi faire simple ...*", **André Cauty** traite des problèmes de la dénomination des grands nombres.

– **Stefan Turnan** (Pologne) présente "*Puzzles géométriques*" où il traite de la décomposition et du réarrangement d'un polygone.
– Deux articles illustrent la rubrique "*Mathématique au fil de la plume*" qui souhaite rapprocher deux enseignements (Français et Mathématiques.
– Les rubriques habituelles complètent ce numéro de la revue de l'APMEP.

Claude Villers

La brochure "Olympiade Mathématique Belge, n°4"

Le quatrième recueil des questions posées aux Olympiades Mathématiques Belges est disponible.
Les trois premières brochures (1976-1981, 1982-1987 et 1988-1993) couvraient toutes des périodes de 6 années. Le détriplement de l'Olympiade depuis 1996 a eu pour conséquences une augmentation substantielle du nombre des questions proposées. Ce quatrième tome de la série ne couvre donc que 5 années d'Olympiades Mathématiques Belges.
Dans ce recueil n°4, toutes les questions des Olympiades des années 1994 à 1998 ont été regroupées par sujet et présentées, autant que faire se pouvait, selon un ordre croissant de difficultés.
Toutes ont été réparties selon les trois catégories Mini, Midi et Maxi. Les questions des deux seules catégories existant en 1994, 1995 ont été distribuées au mieux dans les trois catégories actuelles. Des notations évidentes indiquent à l'utilisateur à quel stade de l'épreuve les questions furent proposées. Des tableaux fournissent les réponses attendues. Tout cela doit donc permettre d'exploiter cette brochure aussi bien dans le cadre d'une préparation à l'Olympiade que dans celui du cours de mathématique dispensé dans les classes. Les Professeurs et leurs élèves tireront le plus grand profit de cette brochure utilisable pendant toutes les années de l'enseignement secondaire.
Les énoncés des problèmes proposés aux **finales** terminent cet ouvrage.

Olympiades

C. Festraets,

Voici les solutions de quatre problèmes MIDI de la finale de l'Olympiade Mathématique Belge de 1998.

1. *Dans une école, un tournoi d'échecs a été organisé pour les élèves de 3ème et de 4ème ; deux élèves de 3ème année y ont pris part. Chaque participant a joué exactement une fois contre chaque autre. Le gagnant de chaque partie marquait* 1 *point et le perdant n'en marquait pas ; en cas de partie nulle, chacun des deux adversaires marquait* 1/2 *point. A la fin du tournoi, les élèves de 3ème ont, ensemble, marqué* 8 *points. Les élèves de 4ème ont tous obtenu le même nombre entier de points.*

Quel est ce nombre et combien y avait-il de participants de 4ème ? (Si plusieurs solutions existent, les mentionner toutes.)

Solution de François FOUCART, Athénée Emile Bockstael, Bruxelles.

Soient x le nombre d'élèves de 4ème participant au tournoi et n le nombre total de participants.

On a $n = x + 2$.

Soit m le nombre de matches. Si chaque participant rencontre une fois chaque adversaire, on a

$$m = \frac{n(n-1)}{2} = \frac{x^2 + 3x + 2}{2}.$$

Dans tous les cas, on donne un point par match.

Soit y le nombre de points de chaque élève de 4ème, on a donc

$$y = \frac{m - 8}{x} = \frac{x^2 + 3x - 14}{2x}.$$

Comme x et y appartiennent à $\mathbb{N}$,

$$\frac{x+3}{2} - \frac{7}{x} \in \mathbb{N}.$$

1. Soit x est impair (pour obtenir un nombre pair de demis) et diviseur de 7 ;

   pour $x = 1$, on a $y = -5$, à rejeter car $y \in \mathbb{N}$,

   pour $x = 7$, on a $y = 4$.

2. Soit x est pair et alors $\frac{x+3}{2}$ est un nombre impair de demis et la fraction $\frac{7}{x}$ doit se simplifier en un nombre impair de demis. Ceci n'est possible que si x vaut 2 ou 14 ;

   pour $x = 2$, on a $y = -1$, à rejeter car $y \in \mathbb{N}$,

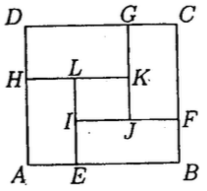
   pour $x = 14$, on a $y = 8$.

On a donc deux possibilités :

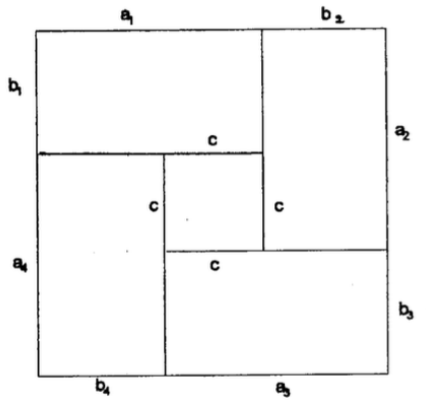
– 7 joueurs de 4ème ont chacun obtenu 4 points (on peut vérifier que dans ce cas, 36 matches ont été joués et à chaque partie, chaque joueur a obtenu $\frac{1}{2}$ point) ;
– 14 joueurs de 4ème ont chacun obtenu 8 points (on peut vérifier que dans ce cas, 120 matches ont été joués, 7 joueurs de 4ème ont gagné 8 parties dont deux contre les joueurs de 3ème, les 7 autres joueurs de 4ème ont gagné 7 parties et fait match nul contre les 2 joueurs de 3ème et les 2 joueurs de 3ème jouant l'un contre l'autre ont fait match nul).

2. *Dans la figure représentée ci-dessous (de manière peu précise), $AELH$, $BFIE$, $CGJF$ et $DHKG$ sont quatre rectangles de même aire et $IJKL$ est un carré.*

Quelle est la nature du quadrilatère $ABCD$?



Solution de Ming-Koon HSU, Lycée Michel Rodange, Luxembourg.



Ce quadrilatère doit au moins être un rectangle puisqu'il possède quatre angles droits.

Donc $a_1 + b_2 = b_4 + a_3$ et $b_1 + a_4 = a_2 + b_3$.

Démontrons d'abord que le carré de côté c doit se trouver "au milieu".

Si, par exemple, il se trouve "au coin inférieur gauche" de sorte que $b_4 < b_2$, alors

- si $a_4 < a_2$, on a $a_4 b_4 < a_2 b_2$, ce qui contredit l'hypothèse (aire $AELH$ = aire $CGJF$) ;
- si $a_4 > a_2$, on a $b_1 < b_3$ car $b_1 + a_4 = a_2 + b_3$, $b_4 < b_2$ donne $a_3 > a_1$ car $a_1 + b_2 = b_4 + a_3$; d'où $a_1 b_1 < a_3 b_3$, ce qui contredit l'hypothèse (aire $DHKG$ = aire $BFIE$)

et il faut donc $a_4 = a_2$ et $b_4 = b_2$.

Dès lors, $b_1 = b_3$ et $a_1 = a_3$.

Nous savons aussi que

$$\begin{aligned} b_1 a_1 &= b_2 a_2 \\ b_1(b_4 + c) &= b_2(b_1 + c) \\ b_1(b_2 + c) &= b_2(b_1 + c) \\ b_1 b_2 + b_1 c &= b_1 b_2 + b_2 c \\ b_1 c &= b_2 c \\ b_1 &= b_2. \end{aligned}$$

Donc, $b_1 = b_2 = b_3 = b_4$ et $a_1 = a_2 = a_3 = a_4$ puisque $a_1b_1 = a_2b_2 = a_3b_3 = a_4b_4$.

Le quadrilatère est donc un carré.

3. *Lorsque, dans un aquarium, deux poissons d'une même espèce mais de couleurs différentes se rencontrent, ils changent de couleur, devenant tous deux, au hasard, de l'une des autres couleurs que peut prendre cette espèce.*

a) *Les tétrocampes peuvent être oranges, rouges, verts ou bleus. Si un aquarium contient initialement* 1 *tétrocampe orange, 9 tétrocampes rouges, 9 tétrocampes verts et 8 tétrocampes bleus, les rencontres successives peuvent-elles mener à ce que ces 27 tétrocampes deviennent tous d'une même couleur ?*

b) *Les hippodons peuvent être oranges, rouges ou bleus. Si un aquarium contient initialement 1 hippodon orange, 9 hippodons rouges et 8 hippodons bleus, les rencontres successives peuvent-elles mener à ce que ces 18 hippodons deviennent tous d'une même couleur ?*

Solution de Jean-Noël MONETTE, Collège du Sacré-Coeur, Charleroi.

a) Oui. Par exemple, 5 tétrocampes rouges croisent 5 verts et deviennent tous oranges, les 4 tétrocampes rouges restants en croisent 4 bleus et ils deviennent tous oranges, les 4 tétrocampes verts restants croisent les 4 bleus restants et ils deviennent oranges, le tétrocampe orange ne croise personne et les 26 autres sont devenus oranges.

b) Non. Pour que tous les poissons aient une même couleur, il faut parvenir à un même nombre de poissons dans deux couleurs différentes. Pour y arriver, il faut que les différences entre les nombres de poissons de couleurs différentes pris deux à deux soient multiples de 3 (par exemple, 10 rouges, 7 bleus, 1 orange : $10 - 7 = 3$, $7 - 1 = 6$, $10 - 1 = 9$). En effet, quand un poisson sort de chacune de 2 couleurs différentes, il y en a deux qui entrent dans la 3ème couleur. Les différences entre couleurs augmentent ou diminuent d'un multiple de 3.
Or ici, les différences sont $9 - 1 = 8$, $8 - 1 = 7$ et $9 - 8 = 1$. On ne pourra donc jamais arriver à une différence qui soit multiple de 3 et on ne pourra jamais avoir les 18 hippodons de la même couleur.

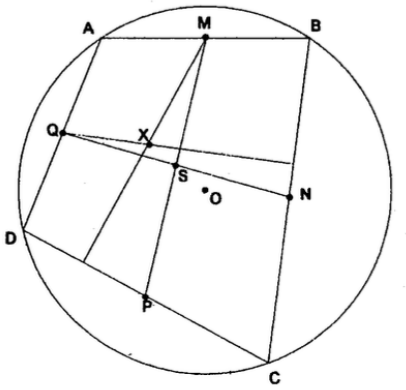
4. *Démontrer que, si un quadrilatère est inscrit à un cercle, les perpendiculaires abaissées du milieu de chaque côté sur le côté opposé sont concourantes.*

Solution.

Aucun élève n'a réussi à faire une démonstration complète. Vous trouverez ci-dessous la démonstration "officielle".

Ajoutons que 16 candidats (sur 38) n'ont pas lu attentivement l'énoncé, ont tracé les médiatrices de quatre côtés du quadrilatère et démontré plus ou moins laborieusement qu'elles se coupaient au centre du cercle circonscrit au quadrilatère!!!

Comme on peut supposer que les 38 élèves participant à la finale de l'OMB sont de bons, voire de très bons élèves (tout au moins en ce qui concerne les mathématiques), il est vraiment regrettable de constater qu'ils sont incapables de trouver une démonstration en géométrie.



Soient M, N, P, Q les milieux respectifs des côtés $[AB]$, $[BC]$, $[CD]$, $[DA]$ du quadrilatère et soit O le centre du cercle circonscrit.

$MNPQ$ est un parallélogramme (car $MN//AC//QP$ et $MQ//BD//NP$). Ses diagonales se coupent en S milieu de $[MP]$ et de $[NQ]$.

Menons de M la perpendiculaire sur CD et de Q la perpendiculaire sur BC. Ces deux droites se coupent en X. La symétrie centrale de centre S applique

- P sur M
- la droite OP sur sa parallèle XM
- N sur Q
- la droite ON sur sa parallèle à XQ

et donc applique X sur O.

Le point X est donc le symétrique de O par rapport à S.

Si on désigne par Y le point d'intersection des perpendiculaires menées de N et P sur AD et AB respectivement, Y est aussi le symétrique de O par rapport à S.

D'où $X = Y$ et les quatre droites sont bien concourantes.

. . . . . .

Voici à présent les énoncés des problèmes proposés à l'Olympiade Mathématique Internationale.

Les résultats de nos concurrents francophones ne sont pas fameux, pas de médaille cette année. Cependant, la Belgique garde sa place au milieu du classement par pays (39ème sur 78 pays présents) grâce, il faut le dire, à l'apport de points des concurrents néerlandophones.

Ces problèmes m'ont paru vraiment très difficiles. D'ailleurs, un seul étudiant (sur 419) a obtenu le maximum des points.

39ème Olympiade Internationale de Mathématique

Premier jour - Taïpei - 15 juillet 1998

Problème 1

Dans un quadrilatère convexe $ABCD$, les diagonales AC et BD sont perpendiculaires et les côtés opposés AB et DC ne sont pas parallèles. On suppose que le point P, intersection des médiatrices de AB et de DC, se trouve à l'intérieur de $ABCD$. Prouver que le quadrilatère $ABCD$ est inscriptible si et seulement si les triangles ABP et CDP ont même aire.

Problème 2

Une compétition regroupe a participants et b examinateurs, où $b \geqslant 3$ est un nombre entier impair. Chaque examinateur attribue à chaque participant une des mentions "réussi" ou "échoué". On suppose que le nombre k est tel que : pour deux examinateurs quelconques, leurs décisions coïncident pour au plus k participants. Prouver que

$$\frac{k}{a} \geqslant \frac{b-1}{2b}.$$

Problème 3

Pour tout entier n strictement positif, $d(n)$ désigne le nombre de diviseurs positifs de n (y compris 1 et n).

Trouver tous les entiers strictement positifs k pour lesquels il existe n tel que

$$\frac{d(n^2)}{d(n)} = k.$$

Temps accordé : quatre heures et demie.

Chaque problème vaut 7 points.

Deuxième jour - Taïpei - 16 juillet 1998

Problème 4

Trouver tous les couples (a, b) d'entiers strictement positifs tels que $ab^2 + b + 7$ divise $a^2b + a + b$.

Problème 5

Soit I le centre du cercle inscrit dans le triangle ABC. Ce cercle est tangent aux côtés BC, CA et AB du triangle, en les points K, L et M respectivement. La droite parallèle à MK passant par B coupe les droites LM et LK respectivement en R et S. Prouver que l'angle $\widehat{RIS}$ est aigu.

Problème 6

On considère toutes les applications f de l'ensemble N^* de tous les entiers strictement positifs dans lui-même vérifiant

$$f(t^2 f(s)) = s(f(t))^2, \quad \text{quels que soient } s \text{ et } t \text{ dans } N^*.$$

Déterminer la plus petite valeur possible de $f(1998)$.

Temps accordé : quatre heures et demie.

Chaque problème vaut 7 points.

Des problèmes et des jeux

C. Festraets,

J'ai reçu récemment une solution intéressante du problème 199 ; cette solution intéressera sans aucun doute certains de mes lecteurs.Il est à remarquer que cette solution et celle qui a été publiée dans le n° précédent de *Mathématique et Pédagogie*sont toutes deux basées sur la méthode de descente infinie.

Pythagore voit double problème n° 199 de M. et P. n° 115.

Trouver toutes les solutions du système

$$(S)\begin{cases} a^2+b^2=c^2 \\ b^2+c^2=d^2 \end{cases}$$

avec $a, b, c, d \in \mathbb{N}$.

Solution de J. FINOULST de Diepenbeek

Multipliant membre à membre les relations

$$\begin{aligned} c^2-b^2 &= a^2 \\ c^2+b^2 &= d^2 \end{aligned}$$

on trouve

$$\boxed{c^4-b^4=(ad)^2} \qquad (1)$$

Nous allons montrer que cette équation n'a pas de solution non triviale en nombres naturels.

Dans ce but, nous suivons le raisonnement de Oysteyn Ore dans son livre "Number Theory and its History", Mc Graw-Hill Book Company, inc., New York, 1948, où il démontre que l'aire d'un triangle primitif de Pythagore n'est jamais un carré (le terme "primitif" suppose que les nombres a, b et c avec $b^2+c^2=a^2$ sont premiers entre eux).

On sait que les côtés peuvent s'écrire

$$b=2mn, \qquad c=m^2-n^2, \qquad a=m^2+n^2.$$

L'aire de ce triangle est

$$A = \frac{1}{2}\, bc = mn(m^2 - n^2). \tag{2}$$

Dans l'hypothèse où A est un carré t^2,

$$mn(m-n)(m+n) = t^2.$$

Dans un triangle primitif, les nombres m et n sont premiers entre eux, l'un pair, l'autre impair. Il s'ensuit que les quatre nombres

$$m, \qquad n, \qquad m-n, \qquad m+n$$

sont premier entre eux, deux à deux.

Comme leur produit est un carré, chacun de ces nombres est un carré, d'où

$$m = u^2, \qquad n = v^2, \qquad u^2 - v^2 = p^2, \qquad u^2 + v^2 = q^2.$$

Il est clair que les nombres u, v, p et q sont premiers entre eux, deux à deux. En additionnant et soustrayant les deux dernières équations, on trouve

$$2u^2 = p^2 + q^2, \qquad 2v^2 = (q-p)(q+p). \tag{3}$$

Comme un des nombres m et n est pair et l'autre impair, u et v ont cette même propriété et donc p et q sont impairs. Cela prouve aussi que $q-p$ et $q+p$ sont pairs et la seconde égalité dans (3) nous permet d'écrire

$$v = 2w.$$

Et cette même égalité donne

$$2w^2 = \frac{q-p}{2}\,\frac{q+p}{2}. \tag{4}$$

Les deux facteurs du second membre sont premiers entre eux ; un diviseur commun diviserait leur somme q et leur différence p, mais p et q sont premiers entre eux.

Selon (4), un des facteurs du second membre est pair. Cela mène aux possibilités :

$$\frac{q-p}{2} = 2k^2, \qquad \frac{q-p}{2} = r^2$$

d'où

$$p = r^2 - 2k^2, \qquad q = r^2 + 2k^2$$

et

$$\frac{q-p}{2} = r^2, \qquad \frac{q+p}{2} = 2k^2$$

d'où

$$p = 2k^2 - r^2, \qquad q = 2k^2 + r^2.$$

En substituant ces paires de valeur de p et q dans la première égalité (3), on obtient dans les deux cas

$$u^2 = (r^2)^2 + (2k^2)^2.$$

On trouve ainsi un triangle du même type de côtés

$$r^2, \quad 2k^2, \quad u.$$

L'aire de ce triangle est

$$A_1 = \frac{1}{2}.r^2.2k^2 = w^2 = \left(\frac{1}{2}\, v\right)^2 = \frac{1}{4}\, n.$$

Cette aire est un nombre entier plus petit que l'aire A.

A partir de ce second triangle, on peut déduire un troisième, un quatrième, etc. dont les aires vont en décroissant. Comme l'aire est un entier > 1, cela mène à une contradiction.

L'hypothèse – l'aire d'un triangle (primitif ou non) de Pythagore est un carré – est à rejeter.

Considérons finalement le triangle de Pythagore défini par $m = x^2$, $n = y^2$; ce triangle aurait selon (2) une aire

$$x^2y^2(x^4 - y^4) = x^2y^2z^2 = (xyz)^2.$$

Cette aire serait donc un carré parfait, contrairement à ce qui précède.

Et il s'ensuit immédiatement que l'équation

$$x^4 - y^4 = z^2$$

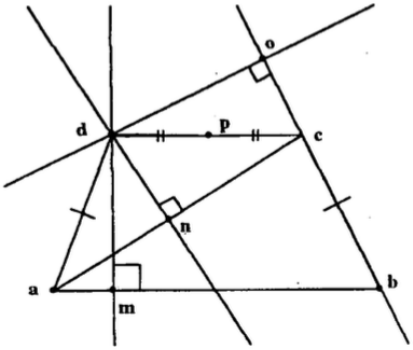
n'a pas de solutions en nombre entiers.

La relation (1) étant de cette forme, on conclut que le système proposé n'a pas de solution non triviale.

Trapèze problème n°202 de M. et P. n°116.

On considère le trapèze isocèle abcd où ab//cd. Les points m et n sont les pieds des perpendiculaires abaissées de d sur ab et sur ac respectivement. Démontrer que si m, n et p milieu de [cd] sont colinéaires, alors l'angle acb est droit.

Solution de L. COLOT de Bouge.



Le trapèze $(abcd)$ étant isocèle, cela entraîne que ses angles opposés (a et c, d et b) sont supplémentaires. On peut donc en déduire que ce trapèze est inscriptible.

Le cercle circonscrit à ce trapèze est aussi le cercle circonscrit au triangle (abc). De plus, le point d appartient aussi à ce cercle.

Par d, considérons la perpendiculaire do à cb (avec o sur cb).

Les points m, n et o sont alignés (droite de Simpson ou de Wallace). Par conséquent, les quatre points m, n, p et o sont alignés.

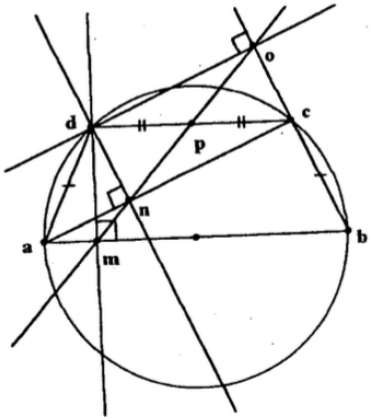
Dans les triangles rectangles (doc) et (cdn), p étant le milieu de l'hypoténuse $[dc]$, les médiales $[po]$ et $[pn]$ ont une longueur qui est la moitié de celle de l'hypoténuse $[dc]$: donc $|po| = |pn| = |dp| = |pc|$.

Le point p est donc centre de symétrie du quadrilatère convexe $(docn)$: celui-ci est donc un parallélogramme.

Comme dans ce parallélogramme l'angle n est droit, ce parallélogramme est un rectangle et l'angle nco est droit, ce qui permet de conclure que l'angle acb est droit également.

Il en résulte que la base $[ab]$ du trapèze est un diamètre du cercle circonscrit au trapèze.

La figure est donc la suivante :



Bonnes solutions de N. BERCKMANS de Waterloo, J. FINOULST de Diepenbeek, J. JANSSEN de Lambermont, B. LOISEAU de Mouscron, A. PATERNOTTRE de Boussu, H.-J. SEIFFERT de Berlin et M. VERHEYLEWEGHEN de Bruxelles.

Nous progressons problème n°203 de M. et P. n°116.

Déterminer toutes les valeurs positives du paramètre m pour que les solutions non négatives de l'équation

$$\cos((18m-3)x) = \cos((14m+5)x)$$

forment une progression arithmétique.

Solution de N. BERCKMANS de Waterloo.

Pour m positif et $m \neq 2$, les solutions de cette équation sont

$$x = \frac{k\pi}{2(m-2)} \quad \text{et} \quad x = \frac{k\pi}{16m+1}$$

où $k \in Z$.

Remarquons que si $m = 2$, alors $S = R$ et donc $m = 2$ est à exclure de la réponse.

1er cas : $2 < m$**.**

On remarque que l'on a

$$0 < \frac{1}{16m+1} < \frac{1}{2(m-2)}.$$

Pour que les solutions non négatives forment une progression arithmétique, il faut que

$$\exists k \in N_0 \text{ tel que } \frac{k}{16m+1} = \frac{1}{2(m-2)}.$$

On en déduit

$$\boxed{m = \frac{4k+1}{2(k-8)}.}$$

La condition $2 < m$ implique $\boxed{8 < k}$.

2nd cas : $0 \leqslant m < 2$**.**

On aura

$$0 < \frac{1}{16m+1} \leqslant \frac{1}{2(2-m)} \quad \text{si} \quad m \geqslant \frac{1}{6}.$$

2.1 $\frac{1}{6} \leqslant m < 2$.

Pour que les solutions non négatives forment une progression arithmétique, on doit avoir :

$$\exists k \in N_0 \text{ tel que } \frac{k}{16m+1} = \frac{1}{2(2-m)}.$$

On en déduit

$$\boxed{m = \frac{4k-1}{2(k+8)}.}$$

La condition $\frac{1}{6} \leqslant m < 2$ est vérifiée $\boxed{\forall k \in N_0}$.

2.2 $0 \leqslant m \leqslant \frac{1}{6}$.

Pour que les solutions non négatives forment une progression arithmétique, on doit avoir

$$\exists k \in N_0 \text{ tel que } \frac{k}{2(2-m)} = \frac{1}{16m+1}.$$

On en déduit

$$\boxed{m = \frac{4-k}{2(2k+1)}.}$$

La condition $0 \leqslant m \leqslant \frac{1}{6}$ est vérifiée si $\boxed{k \in \{1,2,3,4\}}$.

Réponse :

$$\boxed{\begin{array}{rcll} m & = & \dfrac{4k+1}{2(k-8)} & \text{où } k \in N_0 \text{ et } k > 8, \\ m & = & \dfrac{4k-1}{2(k+8)} & \text{où k} \in N_0, \\ m & = & \dfrac{4-k}{2(8k+1)} & \text{où } k \in \{1,2,3,4\}. \end{array}}$$

Je n'ai eu qu'une seule autre solution complète, avec toutefois une petite erreur, $16m+1$ a été remplacé par $16m+2$ dans l'une des solutions de l'équation.

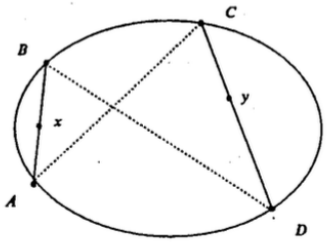
Prenons le bus problème n°204 de M. et P. n°116.

La carte d'une ville a la forme d'un polygone convexe. Chaque diagonale du polygone est une rue et les points d'intersection de ces diagonales sont des carrefours (les côtés du polygone ne sont pas des rues et ses sommets ne sont pas considérés comme des carrefours). Des lignes d'autobus parcourent la ville. Chaque ligne va de l'extrémité d'une rue à l'autre extrémité et a un arrêt à chaque carrefours et à chacune de ses deux extrémités. A chaque carrefour, deux rues seulement se coupent et au moins l'une d'elles possède une ligne d'autobus. Montrer que l'on peut aller de tout carrefour à tout autre carrefour en effectuant au plus deux changements d'autobus.

Solution de B. LOISEAU de Mouscron.

Remarque : l'hypothèse que le polygone est convexe garantit que toutes les diagonales sont entièrement intérieures au polygone : ce fait reste implicite tout au long du problème.

Considérons deux carrefours x et y et, pour chacun de ces carrefours, une rue passant par ce carrefour et desservie par une ligne d'autobus. Si par hasard ces deux rues sont confondues, on peut passer d'un carrefour à l'autre en prenant un seul bus ; si ces deux rues ont un point d'intersection, que ce soit un point intérieur au polygone (carrefour) ou un sommet du polygone, on peut passer d'un carrefour à l'autre en prenant deux bus : un premier du premier carrefour à ce point d'intersection, un second du point d'intersection au second carrefour. Enfin, si ces deux rues ne se coupent pas à l'intérieur du polygone, on peut étiqueter leurs sommets A, B, C, D de façon que la première rue soit AB et la seconde CD et que $ABCD$ soient rencontrés dans cet ordre sur le contour du polygone :



(le polygone est figuré par une ellipse : c'est une image. Mais en réalité, le problème est essentiellement topologique, et on pourrait en donner un énoncé en termes d'arcs qui ne supposerait ni que les rues sont droites, ni que la ville est convexe).

Alors, les rues BD et AC se coupent nécessairement en un point intérieur au polygone, donc en un carrefour, et l'une des rues AC et BD est nécessairement desservie par un bus. Par symétrie, on peut supposer que c'est BD. On peut donc passer du premier carrefour x au second y en prenant le bus de x à B, puis un second bus de B à D et un troisième enfin de B à y.

Il est donc possible de passer de tout carrefour à tout autre en changeant au plus deux fois de bus.

Remarque : Si on retire l'hypothèse que par chaque carrefour passent exactement deux rues, il faut supposer que de toutes les rues passant par un carrefour donné, toutes sauf au plus une sont desservies par un bus. Le raisonnement ci-dessus reste alors valable.

Bonne solution de J. JANSSEN de Lambermont.

* * **

Les solutions des problèmes suivants doivent me parvenir avant le 1er avril 1999.

211. Quelle puissance !

Soit $n = (1998^{1998})^{1998}$.

Désignons par s la somme des chiffres de n, par t celle de s et par u celle de t. Que vaut u ?
(problème proposé par Marc LARDINOIS de Haine-St-Pierre).

212. Soyons constructifs

On donne dans le plan trois cercles concentriques et tels que le plus grand des trois rayons est inférieur à la somme des deux autres. Construire un triangle équilatéral dont chaque sommet appartient à un cercle différent.

213. Plus ou moins

La suite (a_n) est définie par

$$\begin{aligned} a_1 &= a_3 = 1 \\ a_2 &= a_4 = -1 \\ a_n &= a_{n-1}.a_{n-2}.a_{n-4}, \quad n \in \{5, 6, 7, \ldots\} \end{aligned}$$

Déterminer a_{1999}.

13^{e} Championnat International des Jeux Mathématiques et Logiques

C. Rédaction,

LES PARTICIPANTS

Tous les élèves de votre établissement peuvent disputer les quarts de finale scolaires. Sept participants au minimum par catégorie sont requis pour organiser un quart de finale. Si ce minimum n'est pas atteint, les élèves concourent individuellement.

Même s'il a participé à des quarts de finale scolaires, un élève peut néanmoins participer individuellement à l'aide des bulletins se trouvant dans *Math-Jeunes* pour les catégories CM, C1, C2 et L1. Des bulletins sont également disponibles auprès de la FFJM–B.P. 157 - 7700 MOUSCRON.

LES CATEGORIES SCOLAIRES

CL : écoliers de 5ème et 6ème primaire
C1 : élèves de 1ère secondaire
C2 : élèves de 2ème et 3ème secondaire
L1 : élèves de 4ème, 5ème et 6ème secondaire

LE CALENDRIER

Phase 1 : quarts de finale jusqu'au 31 janvier 1999
Phase 2 : demi-finales régionales le 13 mars 1999
Phase 3 : finales régionales le 15 mai 1999
Phase 4 : finale internationale fin août ou début septembre 1999

LES MODALITES

Il vous suffit de **demander un dossier de participation à :**

FFJM - B.P. 157 - 7700 MOUSCRON

Vous trouverez ci-dessous, classés par ordre de difficulté croissante, 12 énoncés de quarts de finale fermés (confidentiels), *pour les collègues du fondamental une autre série de 9 énoncés*, qui servent à l'épreuve de qualification, fixée au même moment pour tout votre établissement, épreuve à l'issue de laquelle vous corrigez les réponses (fournies également).

Vous choisissez à votre guise : date, nombre de sujets, coefficients, durée, mode de qualification, etc.

Une seule contrainte : les résultats doivent parvenir à la FFJM le 31 janvier 1999 au plus tard. Vous ne renvoyez aucune réponse à la FFJM. Seul le bordereau de retour qui donne la liste des qualitifés de l'établissement est à retourner.

LE CENTRE DE DEMI-FINALE

Voici la liste provisoire des centres belges : Ath, Bruxelles, Liège, Mouscron, Namur, Thuin et Virton.

Les personnes inscrites sur le bordereau doivent pouvoir se déplacer le samedi 13 mars 1998 dans le centre de demi-finale choisi. A ce stade de l'épreuve, la cotisation FFJM doit être acquitée : catégorie CM : 175F, catégorie C1 et C2 : 350F et catégorie L1 : 450F.

La finale belge est déjà dotée de nombreux prix.

QUESTIONNAIRE

Le concours ne vous intéresse pas ?

Utilisez ces jeux-problèmes pour une activité collective dans vos classes, vos cours d'éducation mathématique, clubs mathématiques ...

Veuillez attendre la date limite du 31 janvier 1999 pour les utiliser à votre guise.

Le concours vous intéresse ?

Demandez le dossier gratuit de participation à :

FFJM - B.P. 157 - 7700 MOUSCRON
ou par **télécopie au 056 33 14 53**
ou par **courrier électronique : andre.parent@ping.be**

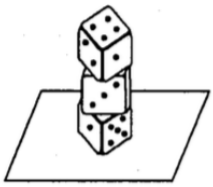
Vous y trouverez une information plus détaillée, les questions (celles ci-dessous), les réponses, le bordereau de retour ...

Dans la revue *Math-Jeunes*, vous trouverez le questionnaire individuel de participation. N'oubliez pas d'abonner ou de réabonner vos élèves.

13ème Championnat International des Jeux Mathématiques et Logiques 1/4 de finale Collèges et Lycées (sujets confidentiels)

1. LES TROIS DÉS

Sur un dé "normal", la somme des points portés par deux faces opposées est toujours égale à 7.
Sur une table, Dédé a construit un tour avec trois dés normaux. La face du dessus du dé du dessus porte un 4.
Combien vaut la somme des points portés par les 5 faces cachées (entre elles et par la table) ?



2. LA JOURNEE DE MONSIEUR TÊTENLAIR

Monsieur Têtenlair, qui est représentant, habite sur la Nationale 7. Aujourd'hui, en partant de chez lui, il a fait un premier parcours, d'une traite, de 53 km pour voir un client. Il a ensuite effectué un second trajet de 79 km, puis un troisième de 27 km, et, enfin, un quatrième de 9 km. M. Têtenlair sait qu'il fait ces quatre trajets, les seuls de sa journée, sur la Nationale 7, mais, très étourdi,il ne sait plus dans quel sens il a effectué chacun d'eux. "De toutes façons, pense-t-il en calculant, je suis au maximum à 168 km de chez moi !". **A combien de kilomètres est-il de chez lui, au minimum ?**

3. LE GRAND TRIANGLE

A l'aide de petits triangles noirs, on veut recouvrir un triangle blanc de dimensions deux fois plus grandes. Les triangles noirs étant disposés comme sur le dessin, on doit les déplacer en les faisant glisser **sans les retourner**, mais ils peuvent se chevaucher.
Combien de triangles noirs faudra-t-il utiliser, au minimum, pour que toute la surface du triangle blanc soit recouverte ?

4. CONCOURS

Huit concurrents, élèves d'une classe de 6ème et d'une classe de 5ème, participent au concours "Je sais tout" organisé dans leur collège. Les huit concurrents obtiennent des nombres de points tous différents, le vainqueur ayant obtenu 8 points et le dernier 1 point. Les élèves de 6ème ont totalisé 18 points. Dans le classement, entre deux élèves de 6ème, il y avait toujours au moins un élève de 5ème. Par contre, Jean et Dominique étaient les seuls élèves de 5ème à ne pas être séparés par un élève de 6ème.
Combien de points Jean et Dominique ont-ils obtenu, à eux deux ?

5. LES TRIANGLES

Combien de vrais triangles non superposables, même avec retournement, peut-on tracer en utilisant trois points quelconques du réseau ci- contre ?
Note : un "vrai" triangle est un triangle non aplati.

6. LES TROIS NOMBRES

Trois nombres à deux chiffres sont écrits avec les six chiffres 2, 3, 4, 5, 6 et 7. La somme des trois nombres est égale à 171, et la différence entre les deux plus petits est égale à 11.
Trouvez les trois nombres. Donnez-les dans l'ordre croissant.

7. SAULE QUI PEUT !

Un magnifique saule est planté à l'intérieur d'un terrain carré. La somme des distances du saule à deux des côtés du terrain est égale à 100 mètres, tandis que la somme des distances du saule aux deux autres côtés du terrain est égale à 120 mètres.
Quelle est l'aire du terrain ? On donnera la réponse en m^2.

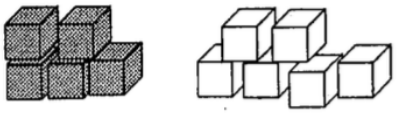
8. LE JEU DES CHIFFRES

Julien et Bernard jouent à un jeu qui consiste à écrire un nombre à plusieurs chiffres. Le joueur qui commence écrit le premier chiffre à gauche, obligatoirement différent de 0, et les joueurs jouent ensuite alternativement en écrivant les chiffres suivants à droite du chiffre ou des chiffres déjà écrits. Ils doivent respecter les règles suivantes :
• après un 9, on peut écrire n'importe quel chiffre
• après un chiffre inférieur à 9, on doit écrire un chiffre plus grand
• chacun des chiffres doit apparaître au plus 3 fois dans le nombre.
Le premier joueur ne pouvant écrire aucun chiffre a perdu. Julien commence.

Quel chiffre doit-il écrire pour être sûr de gagner, quel que soit le jeu de Bernard ? Répondez 0 si vous pensez qu'une stratégie gagnante n'existe pas pour le premier joueur.

9. LES CUBES

Mathias dispose de 120 petits cubes : 80 cubes entièrement bleus et 40 cubes entièrement blancs. Il veut utiliser ces 120 cubes et de la colle pour construire un grand parallélépipède rectangle. La surface du parallélépipède sera entièrement formée de faces des petits cubes.



Combien de faces visibles de petits cubes, au minimum, seront bleues ?

10. PARTAGE DU CERCLE

Sur un cercle de longeur 24 cm, on place des points de façon que les arcs de cercle compris entre deux points consécutifs mesurent tous 2 cm ou 3 cm. De plus, en joignant deux points quelconques, on n'obtient jamais un diamètre du cercle.
Les points placés sur le cercle déterminent combien d'arcs de cercle de longueur 3 cm ?

11. PARTAGE DU TRIANGLE

On a partagé un rectangle en 5 triangles rectangles semblables. Si deux de ces 5 triangles ne sont pas disjoints, leur partie commune est soit un sommet, soit un côté entier qui est alors l'hypoténuse d'un des deux triangles et un côté de l'angle droit dans l'autre. L'aire du plus petit triangle est égale à 2 cm^2. **Quelle est l'aire du rectangle ?**

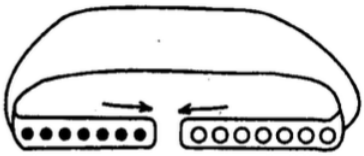
12. DIVISEURS

Le produit de tous les diviseurs d'un certain nombre entier naturel supérieur à 1 est égal à la puissance 5ème de ce nombre.
Combien de diviseurs ce nombre possède-t-il ?

13ème Championnat International des Jeux Mathématiques et Logiques 1/4 de finale Scolaires

1. LA CASQUETTE A JOJO

Jojo est sympa, il m'a prêté sa casquette ! Mais comme il a la grosse tête, il a fallu que je décale les picots d'un cran pour la régler à ma taille. Une fois ce décalage effectué, le nombre de trous libres était devenu plus petit que le nombre de trous occupés par les picots.



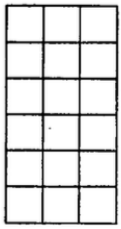
Avant que Jojo ne prête sa casquette, combien y avait-il de picots dans les trous ?

2. LES NOMBRES DE MATHIAS

Mathias s'amuse à écrire tous les nombres décimaux possibles utilisant un chiffre 1, un chiffre 2, un chiffre 3 et une virgule, à l'exception de tout autre signe. **Combien Mathias peut-il écrire de nombres différents ?**

3. LE RECTANGLE À SECRETS

Mathilde et Mathias ont inventé un moyen de communication secret. L'expéditeur écrit le texte dans le rectangle, ligne par ligne, puis le recopie colonne par colonne, en séparant les lettres en trois "mots" de six lettres. Celui qui reçoit le message a vite fait de décoder. Mathilde, pendant le contrôle de mathématiques, a oublié sa calculette. Angoissée, elle adresse à Mathias le message suivant :



"S T I U O E E F S A R ? P O Q T Z".

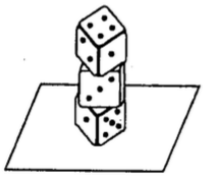
Quelle doit être la réponse de Mathias (en clair) **?**

4. DECOUPAGE

Les trois figures ci-contre sont formées de treize petits carrés. **Partagez la première de ces trois figures en deux morceaux**, de telle sorte qu'en réarrangeant différemment ces deux morceaux, on puisse reconstituer les deux autres figures.

5. LES TROIS DÉS

Sur un dé "normal", la somme des points portés par deux faces opposées est toujours égale à 7.
Sur une table, Dédé a construit un tour avec trois dés normaux. La face du dessus du dé du dessus porte un 4.
Combien vaut la somme des points portés par les 5 faces cachées (entre elles et par la table) ?

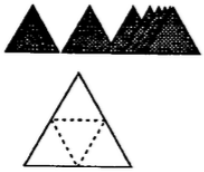


6. LA JOURNEE DE MONSIEUR TÊTENLAIR

Monsieur Têtenlair, qui est représentant, habite sur la Nationale 7. Aujourd'hui, en partant de chez lui, il a fait un premier parcours, d'une traite, de 53 km pour voir un client. Il a ensuite effectué un second trajet de 79 km, puis un troisième de 27 km, et, enfin, un quatrième de 9 km. M. Têtenlair sait qu'il fait ces quatre trajets, les seuls de sa journée, sur la Nationale 7, mais, très étourdi,il ne sait plus dans quel sens il a effectué chacun d'eux. "De toutes façons, pense-t-il en calculant, je suis au maximum à 168 km de chez moi !". **A combien de kilomètres est-il de chez lui, au minimum ?**

7. LE GRAND TRIANGLE

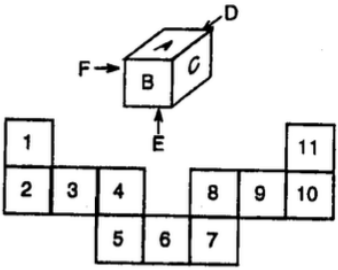
A l'aide de petits triangles noirs, on veut recouvrir un triangle blanc de dimensions deux fois plus grandes. Les triangles noirs étant disposés comme sur le dessin, on doit les déplacer en les faisant glisser **sans les retourner**, mais ils peuvent se chevaucher.



Combien de triangles noirs faudra-t-il utiliser, au minimum, pour que toute la surface du triangle blanc soit recouverte ?

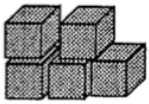
8. EMBALLEZ LE CUBE !

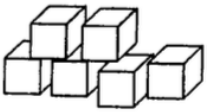
On veut emballer le cube représenté à droite à l'aide de la bande de papier dessinée en-dessous. Pour cela, on applique le carré 1 de la bande sur la face A du cube, puis le carré 2 sur la face B, le carré 3 sur la face C, et on continue ainsi, sans jamais froisser ni déchirer la bande de papier, un carré de papier s'appliquant toujours exactement sur une face du cube.



Quelle est la somme des carrés appliqués sur la face E ?

9. LES PETITS CUBES





Mathilde dispose de 27 petits cubes : 13 cubes entièrement rouges et 14 cubes entièrement blancs. Elle veut utiliser ces 27 petits cubes et de la colle pour construire un grand cube. La surface du grand cube sera formée de 54 faces de petits cubes.

Sur ces 54 faces, combien, au minimum, seront rouges ?