Bulletin
432

Bimestriel

Janvier-Février 2001

L'ARITHMÉTIQUE

Association des Professeurs de Mathématiques
de l'Enseignement Public

APMEP

de la maternelle à l'université...

Association des Professeurs de Mathématiques de l'Enseignement Public

26, rue Duméril, 75013 Paris

Tél. 01.43.31.34.05 – Fax : 01.42.17.08.77

Mél : apmep@apmep.asso.fr – internet : http://www.apmep.asso.fr

Directeur de publication : Rémi Bellœil
Rédactrice en chef : Christiane Zehren
Rédacteur en chef adjoint : Henri Bareil
Mise en page : Roger Cuppens
Impression : Louis Jean, 05003 Gap Cédex
Dépôt légal : 51-Janvier 2001
Numéro d'enregistrement à la commission paritaire : 52819

ISSN 0240-5709

Sommaire

Éditorial

Dans nos classes

Dossier : L'arithmétique (Première partie)

Pour chercher et approfondir

Vie de l'association

Dessin de couverture : Tapisserie L'Arithmétique (extrait). Vers 1520. Musée du Moyen-Âge. Cluny. © Photo RMN. J.-G. Berizzi.

Pour notre *Bulletin*

Notre publication, l'un des outils de communication de l'APMEP, est toujours bien vivante, l'abondance de vos propositions d'articles en témoigne. Nous vous invitons à continuer à nous faire parvenir vos textes, nombreux et variés, si possible courts (pas plus de quinze pages, s'il vous plaît !), ils sont le cœur même de notre expression associative.

Vous connaissez à ce sujet nos us et coutumes :

• Chaque article, après lecture par trois collègues, est soumis à l'approbation de la Commission du Bulletin qui décide de l'accepter avec ou sans modifications de votre part, ou de le refuser.

• Les auteurs sont régulièrement tenus informés de ces décisions ainsi que du délai de publication, qui peut être assez long pour ménager l'équilibre des différents numéros. En cas d'acceptation, aucun tiré à part n'est envoyé.

• Les articles doivent être dactylographiés, avec version papier en quatre exemplaires dont un original portant très précisément l'adresse de l'auteur. Les disquettes (Mac ou PC) sont les bienvenues. Pour nous faciliter la saisie, le texte doit être frappé au kilomètre si possible en Word 5, police Times 10 (sinon enregistrer le fichier en format Texte). Les figures de largeur maximum 12cm doivent être fournies en fichier séparé (un par figure) si possible aux formats EPS ou TIF.

• Pour chaque article, vous voudrez bien résumer en cinq lignes maximum les idées essentielles, et donner un aperçu de vos motivations, et du public visé. Faute de résumé, l'article ne pourra en tout cas pas être publié.

• Les manuscrits non publiés ne sont pas retournés.

Nous sommes par ailleurs, comme vous, toujours sensibles à l'image publique des mathématiques et de leur enseignement. Soyez nombreux à y être attentifs, et à nous faire parvenir vos coupures de presse, vos remarques sur telle ou telle émission, où l'on aura parlé de mathématiques.

Les mathématiques sont vivantes, leur enseignement aussi.
À nous de le montrer !

Vos envois sont à adresser à
Christiane Zehren
Les Sylphides A2
Place Fontaine-du-Temple
06100 Nice
Téléphone et Fax : 04.93.84.32.36
E-mail : czehren.apmep.@wanadoo.fr

Bonne année, bon siècle, bon millénaire

Rémi Belloeil

À l'aube du nouveau millénaire, je formule pour tous les enseignants de Mathématiques les meilleurs vœux pour le développement de notre discipline et de son enseignement.

Alors que l'Informatique vient de naître depuis moins d'un siècle et a connu un développement rapide au point de revendiquer son indépendance vis-à-vis des Mathématiques pour devenir la science du traitement de l'information, personne ne doute qu'elle nous apportera de nouveaux problèmes et de nouveaux développements.

Déjà la **Géométrie** est devenue dynamique par l'utilisation de nouveaux logiciels. Les figures sont animées en conservant les caractéristiques données aux objets tandis que l'on peut déplacer séparément les points « libres » sur lesquels l'utilisateur a fondé sa figure. Ceci devient banal, et beaucoup d'établissements scolaires, de la maternelle à l'université, disposent de tels logiciels ou en disposeront très prochainement. Pourtant, c'est une révolution pour la Géométrie qui passe d'une conception statique à une conception interactive et dynamique. Les transformations imposées par l'utilisateur mettent davantage en évidence les invariants de la figure(1).

Pour les générations futures, le concept de Géométrie sera basé sur une expérience différente de la nôtre.

L'enseignement de l'**Analyse** est aussi au croisement de plusieurs questions. De quelle maîtrise du calcul numérique et littéral, écrit ou mental, doit disposer l'élève du troisième millénaire ? Dans quelle mesure celle-ci est-elle nécessaire pour anticiper les résultats fournis par les calculatrices ou ordinateurs ? Et dans quelle mesure le développement des notions d'Analyse peut-il s'appuyer sur ces outils ? À quel moment faut-il définir l'ensemble des nombres réels et comment ? Et conjointement comment introduire la notion de limite et quelle définition en donner ? Quand faut-il travailler sur les encadrements de nombres et de fonctions ? Faut-il aborder dès le secondaire les notions de structures d'algèbre ?

---

(1) Je renvoie le lecteur au dossier « Géométrie » des précédents numéros et au compte rendu d'atelier décrit dans le bulletin 428, page 327. Bien entendu, le pédagogue qui utilise ces logiciels doit être conscient de la structure intime de leur fonctionnement. La lecture de la brochure « Faire de la Géométrie avec Cabri-Géomètre » est bien utile pour cela. Simple retour de l'histoire : Cabri-Géomètre est né dans le Laboratoire de Structures discrètes et Didactique (rebaptisé depuis Laboratoire Leibniz) de Grenoble.

Quelle place dans l'enseignement doit-on donner à l'**Arithmétique** ? à la **Logique** ? aux **Probabilités** et à la **Statistique** ? Quels liens avec les autres disciplines ? Nous voyons tous que les réponses à ces questions ont évolué et évolueront encore. De la même façon, le sens même de l'expression « **faire des Mathématiques** » peut évoluer. Selon les personnes, les niveaux d'enseignement et les époques, l'équilibre est variable entre démontrer, conjecturer, appliquer des techniques, expérimenter… Enfin, nous nous demandons aussi comment intéresser les élèves à ces problématiques.

Voilà beaucoup de questions pour ce nouveau millénaire. Qui y répondra ? Nous, les enseignants de mathématiques, regroupés dans l'A.P.M.E.P., avec l'aide de la commission de réflexion sur l'enseignement des mathématiques(2) à laquelle nous participons – et dont j'ai le plaisir de vous annoncer la poursuite de ses travaux pour au moins deux ans – et, au delà, les décideurs politiques et le peuple qui les nomme et les révoque ! Puis encore chacun de nous dans son travail quotidien.

Aussi je nous souhaite à nouveau à tous un bon millénaire, riche en développements mathématiques, en concepts nouveaux, en rebondissements sur des notions anciennes, en bref un millénaire qui ajoute une nouvelle pierre à l'histoire de l'humanité.

Rémi Belloeil

(2) Appelée aussi commission Kahane.

Quelques exercices ayant pour thème l'Euro

Jean-Gullaume Cuaz

Cet article regroupe quelques exercices ayant pour thème un sujet d'actualité : l'Euro. Ces exercices, que chaque professeur pourra adapter à sa classe, traitent du problème des arrondis ; ils sont regroupés par niveau (collège, lycée), et utilisent un large éventail d'outils mathématiques et de méthodes.

On trouvera des exercices sur :
– la question des arrondis : le poids des décimales, la règle d'arrondi au cent le plus proche, les écarts en résultant, les conversions successives, les opérations et les arrondis,
– le maniement des inégalités et des encadrements relatifs à l'Euro.

Chaque exercice est constitué d'un énoncé, de son corrigé ou d'indications de réponses s'il y a lieu et d'un complémént d'information, pouvant servir de base à un exposé général sur l'Euro.

1. Arrondis du taux de conversion

Comme on le voit, le taux de conversion euro-franc comporte six chiffres significatifs. Ceci est assez ennuyeux pour qui veut effectuer une conversion « de tête ». L'exercice suivant peut faire prendre conscience des conséquences d'un arrondi du taux de conversion.

Exercice n° 1

Public concerné : Classe de quatrième.

Un défi à lancer à un élève : Tu me donnes 400 francs et je te rends la valeur d'un euro par jour, et ce pendant 2 mois (30 + 31 = 61 jours). Acceptes-tu ?

Indication de réponse : Vous l'aurez compris, selon que 1 € = 6,55957 F ; 6,5 F ; 6,6 F, l'un ou l'autre des protagonistes sera perdant de … 3 Francs. C'est peu, me direz-vous, mais imaginez un élève susceptible !

Prolongement : Prise en compte du fait qu'une (petite !) erreur d'arrondi réitérée un grand nombre de fois (voir par exemple Exercice n° 5) peut avoir de très lourdes conséquences.

Exercice n° 2 : Une conversion rapide et efficace grâce au calcul mental

Objectif : Donner un procédé rapide de conversion et en évaluer la fiabilité.

Compétences exigées : Factorisation, fractions (somme, inverse), calcul algébrique. Valeur absolue, approximations. Utilisation de la calculatrice.

Public concerné : Première question : classe de troisième. Deuxième et troisième question : classe de seconde.

Pour convertir en euros une somme donnée en francs, il faut la diviser par 6,559 57. Il existe un moyen mental d'obtenir une bonne approximation de cette conversion : « Pour convertir des francs en euros, il faut ajouter à la somme à convertir sa propre moitié, et diviser le tout par 10 ».

Exemple : conversion de 50 francs en euros :

On ajoute à 50 sa moitié 25, soit 50 + 25 = 75, et on divise le tout par 10. On obtient 7.5 € (le résultat exact est 7.62 €).

1) Soit x la somme en francs à convertir en euros. Décrire les étapes du calcul de l'énoncé. Peut-on justifier l'intérêt de ce calcul ?

2) Donner une majoration, en fonction de la somme à convertir, de l'erreur relative commise en utilisant cette méthode.

3) Pour quelles valeurs de la somme à convertir est-on sûr que cette méthode de conversion fournira une valeur approchée à 0,10 euros ?

Indications de réponse : Si on appelle x la somme en francs à convertir en euros, le procédé mental nous fait donc calculer $\dfrac{x+\dfrac{x}{2}}{10}=\dfrac{3x}{20}=\dfrac{x}{\dfrac{20}{3}}$. Justification : 6,55957 est « proche » de $\dfrac{2}{3}$ de 10 (i. e. $\dfrac{20}{3}$).

L'erreur relative commise en utilisant cette méthode peut s'exprimer en fonction de x par $\left|\dfrac{3x}{20}-\dfrac{x}{6{,}559\,57}\right|\leq|x|\times 2{,}45\times 10^{-3}$. On a alors $|x|\times 2{,}45\times 10^{-3}<0{,}1 \Leftrightarrow x<40{,}84\text{ F}$.

Exercice n° 3

Objectifs et compétences : Maniement des inégalités, résolution d'inéquation. Établissement d'un encadrement. Multiplication/division des termes d'un encadrement par un même nombre.

Public concerné : classe de seconde.

Se trouvant au Supermarché, M. Untel constate que tous les prix sont affichés en euros. Malheureusement pour lui, il ne se souvient pas du taux de conversion exact. Il se souvient cependant que la valeur d'un euro est comprise entre 6 et 7 francs.

1) On appelle t la valeur en francs d'un euro. Traduire sous forme d'un encadrement l'hypothèse de l'énoncé.

2) M. Untel dispose de 200 F sur lui. Si 1 = 6 F, combien de livres de poche à 6 euros peut-il acheter au maximum ? Même question avec 1 € = 7 F.

3) M. Untel achète deux boites de conserve à 2 euros chacune. Donner un encadrement de la valeur en francs de ce dernier achat.

4) Ayant acheté trois livres de poches et deux boites de conserve, M. Untel arrive à la caisse et s'apprête à payer avec son billet de 200 F.

a) Donner un encadrement en francs de la monnaie qui lui sera rendue.

b) (facultatif) Donner un encadrement en euros de la monnaie qui lui sera rendue.

2. Arrondis des conversions

Exercice nº 4

Objectifs : la mise en place de la règle de l'arrondi « au cent le plus proche ».

Compétences exigées : Travaux sur les décimaux. Règle d'arrondis. Utilisation de la calculatrice.

Public concerné : classes de collège.

Rappel de la règle de conversion :
Pour transformer en francs une somme en euros, il faut la multiplier par 6.559 57.
Pour transformer en euros une somme en francs, il faut la diviser par 6.559 57.

Le problème est que le résultat de ces opérations comporte un grand nombre de décimales, et il se peut même que la division ne s'arrête jamais !

1) Combien de décimales sont nécessaires à l'expression d'un prix en euros ?
(on pourra mettre cette question en rapport avec l'exercice nº 1).

2) *Pour aboutir à des valeurs ne comportant que deux chiffres après la virgule les cents ou centimes (appelées cents ou centimes), on applique la règle suivante : Si le troisième chiffre après la virgule est inférieur à 5, on arrondit au cent ou centime inférieur. S'il est égal ou supérieur à 5, on arrondit au cent ou centime supérieur.*

Appliquer cette règle pour convertir 10 F en Euros. Même question avec 35 F et 60 F.

3. Arrondis et opérations

Exercice nº 5

Objectif : Sensibiliser les élèves au fait que la somme des arrondis n'est pas égale (en général) à l'arrondi de la somme.

Compétences exigées : Règle de l'arrondi au cent le plus proche (utilisation possible d'un tableur).

Public concerné : Tout public.

Considérons le relevé bancaire suivant, en francs :

Nature	Crédit	Débit	Solde
Solde précédent			1 000,00
Salaire	10 300,00		11 300,00
Chèque		125,00	11 175,00
CB		235,00	10 940,00
Remise	300,00		11 240,00
Chèque		325,00	10 915,00
CB		190,00	10 725,00
Remise	700,00		11 425,00
		Solde en F	11 425,00

1) Convertir le nouveau solde en euros.

2) Reprendre le relevé en effectuant les opérations suivantes :
– convertir en euros chaque valeur en francs (arrondir à chaque fois en utilisant la règle d'arrondi au cent le plus proche),
– Effectuer les opérations entre ces valeurs en euros.

3) Quel écart constate-t-on entre l'arrondi de la somme et la somme des arrondis ?

Indication de réponse :
Si nous effectuons la conversion en euros du nouveau solde, nous obtenons :

$\frac{11\,425}{6{,}559\,57} \approx 1\,741{,}730\,02$ ... arrondi à 1741,73 €.

Si en revanche, on effectue la conversion en euros de chaque ligne de calcul, et que l'on effectue les opérations entre ces conversions en euros, on obtiendra :

Nature	Crédit	Débit	Solde
Solde précédent			152,45
Salaire	1 570,22		1 722,67
Chèque		19,06	1 703,61
CB		35,83	1 667,78
Remise	45,73		1 713,51
Chèque		49,55	1 663,96
CB		28,97	1 634,99
Remise	106,71		1 741,70
		Solde en F	1 741,70

L'écart est de 0,03 € à l'arrivée, soit 0,196 787... F, c'est à dire un écart de 20 centimes !

Prolongement : Prise en compte du fait qu'une opération d'arrondi réitérée des milliers de fois peut avoir de très lourdes conséquences. À mettre en relation avec l'exercice n° 1.

4. Le problème de la double conversion

Exercice n° 6

Objectifs : Travailler sur les écarts résultant de conversions et d'arrondis successifs.

Compétences exigées : Maniement des nombres décimaux et des inégalités. Établissement d'un encadrement. Valeur absolue, approximations. Résolution d'inéquation.

Public concerné : classe de seconde.

Convertir 10,01 F en euros, en appliquant la règle officielle de l'arrondi.

Puis reconvertir cette somme en francs, toujours en appliquant la règle officielle de l'arrondi.

Quelle somme a-t-on gagné dans l'opération ?

Généralisons le problème :

On appelle t la valeur d'un euro en franc. On a ainsi $t = 6.559\ 57$.

On suppose que l'on part d'une somme x en francs, et qu'on la convertit en euros. Notons y la contre-valeur en euros, comportant plus de 2 décimales (*a priori* !).

1) Exprimer y en fonction de x et t.

2) Donner un encadrement de la somme $A(y)$ obtenue en appliquant à y la règle d'arrondi au cent le plus proche.

3) Supposons que cette somme $A(y)$ soit reconvertie en francs. On note z la valeur en francs trouvée (avec *a priori* plus de 2 décimales !) Exprimer z en fonction de t et de $A(y)$.

4) Donner un encadrement de la somme $A(z)$ obtenue en appliquant à z la règle d'arrondi au centime le plus proche.

5) Donner un encadrement en fonction de t de l'écart absolu entre z et x observable après cette double conversion.

6) Quelle est la somme maximale que l'on peut gagner (ou perdre) dans une telle opération ? À partir de quelle valeur de t pourrait-on voir apparaître des écarts de 4 centimes ?

7) Recommencer l'exercice en partant cette fois-ci d'une somme en euros, convertie en francs, puis reconvertie en euros. Que constate-t-on ? Quelle explication peut-on fournir ?

Indications de réponses et prolongements : Cas d'une double conversion franc → euro → franc.

1) $y = \frac{x}{t}$.

2) Étant donné qu'en appliquant la règle d'arrondi au cent le plus proche, on peut provoquer un écart d'au plus 0,005 €, on a :

$$\frac{x}{t} - \frac{1}{200} < \mathrm{A}(y) < \frac{x}{t} + \frac{1}{200}.$$

3) $z = t \times \mathrm{A}(y)$.

4) À partir des questions 2) et 3), on établit que

$$x - \frac{t}{200} < z < x + \frac{t}{200},$$

donc :

$$x - \frac{t}{200} - \frac{1}{200} < \mathrm{A}(z) < x + \frac{t}{200} + \frac{1}{200},$$

c'est à dire :

$$x - \frac{t+1}{200} < \mathrm{A}(z) < x + \frac{t+1}{200}.$$

5) L'inégalité précédente donne :

$$\frac{t+1}{200} < \mathrm{A}(z) - x < \frac{t+1}{200}.$$

6) On en déduit que

$$\left|\mathrm{A}(z) - x\right| < \frac{t+1}{200}.$$

Finalement la différence maximale entre la somme de départ x et la somme d'arrivée après double conversion est de $\frac{t+1}{200}$ francs. Pour t = 6,559 57, cet écart représente 0,038 F (3,8 centimes). Mais comme x et z sont des nombres entiers de centimes, la différence est au maximum de 3 centimes (dans un sens ou dans un autre).

Pour constater un écart de 4 centimes, il faudrait que $\frac{t+1}{200} \geq 0{,}04$, c'est à dire que $t \geq 7$. À partir d'1 € = 7 F, on pourrait constater des écarts supérieurs à 4 centimes.

7) On suppose qu'on part d'une somme x en euros, et qu'on la convertit en francs. Notons y la contre-valeur en francs, comportant plus de 2 décimales (*a priori* !)
Exprimer y en fonction de x et t : $y = t \times x$.

Encadrement de la somme A(y). Étant donné qu'en appliquant la règle d'arrondi au centime le plus proche, on peut provoquer un écart d'au plus 0,005 francs, on a :

$$tx - \frac{1}{200} < \mathrm{A}(y) < tx + \frac{1}{200}.$$

Supposons que cette somme A(y) soit reconvertie en euros. On note z la valeur en euros trouvée, avec *a priori* plus de 2 décimales. En fonction de t et de A(y), on a : $z = \frac{A(y)}{t}$.

Encadrement de la somme A(z). À partir des questions précédentes, on établit que

$$x - \frac{1}{200 \times t} < z < x + \frac{1}{200 \times t},$$

donc :

$$x - \frac{1}{200t} - \frac{1}{200} < A(z) < x + \frac{1}{200 \times t} + \frac{1}{200},$$

c'est à dire :

$$x - \frac{t+1}{200t} < A(z) < x + \frac{t+1}{200 \times t}.$$

Encadrement en fonction de t de l'écart absolu entre z et x observable après cette double conversion :

$$|A(z) - x| < \frac{t+1}{200 \times t} < 5{,}763 \times 10^{-3}.$$

Lors d'une double conversion euro → franc → euro, on ne constate aucun écart dû aux arrondis. Ceci restera vrai tant que un euro vaudra plus d'un franc.

Exercice n° 7 : Conversions consécutives – idempotence

Objectifs : Composition d'applications. Évolution des erreurs d'arrondi lors de conversions successives.

Public concerné : Enseignement supérieur.

Remarque : on suppose les exercices précédents assimilés (surtout l'exercice n° 6).

Notons F l'ensemble des montants possibles en francs et E l'ensemble des montants possibles en euros (dans les deux cas, il s'agit de nombres réels multiples de 0,01).

On définit deux opérations :

ef : E → F qui convertit un montant en euros en un montant en francs,

et

fe : F → E qui convertit un montant en francs en un montant en euros,

Par exemple *ef*(x) = A(xt) et *fe*(y) = $A\left(\frac{y}{t}\right)$, où t est le taux de conversion (t = 6,559 57) et A est l'opération d'arrondi au centième le plus proche.

1) Démontrer que $ef \circ fe$ est idempotent.

2) Par quelle propriété sur les arrondis cela se traduit-il ?

Éléments de réponse :
Le problème est de savoir, comment se composent les applications *ef* et *fe*.
On a vu dans l'exercice n° 6 que $fe \circ ef$ était l'identité de E, c'est à dire $fe(ef(x)) = x$ pour tout x. Ceci est dû au fait que t est plus grand que 1.
En d'autres termes, *ef* est l'inverse à droite de *fe*, et donc *ef* est injective, et *fe* est surjective
En revanche, $ef \circ fe$ est différente de l'identité, l'écart pouvant atteindre 0,03 centimes.
Quand on convertit plus de deux fois, on fait par exemple $ef \circ fe \circ ef \circ fe \circ ef \circ fe$ (c'est à dire francs → euros → francs → euros → francs → euros → francs), on peut se dire que chaque $ef \circ fe$ va faire varier le montant d'au plus 3 centimes, et que si on n'a pas de chance, ces effets vont se cumuler pour atteindre dans ce cas 9 centimes.
Il n'en est rien, heureusement ; on peut en effet écrire :

$$ef \circ fe \circ ef \circ fe \circ ef \circ fe = ef \circ (fe \circ ef) \circ (fe \circ ef) \circ fe = ef \circ fe,$$

et donc l'écart sera au plus de 3 centimes, quel que soit le nombre de conversions successives. En d'autres termes, $ef \circ fe$ est idempotent (c'est à dire $(ef \circ fe)^2 = ef \circ fe$).

5) Les conversions entre monnaies européennes via l'euro (conversions unitaires croisées)

Pour une conversion franc-mark, par exemple, les textes officiels disent :
« *Il faut effectuer deux opérations consécutives puisqu'il n'y a plus de taux de change entre deux monnaies :*
Montant en francs/taux de conversion euro-franc = montant intermédiaire en euros.
Montant intermédiaire en euros × taux de conversion euro-mark = montant en marks.
Ce montant intermédiaire doit être arrondi à au moins trois décimales.
Le règlement prévoit que toute autre méthode qui produit les mêmes résultats peut être utilisée.
Commentaire : dans le cas de conversion unitaire croisée, la proposition de règlement est claire et suffisante ».

Il y a une ambiguïté qui réside dans la phrase : « *Ce montant intermédiaire doit être arrondi à au moins trois décimales.* »
En effet, on peut obtenir des résultats différents selon le nombre de décimales utilisées pour le montant intermédiaire.
Notons t le taux de conversion euro → franc et u le taux de conversion euro → deutschemark. On a $t = 6{,}559\,57$ et $u = 1{,}955\,83$.

Une somme x en francs est d'abord convertie en une somme $x_k = \mathrm{A}_k\left(\dfrac{x}{t}\right)$ en euros, où A_k est l'opération « arrondi au plus proche avec k décimales ». Puis x_k est convertie en $z_k = \mathrm{A}(x_k \times u)$ où $\mathrm{A} = \mathrm{A}_2$.
On a :

$$\left|x_k - \frac{x}{t}\right| < 0,5 \times 10^{-k}$$

et

$$|z_k - x_k \times u| < 0,005\,.$$

Finalement

$$\left|z_k - \frac{x}{t} \times u\right| < 0,5 \times (0,01 + u \times 10^{-k}) < 0,006$$

puisque $k \geq 3$ et $u < 2$.
Pour deux valeurs de k différentes, mettons 3 et 4, on a donc

$$|z_3 - z_4| \leq \left|z_3 - \frac{x}{t} \times u + \frac{x}{t} \times u - z_4\right| \leq \left|z_3 - \frac{x}{t} \times u\right| + \left|z_4 - \frac{x}{t} \times u\right| \leq 2 \times 0,006 = 0,012.$$

Comme ce sont des nombres entiers de pfennigs, la différence est au plus de 0,01 DM.
Cette différence est-elle vraiment possible ? Oui.

Par exemple, voici 5 exemples entre 0 F et 1 F :

Somme F	Arrondi euro 3 décimales	Reconversion Mark	Arrondi euro 3 décimales	Reconversion Mark	Différence entre les 2
0,05	0,008	0,02	0,0076	0,01	0,01
0,52	0,079	0,15	0,0793	0,16	–0,01
0,62	0,095	0,19	0,0945	0,18	0,01
0,72	0,11	0,22	0,1098	0,21	0,01
0,79	0,12	0,23	0,1204	0,24	–0,01

Augmenter le nombre de chiffres du résultat intermédiaire ne fait que raréfier le problème, sans l'éliminer. Pour être complètement explicite, le règlement aurait dû imposer le nombre de décimales à utiliser pour le résultat intermédiaire, ou mieux, donner une procédure sans arrondi intermédiaire : c'est facile, il suffit de faire la multiplication d'abord, c'est à dire de calculer $w = x \times u$ de manière exacte (7 décimales), puis $z = \mathrm{A}\left(\frac{w}{t}\right)$, mais w est alors dans une unité qui n'existe pas, ce qui doit être difficile à faire accepter aux financiers.

Zéro, un nombre à part

Frédéric Junier & François Soulard(*)

Introduction

Notre expérience d'élèves ainsi que diverses observations dans notre pratique nous ont permis de savoir que les élèves sont souvent confrontés à des problèmes avec zéro. En effet zéro est un cas « à part » dans les pratiques du calcul numérique simple ainsi que dans la représentation des nombres.

Voici quelques exemples simples illustrant la particularité de zéro : zéro n'a pas de signe ou bien les deux à la fois. C'est l'élément neutre additif, l'absorbant multiplicatif, on ne peut diviser par zéro et la puissance 0 d'un nombre vaut toujours 1 sauf pour 0^0 justement. Son rôle apparaît contradictoire : il dénombre l'ensemble vide mais ce sont les puissances de 10 c'est à dire le nombre de « 0 » qui permettent l'écriture des grands nombres.

Dans des classes de quatrième et de seconde, à partir d'une enquête sur la représentation sociale de zéro, et d'un QCM contenant opérations élémentaires et équations du premier degré, nous essayons de comprendre les difficultés et les intérêts qu'apporte la spécificité de zéro. De l'enquête on dégage sept représentations et des deux QCM on propose quatre théorèmes-élèves.

Ces études sont faites en classes de quatrième et de seconde à l'occasion de notre mémoire professionnel à l'IUFM.

I. Enquête sur zéro

Auprès de nos élèves, nous avons fait une même enquête afin de repérer les diverses représentations sociales de zéro au moyen de questions variées et ouvertes (annexe 1). En fonction des expressions et du vocabulaire utilisés nous avons essayé de regrouper en famille les différents types de représentations auxquelles faisaient référence les élèves. Nous avons dégagé ainsi sept représentations. Vingt-cinq élèves de quatrième et 36 de seconde ont répondu à l'enquête.

1) Zéro élément de la comptine

Type de réponse d'élèves : « Zéro c'est le chiffre (le nombre) avant 1 ». Cette définition de zéro est proposée par cinq élèves de quatrième, mais aucun en seconde.

Lorsque les enfants jouent avec les nombres par exemple lors d'un compte, zéro est le premier ou le dernier élément.

2) Zéro référentiel ou frontière entre le positif et le négatif

Type de réponse d'élèves : « Zéro est utilisé pour la température », « Zéro est le nombre qui sépare les nombres positifs et négatifs », « Zéro est entre –1 et 1 ».

(*) stagiaires à l'IUFM de Lyon en 98/99.

Sept élèves de seconde définissent zéro comme frontière contre deux en quatrième. De plus à la question n° 5 : « Qu'y a-t-il en dessous de zéro ? », six élèves de quatrième répondent « rien » ou ne répondent pas. En seconde, seulement deux élèves ne répondent pas. Ce constat laisse à penser que les élèves de seconde seraient plus familiers avec cette représentation.

3) Zéro dénombre un ensemble vide (notion discrète)

Type de réponse d'élèves : « Il y a zéro pomme dans le panier ». Nous supposons que les élèves sont habitués dans le primaire à dénombrer des ensembles finis (on compte sur ses doigts…). Quand on les a enlevés un à un jusqu'au dernier, on dit alors qu'il y a « zéro objets ».

Pour expliquer l'apparition tardive du zéro (question n° 9), certains élèves proposent l'argument de l'inutilité de zéro dans les dénombrements quotidiens (par exemple le cheptel).

4) Zéro nombre qui représente le rien (notion continue)

Type de réponse d'élèves : « Il y a zéro litre de jus de pomme dans la bouteille ». Cette notion continue a été retrouvée chez les élèves pour lesquels zéro représente le vide, le rien. Pour ces même élèves, le fait que zéro représente le rien explique son apparition tardive. Les secondes citent plus souvent cette notion continue que les quatrièmes (43% contre 20%). Nous expliquons cette différence par une plus grande habitude au quotidien des nombres décimaux rationnels et réels pour les élèves de seconde. On peut remarquer aussi que l'utilisation des nombres décimaux au collège est très souvent liée aux unités de mesure : longueur, poids, volume… et un objet qui pèse 0 gramme n'a pas d'aspect concret.

5) Zéro chiffre utile dans l'écriture des nombres

Type de réponse d'élèves : « Zéro sert à écrire de grands nombres », « Zéro n'est pas un nombre, c'est un chiffre ».

Ici les justifications et les exemples donnés par les élèves sur l'utilité de zéro sont exclusivement en référence au chiffre (écrit avec d'autres chiffres évidemment). Zéro n'est pas un nombre en tant que tel, mais c'est seulement un symbole pour construire des nombres.

6) Zéro symbole qui s'écrit comme un rond, un ovale

Type de réponse d'élèves : « Zéro c'est rond comme un œuf ».

Ces réponses sont plutôt rares mais nous ont frappés car pour ces quelques élèves, la définition de zéro se réduit à la manière de l'écrire.

Peut-être y a-t-il un rapport pour les élèves avec l'expression qu'ils utilisent souvent : « zéro sert à arrondir » (question n° 8).

7) Zéro note synonyme de sanction ou d'échec

Type de réponse d'élèves : « Zéro est inutile pour la notation », « Zéro est un inconvénient quand on a 0/20 ». La fréquence de ces réponses nous a questionnés sur le vécu des élèves quant à la notation.

Conclusion de l'enquête :

Suivant les représentations, il y a des différences dans les réponses entre les quatrièmes et les secondes. Par exemple, on remarque que les élèves de quatrième répondent que zéro est pair plus facilement que les secondes. Cela est sûrement dû à la représentation « référentiel » plus fréquemment utilisée par les secondes mais qui n'aide pas pour la parité, alors qu'en quatrième la représentation la plus utilisée est celle de la comptine (l'alternance pair/impair de la comptine aide à affirmer que zéro est pair).

On retrouve très fortement l'idée que zéro est un chiffre qui sert à écrire non seulement les nombres mais surtout « les grands nombres » (avec beaucoup de zéros…). La notion de zéro comme nombre à part entière est rare. Ceci explique peut-être le malaise de certains élèves face à un résultat d'équation égal à zéro : « Je n'ai pas trouvé de solution ».

On retrouve historiquement la nécessité du zéro-chiffre dans l'écriture des nombres et des grands nombres et la difficulté qu'il a eue à apparaître comme un nombre intervenant dans les calculs.

II. QCM d'opérations arithmétiques avec zéro (Annexe 2)

Ce premier QCM (annexe 1-b) contient des calculs élémentaires avec zéro (les quatre opérations et les puissances). Pour chaque question, les élèves avaient le même choix de réponses : *1 ; -1 ; 0 ; 1/3 ; 3 ; -3 ; impossible.*

Nous avons analysé les réponses à trois niveaux : d'abord pour un même élève en détectant les différences d'erreurs entre des questions apparemment similaires (par exemple $3 + 0$ et $0 + 0$ ou bien 0×3, 3×0 et 0×0…). Ensuite en repérant les erreurs les plus fréquentes en quatrième puis en seconde. Enfin, le dernier type d'analyse a été de comparer les résultats seconde/quatrième en essayant d'expliquer les différences les plus nettes entre les deux niveaux. Nous avons dégagé ainsi quatre règles ou « théorèmes-élèves » qui nous semblaient synthétiser les différentes attitudes des élèves face aux calculs :

Zéro élément neutre :

« *Zéro ne change rien dans un calcul* ».

Nous attendions pour les opérations $0 + 0$, $0 + 3$, $3 + 0$ et $0 - 0$ 100% de bonnes réponses. En classe de quatrième, sur 25 élèves, quatre répondent impossible pour le calcul $0 + 0$, et huit pour $0 - 0$. À l'opération $3 / 0$, 29% des élèves donnent le résultat égal à 3. En seconde, seulement 2 élèves sur 36 proposent cette réponse. Un quart des élèves de quatrième écrivent $0 / 3 = 3$, $(-3)^0 = -3$, $0 \times (0 - 1) = -1$ et $3^0 = 3$. Ces réponses ont été retrouvées chez seulement un élève de seconde. La règle du zéro élément neutre semble être plus présente chez les élèves de quatrième. Enfin, on retrouve le même type d'observation avec les calculs $0/0$ et 0^0 qui gênent plus facilement les élèves de quatrième que les secondes. Nous l'expliquons par ce raisonnement : « *Ne rien changer à quelque chose qui ne change rien est impossible !* ».

Zéro absorbant :

« *Tout devient nul quand zéro intervient* ».

En quatrième, pour les équations 3/0 et 0/0, les élèves donnent le résultat égal à zéro dans respectivement 50% et 75% des cas. Les égalités $3 - 0 = 0$, $3^0 = 0$ sont également souvent proposées par les élèves. En seconde, le résultat zéro est proposé par 14% des élèves pour le calcul 3/0.

On pourrait résumer ainsi « *Quand zéro n'est pas neutre il est absorbant* ». Cette notion d'élément absorbant est beaucoup plus marquée pour les élèves de quatrième.

Zéro dénombre l'ensemble vide :

« *Il est impossible d'enlever des éléments à un ensemble vide* ».

Exemple : en quatrième pour le calcul 0 – 3, 25% des élèves répondent 3, 0 ou impossible, cette question ne pose pas de problème aux secondes. Nous pensons ici que les élèves utilisent les représentations « Zéro dénombre l'ensemble vide » ou « Zéro représente le rien ». Ceci pose des problèmes notamment pour la soustraction (par exemple en enlevant les éléments un à un d'un ensemble de pommes dans un panier).

Zéro danger :

« *Il faut se méfier quand il y a zéro, ce n'est pas comme d'habitude* ».

Cette prudence est surtout acquise par les élèves de seconde qui par leur vécu d'élèves semblent être trop prudents dans les calculs contenant zéro et cela a des conséquences : 0/3 est impossible dans 32% des cas en seconde contre 17% en quatrième.

On peut remarquer que, alors que les trois premiers théorèmes-élèves sont plus marqués pour les élèves de quatrième, le dernier semble plus affirmé en classe de seconde.

III. QCM d'équations avec zéro

Dans cette deuxième série de questions (annexe 1-c) on demandait aux élèves de déterminer toutes les valeurs de *x* possibles vérifiant l'égalité donnée. Ils avaient le choix entre les réponses suivantes : *x = 1 ; x = -1 ; x = 0 ; x = 1/3 ; x = 3 ; x = -3 ; pas de solution ; tout nombre x est solution ; tout nombre x sauf « x = 0 » est solution.* Nous n'avons pas employé le mot équation car le chapitre équation n'avait pas été étudié en quatrième.

La comparaison quatrième/seconde nous paraissait particulièrement intéressante. En effet, les quatrièmes ne pouvaient déterminer les réponses que par une démarche par essai/erreurs. Ils ne pouvaient pas faire appel à des méthodes de résolution qu'ils n'avaient pas encore apprises.

Nos hypothèses concernant les résultats étaient en faveur de meilleures performances pour la classe de seconde. Il a été surprenant de constater que cette hypothèse n'a pas toujours été confirmée. En effet, voici, les résultats principaux :

À l'équation $0/x = 1$, 48% des élèves de quatrième répondent qu'il n'y a pas de solution contre seulement 38% en classe de seconde.

À l'équation $x/0 = 3$, 46% des élèves de quatrième répondent qu'il n'y a pas de solution contre 77% en classe de seconde.

Aux équations $0x = 0$; $0x = 3$; $3x = 3$; $1/x = 0$ et $3/x = 0$, les résultats sont équivalents en quatrième et en seconde.

À noter, qu'en quatrième 54% des élèves répondent correctement à l'équation $0x = 0$ c'est à dire « tout x est solution » ce qui signifie qu'ils envisagent bien la possibilité de plusieurs solutions à une équation. Nous pensions qu'ils procéderaient par tâtonnement ce qui les inciterait à s'arrêter dès qu'ils auraient trouvé une solution, ce qui n'a pas été le cas.

Dans tous ces calculs, les quatrièmes font certainement un lien direct entre l'équation donnée et le résultat : j'essaie telle valeur, je regarde si ça marche, puis j'essaie d'autres valeurs. En seconde beaucoup peuvent appliquer des « recettes » sans voir si cela convient dans l'équation donnée. On peut noter que la baisse de performances dans un apprentissage nouveau est un phénomène fréquent car souvent il faut renoncer au savoir empirique précédent avant de pouvoir acquérir un savoir nouveau et peut-être que les secondes sont encore dans cette phase creuse de l'apprentissage.

Du QCM nous retenons que les élèves de quatrième donnent beaucoup de sens à zéro mais leurs références font souvent appel au primaire (notamment pour la division). Les secondes sont davantage prudents dans les résultats où intervient zéro (dans le calcul ou le résultat).

Annexe 1 : enquête et QCM.

a) Enquête sur zéro

Le but de cette enquête est de savoir ce que zéro représente pour les gens dans la vie courante. Voici quelques exemples de questions posées :

1. Donner deux exemples où zéro est un avantage, un inconvénient.
2. Est-ce que zéro est un nombre ?
3. Donner des exemples où zéro est utilisé, puis où zéro est inutile.
4. Essayer d'expliquer ce qu'est zéro à quelqu'un qui n'en a jamais entendu parler.
5. Qu'y a-t-il en dessous de zéro ?
6. Est-ce que zéro a une valeur ? Pourquoi ?
7. À votre avis zéro est-il pair ou impair ?
8. Zéro sert-il à quelque chose ? Donner un ou deux exemples.
9. Quand les hommes ont commencé à utiliser les chiffres ils n'utilisaient pas le chiffre zéro et ils ont mis très longtemps à s'en servir. À votre avis pourquoi ?
10. Pourriez-vous vous passer de zéro dans la vie courante ? Pourquoi ?

b) QCM d'opérations arithmétiques sur zéro

Ce QCM contient des calculs élémentaires avec zéro (les quatre opérations et les puissances). Pour chaque question, les élèves avaient le même choix de réponses : 1 ; –1 ; 0 ; 1/3 ; 3 ; –3 ; impossible.

1) $0+0=$
2) $0+3=$
3) $3+0=$
4) $0-0=$
5) $0-3=$
6) $3-0=$
7) $0\times 3=$
8) $3\times 0=$
9) $0\times 0=$
10) $3^0=$
11) $0^3=$
12) $(-3)^0=$
13) $\dfrac{0}{3}=$
14) $\dfrac{3}{0}=$
15) $\dfrac{0}{0}=$
16) $3\times(1-1)=$
17) $(1-1)^2=$
18) $\dfrac{1}{3}-\dfrac{2}{6}=$
19) $0\times(0-1)=$
20) $0^0=$

c) QCM d'opérations arithmétiques sur zéro

Dans cette deuxième série de questions on demandait aux élèves de déterminer toutes les valeurs de x qui vérifiaient l'égalité donnée. Ils avaient le choix entre les réponses suivantes : $x=1$; $x=-1$; $x=0$; $x=1/3$; $x=3$; $x=-3$; pas de solution ; tout nombre x est solution ; tout nombre x sauf “ $x=0$ ” est solution.

1) $3-x=0$
2) $3+x=0$
3) $0+x=0$
4) $0-x=0$
5) $0\times x=0$
6) $0\times x=3$
7) $3\times x=0$
8) $3\times x=3$
9) $\dfrac{0}{x}=1$
10) $\dfrac{x}{0}=3$
11) $\dfrac{0}{x}=0$
12) $\dfrac{1}{x}=0$
13) $\dfrac{3}{x}=0$
14) $\dfrac{x}{3}=0$

Annexe 2

Nous avons fait *a priori* pour constituer notre QCM un inventaire des erreurs connues ou supposées de nos élèves. À partir de là chaque calcul se voit proposer une première et une deuxième réponse attendues (par exemple pour la question « 0 – 3 = », nous pensions que la majorité des élèves de quatrième répondraient –3 et une partie 3, les résultats obtenus confirment notre analyse sauf pour 3 élèves).

Attention, nous parlons en pourcentage et ce sont des classes de 25 et 36 élèves ce qui signifie que 12% représente 3 ou 4 élèves.

Classe de second

Questions	1^{re} réponse attendue	2^{e} réponse attendue	Réponse la plus fréquente	Pourcentage	Réponses suivantes	Pourcentage
$0 + 3 =$	3		3	100%		
$3 + 0 =$	3		3	100%		
$0 - 0 =$	0		0	93%	impossible	7%
$0 - 3 =$	–3		–3	97%	0	
$3 - 0 =$	3		3	93%	–3	
$0 \times 3 =$	0		0	100%		
$3 \times 0 =$	0		0	100%		
$0 \times 0 =$	0		0	93%	impossible	7%
$3^0 =$	1	0	1	77%	impossible 0 3	10% 10% 3%
$0^3 =$	0	impossible	0	93%	impossible	7%
$(-3)^0 =$	1	–1	–1	33%	1 0 impossible –3	22% 19% 19% 7%
$\frac{0}{3} =$	0	–3	0	68%	impossible	32%
$\frac{3}{0} =$	impossible	3	impossible	62%	3 0	24% 14%
$3 \times (1 - 1) =$	0		0	89%	3 –3	7% 4%
$0 \times (0 - 1) =$	0		0	86%	–1	14%
$0^0 =$	1	impossible	0	48%	1 impossible	45% 7%

Classe de quatrième

Questions	1^{re} réponse attendue	2^{e} réponse attendue	Réponse la plus fréquente	Pourcentage	Réponses suivantes	Pourcentage
$0 + 0 =$	0		0	92%	impossible	8%
$0 + 3 =$	3		3	100%		
$3 + 0 =$	3		3	100%		
$0 - 0 =$	0		0	87,5%	impossible	12,5%
$0 - 3 =$	–3	3	–3	75%	3 0 impossible	12,5% 4% 8,5%

Questions	1re réponse attendue	2e réponse attendue	Réponse la plus fréquente	Pourcentage	Réponses suivantes	Pourcentage
$3-0=$	3		3	87,5%	0	12,5%
$0\times 3=$	0	3	0	96%	0	4%
$3\times 0=$	0	3	0	87,5%	3	12,5%
$0\times 0=$	0		0	87,5%	impossible	12,5%
$3^0=$	1	3	1	33%	3 impossible 0	25% 25% 17%
$0^3=$	0	3	0	75%	impossible autres	12,5% 12,5%
$(-3)^0=$	–1	1 ou –3	–3	46%	impossible 0 1 autres	17% 17% 8% 12%
$\frac{0}{3}=$	0	impossible	0	46%	3 impossible autres	17% 17% 10%
$\frac{3}{0}=$	impossible	0	0	50%	3 impossible autres	29% 12,5% 8,5%
$\frac{0}{0}=$	impossible	1	0	75%	impossible	25%
$3\times(1-1)=$	0		0	71%	3 autres	21% 8%
$(1-1)^2=$	0	1	0	83%	impossible autres	8% 9%
$\frac{1}{3}-\frac{2}{6}=$	0	1/3	0	71%	3 autres	8% 21%
$0\times(0-1)=$	0	–1	0	71%	–1 impossible autres	13% 8% 8%
$0^0=$	0	impossible	0	54%	1 impossible autres	21% 17% 8%

Annexe 3

QCM d'équations avec zéro : Tableau des résultats attendus et obtenus

Les élèves avaient la question : donner toutes les valeurs possibles de x qui vérifient les égalités quivantes.

Classe de quatrième

Questions	1re réponse attendue	2e réponse attendue	Réponse la plus fréquente	Pourcentage	Réponses suivantes	Pourcentage
$3-x=0$	3		3	80%	autres	20%
$3+x=0$	–3	3	–3	50%	pas de sol. autres	30% 20%
$0+x=0$	0		0	87%	tout x autre	8% 4%
$0-x=0$	0	tout x	0	80%	pas de sol. autres	8% 12%
$0\times x=0$	1	tout x	tout x	54%	0 autres	37% 9%
$0\times x=3$	3	pas de solution	pas de solution	80%	3 autres	8% 12%
$3\times x=0$	0		0	62%	pas de sol. autres	21% 13%
$3\times x=3$	1	0	1	92%	autres	8%
$\frac{0}{x}=1$	pas de solution	0	pas de solution	48%	1 –1 0 autres	24% 12% 8% 8%
$\frac{x}{0}=3$	pas de solution	3	pas de solution	46%	3 –3 autres	38% 8% 8%
$\frac{0}{x}=0$	1	tout x tout x sauf zéro	0	67%	tout x 3 autres	19% 11% 3%
$\frac{1}{x}=0$	1	0 pas de solution	0	48%	pas de sol. 1 –1 autres	20% 16% 8% 8%
$\frac{3}{x}=0$	pas de solution	0	0	44%	pas de sol. 3 –3 autres	20% 16% 8% 12%
$\frac{x}{3}=0$	0	3	0	36%	pas de sol. 1 3 –1 autres	28% 12% 12% 8% 4%

Classe de seconde

Questions	1re réponse attendue	2e réponse attendue	Réponse la plus fréquente	Pourcentage	Réponses suivantes	Pourcentage
$\frac{3}{x}=0$	pas de solution		pas de solution	64%	$x=3$ $x=0$ tout x sol. $x=-3$ tout $x\neq 0$	9% 9% 9% 4% 4%
$0\times x=0$	tout x solution	$x=1$	tout x solution	63%	$x=0$ pas de sol.	34% 3%
$0\times x=3$	pas de solution		pas de solution	78%	$x=3$ $x=-3$	13% 9%
$3\times x=0$	$x=0$		$x=0$	70%	$x=-3$ pas de sol. tout x sol. $x=3$	15% 8% 4% 4%
$3\times x=3$	$x=1$		$x=1$	93%	$x=0$	7%
$\frac{0}{x}=1$	pas de solution	$x=0$	pas de solution	38%	$x=1$ $x=0$ tout $x\neq 0$	29% 24% 9%
$\frac{x}{0}=3$	pas de solution		pas de solution	77%	tout x sol. $x=0$ $x=3$	11% 8% 4%
$\frac{0}{x}=0$	tout x solution	tout x sauf zéro	tout x solution	50%	$x=0$ pas de sol. tout $x\neq 0$ $x=-1$	27% 11% 8% 4%
$\frac{1}{x}=0$	pas de solution	$x=0$	pas de solution	40%	$x=0$ $x=1$ $x=-1$ tout $x\neq 0$	28% 16% 12% 4%
$\frac{x}{3}=0$	$x=0$	$x=3$	$x=0$	52%	pas de sol. $x=-3$ tout x sol. $x=3$ $x=1/3$	28% 8% 4% 4% 4%

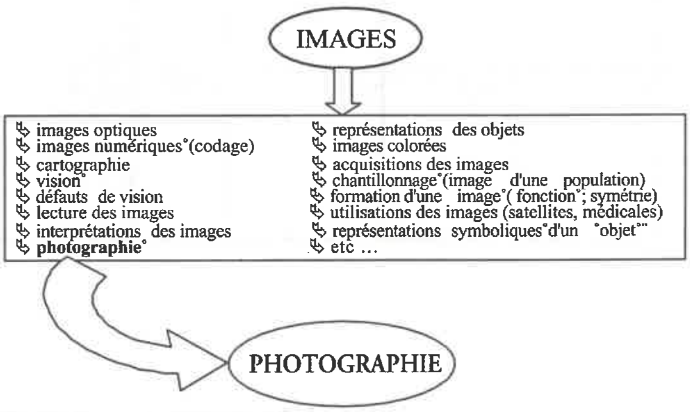
Comment expliquer les TPE aux élèves ?

Magali Herreros (sciences physiques)
Jean-Paul Bardoulat (mathématiques)(*)

Volontaires pour encadrer ensemble les TPE en première scientifique dès la rentrée 2000, l'un de nos premiers souci était de faire comprendre à nos élèves ce que sont les Travaux Personnels Encadrés. Nous voulions, à la fois, leur apprendre à distinguer le thème d'un sujet, leur montrer comment passer de l'un à l'autre, leur faire comprendre que la qualité de la démarche est plus importante que celle de la production qui peut être d'ambition modeste, leur montrer l'apport et la complémentarité de nos disciplines, tout cela d'une manière simple, sans trop les inquiéter et dans le minimum de temps. Il nous a semblé alors que nous devions vivre nous-même ces différentes phases afin d'en mesurer les difficultés et de pouvoir mieux les décrire et les expliquer à nos élèves. Nous avons donc décidé de faire un TPE ou plutôt une simulation de TPE, puis de la présenter, à titre d'exemple.

Comment passer du thème au sujet :

Le thème retenu pour la classe étant « temps, rythmes et périodes », nous avons choisi « images » pour notre simulation. Aussitôt commence une drôle d'aventure, avec l'inquiétude de ne pas aboutir. Que met-on derrière ce mot ? Qu'évoque-t-il ? Comment le lier à nos connaissances, à nos disciplines ? Diverses choses arrivent alors à l'esprit, sans ordre apparent, à travers le filtre de sa discipline, de ses intérêts, du moment... Le travail en équipe se révèle là particulièrement efficace, de l'émulation des idées au tri que l'on fait mieux ensemble que seul. Voici un aperçu des « divagations » qui nous ont amenés jusqu'au choix d'un sujet.



(*) Lycée Gabriel Fauré de Foix

Ce premier choix n'est pas encore un sujet, il est donc nécessaire de recommencer à décliner quelques idées à partir de ce sous-thème :

PHOTOGRAPHIE

↳ appareil photographique	↳ image	↳ agrandissement
↳ pellicule	↳ développement	↳ autofocus
↳ objectif	↳ flash	↳ panoramique
↳ temps de pose	↳ sensibilité	↳ numrique
↳ lumière	↳ luminosité	↳ hologramme
↳ **réglage**	↳ macro	↳ exposition

Quels facteurs interviennent dans le réglage de l'appareil pour obtenir une photo correcte ?

Notre sujet se précise ; même s'il ne s'agit pas encore d'une problématique, c'est une analyse scientifique qui commence. Nos connaissances scientifiques, notre pratique de la photo et l'exploitation de quelques documents nous ont permis de dresser la liste des divers facteurs qui interviennent dans le réglage d'une photo.

Facteurs concernant l'objet photographier	**Facteurs concernant les caractéristiques ou les réglagesde l'appareil**
↳ l'objet immobile ou en mouvement ↳ la distance objet-appareil photographique ↳ L'exposition lumineuse de lobjet	↳ l'objectif { - la focale de la lentille / - **l'ouverture du diaphragme** ↳ **le temps de pose** ↳ la sensibilité de la pellicule

Cela fait beaucoup de variables, fixons donc les conditions de prises de vue (**objet, distance, luminosité**) ainsi que la **distance focale** de l'objectif et la **sensibilité de la pellicule**

Les autres paramètres étant fixés, existe-t-il un lien entre le temps de pose et l'ouverture du diaphragme ?

Ceci est une problématique, c'est notre sujet.

Comment traiter le sujet choisi :

Notre sujet, notre problématique étant choisis, il s'agit maintenant de chercher les réglages « temps de pose-ouverture du diaphragme » qui permettent d'obtenir des photos « correctes », c'est à dire des « réglages équivalents » en ce qui concerne la quantité de lumière.

Ouvertures du diaphragme et temps de pose usuels :

Sur les objectifs des appareils photos manuels, on trouve les temps de pose et les « nombres d'ouverture » utilisés. Ces derniers indiquent l'ouverture du diaphragme qui est approximativement un disque. Le nombre de valeurs proposées varie selon le type d'appareil photo, mais elles sont toujours choisies parmi celles qui sont données ci-dessous.

Temps de pose T en secondes	1/1000	1/500	1/250	1/125	1/60	1/30	1/15	1/8	1/4	1/2	1	2

Chaque temps de pose, sauf le premier, est approximativement le double du précédent. Pour que la quantité de lumière reste constante, si l'on double le temps de pose il faut donc diviser par deux l'aire du diaphragme, c'est-à-dire diviser par $\sqrt{2}$ son diamètre.

Nombre d'ouverture N	1.4	2	2.8	4	5,6	8	11	16	22

Le lien entre le nombre d'ouverture N et l'ouverture du diaphragme se trouve dans de nombreux documents : certains cours d'optique, « La photographie » de John Hedgecoe (édition prestige Solar), « Principe de la photographie » dans la chronique expérimentale du n° 497 du bulletin de l'Union Des Physiciens de juillet 1967...

$$\mathrm{N} = \frac{f}{d}$$

où f désigne la focale de l'objectif et d le diamètre du diaphragme.

On remarque que, pour f fixé, N est inversement proportionnel à d. Plus N est grand, plus d et l'aire du diaphragme sont petits.

Si $\mathrm{N}' = \dfrac{f}{\frac{d}{\sqrt{2}}}$, c'est à dire $\mathrm{N}' = \dfrac{f}{d}\sqrt{2}$, alors $\mathrm{N}' = \mathrm{N}\sqrt{2}$.

Donc, si l'on double le temps de pose, il faut multiplier par $\sqrt{2}$ le nombre d'ouverture pour conserver la même quantité de lumière. On peut d'ailleurs remarquer que :

Nombre d'ouverture N	1.4	2	2.8	4	5,6	8	11	16	22
$\mathrm{N}\sqrt{2}$	1,979	2,828	3,959	5,657	7,919	11,31	15,56	22,63	

Avec ces temps de pose et ces nombres d'ouverture, la règle pour obtenir des « réglages équivalents », quant à la quantité de lumière, est très simple. Ces choix ont probablement été faits pour faciliter la tâche du photographe amateur. **Lorsque l'on double le temps de pose, il faut réduire de moitié l'ouverture, c'est-à-dire prendre le nombre d'ouverture immédiatement supérieur**.

Expérimentation :

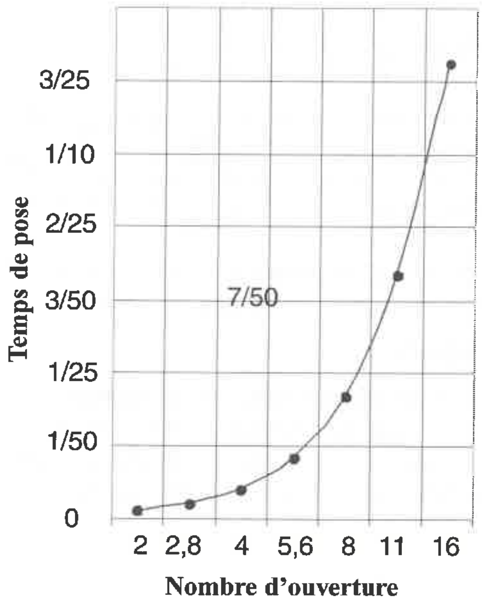
Nous avons réalisé une série de photos du château de Foix prises du même endroit, avec un même appareil à réglage manuel, avec une même pellicule, un jour de plein soleil sur une durée suffisamment courte pour que les variations de quantité de lumière soient négligeables. Nous avons ainsi fixé : la mobilité de l'objet, la distance objet-appareil, la quantité de lumière, la focale de l'objectif et la sensibilité de la pellicule. Nous avons fait les photos correspondant à toutes les combinaisons « nombre d'ouverture–temps de pose » possibles avec notre appareil, en les notant soigneusement. Les photos correctes relativement à la quantité de lumière ont été obtenues pour les réglages suivants :

Nombre d'ouverture N	5,6	8	11
Temps de pose T en s	1/125	1/60	1/30

Exploitation des résultats :

À partir de ces résultats expérimentaux et en appliquant la règle des « réglages équivalents », on obtient :

Nombre d'ouverture N	2	2.8	4	**5,6**	**8**	**11**	16	22
Temps de pose T en s	1/1000	1/500	1/250	**1/125**	**1/60**	**1/30**	1/15	1/8



Cette courbe semble être une partie de parabole passant par l'origine du repère. Pour nous en assurer calculons T/N².

T/N²	$2{,}5.10^{-4}$	$2{,}551.10^{-4}$	$2{,}5.10^{-4}$	$2{,}551.10^{-4}$	$2{,}604.10^{-4}$	$2{,}754.10^{-4}$	$2{,}604.10^{-4}$	$2{,}583.10^{-4}$

T/N² est quasiment constant. Les légères variations proviennent des approximations sur les nombres d'ouverture et les temps de pose.

On peut donc estimer que la courbe est une partie de la parabole d'équation :

$$T = k\,N^2$$

avec $k \approx 2{,}581 \cdot 10^{-4}$.

Avec d'autres conditions de prises de vues, obtient-on une relation du même type ?

* Dans « La photographie », l'auteur, John Hedgecoe, propose d'autres réglages équivalents :

N	2	2.8	4	5.6	8	11	16
T	1/60	1/30	1/15	1/8	1/4	1/2	1
T/N²	$4{,}167.10^{-3}$	$4{,}252.10^{-3}$	$4{,}167.10^{-3}$	$3{,}986.10^{-3}$	$3{,}906.10^{-3}$	$4{,}132.10^{-3}$	$3{,}906.10^{-3}$

On constate encore que $T = k\,N^2$ avec $k \approx 4{,}074 \cdot 10^{-3}$.

* Extraits de l'Encyclopédie Encarta 97 (Microsoft), rubrique « photographie » :

N	1.4	2	2.8	4	5.6
T	1/1000	1/500	1/250	1/125	1/60
T/N²	$5{,}102.10^{-4}$	$5{,}000.10^{-4}$	$5{,}102.10^{-4}$	$5{,}000.10^{-4}$	$5{,}314.10^{-4}$

Une fois encore $T = k\,N^2$ avec $k \approx 5{,}104 \cdot 10^{-4}$.

* Dans « Principe de la photographie », on trouve :

N	1.4	2	2.8	4	5.6	8	11
T	1/500	1/250	1/125	1/60	1/30	1/15	1/8
T/N²	$1{,}020.10^{-3}$	1.10^{-3}	$1{,}020.10^{-3}$	$1{,}042.10^{-3}$	$1{,}063.10^{-3}$	$1{,}042.10^{-3}$	$1{,}033.10^{-3}$

À nouveau $T = k\,N^2$ avec $k \approx 1{,}03 \cdot 10^{-4}$.

* Enfin dans « Principe de la photographie », on trouve page 63 la confirmation que T varie bien en fonction du carré de N, lorsque les autres facteurs sont fixés.

Réglage de l'appareil photo

La réussite d'une bonne photographie, indépendamment de l'aspect purement optique du problème qui réside dans la bonne mise au point (image nette ou floue), se situe dans les considérations chimiques de la bonne impression de la plaque sensible (négatif convenablement, ou sur, ou sous-exposé).

Les quatre grandeurs mesurables qui président à cette bonne exposition sont :

– La luminance du sujet	B
– Le temps de pose	T
– Le nombre d'ouverture du diaphragme	N
– La sensibilité du film	S

Ces quatre paramètres sont dépendants et l'on peut admettre qu'ils sont liés par une formule du type :

$$BT = C\frac{N^2}{S}.$$

où C est une constante fonction des unités employées.

Documents utilisés :

– Article page 16 du livre : « La photographie ». Auteur : John Hedgecoe. Édition prestige SOLAR.
– Encyclopédie ENCARTA 97 (Microsoft), rubrique « photographie ».
– Bulletin de l'Union des Physiciens du 07/67. Article page 23 : « Chronique expérimentale : Principe de l'appareil photographique ».
– Boîte de pellicule photographique.

Ce qui relève plus particulièrement des sciences physiques dans cette étude:

– Notion de focale, de nombre d'ouverture.
– Notion de quantité de lumière.
– Vitesse d'obturation.

Ce qui relève plus particulièrement des mathématiques dans cette étude :

– Agrandissement et réduction d'une longueur, d'une aire.
– Proportionnalité.
– Fonctions du type $x \rightarrow kx^2$.

Ce qui relève des deux disciplines :

– Isoler deux paramètres, fixer les autres, puis étudier comment ils sont liés.

PROBLÈME

(extrait de la revue « Réciproques », Bulletin de l'Académie de Bordeaux, coordonné par Xavier Sorbe, IPR-IA)

Un triangle équilatéral peut-il avoir ses trois sommets en des nœuds d'un quadrillage carré ?

(solution, p. 110)

Variations sur un mini-problème de géométrie

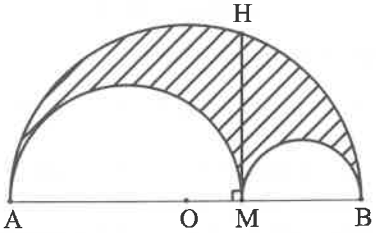
Henri Bareil(*)

I. Problème

Soit un segment AB *fixe – on pourra prendre* AB = 10 –, *un point* M *variable sur* [AB], *un demi-disque, d'aire* S, *de diamètre* [AB], *et, à l'intérieur de ce demi-disque, les demi-disques d'aires respectives* S_a *et* S_b, *de diamètres* [MA] *et* [MB].

Soit f(M) *l'aire, hachurée sur la figure, telle que*

$$f(\mathrm{M}) = \mathrm{S} - (\mathrm{S}_a + \mathrm{S}_b).$$



L'aire f(M) *varie-t-elle avec* M *?*

Si oui, existe-t-il un minimum ? un maximum ? et lesquels ?

I.1. Remarquons d'abord que :

- f(M) varie avec M : il n'est que de voir diverses positions de M.
  Lorsque M est en A ou B, $\mathrm{S} = \mathrm{S}_a$ ou $\mathrm{S} = \mathrm{S}_b$ et $f(\mathrm{M}) = 0$.
  Tel est donc le minimum.
  Comme, d'autre part, $f(\mathrm{M}) < \mathrm{S}$, il y a un maximum de f(M) (éventuellement, *a priori*, pour une ou plusieurs positions de M).
- Des positions de M symétriques par rapport à O, milieu de [AB], donnent des figures symétriques, donc la même valeur de f(M).
- Il est équivalent de chercher le maximum de f(M) ou le minimum de $\mathrm{S}_a + \mathrm{S}_b$.
- Le choix de AB = 10 ne diminue pas la généralité de nos études, encore qu'il puisse peut-être parfois la masquer..

I.2. Vers une conjecture

Soit avec un logiciel de géométrie, soit avec quelques calculs numériques, il semble que le maximum de f(M) se produise une fois, lorsque M est en O.

I.3. Recherche du maximum

Méthodes 1 *– qui utilisent la relation de Pythagore –*

$$f(\mathrm{M}) = \frac{\pi}{8}(\mathrm{AB}^2 - \mathrm{AM}^2 - \mathrm{MB}^2).$$

(*) IREM de Toulouse

Première méthode

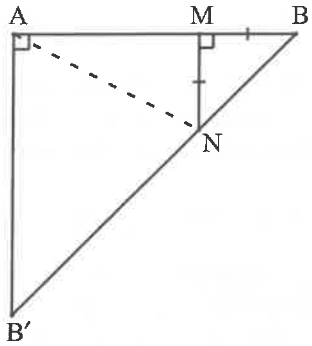
Soit H, sur le demi-cercle de diamètre [AB], dont le projeté orthogonal sur [AB] est M.
Alors $AB^2 = AH^2 + HB^2$,
puis $AB^2 = (AM^2 + MH^2) + (MB^2 + MH^2)$.

D'où $f(M) = \frac{\pi}{8} \times 2MH^2 = \frac{\pi}{4}MH^2$: l'aire $f(M)$ est donc celle du disque de diamètre MH.

Le maximum de $f(M)$ est aussi celui de MH. Il se produit bien quand M est en O et il vaut $\frac{25\pi}{4}$.

Cette méthode semble ignorer le rôle « central » de O. En fait elle utilise l'inscriptibilité d'un triangle rectangle dans le cercle dont l'hypoténuse est diamètre, ce qui, indirectement, fait intervenir le centre O du cercle.

Deuxième méthode



Le maximum de $f(M)$ correspond au minimum de $MA^2 + MB^2$.

Réduisons cette somme en « pliant » [AB] selon [AM] plus [MN], avec MN = MB et (MN) ⊥ (AB).

Alors $MA^2 + MB^2 = AN^2$. Or, quand M décrit [AB], N décrit le segment BB′ tel que $\widehat{ABB'} = 45°$ et $\widehat{BAB'} = 90°$.

Le minimum de AN se produit lorsque (AN) est perpendiculaire à (BB′). Alors N est le milieu de [BB′] et M celui de [AB].

***Méthode 2** – qui utilise directement la symétrie par rapport à O en axant sur OM –*

$$\begin{aligned} S_a + S_b &= \frac{\pi}{8}(MA^2 + MB^2) \\ &= \frac{\pi}{8}\left[(5+OM)^2 + (5-OM)^2\right] \\ &= \frac{\pi}{4}(50 + 2OM^2). \end{aligned}$$

$S_a + S_b$ est donc minimum quand OM = 0.

Cette méthode correspondrait, s'il y avait choix initial d'une inconnue x, au choix de x = OM qui privilégie le rôle de O.

***Méthodes 3** – qui négligent d'abord le rôle de O et la symétrie par rapport à O –*

$$f(\mathrm{M})=\frac{\pi}{8}\left[(\mathrm{MA}+\mathrm{MB})^2-\mathrm{MA}^2-\mathrm{MB}^2\right]$$
$$=\frac{\pi}{8}\times 2\mathrm{MA}\times\mathrm{MB}=\frac{\pi}{4}\mathrm{MA}\times\mathrm{MB}.$$

Cette méthode correspondrait à un choix d'origine en A ou en B pour situer M, par exemple avec AM = x.

Alors $f(\mathrm{M})=\frac{\pi}{4}x\,(10-x)$.

À ce stade :

a) Ou bien on sait que, *les deux facteurs x et $10-x$ ayant une somme constante, leur produit est maximum quand ils sont égaux.* D'où $x = 5$.

b) Ou bien on le retrouve, par exemple *en réintroduisant la valeur* 5 (demi-somme) dans chaque facteur explicité à partir de 5 :

$f(\mathrm{M})=\frac{\pi}{4}(5+\mathrm{OM})\,(5-\mathrm{OM})=\frac{\pi}{4}(25-\mathrm{OM}^2)$, maximum pour OM = 0.

c) Ou bien on utilise un *corollaire de la relation de Pythagore : Dans un triangle rectangle, la hauteur relative à l'hypoténuse est la moyenne géométrique des longueurs qu'elle détermine sur l'hypoténuse…* Ici $\mathrm{MA}\times\mathrm{MB}=\mathrm{MH}^2$.

De là $f(\mathrm{M})=\frac{\pi}{4}\mathrm{MH}^2$ et le maximum a lieu pour MH rayon donc M en O…

Remarquons que ces méthodes b) et c) pourraient aussi s'exprimer (hors du programme actuel des lycées, *a fortiori* du collège) en utilisant des expressions variées de la puissance de M par rapport au cercle de diamètre [AB].

d) Ou bien *en comparant f(M) au maximum présumé.*

Avec AM = x, (et $f(\mathrm{M})=f(x)$)

$f(5)-f(x)=\frac{\pi}{4}(25-10x+x^2)=\frac{\pi}{4}(5-x)^2$. D'où le maximum de $f(x)$ obtenu pour $x = 5$.

e) Ou bien *en travaillant x^2-10x comme le début du développement d'un carré* (cf. théorie du second degré), ce qui conduit à $f(x)=\frac{\pi}{4}\left[25-(x-5)^2\right]$. D'où le maximum.

f) Ou bien, classe de Première, *avec la dérivée…*

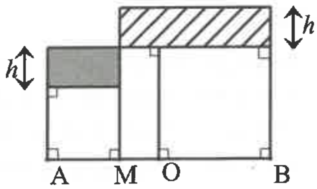
Méthode 4 – *Comparaison géométrique au maximum présumé*

$S_a + S_b$ varie comme $MA^2 + MB^2$, qui semble minimum quand MA = MB, M en O.

Comparons géométriquement $MA^2 + MB^2$ à $OA^2 + OB^2$ (cf. figure).

La première somme surpasse la seconde de (aire hachurée – aire grisée), l'aire hachurée étant supérieure ou égale à l'aire grisée (même dimension *h*, …).

Le minimum de $S_a + S_b$ se produit donc pour M en O.

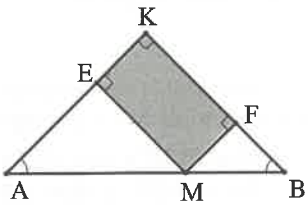


II. Tranferts sur d'autres figures

II.1. Sur des triangles rectangles isocèles

Les aires des demi-disques sont proportionnelles à celles des triangles rectangles isocèles d'hypoténuses respectives AB, AM, MB.

Soit toujours f(M) l'aire grisée définie de façon analogue à la précédente.



Ici $f(\mathrm{M}) = \frac{1}{4}(\mathrm{AB}^2 - \mathrm{MA}^2 - \mathrm{MB}^2)$

Il s'agit, à un coefficient numérique constant près ($\frac{1}{4}$ au lieu de $\frac{\pi}{8}$), de la même expression.

On peut donc ramener le problème initial à une étude classique relative à la figure ci-contre, avec recherche du maximum de l'aire du rectangle MEKF. De là de nouvelles méthodes :

Méthodes 5

On sait que $\mathrm{ME} = \frac{\mathrm{MA}}{\sqrt{2}}$ et $\mathrm{MF} = \frac{\mathrm{MB}}{\sqrt{2}}$. Dès lors :

Première méthode

MA + MB étant constante, ME + MF l'est aussi.

Le rectangle MRKF est donc de périmètre constant. On peut en déduire que son aire est maximum quand il est carré, ce qui correspond à M en O.

Si ce résultat n'est pas connu, on peut le retrouver, par exemple par la méthode 3.b, ou la 6.a ci-dessous, ou par $ab = \frac{1}{4}\left[(a+b)^2 - (a-b)^2\right]$, qui, pour $a + b$ constant, indique que le maximum de ab se produit pour $a - b = 0$, i.e. $a = b$.

Deuxième méthode

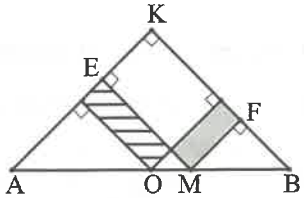
$MA^2 + MB^2 = 2\,(ME^2 + MF^2) = 2EF^2 = 2KM^2$.
Le minimum de la somme se produit pour KM minimal, donc M en O.

Méthodes 6

La brochure APMEP n° 79 (« Classe de Seconde : un outil pour des changements » – Avril 1990) *étudie un tel problème, ainsi que celui, plus général, où* KAB *est un triangle quelconque, avec* MEKF *parallélogramme.*

Elle signale plusieurs méthodes de résolution, notamment :

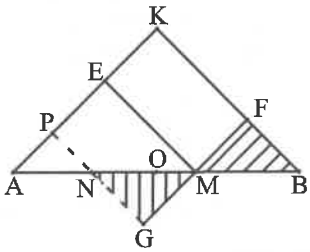
a) *Comparaison avec le carré conjecturé comme donnant l'aire maximale* (p. 133). On compare les aires hachurée et grisée.



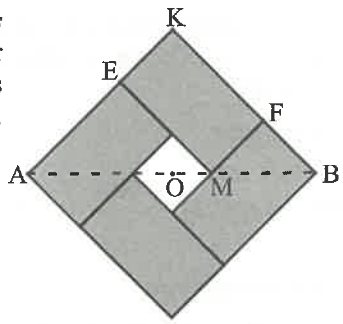
b) *Redistribution des aires* (p. 60) : par exemple, on peut symétriser MFB, par rapport à M, en MGN.

Alors aire MEKF = aire MEPG et la somme des aires de MAE et MBF excède celle de MEKF de l'aire APN. Or, si $y + z$ est constant, et $z \geq y$, y est maximum lorsque $z - y = 0$.

Ici, il s'agit donc d'annuler l'aire APN, ce qui est fait quand M est en O.



c) *Triangle KAB complété en carré par des rotations* (O, 90°) – pas besoin de cours sur les rotations pour cela – de façon à inscrire dans un carré quatre fois l'aire de MEKF … avec un trou (carré) central (p. 134 et 95). D'où le maximum en annulant ce trou … avec M en O.



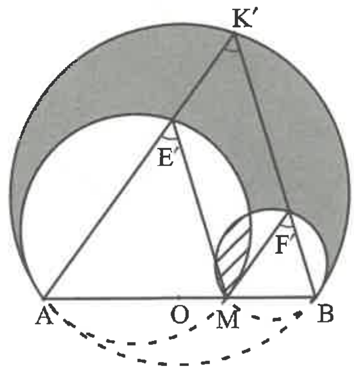
II.2. Sur des triangles quelconques

Remplaçons le triangle rectangle isocèle KAB *par un triangle quelconque* K′AB,

M variable sur [AB], avec ME′K′F′ parallélogramme (cf. figure avec $\widehat{AK'B} < 90°$).
Je montrerai, au § II.3, comment obtenir immédiatement le maximum de l'aire de ce parallélogramme à partir du cas particulier où KAB est rectangle isocèle.

Mais faisons d'abord des études directes, plus élémentaires :

1° Un lien direct avec le problème initial



Associons à chacun des triangles (semblables) K′AB, E′AM, F′MB, *leurs cercles circonscrits* Γ, γ_a et γ_b.

Par l'homothétie (ou le « théorème de l'angle inscrit » en son cas limite…), on démontre que Γ et γ_a sont tangents en A, Γ et γ_b en B.

Considérons les portions de disques d'aires respectives S, S_a et S_b définies par les cercles précédents et la droite AB dans le demi-plan qui contient K′. Ces aires sont respectivement proportionnelles à celles des triangles AK′B, AE′M et MF′B.

Par différences, l'aire du parallélogramme ME′K′F′ l'est ainsi à celle de $d = S - (S_a + S_b)$.

Les aires d et ME′K′F′ sont donc maximales en même temps.

Pour la figure ci-dessus, d = aire grisée – aire hachurée, cette aire hachurée, intersection des portions de disques d'aires S_a et S_b, n'intervenant que si $\widehat{AK'B} < 90°$.

2° ***Position de M pour le maximum de l'aire* ME′K′F′**

Aménageons, par exemple, quelques méthodes vues dans le cas particulier (on en trouvera d'autres dans la brochure APMEP n° 79 déjà citée…).

La méthode 6.b, qui n'utilise que des propriétés affines, reste la même.

Par contre, lorsque les méthodes du cas particulier s'appuient sur des propriétés métriques, il faut les reprendre.

Les relations initiales des méthodes 5 sont à modifier :

Aire ME′K′F′ = ME′ × MF′ sin K′.

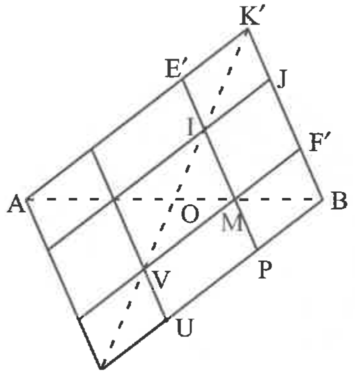
Or, d'après « Thalès-triangle » : $\dfrac{ME'}{BK'} = \dfrac{MA}{AB}$ et $\dfrac{MF'}{AK'} = \dfrac{MB}{AB}$.

Donc ME′ × MF′ = (MA × MB) × constante.

On se retrouve au cœur des méthodes 3, par l'intermédiaire de MA × MB (alors qu'on démontrerait que ME′ + MF′ n'est constante que si $\widehat{A} = \widehat{B}$.

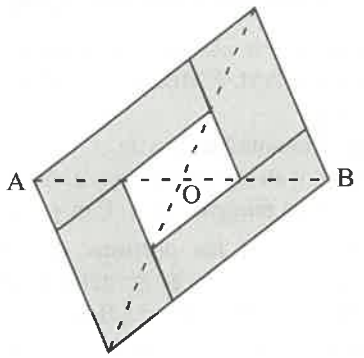
La méthode 6.c se complique un peu, … mais pas trop :

On peut retrouver des symétries (cf. figure ci-dessous) et en déduire des égalités successives d'aires par les seuls lemmes indiqués par Daniel Perrin dans le Bulletin 431, page 762. Des différences d'aires égales conduisent à l'égalité des aires MIJF′ et MPUV, puis à celle des aires E′K′F′M et F′BUV…



→

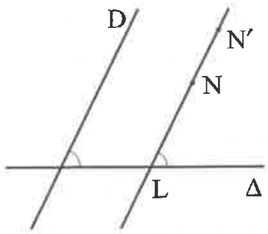
les aires grisées sont égales



…et on retrouve le trou central.

II.3. Des généralisations grâce à l'affinité

1. Rappels



Soient deux droites sécantes Δ et D et un réel λ. L'affinité d'axe Δ, de direction D, de rapport λ, associe, à tout point N (du plan (Δ, D)), le point N′ tel que (NN′) soit parallèle à D et que, L étant l'intersection de (NN′) et de Δ, $\overline{LN'} = \lambda\,\overline{LN}$.

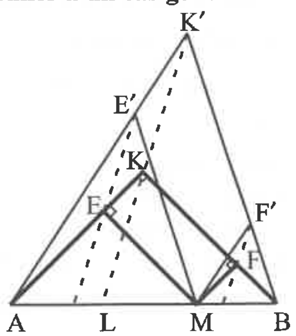
La donnée de D et de λ peut être remplacée par celle de deux points homologues.

La traduction de la définition par l'analytique est immédiate.

Grâce, par exemple, à la géométrie analytique ou à l'homothétie (ou, donc, à « Thalès-triangle »), on peut établir que :
– toute droite z sécante à l'axe Δ a pour image une droite z' qui la coupe sur Δ ;
– toute droite z parallèle à l'axe Δ a une image parallèle ;
– si deux droites sont parallèles, leurs images le sont.

Par ailleurs l'affinité conserve les rapports d'aires, donc n'altère pas les problèmes de maxima ou de minima d'aires (cf. le texte de Daniel Perrin).

2. Utilisation de l'affinité pour passer du cas particulier à un cas général



La « forme » des triangles comptant seule, ramenons-nous à KAB rectangle isocèle et K′AB quelconque, avec K et K′ dans le même demi-plan de frontière (AB) :

Si (KK′) //(AB), il en va de même de (EE′) et (FF′) et les aires de AKB, AEM, BFM sont conservées avec AK′B, AE′M, BF′M.

Sinon, il suffit de considérer l'affinité d'axe (AB) qui transforme K en K′.

Les propriétés rappelées démontrent que l'image du rectangle MEKF est le parallélogramme ME′K′F′, et réciproquement par l'affinité qui transforme K′ en K.

La conservation des rapports d'aires induit aussitôt la simultanéité des maxima.

Remarque : On peut aussi se ramener au triangle rectangle isocèle AKB en situant AK′B dans un plan différent et en utilisant une projection cylindrique. *Ce type de démonstration* est développé dans le Deltheil-Caire cité, p. 155 à 157 des compléments.

3. Des cercles aux ellipses.

- Je rappelle que l'image d'un cercle par affinité est une ellipse.

  Pour des démonstrations, par l'analytique :

– cas général : voir le Deltheil-Caire « Géométrie et Compléments », page 202 des Compléments.

– cas particulier : D ⊥ Δ et cercle centré sur Δ : démonstration immédiate.

- Associons les demi-cercles de la figure initiale à la figure précédente.

  Dans l'affinité considérée, les cercles KAB, AEM, et BFM ont pour images des ellipses et, réciproquement, il en va de même pour les arcs de cercle de la figure initiale du 6 II.2, ce qui généralise d'autant notre problème initial et sa solution.

- *Ce § II.3 montre l'intérêt d'une intervention conjuguée de cas particuliers et de transformations géométriques pour résoudre immédiatement des cas plus généraux* (cf. Bulletin 431, p. 790), *ou les susciter*. Pour une étude théorique générale de cette possibilité, voir le chapitre 11, p. 349 à 356, de l'« Initiation à la géométrie » de Daniel Lehmann (« Initiation » pas tellement élémentaire…).

III. Des lapins hors des chapeaux.

1. Nous avons étudié, séparément d'abord, diverses figures élémentaires (demi-cercles, triangles isocèles, triangles quelconques) ainsi que des passages des unes aux autres qui ont étendu nos propos à des arcs de cercles quelconques et à des ellipses.

- **Cela relèverait-il d'une configuration générale ?**

  Oui, dit un premier lapin sortant du chapeau :

  Il s'agit toujours d'une courbe (ou figure) F associée à [AB] fixe et de deux courbes (ou figures) F_a et F_b en « réduction » de F (i.e. « semblables » ou, plus précisément « homothétiques »), associées l'une à [MA], l'autre à [MB] : F_a est l'image de F dans l'homothétie (A, MA/AB), et F_b l'est de F dans l'homothétie (B, MB/AB).

  Nous envisagerons désormais cela quelle que soit la courbe (ou figure) initiale F, pourvu qu'elle permette de cerner les aires qui interviennent, (AB) intervenant pour fermer F si besoin est.

- **Comment traiter un cas aussi général ?**
... Grâce à un deuxième lapin sorti du chapeau, nommé « *proposition A-R* » (Agrandissement-Réduction) par Jean-Pierre Friedelmeyer, qui dit que « *Dans un agrandissement-réduction de rapport k, l'aire est multipliée par k^2* ».

Associons nos deux lapins :
Soit S, S_a, S_b les aires respectives cernées par F, F_a, F_b.

$$S_a = S\times\left(\frac{MA}{AB}\right)^2 \text{ et } S_b = S\times\left(\frac{MB}{AB}\right)^2.$$

D'où $S - S_a - S_b = \dfrac{S}{AB^2}\left[AB^2 - (MA^2 + MB^2)\right]$.

Nous voilà ramenés, *quelle que soit* F, à l'étude faite en I et II de diverses façons.

Plus besoin de se limiter à des figures élémentaires ou de multiplier les outils (affinité par exemple) *pour aller de l'une à l'autre...*

Désormais, grâce à la « basique » (dès le collège) « propriété A-R », *voilà réglé un problème général* !

Quelle superbe efficacité dans la simplicité ! Cela parce que la propriété utilisée est liée à une claire perception de la structure interne de la figure, structure d'abord ignorée à l'occasion des études séparées des cas particuliers.

J'aurais certes pu utiliser la propriété « A-R » pour compléter, dans chaque cas, la kyrielle des méthodes proposées, mais elle aurait alors peu apporté et j'ai préféré la réserver à son effet sur une configuration générale !

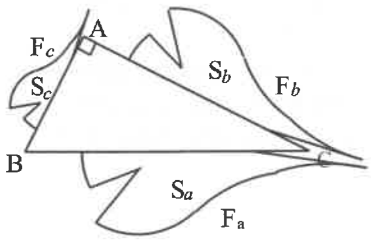
Pour autant nous n'en sommes pas à une clôture de la situation-problème : par exemple, que se passerait-il avec d'autres transformations que l'homothétie ? Mais *nous voyons déjà que l'utilisation conjointe de la structure interne d'une figure, quelles que soient les modalités de son expression, et d'un théorème général, est donc un merveilleux outil.*

2. ***Je me permets d'en donner un autre exemple***, qui est une variante des pages 225-226 du très bel article de Jean-Pierre Friedelmeyer, paru dans notre Bulletin 427, consacrées à la famille de figures relevant de la relation de Pythagore.
Cette variante permet d'accéder directement au cas général :

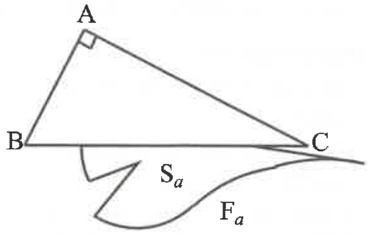
• Soient **trois figures semblables** dont les dimensions sont respectivement proportionnelles aux longueurs des côtés d'un triangle rectangle ABC.

Soient S_a, S_b, S_c les aires respectives de ces figures.

On peut, d'abord, toujours se ramener à des figures F_a, F_b, F_c isométriques des précédentes, pareillement construites, extérieurement au triangle ABC, à partir de ses côtés. Cf. exemple de la figure ci-contre.



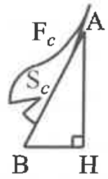
Existe-t-il une structure interne générale de la figure globale qui lui étendrait les similitudes des F_i ?



Pourrait-on, par exemple, associer à F_b et F_c deux triangles rectangles qui leur seraient ce qu'est le triangle ABC à F_a ?

Eh bien, oui ! *en traçant la hauteur* [AH] qui décompose ABC en deux triangles rectangles AHB et AHC, les trois triangles rectangles relevant des mêmes similitudes que F_a, F_b, F_c.

Dès lors, en associant à chaque figure F_i « son » triangle rectangle, voici, par exemple, *deux figures semblables, dessinées séparément ci-contre*, extraites de la figure générale :



Faisons alors intervenir une *propriété fondamentale* P :

« *Le rapport des aires de deux parties d'une figure est conservé par agrandissement-réduction* »,

propriété qui peut apparaître rapidement lors de la construction expérimentale de la notion d'aire et qui est un des invariants fondamentaux soulignés par Daniel Perrin.

Dès lors $\dfrac{S_a}{\text{aire ABC}} = \dfrac{S_b}{\text{aire HBA}}$,

d'où $S_a \times (\text{aire HBA}) = S_b \times (\text{aire ABC})$.

De même, en utilisant les figures mixtilignes formées par « ABC et F_a » et « AHC et F_b » , il vient :

$$S_a \times (\text{aire HCA}) = S_c \times (\text{aire ABC}).$$

De là, par addition membre à membre :

$$S_a \times (\text{aire HBA} + \text{aire HCA}) = (S_b + S_c) \times (\text{aire ABC}).$$

C'est-à-dire :

$$S_a = S_b + S_c.$$

Ce résultat général vaut quelle que soit F_a … : carré, triangle, demi-disque, lunule, poisson ou chat, … !

• En prenant pour F_a le carré de coté BC, F_b et F_c sont les carrés de cotés respectifs AC et AB, on obtient la célèbre relation :

$a^2 = b^2 + c^2$.

• **C'est bien une structure interne du triangle rectangle qui a été utilisée** : parmi tous les triangles, le triangle rectangle se caractérise par son partage en deux triangles semblables entre eux et au premier. **Cette structure interne « épouse » celle des trois figures F_i**… Une méthode qui les unifie ne peut qu'être féconde !

3. De telles situations se retrouveraient en *géométrie dans l'espace* où, s'agissant de volumes, interviendrait alors, si besoin était, le coefficient k^3.

IV - Exploitation selon les classes

– avec des adéquations selon les classes et les élèves –

- **Dès la Sixième,**

  on peut faire réaliser le dessin initial, avec des choix différents de M selon les élèves.

  Il est possible de calculer le périmètre de la figure grisée. Avec une bonne amplitude des choix de M et les cas particuliers, on pourrait faire percevoir que l'aire (non calculée) est variable, tandis que le périmètre est constant.

  Même conclusion pour la figure des triangles rectangles isocèles... Ainsi s'enrichirait la panoplie des figures à périmètre constant et aire variable, ce qui contribue à la distinction aire-périmètre.

- **En Cinquième,** dès que l'aire du disque est connue, on peut :

a) Pour le dessin initial

– faire calculer $f(M)$ – avec une notation plus simple – ainsi que l'aire du disque de diamètre HM,
– travailler sur les approximations, les cas aberrants d'erreurs de calcul,
– aller vers des conjectures,
– expliquer que cela ne permet pas d'affirmer,
– faire dégager l'intérêt de la mise en évidence de la symétrie par rapport à O.

b)

– aborder des démonstrations « géométriques » (méthodes 4 et 6) qui ont, de plus, le mérite d'un réinvestissement de la proportionnalité (parmi les méthodes 6, la comparaison au maximum présumé peut être préconisée).

- **En Quatrième-Troisième** :

– outre ce qui précède, on peut apprécier des interventions multipliées, dans les méthodes ci-dessus, de la relation de Pythagore, des « identités remarquables », ainsi que l'intervention des symétries et d'une rotation simple.
  Les figures traitées conduisent à l'étude, pour $f(M)$, d'un facteur du type $(a + b)^2 - (a - b)^2$, ce qui lutte d'autant contre l'assimilation de $(a + b)^2$ et de $a^2 + b^2$...
– Peut-être pourrait-on aussi comparer utilement des méthodes des § I et II.1 : simplicité, par exemple, de la méthode 2 ou de celle du trou central. Or la méthode 2 utilise d'emblée la symétrie par rapport à O, tandis que la méthode du trou central *complète une figure pour l'enrichir en symétries...*

- **Dès la Seconde,**

– outre ce qui précède, on pourrait faire dégager le théorème sur le maximum d'un produit de deux facteurs dont la somme est constante : il s'agit en effet d'une situation fréquente, et, ici, il rend la méthode 3 rapidement performante ;
– on pourrait aussi s'intéresser au § II.2.

- **En Première,**
  la recherche du maximum peut se faire par la dérivée. Mais le présent problème montre que les dérivées n'ont pas à monopoliser la recherche de façon systématique : ici il y a plus simple, plus éclairant ou plus joli !

- **Dès la Terminale,**

– le § II.3 peut être proposé en exercice et la méthode « cas particulier démontrant le cas général » dégagée !

– le § III serait bienvenu pour une réflexion sur les classes de problèmes et les méthodes de résolution et une vision panoramique de la progression des § I, II, III…

V. Des maths « utiles » ?

L'intérêt pratique de la situation initiale n'est pas évident !

Mais son étude ne va-t-elle pas bien au-delà ?
Elle a fait émerger tant de problèmes, tant d'approches, de recoupements, d'extensions exemplaires ! Ces émergences mêmes, la façon de les susciter, de les accompagner et de les exploiter ne sont-elles pas au cœur d'un enseignement qui a l'ambition d'être transférable ?

Il s'est agi, tout au long, d'être à l'écoute des situations, d'en débattre, de se référer à des savoirs fondamentaux ou de les créer, d'imaginer, de saisir et d'exploiter des analogies, de rechercher la substance même des choses… Il doit d'ailleurs apparaître que nous ne sommes sûrement pas allés au bout, qu'il n'y a pas de « bout », … qu'il n'y a que des approfondissements successifs…

Une telle formation me semble une école de pensée, de jugement, de capacité de se créer, donc de liberté, c'est-à-dire une école de vie. Dès les années de collège ou de lycée, elle contribuera à armer nos élèves pour affronter au mieux aussi bien les problèmes de la vie courante et citoyenne que ceux inhérents aux plus essentiels questionnements de l'humain.
De quoi mettre en évidence le profond intérêt de l'enseignement des mathématiques !

Henri BAREIL

en remerciant chaleureusement Christiane Zehren pour une éminente et patiente contribution à la rédaction de l'article.

Bibliographie

– Brochure APMEP n° 79 : Classe de Seconde, Avril 1990.

– Bulletin APMEP n° 427, article de Jean Pierre Friedelmeyer.

– Bulletin APMEP n°431 : articles de Daniel Perrin, Michel Carral et Roger Cuppens.

– Coxeter. « Redécouvrons la géométrie ». Réédition Gabay.

– Deltheil-Caire, « Géométrie et compléments ». Réédition Gabay.

– Lehmann D. « Initiation à la géométrie ». P.U.F.

Enseignants, vous êtes particulièrement concernés :

- EN LYCÉE, par nos brochures
  - d'ARITHMÉTIQUE : cf. page 45
  - de STATISTIQUE : cf page 136
  - de CONCOURS : cf page 134
  - de LP (LP, STT, L) : cf page 137
- EN COLLÈGE :

  par FICHIER ÉVARISTE 2
  et son jumelage avec le volume 1 : cf page 134

Dossier : L'arithmétique

En arithmétique, un et un font deux.
En amour un et un devraient faire un,
et ça fait deux tout de même.

Guy de Maupassant, *Yvette*

Dans le petit monde des mathématiciens, du chercheur de pointe jusqu'à l'humble amateur et en passant par tous ceux qui enseignent cette noble discipline, l'arithmétique occupe une place à part : nous en sommes presque tous amoureux !

D'où vient cet amour ?

Sans doute l'objet fondamental même de l'arithmétique, ces simples entiers naturels, n'y sont pas pour rien. Kronecker en disait qu'ils étaient l'œuvre de Dieu et que tout le reste était fabriqué par les hommes. En tout cas, avec la perception de l'espace (géométrie), ils forment les deux piliers *naturels* les plus anciens des mathématiques.

Sans doute aussi du fait que beaucoup de problèmes de l'arithmétique se posent en termes simples, faisant immédiatement sens, et que leurs solutions, par contre, peuvent être immédiates, moins immédiates, franchement difficiles ou compliquées, très ardues, voire inconnues. Le grand théorème de Fermat, déjà évoqué par Diophante, et dont la démonstration a résisté, de Fermat à Wiles, durant plus de trois siècles à tant d'amateurs et de mathématiciens de première grandeur, est un superbe exemple d'une telle situation (en outre, sa résolution, avec toute une dramaturgie d'espoirs et de doutes jusqu'à la certitude finale, a bénéficié, pour le plus grand bien de l'image des mathématiques, d'une belle couverture médiatique).

Présente dans l'enseignement secondaire pendant de longues années, l'arithmétique en a été éliminée au début des années 80 par une commission de programmes à laquelle j'appartenais (mea culpa !). Ne croyez pas que cela ait été fait dans l'enthousiasme ou dans un délire masochiste. Nous étions en face d'un discours qui mettait face à notre amour de matheux pour l'arithmétique, un appétit beaucoup moins évident de ceux de nos élèves qui, même scientifiques, n'avaient pas cette fibre particulière (y a-t-il un gène de l'arithmétique ?). L'arithmétique comme signe distinctif des *vrais* matheux ! Et puis il fallait *alléger* d'une quantité significative : la déesse Arithmétique dans son splendide isolement en fit les frais !

Pendant plus de dix ans, nous autres profs de maths vivions avec cet amour caché. Certes beaucoup d'entre nous continuaient de pratiquer l'arithmétique avec plaisir et émotion, mais c'était un plaisir solitaire que nous ne faisions plus partager à nos élèves. Et, pour un enseignant digne de ce nom, ne pas faire partager avait quelque chose de frustrant.

Miracle ! Notre arithmétique revient, très modestement, dans les programmes de l'enseignement secondaire. Dans ceux de Terminale Scientifique évidemment, mais quelques allusions ici ou là, l'air du temps, l'importance du numérique discret dans les calculatrices, les tableurs, donnent à toutes ces questions une place de plus en plus prégnante, même si elle reste parfois encore discrète, implicite.

Quel plaisir de voir les IREM, malgré leur peu de moyens, publier maintes brochures, opérationaliser cet élan, diffuser ce fourmillement d'idées, animer ce qui reste de formation continue. Et à lire les brochures on sent le plaisir que leurs auteurs y ont pris (ou retrouvé). Une fois de plus les IREM montrent toute l'importance de leur existence, tout l'intérêt de leur statut mettant ensemble les enseignants du primaire, du supérieur et du secondaire, un peu en dehors de la hiérarchie administrative. Bref un espace de liberté, de rencontre et de travail !

L'APM ne pouvait pas rester en dehors du mouvement. Elle a déjà publié la très belle brochure de Mathieu Savin, *Arithmétique : des résultats classiques par des moyens élémentaires*. Quel que soit votre niveau en la matière, vous y trouverez de quoi vous régaler et, pour vous faire une opinion plus précise, vous pouvez lire la recension qu'Henri Bareil en a fait dans le numéro 431. Après le dossier consacré à la géométrie, voilà donc un dossier consacré à l'arithmétique. Il s'étendra sur deux, voire trois bulletins. Notre intention première n'est pas de produire des documents directement utilisables dans la classe, dans le droit fil des programmes. Cela est fait dans les manuels et puis chacun, en plus, adaptera son enseignement à ses élèves et à ses convictions didactiques. Notre volonté est d'apporter aux uns, de rappeler aux autres, dans quel contexte historique, technique, culturel, utilitaire, l'arithmétique évolue. Nous espérons que chacun y trouvera son plaisir, des idées pour illustrer son enseignement, pour le resituer dans un contexte plus large.

Dans ce bulletin, nous ouvrons ce dossier par une promenade ou plutôt une randonnée (il y a quand même quelques passages ardus) dont le guide est Marc Guinot à travers un texte fort judicieusement intitulé *L'arithmétique, pourquoi ?* et essentiellement centré sur deux thèmes : les entiers sommes de deux carrés et l'infinité des nombres premiers. Cette randonnée est à la fois mathématique, à travers différentes méthodes pour démontrer un même résultat, et historique, à travers le rôle qu'ont joué des mathématiciens aussi prestigieux que Fermat, Euler, Gauss, ... ou des amateurs plus ou moins connus comme Aubry ou Goldbach.

Mathieu Savin aborde avec sa clarté coutumière un problème qui est à la fois du ressort de l'arithmétique et de l'analyse, du ressort du discret et du continu : *L'approximation des réels par des rationnels*. Même si parfois cela va assez loin et participe à notre formation scientifique de fond, il y a là aussi des idées simples pour donner du contenu, du sens à tel ou tel calcul technique et creux sur les inégalités ou les encadrements.

Jean Lefort nous emmène dans un monde très différent, celui du langage, celui de l'ethnolinguistique, à travers une interrogation quelque peu provocatrice *Y a-t-il un naturel après 3 ?* Si ce n'est pas l'œuvre de Dieu comme le prétend Kronecker, comment l'homme a-t-il mis en place les entiers naturels, quels ont été les statuts de 0, de 1, de 2 ?

Les quelques activités liées aux codes correcteurs et à la cryptographie de Robert Rolland permettront de comprendre comment ces nombreux numéros qui nous identifient (numéro INSEE, carte bancaire, …) sont protégés par des codes qui détectent la plupart des erreurs de transcription et, pour certains, les corrigent automatiquement. L'auteur nous fait aussi pénétrer dans les secrets de la cryptographie à travers le petit théorème de Fermat et le code RSA. Tout cela à travers une démarche très pédagogique où le lecteur est sans cesse sollicité à agir, tout en étant guidé par un questionnement très éclairant. La première partie de l'article est un rappel de quelques théorèmes et algorithmes classiques de l'arithmétique élémentaire que Robert Rolland sait mettre en perspective avec beaucoup de clarté.

Tous nos textes ne sont pas écrits par des collègues contemporains ! Ainsi vous trouverez l'analyse par Michel Guillemot d'un texte d'un certain Bernelin, élève de Gerbert d'Aurillac, savant et pape de l'an mil. Il y décrit un abaque de ce dernier pour faire des divisions simples.

La suite dans le prochain numéro !

Daniel REISZ

L'arithmétique, pourquoi ?

Marc Guinot

L'arithmétique ou théorie des nombres (des nombres entiers s'entend : c'est le sens premier du mot « arithmos » en grec) occupe une place singulière en mathématiques. Aussi ancienne que les mathématiques elles-mêmes, elle n'eut, pendant longtemps, que des adeptes prestigieux mais peu nombreux, qui étaient soit des mathématiciens confirmés, comme Fermat, Euler, Lagrange, Legendre, Gauss ou Dirichlet, soit des amateurs brillants tel Christian Goldbach, correspondant d'Euler. Tout en œuvrant dans bien d'autres domaines des mathématiques, tous manifestèrent avec ardeur leur intérêt pour cette discipline particulière que Gauss qualifiait de « reine des mathématiques » et dont Euler célébrait dans sa correspondance la magnificence (« Herrlichkeit »).

Un des attraits de l'arithmétique réside dans le décalage qui existe entre la simplicité de beaucoup de ses énoncés et la subtilité qui préside à leurs démonstrations. On s'est beaucoup moqué d'Euclide qui crut bon de développer toute une argumentation pour démontrer, en géométrie, l'inégalité du triangle $AC \leq AB + BC$ (Euclide, *Les Éléments*, Livre I, proposition 20) alors que l'âne sait bien que pour aller à la botte de foin qu'il convoite, il n'est pas utile de faire un détour par un autre endroit. L'arithmétique elle-même n'est pas exempte de ce genre de travers et c'est avec le plus grand sérieux que le même Euclide démontre que la somme de plusieurs nombres pairs est encore un nombre pair (*Les Éléments*, Livre IX, proposition 21).

Mais prenons le célèbre théorème selon lequel *il existe une infinité de nombres premiers*. On ne sait pas justifier cette affirmation en donnant directement un exemple de famille infinie de nombres tous premiers comme on le ferait, par exemple, pour expliquer qu'il y a une infinité de nombres impairs. La démonstration astucieuse et évidemment irréfutable, se trouve dans les *Éléments* (Livre IX, proposition 20) et consiste à considérer *a priori* une quantité limitée de nombres premiers $p_1, \ldots, p_r$ et à montrer que cette liste, aussi étendue soit-elle, n'épuise pas tous les nombres premiers possibles, et cela, en donnant un exemple de nombre premier p qui ne figure pas dans la liste. Pour y parvenir, on forme le produit de tous les nombres premiers considérés et on lui ajoute 1. Comme tout nombre entier > 1, le nombre obtenu est soit lui-même un nombre premier (ce qui arrive), soit un multiple d'un nombre premier p (il suffit de considérer le plus petit diviseur $p > 1$ de N). Le nombre premier p mis ainsi en évidence ne figure pas parmi les nombres premiers $p_1, \ldots, p_r$ car s'il y figurait, ce serait un diviseur du produit $p_1 \ldots p_r$ et comme c'est aussi un diviseur de N, ce serait un diviseur de la différence $N - p_1 \ldots p_r$, c'est-à-dire de 1, ce qui est impossible pour un nombre premier normalement constitué. Le résultat est donc démontré.

Les entiers qui sont somme de deux carrés : quelques résultats préliminaires

Dans beaucoup de cas, on ne parvient à démontrer un résultat d'arithmétique qu'au prix de subtilités et de détours qui ont demandé à leurs auteurs des années d'efforts et de méditations. Prenons l'exemple des nombres entiers qui sont susceptibles de se décomposer d'une manière ou d'une autre en somme de deux carrés parfaits, comme 13 (qui est égal à $3^2 + 2^2$) ou 4 294 967 297 (qui est égal à $62\,264^2 + 20\,449^2$). Pour des raisons qui tiennent à l'identité algébrique

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' - yy')^2 + (xy' + x'y)^2,$$

un premier point à élucider est de trouver tous les nombres premiers p qui admettent déjà ce genre de décompositions en deux carrés. Une observation sommaire dans la liste des premiers nombres premiers amène à proposer la conjecture suivante : sont décomposables en sommes de deux carrés le nombre premier 2 et les nombres premiers qui, comme le dit Fermat lui-même, « surpassent de l'unité un multiple de 4 ». Ces derniers sont donc les nombres premiers de la forme $4n + 1$ ou, pour employer le langage si commode des congruences (inventé par Gauss plus d'un siècle après Fermat), les nombres premiers p congrus à 1 modulo 4, ce qui peut encore s'écrire $p \equiv 1 \pmod 4$.

Dans sa correspondance, Fermat prétend qu'il est parvenu non sans mal à démontrer le résultat invoqué grâce à une variante subtile de sa méthode (déjà fort astucieuse) de descente infinie. Mais il n'en dit pas plus et Euler qui, sur l'incitation de Goldbach, reprit la question plus de 60 ans après la mort de Fermat, mit de nombreuses années à en venir à bout. Il vaut la peine de voir comment il s'y est pris.

Un premier préalable est de connaître les propriétés particulières des nombres premiers. En dehors du fait qu'un nombre de ce genre n'a pas de diviseurs hormis 1 et lui-même, l'essentiel réside dans la propriété (qu'on admettra ici sans discuter et qu'on trouve déjà dans Euclide : *Éléments*, Livre VII, proposition 30) que *tout nombre premier p qui divise un produit de facteurs divise nécessairement l'un de ces facteurs* (on notera que ce n'est pas le cas d'un nombre aussi simple que 4 qui divise le produit 6×2 sans diviser ni 6 ni 2). Dans le langage des congruences, cette propriété veut dire que la relation $xy \equiv 0 \pmod p$ implique $x \equiv 0 \pmod p$ ou $y \equiv 0 \pmod p$, ce qui est très satisfaisant (et faux quand on remplace le module premier p par un nombre composé tel que 4…).

Une autre propriété cruciale est le « petit théorème de Fermat » selon lequel *si x est un entier quelconque, $x^p - x$ est toujours divisible par p* si p est un nombre premier. Dans le langage des congruences, on a donc $x^p \equiv x \pmod p$. On notera que $2^{341} \not\equiv 2 \pmod{341}$, ce qui prouve au passage que 341 n'est pas premier…

Lorsque x est divisible par p, la congruence en question est évidente. Lorsque x n'est pas divisible par p, la décomposition $x^p - x = x\,(x^{p-1} - 1)$ et la propriété du paragraphe précédent fournissent une variante du théorème de Fermat: *si p est un nombre premier et si x n'est pas divisible par p, alors $x^{p-1} - 1$ est toujours divisible par p.* En d'autres termes, avec ces hypothèses, on a toujours $x^{p-1} \equiv 1 \pmod p$.

Pour démontrer la première des affirmations précédentes (et donc aussi la deuxième), on peut procéder comme l'avait fait Leibniz en son temps en remarquant que lorsqu'on développe $(a + b)^p$ par la formule du binôme, on obtient une somme qui s'écrit $a^p + pa^{p-1}b + \frac{p(p-1)}{2}a^{p-2}b^2 + \ldots + b^p$, avec des termes intermédiaires (extrêmes exclus) affectés de coefficients qui sont tous divisibles par p. En effet, comme ces coefficients, tous entiers, sont $C_p^k = \frac{p!}{k!(p-k)!}$ avec $1 \leq k \leq p - 1$, on a la relation $p! = k!(p-k)!C_p^k$ qui montre que p divise le produit $k!(p-k)!C_p^k$. Comme, par hypothèse, p est plus grand que k et que $p - k$, il ne peut diviser ni $k!$ ni $(p - k)!$ comme on l'a vu précédemment, donc, pour la même raison, il divise C_p^k.

On déduit de là que $(a + b)^p \equiv a^p + b^p \pmod p$ quels que soient les entiers a et b. Par récurrence, on a aussitôt plus généralement

$$(a + b + \ldots + c)^p \equiv a^p + b^p + \ldots + c^p \pmod p$$

si $a, b, \ldots, c$ sont des entiers quelconques. Si, en particulier, on prend $a = b = \ldots = c = 1$, on voit alors que $x^p \equiv x \pmod p$, x étant le nombre de termes de la somme $a + b + \ldots + c$. D'où la relation cherchée dans le cas où x est un entier positif. Le cas négatif s'en déduit sans peine.

Les entiers qui sont somme de deux carrés : le noeud de l'affaire

Venons-en aux sommes de deux carrés, en étudiant celles d'entre elles qui s'écrivent $a^2 + b^2$ avec des entiers a et b premiers entre eux, c'est-à-dire sans diviseurs communs autres que 1. Comme l'a montré Euler, cette hypothèse n'est pas sans conséquences sur les facteurs premiers du nombre correspondant car *si un nombre* N *est de la forme* $a^2 + b^2$ *avec des entiers a et b premiers entre eux, alors tous les diviseurs premiers impairs de* N *sont de la forme* $4n + 1$. En parlant des « diviseurs premiers impairs » de N, on exclut expressément le diviseur 2, seul nombre premier pair possible. Raisonnons par l'absurde en supposant que le nombre N précédant admette un diviseur premier impair p qui ne soit pas de la forme voulue. Comme p est impair, il est de la forme $4n + 3$. Posons alors $m = 2n + 1$. De la relation $a^2 + b^2 \equiv 0 \pmod p$ qui résulte des hypothèses, on déduit successivement $a^2 \equiv -b^2 \pmod p$, $(a^2)^m \equiv (-b^2)^m \pmod p$ et $a^{2m} \equiv -b^{2m} \pmod p$ puisque m est impair. Comme $2m = 4n + 2 = p - 1$, cette dernière congruence s'écrit $a^{p-1} \equiv -b^{p-1} \pmod p$. Comme a n'est pas divisible par p (sinon b le serait aussi à cause de la relation $b^2 = \mathrm{N} - a^2$) et que b n'est pas divisible par p (sinon a le serait aussi pour une raison analogue) – le tout en contradiction avec l'hypothèse que a et b sont premiers entre eux –, la congruence obtenue se réduit, grâce au petit théorème de Fermat, à $1 \equiv -1 \pmod p$, ce qui est absurde car cela voudrait dire que p divise 2. D'où le résultat.

Et réciproquement ?

Ce résultat admet une sorte de réciproque puisque *si p est un nombre premier de la forme* $4n + 1$, *alors il existe deux entiers a et b premiers entre eux tels que p divise* $a^2 + b^2$.

On s'approche ainsi du résultat final cherché qui veut que p soit en fait un nombre de cette forme (on notera que la relation $p = a^2 + b^2$ implique que a et b sont premiers entre eux).

Le nombre premier p étant de la forme $4n + 1$, considérons deux entiers x et y premiers entre eux et supposés non divisibles par p. Les deux entiers $a = x^n$ et $b = y^n$ sont encore deux entiers premiers entre eux et non divisibles par p. Comme $a^4 = x^{4n} = x^{p-1}$ et $b^4 = y^{4n} = y^{p-1}$, il résulte du théorème de Fermat que $a^4 \equiv b^4 \pmod{p}$, autrement dit que p divise $a^4 - b^4$, c'est-à-dire le produit $(a^2 - b^2)(a^2 + b^2)$ et donc $a^2 - b^2$ ou $a^2 + b^2$. Si p divise $a^2 + b^2$ pour au moins une valeur de x et une valeur de y, le résultat cherché est démontré. Si ce n'est pas le cas, p divise $a^2 - b^2 = x^{2n} - y^{2n}$ quelles que soient les valeurs de x et de y (soumises aux conditions que l'on sait). En particulier, en prenant $y = 1$, p doit diviser $x^{2n} - 1$ quel que soit x non multiple de p.

Pour montrer que cela est absurde (donc que p divise bien $a^2 + b^2$ pour des valeurs convenables de x et de y), Euler fait un petit détour par l'*opérateur de différence* D qui associe à toute fonction f (définie disons sur $\mathbf{R}$) la fonction $g = \mathrm{D}f$ (définie sur le même ensemble) telle que $g(x) = f(x + 1) - f(x)$ pour tout x. Bref, on a

$$\mathrm{D}f(x) = f(x+1) - f(x) \text{ quel que soit } x.$$

On vérifie aussitôt que D est un opérateur linéaire, c'est-à-dire que

$$\mathrm{D}(f + g) = \mathrm{D}f + \mathrm{D}g \text{ et } \mathrm{D}(af) = a\,\mathrm{D}f \text{ si } a \in \mathbf{R}.$$

En particulier, avec des notations incorrectes, mais compréhensibles, on a

$$\mathrm{D}(a_0 + a_1x + \ldots + a_mx^m) = a_0\mathrm{D}(1) + a_1\mathrm{D}(x) + \ldots + a_m\mathrm{D}(x^m)$$

pour n'importe quel polynôme $a_0 + a_1x + \ldots + a_mx^m$. Comme

$$\mathrm{D}(1) = 0,\ \mathrm{D}(x) = x + 1 - x = 1,\ \mathrm{D}(x^2) = (x+1)^2 - x^2 = 2x + 1,\ \ldots,$$

$$\mathrm{D}(x^m) = (x+1)^m - x^m = mx^{m-1} + \frac{m(m-1)}{2}x^{m-2} + \ldots + 1,$$

on voit aussitôt que si $a_m \neq 0$, $\mathrm{D}(a_0 + a_1x + \ldots + a_mx^m)$ est un polynôme en x de degré $m - 1$, dont le coefficient dominant (celui du terme de degré $m - 1$) est ma_m.

On peut bien sûr répéter cette opération plusieurs fois, ce qui donne des opérateurs D^2, D^3, … pour lesquels

$$\mathrm{D}^2f(x) = f(x+2) - f(x+1) - f(x+1) + f(x)) = f(x+2) - 2\,f(x+1) + f(x),$$

$$\mathrm{D}^3f(x) = f(x+3) - f(x+2) - 2\,f(x+2) + 2\,f(x+1) + f(x+1) - f(x)$$

$$= f(x+3) - 3\,f(x+2) + 3\,f(x+1) - f(x)\ldots$$

Un raisonnement par récurrence, laissé au lecteur, montre que $\mathrm{D}^mf(x)$ est une combinaison linéaire à coefficients entiers de $f(x), f(x + 1), \ldots, f(x + m)$.

D'autre part, si on applique D^2 à un polynôme de degré m, on trouve 0 si $m \leq 1$ et sinon un polynôme de degré $m - 2$, dont le coefficient dominant est $m\,(m - 1)\,a_m$.

On a des résultats analogues pour D^3, D^4, etc. En particulier, si m est un entier ≥ 1, $D^m(x^m)$ et $D^m(x^m - 1)$ se réduisent à la constante $m!$.

Il résulte de tout cela qu'en posant $f(x) = x^m - 1$, on a

$$m! = c_0 f(x) + c_1 f(x+1) + \ldots + c_m f(x+m)$$

où $c_0, c_1, \ldots, c_m$ sont des coefficients entiers. En particulier, avec $x = 1$, on a

$$m! = c_0 f(1) + c_1 f(2) + \ldots + c_m f(m+1).$$

Si on prend pour m le nombre $2n$ introduit plus haut il résulte de l'hypothèse faite sur $x^{2n} - 1$ que p divise $f(1)$, $f(2)$, ... , $f(4n)$, donc a fortiori $f(1)$, $f(2)$,..., $f(2n+1) = f(m)$ (car $2n + 1 < 4n$), et donc p divise $m!$ Mais cela n'est pas possible puisque $m = 2n < 4n - 1 = p$. CQFD.

Le Saint-Graal

Pour accéder au Saint-Graal, il reste un dernier résultat à démontrer : *si* N *est un entier de la forme* $a^2 + b^2$ *et* q *un diviseur premier de* N *de la forme* $x^2 + y^2$*, alors* N/q *peut être mis sous la forme* $u^2 + v^2$.

Comme $N = a^2 + b^2$ et $q = x^2 + y^2$, on a

$$Nq = (a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (ay + bx)^2$$

d'après une identité algébrique signalée plus haut. En fait, comme on peut remplacer sans dommages y par $-y$, on a

$$Nq = (ax \pm by)^2 + (ay \mp bx)^2 \qquad (*)$$

Comme q divise N, q divise

$$Ny^2 - b^2q = (a^2 + b^2)y^2 - b^2(x^2 + y^2) = a^2y^2 - b^2x^2 = (ay - bx)(ay + bx).$$

Comme q est premier, il divise alors $ay - bx$ ou $ay + bx$. S'il divise $ay - bx$, il divise aussi $Nq - (ay - bx)^2$, c'est à dire $(ax + by)^2$ d'après (*) et donc finalement $ax + by$. S'il divise $ay + bx$, il divise $Nq - (ay + bx)^2$, c'est à dire $(ax - by)^2$ et donc aussi $ax - by$. Bref, il existe un nombre ε égal à ± 1 tel que q divise à la fois $ay + \varepsilon bx$ et $ax - \varepsilon by$. On peut donc écrire $ax - \varepsilon by = qu$ et $ay + \varepsilon bx = qv$ où u et v sont deux entiers. Donc

$$Nq = (ax - \varepsilon by)^2 + (ay + \varepsilon bx)^2 = q^2u^2 + q^2v^2,$$

d'où la relation

$$\frac{N}{q} = u^2 + v^2$$

qu'il nous fallait démontrer.

Nous sommes maintenant à même de prouver entièrement le théorème attendu dont l'énoncé revient à Fermat et la démonstration à Euler : *tout nombre premier* p *de la forme* $4n + 1$ *est une somme de deux carrés.*

Le raisonnement pourrait être présenté comme une récurrence portant sur p (c'est peut-être comme cela qu'il faut comprendre Fermat quand il disait pouvoir appliquer à ce problème sa méthode de descente). Mais il est plus simple de raisonner par l'absurde en supposant qu'il existe un nombre premier p de la forme $4n + 1$ qui ne soit pas somme de deux carrés et en choisissant p le plus petit possible. Comme p est de la forme $4n + 1$, il existe deux nombres a et b premiers entre eux, tels que p divise $a^2 + b^2$. Comme on l'a déjà noté, a et b ne peuvent pas être divisibles par p. Effectuons alors la division euclidienne de a et de b par p : cela permet d'écrire

$$a = kp + r \text{ avec } 0 < r < p, \text{ soit } r \equiv a \pmod p,$$

$$b = lp + s \text{ avec } 0 < s < p \text{ soit } s \equiv b \pmod p.$$

Si $r < \frac{p}{2}$, posons $r' = r$. Si $r > \frac{p}{2}$ posons $r' = p - r$ (on notera que $\frac{p}{2}$ n'est pas un entier). On obtient ainsi un entier r' congru à r, donc à a, modulo p tel que $0 < r' < \frac{p}{2}$. Définissons de même, à partir de s, un entier s' tel que $s' \equiv s \equiv b$ avec $0 < s' < \frac{p}{2}$. Comme $r'^2 + s'^2 \equiv r^2 + s^2 \equiv a^2 + b^2 \equiv 0 \pmod p$, on voit que p divise $r'^2 + s'^2$. Soit g le PGCD de r' et de s'. Alors $r' = gr''$ et $s' = gs''$ où r'' et s'' sont des entiers premiers entre eux, vérifiant encore $0 < r'' < \frac{p}{2}$ et $0 < s'' < \frac{p}{2}$. Il est clair que p ne divise pas g, mais comme il divise $r'^2 + s'^2 = g^2\,(r''^2 + s''^2)$, il divise nécessairement $r''^2 + s''^2$. Bref, en changeant hardiment de notations, on peut conclure à l'existence de deux entiers a et b premiers entre eux qui vérifient $0 < a < \frac{p}{2}$ et $0 < b < \frac{p}{2}$ et tels que p divise $a^2 + b^2$.

Soit $N = a^2 + b^2$. On peut alors écrire $N = a^2 + b^2 < \frac{p^2}{4} + \frac{p^2}{4} < p^2$, c'est à dire $0 < \frac{N}{p} < p$. Il en résulte que les facteurs premiers $q_1, \ldots, q_n$ (avec des répétitions éventuelles) de $\frac{N}{p}$ sont tous inférieurs à p et on a $N = p\, q_1 \ldots q_n$.

On peut alors affirmer que q_i est toujours une somme de deux carrés. C'est évident si $q_i = 2$ car $2 = 1^2 + 1^2$ et cela résulte de ce que nous avons vu plus haut et du choix de p, si q_i est impair. Nous pouvons maintenant appliquer le résultat ci-dessus qui ouvre la voie du Saint Graal, autant de fois que nécessaire : N/q_1 est une somme de deux carrés $u_1^2 + v_1^2$, $N/(q_1q_2)$ est une somme de deux carrés $u_2^2 + v_2^2$, et ainsi de suite jusqu'à $N/(q_1q_2\ldots q_n)$ qu'on peut donc écrire $u_n^2 + v_n^2$. Mais cela est absurde car $N/(q_1q_2\ldots q_n) = p$. Cette contradiction clôt la démonstration.

Wilson au secours d'Euler

Le décalage entre l'énoncé d'un théorème et sa démonstration illustré par ce qui précède, a pour conséquence qu'un même théorème a souvent d'autres démonstrations, de nature tout à fait différente. Ainsi, le laborieux raisonnement d'Euler, passant par l'opérateur de différence, pour démontrer que tout nombre premier p de la forme $4n + 1$ divise une somme de deux carrés premiers entre eux peut être obtenu très rapidement et d'une toute autre manière grâce au *théorème de Wilson* selon lequel *pour tout nombre premier p, on a* $(p - 1)! \equiv -1$ (modulo p). Admettons en effet provisoirement ce résultat, supposons p de la forme $4n + 1$ et posons $m = 2n$ (ce qui fait $p = 2m + 1$). Ecrivons le produit $(p - 1)!$ sous la forme :

$$(p - 1)! = 1 \cdot 2 \ldots m\,(m + 1) \ldots (m + m)$$

ou mieux

$$(p - 1)! = (m + m)\,(m + m - 1) \ldots (m + 1)\,1 \cdot 2 \ldots m.$$

Puisque $p = 2m + 1$, il est clair que l'on a

$$m + m \equiv -1,\ m + m - 1 \equiv -2,\ \ldots,\ m + 1 \equiv -m \pmod p.$$

Par suite, le produit précédent, c'est à dire $(p - 1)!$, est congru, modulo p, à

$$(-1^2)\,(-2^2) \ldots (-m^2) = (-1)^m\,(m!)^2,$$

c'est à dire $(m!)^2$ puisque m est pair.
Comme p divise $(p - 1)! + 1$ d'après le théorème de Wilson, p divise aussi $(m!)^2 + 1$, c'est-à-dire une somme de carrés premiers entre eux…

Reste évidemment à démontrer le théorème de Wilson lui-même. Il y a, là encore, plusieurs façons de faire. L'une des plus simples consiste à vérifier que si a est un des nombres $1, 2, \ldots, p - 1$, il existe un nombre a' et un seul, figurant lui aussi dans la liste $1, 2, \ldots, p - 1$, tel que

$$aa' \equiv 1 \pmod p$$

On peut appeler a' l'inverse de a modulo p.

L'unicité de a' découle des propriétés usuelles des nombres premiers, car si a' et a'' sont deux entiers tels que $aa' \equiv 1 \pmod p$ et $aa'' \equiv 1 \pmod p$, on a aussi $aa' \equiv aa'' \pmod p$, ce qui veut dire que p divise $aa' - aa'' = a\,(a' - a'')$.
Comme p ne peut diviser a (car on a supposé $1 \le a \le p - 1$), p divise $a' - a''$. Mais si on suppose en outre $1 \le a' \le p - 1$ et $1 \le a'' \le p - 1$, on a

$$-(p - 2) \le a' - a'' \le p - 2$$

Comme le seul nombre compris entre $-(p - 2)$ et $p - 2$ qui soit divisible par p est 0, on a $a' - a'' = 0$, donc $a' = a''$.

L'existence de a' est une conséquence évidente du théorème de Bézout (que nous admettrons ici et qui en réalité était déjà connu de Bachet de Méziriac)) qui veut que *pour deux entiers a et b premiers entre eux, il existe des entiers x et y tels que* $ax + by = 1$. Appliqué au nombre a ci-dessus et au nombre premier p (qui sont premiers entre eux), il donne une relation du type $ax + py = 1$, qui implique $ax \equiv 1 \pmod p$, c'est-à-dire le résultat, avec $a' = x$.

Il est clair que a joue vis-à-vis de a' le rôle que a' joue vis-à-vis de a. Cela veut dire que $(a')' = a$. En d'autres termes, l'application $a \mapsto a'$ de l'ensemble $E = \{1, \ldots, p - 1\}$ dans lui-même est une transformation involutive (ou une involution).Bien entendu, il se peut que cette transformation ait des « points fixes », c'est-à-dire qu'il existe des éléments a de E tels que $a' = a$. Cela veut dire en fait que

$a^2 \equiv 1 \pmod p$. Comme cette congruence signifie que p divise $a^2 - 1 = (a-1)(a+1)$, elle veut dire aussi que p divise $a - 1$ ou p divise $a + 1$. Comme $1 \le a \le p - 1$, le premier cas ne peut avoir lieu que pour $a = 1$ et le second pour $a = p - 1$. Ce sont donc les deux seuls points fixes. Si on suppose $p \ge 5$ (les cas $p = 2$, $p = 3$ peuvent être traités à part), il est intéressant de restreindre l'application $a \to a'$ à l'ensemble $F = \{2, \ldots, p-2\}$. On vérifie aisément que si $a \in F$, alors $a' \in F$, de sorte qu'on a une nouvelle involution, cette fois de F, qui est sans point fixe.

Si on regroupe chaque élément a de F avec son inverse a¢, on partage F en $\frac{p-3}{2}$ classes différentes, ayant chacune deux éléments distincts. Si on procède à ce regroupement avec les facteurs du produit 2 . 3 … (p - 2), on obtient alors $\frac{p-3}{2}$ facteurs, tous congrus à 1 modulo p (puisque aa¢ ∫ 1). D'où

$$(p-1)! = 1 \cdot 2 \cdot 3 \ldots (p-2)\,(p-1) \equiv 1\,(p-1) = p - 1 \equiv -1 \pmod p.$$

Le théorème de Wilson est démontré.

De mieux en mieux

On pourrait donner d'autres exemples de démonstrations multiples dans le domaine des sommes de deux carrés. La plus spectaculaire, découverte récemment, consiste à démontrer directement le principal résultat qui a fait l'objet des développements précédents sans passer par aucune des étapes intermédiaires décrites ci-dessus. Curieusement ce nouveau raisonnement fait intervenir les propriétés des transformations involutives vues dans la partie précédente et, en particulier, le résultat auquel on était parvenu en substance selon lequel *si on enlève d'un ensemble fini* E *les points fixes d'une involution f de* E, *le nombre d'éléments restants est pair*. Corollairement, *s'il existe dans* E *une involution ayant un nombre impair de points fixes, alors* le nombre d'éléments de E est lui aussi impair et surtout *toute involution de* E *admet au moins un point fixe.*

Considérons dans ces conditions un nombre premier p de la forme $4n + 1$ et appelons E l'ensemble des triplets $(x,y,z) \in \mathbf{N}^3$ tels que $x^2 + 4yz = p$. Il est clair que l'application $(x,y,z) \mapsto (z,y,x)$ est une involution de E et que tout point fixe de cette involution fournit une relation du type $x^2 + 4y^2$, donc une décomposition de p en sommes de deux carrés. Pour démontrer alors l'existence de ce genre de décomposition, il suffit, d'après ce qui précède, de trouver une seconde involution de E, ayant un nombre impair de points fixes.

Cette involution est l'application f définie par

$$(x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z) & \text{si } x < y-z, \\ (2y-x, y, x-y+z) & \text{si } y-z < x < 2y, \\ (x-2y, x-y+z, y) & \text{si } x > 2y. \end{cases}$$

Sans entrer dans tous les détails de la vérification, notons d'abord que dans tous les cas $f(x,y,z) \in \mathbf{N}^3$. Ensuite, si on appelle A, B, C les ensembles de triplets $(x,y,z) \in$ E tels que l'on ait $x < y - z$, $y - z < x < 2y$, $x > 2y$ respectivement, alors A, B et C forment une « partition » de E (ce sont trois ensembles deux à deux disjoints dont la réunion est E) ; on notera que les relations $x = y - z$ et $x = 2y$ sont impossibles, de même d'ailleurs que $xyz = 0$.

Puis pour vérifier que f est bien une involution, on montrera que f applique A dans C, B dans B et C dans A. Quant aux points fixes éventuels, ils ne peuvent être que dans B. Comme ce sont alors ceux pour lesquels $2y - x = x$ et $x - y + z = z$ on doit avoir $x = y$, donc $x^2 + 4xz = p$. Comme p est premier, on a nécessairement $x = 1$ et donc $y = 1$, et $z = \dfrac{p-1}{4}$. Ces relations fournissent effectivement un point fixe, le seul possible. CQFD.

Une petite pause du coté de l'infinité des nombres premiers

Pour ceux que les sommes de carrés commencent à fatiguer, revenons au problème tout différent de l'infinité des nombres premiers, déjà abordé dans l'introduction. Beaucoup d'autres méthodes, d'autres démonstrations ont été proposées depuis Euclide. En voici une, trouvée dans un numéro de l'*American Mathematical Monthly* (mars 1971, p. 272). Elle consiste à s'intéresser à la « série » $\dfrac{1}{p}$ où p parcourt l'ensemble des nombres premiers (attention, compte tenu de notre propos, il peut s'agir d'un ensemble fini…) et parallèlement à la « série » $\dfrac{1}{q}$ où q parcourt l'ensemble (fini ou non !) des nombres sans facteurs carrés, c'est-à-dire des nombres (entiers positifs) qui ne sont divisibles par aucun carré > 1.

En fait, il est facile de montrer que cette dernière série comporte nécessairement une infinité de termes et, même mieux, que c'est une série divergente. Pour cela, on commence par remarquer que tout entier $n \geq 1$ peut s'écrire sous la forme d'un produit qc^2 où q est un nombre sans facteurs carrés et c un entier ≥ 1. Cette écriture est d'ailleurs unique, mais on n'a pas besoin de le savoir pour la suite. Si on développe alors un produit de la forme $\left(\sum_{q \leq N} \dfrac{1}{q}\right)\left(\sum_{c \leq N} \dfrac{1}{c^2}\right)$ où N est un entier ≥ 1 fixé (et où q est sans facteurs carrés !), on obtient, entre autres choses, au moins une fois, tous les inverses $\dfrac{1}{n}$ où $1 \leq n \leq N$. On a donc l'inégalité

$$\left(\sum_{q \leq N} \frac{1}{q}\right)\left(\sum_{c \leq N} \frac{1}{c^2}\right) \geq \sum_{n \leq N} \frac{1}{n}.$$

La somme du second membre peut être rendue aussi grande que l'on veut (divergence de la série harmonique) et au contraire la somme $\sum_{n \leq N} \dfrac{1}{n^2}$ est bornée car, à cause de la relation $\frac{1}{n^2} < \frac{1}{n(n-1)} = \frac{1}{n-1} - \frac{1}{n}$, on peut écrire

$$\sum_{n \le N} \frac{1}{n^2} < 1 + 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \ldots + \frac{1}{N-1} - \frac{1}{N} = 2 - \frac{1}{N} < 2.$$

La série $\sum \frac{1}{q}$ ne peut donc être que divergente. On peut alors en déduire que la série $\sum \frac{1}{p}$ est aussi divergente. Pour cela on fait intervenir l'inégalité élémentaire $e^x > 1 + x$ valable pour tout $x > 0$. Si la série des inverses des nombres premiers convergeait vers un nombre a, on aurait (avec un entier $N \ge 1$ quelconque)

$$e^a > e^{\sum_{p \le N} \frac{1}{p}} = \prod_{p \le N} e^{\frac{1}{p}} > \prod_{p \le N} \left(1 + \frac{1}{p}\right)$$

Mais si on développe le produit final, on obtient entre autres tous les nombres $\frac{1}{q}$ avec $q \le N$ et q sans facteurs carrés. D'où

$$e^a > \prod_{p \le N} \left(1 + \frac{1}{p}\right) \ge \sum_{q \le N} \frac{1}{q},$$

ce qui est absurde car la somme obtenue dépasse, comme on l'a vu, n'importe quel nombre donné à l'avance.

Ainsi, non seulement il y a une infinité de nombres premiers p mais en plus on a $\sum \frac{1}{p} = +\infty$, résultat assez étonnant qui fut démontré pour la première fois par Euler en 1737.

Comme disait Gauss, « la diversité des méthodes aide beaucoup à jeter du jour sur les points les plus obscurs ». Gauss savait de quoi il parlait, lui qui a donné quatre démonstrations différentes du théorème fondamental de l'algèbre et huit de la loi de réciprocité quadratique !

Ultime retour sur les entiers somme de deux carrés

Tout ce foisonnement fait évidemment le bonheur de l'amateur, éclairé ou non. S'il est un peu au-dessus de la moyenne, il peut lui-même intervenir en démontrant des résultats ou en simplifiant des raisonnements qui ont pu échapper à l'attention de ses prédécesseurs plus ou moins illustres. L'histoire de la théorie des nombres en offre de multiples exemples.

Citons seulement le cas d'un certain L. Aubry qui fit paraître en 1912 dans une revue bizarrement appelée *Sphinx-Œdipe* une démonstration élémentaire sur les sommes de carrés qu'auraient bien aimé connaître Fermat et Euler lorsqu'ils faisaient leurs propres recherches. C'est une autre façon de démontrer un résultat déjà étudié précédemment sans passer par l'astuce, pas facile à trouver, du signe à utiliser à bon escient dans la formule :

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' \pm yy')^2 + (xy' \mp x'y)^2.$$

Rappelons qu'il s'agit de démontrer que, si q divise une somme N de deux carrés $a^2 + b^2$ et si q lui-même est une somme de deux carrés $x^2 + y^2$, alors $\frac{N}{q}$ est à son tour une somme de deux carrés $u^2 + v^2$. À cause de la formule rappelée ci-dessus (et avec un seul signe), on a

$$\frac{N}{q} = \frac{a^2+b^2}{x^2+y^2} = \frac{(a^2+b^2)(x^2+y^2)}{(x^2+y^2)^2} = \left(\frac{ax-by}{x^2+y^2}\right)^2 + \left(\frac{ay+bx}{x^2+y^2}\right)^2,$$

ce qui veut dire que N/q est une somme de deux carrés « in fractis » comme disait Euler. Peut-on en déduire que c'est une somme de deux carrés « in integris » ? C'est ce qu'affirme le théorème d'Aubry, qu'on peut présenter sous une forme agréablement géométrique en disant que *si un cercle du plan* $\mathbf{R}^2$*, d'équation* $x^2 + y^2 = \mathrm{N}$ *(avec* N *entier* ≥ 1*), passe par un point rationnel* (i.e. un point à coordonnées rationnelles), *alors il passe aussi par un point entier* (i.e. un point à coordonnées entières).

On partira d'un résultat préliminaire simple selon lequel *pour tout point* $\mathrm{A} = (x,y)$ *du plan* $\mathbf{R}^2$*, il existe un point entier* $\mathrm{A}' = (x',y')$ *dont la distance à* A *est plus petite que* 1. Il suffit en fait d'appeler x' l'entier le plus proche de x (égal à la partie entière de $x + 1/2$) et y' l'entier le plus proche de y car on a alors $|x - x'| \leq 1/2$ et $|y - y'| \leq 1/2$, d'où

$$\mathrm{AA}' = \sqrt{(x-x')^2 + (y-y')^2} \leq \sqrt{\frac{1}{4}+\frac{1}{4}} = \frac{\sqrt{2}}{2} < 1.$$

Cela étant, considérons un cercle d'équation $x^2 + y^2 = \mathrm{N}$ (N entier ≥ 1) passant par un point rationnel A_0. Si A_0 est un point entier, il n'y a rien à démontrer. Sinon, considérons un point entier A'_0 tel que $\mathrm{A}_0\mathrm{A}'_0 < 1$. Comme $\mathrm{A}_0 \neq \mathrm{A}'_0$, on peut considérer la droite $\mathrm{A}_0\mathrm{A}'_0$, qui coupe le cercle en A_0, et en un « autre » point A_1 (qu'on prendra égal à A_0 si d'aventure la droite est tangente au cercle). Si A_1 est un point entier, on arrête. Sinon, on recommence en considérant un point entier A'_1 du plan tel que $\mathrm{A}_1\mathrm{A}'_1 < 1$ et la droite $\mathrm{A}_1\mathrm{A}'_1$ qui recoupe le cercle en un point A_2. Si A_2 est un point entier, on arrête sinon on recommence.

Tout le problème est de montrer que le processus ainsi décrit ne peut pas se poursuivre indéfiniment. Pour le voir, on commence par vérifier que tous les points A_i précédents sont rationnels. Il suffit de procéder par récurrence en vérifiant que lorsque A_i est un point rationnel non entier, alors A_{i+1} est encore un point rationnel. Sinon, posons $\mathrm{A}_i = (x,y) = (m/d,n/d)$ où m, n, d sont des entiers et où $d \geq 2$. Comme

A'_i est supposé entier, on peut poser simplement $A'_i = (x', y') = (m', n')$ avec m' et n' entiers. Dans ces conditions, les points de la droite $A_i A'_i$ sont les points du plan de la forme $\left(m' + t\left(\frac{m}{d} - m'\right), n' + t\left(\frac{n}{d} - n'\right)\right)$ où t est un paramètre variable. La recherche des points de cette droite qui appartiennent au cercle $x^2 + y^2 = \mathrm{N}$ conduit immédiatement à une équation du second degré en t qui s'écrit

$$\left[\left(\frac{m}{d} - m'\right)^2 + \left(\frac{n}{d} - n'\right)^2\right] t^2 + 2\left[m'\left(\frac{m}{d} - m'\right) + n'\left(\frac{n}{d} - n'\right)\right] t + m'^2 + n'^2 - \mathrm{N} = 0.$$

Cette équation a une solution simple $t = 1$ qui correspond en fait à $A_i = (m/d, n/d)$, alors que l'autre solution

$$t = \frac{m'^2 + n'^2 - \mathrm{N}}{\left(\frac{m}{d} - m'\right)^2 + \left(\frac{n}{d} - n'\right)^2}$$

(qu'on écrira $t = \frac{\mathrm{M}}{\mathrm{D}^2}$ où $\mathrm{M} \in \mathbf{Z}$ et où D est la distance $A_i A'_i$) correspond au point A_{i+1}. Cette expression prouve bien que les coordonnées de A_{i+1} sont deux nombres rationnels, à savoir $m' + \frac{\mathrm{M}}{\mathrm{D}^2}\left(\frac{m}{d} - m'\right)$ et $n' + \frac{\mathrm{M}}{\mathrm{D}^2}\left(\frac{n}{d} - n'\right)$. Mais le carré D^2 vaut en fait $\mathrm{N} + m'^2 + n'^2 - 2\frac{mm' + nn'}{d}$ comme on le vérifie aussitôt. C'est donc une fraction qu'on peut écrire $\frac{d_1}{d}$ avec d_1 entier > 0. Si on reporte cette fraction dans les expressions donnant les coordonnées de A_{i+1}, celles-ci se simplifient pour donner deux nombres s'écrivant $\frac{m_1}{d_1}$ et $\frac{n_1}{d_1}$ avec m_1 et n_1 entiers. Enfin comme $\mathrm{D}^2 < 1$, on a nécessairement $d_1 < d$.

On voit alors que si le processus décrit ci-dessus se poursuivait indéfiniment, on aurait une suite illimitée d'entiers > 0, d_0, d_1, d_2, d_3, … telle que $d_0 > d_1 > d_2 > d_3 > \ldots$, ce qui est absurde (impossibilité d'une descente infinie portant sur des entiers positifs). D'où le résultat.

Pour notre plaisir à tous

Si on désespère de rivaliser avec L. Aubry, on peut se transformer en amateur d'histoire des mathématiques, spécialité arithmétique, car, comme on vient de le voir, on peut faire de l'arithmétique en se référant aux grands noms du passé. C'est d'autant plus facile que de 1636 à 1837 la théorie des nombres a une histoire assez simplissime qui se résume aux noms de Fermat, Euler, Lagrange, Legendre, Gauss et Dirichlet. Mais l'amateur peut remonter au Moyen Age, en se procurant par exemple le *Liber quadratorum* de Fibonacci ou en s'initiant aux mathématiques arabes par l'intermédiaire de Roshdi Rashid, ou même à l'Antiquité grecque puisque Fermat lui-même puisait son inspiration dans les *Arithmétiques* de Diophante. S'il a du courage, il peut s'attaquer à l'imposant XIX^e siècle où les découvertes en en arithmétique abondent (de Gauss, avec ses *Disquisitiones arithmeticae* de 1801 à Hilbert avec son célèbre *Zahlbericht* de 1897) et, pourquoi pas, au siècle tout juste défunt… même si on peut trouver plutôt déprimante la lecture du *Journal of Number Theory* ou des *Acta Arithmetica*.

Mais l'amateur lambda peut aussi, comme Lagrange à la fin de sa vie, se contenter « de jouir sur cette matière, comme sur plusieurs autres, du fruit des veilles d'autrui ». Sans aller jusqu'à éprouver ce plaisir si singulier qui accompagne, selon André Weil, la découverte chez les chercheurs (Weil va jusqu'à le comparer au plaisir érotique, en plus durable !), on peut faire son miel en arithmétique de beaucoup de bonnes choses. Outre les sommes de carrés ou la théorie des nombres premiers, bien d'autres domaines d'étude sont accessibles pour l'amateur de bonne volonté. On peut ainsi lire des merveilles sur les fractions continues, les nombres transcendants, le grand théorème de Fermat ou la fonction zêta. Même de nos jours, il se publie des choses propres à satisfaire l'amateur comme le montrent les exemples cités plus haut. Mais il faut faire le tri et ce n'est pas si simple, même si on dispose des « *Reviews in Number Theory* » de l'American Mathematical Society. En fait, ce qui manque, il faut bien le dire, c'est un Journal d'arithmétique pour amateurs (JAPA). Il faudrait des bonnes volontés et un éditeur. Qu'est-ce qu'on attend ?

Éléments bibliographiques

Peter BUNDSCHUH, *Einführung in die Zahlentheorie*, Springer-Verlag, Berlin Heidelberg, 1988

Marc GUINOT, *Les « resveries » de Fermat* (*Arithmétique pour amateur, Livre II*), Aléas Editeur, Lyon, 1993

Michel DEMAZURE, *Cours d'algèbre*. Cassini, 1997.

HARDY, WRIGHT, *An Introduction to the Theory of Numbers*, 5^e éd., Oxford University Press, 1975.

H.E. ROSE (quelle manie, ces prénoms réduits à des initiales !), *A Course in Number Theory*, Oxford University Press, Oxford, 1988

André WEIL, *Number Theory, An approach through history, From Hammurapi to Legendre*, Birkhäuser, Bâle, 1983

Approximation des nombres réels par des rationnels

Mathieu Savin

Position du problème

La découverte de nombres irrationnels a profondément troublé les mathématiciens grecs. En effet, ils étaient habitués à des énoncés de théorèmes qui avaient un support graphique clair : la géométrie euclidienne fournit des énoncés qui pourraient être considérés comme des assertions décrivant le monde réel. Les théorèmes de la géométrie euclidienne sont tous vérifiables à la règle et au compas ; ils ne sont certes pas démontrables sans utiliser des outils mathématiques comme des axiomes et des règles de logique, mais on peut en vérifier la pertinence et l'exactitude. Même l'arithmétique a un support palpable : les énoncés des problèmes et exercices classiques se placent souvent dans un cadre assez rural (des moutons, des épis de blé, de sombres histoires d'héritage à partager…).

Mais l'irrationalité de certains nombres, c'est-à-dire l'impossibilité de les exprimer comme des quotients de nombres entiers, n'a absolument aucun support dans le monde réel. Il est impossible de mesurer une longueur et d'affirmer aussitôt que cette longueur est incommensurable avec l'unité : aucune règle, si perfectionnée soit-elle, ne pourra jamais permettre à elle seule de vérifier ce théorème. Non seulement il faut rentrer dans le domaine des mathématiques pures pour prouver que $\sqrt{2}$ est irrationnel, mais il est impossible d'en sortir pour le vérifier.

Le problème avec ces nombres irrationnels est qu'il n'existe pas de manière simple d'effectuer avec eux des opérations qui sont usuelles et faciles avec des rationnels. Il est par exemple difficile de décrire le nombre $\sqrt{2}+\sqrt{3}$: on peut, bien sûr, construire géométriquement cette longueur à l'aide de triangles rectangles, mais il n'est pas facile d'expliquer que ce nombre comporte une réalité mathématique que le dessin ne permet pas d'appréhender. Quant à des nombres tels que e, π, ou ln 2, on ne peut pas les dessiner, bien qu'ils aient une existence. Les nombres irrationnels sont souvent définis par des propriétés qui, si elles permettent certains calculs, compliquent tous les autres. Il est donc naturel d'essayer de remplacer dans les calculs ces nombres irrationnels par des fractions de nombres entiers, qui rendent les calculs plus faciles. Le problème qui se pose alors est celui de l'approximation de ces nombres. On a ainsi longtemps utilisé en pratique l'approximation $\pi \approx 22/7$ pour trouver une valeur approchée de l'aire d'un disque.

Notre objectif sera de présenter des résultats généraux sur l'approximation des réels par des nombres rationnels. Un des résultats les plus surprenants que fournit cette théorie est le suivant : plus il est facile de trouver une approximation correcte d'un nombre réel, plus celui-ci est compliqué. Nous donnerons bien sûr un sens précis à cette expression au cours de ces quelques pages. Pour l'essentiel, l'esprit de cet article est bien d'étudier les réels et d'essayer de voir quelles sont les caractéristiques de ces nombres qui permettent une approximation plus efficace par des rationnels. Nous laisserons de côté des questions plus complexes, comme celle de l'influence de l'approximation sur les calculs, autrement dit de l'évaluation de l'erreur commise lorsqu'on remplace dans un calcul le nombre par son approximation. Dans la mesure où il faudrait développer l'artillerie lourde des fractions continues, qui fournissent la solution du problème, nous n'aborderons pas les méthodes permettant d'obtenir les meilleures approximations. Nous nous cantonnerons à l'aspect théorique de cette question.

Dans toute la suite, ξ désignera un nombre réel fixé.

Quelques résultats faciles

Théorème 1. *Tout nombre réel est limite d'une suite de nombre rationnels.*

On ne peut pas démontrer rigoureusement ce théorème à un niveau élémentaire. En effet, si on essaye de le prouver, il faut définir précisément un nombre réel : il faut avoir un moyen de décrire les éléments de $\mathbf{R}$ et pour cela il faut savoir comment cet ensemble est construit. Or justement cette construction n'est pas élémentaire : c'est ce qui rend le théorème difficile. On peut en tout cas presque voir ce théorème comme une définition des nombres réels : on n'est pas très loin de la réalité.

Mais si la preuve rigoureuse de ce théorème n'est pas élémentaire, il est en tout cas facile d'en donner une preuve en utilisant une définition intuitive des nombres réels. Un réel a une écriture décimale, qui n'est peut-être pas unique(1), mais ce n'est pas important. Si on considère le nombre qu'on obtient en prenant les n premières décimales de ξ, c'est un nombre qui s'écrit sous la forme $\frac{p}{10^n}$, où p est entier ; la différence entre ξ et ce nombre rationnel est inférieure à 10^{-n} : et ainsi ce rationnel est une approximation de ξ à la précision 10^{-n}. Comme n est arbitraire, on obtient ainsi une approximation aussi bonne qu'on veut. Il existe ainsi une infinité de solutions $(p,q) \in \mathbf{Z} \times \mathbf{N}^*$ de l'inéquation

$$\left|\xi - \frac{p}{q}\right| \leq \frac{1}{q} \ ;$$

nous n'avons pas démontré ce résultat pour tous les dénominateurs q possibles, mais seulement pour ceux qui sont de la forme 10^n. Nous n'avons pas non plus démontré que les fractions p/q représentent toutes des rationnels distincts : ce serait d'ailleurs faux si ξ était un nombre décimal.

(1) En effet, on peut écrire $1 = 0{,}999\ldots$. Ceci se démontre simplement : si on pose $x = 0{,}999\ldots$, alors $10x = 9{,}99\ldots$, et ainsi $10x = 9 + x$; on en déduit $9x = 9$, puis $x = 1$.

Mais on peut améliorer ce résultat :

Théorème 2. *Si $q \in \mathbf{N}^*$, il existe $p \in \mathbf{Z}$ tel que*

$$\left|\xi - \frac{p}{q}\right| \leq \frac{1}{2q}.$$

Notons ici qu'on améliore le résultat de deux points de vue : premièrement, on a une majoration avec un dénominateur arbitraire ; et ensuite, nous remplaçons $1/q$ par $1/2q$, en diminuant ainsi de moitié l'erreur commise dans l'approximation.

Preuve. Considérons l'ensemble $\frac{1}{q}\mathbf{Z}$ de tous les nombres rationnels qui peuvent s'écrire sous la forme k/q, où k est entier. Ces nombres définissent des intervalles semi-ouverts de la forme $\left[\frac{k}{q}, \frac{k+1}{q}\right[$; chacun de ces intervalles est de longueur $\frac{1}{q}$, ils sont disjoints et leur réunion est $\mathbf{R}$ tout entier.

Ainsi ξ se trouve nécessairement dans un de ces intervalles $\left[\frac{k}{q}, \frac{k+1}{q}\right[$; mais alors :

– si $\xi \in \left[\frac{k}{q}, \frac{k}{q} + \frac{1}{2q}\right[$, on prend $p = k$ et alors $\left|\xi - \frac{p}{q}\right| \leq \frac{1}{2q}$;

– si $\xi \in \left[\frac{k}{q} + \frac{1}{2q}, \frac{k+1}{q}\right[$, on prend $p = k + 1$ et on obtient encore la même inégalité.

Ce théorème est déjà très utile dans la pratique. On peut l'appliquer de deux façons : soit on se donne une valeur du dénominateur à ne pas dépasser, et cela détermine la marge d'erreur que nous obtiendrons ; soit on se donne une marge d'erreur à l'avance, et cela détermine alors une taille minimum du dénominateur qu'il nous faudra utiliser pour notre approximation. Remarquons aussi que rien ne garantit ici que les fractions obtenues sont écrites sous forme irréductible.

En tout cas, nous allons nous orienter dans les directions suivantes :

• Nous essaierons de trouver une infinité d'approximations *distinctes* : c'est-à-dire que nous chercherons des rationnels distincts qui s'approchent de ξ.

• Nous ne chercherons pas à avoir des approximations avec un dénominateur imposé, pour deux raisons : il est difficile de contrôler qu'on obtient une infinité d'approximations, et les meilleures approximations ne peuvent pas se faire en imposant le dénominateur. Par exemple, il est hérétique d'approximer π avec un dénominateur égal à 10, puisque 31/10 est une approximation moins bonne que 22/7.

• Nous chercherons à majorer l'erreur de l'approximation en fonction du dénominateur du rationnel ; les fonctions les plus simples étant les fonctions puissances, nous chercherons à majorer l'erreur par l'inverse de puissances du dénominateur.

Définition. *Fixons un entier $\alpha \geq 1$; on dira qu'un réel ξ est* ***approximable à l'ordre*** α *s'il existe une constante* A > 0 *pour laquelle l'inégalité*

$$\left|\xi - \frac{p}{q}\right| \leq \frac{A}{q^\alpha}$$

est vérifiée pour une infinité de rationnels p/q.

Nous verrons assez vite que ce problème n'admet pas toujours des solutions, et que le rôle de α est essentiel. Notons aussi que le nombre A peut dépendre de ξ, et que, si ξ est approximable à l'ordre α, il est approximable à n'importe quel ordre inférieur à α.

Un exemple : approximation de $\sqrt{2}$

Nous allons définir une suite de rationnels qui convergera vers $\sqrt{2}$, et dont nous contrôlerons facilement l'écart avec sa limite ; nous nous efforcerons ensuite d'exprimer cet écart en fonction du dénominateur des fractions, et nous démontrerons ainsi que $\sqrt{2}$ est approximable à l'ordre 2.

Considérons la suite $(u_n)_{n\in\mathbf{N}}$ définie par(2) : $u_0 = 1$, et

$$\forall n \in \mathbf{N} \quad u_{n+1} = \frac{u_n}{2} + \frac{1}{u_n}.$$

On trouve, comme valeurs approchées à 10^{-12} près :

$$u_1 = 1{,}5$$
$$u_2 = 1{,}416\,666\,666\,667$$
$$u_3 = 1{,}414\,215\,686\,275$$
$$u_4 = 1{,}414\,213\,562\,375$$

et on voit que cette suite approche très vite de $\sqrt{2}$.

Il est facile de vérifier par récurrence que, pour tout $n \in \mathbf{N}$, u_n est un rationnel qui vérifie l'inégalité $1 \leq u_n \leq 2$. De plus, si on écrit $u_n = p_n/q_n$, alors les suites $(p_n)_{n\in\mathbf{N}}$ et $(q_n)_{n\in\mathbf{N}}$ peuvent être définies par récurrence en posant $p_0 = q_0 = 1$, et :

$$\forall n \in \mathbf{N} \quad \begin{cases} p_{n+1} = p_n^2 + 2q_n^2, \\ q_{n+1} = 2p_nq_n. \end{cases}$$

On ne se complique pas la tâche ici de savoir si l'écriture p_n/q_n donnée par cette formule est irréductible ou pas ; ce n'est pas important. Signalons simplement que

(2) Cette suite ne sort pas magiquement d'un chapeau : elle est un cas particulier de la méthode de Newton, appliquée à la fonction $f(x) = x^2 - 2$ au voisinage de $\sqrt{2}$. Quand la méthode s'applique, la suite définie par $u_{n+1} = u_n - \dfrac{f(u_n)}{f'(u_n)}$ converge vers le point c tel que $f(c) = 0$.

cette formule montre, par récurrence, que $q_n > 0$ et $p_n > 0$.

Remarquons que p_{n+1} ressemble à une somme de carrés, et que q_{n+1} ressemble à un double produit ; en tâtonnant un peu, on trouve :

$$\forall n \in \mathbf{N} \quad p_{n+1} - \sqrt{2}\, q_{n+1} = (p_n - \sqrt{2}\, q_n)^2$$

et ainsi, par une récurrence facile, on obtient

$$\forall n \in \mathbf{N} \quad p_n - \sqrt{2}\, q_n = (p_0 - \sqrt{2}\, q_0)^{2^n} = (1 - \sqrt{2})^{2^n}.$$

On en déduit que, comme 2^n est pair dès que $n \geq 1$,

$$\forall n \in \mathbf{N} \quad \frac{p_n}{q_n} - \sqrt{2} = (\sqrt{2} - 1)^{2^n} \frac{1}{q_n}.$$

On obtient ainsi une approximation de $\sqrt{2}$ à l'ordre 1, mais le coefficient devant $1/q_n$ tend vers 0 très rapidement : on doit pouvoir mieux faire. Signalons en tout cas que, comme $q_n \geq 1$, on peut majorer $\left|u_n - \sqrt{2}\right|$ par une suite qui converge très rapidement vers 0, ce qui prouve que $\lim\limits_{n \to +\infty} u_n = \sqrt{2}$.

De façon plus précise, l'égalité obtenue prouve que $u_n - \sqrt{2}$ est un nombre strictement positif dès que $n \geq 1$; et ainsi $u_n > \sqrt{2}$, pour tout $n \geq 1$. Mais aussi

$$\forall n \geq 1 \quad u_{n+1} - u_n = \frac{1}{u_n} - \frac{u_n}{2} = \frac{2 - u_n^2}{2u_n} < 0,$$

et ainsi la suite $(u_n)_{n \in \mathbf{N}}$ est strictement décroissante à partir de u_1 : on en déduit que tous les termes de cette suite sont distincts, puisque de plus $u_0 < \sqrt{2} < u_n$ si $n \geq 1$.

Pour améliorer les résultats obtenus, remarquons d'abord qu'on a utilisé ci-dessus une identité remarquable, celle qui fournit $(a - b)^2$; si on utilise l'autre identité pour $(a + b)^2$, on trouve :

$$\forall n \in \mathbf{N} \quad p_{n+1} + \sqrt{2}\, q_{n+1} = (p_n + \sqrt{2}\, q_n)^2$$

et ainsi

$$\forall n \in \mathbf{N} \quad p_n + \sqrt{2}\, q_n = (p_0 + \sqrt{2}\, q_0)^{2^n} = (1 + \sqrt{2})^{2^n}.$$

L'inégalité que vérifie u_n montre que $q_n \leq p_n$, et ainsi

$$(1 + \sqrt{2})q_n \leq p_n + \sqrt{2}\, q_n$$

et donc

$$\frac{1}{1+\sqrt{2}}\frac{1}{q_n}\geq\frac{1}{(1+\sqrt{2})^{2^n}}.$$

Or $\sqrt{2}-1=\dfrac{1}{\sqrt{2}+1}$, et on peut écrire

$$\left|\frac{p_n}{q_n}-\sqrt{2}\right|=(\sqrt{2}-1)^{2^n}\frac{1}{q_n}=\frac{1}{(\sqrt{2}+1)^{2^n}}\frac{1}{q_n}\leq\frac{1}{1+\sqrt{2}}\frac{1}{q_n^2}=\frac{\sqrt{2}-1}{q_n^2}.$$

Comme ceci est vrai pour tout n et que tous les rationnels $u_n = p_n/q_n$ sont distincts, on en déduit que $\sqrt{2}$ est approximable à l'ordre 2 (le nombre A de la définition vaut ici $\sqrt{2}-1$), et que la suite $(u_n)_{n\in\mathrm{N}}$ donne une infinité d'approximations à l'ordre 2. Nous avions remarqué que la convergence de $(u_n)_{n\in\mathrm{N}}$ vers $\sqrt{2}$ est très rapide, et cela ne se voit pas dans cette inégalité : tout ce que cette dernière majoration montre, c'est que $\sqrt{2}$ est approximable à l'ordre 2.

Au passage, les deux égalités obtenues pour $p_n+\sqrt{2}\,q_n$ et $p_n-\sqrt{2}\,q_n$ permettent de calculer explicitement p_n et q_n, en résolvant un système de deux équations à deux inconnues ; on trouve :

$$\begin{cases} p_n=\dfrac{(1+\sqrt{2})^{2^n}+(1-\sqrt{2})^{2^n}}{2}, \\ q_n=\dfrac{(1+\sqrt{2})^{2^n}-(1-\sqrt{2})^{2^n}}{2\sqrt{2}}. \end{cases}$$

C'est un exercice d'application de la formule du binôme que de vérifier sur ces formules que p_n et q_n sont entiers, et d'en donner une expression à l'aide de sommes de coefficients binomiaux.

Approximations d'ordre 1 et d'ordre 2

Nous allons caractériser maintenant les nombres réels qui sont approximables à l'ordre 1, et ceux qui sont approximables à l'ordre 2.

Lemme 3. *Soit $(r_n)_{n\in\mathrm{N}}$ une suite bornée de rationnels ; écrivons $r_n = p_n/q_n$, avec $q_n > 0$. Si tous les r_n sont distincts, alors la suite $(q_n)_{n\in\mathrm{N}}$ n'est pas majorée.*

Ce lemme peut être admis : il est intuitivement évident, puisqu'il semble difficile d'obtenir une infinité de fractions dans un intervalle donné avec un dénominateur borné.

Preuve. Procédons par contraposée ; si la suite $(q_n)_{n\in\mathrm{N}}$ est majorée, elle admet un plus grand élément N ; tous les rationnels r_n s'écrivent alors avec un dénominateur inférieur à N. Posons $r_n = \frac{p'_n}{N!}$; les p'_n sont entiers, puisque N! est forcément multiple de q_n.

La suite $(r_n)_{n \in \mathbf{N}}$ étant bornée, on en déduit que la suite d'entiers (p'_n $)_{n \in \mathbf{N}}$ est bornée aussi, car $p'_n = ar_n$, où $a = N!$ est une constante. Elle ne peut donc pas prendre une infinité de valeurs distinctes, puisque tout sous-ensemble borné de **Z** est fini. On en déduit que les p'_n ne sont pas tous distincts, c'est-à-dire que les r_n ne sont pas tous distincts.

Proposition 4. *En particulier, si un réel est approximable à un certain ordre* α, *l'ensemble des dénominateurs* $q > 0$ *des rationnels* p/q *tels que*

$$\left|\xi - \frac{p}{q}\right| \leq \frac{A}{q^\alpha}$$

est non majoré.

Cette proposition peut elle aussi être admise. Elle nous servira dans des démonstrations par l'absurde : pour montrer que certains nombres ξ ne sont pas approximables à un certain ordre α, on supposera qu'ils le sont, et on montrera alors que l'ensemble des dénominateurs des approximations est majoré : on en déduira que l'hypothèse initiale, c'est-à-dire que ξ est approximable à l'ordre α, est absurde.

Preuve. On peut construire une suite $(r_n)_{n \in \mathbf{N}}$ d'approximations distinctes de ξ, où $r_n = p_n/q_n$, telles que

$$\left|\frac{p_n}{q_n}\right| \leq |\xi| + \left|\frac{p}{q} - \xi\right| \leq |\xi| + \frac{A}{q_n^\alpha} \leq |\xi| + A \ ;$$

la suite r_n étant bornée et formée de rationnels distincts, on en déduit, d'après le lemme 3, que les dénominateurs q_n ne sont pas majorés.

Le résultat suivant démontre, si on en avait besoin, qu'il n'est pas très raisonnable de chercher à approximer un rationnel : non seulement cela semble ridicule, mais en plus les approximations sont forcément les moins efficaces possibles.

Théorème 5. *Si* ξ *est un rationnel, alors* ξ *est approximable à l'ordre* 1 *et à aucun ordre supérieur.*

Preuve. Écrivons $\xi = a/b$ sous forme irréductible. Comme a et b sont premiers entre eux, le théorème de Bezout affirme que l'équation $aq - bp = 1$ admet un couple de solutions (q_0, p_0). Mais alors, si k est entier, le couple $(q_0 + kb, p_0 + ka)$ est aussi solution de cette équation. Nous avons ainsi une infinité de quotients p/q tels que :

$$\frac{a}{b} - \frac{p}{q} = \frac{1}{bq}.$$

Ces quotients sont en fait écrits sous forme irréductible, mais nous allons prouver uniquement qu'ils sont tous distincts : en effet, si p/q et p'/q' vérifient l'égalité plus haut et si $\frac{p}{q} = \frac{p'}{q'}$, alors

$$\frac{a}{b} - \frac{p}{q} = \frac{1}{bq} = \frac{1}{bq'} = \frac{a}{b} - \frac{p'}{q'},$$

et ainsi $q = q'$, et on en déduit $p = p'$. Il existe ainsi une infinité de rationnels p/q tels que

$$\left|\xi - \frac{p}{q}\right| \leq \frac{1}{bq},$$

et ainsi ξ est approximable à l'ordre 1.

Il nous reste à voir que ξ n'est pas approximable à un ordre supérieur à 1 ; pour cela, il suffit de montrer qu'il n'est pas approximable à l'ordre 2. Cela se fait par l'absurde : si on peut approximer $\xi = a/b$ à l'ordre 2, il existe une constante A telle que l'inégalité

$$\left|\xi - \frac{p}{q}\right| \leq \frac{A}{q^2}$$

admette une infinité de solutions. Mais si $p/q \neq \xi$, on peut calculer :

$$\left|\xi - \frac{p}{q}\right| = \left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq},$$

puisque le numérateur est un nombre entier qui n'est pas nul ; et ainsi nous avons $bq \geq q^2/A$, soit $q \leq bA$. L'ensemble des dénominateurs des approximations de ξ est majoré : il y a une contradiction, au vu de la proposition précédente. Ainsi ξ n'est pas approximable à l'ordre 2, ni à aucun ordre supérieur.

Corollaire 6. $\sqrt{2}$ *est irrationnel.*

Preuve. C'est une des démonstrations les plus compliquées de ce fait que je connaisse ; nous avons montré plus haut que $\sqrt{2}$ est approximable à l'ordre 2 : ceci entraîne que $\sqrt{2}$ n'est pas rationnel.

Pour démontrer que certains réels sont approximables à l'ordre 2, nous allons d'abord prouver qu'il existe des approximations d'ordre 2 pour tout réel, puis que, dans certains cas, il y a une infinité de telles approximations.

Lemme 7. *Si* $N \in \mathbf{N}^*$, *il existe une fraction* p/q *telle que*

$$1 \leq q \leq N \quad \text{et} \quad \left|\xi - \frac{p}{q}\right| \leq \frac{1}{qN}.$$

En particulier, cette fraction p/q *vérifie*

$$1 \leq q \leq \mathrm{N} \quad \text{et} \quad \left|\xi - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

Preuve. La démonstration de ce résultat repose sur une utilisation judicieuse du principe des tiroirs.

Si x est un réel, notons $\mathrm{E}(x)$ sa partie entière, et (x) sa partie fractionnaire : $(x) = x - \mathrm{E}(x)$. Soit N un entier naturel. Considérons les N + 1 réels 0, (ξ), (2ξ), ..., $(\mathrm{N}\xi)$. Ces points sont tous contenus dans les N intervalles

$$\left[0, \frac{1}{\mathrm{N}}\right[, \left[\frac{1}{\mathrm{N}}, \frac{2}{\mathrm{N}}\right[, \ldots, \left[\frac{\mathrm{N}-1}{\mathrm{N}}, 1\right[.$$

D'après le principe des tiroirs, l'un au moins des intervalles contient deux points et ainsi il existe deux entiers q_1 et q_2 tels que

$$1 \leq q_1 < q_2 \leq \mathrm{N} \quad \text{et} \quad |(q_2\xi) - (q_1\xi)| < \frac{1}{\mathrm{N}}.$$

Mais ceci s'écrit encore :

$$|q\xi - p| < \frac{1}{\mathrm{N}},$$

où $q = q_2 - q_1$ et $p = \mathrm{E}(q_2\xi) - \mathrm{E}(q_1\xi) \in \mathbf{Z}$. Remarquons que $1 \leq q \leq \mathrm{N}$; on en déduit qu'il existe une fraction p/q telle que

$$1 \leq q \leq \mathrm{N} \quad \text{et} \quad \left|\xi - \frac{p}{q}\right| < \frac{1}{q\mathrm{N}} \leq \frac{1}{q^2}.$$

Ainsi tout réel admet une approximation d'ordre 2 ; seulement, quand ξ est rationnel, il n'y a qu'un nombre fini de telles approximations. Voici la réciproque de ce résultat.

Théorème 8. *Si ξ est un réel irrationnel, alors ξ est approximable à l'ordre* 2.

Les nombres les plus intéressants à approximer sont les irrationnels ; on pouvait s'en douter !

Preuve. Il reste à voir que, quand ξ est irrationnel, il y a une infinité de solutions de l'inéquation

$$\left|\xi - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

Supposons qu'il n'y en ait qu'un nombre fini :

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}.$$

Comme ξ est irrationnel, aucun de ces nombres n'est égal à ξ ; en particulier,

$$\min_{1 \le i \le k} \left| \xi - \frac{p_i}{q_i} \right| > 0.$$

Ainsi il existe un entier N > 0 tel que

$$\forall i \in \{1,2,\ldots,k\} \quad \left| \xi - \frac{p_i}{q_i} \right| > \frac{1}{\mathrm{N}} \ ;$$

mais alors la fraction p/q donnée par le lemme plus haut pour cette valeur de N vérifie

$$1 \le q \le \mathrm{N} \quad \text{et} \quad \left| \xi - \frac{p}{q} \right| \le \frac{1}{q^2},$$

de même que

$$\left| \xi - \frac{p}{q} \right| \le \frac{1}{q\mathrm{N}} \le \frac{1}{\mathrm{N}},$$

ce qui prouve que p/q, tout en fournissant une approximation d'ordre 2 de ξ, n'est pas dans la liste des fractions p_i/q_i : on a ainsi trouvé une contradiction.

Approximations d'ordre supérieur

Dans cette section, nous allons exhiber des ensembles de réels qui ne sont pas approximables à l'ordre n, où n est fixé à l'avance. Quand $n = 1$, nous avons la réponse : les seuls réels qui ne sont pas approximables à l'ordre 2 sont les nombres rationnels.

Les nombres rationnels sont les solution des équations polynomiales de degré 1, à coefficients entiers : ainsi p/q est la solution de l'équation

$$qx - p = 0.$$

La clé pour exhiber des nombres qui ne sont pas approximables à l'ordre n est justement cette notion de solution d'une équation polynomiale à coefficients entiers.

Définition. *On dit que ξ est un **nombre algébrique** si ξ est solution d'une équation polynomiale à coefficients entiers. Parmi tous les polynômes dont ξ est racine, il y en a qui ont un degré minimum : on appelle ce degré le **degré** de ξ. Si ξ n'est pas algébrique, on dit que ξ est **transcendant**.*

Si ξ est algébrique, il y a une infinité de polynômes dont ξ est racine ; ainsi, par exemple, $\sqrt{2}$ est racine de $x^2 - 2$, mais aussi de $x^4 - 4$, de $x^6 - 8$, de $3x^2 - 6$; mais chacun de ces polynômes est au moins de degré 2, et ainsi $\sqrt{2}$ est un nombre algébrique de degré 2. De la même façon, $\sqrt[n]{2}$ est un réel algébrique de degré n.

Théorème 9. *Si ξ est un réel algébrique de degré n, alors ξ n'est pas approximable à un degré supérieur à n.*

Preuve. La démonstration est relativement simple. Soit

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

un polynôme de degré minimal à coefficients entiers dont ξ est racine.
Supposons que ξ soit approximable à l'ordre $n + 1$. Il existe alors un nombre réel A tel que l'inéquation

$$\left|\xi - \frac{p}{q}\right| \leq \frac{\mathrm{A}}{q^{n+1}}$$

admette une infinité de solutions distinctes. Parmi celles-là, écartons éventuellement les autres racines de f (on en enlève un nombre fini), et écartons aussi les fractions qui se trouvent à une distance supérieure à 1 de ξ : on garde une infinité de fractions, puisqu'on garde celles dont le dénominateur est supérieur à $\sqrt[n+1]{\mathrm{A}}$.
On peut écrire, après réduction au même dénominateur,

$$\left|f\left(\frac{p}{q}\right)\right| = \frac{\left|a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 p q^{n-1} + a_0 q^n\right|}{q^n} \geq \frac{1}{q^n},$$

puisque le numérateur est un nombre entier qui ne peut pas être nul (sans quoi p/q serait racine de f, ce qu'on a exclu).
Soit M un majorant de $f'(x)$ dans l'intervalle $[\xi - 1, \xi + 1]$. L'inégalité des accroissements finis fournit alors :

$$\left|f\left(\frac{p}{q}\right)\right| = \left|f\left(\frac{p}{q}\right) - f(\xi)\right| \leq \mathrm{M}\left|\frac{p}{q} - \xi\right|,$$

d'où encore

$$\left|\frac{p}{q} - \xi\right| \geq \frac{1}{\mathrm{M}}\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{\mathrm{M}}\frac{1}{q^n}.$$

On obtient ici une inégalité :

$$\frac{1}{\mathrm{M}}\frac{1}{q^n} \leq \frac{\mathrm{A}}{q^{n+1}},$$

c'est-à-dire $q \leq \mathrm{AM}$; ainsi l'ensemble des dénominateurs des approximations de ξ est borné, ce qui est une contradiction : on en déduit que ξ n'est pas approximable à l'ordre $n + 1$, ni donc à aucun ordre supérieur.

C'est ce théorème qui nous a fait dire que les nombres qui s'approximent le mieux sont les plus compliqués : en effet, si un nombre s'approxime à un ordre élevé, il est soit racine d'un polynôme de degré grand, soit (encore pire) transcendant. Les irrationnels les plus simples (et en particulier les racines carrées des nombres entiers, qui sont algébriques de degré 2) ne sont approximables qu'à l'ordre 2.

Ce théorème peut aussi servir à montrer qu'un nombre donné est transcendant ; mais cette utilisation semble toujours artificielle, puisque les exemples sont toujours taillés sur mesure. Ainsi, Liouville a construit, pour appliquer ce théorème, une famille de réels ; ces nombres sont définis par des séries de la forme suivante :

$$\xi = \sum_{n=1}^{+\infty} \frac{a_n}{10^{n!}},$$

où $a_n \in \mathbf{N}$ et $1 \leq a_n \leq 9$. La démonstration du fait que les nombres de Liouville sont approximables à tout ordre et donc transcendants n'est pas très difficile, mais elle est technique, et nous la laissons en exercice pour les lecteurs motivés. Ce qui est surtout intéressant dans l'approche de Liouville est que cette construction fournit explicitement une famille non dénombrable de réels, prouvant que l'ensemble des nombres transcendants n'est pas dénombrable et, au passage, que **R** n'est pas dénombrable.

Bibliographie

– Guinot, *Arithmétique pour amateurs, Une époque de transition : Lagrange et Legendre*, Aléas, 1996.

– Hardy, Wright, *An Introduction to the Theory of Numbers*, 5ᵉ éd., Oxford University Press, 1975.

2001 ?

Avez-vous remarqué que 2001 est le **millième du deux millième nombre triangulaire** ?

et que $2001 = \underbrace{2^4 + 2^4 + 2^4 + 2^4 + 2^4}_{5 \text{ termes}} + 5^4 + 6^4$?

– Communiqué par **Maurice Carmagnole** … en même temps que 44 décompositions de 2001 en sommes de quatre carrés d'entiers –

Y a-t-il un naturel après 3 ?

Jean Lefort(*)

0. Introduction

Le propre des mathématiques, c'est l'abstraction. Abstraire c'est permettre de simplifier puisqu'une même théorie s'appliquera alors à diverses situations. Mais la démarche de l'abstraction est difficile car elle nous oblige à nous débarrasser d'un symbolisme culturel ou non pour en adopter un autre, le symbolisme mathématique, soi-disant plus universel. Impossible d'enseigner les mathématiques sans connaître la culture des enseignés. Ce fait était particulièrement patent à l'époque des mathématiques dites modernes où les enseignants passaient beaucoup de temps à expliquer la différence entre, par exemple, le « et » du français courant et le « et » ($\wedge$) mathématique. La notion de fonction est toujours l'occasion d'un tel aller-retour entre la pratique quotidienne du mot et son sens mathématique. Mais on oublie trop souvent que sur des notions très simples comme le dénombrement, ou même le simple comptage, ces questions sont tout aussi pertinentes. Il y a sans doute un biais culturel, le numérique ayant envahi notre civilisation, mais pas seulement. Certes, tous les professeurs sont sensibilisés aux difficultés qui surgissent à propos de 0 ; mais est-ce le seul nombre à propos duquel surgissent ces difficultés ?

Les réflexions personnelles qui suivent invitent à montrer que les entiers 1, 2 et 3 ont un statut très particulier dans la pensée humaine. Ces réflexions devraient permettre un retour sur l'enseignement du calcul littéral en collège en faisant mieux comprendre les raisons des erreurs des élèves face, par exemple, à l'utilisation du 1.

1 - Aspects linguistiques des petits nombres

Si les mathématiques peuvent être considérées comme un des fondements de la pensée humaine et le nombre le fondement des mathématiques, c'est à travers la linguistique que l'on peut remonter aux aspects primordiaux et à la structure de ladite pensée humaine, en particulier aux premières notions de nombre.

Nous allons voir que l'utilisation des petits nombres (1, 2, 3, rarement 4 ou plus) est systématiquement incluse dans la grammaire de toutes les langues humaines. Ceci tendrait à prouver que ces nombres jouent un rôle particulier dans la structuration de la pensée. Sans prétendre à une étude exhaustive, les quelques pistes de recherches citées permettent de montrer que ces petits nombres n'ont pas le même statut que les suivants.

(*) Lycée B. Pascal, Colmar.

1.1 - Les conjugaisons

Il est quand même curieux que (toutes ?) les langues humaines n'envisagent que trois personnes (pour le singulier au moins) dans la conjugaison des verbes ou l'usage des pronoms puisque dans certaines langues les verbes ont une forme invariable. Les trois pronoms du singulier sont, en français, *je*, *tu*, *il*[1]. Remarquons que le *il* est bien plus ambigu que le *je* ou le *tu*. En effet le *il* renvoie à une personne ou un objet sur lequel les deux interlocuteurs ont dû se mettre d'accord, ce qui n'est pas toujours évident comme le montre la phrase suivante : *L'expérimentateur introduit le carbonate de calcium dans ce milieu ; il subsiste après filtration*[2].

En revanche, *je* et *tu* ne présentent aucune ambiguïté. *Je*, c'est moi, l'unité. *Tu*, c'est toi, la deuxième personne, l'autre moi-même avec qui je converse. *Il* renvoie à un tout indistinct, une pluralité singulière.

Disons un mot de la conjugaison au pluriel. *Nous*, *vous*, *ils* sont beaucoup plus ambigus. À tel point que plusieurs langues distinguent deux formes du nous. C'est le cas de certaines langues amérindiennes. Le guarani admet les formes *ñande* et *ore*, la première forme incluant la ou les personnes avec lesquelles parle le locuteur, la deuxième les excluant. Ces formes plurielles, *nous*, *vous* (je ne parle pas ici de la forme de politesse utilisée en français standard) et *ils*, impliquent une certaine généralisation sur laquelle il n'est pas toujours possible de se mettre entièrement d'accord. Nous retrouvons ici la difficulté vue à propos du *il*. Nous nous heurtons alors à des généralisations abusives source d'incompréhensions et de conflits.

1.2 - Singulier, duel, pluriel.

Dans l'ancien indo-européen (langue reconstituée dont sont issues la plupart des langues européennes mais aussi le sanskrit) existait un nombre spécial intermédiaire entre le singulier (réservé à l'unité) et le pluriel, le duel qui servait à dénombrer les couples et, d'une façon générale, était utilisé dès qu'il s'agissait de deux éléments. On peut noter que nombreux sont les éléments qui vont par couple, des différents organes du corps (mains, yeux, oreilles, ...) à la sexualité. Le grec ancien a gardé le duel, mais d'autres langues non apparentées comme l'arabe classique, le huron (langue amérindienne d'Amérique du nord), ... ont également une forme de duel. Il en reste quelques traces dans les langues européennes modernes par des formes spéciales pour un et deux alors que la régularité commence à partir de trois (et parfois de quatre, mais il faudrait faire une étude poussée sur la reconstruction des formes après usure linguistique à partir de forme régulière) :

En anglais : *once*, *twice*, *three times*, ... avec deux niveaux irréguliers, mais *first*, *second*, *third*, *fourth*, ... où il y a trois niveaux irréguliers avant de rencontrer la régularité.

---

(1) Je n'oublie pas le féminin, mais il est, dans le cadre qui nous intéresse ici, très secondaire d'avoir ou non un verbe qui s'accorde en genre avec son sujet. L'étude du genre fait l'objet d'un autre paragraphe.

(2) D'après « *Les langues du monde* » ouvrage collectif, Éditions Pour la Science.

En français : *premier*, *second* (*deuxième* ?), *troisième*, …, mais *demi*, *tiers*, *quart*, *cinquième*, …

1.3 - Masculin, féminin, neutre.

La distinction masculin-féminin semble résulter d'une distinction assez naturelle des sexes où l'on retrouve la notion de couples, de 2. Le problème est que cette distinction n'est pas aussi nette dans toutes les langues. Et cela se comprend. En effet le sexe de certains êtres vivants n'est pas facile à déterminer (pour certains végétaux, insectes, oiseaux, …). Il est alors naturel d'envisager trois genres : masculin, féminin et neutre. Mais ce n'est qu'un choix possible, ce qui traduit une influence culturelle dans cette distinction des genres. L'ancien indo-européen distinguait le genre « animé » du genre « inanimé » et il en reste des traces dans les langues slaves. Nous pouvons observer que dans la plupart des langues il y a un partage en deux ou trois classes. Il existe cependant des langues où le partage se fait en un bien plus grand nombre de catégories comme, par exemple, dans les langues sino-tibétaines avec l'usage des classificateurs. Les classificateurs jouent effectivement un rôle voisin de celui du genre en français, mais il arrive qu'un même mot puisse recevoir différents classificateurs(3). Dans ce cas, il est cependant possible de se demander s'il n'y a pas eu nécessité de distinguer un grand nombre d'homonymes. C'est en tout cas une possibilité pour le mandarin (chinois officiel), langue pour laquelle le nombre de classificateurs est le plus grand. Comme le nombre de classificateurs a beaucoup changé au cours de l'histoire du chinois (une dizaine en chinois ancien, puis plus de 300 aujourd'hui avec toutefois une tendance à la diminution dans certains dialectes), il est difficile de lier cette notion à celle de genre et surtout de penser que cette notion soit primitive.

1.4 - Les positions spatio-temporelles

La plupart des systèmes verbaux reposent soit sur une distinction de temps, soit sur une distinction d'aspect. Les temps distinguent trois niveaux : passé, présent, futur. Les aspects sont en général deux : perfectif et imperfectif (comme dans les langues slaves) ou accompli et inaccompli (comme dans les langues sémitiques). Il n'est pas question de faire une étude comparée et détaillée des divers systèmes verbaux, mais d'attirer l'attention sur cette décomposition en deux ou trois catégories. Toutefois d'autres notions interviennent comme l'hypothétique, le souhaitable, … Temps et aspects se recoupent largement. On sait que passé et futur s'opposent au présent puisque les deux premiers ont une durée et que le dernier n'est qu'un point sur l'échelle temporelle. Si nous nous contentons de regarder le système français de l'indicatif, nous remarquons que les temps simples correspondent à l'aspect inaccompli (ou imperfectif) et les temps composés à l'aspect accompli (ou perfectif) :

je chante		*j'ai chanté*	
je chantais	action en cours (inachevée)	*j'avais chanté*	action achevée.
je chanterai		*j'aurai chanté*	

(3) C'est ainsi que l'on peut distinguer *yi lún yùe* (« la lune » avec le classificateur *lún*) et *yi gè yùe* (« le mois lunaire » avec le classificateur *gè*), le premier mot *yi* correspondant à l'unité.

D'un point de vue spatial la distinction entre quelques positions est tout aussi patente dans les différentes langues. Il y a toujours deux ou trois catégories correspondant à chacune des extrémités et parfois au milieu, quelquefois quatre par dédoublement de deux catégories initiales. Chacune des trois (!) directions de l'espace donne naissance à au moins un couple de mots : droite et gauche, devant et derrière, dessus et dessous, et, éventuellement, le milieu. Le français distingue *ici* et *là*, *en deçà* et *au delà*. L'espagnol utilisera jusqu'à trois niveaux *aquí*, *ahí* et *allí*. En fait, la recombinaison des différentes directions conduit souvent à multiplier le nombre de positions spatiales. Notons, par exemple, les quatre directions de la rose des vents (nord, est, sud, ouest) qui combinent ainsi la droite et la gauche avec l'avant et l'arrière, mais certaines cultures comptent six directions, ajoutant le zénith et le nadir, c'est-à-dire le dessus et le dessous.

1.5 - Conclusion linguistique

Cette très rapide étude montre bien que les nombres 1 et 2 ont un statut fondamental, apparaissant systématiquement en opposition. Le 3 a un rôle légèrement « second » mais aussi très fort dans les différentes grammaires. Sauf cas de recombinaison, les autres nombres n'ont pas un rôle aussi important, ce qui laisse penser que les nombres 1 et 2 sont imprimés dans nos gènes ou dans la structure de notre cerveau et que le nombre 3 n'y est peut-être que l'initial de tous les autres. Bien sûr, tous les autres nombres sont en germe sinon il n'y aurait pas de mathématiques telles que nous les connaissons, mais il faut envisager que, contrairement aux axiomes de Peano (première version(4)), ce n'est pas 1 qui engendre tous les naturels, du moins pas au niveau du fonctionnement de notre cerveau.

2 - Historique de la construction des petits nombres

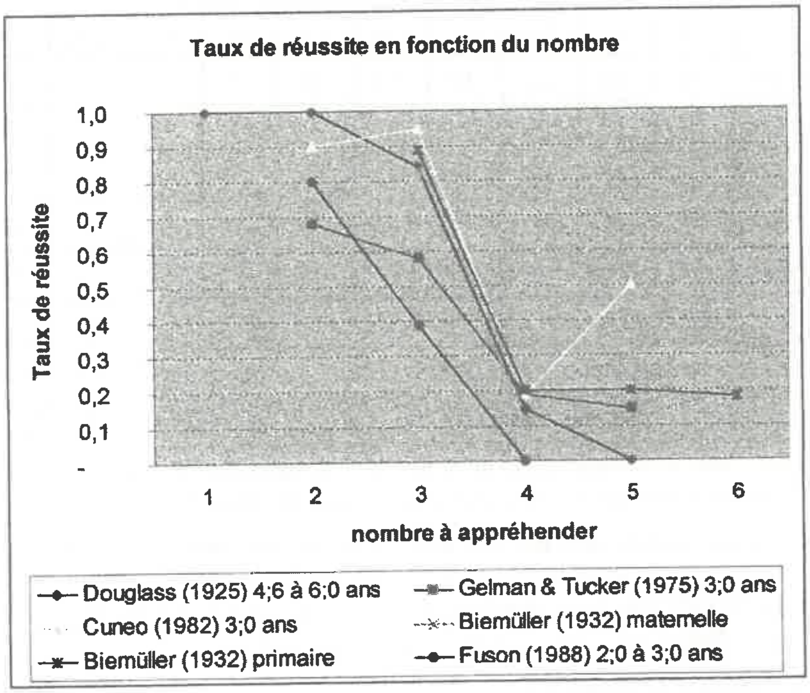
2.1 - La construction du nombre chez l'enfant

De très nombreuses études de didactique ont été consacrées à la genèse de la notion de nombre chez l'enfant. Les résultats qui suivent sont extraits essentiellement de l'ouvrage « Apprentissages numériques » de Jean-Paul Fischer(5). L'auteur y présente les résultats d'expériences passées qui sont résumés dans le tableau ci-après. Ces expériences ont en commun d'avoir présenté des collections linéaires de points ou de boules régulièrement espacés et d'avoir empêché le comptage un par un par une limitation du temps d'exposition ou par des consignes données aux enfants (les âges du type 3;6 ans signifient 3 ans et 6 mois).

Ces différentes expériences passées montrent parfaitement que les nombres 1 et 2 sont très rapidement assimilés ou maîtrisés, que 3 l'est assez vite mais qu'au delà il y a une chute spectaculaire de l'appréhension du nombre. Le nombre 3 apparaît comme le terme ultime de la numération immédiate, c'est-à-dire des nombres que l'on peut évaluer sans compter.

(4) Dans une première version, Peano construisit les entiers en partant de 1. Toutes les versions ultérieures commencent en 0.

(5) *Apprentissages numériques* par Jean-Paul Fischer, Presses Universitaires de Nancy, 1992.



En fait Fischer montre dans son ouvrage que les choses sont un petit peu plus compliquées. Il fait en effet une distinction selon la représentation figurée des nombres : soit en ligne, soit en constellation.

	1	2	3	4	5	6
représentation en ligne	•	••	•••	••••	•••••	••••••
représentation en constellation	•	:	∴	::	⁙	⠿

La reconnaissance de la forme géométrique facilite l'appréhension du nombre. Une étude systématique n'a pas été faite pour 6, mais il apparaît que si 3 reste le nombre ultime pour bien des enfants, surtout des plus jeunes, la disposition symétrique des points facilite la dénomination des nombres 4 et 5 sauf justement pour les plus jeunes. Le tableau suivant donne le nombre d'enfants ayant réussi la dénomination du nombre présenté en fonction du groupe d'âge. Chaque groupe d'âge de 4;3 ans à 5;9 ans comporte 36 individus.

	1 L	1 C	2 L	2 C	3 L	3 C	4 L	4 C	5 L	5 C
4;3 ans	35	34	32	30	14	16	5	3	2	0
4;9 ans	36	36	32	30	21	23	3	10	5	8
5;3 ans	36	36	34	34	28	29	10	19	6	19
5;9 ans	36	36	36	36	35	34	12	27	9	26
Total.	143	142	134	130	98	102	30	59	22	53

La différence entre 3 en ligne (3 L) et 3 en constellation (3 C) n'est pas significative. De nombreuses expériences tendent à prouver que les bons résultats relatifs à 4 et 5 en constellation résultent d'un comptage qu'il est beaucoup plus facile et rapide de faire dans ce type de présentation plutôt que dans la présentation en ligne. Il y a ensuite mémorisation de la forme de la constellation. Ceci prouve que 3 reste bien une borne supérieure dans l'appréhension des nombres.

En fait une analyse plus fine des diverses expériences faites auprès des enfants tend à montrer que la reconnaissance de 3 résulte également d'un comptage qui a lieu beaucoup plus tôt dans le développement. Il faut également noter que pour bien des plus jeunes, tout ce qui n'est pas 1 ou 2 est nécessairement 3.

2.2 - Les grecs et le nombre 3

On sait que Pythagore avait créé une sorte de secte mathématico-religieuse. Le nombre y était la base de la théologie et plus particulièrement les nombres 1, 2, 3 et 4. C'est la fameuse tétraktys célébrée dans cet hymne :

Bénis-nous, nombre divin, toi qui as engendré les dieux et les hommes, O Sainte, Sainte Tétraktys, toi qui contiens la racine et la source du flux éternel de la création car le nombre divin débute par l'unité pure et profonde et atteint ensuite le 4 sacré puis il engendre la mère de tout, qui relie tout, le premier né, celui qui ne dévie jamais, qui ne se lasse jamais, le 10 sacré qui détient la clé de toute chose.(6)

Pour Pythagore, le 1, la monade est la source de tous les nombres. Le 2, premier nombre pair est le symbole du féminin et 3 premier nombre impair (ce qui prouve que 1 n'est pas un nombre) est le symbole du masculin. Le rôle de la Tétraktys ne peut se comprendre si on ne se réfère pas aux nombres triangulaires dont l'importance dans la pensée pythagoricienne est indéniable. Le 1, le 2 et le 3 appartiennent aux hommes car ils correspondent aux trois directions de l'espace sensible, et $1 + 2 + 3$ donne 6, nombre triangulaire, le premier nombre parfait. Et $1 + 2 + 3 + 4 = 10$, la décade, nombre sacré car il correspond à la base de la numération des grecs(7). En dépassant les nombres des hommes, ne serait-ce que d'une unité, on atteint les nombres des dieux, ce qui explique le caractère sacré de 4 (et de 10).

(6) D'après *Les mathématiques ? Quelle Histoire !* Cassette vidéo d'André Stoll, IREM de Strasbourg.

(7) Heureuse coïncidence qui n'aurait pu avoir lieu chez les mayas avec la base 20.

L'étude des nombres est alors un moyen de comprendre les dieux et par voie de conséquence la nature que les dieux ont créée :

Là où on ne trouve ni le nombre ni sa nature, rien ne peut exister qui soit intelligible à quiconque en soi-même ou en relation avec d'autres choses. Vous pouvez observer le pouvoir du nombre s'exerçant par lui-même dans tous les actes et toutes les pensées des hommes, dans tous les métiers et la musique.

On retrouve cette vision des mathématiques dans la célèbre phrase de Galilée sur l'univers, livre ouvert écrit en langage mathématique.

2.3 - Religion et nombres

Nous venons de voir le rôle très particulier que Pythagore attribuait aux nombres et en particulier aux premiers d'entre eux. Les religions monothéistes vont très vite assimiler le nombre 1 à Dieu, ce qui implique que 1 ne saurait être un nombre avec les propriétés des nombres puisque Dieu transcende tout. Cette vision religieuse du nombre 1 va perdurer pendant tout le moyen âge, surtout dans l'empire arabe alors au sommet de sa puissance. Les mathématiciens, tant musulmans que juifs, travaillant à Bagdad expliqueront plus d'une fois que 1 n'est pas un nombre puisqu'il représente Dieu qui ne saurait être divisé. En effet 1 n'a pas de diviseur autre que lui-même.

Chez les chrétiens, l'invention de la Trinité peut très bien se concevoir comme une concession à la philosophie pythagoricienne qui imprégnait de façon diffuse la pensée grecque au début de notre ère. C'est dans le fond la trace d'un certain syncrétisme. Mais cela prouve la force du nombre 3 qui tend à resurgir dans différents domaines.

D'une façon générale, dans toutes les religions, certains nombres vont recevoir une charge symbolique très forte : il en est ainsi du nombre 7 qui, des sumériens aux juifs, puis au chrétiens et aux musulmans, finira par rythmer le temps quotidien avec la semaine. On sait que la Bible fait un grand usage des nombres 10 et 12, et on sait aussi qu'une multitude de livres ont été écrits à propos du fameux 666 de l'Apocalypse (Apoc. XIII 18), nombre auquel il faudrait joindre le 153 de l'évangile de Jean (Jean XXI 11)[(8)]. Il est plus que vraisemblable que tous ces nombres se renvoient les uns les autres par l'intermédiaire de sommes et de produits. Il semble donc que l'on retrouve ici une influence pythagoricienne à moins que Pythagore et juifs n'aient emprunté à la même source. Mais tout ceci est hors de notre présent propos.

La notion de couple, couples primitifs engendrant toute l'humanité ou couples divins se partageant le monde soit en opposition soit en parallèle, se retrouve dans la plupart des cultures. Que l'on pense aux religions de l'Inde, à la religion de l'Égypte antique, au manichéisme, ou à bien d'autres.

(8) 666 est le nombre triangulaire de $36 = 6^2$ et 6 est lui-même triangulaire en même temps que nombre parfait mais auquel il manque 1 pour atteindre le 7 divin ! 153 est le nombre triangulaire de $17 = 10 + 7$, deux nombres relatifs à la perfection de Dieu. $10 = 5 \times 2$ et $5 + 2 = 7$ de même $12 = 4 \times 3$ et $4 + 3 = 7$, etc.

2.4 - Fermat et le nombre 1[9].

Dans un défi adressé à divers mathématiciens étrangers et en particulier à Wallis, Fermat propose, le 3 janvier 1657, de chercher un carré ou un cube qui, ajouté à ses parties aliquotes, fasse un cube[10], comme $7^3 = 343$ qui, ajouté à ses parties aliquotes, fait un carré : $343 + 1 + 7 + 49 = 20^2$. Wallis proposera rapidement la seule solution 1. Cette réponse va déclencher une controverse sur la nature du nombre 1 dont les extraits suivants montrent la nature et prouvent la difficulté de concevoir le nombre 1 comme un nombre ordinaire.

Ainsi on demande un nombre qui ait des parties aliquotes ; mais un nombre est une pluralité d'unités, et l'unité elle-même n'est pas un nombre ; elle ne résout donc pas la question, où l'on demande un nombre, non pas quelconque, mais qui ait des parties aliquotes qui puissent lui être ajoutées et qui soit de même nature que le nombre 343, dont les parties sont énumérées. Mais quelles sont les parties de l'unité ? Il est clair que si elle n'en a pas, ainsi que l'avoue Wallis lui-même, elle n'est aucunement de la même nature que le nombre 343, cube ayant des parties aliquotes, qui, ajoutées à ce nombre, en donnent un autre carré.

[.................................]

Mais quand Wallis présente à plusieurs reprises l'unité comme étant le cube cherché et [...], il est inexcusable, puisqu'en donnant l'unité, il ne donne en fait aucun cube.

Lettre de Frenicle à Digby du 3 février 1658

Sa chicane sur votre solution par le nombre 1 est bien mauvaise ; car chacun sait que quelques uns sont de l'opinion que 1 n'est pas un nombre ; mais ceux-là même savent tout aussi bien que, dans l'opinion des autres, il en est un.

Lettre de Brouncker à Wallis du 28 février 1658
(datée du 18 février 1657 style anglais[11])

En dehors de la controverse, il faut noter le vocabulaire qui trahit bien la difficulté qu'ont les mathématiciens de l'époque à donner au nombre 1 le même statut qu'aux autres nombres. Aujourd'hui, on parle du nombre 1, pas de l'unité, mot qui a une signification bien précise dans le cadre de la structure d'anneau. L'extrait suivant montre que le nombre 2 a aussi un synonyme, binaire, dont le sens, de nos jours, a été considérablement restreint.

Je lui avois écrit qu'il n'y a qu'un seul nombre quarré en entiers qui, joint au binaire, fasse un cube, et que ledit quarré est 25, auquel si vous ajoutez 2, il se fait 27 qui est cube.

Lettre de Fermat à Digby du 15 août 1657

---

(9) Tous les exemples de cet alinéa sont extraits de « *Œuvres de Pierre Fermat, I. Théorie des nombres* » présenté par R. Rashed *et al* et publié chez Blanchard (1999).

(10) Les parties aliquotes sont les diviseurs stricts. Ainsi les parties aliquotes de 6 sont 1, 2, 3.

(11) Non seulement les anglais utilisaient le calendrier julien en retard de 10 jours sur le calendrier grégorien, mais leur année commençait au 1er avril !

Une autre trace du rôle particulier de deux est la notation xx pour x^2 encore très vivace au XVIII^e siècle.

Ces quelques exemples sont des indices forts du rôle très particulier qu'ont encore les petits nombres dans la pensée mathématique du XVII^e siècle.

3 - Conclusion et retour sur l'enseignement des maths

3.1 - Conclusion provisoire

Le développement de la notion de nombre chez l'enfant, dans la linguistique, la sociologie, les religions, l'histoire, (on pourrait y ajouter la psychanalyse), tous ces aspects de la pensée humaine tendent à prouver que notre esprit fonctionne à partir de la notion de 1 et de 2 et que tous les autres nombres sont construits à partir de ces deux là. Si le nombre 3 apparaît très vite il semble, cependant, jouer un rôle un peu différent. Il regroupe la notion de pluriel et il est le début du comptage. Mais nous n'avons ici que des aspects indirects du fonctionnement de notre cerveau. Bien des recherches seront encore nécessaires pour améliorer la compréhension de notre nature et en particulier la compréhension de notre façon de penser les nombres, à commencer par **N**.

3.2 - Influence sur l'enseignement

Mon professeur de Quatrième avait l'habitude de nous répéter : « Le prochain qui me dit que 0 c'est rien aura 0, il verra si c'est rien ! » Bien évidemment il n'en faisait jamais rien (!) et nous répétait inlassablement le rôle mathématique du 0. Mais le nombre 0 est apparu très tardivement dans l'histoire des mathématiques et tous les pédagogues sont depuis longtemps sensibilisés aux difficultés de son appréhension mathématique.

Il est curieux que le nombre 1 qui joue rigoureusement le même rôle d'élément neutre pour la multiplication que le 0 pour l'addition ne fasse pas l'objet de soins aussi attentifs de la part des pédagogues. De même que le 0 disparaît de l'écriture, de même le 1 disparaît : on écrit x et non $1\ x$ ou $x\ 1$. Il ne faut donc pas s'étonner que les élèves oublient ce facteur 1 dans une factorisation. Il serait intéressant de savoir si la disparition du « 1 » dans les écritures algébriques n'est pas vécue comme une disparition du moi, à moins qu'il ne s'agisse de la non visibilité de Dieu ? Question qui n'est pas si idiote quand on a vu l'influence de la religion sur la perception de « 1 » comme nombre.

« Deux » paraît être ressenti essentiellement comme la valeur du couple (au sens sexuel), de tout ce qui va par deux dans la vie, donc de la paire : bras, jambes, yeux, oreilles, etc. Cette référence quasi obligée de « 2 » à bien des aspects du corps ne pourrait-elle pas jouer un rôle analogue dans le refus de l'abstraction qu'impose l'aspect mathématique du nombre 2. Là encore, je soulève plus de questions que je n'apporte de réponses, le seul fait de s'interroger permettant une prise de conscience qui ne peut être que bénéfique du point de vue didactique et pédagogique.

Il serait intéressant de savoir si la construction de la numération au delà de « 3 » n'est pas vécue comme une approche de l'infini, que l'on pense à cette réflexion classique d'enfants s'adressant à un de leur parent : « Dis, papa (maman), jusqu'à combien tu sais compter ? » Cet aspect peu pris en compte dans la pédagogie actuelle mériterait une réflexion, le vertige que l'on éprouve face à l'infini pouvant se révéler traumatisant pour certains enfants qui seront peut-être justement ceux qui rejetteront ultérieurement les mathématiques.

Une des difficultés essentielles qu'ont les élèves pour comprendre les maths, c'est d'admettre que l'abstraction n'est pas une perte de sens, mais bien plutôt une multiplication des sens. Pour rester au niveau numérique qui est le mien dans cet article, l'abstraction « deux » recouvre non seulement la notion de couple mais aussi toutes sortes d'ensembles dont « 2 » sera le cardinal commun. Ce « 2 » peut être précisé par un mot qui incarnera(12) alors son sens. Cette prise de conscience me paraît nécessaire pour entrer dans les mathématiques et éviter des blocages affectifs. Le mieux est de commencer tôt.

3.3 - 1, 2, 3 et après ?

Tout le monde connaît la réponse au titre de cet article. Mais si nous dépassons la simple étude des naturels nous arrivons aux nombres *irrationnels*, puis aux nombres *négatifs* (qui donnaient de *fausses* solutions), puis aux nombres *imaginaires*, aux nombres *transcendants*, aux nombres *idéaux*…(13) et finalement nous sommes confrontés à la notion même de nombre : qu'est-ce qu'un nombre ?

Ici le vocabulaire porte la trace des difficultés qu'ont eu les mathématiciens à dégager les bonnes notions et ce vocabulaire même incite les enseignants à faire preuve de toute leur capacité pédagogique pour que leurs élèves, à leur tour, dégagent les bonnes notions mathématiques à partir de leur symbolique propre à ladite notion.

Mais les mathématiques ne s'arrêtent pas aux nombres quelle que soit l'étendue que nous donnons à ce concept. Il faut ensuite parler des structures et des fonctions. Mais ceci est un autre chapitre bien plus long. Gageons qu'il sera d'autant mieux compris par les étudiants que ceux-ci auront bien démarré sur 1, 2 et 3.

(12) J'utilise volontairement le mot « incarner » qui a une forte connotation religieuse.
(13) Et ce n'est pas fini (!). Voir par exemple « *Et pourtant ils ne remplissent pas* **N** *!* » de Claude Lobry, éditions ALÉAS.

Quelques activités arithmétiques liées aux codes correcteurs et à la cryptographie

Robert Rolland(*)

1. Avertissement

Une partie des activités proposées dans la suite de cet article sont extraites de la brochure [5]. Nous renvoyons le lecteur à cette référence pour des compléments ou des aides concernant les thèmes abordés ici, ainsi que pour un cours d'arithmétique respectant les programmes actuels des classes terminales des lycées.

2. Enseigner l'arithmétique

Durant quelques années, l'arithmétique a complètement disparu des programmes de mathématiques du secondaire. Ce choix a été regrettable. En effet l'enseignement de cette discipline possède un grand intérêt pour diverses raisons que je voudrais énumérer ; celles-ci peuvent en outre aider à préciser l'esprit dans lequel on devrait le dispenser.

- **Histoire et culture.** L'arithmétique est un des secteurs scientifiques les plus anciens. Ses problèmes internes ont motivé durant des siècles des développements fondamentaux dans diverses parties des mathématiques.
- **Raisonnement, démonstrations.** Les méthodes de raisonnement et de démonstration utilisées dans ce domaine sont d'une grande richesse et d'une grande variété. Ceci est particulièrement intéressant à l'heure actuelle, où dans l'enseignement scientifique scolaire, la part de pensée abstraite est réduite à la portion congrue au bénéfice de larges pans descriptifs.
- **Applications récentes.** Dans une période récente de nombreux problèmes concrets liés à l'informatique, l'électronique ainsi qu'à la représentation, la compression, l'intégrité et la confidentialité des données, ont été résolus dans le cadre de l'arithmétique. L'arithmétique a trouvé là un champ d'applications et de problèmes ayant une implication immédiate dans la vie de tous les jours (sécurité des communications sur les réseaux informatiques et téléphoniques, commerce électronique, sécurité des transactions bancaires, etc.).
- **Algorithmique.** De nombreux problèmes donnent lieu à la mise en place d'algorithmes tant pour démontrer l'existence de solutions que pour en faire un calcul effectif.

(*) IREM de Marseille

- **Expérimentation, test des hypothèses.** En arithmétique de nombreuses situations se prêtent particulièrement bien à une phase exploratoire consistant en une expérimentation sur ordinateur dans le but de conjecturer un résultat, de tester des hypothèses.

Je voudrais enfin insister sur l'importance des mathématiques et du raisonnement abstrait dans la démarche scientifique. L'expérimentation a bien entendu son rôle, mais elle doit forcément être sous-tendue par une réflexion théorique. De ce point de vue il ne faut pas oublier que les théories mathématiques, éventuellement très abstraites, développées aujourd'hui sont les bases d'applications de demain ou d'après-demain. Le meilleur exemple en est justement l'arithmétique dont on a pu dire à une certaine époque qu'elle était une réflexion de salon et qui se retrouve aujourd'hui au centre de réalisations concrètes très riches.

Pour toutes ces raisons il convenait que l'arithmétique élémentaire ait une place dans la formation des élèves scientifiques. C'est ce que prévoit maintenant le programme de la spécialité mathématique des classes terminales.

3. Quelques rappels

Nous rappelons ici quelques résultats importants et quelques méthodes classiques dont nous aurons besoin. Cela concerne essentiellement le théorème de Bézout ainsi que l'utilisation des congruences.

3.1. Théorème de Bézout

3.1.1. Les théorèmes

Théorème 3.1. *Si* pgcd$(a,b) = d$, *il existe deux entiers* u *et* v *tels que* $ua + vb = d$.

Dans le cas où a et b sont premiers entre eux, la réciproque est vraie. On dispose alors du théorème suivant :

Théorème 3.2. *Deux nombres entiers* a *et* b *sont premiers entre eux si et seulement s'il existe des entiers* u *et* v *tels que* $au + bv = 1$.

Ce résultat joue un rôle important et permet d'établir diverses propositions, par exemple le lemme d'Euclide-Gauss :

Théorème 3.3. *(Lemme d'Euclide-Gauss) Si* c *divise* ab *et si* c *est premier avec* b, *alors* c *divise* a.

Preuve. Si c est premier avec b, alors on peut trouver u et v tels que $uc + bv = 1$. Par suite $auc + abv = a$. Mais auc est divisible par c et abv aussi, donc a est divisible par c.

3.2. Résolution complète de $ua + vb = d$ (où $d =$ pgcd(a,b))

Supposons tout d'abord a et b premiers entre eux. On sait qu'il existe un couple (u_0,v_0) tel que $u_0a + v_0b = 1$. En existe-t-il d'autres ? Si oui, trouver tous les couples (u,v) tels que $ua + vb = 1$.

Soit (u,v) un couple quelconque répondant à la question. Alors

$$a(u - u_0) + b(v - v_0) = 0.$$

Donc b divise $a(u - u_0)$, et puisque b est premier avec a, b divise $u - u_0$. Par suite u est nécessairement de la forme $u = u_0 + kb$. Si bien que

$$akb + b(v - v_0) = 0$$

ou encore

$$v = v_0 - ka.$$

Ainsi tout couple (u,v) répondant à la question vérifie

$$u = u_0 + kb,$$

$$v = v_0 - ka$$

pour un certain $k \in \mathbf{Z}$. D'autre part on vérifie immédiatement, que pour tout $k \in \mathbf{Z}$, le couple (u,v) défini précédemment convient.

Remarque. Existe-t-il une solution (u,v), où u et v sont petits en valeur absolue ? Supposons $a > 0$, $b = 1$. Alors $u_0 = 0$, $v_0 = 1$ convient. On a bien entendu un résultat analogue pour $a = 1$, $b > 0$.
Supposons maintenant $a > 1$, $b > 1$. Puisque pour tout couple (u,v) qui convient on a

$$u = u_0 + kb$$

où (u_0,v_0) est une solution particulière et que réciproquement si u est de cette forme, il existe v tel que le couple (u,v) convienne, on peut supposer, quitte à faire la division euclidienne par b que cette solution particulière u_0 vérifie $0 \leq u_0 < b$. De plus il n'y a qu'une solution telle que u_0 soit dans cet intervalle. On ne peut pas avoir $u_0 = 0$ car alors $v_0 b$ vaudrait 1 ce qui est impossible puisque $b > 1$. Donc

$$0 < u_0 < b.$$

Pour v_0 nous avons alors

$$v_0 = \frac{1 - au_0}{b},$$

d'où

$$\frac{1}{b} - a < v_0 < 0,$$

ce qui donne

$$-a < v_0 < 0.$$

En particulier si b (ou a) est petit, on peut trouver rapidement une solution par recherche exhaustive. Par exemple si $b = 3$ alors $u_0 = 1$ ou 2 et on cherche lequel des deux nombres $1 - a$, $1 - 2a$ est divisible par 3.

Supposons qu'on veuille maintenant résoudre

$$ua + vb = d$$

où $d = \text{pgcd}(a,b)$. Dans ces conditions on a $ua' + bv' = 1$ avec $a' = \dfrac{a}{\text{pgcd}(a,b)}$ et

$b' = \dfrac{b}{\text{pgcd}(a,b)}$. Mais on sait qu'alors a' et b' sont premiers entre eux. On est donc ramené au problème précédent.

3.2. Congruences

La notion de congruence est une notion naturelle très courante. Par exemple on identifie usuellement 14h avec 2h de l'après midi, ce qui constitue un calcul modulo 12.

Définition 3.1. *Soit n un entier strictement positif. Deux entiers x et y étant donnés nous dirons que x est congru à y modulo n et nous noterons*

$$x \equiv y \quad (n),$$

si $x - y$ est un multiple de n, c'est-à-dire si on peut écrire

$$x = y + kn.$$

Remarquons que la définition nous permet de dire que :

- x est congru à lui-même modulo n,
- si x est congru à y modulo n, alors y est congru à x modulo n,
- si x est congru à y modulo n et y est congru à z modulo n, alors x est congru à z modulo n.

La congruence s'interprète aussi très bien avec la division euclidienne :

Théorème 3.4. *L'entier x est congru à l'entier y modulo n si et seulement si les restes des divisions euclidiennes de x par n et de y par n sont égaux.*

Ceci donne un intérêt particulier à ce reste commun. On notera

$$x \bmod n$$

le reste de la division de x par n. C'est l'unique nombre r tel que $0 \leq r < n$ qui soit congru à x modulo n.

Attention, certains langages de programmation ne donnent pas exactement ce résultat (en particulier si x est négatif). Ils donnent aussi un résultat pour n négatif (cas qu'on a exclu ici).

La congruence se comporte bien vis à vis des opérations habituelles.

Proposition 3.1. *Si*

$$x_1 \equiv y_1 \quad (n)$$

et

$$x_2 \equiv y_2 \quad (n),$$

alors

$$x_1 + x_2 \equiv y_1 + y_2 \quad (n)$$

et

$$x_1x_2 \equiv y_1y_2 \quad (n).$$

En particulier si

$$x \equiv y \quad (n),$$

alors

$$x^k \equiv y^k \quad (n).$$

3.3. Algorithmes

Les applications de l'arithmétique et le développement des moyens de calcul ont rendu cruciales les questions sur la possibilité effective de réaliser certaines opérations. Prenons par exemple un nombre n produit de deux grands nombres premiers p et q de 150 chiffres chacun. Peut-on calculer p et q connaissant n ? Bien entendu il existe un algorithme naïf : essayer de diviser n successivement par tous les nombres qui lui sont inférieurs. Mais compte tenu de la taille des nombres utilisés, cet algorithme ne peut se réaliser en un temps raisonnable. Jusqu'à présent, bien que des progrès soient faits sur les algorithmes utilisés et sur la puissance de calcul des machines, on ne sait pas résoudre pratiquement un tel problème. En revanche si a et b sont deux nombres très grands, on sait trouver en temps raisonnable $d = \text{pgcd}(a,b)$ ainsi que u et v tels que $au + bv = d$.

Ainsi, il y a des opérations réalisables pratiquement et d'autres qui dans l'état actuel de nos connaissances et de nos moyens techniques ne le sont pas.

Citons quelques exemples de calculs réalisables avec des nombres donnés très grands :

- Trouver $d = \text{pgcd}(a,b)$ ainsi que u et v tels que $au + bv = d$ (algorithme d'Euclide étendu par exemple).
- Calculer $a^k \bmod n$.
- Trouver de grands nombres premiers.

Voici maintenant quelques problèmes actuellement hors d'atteinte pour des nombres très grands :

- Factoriser un nombre n produit de deux grands nombres premiers.
- Étant donnés des nombres a, b, n tels qu'il existe k vérifiant $a^k \equiv b \ \ (n)$, trouver k (problème du logarithme discret).
- Étant donnés un nombre n, produit de deux grands nombres premiers inconnus, et b tel qu'il existe x vérifiant $x^2 \equiv b$ (n), trouver x (problème de la racine carrée).

3.3.1. Algorithme d'Euclide étendu

On sait que si $\text{pgcd}(a,b) = d$, il existe deux entiers u et v tels que $ua + vb = d$. Nous supposerons que $a > 0$ et $b \geq 0$. Le cas général s'en déduit.

Voici un algorithme (**algorithme d'Euclide étendu**, adaptation de l'algorithme d'Euclide) qui permet de trouver explicitement d, ainsi qu'un couple (u,v) qui convient.

Rappelons que l'algorithme d'Euclide calcule le reste r_2 de la division euclidienne de $r_0 = a$ par $r_1 = b$:

$$r_0 = q_1 r_1 + r_2,$$

puis de proche en proche r_k reste de la division euclidienne de r_{k-2} par r_{k-1} :

$$r_{k-2} = q_{k-1} r_{k-1} + r_k,$$

jusqu'à obtenir un reste r_{n+1} nul. Le dernier reste r_n non nul est pgcd(a,b). Dans l'algorithme d'Euclide étendu on ajoute à chaque pas du calcul la phase suivante :
en supposant que pour tout $j \leq k - 1$ on ait pu écrire

$$r_j = u_j a + v_j b$$

(on constate que ceci est vrai pour r_0 avec $u_0 = 1$ et $v_0 = 0$ et pour r_1 avec $u_1 = 0$ et $v_1 = 1$), alors

$$r_{k-2} = q_{k-1} r_{k-1} + r_k,$$

ce qui nous donne

$$r_k = (u_{k-2} - q_{k-1} u_{k-1})a + (v_{k-2} - q_{k-1} v_{k-1})b.$$

On obtient donc

$$r_k = u_k a + v_k b,$$

avec

$$u_k = u_{k-2} - q_{k-1} u_{k-1}$$

et

$$v_k = v_{k-2} - q_{k-1} v_{k-1}.$$

Ainsi le couple (u_n, v_n) dont on a expliqué le calcul convient.

Donnons l'algorithme sous forme de programme :

```
R0 := a ;  (a ≥ 0)
R1 := b ;  (b ≥ 0)
U0 := 1 ;
U1 := 0 ;
V0 := 0 ;
V1 := 1 ;
tant que R1 > 0 faire
   début
      Q := Quotient_Division(R0,R1) ;
      R := Reste_Division(R0,R1) ;
      U := U0 – Q * U1 ;
      V := V0 – Q * V1 ;
      R0 := R1 ;
      R1 := R ;
      U0 := U1 ;
      U1 := U ;
      V0 := V1 ;
      V1 := V ;
   fin.
```

En sortie, R0 = pgcd(a,b), U0 = u et V0 = v.

Afin de préciser le coût de l'algorithme d'Euclide (cf. [4], page 25) introduisons la suite de Fibonacci qui est définie par $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$. En posant $\phi = \frac{1+\sqrt{5}}{2}$ (nombre d'or), on peut calculer

$$F_n = \frac{1}{\sqrt{5}}(\phi^n - (-\phi)^{-n}),$$

ce qui permet de dire que

$$F_n = \mathrm{round}\left(\frac{1}{\sqrt{5}}\phi^n\right),$$

où round(x) est l'entier le plus proche de x. Comme $F_{n-1} < F_n$, la formule

$$F_{n+1} = F_n + F_{n-1}$$

exprime la division euclidienne de F_{n+1} par F_n. L'algorithme d'Euclide appliqué à ces deux nombres donne pour résultat $F_1 = 1$ et possède n pas. C'est le cas le plus défavorable, c'est-à-dire le cas où l'algorithme est le plus long relativement à la taille des données. Plus précisément :

Théorème 3.1. *Soit* N *un entier > 1 et n le plus grand entier tel que* $F_{n+1} < N$. *Si* $0 \leq a \leq b < N$, *alors le nombre de pas de l'algorithme d'Euclide appliqué au couple* (a,b) *est majoré par n. Ce nombre de pas est exactement n si et seulement si* $a = F_n$ *et* $b = F_{n+1}$.

On pourra trouver une preuve de ce résultat dans [4] (p. 25) ou [7] (p. 47).

3.3.2. Calcul d'une puissance. Utilisation de la base 2 pour accélérer le calcul de x^n

En calculant directement $x \cdot x \dots \cdot x$, on fait $n - 1$ multiplications. Si on décompose n en base 2 on obtient

$$n = a_k 2^k + \dots + a_1 2 + a_0.$$

Alors

$$x^n = x^{a_k 2^k + \dots + a_1 2 + a_0} = x^{a_0} \times (x^2)^{a_1} \times ((x^2)^2)^{a_2} \times \dots \times ((x^{2^{k-1}})^2)^{a_k}.$$

Il y a donc au maximum k carrés à effectuer de proche en proche et au maximum k autres produits, donc au plus $2k$ multiplications.

Par exemple si $n = 15$ alors on calcule x^2 puis $x^4 = (x^2)^2$ puis $x^8 = (x^4)^2$ et enfin $x^{15} = x \times x^2 \times x^4 \times x^8$, soit 6 multiplications. Remarquons qu'une décomposition astucieuse de 15 en 6 + 9 permet de ne faire que 5 multiplications.

Cette méthode s'applique bien entendu au calcul de x^k mod n, en prenant bien soin, pour ne pas introduire de nombres gigantesques, de prendre le modulo à chaque étape et non pas à la fin du calcul.

Détaillons sous forme de programme un calcul de a^k mod n, inspiré de ce qui vient d'être dit :

```
A := a ;
K := k ;
N := n ;
R := 1;
tant que K > 0 faire
    si K pair
        alors  début
                   A := A * A mod N ;
                   K := K/2 ;
               fin
        sinon  début
                   R := R * A mod N ;
                   K := K – 1 ;
               fin.
```

En sortie R contient a^k mod n.

4. Détection et correction des erreurs

On pourra trouver des solutions ou des indications pour les exercices de ce paragraphe dans [5].

4.1. Clés de contrôle

Dans la vie courante, on est amené à manipuler des numéros d'identification, par exemple les numéros I.N.S.E.E. (Institut National de la Statistique et d'Études Économiques), les numéros de comptes bancaires, les numéros I.S.B.N. (International Standard Book Number), etc. Ces numéros pouvant être assez longs, on les munit d'une clé qui permet de détecter (pas toujours) des erreurs de saisie éventuelles.

4.1.1. Numéro I.N.S.E.E

Le numéro I.N.S.E.E. d'un individu est constitué de 15 chiffres. En lisant de gauche à droite, le premier est 1 ou 2 suivant qu'il s'agit d'un homme ou d'une femme. Les deux chiffres suivants désignent les deux derniers chiffres de l'année de naissance, les deux suivants le mois de naissance, les deux suivants le département, les trois suivants la commune de naissance, les trois suivants le numéro d'inscription sur le registre d'état civil, les deux derniers forment une clé K calculée de la manière suivante : désignons par A le nombre entier constitué par les 13 chiffres de gauche ; soit r le reste de la division euclidienne de A par 97 ; on prend $K = 97 - r$.

a) Vérifiez pour votre numéro I.N.S.E.E.

b) Écrivons A sous la forme

$$A = H \times 10^6 + L$$

avec $0 \leq L < 10^6$.

Montrer que r est aussi le reste de la division euclidienne de $27 \times H + L$ par 97.

c) Soit A_1 le nombre constitué par un numéro I.N.S.E.E. (y compris la clé). Montrer que si un des chiffres de A_1 et un seul est erroné, l'erreur est détectée. Montrer que si deux chiffres consécutifs distincts sont permutés, l'erreur est détectée.

d) Donner un exemple d'erreur non détectée.

4.1.2. Clé de relevé d'identité bancaire (RIB)

Le relevé d'identité bancaire comporte de gauche à droite 5 chiffres pour le code de la banque, 5 chiffres pour le code du guichet, 11 chiffres pour le numéro de compte, 2 chiffres pour la clé. La clé K est calculée de la manière suivante : soit A le nombre constitué par les 21 chiffres de gauche ; on calcule le reste r de la division euclidienne de $100 \times A$ par 97. On prend $K = 97 - r$.

a) Calculer la clé pour le relevé 14607 00052 05215075057 *xx*.

b) Comment mener le calcul avec une calculette ?
(indication : écrire $100 \times A = H \times 10^{12} + M \times 10^{6} + L$).

c) Soit A_1 le nombre constitué par un RIB (y compris la clé). Montrer que si un des chiffres de A_1 et un seul est erroné, l'erreur est détectée. Montrer que si deux chiffres consécutifs distincts sont permutés, l'erreur est détectée.

4.1.3. Numéro I.S.B.N.

L'*International Standard Book Number* utilise des mots de longueur 10 constitués avec les chiffres 0, 1, ..., 9 et le symbole X (qui représente le nombre 10) ; le symbole X ne sera utilisé, si nécessaire, que pour la clé.

Exemples : 2 84180 013 X, 2 84225 000 1, 0 471 62187 0, 0 12 163251 2.

Le premier chiffre représente le pays, un bloc de chiffres est attribué à un éditeur, un autre bloc est le numéro donné par l'éditeur, le dernier symbole est la clé, calculée de telle sorte que si $a_1a_2\ldots a_{10}$ désigne un numéro I.S.B.N.,

$$\sum_{i=1}^{10} i a_{11-i}$$

soit divisible par 11.

a) Vérifier les exemples donnés.

b) Montrer que si un chiffre (et un seul) est erroné, l'erreur est détectée.

c) Montrer que si deux chiffres distincts sont permutés, l'erreur est détectée.

d) Trouver toutes les valeurs de a et de b telles que 2 84225 0*ab* 1 soit un code I.S.B.N. valide.

e) Pourquoi prendre la somme des ia_{11-i} et pas seulement la somme des a_i ?

4.1.4. Le code UPC (universal product code)

Le code I.S.B.N. a le désavantage d'utiliser pour la clé un symbole « parasite » (le X). Ceci provient du fait que l'on travaille modulo 11. Peut-on faire une étude analogue en travaillant modulo 10 ? Voici le code UPC, utilisé avec les codes barres, qui est basé sur ce principe. Le code UPC utilise des nombres de 12 chiffres $a_1 \dots a_{12}$ (11 chiffres pour désigner un produit, et une clé), de telle sorte que

$$\sum_{i=0}^{5} 3a_{2i+1} + \sum_{i=1}^{6} a_{2i}$$

soit divisible par 10.

a) Calculer la clé si le nombre formé par les 11 chiffres de gauche est 35602387190.

b) Montrer que si un chiffre (et un seul) est erroné, l'erreur est détectée.

c) Montrer que, sauf cas particulier à déterminer, la permutation de deux chiffres successifs distincts est détectée (hélas il y a des cas particuliers ; personne n'est parfait !).

4.1.5. Numéro de carte bancaire (règle de Luhn)

Un numéro de carte bancaire est de la forme

$$a_n a_{n-1} \dots a_2 a_1 a_0,$$

où les a_i sont des chiffres décimaux qu'on identifiera aux nombres 0, 1, …, 9. Sur ces nombres on définit l'application

$$m(x) = \begin{cases} 2x & \text{si } 0 \le 2x \le 9, \\ x_1 + x_2 & \text{si } 2x = 10x_1 + x_2, \end{cases}$$

avec $0 \le x_i \le 9$.

a) Montrer que $m(x) = 2x \bmod 9$. En conclure que $0 \le m(x) \le 9$.

On impose à un numéro de carte bancaire de vérifier (règle de Luhn)

$$a_0 + m(a_1) + a_2 + m(a_3) + \dots \equiv 0 \ \ (10).$$

Montrer que là aussi, si un chiffre (et un seul) est erroné, l'erreur est détectée et que, sauf cas particulier à déterminer, la permutation de deux chiffres successifs distincts est détectée.

4.1.6. Peut-on faire mieux ?

Ainsi le code UPC et la règle de Luhn ont l'avantage d'avoir une clé comprise entre 0 et 9, ils détectent une erreur, mais hélas ne détectent pas toujours une permutation de deux chiffres contigüs distincts. Peut-on construire un code détecteur, travaillant sur une suite de chiffres décimaux et ayant comme les deux codes précédents pour clé un chiffre décimal, qui détecte une erreur et qui détecte toujours une permutation de deux chiffres contigüs distincts ? La réponse est oui. On peut trouver un tel exemple dans [3] (p. 590).

Montrer qu'avec un tel exemple on peut construire un tableau carré T de 10 cases sur 10 cases pour lequel chaque ligne et chaque colonne est une permutation de $\{0,\ldots,9\}$ (donc un carré latin) et pour lequel pour tout $i, j \in \{0,1\}$, on ait : si $i \neq j$ alors $T(i,j) \neq T(j,i)$.

4.2. Un code correcteur de Hamming

Ici on se propose non plus seulement de détecter, mais de corriger une erreur éventuelle. Considérons les nombres de 10 chiffres (numéros de téléphone par exemple) $a_1a_2\ldots a_{10}$ où les a_i peuvent prendre les valeurs 0, 1, …, 9. On rajoute une clé constituée de deux chiffres $a_{11}a_{12}$ où a_{11} et a_{12} peuvent prendre les valeurs 0, 1, …, 9 et aussi la valeur X, représentant le nombre 10. La clé est calculée de telle sorte que

1) a_{11} soit le reste de la division de $\sum_{i=1}^{10} a_i$ par 11,

2) a_{12} soit le reste de la division de $\sum_{i=1}^{10} i\,a_i$ par 11.

a) Calculer la clé pour le numéro 0491413940.

b) On part d'un numéro muni de sa clé $a_1a_2\ldots a_{12}$. On se propose de montrer que si en communiquant ce numéro on fait **une erreur sur un chiffre** (et pas plus), on peut reconstituer le bon numéro.

Montrer que si l'erreur est faite sur un a_i avec $1 \leq i \leq 10$, alors aucune des relations 1) et 2) n'est vérifiée.

Montrer que si l'erreur est faite sur a_{11}, la relation 1) n'est pas vérifiée, mais la relation 2) l'est.

Montrer que si l'erreur est faite sur a_{12}, la relation 1) est vérifiée mais pas la relation 2).

Montrer qu'on peut corriger l'erreur. Indiquer comment.

Exemple : Soit le numéro 049132900000. Vérifier que ce numéro n'est pas correct. En supposant qu'un seul chiffre soit faux, retrouver le bon numéro.

Le seul ennui du codage précédent est la présence éventuelle dans la clé du symbole « parasite » X. Mais on va voir qu'avec une clé de deux chiffres on ne peut pas se contenter des chiffres décimaux.

Impossibilité de réaliser une correction du type précédent uniquement avec les chiffres décimaux

Soit E l'ensemble des nombres de dix chiffres $a_1a_2\ldots a_{10}$ où les a_i sont des chiffres décimaux habituels. Soit F l'ensemble des nombres de 12 chiffres décimaux.

a) Quels sont les nombres d'éléments de E et de F ?

Si $x = x_1x_2\ldots x_{10}$ est un élément de E, on calcule à partir de x une clé $K(x) = x_{11}x_{12}$ formée de 2 chiffres décimaux. Notons f l'application de E dans F qui à x associe $f(x) = x_1x_2\ldots x_{10}x_{11}x_{12}$ et $C = f(E)$ l'image de E.

b) Quel est le nombre d'éléments de C ?

Si y est un élément de C, on note B_y l'ensemble formé de y ainsi que de tous les éléments obtenus à partir de y en modifiant un (et un seul) chiffre de y.

c) Quel est le nombre d'éléments de B_y ? Montrer qu'il existe au moins deux éléments distincts z_1, z_2 dans C tels que $B_{z_1} \cap B_{z_2} \neq \varnothing$.

Si $t \in B_{z_1} \cap B_{z_2}$, il est impossible de savoir si t provient d'une erreur faite sur z_1 ou d'une erreur faite sur z_2. Cette obstruction montre qu'on ne peut pas réaliser un code correcteur du type de l'exemple précédent avec uniquement des digits décimaux. En essayant de faire ce même calcul sur l'exemple précédent (avec 11 digits), on verra évidemment que cette obstruction n'a pas lieu, mais que « ça passe juste » (pour simplifier un peu le calcul on supposera que pour **toutes** les positions et pas seulement pour la clé, les chiffres peuvent prendre les 11 valeurs 0, 1, …, 9, X).

5. Cryptographie

5.1. Le petit théorème de Fermat

1) Soit p un nombre premier. Montrer que si $1 \leq k \leq p-1$, alors :

$$C_p^k \equiv 0 \quad (p),$$

où les C_p^k sont les coefficients binomiaux.

2) Montrer que $(1 + 1)^p \equiv 1 + 1$ (p). Puis par récurrence trouver une expression de $(1 + 1 + \ldots + 1)^p$. En conclure que pour tout entier a,

$$a^p \equiv a \quad (p)$$

(on pourra distinguer les cas $a = 0$, $a > 0$, $a < 0$).

3) En conclure que si a est premier avec p, alors (petit théorème de Fermat) :

$$a^{p-1} \equiv 1 \quad (p).$$

4) Soit $n = pq$ où p et q sont deux nombres premiers.
Supposons tout d'abord a premier avec n. Montrer que

$$(a^{p-1})^{q-1} \equiv 1 \quad (p),$$

et que

$$(a^{p-1})^{q-1} \equiv 1 \quad (q).$$

En conclure que pour tout $k \geq 0$

$$a^{k(p-1)(q-1)} \equiv 1 \quad (n).$$

Supposons maintenant que $a = lp$ avec $0 < l < q$. Montrer que

$$a^{k(p-1)(q-1)+1} \equiv a \quad (p),$$

et que

$$a^{k(p-1)(q-1)+1} \equiv a \quad (q).$$

En conclure que pour tout k

$$a^{k(p-1)(q-1)} \equiv 1 \quad (n).$$

Montrer que dans tous les cas, pour tout a et tout k on a

$$a^{k(p-1)(q-1)+1} \equiv a \quad (n).$$

5.2. Principe du chiffrement de Rivest, Shamir et Adleman (RSA)

Le chiffrement RSA est certainement le plus connu et le plus utilisé des chiffrements à clé publique. Dans un chiffrement à clé publique, chaque participant X possède une clé publique e_X connue de tous, et une clé privée d_X qu'il ne communique à personne. Si un autre participant veut envoyer un message m à X, il calcule $c = e_X(m)$ (message chiffré grâce à la clé publique de X), et transmet c à X. X peut retrouver m grâce à sa clé privée en calculant $d_X(c)$ qui, par construction des paires de clés publiques-clés privées, redonne m. L'avantage d'un tel système non symétrique (clé de déchiffrement différente de la clé de chiffrement et **incalculable** à partir de celle-ci) est d'éviter d'avoir à échanger avec son correspondant une clé secrète. Le problème bien sûr est de trouver un moyen de réaliser concrètement un tel système. Le système RSA répond à la question.

Alice choisit deux grands nombres premiers p et q, calcule $n = pq$ ainsi que $(p - 1)(q - 1)$. Elle choisit un nombre e premier avec $(p - 1)(q - 1)$ et calcule d et k tels que $ed = k(p - 1)(q - 1) + 1$. Comment peut-elle mener ce calcul ? Remarque : elle peut trouver un k tel que $0 < k < e$ (pourquoi ?).

Elle rend publics les nombres n et e (c'est sa clé publique) mais pas p, ni q, ni sa clé privée d.

Bob qui veut envoyer à Alice un message numérisé en un nombre $0 \leq x < n$ (si le message est trop long il le découpe en blocs) utilise la clé publique d'Alice pour calculer $y = x^e \bmod n$. Il transmet y à Alice. Alice peut retrouver x grâce à sa clé privée d en calculant $y^d \bmod n$ (montrer qu'on a bien $x = y^d \bmod n$).

On ne sait pas reconstituer la clé privée d d'Alice à partir de sa clé publique (n,e). Bien sûr si on connaissait la décomposition de n en facteurs premiers on pourrait retrouver d en faisant le même calcul que celui qu'a fait Alice pour construire sa paire de clés. La sécurité du système repose sur la difficulté de retrouver p et q connaissant n.

Exemple (non réaliste à cause des nombres minuscules utilisés) :

Alice choisit $p = 263$, $q = 419$. On vérifiera que ces nombres sont premiers. Elle calcule $n = pq$ et $f = (p - 1)(q - 1)$. Constater que f n'est pas divisible par 3. Alice choisit alors $e = 3$. Ainsi sa clé publique est (n,e). On cherche alors d et k tels que

$$3d = kf + 1.$$

Montrer qu'il y a nécessairement une solution avec $k = 1$ ou avec $k = 2$ (revoir le paragraphe 3.1.2 et en particulier la remarque).
Trouver d.

Bob qui dispose de la clé publique d'Alice veut lui envoyer le message $x = 187$. Quel message chiffré lui envoie-t-il ?

Que fait Alice pour retrouver le message clair ? Faire le calcul.

Bibliographie

[1] T.M. Apostol, *Introduction to analytic number theory*. Springer-Verlag, 1976.

[2] L. Chambadal, *Calcul pratique*. Hachette, 1983.

[3] COMAP, *Principles and practice of Mathematics*. Springer-Verlag, 1997.

[4] M. Demazure, *Cours d'algèbre*. Cassini, 1997.

[5] Groupe de travail sur la liaison Lycées-Universités, *Cours et activités en arithmétique pour les classes terminales (2e Éd.)*. IREM de Marseille, 1999.

[6] IREM de Clermont, *Arithmétique en terminale S, enseignement de spécialité*. CRDP de Clermont.

[7] R. Kumanduri, C. Romero, *Number theory with computer applications*. Prentice Hall, 1998.

[8] M. Mignotte, *Mathématiques pour le calcul formel*. Puf, 1989.

L'ARITHMÉTIQUE DANS LES BULLETINS VERTS LES PLUS RÉCENTS

(en tête, numéro du Bulletin en gras, puis pages entre parenthèses)

(suite page 99)

La division simple à l'aide de l'abaque de Gerbert(*)

D'après Bernelin (élève de Gerbert d'Aurillac) Libre d'Abaque
trad. Bakkouche, B., CIHSO, Toulouse, 1999, p. 35-37(**)

Michel Guillemot

On appelle « simple » la division dont nous nous apprêtons à parler maintenant, parce qu'on propose un diviseur à un chiffre, mais qu'on place au-dessus un dividende à un ou plusieurs chiffres. Divisons donc 668 par le diviseur 6 de la façon suivante : plaçons dans le premier tracé de l'unité le diviseur 6 et au-dessous de lui la différence 4, pour qu'ils arrivent au total de 10 ; plaçons un 6 du dividende dans le second tracé des centaines, l'autre dans le second aussi des dizaines, et 8 dans le second des unités. Au-dessous d'eux, plaçons ces mêmes nombres aussi dans le troisième tracé, selon la première façon, pour que ces nombres étant pris pour la dénomination et les premiers d'entre eux restant à leur place, on puisse plus facilement retenir quel nombre est proposé pour dividende.

Il s'agit de diviser 668 par 6. Pour des raisons typographiques, nous limitons l'abaque à un damier comportant trois colonnes et quatre rangées.

		6 4	diviseur différence : $10 - 6 = 4$
6	6	8	dividende
6	6	8	dividende

Puisque donc le diviseur, ajouté à la différence, atteint la seconde colonne, c'est à dire les dizaines, y occupant la place de la première unité, prends le nombre 6 en entier du troisième tracé des centaines et place-le en seconde position pour la dénomination totale dans le quatrième tracé des dizaines.

		6 4	
6	6	8	
	6	8	
	6		quotient partiel q_1 (dénomination)

on obtient un premier quotient partiel : 60

$$\frac{668}{6} > \frac{600}{10} = 60$$

(*) Cf. Article sur Gerbert, Bulletin n° 431, pages 831-832.

(**) En vente à la Régionale APMEP de Toulouse, 200 F avec port.

Multiplie par ce nombre la différence du diviseur de cette façon : 6 fois 4, 24, c'est-à-dire 2 dans le troisième tracé des centaines, mais 4 dans le même des dizaines [...]

		6 4
6	6	8
2	6 **4**	8
	6	

$4q_1 = 4 \times 6 = 24$

$$\frac{668}{6} = 60 + \frac{68}{6} + \frac{240}{6}$$

De nouveau, prends le 2 des centaines et, comme auparavant, place-le pour en faire la dénomination ; multiplie-le par la différence du diviseur de cette façon 2 fois 4, 8 avec les autres dans le troisième des dizaines.

		6 4
6	6	8
	6 4 **8**	8
	6 **2**	

d

$r = 10 - d$

D

de manière générale

$$(1) \quad \frac{\mathrm{D}}{d} = \frac{a \cdot 10^{n+1} + b}{d} = a \cdot 10^n + \frac{ar + b}{d}$$

Si tu les additionnes, c'est-à-dire 6, 4 et 8, tu auras un nombre qui compte 18 unités, c'est-à-dire 1 dans le troisième tracé des centaines, mais 8 dans le troisième tracé des dizaines.

		6 4
6	6	8
1	**8**	8
	6 2	

De même, prends l'unité des centaines et place-la aussi, de la façon précédente, en seconde position pour en faire la dénomination ; multiplie-la par la différence du diviseur de cette façon : une fois 4, 4, dans le troisième tracé des dizaines.

		6 4
6	6	8
	8 4	8
	6 2 **1**	

d'après (1)

ar

$a \cdot 10^n$

Si tu additionnes ce nombre au 8 restant, tu obtiendras le nombre 12, c'est à dire 1 dans le troisième nombre des centaines et 2 dans le troisième aussi des dizaines.

		6 4
6	6	8
1	**2**	8
	6 2 1	

Encore une fois, prend le 1 des centaines et place-le pour la dénomination ; multiplie-le par la différence du diviseur, de cette façon : 1 fois 4, 4, dans le troisième des dizaines.

		6 4	d'après (1)
6	6	8	
	2 **4**	8	*ar*
	6 2 1 **1**		$a \cdot 10^n$

Si tu additionnes ce chiffre au 2 restant, tu auras le nombre 6 dans le troisième aussi.

		6 4
6	6	8
	6	8
	6 2 1 1	

Prends donc de même ce nombre de sa place, et place-le en seconde position, dans le quatrième tracé de l'unité, pour la dénomination, multiplie-le par la différence du diviseur de cette façon : 6 fois 4, 24, c'est-à-dire 2 dans le troisième des dizaines, 4 dans le même des unités [...]

		6 4	d'après (1)
6	6	8	
	2	8 **4**	*ar*
	6 2 1 1	**6**	$a \cdot 10^n$

De même prends le 2 des dizaines et place-le en seconde position pour la dénomination : multiplie par la différence du diviseur de cette façon : 2 fois 4, 8, dans la troisième des unités.

		6 4	d'après (1)
6	6	8	
		8 4 **8**	*ar*
	6 2 1 1	6 **2**	$a \cdot 10^n$

Si tu l'additionnes aux deux nombres restants, c'est-à-dire 8 et 4, tu auras 20, c'est-à-dire 2 dans le troisième tracé des dizaines.

		6 4	
6	6	8	
	2		
	6 2 1 1	6 2	il n'y a pas de signe numérique pour 0 : c'est le vide

Prends-le de sa place, place-le en seconde position, comme précédemment, pour la dénomination ; multiplie-le par la différence du diviseur de cette façon : 2 fois 4, 8, dans le troisième des unités.

		6 4	d'après (1)
6	6	8	
		8	*ar*
	6 2 1 1	6 2 **2**	$a \cdot 10^n$

Parce que donc tu ne peux continuer à placer en seconde position, sans plus t'occuper de la différence, compare le diviseur au dividende pour savoir lequel des deux – du diviseur ou du dividende – est considéré comme le plus grand. Mais le dividende est supérieur au diviseur de 2 ; il te reste donc, des nombres additionnés auparavant, à accorder aux dénominations le 1 des unités et à replacer le reste des dividendes, 2 dans le troisième tracé des unités aussi.

		6 4	
6	6	8	
		2	$b - d$
	6 2 1 1	6 2 2 **1**	

(2) $\frac{b}{d} = 1 + \frac{b-d}{d}$ si $b > d$

Cela fait, il faut voir la valeur à laquelle arrivent les dénominations ajoutées ensemble, de façon à conclure que c'est par leur quantité que le diviseur divise les dividendes. De fait, si tu ajoutes les 6 et deux 2 à 1, tu auras un 1 avec les autres dénominations des dizaines et tu placeras l'autre dans le même tracé des unités.

		6 4
6	6	8
		2
	6 2 1 **1**	**1**

		6 4
6	6	8
		2
	6 2 1 **1**	1

Si tu ajoutes 6, 2 et deux 1 à l'unité restante, tu placeras un 1 dans le quatrième des centaines, tu ramèneras l'autre dans la quatrième aussi des dizaines. Concluons donc que 668 est divisé cent onze fois par le diviseur 6, reste 2 précisément.
Remarque. Ici, Bernelin joue habilement en déplaçant un jeton marqué 1.

		6 4	diviseur différence : $10 - 6 = 4$
6	6	8	dividende
		2	reste de la division
1	**1**	1	quotient

$668 = 6 \times 111 + 2$

L'ARITHMÉTIQUE DANS LES BULLETINS VERTS LES PLUS RÉCENTS

(suite de la page 94)

426 (78-88) *Les critères de divisibilité en Inde*, par C. Morice-Singh.

421 (219-232) *Codage et cryptage*, par D.-J. Mercier.

417 (459-463) *Le carré de tout nombre premier (sauf 2 et 5) est somme de 3 carrés non nuls*, par J.-P. Brévan.

408 (568-581) *Cryptographie classique et cryptographie publique à clé révélée*, par D.-J. Mercier.

403 (173-182) *Pell-Fermat toujours d'actualité*, par Ch. Jeanbreau et Ch. Notari.

398-399 (531-550 et 675-685) *Commentaires des histoires de numérations du Ifrah*.

• De plus, signalons dans le **415** (173-192), *L'algèbre et la correction des erreurs*, par D.-J. Mercier

Dénombrement des polyèdres convexes

Michel Lafond

Depuis de nombreuses années je me posais la question suivante : « **Combien y a t-il de polyèdres convexes distincts à *n* faces ?** ».

Je savais qu'il y a un seul tétraèdre et deux pentaèdres (dessinés dans 4)

Pour la suite j'étais dans l'ignorance jusqu'à ce que je tombe sur un livre magique : « The encyclopedia of integer sequences » de N.J.A. SLOANE et Simon PLOUFFE chez Academic Press.

Ce livre référencie plus de 5 000 suites numériques à valeurs entières positives, lesquelles sont classées dans l'ordre lexicographique des premiers termes avec quelques commentaires et références, et éventuellement une formule ou une relation de récurrence.

Par exemple la suite à la référence M2981 est :

1,1,3,14,147,3462,294392 ... [1,3]

egyptian fractions : partitions of 1 into parts $1/n$, donc il y a 147 solutions à l'équation diophantienne $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}+\frac{1}{e}=1$.

En parcourant ce livre j'ai remarqué à la référence M1796 la suite

1,2,7,34,257,2606,32300,440564,6384634

polyedra with n nodes ... [4,2] qui donne donc à partir de $n = 4$ le nombre de polyèdres (convexes) ayant n sommets. Comme il y a autant de polyèdres à n sommets que de polyèdres à n faces (nous verrons pourquoi), j'avais la réponse à ma question en tous cas jusqu'à $n = 12$.

J'ai ainsi appris qu'il y avait 7 hexaèdres et 34 heptaèdres. Ce dernier résultat me sembla exagéré aussi je me suis amusé à les recenser et j'en ai bien trouvé 34 (ils sont dessinés à la fin). 257 octaèdres ce n'est déjà pas rien, mais plus de 6 millions de dodécaèdres c'est dur à digérer !

Ceux qui sont intéressés par ce livre mais qui ne veulent pas l'acheter peuvent comme il est dit dans la préface procéder ainsi pour avoir des renseignements sur une suite connaissant seulement les premiers termes :

Il faut disposer d'une adresse électronique (e-mail).

Si vous êtes connecté à Internet, il n'y a pas de problème, **mais ce n'est pas nécessaire** !.

Si vous êtes enseignant, votre lycée vous en donne une (CARAMAIL, LEMEL, ...).

Sinon il y a un moyen très simple que j'utilise encore : faire à partir d'un **simple minitel** le 3615 minitelnet et suivre les indications pour avoir un e-mail **gratuit**.

Bref, vous êtes dans votre messagerie préférée et à partir de là c'est enfantin :

Vous envoyez le courrier à l'adresse superseeker@research.att.com et à objet vous tapez lookup 3 4 5 7 9 12 16 22 30 42 58 81 113 (ou les premiers termes de votre suite séparés par des blancs).

Il n'y a plus qu'à envoyer le message (qui est vide) et à attendre. Des algorithmes très élaborés (décrits au début du livre) sont alors mis en œuvre et si votre suite n'est pas trop tordue vous obtiendrez une réponse par retour de courrier (électronique) (*attention les adresses électroniques peuvent changer*).

1) Avant d'entreprendre le dénombrement de tel ou tel type de polyèdre, une question se pose tout de suite : si on utilise les notations usuelles pour un polyèdre

S pour le nombre de sommets

F pour le nombre de faces

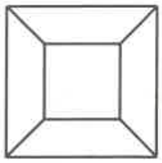
A pour le nombre d'arêtes,

Q1 : (S,F,A) étant un triplet d'entiers donnés, existe-t-il un polyèdre convexe ayant S sommets, F faces et A arêtes ?

La réponse à Q1 est non car S, F et A sont liés par la condition nécessaire suivante dite relation d'EULER :

$$S + F = A + 2 \qquad (1)$$

La démonstration de (1) est assez simple :



Si (P) est un polyèdre convexe donné, supprimons une face de (P) et, quitte à déformer un peu les faces, aplatissons-le de manière à se ramener à un polygone convexe (P′), pavé de F – 1 polygones, chacun correspondant à une face de (P).

Bien sûr on préserve la topologie, on ne fait que déformer (*la figure ci-contre montre l'aplatissement du cube.*)

Pour démontrer (1), il suffit de démontrer S + F = A + 1 dans (P′).

Pour cela posons $k = S + F - A$

De deux choses l'une :

Ou bien (P′) n'a pas de sommet intérieur et alors (P′) possède n sommets, une face, n arêtes donc $k = n + 1 - n = 1$.

Ou bien (P′) possède (au moins) un sommet intérieur. Supprimons ce sommet ainsi que les p arêtes qui en partent. La suppression fait perdre 1 sommet, p arêtes et $p - 1$ faces, donc k est inchangé. En supprimant de proche en proche tous les sommets intérieurs, on se ramènera (sans changer k) au cas précédent pour lequel on a vu que k valait 1. CQFD.

Puisqu'on a nécessairement S + F = A + 2 pour tout polyèdre, il suffit dans la question Q1 de se donner S et F. On dira dans la suite qu'**un polyèdre est de type (S,F) s'il a S sommets et F faces.**

La question Q1 devient :

Q2 : Étant donnés deux entiers S et F, existe-t-il un polyèdre de type (S,F) ?

Un théorème de STEINIZ répond à Q2 :

Il existe un polyèdre convexe de type (S,F) si et seulement si

$$\mathbf{S \geq 4} \quad \textbf{et} \quad \mathbf{\frac{1}{2}S + 2 \leq F \leq 2S - 4} \quad (2)$$

La démonstration de (2) faisait l'objet d'une question posée par Marc ROYER dans le bulletin n° 415 à propos de l'avis de recherche n° 86 sur les polyèdres convexes à 7 arêtes.

La voici :

Les conditions de* (2) *sont nécessaires :
S ≥ 4 sinon le polyèdre serait plan.
2 A ≥ 3 F car chaque face a au moins 3 arêtes, chacune comptée 2 fois.
2 A ≥ 3 S car de chaque face partent au moins 3 arêtes, chacune comptée 2 fois.
Donc

$$F = A - S + 2 \geq \frac{3}{2}S - S + 2 = \frac{1}{2}S + 2 \Rightarrow \mathbf{F \geq \frac{1}{2}S + 2},$$

$$S = A - F + 2 \geq \frac{3}{2}F - F + 2 = \frac{1}{2}F + 2 \Rightarrow \mathbf{F \leq 2S - 4}.$$

Les conditions de* (2) *sont suffisantes : c'est un peu plus difficile, car si

$$\mathbf{S \geq 4} \text{ et } \mathbf{\frac{1}{2}S + 2 \leq F \leq 2S - 4},$$

il faut exhiber un polyèdre de type (S,F).
* Si **S = 4,** alors 4 ≤ F ≤ 4 : le tétraèdre convient.
* Si **S = 5,** alors 5 ≤ F ≤ 6.
Pour F = 5, la pyramide à base carrée convient.
Pour F = 6, deux tétraèdres accolés (bipyramide) font l'affaire.

* Si **S ≥ 6,** on distingue deux cas : $\frac{1}{2}S + 2 \leq F \leq S$ ou S + 1 ≤ F ≤ 2 S – 4.

PREMIER CAS : $\mathbf{\frac{1}{2}S + 2 \leq F \leq S}$ (α)

– **ou bien S = 2*n*** et (α) équivaut à $n + 2 \leq F \leq 2n$.
Considérons le prisme (P) dont les bases sont deux polygones à n côtés (la figure 1 est possible puisque $S \geq 6 \Rightarrow n \geq 3$) . (P) a **2*n* sommets** et n + 2 faces ; or si on rapproche légèrement B de C le long de (BC), (BCB′C′) n'est que déformé, mais le quadrilatère (ABA′B′) devient gauche avec deux faces triangulaires (AA′B′) et (AB′B). Le résultat est qu'on a **autant de sommets** mais **une face de plus.** On peut faire ceci pour toutes les faces de (P) autres que les bases. Si on le fait k fois $[0 \leq k \leq n - 2]$, on aboutit à un polyèdre ayant $n + 2 + k$ faces, nombre compris **entre *n* + 2 et 2*n*.** *De plus ce polyèdre possède deux faces quadrangulaires voisines.*

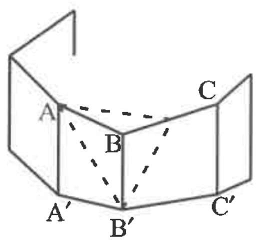


Figure 1

– **ou bien** $\mathbf{S = 2n + 1}$ et (α) équivaut à
$$n + 2 \leq F \leq 2n + 1.$$
On sait d'après le cas précédent obtenir un polyèdre (P) ayant $2n$ sommets et F–1 faces, dont deux faces voisines sont des quadrilatères (Figure 2). Si on « tronque » le sommet X de (P), on augmente le nombre de faces et le nombre de sommets de 1, ce qui nous amène pour les faces de $n + 2 \leq F - 1 \leq 2n$ à $\boldsymbol{n + 3 \leq F \leq 2n + 1}$ et pour les sommets de $2n$ à $\boldsymbol{2n + 1}$.

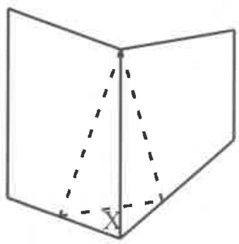


Figure 2

DEUXIÈME CAS : $\mathbf{S + 1 \leq F \leq 2S - 4}$.
Partons de la pyramide (P) de base un polygone à 2S – F – 1 sommets [c'est possible puisque 2S – F – 1 ≥ 3]. (P) a 2S – F sommets et 2S – F faces dont au moins trois sont des triangles.
Considérons l'opération Ω consistant à accoler à une face triangulaire de (P) un tétraèdre (suffisamment aplati). Dans Ω, le nombre de sommets augmente de 1 et celui des triangles de 2.
Itérons F – S fois Ω [c'est possible puisque F – S ≥ 1]. On arrive à un polyèdre (P′) ayant (2S – F) + F – S = **S sommets** et (2S – F) + 2(F – S) = **F faces**. C Q F D.

2) On peut maintenant entrer dans le vif du sujet et poser la question
Q3 : Combien y a-t-il de polyèdres convexes distincts de type (S,F) ?
Précisons ce qu'on entend par polyèdres distincts. Disons qu'on ne s'intéresse qu'à la topologie (forme) des polyèdres : disposition des faces les unes par rapport aux autres, mais pas aux longueurs des arêtes, surfaces des faces…
On considère donc comme équivalents deux polyèdres qui diffèrent par :
– des rotations, translations, homothéties, symétries de $\mathbf{R}^3$.
– des déformations comme l'étirement d'une arête…
Dans cette optique **il n'existe par exemple qu'un seul tétraèdre.**
À partir de maintenant notons π**(S,F) le nombre de polyèdres convexes distincts de type (S,F).**

Indiquons dans un tableau quelques valeurs de π**(S,F)** :

Polyèdres convexes		Nombre de faces								
		4	5	6	7	8	9	10	11	12
Nombre de sommets	4	**1**	0	0	0	0	0	0	0	0
	5	0	**1**	**1**	0	0	0	0	0	0
	6	0	**1**	**2**	**2**	**2**	0	0	0	0
	7	0	0	**2**	**8**	**11**	**8**	**5**	0	0
	8	0	0	**2**	**11**	**42**	**74**	**?**	**?**	**?**
	9	0	0	0	**8**	**74**	**296**	**?**	**?**	**?**

On verra bientôt comment sont obtenues certaines de ces valeurs.

3) Que remarque t-on dans ce tableau ?

Bien entendu, les 0 correspondent aux couples (S,F) qui ne vérifient pas la condition (2) de STEINIZ. Ainsi :
si $S = 4$, alors (2) implique $4 \leq F \leq 4$, donc $F = 4$;
si $S = 5$, alors (2) implique $5 \leq F \leq 6$, etc .

Mais **d'où vient la symétrie du tableau** ? Elle vient d'une notion fondamentale : la **DUALITÉ**. Le dual d'un polyèdre convexe (P) de type (S,F) est un polyèdre convexe que je note (P~) de type (F,S). (P) a donc autant de sommets que (P~) a de faces et réciproquement, et, d'après la relation d'EULER, ils ont tous deux le même nombre d'arêtes : $A = S + F - 2$. De plus il existe une bijection involutive δ qui
– à chaque sommet X de (P) associe une face $\delta(X)$ de (P~),
– à chaque face π de (P) associe un sommet $\delta(\pi)$ de (P~),
et qui vérifie la propriété suivante :
Si $\pi = (X_1, X_2, X_3, \ldots, X_q)$ est une face quelconque de (P) alors le sommet $\delta(\pi)$ de (P~) est commun aux faces $\delta(X_1)$, $\delta(X_2)$, …, $\delta(X_q)$ de (P~) et seulement à ces faces-là.
Cette définition ainsi que l'existence du dual ne sont pas évidentes. Je me contenterai de donner deux méthodes de constructions effectives sur l'exemple de l'hexaèdre (P) ci-dessous. Les arêtes en trait gras doivent être vues en avant.

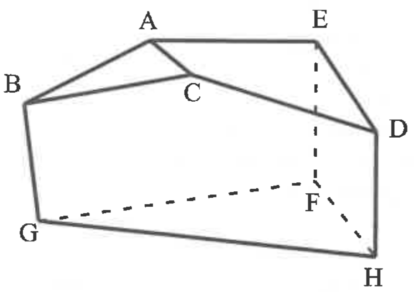


Figure 3

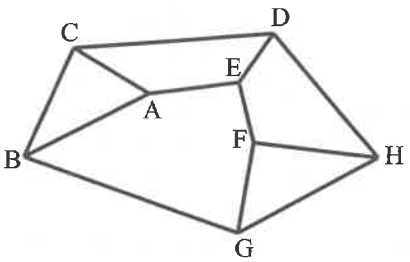


Figure 4

Construction du dual utilisant le graphe dual :
On supprime une face par exemple (BCDHG) et on aplatit comme vu dans la démonstration de la formule d'EULER au début. On obtient le polygone (P′) de la Figure 4.
Remarquez que les faces sont bien les mêmes sauf (BCDHG) qu'on a perdue mais qu'on peut considérer comme l'extérieur de la Figure 4.
Ensuite on choisit un point à l'intérieur de chaque polygone du pavage, y compris un point à l'extérieur pour (BCDHG). Ces points vont constituer les sommets du dual (P~).
Il ne reste plus qu'à joindre deux de ces points si et seulement si ce sont les points intérieurs à deux faces adjacentes de (P). Ce qui est réalisé par des pointillés sur la Figure 5.
Le dessin en pointillé est une vue de (P~) qu'on redessine proprement (Figure 6).

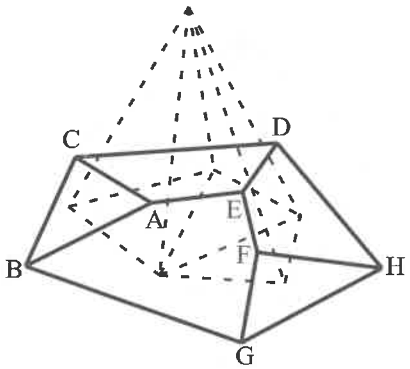


Figure 5

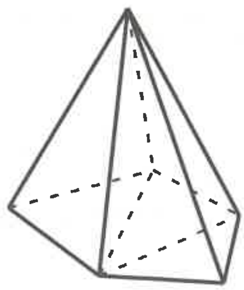


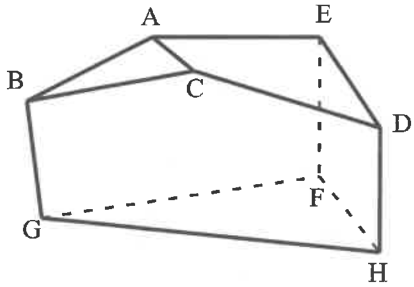
Figure 6

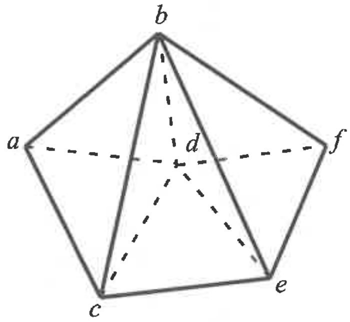
Construction du dual utilisant une représentation matricielle :
On commence par coder le polyèdre convexe (P) de type (S,F) par une matrice booléenne P de type (S,F) c'est-à-dire avec S lignes et F colonnes, avec la convention : $p_{i,j} = 1$ si et seulement si le sommet i appartient à la face j.
Pour notre exemple :

P =

	a	*b*	*c*	*d*	*e*	*f*
A	1	1	1	0	0	0
B	1	1	0	1	0	0
C	1	0	1	1	0	0
D	0	0	1	1	1	0
E	0	1	1	0	1	0
F	0	1	0	0	1	1
G	0	1	0	1	0	1
H	0	0	0	1	1	1

Dans ces conditions le dual (P~) a tout simplement pour matrice la transposée de P : P~
Pour effectuer la transposition, il suffit de permuter les lignes et les colonnes de la matrice P ainsi :
(P) a pour sommets {A,B,C,D,E,F,G,H} et pour faces a = {ABC}, b = {ABEFG}, c = {ACDE}, d = {BCDGH}, e = {DEFH}, f = {FGH}.
Donc, en tranposant, son dual (P~) a pour sommets {*a*,*b*,*c*,*d*,*e*,*f*} et pour faces A = {*abc*} B = {*abd*} C = {*acd*} D = {*cde*} E = {*bce*} F = {*bef*} G = {*bdf*} H = {*def*}.
Ce qui donne directement :





Polyèdre (P) Figure 6

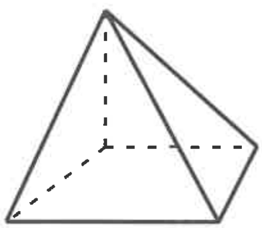
Ce dual peut être vu comme la réunion des 3 tétraèdres (abcd), (bcde) et (bdef).

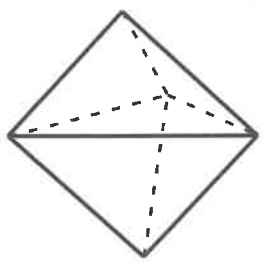
Il faut bien se persuader que **la matrice P détermine parfaitement le polyèdre (P).** Bien sûr pour dessiner (P) à partir de P, il y a un petit problème : pour chaque face on connaît les sommets mais pas l'ordre dans lequel ils se présentent. Mais il suffit de remarquer que (P) possède l'arête (X_i, X_j) si et seulement si dans les lignes i et j de P il existe deux colonnes k et l telles que $p_{i,k} = p_{i,l} = p_{j,k} = p_{j,l} = 1$. Alors l'arête ($X_i$, X_j) est l'intersection des faces k et l.
Par contre, comme on peut numéroter arbitrairement les sommets et les faces, un polyèdre (P) possède plusieurs matrices représentatives se déduisant les une des autres par permutations des lignes ou permutations des colonnes.

La dualité est importante car tout résultat concernant les polyèdres convexes a automatiquement un résultat dual. On échange S et F tout simplement. Voici quelques exemples :

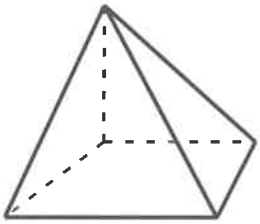
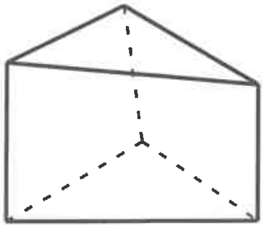
Exemple 1. **Le nombre de polyèdres à *n* faces est égal au nombre de polyèdres à *n* sommets.**

Ainsi : Il y a deux polyèdres convexes à 5 sommets : (la 4-pyramide et la 3-bipyramide).





DONC Il y a deux polyèdres convexes à 5 faces : (la 4-pyramide auto-duale et le 3-prisme).

Exemple 2. La condition de STEINIZ a deux formes duales équivalentes :

$$\mathbf{S \geq 4 \quad \text{et} \quad \frac{1}{2}S + 2 \leq F \leq 2S - 4}$$

ou

$$\mathbf{F \geq 4 \quad \text{et} \quad \frac{1}{2}F + 2 \leq S \leq 2F - 4}$$

Exemple 3. Si on note s_p le nombre de sommets d'ordre p (appartenant à p faces) et f_p le nombre de faces d'ordre p (ayant p sommets), on a les deux relations duales :

$$s_4 + 2\,s_5 + 3\,s_6 + 4\,s_7 + \ldots = 2\,\mathrm{F} - \mathrm{S} - 4,$$

$$f_4 + 2\,f_5 + 3\,f_6 + 4\,f_7 + \ldots = 2\,\mathrm{S} - \mathrm{F} - 4,$$

et aussi

$$3\,s_3 + 2\,s_4 + s_5 \geq 12,$$
$$3\,f_3 + 2\,f_4 + f_5 \geq 12,$$

qui sont autant d'exercices amusants.

4) Passons aux dénombrements proprement dits.

En utilisant tout ce qui précède, montrons par exemple qu'il y a sept polyèdres convexes à 6 faces :

– D'abord il est évident que : **si $i \geq 6$ alors $f_i = 0$.**

– F = 6 , la condition de STEINIZ implique $\mathbf{5 \leq S \leq 8}$ et la relation

$$f_4 + 2\,f_5 + 3\,f_6 + 4\,f_7 + \ldots = 2\,\mathrm{S} - \mathrm{F} - 4$$

devient

$$\boldsymbol{f_4 + 2\,f_5 = 2\,\mathrm{S} - 10,}$$

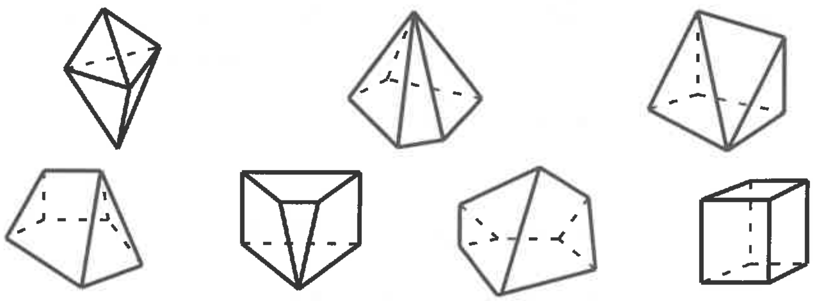
d'où l'algorithme :

Pour S variant de 5 à 8 on résout l'équation diophantienne $f_4 + 2\,f_5 = 2\,\mathrm{S} - 10$ et pour chaque solution (f_4, f_5) on tire $f_3 = \mathrm{F} - f_4 - f_5 = 6 - f_4 - f_5$.
On connait donc le nombre de faces de chaque ordre et on essaie de les placer de toutes les façons possibles à partir de l'une d'elles choisie comme base (on peut s'aider de la relation duale, ici : $s_4 + 2\,s_5 = 8 - \mathrm{S}$).
fin.

Cela donne :

pour S = 5, une solution : $f_3 = 6, f_4 = 0, f_5 = 0$;
pour S = 6, deux solutions : $f_3 = 5, f_4 = 0, f_5 = 1$ et $f_3 = 4, f_4 = 2, f_5 = 0$;
pour S = 7, deux solutions : $f_3 = 3, f_4 = 2, f_5 = 1$ et $f_3 = 2, f_4 = 4, f_5 = 0$;
pour S = 8, deux solutions : $f_3 = 2, f_4 = 2, f_5 = 2$ et $f_3 = 0, f_4 = 6, f_5 = 0$.

Voici les sept hexaèdres dans l'ordre précédent :



5) Combien y a t-il de polyèdres convexes à *n* arêtes ?

Si le nombre d'arêtes n est donné, alors $S + F = n + 2$ est constant, donc pour avoir le nombre de polyèdres convexes à n arêtes, il suffit dans le tableau donnant le nombre $\pi(S,F)$ de polyèdres convexes de type (S,F) de faire la somme des $\pi(S,F)$ pour $S + F = n + 2$, $S \geq 4$, $F \geq 4$.

On obtient :

nombre d'arêtes	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
nombre de polyèdres	**1**	**0**	**1**	**2**	**2**	**4**	**12**	**22**	**58**

Il s'agit de la suite M0339 de l'encyclopédie intitulée « polyedral graphs with *n* edges ».

J'ai obtenu les dessins des **34 heptaèdres convexes** (en fin d'article) en utilisant leur représentation aplatie comme vue précédemment, et en me ramenant donc à la recherche de tous les pavages polygonaux en six polygones. Ce qui ne va pas tout seul car deux pavages distincts peuvent être ceux d'un même polyèdre qu'on a aplati de deux façons en ne supprimant pas la même face.
Le codage par matrice booléenne est évidemment plus adapté au calcul (informatique) mais encore faudrait-il caractériser les matrices qui représentent des polyèdres convexes qui existent !
Ces 34 heptaèdres sont classés selon leur nombre de sommets (voir la colonne F = 7 du tableau $\pi(S,F)$) :

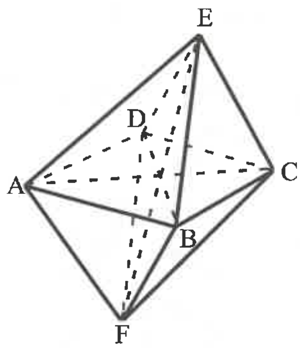
1 à 2, ceux qui ont 6 sommets,
3 à 10 ceux qui ont 7 sommets,
11 à 21, ceux qui ont 8 sommets,
22 à 29, ceux qui ont 9 sommets,
30 à 34, ceux qui ont 10 sommets.

6) Le sujet est loin d'être épuisé.

Le fait que tout polyèdre convexe est la juxtaposition d'un nombre fini de tétraèdres est une piste intéressante.

Lorsqu'on « tronque » un sommet d'un polyèdre convexe, on obtient un polyèdre convexe de type voisin. C'est une autre piste.

Et je me suis limité aux convexes ! Pour les autres, la relation d'EULER n'est même pas garantie. Par exemple, il n'est pas évident même avec le dessin de se représenter l'heptaèdre croisé ci-contre (certaines faces se coupent selon des segments qui ne sont pas des arêtes) de matrice



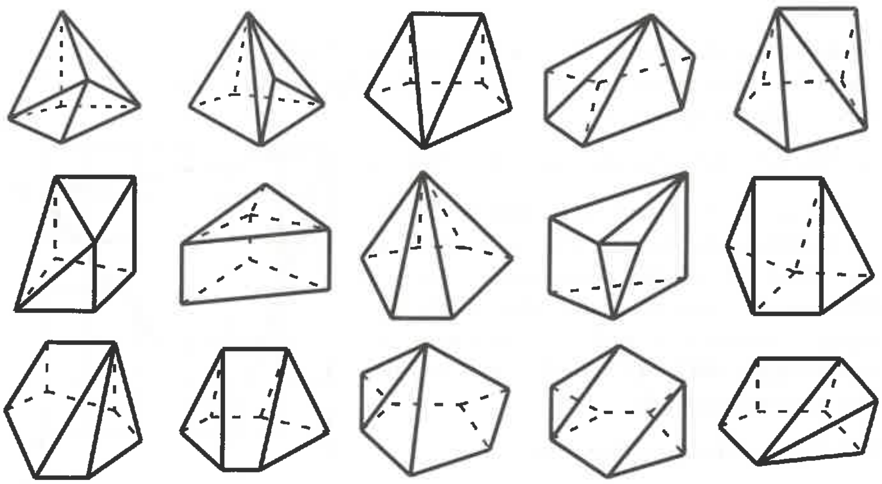
1 1 0 1 0 1 0
1 0 1 0 1 1 0
1 1 0 0 1 0 1
1 0 1 1 0 0 1
0 1 1 1 1 0 0
0 1 1 0 0 1 1

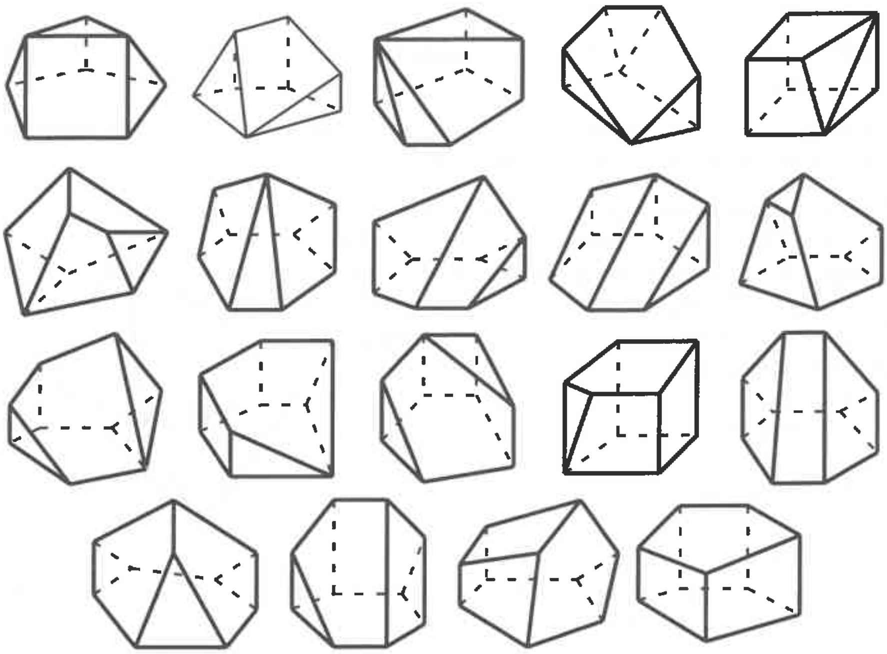
Ce polyèdre n'a que 7 faces : les trois quadrilatères ABCD, ACEF et BDEF et les quatre triangles ADE, BCE, ABF et CDF.

Bibliographie :

H.M. CUNDY et A.P. ROLLETT. *Modèles mathématiques*. CEDIC.
N.J.A. SLOANE S. PLOUFFE. *The encyclopedia of integer sequences*. Academic Press.
A. HOLDEN. *Formes espace et symétries*. CEDIC (Les Distracts).

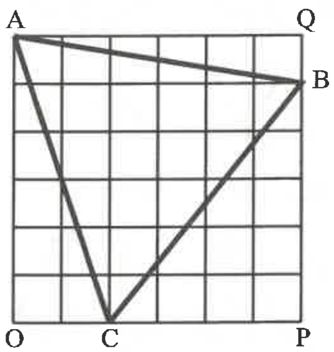
Les 34 heptaèdres convexes





SOLUTION DU PROBLÈME DE LA PAGE 29

Supposons qu'il existe un triangle ABC équilatéral dont les sommets sont sur les nœuds d'un quadrillage carré et appelons a la longueur de son côté (l'unité choisie étant le côté des carrés).



On démontre sans peine que l'aire du triangle est égale à $a^2\sqrt{3}/4$ qui est un nombre irrationnel car, d'après le théorème de Pythagore, a^2 est un entier. Mais, en calculant cette même aire comme différence de l'aire du quadrilatère AOPQ dans lequel est inscrit le triangle et de la somme des trois triangles ABQ, ACO et BPC, on trouve que cette aire est rationnelle.

Un tel triangle n'existe donc pas.

Avis de recherche

Vous pouvez utiliser cette rubrique pour poser des questions de tout ordre : demande d'une démonstration, d'une référence, de résolution d'un problème, d'éclaircissement d'un point historique, etc.
Veuillez envoyer vos questions et réponses, avec une feuille par sujet et votre nom sur chacune, et, si possible, le texte sur disquette (avec enveloppe affranchie si vous souhaitez son retour) à :

Robert FERRÉOL
6, rue des annelets
75019 PARIS.

par Internet : rferreol@club-internet.fr

Nouvel avis de recherche

Avis de recherche n° 125 transmis par Annie Michel-Pajus.

Quels sont les modes de calcul de l'espérance de vie ?

(En espérant que cette question aura plus de succès que mon AR sur la fixation des taux de change…)

Ancien avis de recherche

Avis de recherche n° 114 sur les nombres figurés (cf. bulletin 429, p. 497)

Contribution de Jean Moreau de Saint Martin (Paris).

Je suis étonné d'une indication donnée par P. Bornsztein dans sa réponse à l'avis de recherche 114, selon laquelle un recours aux courbes elliptiques serait nécessaire pour trouver les carrés impairs qui sont des nombres tétraédriques.
Ce problème se résout par des moyens élémentaires, comme je vais le montrer ci-dessous. Il doit y avoir confusion avec le « cas impair du problème de Lucas (pyramidaux carrés) », dont maintenant des solutions élémentaires sont connues, comme P. Bornsztein le signale.
Soit donc $y\,(y+1)\,(y+2) = 6x^2$ avec x impair.
Aucun des facteurs y, $y+1$, $y+2$ n'est multiple de 4, leurs restes modulo 4 sont donc 1, 2, 3 dans cet ordre.

Les diviseurs premiers de x se répartissent en trois facteurs a, b, c, qui sont impairs et dont les carrés divisent respectivement y, $y+1$, $y+2$. Ces carrés ont pour reste 1 modulo 4, ce qui entraîne que y, $y+1$, $y+2$ valent respectivement a^2, $2b^2$, $3c^2$. En outre a, b, c sont premiers deux à deux.

On en tire $y + 2 = 3c^2 = a^2 + 2 = 2b^2 + 1 = 4b^2 - a^2 = (2b + a)\,(2b - a)$.

Je vais utiliser deux fois la propriété :
(P) Si les facteurs d'un produit sont deux à deux premiers entre eux, tout diviseur premier qui divise un facteur y a le même exposant que dans le produit.

Celui des facteurs $(2b + a)$ et $(2b - a)$ qui n'est pas multiple de 3 est un carré, car ces facteurs sont premiers entre eux et ont pour produit $3c^2$. Quitte à changer le signe de a, je peux supposer que c'est $2b - a = u^2$, carré impair : $u = 2t + 1$.

On a ensuite $1 = 2b^2 - a^2 = (2b - a)^2 - 2(a - b)^2$.

$\dfrac{a-b}{2}$ est un entier de carré : $\dfrac{u^4-1}{8} = t\,(t+1)\,(2t\,(t+1)+1)$.

Dans ce dernier produit, il est clair que les trois facteurs sont deux à deux premiers entre eux. Le produit étant un carré, s'il est non nul ($t > 0$), par (P) chacun des facteurs est un carré et les entiers consécutifs t et $t + 1$ seraient tous deux des carrés. C'est impossible.

Il en résulte $t = 0$, $u = 1$, puis $a = b = c = 1$, $x = y = 1$. CQFD.

Avis de recherche n° 123 :

Dans son excellent livre : « Visions géométriques », Belin, 1993, Ian Stewart donne (page 15) une formule donnant l'équation de la conique des positions possibles d'un point P pour un birapport du faisceau de droites (PA), (PB), (PC), (PD) donné. Où peut-on trouver une démonstration de cette formule ?

Réponse de Jacques Bouteloup (Rouen), qui précise que ce problème lui a été posé en 1945 lors de sa préparation à l'agrégation, que la solution qu'il en donne ici est celle qu'il avait donnée à l'époque, et qu'il n'a jamais vu la question évoquée dans aucun livre.

Étant donnés quatre points A, B, C, D distincts fixés dans le plan, il s'agit donc d'établir l'équation de l'ensemble des points P du plan tels que le birapport ((PA),(PB),(PC),(PD)) soit égal à une constante r donnée.

C'est un problème projectif. Mais nous le résoudrons par un calcul affine, ce qui est plus commode et nous conduira à une équation analogue à celle du livre de Ian Stewart. Nous supposons donc les points non à l'infini.

Le birapport de quatre droites concourantes, dont les équations peuvent s'écrire $y - y_0 = m(x - x_0)$ pour quatre valeurs de m, est le birapport de leurs points à l'infini, qui peuvent être représentés par $(1,m)$, donc celui des paramètres m. C'est encore valable si l'une est parallèle à Oy, en acceptant, ce qui est loisible, la valeur ∞ dans le birapport.

Désignons par (x_i,y_i) les coordonnées des points donnés (i = A, B, C, D), et par (x,y) celles de P. Le paramètre m de (PA) est $t_A = \dfrac{y - y_A}{x - x_A}$. Nous introduisons de même t_B, t_C, t_D.

Nous aurons donc, pour $((PA),(PB),(PC),(PD)) = r$, la relation $(t_A,t_B,t_C,t_D) = r$ qui s'écrit :

$$(t_C - t_A)(t_D - t_B) - r(t_C - t_B)(t_D - t_A) = 0.$$

Or

$$t_C - t_A = \frac{\begin{vmatrix} x - x_A & x - x_C \\ y - y_A & y - y_C \end{vmatrix}}{(x - x_C)(x - x_A)} = \frac{\Delta(A,C)}{(x - x_C)(x - x_A)}.$$

$\Delta(A,C)$ est un polynôme en (x,y) du premier degré, et $\Delta(A,C) = 0$ représente une équation de (AC). Nous définissons de façon analogue les autres fonctions Δ de deux lettres. Après multiplication par $(x - x_A)(x - x_B)(x - x_C)(x - x_D)$, nous obtenons l'équation de la conique décrite par les points P sous la forme :

$$\Delta(A,C)\,\Delta(B,D) - r\,\Delta(A,D)\,\Delta(B,C) = 0.$$

Elle passe par A, B, C, D (les coordonnées de A, par exemple, annulent $\Delta(A,C)$ et $\Delta(A,D)$). On la retrouve aisément par analogie avec l'expression du birapport de quatre points A, B, C, D alignés : $\overline{AC}\cdot\overline{BD} - r\overline{AD}\cdot\overline{BC}$.

Dans son article « D'où a été prise la photo ? » de « Pour la Science » (Février 1990), article repris tel quel dans l'ouvrage « Visions géométriques », Ian Stewart donne, avec mes notations, l'équation apparemment différente :

$$(r - 1)\,\Delta(A,C)\,\Delta(B,D) - r\,\Delta(A,B)\,\Delta(D,C) = 0.$$

Mais la suite des quatre droites (PA), (PB), (PC), (PD) présente 24 permutations, conduisant à six valeurs en général distinctes du birapport, chacune obtenue quatre fois. La permutation de B et D donne $((PA),(PD),(PC),(PB)) = \dfrac{r}{r-1}$. Les deux équations sont donc identiques.

Dans cet article, Ian Stewart développait une méthode pour résoudre le problème posé par le titre utilisant notamment cette équation. C'est en fait une méthode non rigoureuse, ne conduisant qu'à un résultat approché. En réponse à mes questions, Ian Stewart m'a écrit qu'elle était valable lorsque le photographe était « très près » du sol.

Il m'apparaît bon de dire quelques mots du problème projectif général. Désignons par $E(A,C) = 0$, $E(B,D) = 0$, $E(A,D) = 0$, $E(B,C) = 0$ des équations de (AC), (BD), (AD), (BC) dans un repère projectif quelconque. L'équation

$$E(A,C)\,E(B,D) - k\,E(A,D)\,E(B,C) = 0$$

représente une conique passant par A, B, C, D. On démontre que le birapport $((PA),(PB),(PC),(PD))$ demeure constant lorsque P parcourt la conique, et qu'on obtient une autre valeur pour k différent, ce qui résout le problème général du lieu évoqué. Mais les premiers membres des équations n'étant définis qu'à un facteur multiplicatif près, ce birapport r n'a aucune raison d'être égal à k. Cependant, trois équations étant fixées, k prend toutes valeurs lorsque le facteur multiplicatif de la quatrième varie. On peut donc choisir la bonne équation pour que $k = r$, et obtenir ainsi une équation analogue à l'équation affine. L'intérêt du calcul élémentaire du début est que les « bonnes » équations se sont introduites automatiquement.

Les problèmes de l'APMEP

Cette rubrique propose des problèmes choisis pour l'originalité de leur caractère : esthétique, subtil, ingénieux voire récréatif, dont la résolution nécessite initiatives, démarche inventive, recherche, effort intellectuel.
Elle accueille tous ceux qui aiment inventer, chercher de « beaux problèmes »… si possible trouver des solutions, et les invite à donner libre cours à leur imagination créatrice. La rubrique s'efforce de rendre compte de la pluralité des méthodes proposées par les lecteurs, des généralisations des problèmes…
Les auteurs sont priés de joindre les solutions aux propositions d'énoncés. Solutions et énoncés sont à envoyer à l'adresse suivante (réponse à des problèmes différents sur feuilles séparées S.V.P., sans oublier votre nom sur chaque feuille) :

François LO JACOMO,
42 quai de la Loire,
75019 Paris.

Solutions

Énoncé n° 276 (Michel LAFOND, 21-Dijon)

Quels sont les polyèdres convexes qui ne possèdent pas trois faces ayant le même nombre de côtés ?

SOLUTION

Cet énoncé s'inscrit dans le cadre d'un vaste travail de Michel LAFOND sur les polyèdres : à la même époque, celui-ci m'envoyait, à propos de l'avis de recherche n° 86, une étude exhaustive des 34 heptaèdres convexes. J'ai reçu quatre autres solutions, plus ou moins complètes, de Marie-Laure CHAILLOUT (95-Sarcelles), René MANZONI (76-Le Havre), Marguerite PONCHAUX (59-Lille) et Pierre RENFER (67-Ostwald).

Le problème se scinde en deux : premièrement, trouver quel nombre de faces, de sommets et d'arêtes doit avoir un polyèdre solution, et deuxièmement, déterminer tous les polyèdres solutions. C'est essentiellement sur ce second point que les réponses ont été inégales, les lecteurs proposant deux, trois ou quatre polyèdres solutions avec plus ou moins de justifications. Sans compter que, pour trouver tous les polyèdres solutions, il faut préciser à quelle condition deux polyèdres sont considérés comme équivalents, donc comme deux représentants de la même solution, ce qui n'est pas évident *a priori*. On peut, par exemple, considérer que deux polyèdres sont équivalents s'il existe deux bijections, de l'ensemble des faces du premier vers l'ensemble des faces du second et de l'ensemble des sommets du premier vers l'ensemble des sommets du second, telles que si un sommet du premier polyèdre appartient à une face, son image (sommet du second polyèdre) appartient à l'image de ladite face.

Pour la première partie du problème, il convient évidemment d'utiliser la relation d'Euler : si F, S et A désignent le nombre de faces, de sommets et d'arêtes d'un polyèdre convexe, F + S = A + 2. Comme chaque arête contient deux sommets, et chaque sommet appartient à au moins trois arêtes, on a : $2A \geq 3S = 3\,(A + 2 - F)$, d'où $A \leq 3F - 6$. Pour obtenir une majoration de A, l'idée la plus astucieuse me semble être celle mise en œuvre par Marie-Laure CHAILLOUT et Pierre RENFER : classons les faces par ordre croissant du nombre d'arêtes. Les $(2k-1)$-ème et $(2k)$-ième faces ont au moins $(k + 2)$ arêtes, vu que, par hypothèse, le polyèdre n'a pas plus de deux faces triangulaires, de deux faces quadrilatérales, de deux faces pentagonales… Or chaque arête appartient à deux faces, donc

• si F est pair ($F = 2k$),

$$2A \geq (3 + 3) + \ldots + ((k + 2) + (k + 2)) = k^2 + 5k\,;$$

• si F est impair ($F = 2k + 1$),

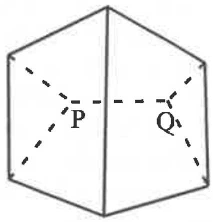
$$2A \geq (3 + 3) + \ldots\ ((k + 2) + (k + 2)) + (k + 3) = k^2 + 6k + 3.$$

Dans le premier cas ($F = 2k$), on doit donc avoir : $k^2 + 5k \leq 2A \leq 12k - 12$, soit : $k^2 - 7k + 12 \leq 0$, ce qui n'est vérifié que pour $k = 3$ ou $k = 4$. Pour $k = 3$, F = 6, A = 12 (le majorant et le minorant de 2A sont égaux), d'où S = 8 d'après la relation d'Euler. Pour $k = 4$, le même raisonnement conduit à : F = 8, A = 18 et S = 12.

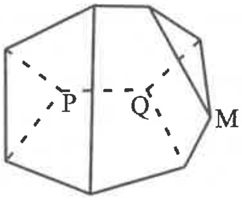
Dans le deuxième cas ($F = 2k + 1$), on doit avoir : $k^2 + 6k + 3 \leq 2A \leq 12k - 6$, soit : $k^2 - 6k + 9 \leq 0$, ce qui n'est vérifié que pour $k = 3$: on a alors F = 7, A = 15 donc S = 10.

Il reste à déterminer tous les polyèdres solutions, dans chacun des trois cas ci-dessus : F = 6, S = 8, A = 12 ; F = 7, S = 10, A = 15 ; F = 8, S = 12, A = 18. On remarquera pour commencer que, dans chaque cas, la majoration et la minoration de A sont toutes deux des égalités. Pour la minoration, on a : 2A = 3S, ce qui prouve que chaque sommet appartient exactement à trois arêtes, donc que deux faces qui ne sont pas disjointes ont obligatoirement une arête en commun (si elles n'avaient qu'un sommet commun, de ce sommet partiraient quatre arêtes). Pour la majoration, le fait qu'elle soit une égalité entraîne que le polyèdre a exactement deux faces triangulaires, deux faces quadrilatérales, deux faces pentagonales, et zéro, une ou deux faces hexagonales.

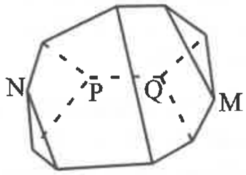
Dans le cas où F = 6, S = 8, A = 12, les deux faces pentagonales ne sont pas disjointes (cela ferait 10 sommets), elles ont donc une arête PQ en commun. Ces deux faces à elles seules définissent 8 sommets et 9 arêtes du polyèdre : celui-ci n'a pas d'autre sommet, et il a trois autres arêtes, qui nécessairement joignent chacun un sommet d'un pentagone à un sommet de l'autre pentagone. S'agissant d'un polyèdre convexe, cela laisse une seule possibilité.



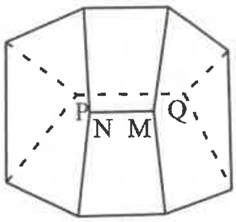
Lorsque F = 7, S = 10, A = 15, le polyèdre a une face hexagonale en plus des deux faces pentagonales. Considérons la face hexagonale et l'une quelconque des faces pentagonales : elles ne peuvent pas être disjointes, cela ferait 11 sommets, elles ont donc une arête PQ en commun. Elles définissent à elles seules 9 sommets et 10 arêtes, il reste donc un sommet M et cinq arêtes. De M partent obligatoirement trois arêtes, et les deux dernières arêtes joignent un sommet de l'hexagone à un sommet du pentagone. Donc deux des arêtes issues de M atteignent deux sommets (nécessairement voisins) de l'hexagone, définissant une face triangulaire, l'autre arête atteint un sommet du pentagone et délimite deux faces dont une seule (au plus) est un pentagone (il n'y a que deux faces pentagonales en tout) : l'autre contient donc nécessairement P ou Q, ce qui laisse une seule possibilité à équivalence près.

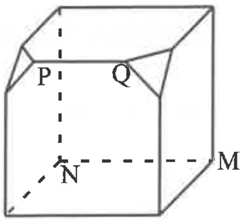


Lorsque F = 8, S = 12, A = 18, le polyèdre a deux faces hexagonales, qui ne sont pas disjointes, sinon il n'y aurait pas d'autre sommet que ceux des hexagones et une face pentagonale aurait trois sommets communs avec un hexagone, ce qui est absurde. Les deux hexagones ont donc une arête PQ en commun, ils définissent 10 sommets et 11 arêtes du polyèdre, il reste deux sommets M et N et 7 arêtes. Mais là, il convient de distinguer deux cas : soit M et N sont joints par une arête, soit ils ne sont pas joints par une arête. Dans ce second cas, de M partent trois arêtes, de N partent trois arêtes, et il reste une septième arête joignant un sommet d'un hexagone à un sommet de l'autre hexagone. Deux des arêtes issues de M atteignent deux sommets voisins d'un hexagone, définissant une face triangulaire, et deux arêtes issues de N atteignent deux sommets voisins de l'autre hexagone (sinon il ne resterait pas de sommet libre pour la septième arête), définissant une seconde face triangulaire. Il n'existe donc pas d'autre face triangulaire, donc l'arête restante ne peut pas joindre les deux sommets voisins de P ni les deux sommets voisins de Q : les deux sommets voisins de P sont donc joints à N et les deux sommets voisins de Q, à M (ou inversement), ce qui laisse, en définitive, une seule possibilité à équivalence près.



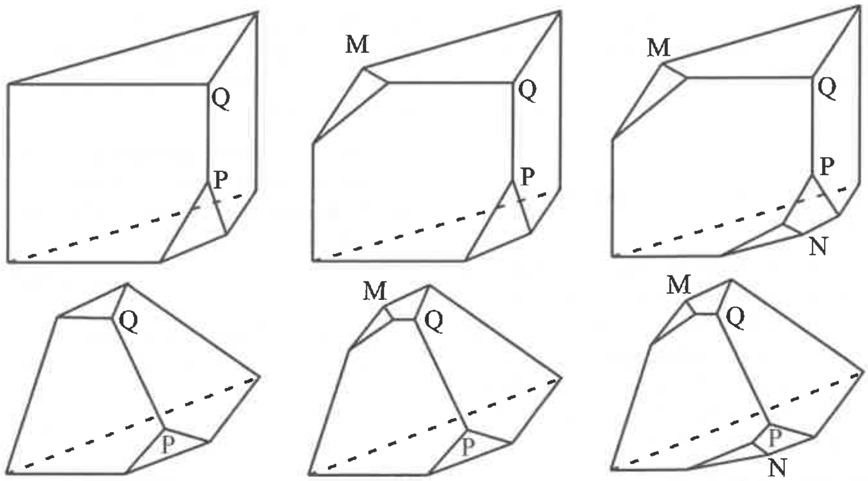
Reste le cas où M et N sont joints par une arête : par M ou N passent 5 arêtes en tout, il en reste deux joignant un sommet de l'hexagone à un sommet de l'autre hexagone. Chaque face pentagonale a au plus deux sommets communs avec chaque hexagone, et au plus deux sommets dans {M, N} : elle a donc nécessairement un sommet au moins dans chacun des trois ensembles, donc une arête commune avec chaque hexagone, et un cinquième sommet égal à M ou N. Comme elles ne peuvent pas avoir en commun un et un seul point, M appartient à une face pentagonale, N à l'autre. Les deux arêtes issues de M (autres que MN), qui délimitent le pentagone, atteignent donc chacun des hexagones, et de même pour les deux arêtes issues de N. Les deux arêtes restantes appartiennent obligatoirement chacune à une face pentagonale et à une face





triangulaire, qui contient donc P ou Q, ce qui laisse une seule possibilité à équivalence près.

On remarquera que cette quatrième et dernière solution équivaut à un cube tronqué en deux sommets voisins. Les trois premières solutions équivalent, elles, à des prismes triangulaires tronqués une, deux ou trois fois. Si l'on redescend le point à l'infini intersection des arêtes verticales, ledit prisme équivaut à un tétraèdre décapité, donc ces trois premières solutions équivalent à des tétraèdres tronqués deux, trois ou quatre fois.



Matériaux pour une documentation

NB. Sauf pour les brochures APMEP ou co-diffusées par elle, les ouvrages ci-après recensés, ainsi que ceux de « Pour un inventaire », ne doivent pas être commandés à l'APMEP, mais chez votre libraire habituel.
Tout adhérent peut proposer un compte rendu d'un ouvrage auquel il n'a pas collaboré. Pour éviter les doublons, un accord préalable doit être demandé à Henri Bareil, responsable de la rubrique (Tél. 05 61 52 74 53). Merci d'avance.

« SYMÉTRIE CENTRALE EN 5ème DANS UN ENVIRONNEMENT INFORMATIQUE », par une équipe de quatre enseignants en Collège. Éd. : IREM de Clermont, Complexe Scientifique des Cézeaux, 63177 Aubière Cedex.
74 pages en A4. Très bonne présentation. Prix : 40 F (+ port : 15 F)

L'INTRODUCTION précise que le fascicule comprend deux parties et réfléchit au bien-fondé de l'utilisation de l'outil informatique en géométrie. Aussitôt après viennent des précautions à prendre pour mettre en place et conduire une séance de « géométrie dynamique au collège ». Puis :

PREMIÈRE PARTIE – *par trois auteurs – qui utilise CABRI2 : Huit fiches*, de 1 h ou 2 h, menant de front un apprentissage sommaire, minimal et progressif, du logiciel et l'appropriation du concept de symétrie centrale.
La première séquence est directive. L'autonomie des élèves est ensuite de plus en plus possible.
Il y a quatre activités de découverte (du concept), quatre de réinvestissement. Une « Annexe » permet de faire du « papier pointé ».

DEUXIÈME PARTIE – *par un auteur – qui utilise GEOPLAN W*. Ici les élèves utilisent d'emblée le logiciel « comme imagiciel » « ouvrant un fichier préparé à l'avance, animant une figure, … ». Quatre activités de découverte.

CHACUNE DES DOUZE ACTIVITÉS comporte :
– une fiche élève photocopiable,
– une fiche de « commentaires », clairs et bienvenus, pour le professeur.
(téléchargeabilité sur le serveur du Rectorat de Clermont : http//crdp.ac-clermont.fr/pedago/maths/).

L'ensemble me semble plaisant pour l'élève, éducatif pour conjecturer, construire, découvrir. Ce doit être aussi un bon outil pour l'enseignement.

Henri BAREIL

« MATHÉMATIQUES ET TABLEUR AU COLLÈGE, Classes de 4ème et 3ème », par sept enseignants en Collège. Éd. : IREM de Clermont, Complexe Scientifique des Cézeaux, 63177 Aubière Cedex.
40 pages en A4. Très bonne présentation. Prix : 30 F (+ port : 12 F).
(« Feuilles de calcul au format Works ou Excel disponibles – téléchargeables – sur le serveur du Rectorat de Clermont : http:/www.ac-clermont.fr/pedago.maths/).

Cette brochure en complète deux déjà publiées par le même IREM sur le même sujet : Classe de 4^e (1998), *Classe de 3^e* (1999). Le lot des trois brochures : 80 F (+ port 16 F). Les trois brochures + symétrie centrale en 5^e : 100 F (+ port : 35 F)

Les fiches ont été expérimentées par les enseignants dans leurs classes.

Première partie (8 pages) : **Les mathématiques et le tableur** : Effet dynamique du tableur (liens entre les cellules, …) – Fonction « Recopie » – Quelle progression avec le tableur dans une leçon ? Comment noter le contenu des cellules ? – mise en place de formules avec le zéro – …

Deuxième partie (5 pages) : **Fiches techniques** (Works et Excel). Protéger une feuille de calcul – Nommer une cellule ou une plage – « Valeur cible » (Excel seul).

Troisième partie (24 pages) : **Fiches élève et fiches professeur** (Works et Excel sauf ...) (six pour la 3^{e}, une pour la 4^{e} et une 4^{e}-3^{e}).
– « *Cours* » :
– Moyenne pondérée et référence absolue d'une cellule en tableur.
– Activité pour mise à niveau en 3^{e} quant au tableur (Excel seul).
– Fonction affine et graphique sur tableur (Excel seul).
– « *Problèmes* » : Trois débouchent sur des inéquations. Un autre, lié aux nombres triangulaires et à la somme d'entiers successifs de 1 à n, débouche sur la création de suites au tableur. Le dernier est un « codage-décodage » lié à la division euclidienne.

L'ensemble me paraît excellent, avec beaucoup de remarques, incitations, analyses, d'une grande finesse et d'un talent pédagogique confirmé, tant du point de vue des mathématiques que de l'usage du tableur.

Henri BAREIL

« **10 EXPÉRIENCES MATHÉMATIQUES à la portée des collégiens : FIGURES ET NOMBRES AU FIL DES CIVILISATIONS** » par une équipe, animée par Francis DUPUIS, initialement épaulée par l'Association Tunisienne des Sciences Mathématiques. **Numéro spécial 32-33 de la revue HYPERCUBE**. Éd. Archimède, 5 rue Jean Grandel. 95100 Argenteuil. Diffusion Belin.
48 pages en A4 d'un bon papier couché, et, à l'intérieur, 12 pages, de figures à découper, en papier fort.
Brochure en couleurs, très illustrée, séduisante. Prix : 65 F.
ISSN : 1256-7647, ISBN : 2-84469-022-X.

• « **10 EXPÉRIENCES-JEUX,** 10 raccourcis à travers le temps et l'espace »..., autant de « haltes rapides, quelques fenêtres ouvertes sur 25 siècles de l'histoire des maths »... :
– « *les poids de Babylone* » : numération en diverses bases, de Babylone aux Shadocks et aux ordinateurs,
– « *la pierre angulaire* » : cubes, pavés droits, pyramides, troncs de pyramide... (avec formules de volumes), puzzles, ... et pyramides égyptiennes,
– « *Thalès en un clin d'œil* » : de Thalès – ou des égyptiens – à la croix du bûcheron et à la trigo,
– « *les nombres figurés* » : triangulaires, ..., chers à Pythagore, avec des assemblages de formes qui appuient des calculs,
– « *Pythagore en pièces* » avec sa démonstration par Pappus, un peu d'historique, et l'extension générale,
– « *Pavage magique* » : en carrés magiques,
– « *Kwarizmath* » : une équerre pour résoudre $x^2 + bx = c^2$!, ... un peu d'histoire avec les arabes et Al-Kwarizmi,
– « *Trois carrés en un* » : des carrés du Ménon à ceux d'Abu-l'Wafa,
– « *L'escalier de Leonardo* » : des manières de monter un escalier à Fibonacci et au nombre d'or,
– « *Curieux carrelages* » : du 12^{e} siècle à Escher, Penrose et les quasi-cristaux.

• **CHAQUE ACTIVITÉ EST** :
– *inaugurée en deux pages* : un problème ... et un conseil, avec appel, en général, à des découpages et expérimentations,
– *poursuivie en deux pages de commentaires* qui rattachent à un problème plus général, l'innervent par son histoire en proposant, au fil du courant, éclairages et questions...
Quelques exemples de celles-ci :
« Trouvez un puzzle pour calculer le volume d'une pyramide ».
« Appliquez le découpage d'Abu-l'Wafa à trois carrés inégaux, de côtés 1, 2 et 3, puis à trois carrés inégaux de côtés 1, 1 et 2 »,
« Ne gardez qu'un nombre sur deux de la suite de Fibonacci. Comment retrouver l'un des nombres à partir de ceux qui précèdent ? ».

• La brochure se termine par quatre pages de « **SOLUTIONS** ».

• *J'avoue m'être régalé.* Certes, point d'austères démonstrations téléguidant en cascade, souvent seulement des allusions à telle ouverture, telle application… Mais quel art pour captiver, faire naître la curiosité, le désir, la volonté de s'investir ! Cela en associant harmonieusement manipulations, thèmes mathématiques, aperçus d'histoire des maths, coups de projecteurs et interrogations, en des lumières d'aurore…
Bref un livre à la fois clair, agréable et nourrissant, alliant intelligemment la tête et les mains en une ludique symphonie. BRAVO !

Henri BAREIL

N.B. Cet ouvrage, diffusé en librairie, est aussi le catalogue de l'exposition payante « RIVAGES MATHÉMATIQUES » constituée soit de 10 panneaux grand format, guides pédagogiques, en « Version établissement », soit en « Version expo-classe », d'un matériel plus léger … et moins cher. Renseignements et réservations au 01 39 98 83 50.

GÉOMÉTRIE EXPÉRIMENTALE AU COLLÈGE : activités mathématiques avec … un rétroprojecteur, un ordinateur et Cabri-géomètre, par Michel ROUSSELET. Éd. : CRDP de Versailles.
160 pages en A4. Bonne présentation, très claire.
ISBN : 2-907852-48-5. Prix : 88 F (+ port : 20F). Co-diffusion par l'APMEP à 83 F (cf. page 134).

La brochure est accompagnée d'une disquette (comprise dans le prix) qui permet la réalisation immédiate de constructions, sinon trop longues, avec Cabri 1.7 pour CABRI I et avec CABRI II. La disquette contient également des macro-commandes, possédées par Cabri II, données ici pour les usagers de Cabri I, version 1.7.

Le tout propose « *une palette d'activités de base, déclinée à tous les niveaux du Collège et étroitement liée aux programmes des différentes classes* » : 26 activités pour la Sixième (dont 5 pour l'espace), 25 pour la Cinquième (4 pour l'espace), 29 pour la Quatrième (3 pour l'espace), 29 pour la Troisième (1 pour l'espace).

Généralement, chaque fiche précise *l'objectif* et les *prérequis*, puis développe une *construction*, son *utilisation*, et conclut par un « *prolongement* ».
On sait que la pratique d'un logiciel (ici pour la construction en jeu et son utilisation) mobilise des qualités d'attention et qu'un intérêt majeur réside dans la possibilité, largement maîtrisée par Cabri, de décomposer et recomposer des figures, de les déplacer, éventuellement de les modifier en gardant tel ou tel caractère, d'une manière très convaincante *pour conjecturer et constituer de bonnes images mentales*.
La structure de Cabri permet d'ériger des conjectures de base (parallélisme, orthogonalité, appartenance d'un point, …) en certitudes quasi-absolues. Ce ne serait pas, quant à une formation de l'esprit critique, tellement souhaitable. Aussi Michel Rousselet, dans les « prolongements », *engage-t-il l'élève dans des démonstrations* – sans y limiter ces « prolongements » qui intéressent aussi à des généralisations, transferts ou autres points de vue.

Prenons l'exemple du théorème de Pythagore :

Une première fiche fait relever les « BC^2 » et « $AB^2 + AC^2$ » d'un triangle rectangle aux côtés modifiés. « Comme les mesures faites par Cabri sont arrondies au dixième près, on peut observer qu'on obtient rarement $BC^2 = AB^2 + AC^2$. L'imprécision de la méthode oblige à donner des arguments plus forts ». Une seconde fiche établit le théorème. Une troisième étudie la réciproque, d'abord avec des dessins de triangles, puis, « pour trancher », en donnant des étapes d'une démonstration classique – à faire –.

Cela suggère bien, je crois, l'intérêt de la brochure avec « des plus » côté expérimental, mais sans rien retrancher, au contraire, des aspects raisonnement et démonstration. Je lui souhaite un bon succès !

Henri BAREIL

« LA GÉOMÉTRIE CLASSIQUE. Objets et transformations »,par Benoit RITTAUD. Éd. Le Pommier.
160 pages en 13,5 × 19,9. Bonne présentation. Bibliographie. Glossaire. Index.
ISBN : 2-746-50037-X. Prix : 85 F.

Cet ouvrage relève d'une collection « Quatre à quatre » de quatre livres par an sur quatre ans, chaque année s'appuyant sur les précédentes, déjà présentée, dans notre Bulletin 429, page 511, à l'occasion de son premier titre « Qu'est-ce-que les mathématiques ? ». On s'y reportera.

Les chapitres 1 et 2 présentent les objets et instruments primitifs (point, droite, longueur, ..., triangle, ..., polyèdres, ..., compas, équerre, rapporteur, ...), avec une sagacité qui sait s'exprimer de façon imagée et soulever des à propos pertinents ..., par exemple en généralisant la notion de distance, en liant les angles alternes-internes à la taille des pierres de voûte, en évoquant le peu de contraintes pour créer un compas, ou le cercle comme « l'unique courbe plane à courbure constante ». Tout cela est dit simplement, sur le ton d'une attrayante conversation, avec *peu de démonstrations* (j'en ai relevé trois, à propos du triangle : pour ses médiatrices, ses bissectrices, la somme des angles) *mais avec, déjà, pas mal de propriétés.*
Les cas d'égalité des triangles tiennent une grande place. Oui, « d'égalité » : l'auteur y tient et, pour lui, deux figures planes sont « égales » si et seulement si elles peuvent coïncider par glissement. Notons aussi que, pour les angles, la seule notation utilisée est l'anglo-saxonne ($\angle$ABC, par exemple).

Le chapitre 3 est consacré à « Deux grands théorèmes » :
– introduit par quelques applications, *le théorème de Thalès* est démontré à partir des parallèles équidistantes par une progression, quant à la nature des nombres-rapports, terminée par un convaincant passage à la limite simplement présenté,
– une courte promenade dans l'entourage historique ou pratique du *théorème de Pythagore* débouche sur sa démonstration à partir du « $BA^2 = BC \times BH$ » établi par de classiques similitudes.

Le chapitre 4 présente d'abord les transformations isométriques et l'homothétie, avec de familiers assaisonnements (plus court chemin après réflexion, formats de papier, nombre d'or) et un joli conte sur l'incapacité de l'être humain à changer fortement de taille sans changer de forme.
On y devient, déjà, érudit quant aux objets énantiomorphes et chiraux (cf. nos deux mains, qui ne sauraient coïncider) avec ouverture sur biologie, escalier de Chambord et tire-bouchons.
Enfin les *projections* et, sans insister, *l'inversion*, nous disent leurs actions sur les objets les plus élémentaires.

Le chapitre 5 pique la curiosité avec « D'autres géométries » :
– allusive promotion des figures semblables au statut de figures égales,
– aperçu de la géométrie sphérique,
– quatrième dimension,
– fractales.
L'interrogation finale « Dans quel monde vivons-nous ? » se clôt par une évocation du tore.

Ma conclusion : Un excellent livre de CDI de Collège, également utile en CDI de lycée (notamment, culturellement, pour les L), facile à lire et, cependant, aussi profond que possible dans son panorama élémentaire.

Henri BAREIL.

SIMULATION ET STATISTIQUE EN SECONDE, par Ph. DUTARTE, Ch. KERN, B. VERLANT, épaulés par huit autres collègues. Éd. : IREM de Paris Nord. Avenue Jean-Baptiste Clément, 94430 Villetaneuse. http://www-irem.univ-paris13.fr
232 pages en A4. Présentation aérée pour changer de thème ou de type d'activité et dense dans le déroulement des programmes sur calculatrice ou tableur. Bibliographie. Tableaux de programmation de six séries de Casio, de quatre TI, de deux Sharp et d'une HP (48GX).
ISBN : 2-86240-102-X. Prix : 100 F.

• Il y a d'abord :
– des **COMPLÉMENTS DE PROBABILITÉS** (9 pages très denses !) : Loi des grands nombres et loi normale. Échantillonnage d'une fréquence.
– une étude de **GÉNÉRATEURS DE NOMBRES ALÉATOIRES** (37 pages) : « Travaux pratiques » avec calculatrice (fonction « random ») ou sur Excel (outils de base, fonction aléa) et « Un peu de théorie : comment simuler le hasard ».
• La brochure se termine (en 12 pages) par des **EXERCICES D'ÉVALUATION**, et leurs corrigés, portant sur tous les chapitres.
• **Entre les deux, la brochure traite (en 157 pages) des GRANDS THÈMES D'ÉTUDE proposés en Seconde** : *jeux de pile ou face, lancer de dés, sondages, promenades aléatoires, naissances.* À travers eux sont étudiés les distributions et fluctuations de fréquences, les temps d'attente ou de réalisation, l'impact des tailles d'échantillons, les problèmes de fourchettes et d'intervalles de confiance, …

POUR CHAQUE THÈME, TROIS PARTIES :
1. « *Travaux pratiques avec calculatrice* » (en listant toutes les instructions à suivre sur des Casio ou Texas disposant de programmes de simulation).
2. « *Travaux pratiques sur Excel* », en guidant pas à pas.
3. « *Développements sous Excel* », en utilisant des macros.

DANS CHAQUE PARTIE, DES « ACTIVITÉS ».
Par exemple, pour « *Jeux de pile ou face* » :
– partie 1 :
 – Comment détecter une pièce truquée.
 – Lancers consécutifs égaux à pile ou face.
 – Une martingale.
– partie 2 : Pile ou face : suites de coups égaux.
– partie 3 : Coups consécutifs égaux.
Autre exemple, pour « *Promenades aléatoires* » :
– partie 1 :
 – La traversée de l'hexagone.
 – Le cube et la fourmi.
– partie 2 : Promenade aléatoire sur un polygone.
– partie 3 :
 – … sur un polygone.
 – … sur un cube.
 – Planche de Galton.
La même activité, avec des variantes dues aux matériels, parfois avec des niveaux d'approfondissement différents, *peut ainsi se retrouver dans deux ou trois parties.* De là, pour un lecteur, la répétition à satiété de quelques mêmes phrases, questions, analyses ou conclusions. Mais cela rend *les trois parties parfaitement autonomes*, ce qui en facilitera l'usage !

POUR CHAQUE « ACTIVITÉ », dans chaque partie s'il y a lieu, sont précisés :
– sa *durée* (pas en partie 3 utilisable par le professeur ou, individuellement, par élève librement), ses objectifs, sa matière,
– son *déroulement*, parsemé de questions (Exemple pour « le problème du Grand Duc de Toscane » : « En lançant trois dés et en sommant, il est plus fréquent d'obtenir 10 que 9. Pourquoi ? ». Suit une simulation…).
– un *compte rendu* de ce déroulement, enrichi de réponses (commentées) aux questions et d'« ENTRE NOUS » très substantiels qui éclairent les constatations statistiques par des aperçus théoriques empruntés le plus souvent aux probabilités.
• **L'ENSEMBLE CONSTITUE UNE VRAIE SOMME**, gamme d'outils diversifiés d'utilisation immédiate, d'autant que « *le CDRom d'accompagnement*, lisible sur PC, contient, outre les développements sous Excel 97 ou 2000, les énoncés des travaux pratiques (calculatrices et tableur), lisibles sous Word 97 ou supérieur » (ce qui rend donc ces énoncés adaptables).
J'ajoute qu'il s'agirait, même sans calculatrice, ni tableur, d'un bon document-ressource ! Mais alors quel sous-emploi !

Henri BAREIL

« ESPACE CALCULATRICES. Mathématiques. Classe de Lycée », par une équipe coordonnée par Xavier Sorbe, IPR maths de Bordeaux. Éd. CRDP, 3375 Bordeaux Cedex.

112 pages en A4. Présentation très soignée et agréable.
ISBN : 2-86617-360-0. Prix : 75 F (+ 20 F de port). Co-diffusion à l'APMEP à 71 F (cf. page 136).

En 22 séquences, l'ouvrage implique les calculatrices dans la formation et la recherche en mathématiques.
Sept « domaines d'utilisation » (je cite, entre parenthèses, le nombre de séquences correspondantes) : Calculer (9), Conjecturer (4), Représenter graphiquement (5), Programmer (7), Utiliser le calcul symbolique (5), Utiliser un logiciel de géométrie (1), Fiches méthode (2).
Cinq séquences concernent les classes de Seconde, 14 les Premières, 18 les Terminales (dont, spécifiquement, 3 les ES et 8 les S).

Chaque séquence indique initialement *l'objectif, le niveau, le « support »* (par exemple : « Arithmétique – Suites – Raisonnement par récurrence » pour la séquence 0) et *le type de calculatrice* (scientifique (4 séquences), graphique (3), programmable (7), symbolique (4), un peu de chaque (8), TI 92 – pour la géométrie –).
Puis vient la *situation-problème* étudiée, analysée et décortiquée en éléments de recherche. Suivent des *« Éléments de solution »*, abondants.
L'ensemble me parait très bien fait, à partir de situations tantôt classiques (parachutiste, emprunts, intérêts, ellipse, recherche de π, crible d'Ératosthène, ...) toujours intéressantes, et tantôt plus originales (par exemple à propos des répartitions dans un jury d'examen et des péréquations), elles aussi très bien exploitées.

Les études sont fouillées, clairement menées, avec de jolies ouvertures. En voici une :
« *Une propriété inattendue !*
On considère les entiers naturels qui ne s'écrivent en numération décimale qu'avec des chiffres 1. *Quels sont ceux qui sont divisibles par leur nombre de chiffres ?*
1. Par simple calcul mental, donner trois exemples de nombres répondant à ce problème.
2. Quels sont les six plus petits d'entre eux ? (calculatrice conseillée !)
3. Vérifier que leurs nombres de chiffres sont en progression géométrique.
4. Démontrer que le nombre formé de n chiffres 1 *est égal à* $\dfrac{10^n-1}{9}$.
5. Démontrer par récurrence la propriété suivante : pour tout entier naturel k, on a
$$10^{3^k} \equiv 1 \pmod{3^{k+2}}.$$
En déduire que, pour k entier, $\dfrac{10^{3^k}-1}{3^{k+2}}$ *est un entier.*
6. Démontrer alors que, pour k entier naturel, tout entier formé de 3^k *chiffres* 1 *est divisible par* 3^k.
7. Problème ouvert : existe-t-il des solutions au problème autres que celles trouvées à la question précédente ? »
Chemin faisant, les « Éléments de solution » correspondants dévoilent, au 3), « la progression géométrique de raison 3 et de premier terme 1 » et, après de nettes explications pour les 4), 5) et 6), proposent, au 7), une jolie suite d'autres solutions, non sans avoir précisé qu'une recherche complète exigerait « la théorie des groupes cycliques ».

Voilà donc, me semble-t-il, une belle publication qui valorise l'apport des calculatrices érigées en attrayant outil de « recherche formatrice ». Comme l'écrit J.P. Richeton, **« ce travail va dans le sens d'une aide efficace au service des élèves et des enseignants. Merci pour eux ! »**

Henri BAREIL

Les Cahiers de Science et Vie d'Octobre 2000 : DOSSIER LES GRANDES INVENTIONS DE LA GÉOMÉTRIE.

Conseillère : Amy Dahan.
96 pages en 21 × 28,5, dont 57 – abondantes illustrations comprises – pour le Dossier. 40 F, port compris, à Excelsior Publications (Chantal Poirier) 75503 Paris Cedex 15.

• Huit articles du Dossier troussent, d'une plume alerte, « *des moments créateurs de*

nouvelles façons de représenter l'espace » :
– « *Les figures du cosmos* », par B. Vitrac : Des cinq polyèdres réguliers platoniciens à la vision de l'Univers des Grecs à Kepler.
– « *La quadrature des cartes* », par C. Frémontier-Murphy : de Claude Ptolémée à Mercator : Que conserver ?
– « *Le cercle mortel des géo-maîtres d'armes* », par P. Brioist : Une des préoccupations de la Renaissance !
– « *Un monde en trompe l'œil* » par J. Peiffer : Encore la Renaissance, cette fois par la perspective.
– « *Des solides pathologiques* », par G. Orvas : ceux qui ne se plient pas à « S - A + F = 2 », … et se font exclure !
– « *Une géométrie taillée dans la pierre* », par J. Sakarovitch : Des techniques de découpage et d'assemblage à la géométrie descriptive de Monge.
– « *La géométrie sans la mesure* », par B. Belhoste : géométrie projective de Poncelet, points à l'infini et principe de continuité incluant les imaginaires (cf. notre Bulletin n° 431, haut de la page 736 et Brochure n° 124 de Roger Cuppens).
– « *Un monde non euclidien* ? », par J. Gray : Lobatchevski, Riemann et la courbure de l'espace, … sans oublier ni Escher, ni Beltrami et sa pseudosphère, ni Vasarely,…

• *De quoi intéresser un vaste public, … des C.D.I. de Collège aux enseignants eux-mêmes…*

Henri BAREIL

« LES MATHÉMATIQUES. PLAISIR ET NÉCESSITÉ. Un parcours guidé dans l'Univers des mathématiques », par Albert DUCROCQ et André WARUSFEL. Éd. Vuibert.
384 pages en 16,8 × 26. Très claire présentation. Table des matières très détaillée. Index d'environ mille noms propres ou concepts.
ISBN : 2 7117 5266 6. Prix : 199 F.

• *Les auteurs ont d'abord voulu souligner « le caractère exaltant des mathématiques, science passionnante de toujours, …* » avec, désormais, la nouvelle « dimension qui prend une fascination alors que l'esprit accède aujourd'hui à maints mondes mentaux : la culture mathématique donne accès à tous ».
« 95% de l'ouvrage devrait apparaître lisible par quiconque veut découvrir cette évolution, même s'il n'est pas géomètre »…
Il s'agit, ensuite, de « rassurer » après « un haro inconsidérément jeté sur les mathématiciens » alors que, aux États-Unis par exemple, l'élite scientifique unanime proclame que « *la mathématique est la seule discipline qui devrait être substantiellement renforcée* » afin de dissiper les blocages qui menacent toutes les disciplines de pointe « faute d'outils mathématiques » – cf. en France : « *Les mathématiques méritent considération* », texte de soixante-quinze personnalités liées à l'Académie des Sciences paru dans notre Bulletin 427 –.
Les auteurs insistent aussi, en écho à un responsable physicien, sur le fait que la semence mathématique fait se lever d'inattendus « cadeaux à récolter ». « Les exemples (de très frappants sont cités) sont légion ».
Le prologue continue par quelques points forts liés aux « sept problèmes du millénaire » proposés, le 24 mai 2000, par le « Clay Mathematics Institute » (cf. Bulletin 429, page 459) – trois de ces problèmes seront présentés au Chapitre 5 –.

• **Viennent ensuite DOUZE CHAPITRES** (aux titres ici parfois abrégés) :
1. LE MATIN DES MATHÉMATICIENS : Les Grecs et leurs bases des maths.
2. LE LANGAGE DES MATHS : Des Arabes à Newton et Leibniz.
3. LE CALCUL DES LIMITES : De Fermat à Lebesgue et à la théorie des distributions.
4. MATHÉMATIQUE DU CIEL : Cosmologies, relativité et courbure de l'espace, calendriers, et … « un bref cours de cosmonautique » (orbites, vitesses d'évasion, …).
5. L'ACADÉMIE DES QUARANTE PROBLÈMES.
Référés à quarante savants, des Grecs à nos jours, il s'agit de problèmes fondamentaux : définitions de concepts, axiomes (d'Euclide à Peano et à celui du choix), dénombrements et constructions, … classés par ordre alphabé-

tique des savants impliqués, d'Apollonius à Zermelo, en passant par Burnside, Cantor, Euler, Galois, Gauss, Gödel, Hilbert, Mandelbrot, Poincaré, Riemann, Turing, … pour en citer quelques-uns…
6 et 7. QU'EST-CE QU'UN POINT ? UN NOMBRE ? … Aperçus sur diverses géométries, les divers ensembles de nombres, les quaternions…
8 et 9. MATHÉMATIQUES ET INFORMATION : « *Vaincre les distances* » et « *un ordinateur pour chacun* », avec les interactions maths-physique, maths-informatique…
10. MATHÉMATIQUES ET MATÉRIAUX : Fusées, quanta, photons et phonons, les 230 groupes de symétrie, la cristallographie,…
11. LA TERRE EN ÉQUATIONS : Polynômes de Legendre, climatologie (périodes de réchauffement ou de glaciation, …, effets industriels, …), architecture fractale,…
12. MATHÉMATIQUES ET BIOLOGIE : le vivant, « univers dans l'univers » ; ses « briques » ; ses synergies ; l'évolutionnisme ; le « nouveau hasard » ; le cerveau, … potentialités de l'esprit et thèses de Ch. Ehresmann.

LA CONCLUSION fait un historique des dernières décennies (« math. modernes », …), *puis développe la puissance des mathématiques*, « meilleur instrument de connaissance du réel qu'elles ne cessent d'interroger, au plus grand profit de toutes les sciences », qui
– *« obligent à la rigueur de l'esprit »,*
– *« conduisent au doute systématique et contraignent à la probité intellectuelle »,*
– *« glorifient la liberté individuelle »,*
– *« apprennent l'efficacité, par exemple par la généralisation systématique »,*
– *« forgent la curiosité scientifique »,*
– *« forcent à expérimenter »,*
– *« obligent à observer tout azimut et à prendre des initiatives »,*
– *« impulsent une émotion esthétique incomparable »*
(… à nous aussi de le prouver par nos façons d'enseigner).
• **Tous les textes sont riches d'exemples de tous ordres qui semblent couler de source…** *Ils sont, de plus, émaillés d'encarts sur des points d'histoire, sur quelques problèmes ou développements particuliers* : équations de Navier-Stokes, trois démonstrations du théorème de Pythagore, les nombres chanceux (ou de Ulam), le nombre d'or, les problèmes de Nicolas Chuquet, le troisième degré, l'hypocycloïde de Steiner, des paradoxes en probabilités, etc.

L'ensemble est remarquable. Cet ouvrage a sa place dans toute bibliothèque d'enseignant de mathématiques, d'Université ou de C.D.I. de lycée. Est-il cher ? Sûrement pas en un rapport qualité/prix au-dessus de tout éloge !

Je terminerai par un joli petit problème du Chapitre 6 volontairement résolu à un niveau « Collège » :
« Étant donnés deux points distincts B *et* C *d'un cercle* Γ, *on appelle* P *et* Q *les points d'intersection d'une tangente à* Γ *avec les tangentes en* B *et* C, *et* R *et* S *leurs projetés orthogonaux sur la médiatrice de* BC. *Que peut-on dire des droites* RC *et* SB *? »*
La solution est assortie d'une heureuse remarque : « La figure, tracée ici avec soin – c'est souvent essentiel – permet une bonne conjecture, mais les élèves ont beau avoir mille fois entendu le conseil élémentaire “ Regardez la figure ! ”, il faut tout le temps le leur redire… ».
… Manière de conclure, pour moi, en disant que l'ouvrage me semble aussi un modèle de pédagogie pour un superbe parcours dans un univers des mathématiques rendu pleinement intelligible et … jubilatoire !

Henri BAREIL

« **LES INFINIS ». Dossier de 116 pages – sur 152 – du numéro spécial, Décembre 2000, de « POUR LA SCIENCE »** (format 21 × 28) *abondamment illustré et nourri d'encarts éclairants.*
40 F à « Pour la Science », 75278 Paris Cedex 06.

20 articles, dont le dernier sur « l'infini littéraire ». Des auteurs souvent célèbres.

Tous les domaines sont amplement abordés : l'infini (ou, plutôt, les infinis en leur variété) en analyse, classique ou « non standard », en géométrie (les classiques et les non commutatives), pour l'univers des algorithmes, en physique (pour l'infiniment petit et l'infiniment grand).

L'histoire des maths est, à propos des infinis, revisitée : nombres d'Archimède, Chine de Liu Hui (fin du 3^e^ siècle) ou de Shen Gua (11^e^ siècle), paradoxes de l'infini aristotélicien et infini numérique actuel de Thabit ibn Qurra, Univers infini de Giordano Bruno, science du mouvement au 18^e^ siècle, Wallis et le symbole ∞, espace-temps,…

Chemin faisant, on découvre ou redécouvre les courbes continues sans dérivées, les célèbres paradoxes de l'hôtel de Hilbert, de la réflexivité, de Banach-Tarski, de Russell, de l'auto-référence, …, les infinis de Cantor, les « grands cardinaux », l'ensemble triadique de Cantor (humoristiquement raconté en termes de nettoyage !), les fractals (y compris avec un Pappus généralisé), Penrose, les probabilités en géométrie…

L'infini s'y révèle « pierre de touche du constructivisme » … et parfois outil de démonstration indispensable dans des domaines ne mettant pourtant en jeu que des quantités finies (ainsi à propos des suites de Goodstein où, fait étrange, des nombres de plus en plus gigantesques sont finalement détruits par une pauvre soustraction de 1 à chaque étape ! – à lire absolument ! –).

La mathématique s'y affirme, tout au long, « science de l'infini », qu'il soit « potentiel » (on peut toujours faire un pas de plus) *ou « actuel »* (où « l'essentiel est moins d'objectiver cet infini que de saisir ce qui lui est consubstantiel : les notions premières d'ensemble et d'application bijective entre ensembles »).

L'éventail des textes est un vaste panorama, proposé avec une écriture aussi simple que possible, parfois sur le ton du conte – et c'est réussi –, mais qui n'en est pas moins d'un niveau parfois élevé. *À coup sûr, un ouvrage de talent pour tous publics cultivés … ou qui veulent le devenir !*

Henri BAREIL

L'INFINI AU CARREFOUR DE LA PHILOSOPHIE ET DES MATHÉMATIQUES, par Jacqueline GUICHARD.
Collection « IREM – Histoire des mathématiques ». Éd. Ellipses.
208 Pages en 17,5 × 26, dont 21 (en titres) de bibliographies, 6 d'index des noms, 5 d'index des notions, 2 de « Table des schémas et tableaux », 5 de Table des matières détaillée. Excellente présentation, sans couleurs.
ISBN 2-7298-7987-0. Prix : 160 F.

Par rapport au « Pour la Science » précédent, ce n'est plus un ouvrage « tous publics », mais les Bibliographies, Index, … l'indiquent déjà, une étude de référence – qui mérite amplement son titre –.

• *Il s'agit d'abord d'enquêter sur la naissance du concept d'infini,* d'y rechercher les interactions, influences et, à l'opposé, ségrégations, entre les perspectives métaphysiques, théologiques et mathématiques.

Cela s'articule autour de « trois grands repères » qui sont autant de chapitres du livre (chacun avec une bibliographie propre – il y aura ensuite une Bibliographie générale –).

Chapitre 1 : « LES ORIGINES DE LA QUESTION » (60 pages).
Les « Grecs » nous donnent à la fois une réflexion philosophique et une pratique démonstrative de la mathématique. La première fait s'opposer, au sujet du continu, pluralité et indivisibilité. Pour la seconde, l'infini n'a pas de statut : c'est l'innombrable…

Chapitre 2 : « ÉLABORATION PHILOSOPHIQUE D'UN CONCEPT POSITIF » (98 pages).
Après les débats philosophico-théologiques du Moyen Âge, voici « *l'Âge classique* » où prévaut un concept d'infini « fondamentalement différent de celui des Grecs ». L'infini devient, avec Descartes, « l'absolument premier dans l'ordre de l'être aussi bien que dans celui du connaître ». Au lieu d'un infini « conçu à partir du fini, comme sa néga-

tion », c'est le fini qui ne « peut être conçu, connu [...] qu'à partir de l'infini »... Contradictoirement, avec Spinoza, « le concept métaphysique d'infini accède à la pleine intelligibilité pour l'entendement humain, ce que Descartes refusait par la distinction du connaissable et du compréhensible ». Vient Leibniz, « métaphysicien de la monade et inventeur du " *calcul de l'infini* " ». Du fini à l'infini, « la différence est de degré, et non pas de nature à proprement parler, comme dans la conception cartésienne ». Cependant, Locke s'insurge et refuse tout caractère positif à l'idée d'infini, même en théologie.

Chapitre 3 : « DE L'ÉLABORATION DU " CALCUL DE L'INFINI " AU CONCEPT MATHÉMATIQUE D'INFINI » (90 pages).
Du débat sur la métaphysique des infiniment petits, on aboutit à ceux de la fin du 19e siècle, surtout de G. Cantor qui distingue « *l'infini improprement dit ou infini variable et l'infini proprement dit ou infini déterminé* ». Cela débouche sur les *cardinaux d'ensembles* et une visée *d'arithmétique transfinie.*

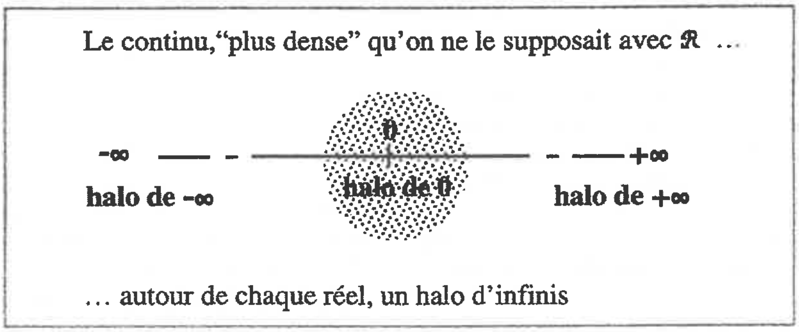
UNE « CONCLUSION » : « LA PERMANENCE DE LA QUESTION DU CONTINU » (2 pages).
Elle souligne l'apport d'un « *second Cantor* », Abraham Robinson, avec *l'Analyse non standard* **(cf. Brochure APMEP no 103 !)** où « le calcul de Leibniz trouve son fondement mathématique et, par voie de conséquence, se trouve affiné le modèle mathématique de sa vision de l'infinie continuité du monde ». En voici le schéma final :

• **Jacqueline Guichard, avec de nombreuses citations structurées par d'éclairants commentaires,** présente des études fouillées des apports les plus décisifs, sans négliger pour autant des contributions plus secondaires. Et, du début à la fin, court la trame des grandeurs et des nombres.

Très « savant », le livre l'est au meilleur sens du terme : très lisible, avec des encarts, des tableaux récapitulatifs sur les époques et les concepts... *En Annexes, une NOTE sur les catégories d'infini et un Questionnaire invitant à choisir parmi 23 affirmations de ce qu'est l'infini ... et à en proposer une 24e...*

• *Jacqueline Guichard a ainsi sculpté, avec art et science, une belle œuvre.* Les pléthoriques bibliographies pourraient faire accroire qu'elle ne concerne que des spécialistes actuels ou potentiels. Il n'en est rien. *Elle peut intéresser au plus haut point tout enseignant, surtout de philosophie ou de mathématique !*

Henri BAREIL



Pour un inventaire

TROIS OUVRAGES « d'initiation à l'usage des acteurs du sport et de l'éducation physique », par Patrick TRABAL. Collection STAPS, chez Vuibert, en 16,7 ¥ 24.

Nos ISBN respectifs : 2-71178917-9, 2-71178918-9, 2-71178919-5.

Ils conviennent, me semble-t-il, **pour toute initiation**, quel que soit le public.

1. *« PRATIQUER LE TRAITEMENT DE TEXTE ».*
112 pages. Logiciel de base : Word 97.
2. *« PRATIQUER LES STATISTIQUES ».*
128 pages. Logiciel de base : Excel 97.
3. *« PRATIQUER LE TABLEUR ».*
120 pages. Logiciel de base : Excel 97.

Pour les trois ouvrages, le logiciel « de base » fonctionne sous Windows 95 ou supérieur. Mais l'auteur avance qu'une autre version « ne devrait pas pénaliser ». De même, dit-il, pour tout autre logiciel « moderne ».

Henri BAREIL

UNE HISTOIRE DES MATHÉMATIQUES CHINOISES, par Kiyosi Yabuti. Collection « Regards sur la science ». Éditeur : BELIN. Pour la Science.

192 pages, en 13,5 × 21,5, dont 2 de chronologie, 1 d'unités de mesure, 11 – très denses – de trois Index (personnes, termes, ouvrages). Très bonne présentation.
ISBN 2-7011-2404-2. Prix : 130 F.

L'essentiel est consacré aux « mathématiques traditionnelles » avec, notamment, les « *Neuf chapitres sur l'art mathématique* » (époque des Han, mentionné au 1er siècle de notre ère), dérivé d'un autre classique (« Du gnomon des Zhou ») dont une méthode en « base-hauteur » a resurgi au 17e siècle comme « base de la géométrie occidentale » réinterprétée par la Chine…
Les Chinois étaient des précurseurs pour les problèmes d'arithmétique, de dénombrement (d'empilements, …), de calcul algébrique… C'est intéressant !

Henri BAREIL

TROIS OUVRAGES (belges) de l'éditeur DE BOECK-UNIVERSITÉ, au format 18 × 25 (ou 17 × 24). Distributeur en France : Éditions BELIN.

1. « MATHÉMATIQUES GÉNÉRALES, à l'usage des Sciences économiques, de gestion et AES », par Jacques BAIR.
426 pages. Présentation dense, mais claire.
ISBN : 2-8041-1786-3. Prix : 245 FF.
Très complet, mais avec peu de théorie, beaucoup d'applications, d'exemples, d'exercices, de problèmes (certains résolus, d'autres avec les seules « réponses finales »).
Un ouvrage de base, extrêmement riche, très utile du lycée au post-bac. Une mine de grande qualité.

2 et 3. « EXERCICES DE MATHÉMATIQUES pour le premier cycle », par Pascal DUPONT.
« Plus de 3000 exercices de mathématiques générales couvrant les premiers cycles agronomiques, chimiques, économiques, … », avec rappels de théories, exemples résolus en détail, exercices avec au moins les « réponses ». De quoi pouvoir s'entraîner et chercher avec profit !
Volume 1 : Algèbre et géométrie. 474 pages. ISBN : 2-8041-3465-2. Prix : 225 F.
Volume -2 : Analyse. 513 pages. ISBN : 2-8041-3466-2. Prix : 225 F.

Henri BAREIL.

ALGÈBRE, ANALYSE, GÉOMÉTRIE, Prépa PT/PT*/TSI, par François DEHAME et Christophe HÉNOCQ. Collection Chevallet. Éd. Vuibert (octobre 2000).
416 pages en 17 × 24,dont 2 pour le programme de seconde année PT et 4 pour un bon Index. Très bonne présentation.
ISBN : 2 7117 2085 3. Prix : 220 F.

Il s'agit, en fait, d'un recueil d'exercices (il y en a 418) sous la forme suivante :
L'ouvrage comporte 12 chapitres répartis en *39 sous-chapitres. Dans chacun de ceux-ci,* un intéressant et concis *rappel de cours* précède des « *exercices progressifs corrigés* »,

pui des « *exercices proposés* ». Chaque chapitre se termine par des « *Vrai-Faux* » et par des « *Indications pour les exercices proposés* ».
25 exercices utilisent MAPLE de façon bien intégrée.
L'ensemble constitue ainsi un tout autonome, cohérent, prograssif, riche de possibilités. Quelques sondages, ici ou là, me l'ont fait trouver excellent.

Henri BAREIL

Les exercices de MATHS en MP-MP*, par Michel GONNORD. « Un choix de 662 exercices corrigés. Index des notions et définitions ». Éd. Ellipses.
638 pages en 7,5 × 26. Présentation assez dense, mais claire. Répertoire des notations. Sommaire détaillé. ISBN : 2-7298-0350-5.

Les exercices sont classés par chapitres, sous-chapitres et indexés selon trois niveaux de difficulté et la mention « classique » ou « technique ». S'il y a lieu, les énoncés sont *surtitrés du concept étudié* (Exemples : « Entiers de Gauss », « Anneaux euclidiens », ...). Ils sont alors aisément repérables par l'Index.
Les énoncés utilisent 217 pages et les solutions 409 dont 46 pour des sujets d'oral et 82 pour des sujets d'étude.
Il y a d'assez fréquentes références au « Cours de maths en prépas », 2e année, MP et MP*, du même auteur. La possession de ce livre facilite la compréhension des corrigés – sans être pour autant une nécessité –.
Cette somme d'exercices me semble être un remarquable outil de travail.

Henri BAREIL

Espaces quadratiques, euclidiens, hermitiens, par Jean FRESNEL. Hermann, Paris, 1999.
315 p. 160 F. N° ISBN 2-7056-1445-1.

L'ouvrage traite, à l'intention des étudiants de premier cycle, mais aussi de second cycle, l'algèbre bilinéaire en 300 pages et 150 exercices. Il est structuré en trois chapitres : Espaces vectoriels quadratiques (50 pages), Espaces vectoriels euclidiens (170 pages), Espaces vectoriels hermitiens (70 pages). Il est complété par une bibliographie, un index des notations et un index des noms qui occupe six pages à lui seul.
Un outil particulièrement utile pour les candidats au CAPES et à l'Agrégation.

Paul-Louis HENNEQUIN

LES GROUPES FINIS ET LEURS REPRÉSENTATIONS, Mathématiques 2e cycle, Cours et exercices corrigés, par Gérard RAUCH. Collection dirigée par Ch.-M. Marle et Ph. Pilibossian. Éd. Ellipses.
Brochure de 142 pages en 175 × 259. Bibliographie. Index. Bonne typographie.

Il s'agit d'un ouvrage pour *licence et maîtrise*, susceptible par ses exemples d'arithmétique et de géométrie d'intéresser aussi les candidats au Capes et à l'Agrégation.
108 pages sont consacrées à un cours détaillé, clair, structuré en neuf chapitres : Vocabulaire de base ; Groupes abéliens de type fini ; Théorèmes de Sylow et groupe symétrique ; Introduction à la théorie des représentations linéaires ; Les outils ; premières applications ; Intégralité des caractères ; Représentation induite ; Applications de la théorie des représentations linéaires ; Représentations du groupe symétrique.
Puis *19 énoncés d'exercices et problèmes sur les groupes*, proposés en cinq pages sont l'objet de trois pages « d'éléments de solutions ».
Une autre Annexe fournit *13 exercices et problèmes* (en cinq pages) *sur les caractères*, avec quatre pages « d'éléments de solutions ».
La dernière Annexe concerne les *représentations induites* : cinq pages d'énoncés de *11 exercices*, avec quatre pages « d'éléments de solutions ».
Une lecture rapide donne à penser que, dans les diverses Annexes, les « éléments de solutions » sont éclairants.

Henri BAREIL

A.P.M.E.P. - INFORMATIONS

Siège Social et Secrétariat :

A.P.M.E.P. 26 rue Duméril, 75013 PARIS
Tél. : 01 43 31 34 05 - Fax : 01 42 17 08 77
Mél : apmep @ apmep.asso.fr
Internet : http://www.apmep.asso.fr
CCP PARIS 5708 - 21 N

Prix du numéro du Bulletin : 85 F.

ADHÉSIONS ET ABONNEMENTS NOUVEAUX :

Concernent, depuis juin 2000, l'année civile 2001 (en incluant le service du Bulletin dès le numéro qui suit l'adhésion ou l'abonnement).
Bulletins d'adhésion ou d'abonnement : cf. pages suivantes. Les demander au Secrétariat (adresse ci-dessus) ou aux Régionales (liste p. 140).

ADHÉSIONS EN IUFM :

130 F seulement (et cela permet d'avoir ultérieurement le tarif – réduit – « Première adhésion » (cf. page suivante).

ADHÉSIONS JUMELÉES :

Des tarifs spéciaux sont prévus pour les enseignants membres de l'APMEP et de l'une des Associations suivantes : AFEF (français), APBG (Biologie, Géologie), APISP (Physique Collège), UDP (Physique – Lycée-Collège ou collège seul). *Les demander au Secrétariat.*

CHANGEMENT D'ADRESSE (OU D'ÉTAT CIVIL) :

Joindre l'ancienne adresse et, *autant que possible, la dernière étiquette du Bulletin*, portant le numéro d'adhérent de l'APMEP.

S.B.P.M.ef
(SOCIÉTÉ BELGE DES PROFESSEURS DE MATHÉMATIQUES d'expression française)

Productions : cf. p. 138.

ADHESIONS-ABONNEMENTS
ANNEE CIVILE 2001

(cf. page précédente et page suivante)

0. ADHÉSION IUFM : 130 F (cf. page précédente).

I. PREMIÈRE ADHÉSION À L'APMEP

(ne concerne que les personnes physiques)
260 F, code A1 pour adhérer (en bénéficiant ainsi des divers services de l'APMEP dont une réduction de 30% sur ses brochures et pour recevoir :
– les six numéros annuels du « Bulletin vert »,
– les six numéros annuels du « BGV ».

II. ABONNEMENTS D'ÉTABLISSEMENTS

– au « Bulletin vert » seul, six numéros par an	**470 F**	Code B1
– au « BGV » seul, six numéros par an	**130 F**	Code B2
– aux deux ensemble	**555 F**	Code B3

III. FRAIS D'ENVOI SPÉCIAUX

Frais, y compris surtaxes aériennes, pour expédition hors CEE ; **150 F**

IV. BROCHURES À PRIX TRÈS RÉDUIT

Les brochures ci-après proposéees vous permettent, *dans la mesure des stocks disponibles*, de bénéficier de **réductions très supérieures aux 30% habituels**. Vous pouvez commander toute autre brochure (cf. p. 133) au prix habituel.

N°	Titre des brochures	Prix réduit Port compris
102	EVAPM : actes de l'université d'été 1995	35 F – 5,34 €
119	Jeux 5, 1998	40 F – 6,10 €
46	Mots VI, 1982	25 F – 3,81 €
115	LP : math séries technologiques et professionnelles, brevet 95 à 97	25 F – 3,81 €
305	Plaquettes Galion – 10 thèmes pour la seconde	60 F – 9,15 €
96	Fondements de l'évaluation en mathématiques, 1995	30 F – 4,57 €
86	Fragments d'histoire des mathématiques, Tome 4, 1992	60 F – 9,15 €
70	La trisection de l'angle, 1988	45 F – 6,86 €

V. LES RENOUVELLEMENTS D'ADHÉSION FONT L'OBJET D'UN APPEL SÉPARÉ, avec la même offre pour les brochures.

A.P.M.E.P.
PREMIÈRES ADHÉSIONS
ABONNEMENTS D'ÉTABLISSEMENTS

Partie à retourner à : APMEP, 26 rue Duméril, 75013 PARIS.

– Lisez d'abord les deux pages précédentes –

I - ADHÉSIONS-ABONNEMENTS

NOM : ....

Adresse : ....

....

Tél : ....**Mél :** ....

Lieu d'exercice (pour les nouveaux adhérents) :

....

	Code	Montant
		F
Frais d'envoi éventuels		F

II - COMMANDE DE BROCHURES

a) Liste précédente

Brochures	Montant
	F
	F
	F
	F

b) Autres brochures (cf. p. 693)

Brochures	Montant
	F
	F
	F
	F

III - MONTANT TOTAL (I + II)

F

Joindre, à l'ordre de l'APMEP,
un chèque ☐, un mandat administratif ☐

Date : **Signature**

BROCHURES

- de l'A.P.M.E.P. (avec remise de 30%, environ, aux adhérents)
- ou en co-édition ou co-diffusion : elles sont alors signalées par une ✭.
  Leurs prix, fixés en accord avec les intervenants, ne peuvent être modifiés.

➠ Les brochures de moins de deux ans sont en vert.
➠ Frais de port : voir en fin de liste (sauf indication contraire).
➠ Sauf indication contraire, les brochures sont au format A5 ou voisin.

N°	Nom des brochures	Union Européenne Prix public TTC sans port	Union Européenne Prix Adhérents TTC sans port
	I. TEXTES D'ORIENTATION		
6	**Charte de Caen** (1972)	gratuit	gratuit
32	**Texte d'orientation** (1978)	gratuit	gratuit
	(supplément au Bulletin 401) **Problématiques au lycée**	15 F	gratuit
	(supplément au Bulletin 414) **Bac Mathématiques horizon 2000**	15 F	gratuit
	II. MATHÉMATIQUES SUR PLUSIEURS NIVEAUX		
	II.1. Sur quelques grands thèmes		
202	✭ **Courbes mathématiques.** 1996. 150 courbes. 168 p.	25 F	25 F
121	**Maths en scène.** 1998. 224 pages en A4 (cf. Bulletin 419, p. 678)	72 F	50F
103	**Pour un enseignement de l'Analyse en termes d'ordre de grandeurs (« Analyse non standard »)** (cf. Bulletin 405, pages 481 à 483)	60 F	40 F
129	**Arithmétique – des résultats classiques par des moyens élémentaires –**, parMathieu Savin. 2000. 120 pages. Cf. Bulletin 431, p. 840-841	65 F	45F
	Faire de la géométrie supérieure en jouant avec Cabri-Géomètre II, 1999. Deux tomes en 17 × 24 (cf. Bulletin 423, p. 500-501). Téléchargement des figures et macros sur le serveur APMEP.		
124	176 pages	70 F	45 F
125	112 pages	55 F	35 F
	Les deux ensemble	115 F	70 F
	II.2. Problèmes et Rallyes		
	Collection : « Les Problèmes de l'A.P.M.E.P. » : cf. Bulletin 430, p. 693		
250	✭ **PanoraMath 96** (coédition APMEP, CIJM, ACL)	80 F	56 F
251	✭ **PanoraMath 2.** 288 p. 28 compétitions (cf. Bulletin 422, p. 384)	90 F	63 F
	Les deux ensemble	170 F	82 F

		Union Européenne	
N°	Prix Nom des brochures	Prix public TTC sans port	Adhérents TTC sans port
	Rallyes		
97	**Jeux IV :** De l'intérêt des problèmes de rallyes. 1995. 164 p.	107 F	75 F
	Fichiers Évariste : 480 fiches en A4 « Benjamins », « Cadets ».		
98	**Tome 1.** 1995.	72 F	50 F
132	**Tome 2.** Novembre 2000. Cf Bulletin 431, p. 842-846	85 F	60F
	Les deux ensemble	140 F	100 F
402	★ **Jeux du *Scientific American*** de Martin Gardner. Traduction Yves Roussel. 234 p. Co-diffusion ADCS	135 F	95 F
451	★ **Concours australien de Mathématiques. 256 p. en 17 × 24.** (cf. Bulletin 421, p. 157-158)	104 F	72 F
	Pour les problèmes Lycées, voir aussi § III.L.		
	II.3. Histoire des maths : cf. Bulletin 430, p. 694		
	II.4. Prospective – Didactique – Concours – ...		
76	**Analyse et synthèse.** G. Glaeser. 1990. 59 p.	72 F	50 F
96	**Fondements de l'évaluation en maths.** G. Glaeser. 1995. 78 p.	50 F	35 F
102	**L'évaluation en mathématiques :** perspectives institutionnelles, pédagogiques et statistiques. 264 p.	72 F	50 F
117	**Corrigés détaillés de cinq concours (1997) :** CA/PLP2, Capes, Agrégation interne, 272 p.	70F	49 F
127	★ **Corrigés détaillés de six concours :** CA/PLP2 internes et externes 1998 et 1999, Capes externe 1999 240 p. décembre 1999 (cf. Bulletin 426, p. 112)	70F	50F
134	**Corrigés détaillés Concours 2000** : CAPES externe, CAPLP2 interne et externe, 104 pages (cf. Bulletin 431, p. 846-847)	50 F	35 F
	127 et 134, les deux brochures ensemble	80 F	65 F
350	★ **Dessiner l'espace** (avec Cabri-Géomètre) dès le collège + disquette. Co-diffusion Tangente. 126 p.	140 F	140 F
351	★ **Derive-Classe** + disquette (au Collège). 140 p. en A4. Co-diffusion Tangente	110 F	110 F
362	★ Tableur Excel. Co-diffusion Tangente	80 F	65 F
502	★ CD Rom Excel Classe Version individuelle	110 F	110 F
	Version établissement	450 F	450 F
550	★ **Géométrie expérimentale au Collège,** M. Rousselet. Co-diffusion CRDP de Versailles (cf. Bulletin 432, p.)	88 F	83 F
500	★ **Actes de la CIEAEM 50** (cf. Bulletin 425, pages 820-821) Exceptionnellement, port 25F.	140F	100F
501	★ **Femmes et maths :** « Maths – Sections L – Filles » (cf. Bulletin 426, p. 123)	80F	65F

II.5. Vocabulaire et concepts

Collection «Mots» : cf. Bulletin 430, p. 694

II.6. Collection « JEUX mathématiques »

N°	Nom des brochures	Prix public	Adhérents
401	✯ **Jeux de Nim.** J. Bouteloup. 300 pages. 108 exercices (corrigés). Co-diffusion ADCS	175 F	120 F
402	✯ **Jeux du *Scientific American*** de Martin Gardner. Trad. Y. Roussel. 234 p. Co-diffusion ADCS	135 F	95 F

Collection "JEUX" de l'A.P.M.E.P. : cf. Bulletin 430, p. 695

III. ACCOMPAGNEMENT DES PROGRAMMES

III.E : ÉCOLE

Collection «Elem-Math» (brochures issues des IREM) cf. Bulletin 430, p. 695

N°	Nom des brochures	Prix public	Adhérents
603	✯ **Jeu de calcul « Mathador ». Coffret 37 × 15 × 6.** Jeu mathématique pour les **CM et Sixièmes, Cinquièmes** Parcours de 63 cases (avec +, –, ×, :), 8 dés (4, 6, 8, 10, 12 et 20 faces), 250 cartes-problèmes, sablier, Cf. Bulletin 425, p. 712 et **429, p. 421 à 424.**	199 F + port 50 F	199 F + port 50 F

III.C : COLLÈGE

✯ **Galion-thèmes** : cf. Bulletin 430, p. 696 pour Séries 1 et 4

N°	Nom des brochures	Prix public	Adhérents
119	**Des activités mathématiques au Collège : Jeux 5.** 1998. 132 pages-fiches en A4, photocopiables. Cf. Bulletin 419, p. 698-699	72F	50F
701	✯ **Mathématiques au Collège** (disquette contenant 800 documents et un logiciel de gestion qui fonctionne sur PC avec WinWord 2 (une réalisation APMEP-CNDP) Version monoposte (une seule installation) + port 21 F	400 F	280 F
350	✯ **Dessiner l'espace** (avec Cabri-Géomètre) + disquette Dès le Collège. M. Rousselet. Co-diffusion Tangente	140 F	140 F
351	✯ **Derive-Classe** (+ disquette). M. Rousselet. Co-diffusion Tangente	110 F	110 F
352	✯ **Tableur et mathématiques.** M. Rousselet Co-diffusion CRDP de Versailles (cf. Bulletin 425, p. 819)	80F	65F
550	✯ **Géométrie expérimentale au Collège,** M. Rousselet. Co-diffusion CRDP de Versailles (cf. Bulletin 432, p. 120)	88 F	83 F
502	✯ **Excel-Classe.** M. Rousselet et Ph. Béthune		
	CD Rom usage individuel	110F	110F
	CD Rom version établissement (avec droits de photocopie et d'autoédition des fiches élèves)	450F	450F

Cf. aussi,
ci-dessus le III.E, ainsi que § II.1, les n° **75**, 202, § II.2, les n° 97, **98**, 250, 251, **451** ; § II.4, les n° 76, 96, **102**, § II.5, particulièrement le n° **46**, le § **II.6**, et ci-dessous, les § **III.L, III.LP et IV**

N°	Nom des brochures	Union Européenne Prix public TTC sans port	Adhérents
	III.L : LYCÉE		
	Tous niveaux		
	✯ **Galion-thèmes.** cf. Bulletin 430 p. 696		
3450	**MathÉvasion.** 72 p. A4 (cf. Bulletin 419, p. 791-792, Bulletin 420, IVe de couverture, Bulletin 422, p. 362-364)	.50 F	35 F
99	**Enseigner la Géométrie dans l'Espace au Collège et au Lycée.** G. Destainville, IREM de Toulouse (brochure centrée sur la 2de, et 1ère surtout). 1996	. . .114 F	80 F
103	**Pour un enseignement de l'Analyse en termes d'ordres de grandeur.** Lutz, Makhlouf, Meyer. 208 p.	.60 F	40 F
120	**ClasMath Lycée. Classeur informatisé de documents mathématiques.** Cf. Bulletin 419, p. 700. 12 disquettes et non 17 comme annoncé par erreur. Version 10 installations, port compris Version 26 installations, port compris CD Rom de mise à jour	 . . .300F . . .600F 70 F	 200F 400F 50 F
551	**Espace calculatrice.** Codiffusion CRDP d'Aquitaine. Cf. Bulletin 432 p. 122	.75 F	71 F
	Cf. aussi la plupart des brochures du catalogue, notamment au § I, les **suppléments**, au § II.I, le n° 202, **tout le § II.2** (dont deux titres récents), au § II.6, le n° **97**, au § III.C, les n° **350, 351 et 352 (Tableur)**, et ci-dessous le n° **79** (méthodes générales).		
	Classes de Seconde		
27	**Pour une mathématique vivante en Seconde.** 1985. 160 p.	.57 F	40 F
79	**Classe de Seconde : un outil pour des changements.** 1990 150 p. (denses !) en A4 à l'Italienne	.93 F	65 F
305	**Galion-thèmes** (dix thèmes pour la Seconde, programme 2000 !) Le nombre d'or autour du nombre d'or le nombre π autour de π, radical de 2 vers les fonctions graphiques démontrer avec des aires figures de la terre, avec des polyèdres	.75F	65F
100	✯ **Le trésor de Tonton Lulu** (J. Lubczanski,. .). Volume 1. 28 problèmes originaux et attrayants avec corrigés et pistes de recherche. 1992. 96 p. en A4	.90 F	90 F
130	**Statistiques en Seconde,** par Pascale Pombourcq (octobre 2000) 80 p. Cf. Bulletin 431 p. 842-843	.60 F	40 F
	• **Et aussi**, spécifiquement, § IV, la brochure n° **88**, et § III.C les brochures n° **350, 351**		
	Classes de Première		
101	✯ **Le trésor de Tonton Lulu** (J. Lubczanski,. .). Volume 2. 24 problèmes originaux et attrayants avec corrigés et pistes de recherche. 1994. 56 p. en A4	.95 F	95 F
	• **Et aussi,** spécifiquement, **§ IV**, les brochures n° **90**, **107** et **108**.		

	Classes de Terminale		
129	**Arithmétique, par M. Savin, cf § II.1.**	65F	45F

Voir particulièrement, en plus des brochures signalées ci-dessus dans «Tous niveaux» : en II.1, les n° **202** et **121**, en II.3, les n° **70, 83, 86** en II.4, les n^{os} 117, 127 et 134, et en I, **le supplément au Bulletin 414**.

III.LP : LYCÉES PROFESSIONNELS : Brochures en A4

126	**Maths en BEP et CAP tertiaires et assimilés, 100 p. aisément reproductibles. Épreuves de 1999**	64F	45F
131	**Sujets 2000 Maths et Sciences**. 187 p. en A4. Cf. Bulletin 431, p.846	80 F	55 F
	PRIX PROMOTIONNELS :		
	Lot n° 1. TERTIAIRES :	70 F	50 F
91	**Métiers du Tertiaire.** 1993. 140 p.		
116	**Maths BEP tertiaires et assimilés.** 1996-1997. 97 p.		
	Lot n° 2. INDUSTRIELS :	80 F	55 F
109	**BEP Industriels.** 1996. 156 p.		
122	**Maths BEP industriels.** 1998. 150 p.		
	Lot n° 3. EVAPM LP	80 F	55 F
95	**Terminale BEP. Première partie** (1995) : Dossier professeur		
106	**Terminale BEP. Deuxième partie** (1998) : Analyses		
	Cf. Bulletin 419, p. 782		
	TECHNOLOGIQUES ET PROFESSIONNELS :		
115	**Brevets** 1995-1997. 55 p.		
	Prix promotionnel à l'occasion des adhésions ou réadhésions	43 F	25 F

• Et aussi, en plus des brochures de la rubrique «Lycées» ci-dessus, plus spécifiquement les brochures **Terminale BEP n° 95 et 106 du IV**.

IV. «E.V.A.P.M.»

Évaluation, sur de grands effectifs, de l'impact de l'enseignement des programmes de mathématiques. Volumes en A4.

81	**Actualisation 4e et 3e**. 1993. 196 p. en A4	129 F	90 F
88	**Seconde**. 1991. 196 p. en A4	135 F	95 F
	Premières, cf. Bulletin 413, p. 802-803 :		
90	Documents pour l'évaluation. 1997. 134 p.	65 F	45 F
107	Résultats. 1997. 96 p.	45 F	30 F
108	Analyses et actualisation. 1997. 174 p	65 F	45 F
	Les trois fascicules ensemble	140 F	95 F
112	**Sixième 1997**, Fascicule 1. Dossier professeur	50 F	35 F
118	**Sixième 1997**. Fascicule 2. Analyses		
	Cf. Bulletin 419, page 697	85F	60F
	Pour tout achat de ce fascicule, le fascicule 1 pour	30 F	20 F

N°	Nom des brochures	Union Européenne Prix public TTC sans port	Adhérents
123	**Terminales lycées** (1999) Tome 1. Dossier professeurs (cf. Bulletin 423, p. 499)	90F	75F
	V. CULTURE GÉNÉRALE		
51	**Ciel, passé, présent**, G. Walusinski. 1981. 222 p.	64 F	45 F
53	**Musique et Mathématiques**, B. Parzysz, suivi de **«Gammes naturelles»**, par Y. Hellegouarch. 1984 - 164 p.	72 F	50 F
403	✮ **Le système métrique hier et aujourd'hui.** 132 p. + illustrations couleurs (co-diffusion ADCS)	135 F	95 F

Tarifs hors Union européenne : Pour les **DOM** (97), TVA 1,05%. Calculer les prix TTC en multipliant par **0,958** les prix de la colonne correspondante. Pour **l'étranger** et les **TOM** (98), TVA 0%, le prix TTC s'obtient en multipliant le prix affiché par **0,94**.

PORT : • France métropolitaine, CEE, pays assimilés :
1 brochure : 15 F, 2 ou 3 brochures : 25 F, 4 brochures et plus : 40 F
• Autres pays : frais réels sur facture.

SBPMef

(Société Belge des Professeurs de Mathématiques d'expression française)

• Revue « Mathématiques et Pédagogie » (cf. pages 519 à 521 du Bulletin 423) : 180 FF

• Revue « Math-Jeunes » ou « Math-Jeunes junior »: 65 FF

• Explorations didactiques. Dossier 6 (Statistique) : 59 FF (port compris)

• Olympiades mathématiques belges (prix port compris)
– Tome 4 (1994 à 1998). Trois séries : Mini, Midi, Maxi.
230 pages en A5 : 50 FF
– Tome 4 + Tome 3 (1988 à 1993 : Mini et Maxi) : 80 FF

Réglement, à l'ordre « APMEP », envoyé à l'APMEP, 26 rue Duméril, 75013 PARIS.

COMITÉ NATIONAL DE L'A.P.M.E.P.

Organisme élu par les adhérents et qui a la responsabilité de l'action de l'A.P.M.E.P., il est renouvelé par quart chaque année à l'occasion d'un vote par correspondance, le quart sortant n'étant pas immédiatement rééligible.
Le Comité se réunit trois fois par an. Il élit le Bureau National à qui il délègue ses pouvoirs de façon permanente. La composition du Bureau et la liste des Commissions sont rappelées sur la deuxième page de couverture du Bulletin.

Sortants en 2001 : Maryvonne AUBRÉE-DUMONT (*Collège*, Combourg) ; Marie-José BALIVIERA (*L.P.*, Raon-l'Etape) ; Rémi BELLOEIL (*Lycée*, Rennes) ; Roger CARDOT (*Lycée*, Villers-lès-Nancy) ; Farida CHAÏBAÏ (*Collège*, Jarville) ; Marc DAMON (*L.P.*, St Etienne) ; Martine JOLY (*L.P.*, Marseille) ; Michel KERVERN (*Lycée Technique*, Brest) ; Jean-Luc LE CHEVALIER (*Lycée*, Douai) ; Philippe LOMBARD (*IREM de Lorraine*) ; Arnaud PASCAL (*Collège*, Draguignan) ; Serge PETIT (*IUFM*, Colmar) ; Pierre STEPHAN (*Lycée*, Lille) ; Jacques VERDIER (*Lycée*, Tomblaine).

Sortants en 2002 : *Régionale de Bourgogne* : Gérard BONNEVAL (*Lycée*), suppléant : Frédéric METIN (*Lycée*) ; *Régionale Champagne-Ardenne* : Arnaud GAZAGNES (*T.A.*), suppléant : Bernard SCHMITT (*Collège*) ; *Régionale de Clermont-Ferrand* : Monique MAZE (*Collège*), suppléante : Geneviève LE QUANG (*Collège*) ; *Régionale de Grenoble* : Marie-Josèphe SCHMITT (*Lycée*), suppléant : Yves BERTHOLET (*Lycée*) ; *Régionale Ile-de-France* : Christine CHAMBRIS (*Cité des Sciences*), suppléant : Philippe TCHIBOUKDJIAN (*Lycée*) ; *Régionale de Haute-Normandie* : Danielle BERGUE (*Collège*), suppléant : Laurent BREITBACH (*L.P.*) ; *Régionale de Lille* : Anne-Marie MARMIER (*Université*), suppléant : Michel RODRIGUEZ (*Lycée*) ; *Régionale de Lorraine* : Daniel VAGOST (*IUT*), suppléante : Odile BACKSCHEIDER (*L.P.*) ; *Régionale de Lyon* : Maryvonne LE BERRE (*Collège*), suppléante : G. MISON (*Lycée*) ; *Régionale de Montpellier* : Marc ROUX (*Lycée*), suppléant : Pierre POMAREDE (*Lycée*) ; *Régionale de Nice* : Alain TAVERNIER (*Lycée*), suppléante Clarisse FIOL (*L.T.*) ; *Régionale de Orléans-Tours* : Jean-Pierre GERBAL (*Lycée*), suppléante : Josiane GUIBERT (*Collège*) ; *Régionale de Poitiers* : Jackie CITRON (*Collège*), suppléante : Françoise DELORS (*Lycée*) ; *Régionale de Strasbourg* : Jean-Pierre DAROU (*Lycée*), suppléant : Richard CABASSUT (*Lycée*).

Sortants en 2003 : Colette ASTIER (*Lycée*, St Orens (31)) ; Jean-Paul BARDOULAT (*Lycée*, Foix) ; Jean BICHARA (*Collège*, Raizet-Abymes (97)) ; Alex BISSAINTE ((97)) ; Michel MÉRIGOT (*Université*, Nice) ; Brigitte MOREL (*IUFM*, Le Tampon, La Réunion) ; Bernard PARZYSZ (*IUFM*, Metz) ; Pascale POMBOURCQ (*Collège*, Toulouse) ; Jean-Claude SACHET (*L.P.*, Olivet (45)) ; Marie-Odile SACHET (*École Primaire*, Jouy le Potier (45)) ; Claude TERRAS (*Lycée*, Pau) ; Luc TIENNOT (*IUFM*, Bastia) ; Denis VERGES (*Lycée*, Seyresse (40)).

Sortants en 2004 : *Régionale d'Aix-Marseille* : Marie MEGARD (*Lycée*, Salon de Provence), suppléant : Joël DENISOT (*Collège*, Marseille). *Régionale d'Aquitaine* : Chantal DAURIAC, suppléante : Annick BAILLOU. *Régionale de Basse-Normandie* : Éric TROTOUX (*Lycée*, Caen), suppléant : Gilles PATRY (*Lycée*, L'Aigle) *Régionale de Bretagne Occidentale* : Jean-Claude EMEILLAT (*Lycée*, Brest), suppléant : Daniel QUEMENER (*Lycée*, Pont l'Abbé). *Régionale de Franche-Comté* : Jean-Pierre GRANGÉ (*Lycée*), suppléant : François COUTURIER (*Téléenseignement*, Besançon). *Régionale d'Ile-de-France* : Catherine BRUNET (*Collège*, Noisy le Sec), suppléante : Valérie LAROSE (*Collège*, Les Ulis). *Régionale de Limoges* : Madeleine MICHARD (*Collège*, Aubusson), suppléant : Claude MORIN (*Lycée*, Limoges). *Régionale de Rennes* : Lise HEILBRONNER, suppléante : Annie UTARD (*Lycée agricole*). *Régionale de Toulouse* : Roseline CASES (*Lycée*, Toulouse), suppléante : Nicole ABADIE (*Collège*, Auch).

Sièges vacants : *Régionales de Nantes* et *Picardie*.

LES RÉGIONALES DE L'A.P.M.E.P.

L'APMEP est structurée en Régionales qui correspondent, à quelques exceptions près, aux académies et qui sont donc proches des adhérents.

Chacune a ses activités propres : groupes de réflexion, journées, publication, etc. Mais ces Régionales participent également au travail des instances de l'APMEP par le biais des commissions ou groupes de travail nationaux, etc. Elles disposent d'élus au Comité National. Chaque année, une des Régionales organise les Journées Nationales de l'APMEP.

Pour de plus amples informations, contacter le Président de votre Régionale, dont les coordonnées sont inscrites ci-dessous.

Entre crochets [.], nous donnons les numéros des départements du ressort de chaque Régionale. Entre doubles parenthèses ((.)), le numéro du Compte Chèque Postal quand il y a lieu ; son intitulé est «Régionale APMEP de...».

AIX-MARSEILLE [04, 05, 13, 84] ((Marseille 2894-82 U))
Catherine DUFOSSÉ, Alcade, Bât.A, Parc du Roy d'Espagne, Allée Granados,
13009 MARSEILLE – Tél. 04 91 25 08 85 – Mél : cdufosse@club-internet.fr

AQUITAINE (Bordeaux) [24, 33, 40, 47, 64] ((Bordeaux 3902-91 Y))
Jean-Pierre GUIBBAUD – Hameau de Noailles, Villa 3, 33400 TALENCE
Tél. 05 56 80 45 91 – Mél : jean-pierre.guibbaud@fnac.net

BASSE NORMANDIE (Caen) [14, 50, 61] ((Rouen 1084-56 R))
Muriel ALLIOT – 403 Boulevard du Grand Parc, 14200 HEROUVILLE-SAINT-CLAIR
Tél. 02 31 47 44 75 – Mél : muriel.alliot@etab.ac-caen.fr

BOURGOGNE [21, 58, 71, 89] ((Dijon 1751-05V))
Richard BECZOWSZKI – 43 bis avenue Boucicaut, 71100 CHALON SUR SAONE -
Tél. 03 85 48 77 91

BRETAGNE OCCIDENTALE (Brest) [29, 22-ouest]
Henri JONCOUR – LA TORCHE, 29120 PLOMEUR – Tél. 02 98 58 76 09

CHAMPAGNE-ARDENNE (Reims) [08, 10, 51, 52] ((Châlons sur Marne 1262-80 L))
Françoise HUGOT – 42 rue aux Luats, 10130 CHAMOY
Tél. 03 25 42 17 02 – Mél : françoise.hugot3@freesbee.fr

CLERMONT-FERRAND [03, 15, 43, 63] ((Clermont 1569-75 G))
Daniel THIRIET – 13 rue du Cratère, 63122 CEYRAT
Tél. 04 73 35 90 07 – Mél : daniel.thiriet@libertysurf.fr

FRANCHE-COMTÉ [25, 39, 70, 90] ((Dijon 2505-45V))
Michel MAGNENET – 1 rue Léon Jouhaux, 25000 BESANÇON
Tél. 03 81 80 61 67 – Mél : michelmagnenet@lemel.fr

GRENOBLE [07, 26, 38, 73, 74] ((Grenoble 343 49U))
Marie-Claire REMILLIEUX – 23 av. Marcelin Berthelot, 38100 GRENOBLE
Tél. 04 76 47 03 71 – Mél : m-claire.remillieux@wanadoo.fr
Pour toute commande : Michèle BENOIS – Tour Math, BP 53 X
38041 GRENOBLE CEDEX – Tél. 04 76 23 33 97

GUADELOUPE
Jean BICHARA – BP 588, 97617 POINTE A PITRE CEDEX
Tél. 0 5 90 62 11 88 – Fax 0 590 91 93 54 – Mél : jean.bichara@wanadoo.fr

HAUTE-NORMANDIE (Rouen) [27, 76] ((Rouen 1350-13 G))
Eliane ANDRIEU – 10 rue du Beau Site 76960 NOTRE DAME DE BONDEVILLE
Tél. 02 35 75 99 52 – Mél : aandrieu@worldnet.fr

ILE-DE-FRANCE [75, 77, 78, 91, 92, 93, 94, 95] ((Paris 25 108 63 E))
Valérie LAROSE – 32 Boulevard Nélaton, 91460 MARCOUSSIS
Tél. 01 64 49 39 29 – Mél : vlarose@club-internet.fr

LA RÉUNION ((Saint-Denis 533 09 M))
Éric BUTZ – 30 Lotissement Rosiers, Les Camélias, 97400 SAINT DENIS
Tél. 02 62 30 40 37 – Mél : BUTZ.Eric@wanadoo.fr
LILLE [59,62] ((Lille 4242-55 S))
Pierre STEPHAN – 34 avenue des Lilas, 59800 LILLE
Tél. 03 20 06 09 40 (+ Fax) – Mél : stephanpierre@worldonline.fr
LIMOGES [19, 23, 87] ((Limoges 117-66 R))
Noëlle VIGIER – 29 D rue du Puy Las Rodas, 87000 LIMOGES
Tél. 05 55 01 84 47 – Mél : irem@unilim.fr
LORRAINE [54, 55, 57, 88] ((Nancy 1394-64 U))
Pierre-Alain MULLER – 10 rue des Roses, 57200 SARREGUEMINES
Tél. 03 87 28 75 51 – Mél : pierre-alain.muller@fnac.net
LYON [01, 42, 69] ((Lyon 702-06 J))
Josette FEURLY-REYNAUD – Rue C. Bizollon, 69002 LYON
Tél. 04 78 42 52 25 – Mél : feurly.josette@libertysurf.fr
MONTPELLIER [11, 30, 34, 48, 66] ((Montpellier 385-25 W))
Pierre ANDRIEU – 140 rue Paul Eluard, 34490 LIGNAN SUR ORB
Tél. 04 67 49 28 25 – Mél : Pierreandrieu@wanadoo.fr
NANTES [44, 49, 53, 72, 85] ((Nantes 3118-23 X))
Nicole DERSOIR – 17 rue du Maréchal Juin 44420 LA TURBALLE
Tél. 02 40 23 42 95 – Mél : n.dersoir@wanadoo.fr
NICE [06,20, 83] ((Marseille 5758-43F))
Michèle PÉCAL – 260 chemin des Cerisiers, 06740 CHATEAUNEUF DE GRASSE
Tél : 04 93 42 53 43 – Mél : michele.pecal@fnac.net
ORLÉANS-TOURS [18, 28, 36, 37, 41, 45]
Jean Claude. SACHET – 103 rue Gustave Flaubert, 45100 ORLEANS
Tél. 02 38 63 71 07 – Fax : 02 38 76 43 76 – Mél : jcsachet@noos.fr
PICARDIE (Amiens) [02, 60, 80] ((Lille 862 04 V))
Claude SERRIS – 3 rue de la Rochefoucault 60180 NOGENT SUR OISE
Tél. 03 44 71 80 12 – Mél : cserris@hotmail.com
POITOU-CHARENTE (Poitiers) [16, 17, 79, 86] ((Bordeaux 3852-59 D))
Jackie CITRON, 6 rue de Flandre, 86530 CENON SUR VIENNE,
Tél. 05 49 21 09 74 – Mél : jcitron.apmep@wanadoo.fr
RENNES [22-est, 35, 56] ((Rennes 170-729 X))
Philippe BARDY – La Croix Dom Guilaume, 56380 BEIGNON
Tél. 02 97 75 72 39 – Mél : p.bardy@infonie.fr
STRASBOURG [67, 68] ((Strasbourg 1538-47 K))
Jean-Pierre DAROU – Lehrwaldstrasse 5, D77694 KEHL KORK, Allemagne
Tél. 00 49 7851 3371 – Mél : jpdarou@T-online.de
TOULOUSE [09, 12, 31, 32, 46, 65, 81, 82] ((Toulouse 2035 51 T))
Valérie DUCASSÉ – 140 Chemin des Cartanes 31840 AUSSONNE
Tél. 05 61 85 69 93 – Mél : valerie.ducasse@free.fr

SECTIONS DE L'APMEP À L'ÉTRANGER

Pour les collègues ou lecteurs résidant à l'étranger dans les pays cités :

Allemagne Annie BARTEZ – Camille St-Saens, Allée 22/3, D-13405 BERLIN
Liban P.CROTTEREAU – GREM, Centre culturel de l'Ambassade de France au Liban, 128 bis rue de l'Université, 75351 Paris SP07

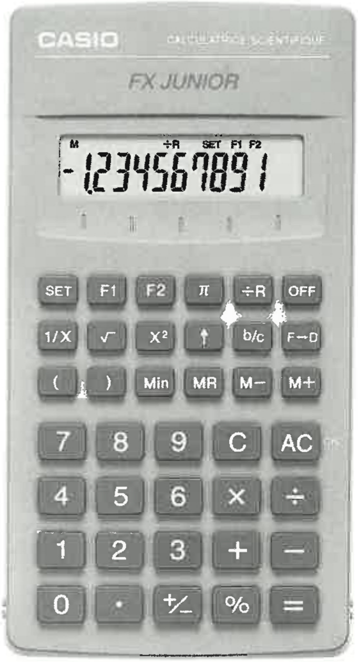
RESPONSABLES DES COMMISSIONS ET CHARGÉS DE MISSION

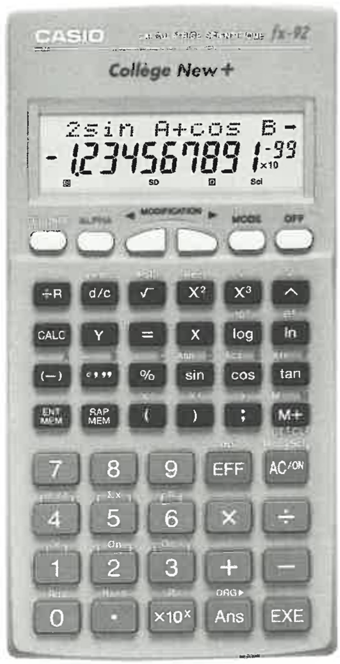
André ANDRIEUX, 1 rue G. Apollinaire, 60200 COMPIEGNE – Tél. 03 44 20 04 03
Marie-José BALIVIERA, rue du Haut Regard, 88110 ALLARMONT
Tél. 03 29 41 16 07 (+ Fax) – Mél : m-j.baliviera@ac-nancy-metz.fr
Jean-Paul BARDOULAT, chemin de Malet, 09000 FOIX
Tél. 05 61 65 34 15 (+ Fax) – Mél : jean-paul.bardoulat@wanadoo.fr
Philippe BARDY, La grande Croix, Dom Guillaume, 56380 BEIGNON
Tél 02 97 75 72 39 (+ Fax) – Mél : p.bardy@infonie.fr
Henri BAREIL, 7 rue des Pivoines, 31400 TOULOUSE – Tél. 05 61 52 74 53
Fax : 05 61 25 52 05 – Mél : christianezehren@libertysurf.fr (pour H. Bareil)
Rémi BELLOEIL, 1 rue de la Warta, 35200 RENNES
Tél. 02 99 50 88 35 – Mél : belloeilre@aol.com
Antoine BODIN, Scey-en-Varais, 25290 ORNANS
Tél. 03 81 62 11 24 (+ Fax) – Mél : a.bodin@math.univ-fcomte.fr
Laurent BREITBACH, 5 square des Platanes, 76240 BONSECOURS
Tél. 02 35 80 58 32 (+ Fax) – Mél : laurent-breitbach@club-internet.fr
Michel CARRAL, 21 rue Rémuzat, 31000 TOULOUSE
Tél. 05 61 21 48 56 – Mél : carral@cict.fr
François COLMEZ, 55 bis avenue du bois de Verrières, 92160 ANTHONY
Tél 01 46 66 01 27 – Mél : fcolmez@gauss.math.jussieu.fr
Rémy COSTE, 12 rue du Pré de la Barrière, 91470 FORGES LES BAINS
Tél. 01 64 91 26 20
Roger CUPPENS, Le Président, Bloc A, Appt 19, 1 rue des Lauriers, 31650 SAINT ORENS DE GAMEVILLE – Tél. 05 61 39 03 94 – Mél :
Catherine DUFOSSÉ, Alcade, Bât.A, Parc du Roy d'Espagne, Allée Granados, 13009 MARSEILLE – Tél. 04 91 25 08 85 – Mél : cdufosse@club-internet.fr
François DUSSON, 72 quai Cavelier de la Salle, 76000 ROUEN
Tél. 02 35 03 20 82 –
Louis DUVERT, La Rémireille, 380, route des Grottes, 06780 SAINT CEZAIRE SUR SIAGNE – Tél. 04 93 60 24 99
Pierre ETTINGER, 5 allée du Clair Matin, 31520 RAMONVILLE SAINT AGNE
Tél. 05 61 55 68 83 – Mél : ettinger @cict.fr
Jacqueline EURIAT, 44 rue Bésonfosse, St Laurent, 88000 EPINAL
Tél. 03 29 35 71 77 – Mél : j.euriat@ac-nancy-metz.fr
Michèle FABREGAS, 1 rue de la Corrèze, 57070 METZ
Tél. 03 87 36 25 30 – Mél : m.fabregas@ac-nancy-metz.fr
Jean FROMENTIN, 17 rue de la Roussille, 79000 NIORT
Tél. 05 49 73 43 48 – Mél : jean.fromentin@libertysurf.fr
Régis GOIFFON, 4 rue Pasteur, 69007 LYON
Tél. 04 78 58 07 84 (+ Fax) – Mél: goiffon@cismsun.univ-lyon1.fr
Régis GRAS, 14 avenue de la Chaise, Cicé-Blossac, 35170 BRUZ – Tél. 02.99.52.73.98
Fax : 02 99 52 73 98 – Mél : gras@univ-rennes1.fr
Gilbert GRIBONVAL, 85 avenue du Général Leclerc, 91120 PALAISEAU
Tél. 01 60 10 15 25 – Mél : Gilbert.Gribonval@fnac.net
André GUILLEMOT, La Croix d'Alliance, Saint Gilles, 35590 L'HERMITAGE
Tél. 02 99 64 64 82 – Mél : a-guillemot@infonie.fr

Michel GUILLEMOT, 10 impasse de la Pélude, 31400 TOULOUSE
Tél. 05 61 53 17 23 – Mél : guillemo@cict.fr
Suzy HAEGEL, 4 rue de Wangenbourg Cosswiller, 67310 WASSELONNE
Tél. 03 88 87 17 02
Lise HEILBRONNER, 12 avenue de la Haye Renaud, 35830 BETTON
Tél. 02 99 55 09 23 – Mél : lise.heilbronner@wanadoo.fr
Anfré LAUR, 12 rue Alphonse Daudet, 38100 GRENOBLE
Tél. 04 76 23 33 97 –
Maryvonne LE BERRE, 24 rue des Remparts d'Ainay, 69002 LYON
Tél. 04 72 40 08 12 – Mél : leberre.maryvonne@free.fr
Françoise MAGNA, 14 bis rue F.Lemaître, 75020 PARIS
Tél. 01 47 97 27 52 (+ Fax) – Mél : fmagna@libertysurf.fr
Anne-Marie MARMIER, 132 avenue de la République, 59110 LA MADELEINE
TÉL. 03 20 31 67 61 – Mél : anne-marie.marmier@univ-lille1.fr
Monique MAZE 6 rue de Wailly, 63000 CLERMONT
Tél. 04 73 93 04 37 – Mél : mmaze@ac-clermont.fr
Bernard PARZYSZ, IUFM d'Orléans-Tours, 72 Faubourg de Bourgogne, 45044 ORLEANS CEDEX 1 – Tél : 01 46 83 03 62 – Mél : parzysz.bernard@wanadoo.fr
Michèle PÉCAL, 260 chemin des Cerisiers, 06740 CHATEAUNEUF DE GRASSE
Tél 04 93 42 53 43 (+ Fax) – Mél : michele.pecal@wanadoo.fr
Pascale POMBOURCQ, Le Bourg, 81630 MONTVALEN
Tél. 05 63 33 58 87 – Mél :ppombour@ac-toulouse.fr
Pierre REY, chemin de Bertrand, 04300 DAUPHIN
Tél. 04 92 79 51 09 (+ Fax) – Mél : prey.apmep@wanadoo.fr
Jeanne ROLLAND, 26 rue de Posmoguer, 29600 MORLAIX
Tél. 02 98 88 77 45 – Mél : jeanne.rolland@educagri.fr
Marc ROUX, 6 rue Louis Laget, 30900 NIMES
Tél. 04 66 21 49 35 – Mél :
Jean-Pierre RICHETON, 16 rue de Plobsheim, 67100 STRASBOURG
Tél. 03 88 84 87 38 (+ Fax) – Mél :
Marie-Odile SACHET, 103 rue G. Flaubert, 45100 ORLEANS – Tél. 02 38 63 71 07
Fax : 02 38 76 43 76 – Mél : mosachet@cybercable.fr
Jean-Claude SACHET même adresse que Marie-Odile sauf le mél : jcsachet@noos.fr
Nicole TOUSSAINT, 20 rue Renaudot, 10160 AIX EN OTHE – Tél. 03 25 46 71 57
Fax : 03 25 46 72 93 – Mél :
Daniel VAGOST, 6 rue du Pont, 57310 BOUSSE
Tél. 03 87 73 09 31 – Mél : vagost@iut.univ-metz.fr
Jacques VERDIER, 46 rue de la Grande Haie, 54510 TOMBLAINE
Tél. 03 83 20 94 72 – Mél : jacquesverdier@free.fr
Gilbert WALUSINSKI, 26 parc Bérangère, 92210 SAINT CLOUD – Tél. 01.47.71.69.09
Christiane ZEHREN, Les Sylphides A2, place Fontaine du Temple, 06100 NICE
Tél. 04 93 84 32 36 (+ Fax) – Mél : christianezehren@libertysurf.fr

CASIO®

CM 1/CM 2 - COLLÈGE





FX Junior

- Spéciale pour CM 1 / CM 2
- Priorité de X et ÷
- Parenthèses
- Division Euclidienne
- 2 opérateurs constants

FX 92 Collège New +

- Ecran à 2 lignes
- Véritable écriture directe de gauche à droite
- Fonction Replay
- 9 mémoires
- Statistiques à 1 variable
- Fonction CALC

Modifications techniques et changement de couleurs sans préavis. Nous consulter pour la disponibilité des produits.

INFORMATION CONSOMMATEUR :
08 36 68 33 44*
CLUB CASIO : 36.15 CLUB CASIO*
INTERNET : www.casio.fr
*2,23 F/mn

invent
*HP 40G IDÉALE POUR LES NOUVEAUX PROGRAMMES DU LYCÉE !
HP 40G
Idéale
pour les nouveaux
programmes
du lycée
www.hp.com/go/calculatrices
Mode de saisie algébrique
Aide en ligne
Mode de calcul "pas à pas"
Calcul formel
Programmes à caractère didactique
Statistiques inférentielles
alligator design
* Prix conseillé