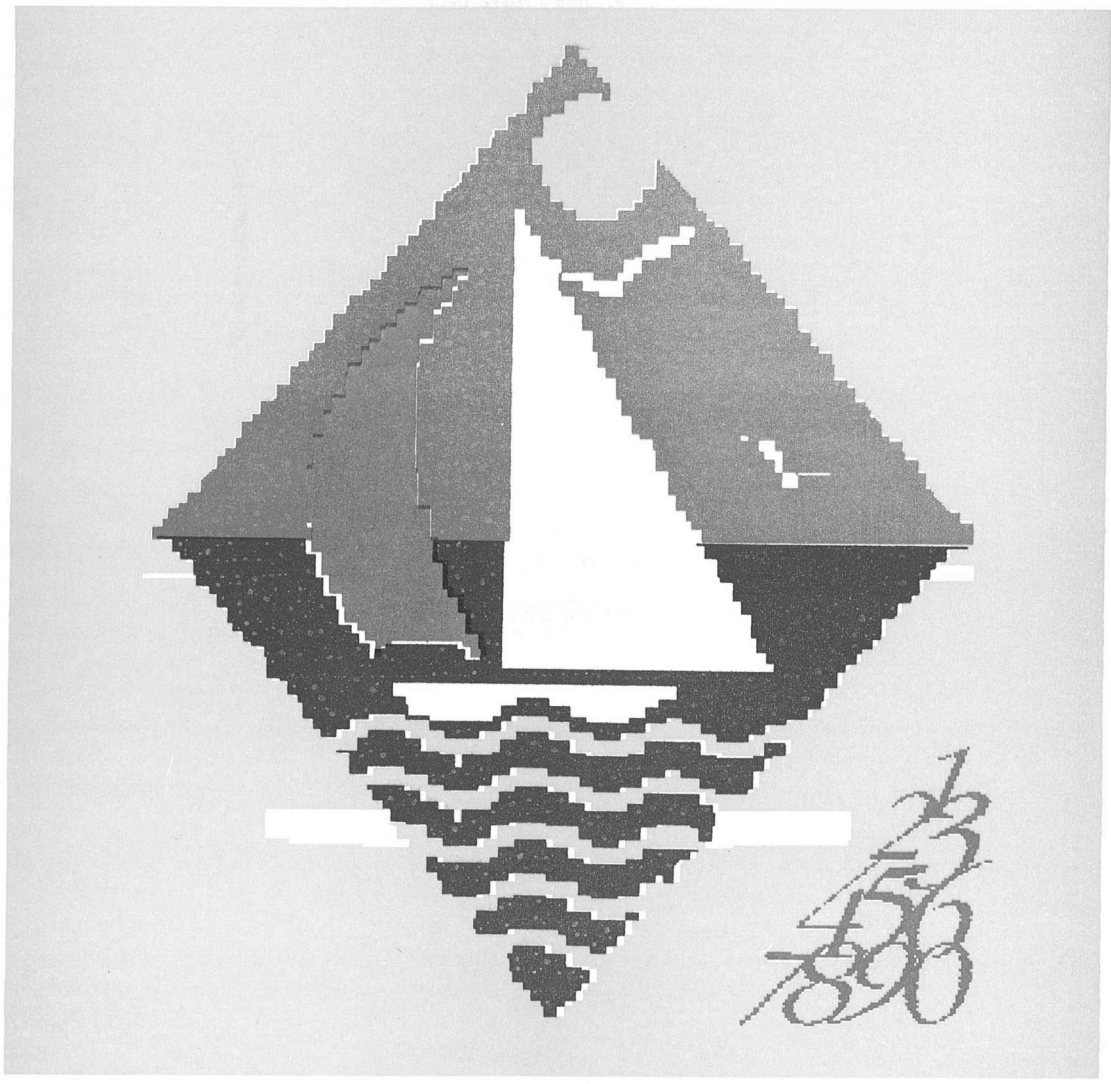
INSTITUT DE RECHERCHE SUR L'ENSEIGNEMENT DES MATHÉMATIQUES

Université Montpellier II

Journées IREM-Montpellier
Port Leucate. 23 et 24 mai 1997

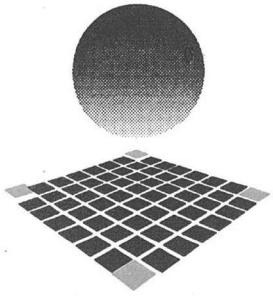
Nombres et calculs



Groupe analyse IREM de Montpellier

- Octobre 1997 -

INSTITUT DE RECHERCHE SUR L'ENSEIGNEMENT DES MATHÉMATIQUES



Université Montpellier II

Place Eugène Bataillon
cc 040
34095 MONTPELLIER Cedex 05
Tél. : 04.67.14.33.83 - 04.67.14.33.84
Fax : 04.67.14.39.09
e.mail : irem@math.univ-montp2.fr

Journées IREM-Montpellier
Port Leucate. 23 et 24 mai 1997

Nombres et calculs

Groupe analyse IREM de Montpellier
- Octobre 1997 -

Avant propos

Il est, depuis 1993, une tradition qui s'ancre à l'IREM de Montpellier et dont nous ne pouvons que nous réjouir, celle d'organiser régulièrement deux journées de réflexion et d'échanges pour les animateurs IREM autour d'un thème particulier (1993, 1994, 1995). Tour à tour, chaque groupe se mobilise pour prévoir et organiser ces journées, ainsi après le groupe didactique et géométrie c'est au groupe analyse qu'a incombé cette tâche en 1997.

Le thème que nous avons proposé, "nombres et calculs", est certainement bien trop vaste pour que tous les aspects aient pu être abordés au cours de ces deux jours, mais la diversité des propositions d'ateliers et d'exposés, nous a bien confirmé combien celui-ci peut être fédérateur dans nos différentes démarches de recherche.

Pour les membres de notre groupe, un des soucis en proposant ce thème était de susciter une réflexion autour des nouvelles technologies (calculatrices, formelles en particulier) qui modifient le rapport des élèves aux nombres et aux calculs. Si cet aspect est aussi apparu dans des exposés et des ateliers faisant référence à ces nouvelles technologies, d'autres exposés et ateliers nous ont aussi permis d'aborder des aspects tout aussi importants concernant les conceptions des élèves sur les nombres ou encore des démarches d'introduction historique de certaines techniques de calcul.

Les Actes de ces rencontres concrétisent les informations qui ont été échangés lors de ces deux jours et nous remercions tous les animateurs d'avoir bien voulu nous en donner un compte rendu[1].

Enfin, comme cela a pu être dit lors de ces deux jours, il serait utile que les prochaines journées soient aussi ouvertes à des enseignants de l'académie qui sans être formateurs manifestent, un intérêt certain pour nos travaux.

---

[1] Il manque seulement un compte rendu de l'exposé de Mme Anne Michel-Pajus, mais celui-ci a fait l'objet d'une publication dans le numéro n°13 de la revue Mnémosyne édité par l'IREM de Paris VII.

Sommaire

Liste des participants.....p. 2

Organisation des journées.....p. 3

Introduction
D. Guin.....p. 4

Exposés et ateliers
- " Des calculs aux nombres ".
A. Bernard..... p. 7

- "Différentes sortes de nombres et logiciels de calcul formel".
M. Janvier.....p. 19

- "Les règles de calcul algébrique pour les élèves, mythe ou réalité".
Groupe Didactique..... p. 54

- "Narrations de recherche et dénombrement".
F. Bonafé - M.C. Combes - L. Dray - J.P. Robert - M. Sauter -... p. 61

- "Quelques considérations sur les nombres en seconde".
J. Delgoulet..... p. 72

- "De l'importance de l'environnement pour la recherche en mathématiques"
L. Trouche..... p. 82

- "De la figure à la représentation graphique avec cabri - géomètre"
R. Brunet - J. Naudeillo.....p. 87

- "Les parcours diversifiés à propos des Nombres et du Calcul"
A. Bronner..... p. 99

Table ronde
- "Arithmétique à l'école, au collège et au lycée : perspectives, problèmes"
Participants : T. Murgier, A. Bronner, Y. Nouazé, Y. Girmens,
C. Faure, M. Noguès.
Compte rendu : C. Faure..... p. 109

Participants

Amsalem	André	Université Montpellier II.
Bascou	Noël	Lycée J. Mermoz, Montpellier.
Bellard	Nicole	Lycée J. Monnet, Montpellier
Bernard	Alain	Lycée Dhuoda, Nîmes.
Bernard	René	Lycée G. Philippe, Bagnols Sur Cèze.
Bonafé	Freddy	Lycée Mas deTesse, Montpellier.
Boutté	Daniel	IPR, Montpellier.
Braesch	Claude	Invité.
Bronner	Alain	I.U.F.M. Montpellier.
Brunet	Robert	Lycée J. Mermoz, Montpellier.
Casenove	Bernard	Collège P. Moréto, Thuir.
Chevalier	Arlette	Retraitée. Animateur IREM de Montpellier.
Chiocca	Marie Catherine	Invité.
Combes	Marie Claire	Collège F. Villon, St Gély du Fesc.
Caulat	Nathalie	Invité.
Cuer	Dominique	Lycée J. Mermoz, Montpellier.
Delgoulet	Jacques	Lycée R. Gosse, Clermont l'Hérault.
Deville	Alain	Lycée Mas deTesse, Montpellier.
Dray	Liliane	Collège la Providence, Montpellier.
Faure	Christian	Lycée Joffre, Montpellier.
Fuchs	Michèle	Lycée Mas deTesse, Montpellier.
Girmens	Yves	I.U.F.M. Perpignan.
Guilhaumou	Danièle	Collège J. Benes, Pézenas.
Guin	Dominique	Université Montpellier II. Directrice de l'IREM.
Janvier	Michel	Université Montpellier II.
Kieffer	Françoise	Lycée J. Mermoz, Montpellier.
Larguier	Mirène	Collège Ambrussum, Lunel.
Lewillon	Martine	Lycée Pompidou, Montpellier.
Michel -Pajus	Anne	Invité, IREM de Paris VII.
Murgier	Thierry	IPR, Montpellier.
Naudeillo	Jacques	Collège Joffre, Montpellier.
Noguès	Maryse	Lycée L. Feuillade, Lunel.
Nouazé	Yvon	Université Montpellier II.
Nouguès	Marie France	Université Montpellier II.
Pellequer	Sylvie	Collège Pic St Loup, St Clément de Rivière.
Robert	Jean Pierre	Lycée Mas deTesse, Montpellier.
Sala	Michel	Lycée J. Monnet, Montpellier.
Sauter	Mireille	Collège P. Lamour, La Grande Motte.
Seco	Michel	Lycée A. Loubatières, Agde.
Tisseron	Christiane	Lycée Mas deTesse, Montpellier.
Trouche	Luc	Lycée Joffre, Montpellier.

Organisation des journées

Vendredi 23 Mai

8h30-10h	Accueil formateurs		
10h-10h30	Séance d'ouverture		Dominique Guin
10h30-11h30	Exposés	*Du calcul aux nombres*	Alain Bernard. Groupe histoire
11h30-12h30		*Différentes sortes de nombres et logiciels de calcul formel*	Michel Janvier. Groupe informatique
12h30-13h30	Repas		
14h-16h	Ateliers	*1. Les règles de calcul algébrique pour les élèves, mythe ou réalité ?*	Groupe didactique
		2. Narrations de recherche et dénombrement	Groupe géométrie
		3. La perception des nombres en seconde	Groupe intégration des outils informatique
		4. Combinatoire et arithmétique à l'aide de tableurs	Groupe informatique
16h30-17h30	Table ronde	*Arithmétique au collège et au lycée, perspectives, problèmes ?*	Participation de diverses personnes : IPR, formateurs...
17h30-19h	Temps libre		
19h30-20h30	Repas		

Samedi 24 Mai

8h	Déjeuner		
9h-11h	Ateliers	*1. Calcul, calculatrices (TI 92), conjectures*	Groupe analyse
		2. Cabri : bas les masques	Groupe géométrie
		3. La perception des nombres en seconde	Groupe intégration des outils informatique
		4. Nombres aléatoires, simulation de distribution de probabilité, en Mathematica	Groupe informatique
11h30-12h30	Exposé	*De la combinatoire au calcul différentiel en suivant Leibniz*	Anne Michel-Pajus. Groupe M:ATH (approche par les textes historiques), Paris VII
12h30-13h30	Repas		
14h-15h	Exposé	*1. Nombres réels et racine carrée*	Alain Bronner. Groupe didactique
15h30-16h30	Bilan		

INTRODUCTION

Dominique Guin
Directrice de l'IREM

Afin d'introduire ce colloque intitulé "Nombres et calcul", voici quelques éléments historiques marquant les difficultés qui ont accompagné la conceptualisation du nombre. Alors qu'il est difficile de définir ce qu'est un nombre, ce qui explique que ce concept ait mis des siècles à se former, le calcul s'est développé beaucoup plus rapidement : la résolution de certaines équations diophantiennes précède de quinze siècles la démonstration de la transcendance du nombre e (Hermite, 1872) !

Le calcul, qui était à l'origine synonyme d'utilisation d'opérations sur les nombres, désigne aujourd'hui toute manipulation de règles opératoires ou non (par opposition aux démonstrations qui s'obtiennent à l'aide de raisonnements purement logiques et abstraits). Cependant, au cours des siècles, on observe une interaction constante entre les progrès du calcul numérique et l'approfondissement des concepts mathématiques : ces deux aspects des mathématiques interviennent de manière dialectique dans toute démarche expérimentale ; à toutes les époques, le calcul numérique a permis de formuler des conjectures mathématiques (répartition des nombres premiers, théorème des quatre couleurs...).

MARQUES HISTORIQUES

I Grèce

Le nombre est une collection d'unités, une quantité divisible un nombre fini de fois. A l'époque de Platon (IV^{ème} av. J.-C.), seuls les entiers naturels non nuls sont reconnus comme nombres. A cette idée du nombre s'oppose l'idée de grandeur mise en évidence par les rapports irrationnels (diagonale du carré), de quantité "continue" divisible infiniment .

Il y a une séparation nette entre ces deux domaines des mathématiques : la géométrie dont l'objet est l'étude des grandeurs et l'arithmétique dont l'objet est l'étude des nombres. Pour Euclide, les radicaux ne sont pas des nombres ; seules les grandeurs commensurables appartiennent à cette catégorie. Cette impossibilité de concevoir sous forme abstraite la notion de nombre réel va persister durant des siècles.

II Stevin (XVI^{ème})

On assiste de 1500 à 1650 au développement du calcul numérique au travers de problèmes concrets liés au commerce, à la navigation, l'astronomie... Simultanément, Stevin recherche l'abstraction à partir des opérations, la possibilité d'effectuer des opérations sans se référer aux quantités, il désire situer le nombre à un niveau supérieur. Il contribue dans son "Traité des incommensurables grandeurs" à l'émergence du concept analytique de nombre en essayant d'unifier rationnels et radicaux, en proposant un seul traitement pour les deux types de quantité continues et discrètes.

L'introduction dans l'occident de la notation décimale permet grâce aux développements décimaux d'exprimer les fractions et les nombres définis par des radicaux : c'est ainsi qu'émerge l'idée de nombre, indépendamment des quantités, sans l'opposition discret/continu. L'influence de ces travaux sur Weierstrass et Newton est grande (calcul différentiel, analogie

Points de repère dans l'évolution du concept du nombre

DANTZIG T. (1974), Le nombre, le langage de la science,
trad. fr., Paris, A. Blanchard (1ère édition : 1930).

L'OEUVRE	L'AUTEUR	LE PAYS	L'ÉPOQUE
Découverte des valeurs irrationnelles	Pythagore	Grèce	VI^{è} siècle av. J.C.
Première crise du concept de l'infini	Zénon, Platon Aristote	Grèce	IVè siècle av. J.C.
L'invention du symbole zéro	Inconnu	Inde	Premiers siècles après J.C.
Les nombres *négatifs*	Inconnu	Inde	Premiers siècles après J.C.
On formule pour la première fois les nombres complexes	Cardano	Italie	XVI^{è} siècle
Invention de la *notation littérale*	Viète	France	Fin du XVI^{è} s.
Invention de la géométrie analytique	Descartes	France	1639
L'invention du calcul infinitésimal	Leibniz	Allemagne	Vers 1677
Découverte des nombres *algébriques*, ne pouvant s'exprimer par des radicaux	Abel	Norvège	1825
Découverte des nombres transcendants	Liouville	France	1844
Première théorie scientifique des valeurs irrationnelles	Dedekind	Allemagne	1872
L'invention du transfini	Cantor	Allemagne	1883

avec la théorie des développements décimaux : développement en série entière). C'est à la fin du dix-septième siècle que paraît le premier traité de calcul infinitésimal (L'Hopital, 1696).

III Cantor, Dedekind, Weierstrass (XIX^{ème})

C'est seulement au dix-neuvième siècle que l'on assiste à la construction du nombre réel. Le concept analytique de nombre voit le jour et l'infini acquiert enfin le statut de nombre. On peut réellement parler d'obstacle épistémologique[2], au sens où la structuration antérieure du système a fait obstacle à la conceptualisation. Georges Glaeser dans son "Etude historique sur la genèse du concept de nombre relatif" (1981) a réalisé une étude épistémologique où il met en évidence les 3 points suivants :

1) inaptitude à manipuler des quantités négatives isolées ;
2) difficulté de donner un sens à des quantités négatives isolées ;
3) difficulté à unifier la droite numérique.

DU POINT DE VUE DE L'ENSEIGNEMENT

Un obstacle épistémologique ne donne pas lieu nécessairement à un obstacle didactique. Cependant, il nous faut rechercher les conditions d'un équilibre entre la présentation historique et la présentation directe de ce que l'on sait aujourd'hui. La transposition didactique[3] qui reflète l'écart entre le concept, tel qu'il est reconnu par la communauté des mathématiciens, et le concept tel qu'il est enseigné intervient également dans ce processus.

D'un point de vue didactique, ce sont les problèmes posés par l'enseignement des décimaux et des nombres rationnels à l'école élémentaire qui ont été le plus largement étudiés par Guy Brousseau[4], que ce soit en ce qui concerne les effets épistémologiques de la réforme des programmes de 1970 sur les conceptions des élèves et maîtres ou la réorganisation des apprentissages.

C'est avec un exposé portant sur une recherche intégrant simultanément ces deux aspects épistémologiques et didactique que nous terminerons ce colloque : Alain Bronner nous présentera essentiellement l'aspect épistémologique de son travail de thèse portant sur les radicaux. Mais pour commencer, Alain Bernard nous propose de suivre les traces des calculs jusqu'aux nombres.

---

[2] Effet limitatif d'un système de concepts pour le développement de la pensée (Bachelard, "La formation de l'esprit scientifique", 1938).
[3] Transposition du savoir savant au savoir enseigné (Chevallard 1985, La pensée sauvage)
[4] Thèse de l'Université de Bordeaux ou Revue en Didactique des Mathématiques, vol 2.3, La pensée sauvage.

Alain Bernard
Groupe histoire

> *J'ai fait tous les calculs. Ils confirment l'opinion de tous les spécialistes, notre idée est irréalisable. Il ne reste plus qu'à la réaliser.*
> Latécoère, constructeur d'avions à Toulouse, créateur de l'aéropostale, vers 1920.

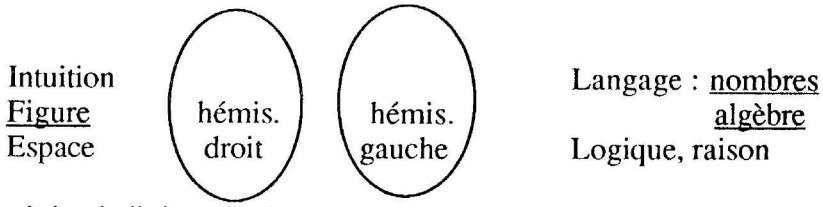
Il est évident que nous construisons d'abord des nombres avec lesquels nous effectuons ensuite des calculs. Et si c'était le contraire....Et si les calculs avaient précédé les nombres ? Et si nos ancêtres avaient longtemps calculé avant de dégager le concept de nombre ? Latécoère et avec lui tous les ingénieurs ont-ils besoin du concept de nombre ?

Cette approche des nombres reprend pour partie la troisième journée du stage « une approche pédagogique déduite de l'histoire ».

QUELQUES REPERES

I : La mathématique de base créée par notre cerveau est la géométrie algébrique.

> *L'algèbre est une géométrie écrite,*
> *la géométrie est une algèbre figurée*
> Sophie Germain.



La géométrie algébrique "naît" en 1637 quand Descartes et Fermat relient les droites et les coniques (figures) à leurs équations (nombres) dans un repère (les 2 côtés du cerveau). En recherche, au 20ème siècle, la géométrie algébrique fédère les nombreuses et diverses branches des mathématiques.

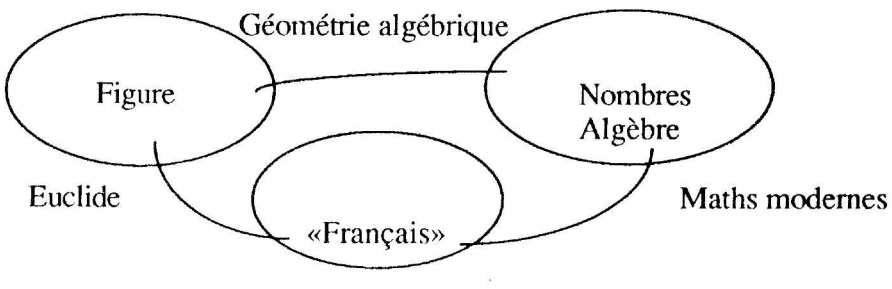
L'énoncé purement arithmétique de Fermat : $x^n + y^n = z^n$ est impossible en nombres entiers pour $n \geq 3$, a été démontré en 1993 par A. Wiles en géométrie algébrique.

II : Le système de mesure.

Avant de devenir la science déductive, les mathématiques sont un système de mesure.

1) Construire des figures simples
2) Mesurer les éléments de ces figures avec des nombres.
3) Déduire des propriétés avec la logique.

III : Les 3 langages :



Pour suivre l'épistémologie des nombres, un article de Christian Houzel dans « La Recherche » de Novembre 95 sert de fil conducteur.

AVATAR DU NOMBRE

Voici d'après Ed. Lucas, quelques-unes des transformations curieuses et subtiles du nombre : au début, on fit des marques sur les arbres et des stries sur les os des animaux ; le nombre prit plus tard la forme digitale (Alcuin) ; il devint ensuite successivement mystique (Pythagore), nuptial (Platon), magique (Persans), abracadabrant (Zoroastre), premier ou composé, entier ou fractionnaire, commensurable ou incommensurable, exact ou approché (Euclide), triangulaire, carré, pentagonal, polygonal, pyramidal (Diophante), cubo-cubique (Indiens), ortho-triangulaire, congruent (Arabes), sourd, aveugle (Moyen-âge), plaisant et délectable (Bachet), récréatif (Ozanam), indivisible (Cavaliéri), différentiel, incrémentiel (Leibniz), fluent (Newton), exponentiel, logarithmique, rhabdologique (Neper), parfait, amiable, abondant, déficient, aliquotaire, (Fermat, Frénicle....), congru ou incongru (Gauss), complexe, idéal, normé (Kümmer), réel ou imaginaire, équivalent, anastrophique (Cauchy), équipollent (Bellevitis), quaternion (Hamilton), enfin hypertrenscendantal (Hermite).

Rebière, 1926
Mathématiques et mathématiciens.

1. De Sumer à Milet : -3000, -600.

« La Recherche » en novembre 1995. Christian Houzel :

Qu'est-ce qu'un nombre ?
« Il ne faut pas se leurrer, en dernier ressort on ne sait pas très bien. »

La Recherche : Peut-on repérer dans l'histoire le moment où émerge la notion abstraite de nombre ?

C. Houzel : Oui, on a cette chance-là. Dans l'antique Mésopotamie, les Sumériens avaient des notations différentes suivant qu'il s'agissait d'objets qu'on peut compter un à un, comme des têtes de bétail, ou bien de mesures de volume pour le liquide ou encore pour le grain, et ainsi de suite. Et puis, vers la fin du III^{ème} millénaire, les scribes sumériens ont inventé un système savant destiné à s'appliquer à tout ce qui se compte. C'est là qu'on voit se former ce concept de nombre abstrait dans la notation écrite. Ils unifient toutes les notations existantes sur la base soixante.

La Recherche : Pourquoi soixante ?

C. Houzel : Parce que cela vient de l'un des systèmes métrologiques antérieurs dans lequel les multiplicateurs, pour passer d'une unité au groupement de l'échelon supérieur, étaient alternativement six et dix. Ils ont donc regroupé. Les Babyloniens hériteront ensuite de cette notation en base soixante, dont nous avons nous-mêmes hérité dans notre décompte des heures, des minutes et des secondes.

2. Le nombre géométrique chez Euclide.

Les Grecs utilisaient les lettres de l'alphabet pour écrire les nombres entiers. Ils ont réussi le tour de force de ne pas créer de système d'écriture des nombres mais de créer l'arithmétique, théorie des nombres. Leur approche géométrique des nombres dont il nous reste les dénominations de carrés ou de cubes d'un nombre, leur a permis d'obtenir des résultats théoriques exceptionnels sur les nombres entiers et de créer de nouveaux nombres tels les irrationnels. Nous retrouvons le transfert usuel en mathématiques entre intuition spatiale et raisonnement théorique, la situation figure-nombre calquée sur la configuration de notre cerveau.

La Recherche : *Donc, il faut attendre la Grèce antique pour voir apparaître les rationnels et aussi les irrationnels...*

C. Houzel : ***Pas vraiment non plus, car pour les mathématiciens grecs les seuls nombres identifiés comme tels étaient les entiers.***

Ils ont inventé, non pas un nouveau type de nombre, mais une théorie des proportions en grandeurs géométriques, complètement indépendante des nombres.

C'est ce qu'on trouve au livre V des Eléments d'Euclide : une théorie qui permet de manipuler des proportions entre des grandeurs géométriques. Mais ces grandeurs ne sont pas conçues comme des nombres. On ne peut pas dire que $\sqrt{2}$ existe dans la mathématique grecque. Ce qui exite, ce sont des grandeurs géométriques, des rapports entre grandeurs géométriques, qui ne sont pas forcément rationnels.

La Recherche : *π non plus n'est pas un nombre ?*

C. Houzel : *Non. Au livre XII des Eléments d'Euclide, il y a une proposition qui dit que l'aire d'un cercle est proportionnelle au carré du rayon du cercle. On peut donc concevoir, dans le cadre de la géométrie grecque, le rapport entre l'aire du cercle et le carré du rayon. C'est ce que nous appellerions π. Mais ce type de rapport n'est pas conçu comme un objet mathématique. Il s'agit de relations entre grandeurs. Bien qu'Archimède en calcule une approximation, il n'y a pas de nombre π dans la mathématique grecque.*

Nous retiendrons les définitions d'Euclide au début du Livre VII, quand naquit l'homogénéité.

1. L'unité est ce selon quoi chacune des choses existantes est dite une.

2. Un nombre est un assemblage d'unités.

.....

16. Un nombre est dit multiplier un nombre, lorsque le multiplié est ajouté autant de fois qu'il y a d'unités dans celui qui le multiplie, et qu'un nombre est produit.

17. Lorsque deux nombres se multipliant font un nombre, celui qui est produit se nomme plan, et les nombres qui se multiplient, se nomment les côtés du produit.

18. Lorsque trois nombres se multipliant entre eux font un nombre, celui qui est produit est appelé solide ; et les nombres qui se multiplient, se nomment les côtés du produit.

.....

22. Les nombres plans et solides semblables sont ceux qui ont leurs côtés proportionnels.

3. Brahmagupta (500, Inde) : le système de position, nombres négatifs et zéro.

De leur côté, les Hindous ne développèrent pas (ou très peu ?) de géométrie et accordèrent une plus grande importance aux nombres. **Notre système d'écriture des nombres apparaît vers le cinquième siècle en Inde. Les nombres négatifs et le zéro vinrent aussi de la Chine ou de l'Inde,** pays où les règles de calcul sur des nombres inconnus étaient connues dès le 7ème siècle.

Nos chiffres ont pour origine des noms sanscrits :

eka	*dvi*	*tri*	*catur*	*panca*	*sat*	*sapta*	*esta*	*nava*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*

Michèle Roux
L'homme et son nombre Irem de Besançon.

Par contre, le mot - chiffre - a la même étymologie que « zéro », à savoir « zifr », le zéphyr, le vent.

Dès le cinquième siècle de notre ère, les Indiens disposent d'une écriture symbolique sophistiquée pour travailler sur les nombres et savent écrire et résoudre des problèmes du second degré.

- Les constantes sont notées avec les 2 premières lettres de l'unité monétaire, la roupie, soit : ru
- Les nombres négatifs sont surmontés d'un petit rond : 9°
- L'inconnue est aussi notée avec les 2 premières lettres du mot désignant la chose que l'on cherche : ya.
- Le carré de l'inconnue est selon le même principe : yava.
- Les égalités de nombres inconnues sont notées sur 2 lignes.
- L'égalité : $2x^2 - 6x = -7$ s'écrira ainsi yava2 ya 6¡
  7°

Les Arabes au 9ème siècle ont récupéré les nombres indiens. Ils ont donné aux équations leurs règles de travail. La règle de restitution (algèbre) permet de ne conserver que des nombres « positifs » et la règle de simplification (muqqabala) la complète. Mais pas de nouveaux nombres dans un premier temps.

Vers le 13ème ou 14ème siècle, les Arabes, et Al-Kashi en particulier, ont créé les nombres décimaux et leurs règles opératoires.

4. Stevin : la Disme

Entrée en Europe des nombres décimaux fraîchement créés par Al-Kashi.

La première édition date de 1585. Jusqu'à cette date, les astronomes utilisent traditionnellement les calculs en base 60 et chaque corporation a son écriture des nombres. Les fractions sont écrites en juxtaposant le nombre entier écrit en base 10 et la partie fractionnaire appelée nombre rompu ou plus simplement rompu. Les rompus de base 10 ne sont pas plus utilisés que les autres. La « Disme » connut un grand succès et la méthode proposée par Stevin se généralisa en quelques dizaines d'années.

ATTENTION : une fois de plus, il ne s'agit pas de proposer une théorie. La « Disme » donne une méthode pour « facilement expédier par nombres entiers sans rompus, tous comptes se rencontrans aux affaires des hommes » et uniquement sur les quatre opérations de l'arithmétique et uniquement sur un exemple pour chaque opération.

ARGVMENT

La Disme a deux parties, Définitions, & Opération. En la première partie se déclarera par la première Définition, quelle chose soit Disme ; Par la Seconde, troisième & quatrième, que signifie Commencement, Prime, Seconde, &c. & nombres de Disme.

En l'opération se déclarera par quatre propositions, l'Addition, Soubstraction, Multiplication, & Division des nombres de Disme, Dequoy l'ordre se peut représenter succintement par telle table :

- Le Disme a deux parties
  - Definitions, comme quelle chose soit
    - Disme
    - Commencement
    - Prime, Seconde, &.
    - Nombre de Disme.
  - Opération de :
    - l'Addition
    - Soubstraction
    - Multiplication.
    - Division.

A la fin du précédent sera encore appliqué une Appendice, declarant l'usage de la Disme par quelques exemples és choses.

LA PREMIERE PARTIE DE LA DISME DES définitions.

DEFINITION I.

Disme est une espece d'arithmetique, inventée par la disiesme progression, consistente es characteres des ciffres, par lesquels se descrips quelque nombre, és par laquelle l'on depesche par nombres entiers sans rompus, tous comptes se rencontrans aux affaires des hommes.

PROPOSITION I, DE L'ADDITION.

Estant donnez nombres de Disme à ajouter : Trouver leur somme :

Explication du donné. Il y a trois ordres de nombres de Disme, desquels le premier 27 ⓪ 8 ① 4 ② 7 ③, le deuxieme 37 ⓪ 6 ① 7 ② 5 ③,

Explication du requis. Il nous faut trouver leur somme.

Construction.

On mettra les nombres donnez en ordre comme ci joignant, les aioustant selon la vulgaire maniere d'aiouster nombres entiers, en ceste sorte :

	⓪	①	②	③
	2	7	8	4
	3	7	6	7
	8	7	5	7
	9	4	1	3

	7
	5
	2
	4

onne somme (par le I probleme de l'Arithmetique) 941304, qui sont (ce que demonstrent les signes dessus les nombres) 941 ⓪ 3 ① 0 ② 4 ③ Je di, que les mesmes sont la somme requise. demonstration.

Les 27 ⓪ 8 ① 4 ② 7 ③ donnez, sont (par la 3e definition) $27\frac{8}{10}$, $\frac{4}{100}$, $\frac{7}{1000}$, ensemble $27\frac{847}{1000}$, & par mesme raison les 37 ⓪ 6 ① 7 ② 5 ③ valent $37\frac{675}{1000}$, & les 875 ⓪ 7 ① 8 ② 2 ③ seront $875\frac{782}{1000}$, lesquels trois nombres, comme $27\frac{847}{1000}$, $37\frac{675}{1000}$, $875\frac{782}{1000}$ sont ensemble (par le 10e probleme de l'Arith.) $941\frac{304}{1000}$ mais autant vaut aussi la somme 941 ⓪ 3 ① 0 ② 4 ③ c'est donc la vraye Somme, ce qu'il falloit demontrer. Conclusion. Estant doncques donnez nombres de Disme à ajouster, nous avons trouvé leur Somme, ce qu'il falloit faire.

NOTA

Si aux nombres donnez defalloit quelque signe de leur naturel ordre, on emplira son lieu par le diffaillant. Soyent par exemple les nombres donnez 8 ⓪ 5 ① 6 ② & 5 ⓪ 7 ② auquel dernier defaut le signe de l'ordre ①.

L'on mettra en son lieu 0 ①, prennant alors comme pour nombre donné 5 ⓪ 0 ① 7 ② les ajoustant comme cy devant en ceste sorte :

	⓪	①	②
	8	5	6
	5	0	7
	1	3	6

3

5. Cardan (1545) et Bombelli (1572) : les nombres imaginaires.

La vie la plus belle, la mieux remplie, la moins sujette aux déceptions, est encore celle du fou sublime qui cherche à déterminer l'inconnue d'une équation à racines imaginaires.

Honoré de Balzac.

Combien il peut y avoir de racines en chasq Equation

Scachés donc qu'en chaque Equation, autant que la quantité inconnue a de dimensions, autant peut il y avoir de diverses racines, c'est-à-dire de valeurs de cete quantité ....

Quelles sont les fausses racines.

...Mais souvent il arrive, que quelques vnes de ces racines sont fausses, ou moindres que rien. comme si on suppose que x designe aussy le defaut d'vne quantité qui soit 5, on a x + 5 = 0 .....

Que les racines, tant vrayes que fausses peuuent estre reelles ou imaginaires.

... Au reste tant les vrayes racines que les fausses ne sont pas toujours reelles ; mais quelquefois seulement imaginaires ; c'est-à-dire qu'on peut bien toujours en imaginer autant que iay dit en chaque Equation ; mais qu'il n'y a quelquefois aucune quantité, qui corresponde a celles qu'on imagine.

Descartes, la Géométrie,1637

La Recherche : *On peut considérer qu'à partir de ce moment-là, à la fin du XVIè siècle, le concept de nombre tel que nous le connaissons et le pratiquons aujourd'hui est établi ?*

C. Houzel : *Oui, mais tout de même avec des nuances, liées au statut qu'on attribue aux divers types de nombres.(.....) Les nombres complexes apparaissent pour la première fois dans un livre de Jérôme Cardan.....Mais il n'en fait rien. Le premier texte où l'on voit à l'oeuvre ces nombres imaginaires est un peu ultérieur. Il est d'un autre Italien, Bombelli, en 1572. Il s'agit simplement des racines carrées des nombres négatifs. Il y a une règle des signes connue depuis très longtemps qui dit que si l'on multiplie du plus par du plus ou du moins par du moins, on obtient toujours du plus. Donc un carré d'un nombre ordinaire est forcément positif. Bombelli se place justement dans le cadre du développement arithmétique de la théorie des irrationnels, qui a son origine dans l'algèbre arabe. Il lui donne une extension plus grande. Il dit : j'ai découvert un nouveau type d'irrationnel, il donne des règles de calcul et montre que ces nombres sont utiles pour étudier l'équation du troisième degré. C'est une espèce de* ***calcul formel, qui n'était pas du tout interprétable géométriquement.....***

6. Descartes (1637) nomme les lignes.

Vers la fin de l'homogénéité.

La règle 18 des *« Règles pour la direction de l'esprit »* de 1628 traite de ces liens entre nombres et figures. Descartes cherche à s'affranchir de la contrainte euclidienne sans y parvenir tout à fait. La notion abstraite (isolée) de nombre se fera vers la fin du 17-me siècle avec Newton et Leibniz. Descartes écrit dans cette règle 18 :

> ***« Il est donc important d'exposer ici comment tout rectangle peut être transformé en une ligne**, et inversement une ligne ou même un rectangle en un autre rectangle dont le côté soit désigné. Cela est très facile pour les géomètres, pourvu qu'ils remarquent que toutes les fois que nous comparons, comme ici, des lignes à un rectangle, nous les concevons toujours comme des rectangles, dont un côté est la longueur que nous avons prise pour unité. Ainsi tout se ramène en effet à cette proposition : étant donné un rectangle, en construire un autre, qui lui soit égal, sur un côté donné. »*

Et voici ce que l'on peut trouver au début de la « Géométrie » de 1637.

« Comment on peut user de chiffres en géométrie. »

Tel est le titre du premier paragraphe de la *« Géométrie »* que voici :

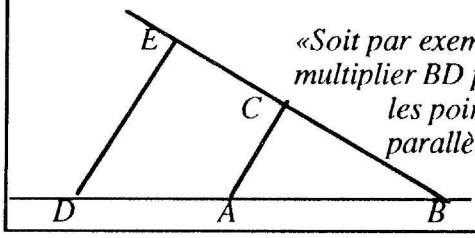
Naissance de la géométrie algébrique :

« Mais souvent on n'a pas besoin de tracer ainsi ces lignes sur le papier, & il suffit de les désigner par quelques lettres, chacune par une seule. »

Perte de la sacro-sainte homogénéité euclidienne :

« Où il est à remarquer que par a^2 ou b^3 ou semblables, ie ne conçoy ordinairement que des lignes toutes simples, encore que pour me servir des noms usités en l'Algèbre, ie les nomme des quarrés ou des cubes. »

Ou encore le lien très fort entre la multiplication et le théorème de Thalès :



«Soit par exemple AB l'unité, & qu'il faille multiplier BD par BC, je n'ai qu'à joindre l les points A & C, puis tirer DE parallèle à CA, & BE est le produit de cette multiplication. »

7. L'Europe au 17 ème siècle.

LES FRACTIONS

L'histoire des fractions semble commencer avec les inverses des entiers en Egypte comme en témoignent les problèmes du papyrus de Rhind vieux d'environ 40 siècles. Les Grecs ne maniaient que les nombres entiers mais la notion de proportionnalité leur était très familière et ils connaissaient bien les propriétés des proportions de nombres entiers dont nous ferons les égalités de fractions.

Dans *« Mathématiques et mathématiciens »*, Dedron et Itard donnent d'autres renseignements sur les fractions. A savoir :

« Les Hindous notaient les fractions comme nous, mais sans la barre horizontale. Les Arabes eurent d'abord la même notation qu'eux, puis introduisirent la barre. Le calcul des fractions ordinaires de ces deux peuples était dans l'ensemble analogue au nôtre. »

Dedron et Itard signalent un type de fractions oublié de nos jours, les fractions en degrés : $\frac{1}{2}\ \frac{4}{7}$ qui représente $\frac{4}{7} + \frac{1}{2}$ septième , lu de droite à gauche comme chez les Arabes et conservé chez le pisan Léonard. Léonard de Pise était allé s'instruire en Afrique du nord. Il utilisait aussi la notation suivante : $\frac{9}{10}\ \frac{6}{10}$ 13 pour écrire 13,69.

« Cependant, ni les Hindous, ni les Arabes, ni les Occidentaux jusqu'à la fin du XVIè siècle ne se sont aperçus de l'intérêt qu'il y aurait à développer le système décimal de position dans les deux sens, comme les Babyloniens avaient développé leur système sexagésimal.

Ce retard provient essentiellement de la perfection même de la numérotation à base 60. Adoptée à partir du IIè siècle avant notre ère par les astronomes grecs, conservée par les astronomes arabes, puis par les occidentaux (toutes les tables avaient été calculées dans cette base) elle fut utilisée dans les calculs astronomiques jusqu'au XVII^{ème} siècle et est encore employée pour les angles et les temps. »

Viète, en 1579, écrit :

« En Mathématiques, les soixantièmes et les soixantaines doivent être d'un usage rare ou nul. Au contraire les Millièmes et les Milles, les centaines et les centièmes, les dizièmes et les dizaines, et les progressions de même genre ascendantes ou descendantes, doivent être d'un usage fréquent ou constant. »

Viète utilise une notation particulière pour les nombres décimaux très voisine de la nôtre : 123,456,^{789} ou encore 123, 456 | 789

Simon Stevin, dans la « Disme », en 1585 calque ses notations de nombres décimaux sur les notations utilisées à l'époque en algèbre pour noter les exposants :

123,45 est écrit par Stevin : 123 (0) 4 (1) 5 (2)

Burgi note : 123456 pour 123,456

Kepler écrit : 12 (34 pour 12,34

En résumé, Stevin, Burgi et quelques autres mathématiciens font entrer dans les habitudes scientifiques européennes le système décimal et les nombres décimaux.

La Recherche *: Mais encore au XVII^{ème} siècle, quand Pascal écrit : « La géométrie ne peut définir ni les nombres ni le mouvement ni l'espace », il considère encore qu'il y a d'un côté les nombres, et de l'autre ce qu'il appelle l'espace, c'est-à-dire ce que nous appelons la géométrie ?*

C. Houzel *: **Certainement**. La mathématique européenne a vécu jusqu'au XVII^{ème} siècle sur cette théorie des proportions euclidiennes. C'est d'ailleurs seulement à cette époque qu'ont été adoptés les nombres décimaux avec les chiffres après la virgule, devenus d'usage courant pour les calculs astronomiques. C'est aussi au début du XVII^{ème} siècle qu'on a inventé les logarithmes, ce qui témoignait déjà d'une espèce de conception d'un continu numérique, mais ils sont apparus pour des raisons pratiques, avant d'être acceptés sur le plan théorique par Newton et Leibniz, qui en fondant le calcul différentiel et le calcul intégral, ont imposé cette conception du continu numérique analysé par les nombres. Les rapports qu'Euclide considérait entre grandeurs géométriques étaient enfin devenus des nombres.*

8. « Négatif » dans l'Encyclopédie.

NEGATIF, adj. (Algèb.) quantités négatives, en algèbre, sont celles qui sont affectées du signe - , & qui sont regardées par plusieurs mathématiciens, comme plus petites que zéro. Cette dernière idée n'est cependant pas juste, comme on verra dans un moment. Voyez QUANTITES.

Les quantités négatives sont le contraire des positives : où le positif finit, le négatif commence. Voyez POSITIF.

Il faut avouer qu'il n'est pas facile de fixer l'idée des quantités négatives, & que quelques habiles gens ont même contribué à l'embrouiller par les notions peu exactes qu'ils en ont donné. Dire que la quantité négative est au dessous du rien, c'est avancer une chose qui ne se peux pas concevoir. Ceux qui prétendent que 1 n'est pas comparable à -1 & que le rapport entre 1 & -1 est différent du rapport entre -1 & 1 sont dans une double erreur : 1° parce qu'on divise tous les jours dans les opérations algébriques 1 par -1 ; 2° l'égalité du produit de -1 par -1, & de +1 par +1, fait voir que 1 est à -1 comme -1 est à 1.

Quand on considère l'exactitude et la simplicité des opérations algébriques sur les quantités négatives, on est bien tenté de croire que l'idée précise que l'on doit attacher aux quantités négatives doit être une idée simple, & n'être point déduite d'une métaphysique alambiquée. Pour tâcher d'en découvrir la vraie notion, on doit d'abord remarquer que les quantités qu'on appelle négatives, & qu'on regarde faussement comme au-dessous de zéro, sont très souvent représentées par des quantités réelles, comme dans la Géométrie, où les lignes négatives ne diffèrent des positives que par leur situation à l'égard de quelque ligne ou point commun. Voyez COURBE.

De là, il est assez naturel de conclure que les quantités négatives que l'on rencontre dans le calcul, sont en effet des quantités réelles; mais des quantités réelles auxquelles il faut attacher une idée autre que celle qu'on avoit supposée. Imaginons, par exemple, qu'on cherche la valeur d'un nombre x, qui ajouté à 100 fasse 50 ; on aura par les règles de l'Algèbre, x + 100 = 50, & x = - 50 ; ce qui fait voir que la quantité x est égale à 50, & qu'au lieu d'être ajoutée à 100 elle doit en être retranchée ; de sorte qu'on auroit dû énoncer le problème ainsi : trouver une quantité x qui étant retranchée de 100, il reste 50 ; en énonçant le problème ainsi, on auroit 100 - x = 50, & x = 50 ; & et la forme négative de x ne subsisteroit plus.

.....

Remarquez que nous ne parlons ici que des quantités négatives isolées, comme -a, ou des quantités a - b , dans lesquelles b est plus grand que a ; car pour celles où a - b est positif, c'est-à-dire, où b est plus petit que a, le signe ne fait aucune difficulté.

Il n'y a donc point réellement & absolument de quantité négative isolée : - 3 pris arbitrairement ne présente à l'esprit aucune idée ; mais si je dis qu'un homme a donné à un autre - 3 écus, cela veut dire en langage intelligible, qu'il lui a ôté 3 écus.

Voilà pourquoi le produit de -a par -b, donne + ab : car a & b étant précédés du signe - par la supposition, c'est une marque que ces quantités a, b, se trouvent mêlées & combinées avec d'autres à qui on les compare, puisque si elles étoient considérées comme seules & isolées, les signes - dont elles sont précédées, ne présenteroient rien de net à l'esprit.

.....Beaucoup plus tard, en 1902.

COURS
D'ALGEBRE

A L'USAGE DES ELEVES
DE LA CLASSE DE MATHEMATIQUES SPECIALES
ET DES CANDIDATS
A L'ECOLE NORMALE SUPERIEURE ET A L'ECOLE POLYTECHNIQUE

PAR
B. NIEWENGLOWSKI
Ancien professeur de mathématiques spéciales au lycée Louis-le-grand

CHAPITRE PREMIER
NOMBRE POSITIFS - NOMBRES NEGATIFS

1. La théorie des nombres positifs et des nombres négatifs (qu'on nomme quelquefois nombres algébriques et aussi nombres qualifiés) est exposée dans tous les traités d'algèbre élémentaire : nous ne ferons que rappeler les points essentiels.

On appelle *nombre positif* l'ensemble formé par un nombre et le signe + placé devant ce nombre ; *nombre négatif* l'ensemble formé par un nombre et le signe - placé devant lui. Ainsi +3, $+\frac{4}{5}$ sont des nombres positifs; -1, $-\frac{3}{7}$, $-\frac{15}{8}$ .... sont des nombres négatifs. Dans ces exemples 3, $\frac{4}{5}$, 1, $\frac{3}{7}$, $\frac{15}{8}$ ... sont les *valeurs absolues* des nombres qualifiés considérés.

Le signe qui précède la valeur absolue se nomme le signe du nombre qualifié. On dit que deux nombres qualifiés sont égaux quand ils ont le même signe et la même valeur absolue.

Deux nombres qualifiés ayant la même valeur absolue et de signes différents sont dits *opposés*, ou encore *égaux et de signes contraires*. Les nombres, tels qu'on les considère en arithmétique sont dits *neutres*.

2. Comme il est arrivé plusieurs fois en mathématiques, la théorie des nombres négatifs a pris naissance dans l'indication d'une opération impossible. On a été conduit à poser, par définition,

$$a - b = - (b - a)$$

quand b surpasse a, a et b étant deux nombres neutres. Ainsi on convient de remplacer 3 - 7 par - (7 - 3), c'est-à-dire -4.

Ce début de cours de Spéciales de 1902 (Prix 8fr.) renseigne assez précisément sur la difficulté de justifier les nombres, de leur redonner une valeur ontologique qui semble bien s'être perdue dans la nuit des temps.

9. De Weierstrass à Dedekind : les nombres réels.

Weierstrass 1815-1897
Dedekind 1831-1916
Cantor 1845-1918

> *La théorie des ensembles ..... embrasse.....les domaines de l'arithmétique, de la théorie des fonctions et de la géométrie ; elle les réduit sur la base du concept de puissance en* ***une unité supérieure****.*
> *Discontinu et continu se trouvent de la sorte considérés du même point de vue et* ***mesurés avec une mesure commune****.*
> Cantor, 31 mars 1892.

> ***Quand Gauss dit qu'il a démontré quelque chose, cela me paraît très probable, quand Cauchy le dit, il y a autant à parier pour que contre, quand Dirichlet le dit, cela est certain.***
> Weierstrass

Ces deux citations évoquent d'une part la recherche d'une unité que les mathématiques vont trouver dans la théorie des ensembles et d'autre part le problème de la qualité des démonstrations y compris chez les meilleurs !

L'école allemande avec Weierstrass, Dirichlet, Riemann, Dedekind et Cantor entame au milieu du XIX^{ème} siècle une réflexion sur les fondements de l'analyse, en particulier de la continuité et de l'intégration. La théorie des ensembles naît de la rencontre en 1872 de Cantor et Dedekind. La correspondance passionnée entre les 2 mathématiciens tourne autour de la droite réelle et des bijections entre ensembles « transfinis ». Vers 1870, les nombres réels restent une donnée intuitive et les travaux de Riemann commencent à montrer un certain « flou artistique ».

Dedekind, en 1872, donne **une construction des rationnels** puis place ces rationnels sur une droite et réalise des « coupures » de cet ensemble où il place les irrationnels obtenant un ensemble continu, **R, la droite réelle, magnifique objet de la géométrie algébrique.**

Les détracteurs de Dedekind pensent que sa construction reprend celle... d'Euclide. Pour Dedekind, les « coupures de rationnels » sont le fondement axiomatique de la limite d'une suite, de la continuité, permettant ainsi de démontrer correctement le théorème des valeurs intermédiaires pour une fonction continue.

La théorie des ensembles, en donnant une construction de la droite réelle, a répondu aux questions posées par l'analyse autour des fonctions, continuité ou intégration. A partir de là, allait naître différentes théories de la.. mesure !!!

Eh oui, tout comme la rédaction axiomatisée d'Euclide avait donné la mesure des grandeurs, la théorie des ensembles allait donner toute une série de théories de la mesure. La mesure de Borel sembla donner les meilleurs résultats mais beaucoup d'autres théories mirent à la disposition des physiciens des modèles de l'espace.
(Notons pour finir que le dernier ensemble à recevoir une définition axiomatique fut l'ensemble des entiers naturels Péano, vers 1900)

La **construction** (sic) de l'ensemble des nombres réels génère aussitôt des paradoxes venus... des figures : courbe de Péano, ensemble de Cantor, la « galerie des Monstres » dont Mandelbrot tirera la géométrie fractale De bien beaux objets de la géométrie algébrique.

10. Qu'est-ce qu'un nombre au XX^{ème} siècle ?

« *En définitive, il ne faut pas se leurrer, on ne sait pas très bien.* » disait Houzel.
L'histoire est quand même disponible, depuis peu, pour renseigner sur l'épistémologie des nombres et leur passé. Pourquoi l'espèce humaine a-t-elle créé les nombres ?

1°) Compter : l'arithmétique.
Pour Euclide, les seuls nombres dignes d'une théorie étaient les entiers naturels. Gauss, au XIX^{ème} siècle, a tout de même étendu le domaine de l'arithmétique aux entiers relatifs modulo les congruences.

2°) Mesurer : la géométrie, les géométries.
La théorie des proportions a mis en évidence les nombres rationnels, rapports d'entiers pour mesurer les segments. Puis les irrationnels sous la contrainte des théorèmes.

3°) Résoudre : l'algèbre, chapitre I, ouvert par Al-Khwarizm : les équations.
Les équations algébriques étendent le domaine des nombres par la création des nombres complexes.

4°) Structurer : l'algèbre, chapitre II, ouvert par Galois : les structures.
Au cours du XIX^{ème} siècle, les structures algébriques ont donné naissance à de multiples théories des nombres. L'encyclopédie Universalis n'évoque d'ailleurs que les théories des nombres :

A) Théorie analytique des nombres
B) Théorie des nombres p-adiques
C) Théorie des nombres algébriques

Dedekind construit des extensions finies de $\mathbf{Q}$, des corps de nombres algébriques.

5°) La théorie des ensembles.
L'ensemble des nombres réels est à l'origine de cette théorie. La droite réelle doit-elle être considérée comme le but ultime des mathématiciens ?
Probablement pas.
(Les nombres complexes seraient-ils alors des nombres ?)

6°) Déduire : la logique.
L'analyse non-standard, Robinson, 1961.
L'infiniment grand est-il un nombre ? Leibniz : « Le réel ϖ est infiniment grand s'il est supérieur à tout entier. » $\Rightarrow$ Le réel ϖ n'existe pas.
L'analyse non-standard propose de considérer ϖ comme un nombre vérifiant :

$$\text{Pour tout } n \in N \text{ , } \varpi > n.$$

Cette extension du domaine des nombres nécessite cette fois une extension du système logique usuel, dit de Zermelo-Fraenckel (ZF) en un système ZFL (Leibniz). Cette extension de **R** donne un calcul infinitésimal efficace dans certains problèmes, calcul impossible dans **R**.

En Résumé

On ne sait pas très bien où l'on s'arrêtera dans l'extension du domaine des nombres. Mais on sait assez bien d'où l'on vient.

Nombres	Utilisation	Espace
Entiers	Compter	Discret
Réels	Mesurer	Droite continue
Complexes	Résoudre	Plan

Et on ne sait toujours pas très bien ce qu'est un nombre. Mais, selon Pascal,

> *« cette admirable science [la géométrie] ne s'attachant qu'aux choses les plus simples, cette même qualité qui les rend dignes d'être ses objets, les rend incapables d'être définis. »*

DIFFERENTES SORTES DE NOMBRES ET LOGICIELS DE CALCUL FORMEL.

Michel Janvier
Groupe Informatique

Pour une bonne utilisation des logiciels de calcul formel il est utile, sinon indispensable de connaître les méthodes de calcul qu'ils emploient. Ces logiciels permettent par exemple d'obtenir des simulations d'expériences aléatoires, mais pour bien en tirer partie il faut savoir comment sont engendrés les nombres pseudo-aléatoires qui sont à la base de ces simulations. De même, ils utilisent la théorie des bases de Gröbner pour résoudre les systèmes d'équations polynomiales. La connaissance de cette théorie permet de mieux programmer les calculs que l'on désire effectuer. De plus ces théories ont des applications permettant de réaliser des taches nouvelles et souvent inattendues, comme, par exemple, la démonstration de théorèmes de géométrie, à l'aide des bases de Gröbner. A contrario, la méconnaissance des procédés employés par le logiciel le transforme en une sorte de boite noire, dont le fonctionnement n'est pas maîtrisé..

1. Les nombres pseudo-aléatoires.

1.1 Production de nombres pseudo-aléatoires.

Tous les logiciels de calcul, comme les tableurs ou les logiciels de calculs formels, possèdent des générateurs de nombres aléatoires. Par exemple, dans SWP, Maple nous fournit dix nombres aléatoires, répartis suivant une loi uniforme dans l'intervalle [0,1] :

0.95105, 0.14649, 0.42939, 0 52543, 0.02726, 0.21976, 0.067598, 0.84547, 0.67647, 0.45375, 0.64403, 0.92062

(Par Maple, Statistics, Random Numbers, puis dans la boite de dialogue qui s'ouvre choisir le nombre de nombres désirés, la distribution de probabilité, ici "uniform", les bornes de l'intervalle dans lequel doivent se trouver les nombres). Pour obtenir le même résultat avec Mathematica on utiliserait Table[Random[Real,{0,1}],{10}]. La principale méthode employée pour engendrer une suite de nombres aléatoires consiste à considérer un grand nombre premier p puis à construire une suite $(x_n)_n$ d'éléments de $\mathbb{Z}/p\mathbb{Z}$ définie par itérations d'une fonction $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ de le forme $f(x) = (ax + b)_p$, la suite $(x_n)_n$ est définie par :

$$\begin{cases} x_0 &= s \\ x_n &= f(x_n - 1) \end{cases}$$

s s'appelle le germe de la suite $(x_n)_n$. Si y_n désigne l'unique entier de l'intervalle $[0, p-1]$, représentant la classe x_n, dans la congruence modulo p, le réel $z_n = \frac{y_n}{p} \in [0, 1]$.

Exemple 1 *Commençons par un exemple peu réaliste, en prenant* $p = 7$, $s = 0, a = 3, b = 2$.

```
a=3 ; b= 2;(* introduction des valeurs de a et b *)
f[x_]:= a x+ b (* définition de la fonction f *) ;
g[x_, p_Integer] := Mod[f[x],p] (* indique modulo quel entier p il faut calculer *) ;
NestList[g[#,7] &,0,6] (* On fixe l'entier p à la valeur 7, le germe à 0,
et on itère 6 fois *)
{0,2,1,5,3,4,0}
```

On obtient six valeurs différentes, puis on retrouve le germe $s = 0$.

Comme $\mathbb{Z}/p\mathbb{Z}$ est fini, la suite $(x_n)_n$ est nécessairement périodique. Essayons le germe $s = 6$.

```
NestList[g[#,7]&,6,6]
{6,6,6,6,6,6,6}
```

On a obtenu une suite stationnaire. $(6)_7$ est un point fixe de f. Il nous faut donc éviter de prendre comme germe un point fixe. Il est facile de trouver le point fixe de f, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps.

```
Solve[a x + b ==x && Modulus == 7,x]
{{Modulus ->7,x -> 6}}
```

Remarque 1 *En Mathematica, les équations se présentent à l'aide de la fonction booléenne Equal, dont la forme infixe est* `==`. *On ajoute ici l'équation Modulus == 7, pour contraindre Mathematica à calculer dans* $\mathbb{Z}/7\mathbb{Z}$. *&& est la forme infixe de la fonction booléenne And. Elle permet ici d'introduire un système d'équations, que l'on aurait aussi bien pu présenter comme une liste d'équations. La fonction Solve résout le système d'équations proposées, sous la forme de règles de substitutions : Ainsi x -> 6, qui indique qu'il faut substituer 6 à x dans l'expression Equal[ax + b,x] pour obtenir la valeur "True". 6 est bien une solution de l'équation que l'on voulait résoudre.*

Prenons un exemple plus réaliste avec $p = 97, a = 37, b = 57$ et $s = 77$

```
a=37; b= 57;
list1 = NestList[g[#,97]&,77,96]
{77,93,6,85,1,94,43,96,20,21,58,69,88,15,30,3,71,65,37,68,51,4,
11,76,56,92,66,74,79,70,28,26,49,27,86,38,8,62,23,35,91,29,63,
60,46,13,53,78,33,17,7,25,12,16,67,14,90,89,52,41,22,95,80,10,
39,45,73,42,59,9,2,34,54,18,44,36,31,40,82,84,61,83,24,72,5,48,
87,75,19,81,47,50,64,0,57,32,77}
```

Y-a-t-il des répétitions dans cette liste?

```
Length[Union[Drop[list1,1]] ]
96
```

Drop[List1,1] retire à la liste précédente son premier élément 77. Union classe ensuite les éléments de la liste par ordre croissant en supprimant les répétitions. Puis Length donne le nombre d'éléments de la suite ainsi obtenue : il y en a 96. On a obtenu 96 éléments distincts de $\mathbb{Z}/97\mathbb{Z}$. Les voici rangés par ordre croissant :

```
Union[Drop[list1,1]]

{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,
27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,
50,51,52,53,54,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,
74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96}
```

55 n'apparaîtapparait pas dans cette liste. Vérifions que 55 est le point fixe de f.

```
Solve[a x + b ==x && Modulus == 97,x]

{{Modulus -> 97,x -> 55}}
```

Drop[List1,1] fournit donc 96 éléments distincts de $\mathbb{Z}/97\mathbb{Z}$, dans un ordre qu'il est difficile de prévoir quand on ne connaît pas le secret de sa fabrication. On en tire une suite de 96 nombres réels compris entre 0 et 1.

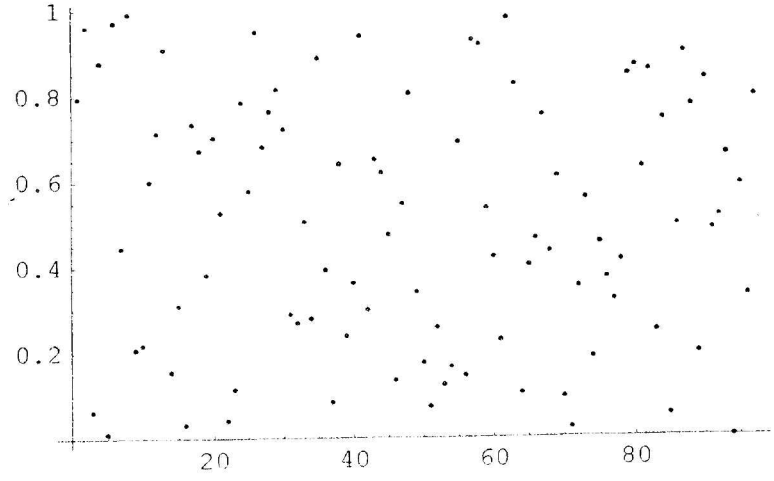
```
list2 = Drop[list1,1]/97 //N

{0.958763,0.0618557,0.876289,0.0103093,0.969072,0.443299,0.989691,
0.206186,0.216495,0.597938,0.71134,0.907216,0.154639,0.309278,
0.0309278,0.731959,0.670103,0.381443,0.701031,0.525773,0.0412371,
0.113402,0.783505,0.57732,0.948454,0.680412,0.762887,0.814433,
0.721649,0.28866,0.268041,0.505155,0.278351,0.886598,0.391753,
0.0824742,0.639175,0.237113,0.360825,0.938144,0.298969,0.649485,
0.618557,0.474227,0.134021,0.546392,0.804124,0.340206,0.175258,
0.0721649,0.257732,0.123711,0.164948,0.690722,0.14433,0.927835,
0.917526,0.536082,0.42268,0.226804,0.979381,0.824742,0.103093,
0.402062,0.463918,0.752577,0.43299,0.608247,0.0927835,0.0206186,
0.350515,0.556701,0.185567,0.453608,0.371134,0.319588,0.412371,
0.845361,0.865979,0.628866,0.85567,0.247423,0.742268,0.0515464,
0.494845,0.896907,0.773196,0.195876,0.835052,0.484536,0.515464,
0.659794,0,0.587629,0.329897,0.793814}
```

Remarque 2 *Pour diviser chacun des termes de Drop[list1,1] par 97, il suffit d'écrire Drop[list1,1] 97. On dit que la division est une opération listable. N[a] fournit une valeur approchée de a. On utilise ici la fonction N sous sa forme postfixe //N. N est également listable.*

Représentons les points (n, x_n) pour $1 \leq n \leq 96$.

```
1. ListPlot[list2]
```



-Graphics-

Suivant le choix de a on obtient pas nécessairement $p-1$ éléments distincts de $\mathbb{Z}/p\mathbb{Z}$. Prenons, par exemple $a=64, b=57$.

```
a=64; b= 57;
list2 = NestList[g[#,97]&,77,96]
Union[Drop[list2,1]]
Length[Union[Drop[list2,1]] ]
{77,38,64,79,69,11,82,67,77,38,64,79,69,11,82,67,77,38,64,79,69,11,
82,67,77,38,64,79,69,11,82,67,77,38,64,79,69,11,82,67,77,38,64,79,69,
11,82,67,77,38,64,79,69,11,82,67,77,38,64,79,69,11,82,67,77,38,64,79,
69,11,82,67,77,38,64,79,69,11,82,67,77,38,64,79,69,11,82,67,77,38,64,
79,69,11,82,67,77}
{11,38,64,67,69,77,79,82}
8
```

On a obtenu que huit éléments distincts. On est donc amené à trouver une caractérisation des éléments $(a)_p$ de $\mathbb{Z}/p\mathbb{Z}$ tels que la suite $(x_n)_n$ fournisse $p-1$ éléments distincts de $\mathbb{Z}/p\mathbb{Z}$.

Proposition 1 *Soit y le point fixe de f. Pour tout $n \in \mathbb{N}^*$, $f^n(x) = (a^n(x-y)+y)_p$*

La relation est vraie pour $n=1$. Par définition

$$y = ay + b$$

Par ailleurs

$$f(x) = ax + b$$

En soustrayant $f(x) - y = a(x-y)$, et par suite

$$f(x) = a(x-y) + y$$

Supposons, la relation établie à l'ordre n, alors

$$\begin{aligned} f^{n+1}(x) &= f(f^n(x)) \\ &= a(a^n(x-y)+y)+b \end{aligned}$$

$$\begin{aligned} &= a^{n+1}(x-y)+ay+b \\ &= a^{n+1}(x-y)+y \end{aligned}$$

La relation est encore vraie à l'ordre $n+1$.
On a établi la par récurrence la relation annoncée pour tout $n \in \mathbb{N}^*$.

Corollaire 2 *Les périodes de la suite $(x_n)_n$ sont les entiers q tels que $(a^q)_p = 1_p$.*

En effet, si $(a^n)_p = 1_p$, $f^n(x) = x - y + y = x$. Inversement si q est une période de la suite $(x_n)_n$, pour tout $n \in \mathbb{N}$, $x_{n+q} = x_n$ et $f^{n+q}(s) = f^n(s)$, où s est le germe de la suite $(x_n)_n$, donc $(a^{n+q}(s-y))_p = (a^n(s-y))_p$, comme s n'est pas le point fixe de f, $s-y$ est non nul, et $(a^q)_p = 1_p$.

1.2 Petit théorème de Fermat.

Rappelons la définition de l'ordre d'un élément dans $\mathbb{Z}/p\mathbb{Z}$.

Définition 1 *L'ordre d'un élément a dans $(\mathbb{Z}/p\mathbb{Z}, \times)$ est le plus petit entier n tel que $a^n = 1_p$.*

Corollaire 3 *La plus petite période de la suite $(x_n)_n$ est la période de a_p.*

Nous allons établir que l'ordre d'un élément a dans $(\mathbb{Z}/p\mathbb{Z}, \times)$ est un diviseur de $p-1$. Pour cela nous aurons besoin du petit théorème de Fermat , selon lequel $a^{p-1} = 1_p$ quel que soit $a \in \mathbb{Z}/p\mathbb{Z}$..

THEOREME 4 *(petit théorème de Fermat). Dans $\mathbb{Z}/p\mathbb{Z}$, $a^{p-1} = 1_p$.*

Lemme 5 *Dans $\mathbb{Z}/p\mathbb{Z}$, $(a+b)^p = a^p + b^p$*

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif, on peut appliquer la formule du binôme de Newton

$$(a+b)^p = \sum_{k=0}^{p} C_p^k a^k b^{p-k}$$

$C_p^k = p(p-1)...(p-k+1)$ est divisible par p pour $1 \leq k \leq p-1$. Donc $C_p^k a^k b^{p-k} = 0_p$, pour $1 \leq k \leq p-1$, et $(a+b)^p = a^p + b^p$

Lemme 6 *Dans $\mathbb{Z}/p\mathbb{Z}$, pour $n \geq 2$, $(x_1 + x_2 + ... + x_n)^p = x_1^p + x_2^p + ... + x_n^p$*

D'après le lemme précédent, la formule est vraie pour $n = 2$.
Supposons la formule vraie à l'ordre n, alors

$$\begin{aligned} (x_1 + x_2 + ... + x_{n+1})^p &= ((x_1 + x_2 + ... + x_n) + x_{n+1})^p \\ &= (x_1 + x_2 + ... + x_n)^p + x_{n+1}^p \end{aligned}$$

grâce au lemme précédent. En appliquant l'hypothèse de récurrence,

$$(x_1 + x_2 + ... + x_{n-1})^p = x_1^p + x_2^p + ... + x_n^p + x_{n-1}^p$$

On a établi la formule par récurrence pour tout entier $n \geq 2$.

Soit a un entier qui vérifie $1 \leq a \leq p-1$, en prenant $x_i = 1$, pour $1 \leq i \leq a$, le lemme précédent donne en confondant a et a_p, la classe de a modulo p

$$a^p = (1 + 1 + ... + 1)^p = 1^p + 1^p + ... + 1^p = a1^p = a$$

et comme a est inversible dans $\mathbb{Z}/p\mathbb{Z}$, $a^{p-1} = 1$, ce qui démontre le petit théorème de Fermat.

Proposition 7 *L'ordre d'un élément dans $\mathbb{Z}/p\mathbb{Z}$ est un diviseur de $p-1$.*

Soit n l'ordre de a, dans $\mathbb{Z}/p\mathbb{Z}$. $n \leq p-1$, car $a^{p-1} = 1$. Soit q et r le quotient et le reste de $p-1$, dans la division euclidienne de $p-1$ par n :

$$p - 1 = qn + r,\ 0 \leq r < n$$

Alors $1 = a^{p-1} = a^{qn+r} = (a^n)^q a^r = 1^q a^r = a^r$. Si r n'était pas nul, on aurait $a^r = 1$, avec $0 < r < n$, ce qui contredirait la définition de n. Par suite $r = 0$, et $p - 1 = qn$, n est un diviseur de $p-1$.

En conséquence, si l'on veut obtenir une suite $(x_n)_n$ dont le plus petite période soit égale à $p-1$, il nous faut rechercher les éléments a de $\mathbb{Z}/p\mathbb{Z}$ d'ordre $p-1$, de tels éléments s'appellent des racines primitives de p.

Definition 1 *Si a est un élément d'ordre $p-1$ de $\mathbb{Z}/p\mathbb{Z}$, on dit que a est une racine primitive de p.*

Heureusement, les racines primitives de p ne sont pas rares, grâce à un résultat de Legendre.

THEOREME 8 *(Legendre) Soit p un nombre premier impair. Il existe $\Phi(p-1)$ racines primitives de p, où Φ désigne la fonction d'Euler.*

Rappelons la définition de la fonction Φ d'Euler.

1.3 La fonction Φ d'Euler.

Definition 2 *Pour tout entier naturel n on note $\Phi(n)$ le nombre d'entiers naturels non nuls inférieurs à n et premiers avec n.*

Exemple 2 $\Phi(1) = 1$.
$\Phi(10) = 4$
$\Phi(p) = p - 1$, *si p est un nombre premier*

On démontre dans tous les traités d'arithmétique le lemme suivant :

Lemme 9 *Si $n = m_1 m_2 ... m_p$ où les entiers m_i et m_j sont premiers entre eux pour toute paire d'entiers $\{i, j\}$ de $\{1, 2, ..., p\}$*

$$\Phi(n) = \Phi(m_1)\Phi(m_2)...\Phi(m_p)$$

En utilisant ce lemme, Euler a démontré en 1760 le théorème suivant :

THEOREME 10 *(Euler, 1760) Soit n un entier naturel et $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ sa décomposition en produit de facteurs premiers. Alors*

$$\Phi(n) = \Phi(p_1^{\alpha_1})\Phi(p_2^{\alpha_2})...\Phi(p_k^{\alpha_k})$$

Par ailleurs, on démontre que si p est un nombre premier

$$\Phi(p^\alpha) = p^{\alpha-1}(p-1) = p^\alpha(1 - \frac{1}{p})$$

En conséquence, si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$,

$$\begin{aligned} \Phi(n) &= p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1)...p_k^{\alpha_k}(p_k - 1) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k}) \end{aligned}$$

Exemple 3 $\Phi(2560) = \Phi(2^9.5) = 2560(1 - \frac{1}{2})(1 - \frac{1}{5})$.

On a alors comme conséquence du lemme, un résultat assez surprenant, dont nous allons avoir besoin.

THEOREME 11 *Si n est un entier positif, alors $n = \sum_{d|n} \Phi(d)$. (La sommation s'effectue sur l'ensemble des diviseurs de n).*

Nous allons raisonner par récurrence sur n. Il est clair que la propriété est vraie si $n = 1$. Supposons la propriété vraie pour tout entier $n \leq N - 1$, et démontrons la dans le cas où $n = N$. Soit p un diviseur premier de n. Posons $N = p^\alpha M$ où M et p sont premiers entre eux. Lorsque d parcourt l'ensemble des diviseurs de M, les diviseurs de n sont les nombres de la forme $d, pd, p^2d, ..., p^\alpha d$. Il s'en suit que

$$\sum_{\delta|N} \Phi(\delta) = \sum_{d|M} [\Phi(d) + \Phi(pd) + ... + \Phi(p^\alpha d)]$$

D'après le lemme, pour chaque entier i, vérifiant $1 \leq i \leq \alpha$

$$\Phi(p^i d) = \Phi(p^i)\Phi(d)$$

Il en résulte que

$$\begin{aligned} \sum_{\delta|N} \Phi(\delta) &= \sum_{d|M} \Phi(d)[1 + (p-1) + p(p-1) + ... + p^{\alpha-1}(p-1)] \\ &= \sum_{d|M} \Phi(d)p^\alpha \\ &= p^\alpha \sum_{d|M} \Phi(d) \end{aligned}$$

Par hypothèse de récurrence, $\sum_{d|M} \Phi(d) = M$, et $\sum_{\delta|N} \Phi(\delta) = p^\alpha M = N$.

Avant d'établir le théorème de Legendre, il nous faut énoncer et démontrer le théorème de Lagrange sur les polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, qui ressemble au théorème de d'Alembert sur les polynômes à coefficients complexes.

1.4 Théorème de Lagrange.

THEOREME 12 *(Lagrange, 1768) Soit p un nombre premier, et soit $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, de degré n. Alors la congruence $f(x) \equiv 0 \bmod(p)$, admet au plus n solutions dans $\mathbb{Z}/p\mathbb{Z}$.*

Pour établir ce théorème, nous commencerons par la démonstration de résultats, analogues à ceux que l'on établit pour les polynômes à coefficients réels ou complexes.

THEOREME 13 *Soit $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$, un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ et c_1 une solution dans $\mathbb{Z}/p\mathbb{Z}$ de l'équation $f(x) = 0$. On peut alors écrire que $f(x) = (x - c_1)f_1(x)$, où $f_1(x)$ est un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ et de degré $n - 1$.*

En effet si c_1 est une solution de l'équation $f(x) = 0$, $f(x) = f(x) - f(c_1)$ dans l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$. Mais $f(x) - f(c_1) = \sum_{i=1}^{n} a_i(x^i - c_1^i)$, la sommation pouvant débuter à $i = 1$. Pour $1 \leq i \leq n$,

$$x^i - c_1^i = (x - c_1)[\sum_{k=0}^{i-1} x^{i-1-k}c_1^k]$$

Par suite

$$f(x) - f(c_1) = (x - c_1)\sum_{i=1}^{n} a_i[\sum_{k=0}^{i-1} x^{i-1-k}c_1^k] = (x - c_1)f_1(x)$$

où $f_1(x)$ est un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, de degré $n - 1$, son coefficient de degré $n - 1$ étant égal à a_n.

Corollaire 14 *Soit $c_1, c_2, ..., c_r$ r solutions distinctes de $f(x) = 0$ dans $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier. Alors*

$$f(x) = (x - c_1)(x - c_2)...(x - c_r)f_r(x)$$

où $f_r(x)$ est un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, de degré $n - r$.

D'après le théorème que l'on vient d'établir $f(x) = (x-c_1)f_1(x)$ où $f_1(x)$ est un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Comme c_2 est aussi une solution de l'équation $f(x) = 0$, $(c_2 - c_1)f_1(c_2) = 0$. Comme c_1 est distinct de c_2, $c_1 - c_2$ est non nul et $\mathbb{Z}/p\mathbb{Z}$ étant un corps, $f_1(c_2) = 0$. En appliquant le théorème à f_1, on conclue à l'existence d'un polynôme $f_2(x)$, à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, de degré $n - 2$, tel que $f_1(x) = (x-c_2)f_2(x)$. Continuant ainsi de proche en proche on démontre le corollaire.
Nous sommes maintenant en mesure de démontrer le théorème de Lagrange.

Soit $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$, un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ de degré n. Supposons que $f(x)$ ait $n+1$ racines distinctes dans $\mathbb{Z}/p\mathbb{Z}$: $c_1, c_2, ..., c_n, c_{n+1}$. En appliquant le corollaire précédent aux n premières racines, on montre qu'il existe un polynôme de degré 0, $f_n(x)$, à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ tel que

$$f(x) = (x - c_1)(x - c_2)...(x - c_n)f_n(x)$$

$f_n(x)$ est donc un polynôme constant. Posons $f_n(x) = b$ On voit immédiatement que $b = a_n$. c_{n+1} étant une racine de $f(x)$, on a la relation

$$b(c_{n+1} - c_1)(c_{n+1} - c_2)...(c_{n+1} - c_n) = 0$$

Comme pour tout i, vérifiant $1 \leq i \leq n$, $c_{n+1} - c_i$ est non nul et que cette relation est écrite dans le corps $\mathbb{Z}/p\mathbb{Z}$ on en conclue que $b = a_n = 0$, ce qui contredit le fait que $f(x)$ soit un polynôme de degré n. Par suite $f(x)$ ne saurait avoir plus de n racines distinctes.

Remarque 3 *Le fait que p soit premier est essentiel. Par exemple l'équation* $2x - 2 = 0$ *admet deux solutions dans* $\mathbb{Z}/4\mathbb{Z}$, *à savoir* $x = (2)_4$ *et* $x = (3)_4$, *bien que* $2x - 2$ *soit un polynôme du premier degré.*

Il nous faut encore établir deux corollaires du théorème de Lagrange.

Corollaire 15 *Soit p un nombre premier, alors dans* $\mathbb{Z}/p\mathbb{Z}[X]$

$$x^{p-1} - 1_p = (x - 1_p)(x - 2_p)...(x - (p-1)_p)$$

En effet d'après le petit théorème de Fermat, $x^{p-1} = 1_p$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$. Par suite

$$x^{p-1} - 1_p = (x - 1_p)(x - 2_p)...(x - (p-1)_p)f_p(x)$$

où $f_p(x)$ est de degré 0. Naturellement $f_p(x) = 1_p$.
Nous en arrivons enfin au corollaire du théorème de Lagrange, dont nous aurons besoin pour démontrer le théorème de Legendre.

Corollaire 16 *Soit p un nombre premier et d un diviseur de* $p - 1$. *Le polynôme* $x^d - 1_p$ *a exactement d racines dans* $\mathbb{Z}/p\mathbb{Z}$.

Comme d divise $p - 1$, il existe un entier q tel que $p - 1 = qd$. Alors, en posant $X = x^d$, on a

$$x^{p-1} - 1_p = X^q - 1_p = (X - 1_p)(X^{q-1} + X^{q-2} + ... + X + 1) = (x^d - 1)g(x)$$

où $g(x)$ est un polynôme de degré $p - 1 - d$. Considérons maintenant les équations

$$\begin{aligned} x^d - 1_p &= 0 \\ g(x) &= 0 \end{aligned}$$

dans $\mathbb{Z}/p\mathbb{Z}$. La première a, d'après le théorème de Lagrange, au plus d solutions et la seconde a au plus $p - 1 - d$ solutions. Comme p est un nombre premier, toute solution u, dans $\mathbb{Z}/p\mathbb{Z}$, de l'équation $x^{p-1} - 1_p = 0$, est soit une solution de $x^d - 1_p = 0$, soit une solution de $g(x) = 0$. Si l'équation $x^d - 1_p = 0$ avait moins de d solutions dans $\mathbb{Z}/p\mathbb{Z}$, l'équation $x^{p-1} - 1_p = 0$ aurait moins de $d + p - 1 - d = p - 1$ solutions. Or on a vu

que l'équation $x^{p-1} - 1_p = 0$ a exactement $p-1$ solutions dans $\mathbb{Z}/p\mathbb{Z}$ on aboutit à une contradiction. Par suite l'équation $x^d - 1$ a exactement d solutions dans $\mathbb{Z}/p\mathbb{Z}$.
Nous allons maintenant démontrer le théorème de Legendre.

1.5 Théorème de Legendre.

Soit p un nombre premier, alors il existe $\Phi(p-1)$ racines primitives de p.
Notons $\Psi(e)$, le nombre de solutions de l'équation $x^{p-1} - 1_p = 0$, dans $\mathbb{Z}/p\mathbb{Z}$ d'ordre e exactement. Nous nous proposons d'établir que $\Psi(e) = \Phi(e)$.
Cette égalité est évidente si $e = 1$, car alors $x = 1_p$ et $\Psi(e) = 1$, donc $\Psi(e) = \Phi(e) = 1$.
On a vu que si a est un élément de $\mathbb{Z}/p\mathbb{Z}$ d'ordre e, alors e divise $p-1$. On peut donc restreindre son attention aux diviseurs de $p-1$. Soit d un tel diviseur supposons que l'on ait établi l'égalité $\Psi(\delta) = \Phi(\delta)$ pour tout diviseur δ de $p-1$, inférieur à d. D'après le corollaire du théorème de Lagrange, on sait que l'équation $x^d - 1_p = 0$ a exactement d solutions. Chacune de ces solutions est évidemment une solution, dont l'ordre est un diviseur de d, de l'équation $x^{p-1} - 1_p = 0$. Réciproquement toute solution de l'équation $x^{p-1} - 1_p = 0$, dont l'ordre divise d, est trivialement, par définition même de l'ordre, une solution de l'équation $x^d - 1_p = 0$. Par conséquent $d = \sum_{\delta|d} \Psi(\delta)$. Par hypothèse de récurrence, $\Psi(\delta) = \Phi(\delta)$ si $\delta|d$ et $\delta < d$. On peut donc réécrire la sommation précédente sous la forme

$$d = \sum_{\delta|d} \Psi(\delta) = \sum_{\delta|d} \Phi(\delta) = \Phi(d) + \Psi(d)$$

Mais on a vu que pour tout entier naturel non nul t, $t = \sum_{\tau|t} \Phi(\tau)$. Par suite $d = d - \Phi(d) + \Psi(d)$, c'est à dire que $\Phi(d) = \Psi(d)$.
Le théorème de Legendre s'en déduit immédiatement en prenant $e = p-1$. On obtient $\Psi(p-1) = \Phi(p-1)$, comme le dit le théorème.

Exemple 4 *Si* $p = 11$, *alors* $1^1 = 2^{10} \equiv 3^5 \equiv 4^5 \equiv 5^5 \equiv 6^{10} \equiv 7^{10} \equiv 8^{10} \equiv 9^5 \equiv 10^2 \bmod(p)$. *Ainsi* $2, 6, 7$ *et* 8 *sont les* $4 = \Phi(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5})$ *racines primitives de* 1_{11} *dans* $\mathbb{Z}/11\mathbb{Z}$.

Le théorème de Legendre nous indique que les racines primitives de 1_p ne sont pas rares, pour un nombre premier donné p. Par contre il n'existe pas d'algorithme permettant de les trouver. Gauss disait que "leur distribution était un grand mystère" et Euler ne connaissait aucune règle pour en trouver une. On peut évidemment procéder par essai successifs pour des nombres premiers pas trop grand et se faire aider par des ordinateurs.

1.6 Racines primitives de p, lorsque p est premier.

On choisira un très grand nombre premier p , par exemple supérieur à 10000, de manière à obtenir, en prenant pour a une racine primitive de p, une suite $(x_n)_n$ dont la période soit grande.

Prime[10000]

104729

p = Prime[n] est le n-ième nombre premier. Décomposons $p-1$ en produit de facteurs premiers à l'aide de la fonction FactorInteger.

FactorInteger[104729-1]

{{2,3},{13,1},{19,1},{53,1}}

104 728 $=2^3.13.19.53$. Calculons $\Phi(104728)$

phi = 104728 (1-1/2)(1-1/13)(1-1/19)(1-1/53)

44928

En prenant un entier au hasard entre 1 et 104728 on a donc, grâce au théorème de Legendre une probabilité égale à 44928/104728, de tomber sur un entier a tel que $(a)_{104729}$ soit une racine primitive de 104729. Essayons 3.

L'ordre de 3 est un diviseur de 104728. Les diviseurs de 104728 sont de la forme $2^\alpha 13^\beta 19^\gamma 53^\delta$, avec $0 \leq \alpha \leq 3, 0 \leq \beta \leq 1, 0 \leq \gamma \leq 1, 0 \leq \delta \leq 1$. Il y en a donc $4.2.2.2 = 32$. Construisons la liste des diviseurs de 104728.

list3 =
Distribute[{{0,1,2,3},{0,1},{0,1},{0,1}},List,List]

{{0,0,0,0},{0,0,0,1},{0,0,1,0},{0,0,1,1},{0,1,0,0},{0,1,0,1},{0,1,1,0},
{0,1,1,1},{1,0,0,0},{1,0,0,1},{1,0,1,0},{1,0,1,1},{1,1,0,0},{1,1,0,1},
{1,1,1,0},{1,1,1,1},{2,0,0,0},{2,0,0,1},{2,0,1,0},{2,0,1,1},{2,1,0,0},
{2,1,0,1},{2,1,1,0},{2,1,1,1},{3,0,0,0},{3,0,0,1},{3,0,1,0},{3,0,1,1},
{3,1,0,0},{3,1,0,1},{3,1,1,0},{3,1,1,1}}

On a construit d'abord l'ensemble produit A = {0,1,2,3}× {0,1} × {0,1}× {0,1}. On construit ensuite l'application q de cet ensemble dans l'ensemble des diviseurs de 104728 qui à (x, y, z, t) associe $2^x.13^y.19^z53^t$. On applique ensuite cette application à chacun des éléments de A, ce qui donne la liste, notée div, des diviseurs de 104728.

p[x_, y_, z_, t_] := $2^x.13^y.19^z53^t$
q[u_List] := Apply[p, u]
div = Map[q, list3]
{1,53,19,1007,13,689,247,13091,2,106,38,2014,26,1378,494,26182,4,
212,76,4028,52,2756,988,52364,8,424,152,8056,104,5512,1976,104728}

Elevons $(3)_{104729}$ à toutes les puissances $(3^k)_{104729}$ lorsque k parcourt l'ensemble des diviseurs de 104728.

r[a_, b_] := Mod[a^b, 104729]
Map[r[3, #]&, div]

{3,102446,83754,33964,23388,79730,59571,70765,9,80368,88825,68090,
103706,32058,66605,68090,81,63807,16681,104728,103968,9687,10314,
104728,6561,98103, 95537,1,55476,785,78661,1}

On constate que 3 n'est pas d'ordre 104728, mais d'ordre 8056. Vérifions.

r[3,8056]

1

Faisons d'autres essais.

```
Map[r[5,#]&, div]
```

```
{5,23894,76154,9176,86630,22401,52755,1,25,45457,63341,101589,
86218,48162,21579,1,625,35679,19020,15074,88562,40352,28107,1,
76438,10046,26434,68275, 73034,62141,32602,1}
```

Pas de chance 5 est d'ordre 13091. Vérifions.

```
r[5,13091]
```

```
1
```

Après quelques essais on trouve que 12 est d'ordre 104728.

```
Map[r[12,#]&, div]
```

```
{12,81998,96799,3329,6932,70998,45158,33964,144,70204,47500,
85696,86742,4505,66605,68090,20736,54876,73153,102207,24288,
82328,10314,104728,69151,102439, 23696,76744,73216,48162,
78661,1}
```

On prendra donc $a = 12$, et $b = 3$.
Cherchons alors le point fixe de f.

```
Solve[12 x + 3 ==x && Modulus ==104729,x]
```

```
{{Modulus -> 104729,x -> 38083}}
```

Vérifions que la suite $(x_n)_n$ obtenue en prenant $f(x) = (12x + 3)_{104729}$ a bien pour plus petite période 104728.

```
a=12 ; b= 3;
list4= NestList[g[#,104729]&,0,104728] ;
Length[Union[Drop[list4,1]] ]
```

```
104728
```

Mais les ordinateurs calculent en base 2. Un bon moyen d'accélérer les calculs est donc de se placer dans l'anneau $\mathbb{Z}/2^{16}\mathbb{Z}$. Dans ce cas pour un nombre rationnel compris entre 0 et 1, la division par 2^{16} consistera simplement à déplacer la virgule de 16 places vers la droite. Malheureusement, il n'y a pas d'entiers a tel que $(a)_{2^{16}}$ soit d'ordre $2^{16} - 1$.

1.7 Racine primitive de a, entier non premier.

Les éléments $(a)_n$ de $(\mathbb{Z}/n\mathbb{Z})^*$, inversibles pour la multiplication sont ceux pour lesquels a est premier avec n. En effet si a est premier avec n, d'après l'identité de Bezout, il existe des entiers λ et μ tels que

$$\lambda a + \mu n = 1$$

Par suite, $(\lambda)_n(a)_n = 1_n$ et $(a)_n$ est inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$. Inversement, si $(a)_n$ est inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$, il existe un entier relatif μ tel que $\lambda a - 1 = \mu n$, soit $\lambda a + (-\mu)n = 1$, ce qui prouve que a et n sont premiers entre eux. Par suite le nombre d'éléments du groupe des éléments inversibles de $(\mathbb{Z}/n\mathbb{Z})^*$ est $\Phi(n)$. Soit $(a)_n$ un élément inversible de $(\mathbb{Z}/n\mathbb{Z})^*$, l'ordre k du sous-groupe cyclique engendré par $(a)_n$ est un diviseur de l'ordre

du groupe des éléments inversibles de $(\mathbb{Z}/n\mathbb{Z})^*$. Il existe donc un entier m tel que $k.m = \Phi(n)$, et $a_n^{\Phi(n)} = a_n^{km} = (a_n^k)^m = 1_n^m = 1_n$. On a ainsi démontré un théorème du à Euler.

THEOREME 17 *(Euler, 1760) Si a et n sont premiers entre eux, alors $a^{\Phi(n)} \equiv 1 \bmod(n)$.*

Definition 3 *Soit n un entier supérieur ou égal à 2, et a un entier premier avec n. Si l'ordre de a_n est $\Phi(n)$, on dit que a est une racine primitive de n.*

Exemple 5 *8 n'a pas de racine primitive. En effet* $\Phi(8) = 8(1 - \frac{1}{2}) = 4$ *et* $1^1 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod(8)$
15 n'a pas de racine primitive. En effet $\Phi(15) = 15(1 - \frac{1}{3})(1 - \frac{1}{5}) = 8$ *et* $1^1 \equiv 2^4 \equiv 4^2 \equiv 7^4 \equiv 8^4 \equiv 11^2 \equiv 13^4 \equiv 14^2 \equiv 1 \bmod(15)$
27 a une racine primitive, 2 en est une : $\Phi(27) = 27(1 - \frac{1}{3}) = 18$.

Table[Mod[2^k, 27], {k, 1, 18}]

{2,4,8,16,5,10,20,13,26,25,23,19,11,22,17,7,14,1}

Tout cela semble très chaotique. $\Phi(2^{16}) = 2^{15}(2 - 1) = 2^{15} = 32768$. Par suite le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/2^{16}\mathbb{Z}$ est d'ordre 2^{15}, et n'a pas d'élément d'ordre 2^{16}. Il n'a pas non plus d'élément d'ordre 2^{15} : 2^{15} n'a pas de racine primitive.

THEOREME 18 *Soit $n = 2^k$. Pour $k = 1$ et 2, n a une racine primitive. Pour $k \geq 3$, n n'a pas de racine primitive.*

1 est une racine primitive de 2, tandis que 3 est une racine primitive de 4 : $\Phi(4) = 2^1(2 - 1) = 2$, et $3^2 \equiv 1 \bmod(4)$. Si a est une racine primitive de 2^k, a est impair. Soit $k \geq 3$, $\Phi(k) = 2^{k-1}(2 - 1) = 2^{k-1}$,nous allons prouver que si a est impair, $a^{2^{k-2}} \equiv 1 \bmod(2^k)$. Si $k = 3$, l'exemple ci-dessus a montrer que $8 = 2^3$ n'avait pas de racine primitive. Supposons que pour $3 \leq l$, on ait $a^{2^{l-2}} \equiv 1 \bmod(2^l)$. Il existe alors un entier relatif b tel que $a^{2^{l-2}} = 1 + b2^l$. En élevant au carré les deux membres de cette expression, on obtient

$$a^{2^{l-1}} = (1 + b2^l)^2 = 1 + 2b.2^l + b^2 2^{2l}$$

et $a^{2^{l-1}} \equiv 1 \bmod(2^{l+1})$. La propriété est démontrée pour $n = l + 1$. La proposition est établie par récurrence.
Gauss a démontré en 1801 le théorème suivant :

THEOREME 19 *Soit n un entier supérieur à 1, alors n n'admet de racine primitive que si $n = 2, 4, p^k$ ou $2p^k$, où p est un nombre premier impair.*

Dans le cas où $n = 2^k$ avec $k \geq 3$, tout entier impair a, vérifie $a^{2^{l-2}} \equiv 1 \bmod(2^l)$,comme nous l'avons vu dans la démonstration du théorème . Pour $a = 3$, on vérifie que 3 est d'ordre 2^{k-2}, dans le groupe multiplicatif de $\mathbb{Z}/2^k\mathbb{Z}$. En particulier vérifions à l'aide de Mathematica que 3 est d'ordre 2^{14} dans le groupe $\mathbb{Z}/2^{16}\mathbb{Z}$.

list5 = Table[Mod[3^k, 2^{16}], {k, 2^{14}}];

2^{14}

Length[Union[list5]])

16384

16384

On a fait calculer la liste des puissances 3^k de 3 dans $\mathbb{Z}/2^{16}\mathbb{Z}$, pour k compris entre 1 et 2^{14}, puis on supprime les éventuelles répétitions dans cette liste en lui appliquant la fonction Union. On remarque qu'il n'y en a pas puisque cette liste a bien 2^{14} = 16 384 éléments. 3 est bien d'ordre2^{14} dans $\mathbb{Z}/2^{16}\mathbb{Z}$.

On peut donc construire la suite $(x_n)_n$ d'éléments de $\mathbb{Z}/2^{16}\mathbb{Z}$ en posant $x_0 = s$ et $x_n = f(x_{n-1})$ où $f(x) = ax + b$ en prenant $a = 3$ et par exemple $b = 1$. Alors $s = 0$ n'est pas un point fixe. Calculons les 100 premiers termes de cette liste.

a = 3 ;

b = 1; list6 = NestList[g[#, 2^{16}]&, 0, 99]

{0,1,4,13,40,121,364,1093,3280,9841,29524,23037,3576,10729,32188,
31029,27552,17121,51364,23021,3528,10585,31756,29733,23664,5457,
16372,49117,16280,48841,15452,46357,8000,24001,6468,19405,58216,
43577,65196,64517,62480,56369,38036,48573,14648,43945,764,2293,
6880,20641,61924,54701,33032,33561,35148,39909,54192,31505,28980,
21405,64216,61577,53660,29909,24192,7041,21124,63373,59048,46073,
7148,21445,64336,61937,54740,33149,33912,36201,43068,63669,59936,
48737,15140,45421,5192,15577,46732,9125,27376,16593,49780,18269,
54808,33353,34524,38037,48576,14657,43972,845}

On en déduit 100 nombres aléatoires compris entre 0 et 1.

list7 = list6/2^{16} // N

{0,0.0000152588,0.0000610352,0.000198364,0.000610352,0.00184631,
0.0055542,0.0166779,0.0500488,0.150162,0.4505,0.351517,0.0545654,
0.163712,0.49115,0.473465,0.42041,0.261246,0.783752,0.351273,
0.053833,0.161514,0.484558,0.45369,0.361084,0.0832672,0.249817,
0.749466,0.248413,0.745255,0.235779,0.707352,0.12207,0.366226,
0.0986938,0.296097,0.888306,0.664932,0.994812,0.984451,0.953369,
0.860123,0.580383,0.741165,0.223511,0.670547,0.0116577,0.0349884,
0.10498,0.314957,0.944885,0.834671,0.504028,0.5121,0.536316,
0.608963,0.826904,0.480728,0.4422,0.326614,0.979858,0.93959,
0.818787,0.456375,0.369141,0.107437,0.322327,0.966995,0.901001,
0.703018,0.10907,0.327225,0.981689,0.945084,0.835266,0.505814,
0.517456,0.552383,0.657166,0.971512,0.914551,0.743668,0.231018,
0.693069,0.0792236,0.237686,0.713074,0.139236,0.417725,0.253189,
0.759583,0.278763,0.836304,0.508926,0.526794,0.580399,0.741211,
0.223648,0.670959,0.0128937}

Vérifions que ces nombres sont biens répartis selon une loi uniforme. Pour cela, on les regroupe en classes d'égale amplitude, à savoir 0,1 dans l'intervalle[0,1].Puis on représente les effectifs de ces classes par un diagramme en bâtons.

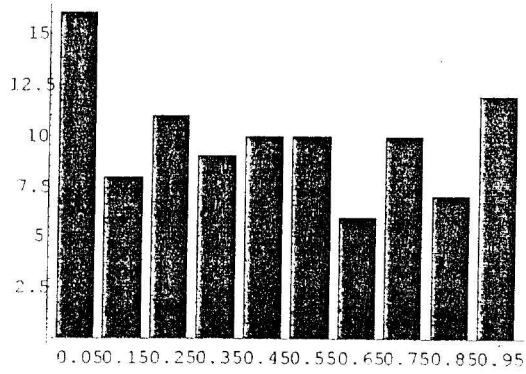
```
<<Statistics`DataManipulation`
list8=BinCounts[list7,{0,1,0.1}]
{16,8,11,9,10,10,6,10,7,12}
```

On dénombre les effectifs de chacune des classes par la fonction BinCounts, du "package" Statistics`DataManipulation`, qu'il faut préalablement charger. On calcule les centres des classes précédentes.

```
centres=Table[0.05+k 0.1, {k,0,9}]
{0.05,0.15,0.25,0.35,0.45,0.55,0.65,0.75,0.85,0.95}
```

On représente enfin par un diagramme en bâtons les effectifs de la série list7, une fois classée.

```
<<Graphics`Graphics`
BarChart[Transpose[{list8,centres}]]
```



Remarque 4 *Pour construire un diagramme en bâtons, il nous faut disposer de la fonction BarChart, qui se trouve dans le "package" Graphics`Graphics`, qu'il faut donc charger préalablement. Transpose vise à constituer une liste de couples dont le premier élément est l'effectif de la classe et le second le centre de cette classe.*

La première classe a un effectif nettement plus élevé que celui des autres classes, cela s'explique sans doute par la trop petite valeur donnée à a, à savoir 3. Il faut donc prendre une valeur de a plus centrale. Essayons $a = 25733$. Il nous faut d'abord trouver l'ordre de $(25733)_{2^{14}}$ dans $\mathbb{Z}/2^{16}\mathbb{Z}$.

```
Mod[25733^2^14, 2^16]
1
```

L'ordre de 25733 est donc un diviseur de 2^{14}. Les diviseurs de 2^{14} sont les nombres de la forme 2^k avec $0 \leq k \leq 14$. Calculons donc $(25733^{2^k})_{2^{16}}$ pour $1 \leq k \leq 14$.

```
Table[Mod[25733^2^k, 2^16], {k, 1, 14}]
{11545,52337,18913,6081,16257,48897,32257,64513,63489,61441,
```

57345,49153,32769,1}

$(25733)_{2^{14}}$ est bien d'ordre 2^{14} dans le groupe multiplicatif de $\mathbb{Z}/2^{16}\mathbb{Z}$. On prend a =$(25733)_{2^{14}}$, $b = (13849)_{2^{14}}$, $s = 0$.

```
a = 25733;
b = 13849;
list9 = NestList[g[#, 2^16]&, 0, 99]
```

{0,13849,5398,49799,572,53061,55538,29651,52920,31665,40206,
18015,57716,42845,32106,50731,63088,65097,54790,48951,2476,
27765,17122,15747,22312,7649,40958,36111,23268,32397,2394,
14811,53472,14969,56054,4071,46364,15781,45266,6963,17304,
46097,26350,42943,63572,2493,6474,16779,36688,60073,9190,
46231,1164,17109,8898,3299,37896,15937,61918,38511,47556,
18669,44346,56635,12736,3801,45270,44359,63484,31749,39090,
4755,18552,48241,16590,22815,40756,15389,50474,3307,47152,
42761,33222,63991,36716,59701,4770,11331,24808,11937,21438,
61391,43172,58189,24858,53403,8864,45881,38582,39591}

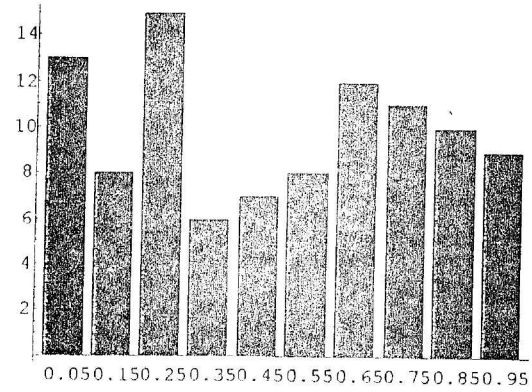
```
list10 = list9/2^16 // N
```

{0,0.211319,0.0823669,0.759872,0.00872803,0.809647,0.847443,
0.452438,0.807495,0.48317,0.613495,0.274887,0.880676,0.653763,
0.489899,0.774094,0.962646,0.993301,0.836029,0.746933,
0.0377808,0.42366,0.261261,0.24028,0.340454,0.116714,0.624969,
0.55101,0.355042,0.494339,0.0365295,0.225998,0.815918,0.228409,
0.855316,0.0621185,0.707458,0.240799,0.690704,0.106247,
0.264038,0.703384,0.402069,0.655258,0.970032,0.0380402,
0.0987854,0.256027,0.559814,0.916641,0.140228,0.705429,
0.0177612,0.261063,0.135773,0.0503387,0.578247,0.243179,
0.944794,0.587631,0.725647,0.284866,0.676666,0.864182,0.194336,
0.0579987,0.690765,0.676865,0.968689,0.484451,0.596466,
0.0725555,0.283081,0.736099,0.253143,0.348129,0.621887,
0.234818,0.770172,0.0504608,0.719482,0.652481,0.506927,
0.976425,0.560242,0.910965,0.0727844,0.172897,0.37854,0.182144,
0.327118,0.936752,0.658752,0.887894,0.379303,0.814865,0.135254,
0.700089,0.588715,0.604111}

```
list11 = BinCounts[list10, {0,1,0.1}]
```

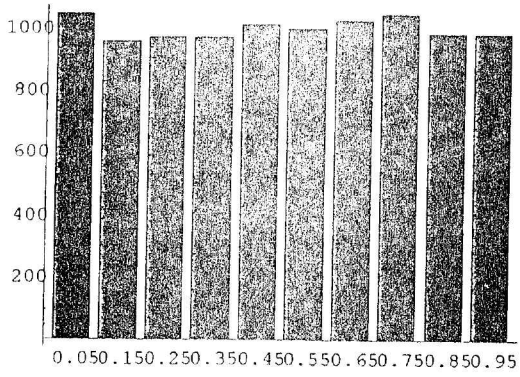
{13,8,15,6,7,8,12,11,10,9}

```
BarChart[Transpose[{list11,centres}]]
```



L'échantillon n'est pas assez grand pour juger. Reprenons les calculs avec un échatillon de taille 10000, sans afficher les résultats intermédiaires.

```
list12 = NestList[g[#, 2^16]&, 0, 9999]
list13 = list12 /2^16 // N ;
list14 = BinCounts[list13, {0, 1, 0.1}] ;
BarChart[Transpose[{list14, centres}]]
```



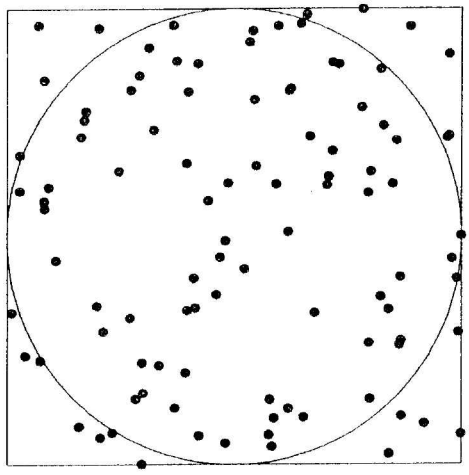
Pour cet échantillon la répartition dans les différentes classes semble suivre une loi uniforme.

1.8 Calcul d'une valeur approchée de π.

Maintenant que nous faisons confiance aux générateurs de nombres aléatoires, utilisons les pour calculer une valeur approchée de π.
On dessine sur le sol un disque de rayon 1, inscrit dans un carré de coté de longueur 2. Il pleut. En faisant l'hypothèse que les gouttes de pluie se répartissent uniformément sur la surface du carré, l'aire du cercle étant égale à π, et celle du carré à 4, la probabilité qu'une goutte d'eau tombe à l'intérieur du disque est égale à $\frac{\pi}{4}$.
Faisons une représentation graphique de cette expérience. Chaque goutte de pluie sera

représentée par un point rouge, le cercle est dessiné en vert, et les bords du carré en noir.

```
g1 = Graphics[
{RGBColor[1,0,0],AbsolutePointSize[4],
Point /@ Table[{Random[Real,{0,1}],Random[Real,{0,1}]},{100}]},
{AspectRatio -> Automatic}]
g2=Graphics[{RGBColor[0,1,0],Circle[{0.5,0.5},0.5] },{
AspectRatio -> Automatic}]
g3 = Graphics[Line[{{0,0},{1,0},{1,1},{0,1},{0,0}}]]
Show[g1, g2, g3]
```



On génère une liste de couples de nombres aléatoires. Puis on transforme chacun de ces couples de réels en un point graphique par la primitive graphique Point. On applique point à chacun des éléments de la liste précédente par la fonction Map, qui apparaît ici sous sa forme infixe /@. La fonction Graphics rassemble alors tous ces objets en un seul graphique g1. L'option AspectRatio -> Automatic oblige Mathematica à utiliser la même échelle sur les deux axes. Les directives graphiques, placées en tete, s'imposent aux objets graphiques qui suivent. Ce sont ici RGBColor[1,0,0] et AbsolutePointSize[4] qui imposent la couleur rouge et la taille 4 pour les points. On construit de même un cercle et une ligne brisée pour représenter le carré. Enfin la fonction Show permet d'afficher simultanément les trois graphiques ainsi consultés.

Qu'obtient-on pour vingt mille gouttes d'eau ?

```
list15 =
Table[{Random[Real, {0, 1}], Random[Real, {0, 1}]}, {20000}];
h1[x_, y_] :=(x - \ 1/2)^2 + (y - 1/2)^2
h2[u_List] := Apply[h1, u]
h3[u_List] := If[h2[u] <= 1/4,1, 0]
list16 = Map[h3, list15] ;
list17 = Select[list16, (# == 1)&] ;
4 (Length[list17]/Length[list16]) // N
```

3.1414

Que pensez-vous de ce résultat ?

2. Les bases de Gröbner

2.1 Une équation du troisième degré à coefficients complexes.

Pour détecter les méthodes de calcul utilisées par Mathematica, proposons-nous de résoudre l'équation du troisième degré à coefficients complexes :

$$z^3 - (2+3i)z^2 + 10iz + 6 - 8i = 0$$

```
Solve[z^3 - (2 + 3 I)z^2 + 10 I z + 6 - 8 I == 0,z]
{{z → -I+3 I},{z → 1+I},{z → 2-I}}
```

Mathematica a réussi. Vérifions, en lui faisant développer le polynôme $(z+1-3i)(z-1-i)(z-2+i)$

```
Expand[(z + 1 - 3 I)(z - 1 - I)(z - 2 + I)]
(6 - 8 I) + 10 I z - (2 + 3 I) z^2 + z^3
```

Cherchons à résoudre notre équation par la méthode traditionnelle, celle de Cardan. On fait d'abord le changement d'inconnue $z = x + \frac{2+3i}{3}$ pour faire disparaître le terme en z^2.

```
p[x_] = Expand[z^3 - (2 + 3 I)z^2 + 10 I z + 6 - 8 I /. z -> x + 1/3 (2 + 3 I)]
(-16/27 - 2 I) + (5/3 + 6 I) x + x^3
```

Mathematica sait encore résoudre cette nouvelle équation d'inconnue x.

```
Solve[p[x] == 0, x]
{{x → -5/3 + 2 I}, {x → 1/3}, {x → 4/3 - 2 I}}
```

On pose ensuite $x = u + v$

```
q[u_,v_] = Expand[p[x] /. x -> u + v]
(-16/27 - 2 I) + (5/3 + 6 I) u + u^3 + (5/3 + 6 I) v + 3 u^2 v + 3u v^2 + v^3
```

Cette dernière expression se réécrit :

$$u^3 + v^3 + (3uv + \frac{5}{3} + 6i)(u+v) - \frac{16}{27} - 2i = 0$$

On exige alors que $3uv + 5/3 + 6i = 0$, ce qui conduit à :

$$u^3 + v^3 = \frac{16}{27} + 2i$$

et à

$$u^3 v^3 = (-\frac{5}{9} - 2i)^3$$

Posons $a = -\frac{5}{9} - 2i$ et faisons calculer a^3 par Mathematica.

```
a = (-5/9 - 2 I)^3
4735/729 + 166/27 I
```

Si $U = u^3$ et $V = v^3$, U et V vérifient

$$U + V = \frac{16}{27} + 2i,\ UV = a$$

donc U et V sont solutions de l'équation d'inconnue x

$$x^2 - (\frac{16}{27} + 2i)x + a = 0$$

Pour la résoudre on met en oeuvre la transformation des lycée et collèges, ce qui revient à prendre comme nouvelle inconnue y, définie par $y = x - \frac{8}{27} + i$.

```
q[y] = Expand[x^2 -(16/27 + 2 I) x + a /. x -> y + 8/27 + I]
```

$\frac{200}{27} + \frac{50}{9}\ I + y^2$

On doit résoudre l'équation q[y] = 0, ce qui revient à chercher la racine carrée d'un nombre complexe. On pose y = r + i t où r et t sont réels.

```
m[r_,t_] := Expand[q[y] /. y -> r + I t]
m[r,t]
```

$(\frac{200}{27} + \frac{50}{9}\ I) + r^2 + 2\ I\ r\ t - t^2$

Pour indiquer que r et t sont des réels, il faut charger le "package" Algebra'ReIm' et indiquer que les parties imaginaires de r et t sont nulles.

On recherche ensuite la partie réelle et la partie imaginaire de m[r,t].

```
<<Algebra'ReIm'
Im[r] ^= 0
Im[t] ^= 0
Re[m[r,t]]
Im[m[r,t]]
```

0

0

$\frac{200}{27} + r^2 - t^2$

$\frac{50}{9} + 2\ r\ t$

Calculons, d'après la dernière équation, la valeur que doit prendre r^2t^2.

```
(-50/18)^2
```

$\frac{625}{81}$

On en déduit que R = r^2 et T = - t^2 sont solution de l'équation d'inconnue x

$$x^2 - \frac{200}{27}x - \frac{625}{81} = 0$$

Demandons à Mathematica la résolution de cette équation.

```
Solve[x^2 + 200/27 x - 625/81 == 0, x]
```

$\{\{x \to -\frac{25}{3}\}, \{x \to \frac{25}{27}\}\}$

Par suite $r = \sqrt{\frac{25}{27}}$ ou $r = -\sqrt{\frac{25}{27}}$

$t = \sqrt{\frac{25}{3}}$ ou $t = -\sqrt{\frac{25}{3}}$.

Mais comme r t < 0, r et t sont de signes opposés et les racines carrées de -200/27 - 50/9 i

sont

$$\sqrt{\frac{25}{27}} - i\sqrt{\frac{25}{3}}, \text{ et } -\sqrt{\frac{25}{27}} + i\sqrt{\frac{25}{3}}$$

Par suite U et V s'obtiennent en ajoutant $8/27 + i$ à ces valeurs.

U = Simplify[8/27 + I + Sqrt[25/27] - I Sqrt[25/3]]

V = Simplify[8/27 + I - Sqrt[25/27] + I Sqrt[25/3]]

$\frac{8}{27} + \mathrm{I} + \frac{\frac{5}{3} - 5\,\mathrm{I}}{\sqrt{3}}$

$\frac{8}{27} + \mathrm{I} - \frac{\frac{5}{3} - 5\,\mathrm{I}}{\sqrt{3}}$

Ce sont ces nombres dont il faut maintenant trouver les racines cubiques.

racine cubique = Solve[u^3 == U, u]

$\{\{u \to \frac{1}{3}\,\mathrm{I}\,\left((-27 + 8\,\mathrm{I}) + (45 + 15\,\mathrm{I})\sqrt{3}\right)^{1/3}\},$

$\{u \to -\frac{1}{3}(-1)^{1/6}\,\left((-27 + 8\,\mathrm{I}) + (45 + 15\,\mathrm{I})\sqrt{3}\right)^{1/3}\},$

$\{u \to -\frac{1}{3}(-1)^{5/6}\,\left((-27 + 8\,\mathrm{I}) + (45 + 15\,\mathrm{I})\sqrt{3}\right)^{1/3}\}\}$

Choisissons la plus simple d'entre elles.

u1 = u /. racinecubique[[1]]

$\frac{1}{3}\,\mathrm{I}\,\left((-27 + 8\,\mathrm{I}) + (45 + 15\,\mathrm{I})\sqrt{3}\right)^{1/3}$

Prenons la valeur de v correspondante.

v1 = (-5/9 - 2 I)/u1

$\frac{6 - \frac{5\,\mathrm{I}}{3}}{\left((-27 + 8\,\mathrm{I}) + (45 + 15\,\mathrm{I})\sqrt{3}\right)^{1/3}}$

ce qui nous fournit la solution $x1 = u1 + v1$ de l'équation $p(x) = 0$.

x1 = u1 + v1

$\frac{6 - \frac{5\,\mathrm{I}}{3}}{\left((-27 + 8\,\mathrm{I}) + (45 + 15\,\mathrm{I})\sqrt{3}\right)^{1/3}} + \frac{1}{3}\,\mathrm{I}\,\left((-27 + 8\,\mathrm{I}) + (45 + 15\,\mathrm{I})\sqrt{3}\right)^{1/3}$

Demandons à Mathematica de nous fournir une valeur approchée de ce résultat.

N[x1]

1.66667 - 2. I

Mathematica avait trouvé 4/3 - 2 I, quand on lui a dmandé de résoudre l'équation $p(x) = 0$.

!

Les autres solutions sont $x2 = u1j + (-5/9 - 2i)/(u1j)$ et $x3 = u1j^2 + (-5/9 - 2i)u1j^2$ où $j = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Faisons les calculer par Mathematica et demandons lui des valeurs numériques approchées.

j = - 1/2 + I (Sqrt[3]/2)

x2 = u1 j + (-5/9 - 2 I)/(u1 j)

x3 = u1 j^2 + (-5/9 - 2 I)/(u1 j^2)

N[x2]

N[x3]

$-\frac{1}{2} + \frac{\sqrt{3}}{2}\,\mathrm{I}$

$\frac{6 - \frac{5\,\mathrm{I}}{3}}{(-\frac{1}{2} + \frac{\sqrt{3}}{2})\left((-27 + 8\,\mathrm{I}) + (45 + 15\,\mathrm{I})\sqrt{3}\right)^{1/3}} + \frac{1}{3}\,\mathrm{I}\,\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}\right)\left((-27 + 8\,\mathrm{I}) + (45 + 15\,\mathrm{I})\sqrt{3}\right)^{1/3}$

$$\frac{6-\frac{5\,I}{3}}{(-\frac{1}{2}+\frac{\sqrt{3}}{2})^2\left((-27+8\,I)+(45+15\,I)\sqrt{3}\right)^{1/3}}+\frac{1}{3}\,I\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}\right)^2\left((-27+8\,I)+(45+15\,I)\sqrt{3}\right)^{1/3}$$

0.33333333333333 + 4.4408920985006 $\times 10^{-16}$ I

1.33333333333333 -2. I

Mathematica avait trouvé - 5/3 + 2 i, et 1/3 !
Mais il n'a probablement pas utilisé la méthode de Cardan.
Posons $z = x + iy$ où x et y sont des réels.

```
r[x_,y_] := Expand[z^3 - (2 + 3 I)z^2 + 10 I z + 6 - 8 I /. z -> x + I y]
r[x,y]
```

$(6 - 8\,I) + 10\,I\,x - (2 + 3\,I)\,x^2 + x^3 - 10\,y + (6 - 4\,I)\,x\,y + 3\,I\,x^2\,y + (2 + 3\,I)\,y^2 - 3\,x\,y^2 - I\,y^3$

Déclarons que les variables x et y sont bien réelles

```
Im[x] ^= 0
Im[y] ^= 0
Re[r[x,y]]
Im[r[x,y]]
```

0

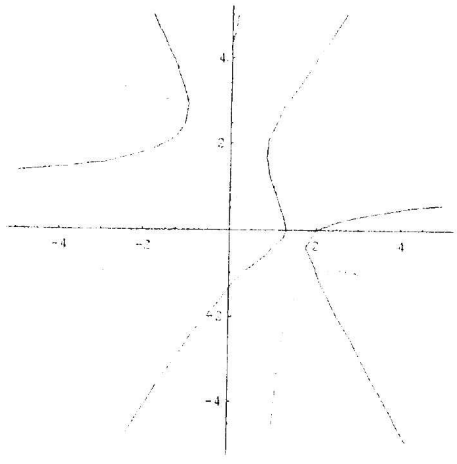
0

$6 - 2\,x^2 + x^3 - 10\,y + 6\,x\,y + 2\,y^2 - 3\,x\,y^2$

$-8 + 10\,x - 3\,x^2 - 4\,x\,y + 3\,x^2\,y + 3\,y^2 - y^3$

Représentons les équations obtenues en annulant les parties réelles et imaginaires du premier membre de l'équation étudiée.

```
ImplicitPlot[{Re[r[x,y]] == 0, Im[r[x,y]] == 0}, {x,-5,5}, {y,-5,5},
PlotStyle -> {RGBColor[1,0,0], RGBColor[0,0,1]}]
```



On voit que les deux courbes se coupent en trois points dont les coordonnées correspondent aux solutions fournies par Mathematica, pour l'équation initiale. Pour résoudre le système

d'équation

$$\begin{cases} \mathcal{R}(r(x,y)) &= 0 \\ \mathcal{I}(r(x,y)) &= 0 \end{cases}$$

Mathematica a probablement utilisé une base de Gröbner de l'idéal de $\mathbb{R}[X,Y]$ engendré par les polynômes qui constituent les premiers membres des équations que l'on veut résoudre.

```
basedeGroebner = GroebnerBasis[ {Re[r[x,y]], Im[r[x,y]]},{x,y}]
{195 - 341 y + 872 y^2 - 1160 y^3 + 117 y^4 + 949 y^5 - 1040 y^6 + 536 y^7 - 144 y^8 + 16 y^9,
-37984485 + 65667600 x - 148095512 y + 203448096 y^2 - 22391096 y^3 - 175942235 y^4
+ 183544568 y^5 - 86289288 y^6 6 + 19775840 y^7 - 1733488 y^8}
```

Mathematica sait résoudre ce système d'équations.

```
Solve[{Re[r[x,y]] == 0, Im[r[x,y]] == 0},{x,y}]
{{x → -1, y → 3}, {x → -I, y → 2 - I}, { x → I, y → 2 + I}, {x → 1/2 - 2 I, y → 1 - 3I/2},
{x → 1/2 + 2 I, y → 1 + 3I/2}, {x → 1, y → 1},{ x → 3/2 - I, y → -I/2}, {x → 3/2 + I, y → I/2},
{x → 2, y → -1}}
```

Il sait calculer les racines du premier polynôme à la seule indéterminée y de la base de Gröbner obtenue.

```
Solve[basedeGroebner[[1]] == 0,y]
{{y → -1}, {y → - 1/2}, {y → I/2}, { y → 1}, {y → 1 - 3I/2}, { y → 1 + 3I/2}, {y → 2 - I},
{y → 2 + I}, { y → 3}}
```

Cette équation admet trois solutions réelles. Le deuxième polynôme de la base de Gröbner est du premier degré en x. Si on porte les valeurs réelles de y que l'on vient d'obtenir, on aura les valeurs correspondantes de x.

```
basedeGroebner[[2]] /. y -> -1
-131335200 + 65667600 x
Solve[% == 0,x]
{{x → 2}}
basedeGroebner[[2]] /. y -> 1
Solve[% == 0,x]
-65667600 + 65667600 x
{{x → 1}}
basedeGroebner[[2]] /. y -> 3
Solve[% == 0,x]
65667600 + 65667600 x
{{x → -1}}
```

On retrouve bien les solutions de l'équation proposée. Pour expliquer ce qui s'est passé il nous faut donner quelques indications sur les bases de Gröbner. En effet la théorie des bases de Gröbner est à la base de nombreux algorithmes symboliques pour la manipulation de polynômes de plusieurs variables et en particulier Mathematica s'en sert dans les fonctions Solve, AlgebraicRules et Eleminate. Nous allons montrer sur plusieurs exemples - les systèmes d'équations polynomiales, l'élimination de paramètres, la démonstration d'un théorème de géométrie - comment on peut utiliser ces bases de Gröbner. Pour la théorie

algébrique nous renvoyons aux articles et aux manuels cités dans la bibliographie.

2.2 Systèmes d'équations polynomiales.

La résolution des systèmes d'équations polynômiales est une bonne introduction aux bases de Gröbner.. La fonction Solve de Mathematica en tire partie. La technique de résolution qui est à la base de la fonction Solve peut-être considérée comme une extension de la *méthode de Gauss* pour la résolution des systèmes d'équations linéaires, méthode consistant à transformer ces systèmes en systèmes triangulaires à l'aide de combinaisons linéaires de leurs équations. Ainsi partant du système d'équations linéaires

$$\begin{cases} 2x + 3y &= 1 \\ 4x - 2y &= 10 \end{cases}$$

on obtient le système

$$\begin{cases} 2x + 3y &= 1 \\ -8y &= 8 \end{cases}$$

en multipliant la première équation par 2 et en la retranchant à la deuxième. La deuxième équation ne comporte plus que la seule inconnue y, et donne $y = -1$. En portant cette valeur de y dans la première équation on obtient la valeur de x, à savoir $x = 2$.
Considérons maintenant un système d'équations polynomiales

$$\begin{cases} x - y^2 + 2 &= 0 \\ x^2 - y^2 - 1 &= 0 \end{cases}$$

Proposons nous d'éliminer la variable x dans la deuxième équation. On commence par multiplier la première équation par x et on la retranche à la seconde :

$$\begin{cases} x - y^2 + 2 &= 0 \\ xy^2 - 2x - y^2 - 1 &= 0 \end{cases}$$

ce qui a permis d'éliminer le terme en x^2 de la seconde équation. Pour éliminer le terme en xy^2 on multiplie ma première équation par y^2 et on la retranche à la seconde :

$$\begin{cases} x - y^2 + 2 &= 0 \\ -2x - y^4 - 3y^2 - 1 &= 0 \end{cases}$$

Pour éliminer le terme en x on multiplie la première équation par 2 et on l'ajoute à la seconde :

$$\begin{cases} x - y^2 + 2 &= 0 \\ y^4 - 3y^2 + 3 &= 0 \end{cases}$$

Nous avons ainsi obtenue une équation qui ne comporte que la seule variable y. Après avoir déterminé ses quatre solutions, et en les injectant dans la première équation on obtient les valeurs correspondantes de x. Le procédé d'élimination utilisé ressemble à la *division euclidienne* des polynômes.. Par exemple posons la division du polynôme $3x^2 - 2x + 5$

par le polynôme $x - 1$.

$$\begin{array}{r|l} 3x^2 - 2x + 5 & x - 1 \\ \cline{2-2} -3x^2 + 3x & 3x + 1 \\ \cline{1-1} x + 5 & \\ -x + 1 & \\ \cline{1-1} 6 & \end{array}$$

Le procédé utilisé dans cette division consiste à multiplier le diviseur par le monôme approprié pour éliminer le terme de plus haut degré du dividende et à répéter l'opération jusqu'à l'obtention d'un polynôme de degré inférieur à celui du diviseur. Pour voir que c'est bien cette même méthode qui a été appliquée dans le cas de la résolution de notre système d'équations linéaires et dans le cas de notre système de deux équations polynomiales, il nous faut d'abord définir un ordre dans l'ensemble des termes.

2.3 Ordre des termes.

Pour un polynôme $P(x)$ en la seule indéterminée x, le terme de rang le plus élevé est le terme de plus haut degré en x. Dans le cas d'un polynôme à plusieurs indéterminées il nous faut ordonner les termes. Nous utiliserons indifféremment le mot *monôme* ou le mot *terme*. Pour le monôme $-7x^3y^2z^5$ le *coefficient* est le nombre -7 et le *produit des puissances* $x^3y^2z^5$. Quel est le terme de rang le plus élevé dans $x^2 - y^2 - 1$? Nous utiliserons la règle selon laquelle de deux produits de puissances $x^a y^b$, le plus grand est celui pour lequel l'exposant a de x est le plus grand. Si les exposant de x sont les mêmes c'est l'exposant de y qui les distinguera. Pour que la règle s'applique dans tous les cas on considère des exposants nuls : $y^4 = x^0y^4$. On peut alors définir le terme de rang le plus élevé d'un polynôme comme étant celui qui contient le produit des puissances le plus grand. Notons que le polynôme nul n'a pas de termes et par conséquent n'a pas de terme de rang le plus élevé. Les procédés d'élimination utilisés à la fois dans le cas du système d'équations linéaires et dans le cas du systèmes d'équations polynomiales vus plus haut peuvent être décrits par "multiplier la première équation par un monôme et la soustraire de la seconde équation pour éliminer le terme de rang le plus élevé de la seconde équation". C'est bien la méthode utilisée dans les divisions euclidiennes.
Cette méthode pour définir le terme de rang le plus élevé dans un polynôme à plusieurs indéterminées est un exemple d'ordre dans les produits de puissances. Nous avons accordé une priorité aux exposants de x. On aurait pu inverser l'ordre des priorités entre les exposants de x et de y. Si on examine d'abord l'exposant de y on obtient un système triangulaire en une seule étape, dans l'exemple du système d'équations polynomiales considéré plus haut. En effet en retranchant à la seconde équation la première, on obtient le système :

$$\begin{cases} x - y^2 + 2 &= 0 \\ x^2 - x - 3 &= 0 \end{cases}$$

Le troisième argument de la fonction Solve, dans Mathematica, permet de contrôler l'ordre utilisé. *L'ordre lexicographique* sur un ensemble $x_1, x_2, ..., x_n$ de variables, est celui pour lequel on examine d'abord l'exposant de x_1, puis celui de x_2, et ainsi de suite. L'ordre lexicographique est utilisé pour la résolution des systèmes d'équations polynomiales, mais

d'autres ordres sont utilisés dans d'autres circonstances. Un autre ordre assez communément employé est l'*ordre lexicographique par degré*. On ordonne d'abord les produits de puissances suivant leur degré total($x^2y^3z^4$ est de degré total $2+3+4=9$) et les exaequo sont départagés par l'ordre lexicographique.
Tous les ordres que l'on peut définir sur les produits de puissances ne conviennent pas. Il faut impérativement que le terme de rang le plus élevé d'un polynôme produit de deux autres polynômes soit le produit des termes de rang le plus élevé de ces deux polynômes et que les termes constants soient classés en dernier. La fonction GroebnerBasisGroebnerBasis de Mathematica propose en option, pour l'ordre des monômes, soit l'*ordre lexicographique* (Lexicographic), soit l'*ordre lexicographique par degré* (DegreeLexicographic), soit l'*ordre lexicographique inverse par degré* (DegreeReverseLexicographic).

2.4 Anneaux et idéaux.

Il est bien clair que l'exemple du système d'équations polynomiales dont nous nous sommes servis est particulièrement simple. En général on travaille dans un anneau $\mathbb{Q}[x, y, z, ..., u]$ de polynômes en les indéterminées $x, y, z, ..., u$ à coefficients dans le corps des rationnels et on considère des idéaux de cet anneau. Un idéal I est une partie non vide de l'anneau stable pour l'addition et telle qu'en multipliant un élément de I par un élément de l'anneau on obtienne un élément de I. Par exemple l'ensemble J des polynômes $p(x, y)$ de l'anneau $\mathbb{Q}[x, y]$ pour lesquels $p(a, b) = 0$, si (a, b) est un point du cercle unité (c'est à dire vérifie $a^2 + b^2 = 1$) est un idéal de $\mathbb{Q}[x, y]$. Par exemple si $p(x, y)$ est un polynôme quelconque et $q(x, y)$ un élément de J, alors $pq(a, b) = p(a, b)q(a, b) = p(a, b) \cdot 0 = 0$ pour tout couple (a, b) du cercle unité, ce qui prouve que $pq \in J$. On démontre de même que $p(x, y) + q(x, y) \in J$, si $p(x, y) \in J$ et $q(x, y) \in J$. Le polynôme $p_0(x, y) = x^2 + y^2 - 1$ est évidemment un élément de J. En fait tout polynôme de J est un multiple de $p_0(x, y)$
Voyons comment on peut démontrer cette assertion par une division euclidienne. Soit $p(x, y)$ un élément de J. En utilisant l'ordre lexicographique, avec x comme première variable, on peut diviser $p(x, y)$ par p_0 : $p(x, y) = p_0(x, y)q(x, y) + xf(y) + g(y)$. ($\mathbb{Q}[x, y] \cong \mathbb{Q}[y][x]$ et les polynômes de $\mathbb{Q}[x, y]$ peuvent être considérés comme des polynômes à coefficients dans $\mathbb{Q}[y]$ en l'indéterminée x, d'où la forme du résultat de la division puisque p_0 et de degré 2 en x). Si (a, b) est un point du cercle unité, il en est de même de $(-a, b)$. Ainsi si a est non nul, on a à la fois $af(b) + g(b) = 0$ et $-af(b) + g(b) = 0$, et par suite $f(b) = g(b) = 0$. Comme ces relations sont vérifiés quel que soit le réel b, les polynômes f et g sont nuls, ce qui prouve que $p(x, y) = p_0(x, y)q(x, y)$.
Les idéaux contiennent évidemment une infinité de polynômes et pour les nécessités des calculs on a besoin d'une représentation finie. Heureusement, un théorème de Hilbert précise que les idéaux d'un anneau de polynômes admettent un *base* finie, c'est à dire qu'il existe une suite finie $b_1, b_2, ..., b_n$ de polynômes tels que tout polynôme p de l'idéal peut s'écrire sous la forme

$$p = p_1b_1 + p_2b_2 + ... + p_nb_n$$

où $p_1, p_2, ..., p_n$ sont aussi des polynômes... L'utilisation du mot base dans ce contexte est en contradiction avec son utilisation en algèbre linéaire, où l'on parlerait plutôt d'un système de générateurs.

Ainsi le polynôme $p_0(x, y) = x^2 + y^2 - 1$ est une base de l'idéal J des polynômes qui s'annulent sur le cercle unité. Toute suite $b_1, b_2, ..., b_n$ de polynômes est la base de l'idéal I formé par les polynômes p de la forme

$$p = p_1 b_1 + p_2 b_2 + ... + p_n b_n$$

où les polynômes p_i parcourent l'anneau des polynômes.. On dit que I est l'idéal engendré par $b_1, b_2, ..., b_n$.

Revenons à notre système d'équations polynomiales. Posons $b_1 = x - y^2 + 2$ et $b_2 = x^2 - y^2 - 1$ Soit I l'idéal engendré par les polynômes b_1 et b_2 dans $\mathbb{Q}[x, y]$. Alors tout polynôme $p(x, y)$ de I s'annule sur l'ensemble de points sur lesquels les polynômes b_1 et b_2 s'annulent, c'est à dire sur les solutions du système. La raison pour laquelle le système triangulaire a exactement les mêmes solutions que le système initial est que les polynômes $x - y^2 - 1$ et $y^4 - 5y^2 + 3$ constituent aussi une base de I. Ces polynômes constituent une base de Gröbner de I, et on les a obtenu en utilisant l'ordre lexicographique; avec x comme première variable.

Une *base de Gröbner* d'un idéal est, par définition, une base qui possède la propriété de le terme de rang le plus élevé de tout polynôme de l'idéal est divisible par le terme de rang le plus élevé d'un des polynômes de la base. Cette condition équivaut à ce que les polynômes $b_1, b_2, ..., b_n$ de la relation

$$p = p_1 b_1 + p_2 b_2 + ... + p_n b_n$$

peuvent être choisis de telle manière qu'aucun des termes de rang le plus élevé des polynômes $p_i b_i$ n'est plus grand que le terme de rang le plus élevé de p, c'est à dire qu'aucun terme de rang le plus élevé dans la somme ne peut être supprimé. L'algorithme de Buchberger calcule la base de Gröbner d'un idéal, quel que soit l'ordre choisi pour les termes. C'est cet algorithme qui est utilisé par Mathematica, dans sa fonction GroebnerBasis.

Revenons à la résolution des systèmes d'équations polynomiales. Considérons un système n'ayant qu'un nombre fini de solutions. On exclue le cas où une courbe entière est solution. On considère des polynômes à coefficients complexes, et on accepte des solutions complexes. On réécrit les équations de manière à ce que les membres de droite des équations soit nuls et soit I l'idéal engendré par les polynômes formant les membres de gauche des équations. Pour simplifier les notations supposons que l'on opère dans $\mathbb{Q}[x, y, z]$. Comme il n'y a qu'un nombre fini de solutions I doit contenir un polynôme $p(x)$ en la seule indéterminée x, libre par rapport aux indéterminées y et z. De même I contiendra des polynômes $q(y)$ et $r(z)$ en les seules indéterminées y et z. Pour voir ce point, supposons qu'il y ait deux solutions $(1, 2, 3)$ et $(4, 5, 6)$. Alors le polynôme $p(x, y, z) = p(x) = (x - 1)(x - 4)$ s'annule en ces deux points. Mais est-ce que p appartient nécessairement à I? La réponse est non. Mais grâce à un résultat de Hilbert, on sait qu'une puissance de p appartient à l'idéal I, et cette puissance, $p(x)^m$ est encore un polynôme en le seule indéterminée x. Maintenant que nous savons que I contient des polynômes à une seule indéterminée, pour chacune des indéterminées x, y, z, il en résulte qu'une base de Gröbner de I, obtenue en utilisant l'ordre lexicographique sur les termes, doit aussi contenir au moins un polynôme en une seule indéterminée. Supposons que l'on ait choisi l'ordre lexicographique avec z en premier, puis y, puis x, alors un des polynômes de la base de Gröbner doit comporter un

polynôme dont le terme de rang le plus élevé doit diviser le terme de rang le plus élevé de $p(x)$, il est donc de la forme x^m. Mais sous l'ordre lexicographique adopté un polynôme dont le terme de rang le plus élevé est de la forme x^m est indépendant des indéterminées y et z. De la même manière on peut établir que la base de Gröbner doit contenir un polynôme $s(x, y)$ indépendant de z, etc..., ce qui permet d'obtenir un système triangulaire.
En général, il n'est pas évident de déterminer si un ensemble donné de polynômes forme ou non une base de Gröbner. D'abord un polynôme isolé constitue une base de Gröbner de l'idéal qu'il engendre. Ensuite si on peut montrer que les termes de rang les plus élevés de chaque paire de polynômes n'ont aucun facteur commun autre que 1, alors l'ensemble des polynômes forment une base de Gröbner. Le cas des polynômes à une seule variable est un cas particulier. Etant donné un ensemble fini de polynômes de $\mathbb{Q}[x]$ alors une base de Gröbner de l'idéal I qu'ils engendrent est le plus grand commun diviseur de cet ensemble de polynômes... Ainsi tous les idéaux de $\mathbb{Q}[x]$ sont formés des multiples d'un seul polynôme...
Les bases de Gröbner d'un idéal dépendent de l'ordre adopté sur les termes, et il n'y a pas unicité des bases même lorsque l'ordre des termes est fixé. Mais si on ajoute la condition que dans les polynômes de la base aucun terme ne doit être divisible par un terme de rang le plus élevé d'un autre polynôme de la base, alors la base est unique, à la multiplication par une constante près. De telles bases sont appelées des *bases inter-réduites*. Pour des systèmes d'équations linéaires, les bases de Gröbner correspondent aux systèmes triangulaires équivalents et les bases de Gröbner inter-réduites - à condition que les termes de rang les plus élevé soient normalisés à 1 - correspondent à la *forme de Gauss-Jordan* des systèmes linéaires. Cette forme est unique lorsque l'ordre des variables est fixé.
La fonction GroebnerBasis de Mathematica associe à toute liste de polynômes une base de Gröbner inter-réduite. Le second argument de la fonction permet de préciser dans quel ordre doivent être considérées les variables. Des options permettent de choisir entre l'ordre lexicographique, l'ordre lexicographique par degré et l'ordre lexicographique inverse par degré. Par défaut c'est l'ordre lexicographique qui est choisi. Par exemple :

```
GroebnerBasis[{x - y^2 + 2, x^2 - y^2 - 1},{x,y}]
```

$\{3 - 5\,y^2+y^4, 2 + x - y^2\}$

qui est la forme triangulaire du système que nous avons déjà obtenue plus haut. Le fait d'échanger l'ordre des variables conduit à un système triangulaire différent.

```
GroebnerBasis[{x - y^2 + 2, x^2 - y^2 - 1},{y,x}]
```

$\{-11 - 5\,x + x^2, -2 - x + y^2\}$

2.5 Elimination des paramètres et projections.

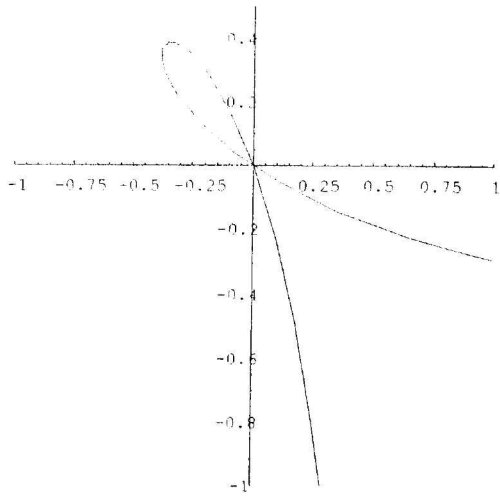
Considérons les équations paramétriques :

$$\begin{cases} x = f(t) &= t(t-1)(t-2) \\ y = g(t) &= (t-1)(t-2)(t-3) \end{cases}$$

d'une courbe du plan. Représentons la, à l'aide de Mathematica.

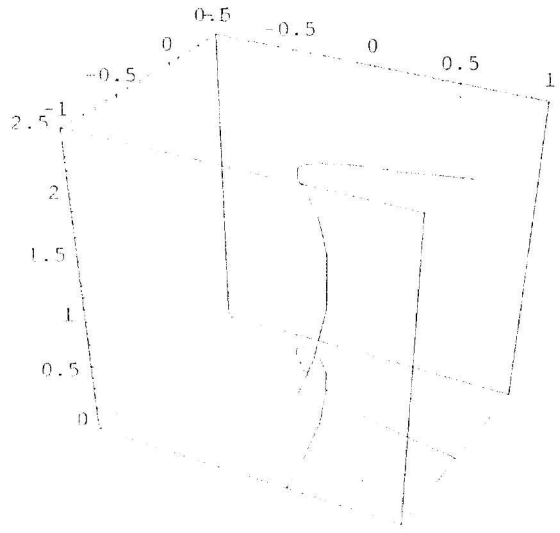
```
f[t_] := t(t-1)(t-2)
g[t_] := (t-1)(t-2)(t-3)
```

```
ParametricPlot[{f[t], g[t]},{t,-2,2.5},AspectRatio -> Automatic,
PlotRange -> {{-1,1},{-1,0.5}}]
```



Pour obtenir une équation de cette courbe de la forme $p(x, y) = 0$ il nous faut éliminer le paramètre t. On peut considérer que la courbe plane $(x(t), y(t))$ est la projection de la courbe gauche $(x(t), y(t), t)$ de l'espace xyt sur le plan xy. L'idéal de $\mathbb{Q}[x, y, t]$ de base $b_1 = x - f(t)$, $b_2 = y - g(t)$ est formée des polynômes qui s'annulent sur la courbe de l'espace $(x(t), y(t), t)$. Représentons cette courbe et sa projection.

```
ParametricPlot3D[{{f[t], g[t],t},{f[t],g[t],0}},{t,-2,2.5},
AspectRatio -> Automatic,
PlotRange -> {{-1,1},{-1,0.5},{0,2.5}}]
```



Considérons maintenant un polynôme quelconque $p(x, y, t)$. Choisissons l'ordre lexicographique en prenant les variables dans l'ordre x, y, t. Divisons $p(x, y, t)$ d'abord par $x - f(t)$, puis le reste de cette division par $y - g(t)$. Le résultat est une relation de la forme

$$p(x, y, t) = h_1(x, y, t)(x - f(t)) + h_2(y, t)(y - g(t)) + h_3(t)$$

Ainsi si l'idéal I contient un polynôme $p(x, y)$, sans l'indéterminée z, alors, à cause de l'absence de la variable t, $p(x, y)$ s'annule sur la surface formée des lignes verticales de l'espace xyt qui coupe la projection de la courbe gauche sur le plan xy. Ainsi $p(x, y)$ considéré comme un polynôme de $\mathbb{Q}[x, y]$ doit s'annuler sur la courbe plane.
Pour trouver un polynôme de la forme $p(x, y)$ dans l'idéal engendré par b_1 et b_2, on choisit l'ordre lexicographique avec t comme première variable et on calcule une base de Gröbner de cet idéal. Si l'idéal I contient des polynômes de la forme $p(x, y)$ il en est de même de la base de Gröbner. En effet avec t comme première variable, tout polynôme contenant t doit avoir t dans son terme de rang le plus élevé et ainsi ce terme de rang le plus élevé ne peut diviser que les termes de rang le plus élevé des polynômes qui contiennent t. Mais pour chaque polynôme q de l'idéal, il doit y avoir un polynôme de la base de Gröbner. dont le terme de rang le plus élevé divise le terme de rang le plus élevé de q.
Voici ce que donne la calcul :

GroebnerBasis[{x-t(t-1)(t-2),y-(t-1)(t-2)(t-3)},{t,x,y}]
{-6 x^2 + x^3 - 15 x y - 3 x^2 y - 6 y^2 + 3x y^2 - y^3,
6 x - x^2 - 6 y + 9 t y + 2 x y - $y^2$2,
-21 x + 9 t x - x^2 - 6 y + 2 x y - y^2,
6 - 9 t + 3 t^2 - x + y}

Le premier polynôme de cette liste fournit une équation de la courbe plane considérée :

$$-6x^2 + x^3 - 15xy - 3x^2y - 6y^2 + 3xy^2 - y^3 = 0$$

Nous venons de donner un exemple d'une approche de la théorie de l'élimination par les bases de Gröbner. Bien que l'ordre lexicographique fonctionne pour les problèmes d'élimination, ce n'est pas toujours le plus efficace. Tout ce qui est nécessaire dans l'exemple ci-dessus c'est de choisir un ordre des variables avec t en premier. On peut ensuite utiliser l'ordre lexicographique par degré, qui en général est plus efficace.

2.6 Division et forme normale.

Avant de présenter une autre application des bases de Gröbner, il faut rappeler certains résultats concernant la division des polynômes...
Un nombre a est la racine d'un polynôme $p(x)$ dans $\mathbb{Q}[x]$ si et seulement si $p(x)$ est divisible par $x - a$. Il existe une proposition analogue pour les polynômes à plusieurs indéterminées. La proposition pour les polynômes à une variable est une conséquence de la division euclidienne. Divisons $p(x)$ par $x - a$, soit $q(x)$ le quotient et $r(x)$ le reste. On obtient la relation

$$p(x) = q(x)(x - a) + r$$

En remplaçant x par a dans cette relation on voit que $r = p(a)$ et que par suite $p(a) = 0$ si et seulement si $r = 0$, c'est à dire si et seulement si $p(x)$ est divisible par $x - a$. Soit maintenant $p(x, y)$ un polynôme de $\mathbb{Q}[x, y]$ et cherchons à quelle condition $p(a, b) = 0$. Par imitation du cas d'une seule variable divisons le polynôme $p(x, y)$ par $x - a$ en considérant y comme une constante. Le résultat est de la forme

$$p(x, y) = q(x, y)(x - a) + r(y)$$

Ensuite divisons $r(y)$ par $y - b$. On obtient un quotient $t(y)$ et un reste s, ce qui donne finalement

$$p(x, y) = q(x, y)(x - a) + t(y)(y - b) + s$$

et en remplaçant x par a et y par b dans cette expression on a $p(a, b) = s$, ce qui prouve que $p(a, b) = 0$ si et seulement si $p(x, y)$ appartient à l'idéal engendré par $x - a$ et $y - b$. Mais nous aurions pu diviser d'abord par $y - b$ et ensuite par $x - a$. Le résultat final aurait été de la forme

$$p(x, y) = f(x, y)(y - b) + g(x)(x - a) + s$$

Le reste s est le même, puisque égal à $p(a, b)$, mais les 'quotients', c'est à dire les coefficients de $x - a$ et $y - b$ ne sont pas les mêmes... La raison qui explique que le reste est le même dans les deux cas est que $\{x - a, y - b\}$ est une base de Gröbner de l'idéal, quel que soit l'ordre choisi sur les variables x et y : les termes de rang le plus élevé, à savoir x, y n'ont pas de diviseurs communs.
Dans le cas général, en partant d'un polynôme p, d'un idéal I, d'un ordre sur les termes, et d'une base de Gröbner $b_1, b_2, ..., b_n$ de I, il existe un algorithme de division qui fournit des quotients $q_1, q_2, ..., q_n$ et un reste r tels que

$$p = q_1 b_1 + q_2 b_2 + ... + q_n b_n + r$$

et le terme de rang le plus élevé de r est plus petit que tout terme de rang le plus élevé d'un polynôme de I. Le reste varie en fonction de l'ordre des termes choisi et les quotients ne sont pas uniques même pour un ordre des termes fixé.
La fonction PolynomialReduce[$p, \{b_1, b_2, ..., b_n\}, \{x_1, x_2, ..., x_m\}$] de Mathematica four-

nit une liste représentant une décomposition de p par rapport aux polynômes $b_1, b_2, ..., b_n$. La liste ayant la forme $\{\{q_1, q_2, ..., q_n\}, r\}$ où r est minimal et où

$$p = q_1 b_1 + q_2 b_2 + ... + q_n b_n + r$$

Le polynôme r a la propriété qu'aucun de ses termes n'est divisible par le terme de rang le plus élevé d'aucun des polynômes b_i. Si $\{b_1, b_2, ..., b_n\}$ est une base de Gröbner, alors r est défini d'une manière unique, pour un ordre de termes déterminé. On précise l'ordre des termes à l'aide d'options.

Par exemple les polynômes $y - 2$ et $x^2 + y^2 - 1$ constituent une base de Gröbner de l'idéal qu'ils engendrent, quand on prend les variables dans l'ordre x, y car leurs termes de rang le plus élevé n'ont pas de diviseurs communs. Décomposons le polynôme $x^3 + y^3$ dans cette base.

```
{q, r} = PolynomialReduce[x^3 + y^3, {y - 2, x^2 + y^2 - 1}, {x, y}]
{{4 - 2 x + 2 y - x y + y^2, x}, 8 - 3 x}
```

ce qui signifie que

$$x^3 + y^3 = (4 - 2x + 2y - xy + y^2)(y - 2) + x(x^2 + y^2 - 1) + 8 - 3x$$

ce que l'on peut vérifier à l'aide de Mathematica :

```
Expand[q.{y - 2, x^2 + y^2 - 1} + r]
x^3 + y^3
```

Deux entiers a et b sont congruents modulo l'entier n s'ils ont le même reste dans la division euclidienne par n. De la même manière deux polynômes p et q sont congrus modulo l'idéal I si $p - q$ est un élément de l'idéal I. Si l'on fixe une base de Gröbner G de l'idéal I et si l'on décide d'un ordre des termes, alors p et q sont congruents modulo I s'ils ont le même reste dans l'algorithme de division que l'on vient de présenter. Ce reste est appelé la forme normale du polynôme p dans la base G. La *forme normale* d'un polynôme p par rapport à un idéal I et à un ordre des termes, a le plus petit des termes de rang le plus élevé parmi tous les polynômes congrus à p par rapport à I.

On peut donner une signification géométrique importante à la congruence modulo un idéal I, dans le cas où I est l'idéal des polynômes s'annulant sur un ensemble de points V. Dans ce cas deux polynômes sont congruents modulo I si leurs restrictions à V définissent la même fonction. Par exemple nous avons vu plus haut que l'idéal des polynômes de $\mathbb{Q}[x, y]$ qui s'annulent sur le cercle unité était l'idéal dont une base est constituée par l'unique polynôme $x^2 + y^2 - 1$. Puisqu'il n'y a qu'un seul polynôme dans cette base, ce polynôme constitue une base de Gröbner de l'idéal I quel que soit l'ordre des termes choisi. Ainsi deux polynômes $p(x, y)$ et $q(x, y)$ vérifieront $p(a, b) = q(a, b)$ pour tout point (a, b) du cercle unité si et seulement si ils ont le même reste dans la division par $x^2 + y^2 - 1$.

La forme normale donne un critère pour décider si un polynôme appartient ou non à un idéal donné, à condition de disposer d'une base de Gröbner de cet idéal. Un polynôme appartient à l'idéal si et seulement si sa forme normale par rapport à la base de Gröbner est le polynôme nul. On peut noter que cette condition ne dépend pas de l'ordre des termes que l'on a adopté. Tout ordre fera l'affaire. Ce détail est important car il existe des ordres qui sont plus efficaces pour le calcul que d'autres.

On peut imaginer facilement que le traitement des congruences simultanées sera aussi fa-

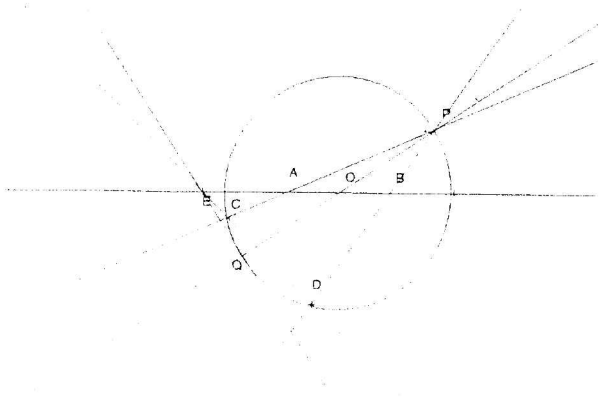


Figure 1:

cilité par l'usage des base de Gröbner, généralisant ce que l'on sait faire grâce au théorème chinois des restes pour les congruences entre entiers relatifs. Nous n'aborderons pas cette question ici. Appliquons ce que l'on vient de voir à la démonstration automatique de théorèmes de géométrie.

2.7 Un peu de géométrie.

Voici un exemple géométrique. On considère un cercle de rayon R centré à l'origine, et deux points, A et B sur l'axe des x, symétriques par rapport à l'origine. Etant donné un point P du cercle, les droites PA et PB coupent le cercle respectivement aux points C et D. La droite CD coupe l'axe des abscisses en un point E. Soit Q le symétrique de P par rapport à l'origine, il s'agit de démontrer que la tangente en Q au cercle passe par E.
On suppose que $R = 1$, ce qui ne restreint pas la généralité du problème mais élimine un paramètre. Puis on met le problème en équations. Les symétries et les positions des points sur l'axe des x donnent

$$x_B = x_A,\ x_Q = -x_P,\ y_Q = -y_P,\ y_A = y_B = y_E = 0$$

Les alignements des points nous donnent

$$\begin{aligned}(x_C - x_P)(y_A - y_P) &= (x_A - x_p)(y_C - y_P)\\ (x_D - x_P)(y_B - y_P) &= (x_B - x_p)(y_D - y_P)\\ (x_E - x_C)(y_C - y_D) &= (x_C - x_D)(y_E - y_C)\end{aligned}$$

Les trois points sur le cercle fournissent les équations

$$x_P^2 + y_P^2 = 1,\ x_C^2 + y_C^2 = 1,\ x_D^2 + y_D^2 = 1$$

Il faut encore exprimer que les points C et P sont distincts, et que les points D et P sont distincts. De plus pour que la droite CD coupe l'axe des abscisses il faut qu'elle ne soit pas parallèle à l'axe des abscisses, c'est à dire C et D n'aient pas la même ordonnée. Pour

cela on ajoute un paramètre t et on considère l'équation

$$1 - t(x_P - x_C)(x_P - x_D)(y_C - y_D) = 0$$

qui ne peut pas avoir de solutions si les abscisses des points P et C d'une part, P et D d'autre part sont égales ainsi que les ordonnées des points C et D. On veut prouver que QE est orthogonale au rayon OQ, c'est à dire que

$$x_Q(x_Q - x_E) + y_Q(y_Q - y_E) = 0$$

Pour cela on réécrit toutes les relations ci-dessus, sauf la dernière, en annulant le second membre, et en considérant le premier membre comme un polynôme en les indéterminées $x_A, x_B, x_C, x_D, x_P, x_Q, x_E, y_A, y_B, y_C, y_D, y_P, y_Q, y_E, t$, en considérant l'idéal I engendré par les polynômes figurant au premier membre. Toute la question revient alors à savoir si le polynôme

$$P = x_Q(x_Q - x_E) + y_Q(y_Q - y_E)$$

appartient à l'idéal I pour cela on calcule une base de Gröbner de l'idéal I, et on calcule la forme normale de P par rapport à cette base de Gröbner.

```
sys = {xb + xa, xq + xp, yp + yq, ya, yb, ye, xp^2 + yp^2 2 - 1, xc^2 + yc^2 - 1,
(xc - xp)(ya - yp) - (xa - xp)(yc - yp), xd^2 + yd^2 - 1, (xd - xp)(yb - yp) - (xb - xp)(yd - yp),
(xe - xc)(yc - yd) - (xc - xd)(ye - yc), 1 - t(xp - xc)(xp - xd)(yc - yd) }
vars = {ya, yb, ye, xa, xb, xp, yp, xq, yq, xc, yc, xd, yd, xe, t}
g = GroebnerBasis[sys, vars, MonomialOrder → DegreeReverseLexicographic];
PolynomialReduce[xq (xq - xe) + yq (yq - ye), g, vars,
MonomialOrder →DegreeReverseLexicographic]\)
```

```
{xa + xb, xp + xq, yp + yq, ya, yb, ye, -1 + xp^2 + yp^2,-1 + xc^2 + yc^2,
(xc - xp)(ya - yp) - (xa - xp)(yc - yp), -1 + xd^2 + yd^2,
(xd - xp)((yb - yp) - (xb - xp)(yd - yp),
(-xc +xe)((yc - yd) - (xc - xd)(-yc + ye),
1 - t(-xc + xp)(-xd + xp)(yc - yd) }
```

```
{ya,yb,ye,xa,xb,xp,yp,xq,yq,xc,yc,xd,yd,xe,t}
```

```
{{0,0,0,-yq,0,0,-1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0},0}
```

On voit que la forme normale de P est le polynôme nul. La propriété est établie.

Bibliographie.

Adams, et P. Loustaunau, 1994. *An introduction to Gröbner bases*, Providence ; American Mathematical Society.

R.B.J. Allendy et E.J. Redfern, 1989. *Introduction to Number Theory with computing*. London, Edward Arnold, Hodder & Stoughton.

Becker, Thomas et Volker Weispfenning, 1993. *Gröbner bases, a computational approach to commutative algebra*. New York, Springer Verlag.

Buchberger, B., 1985, Gröbner bases : an algorithm method in polynomial ideal theory. In *Recent trends in multidimensional systems theory*, ed. N.K. Bose, 184-232, Dordrecht : D. Reidel

Buchberger, B.,G.E. Collins and B. Kutzler, 1988. Algebraic methods in geometric reasoning. *Annual Review of Computer Science* 3:86-119.

Cox, David, John Little, et Donald O'Shea, 1992. *Ideals, varieties and algorithms.* New-York : Springer Verlag.

Cl. Gomez, B. Salvy, P. Zimmermann, 1995. *Calcul formel, mode d'emploi.* Paris : Masson.

Garry Helzer, 1995. *Gröbner Basis.* The Mathematica Journal, Volume 5, Issue 1, 67-73, Miller-Freeman, Palm Coast.

LES REGLES DU CALCUL ALGEBRIQUE POUR LES ELEVES ? MYTHE OU REALITE ?

Groupe Didactique

Nos objectifs dans cet atelier sont :

- *1. Etudier les choix que fait un élève mis en présence d'une expression algébrique ou numérique qu'il doit transformer (simplifier, factoriser, developper) ;*
- *2. Mettre en évidence des types d'erreurs qu'on retrouve d'un élève à un autre et se demander si elles traduisent une cohérence dans la démarche de ces élèves ;*
- *3. Présenter et mettre en débat une proposition d'enseignement conçue par le groupe didactique en réponse à ce questionnement.*

1 . Etudier les choix que fait un élève mis en présence d'une expression algébrique ou numérique qu'il doit transformer.

A partir de photocopies de productions d'élèves (annexe 1) autour de la simplification d'un quotient, les participants de l'atelier sont invités à réfléchir à la question suivante :

Quelles hypothèses pouvez-vous avancer pour expliquer les productions de ces élèves ?

2 . Bilan : Mettre en évidence des types d'erreurs qu'on retrouve d'un élève à un autre et se demander si elles traduisent une cohérence dans la démarche de ces élèves.

Il ressort que les élèves peuvent parvenir régulièrement à des réponses, exactes ou non, en utilisant des gestes non référés à une règle mathématique.

On peut, par exemple, repérer les « gestes » d'élèves suivants :

- L' élève considère l'addition comme une coupure.

exemple : $\dfrac{3+5}{7+5} = \dfrac{3}{7} + \dfrac{5}{5}$

- L'élève supprime des éléments communs sans que ce geste repose sur un sens mathématique.

exemple : $\dfrac{4+a}{6+a} = \dfrac{4+a}{6+a} = \dfrac{4}{6}$

- L'élève contracte l'écriture.

exemple : $\dfrac{4b+20c}{16b+12c} = \dfrac{24bc}{28bc}$

• L'élève veut absolument conserver la lettre.

exemple : $\dfrac{4b + 5c}{16b + 15c} = 0{,}25b + \dfrac{1}{3}c$

3 . Présenter et mettre en débat une proposition d'enseignement conçue par le groupe didactique en réponse à ce questionnement.

a) <u>Essai d'une problématique</u> :

• *Comment attend-t-on qu'un élève utilise la « propriété » :* $\dfrac{a}{b} = \dfrac{ka}{kb}$?

- Lorsqu'un nombre s'écrit a/b alors ce nombre peut sécrire aussi ka / kb

- Lorsqu'un nombre s'écrit sous la forme ka / kb alors ce nombre peut s'écrire aussi a/b

Il est donc nécessaire que l'élève dispose de deux « règles » qui lui permettent à partir de l'une des écritures a/b et ka/kb d'obtenir l'autre écriture :

règle 1		règle 2	
$\dfrac{a}{b}$	$\dfrac{ka}{kb}$	$\dfrac{ka}{kb}$	$\dfrac{a}{b}$

Cela suppose que l'élève est capable d'identifier les formes « initiales » a/b et ka/kb .

Dans la pratique, ces règles de transformation :
- restent plus ou moins implicites (elles deviennent des règles d'actions)
- font partie du commentaire autour de l'égalité (elles ne sont pas un véritable savoir).

• *Ne pourrait-on pas faire un rapprochement avec la démarche déductive ?*

ENONCE
DE PASSAGE

PREMISSES CONCLUSION

Exemple :

Théorème : Si dans un triangle une droite passe par les milieux de deux côtés alors elle est parallèle au troisième côté.

ABC triangle
et I milieu de [AB]
et J milieu de [AC] (IJ) // (BC)

Les analogies :

- même structure ;

- il y a des prémisses à respecter (données géométriques ou forme) ;

- on réalise le passage (la transformation) à l'aide d'un énoncé général (règle ou théorème).

Les différences :

- en géométrie, les « données » sont fournies de manière explicite par la figure (codage) ou par un énoncé (langage) ;

- en algèbre, les prémisses sont à prélever sur des écritures symboliques (formes) ce qui peut exiger parfois un traitement de l'écriture symbolique ;

- en algèbre, contrairement à la géométrie, on passe du signifiant d'un objet à un autre signifiant du même objet ;

- un théorème, en calcul algébrique, sert à obtenir une autre écriture du même nombre.

b) Ebauche de proposition d'enseignement

- Au préalable, il faut avoir construit chez les élèves ces quelques « règles du débat mathématique » :

  - il suffit d'un contre-exemple pour montrer qu'une « phrase algébrique » est fausse ;

  - quelques exemples ne suffisent pas pour conclure ;

  - seuls les théorèmes donnent des moyens pour obtenir une autre écriture d'un même nombre.

De plus le statut de l'égalité est à construire, à savoir qu'une égalité vraie désigne deux écritures d'un même nombre et c'est ceci qui donne du sens aux écritures algébriques.

- Dans son utilisation, une égalité fonctionne différemment suivant le sens de lecture. Il nous a paru nécessaire de l'écrire sous ces deux aspects, **en situation d'apprentissage.**

Ainsi, une égalité va donner lieu a deux théorèmes différents.

Exemple . Ainsi, on peut avoir les deux théorèmes suivants :

théorème 1 : Si un nombre est écrit sous forme d'une somme (ou d'une différence)
et que tous les termes de la somme sont des produits
et que tous les produits ont un facteur commun
alors ce nombre peut s'écrire à l'aide du produit composé du facteur commun
et d'une somme (ou d'une différence).

Si $A = (k \times a) + (k \times b)$ alors $A = k \times (a + b)$ ou $(k \times a) + (k \times b) = k \times (a + b)$
Si $A = (k \times a) - (k \times b)$ alors $A = k \times (a - b)$ ou $(k \times a) - (k \times b) = k \times (a - b)$

théorème 2 : Si un nombre est écrit sous forme d'un produit de deux facteurs
et qu'un des facteurs est une somme (ou une différence)
alors ce nombre peut ausisi s'écrire à l'aide de la somme (ou de la différence)
obtenue en multipliant chaque terme de la somme (ou de la différence) par le facteur restant.

Si $A = k \times (a + b)$ alors $A = (k \times a) + (k \times b)$ ou $k \times (a + b) = (k \times a) + (k \times b)$
Si $A = k \times (a + b)$ alors $A = (k \times a) + (k \times b)$ ou $k \times (a + b) = (k \times a) + (k \times b)$

- Chaque théorème va être travaillé avec les élèves dans l'optique suivante :

  - il va falloir dissocier, comme en géométrie, les prémisses de la conclusion ;

  - il va falloir repérer toutes les prémisses nécessaires à l'application de ce théorème ;

  - il va falloir savoir qu'il ne peut pas s'appliquer s'il manque au moins une prémisses ;

  - il va falloir le différencier de l'autre théorème associé à la même égalité ;

  - il va falloir travailler la formulation du théorème et le décontextualiser, comme pour la géométrie.

Bien entendu, le travail de formulation par écrit dans le registre de la langue naturelle et le passage entre ce registre et le registre algébrique sont essentiels pour la compréhension des écritures algébriques.

- **Ainsi, il y a cohérence entre géométrie et algèbre** : les théorèmes et les définitions sont énoncés de la même manière et le travail est identique dans la phase d'apprentissage.

- **Il ne faut pas oublier que le temps d'apprentissage est long et qu'il ne faut pas arriver trop vite au type d'exercices classiques d'expert qui fonctionnent en évacuant le théorème.**

Remarque : Si on change le type d 'exercice avec les élèves, il est bien entendu qu'il faut changer aussi le type d' évaluation et, aussi, faire évoluer le discours spontané de l'enseignant.

c) Un exemple d'exercice :

Ainsi, on a l'exercice suivant qui peut être proposé aux élèves.

EXERCICE :

Théorème : Si un nombre est écrit sous forme d'une fraction
et que le numérateur et le dénominateur sont des produits
et que les deux produits ont un facteur commun
alors ce nombre a une autre écriture plus simple

$$\text{si } A = \frac{k \times a}{k \times b} \quad \text{alors} \quad A = \frac{a}{b} \qquad \text{ou} \qquad \frac{k \times a}{k \times b} = \frac{a}{b}$$

1 . Peux-tu utiliser ce théorème pour les nombres suivants (a, b et y sont des nombres non fixés) ?

Si oui, explique pourquoi et écris de quoi tu es sur(e) maintenant.
Si non, explique pourquoi.

$$A = \frac{7 \times 9}{7 \times 11} \qquad B = \frac{7 + 9}{7 + 11} \qquad C = \frac{17 - 9}{17 - 11} \qquad D = \frac{7 \times 3 \times 2}{11 \times 3 \times 5}$$

$$E = \frac{9}{15} \qquad F = \frac{7 \times a}{5 \times a} \qquad G = \frac{7 + 3 \times a}{7 + 3 \times a} \qquad H = \frac{3 + 5}{7 + 5}$$

$$H = \frac{3 \times (a + 2)}{3 \times 5} \qquad I = \frac{6 \times (a - 1)}{7 \times a} \qquad J = \frac{7 \times 2 - 7 \times y}{7 \times 3} \qquad K = \frac{27}{18 + 9 \times b}$$

$$L = \frac{12 \times 11}{7 \times 3}$$

2 . Pour certains nombres, il est possible de modifier leurs écritures pour utiliser le théorème précédent. A toi de trouver lesquels de ces nombres et comment modifier leurs écritures.

Pour conclure, cette réflexion est encore en cours car elle fait toujours l'objet d'une recherche dans le groupe tout en s'appuyant sur des expérimentations dans les classes.

ANNEXE 1

Des exercices individuels non notés.

N°		Calculs éventuels ou explications si aucune simplification possible.	Fraction simplifiée, si possible.
1	$\frac{6+2}{6+4}$	$\frac{8+2}{8+4} = \frac{2}{4}$	$\frac{1}{2}$
2	$\frac{2a \times 4}{2}$	$\frac{2a \times 4}{2} = \frac{8a}{2}$	$4a$
3	$\frac{3+5}{7+5}$	$\frac{3+8}{7+8} = \frac{3}{7}$	impossible de réduire plus.
4	$\frac{4b+20c}{16b+12c}$	$\frac{4b+20c}{16b+12c} = \frac{8c}{12b}$	$\frac{3c}{4b}$
5	$\frac{2+7x}{7x}$	$\frac{2+7x}{7x} = \frac{9x}{7x}$	impossible de réduire plus
6	$\frac{4+a}{6+a}$	$\frac{4+a}{6+a} = \frac{4}{6}$	$\frac{2}{3}$
7	$\frac{2a+4}{2}$	$\frac{2a+4}{4} = \frac{6a}{4}$	$\frac{3a}{2}$
8	$\frac{91+1259}{91+3452}$	$\frac{91+1259}{91+3452} = \frac{1259}{3452}$	Je n'y arrive pas parce que les chiffres sont grands, mais c'est
9	$\frac{3(x-1)}{3x}$	Je n'y arrive pas car les fractions avec des parenthèses je n'arrive à résoudre cette fraction	je ne suis jamais
10	$\frac{5+10a}{15-10a}$	$\frac{5+10a}{3\times5\times5-10a} = \frac{10a}{10-10a} = 10a$	impossible de réduire plus.
11	$\frac{4b+5c}{16b+15c}$	$\frac{4b+5c}{16b+15c} = \frac{-10c}{20b}$	$\frac{-1c}{2b}$

ANNEXE 2

Des exercices individuels non notés.

N°		Calculs éventuels ou explications si aucune simplification possible.	Fraction simplifiée possible.
1	$\frac{6+2}{6+4}$	$\frac{6+2}{6+4} = \frac{8}{10}$ J'additionne en haut et en bas les nombres. Si ça avait été $\frac{6}{4} + \frac{2}{6} = \frac{36}{24} + \frac{12}{24} = \frac{36}{24} = \frac{6}{4}$	$\frac{4}{5}$
2	$\frac{2a \times 4}{2}$	$\frac{8a}{2}$ je multiplie en haut	$4a$
3	$\frac{3+5}{7+5}$	① pareil que 1 je sais pas si $\frac{3+5}{7+5} = \frac{8}{12}$ ② $\frac{3}{7} + \frac{5}{5} = \frac{15}{35} + \frac{35}{35} = \frac{50}{35} = \frac{10}{7}$	$\frac{2}{3}$ — $\frac{10}{7}$
4	$\frac{4b+20c}{16b+12c}$	$\frac{4(b+5c)}{4(4b+3c)} = \frac{b+5c}{4b+3c}$	
5	$\frac{2+7x}{7x}$	on peut pas sauf si je fais la solution 2 mais je pense que c'est pas	
6	$\frac{4+a}{6+a}$	pas de facteurs commun	
7	$\frac{2a+4}{2}$	$\frac{2(a+2)}{2} = a+2$	
8	$\frac{91+1259}{91+3452}$	$\frac{1350}{3543} = \frac{450}{1181}$	$\frac{450}{1181}$
9	$\frac{3(x-1)}{3x}$	$\frac{x-1}{x}$	
10	$\frac{5+10a}{15-10a}$	$\frac{5(1+2a)}{5(3-2a)} = \frac{1+2a}{3-2a}$	
11	$\frac{4b+5c}{16b+15c}$	$0{,}25\,b + \frac{1}{3}c$	

(dans la marge, à côté des nos 4 à 10 :) on va faire car je pense que c'est ça

(dans la marge, à côté du no 11 :) ni solution

→ cette feuille a forcément des trucs faux car je sais pas si $\frac{a+b}{[illegible]} = \frac{a}{c} + \frac{b}{d}$ ou pas [illegible]

NARRATION DE RECHERCHE ET DÉNOMBREMENT

F. Bonafé - M. C. Combes - L. Dray - J. P. Robert - M. Sauter
Groupe Géométrie

I. LE PROBLEME.

Nous avons proposé à 195 élèves des classes de 6ième, 5ième, 4ième, 3ième, 2nde et 1ère S, de traiter sous forme de narration de recherche le problème suivant :

"Etant donnés quelques points placés sur une feuille, combien peut on tracer de segments différents joignants deux quelconques de ces points ?"

Compléter le tableau suivant :

Si j'ai	Je peux tracer au plus ....
1 point	0 segment
2 points	1 segment
3 points	3 segments
4 points	6 segments
5 points	
6 points	
7 points	
12 points	
20 points	
108 points	
n points (n est un entier positif)	

Pour ce genre de travail auquel la plus grande partie de nos élèves sont habitués, nous complétons généralement l'énoncé par les consignes ci-après :

Vous raconterez sur votre feuille :

1°) les différentes étapes de votre recherche (vous pouvez minuter le temps, joindre vos brouillons ...) ;
2°) les observations que vous avez pu faire et qui vous ont fait progresser, ou changer de méthode (il vaut mieux chercher seul ...) ;
3°) la façon dont vous expliqueriez votre solution à un (ou une) camarade que vous devez convaincre.

ATTENTION : L'évaluation ne portera pas sur la nature de la solution (juste, fausse, incomplète....) mais sur les trois points évoqués ci-dessus.

La répartition des élèves était la suivante :

Classe	6ième	5ième	4ième	3ième	2nde	1ère S
Effectif	60	25	22	22	29	37

Nous avions pour objectif de :

- repérer les procédures de recherche utilisées par les élèves, observer leur traitement de l'équivalence de formules numériques ainsi que l'introduction du nombre n ;
- favoriser l'apprentissage de la démonstration et son enracinement géométrique dans ce cas.

II. ESSAI D'ANALYSE A PRIORI.

Quelles peuvent être les directions de recherche des élèves sur ce type de problème ?

Afin de mieux cerner les difficultés des élèves, leurs directions de recherche, nous avons proposé aux participants de réfléchir sur un autre problème de dénombrement, de même forme, mais ne présentant pas le même caractère d'évidence pour un enseignant (annexe 1).

La mise en commun des résultats nous a montré que, dans une première phase de recherche, les méthodes adoptées par les participants n'étaient guère éloignées des méthodes adoptées par les élèves dans un contexte comparable.

III. METHODES DE RECHERCHE DES ELEVES.

On relève trois directions différentes dans les recherches conduites par les élèves :

- **comptage effectif** des segments avec ou sans figure ;
- recherche d'une **relation numérique à partir des premiers résultats du tableau ;**
- **transformation d'une formule en une autre** lorsque plusieurs formes de réponses ont été obtenues.

Les deux premières concernent la recherche d'une solution au problème posé. La dernière est une conséquence des résultats entrevus et d'une tentative de réduction du nombre de calculs.

Chacune de ces directions fait référence à un certain nombre de procédures énoncées ci-dessous. Nous n'avons retenu que celles apparaissant au moins dans deux copies différentes.

Comptage effectif des segments

Procédure 1 : "Ajouter point"

L'élève se rend clairement compte que lorsqu'il ajoute un point à la figure déjà tracée et qui en comporte p, il augmente le nombre de segments de p.

Cette procédure conduit à $N_n = N_{n-1} + (n-1)$.

Procédure 2 : "Compter et ajouter point"

L'élève se rend clairement compte que lorsqu'il ajoute un point à la figure déjà tracée et qui en comporte p, il augmente le nombre de segments de p. Il compte les segments commençant à partir de 1 point.

Cette procédure conduit pour le résultat final à $N_n = 1 + 2 + 3 + ... + (n-1)$.

Procédure 3 : "Compter avec méthode"

L'élève compte méthodiquement les segments pour n points. Du premier point il dénombre n - 1 segments, du second n - 2, etc.....

Cette procédure conduit pour le résultat final à $N_n = (n-1) + (n-2) + (n-3) + ... + 1$.

Procédure 4 : "Segments et vecteurs"

L'élève compte méthodiquement les segments pour n points. Du premier point il dénombre n - 1 segments, du second n - 1 encore, etc... Il ajoute qu'en procédant ainsi, chaque segment est compté deux fois.

Cette procédure conduit pour le résultat final à $N_n = \frac{(n-1)n}{2}$.

Procédure 5 : "Faire le tour"

L'élève compte méthodiquement les segments pour n points. Il commence par en compter n sur le pourtour de la figure. Ensuite, à partir d'un point quelconque, il en compte n - 3, d'un autre point quelconque, il en compte également n - 3, puis n - 4, puis n - 5.....

Cette procédure conduit pour le résultat final à $N_n = n + 2(n-3) + (n-4) + ... + 1$.

Procédure 6 : "Groupes de points"

Pour dénombrer les segments formés à l'aide de n points, l'élève établit deux groupes de points, un de p points, l'autre de n - p et utilise ces deux résultats.

Cette procédure conduit pour le résultat final à $N_n = N_p + N_{n-p} + n(n-p)$.

Procédure 7 : "Segments"

Cette procédure est voisine de la 4 mais son début diffère. L'élève compte tous les couples de points, soit n^2, il enlève les couples comportant le même point, soit n, puis ajoute qu'en procédant ainsi chaque segment est compté deux fois.

Cette procédure conduit pour le résultat final à $N_n = \frac{n^2 - n}{2}$.

Recherche d'une relation à partir des premiers résultats du tableau.

Procédure 8 : "Proportionnalité"

En observant le tableau de nombres, l'élève émet l'hypothèse que le nombre de points et le nombre de segments sont proportionnels. Il vérifie et rejette cette hypothèse.

Procédure 9 : "Accroissements proportionnels"

En observant le tableau de nombres, l'élève émet l'hypothèse que l'accroissement du nombre de points et l'accroissement du quotient du nombre de segments par le nombre de points sont proportionnels.

Cette procédure conduit pour le résultat final à $N_n = \frac{(n-1)n}{2}$.

Procédure 10 : "Induction directe"

En observant le tableau de nombres, l'élève émet une hypothèse autre que la proportionnalité qui est confirmée par les résultats qu'il peut contrôler.

Cette procédure conduit pour le résultat final à un de ceux des procédures 1, 2, 3, 4.

Procédure 11 : "Représentation"

L'élève qui a obtenu quelques résultats par comptage place dans un repère les points ayant pour abscisse le nombre n et pour ordonnée le nombre de segments.

Procédure 12 : "Fonction carrée"

L'élève a conjecturé par un graphique que le nombre de segments était une fonction du second degré de n. Il cherche à partir de cas particuliers les coefficients du trinôme.

Cette procédure conduit pour le résultat final à $f(n) = \frac{1}{2} n^2 - \frac{1}{2} n$.

Transformation d'une formule.

Procédure 13 : "Simplification par symétrie"

L'élève qui a déjà un résultat à partir des procédures 2 ou 3, soit $N_n = 1+2+3+...+(n-1)$, soit $N_n = (n-1) + (n-2) + (n-3) + ... + 1$, veut réduire le nombre de calculs. Il y parvient en sommant les termes symétriques de la progression arithmétique.

Procédure 14 : "Simplification par regroupement"

L'élève qui a déjà un résultat à partir des procédures 2 ou 3, soit $N_n = 1+2+3+...+(n-1)$, soit $N_n = (n-1) + (n-2) + (n-3) + ... + 1$, veut réduire le nombre de calculs. Il y parvient en regroupant les termes consécutifs de 1 à 9, puis de 10 à 19, de 20 à 29 etc., et constate que les résultats 45, 145, 245, sont les termes d'une suite arithmétique.

Répartition de ces procédures suivant le niveau scolaire.

Classe / Procédure	6ième	5ième	4ième	3ième	2nde	1ère S
1	4	1	8	6	9	2
2	1	1	1	0	5	2
3	12	4	4	3	10	2
4	8	5	1	4	18	9
5	1	2	0	0	0	0
6	2	0	4	0	2	0
7	0	0	1	0	2	0
8	5	3	5	1	2	1
9	3	3	3	7	5	4
10	22	10	12	17	10	8
11	1	0	1	0	2	0
12	0	0	0	0	0	26
13	0	1	0	1	3	2
14	4	0	0	1	0	0
Total	63	30	40	40	68	56

En relativisant par rapport au nombre d'élèves, pour un total de 100 élèves par niveau :

Classe / Procédure	6ième	5ième	4ième	3ième	2nde	1ère S
1	7	4	36	27	31	5
2	2	4	5	0	17	5
3	20	16	18	14	34	5
4	13	20	5	18	62	24
5	2	8	0	0	0	0
6	3	0	18	0	7	0
7	0	0	5	0	7	0
8	8	12	23	5	7	3
9	5	12	14	32	17	11
10	37	40	54	77	35	22
11	2	0	5	0	7	0
12	0	0	0	0	0	70
13	0	4	0	5	10	5
14	7	0	0	5	0	0
Total	106	120	183	183	234	150

Cette répartition invite à quelques remarques.

- Concernant le total du nombre de procédures par niveau, le cas des élèves de 1ère S mis à part, une augmentation apparaît. On peut émettre comme hypothèse que l'aptitude à changer de méthode dans la recherche d'un problème croît avec le niveau scolaire. Mais comment expliquer alors le cas des élèves de 1ère S ? Justement par l'accroissement du niveau scolaire ! En effet, le travail réalisé sur les fonctions à ce niveau a eu comme conséquence une utilisation massive de la procédure 12 qui conduit à conjecturer $f(n) = \frac{1}{2} n^2 - \frac{1}{2} n$. Ce résultat n'étant pas mis en défaut par les vérifications réalisées, il est accepté par les élèves.

- Concernant la répartition des procédures, le seul résultat notable concerne la procédure 1 qui semble plus fortement présente à partir de la classe de 4ième, mais il est très difficile de la distinguer de la 2.

- Enfin on peut relever le poids important de la procédure 10 qui consiste à délaisser à partir d'un certain rang le comptage pour céder la place au travail sur les nombres. Cette procédure conduit dans presque tous les cas à une conjecture correcte, non rejetée car le résultat n'est pas mis en défaut par les vérifications réalisées.

IV. LE NOMBRE n.

Au delà de ces procédures, nous avons centré notre intérêt sur l'introduction du nombre n dans les copies, aussi bien pour les élèves ayant utilisé des procédés de comptage que pour ceux qui ont travaillé sur les nombres.

Le nombre n apparaît dans les copies à travers 5 formules différentes :

$N_n = 1 + 2 + 3 + ... + (n-1)$, $N_n = (n-1) + (n-2) + (n-3) + ... + 1$, $N_n = \frac{(n-1)n}{2}$, $N_n = \frac{n^2 - n}{2}$, $N_n = n + 2(n-3) + (n-4) + ... + 1$.

On peut tout d'abord relever que les résultats concernant n points n'apparaissent pas dans toutes les copies, d'ailleurs en 6ième ce n'était pas demandé. D'autre part, l'introduction d'une généralisation prend des formes diverses, elle peut être verbale, à l'aide d'une phrase générale, ou bien symbolique, par l'intermédiaire d'une lettre, x, a, n ou autre.

En voici la répartition pour un total de 100 élèves par niveau :

Classe	6ième	5ième	4ième	3ième	2nde	1ère S
Élèves ayant généralisé	2	12	45	59	89	89

L'évolution selon le niveau est remarquable. L'aptitude à formuler une règle observée par l'introduction d'une variable, à donner à un résultat son caractère fonctionnel, croît avec le niveau scolaire.

V. DEMONTRE OU PAS.

Les élèves ayant utilisé des procédés de comptage peuvent, en toute rigueur, démontrer leur résultat en généralisant leur raisonnement au cas de n points. Pour les autres, ayant travaillé sur les nombres, la seule preuve possible est un raisonnement par récurrence avec un retour sur la géométrie pour dégager la relation de récurrence. Un tel raisonnement ne peut être fourni à ce niveau.

Concernant le passage au cas général et la trace ou non d'une démonstration, on constate trois comportements différents.

1 - L'élève fait correctement le raisonnement pour quelques points et le refait ensuite pour n, montrant par là que son traitement des cas particuliers se généralise. Cette généralisation intervient parfois en fin de copie quand il doit raconter à un camarade comment il procède.

2 - L'élève ne ressent pas la nécessité de faire correctement le raisonnement pour quelques points, après un bref comptage pour les premières valeurs de n, il le fait directement pour n quelconque. Ce raisonnement est parfois illustré par l'application simultanée à un cas particulier.

3 - L'élève fait correctement le raisonnement pour quelques points et donne la formule conjecturée pour n. Parfois, il la vérifie sur quelques cas et conclut à sa véracité.

Observons la répartition de ces comportements. Pour un total de 100 élèves par niveau :

Classe	6ième	5ième	4ième	3ième	2nde	1ère S
1	0	0	0	4	31	16
2	0	0	0	4	27	6
3	2	12	45	51	31	67

Les comportements de type 1 ou 2 sont effectivement des preuves du résultat avancé. C'est à partir de la classe de 3ième que l'on peut les observer dans les copies.

Le comportement de type 3 ne peut être considéré a priori comme une preuve, même lorsqu'il est accompagné de vérifications. Pourtant..... on peut se demander si l'exemple, ici, ne peut pas avoir valeur de preuve, car la valeur choisie pour raisonner n'altère en rien la généralité du raisonnement.

Observons à ce sujet la façon dont sont abordées quelques questions d'arithmétique dans deux traités de la fin du siècle dernier.

Dans le "Traité d'arithmétique à l'usage des élèves des Lycées et Collèges et des candidats aux écoles du Gouvernement" par BURAT E. (1875), on trouve la proposition suivante avec sa démonstration :

"Proposition 1 : - Lorsqu'un nombre divise un produit de deux facteurs et qu'il est premier avec l'un des facteurs, il doit diviser l'autre.
Démonstration : - Soit le nombre 15 qui divise le produit 92x60 ; il est premier avec 92, je dis qu'il divise 60. En effet, le plus grand diviseur commun aux nombres 15 et 92 est 1 ; par conséquent celui des nombres 15x60 et 92x60 est 60. Ceci posé, j'observe que 15 divise 92x60 par hypothèse, et 15x60 qui est un multiple de 15 ; or quand un nombre en divise deux autres, il divise aussi leur plus grand diviseur commun ; donc 15 divise 60."

Dans le "Traité d'arithmétique à l'usage des élèves de mathématiques élémentaires, des aspirants aux baccalauréats..... avec des compléments destinés aux candidats des grandes écoles du Gouvernement" par HUMBERT H. (1893), on trouve la proposition suivante (la même bien sur) avec sa démonstration :

" 1° Lorsqu'un nombre divise un produit de deux facteurs et qu'il est premier avec l'un d'eux, il divise l'autre.
Soit c un nombre qui divise le produit ab de deux nombres donnés, et supposons c premier avec b; cela veut dire que c et b ont pour plus grand commun diviseur l'unité ; donc les produits ac et ab ont pour plus grand commun diviseur le nombre a. D'autre part le nombre c divise ac dont il est facteur, il divise ab par hypothèse ; donc il divise le plus grand commun diviseur de ces deux nombres, c'est à dire a."

Il semble qu'il y ait là, sur la notion de preuve en arithmétique, une singularité au regard de ce que l'on appelle communément une preuve. Elle tient à la fois du caractère général que présentent certains cas particuliers à l'égard du contexte et de la non contradiction.

Une autre illustration peut en être fournie avec le jeu du quitte ou double. La vue des premiers gains possibles que sont 1, 2, 4, 8, 16 permet de conjecturer 2^{n-1} pour le gain possible à la question n. Devant l'évidence qu'il s'agit de la suite des puissances croissantes de 2 et sans que ce résultat puisse être mis en défaut par des exemples on s'accorde à dire qu'il est vrai.

Dans notre problème, le caractère de généralité se dégage de la figure. Dès qu'a été observé le procédé de génération des segments et le procédé de comptage qui s'en dégage, son caractère récurrent ne peut être mis en défaut. Que doit on attendre des élèves ayant observé ce procédé de génération ? Autrement dit, une fois que les élèves ont perçu le caractère général qui peut être attribué à tout cas particulier, est-il nécessaire pour eux d'en établir la généralité ou bien leur suffit-il de constater qu'il n'est pas contredit ?

L'étude des comportements de type 3 pour lesquels la preuve semble absente, montre deux grandes tendances concernant la généralisation du mode de calcul lorsque celui-ci est effectué à partir d'une procédure de comptage et donc enraciné dans la géométrie :

- L'élève donne comme démonstration la vérification sur des cas pour lesquels il sait qu'elle fonctionne. C'est la non contradiction comme le montre la copie en annexe 2.

- L'élève donne sur un cas particulier un raisonnement présentant un caractère général irréfutable. C'est l'évidence du caractère général comme le montre la copie en annexe 3.

Ces pratiques étant présentes à tous les niveaux de l'enseignement secondaire, nous avons là deux points d'appui concernant l'apprentissage de la démonstration. La phase de mise en commun et de correction doit montrer l'insuffisance du procédé de non contradiction et la relative faiblesse du procédé dégageant l'évidence du caractère général de quelques cas particuliers.

VI. LES TRIANGLES.

En ce qui concerne le travail portant exclusivement sur les nombres, nous avons vu combien en 1ère S les élèves étaient influencés par les contenus d'enseignement et en particulier par la fonction carré. Après la séance de correction, et pour en mesurer l'impact, nous avons proposé en 2nde et 1ère S le problème suivant :

"Etant donnés quelques points placés sur une feuille, combien peut on tracer de triangles différents dont les sommets sont trois quelconques de ces points ?"

Compléter le tableau suivant :

Si j'ai	Je peux tracer au plus ....
1 point	0 triangle
2 points	0 triangle
3 points	1 triangle
4 points	4 triangles
5 points	
6 points	
7 points	
12 points	
20 points	
108 points	
n points (n est un entier positif)	

Ce travail s'est déroulé en classe et par groupes en 2nde et sous forme de narrations de recherche en 1ère S.

En classe de 2nde, deux groupes sont parvenus au résultat correct, ce fut l'échec total pour les autres. En effet, les méthodes effectives de comptage sont très rapidement en échec ne serait ce qu'à cause de difficultés matérielles. A partir de 5 points, l'utilisation de couleurs différentes par exemple, s'avère très difficile.

On peut remarquer que dans les groupes ayant réussi se trouvaient des élèves ayant traité le cas des segments avec succès en raisonnant directement sur le nombre n. Pour ce nouveau problème, leurs méthodes de comptage ont réinvesti les résultats du comptage des segments. C'est en définissant un triangle comme l'association d'un segment et d'un point extérieur que sont nés leurs procédés généraux de comptage.

Pour les élèves de 1ère S, on retrouve des procédures en tout point comparables à celles observées sur le précédent problèmes :

- 20 comptages effectifs,
- 23 résultats induits à partir d'un travail sur les nombres (dont 11 fonction cube),
- 2 recherches d'équivalences de formules.

On a donc encore près d'un tiers des élèves qui renouvellent le travail sur les fonctions en sachant que cela ne leur permettra pas de dégager une preuve. L'absence de contradiction dans les vérifications est encore très pesante dans leur démarche.

VII. CONCLUSIONS.

Au travers des multiples procédures rencontrées dans ce type de problème, on peut penser que pour traiter les questions d'exhaustion, on relève deux principales directions de travail :

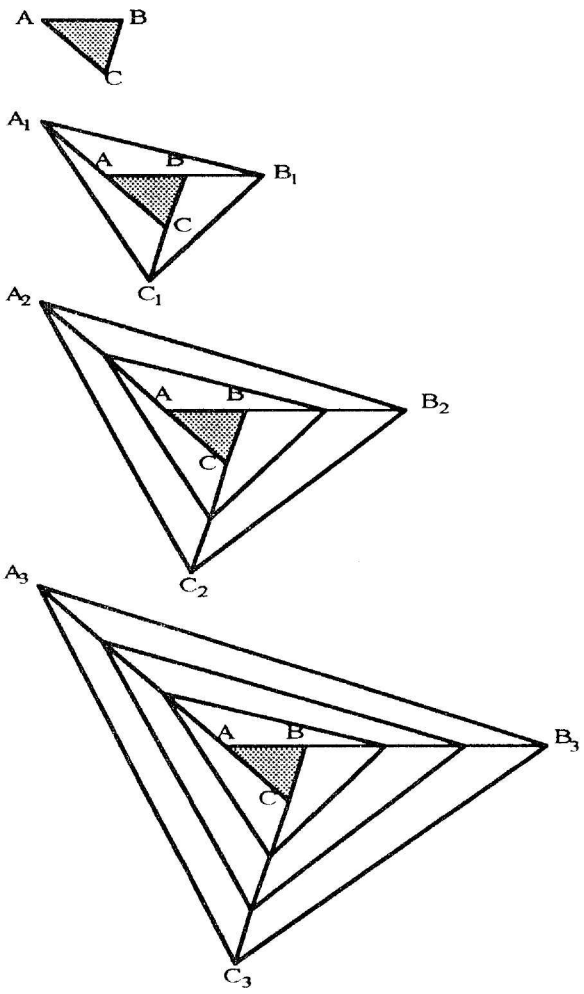
- du particulier au général avec essai d'explication du général ;
- du particulier au général sans contradiction avérée lors du retour sur le particulier.

La première conduit à terme à la notion de preuve quand elle n'en est pas déjà une. C'est la nécessité d'une explication du cas général lorsque celle ci est de même nature que les cas particuliers traités qu'il faut faire émerger.

Pour la deuxième, il nous faut amener les élèves à comprendre que dans ce passage du particulier au général vérifié par des exemples, l'utilisation d'un langage formel ne peut masquer l'absence d'une preuve. Nous devons donc dégager des situations pour lesquelles leur façon de faire sera mise en défaut.

Ce n'est pas pour autant que cela suffira, le travail effectué en 1ère S le montre bien. Nous savons tous, pour avoir parfois cherché sans succès... que toutes les conjectures sont dans un premier temps acceptableS, surtout quand on ne peut les contredire (voir le grand théorème de Fermat par exemple). On doit accepter et même souhaiter que des élèves soient mis dans une situation de recherche et livrent de tels résultats, ni démontrés, ni contredits. C'est en montrant la multiplicité des approches, en privilégiant le débat, que nous parviendrons à semer quelques doutes sur l'évidence et la non contradiction et que pourra surgir la nécessité de la preuve.

ANNEXE 1



A partir du triangle ABC ci-contre, on construit les triangles

$A_1B_1C_1$,

puis $A_2B_2C_2$,

puis $A_3B_3C_3$, ...

.

.

.

.

.

jusqu'à $A_nB_nC_n$.

Pour cela, on reporte les longueurs AB sur la droite (AB), BC sur la droite (BC), CA sur la droite (CA), toujours dans le même sens, d'abord 1 fois, puis 2 fois, 3 fois ..... jusqu'à n fois.

Le problème consiste à évaluer les aires de $A_1B_1C_1$, puis $A_2B_2C_2$, $A_3B_3C_3$, ... jusqu'à $A_nB_nC_n$, en fonction de l'aire du triangle initial ABC.

Compléter le tableau suivant:

Si j'allonge....	Le rapport des aires est....
0 fois	1
1 fois	7
2 fois	19
3 fois	37
4 fois	
10 fois	
23 fois	
n fois	

ANNEXE 2

J'ai trouvé un moyen :

Il faut multiplier le nombre de points par le nombre de points moins 1 puis diviser le résultat obtenu par 2.

Démonstration :

$\frac{3 \times 2}{2} = 3$ ou $\frac{3 \times (3-1)}{2} = 3$

$\frac{4 \times 3}{2} = 6$ ou $\frac{4 \times (4-1)}{2} = 6$

$\frac{5 \times 4}{2} = 10$ ou $\frac{5 \times (4-1)}{2} = 10$

. . . .

Donc pour calculer des gros nombres, je vais me servir de cette méthode.

$\frac{19 \times 14}{2} = \frac{132}{2} = 66$

$\frac{20 \times 19}{2} = \frac{380}{2} = 190$

$\frac{108 \times 107}{2} = \frac{11556}{2} = 5778$

ANNEXE 3

Pour tracer un segment il faut nécessairement 2 points puisqu'il nous faut tout d'abord calculer pour 5 points, le nombre de segments possibles à tracer, nous allons nommer ceux-ci par des lettres (A, B, C, D, E) et nous allons faire un tableau pour chercher ces segments

	A	B	C	D	E
A	AA	AB	AC	AD	AE
B	BA	BB	BC	BD	BE
C	CA	CB	CC	CD	CE
D	DA	DB	DC	DD	DE
E	EA	EB	EC	ED	EE

5 segments impossibles

10 segments en double (AB=BA)

10 segments possibles

Si on essaye de joindre a avec a c'est impossible même que B et B c et C D et D et E et E.

Dans mon tableau il y a 5 colonnes et 5 lignes donc 25 réponses éventuelles. Enlevons les 5 solutions impossibles. Enlevons la 1/2 soit ici 10 solutions identiques car

AB = BA. AC = CA AD = DA AE = EA

BC = CB BD = DB BE = EB CD = DC

CE = EC DE = ED

Donc à partir de là nous pouvons établir une formule Soit N : le nombre de points. Nous avons

$$\frac{(N \times N) - N}{2} = \text{Nombre de segments}$$

Pour 5 points

$$\frac{(5 \times 5) - 5}{2} = \frac{25 - 5}{2} = \frac{20}{2} = 10 \text{ segments}$$

QUELQUES CONSIDERATIONS SUR LES NOMBRES EN SECONDE

Jacques Delgoulet
Groupe Intégration des Outils Informatiques

OBJECTIFS

L'objectif de cet atelier était de montrer comment le groupe intégration des outils informatiques de l'IREM de Montpellier a été conduit, en classe de seconde, à s'intéresser aux notions de valeur exacte et de valeur approchée. Il s'agit d'un travail en cours et les idées qui sont présentées à travers un certain nombre d'activités seront approfondies dans les années à venir.

LA TI-92 EN SECONDE AU LYCEE DE CLERMONT L'HERAULT

Depuis deux ans une classe de seconde du lycée de Clermont l'Hérault est dotée d'une TI-92. Le groupe Intégration des outils informatiques élabore depuis janvier 1996 des activités destinées à intégrer cette machine dans la classe. Parmi les thèmes que le groupe a abordés au cours de ces deux années, on peut citer :

- les formes algébriques ;
- les fonctions ;
- les notions de valeurs exactes et de valeurs approchées.

Parallèlement à ces thèmes, le groupe essaye d'inciter les élèves à considérer la machine comme un outil de contrôle de leurs propres résultats, en particulier grâce à des activités qui nécessitent plusieurs cadres de résolution (algébrique, graphique, géométrique).

Au cours de ces deux années les élèves ont eu l'occasion de remplir des questionnaires, certains élèves ont été interviewés, dans le but de cerner l'évolution de leur rapport avec la machine ainsi que d'évaluer les apprentissages effectués, les connaissances mises en œuvre. L'expérimentation de la première année a donné lieu à un rapport.

POURQUOI LES NOMBRES EN SECONDE ?

Une des caractéristiques de la TI-92 est de faire coexister "valeurs exactes" et "valeurs approchées" avec une nuance de taille : on ne parle de valeurs exactes que dans l'application initiale !

Dans les autres applications, qu'ils s'agissent des applications graphiques ou géométriques, les nombres affichés sont des approximations décimales comme sur une machine classique.

Une hypothèse tentante est de penser que cette caractéristique de la TI-92 va aider les élèves à faire la distinction entre un nombre et ses approximations décimales.

La réalité est bien sûr plus complexe et se heurte aux conceptions que les élèves ont des nombres ainsi qu'à la représentation qu'ils s'en font.

Concernant les nombres, le modèle dominant est fourni par les machines que, d'une façon générale, les élèves utilisent après un apprentissage réduit ou inexistant (**voir expérimentation 95/96**). D'une façon générale, on considère que c'est l'élève qui doit prendre en charge, en grande partie du moins, l'apprentissage des machines. Ce point de vue est certainement à nuancer mais, en classe de seconde, il semblerait que les enseignants (que ce soit en mathématiques ou en dans les autres matières utilisant des outils de calculs) considèrent que les élèves savent ou devraient savoir utiliser une machine, comprendre, interpréter et contrôler les résultats numériques affichés. Il en résulte que le modèle dominant est le modèle

décimal sans que les caractéristiques propres aux nombres décimaux soient explicitées. En effet, en seconde du moins, rien dans les programmes ne permet d'aborder ce qui est relatif à la nature des nombres que les élèves manipulent.

Parmi les conséquences de ces pratiques, on peut noter un certain nombre d'attitudes chez un élève de seconde qui ont été relevées au cours de l'expérimentation :

- pas de remise en question des résultats affichés (... puisqu'ils sont fournis par une machine ...) - **voir expérimentation 95/96 questionnaire N°1 ;**
- ce que la machine affiche est exact (à la fois dans le sens de valeur exacte que de contraire de faux) ;
- ce qui est approché est décimal ;
- ce qui est décimal est approché.

Remarque : une autre caractéristique de la TI-92 est de transformer systématiquement, en mode exact dans l'application initiale, les nombres décimaux en rationnels ainsi que de faire coexister différentes formes d'un même nombre sans être parfois capable de les identifier (ceci est particulièrement vrai dès lors que le calcul comporte des racines carrées).

LA NOTION DE NOMBRE DANS LE PREMIER CYCLE ET EN SECONDE.

Sans entrer dans les détails, on peut dire que de la sixième à la seconde, rien dans les programmes ne permet d'aborder la nature des nombres manipulés.

En seconde, par exemple, mention est faite des ensembles de nombres sans plus de détails.

En réalité toutes les activités numériques concernent soit le calcul approché (avec systématiquement des approximations décimales), soit le calcul algébrique.

ÉCRITURE DES NOMBRES

Si à aucun moment de la scolarité, entre la sixième et la seconde, les caractéristiques (à défaut des définitions) des différents types de nombres ne sont aux programmes, par contre les systèmes d'écriture des nombres sont étudiés :

- nombres entiers, relatifs ou non ;
- nombres décimaux ;
- nombres rationnels ou fractionnaires ;
- notation scientifique ;
- les "réels" qui seraient tous les précédents plus ceux qui ne peuvent pas s'écrire dans l'un des systèmes ci-dessus.

En fait ce sont les règles de calculs propres à chaque système qui sont abordés (addition soustraction, multiplication, division, puissances).

Concernant ces règles de calculs, on peut constater que certains systèmes sont cohérents d'autres pas : la somme de deux nombres écrits sous forme scientifique nécessite, la plupart du temps, le passage par une écriture intermédiaire afin de pouvoir factoriser une puissance de 10.

En dehors des règles de calculs évoquées ci-dessus, des exercices portent sur le passage d'un système à un autre ainsi que des calculs sur des nombres écrits dans plusieurs systèmes (un décimal et un rationnel, etc.) sont abordés.

QUE SIGNIFIENT VALEUR (S) EXACTE (S), VALEUR (S) APPROCHEE (S) ?

- *pour un élève de seconde...?*
- *pour un professeur...? qui doit l'expliquer à un élève de seconde ?*

Ce sont ces questions, énoncées ici sous forme de boutade, que le groupe s'est posé. Les termes de *valeur (s) exacte (s) d'un nombre, valeur (s) approchée(e) d'un nombre*, employés ici reviennent constamment dans les programmes, chez les élèves et chez les enseignants. En fait c'est surtout le mot ***valeur*** qui soulève un réel problème de sens dès lors qu'on l'associe au mot ***nombre***. En effet, qu'est ce que la valeur d'un nombre ? Un nombre aurait-il plusieurs valeurs ? La valeur exacte d'un nombre n'est-elle pas le nombre lui-même qui peut bien sûr avoir plusieurs écritures. De même la notion de valeur approchée n'a de sens que si on mentionne la précision !

Ces difficultés a donner un sens à des mots particulièrement mal adaptés ont conduit le groupe à essayer (et ce n'est pas facile ...) de remplacer les termes valeur exacte par nombre et valeur approchée par approximation (non nécessairement décimale).

QUELQUES IDEES DIRECTRICES

Concernant le thème de valeur exacte/valeur approchée, le groupe a essayé de faire passer un certain nombre d'idées :

- une approximation n'est pas nécessairement décimale ;
- tout ce qui est décimal n'est pas approché ;
- un nombre ("valeur exacte") a plusieurs formes (en particulier, on rencontre cela sur la TI-92) ;
- donner du sens à valeur exacte et valeur approchée en essayant de les remplacer par nombre et approximation (décimale ou non) ;
- donner des éléments permettant une représentation mentale de certains nombres ou type de nombres (rationnels positifs représentés par des segments, dichotomie : le nombre cherché est la solution d'une équation sur un intervalle donné, fraction continue de $\sqrt{2}$, développement décimal d'un rationnel, etc).

C'est dans cet esprit que les activités présentées ici ont été conçues et proposées aux élèves avec le souci de les intégrer à la fois dans le déroulement du programme et dans le cadre de l'expérimentation.

En conclusion c'est plus sur la représentation des nombres que sur leur nature que le groupe a essayé d'agir. Il dispose maintenant d'un certain nombre d'activités, souvent classiques, qui permettent de le faire. Il est clair que c'est insuffisant pour modifier radicalement les pratiques des élèves, cependant les entretiens effectués en avril 97 ainsi que le comportement devant les résultats affichés par la machine a considérablement évolué. Il reste maintenant à élaborer des activités qui vont permettre aux élèves de commencer à faire la distinction entre les divers types de nombres qu'ils manipulent.

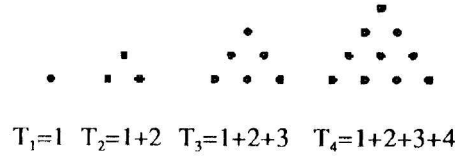
REPRESENTATION DES NOMBRES

REPRESENTATION DES NOMBRES ENTIERS

Les mathématiciens grecs ne disposaient pas de notre système décimal. Pour écrire les nombres, ils utilisaient des lettres dont le maniement devait être délicat. Un grand nombre de propriétés arithmétiques leur étaient déjà connues, entre autres celles qui concernent les nombres entiers premiers[5]*. Pour démontrer ces propriétés ils utilisaient diverses représentations des nombres et parlaient de nombres linéaires (en ligne), en "triangles", en "polygones".*

Les mathématiciens grecs du VI^{ème} *siècle avant Jésus-Christ qui travaillaient avec Pythagore représentaient les nombres entiers par des points. Ces points pouvaient être disposés selon des figures comme le triangle, le rectangle ou le carré.*

1) Voici les représentations des quatre premiers nombres "triangles"
Calculez T_1, T_2, T_3, T_4, dessinez et calculez les six nombres suivants.



$T_1=1$ $T_2=1+2$ $T_3=1+2+3$ $T_4=1+2+3+4$

2) On peut aussi représenter ces nombres par des "escaliers".

3) En s'aidant du schéma et des calculs ci-contre, calculez T_3, T_4, T_8.

$$T_3 + T_3 = 2 \times 3$$
$$2 \times T_3 = 2 \times 3$$
$$T_3 = \frac{2 \times 3}{2}$$

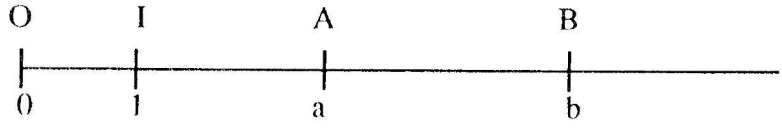
Pouvez-vous, en vous aidant des calculs et des schémas ci-dessus, trouver une façon de calculer rapidement la somme des 23 premiers nombres entiers naturels ? la somme des n premiers entiers naturels ?

REPRESENTATION DES FRACTIONS

Rappels : historiquement une fraction est le quotient de deux nombres entiers naturels a et b, avec a inférieur ou égal à b et b non nul. Dans le cas où aurait et b sont des entiers relatifs, on devrait parler de nombre rationnel. Dans le cas où a et b sont des nombres quelconques ($\sqrt{2}$ et π) on devrait parler de quotient.

Ici on s'intéresse aux nombres du type $\frac{a}{b}$ où a et b sont des entiers naturels (donc positifs).

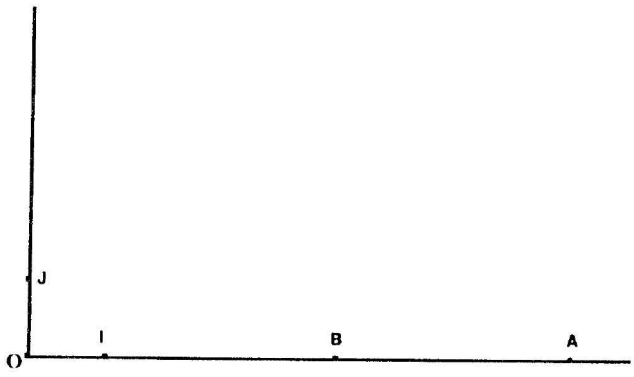
Objectif : on considère une graduation où l'unité est choisie arbitrairement, on place le point A d'abscisse a et le point b d'abscisse b (a et b étant entiers il suffit de reporter correctement). On se propose de construire sur cette graduation le point d'abscisse $\frac{a}{b}$.



[5] Un nombre entier naturel différent de 1 est premier si il n'est divisible que par 1 et par lui-même. Par exemples 2, 3, 5, 7 et 11 sont premiers, 24 ne l'est pas (il est divisible par 1, 2, 3, 4, 6, 12 et 24).

Pour faire cette construction que les Grecs connaissaient déjà on va utiliser le théorème de Thalès.

1) On considère un repère orthonormal (0 ; I, J). On a : OI = OJ = 1 (c'est-à-dire une unité, arbitrairement choisie).



Placer le point A tel que OA=7 et le point B tel que OB=4.

On se propose de construire le point M de la demi-droite [OI) tel que $OM=\frac{7}{4}$.

2) La parallèle à (BJ) passant par A coupe (OJ) en L. Démontrer que $OL=\frac{OA}{OB}=\frac{7}{4}$.

3) La parallèle à (IJ) passant par L coupe [OI) en M. Démontrer que $OM=\frac{OA}{OB}=\frac{7}{4}$

4) Reprendre cette construction avec OA=5 et OB=8.

5) Application : construire une autre figure avec OA=9 (9 unités) et utiliser la méthode ci-dessus pour partager le segment [OA] en 7 segments de même longueur.

On conçoit qu'avec cette construction il est possible de représenter tous les nombres du type $\frac{a}{b}$, *où* a et b *sont des entiers naturels. En fait, cette construction fonctionne également avec des entiers relatifs ; en particulier si on choisit a et b négatifs la construction permet de voir que* $\frac{a}{b}$ est *positif.*

Conclusion : une unité ayant été choisie, la fraction est ici représentée par le segment [OM].

APPROXIMATION DE $\sqrt{2}$ PAR DES NOMBRES RATIONNELS METHODE PAR FRACTIONS CONTINUES

Première partie

Expliquez par un calcul numérique les résultats présentés dans la première phrase du deuxième paragraphe du texte historique ci-joint, à savoir :

> « *Le jour entier contient 86400'', et l'excès de l'année tropique sur l'année commune, ou 5h48'50'', en contient 20930* ».

On vous propose dans cette question de retrouver la décomposition de la fraction $\frac{8640}{2093}$ en la fraction continue :

$$4+\cfrac{1}{7+\cfrac{1}{1+\ldots\text{etc}}}$$

1) Complétez les égalités suivantes en calculant les nombres entiers manquants :

$\frac{8640}{2093}=4+\frac{\ldots\ldots}{2093}$

$\frac{8640}{2093}=4+\cfrac{1}{\cfrac{2093}{\ldots\ldots}}$

$\frac{8640}{2093}=4+\cfrac{1}{7+\cfrac{\ldots\ldots}{\ldots\ldots}}$

$\frac{8640}{2093}=4+\cfrac{1}{7+\cfrac{1}{\cfrac{\ldots\ldots}{\ldots\ldots}}}$

$\frac{8640}{2093}=4+\cfrac{1}{7+\cfrac{1}{1+\cfrac{\ldots\ldots}{\ldots\ldots}}}$

$\frac{8640}{2093}=4+\cfrac{1}{7+\cfrac{1}{1+\cfrac{1}{\cfrac{\ldots\ldots}{\ldots\ldots}}}}$

Ecrivez l'étape suivante.

On dit que l'on réduit ainsi la fraction $\frac{8640}{2093}$ en fraction continue.

2) a) Ecrivez sous la forme d'une fraction irréductible les nombres :

$r_0=4$ $\quad r_1=4+\frac{1}{7}$ $\quad r_2=4+\cfrac{1}{7+\cfrac{1}{1}}$ $\quad r_3=4+\cfrac{1}{7+\cfrac{1}{1+\cfrac{1}{4}}}$

b) Les nombres r_0, r_1, r_2, r_3, ... sont des approximations de la fraction $\frac{8640}{2093}$ qui représente « *le rapport du jour entier à l'excès de l'année tropique sur l'année commune* ». Reconnaissez-vous parmi les nombres précédents celui qu'utilisaient les Perses ?

c) r_3 est une approximation de $\frac{8640}{2093}$. Montrer que la distance [6] entre $\frac{8640}{2093}$ et r_3 est inférieure à 2×10^{-4} [7].

---

[6] La distance entre deux nombres réels x et y est égal à la différence entre le plus grand et le plus petit, c'est donc un nombre positif ou nul.

[7] On dit que r_3 est une approximation de $\frac{8640}{2093}$ avec une précision de 2×10^{-4}.

Deuxième partie

1) La partie entière de $\sqrt{2}$ est 1. Trouvez une expression simplifiée de l'inverse de $1+\sqrt{2}$.
En déduire que :

$$\sqrt{2} = 1 + \frac{1}{1+\sqrt{2}} \text{ puis que } \sqrt{2} = 1 + \frac{1}{2 + \frac{1}{1+\sqrt{2}}}$$

Trouvez, ainsi de suite, des expressions de $\sqrt{2}$ où figurent 3, 4, 5 traits de fraction et les nombres 1, 2 et $\sqrt{2}$.
Vérifiez avec la machine que ces expressions sont égales à $\sqrt{2}$.
Notez, pour la dernière, la séquence tapée sur la ligne de commandes.

2) Une suite de nombres rationnels est définie par :

$a_0=1$ $\quad a_1=1+\frac{1}{2}$ $\quad a_2=1+\frac{1}{2+\frac{1}{2}}$ $\quad a_3=1+\frac{1}{2+\frac{1}{2+\frac{1}{2}}}$ (3 traits de fraction, 3 chiffres 2, 4 chiffres 1)

et pour tout entier n non nul :

$$a_n = \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{\ddots}}}} + \cfrac{1}{2+\cfrac{1}{2+\frac{1}{2}}}$$

n traits de fraction,
n chiffres 2,
n+1 chiffres 1.

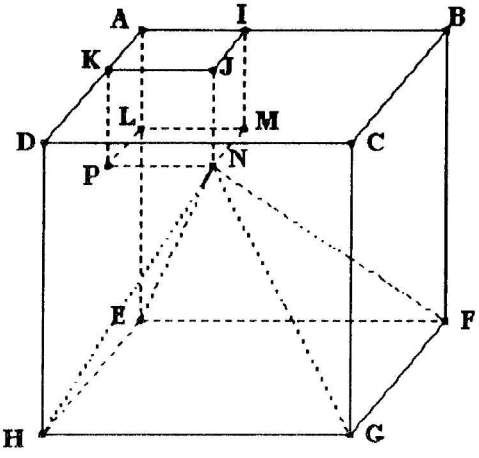
Ecrivez sous la forme d'une fraction irréductible les nombres a_1, a_2, a_3, puis les nombres $1+\frac{1}{1+a_0}$ et $1+\frac{1}{1+a_1}$.
En déduire une expression de a_3 en fonction de a_2. Que remarquez-vous ?
Ces égalités suggèrent une expression de a_{n+1} en fonction de a_n. Laquelle ?
En déduire, à l'aide de la TI-92, l'expression de a_4, a_5, a_6, a_7, et a_8 sous forme de fraction irréductible.
a_8 est une approximation de $\sqrt{2}$. Avec quelle précision (voir première partie 2)c)) ?

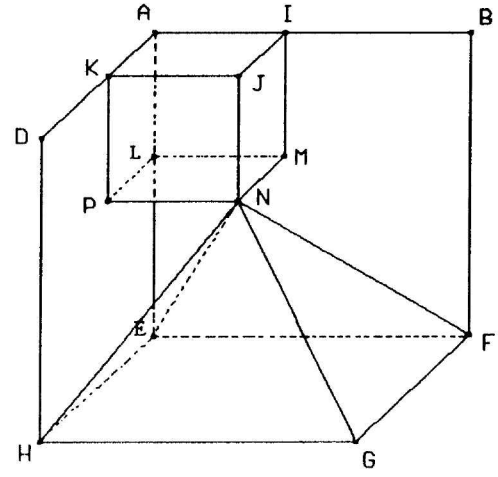
En suivant la démarche précédente trouver un nombre a_n qui fournit une approximation de $\sqrt{2}$ avec 10 décimales exactes.

TP N°6 : INTERSECTION DE DEUX COURBES (1)

Applications utilisées : *l'application graphique et l'application initiale.*

Préparation de la TI92 : *s'assurer que* EXACT *et* FUNC *figurent sur la ligne d'état.*





On considère un cube ABCDEFGH d'arête 8 cm. Sur l'arête [AB] on considère un point variable I. On pose AI = x. On construit le cube AIJKLMNP; on obtient ainsi la pyramide à base carrée NEFGH (voir figures ci-dessus).

On se propose de montrer qu'il existe une position du point I sur [AB] telle que le volume du cube AIJKLMNP *soit égal au volume de la pyramide* NEFGH.

Préliminaire

- Lorsque I est en A, que devient le cube ? Quel est le volume de la pyramide ?
- Lorsque I est en B, quel est le volume du cube ? Que devient la pyramide ?
- Lorsque I est au milieu de [AB], comparez les volumes du cube et de la pyramide ?

Première partie

1) Exprimez le volume du cube AIJKLMNP en fonction de x ; précisez, en utilisant les informations de l'énoncé, l'intervalle auquel x appartient.
Exprimez le volume de la pyramide NEFGH en fonction de x.

2) On considère les fonctions f et g définies sur [0,8] par $f(x) = x^3$ et $g(x) = \frac{64}{3}(8 - x)$.

Tracez les courbes d'équations $y = f(x)$ et $y = g(x)$. dans une même fenêtre graphique.
Choisissez une fenêtre qui permette de conjecturer le nombre de solutions au problème ; notez cette fenêtre sur le cahier et justifiez son choix.
Proposez, par lecture graphique, un encadrement d'amplitude 1 de chaque solution éventuelle.

3) Validez votre conjecture dans **l'application initiale** ; précisez les commandes utilisées.

TP N°6 : INTERSECTION DE DEUX COURBES (2)

Deuxième partie

1) ✍ Démontrez que résoudre $f(x)=g(x)$ revient à résoudre $P(x)=0$ avec : $P(x)=3x^3 + 64x - 512$.

2) 📻 Construisez sur l'intervalle [0,8] la représentation graphique de la fonction P.

✍ Expliquez pourquoi le graphique précédent suggère l'existence d'une solution à l'équation $P(x)=0$.

On admet désormais que cette équation a une solution unique sur l'intervalle [0,8], on la note x_0.

3) ✍/📻 On se propose de déterminer un encadrement d'amplitude inférieure ou égale à 10^{-2} du nombre x_0.

Pour cela on va utiliser la représentation graphique de P sur différents intervalles.

On sait que $P(x_0)=0$, $P(4)<0$, $P(5)>0$; les propriétés de la fonction P permettent de dire $4< x_0 <5$.

Le centre de l'intervalle [4 ;5] est 4,5 ; graphiquement on peut dire que $P(4)<0$ et $P(4,5)>0$. On peut en déduire comme précédemment que $4< x_0 <4,5$.

On recommence ainsi de suite [8], en utilisant %, jusqu'à ce que l'encadrement de x_0 ait une amplitude inférieure ou égale à 10^{-2}.

Pour présenter les calculs utilisez le tableau de la page 3 où figurent les indications nécessaires pour construire les différentes courbes.

Retour au problème

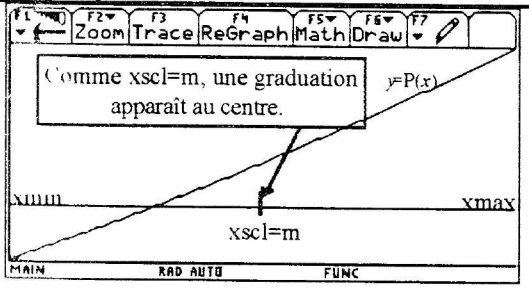
Donner une réponse au problème initial.

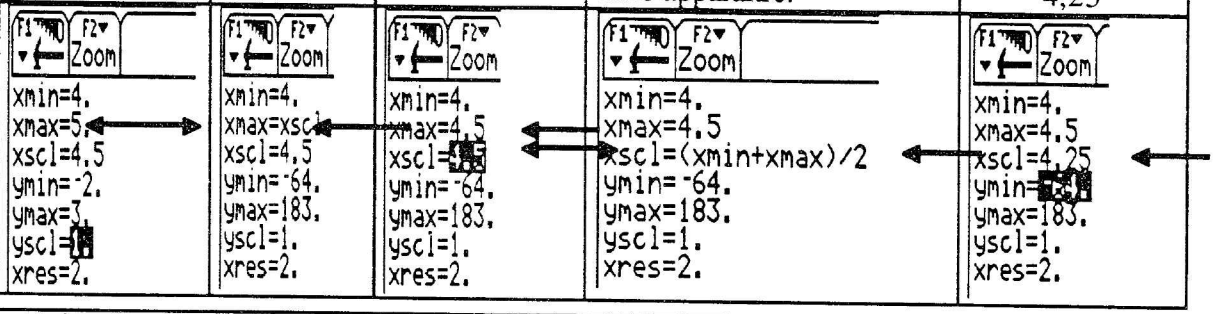
---

[8] Le procédé utilisé ci-dessus pour trouver un encadrement de x_0 est la **dichotomie** du grec Dikhotomia : « division en deux parties égales ». Il permet d'obtenir un encadrement de x_0 dont l'amplitude peut être aussi petite que l'on veut.

TP N°6 : INTERSECTION DE DEUX COURBES – APPROXIMATION DE x_0 PAR DICHOTOMIE

	Fenêtre N°1	Etape 1	Résultat	Etape N°2	Fenêtre N°2
On pourra commencer par tracer la courbe dans la fenêtre N°1 puis faire ZoomFit pour obtenir le graphique ci-dessus.	xmax: Taper xscl puis ENTER		xmax prend la valeur 4,5	xscl: taper (xmin+xmax)/2 pour calculer le centre et le faire apparaître.	Le centre de [4 ;4,5] est 4,25





Indications : 1) Lorsque xscl prend la valeur $\frac{xmin+xmax}{2}$ une graduation permettant de repérer le centre de l'intervalle apparaît à l'écran. De plus, c'est la machine qui calcule et mémorise sa valeur.

2) Au lieu de taper en toutes lettres xscl, xmin et xmax on peut taper les nombres observés avec des risques d'erreurs de frappe lorsqu'il y a beaucoup de décimales.

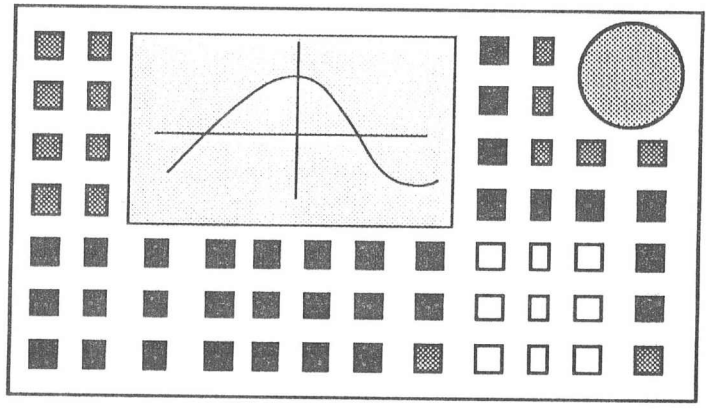
3) Afin d'améliorer la lecture on fera ZoomFit (F4 A) après chaque graphique.

xmin	xmax	Centre $m=\frac{xmin+xmax}{2}$	Signe de P(xmin)	Signe de P(m)	Signe de P(xmax)	Encadrement	Amplitude de l'encadrement inférieure ou égale à
4	5	4,5	–	+	+	$4< x_0 <4,5$	0,5
4	4,5	4,25	–	–	+	$< x_0 <$	
						$< x_0 <$	
						$< x_0 <$	
						$< x_0 <$	
						$< x_0 <$	
						$< x_0 <$	
						$< x_0 <$	
						$< x_0 <$	
						$< x_0 <$	

DE L'IMPORTANCE DE L'ENVIRONNEMENT POUR LA RECHERCHE EN MATHÉMATIQUES

Luc Trouche
Groupe Analyse

Les journées IREM de Juin 1997, consacrées au "calcul", ont été aussi l'occasion de réfléchir à l'influence des nouveaux outils de calcul sur les procédures de recherche en mathématiques. L'atelier dont il est question ici a proposé une recherche dans un environnement TI-92 [9]. Il s'agissait de déterminer le nombre de dérangements d'un ensemble ordonné de n éléments.



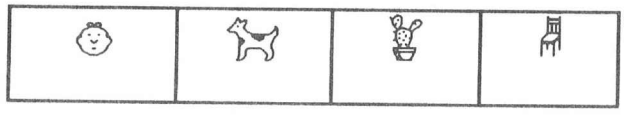
I. UNE DEFINITION ET UNE PREMIERE RECHERCHE "ARTISANALE".

Un dérangement est défini comme une permutation sans point fixe. Par exemple, il existe 2 dérangements pour 3 objets :

- un dérangement
- et l'autre

Nous savons qu'il y a n! permutations pour n objets. Parmi ces permutations, combien de dérangements possibles ? Appelons u(n) ce nombre. Pour n petit, il est facile de compter : u(1) = 0 (c'est assez évident), u(2) = 1, u(3) = 2 (nous l'avons compté ci-dessus). Comment poursuivre ? Nous avons au moins deux pistes possibles :

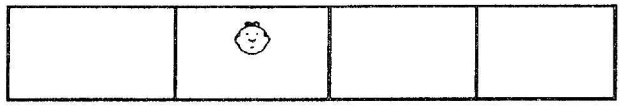
- on peut ôter de n! le nombre de permutations qui ont exactement un point fixe, le nombre de permutations qui ont exactement deux points fixes, etc. [10] ; la réalisation d'un tel calcul est assez délicate. Nous y reviendrons à la fin de cet article ;
- on peut essayer de trouver une relation de récurrence en réfléchissant aux mécanismes de passage d'un rang au rang suivant. Voyons ce qui se passe par exemple pour le calcul de u(4) :



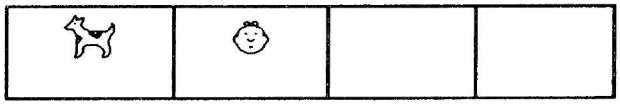
Le bonhomme peut être placé à la seconde, troisième ou quatrième place. Ces trois positions sont équivalentes pour la suite des calculs. Aussi, il nous suffit de compter les dérangements

[9] Calculatrice de Texas Instruments, pourvue en particulier d'un logiciel de calcul formel Derive.
[10] On trouvera l'exploitation de cette piste dans Tissier, 1991, *Mathématiques générales*, pp. 53-54, Éditeur Bréal.

avec le bonhomme à la seconde place, et nous multiplierons le nombre trouvé par 3 pour obtenir u(4).

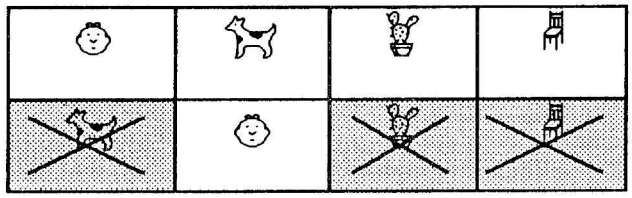


- on peut soit mettre le chien à la première place :



(il nous reste alors à réaliser un dérangement pour le cactus et le fauteuil, qui sont isolés à la troisième et quatrième place : u(2) possibilités).

- ou alors on peut mettre le chien à la troisième ou la quatrième place :



(alors nous avons un dérangement à réaliser pour 3 objets : pour chacun d'entre eux, il y a une place interdite ; ainsi nous avons u(3) possibilités).

Conclusion : u(4) = 3[u(2)+u(3)] = 9. Nous pouvons aisément généraliser :

$$\mathbf{u(n) = (n-1)\ [u(n-1) + u(n-2)]}$$

II. LA RECHERCHE D'UNE EXPRESSION GENERALE.

Deux méthodes (au moins...) sont possibles :

- on peut utiliser les séries formelles en posant $S(x) = \sum_{k=0}^{\infty} \frac{u(k)}{k!} x^k$.

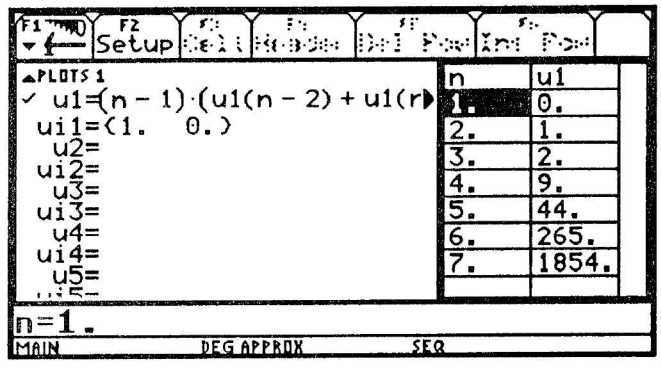
L'exploitation de la relation de récurrence nous permet alors d'obtenir une équation différentielle, d'en déduire S(x) et le coefficient de x^k, donc u(k), à partir des développements en série usuels ;

- on peut aussi, dans un environnement TI-92 (ou autre calculatrice), se livrer à des observations numériques ou graphiques d'un échantillon de valeurs de la suite :

La suite u(n) est entrée dans le fichier de suites (elle apparaît ci-contre incomplètement sur la partie gauche de l'écran).

Une table de valeurs permet d'observer le comportement des premiers termes.

On peut alors opérer une comparaison interne ou externe des termes de la suite.

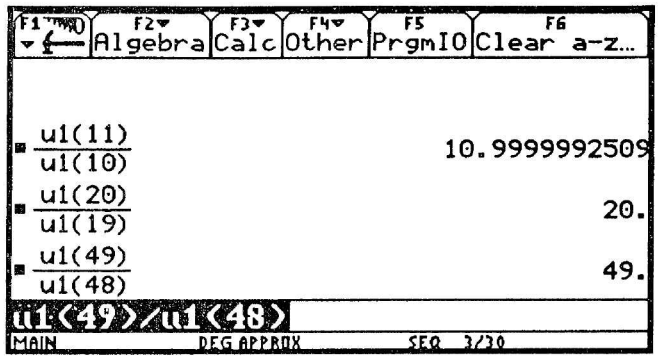


Une comparaison "interne" consiste à rechercher des régularités dans le déroulement de la suite : est-elle arithmétique, géométrique ou quasi-géométrique... Ceci peut nous amener à faire les quotients des termes successifs :

Une telle observation débouche assez facilement sur le fait que le rapport de u(n) et de u(n-1) ressemble à n (attention, dans l'application "suites", la TI-92 fonctionne toujours en calcul approché).

Cela peut induire l'idée que u(n) est du type k.n!

On pourrait alors considérer la suite n!/u(n).

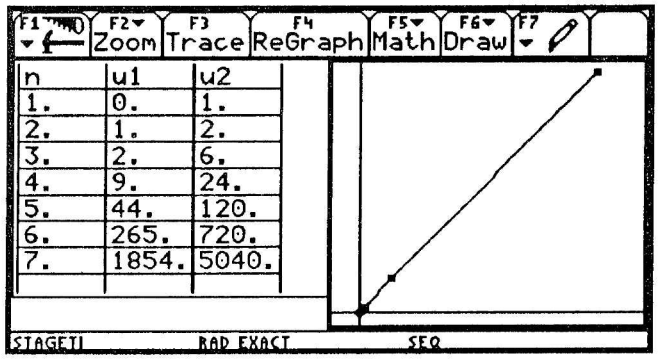


On peut aussi procéder à une comparaison "externe", en confrontant u(n) à une suite "naturellement proche". S'agissant des dérangements, on peut comparer u(n) à la suite des permutations n!.

La suite u1 représente la suite u(n), la suite u2 représente la suite n!.

On peut observer à droite quelques points de coordonnées (u(n), n!). Il semble bien que ces points soient alignés, ce qui traduit la quasi-proportionnalité des deux suites u(n) et n!.

Peut-on estimer le coefficient de "quasi-proportonnalité ?"



On peut avoir une information par le recours à une étude statistique : la recherche de la droite de régression ajustant le nuage de points nous donne le résultat cherché :

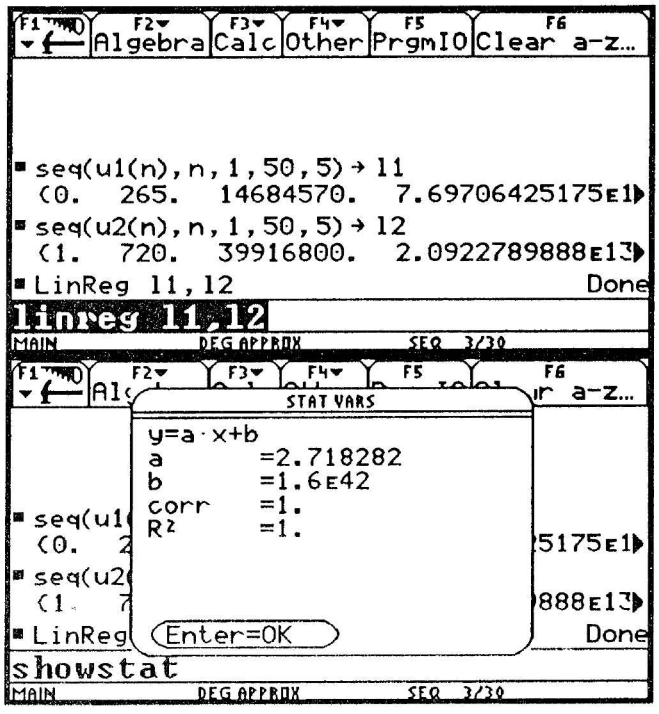
Quelques valeurs des suites u1 et u2 sont stockées dans deux listes L1 et L2 ; on demande ensuite à la calculatrice d'opérer une régression linéaire entre ces deux suites.

Les résultats apparaissent ci-dessous.

Le coefficient de "quasi-proportionnalité" ressemble à un nombre bien connu : e.

Ceci reste bien sûr du domaine de la conjecture.

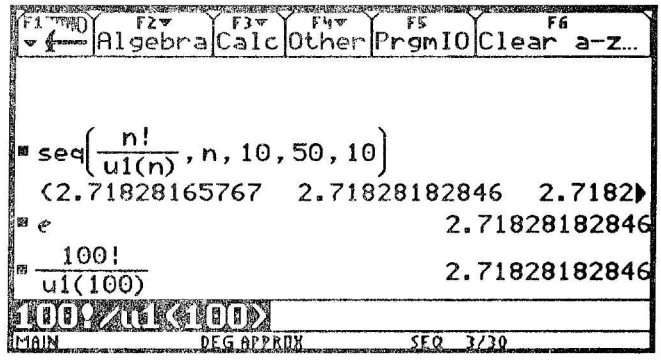
On peut alors soit en revenir à une étude théorique, soit pousser la curiosité un peu plus loin, en regardant si cette même régularité est confirmée hors étude statistique.



Cela nous conduit (comme nous auraient conduit aussi les procédures de comparaison interne de la suite) à considérer la suite $\frac{n!}{u(n)}$.

La conjecture est bien "validée" par l'observation numérique qui fait apparaître une grande proximité entre la suite $\frac{n!}{u(n)}$ et e.

La calculatrice, pour la précision qui est la sienne, identifie d'ailleurs les deux valeurs pour n = 100.



III. UNE CONJECTURE ET SA VALIDATION.

Formulons précisément cette conjecture : la suite u(n) cherchée semble être égale au produit de n! et d'une suite v(n) dont la limite serait $\frac{1}{e}$. On dispose pour v(n) de plusieurs candidates (la liste n'est évidemment pas exhaustive...), par exemples :

$$v(n) = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \quad \text{ou} \quad v(n) = (1+\frac{1}{n})^{-n}.$$

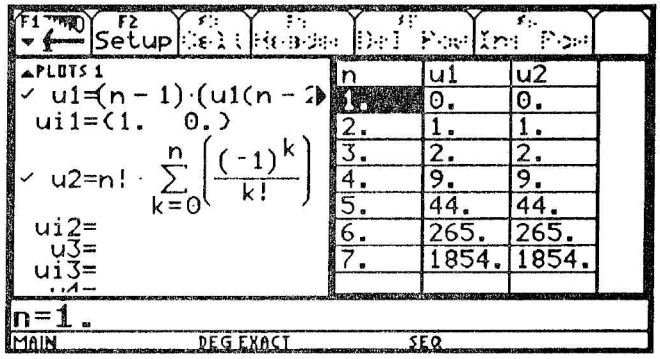
La première suite est une bonne candidate car le produit de n! et de v(n) doit être un nombre entier. A-t-on bien $u(n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$?

Une vérification pour les premiers termes est aisée :

En u2, la suite $n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

L'observation de la table indique bien la coïncidence des deux suites pour les premières valeurs de n.

Le fonctionnement en calcul approché du tableau de valeurs n'empêche pas de conclure à l'égalité des valeurs affichées : en effet, par construction, les deux suites ne prennent que des valeurs entières.

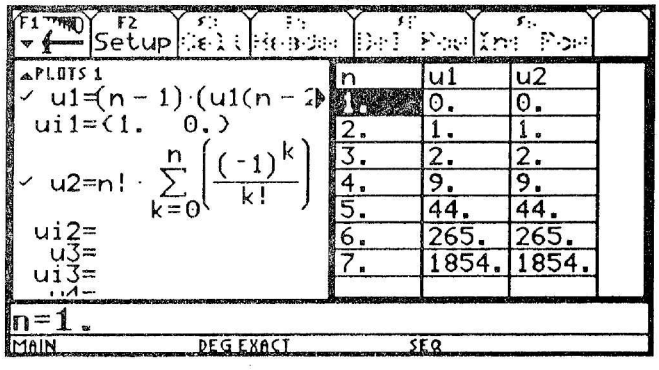


D'où la possibilité de conclure à la coïncidence des deux suites pour les premières valeurs.

Pour autant, peut-on en conclure que la suite u(n) est bien égale à $n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$?

On peut évidemment faire d'autres tests avec la calculatrice :

- on peut observer ci-contre qu'au rang 50 on retrouve l'égalité des valeurs ;
- par contre, la calculatrice annonce que u1(100) est différent de u2(100)...



Cela découle des mécanismes de calcul approché et du cumul des erreurs pour le calcul des termes de u2.

La validation de notre conjecture ne peut venir que d'un raisonnement par récurrence, qui nécessite un travail "papier/crayon". Il suffit de vérifier que :

si $u(n-2) = n! \sum_{k=0}^{n-2} \frac{(-1)^k}{k!}$ et $u(n-1) = n! \sum_{k=0}^{n-1} \frac{(-1)^k}{k!}$, alors on a $u(n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$ nécessairement. Le calcul, qui ne présente pas de difficultés théoriques majeures, est laissé à la charge du lecteur.

On peut bien conclure maintenant que le nombre de dérangements de n objets est :

$$u(n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} .$$

Le lecteur curieux pourra constater que cette expression peut aussi se mettre sous la forme : $u(n) = n! - C_n^1 (n-1)! + C_n^2 (n-2)! + \ldots + (-1)^p C_n^p (n-p)! + \ldots + (-1)^n$. Cette expression est tout simplement le résultat du calcul envisagé dans le premier paragraphe, consistant à retrancher du nombre total de permutations les permutations à points fixes. Cette identification, reposant sur les résultats fondamentaux du dénombrement [11], est laissée aussi au soin du lecteur.

IV. QUELQUES ENSEIGNEMENTS.

Ce qui précède n'est qu'une trame. On peut en tirer plusieurs scénarios pour application dans une classe de Terminale ou post bac. L'intérêt de cette trame est qu'elle fait ressortir l'importance des changements de points de vues dans la recherche mathématique : observations graphiques et numériques, conjectures issues du croisement de ces observations et des références théoriques (pour les suites qui convergent vers e par exemple), validations partielles, et aboutissement du travail par une démonstration "en bonne et due forme". **On peut voir aussi à travers cette activité l'importance des environnements calculatrices pour supporter et même développer de tels comportements de recherche.**

La mise en musique des différents scénarios n'est évidemment pas indifférente au succès de l'entreprise : il faut laisser du temps au temps pour que la recherche propre des élèves puisse se développer ; on peut susciter aussi le travail en petits groupes et la mise en commun des résultats partiels pour que personne ne reste bloqué trop longtemps [12].

Essayer et voir !

Petite bibliographie

Quelques références où on pourra trouver d'autres idées de recherche avec les élèves ou des réflexions plus théoriques sur l'enseignement des mathématiques en "environnement calculatrice".

Enseigner les mathématiques en TS avec des calculatrices graphiques et formelles (deux volumes) (1996, IREM de Montpellier)

L'intégration de calculatrices symboliques en lycée, un défi mathématique (1997, CRDP de Montpellier)

A propos de l'enseignement des limites dans un "environnement calculatrice", étude des rapports entre processus d'instrumentation et processus de conceptualisation (1997, IREM de Montpellier).

---

[11] Card(A∪B) = CardA + CardB - Card(A∩B) bien sûr.

[12] Il est évident par exemple qu'il est plus facile de "reconnaître" e que $\frac{1}{e}$. Si des élèves ont échangé le rôle des deux suites dans l'étude de la régression linéaire, ils auront quelques difficultés à formuler une conjecture... Le croisement des résultats des différentes recherches est ici décisif !

DE LA FIGURE À LA REPRÉSENTATION GRAPHIQUE AVEC CABRI GÉOMÈTRE.

Robert Brunet, Jacques Naudeillo
Groupe Géométrie

INTRODUCTION

Ce travail s'inscrit dans la continuité de celui que nous avons présenté au Colloque Inter-IREM de Géométrie de 1994 [1], à savoir une réflexion sur les possibilités d'utilisation de l'ordinateur et du logiciel Cabri-Géomètre dans l'enseignement de la géométrie pour faciliter aux élèves la compréhension de certains concepts ; ici, il s'agit de la variation d'une grandeur en fonction d'une autre.

Cet exposé décrit de façon fixe des activités qui ne peuvent être envisagées que dans le cadre d'une animation que permet l'ordinateur, et comporte trois parties :

- une leçon faite dans une classe de troisième et visant à introduire les notions de fonction linéaire et de fonction affine à partir de droites tracées dans un repère ;

- une activité d'application réalisée dans la même classe de troisième visant à faire fonctionner les notions précédentes, et les prolongements auxquels nous ont conduit les questions des élèves ;

- des ouvertures possibles à différents niveaux et dans le même état d'esprit.

Le matériel utilisé en classe était composé d'un ordinateur couplé à une tablette rétro-projetable et d'un rétroprojecteur assez puissant pour que les images soient correctes sur le tableau ou sur un mur dans une salle semi-obscure.

II. FONCTIONS LINEAIRE ET AFFINE EN 3° - EQUATION D'UNE DROITE.

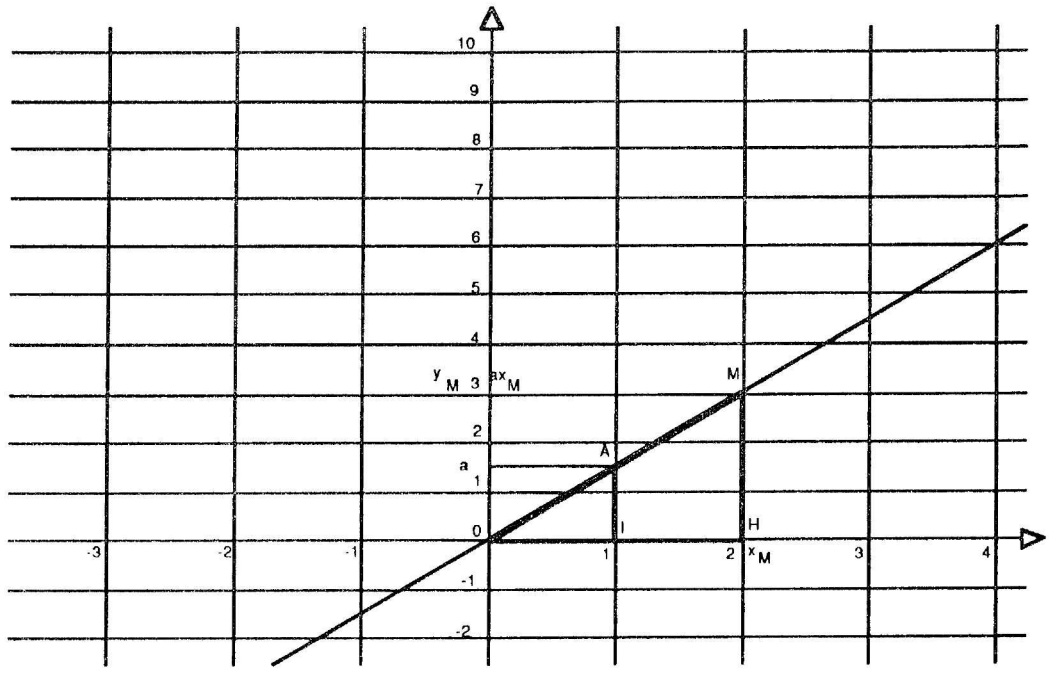
Cette activité a été réalisée dans une classe de 3° dans laquelle les élèves connaissent le parallélogramme, les transformations, les vecteurs, les coordonnées des points et les composantes des vecteurs ; ils ont de plus une pratique des énoncés de Thalés.

Il s'agit d'une leçon tout à fait classique avec, au tableau, agrandie, une figure réalisée avec Cabri - Géomètre sur un écran quadrillé à partir d'un repère orthogonal.

Partie I :

On trace la droite passant par l'origine du repère et un point A(1 ; a); on considère un point H sur l'axe des abscisses, et on lui associe M sur la droite (OA) ; on met en évidence y_M sur l'axe des ordonnées. Les élèves reproduisent la figure.

On déplace H, ce qui revient à faire varier x_M sur un intervalle contenant des positifs et des négatifs et on lit les valeurs correspondantes de y_M. On écrit les diverses valeurs dans un tableau que les élèves ont préparé sur leur cahier, ce qui permet de mettre en évidence le coefficient a et l'application du théorème de Thalés donne $y_M = a\ x_M$.

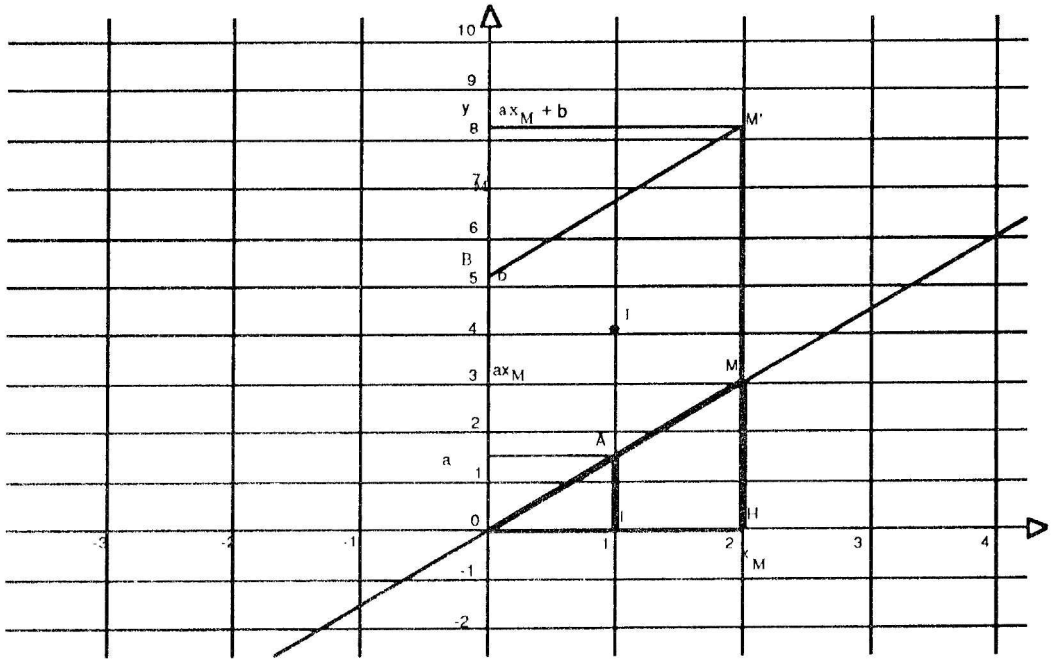


Application : on considère la droite passant par O et par M(3;4) ; lire puis calculer a.

On fait ensuite varier a sur l'écran, et la droite (OA) tourne autour du point O.
La variation de a change la direction de la droite passant par O.

Partie II :

On construit le point M' d'abscisse x_M et d'ordonnée y_M + b; la construction est effectuée par translation du point M, en plaçant M' comme quatrième sommet du parallélogramme OMM'B à l'aide du centre I de ce parallélogramme.



On construit ainsi la droite d'équation $y = a x + b$.

On fait alors varier a et b sur l'écran, ce qui permet de mettre en évidence les rôles respectifs du coefficient directeur a et de l'ordonnée à l'origine b.

III. APPLICATION A LA RESOLUTION D'UN PROBLEME.

Pour la séance suivante, on propose aux élèves le problème suivant:

On considère un rectangle ABCD tel que AB = 7 cm et AD = 3,5 cm, le point F du segment [AD] tel que DF = 1,5 cm, et le point E du segment [BC] tel que CE = 1,5 cm. Soit alors M un point du segment [AB], la parallèle à la droite (AD) passant par M coupe [FE] en I et [DC] en P.
On pose AM = x cm.

1°) Exprimer en fonction de x les aires des rectangles AFIM et PIEC.

2°) Représenter dans un même repère (sur une feuille de papier millimétré) les variations de chacune des aires.

3°) Calculer la valeur de x pour que ces aires soient égales.

4°) Vérifier sur le graphique.

A la séance suivante, on corrige ce problème en discussion avec les élèves :
- on écrit les aires en fonction de x, aire(AFIM) = 2 x et aire(PIEC) = 10,5 - 1,5 x ;
- les aires sont égales si 2 x = 10,5 - 1,5 x ; les élèves résolvent l'équation pour trouver x = 3.

On a donc les deux rectangles de même aire lorsque AM = 3 cm.

Les élèves ont tracé dans un repère les droites d_1 d'équation $y = 2 x$ et d_2 d'équation $y = 10,5 - 1,5 x$; on se rend compte qu'ils ont des difficultés dans la lecture du graphique et on essaie de les aider en utilisant l'ordinateur ; pour ce faire, nous avons plusieurs possibilités.

1°) A partir des dimensions des rectangles récupérées sur la figure - écran, on utilise une macro « produit » qui permet de refabriquer les deux droites dans un repère dessiné, et de retrouver la solution déjà calculée.

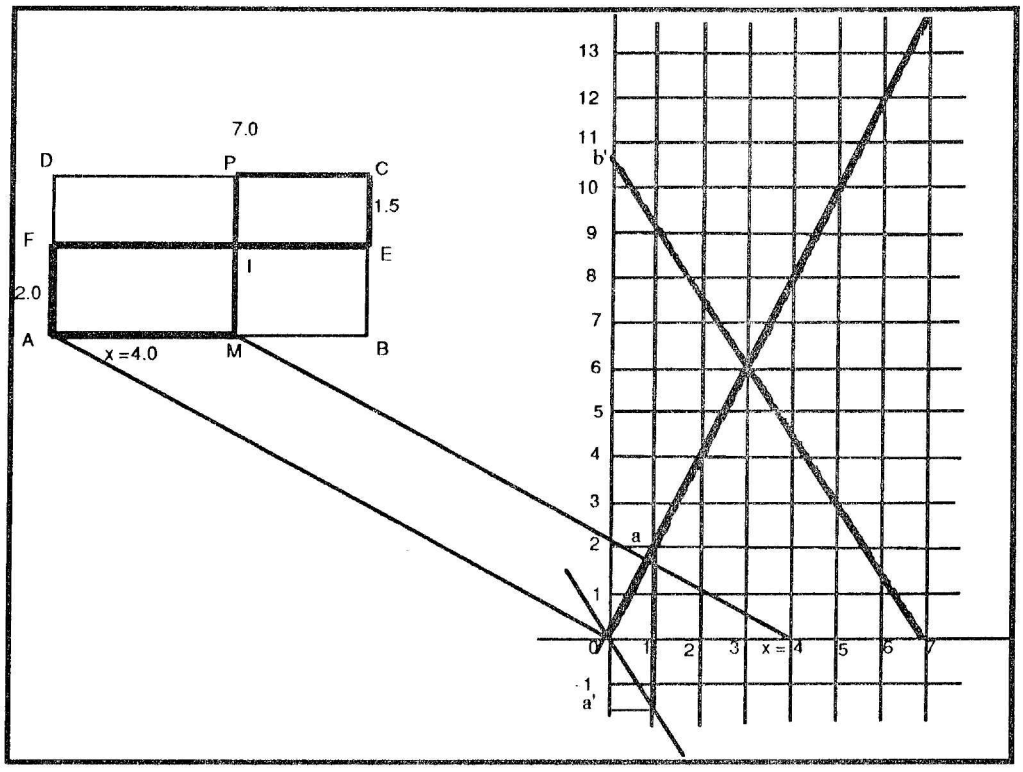
Inconvénient : la macro-construction fabrique les produits qu'elle représente par un segment, le tout restant caché : elle fabrique deux lieux ; les élèves ne voient pas les constructions et perdent le sens.

2°) Faire apparaître les deux droites à partir de leurs caractéristiques (coefficient directeur et ordonnée à l'origine). Faire varier x par report de la longueur AM sur l'axe des abscisses, ce qui permet de lire simultanément les valeurs de x et les deux aires ; on peut ainsi déplacer le point M pour l'amener à la position pour laquelle les aires sont égales.

Inconvénient : sur un même écran, une aire est visualisée par la surface associée, et représentée par un point, extrémité d'un segment. Se posera, pour les élèves, le problème du passage de la dimension 2 à la dimension 1 lors de l'animation de la figure.

3°) Faciliter le passage de l'aire à la longueur, en utilisant les constructions d'Euclide [2], reprises par Clairaut [3] et Descartes [4].

Nous choisissons de montrer aux élèves la 2° possibilité.

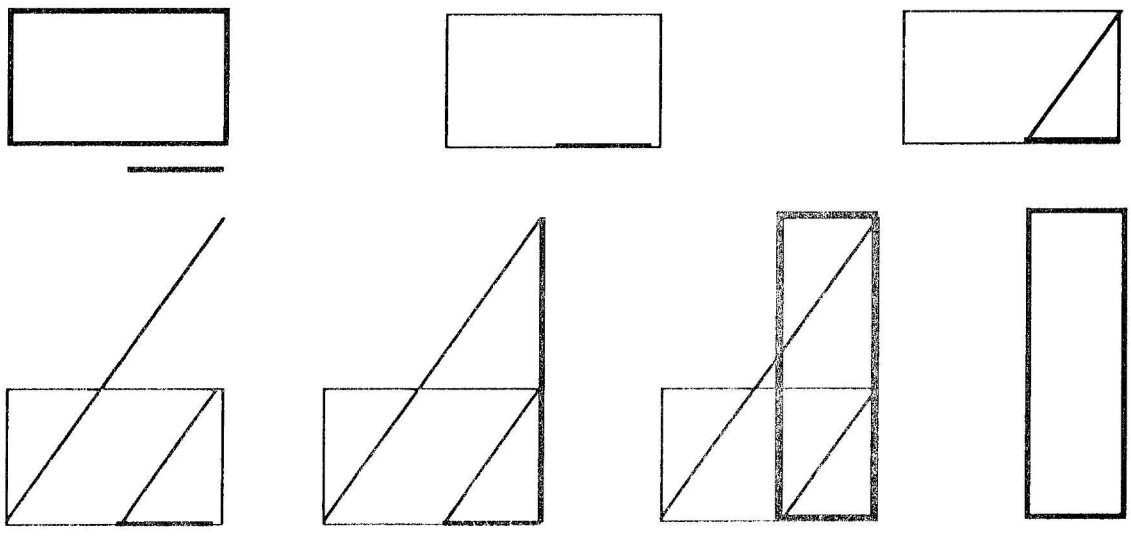


A la fin de l'animation commentée de la figure, une élève de la classe intervient : « Je comprends la figure avec l'évolution des rectangles, je comprends le dessin des deux droites, avec leur intersection, mais comment une aire devient la longueur d'un segment ? »

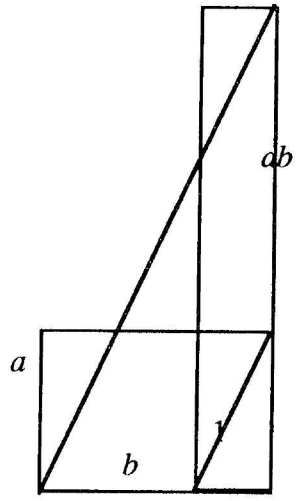
Elle met ainsi l'accent sur une difficulté réelle, numérique, et surtout graphique. A deux nombres, le produit, pour le calcul de l'aire, associe un seul nombre, et graphiquement, à une surface rectangulaire, on associe un segment dont la longueur est mesurée par le même nombre que l'aire.

Pour aider cette élève, nous sommes amenés à chercher dans les mathématiques d'une époque où le formalisme n'existait pas, et à utiliser la troisième possibilité envisagée.

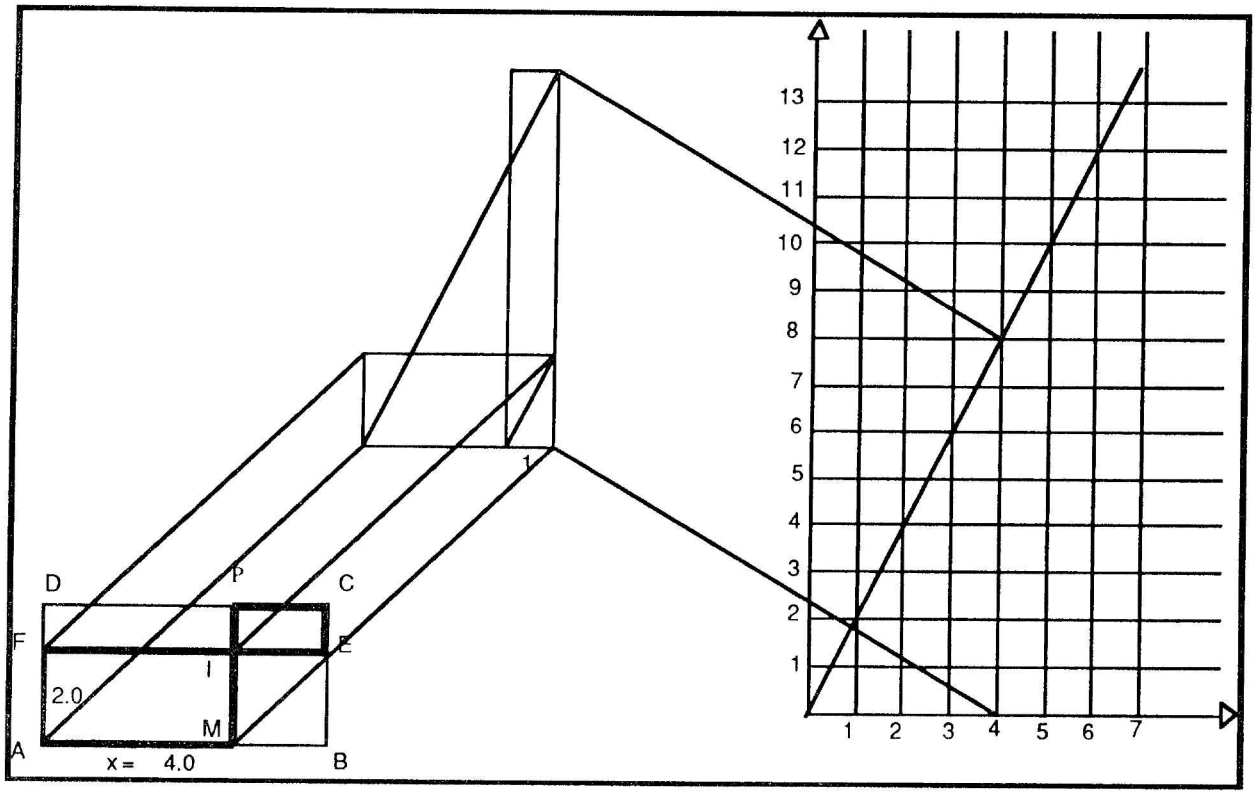
Le problème consiste à construire un rectangle qui a la même aire qu'un rectangle donné et une dimension fixée ; la solution est donnée par Clairaut [3] *en utilisant Thalés :*



On peut alors montrer aux élèves la construction dans le cas particulier où la dimension donnée est l'unité; on obtient sans intervention numérique et sans mesure, un segment dont la longueur est égale à l'aire d'un rectangle donné, donc au produit des longueurs de deux segments donnés.

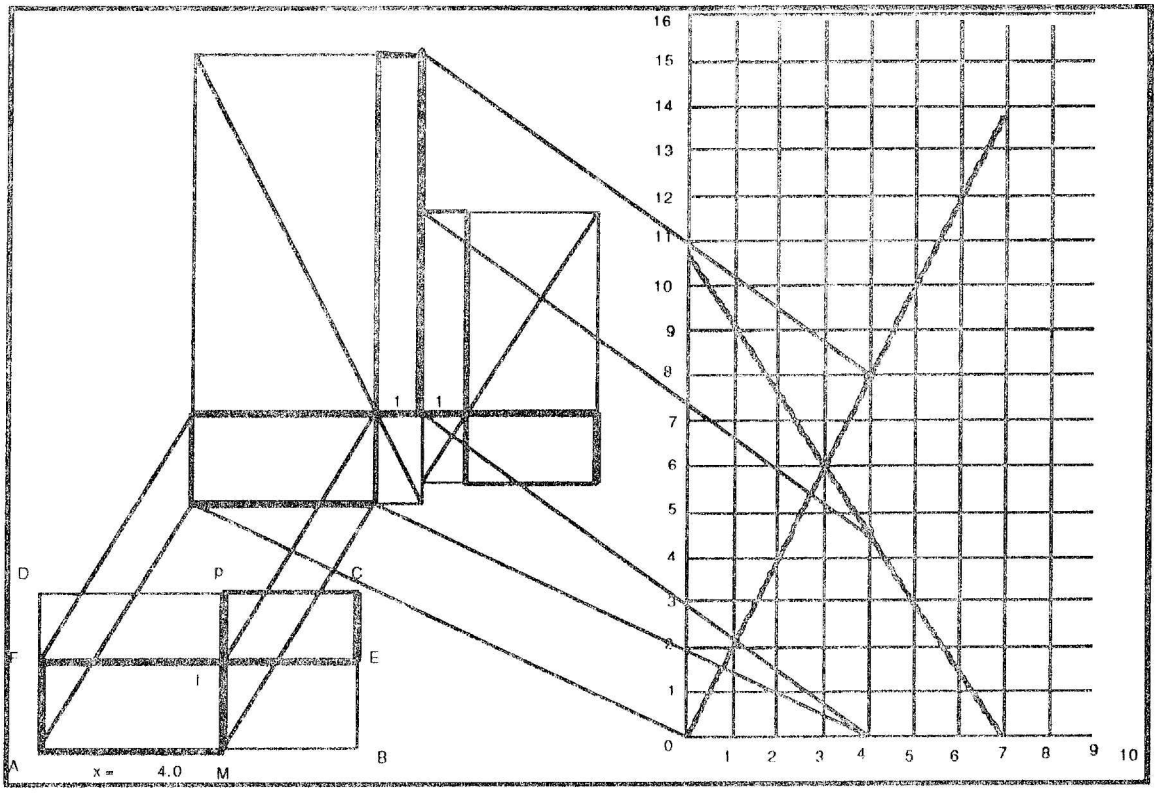


Les élèves ayant compris la construction précédente, nous l'appliquons aux deux rectangles étudiés dans le problème et nous reportons les diverses longueurs dans le graphique par des translations. Il est aisé de leur expliquer la construction complète, dont la complexité n'est qu'apparente, aprés avoir utilisé la construction de base sur un premier rectangle.

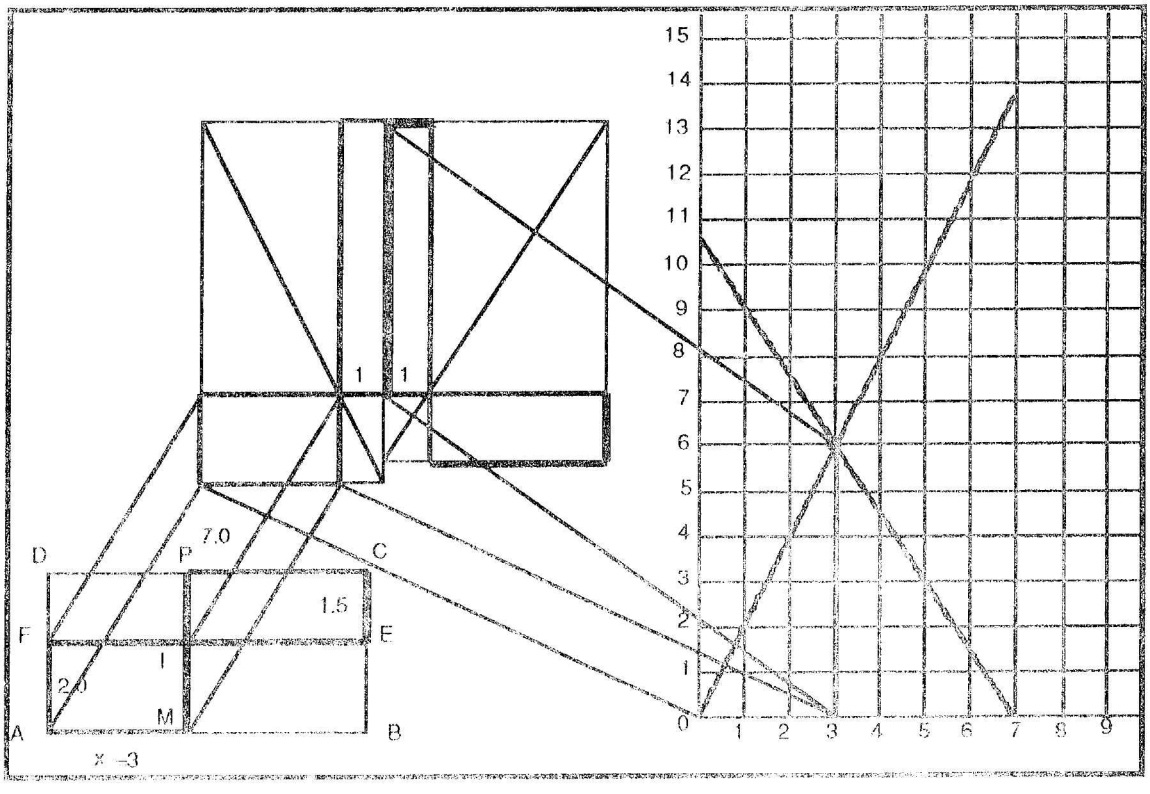


Construction de base expliquée pour le rectangle AMIF.

Construction complète :



Copie d'écran montrant la position de M pour laquelle les deux rectangles ont la même aire :



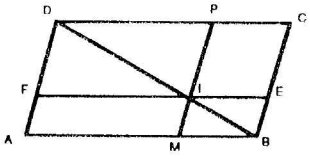
IV. RETOUR SUR UNE CONSTRUCTION D'EUCLIDE ET SES APPLICATIONS.

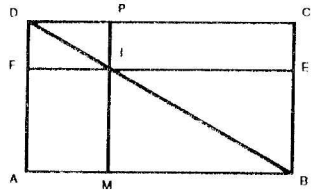
A - Proposition 43 des Eléments d'Euclide:

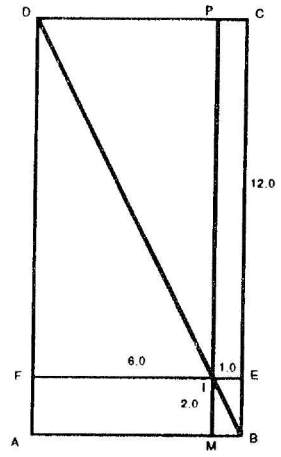
Nous l'avons dans un premier temps trouvée dans Clairaut [3] puis retrouvée dans les Eléments d'Euclide [2] sous la forme suivante :

Proposition 43 : « Dans tout parallélogramme, les compléments des parallélogrammes situés autour de la diagonale sont égaux. »

Une application intéressante de cet énoncé apparaît dans la troisième figure où un rectangle de dimensions 6 cm et 2 cm est remplacé par un rectangle dont un côté mesure 1 cm, le second côté mesurant alors 12 cm, ce qui permet de matérialiser par la longueur d'un segment le nombre mesurant l'aire du rectangle de départ.







Il est à noter que la démonstration de ce résultat est un exercice classique d'application des propriétés de la symétrie centrale en classe de 5°.

Cette proposition permet dés le début du collège d'utiliser la méthode précédente puisqu'il n'est plus nécessaire de connaître l'énoncé classique de Thalés.

B - Applications.

1°) Longueurs.

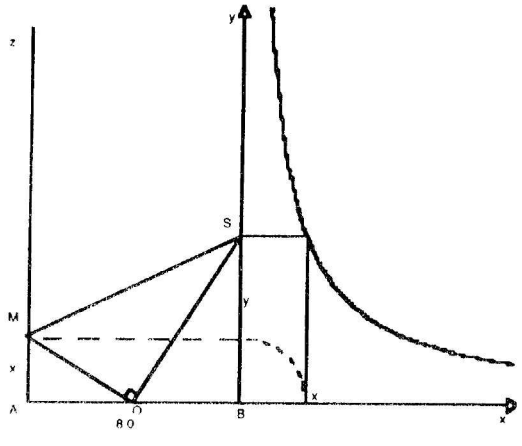
Pour des reports de longueurs, on n'a, bien sur, pas besoin de la méthode précédente. Le lien entre le dessin et la représentation graphique par la visualisation de translations, rotations et symétries, voire d' homothéties (changements d'unité pour mieux gérer l'écran) permet de donner plus de sens à l'expression « ...en fonction de x... »

Exemple en géométrie plane:

Soit M un point de la demi-droite [Az) et O le milieu du segment [AB]; on place S sur la demi-droite [By) de telle sorte que MOS soit un triangle rectangle en O.

Si on pose AM = x (x réel positif) et BS = y, il s'agit d'étudier les variations de y en fonction de x.

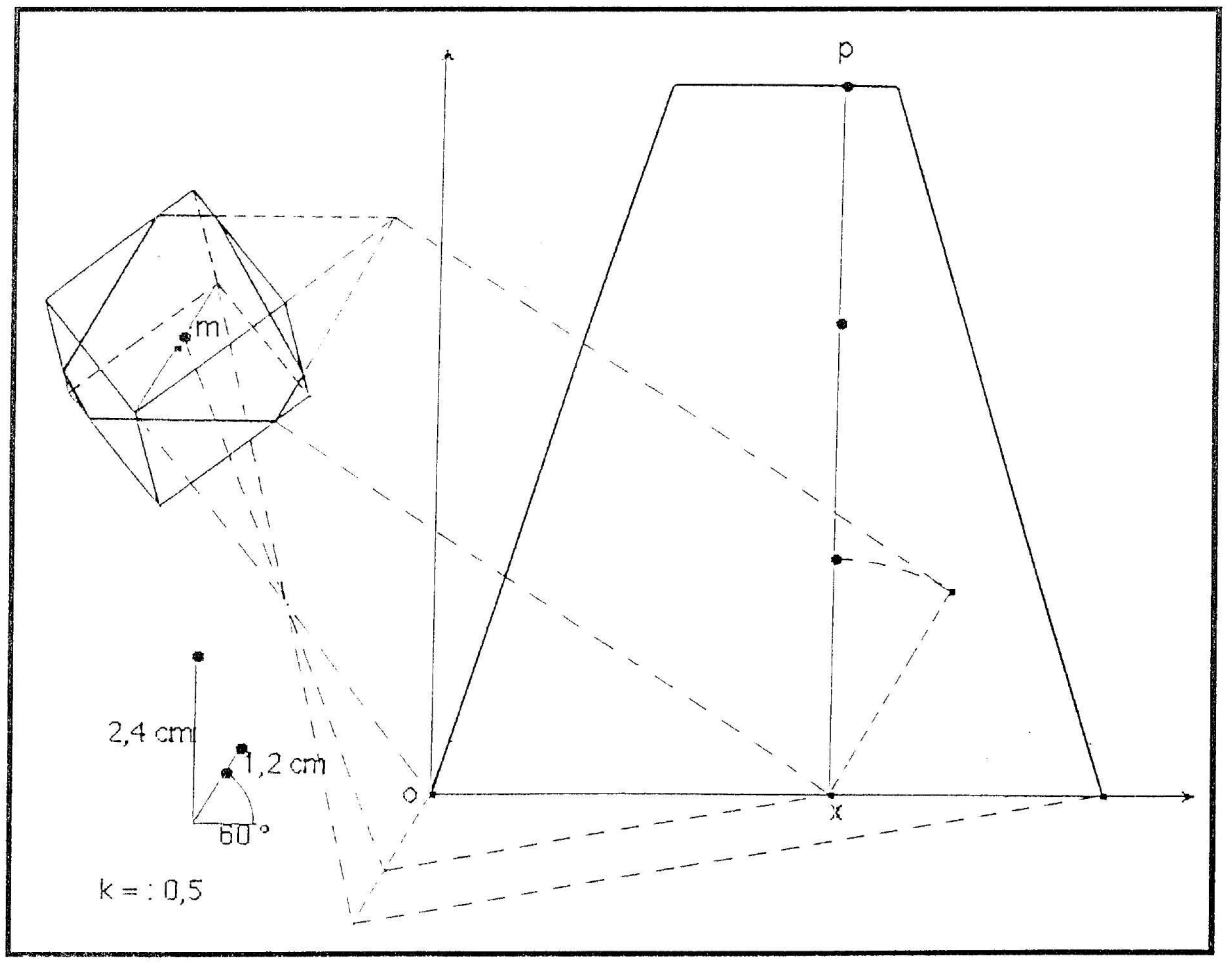
Ceci peut se faire quel que soit le niveau par animation de la figure (voir la copie d'écran à droite), l'écriture de y en fonction de x pouvant intervenir avec la trigonométrie dès la 3°.



Exemple en géométrie dans l'espace:

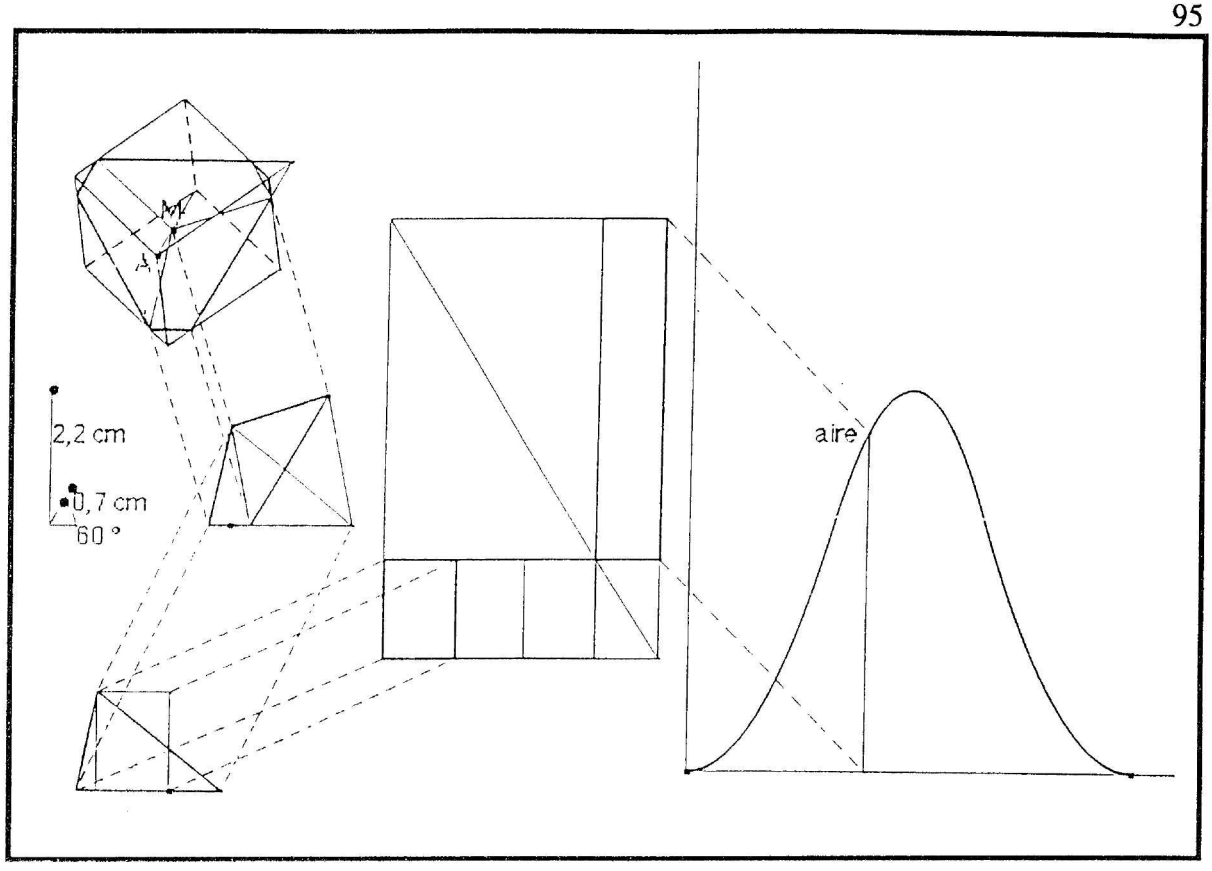
On est amené à positionner les objets pour avoir les dimensions en vraie grandeur, ce que nous avons développé dans [1], afin d'éviter d'avoir à réaliser des rabattements dont la complexité serait un obstacle dans la liaison entre la figure et la courbe.

La copie d'écran suivante illustre l'étude du périmètre de la section d'un cube par un plan perpendiculaire à une diagonale de ce cube, avec des conjectures intéressantes à l'arrivée, notamment lorsque la section est un hexagone.

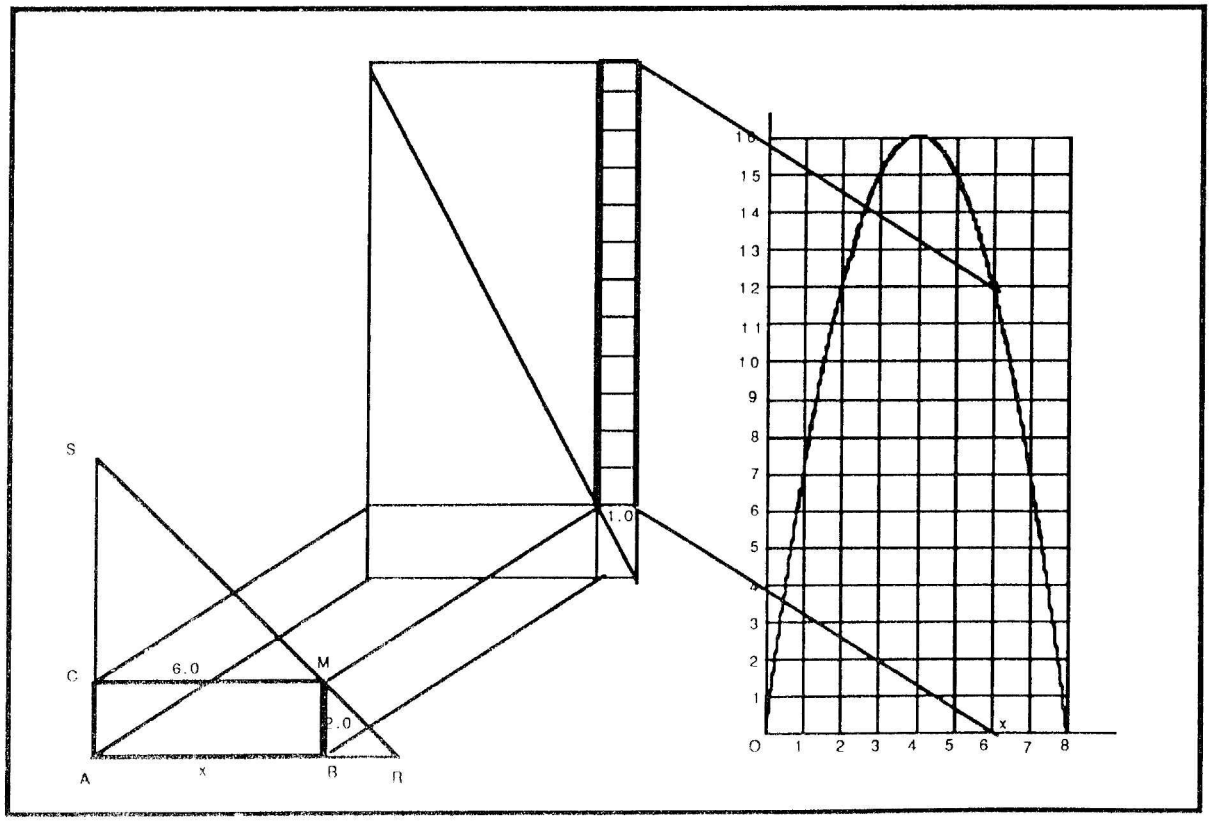


2°) Aires.

Dans l'exemple précédent de la section d'un cube par un plan perpendiculaire à une diagonale, on peut étudier l'aire de l'hexagone obtenu en fonction de la longueur AM. Pour cela (voir la figure sur la page suivante), on a besoin de transformer le quadrilatère tiers de l'hexagone étudié en un rectangle de même aire, et ceci en le transformant d'abord (méthode tirée de [5] page 97) en un triangle équivalent, qu'il est ensuite facile de transformer en rectangle; il reste alors à appliquer la construction du IV -A pour obtenir la courbe formée de trois morceaux de paraboles.



On pourra réaliser un exemple plus simple en étudiant l'aire d'un rectangle de périmètre constant.



3) Volumes.

On applique deux fois la construction de Euclide - Thalés, ce qui, sur la figure intermédiaire, permet de transformer un pavé de base quelconque en un pavé de même volume, mais dont l'aire de la base est l'unité.

Exemple : **Etude du volume d'un pavé construit dans un « tiers-de-cube ».**

On considère une pyramide "tiers de cube" FADHE de sommet F, dont la base est le carré ADHE de côté 9 cm, et de hauteur FE. Soit M un point de l'arête [FE]; on désigne par x la longueur ME exprimée en cm.

On coupe la pyramide par un plan parallèle à la base et passant par M.

a) Prouver que le quadrilatère MNPQ est un carré.

b) Les parallèles à (ME) passant par N, P et Q coupent la base respectivement en R, S et T. Quelle est la nature du solide MNPQERST ?

c) On vous propose d'étudier le volume de ce solide lorsque le point occupe des positions diverses sur le segment [EF].Pour cela on exprimera en fonction de x les longueurs MN et MQ et on écrira le volume V(x) du solide.

Sur la figure-écran Cabri-Géomètre fournie, déplacer M sur le segment [EF] et construire le lieu du point Vol pour conjecturer la valeur de x pour laquelle le volume du pavé est minimum.

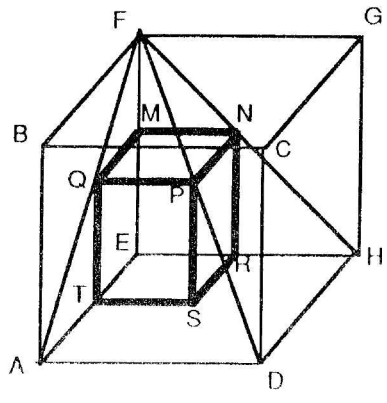
On construira un tableau de valeurs de V(x) pour x compris entre 0 et 9 et on en fera une représentation graphique sur une feuille de papier millimétré en prenant 2 cm pour unité sur l'axe des x , et sur l'axe des y (volume V) 1 cm pour 5 cm^3 .

On développera alors V(x), puis l'expression $A = (x - 3)^2(x - 12) + 108$, ce qui permettra de vérifier que la valeur de x pour laquelle le volume étudié est maximum est bien 3.

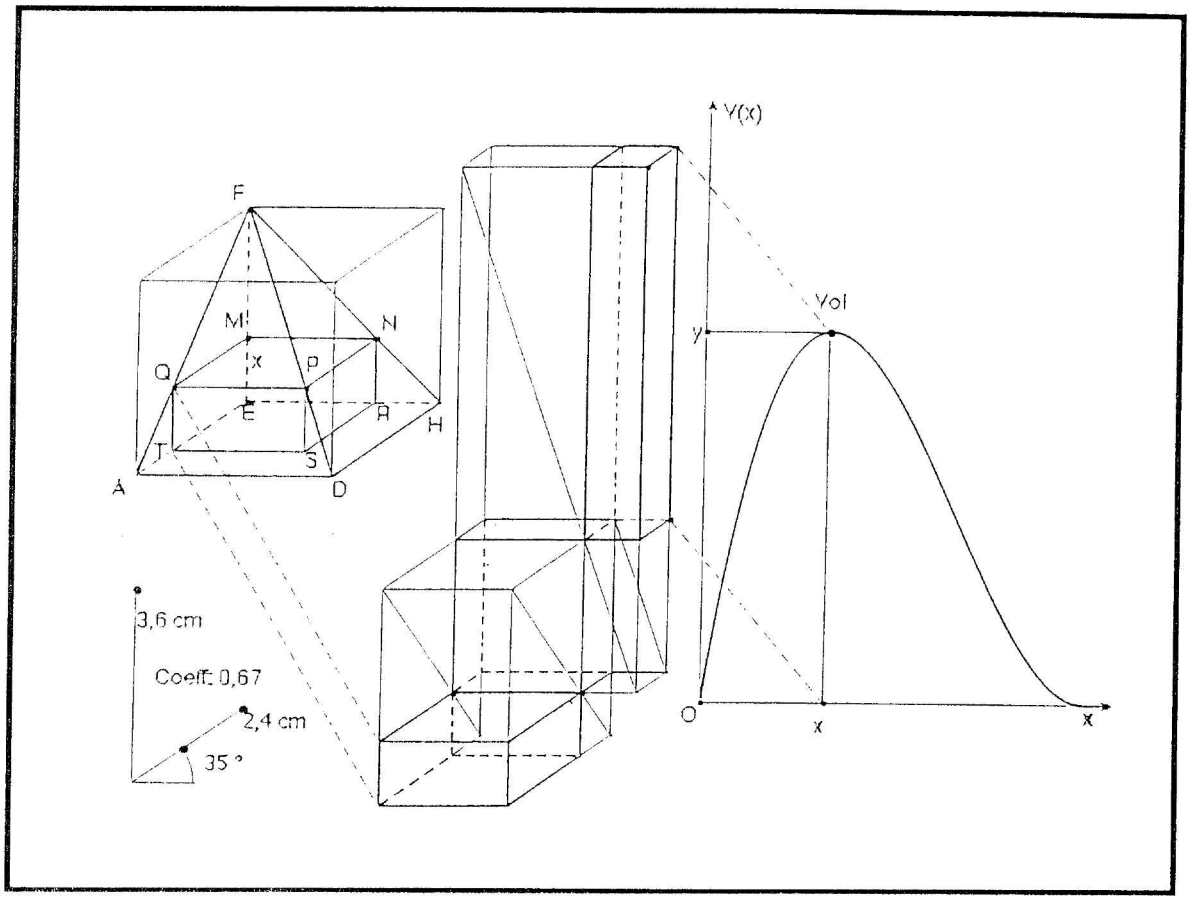
d) On pourra étudier de la même façon , c'est-à-dire à partir de la figure Cabri, l'aire latérale de ce pavé, ce qui revient à étudier l'aire du rectangle MNRE, puis à la quadrupler. Pour quelle valeur de x semble-t-elle maximum?

Vérifier la conjecture en développant $B = 81 - (2x - 9)^2$.

e) On pourra également étudier l'aire de la boite sans couvercle associée à ce pavé, et chercher son maximum en utilisant le développement de l'expression $C = 108 - 3(x - 3)^2$.



Copie d'écran correspondant à l'étude du volume du pavé



Remarque : On obtient des courbes qui permettent l'élaboration de conjectures qui seront confirmées par les calculs, et éventuellement, un travail sur les problèmes d'optimisation.

En guise de conclusion provisoire :

Si nous essayons d'analyser l'apport de l'ordinateur et du logiciel Cabri-Géomètre dans l'étude d'un problème de géométrie, il faut d'abord être conscient que les figures du document papier rendent mal compte de la réalité de l'écran, ne serait-ce que parce qu'elles sont fixes.

Un avantage de l'ordinateur réside dans le nombre important de figures que l'on peut avoir en réserve et que l'on peut utiliser selon les besoins. Dans la démonstration de la proposition d'Euclide sur les aires des rectangles, il nous a été possible de montrer aux élèves plusieurs cas de figure et de présenter une autre forme de la propriété que nous utilisons par la suite dans les constructions.

Autre intérêt de l'ordinateur dans cette activité, la possibilité de présenter des figures compliquées, et surtout de les décomposer en parties simples pour faire comprendre aux élèves le mécanisme utilisé pour représenter la résolution du problème. Le logiciel Cabri permet ainsi

une visualisation des divers stades du raisonnement et une synthèse animée de la résolution du problème. On peut penser que cette visualisation de concepts non triviaux pour les élèves va les aider dans leur apprentissage du raisonnement.

Enfin, l'intérêt le plus évident réside dans la possibilité d'animation des figures qui permet une visualisation de la variation d'une grandeur et donc de la notion de fonction, depuis l'évolution d'une figure géométrique dans laquelle on introduit une variable, jusqu'à la représentation graphique. Le tout permet d'établir des conjectures extrêmement fiables. Là encore, « voir » la variation doit permettre aux élèves de concevoir plus facilement la fonction.

□○□○□○□○□

Petite bibliographie :

[1] Le cube, changement de position - R. BRUNET - J. NAUDEILLO. Actes du Colloque Inter-IREM de Géométrie - Juin 1994 - IREM de Lille.
[2] Les Eléments d'Euclide - G. KAYAS - Ed. du CNRS.
[3] Eléments de géométrie - CLAIRAUT - Siloë.
[4] La géométrie - Livre premier - DESCARTES.
[5] Eléments de géométrie - LEGENDRE - Firmin Didot Frères 1855.

❑◆❑◆❑◆❑◆❑

LES PARCOURS DIVERSIFIES A PROPOS DES NOMBRES ET DU CALCUL "

Alain Bronner
IUFM et IREM de Montpellier

INTRODUCTION

Tout projet d'enseignement des *nombres et du calcul*, au niveau du collège et du lycée, est confronté au problème didactique du choix de la nature et de la mise en place d'un *espace numérique* plus vaste que celui organisé autour des nombres rationnels. Il doit permettre l'acquisition chez les élèves de techniques permettant de résoudre certains problèmes des cadres géométrique, algébrique et de celui de l'analyse, ainsi que la construction de concepts fondamentaux à propos *des nombres et du calcul*.

Je me propose ici de mettre en évidence les choix fondamentaux de quelques projets d'enseignement du Numérique à diverses périodes. Je commencerai par examiner ce que peut être un « nombre » dans ces différents projets, notamment un nombre réel, et les problématiques correspondantes. Je ferai ressortir le rôle fondamental de deux objets, à savoir « la racine carrée » et les « nombres décimaux », dans ces problématiques. Je montrerai notamment qu'il se constitue actuellement au niveau de l'enseignement secondaire des *vides didactiques institutionnels* dans le passage des nombres décimaux aux nombres irrationnels.

L'exposé s'appuie sur mon travail de thèse[13] et on pourra s'y reporter pour de plus amples développements.

L'ENSEIGNEMENT DES NOMBRES ET DU CALCUL A TRAVERS LES AGES

L'institution d'enseignement, l'Enseignement Mathématique Secondaire - que je noterai dans la suite EMS-, se distingue par sa régularité à proposer une réforme avec une pseudo-période d'une dizaine d'année depuis cinquante ans. Je ferai ainsi référence aux périodes classiquement délimitées par les dates des réformes successives.

- 1947-1958 (période intermédiaire)
- 1958-1968 (la préparation de la réforme)
- 1968-1978 (la réforme dite des mathématiques modernes)
- 1978-1985 (la fermeture de la réforme)
- 1985-1996 (période dite actuelle dans l'exposé)

Je considère aussi une période antérieure longue d'un siècle :

- 1854-1947 (époque dite classique)

Dans toutes les périodes le Numérique a un habitat principal : à l'époque classique c'était l'arithmétique, puis l'algèbre aux périodes suivantes et maintenant il est engendré par les « travaux numériques ». En fait ces changements ne portent pas seulement sur les étiquettes, mais il s'agit bien de véritables changements d'adresse correspondant à des évolutions significatives de l'enseignement.

A la période classique (1854-1947) la problématique de la mesure reste sous-jacente à la construction du Numérique montrant toujours une filiation avec la théorie euclidienne. Cette problématique fait l'objet d'une tentative de définition, souvent placé en début des ouvrages de l'époque :

> « *Mesurer une grandeur, c'est s'en faire une idée précise en la comparant à une autre grandeur de même espèce, que l'on connaît [...] Le résultat de la comparaison d'une grandeur à son unité s'exprime par un* ***nombre***. » (Guilmin, 1855)

---

[13] Alain Bronner, *Etude didactique des nombres réels, idécimalité et racine carrée*, Thèse de didactique des mathématiques, Université J. fourrier, Grenoble, 1997.

Elle aboutit à trois éventualités :

- soit des nombres entiers « *quand une grandeur se compose exactement de l'unité répétée un certain nombre de fois* » ;
- soit des nombres fractionnaires « *quand une grandeur se trouve composée d'un certain nombre d'unités, plus une fraction moindre que l'unité* » ;
- soit la grandeur ne rentre pas dans l'un des deux cas précédents et « *on dit alors que la grandeur est incommensurable avec cette unité : elle ne peut être mesurée qu'approximativement avec cette unité* ».

Cette dernière éventualité donnera naissance aux nombres incommensurables par l'intermédiaire d'un autre objet : la racine carrée. A partir des fondations constituées par les nombres fractionnaires, l'objet « racine carrée » s'impose sous la forme d'un algorithme, dit « méthode d'extraction », qui disparaîtra dans les années soixante. Cet objet conduit à une première extension de l'espace numérique sous les traits des *racines carrées incommensurables*. Ces dernières vont permettre une nouvelle extension du Numérique vers les *nombres incommensurables*. Pour cela, une autre signification de la racine d'un nombre A est recherchée et est obtenue en terme de limite des racines carrées $\frac{a_n}{n}$ approchées à 1/n près : $(\frac{a_n}{n})^2 \leq A < (\frac{a_n+1}{n})^2$, où a_n est entier.

Ainsi l'idée de nombre à cette époque est celle de « mesure » : « mesure d'une grandeur », appuyée par une approche analytique pour introduire les nombres incommensurables.

Dans la période de la préparation de la réforme des mathématiques modernes (1958/68), l'organisation classique s'effondre. En effet les ensembles structurés de nombres font leur apparition bien avant la dite réforme. Dans Marvillet et Adam (1961), ouvrage pour la classe de Troisième, la première page introduit « *les trois ensembles fondamentaux de l'algèbre :* $\mathbb{N}$, $\mathbb{Z}$, *et* $\mathbb{Q}$ ». Les propriétés de ces ensembles munis de ces lois vont être énumérées selon les structures de l'algèbre moderne (annexe 1). L'ouvrage de Monge et Guinchan de 1966 (annexe 2) présente des caractéristiques analogues et, de plus, les rationnels sont définis comme classe de fractions équivalentes.

L'enseignement s'appuie sur la classification rationnel/irrationnel alors qu'il ne figure aucune ligne de programme à ce sujet. Ce thème est toujours lié au problème de l'existence de racines carrées de nombres non carrés.

> *" Plus généralement, étant donné un nombre arithmétique A (entier, fractionnaire ou décimal), il n'existe pas nécessairement un nombre (entier, fractionnaire ou décimal) dont le carré est égal à A. Mais de toute façon, nous énoncerons la définition suivante :*
> *Définition : On appelle racine carrée arithmétique A, le nombre arithmétique représenté par le symbole* $\sqrt{A}$ *dont le carré est égal à A.* $(\sqrt{A})^2 = A$. *Le symbole* $\sqrt{}$ *s'appelle un radical.*
> *REMARQUES IMPORTANTES.*
> *I. Les nombres A et* $\sqrt{A}$ *sont des nombres arithmétiques.*
> *II. Dans les calculs où figurent des radicaux, on convient de traiter ces symboles comme des nombres ordinaires et de leur appliquer les règles usuelles des opérations »*
>
> Maillard et Millet (1966)

Nous pouvons ainsi voir que le statut de nombre des racines carrées irrationnelles n'est pas facile à acquérir, et seuls les rationnels semblent le « mériter ». Dans les ouvrages, les racines carrées, en raison de la nature irrationnelle de certaines d'entre elles, vont permettre aux auteurs de faire le saut dans l'ensemble des nombres réels. L'adaptation se réalise de la façon suivante chez Monge et Guinchan.

« *Ensemble* $\mathbb{R}^+$ *des réels positifs.*
Lorsque A n'est pas le carré d'un entier naturel ou le carré d'un rationnel, le symbole $\sqrt{A}$ *permet donc de définir un nombre irrationnel positif. Il existe d'autres nombres positifs non rationnels, qui ne sont égaux ni à un entier, ni à un décimal, ni à une fraction arithmétique. Par exemple on démontre qu'il en est ainsi pour le nombre* π *par lequel on doit multiplier la longueur du diamètre d'un cercle pour obtenir le périmètre de ce cercle. La réunion des rationnels positifs et des irrationnels positifs forme un ensemble que l'on appelle ensemble des réels positifs et que l'on désigne par la notation* $\mathbb{R}^+$ ».

$\mathbb{R}^+$ est construit par réunion de deux classes de nombres, dont l'une garde beaucoup de mystère. Le prolongement des opérations s'effectue selon un discours classique :

« *Nous admettons que toutes les opérations que nous avons définies dans l'ensemble* $\mathbb{Q}$ *des nombres rationnels peuvent aussi être définies dans l'ensemble* $\mathbb{R}$ *des nombres réels, et qu'elles possèdent dans l'ensemble* $\mathbb{R}$ *les mêmes propriétés que dans l'ensemble* $\mathbb{Q}$ ».

Après $\mathbb{N}$, $\mathbb{Z}$, et $\mathbb{Q}$, l'ensemble $\mathbb{R}$ est alors déclaré comme le quatrième ensemble fondamental de l'algèbre, tandis que l'ensemble $\mathbb{D}$ est complètement oublié dans la problématique précédente.

Les ensembles de nombres et, notamment l'ensemble $\mathbb{R}$, vont légitimer la présence de calculs sur les radicaux. Ainsi une dialectique entre les racines carrées et les nombres réels s'établit : les racines carrées irrationnelles ont permis d'introduire le corps des nombres réels qui en retour donne un cadre théorique permettant de justifier des calculs ou des transformations d'expressions numériques ou algébriques qui étaient effectués « naturellement » dans les périodes précédentes. Nous voyons apparaître avec cette période un nouveau rapport au nombre : le nombre est alors un élément d'une structure algébrique, ou encore il est caractérisé par des propriétés algébriques indépendamment de toute référence aux grandeurs.

Les programmes pour la classe de Mathématiques Élémentaires[14] vont sanctionner une évolution déjà significative en Seconde et confirmer la place des structures dans l'enseignement secondaire. L'institution EMS exprime le souhait de donner des « *indications sommaires* » sur le mode de construction de $\mathbb{R}$. Ce souhait laisse la porte ouverte à de nombreuses variations sur le mode de construction de $\mathbb{R}$ et le niveau d'approfondissement. On peut repérer :

- une construction par les suites de Cauchy chez Monge et Ruff (1962) ;
- une construction par les sections ouvertes commençantes chez Bréard C. (1963), dans l'esprit de la construction de Dedekind ;
- une construction bien tortueuse chez Lespinard et Pernet (1962) où un réel va apparaître encore ici comme limite d'une suite de rationnels, mais, après un jeu subtil entre la droite et les nombres, en sollicitant l'axiome de continuité Cantor-Dedekind : « une suite d'intervalles ouverts emboîtés dont la longueur tend vers 0 contient un unique point ». On pourra noter qu'il s'agit d'une démarche que voulaient absolument éviter les mathématiciens de la sphère savante de la fin du 19ème siècle.

En fait l'institution a conduit les auteurs de manuels devant un problème didactique difficile qui va amener des traitements assez différents.

[14] Classe de Terminale scientifique de l'époque.

J. Lelong-Ferrand[15] (1964) pose le problème de la façon suivante.

> *« Les nouveaux programmes de Mathématiques Élémentaires, qui proposent de donner des indications sommaires sur la définition des nombres réels, placent donc le professeur devant une situation embarrassante ; car, quelle que soit la méthode adoptée, il n'est pas possible d'en donner un exposé rigoureux sans lui consacrer plusieurs leçons, au détriment du reste du cours. Les méthodes fondées sur la théorie des limites présentent, de plus, l'inconvénient de retarder la définition des nombres réels jusqu'à ce qu'on ait exposé le cours dans un ordre peu naturel à ce niveau ».*

La période des mathématiques modernes sanctionne une évolution de la constitution du Numérique dans l'institution EMS en réduisant le plus tôt possible et au plus près la distance avec le savoir mathématique de référence. L'institution fait alors jouer un rôle fondamental à des nombres qui restent souvent dans l'ombre : les nombres non décimaux que j'appelle *les nombres idécimaux* . De même, j'appelle *idécimalité* le caractère d'être idécimal pour un nombre de façon analogue aux classiques définitions sur l'irrationalité. L'institution propose alors une nouvelle épistémologie scolaire des nombres réels basée sur l'opposition décimal/idécimal et introduit les réels sous la forme des suites décimales illimitées. En effet les nouveaux programmes (arrêté du 22 juillet 1971) demandent d'introduire les nombres réels dès la classe de Quatrième en suivant un plan précis d'enseignement. Avant d'aborder les propriétés structurelles de l'ensemble des réels (dont la notion de quotient), nous relevons :

- la consolidation de l'étude de l'anneau ordonné des nombres décimaux ;
- un travail d'approximation, basé sur les encadrements par des décimaux « successifs » des différents ensembles de décimaux $\mathbb{D}_p$, de sommes, produits, inverses et racines carrées de décimaux ;
- et l'introduction des suites décimales illimitées.

Avant la dernière étape, il est suggéré de montrer la nécessité d'introduire des nombres idécimaux. Cette nécessité est notamment motivée par deux problèmes.

- Le premier est celui de la recherche de l'inverse d'un décimal strictement positif dans le cas où cet inverse n'est pas décimal. Par exemple, le manuel de la collection Queysanne-Revuz pose le problème de la recherche de l'inverse de 12 et de 0,37 et aboutit à la conclusion

> *« il n'existe pas de décimal x tel que : 12x=1.*
> *La division avec virgule de 1 par 12, poursuivie indéfiniment, fournit une « écriture décimale illimitée » : 0,083333... ».*

Ce problème permet aux auteurs d'introduire la suite décimale illimitée 0,083333....

- Le second problème suggéré par le programme est celui de l'existence de la racine carrée de certains décimaux. Les auteurs précédents propose la recherche *des racines carrées à 10^{-n} respectivement par défaut et par excès* (notions qui ne seront pas institutionnalisées) du nombre 6. Cette activité conduit à introduire encore, d'une part une écriture décimale illimitée (dont les auteurs demandent d'admettre qu'elle n'est pas périodique), et d'autre part une suite d'intervalles emboîtés qui n'ont en commun aucun point de $\mathbb{D}$.

Nous voyons que ces deux problèmes sont réunis pour une cause commune, l'introduction de nouveaux nombres : les nombres idécimaux. Dans le nouveau projet d'enseignement du Numérique les nombres idécimaux deviennent un objet d'enseignement.

---

[15] J.Lelong Ferrand, Les notions de mathématiques de base dans l'enseignement du second degré, Armand Colin, 1964.

La période de fermeture de la réforme des mathématiques modernes (1977/1985) s'inscrit dans un recul de la théorie élémentaire des ensembles et des relations, ainsi que des structures. Les décimaux restent les fondements du Numérique dans le savoir à enseigner au début du collège (Sixième et Cinquième) mais un changement de problématique se dessine sans que l'on puisse bien en préciser les contours. En Quatrième, le long paragraphe détaillé des programmes de 1971 intitulé « Nombres décimaux et approche des réels » est remplacé par un paragraphe exigu intitulé très sobrement « Calcul numérique ».

> *« Exemples introduisant la notion de fraction.*
> *Révision des opérations sur les décimaux.*
> *Pratique des opérations sur les rationnels, sur les réels.*
> *Relation d'ordre ; valeur absolue ; exemple de calculs approchés.*
> *Produits $(a+b)^2$, $(a-b)^2$, $(a+b)(a-b)$: leur utilisation.*
> *Exemples numériques d'équations et d'inéquations du premier degré à une inconnue. »*
>
> (Arrêté du 16 novembre 1978)

La référence aux réels se résume pratiquement à la lacunaire expression *« pratique des opérations sur les rationnels, sur les réels »*. Nous n'avons pas de réponse à la question de ce que représente l'objet « nombre réel » au collège. Je qualifie ce phénomène de ***vide didactique institutionnel*** dans l'institution officielle EMS. La seule voie officielle que l'on peut déceler est le recours à la droite. Son étude n'attend plus la mise en place de l'ensemble $\mathbb{R}$. Les instructions suggèrent de mener de front l'étude du calcul et de la géométrie. Les notions d'ordre sur la droite et sur $\mathbb{R}$ pourront *« s'éclairer mutuellement »*.

Dans la période actuelle des changements importants aparaissent sous l'effet des nouveaux programmes du collège, mis en oeuvre à partir de la Sixième à la rentrée 1986 (Arrêté du 14 novembre 1985). Les connaissances relatives aux nombres et au calcul sont rassemblées dans un ensemble intitulé *« Travaux numériques »* expédiant la traditionnelle répartition arithmétique-algèbre. Dès la Sixième, l'institution exige des élèves à propos des décimaux qu'ils sachent *« passer d'une écriture décimale à une écriture fractionnaire et vice versa »*. Partout on retrouve des expressions du type *« nombres en écriture décimale »* ou *« nombres en écriture fractionnaire »*. Les transformations d'écriture des nombres prennent une place et un rôle prépondérant dans cette période. Cet enseignement des nombres décimaux et des nombres fractionnaires - qui n'ont pas vraiment statut de nombres rationnels - s'étale sur tout le collège, essentiellement de la Sixième à la Quatrième et consiste à étendre ou mettre en place progressivement les opérations et règles algébriques sur ce domaine numérique. Nous trouvons ainsi selon les classes :

- en Sixième : opérations +, -, x, / sur les décimaux ; multiplication d'un décimal par un quotient ;
- en Cinquième : comparaison et addition de deux nombres en écriture fractionnaire de même dénominateur, multiplication de nombres en écriture fractionnaire ;
- en Quatrième : opérations +, -, x, / sur les nombres en écriture fractionnaire.

Les *travaux numériques* seront complets avec les *« calculs élémentaires sur les radicaux (racines carrées) : produit et quotient de deux radicaux, puissance d'ordre 2 ou 4 d'un radical »* (arrêté du 14 novembre 1985). L'institution EMS semble conduit, actuellement, à présenter la racine carrée comme un objet de l'algèbre, après une « petite touche » de la calculatrice en Quatrième : *« calculer, en faisant éventuellement usage de la touche $\sqrt{}$ de la calculatrice, un côté d'un triangle rectangle à partir de la donnée des deux autres côtés »*. Toute référence à une quelconque nature des racines carrées s'est aussi volatisée, au niveau des programmes comme de la plupart des manuels.

LA PROBLEMATIQUE D'EXTENSION DES SYSTEMES DE NOMBRES, APPARUE DANS LES ANNEES SOIXANTE, PUIS RALENTIE DANS LA PERIODE PRECEDENTE, EST STOPPEE DANS LA PERIODE ACTUELLE. PARALLELEMENT, LA NATURE DES NOMBRES SE TROUVE MISE A L'ECART, ET L'ARITHMETIQUE EST REJETEE DE TOUS LES NIVEAUX D'ENSEIGNEMENT. UN EFFET DE CETTE EVOLUTION PEUT ETRE REMARQUE A TRAVERS N'IMPORTE QUEL MANUEL DE TROISIEME. QUAND UNE PROPRIETE EST ENONCEE, PAR EXEMPLE[16]

« QUELS QUE SOIENT LES NOMBRES A, B ET C :
SI $A \leq B$ ALORS $A + C \leq B + C$ »,

ELLE EST FORMULEE SANS DOMAINE DE REFERENCE ET SANS FAIRE INTERVENIR LA NATURE DES NOMBRES. IMPLICITEMENT LES AUTEURS LAISSENT CIRCULER L'IDEE QUE CES PROPRIETES PEUVENT S'APPLIQUER A TOUS LES NOMBRES RENCONTRES, ET EN PARTICULIER AUX RACINES CARREES PAR EXEMPLE.

Déjà se dessinait un flottement à propos des nombres réels dans la période précédente où le statut des réels n'était plus aussi délimité que dans la période des années soixante-dix. Dans les programmes du collège on ne trouve même plus l'expression « nombres réels ». Les nombres réels ne sont toujours pas un objet d'enseignement en Seconde. Paradoxalement les désignations des ensembles de nombres sont introduites : *« s'ajoutent en Seconde, ..., les notations* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *; sur ces différents points, il s'agit d'un simple vocabulaire et aucun développement n'est au programme »*. La désignation $\mathbb{D}$ et l'ensemble des nombres décimaux sont encore oubliés des commentaires, alors qu'ils ont joué un rôle essentiel dans les « Travaux numériques » au collège. Au lycée, l'ensemble $\mathbb{R}$ apparaît comme *« un grand fourre-tout »*[17] qui s'élabore sur une notion préconstruite de « nombre », indépendant de sa nature arithmétique, et où les règles de calcul vont être officialisées une fois pour toutes. Une représentation en est donnée par la droite numérique. Une stratégie de réduction du vide didactique institutionnel - quasi uniforme - se dégage chez les manuels de Seconde selon deux étapes que l'on peut repérer chez n'importe quel représentant-auteur de l'institution EMS. Tout d'abord, on rappelle et on fait utiliser des « règles de calcul » sur les nombres. Ces règles correspondent pratiquement aux axiomes d'une structure de corps. Un des effets du vide didactique est, ici encore, l'absence d'indication sur l'ensemble de référence des calculs ou sur la nature des nombres. Les auteurs de manuels laissent, peut-être, volontairement flotter un flou sur cette nature. Ensuite, les auteurs présentent les différents types de nombres, les différents ensembles de nombres et les notations de ces ensembles avec un consensus montrant un assujettissement très serré à l'institution. On obtient ainsi une même photographie de « famille » de l'enseignement des nombres et du calcul proposé dans les divers manuels en début de Seconde (annexe 3).

Sur une idée assez vague de « nombre » et sur les fondations organisées autour des nombres décimaux, le Numérique va se développer dans une problématique que je qualifie d'algébrique. L'institution EMS amplifie, dans cette période, le « vide didactique » sur l'objet « nombre réel ».

L'IRRATIONALITE A TRAVERS LES AGES

Officiellement le thème de l'irrationalité n'est jamais un objet d'enseignement. Mais, à certaines périodes, il a été développé de façon importante dans les manuels, puis il a disparu complètement à d'autres. J'ai montré à plusieurs reprises le rôle des racines carrées dans la

---

[16] G. Bonnefond, D. Daviaud, B. Reynaud, Mathématiques Troisième, collection Pythagore, Hatier, 1989.
[17] Selon l'expression des auteurs du manuel Hachette pour la classe de Seconde.

construction du Numérique. Ainsi, c'est encore à travers les racines carrées que le thème de l'irrationalité apparaîtra en Troisième. Le tableau suivant permet de comparer l'intensité de la présence de ce thème et de ses liens avec la racine carrée dans le savoir enseigné selon les périodes.

Périodes	**1854/1947**	**47/58**	**58/68**	**68/78**	**78/85**	**85/96**
Irrationalité **programmes**	incommen surables	absence				
Irrationalité **dans les manuels**	incommen surables	moyenne	assez forte	absence	moyenne	absence
racine carrée et irrationalité **dans les manuels**	très forte à forte			absence	forte	absence

Nous relevons, à la période classique la forte présence du thème, puis l'absence ou une faible présence actuellement. Dans la période actuelle la nature des nombres n'est plus un enjeu didactique officiel. Et l'irrationalité n'apparaît plus actuellement dans l'enseignement du Numérique. Une première raison est, peut-être, le manque d'outils, suite à la disparition de l'arithmétique. On pourra noter, qu'à l'époque classique où l'arithmétique était un élément fondamental du cursus, le thème de l'irrationalité était particulièrement développé. Les conditions d'irrationalité des racines carrées de nombres fractionnaires étaient étudiées dans les manuels. Un autre raison est à rechercher dans les caractéristiques générales de l'enseignement actuel des Nombres et du Calcul : la prédominance des savoirs algébriques et algorithmiques.

CONCLUSION

Le *texte du savoir à enseigner* se présente comme les conditions et contraintes dans lesquelles se développe l'apprentissage. Dans ce *texte* des vides, à propos de certaines notions, sont inévitables. Il ne peut être explicité complètement. Inversement des « blancs », sont même indispensables et une certaine latitude paraît souhaitable dans un système d'enseignement. Mais certains « manques », certains « silences », et surtout l'absence de définition de certains objets d'enseignement, conduisent à des phénomènes qui ne sont plus de l'ordre de la liberté didactique, mais plutôt de l'ordre de l'équivoque et de la « décharge institutionnelle ». Il semble que des périodes de crise amènent l'institution à ce type de phénomène. Ainsi, après la période des mathématiques modernes où le savoir à enseigner était proposé selon un plan d'enseignement bien précis, et proche du savoir savant, l'institution a produit un *vide didactique* à propos des nombres réels.

Je fais l'hypothèse que les effets de la réforme des mathématiques modernes ont été tels que les agents didactiques « auteurs de programme » ont été conduits à produire ce *vide didactique institutionnel* relativement à l'objet « nombre réel ». Ce vide est encore effectif, soit vingt ans après la fermeture de cette réforme. Les problèmes d'enseignement et d'apprentissage, engendrés par la réforme des mathématiques modernes sont réglés par ce vide, laissant aux enseignants la responsabilité complète d'une transposition des réels en classe et faisant apparaître une grande ouverture sur les enseignements proposés[18], et notamment sur les tentatives de réduction de ce vide.

Le retour de l'arithmétique permet d'envisager des reprises possibles d'apprentissages sur les Nombres et le Calcul. Il faudra nous mettre au travail pour des propositions dans ce sens, à moins d'avoir anticiper ce retour comme certains groupes de l'IREM...

[18] On pourra voir une étude montrant la variété des approches découlant de ce vide au niveau des enseignants de Troisième et de Seconde dans Bronner (1997), voir note 1.

ANNEXE 1

Les ensembles de nombres chez Marvillet et Adam. (Mathématique, 3ème, 1961, librairie Armand Colin)

3 - Les trois ensembles fondamentaux de l'algèbre : N, Z et Q

La notion d'*ensemble* est intuitive. On comprend sans peine le sens des mots : l'ensemble des élèves d'une classe, l'ensemble des internes d'un lycée, des militaires d'une garnison, des livres d'une bibliothèque, des assiettes d'un service de table, etc.

En mathématiques, on considère des *ensembles* de nombres, de points, de lignes, de surfaces, de volumes. Exemple :

L'*ensemble* des entiers compris entre 3 et 11 se compose de 7 *éléments*. L'ensemble des nombres rationnels (entiers ou fractions) compris entre 4 et 5 se compose d'une infinité d'éléments. L'ensemble des points d'un segment AB, renferme également une infinité d'éléments.

Nous avons, en classe de 4e, introduit l'*ensemble* des entiers naturels, zéro compris. Nous appellerons N cet ensemble. 0, 1, 2, 3, ... n sont des *éléments* de N.

Nous appellerons Z l'ensemble des entiers positifs, nul ou négatifs. Tout élément n de N (3 par exemple) appartient à Z, mais il n'y a pas de réciprocité. ... — 3, — 2, — 1, 0, 1, 2, 3... sont des éléments de Z.

Nous dirons que N est un *sous-ensemble* de Z. Ainsi, dans un service de table, les assiettes à dessert forment un sous-ensemble de l'ensemble des assiettes du service.

Nous appellerons Q l'ensemble des rationnels positifs, nuls ou négatifs, ou rationnels relatifs [1]. (Classe de 4e, chapitre 5)

1. Les opérations dans N, Z, Q

On a pu définir dans chacun des trois ensembles N, Z, Q, une *addition* et une *multiplication*. Autrement dit, si x et y sont deux éléments de l'un quelconque de ces ensembles, leur somme $x + y$ et leur produit xy sont définis dans l'ensemble choisi. Exemples :

	Dans N	Dans Z	Dans Q
a)	$2 + 1 = 3$	$(-3) + 2 = -1$	$-\frac{2}{3} + \frac{1}{6} = -\frac{1}{2}$
b)	$3 \times 4 = 12$	$(-3) \times (+4) = -12$	$\left(-\frac{3}{4}\right)\left(-\frac{2}{5}\right) = \frac{3}{10}$

2. Propriétés des opérations précédentes dans N, Z, Q, ou lois de composition

a) Commutativité, associativité.

L'*addition*, dans N, Z, Q, est :	La *multiplication*, dans N, Z, Q, est :
commutative : $x + y = y + x$	commutative : $xy = yx$
associative : $(x + y) + z = x + (y + z)$	associative : $(xy)\,z = x\,(yz)$

Les parenthèses indiquent que les calculs placés à l'intérieur sont supposés effectués.

Addition et multiplication possèdent l'une et l'autre un élément neutre :

zéro : $a + 0 = a$ un : $a \times 1 = a$

1. On désigne par R un autre ensemble contenant Q, qui sera introduit plus loin (chap. 2, p. 11).

b) Distribution du produit.

La multiplication est distributive par rapport à l'addition :

$$(a + b + c)\,m = am + bm + cm$$

Lue de droite à gauche, cette égalité représente la mise en facteur commun de m.
Mais l'addition n'est pas distributive par rapport à la multiplication :

$$4 + 5 \times 6 \neq (4 + 5)\,(4 + 6); \quad a \times bc \neq (a + b)\,(a + c)$$

Dans toutes ces relations, les lettres représentent des éléments choisis dans un seul des ensembles, N, Z, Q.

c) Les différences entre N, Z, Q. L'opposé, l'inverse.

1° Il n'existe pas dans N d'élément (autre que zéro) qui, ajouté à un entier donné (autre que zéro), donne zéro. $x + y = 0$ est impossible avec des éléments de N (sauf $0 + 0 = 0$).
Cette opération est possible dans Z et dans Q. Elle a toujours une solution. Exemples :

$$3 + (-3) = 0; \quad 5 + (-5) = 0; \quad \frac{2}{3} + \left(-\frac{4}{6}\right) = 0$$

Le nombre x', tel que $x + x' = 0$, est l'opposé de x, noté $-x$.

2° On ne peut définir la différence $a - b$ de deux entiers éléments de N que si a est plus grand que b : $a > b$ ($2 - 5$ n'a pas de sens). Par contre, la différence de deux éléments de Z ou de Q existe quels que soient ces éléments :

$$3 - 8 = -5; \quad -2 - (-6) = -2 + 6 = 4; \quad -\frac{1}{3} - \frac{3}{4} = -\frac{13}{12}$$

$x - y = x + (-y)$ quels que soient les éléments x et y de Z ou Q.
Les ensembles Z et Q rendent possible une opération impossible dans N.

3° Il n'existe pas dans Z d'élément (autre que 1 ou — 1) qui multiplié par un élément donné de Z (autre que 1 ou — 1) donne 1. Autrement dit, $x.y = 1$ est impossible avec des éléments de Z, sauf $1 \times 1 = 1$ et $(-1) \times (-1) = 1$. Mais cette opération est possible dans Q pour tout élément autre que zéro et elle a une solution.

Le nombre rationnel x' tel que : $x \times x' = 1$ ($x \neq 0$) est l'inverse de x, noté $\frac{1}{x}$.

4° On ne peut définir le quotient $\frac{a}{b}$ de deux entiers relatifs éléments de Z que si a est multiple de b : $\frac{-18}{6} = -3$ $\left(\frac{15}{-6}\right.$ n'a pas de sens dans Z$\left.\right)$. Par contre, le quotient de deux éléments x et y de Q (donc de N et Z) regardé comme élément de Q existe pourvu que $y \neq 0$.
$\frac{x}{y} = x \times \left(\frac{1}{y}\right) = x \times$ inverse de y.

Exemples :

$\frac{-15}{6} = -\frac{5}{2} \in$ Q, $-\frac{9}{4} : \frac{3}{16} = -\frac{9}{4} \times \frac{16}{3} = -12$ est un élément de Z donc de Q, quotient de deux éléments de Q.

16. Nous savons que deux fractions arithmétiques $\frac{a}{b}$ et $\frac{a'}{b'}$ sont égales si et seulement si leurs termes vérifient l'égalité : $a \times b' = b \times a'$.

En particulier, si l'on multiplie les deux termes d'une fraction par un même entier naturel, on obtient une fraction égale à la fraction donnée.

Par exemple les fractions $\frac{2}{5}, \frac{4}{10}, \frac{6}{15}, \frac{10}{25}$ sont égales entre elles.

Appliquons à un segment AB la fraction $\frac{2}{5}$; nous obtenons un segment EF.

Si nous appliquons au même segment AB l'une quelconque des fractions $\frac{4}{10}, \frac{6}{15}, \frac{10}{25}$, nous obtenons des segments tous égaux au segment EF.

Nous disons que ces fractions sont équivalentes, ou qu'elles appartiennent à une même classe de fractions équivalentes.

D'une façon générale, classons toutes les fractions de l'ensemble $\mathcal{F}$ en mettant dans une même classe toutes les fractions qui, appliquées à un même segment AB, donnent des segments égaux entre eux.

Nous établissons ainsi dans l'ensemble $\mathcal{F}$ des classes de fractions équivalentes; chacune de ces classes de fractions forme un ensemble que l'on appelle un rationnel arithmétique.

Ce rationnel arithmétique admet pour représentant l'une quelconque des fractions de la classe qui définit le rationnel.

17. Opérations sur les rationnels arithmétiques.

Considérons deux fractions de l'ensemble $\mathcal{F}$, par exemple les fractions $\frac{2}{5}$ et $\frac{4}{3}$. Calculons leur produit; il est égal à $\frac{8}{15}$.

Remplaçons chacune des fractions par une fraction de la même classe; prenons par exemple les fractions $\frac{6}{15}$ et $\frac{12}{9}$; calculons leur produit; il est égal à $\frac{72}{135}$.

Les deux fractions $\frac{8}{15}$ et $\frac{72}{135}$ sont égales; elles appartiennent donc à une classe de fractions équivalentes.

Nous disons que le rationnel arithmétique dont un représentant est $\frac{8}{15}$ est le produit du rationnel arithmétique dont un représentant est $\frac{2}{5}$ par le rationnel arithmétique dont un représentant est $\frac{4}{3}$.

On démontre et nous admettons que le produit de deux rationnels arithmétiques ne dépend pas des représentants choisis pour ces deux rationnels.

Nous définirions d'une manière analogue le quotient, la somme et la différence de deux rationnels arithmétiques.

Nous admettons que les opérations sur les rationnels ont les mêmes propriétés que les opérations définies dans l'ensemble $\mathcal{F}$ des fractions arithmétiques.

Nombres relatifs.

18. L'introduction des fractions et des rationnels arithmétiques a permis de construire des ensembles de nombres dans lesquels tout élément non nul admet un symétrique pour la loi de multiplication.

L'introduction des nombres relatifs permet de construire des ensembles dans lesquels tout élément a un symétrique pour la loi d'addition.

Nous rappelons les définitions suivantes :

19. DÉFINITIONS : 1° Zéro est un nombre relatif.

2° Tout nombre relatif différent de zéro est formé de l'ensemble d'un signe et d'un nombre arithmétique non nul.

Le nombre arithmétique est appelé valeur absolue du nombre relatif.

Les nombres relatifs dont le signe est + sont appelés nombres positifs ;

les nombres relatifs dont le signe est − sont appelés nombres négatifs.

Par exemple, les nombres + 7 et + 2,5 sont des nombres positifs; leurs valeurs absolues sont respectivement égales à 7 et à 2,5.

Les nombres − 3 et − 1,3 sont des nombres négatifs; leurs valeurs absolues sont respectivement égales à 3 et à 1,3.

La valeur absolue de zéro est égale à zéro; mais zéro n'a pas de signe.

Nous convenons de désigner la valeur absolue d'un nombre relatif a par la notation $|a|$.

Par exemple, nous écrivons :

$$|+7| = 7; \qquad |-2,5| = 2,5.$$

20. Égalité de deux nombres relatifs. On dit que deux nombres relatifs sont égaux s'ils ont même valeur absolue et même signe.

ANNEXE 3

Les ensembles de nombres, $\mathbb{R}$ et la droite dans "Nathan".
(Classe de seconde)

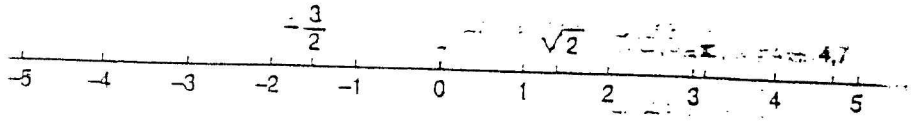
PRÉLIMINAIRE : LES DIFFÉRENTS ENSEMBLES DE NOMBRES

1 Ensemble des réels

L'ensemble de tous les nombres que nous utilisons s'appelle l'ensemble des nombres réels. Il est noté $\mathbb{R}$.

On peut représenter chaque nombre réel par un point d'une droite graduée.

Note
$\sqrt{2} \approx 1{,}41$
$\pi \approx 3{,}14$



2 Des réels particuliers

• Les nombres naturels : 0 ; 1 ; 2 ; 3 ; 4 ...

L'ensemble des naturels est noté $\mathbb{N}$. Chaque naturel est un réel. On dit alors que l'ensemble $\mathbb{N}$ est inclus dans l'ensemble $\mathbb{R}$, ce que l'on note $\mathbb{N} \subset \mathbb{R}$.

• Les nombres entiers relatifs (ou plus simplement les nombres entiers) :

$$\ldots ; -3 ; -2 ; -1 ; 0 ; 1 ; 2 ; 3 ; \ldots$$

L'ensemble des entiers est noté $\mathbb{Z}$.

Chaque entier est un réel. On écrit donc $\mathbb{Z} \subset \mathbb{R}$.

Chaque naturel est un entier. On écrit donc $\mathbb{N} \subset \mathbb{Z}$.

• Les nombres rationnels : ce sont les quotients d'entiers, c'est-à-dire les nombres $\frac{a}{b}$ avec a entier et b entier non nul.

EXEMPLES : $\frac{5}{4}$; $-\frac{3}{2}$; -25, car $-25 = \frac{-25}{1}$.

Note
Il existe des nombres réels qui ne sont pas des rationnels. Par exemple $\sqrt{2}$, π. On dit que ce sont des irrationnels.

L'ensemble des rationnels est noté $\mathbb{Q}$.

Chaque rationnel est un réel. On écrit $\mathbb{Q} \subset \mathbb{R}$.

Chaque entier n, pouvant s'écrire $\frac{n}{1}$, est un rationnel. On écrit donc $\mathbb{Z} \subset \mathbb{Q}$.

On peut regrouper les diverses inclusions précédentes sous la forme suivante :

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

► REMARQUE : Les nombres décimaux, c'est-à-dire les réels n'ayant qu'un nombre fini de chiffres après la virgule, sont des rationnels particuliers. Ainsi, par exemple, 1,54 est un rationnel car il peut s'écrire $\frac{154}{100}$.

Table ronde : "Arithmétique à l'école, au collège et au lycée : perspectives, problèmes"

Compte rendu Christian Faure
Groupe Analyse

Participants : lors de cette table ronde, sont présents :

Thierry Murgier	IPR mathématiques
Yvon Nouazé	Universitaire
Alain Bronner	Formateur I.U.F.M.
Yves Girmens	Formateur I.U.F.M.
Maryse Noguès	Professeur de mathématiques, formateur MAFPEN
Christian Faure	Professeur de mathématiques, formateur MAFPEN

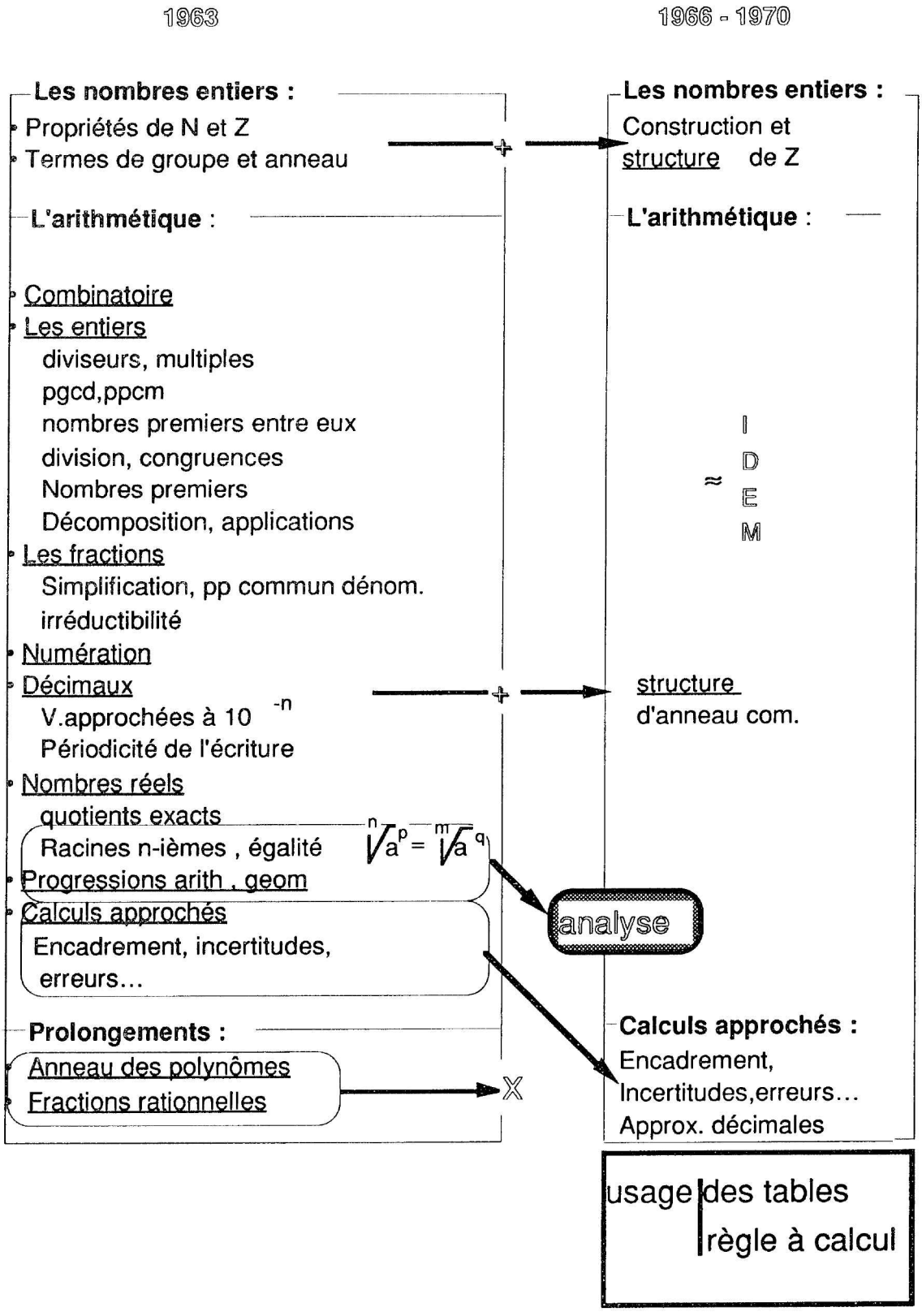
Maryse Noguès présente les participants de cette table ronde, dont l'objectif sera d'essayer d'évaluer la place du concept de nombre dans l'enseignement, du primaire au supérieur, ainsi que dans la formation des maîtres. Un bref historique à travers les anciens programmes sera présenté par Christian Faure, les perspectives et les futurs programmes seront évoqués par Thierry Murgier. Yvon Nouazé, Alain Bronner et Yves Girmens seront invités à présenter la situation dans leurs domaines respectifs.

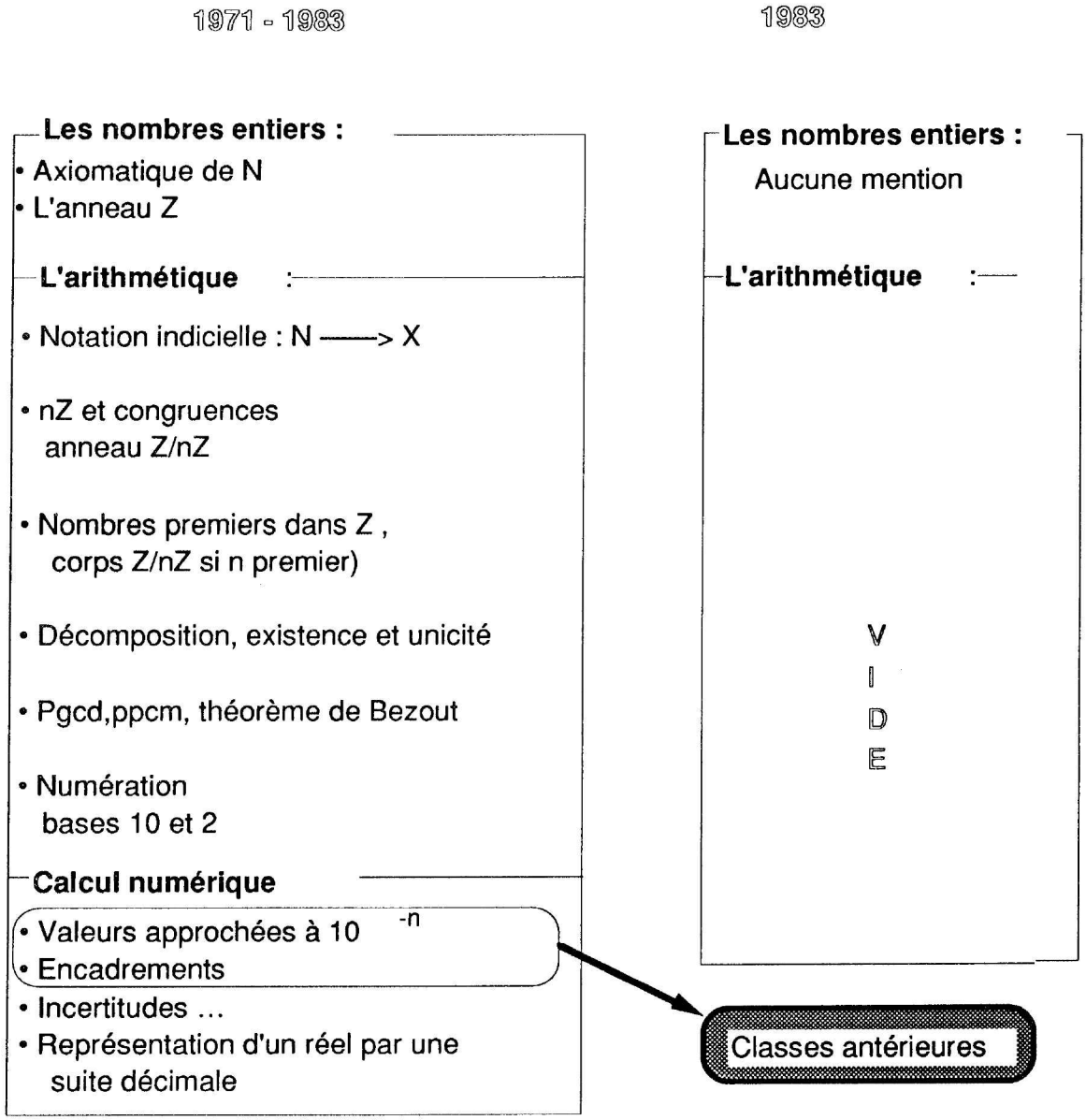
Christian Faure, en suivant l'intitulé «Arithmétique» dans les programmes de Terminales scientifiques, montre l'érosion du concept de nombre et souligne la conjonction avec l'intervention des calculatrices et ordinateurs dans l'enseignement des mathématiques :

- en 63 : le nombre est objet d'étude, et suit une progression des entiers vers les réels, les savoir faire sont clairement explicités dans les programmes ;
- 66-70 : peu de changements : quelques déplacements d'intitulés de l'arithmétique vers l'analyse, apparition de l'approche structurelle et d'une rubrique «calcul numérique» s'appuyant sur des tables et la règle à calculs ;
- 71-83 : l'arithmétique est à la crête de la vague structuraliste : ce n'est plus le nombre qui est centre d'étude mais les ensembles de nombres, évocation des "machines à calculer de bureau" en soutient des tables et des règles à calculs ;
- 83 : c'est le reflux de la vague structuraliste et l'arithmétique en fait fortement les frais, les savoir faire sont distribués dans les programmes des classes précédant la terminale, les calculatrices sont fortement mentionnées ;
- aujourd'hui : beaucoup de compétences ne sont plus demandées. Celles qui restent ont des bases complètement empiriques. Simultanément on observe une monté en puissance de l'analyse (où le nombre n'est pas centre d'étude) et une très large utilisation des calculatrices (par lesquelles l'image du nombre est fortement altérée).

En conclusion : simultanément à une utilisation intensive des calculatrices qui génèrent un certain concept de nombre, l'analyse les utilise en "fond flou", sans aucune sémantique.

Thierry Murgier souligne et détaille l'approche structuraliste qui était en vigueur dans les précédents programmes. Certaines notions d'arithmétiques vont être enseignées dans la partie spécialité des terminales S à partir de la rentrée 98 : PGCD, PPCM, décomposition... Une forte connotation algorithmique apparaît dans les programmes annoncés. Il préconise que l'arithmétique soit un domaine où puissent s'exercer des démarches de recherche et d'expérimentation.


1963
1966 - 1970
Les nombres entiers :
• Propriétés de N et Z
• Termes de groupe et anneau
L'arithmétique :
• Combinatoire
• Les entiers
diviseurs, multiples
pgcd,ppcm
nombres premiers entre eux
division, congruences
Nombres premiers
Décomposition, applications
• Les fractions
Simplification, pp commun dénom.
irréductibilité
• Numération
• Décimaux
V.approchées à 10 -n
Périodicité de l'écriture
• Nombres réels
quotients exacts
Racines n-ièmes , égalité $\sqrt[n]{a^p} = \sqrt[m]{a^q}$
• Progressions arith , geom
• Calculs approchés
Encadrement, incertitudes,
erreurs...
Prolongements :
• Anneau des polynômes
• Fractions rationnelles
X
Les nombres entiers :
Construction et
structure de Z
L'arithmétique :
I
D
≈
E
M
structure
d'anneau com.
analyse
Calculs approchés :
Encadrement,
Incertitudes,erreurs...
Approx. décimales
usage des tables
règle à calcul



1971	1982 *disparition de la rubrique*	1986
tables règle à calcul machine "de bureau"	...utiliser largement les calculatrices	emploi systématique des calculatrices

Intervention de Michel Secco qui exprime ses doutes : faire ou ne pas faire ces démarches relève plus d'une conception de l'activité mathématique et ceci est propre à chaque enseignant ; ce n'est pas une "dose" d'arithmétique qui remettra en cause une approche pédagogique construite depuis des années.

Intervention de Michèle Fuchs qui regrette une construction de la compétence en arithmétique limitée à la seule terminale S spécialité mathématique, d'autant que certains concepts nécessitent une maturation sur plusieurs années.

Yvon Nouazé explicite certains hiatus entre les compétences des élèves bacheliers et les tout premiers exercices (TD) qu'ils vont rencontrer en première année de DEUG :par exemple le concept de relation d'ordre (total ou partiel), introduit en tout débur de cycle , ne peut s'appuyer que sur l'ordre très particulier de $\mathbb{R}$.

Alain Bronner explicite le flou qu'il existe autour du concept de nombre, tant chez les élèves que chez la plupart des futur professeurs. Rien n'est spécifiquement fait dans le cadre de l'IUFM afin de préciser ou rectifier les conceptions.

Yves Girmens indique que les nombres servent de support à certaines situations de recherche présentées comme activités modèles auprès des futurs maîtres des écoles, mais qu'aucune formation spécifique n'est faite sur le concept de nombre.

ETAT DES LIEUX : L'ARITHMETIQUE, NIVEAU BAC S

Au collège :
- "a divise b" <=> "b = a q" <=> " b multiple de a"
- critère de divisibilité par 2 ; 3; 5 ; 9.

Au lycée :
- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$: sont de simples notations, du vocabulaire. (aucun développement sur les représentations décimales)
- Le dénombrement et les notations : n! ; C_n^p et A_n^p .

Aucun intitulé relatif à l'arithmétique (pas de congruences, Bezout, Gauss ...)

Mais l'approche est aussi pragmatique que réduite :
- pas de notation " | " ;
- le concept de fraction irréductible : « on ne peut plus simplifier » ;
- pas de concept de nombres premiers entre eux ;
- les concepts de PGCD , PPCM ne sont pas présentés ;
- le concept de nombre premier est construit de façon empirique sous la forme : « nombre qui n'a pas de diviseur propre » (et 1 ?) mais il n'est fait aucune considération sur l'ensemble des nombres premiers ;
- pas de décomposition en produit de nombres premiers (existence de la décomposition, unicité, pratique) ;
- aucune notion de "base de numération".

Exemples et pratiques :
- dominé : $\sqrt{12} = 2\sqrt{3}$ (la décomposition empirique).
- pas un réflexe : $\ln 128 = 7 \ln 2$ (pas de décomposition systématique).
- laborieux : les calculs élémentaires sur n! ; C_n^p et A_n^p

- Mais : *- pratique de la décomposition en produit de nombres premiers ;*
- mention des mots PGCD et PPCM ;
- on peut lire des énoncés :"exprimer cette probabilité sous forme d'une fraction irréductible" .