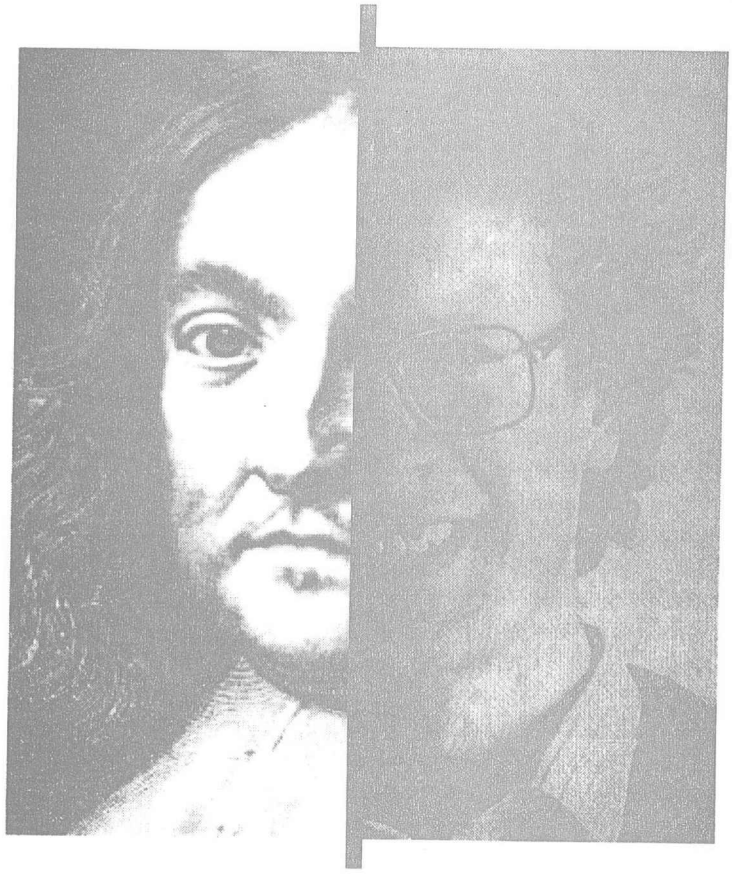
INSTITUT DE RECHERCHE SUR L'ENSEIGNEMENT DES MATHEMATIQUES

Université Montpellier II

FRAGMENTS D'ARITHMETIQUE



René BERNARD, Nathalie BRIANT, Christian FAURE, Joëlle FONTANA,
Maryse NOGUES, Luc TROUCHE

1999

Sommaire

INSTITUT DE RECHERCHE SUR L'ENSEIGNEMENT DES MATHEMATIQUES

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
http://www.univ-montp2.fr/~irem/

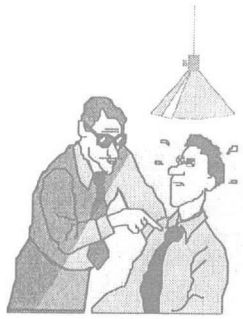
En couverture, Pierre de Fermat et Andrew Wiles. Le premier né en 1601, le second en 1953. Plus de trois siècles entre la formulation du théorème, " l'équation $x^n + y^n = z^n$ n'admet aucune solution entière pour $n > 2$ ", et sa démonstration en 1995. Entre les deux, une longue chaîne de chercheurs plus ou moins heureux : Euler (1753), Legendre (1822), Lejeune-Dirichlet (1825), Lame (1839), Sophie Germain (1840), Kummer (1845), Taniyama-Shimura (1955), Faltings (1983), Ribet (1988).

René BERNARD, Nathalie BRIANT, Christian FAURE, Joëlle FONTANA,
Maryse NOGUES, Luc TROUCHE

1999

Introduction

mathématique) date de septembre 1998. En 1995, notre équipe avait déjà proposé quelques jalons pour préparer ce retour attendu (Bernard et al, 1995.b). La réintroduction de 1998 nous a donné l'occasion de reprendre cette réflexion, tout particulièrement à l'occasion de stages de formation [1]. Des pistes nous ont d'ailleurs été proposées par les stagiaires eux-mêmes, à qui nous avions posé trois questions.



1. Que représente l'arithmétique pour vous ?

« Du travail dans $\mathbb{N}$, ce qui se fait en primaire, mais aussi quelque chose qui m'a passionné à enseigner il y a bien longtemps en TC, mais que j'ai bien oublié... » ; « Un point nouveau au programme, plus enseigné depuis 75 pour moi » ; « Quelques souvenirs, PPCM, PGCD... » ; « Du travail dans N, ce qui se fait en primaire, mais aussi quelque chose qui m'a passionné à enseigner il y a bien longtemps en TC, mais que j'ai bien oublié... » ; « Un point nouveau au programme, plus enseigné depuis 75 pour moi » ; « Quelques souvenirs, PPCM, PGCD... » ; « Etude des propriétés des entiers » ; « Théorie des nombres, calculs dans $\mathbb{Z}/n\mathbb{Z}$, théorème chinois » ; « De belles manipulations de nombres et d'inconnues, mais pas toujours aisées » ; « Tout est nombre, disait Pythagore » ; « C'est la base, le fondement des mathématiques » ; « A partir des nombres, les premières modélisations peuvent apparaître » ; « Une branche fondamentale des math, servant de base à de nombreuses théories » ; « L'origine des concepts » ; « Une autre façon de raisonner (disjonction des cas) » ; « Un moyen de réflexion et d'utilisation de certains outils mathématiques » ; « Une approche théorique construite, cohérente, rigoureuse » ; « Un outil performant » ; « Intérêt culturel » ; « Ludique ».

---

[1] Stages *Nouveaux programmes en terminale S et ES* au lycée Louis Feuillade de Lunel et *Arithmétique et algorithmique* au lycée Montaury de Nîmes.

2. Quelle arithmétique enseigner au lycée ?

« L'ancien programme me plaisait » ; « Celui enseigné au collège autrefois » ; « Divisibilité, nombres premiers » ; « Les bases, PGCD, PPCM, congruences, Bezout, algorithme d'Euclide » ; « Retrouver les concepts générateurs » ; « Présenter les structures et la construction des ensembles » ; « Approches et construction d'ensemble cohérents » ; « La rigueur » ; « Résolution d'exercices et de problèmes non triviaux » ; « Un ensemble ludique, c'est-à-dire autour de recherche, d'expériences, de manipulations ».

3. Pourquoi réintroduire l'arithmétique aujourd'hui ?

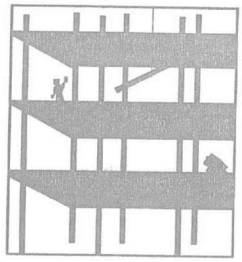
« Aucune idée » ; « Une certaine mode » ; « Pourquoi l'avoir enlevé ? » ; « Pourquoi ne pas l'introduire avant la classe de terminale ? » ; « Pourquoi ne la réintroduire que pour l'enseignement de spécialité ? » ; « Parce qu'on s'est rendu compte que les élèves ne savaient plus compter » ; « Meilleure maîtrise des nombres pour l'enseignement du calcul scientifique » ; « Pour tous ces ordinateurs en quête d'arithmétique» ; « Pour l'informatique » ; « Besoin algorithmique » ; « Travailler la cohérence, la rigueur, le raisonnement » ; « Préserver un minimum d'exigence » ; « Créer un domaine où l'approche recherche pourrait s'exercer » ; « Boucher un trou culturel » ; « Besoin de certaines notions d'arithmétique dans le supérieur (anneaux de polynômes, algèbre... »

Nous avons essayé de répondre à ces attentes très diverses en développant quelques éléments du programme d'arithmétique officiel, mais aussi quelques éléments théoriques plus généraux (anneaux, petit théorème de Fermat, algorithmique) qui pourront parfois être adaptés pour l'enseignement, qui contribueront de toutes façons à une redécouverte d'une "culture arithmétique".

Nous aurions aussi pu trouver des pistes de réflexion en consultant l'Encyclopédie Universalis. À la rubrique « Arithmétique », on trouve les renvois suivants :

- arithmétique et théorie des nombres ;
- arithmétique et divisibilité ;
- arithmétique formelle (théorie de la démonstration, Frege, intuitionnisme, récursivité, Russel) ;
- arithmétique et machines (Pascal) ;
- arithmétique et opérations (calculateurs) ;
- arithmétisation d'une théorie (fondements des mathématiques).

Vaste programme... Le travail arithmétique combine en effet des activités élémentaires sur les nombres entiers, mais aussi le recours à des méthodes très subtiles. De cette ambivalence témoignent les citations bien connues :



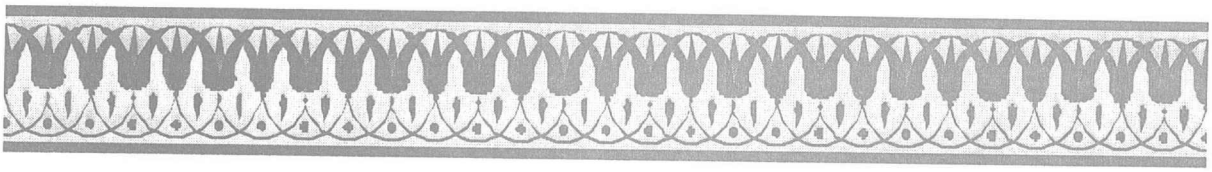
- « Dieu a créé les nombres entiers, tout le reste est l'œuvre de l'homme » [Kronecker] ;
- « La mathématique est la reine des sciences, et l'arithmétique est la reine des mathématiques » [Gauss].

Le lecteur trouvera donc ici des thèmes d'activité et de réflexion de difficulté variée. Bon travail, crayon (et parfois calculatrice) en main ! Nous remercions d'avance tous ceux qui nous feront part de leurs remarques et de leurs critiques.

Cette brochure a été réalisée, en partie, grâce aux heures attribuées par l'IUFM au titre de la formation et grâce au soutien de la DESCO[2] au titre de la recherche.

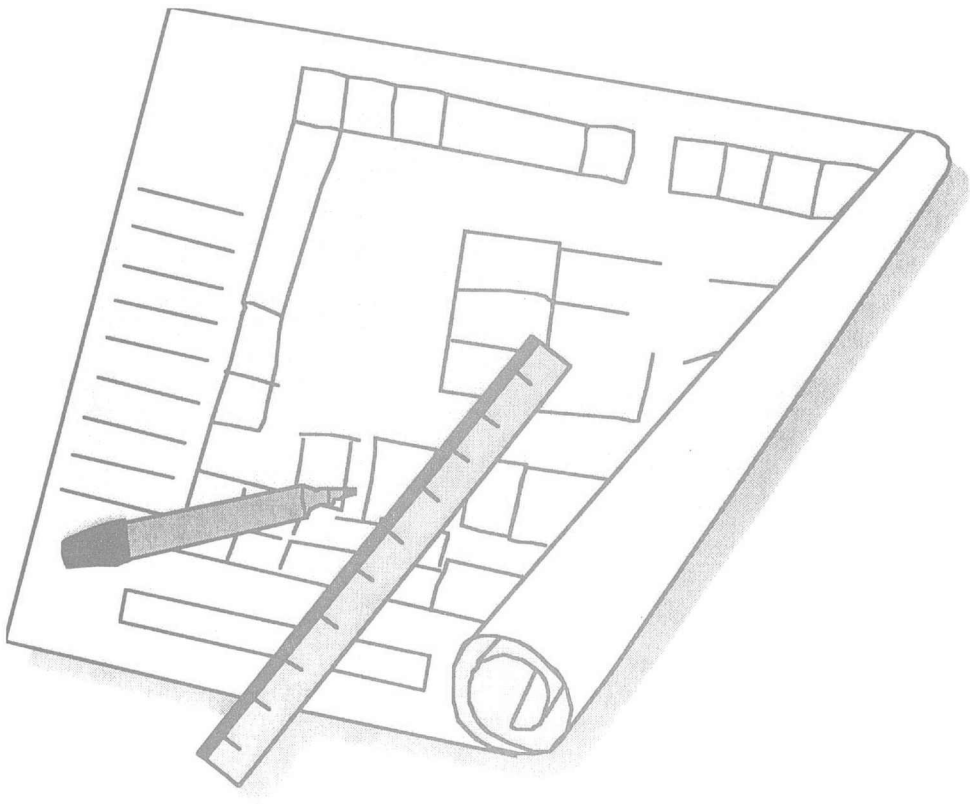
L'équipe Analyse de l'IREM de Montpellier :

René BERNARD (lycée Gérard Philipe, Bagnols-Sur-Cèze) ;
Nathalie BRIANT (lycée Louis Feuillade, Lunel) ;
Christian FAURE (lycée Joffre, Montpellier) ;
Joëlle FONTANA (poste de rattachement au lycée Joffre, Montpellier) ;
Maryse NOGUES (lycée Louis Feuillade, Lunel) ;
Luc TROUCHE (université Montpellier II).



[2] DESCO : Direction de l'Enseignement SCOlaire.

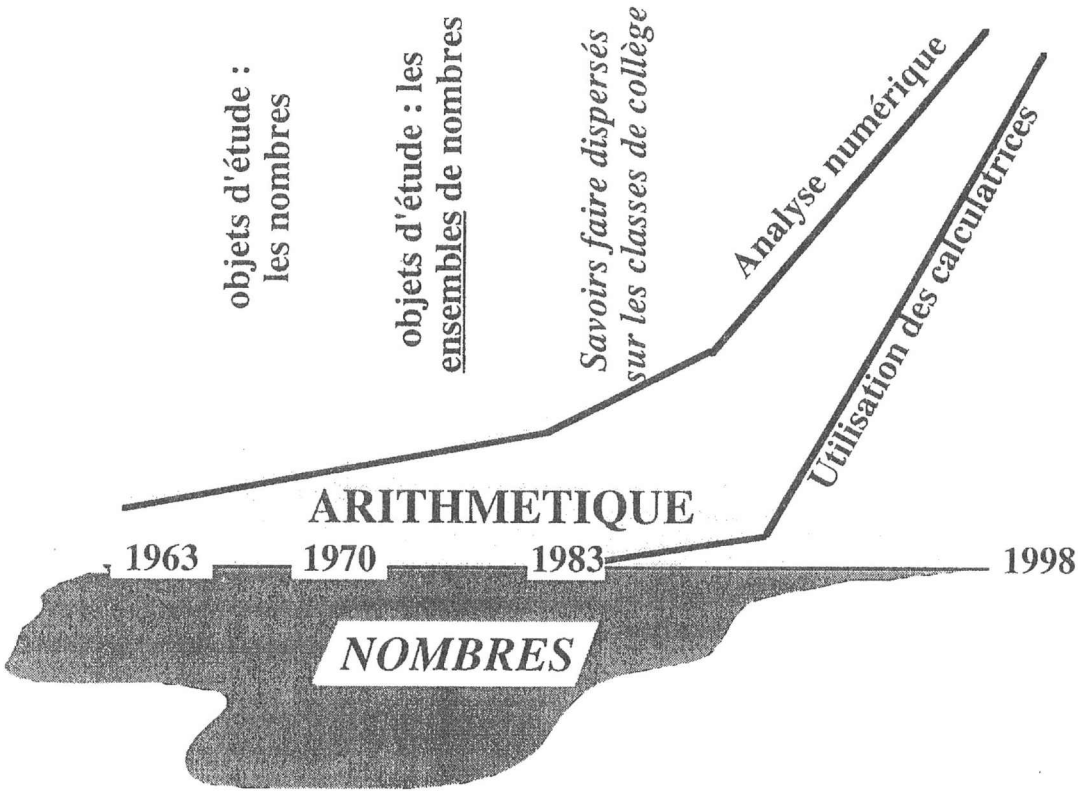
I. Les nombres au lycée : évolution des programmes



1.1. Une approche synthétique

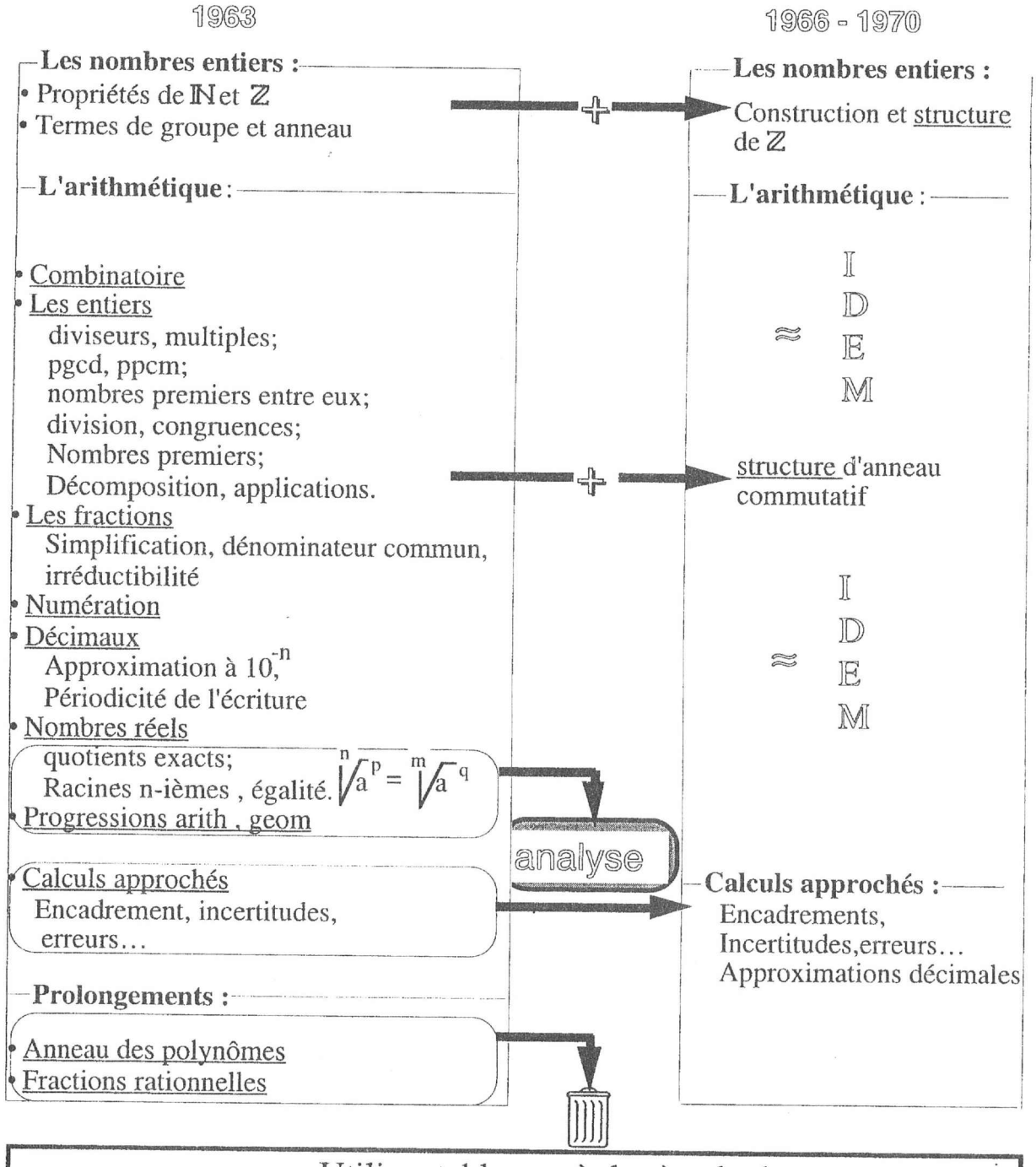
Si les objets mathématiques émergent des pratiques, celles-ci sont dictées par les programmes. La place de l'arithmétique, arène des nombres par excellence, a fortement varié qualitativement et quantitativement. Avec la vague structuraliste, l'objet d'étude s'est déplacé des nombres vers les ensembles de nombres. Avec le reflux de cette vague, l'arithmétique a été ramenée à une liste de savoir-faire dispersés sur les programmes du collège puis réduite à rien.

Force est ainsi de constater sur ces dernières années une érosion du concept de nombre qui coïncide paradoxalement avec une montée en puissance de l'enseignement de l'analyse et une large diffusion des outils de calcul.



L'étude de l'arithmétique et des nombres s'étiole, l'analyse progresse.

I.2. Evolution des programmes entre 1963 et 1983



Utiliser tables et règles à calcul

1971 - 1983

Les nombres entiers :

- Axiomatique de $\mathbb{N}$
- L'anneau $\mathbb{Z}$

L'arithmétique :

- Notation indicielle : $\mathbb{N} \longrightarrow X$
- $n\mathbb{Z}$ et congruences anneau $\mathbb{Z}/n\mathbb{Z}$
- Nombres premiers dans $\mathbb{Z}$, corps $\mathbb{Z}/n\mathbb{Z}$ si n premier)
- Décomposition, existence et unicité
- Pgcd,ppcm, théorème de Bezout
- Numération bases 10 et 2

Calcul numérique

- Valeurs approchées à 10
- Encadrements
- Incertitudes ...
- Représentation d'un réel par une suite décimale

1983 .....

Les nombres entiers :

Aucune mention

L'arithmétique :

V I D E

Classes antérieures

1971	1982	1986
Utiliser : tables, règles à calcul, machines "de bureau"	Utiliser largement les calculatrices	Utiliser systématiquement les calculatrices

I.3. Le nouveau programme de 1998 (Terminale S)

Après des années de purgatoire, il fallait que la réintroduction timide - en spécialité de Terminale S seulement - de l'arithmétique dans les programmes, présentât des objectifs simples mais en cohérence avec la modernité de cette discipline.

Pour les collègues qui se souviennent des programmes d'arithmétique de Terminale des années 70, c'est une vraie rupture. On y trouve, bien entendu les théorèmes et algorithmes fondamentaux (Euclide, Gauss, Bezout) mais l'objectif affirmé n'est plus dans la résolution de problèmes nécessitant cette construction particulière, à la fois intuitive et rigoureuse, qui les rendait si délicats. Non pas que de tels problèmes ne puissent pas se présenter : mais ils sont asservis à l'usage qui peut en être fait dans les domaines de l'informatique par exemple.

C'est autour de la notion d'algorithme que se construit ce nouveau programme. Il s'agit d'initier les candidats bacheliers à la construction d'algorithmes élémentaires ("simples et fondamentaux"), puis d'utiliser ces algorithmes dans la résolution de problèmes "à l'intérieur et en dehors du domaine mathématique" (calendrier, codage). On peut supposer que dans un proche avenir, le programme demandera d'implanter ces algorithmes dans un outil informatique. Alors, des théorèmes fondamentaux à l'élaboration d'algorithmes et jusqu'à leur utilisation dans un ordinateur, le "minimum de cohérence" sera atteint.

Enseignement de spécialité

Le paragraphe suivant n'est au programme que de l'enseignement de spécialité.

2 - Arithmétique

L'arithmétique mérite de tenir une place dans la série scientifique, pour l'enseignement de spécialité, en raison de son importance dans le développement des mathématiques. L'objectif est de donner aux élèves un minimum cohérent de notions élémentaires permettant l'élaboration d'algorithmes simples et fondamentaux et l'introduction d'applications diverses à l'intérieur et en dehors du domaine mathématique.

Divisibilité dans $\mathbb{Z}$: diviseurs, multiples d'un entier.

Nombres premiers. Existence de la décomposition d'un entier naturel en produit de facteurs premiers. Existence d'une infinité de nombres premiers.

Division euclidienne et algorithme d'Euclide. Plus grand commun diviseur et plus petit commun multiple de deux entiers naturels. Entiers premiers entre eux.

Théorème de Bezout, théorème de Gauss.

Aucune virtuosité n'est demandée aux élèves, mais ils devront savoir par exemple dresser la liste des diviseurs d'un entier donné, dans des cas simples. L'unicité de la décomposition en facteurs premiers sera admise et son obtention pourra résulter de l'utilisation d'un logiciel de calcul formel.

Il s'agit d'exploiter l'ensemble constitué de l'égalité et de l'inégalité définissant une division euclidienne. Pour les déterminations de PGCD et PPCM, on évitera le recours systématique à la décomposition en facteurs premiers.

On appliquera les résultats sur les entiers aux fractions : fractions irréductibles par exemple.

Travaux pratiques

Mise en œuvre de l'algorithme d'essai de division par les nombres premiers successifs pour reconnaître si un entier donné est premier. Crible d'Eratosthène.

Pour tester si un nombre est premier, l'algorithme comporte une condition d'arrêt à indiquer. On se limitera à des exemples simples.

Sur des exemples, utilisation de la division euclidienne pour obtenir des critères de divisibilité. Exemples de changements de base de numération.

La division euclidienne permet d'établir des conpatibilités avec les opérations nécessaires pour les problèmes étudiés. Ceux-ci pourront être l'occasion de présenter et de mettre en œuvre la notion de congruence, au sujet de laquelle aucune connaissance spécifique ne peut être exigée. Toute introduction de $\mathbb{Z}/n\mathbb{Z}$ est hors programme. L'aspect algorithmique sera privilégié.

Calculs de PGCD et PPCM.

Exemples de résolution dans $\mathbb{Z}$ d'équations du type $au + bv = d$ où d est le PGCD des entiers a et b.

L'introduction de quelques exemples de problèmes de calendrier, de méthodes de codage ou de cryptage, permet de familiariser les élèves avec les diverses notions du programme, à l'occasion d'applications concrètes, et non d'exiger d'eux la connaissance d'une liste d'algorithmes.

I.4. Les manuels scolaires de TS, spécialité mathématiques

Nous présentons ici un échantillon des manuels scolaires de la terminale S spécialité mathématiques.

Dans les deux tableaux qui suivent, nous dégageons deux catégories de manuels, ceux qui débutent le cours par la notion de nombres premiers entre eux (tableau 1) et ceux qui choisissent de placer la notion de nombres premiers dès le départ (tableau 2) .

Cette remarque n'est pas anodine car elle implique une approche différente du programme et de l'arithmétique. Les ouvrages ayant choisi de commencer par les nombres premiers ont tendance à passer rapidement ou même à occulter l'algorithme d'Euclide de recherche du PGCD. Par contre, ils présentent tous des problèmes de synthèse riches et intéressants.

Trois rubriques sont présentées pour chaque manuel :

- *le contenu des chapitres avec leur progression,*
- *les travaux dirigés,*
- *quelques notes permettant de mettre en évidence la particularité de chaque manuel.*

La liste des manuels présentés est la suivante :

Fractale [BORDAS]
Transmath [NATHAN]
TS Spécialité [BREAL]
Déclic [HACHETTE]
Terracher [HACHETTE]
Dimathème [DIDIER]
TS Spécialité [BELIN]

	Fractale (Bordas)	**Transmath (Nathan)**	**TS Spécialité (Bréal)**
CHAPITRES	75 pages 1 - Divisibilité - Division euclidienne. 2 - PGCD - Nombres premiers entre eux. 3 - PPCM. 4 - Nombres premiers.	75 pages 1 - Divisibilité - PGCD - PPCM. Nombres premiers entre eux Bezout - Gauss. 2 - Nombres premiers en facteurs premiers. 3 - Recherche de PGCD et PPCM.	58 pages 1 - Divisibilité - Division euclidienne. 2 - PGCD - PPCM Nombres premiers entre eux. Euclide - Bezout - Gauss. 3 - Nombres premiers.
TD	- Congruences. - Changement de base de numération. - Simplification de fractions. - Crible d'Eratosthène. - Algorithme de reconnaissance d'un nombre premier. - Décomposition en facteurs premiers. - Nombres de Mersenne.	- Algorithme de recherche du PGCD et des coefficients de Bezout. - Algorithme de reconnaissance d'un nombre premier. - Congruences avec propriétés. - Critères de divisibilité. - Changement de base de numération. - Théorèmes de Fermat (petit) et de Wilson. - Cryptographie (RSA)	- Congruences. - Critères de divisibilité. - Changement de base de numération. - Triangles rectangles à trois côtés entiers. - Application du PGCD aux fractions. - PGCD et PPCM de trois entiers. - Algorithmes : Eratosthène décomposition en facteurs premiers. - Cryptographie.
A NOTER	- A la fin de chaque chapitre, des exercices Post-Bac intéressants (équations diophantiennes, petit théorème de Wilson). - Les différentes notions sont bien amenées de façon simple et précise. - Peu d'algorithmique. - Pas de méthode de cryptage.	- A la fin de chaque chapitre, des conseils, des problèmes de synthèse. (Combinaisons et nombres premiers ; nombres polynomadiques ; suites de Fibonacci ; somme des n entiers premiers, ...). - Manuel très complet, bonnes explications aussi bien pour les notions simples que pous les plus complexes. - Beaucoup d'algorithmique facile à comprendre. - Des commentaires pertinents (méthodes, conseils, historique).	- A la fin de chaque chapitre, des exercices résolus "savoir-faire" bien choisis et bien traités. - Notation délicate pour PGCD et PPCM. - Comparaison de la recherche du PGCD par Euclide ou factorisation en facteurs premiers. - Démonstration du petit théorème de Fermat. - Peu d'algorithmique. - Exposé très classique.

Tableau 1

	Déclic (Hachette)	**Terracher (Hachette)**	**Dimathème (Didier)**	**TS Spécialité (Belin)**
CHAPITRES	73 pages 1 - Divisibilité - Division euclidienne. Nombres premiers. Décomposition d'un entier. 2 - PGCD - PPCM. Nombres premiers entre eux.	50 pages 1- Divisibilité - Nombres premiers. 2 - Division euclidienne - PGCD - PPCM. Nombres premiers entre eux Bezout - Gauss. Congruences et propriétés *	40 pages 1 - Diviseurs et multiples. Nombres premiers. 2 - PGCD - Nombres premiers entre eux - PPCM. 3 - Division Euclidienne - Congruences. 4 - Euclide - Bezout - Gauss.	50 pages 1 - Divisibilité et division euclidienne. 2 - Nombres premiers. 3 - Diviseurs et multiples communs. PGCD et PPCM - Nombres premiers entre eux.
TD	- Congruences. - Changement de base de numération. - Simplification de fractions. - Algorithme de décomposition d'un nombre en facteurs premiers. - Cryptographie (RSA). - Exercices liés au calendrier.	- Problèmes de divisibilité et raisonnement par récurrence. - Changement de base de numération. - Crible d'Erastosthène. - Nombres parfaits. - Problèmes de calendrier. - Reconnaissance de la rationnalité d'un nombre. - Cryptographie (RSA et multiplication modulo).	- Congruences et critères de divisibilité. - Changement de base de numération. - Crible d'Eratosthène. - Cryptographie (RSA).	TD : - Problèmes de calendrier. - Congruence. - Changement de base de numération. - Critères de divisibilité et preuve par 9. - Crible d'Eratosthène. - Cryptographie (RSA). - PGCD et PPCM de plusieurs nombres.
A NOTER	-Activités préparatoires très intéressantes (systèmes de numération égyptien et babylonien ; définitions et propriétés de N et Z). - Quelques équations diophantiennes, sans les nommer. - Peu d'algorithmique. - Progression bien faite, en accord avec les programmes. - Notions bien amenées : exemples et exercices ni triviaux, ni trop difficiles.	- Intérêt d'utiliser Euclide ou la décomposition en facteurs premiers pour le PGCD. - Donne la définition d'une équation diophantienne. - Des problèmes de synthèse riches et originaux (triplets pythagoriciens ; équations de Pell-Fermat ; série harmonique). - Algorithmique (langage Maple). - Crible d'Eratosthène ; Euclide ; changement de base ; recherche des coefficients de Bezout.	- A la fin de chaque chapitre, des exercices résolus "les incontournables " bien rédigés. - Notation délicate pour PGCD et PPCM. - Manuel difficile à aborder pour les élèves. - Progression très rapide. - Peu d'algorithmique. - Ne respecte pas les consignes du BO (PGCD par facteurs premiers uniquement).	A noter : - Exposé très classique mais correct. - Exercices classiques mais quelques problèmes originaux (nombres amiables, parfaits). - Problèmes issus du Bac des années 1975 (fractions irréductibles décimales). - Présentation des deux méthodes pour déterminer un PGCD. - Pas d'algorithmique.

Tableau 2

I.5. Des exercices d'un nouveau style

Les exercices qui suivent ont été posés en 98/99 lors des bacs blancs des lycées nommés. Ils permettent de donner quelques exemples, tels que les envisagent les enseignants, d'un nouveau type d'exercice possible pour l'épreuve du Baccalauréat.

Exemple 1 : Lycée Gérard Philipe de Bagnols sur Cèze

Soit a et b deux entiers naturels tels que $0 < b \leq a$.

On pose $\sigma = PGCD(a , b)$ et $\mu = PPCM(a , b)$.

On se propose de calculer a et b sachant que $\mu^2 - 5\,\sigma^2 = 2000$.

Soit S l'ensemble des couples (a , b) solutions.

1. Montrer que si (a , b) appartient à S, alors σ^2 divise 2000.

2. Décomposer 2000 en produit de facteurs premiers. En déduire les entiers naturels dont le carré divise 2000.

3. Montrer que si (a , b) appartient à S, 5 est un diviseur commun à σ et μ.

4. En déduire les valeurs possibles de σ et achever la résolution du système proposé.

Exemple 2 : Lycée Joffre de Montpellier

x et y étant des entiers naturels, on pose d = pgcd(x, y) et m = ppcm(x, y) et on considère l'équation en (x , y) : (E) $m^3 + 432\,d^3 = 17280$.

1. Décomposer 17280 en facteurs premiers (toutes les étapes de la décomposition devront figurer sur la copie).

2. Quels sont les entiers naturels dont le cube est un diviseur de 17280 ?

3. Montrer que si (x, y) est une solution de (E) alors d^3 divise 17280.

4. Déduire des questions précédentes toutes les solutions (x, y) de l'équation (E).

Exemple 3 : Lycée Louis-Feuillade de Lunel

1. a. Montrer qu'il existe au moins un entier relatif x et un entier relatiy tels que : 661x -991y = 1. Déterminer une valeur de x et une valeur de y.

b. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation 661x - 991y = 1.

c. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation 3305x - 4955y = 10.

2. On considère deux suites arithmétiques (u_n) et (v_n) définies par : $u_0 = 3$, $v_0 = 2$, et pour tout entier naturel n, $u_{n+1} = u_n + 991$ et $v_{n+1} = v_n + 661$.

Déterminer tous les couples (p,q) de $\mathbb{N}\times\mathbb{N}$ tels que $p \leq 2000$, $q \leq 2000$ et $u_p = v_q$.

Exemple 4 : Lycée Clémenceau de Montpellier

x, y et z sont des entiers naturels compris entre 0 et 8.

Le but de l'exercice est de trouver tous les triplets (x, y, z) tels qu'un entier qui s'écrit xyz en base 9 s'écrive zxy en base 13.

1. Montrer qu'un entier N s'écrit xyz en base 9 et zxy en base 13 si et seulement si :

$42z = 17x + 2y$

2. En déduire que x est pair. Quelles sont les valeurs possibles de x ?

3. On prend x = 2. Déterminer y et z s'ils existent tels que le triplet (2, y, z) soit solution de l'exercice.

4. Terminer l'exercice en étudiant successivement les cas x = 4, x = 6, x = 8.

5. Conclure et donner en base 10 les entiers N qui répondent à la question.

Exemple 5 : Lycée Mas de Tesse de Montpellier

On considère les équations (E) et (E') suivantes où *x* et *y* sont deux entiers relatifs.

(E) : 138 x - 55 y = 5 (E') : 138 x - 55 y = 1

1. Calculer le PGCD de 138 et 55.

2. Démontrer que si un couple (x, y) est solution de (E) alors 5 divise x.

3. a) Par l'algorithme d'Euclide, déterminer une solution (x_0, y_0) de l'équation (E'). En déduire une solution (x_1, y_1) de l'équation (E).

b) Démontrer que si un couple (x, y) est solution de (E) alors $138(x - x_1) - 55(y - y_1) = 0$. Déterminer alors toutes les autres solutions de (E).

4. Soit δ le PGCD de deux nombres x et y formant un couple (x, y) solution de (E). Quelles sont les valeurs possibles de δ ? Quelles sont les solutions de (E) telles que x et y soient premiers entre eux ?

Exemple 6 : Exercice du Baccalauréat, session de juin 99

Pour tout entier naturel non nul, on considère les nombres

$a_n = 4 \times 10^n - 1$, $b_n = 2 \times 10^n - 1$ et $c_n = 2 \times 10^n + 1$.

1. a) a_1, b_1, c_1, a_2, b_2, c_2, a_3, b_3, et c_3.

b) Combien les écritures décimales des nombres a_n et c_n ont-elles de chiffres ? Montrer que a_n et c_n sont divisibles par 3.

c) Montrer en utilisant la liste des nombres premiers inférieurs à 100 donnée ci-dessous, que b_3 est premier.

d) Montrer que, pour tout entier naturel non nul n, $b_n \times c_n = a_{2n}$.

En déduire la décomposition en facteurs premiers de a_6.

e) Montrer que PGCD (b_n, c_n) = PGCD $(c_n, 2)$. En déduire que b_n et c_n sont premiers entre eux.

2. On considère l'équation :

(1) $\quad b_3 x + c_3 y = 1$

d'inconnues les entiers relatifs x et y.

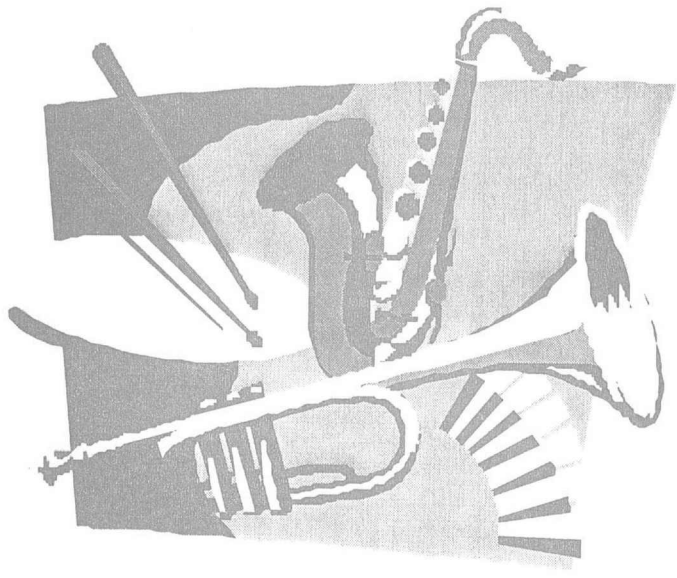
a) Justifier le fait que (1) possède au moins une solution.

b) Appliquer l'algorithme d'Euclide aux nombres c_3 et b_3 ; en déduire une solution particulière de (1).

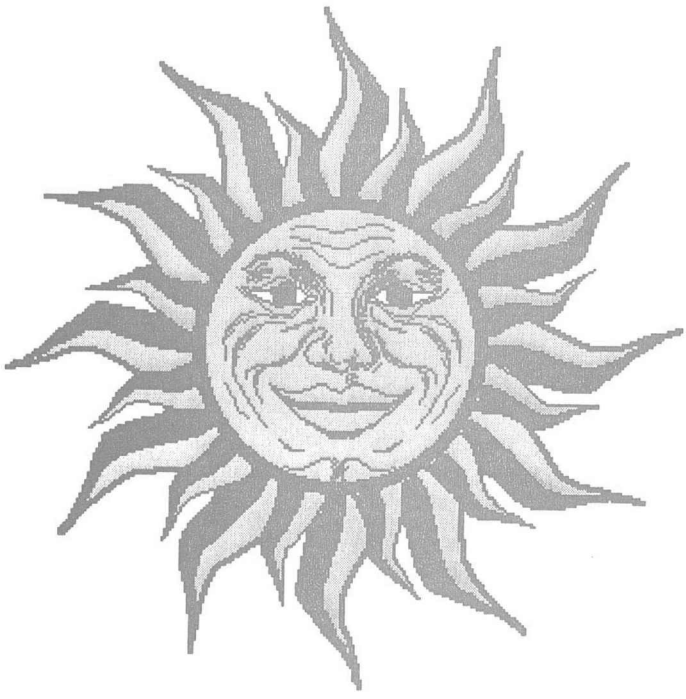
c) Résoudre l'équation (1).

Liste des nombres premiers inférieurs à 100 :

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43 ; 47 ; 53 ; 59 ; 61 ; 67 ; 71 ; 73 ; 79 ; 83 ; 89 ; 97.



II. Divisibilité



II.1. Les fondements théoriques : la structure d'anneau

La théorie des anneaux permet de définir rigoureusement la division euclidienne. Il nous a semblé utile d'en rappeler les résultats fondamentaux avant de nous intéresser plus particulièrement à l'anneau $\mathbb{Z}$, base de l'arithmétique élémentaire.

II.1.1. Anneau commutatif unitaire

Loi +	Loi x
Associative	Associative
Commutative	Commutative
Neutre 0	Neutre 1
Symétrique	.....
Distributive	

Exemples :

1 • $(\mathbb{Z} ; + ; x)$

2 • $(\mathbb{R}[X] ; + ; x)$

3 • $(\mathbb{R}[X;Y] ; + ; x)$

4 • $\mathbb{Z}[i\sqrt{2}] = \{ a + i\, b\sqrt{2} \ ; (a ; b) \in \mathbb{Z} \}$

5 • $(\mathbb{R}^{\mathbb{R}} ; +, x)$ anneau des fonctions numériques définies sur $\mathbb{R}$

Remarque : tous les anneaux que nous évoquerons ici seront commutatifs et unitaires et on dira « anneau » pour parler d'anneau commutatif unitaire (c.u.).

1. Anneau commutatif **intègre**

« $\mathbb{A} \neq \{0\}$ et si $ab = 0$ alors $a = 0$ ou $b = 0$ »

Exemples : - les anneaux des exemples 1, 2, 3 et 4 sont intègres ;

- l'anneau de l'exemple 5 n'est pas intègre.

1. Eléments **inversibles** dans un anneau

« x inversible de $\mathbb{A}$: $\exists!\, x' \in \mathbb{A}$; $x \,.\, x' = 1_{\mathbb{A}}$ »

Remarque : on note généralement $\mathbb{A}^*$ l'ensemble des inversibles de $\mathbb{A}$

Exemples : - les inversibles de $\mathbb{Z}$ sont -1 et 1 ;

- les inversibles de $\mathbb{R}[X]$ et $\mathbb{R}[X;Y]$ sont les inversibles de $\mathbb{R}$: $\mathbb{R}^*$, soit les polynômes constants non nuls ;

- les inversibles de $\mathbb{R}^{\mathbb{R}}$ sont les fonctions qui n'ont pas de zéro sur $\mathbb{R}$.

Remarque : un **corps** commutatif est un anneau (c. u.) dont tous les éléments sauf le neutre additif, sont inversibles .

II.1.2. Dans un anneau intègre : la divisibilité

1. Divisibilité dans $\mathbb{A}$

« $a \mid b$ signifie : $\exists\, c \in \mathbb{A}$; $ac = b$ »

En général, ce n'est pas une relation d'ordre (car non antisymétrique, par exemple $2 \mid -2$ et $-2 \mid 2$).

2. Éléments irréductibles

« p est irréductible dans $\mathbb{A}$ signifie : p est non inversible (ou encore : $p \notin \mathbb{A}^*$)

$p = ab \Rightarrow (a \in \mathbb{A}^* \text{ ou } b \in \mathbb{A}^*)$ »

Exemples : - dans $\mathbb{Z}$, les irréductibles sont les nombres premiers et leurs opposés ;

- dans $\mathbb{R}[X]$, les irréductibles sont les polynômes de de degré 1 ou les trinômes sans racines réelles ;

- dans $\mathbb{Z}[i\sqrt{2}]$, $1 + i\sqrt{2}$ est irréductible. {Par l'absurde : s'il n'est pas irréductible alors il se factorise, voir alors $|1+ i\sqrt{2}|^2$ qui est irréductible}.

3. Nombres premiers (étrangers) entre eux

« a et b sont premiers entre eux signifie :

si $d \mid a$ et $d \mid b$ alors $d \in \mathbb{A}^*$ (est inversible) »

4. Division euclidienne dans $\mathbb{A}$

« On dit avoir défini une division euclidienne dans $\mathbb{A}$ pour exprimer que :

$\forall a \in \mathbb{A}$; $\forall b \in \mathbb{A} - \{0\}$; $\exists (q ; r) \in \mathbb{A}^2$; $a = bq + r$ et $(\varphi(r) = 0$ ou $\varphi(r) < \varphi(b))$

où φ (stathme euclidien), $\varphi : \mathbb{A} - \{0\} \longrightarrow \mathbb{N}$ tel que $\varphi(ab) \geq \varphi(a)$ »

Exemples : - dans $\mathbb{Z}$, φ est défini par $\varphi(n) = |n|$;

- dans $\mathbb{R}[X]$, φ est défini par $\varphi(P) = d^\circ(P)$;

- dans $\mathbb{Z}[i\sqrt{2}]$, φ est défini par $\varphi(z) = |z|$.

Remarque : dans $\mathbb{N}$, la division euclidienne définit (q ; r) unique, en général (q ; r) n'est unique qu'aux inversibles près.

Anneau euclidien *: un anneau où est définie une division euclidienne.*

II.1.3. Idéaux dans un anneau

« Un idéal (I) de $\mathbb{A}$ est :	- un sous groupe additif de $\mathbb{A}$ - $\forall a \in \mathbb{A}$; $\forall i \in (I)$; $i \,.\, a \in (I)$ »

Exemples : - dans $\mathbb{Z}$, l'idéal des nombres pairs ;

- dans $\mathbb{Z}$, l'idéal engendré par $\{2;3\}$ c'est $\mathbb{Z}$;
- dans $\mathbb{R}[X]$, l'idéal des polynômes qui ont 1 et 2 pour racines ;
- dans $\mathbb{Z}[X]$, l'idéal engendré par $\{X+1 ; X^2+1\}$.

Remarque : la notion d'idéal existe dans les anneaux non intègres. Par exemple dans $\mathbb{R}^{\mathbb{R}}$ l'idéal des fonctions qui s'annulent en x_0. Plus généralement, le noyau de tout morphisme d'anneaux est un idéal de l'anneau de départ.

1. Idéal Principal :

« C'est un idéal engendré par un seul élément »

Exemples : - $2\,\mathbb{Z}$: idéal des nombres pairs dans $\mathbb{Z}$;

- $1\,\mathbb{Z}$: $\mathbb{Z}$ lui-même ;
- $(X-1)(X-2)\,\mathbb{R}[X]$: idéal des multiples de $(X-1)(X-2)$ dans $\mathbb{R}[X]$.

Contre-Exemple : - dans $\mathbb{Z}[X]$ l'idéal engendré par $\{X+1 ; X^2+1\}$ formé des polynômes à coefficients entiers de la forme : $(X+1)\,P(X) + (X^2+1)\,Q(X)$; ces polynômes ne peuvent s'écrire sous une forme : $K(X)\,R(X)$ où K serait un polynôme fixé.

***Anneau principal** : tout idéal y est principal.*

Exemples : $\mathbb{Z}$; $\mathbb{R}[X]$; $\mathbb{C}[X]$ {; $\mathbb{K}[X]$} ; ... ; $\mathbb{Z}[i]$; ...

Contre-exemples : $\mathbb{Z}[X]$; $\mathbb{R}[X;Y]$[3] ; ...

2. Idéal Maximal

---

[3] L'idéal engendré par {X ; Y}, formé des polynômes sans terme constant ne peut pas s'écrire $P.\mathbb{R}[X;Y]$. En clair, les polynômes sans terme constant ne peuvent être tous obtenus à partir d'un seul polynôme P.

« C'est un élément maximal au sens de l'inclusion dans les idéaux de $\mathbb{A}$ (distincts de $\mathbb{A}$) »

Exemple : - $3\mathbb{Z}$ est maximal, il contient $6\mathbb{Z}$, $15\mathbb{Z}$ et $9\mathbb{Z}$ et il n'est inclus dans aucun idéal de $\mathbb{Z}$ (sauf $\mathbb{Z}$ lui-même).

3. Idéal de $\mathbb{Z}$ et divisibilité

« $a \mid b \iff b\mathbb{Z} \subset a\mathbb{Z}$ »

Remarque : Autrement dit, la divisibilité s'exprime par une inclusion entre idéaux principaux, le préordre $\mid$ dans $\mathbb{Z}$ devient un ordre dans les idéaux de $\mathbb{Z}$. La même approche peut être faite dans les idéaux de $\mathbb{R}[X]$ et la divisibilité dans $\mathbb{R}[X]$.

4. La décomposition primaire dans $\mathbb{A}$ principal

Soit $a \in \mathbb{A}$ d'où l'idéal : $a\mathbb{A}$

- Si $a\mathbb{A}$ maximal : a n'a pas de diviseur (propre)
- Sinon $a\mathbb{A} \subset b\mathbb{A} \iff b \mid a \iff a = bc$ donc $\begin{cases} a\mathbb{A} \subset b\mathbb{A} \\ a\mathbb{A} \subset c\mathbb{A} \end{cases}$
- Si $b\mathbb{A}$ maximal ... • Sinon $b\mathbb{A} \subset b'\mathbb{A}$ ...
  - Si $c\mathbb{A}$ maximal ...
  - Sinon $c\mathbb{A} \subset c'\mathbb{A}$ ...

De cette « arborescence » d'inclusions, on extrait des « chaînes » d'inclusions :

$$a\mathbb{A} \subset b\mathbb{A} \subset b'\mathbb{A} \ldots$$

et une propriété de $\mathbb{A}$ principal affirme que cette chaîne est finie[4]

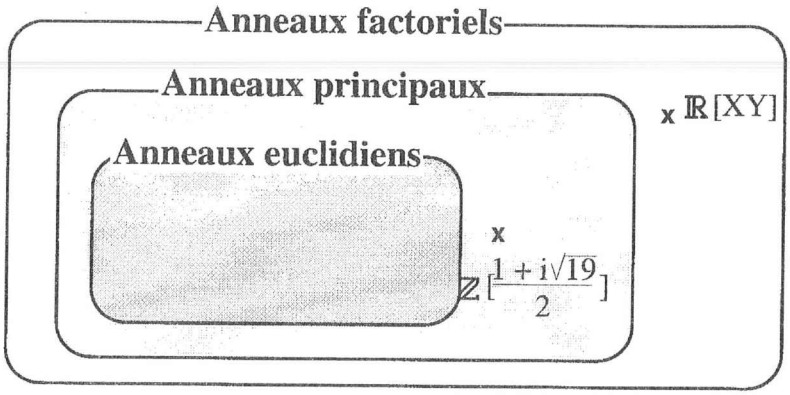
D'où la décomposition de a, décomposition dont on montre l'unicité (à un inversible près) à l'aide de ces éléments particuliers de $\mathbb{A}$ qui engendrent des idéaux maximaux (dans $\mathbb{Z}$: les nombres premiers).

Il existe des anneaux non principaux où la décomposition primaire existe sans que ces anneaux soient principaux ; c'est le cas de $\mathbb{R}[X;Y]$.

Anneaux factoriels : anneaux où il existe une décomposition primaire unique.

[4] Propriété définissant les anneaux noethériens dont les anneaux principaux sont un cas particulier.

II.1.4. En résumé



ANNEAUX FACTORIELS

Il existe (unique aux inversibles près) une décomposition primaire.

- Propriété de PGCD , PPCM
- $a|b \iff \nu_a(p) \leq \nu_b(p)$ {p : premier, ν : exposant de p dans la décomposition appelé : valuation p - adique de a}
- Pas de théorème de Bezout.

ANNEAUX PRINCIPAUX

Tout idéal est un idéal principal.

- Ordre $a\mathbb{A} \subset b\mathbb{A}$ dans les idéaux <---> Préordre b | a
  Idéaux maximaux <-----> Éléments extrémaux
- Théorème de Bezout, notion d'éléments premiers entre eux

(pour le contre exemple de $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ voir page 61 [Perrin 95])

ANNEAUX EUCLIDIENS

Il existe une division euclidienne

Exemple : Dans $A = \mathbb{Z}[i\sqrt{2}] = \{ a + ib\sqrt{2} \ ; (a;b) \in \mathbb{Z}^2 \}$
On a une division euclidienne

Remarque : parmi les anneaux intègres, les anneaux euclidiens sont donc parés de toutes les vertus : théorème de Gauss, décomposition primaire, théorème de Bezout ...

II.1.5. Les anneaux $\mathbb{Z}/n\mathbb{Z}$

Les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont des anneaux quotients[5] de $\mathbb{Z}$. Pour $n \geq 1$ on peut concevoir[6] ces anneaux comme l'ensemble des restes dans la division par n. Ainsi $\mathbb{Z}/6\mathbb{Z} = \{0;1;2;3;4;5\}$; $\mathbb{Z}/2\mathbb{Z} = \{0;1\}$; $\mathbb{Z}/1\mathbb{Z} = \{0\}$... Dans ces anneaux, les opérations + et x induites par celles de $\mathbb{Z}$, donnent des tables d'addition et de multiplication :

Exemple : $\mathbb{Z}/6\mathbb{Z}$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

x	0	1	2	3	4	5
0	*0*	*0*	*0*	*0*	*0*	*0*
1	*0*	1	2	3	4	5
2	*0*	2	4	0	2	4
3	*0*	3	0	3	0	3
4	*0*	4	2	0	4	2
5	*0*	5	4	3	2	1

Remarque : $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre (voir $2 \times 3 = 0$). Les seuls inversibles de $\mathbb{Z}/6\mathbb{Z}$ sont 1 et 5.

Plus généralement on montre (voir Bezout[7]) que les seuls inversibles de $\mathbb{Z}/n\mathbb{Z}^*$ sont les m ($0 \neq m$) qui sont premiers avec n.

Ainsi :
- Dans $\mathbb{Z}/n\mathbb{Z}$, les éléments a et b tels que $ab = 0$ sont appelés "diviseurs de 0".
- $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier ou égal à 0.
- $\mathbb{Z}/n\mathbb{Z}$ est un **corps** fini si et seulement si n est premier.

L'entier n est la **caractéristique** de $\mathbb{Z}/n\mathbb{Z}$.

Exemple : Le corps $\mathbb{Z}/5\mathbb{Z}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

x	0	1	2	3	4
0	*0*	*0*	*0*	*0*	*0*
1	*0*	1	2	3	4
2	*0*	2	4	1	3
3	*0*	3	1	4	2
4	*0*	4	3	2	1

Dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier, on[8] a $(a + b)^p = a^p + b^p$

---

[5] Ce sont les seuls puisque tous les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ ($\mathbb{Z}$ est principal). Par "définition" un anneau quotient se définit par rapport à un de ses idéaux (= noyau de morphisme d'anneaux)

[6] La définition de $\mathbb{Z}/n\mathbb{Z}$ comme ensemble des classes d'équivalences $a \equiv b \iff a-b \in n\mathbb{Z}$ permet une définition plus large incluant $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.

[7] Comme dirait Jacques Vrel.

[8] Démonstration classique : $k!\, C_p^k = p(p-1)\ldots(p-k+1)$; 1;2...k sont premiers avec p car inférieurs à p ; k! est donc premier avec p; p premier avec k! et divisant $k!\, C_p^k$ ...

II.2. Des critères de divisibilité « élargis »

Chacun connaît les critères usuels de divisibilité par 2, 3, 4, etc... En fait, on peut les regrouper en trois catégories. La première consiste en l'observation du ou des derniers chiffres ; la deuxième réside dans la somme des chiffres ou des tranches de chiffres et la troisième dans l'alternance de sommes et différences de chiffres ou tranches. L'intérêt de ce regroupement est double : comprendre les ressemblances entre certains de ces critères (3 et 9 par exemple) et en trouver de nouveaux en s'interrogeant sur leur pertinence.

Considérons un entier naturel n non nul qui s'écrit en base a : "$r_m\, r_{m-1} \ldots r_1\, r_0$".

$$\text{Donc } n = \sum_{i=0}^{m} r_i.a^i.$$

Critère n°1

Si $p \mid a^k$, cherchons un critère de divisibilité par $\frac{a^k}{p}$.

On pose alors $a^k = bp$ donc $a^k \equiv 0$ [b] .

Il est clair que $a^j \equiv a^j$ [b] pour tout $j < k$

et pour $j \geq k$, on pose $j = ck + d$ (avec $0 \leq d < k$)

donc $a^j = a^{ck+d} = (a^k)^c.a^d \equiv 0$ [b]

On peut alors écrire $n \equiv \sum_{i=0}^{k-1} r_i.a^i$ [b]

n est divisible par $\frac{a^k}{p}$ si

la dernière tranche de k chiffres est divisible par $\frac{a^k}{p}$.

Illustration :

divisibilité par 2 , 4 , 8 , 5 , 10 , 25, ... en base 10 ;

divisibilité par 2 , 4 , 8 , ... en base 2.

Critère n°2

Si q | a^k -1, cherchons un critère de divisibilité par $\frac{a^k - 1}{q}$.

On pose $b = \frac{a^k - 1}{q}$ donc $a^k = bq + 1$ d'où $a^k \equiv 1$ [b]

Comme précédemment, $a^j \equiv a^j$ [b] pour tout $j < k$

et pour $j \geq k$, on pose $j = ck + d$ (avec $1 \leq c \leq C$ et $0 \leq d < k$)

en appelant C la plus grande valeur de c obtenue par les divisions ci-dessus.

Et donc $a^j = (a^k)^c.a^d \equiv a^d$ [b].

donc $n \equiv \sum_{c=0}^{C} (\sum_{i=0}^{k-1} r_{ck+i}.a^i)$[b].

n est divisible par $\frac{a^k - 1}{q}$

si la somme des tranches de k chiffres (en commençant par la droite)

est un nombre divisible par $\frac{a^k - 1}{q}$.

Illustration : *divisibilité par 3 , 9 , 33 , 99 , ... en base 10 ;*
divisibilité par 3 , 7 , 15 , ... en base 2.

Critère n°3

Si r | a^k +1, on cherche un critère de divisibilité par $\frac{a^k + 1}{r}$.

On pose $b = \frac{a^k + 1}{r}$ donc $a^k = br - 1$. Donc $a^k \equiv -1$ [b]

Bien entendu, $a^j \equiv a^j$ [b] pour tout $j < k$.

et pour $j \geq k$, on pose $j = ck + d$ (avec $1 \leq c \leq C$ et $0 \leq d < k$)

et donc $a^j = (a^k)^c.a^d \equiv (-1)^c.a^d$ [b].

donc $n \equiv \sum_{c=0}^{C} (-1)^c(\sum_{i=0}^{k-1} r_{ck+i}.a^i))$ [b] .

n est divisible par $\frac{a^k + 1}{r}$

si la somme des tranches de k chiffres de rang impair (en commençant par la droite), diminuée de la somme des tranches de k chiffres de rang pair

est un nombre divisible par $\frac{a^k + 1}{r}$.

Illustration : *divisibilité par 11 , 101 , 1001 , ... en base 10 ;*
divisibilité par 3 , 5 , 9 , ... en base 2.

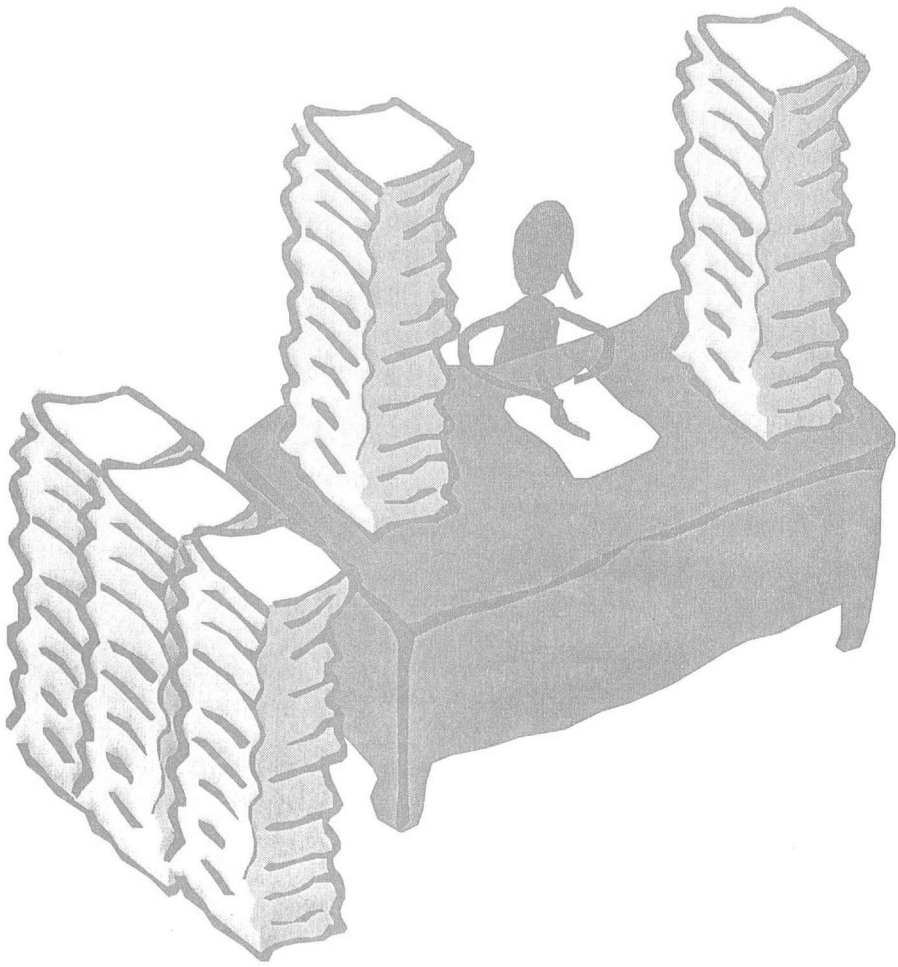
Quelques questions

Existe-t-il, en base 10, un critère "simple" de divisibilité par 7, par 13? (c'est-à-dire qui consomme moins d'énergie que la division elle-même). On peut observer par exemple que $1001 = 7 \times 11 \times 13$. Mais est-ce utile ou assez "simple" ? Dans quels cas, le critère est-il rentable ?

Existe-t-il dans la même base, plusieurs critères de divisibilité par le même nombre ? Peut-il, dans une base donnée, exister un critère utile pour tous les nombres ? Quelles sont les divisions par un entier inférieur à 1000 pour lesquelles il existe un tel critère ?

Peut-on créer des critères de divisibilité par d'autres nombres ?

Et ceci n'achève pas le lot de questions ...



II.3. Les nombres premiers au secours de la cryptographie

La cryptographie est une science centrée sur la création de codes et les méthodes de décodages d'une information qui peut être visible par tous, mais compréhensible seulement par un destinataire. L'arrivée des ordinateurs et le développement considérable de leurs capacités de traitement de l'information oblige les créateurs de codes à développer des recherches concernant l'inviolabilité de leurs informations. Aujourd'hui le code RSA, basé sur la théorie des nombres premiers, est considéré comme l'un des plus performants.

II.3.1. Les systèmes courants de codage

A. Principe :

Il s'agit de définir une bijection d'un ensemble {A, B, C, ...} : l'alphabet-source (qui est l'alphabet naturel éventuellement étendu aux chiffres et à des symboles} vers un alphabet-but[9] qui est en général identique à l'alphabet source. Cette bijection peut être la composée d'une substitution sur un ensemble de nombres. C'est d'ailleurs sur celle-ci qu'interviennent les mathématiques. Les mathématiques interviennent aussi, par des outils statistiques, dans la conceptions d'algorithmes de décodages « en force ».

B. Les codes à clé secrète :

Il s'agit d'une substitution sur l'alphabet naturel. Vu la finalité de la cryptographie, la définition en extension de cette substitution n'est pas retenue. En pratique, cette définition est faite à travers une **clé** et un découpage en blocs de l'information.

Définition de la substitution :

UNE CLE + UNE LONGUEUR DE BLOCS (parfois intrinsèque à la clé).

---

[9] Une telle bijection peut associer à une lettre, un ensemble de symboles : pour brouiller des études statistiques sur le message codé, la lettre A peut être remplacée aléatoirement par A_1 ou A_2 ... A_n.

Exemple : La clé est CALIGULA, ici longueur 6 : C.A.L.I.G.U.

Elle définit la substitution :

C A L I G U
B D E F H J
K M N O P Q
R S T V W X
Y Z

D'où σ(A, B, C,...) = CBKRYADMSZLENTIF... {combinaison de bloc + découpage en colonnes}

Exemple : La clé est CALIGULA, longueur 8 puis on numérote :

C A L I G U L A
3 1 6 5 4 8 7 2

D'où σ(1, 2, 3, 4, 5, 6, 7, 8) = (3, 1, 6, 5, 4, 8, 7, 2).

L'information est alors découpée en blocs de 8 sur chaque bloc et on applique σ au rang de chaque lettre dans le bloc :

ENLEVERΔ BATTERIE S.Δ.C ALCUL ATRICES.Δ

NΔEVELRE.....

Pour plus de confidentialité, on peut empiler les méthodes, mais il faut ménager la « portabilité » de la clé. Dans ce type de codage, on trouve D.E.S. (Data Encrypting System) d'IBM.

De nos jours, le « forçage « direct d'un code, avec un ordinateur spécialisé et des algorithmes ad hoc s'appuyant (entre autres) sur des données statistiques et une information sur le champ sémantique du message, nécessite environ une journée.

C. Le codage R.S.A.

Le codage RSA, dit « codage à clé publique » a trouvé son principe dans les travaux de Rivest Shamir et Adleman (MIT 77). Le principe est d'associer le destinataire du message (message codé visible par tous) avec une clé visible par tous. Mais le forçage direct du message nécessitera un temps de calcul non polynomial [10]

Principe

Soit d'abord n un entier donné.

Soit x (message clair) ..... *«codage»* ..... x^e [n] (message codé)
x^e [n] (message codé ..... «décodage» ..... $(x^e)^d$ [n]

On choisit e et d de sorte que $(x^e)^d \equiv x$ [n]. On appelle e, clé de codage et d clé de décodage.

---

[10] Par "temps polynomial", on entend : le temps de calcul sera asymptotiquement une fonction polynôme de la longueur du message. Dans le cas présent, le temps de calcul de l'algorithme le plus performant est équivalent à $\exp(\sqrt{\ln(n)}\ln(\ln n))$. Il ne s'agit pas toutefois d'un problème dit NP.

Exemple : On choisit n = 33 et on va coder le message x = 15, la clé de codage sera « publique » et d'ailleurs on la donne : e = 7. Chercher à décoder, soit chercher d de sorte que $(15^7)^d \equiv 15$ [33] et vérifier que tout x (< 33) peut ainsi être codé puis décodé.

Avec le même n (= 33), la clé est maintenant e = 4, chercher à décoder en déterminant un entier d de sorte que : $(x^4)^d \equiv x$ [33]. On remarquera l'existence de d pour e = 7 et la non existence de d pour e = 4.

Étant donné n, il faut donc pouvoir décider de l'existence d'une clé de codage e et d'une clé de décodage d. Dans la pratique, qui sera précisée plus loin, e sera connue de tous (du codeur en particulier !) mais e ne sera connue que du destinataire du message.

Il faut donc trouver des solutions à « $(x^e)^d \equiv x$ [n] pour tout x (x < n) » les inconnues étant e et d entiers.

$(x^e)^d \equiv x$ [n] <=> $x^{ed-1} \equiv 1$ [n]. Or d'après la formule d'Euler : $x^{\varphi(n)} \equiv 1$[n] pour tout x strictement positif et n (≥ 2) premiers entre eux (dans le cas présent x, le message, ne sera pas nul et on prendra n produit de nombres premiers plus grands que Max (x)).

On a donc comme solution : $ed - 1 = \varphi(n)$ ou encore : $ed = 1 + \varphi(n)$ ou encore : $ed \equiv [\varphi(n)]$.

A priori, $\varphi(n)$ n'est pas premier (voir l'expression de l'indicatrice d'Euler page 39) et les seuls inversibles dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$ sont les nombres qui sont premiers avec $\varphi(n)$. On prendra donc e premier avec $\varphi(n)$ et d sera son inverse dans l'anneau $\mathbb{Z}/\varphi(n)\mathbb{Z}$.

On détermine si e est premier avec $\varphi(n)$ par l'algorithme d'Euclide; en « dévissant » cet algorithme et en utilisant l'expression $a\,e + b\,\varphi(n) = 1$ issue du théorème de Bezout, on peut calculer d.

Méthode :

Les concepteurs choisissent deux nombres p et q premiers (très grands, beaucoup plus grand que le message le plus grand) et définissent n = pq puis calculent $\varphi(n)$ qui est la fonction indicatrice d'Euler. Celle-ci prend une valeur très facile à calculer quand on connaît p et q : $\varphi(n) = (p - 1)(q - 1)$ mais le calcul de $\varphi(n)$ devient « infaisable » si on ne connaît que n car il faudrait d'abord le factoriser avec ses deux facteurs premiers et ce problème utilise un algorithme très coûteux.

Ensuite, les concepteurs affectent à chaque destinataire une clé e qui sera publiée (type annuaire). Cette clé est choisie de sorte que e et $\varphi(n)$ soient premiers entre eux[11] ainsi e sera inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$. Les concepteurs donnent, confidentiellement, à chaque destinataire sa clé de décodage : d définie par $ed \equiv 1\ [\varphi(n)]$. Les nombres premiers p et q ainsi que $\varphi(n)$ peuvent alors être « enterrés ».

Remarque : On peut combiner ce système de codage avec un système d'authentification de l'origine du message. Dans ce cas, le réceptionnaire procède comme un concepteur : il construit un nombre n' et donne confidentiellement d' à chaque expéditeur et conserve (non caché) e'.

D. Un exemple de codage R.S.A.

On donne n = 221 et d = 55.

Décoder les deux messages suivants : 80 - 1 - 200 - 198 - 1 - 86 - 86 - 112

16 - 67 - 111 - 200 - 86 - 30 - 112 - 200 - 80

sachant que le nombre trouvé correspond à la place de la lettre dans l'alphabet.

On a choisi pour cet exemple : p = 17, q = 13 , n = 221.

L'indicatrice d'Euler vaut alors : $\varphi(n) = (p-1)(q-1) = 16.12 = 192$.

La clef de codage choisie ici est e = 7 (7 premier avec 192).

Alors il existe un nombre d (clef de décodage) tel que e.d soit premier avec $\varphi(n)$. Ce nombre se trouve par l'algorithme de Bezout de la façon suivante :

(1) $192 = 7 \times 27 + 3$

(2) $7 = 3 \times 2 + 1$

On obtient alors :

(1) $3 = 192 - 7 \times 27$

(2) $1 = 7 - 3 \times 2$

D'où finalement : $1 = 7 - (192 - 7 \times 27) \times 2 = 7 \times 55 - 2 \times 192$ et et on obtient d = 55.

Pour coder la lettre S, par exemple, on lui attribue sa place dans l'alphabet (19) et on calcule : $19^7 \equiv 111\ [221]$.

Pour décoder 111, on calcule : $111^{55} \equiv 19\ [221]$.

---

[11]La clé e sera elle aussi un nombre premier avec n dès que le nombre e ($< \varphi(n)$) est choisi plus petit que Inf{p;q}. Ce qui est le cas puisque p et q sont des nombres qui, en pratique, sont formés d'au moins une centaine de chiffres.

II.3.2. Les théorèmes fondamentaux qui sont à l'œuvre

A. Théorème de FERMAT :

> *Quelque soit l'entier naturel a et l'entier premier p on aura : $a^p \equiv a$ [p].*

Démonstration 1 : si a est un multiple de p, l'égalité est évidente. Plaçons nous dans le cas où p ne divise pas a et on considère les nombres : a ; 2a ; 3a … ; (p-1)a. On pose a_k le reste euclidien de la division de ka par p, on a donc : $ka \equiv a_k$ [p]. Ces nombres a_k ne sont pas nuls sinon, d'après le théorème de Gauss, p ne pouvant diviser k ($k \leq p-1$), diviserait a. D'autre part ces nombres a_k sont tous différents, en effet si $a_k = a_l$ alors $ka \equiv la$ [p] donc $(k-l)a \equiv 0$ [p]. Comme p ne peut diviser (k-l), il diviserait a … Finalement (a_1 ; a_2 ; a_3 ; … ; a_{p-1}) sont p-1 nombres entiers non nuls et strictement inférieurs à p donc, à une permutation près, ce sont les entiers successifs de 1 à p-1 (principe des tiroirs[12]). Comme on a :

$1a \cdot 2a \cdot 3a \cdot \ldots (p-1)a \equiv a_1 \cdot a_2 \cdot a_3 \ldots a_{p-1}$ [p], on en déduit :

$(p-1)!\, a^{p-1} \equiv (p-1)!$ [p] ou encore $a^{p-1} \equiv 1$[p] ou encore $a^p \equiv a$ [p].

Démonstration 2 : C_p^k or p premier et $0 < k < p$ est divisible par k. En effet, $C_p^k = \frac{p(p-1)\ldots(p-k+1)}{k!}$ ou encore : $k!\, C_p^k = p(p-1)\ldots(p-k+1)$ donc p divise $k!\, C_p^k$, or il ne divise aucun des facteurs de k! puisque p est premier supérieur à k donc p divise C_p^k.

Pour tout a et b entiers on a donc : $(a + b)^p \equiv a^p + b^p$ [p] qui se généralise (récurrence immédiate) en $(a_1 + \ldots + a_m)^p \equiv a_1^p + \ldots + a_m^p$ [p] donc en prenant : $(1 + 1 + \ldots$ (a-fois) $\ldots + 1)^p = 1^p + \ldots\ldots + 1^p$ [p] ce qui fait $(a \cdot 1)^p \equiv a \cdot 1^p$ [p] c'est à dire : $a^p \equiv a$ [p].

Démonstration 3 : $\mathbb{Z}/p\mathbb{Z}$ est un corps fini et $\mathbb{Z}^*/p\mathbb{Z}$ en est le sous groupe multiplicatif. Il est donc d'ordre (p-1) comme l'ordre d'un élément est un diviseur de l'ordre du groupe, on a : $a^k \equiv 1$ [p] avec $k \mid p-1$ donc $p-1 = qk$ donc $p = qk + 1$. On a donc : $a^p = (a^k)^q . a^1$, puis en calculant modulo p : $a^p \equiv a^1$ [p] puisque $a^k \equiv 1$ [p].

---

[12] Variante du principe des tiroirs : 10 tiroirs, 10 chaussettes, une par tiroir ; tous les tiroirs sont occupés.

B. Indicatrice d'Euler :

Le nombre de nombres premiers avec n et inférieur à n est $\varphi(n)$ *{le nombre d'inversibles de* $\mathbb{Z}/n\mathbb{Z}$ *est* $\varphi(n)$*}.*

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right) \quad où \quad n = p_1^{a1} p_2^{a2} \ldots p_r^{ar}$$

Démonstration (partielle[13]) :

- Pour n = p premier, on a φ(p) = p-1, puisque tous les entiers non nuls inférieurs à p sont premiers avec p.

- Pour $n = p^r$ où p est premier et r > 0, les multiples de p strictement inférieurs à p^r constituent une suite arithmétique de raison p, de premier terme 0 et terminant à : $p^r - p$. On en déduit, en utilisant l'expression explicite des suites arithmétiques, qu'il y a p^{r-1} termes dans cette suite. Mis à part ces multiples de p, tous les autres entiers ($< p^r$) sont premiers avec p^r. Il y a p^r entiers strictement inférieurs à p^r donc $p^r - p^{r-1}$ nombres premiers avec p^r d'où $\varphi(p) = p^r - p^{r-1}$.

- Pour $n = p^r q^s$ où p et q sont des nombres premiers (r > 0 et s > 0). On compte tous les nombres strictement inférieurs à $p^r q^s$; cet ensemble est une réunion des multiples de p strictement inférieurs à $p^r q^s$ et des multiples de q (strictement...) ; cette réunion n'est pas une partition, l'intersection est formée des multiples de pq. On a :

Card{les multiples de p} = $p^{r-1}q^s$;

Card{les multiples de q} = $p^r q^{s-1}$;

et enfin Card{les multiples de pq}= $p^{r-1}q^{s-1}$.

Donc $\varphi(n) = p^r q^s - (p^{r-1}q^s + p^r q^{s-1} - p^{r-1}q^{s-1}) = (p^r - p^{r-1})(q^s - q^{s-1}) = \varphi(p^r)\,\varphi(q^s)$.

---

[13] La démonstration complète nécessite le théorème : $\mathbb{Z}/ab\mathbb{Z}$ est isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ pour a et b premiers entre eux.

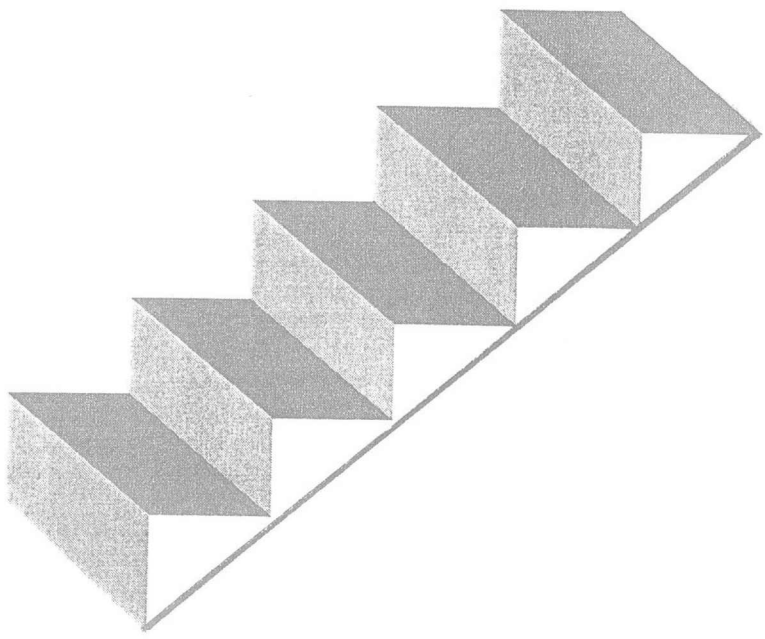
C. Formule d'Euler :

x est un entier strictement positif et n un entier supérieur à 2 avec x et n premiers entre eux alors $x^{\varphi(n)} \equiv 1\ [n]$.

Démonstration : x est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si x et n sont premier entre eux.
Si x et n sont premiers entre eux, d'après le théorème de Bezout, on a : $ax + bn = 1$ donc $ax \equiv 1\ [n]$ donc x a pour inverse a dans $\mathbb{Z}/n\mathbb{Z}$.Si x est inversible dans $\mathbb{Z}/n\mathbb{Z}$ alors il existe a tel que $ax \equiv 1\ [n]$ donc $ax = 1 + kn$; on a donc une égalité de Bezout : $ax - kn = 1$ ce qui prouve que a et x sont premiers entre eux.

L'ensemble des inversibles U[n] de $\mathbb{Z}/n\mathbb{Z}$ constitue un groupe (multiplicatif) d'ordre $\varphi(n)$ puisque $\varphi(n)$ est le cardinal l'ensemble des nombres qui sont premiers avec n. Or l'ordre d'un groupe fini vérifie pour chacun de ses éléments x, $x^{\varphi(n)} \equiv 1\ [n]$.

III. Une méthode éprouvée : la descente infinie



III.1. Introduction

Objectif *: Montrer que certaines équations n'ont pas de solutions en nombres entiers strictement positifs.*

Principe *: On suppose que l'équation admet une telle solution, on montre alors qu'il en existe une autre strictement inférieure et positive.*

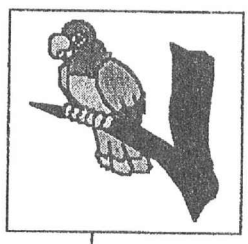
Comme il n'existe qu'un nombre fini de nombres entiers entre 0 et la solution initiale, il est alors impossible qu'une solution initiale existe.

Un bien joli nom que ce type de raisonnement mis au point par Fermat : si on veut prouver qu'un problème n'a pas de solutions en nombres entiers, on montre que, s'il en admettait une, il en aurait une autre avec des nombres plus petits, avait écrit Grosrouvre.

« D'accord, mais pourquoi est-ce une preuve ? se demanda M. Ruche. Pardi, parce qu'il n'y a qu'un nombre fini d'entiers inférieurs à un entier donné. C'est-à-dire, justement parce que la descente n'est pas infinie ! »

Soit un escalier qui démarre au rez-de-chaussée, si chaque fois que l'on se trouve sur une marche on est obligé de redescendre sur la marche précédente, il arrive un moment - le moment où l'on atteint le rez-de-chaussée - où l'on ne peut descendre plus bas. Or notre hypothèse nous contraint de descendre toujours plus bas.

Contradiction ! L'hypothèse est donc fausse. Donc aucun nombre ne possède la propriété en question. CQFD. M. Ruche apprécia ce mélange subtil de raisonnement par l'absurde et de raisonnement par récurrence à rebrousse-poil.



Denis Guedj, "Le théorème du perroquet", *Roman Seuil,* 1998 - chapitre 19, page 378 avec l'aimable autorisation de l'auteur.

Nous allons présenter deux exemples[14] *de descente infinie : le premier permet de montrer que le problème n'a pas de solution ; le second permet d'exhiber les solutions d'une équation diophantienne.*

---

[14] Qui ont aussi été développés par Hervé Lehning dans la revue Tangente, Secrets de nombre, [Lehning, 1998].

III.2. $\sqrt{2}$ n'est pas rationnel.

Si c'était le cas, il existerait un point M_0 à coordonnées entières et strictement positives $(x_0 ; y_0)$ de la droite Δ d'équation $y = \sqrt{2}\, x$.

Supposons qu'un tel point existe. Si on montre qu'alors il existe un point $M_1 (x_1 ; y_1) \in \Delta$ tel que

$0 < x_1 < x_0$

$0 < y_1 < y_0$

où x_1 et y_1 sont aussi entiers.

Conclusion : impossible de poursuivre ainsi à l'infini et donc le point initial M_0 n'existe pas.

Montrer que le point M_1 existe revient à trouver une transformation du plan :

$$f : M (x ; y) \rightarrow M' (x' ; y') \text{ « satisfaisante ».}$$

C'est à dire en recherchant la transformation f sous la forme :

$x' = a\, x + b\, y$

$y' = c\, x + d\, y$

- a) On veut x et y entiers alors x' et y' entiers :
  pour que ceci soit vrai pour tout entier, il faut donc que :

  a, b, c, d soit entiers

- b) On veut : $0 < x' < x$

  $0 < y' < y$

  Puisque x et y sont strictement positifs, si a et b ont le même signe ainsi que c et d on n'aura jamais $x' < x$ et $y' < y$ donc

  a et b doivent avoir des signes différents ainsi que c et d.

- c) On veut que $y - \sqrt{2}\, x = 0 \Leftrightarrow y' - \sqrt{2}\, x' = 0$

  or $y' - \sqrt{2}\, x' = (c\, x + d\, y) - \sqrt{2}\, (a\, x + b\, y) = dy - ax\sqrt{2} + cx - by\sqrt{2}$

  Un moyen simple d'obtenir l'équivalence est de poser :

  a = d et c = 2b.

Puisque alors on aura : $y' - \sqrt{2}\, x' = a\, (y - \sqrt{2}\, x) + b\sqrt{2}\, (\sqrt{2}\, x - y) = (y - \sqrt{2}\, x)\, (a - b\sqrt{2})$

- d) La condition du b) implique aussi : $0 < OM' < OM$,

soit : $0 < x'^2 + y'^2 < x^2 + y^2$

soit en tenant compte du résultat du c) : $0 < (ax + by)^2 + (2bx + ay)^2 < x^2 + y^2$

$0 < a^2 (x^2 + y^2) + b^2 (4x^2 + y^2) + 6\,abxy < x^2 + y^2$

or $y^2 = 2x^2$ et $y'^2 = 2x'^2$: $0 < 3\,a^2 x^2 + 6\,b^2 x^2 + 6\sqrt{2}\,abx^2 < 3\,x^2$

$0 < 3\,x^2 (a + \sqrt{2}\,b)^2 < 3\,x^2$

$0 < (a + \sqrt{2}\,b)^2 < 1$

a et b entiers, non nuls tous deux, de signe opposés vérifient $-1 < (a + \sqrt{2}\,b) < 1$
Différents couples peuvent convenir : a = 2 et b = -1 par exemple.

Vérification.

On peut observer sans problème que toutes les conditions sont remplies en prenant pour la transformation f :

$x' = 2x - y$
$y' = -2x + 2y$

- si x, y entiers on a bien x' et y' entiers
- Si x et y sont les coordonnées d'un point de Δ, x' et y' sont aussi les coordonnées d'un point de Δ puisque si $y - \sqrt{2}\,x = 0$ comme $y' - \sqrt{2}\,x' = (y - \sqrt{2}x)(2 + \sqrt{2})$, alors $y' - \sqrt{2}\,x' = 0$
- si x et y sont les coordonnées d'un point de Δ, x' et y' sont aussi les coordonnées strictement inférieures d'un point de Δ.

$y = \sqrt{2}\,x$, $\quad x' = 2x - y = 2x - \sqrt{2}\,x = x(2 - \sqrt{2})$

$y' = -2x + 2y = -\sqrt{2}\,y + 2y = y(2 - \sqrt{2})$

et puisque $0 < 2 - \sqrt{2} < 1$, on a bien $0 < x' < x$ et $0 < y' < y$

On aurait pu prendre aussi a = 3 et b = -2.

En conclusion, si la démonstration classique de « $\sqrt{2}$ n'est pas rationnel », qui fait intervenir la parité, est peut être plus rapide, celle-ci présente l'avantage d'une recherche de transformation qui convient, et d'un lien avec les graphiques.

III.3. Equation de Pell $y^2 - 2x^2 = 1$

Forme générale $(y^2 - dx^2 = b)$

C'est un type particulier d'équation de Diophante, on en recherche les solutions entières.

Résoudre $y^2 - 2x^2 = 1$ en nombres entiers, revient à rechercher les points à coordonnées entières de la partie d'hyperbole H définie par :

$y^2 - 2x^2 = 1$

$x \geq 0$ et $y \geq 0$

Si dans l'exemple précédent, on prend a = 3 et b = -2,

on aura f : $x' = 3x - 2y$

$y' = -4x + 3y$

et $y' - \sqrt{2}\, x' = (y - \sqrt{2}x)(3 + 2\sqrt{2})$.

On peut aussi obtenir : $y' + \sqrt{2}\, x' = (-4x + 3y) + \sqrt{2}(3x - 2y) = (y + \sqrt{2}x)(3 - 2\sqrt{2})$

Ainsi par produit : $y'^2 - 2x'^2 = y^2 - 2x^2$ puisque $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$;

Ainsi par f, l'image d'un point M de H à coordonnées entières est un point M' de H à coordonnées entières.

Si l'on veut que ce point M' soit à coordonnées inférieures strictement :

- c'est à dire : $0 \leq x' < x$ soit $\quad 0 \leq 3x - 2y < x,$

  ce qui équivaut à $\quad \frac{2}{3} y \leq x < y,$

  équivalent à (puisque nombres positifs) $\quad \frac{4}{9} y^2 \leq x^2 < y^2,$

  comme $y^2 = 2x^2 + 1$ $\quad \frac{4}{9}(2x^2 + 1) \leq x^2 < 2x^2 + 1,$

  soit $\quad 4 \leq x^2$ ainsi on doit avoir $x \geq 2$;

- et $0 \leq y' < y$ $\quad 0 \leq -4x + 3y < 5x$

  $4x \leq 3y < x$

  $16\, x^2 \leq 9y^2 < 25x^2$

  $16\, x^2 \leq 9(2x^2 + 1) < 25x^2$

  $0 \leq 2x^2 + 9 < 9x^2$

  $9 < 7\, x^2$ vrai si $x \geq 2$

Par f, M'(x',y') $\in$ H avec des coordonnées inférieures, si M(x,y) $\in$ H dès que $x \geq 2$

Ce qui va donner, en appliquant la méthode de descente infinie une possibilité de solution.

Considérons un point initial M_0 de H de coordonnées $(x_0 ; y_0)$ entières avec $x_0 \geq 2$.

Il n'est pas possible de construire par f, à partir de ce point, une suite infinie de points M_i qui vérifient les mêmes conditions puisque l'on devrait avoir une suite infinie (x_i) telle que :

$$2 \leq .... < x_n < x_{n-1} < ... < x_0$$

Donc, il existe n tel que $x_n < 2$, ce qui arrête la construction de la suite :

$$x_n < 2 \leq x_{n-1} < ... < x_0.$$

Mais le point M_n de H a malgré tout des coordonnées entières.

Nous n'avons donc que 2 cas à observer :

$x_n = 1 \quad \Rightarrow \quad y^2 = 3$ pas possible, y non entier

$x_n = 0 \quad \Rightarrow \quad y^2 = 1$ donc $y = 1$

Ainsi x_{n-1}, y_{n-1} sont solutions du système :

$$3x - 2y = 0$$
$$-4x + 3y = 1$$

Ce qui entraîne $x_{n-1} = 2$ et $y_{n-1} = 3$

Pour trouver de façon générale les coordonnées du point M_{n-1} à partir de celles de M_n il faut résoudre le système :

$$3x_{n-1} - 2y_{n-1} = x_n$$
$$-4x_{n-1} + 3y_{n-1} = y_n$$

ce qui donne $x_{n-1} = 3\,x_n + 2\,y_n$

et $y_{n-1} = 4\,x_n + 3\,y_n$

On peut ainsi conclure en disant que les couples d'entiers positifs solutions de $y^2 - 2\,x^2 = 1$ sont les couples $(x_n ; y_n)$ définis par les suites[15] :

$$\mathbf{x_{n+1} = 3\,x_n + 2\,y_n}$$

et $\mathbf{y_{n+1} = 4\,x_n + 3\,y_n}$ **avec** $\mathbf{(x_0 ; y_0) = (0 ; 1)}$

---

[15] Un autre exemple de « remontée » semblable d'une descente infinie est proposé dans le chapitre IV.6 : Equations entières et courbes algébriques.

III.4. Les équations diophantiennes dans les manuels de TS

La plupart des manuels de TS[16] proposent des résolutions d'équations diophantiennes, ce qui nous a conduit à nous intéresser de plus près à ce type d'équations.

Diophante, mathématicien des années 250 de notre ère, fut le premier à s'intéresser à la recherche de solutions en nombres entiers ou rationnels d'équations polynomiales à coefficients entiers et Fermat (1601-1665) a apporté une contribution importante à la résolution de ce type de problèmes. Cependant lorsque l'on tente de faire une présentation synthétique de ces problèmes, on se heurte au fait que, comme il n'existe pas d'algorithme universel permettant de décider si une équation diophantienne a une solution en nombres entiers [J. Robinson, Yu. V ; Matijasevic, 1970], les ouvrages consacrés aux équations diophantiennes n'apparaissent que comme une accumulation de résultats disparates.

Malgré cela, nous essayerons ici de classifier certains problèmes proposés aux élèves.

Equations linéaires à 2 inconnues : ax + by = c avec a, b, c entiers.

Tous les manuels traitent cette équation de façon systématique, mais tous ne donnent pas l'interprétation en termes de points à coordonnées entières d'une droite qui cependant est une des méthodes utilisées pour résoudre des équations de degré supérieur.

Les équations du second degré.

- L'équation de Pythagore : $x^2 + y^2 = z^2$.

La méthode de résolution faisant intervenir les points à coordonnées rationnelles du cercle unité[17] est exposée dans certains manuels. Cette méthode permet en particulier de conclure que l'équation $x^2 + y^2 = 3\,z^2$ n'a pas de solutions entières.

---

[16] Sur le tableau récapitulatif des manuels, p 17-18, on peut observer l'importance qui leur est plus spécialement accordée dans le Déclic et le Terracher. Dans les exemples de sujet de bac blanc proposés p 19-20, elles interviennent aussi fréquemment.

[17] On pourra se reporter ici au chapitre V.2 : « nombres pythagoriques » où 3 méthodes sont exposées.

- Les équations de Pell : $y^2 - d x^2 = b$.

Problème traité pour $y^2 - 2 x^2 = 1$ par la méthode de descente infinie et utilisation des points à coordonnées entières de l'hyperbole $y^2 - 2 x^2 = 1$ (voir les pages précédentes, équation de Pell).

Dans les manuels, ce type d'équations est traitée, en général, lorsque $d = 1$ par la factorisation de $y^2 - x^2$ et pour des valeurs particulières de b. On peut aussi rencontrer des équations du type $x^2 - 2 y^2 = 3$ dont on montre qu'elle n'a pas de solution en vérifiant en particulier que x^2, nécessairement impair, est congru à 1 modulo 8.

Les équations de degré supérieur.

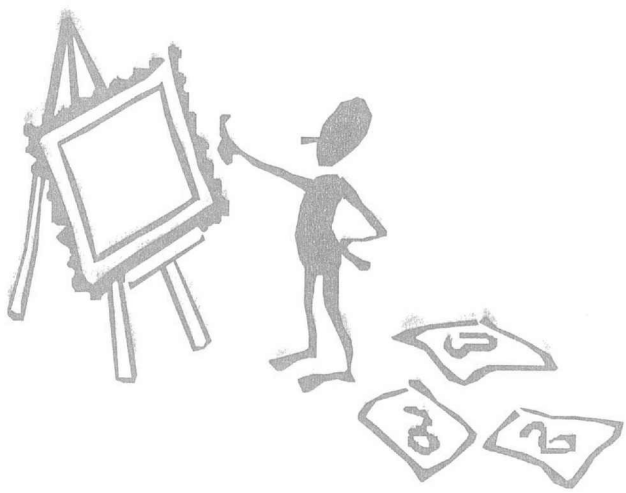
- Les équations de Mordell : $x^2 + n = y^3$.

Ces équations ont un nombre fini de solutions (Théorème de Mordell-Weil, 1928). Plusieurs pistes de résolutions sont proposées dans " Arithmétique : le retour "[18] pour l'équation $x^2 + 2 = y^3$.

Dans les manuels, on peut trouver : démontrer que l'équation $x^2 + 3 = y^3$ n'a pas de solution en discutant sur la parité de x et de y et les restes dans la division par 8.

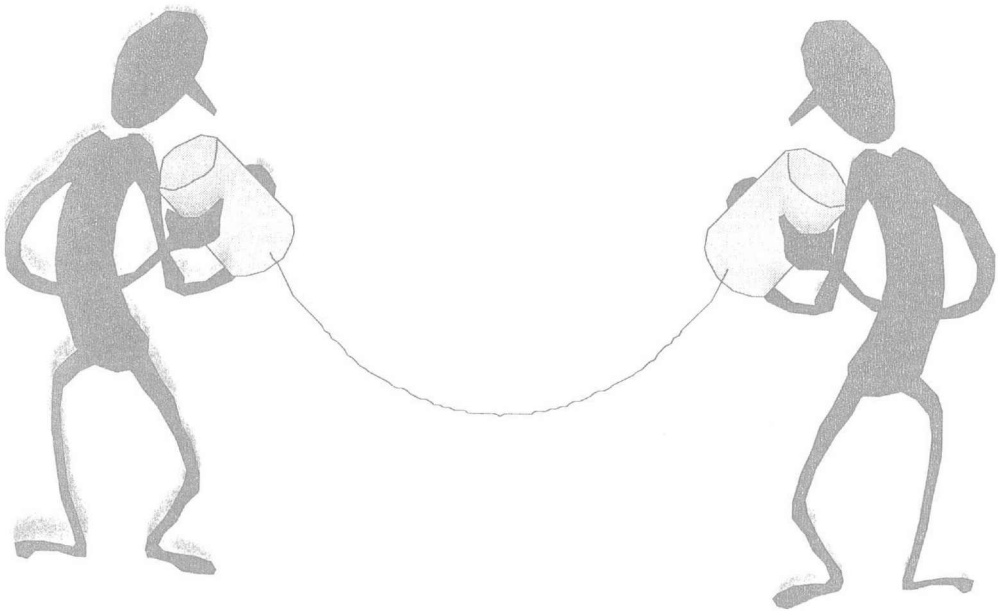
- D'autres équations, comme par exemple : $x^3 - y^3 = a$.

Ce type d'équation proposé dans les manuels se résout par la factorisation de : $x^3 - y^3$ et en utilisant la décomposition en facteur premier de a (un exemple de telle équation est proposé par le sujet du bac blanc du lycée Joffre p. 19).



[18] [Bernard et Ali, 1995].

IV. Du continu au discret... et réciproquement



IV.1. Dynamique du continu et du discret.

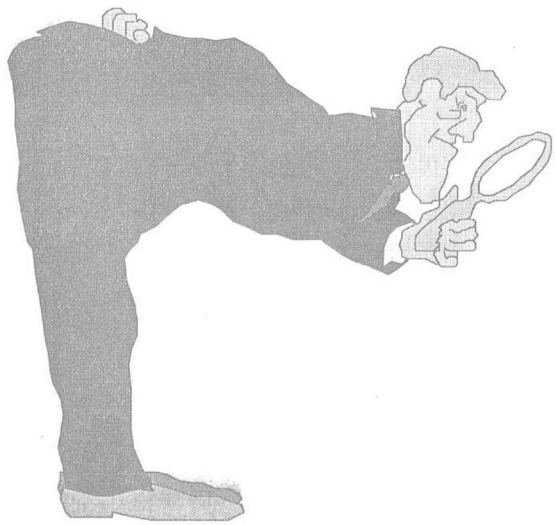
La réintroduction de l'arithmétique, dans un cours de mathématiques où domine l'analyse, est l'occasion de repenser les rapports entre continu et discret, dans leur irréductible opposition et leur nécessaire complémentarité. Après un petit détour théorique, nous examinerons plusieurs domaines où cette complémentarité est particulièrement féconde.

On trouve dans l'Encyclopaedia Universalis[19], à la rubrique " Discret et continu ", une description par Jean-Michel Salanskis de leur opposition :

" (Elle) se retrouve dans une certaine mesure dans celle de l'analyse et de l'algèbre. La définition rigoureuse de ces deux branches traditionnelles de la mathématique est sans doute impossible ; on peut cependant dire que l'algèbre fut d'abord la théorie de la résolution des équations. Dans une large mesure, et pendant longtemps, l'algèbre est d'ailleurs restée dominée par le signe =, on y traitait de relations d'égalité, soit en les affirmant, soit en les transformant, soit en les prouvant, soit en les érigeant en problèmes. Est associée à ce symbole = une question dont la réponse est oui ou non, un test binaire : de la sorte, les possibilités et les structures commandées par le = prennent une tournure discrète, donnant lieu à des arbres de classification ou des arbres algorithmiques, des tableaux consignant les résultats ou régulant la méthode. Il n'est donc pas surprenant que la discipline algébrique traitant des nombres entiers (lesquels "exemplifient" canoniquement le discret comme on l'a vu), c'est-à-dire l'arithmétique, ait servi de modèle pour le projet hilbertien d'une *grammaticalisation* des mathématiques, plus ou moins réussie aujourd'hui. L'idée de ramener les mathématiques à l'exercice d'un jeu discret selon certaines règles, le projet axiomatique disposaient d'un environnement favorable avec l'algèbre ; on notera à ce sujet que la structure de *groupe*, première grande structure axiomatique de la mathématique moderne, est sortie de la réflexion de Galois sur la théorie des équations. Rappelons pour finir que le vocable arabe dont dérive le mot "algèbre" contient déjà les sèmes de "réduction" et de "séparation" (en vue d'une forme stricte), annonçant par là même tout ce que nous venons de dire.

Le mot *analyse*, de son côté, signifie en langue naturelle décomposition du global, mouvement vers le détail : le regard analysant "resserre" sa visée, s'intéresse à la complexité de ce qui se passe dans un lieu réduit (il peut y avoir une infinie richesse dans cette exiguïté).

En mathématiques classiques, cette considération du local donne la prédominance au signe de l'inégalité : cette dernière possède en général un degré, se module, renvoie à une échelle de variations, qui sera continue dans le cas d'un substrat continu. On voit comment la figure topologique et quantitative du continu s'associe naturellement à cette étude du local en tant qu'intense. L'analyse fut d'ailleurs d'abord l'étude des fonctions de la variable réelle, elle se situait donc tout entière et d'emblée dans le cadre du continu. Les méthodes de l'analyse ont conservé pendant la même période un rapport avec le mystère géométrique du premier continu qui se soit historiquement dévoilé, celui de l'espace réputé "sensible". "



L'article se poursuit par l'évocation de ce que Jean-Michel Salanskis appelle le " jeu scientifique sur le discret et le continu, à propos par exemple de la théorie des probabilités :

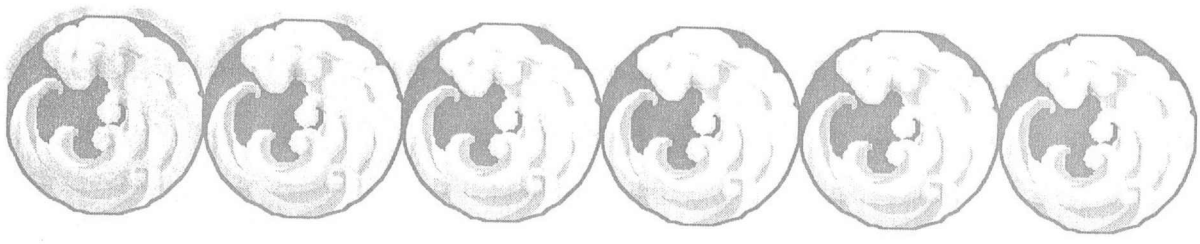
" (...) cette dernière mérite une évocation particulière, parce que le passage du discret au continu est un moment essentiel de cette théorie dans son aspect mathématique pur, et parce que les applications de la théorie sont en rapport avec la charge "ontologique" de l'opposition du continu et du discret. Le calcul mis au point par Pascal portait sur des "univers d'éventualités" *finis* , les applications probabilités définies sur ces ensembles ayant la propriété dite d'*additivité* en langage actuel : celle-ci énonce que des événements logiquement décomposables en sous-événements deux à deux incompatibles ont une probabilité égale à la somme de celle de leurs composants. Ce calcul convient pour les processus aléatoires dont les issues peuvent être isolées les unes des autres, et donner matière à la définition d'un ensemble fini d'"atomes du hasard" ou "événements élémentaires" : c'est un calcul qui se situe résolument dans le discret. La généralisation de cette théorie permet de traiter des processus dont les issues ne sont pas séparables, collent les unes aux autres, ce qui est par exemple le cas lorsqu'elles se distribuent dans un continuum. La théorie mathématique de la mesure, qu'on fait intervenir ici, ne tient plus

---

[19]

pour significative la probabilité de voir sortir un cas parfaitement individué (une telle probabilité est en fait toujours nulle dans le cas continu), mais la probabilité pour que le cas sortant appartienne à une "région" de l'ensemble des cas possibles (on remarque la dimension topologique de cette notion). Au lieu de la propriété d'additivité, la propriété de s-*additivité* exprime la possibilité d'un passage à la limite dans le calcul de la probabilité d'une réunion dénombrable d'événements deux à deux disjoints. L'ouverture sur le continu et le topologique suscite les problèmes de "convergence", comme il est naturel. Or cette théorie des probabilités "générale" s'applique de deux manières : ou bien (en physique essentiellement) à des situations "par elles-mêmes" continues (à des phénomènes naturellement repérés par des grandeurs continues, en raison de la nature des formes a priori dirait Kant), ou bien à des situations discrètes, mais où l'ensemble des cas possibles est "très abondant", si bien que les calculs discrets peuvent être correctement approximés au moyen de formules "continues", de calcul différentiel ou intégral, éventuellement plus simples; dans ce dernier cas, il y a donc renversement du dispositif kantien, le discret est du côté du "donné", du matériel statistique par exemple, et le continu du côté de l'"idéalisation scientifique", il appartient à un univers brodé par le discours rationnel à partir de ce donné, la corrélation entre les deux étant de l'ordre de la convergence, associée à l'idée chez Kant. "

C'est ce jeu scientifique entre discret et continu que nous voudrions exposer maintenant, à propos de différents domaines. Nous ne prétendons pas ici faire une étude exhaustive, mais évoquer simplement quelques problèmes intéressants, qui peuvent sans doute donner matière à des activités mathématiques, à différents niveaux du lycée.



IV.2. Suites et fonctions

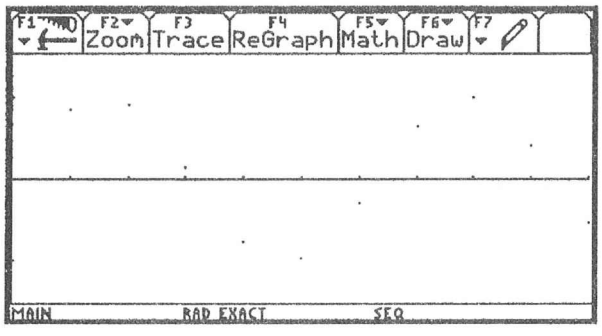
> *C'est bien sûr un domaine des mathématiques où l'aller-retour entre discret et continu est permanent. Il suffit de considérer les rapports entre tableaux de valeurs d'une fonction et représentations graphiques de celle-ci pour réaliser que la distinction discret/continu n'est pas aussi simple qu'on voudrait l'imaginer. Connaître les valeurs que prend une fonction suppose bien une évaluation ponctuelle, récupérer "la totalité" de la courbe suppose un prolongement implicite par continuité. C'est bien d'un aller-retour entre la fonction $x \to f(x)$ et la suite $n \to f(n)$ qu'il s'agit.*

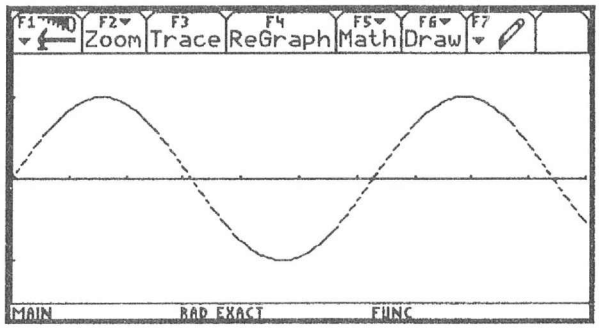
Premier problème que nous envisageons habituellement en classe : quel est le rapport entre les propriétés de la fonction et celles de la suite ? On résume souvent celui-ci en disant que les propriétés de la fonction se prolongent à celle de la suite, du moins en ce qui concerne les variations et les limites en $+\infty$, sans qu'il n'y ait bien sûr de réciproque. Les choses sont cependant à considérer de près :

- si une fonction f est décroissante sur $[0, \pi]$ et croissante sur $[\pi, +\infty[$, peut-on en déduire que la suite (f(n)) est croissante à partir de 4 ? Ou a partir de 3 ?
- si une fonction f est périodique (par exemple la fonction $x \to \sin x$), peut-on en déduire que la suite (f(n)) est périodique ?

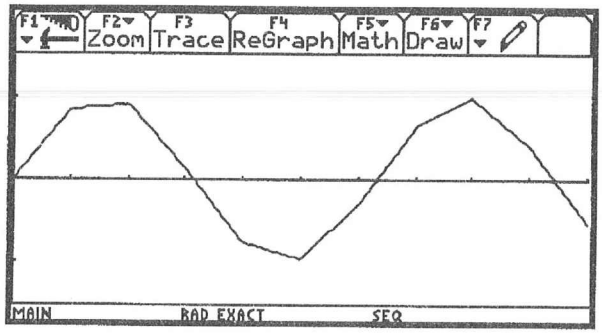
Le transfert des propriétés d'un objet à l'autre n'est pas si automatique que cela !

Deuxième problème, moins souvent envisagé en classe, celui posé par le recours aux outils de calcul. Ceux-ci opèrent nécessairement une discrétisation des tracés. Un phénomène continu est ainsi représenté, via la transposition pour l'écran, par un ensemble fini de pixels. Comparons ainsi les représentations graphiques de la suite sin(n) et de la fonction sin(x), sur des intervalles différents, avec les deux modes de tracés possibles (le tracé des points successifs isolés ou le tracé des points successifs reliés).

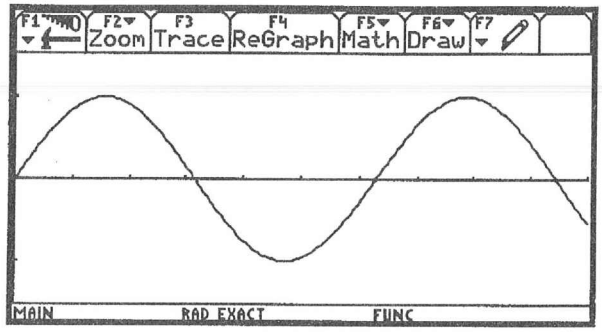




Suite, tracé point par point



Fonction, tracé point par point



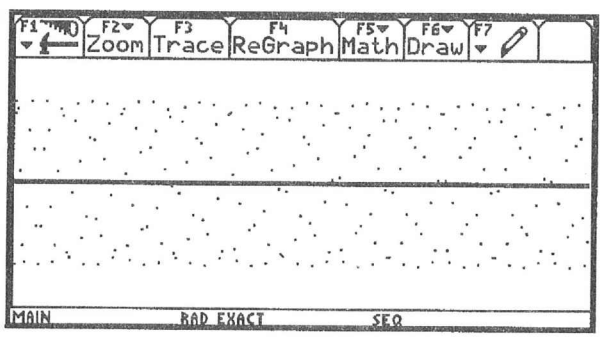
Suite, points successifs reliés

Fonction, points successifs reliés

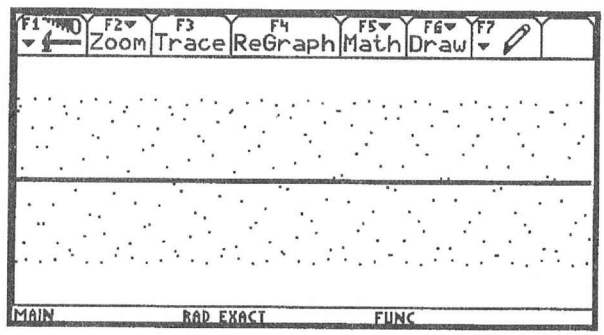
À gauche la suite n→f(n), à droite la fonction x→f(x), sur l'intervalle [0 ; 10]

Sur l'intervalle [0 ; 10] (ci-dessus) rien de mystérieux : la représentation graphique de la suite se compose de 11 points. Si ceux-ci sont reliés, on obtient une ligne brisée. A droite, la représentation graphique de la fonction se compose de 238 points (il s'agit d'une calculatrice TI-92, dont l'écran comporte 238 colonnes de pixels). Les oscillations de la fonction étant très raisonnables, il n'y a pas grande différence entre le tracé " points isolés " et le trace " points reliés ".

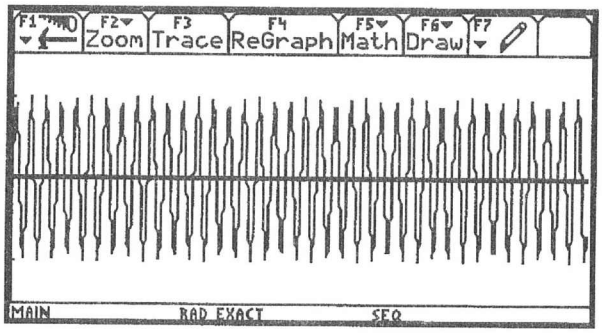
Sur l'intervalle [0 ; 238] (ci-dessous), il y a identité parfaite entre les représentations graphiques de la suite et les représentations graphiques de la fonction. En effet, il y a pour la suite autant de point de calcul que ce que l'écran comporte de colonnes de pixels. Donc il y aura, pour la suite comme pour la fonction, un point par colonne de pixels.



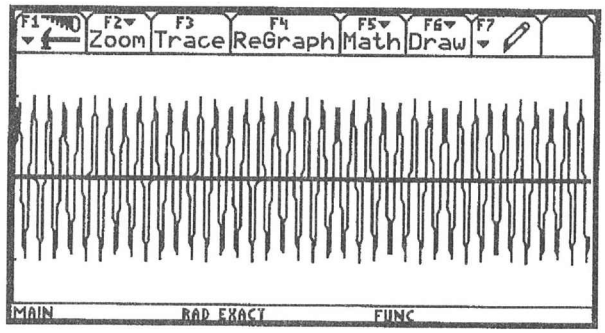
Suite, tracé point par point



Fonction, tracé point par point



Suite, points successifs reliés



Fonction, points successifs reliés

À gauche la suite n→f(n), à droite la fonction x→f(x), sur l'intervalle [0 ; 238]

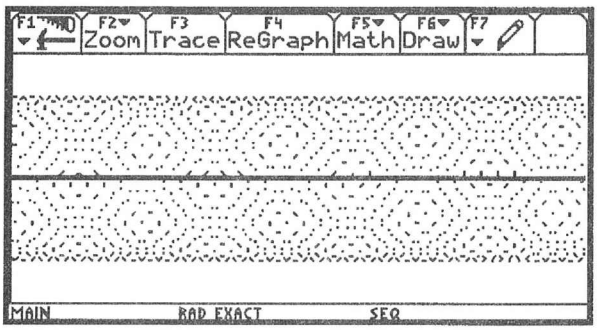
Les surprises arrivent avec l'intervalle [0 ; 1490]. En effet, de façon tout à fait surprenante :

- la représentation graphique de la suite comporte plus de point que la représentation graphique de la fonction sur le même intervalle ;

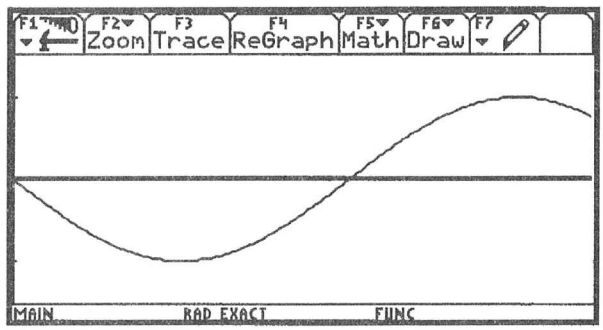
- la représentation graphique de la fonction est étonnamment sage…

Chacun de ces phénomènes s'explique (relativement) aisément. Pour la fonction, la calculatrice trace invariablement un point par colonne de pixels (comment faire sinon, puisqu'un réel n'a pas de successeur !) ; ainsi, sur l'intervalle [0 ; 1490], la représentation graphique de la fonction comporte exactement 238 points. Par contre, pour la suite, la calculatrice va placer 1491 points (puisque chaque naturel a un successeur, le choix de ces points est automatique). Il y a donc environ 6 points par colonne de pixels. Le phénomène discret est représenté par plus de points que le phénomène continu… Ce qui fait que, quand on relie les points qui représentent la suite, on ne voit plus grand chose…

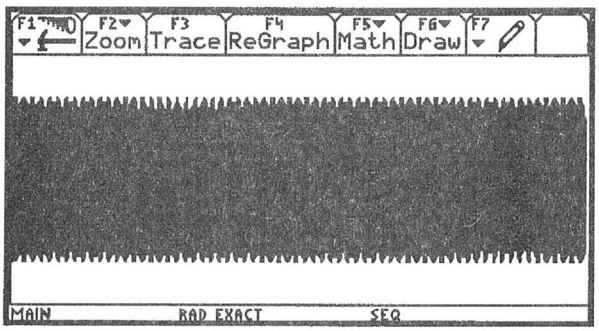
- l'intervalle [0 ; 1490] n'est pas pris au hasard… Comme le lecteur attentif l'aura constaté, 1490 n'est pas très loin de 238 fois (2π). Ainsi, il y a entre deux points de calcul de la fonction presque sa période, ce qui explique qu'il n'y ait qu'un petit décalage dans l'ordonnée et un tracé très raisonnable faisant apparaître une pseudo-période différente de la période attendue pour la fonction sinus !



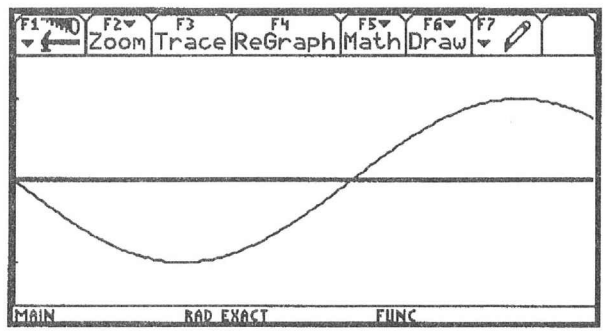
Suite, tracé point par point



Fonction, tracé point par point



Suite, points successifs reliés



Fonction, points successifs reliés

À gauche la suite n→f(n), à droite la fonction x→f(x), sur l'intervalle [0 ; 1490]

On le voit, l'étude des représentations graphiques des phénomènes discrets et continus sur un écran de calculatrice nécessite quelque réflexion…[20]

---

[20] Sur ce point, on pourra consulter avec profit *Pour une prise en compte des calculatrices symboliques en lycée* [Bernard et alii, 1998].

IV.3. Suites récurrentes / équations différentielles[21]

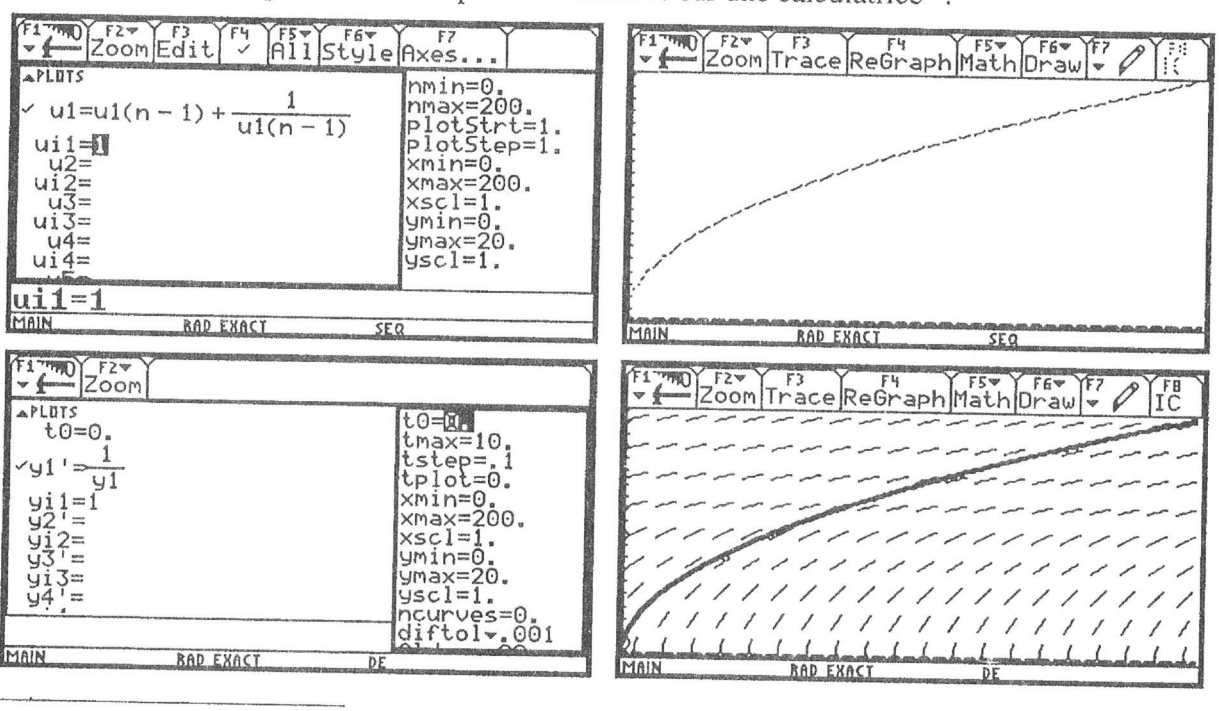
Nous nous proposons ici, toujours dans le cadre de la confrontation suites/fonctions, de comparer les solutions d'équations proches qui leur donnent naissance : récurrences pour les suites, équations différentielles pour les fonctions. Nous traiterons deux exemples.

IV.3.1. Un processus à divergence lente.

Suite récurrente : $u_{n+1} - u_n = \frac{1}{u_n}$ $u_0 = 1$. Équation différentielle : $y' = \frac{1}{y}$ $y(0) = 1$

Le caractère de proximité des deux phénomènes est assez clair : dans les deux cas, la " dérivée " est égale à l'inverse de la fonction. Que la suite diverge vers $+\infty$ est immédiat : par une récurrence simple, tous les termes sont strictement positifs, dont la suite est strictement croissante ; comme la fonction qui définit la suite $x \to x + \frac{1}{x}$ n'a pas de point fixe, la suite ne peut que diverger vers $+\infty$. Cela implique bien sûr que l'inverse de la suite tend vers 0, donc que l'écart entre deux termes consécutifs tend vers 0, ce qui caractérise bien une divergence lente.

Ce caractère de proximité formelle a-t-il des conséquences pour la suite et la fonction correspondants à ces équations ? Ceci peut être observé sur une calculatrice[22].



---

21 On pourra trouver cette étude adaptée pour des élèves de terminale dans la brochure *Des fonctions et des graphes* [Bernard et alii, 1995].

22 On utilisera ici une calculatrice TI-92+ qui possède un module de résolution numérique des équations différentielles.

Sur les mêmes intervalles, on peut considérer ci-dessus d'abord la suite, puis la fonction solution dont une représentation est tracée parmi le champ de tangentes. La proximité des deux phénomènes est assez troublante...

Ceci peut se vérifier par un calcul d'équivalent.

- Pour la fonction, c'est assez simple. De y.y'=1, on tire $\frac{1}{2}y^2 = x + c$, d'où, par utilisation de la condition initiale y(0)=0, $y = \sqrt{2x+1}$. On vérifie bien ainsi la résolution numérique proposée par la calculatrice ci-dessus. Un équivalent pour cette fonction, en $+\infty$, est $y \approx \sqrt{2x}$.

- Pour la suite, la méthode de recherche d'équivalent est classique. On recherche d'abord un exposant a tel que $u_{n+1}^a - u_n^a$ converge vers une limite non nulle. On obtient : $u_{n+1}^a - u_n^a = (u_n + \frac{1}{u_n^2})^a = u_n^a(1 + \frac{1}{u_n^2})^a - u_n^a$, puis par un développement limité (légitime puisque $\frac{1}{u_n}$ tend vers 0) :

$$u_n^n(1 + \frac{1}{u_n^2})^a - u_n^a = u_n^a(1 + \frac{a}{u_n^2} + o(\frac{1}{u_n^2})) - u_n^a = a.u_n^{a-2} + o(u_n^{a-2})$$

La différence $u_{n+1}^a - u_n^a$ converge vers une limite non nulle si et seulement si a = 2. Cette différence converge alors vers 2. On applique alors le lemme de Césaro : si la suite (w_n) converge vers λ, alors la suite $(\frac{1}{n}\sum_{k=1}^{n} w_n)$ converge aussi vers λ (cette propriété s'interprète géométriquement : si une suite converge vers λ, la moyenne arithmétique de ses premiers termes converge aussi vers λ). En appliquant ce lemme à la suite des différences $(u_{n+1}^2 - u_n^2)$ qui converge vers 2, on obtient que la suite $\frac{1}{n}\sum_{k=1}^{n} u_{k+1}^2 - u_k^2 = \frac{1}{n}(u_{n+1}^2 - u_0^2)$ converge vers 2. Cela implique naturellement que $\frac{1}{n}u_{n+1}^2$ converge vers 2, soit $u_n^2 \approx 2n$ c'est-à-dire $u_n \approx \sqrt{2n}$. On retrouve le même résultat asymptotique que pour la fonction.

Ce résultat se comprend à partir de la faible croissance des phénomènes. Ainsi le rapport $\frac{f(n+1)-f(n)}{n+1-n} = u_{n+1} - u_n$ est-il peu différent de f'(n). **Cette proximité du discret et du continu ne subsiste bien sûr pas s'il y a une croissance importante du phénomène observé entre deux points de mesures n et (n+1) successifs.**

IV.3.2. Un processus à divergence rapide

Suite récurrente : $u_{n+1} - u_n = u_n^2 \quad u_0 = 1$. Équation différentielle : $y' = y^2 \quad y(0) = 1$

Le caractère de proximité formelle des deux phénomènes est le même que dans le cas précédent. On démontrerait de même que la suite diverge vers $+\infty$. Mais, à la différence de l'exemple que nous venons de traiter, la différence entre deux termes consécutifs tend vers $+\infty$. Observons la résolution numérique des deux équations à l'aide d'une calculatrice (voir ci-dessous). On peut vérifier que les deux phénomènes (observés sur les mêmes intervalles) n'ont pas le même comportement :

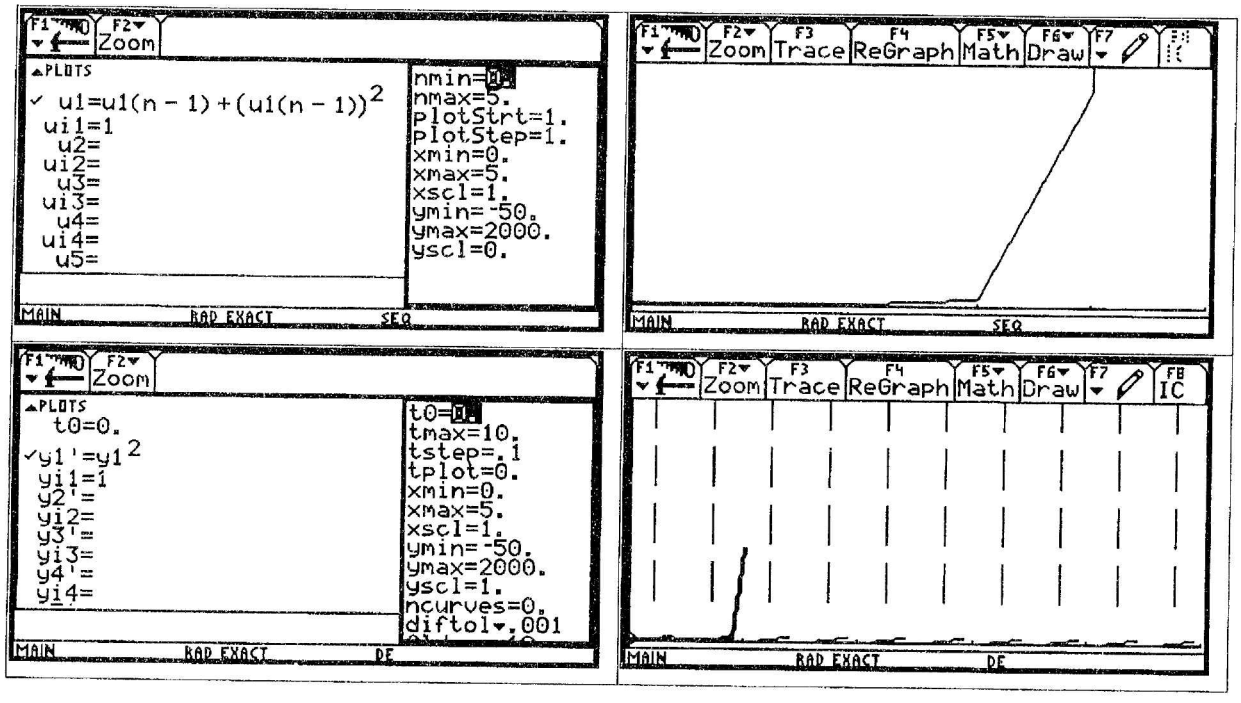
- la suite a une divergence très rapide ;

- la fonction aussi, mais semble accuser une cassure très rapide, aux environs de 1.

Étudions théoriquement ces phénomènes.

Pour la fonction, c'est assez simple. Sur tout intervalle [0 ; A] où elle est définie elle est nécessairement strictement positive (signe de la dérivée). Nous pouvons ainsi écrire :

$\frac{y'}{y^2} = 1$, d'où $-\frac{1}{y} = x + c$ et, par utilisation de la valeur en 0, $y = -\frac{1}{x-1}$. Il y a bien cassure pour x=1. Le phénomène continu qui débute en 0 suit une croissance impétueuse avant 1 et se déchire en 1.



Pour la suite, c'est un peu plus complexe. Le lemme de Césaro ne donne pas les mêmes résultats, du fait de la croissance impétueuse. On " écrase " alors la suite en posant : $v_n = \frac{1}{2^n}\ln(u_n)$. Il est clair que cette nouvelle suite est croissante, en effet :

$$v_{n+1} - v_n = \frac{1}{2^{n+1}}(\ln(u_{n+1}) - 2.\ln(u_n)) = \frac{1}{2^{n+1}}(\ln(u_n + u_n^2) - \ln(u_n)) = \frac{1}{2^{n+1}}(\ln(1 + \frac{1}{u_n}) > 0 .$$

Ce résultat nous permet aussi de majorer cette différence, puisque $\frac{1}{u_n} < 1$.

Ainsi : $0 < v_{n+1} - v_n < \frac{1}{2^{n+1}} \ln 2$. Par addition de ces inégalités du rang 1 à n, il reste :

$0 < v_n - 1 < \ln 2(\frac{1}{2} + \frac{1}{2^2} + ... + \frac{1}{2^n}) < \ln 2$ (en utilisant la somme des termes de la suite géométrique). La suite (v_n) est croissante majorée, elle converge donc vers un réel a inférieur à 1+ln2. Premier résultat, $\frac{1}{2^n}\ln(u_n) \approx a$ donc $\ln(u_n) \approx 2^n.a$. Hélas, on ne peut pas prendre des exponentielles d'équivalent. Il nous faut donc poursuivre notre étude un peu plus loin, en utilisant des majorations plus fines.

En utilisant la concavité de ln, $\ln(1 + \frac{1}{x}) < x$, on obtient : $v_{n+1} - v_n = \frac{1}{2^{n+1}}(\ln(1 + \frac{1}{u_n}) < \frac{1}{2^{n+1}}\frac{1}{u_n}$ Un e nouvelle utilisation des dominos, du rang n au rang p, donne :

$v_{n+p} - v_n < \frac{1}{2^{n+1}u_n} + \frac{1}{2^{n+2}u_{n+1}} + ... + \frac{1}{2^{n+p}u_{n+p-1}}$. Comme la suite $\frac{1}{u_n}$ est décroissante, nous pouvons écrire : $v_{n+p} - v_n < \frac{1}{u_n}(\frac{1}{2^{n+1}} + ... + \frac{1}{2^{n+p}}) < \frac{1}{2^n u_n}$ (en majorant par la somme de la série géométrique). Ceci est valable pour tout naturel p, donc, par passage à la limite (légitime, puisque la suite v converge) :

$0 < a - v_n < \frac{1}{2^n u_n}$, c'est-à-dire $0 < 2^n a - \ln(u_n) < \frac{1}{u_n}$.

La suite $(2^n a - \ln(u_n))$ a donc comme limite 0. Par passage, licite, à l'exponentielle, on en déduit que la suite $\exp(2^n a - \ln(u_n)) = \frac{\exp(2^n a)}{u_n}$ a pour limite 1. D'où le résultat final : $u_n \approx \exp(2^n a)$. La suite u a bien une croissance très rapide, mais elle est définie pour tout n, à la différence de la fonction solution de l'équation différentielle correspondante.

Ceci aura des conséquences importantes : si l'on utilise une méthode numérique de résolution de l'équation différentielle (type méthode d'Euler), ce qui revient à remplacer l'étude du phénomène continu par un phénomène discret, on pourra très bien trouver une solution fausse. En effet, si le pas de calcul est trop grand, la fonction pourra franchir l'asymptote x = 1 (cf. sur ce point la brochure *Des fonctions et des graphes* déjà citée).

IV.3.2. Conclusions de cette comparaison suites récurrentes-équations différentielles

- Parfois phénomènes discrets et continus marchent du même " pas ", parfois les itinéraires sont parfaitement divergents.

- Parfois les phénomènes continus s'étudient de façon plus simple que les phénomènes discrets (on l'a constaté dans la recherche d'équivalents pour le processus à divergence lente).

- Parfois ce sont les méthodes discrètes qui permettent d'aborder les phénomènes continus (c'est ce que l'on fait pour toute résolution numérique d'une équation différentielle).

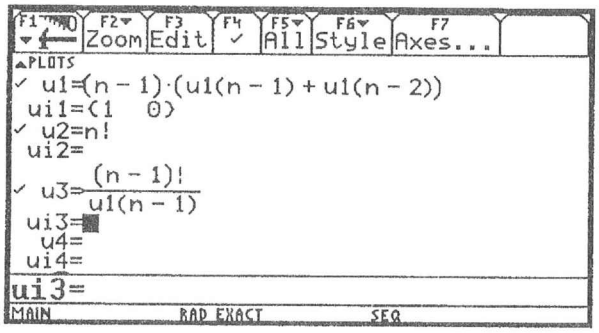
Mais un résultat obtenu dans un domaine ne peut pas se transférer automatiquement à l'autre. Tout est une affaire de contrôle théorique et de discernement.

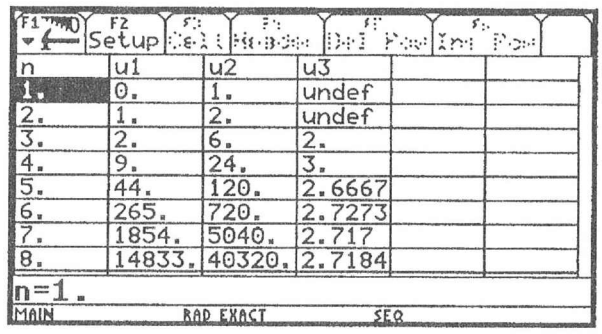
IV.4. Récurrences et fonctions génératrices

Nouveau problème d'étude de suites récurrentes, mais dans une situation où le recours à une équation différentielle est moins direct. Nous proposons d'étudier la suite récurrente définie par :

$$u_{n+2} = (n+1)(u_n + u_{n+1}), \quad u_1 = 0 \quad u_2 = 1$$ [23]

Nous pouvons observer le comportement des premiers termes de la suite, en la comparant à la suite (n!) (cf. ci-dessous). Cette comparaison est assez naturelle, si l'on considère l'origine de la suite (les dérangements) ou son mode de fabrication (on multiplie à chaque fois par n).





Le rapport entre n ! et la suite u semble converger vers un nombre qui ressemble fort à e. Nous nous proposons de le prouver par recours à une méthode fonctionnelle. Il s'agit de la recherche de la " fonction génératrice " de cette suite, c'est-à-dire d'une fonction f, développable en série entière, égale à : $f(x) = \sum_{k=0}^{\infty} \frac{u_n}{n!} x^n$, où u_n est notre suite. Nous aurions donc f(0) = 0

L'objectif est de dériver f, en utilisant la relation de récurrence qui définit la suite u :

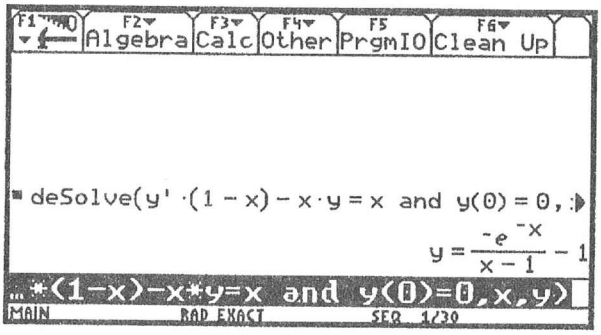
$$f'(x) = \sum_{k=1}^{\infty} \frac{u_n}{(n-1)!} x^{n-1} = x + \sum_{k=3}^{\infty} \frac{(n-1)(u_{n-2} + u_{n-1})}{(n-1)!} x^{n-1} = x + x\sum_{k=3}^{\infty} \frac{u_{n-2}}{(n-2)!} x^{n-2} + x\sum_{k=3}^{\infty} \frac{u_{n-1}}{(n-2)!} x^{n-2}$$

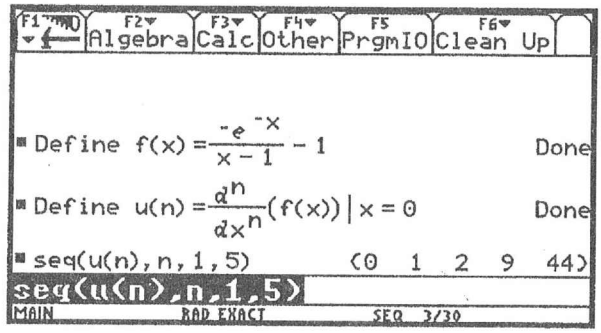
On reconnaît f'(x) = x + xf(x) + xf'(x). La fonction f serait ainsi solution de l'équation différentielle y'(1-x) - xf(x)=x. Nous savons qu'il s'agit d'une équation résolue sur l'intervalle]-1 ; 1[(nous nous intéressons à un intervalle centré en 0 puisque nous recherchons une fonction développable en série entière).

---

[23] Cette suite correspond au nombre de " dérangements ", c'est-à-dire de permutations sans points fixes de n éléments. On en trouvera une étude détaillée dans [Trouche, 1998] ou [Bernard et alii, 1998].

Nous pouvons voir ci-dessous la résolution de cette équation différentielle. La solution est $f(x) = -\frac{e^{-x}}{x-1} - 1$. Le terme de rang n de la suite correspond (via un développement de Taylor) à la valeur que prend la dérivée $n^{ième}$ de f en 0, ce que l'on vérifie ci-dessous.





Mais cette expression de la fonction f nous donne encore davantage. Nous pouvons développer en série les fonctions qui composent f, et, par un produit de convolution retrouver le développement en série de la fonction f : $e^{-x} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} x^k$ et $\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k$

Ainsi, dans le développement en série de f, le coefficient de x^n est $\sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

D'où, en comparant avec l'écriture initiale de f, le résultat :

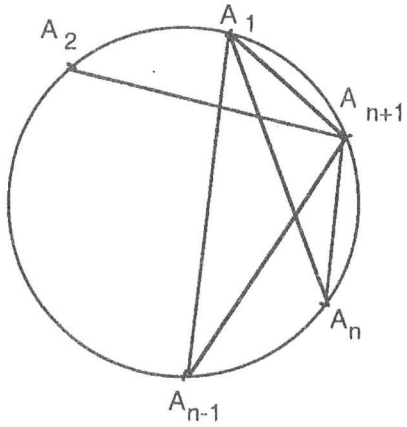
$\frac{u_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$ d'où $u_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$. Nous en tirons immédiatement un équivalent pour la suite : $\lim_{n \to +\infty} \frac{u_n}{n!} = \frac{1}{e}$, ce qui confirme bien l'observation expérimentale.

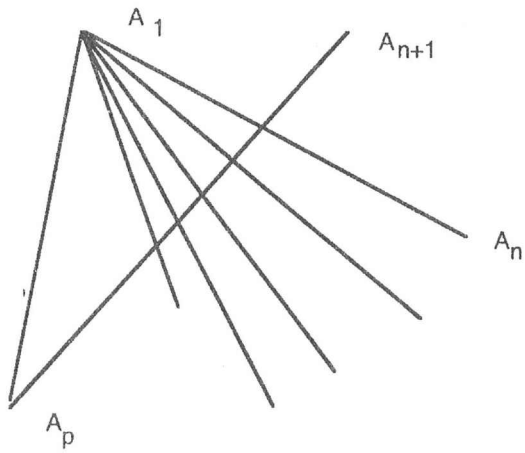
C'est à nouveau un aller-retour entre les domaines du discret et du continu qui nous a permis de traiter cet exercice.

IV.5. Différences finies et formules de Taylor

À nouveau les formules de Taylor, pour traiter de façon (relativement) non classique un problème (relativement) classique. Il s'agit de savoir combien de secteurs l'on peut obtenir dans un disque en reliant de toutes les façons possibles (par des segments) n points situés sur son pourtour. Il est clair que, pour 0 point, on a 1 secteur ; pour 1 point, on a 1 secteur aussi ; pour 2 points, 2 secteurs ; pour 3 points, 4 secteurs ; pour 4 points, 8 secteurs ; pour 5 points, 16 secteurs. Il est tentant de conjecturer l'existence d'une suite géométrique simple... Qu'en est-il vraiment ?

Commençons notre calcul par le choix de notations simples : on appellera r(n) le nombre de secteurs cherché et par s(n) le nombre de régions supplémentaires engendrées par l'ajout du point A_{n+1} sur le cercle (cf. schéma ci-dessous)





IV.5.1. Premiers calculs

Il est clair que l'on a r(n+1)= r(n) + s(n), d'où l'expression générale de r(n) :

$r(n) = r(0) + \sum_{k=0}^{n-1} s(k) = 1 + \sum_{k=0}^{n-1} s(k)$, puisque r(0) = 1. Il nous reste à calculer s(n).

L'idée fondamentale consiste à remarquer que, si une corde $[A_{n+1}, A_p]$ coupe deux cordes " consécutives " $[A_i, A_{j-1}]$ et $[A_i, A_j]$ pour i < j, il y a une région supplémentaire. On en déduit que la corde $[A_{n+1}, A_p]$ coupe (p-1)(n-p) fois les cordes qui ont pour une de leurs extrémités l'un des (p-1)

points A_1, A_2, ..., A_{p-1}, pour autre extrémité l'un des (n-p) points A_{p+1}, A_{p+2}, ..., A_n. Ceci nous donnedonc (p-1)(n-p) régions supplémentaires dans le secteur du disque défini par les points A_1, A_p, A_n, auxquelles il faut ajouter la région qui apparaît dans le secteur circulaire défini par les trois points A_1, A_{n+1}, A_n. D'où, en sommant lorsque p varie de 1 à n, l'expression de s(n) :

$$s(n) = n + \sum_{p=1}^{n} (p-1)(n-p)$$

On peut dès lors affirmer que, sommant un polynôme du deuxième degré en p entre 1 et n, nous allons obtenir un polynôme un polynôme en n du troisième degré (autre analogie avec le processus continu d'intégration). L'obtention de r(n) nécessitant une autre sommation de s(k), nous pouvons affirmer que r(n) est un polynôme en n du quatrième degré.

Nous pourrions bien sûr effectuer ces sommes. Mais il y a plus simple, puisque nous connaissons les valeurs que prend ce polynôme pour 5 valeurs de n (voir le début de cet exercice !). Nous pourrions alors chercher l'écriture de r(n) dans la base canonique par le biais de la résolution d'un système linéaire de 5 équations à 5 inconnues :

$r(n) = a + b.n + c.n^2 + d.n^3 + e.n^4$

IV.5.2. Un grand détour pour une grande simplification

Mais il y a encore plus simple, si l'on choisit une base de polynômes adaptée : la base des polynômes combinatoires : $C_0(x) = 1$ et, pour $p > 1$, $C_p(x) = \dfrac{x(x-1)...(x-p+1)}{p!}$ (polynôme de degré p). L'appellation " combinatoire " résulte bien sûr de ce que, pour n entier, $C_p(n) = C_n^p$. Ces polynômes possèdent des propriétés importantes, en particulier celle de donner à tout entier une image entière[24]. Ces polynômes ayant des degrés échelonnés, ils constituent aussi une base de l'espace des polynômes. Nous pouvons donc chercher des coefficients α, β, γ, δ et ε tels que : $r(n) = \alpha.C_0(n) + \beta.C_1(n) + \gamma.C_2(n) + \delta.C_3(n) + \varepsilon.C_4(n)$.

Ces coefficients vont pouvoir se calculer très facilement grâce à l'opérateur " différence finie " qui, à tout polynôme P associe le polynôme Q tel que Q(x) = P(x+1) - P(x) (on peut constater une certaine ressemblance avec la dérivation). On notera $Q = \Delta(P)$. Quelques propriétés de cet opérateur :

- c'est un opérateur linéaire ;
- il est possible de l'itérer : $\Delta^2(P) = \Delta(\Delta(P))$;

---

[24] On a même mieux : un polynôme donne à tout entier une image entière si et seulement s'il est une combinaison linéaire à coefficients entiers des polynômes combinatoires (sur ce point, voir *Arithmétique, le retour* [Bernard et alii, 1995]).

- il est clair (c'est simplement l'application de la formule additive des combinaisons) que : $\Delta(C_0) = 0$ et $\Delta(C_p) = C_{p-1}$. Comme pour la dérivation, l'image d'un polynôme est un polynôme de degré immédiatement inférieur. L'intérêt, avec les polynômes combinatoires, est que le coefficient multiplicatif est 1, ce qui va nous donner par la suite des calculs particulièrement simples.

IV.5.3. Une nouvelle formule de Taylor

Soit donc un polynôme P égal à $P(x) = a_0 + a_1C_1(x) + a_2C_2(x) + ... + a_nC_n(x)$. Nous voulons calculer les différents coefficients permettant d'exprimer P dans la base des polynômes combinatoires :

- il est clair que $a_0 = P(0)$;

- en utilisant la linéarité de l'opérateur Δ et le résultat concernant l'image de chaque polynôme combinatoire, nous obtenons :

$\Delta(P)(x) = a_1\Delta(C_1)(x) + a_2\Delta(C_2)(x) + ... + a_n\Delta(C_n)(x) = a_1C_0(x) + a_2C_1(x) + ... + a_nC_{n-1}(x)$ D'où le résultat : $\Delta(P)(0) = a_1$.

- nous pouvons alors appliquer à nouveau l'opérateur Δ, ce qui nous donnera $\Delta^2(P)(0) = a_2$, et plus généralement $\Delta^n(P)(0) = a_n$

D'où l'expression générale de P, dont l'analogie avec la formule de Taylor est claire :

$$P(x) = P(0) + \Delta(P)(0).C_1(x) + \Delta^2(P)(0).C_2(x) + ... + \Delta^n(P)(0).C_n(x)$$

L'intérêt de cette formule est que le calcul des différents coefficients est immédiat, avec une disposition de tableau :

x	P(x)	$\Delta(P)(x)$	$\Delta^2(P)(x)$	$\Delta^3(P)(x)$	$\Delta^4(P)(x)$
0	$P(0) = \mathbf{a_0}$	$\Delta(P)(0) = P(1)-P(0) = \mathbf{a_1}$	$\Delta^2(P)(0) = \Delta(P)(1)-\Delta(P)(0) = \mathbf{a_2}$	$\Delta^3(P)(0) = \Delta^2(P)(1)-\Delta^2(P)(0) = \mathbf{a_3}$	.....
1	P(1)	$\Delta(P)(1) = P(2)-P(1)$	$\Delta^2(P)(1) = \Delta(P)(2)-\Delta(P)(1)$	$\Delta^3(P)(1) = \Delta^2(P)(2)-\Delta^2(P)(1)$	.....
2	P(2)	$\Delta(P)(2) = P(3)-P(2)$	$\Delta^2(P)(2) = \Delta(P)(3)-\Delta(P)(2)$	$\Delta^3(P)(2) = \Delta^2(P)(3)-\Delta^2(P)(2)$	
3	P(3)	$\Delta(P)(3) = P(4)-P(3)$	$\Delta^2(P)(3) = \Delta(P)(4)-\Delta(P)(3)$		
4	P(4)	$\Delta(P)(4) = P(5)-P(4)$			
5	P(5)				

IV.5.4. Application au problème des secteurs circulaires

Nous recherchons $r(n) = \alpha.C_0(n) + \beta.C_1(n) + \gamma.C_2(n) + \delta.C_3(n) + \varepsilon.C_4(n)$. Le calcul des 5 coefficients nécessite l'évaluation, déjà faite, de la fonction r en 5 points :

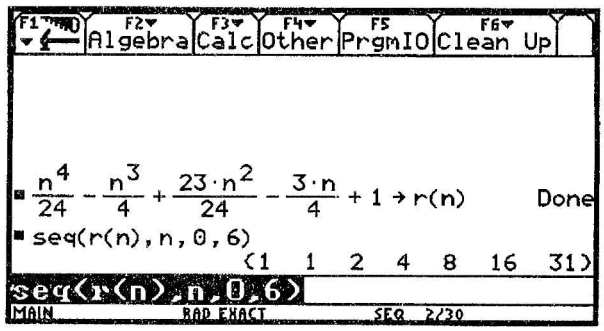
n	r(n)	$\Delta(r)(n)$	$\Delta^2(r)(n)$	$\Delta^3(r)(n)$	$\Delta^4(r)(n)$
1	r(0) = 1= $\mathbf{a_0}$	$\Delta(r)(0) = 0 =$ $\mathbf{a_1}$	$\Delta^2(r)(0) = 1=$ $\mathbf{a_2}$	$\Delta^3(r)(0) = 0 =$ $\mathbf{a_3}$	$\Delta^4(r)(0) = 1=$ $\mathbf{a_4}$
1	r(1) = 1	$\Delta(r)(1) = 1$	$\Delta^2(r)(1)= 1$	$\Delta^3(r)(1)= 1$	.....
2	r(2) = 2	$\Delta(r)(2) = 2$	$\Delta^2(r)(2)= 2$		
3	r(3) = 4	$\Delta(r)(3) = 4$			
4	r(4) = 8				

D'où le résultat immédiat :

$$r(n) = C_0(n) + C_2(n) + C_4(n) = C_n^0 + C_n^2 + C_n^4 = 1 + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)(n-3)}{4!}$$

Petite vérification, à l'aide du module de calcul formel de la calculatrice TI-92 :

La fonction r est définie, puis évaluée pour les valeurs de n de 0 à 6. Nous retrouvons bien les premières valeurs calculées ; quant à r(6), il n'est pas égal à 32, comme nous aurions pu l'espérer au départ. Mais un décompte rapide des secteurs fait souvent voir ce que l'on aimerait bien voir, c'est-à-dire 32...



Cette méthode peut s'appliquer tout aussi simplement à la recherche de tout polynôme dont on connaît le degré et la valeur en suffisamment de points distants de 1. Un exemple simple pour finir : la somme des n premiers naturels est un polynôme de degré 2. Calculons ses coefficients dans la base des polynômes combinatoires. Nous avons besoin de 3 valeurs :

P(0) = 0 P(1) = 1 P(2) = 1+2 = 3

n	P(n)	$\Delta(P)(n)$	$\Delta^2(P)(n)$
0	0	1	1
1	1	2	
2	3		

D'où $P(n) = 0.C_0(n) + 1.C_1(n) + 1.C_2(n) = C_n^1 + C_n^2 = n + \frac{n(n-1)}{2} = \frac{n(n+1)}{2}$

Nous laissons le lecteur curieux appliquer cette méthode à la recherche de la somme des premiers carrés, des premiers cubes, etc...

IV.6. Equations entières et courbes algébriques

Après ces quelques variations algébriques, nous proposons au lecteur encore alerte un dernier "jeu scientifique" autour du discret et du continu, dans le domaine arithmético-analytique pour finir. Le problème : soient a et b deux entiers positifs, il s'agit de prouver que, dès que $\frac{a^2+b^2}{ab+1}$ *est un entier, c'est un carré d'entier*[25].

Remarque préliminaire : le problème est évidemment symétrique en a et b. Nous considèrerons dès lors les couples (a, b) où $a \geq b$.

IV.6.1. Du côté des nombres a ou b

Il est aisé de voir pour, pour a et b nuls, le quotient est égal à 0. Si b est nul, le quotient est égal à a^2, la propriété est encore vérifiée. Nous avons donc une infinité de couples (a, 0) ou (0, b) avec a et b entiers positifs quelconques qui vérifient la propriété. Nous savons aussi que tout les carrés d'entiers peuvent ainsi être atteints. Mais, existe-t-il d'autres couples ? Il est possible d'écrire un petit programme de recherche en testant le caractère d'entier (c'est-à-dire la différence entre le nombre et sa partie entière) de $f(a, b) = \frac{a^2+b^2}{ab+1}$. Le couple (1, 1) convient.

Existe-t-il d'autres couples (a, a) ? $f(a, a) = \frac{2a^2}{a^2+1}$. Il suffit de considérer la fonction $g \to g(x) = \frac{2x}{x+1}$, croissante sur $\mathbb{R}^+$, qui prend la valeur 0 en 0 et a pour limite 2 en $+\infty$, pour réaliser que les seules valeurs entières prises par ce quotient sont 0 et 1, ce sont bien des carrés, ils correspondent aux couples déjà mis en évidence (0, 0) et (1, 1). Il n'y a donc pas d'autres couples (a, a). Nous rechercherons désormais les couples (a, b) avec $a > b$.

Une recherche systématique donne d'autres couples (8, 2), (27, 3)… , qui débouchent, avec un certain sens de l'observation et de la généralisation, sur la famille (a^3, a).

En effet, $f(a^3, a) = \frac{a^6+a^2}{a^4+1} = \frac{a^2(a^4+1)}{a^4+1} = a^2$. Cela donne une autre façon d'atteindre tous les carrés d'entiers.

---

25 Exercice extrait des XXIXe olympiade de mathématiques (1988) publiées, avec les solutions, par les Éditions du Choix en 1991. La solution que l'on présente ici diffère quelque peu de la solution des Éditions du Choix.

A-t-on fait le tour de toutes les solutions possibles ? " Hélas ", non, puisque la même recherche systématique donne f(30, 8) = 4. Nous ne pouvons espérer épuiser le problème avec une recherche systématique dans un ensemble infini... Une étude plus théorique s'impose.

Mais nous avons un premier résultat : il existe une infinité de couples (a, b) tels que le quotient $\frac{a^2+b^2}{ab+1}$ soit entier et, pour tous les couples trouvés, ce quotient est bien un carré d'entier.

IV.6.2. Du côté du quotient k

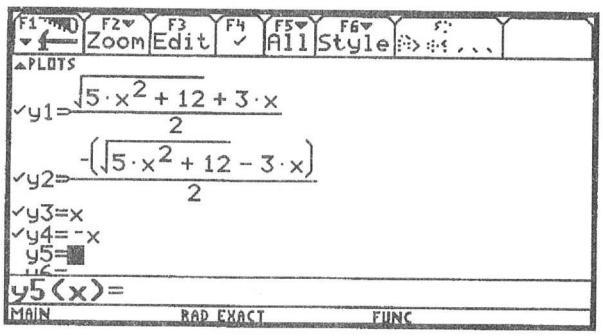
$$k = \frac{a^2+b^2}{ab+1}$$

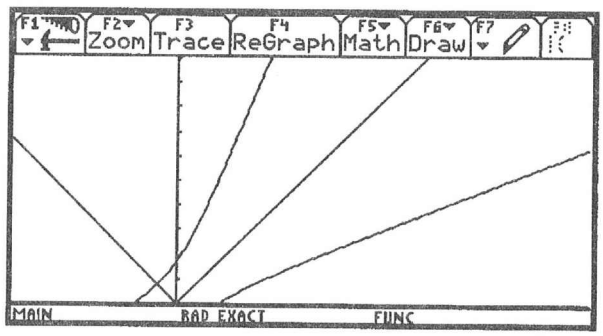
Soient a, b et k des entiers vérifiant $a^2 + b^2 = k.(ab+1)$:

- d'après ce que nous avons vu plus haut, cette équation possède des solutions en a et b entiers pour tout k égal à un carré d'entier ;

- pour le premier entier non carré, 2, il n'y a pas de solutions possibles, l'équation se ramenant à $(a-b)^2 = 2$.

Nous nous placerons désormais dans le cas $k \geq 3$, $a > b > 0$. Nous allons fixer k, en supposant que celui-ci n'est pas un carré d'entier. L'ensemble des points (x, y) vérifiant $x^2 + y^2 = k(xy+1)$ c'est-à-dire $x^2 - kxy + y^2 = k$ ou encore $(x - \frac{k}{2}y)^2 - (\frac{k^2}{4} - 1)y^2 = k$ est une conique. Plus précisément, comme $k \geq 3$, c'est une hyperbole qui a comme centre de symétrie (0, 0), comme axe focal la droite d'équation y = -x, comme deuxième axe de symétrie la droite d'équation y = x (ci-dessous une partie de la courbe en question, pour k = 3).



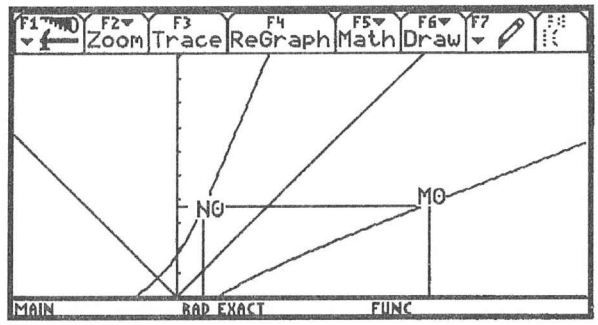


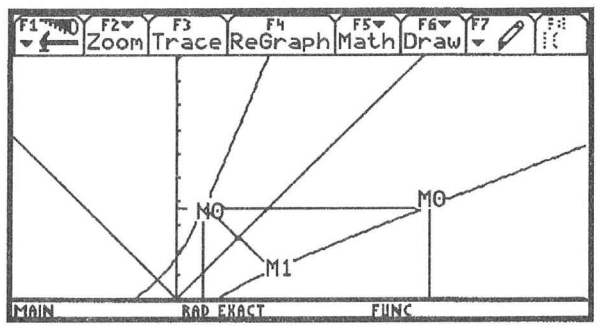
Nous voulons prouver que, puisque k n'est pas un carré d'entier, il n'y a aucun point à coordonnées entières sur cette courbe (dans le quadrant x > 0, y > 0). Comme nous considérons les couples (a, b) avec a > b, nous nous intéresserons seulement à l'arc d'hyperbole H_1 qui est sous la première bissectrice.

IV.6.3. Une descente infinie

La méthode que nous allons utiliser ici est la méthode de " descente infinie ", attribuée à Fermat[26] : nous allons montrer que, s'il existe un point $M_0(x_0, y_0)$ à coordonnées entières sur cet arc d'hyperbole, alors il en existe nécessairement un autre $M_1(x_1, y_1)$ avec $x_1 < x_0$ et $y_1 < y_0$. Comme la descente infinie stricte est impossible dans les entiers naturels, cela prouvera le caractère absurde de notre hypothèse.

Supposons donc l'existence d'un tel point $M_0(x_0, y_0)$ (cf. ci-contre). Il existe alors un point de l'hyperbole, situé sur l'autre arc, de même ordonnée. Son abscisse est solution, comme x_0, de l'équation $x^2 - kxy_0 + y_0^2 = k$. Du fait de la somme des racines de cette équation, l'abscisse de N_0 est donc ky_0-x_0. Elle est bien évidemment entière. Nous pouvons alors considérer le point M_1, symétrique de N_0 par rapport à la première bissectrice. Il se trouve sur l'arc H_1 de l'hyperbole. Ses coordonnées vérifient :
$x_1 = y_0 < x_0$ (puisque l'arc H_1 est sous la première bissectrice) ; $y_1 = x_0$.





Comme cet arc d'hyperbole est la représentation graphique d'une fonction strictement croissante, les abscisses et les ordonnées des points de cet arc sont dans le même ordre strict ; ainsi $x_1 < x_0$ implique $y_1 < y_0$. Il nous reste à prouver que les coordonnées de M_1, qui sont entières, sont strictement positives. x_1 l'est, puisque $x_1 = y_0$!

Peut-on avoir $y_1 < 0$? On aurait alors $y_0\, y_1 < 0$, donc, puisqu'il s'agit d'entiers, $y_0\, y_1 \leq -1$. Or (y_0, y_1) sont les coordonnées du point M_1 et vérifient donc l'équation $y_0^2 + y_1^2 = k(y_0.y_1 + 1)$. La relation $y_0\, y_1 \leq -1$ impliquerait alors $y_0^2 + y_1^2 \leq 0$, ce qui est parfaitement impossible (rappelons que y_0 est strictement positif).

Peut-on avoir alors avoir $y_1 = 0$? La même relation $y_0^2 + y_1^2 = k(y_0.y_1 + 1)$ impliquerait alors que k serait un carré, ce qui est exclu !

Ainsi, nous avons bien notre amorce de descente infinie : s'il existait un point à coordonnées entières strictement positives sur H, il existerait un autre point, à coordonnées entières strictement positives strictement inférieures à celles du premier point. Impossible !

---

[26] Voir le chapitre III.

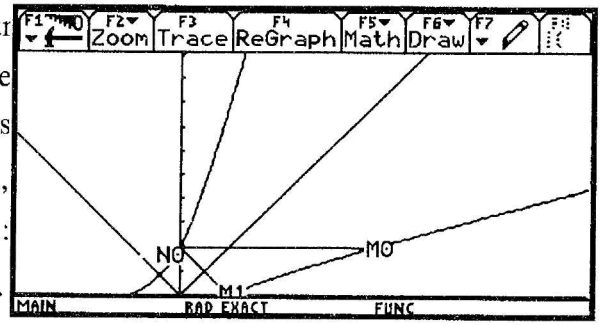
Nous avons bien prouvé que, pour que l'hyperbole contienne des points à coordonnées entières, il fallait nécessairement que k soit un carré.

IV.6.4. Supposons désormais k égal à un carré d'entier

Nous avons observé que les couples $(\sqrt{k},0)$ et $(k\sqrt{k},\sqrt{k})$ conviennent, mais comment obtenir tous les couples qui conviennent pour un carré d'entier k donné ?

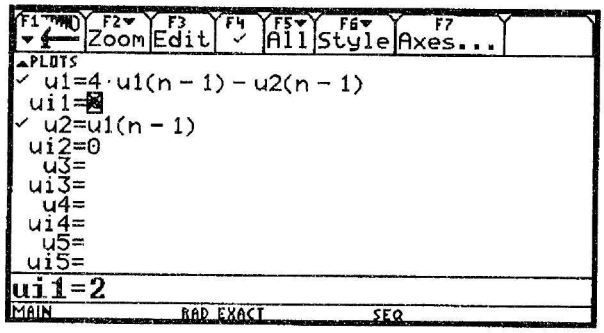
La méthode de descente infinie va pouvoir nous fournir l'ensemble des points à coordonnées entières appartenant à l'hyperbole (on a représenté ci-dessous l'hyperbole pour k = 4). La seule possibilité pour stopper la descente infini est en effet de " tomber " sur 0.

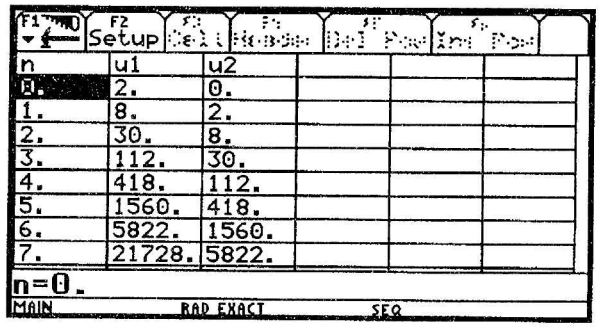
Le point M_1 a alors pour coordonnées $(\sqrt{k},0)$. Pour trouver le point " antérieur ", il suffit de parcourir le chemin inverse, de remonter la descente que nous avons empruntée auparavant : $y_1 = \sqrt{k}$ et $x_1 = k\sqrt{k}$, puisque ces nombres vérifient l'équation : $x_1^2 + y_1^2 = k(x_1y_1 + 1)$, on retrouve les couples (a^3, a).



Ceci débouche sur une récurrence immédiate : $y_{n+1} = x_n$ et $x_{n+1} = kx_n - y_n$, qui nous donne tous les couples solutions au départ du " germe " $(\sqrt{k},0)$.

Nous avons reproduit ci-dessous les premiers couples correspondant au " germe " (2, 0).

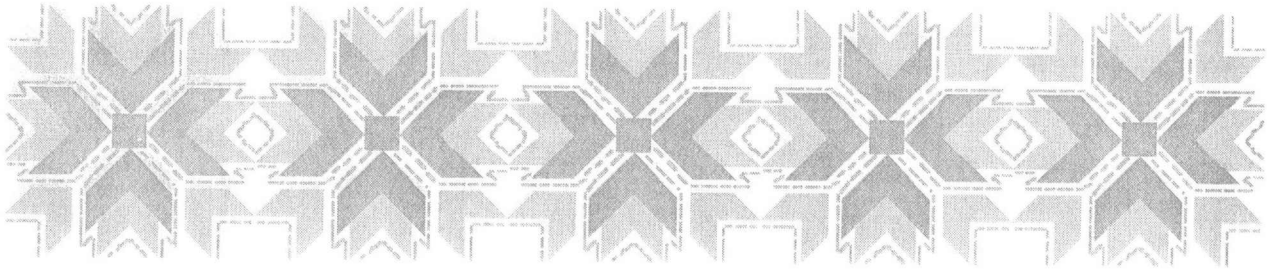




Nous voici arrivés au terme de ce " jeu scientifique " sur le discret et le continu. Il ne s'agit pas bien sûr de problèmes simples qui pourraient se transposer directement dans la classe. Nous croyons qu'il ne s'agit pas plus de mathématiques seulement pour amateurs éclairés. Ces idées peuvent être aménagées pour en faire des sujets de recherche dans les classes. Elles peuvent contribuer à mettre en évidence la richesse des mathématiques, stimuler la volonté de chercher et le désir de connaître davantage.

C'est un défi pour les élèves et aussi un défi pour le professeur !

V. Algorithmique



V.1. Introduction

*Le terme d'**algorithme** est tiré du nom du mathématicien Al-Kharizmi, qui fut au IX^{ème} siècle à Bagdad l'un des fondateurs de l'arithmétique moderne. Ses ouvrages ont permis de transmettre à l'Occident les règles de calculs sur la représentation décimale des nombres.*

Un algorithme est une méthode de résolution d'un problème par une succession d' opérations élémentaires obéissant à un enchaînement déterminé.

V.1.1. Historique

Divers algorithmes ont été mis au point dès l'Antiquité :

- algorithme de calcul des décimales du nombre Π (Archimède, 3ème siècle av J-C) ;
- algorithme de calcul du PGCD de deux nombres (Euclide, 3ème siècle av J-C).

Plus tard, les problèmes de résolution d'équations algébriques ont conduit à de nombreux algorithmes (méthode de Cardan, algorithme de Newton, méthode d'élimination de Gauss...). La recherche de solutions d'équations différentielles a apporté aussi son lot d'algorithmes.

L'avènement des calculateurs électroniques a entraîné un renouvellement complet de l'algorithmique :

- d'une part, les algorithmes se sont exprimés dans une grammaire synthétique : les langages de programmation ;
- la taille des problèmes, c'est à dire leurs données et leurs résultats, a considérablement augmenté (on traite des systèmes linéaires de plusieurs milliers d'équations) ;
- l'efficacité des calculateurs électroniques tend à poser l'algorithme du problème comme un objectif collatéral à la résolution du problème.

On relèvera deux conséquences :

- les résultats fournis par des algorithmes traités par une machine seront parfois invérifiables « à la main » (qui ira vérifier la solution d'un système 1000 x1000 !) ;
- les contraintes très lâches sur la taille des problèmes peuvent avoir des conséquences lourdes sur les durées d'exécutions (on peut lancer un problème sur un nombre à 100 chiffres mais il ne faudrait pas qu'il nécessite 1000 ans pour être traité !).

L'objet de **l'algorithmique** est la construction de programmes, c'est aussi l'évaluation des programmes quant à leur correction et leur efficacité.

V.1.2. Correction d'un programme

Un programme est correct quand son exécution produit, dans un temps fini, le résultat pour lequel il a été construit. Cette problématique conduit à la notion de «démonstrations de programmes». A cette fin des formalisations et leurs axiomatiques ont été développées, on peut citer celles de Hoare, de Dijkstra.

Grâce à ces formalisations, on peut montrer que {D} P {R}, c'est-à-dire qu'un programme P construit pour donner à partir de {D : données}, un résultat {R} fournira exactement ce résultat {R}. On dit qu'on a montré sa *semi-correction.* .

Pour montrer sa correction, il reste à prouver que le résultat est obtenu dans un temps fini (que le programme ne « boucle pas » par exemple). Cette preuve de finitude ne peut pas être établie de façon formelle pour tout type de programme : la finitude des programmes est *indécidable*, c'est-à-dire il ne peut pas y avoir un algorithme qui permette de décider si un programme s'arrête ou pas ; seule une étude cas par cas des algorithmes permet de savoir si ceux-ci s'exécutent en un temps fini ou non.

V.1.3. Efficacité d'un programme

L'efficacité d'un programme se mesure par sa *complexité*. On distingue la *complexité pratique* qui est une mesure du temps d'exécution de ce programme et de la taille mémoire nécessaire. Cette mesure est liée, entre autres, à la machine utilisée. On préfère considérer la *complexité théorique* qui s'exprime indépendamment de la machine et, par là, reste valable à travers les évolutions technologiques. Cette complexité théorique reste liée aux données initiales, ainsi l'efficacité d'un algorithme de tri dépend du désordre initial des données. On définit donc la *complexité théorique maximale* que l'on appellera *complexité* qui est celle obtenue dans le cas le plus défavorable. La notation retenue pour exprimer cette complexité est celle de Landau : $0(n)$, $0(n^2)$, ...

Exemple : « L'algorithme de Machin, basé sur la formule du même nom, permet de calculer les décimales successives de π, c'est un algorithme en $0(n)$ ».

Ceci signifie : si sur une machine, on a mesuré que

	pour calculer	100 décimales	il faut	1,2 secondes,
alors	pour calculer	1000 décimales	il faudra	12 secondes,
et	pour calculer	10^8 décimales	il faudra	$1{,}2\ 10^6$ sec. $\approx$14 j

Remarques : On retiendra toute la signification asymptotique de cette notion de complexité : un algorithme en 0(n) peut, sur la même machine, être plus lent qu'un algorithme en $0(n^2)$: les coefficients, les termes résiduels se révèlent pour de « petites » valeurs de n et sont effacés pour de « grandes » valeurs de n.
On retiendra tout l'intérêt des algorithmes en 0(log n), tels celui de Salamin qui calcule aussi les n premières décimales de π.

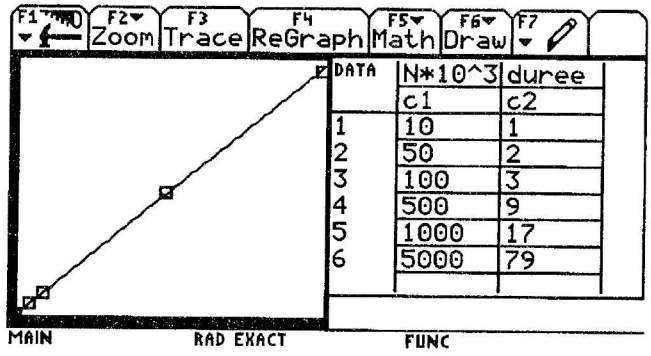
EXEMPLE DE CALCUL DE COMPLEXITE (1) :

Problème : Pour N donné trouver (x ; y) entiers tels que $x \leq y$ et $x^2 + y^2 = N$

Algorithme :
```
N,i ,j ,racn : ENTIERS
{n est donné ; racn = partie entière de √n, est donné}
POUR i:=1 JUSQUA racn FAIRE
    | POUR j:= i JUSQUA racn FAIRE
    |     | SI  i² + j² = N  ALORS  ' solution (i,j)'
```

Complexité : La boucle « j » est effectuée (racn - i) fois et i va de 1 à racn donc le test est effectué $\frac{(racn + 1)\ racn}{2}$ fois l'algorithme est en 0(N) (= $0(racn^2)$).

Une expérimentation[23] simple (N en milliers et durée en secondes) donne la représentation ci-contre et on constate, en régression linéaire, une corrélation de 0,99995 entre les données .



EXEMPLE DE CALCUL DE COMPLEXITE (2) :

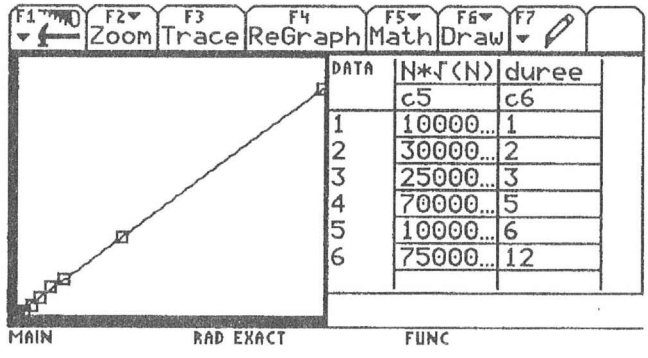
Problème : Pour N donné trouver (x ; y ; z) tel que $x \leq y \leq z$ et $x^2 + y^2 + z^2 = N$

Algorithme :
```
N, i, j, k, racn : ENTIERS
{n est donné ; racn = partie entière de √n, est donné}
POUR i:=1 JUSQUA racn FAIRE
    | POUR j:= i JUSQUA racn FAIRE
    |     | POUR k:= j JUSQUA racn FAIRE
    |     |     | SI  i² + j² + k²= N  ALORS  ' solution (i,j,k)'
```

[23] Turbo Pascal sur Mac, Système 7.

Complexité : La boucle « k » est effectuée (racn - j) fois et j va de i à racn et i de 1 à racn en dénombrant combien de fois le test est fait, il vient $0(N\sqrt{N})$ ($= 0(racn^3)$).

Une expérimentation du même type que précédemment donne des valeurs pour $N\sqrt{N}$ et la duréee correspondante. D'où la représentation ci-contre et on constate, en régression linéaire entre durée et $N\sqrt{N}$, une corrélation de 0,99993.



V.2. Quelques algorithmes et programmes

Les quelques programmes qui suivent sont loin de constituer une liste exhaustive de ce que l'on peut faire avec une calculatrice TI-92, ou une autre calculatrice du même genre, en arithmétique. Une fois de plus nous ne présentons ici que quelques fragments.

V.2.1. Intérêt de la démarche

L'intérêt de cette démarche est double.

- Enrichir la TI-92 de quelques programmes propres à l'arithmétique. Notamment on trouvera des programmes sur l'algorithme d'Euclide, les changements de bases, la liste des diviseurs d'un entier, le crible d'Eratosthène et la décomposition d'un nombre en facteurs premiers. Ces programmes sont présentés sur la TI-92, mais ils ont été conçus pour être facilement adaptés sur tout autre type de calculatrice programmable.
- Initier les élèves à la démarche de l'algorithmique. Rappelons que le programme de TS spécifie que « l'objectif est de donner aux élèves un minimum cohérent de notions élémentaires permettant l'élaboration d'algorithmes simples fondamentaux » et plus loin encore « l'aspect algorithmique sera privilégié ».

On notera que les programmes n'ont pas étés réalisés dans un souci de performance, ni d'ergonomie, mais plutôt dans un but pédagogique. En effet, nous avons cherché à préserver la lisibilité des programmes, afin que les élèves se familiarisent avec la programmation. Tous les programmes présentés peuvent être remaniés et réduits afin d'être plus performants et l'intérêt est justement que chacun les réécrive à sa façon, pour ainsi entrer complètement dans le domaine de l'algorithmique.

V.2.2. Algorithme d'Euclide

L'algorithme d'Euclide a la particularité d'être un des plus ancien algorithme mis au point (environ 300 ans av J-C). Le théorème de Bezout montre l'équivalence entre « deux nombres entiers a et b sont premiers entre eux » et « il existe au moins un couple d'entiers u et v vérifiant au + bv = 1. L'algorithme d'Euclide permet de déterminer deux de ces nombres u et v.

• Problème

Détermination : - du PGCD de a et de b ;

- de u et de v dans l'équation $au+bv = PGCD(a,b)$.

• Exemple

Soit $a = 4992$ et $b = 353$.

Déterminons les restes et quotients successifs des divisions euclidiennes suivantes :

$4992 = a = 353 \times 14 + 50 = 14\,b + 50$ (1)

$353 = b = 50 \times 7 + 3$ (2)

$50 = 3 \times 16 + 2$ (3)

$3 = 2 \times 1 + 1$ (4)

$2 = 2 \times 1 + 0$ (5)

Le premier reste non nul donne le PGCD (il vaut 1 ici).

On reprend alors les égalités précédentes de la façon suivante :

(1) $50 = a - 14\,b$

(2) $3 = b - 50 \times 7 = b - (a - 14\,b) \times 7 = 99\,b - 7a$

(3) $2 = 50 - 3 \times 16 = (a - 14\,b) - (99\,b - 7a) \times 16 = 113\,a - 1598b$

(4) $1 = 3 - 2 = 99\,b - 7a - (113\,a - 1598b) = 1697\,b - 120a$

On a finalement trouvé : $u = -120$ et $v = 1697$.

• Généralisation

Soit a et b deux nombres entiers dont on veut déterminer le PGCD et les coefficients u et v.

Appelons q_i les quotients et r_i les restes successifs dans l'algorithme d'Euclide .

On initialise : $r_0 = a$ et $r_1 = b$ et ensuite on a : $r_i = r_{i+1} \times q_{i+1} + r_{i+2}$ (*)

$$r_0 = a \qquad r_1 = b$$
$$r_0 = r_1 q_1 + r_2$$
$$r_1 = r_2 q_2 + r_3$$
$$\ldots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$
$$r_{n-1} = r_n q_n + r_{n+1} \qquad r_{n+1} = 0$$

Revenons à la relation (*). On voit qu'elle permet de calculer r_{i+2} en fonction de r_{i+1} et de r_i..

Si on arrive à exprimer r_{i+1} et r_i en fonction de a et b, alors on pourra en déduire r_{i+2} en fonction de a et b.

On a :

$r_i = u_i a + v_i b$ *et* $r_{i+1} = u_{i+1} a + v_{i+1} b$ $r_{i+2} = u_{i+2} a + v_{i+2} b$

avec :

$u_{i+2} = u_i - u_{i+1} q_{i+1}$ *et* $v_{i+2} = v_i - v_{i+1} q_{i+1}$

On initialise avec :

$a = u_0 a + v_0 b$ *et* $b = u_1 a + v_1 b$ *avec* $u_0 = 1; u_1 = 0; v_0 = 0; v_1 = 1$

$r_1 = 1 \times a - q_1 b$

$r_1 = (u_0 a + v_0 b) - q_1 (u_1 a + v_1 b)$

$r_1 = (u_0 - u_1 q_1)a - (v_0 - v_1 q_1)b$

Soit encore : $r_1 = u_2 a + v_2 b$, *avec* $u_2 = u_0 - u_1 q_1$ *et* $v_2 = v_0 - v_1 q_1$

$r_2 = b - q_2 \times r_1$

$r_2 = (u_1 a + v_1 b) - q_2 (u_2 a + v_2 b)$

$r_1 = (u_1 - u_2 q_2)a - (v_1 - v_2 q_2)b$

Soit encore : $r_2 = u_3 a + v_3 b$, *avec* $u_3 = u_1 - u_2 q_2$ *et* $v_3 = v_1 - v_2 q_2$

Par récurrence, on montre qu'il est donc possible d'écrire les trois suites (r_i) , (u_i) et (v_i) de la même façon :

$r_{i+2} = r_i - r_{i+1} q_{i+1}$

$u_{i+2} = u_i - u_{i+1} q_{i+1}$ *et* $v_{i+2} = v_i - v_{i+1} q_{i+1}$

Si r_n est le dernier reste non nul, on a : $r_n = PGCD(a,b)$, $u = u_n$ et $v = v_n$.

• Algorithme

Il faudra prévoir de sauvegarder à chaque étape les r_{ii} , r_{i+1} , u_i , u_{i+1} , v_i , v_{i+1} pour calculer les r_{i+2} , u_{i+2} et v_{i+2}.

Appelons u , v , r et u' , v' et r' les variables correspondant à deux indices successifs.

D'après ce qui précède, on peut écrire l'algorithme de la façon suivante :

Initialisation des variables:

Le tableau se lit : stocker 1 dans u ; 0 dans u' ; etc.

u	*u'*	*v*	*v'*	*r*	*r'*
1	0	0	1	a	b

Répéter tant que r n'est pas nul : q = *quotient entier de r par r'*

Le tableau se lit : stocker u' dans u ; u-qu' dans u' ; etc.

u	u'	v	v'	r	r'
u'	$u-qu'$	v'	$v-qv'$	r'	$r-qr'$

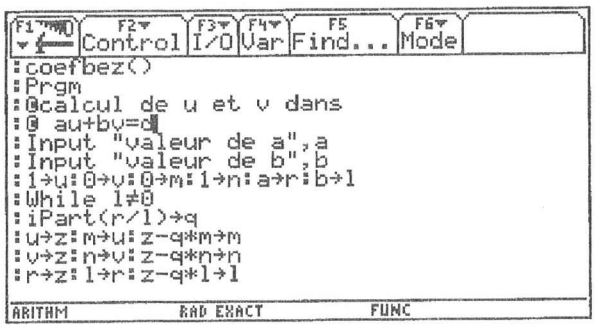
Fin du "répéter".

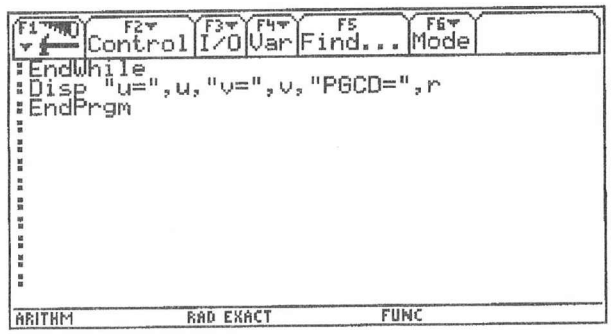
A la sortie de cet algorithme, r contient le PGCD et u et v les coefficients cherchés.

• Programme

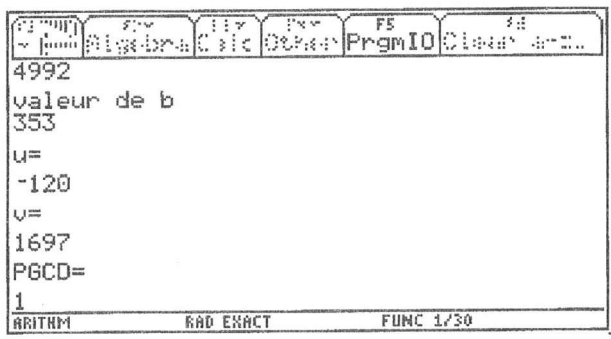
La TI-92 ne considérant pas les u', v' et r' comme variables, ces noms ont été remplacés par respectivement m, n et l.

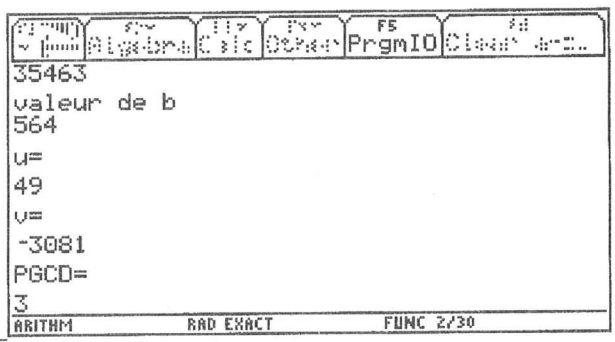
A chaque étape, pour ne pas perdre les valeurs de u, v et r, celles-ci sont stockées dans la variable intermédiaire notée z.





• Exemples





V.2.3. Changements de base

Les programmes qui suivent permettent d'écrire un nombre b dans une base donnée. Quand la base dépasse 10, il faudra transformer les chiffres supérieurs à 9 en lettres. Par exemple, en base 12, le 10 est codé a et le 11 est codé 12. Tous ces programmes peuvent être améliorés (en réalisant des tests en début de programme, par exemple) ou étendus à d'autre bases par des méthodes similaires (en base 16 entre autre).

A. Passage de la base 10 à une base b

• Problème

Soit un nombre a écrit en base 10 et b une base (b est compris entre 2 et 9 ou b=12). On cherche l'écriture de a en base b.

• Algorithme

** - Calculer le quotient entier q de a par b

- Calculer le reste entier r = a-bq

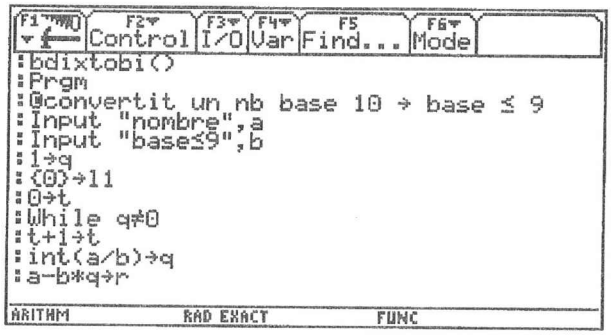
- Stocker r dans une liste l1

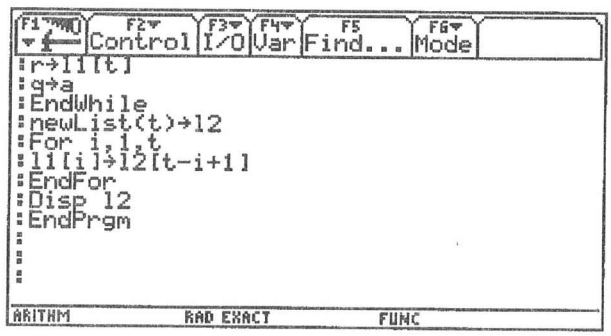
- Stocker q dans a Reprendre ** tant que q n'est pas nul Stocker la liste l1 dans la liste l2, dans le sens inverse.

Remarque : Pour b = 12, il faut transformer 10 en a et 11 en b.

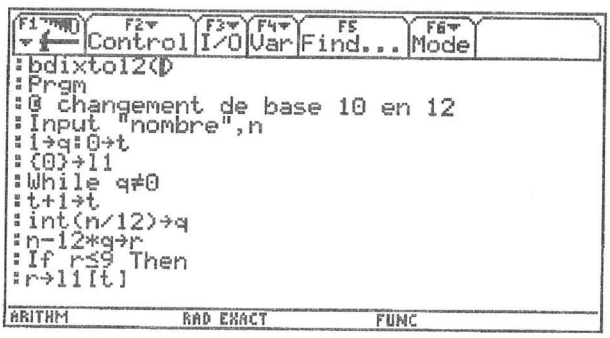
• Programmes

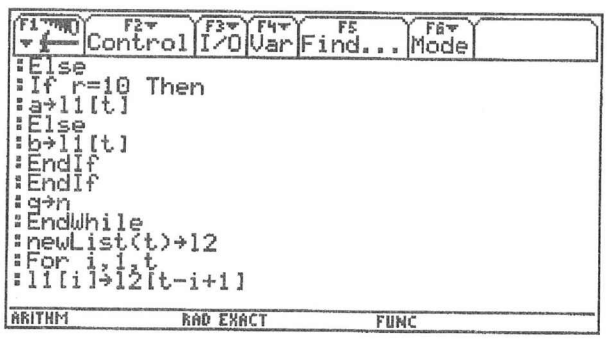
De la base 10 à la base b comprise entre 2 et 9

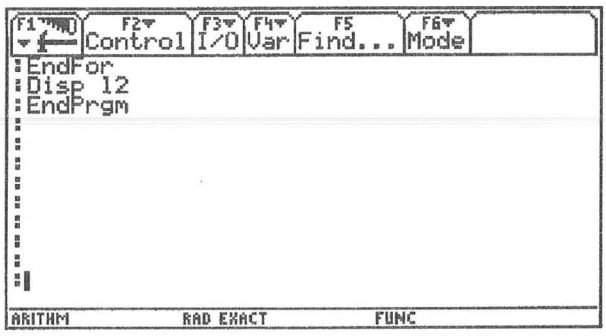




De la base 10 à la base 12

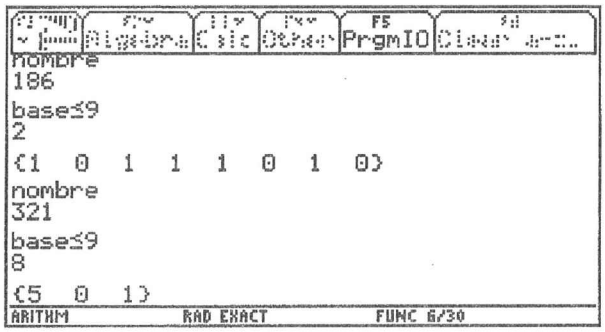


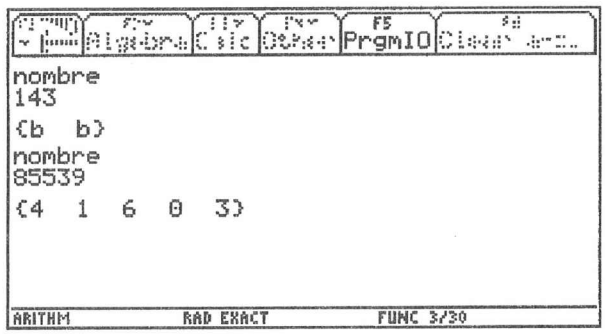




Remarque : On peut réduire les deux programmes précédents à un seul en faisant au départ un test sur la valeur de la base b.

• Exemples





B. Passage d'une base b à la base 10

• Problème Soit a un nombre écrit dans une base b inférieure ou égale à 9. Ecrire un programme permettant d'obtenir ce nombre en système décimal.

• Algorithme

On se limite à une base inférieure ou égale à 9 et à un nombre de 9 chiffres à convertir en base 10. On écrira donc un test correspondant à ces conditions.

On pose d le nombre en base 10 que l'on initialise à 0.

- Boucle :

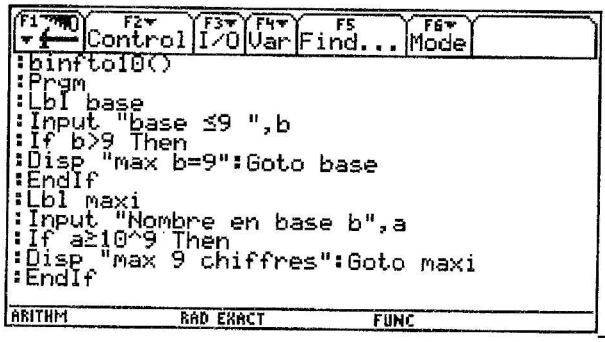
** - pour i variant de 0 à 8 :

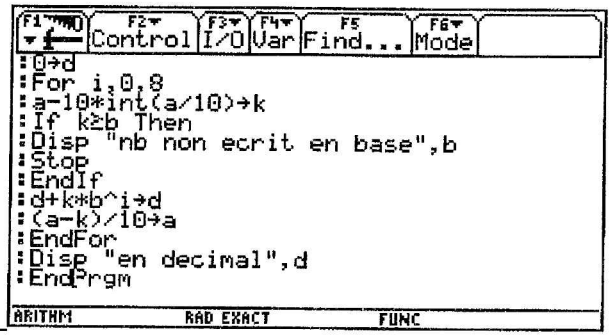
- déterminer le chiffre k de rang i +1 (calcul : k = a-10.E(a/10))
- ajouter à d le nombre k.b^i
- supprimer le chiffre k du nombre a (stocker (a-k)/10 dans a)

Reprendre à ** pour le i suivant.

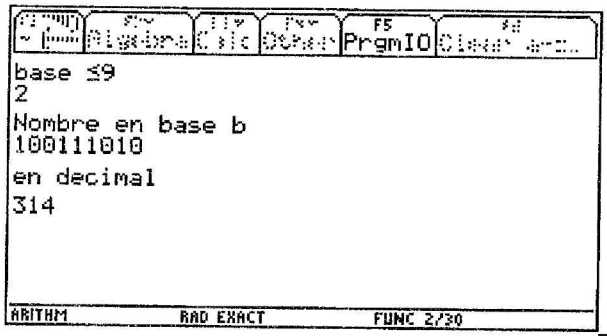
- Le nombre a converti en base 10 est stocké dans d.

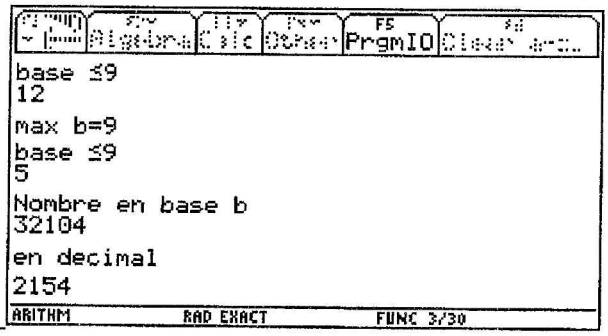
• Programme

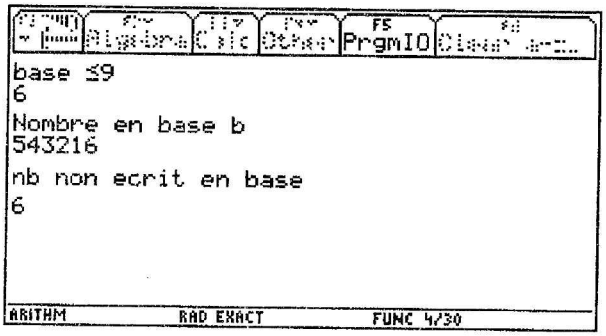


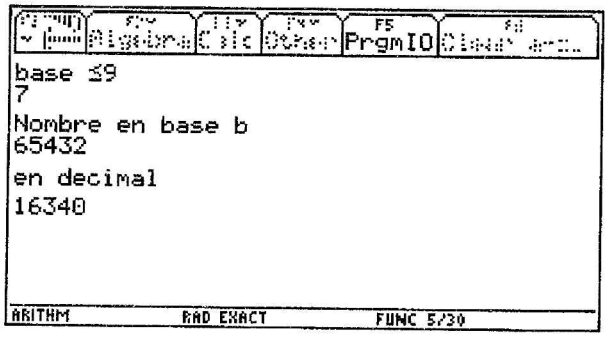


• Exemples









V.2.4 Liste des diviseurs d'un entier

Le programme qui suit repose sur la détermination des facteurs premiers d'un entier donné. Pour faire « défiler » ces nombres premiers rapidement, on évitera les nombres pairs et les impairs multiples de 3 et de 5.

Pour ce faire, à partir de p = 5, on ajoute alternativement 2 puis 4. On laisse subsister de cette façon des nombres non premiers mais on permet quand même à la calculatrice d'éviter une grande quantité de nombres non premiers.

- **Problème**

Soit a un nombre entier positif. On cherche à établir la liste des diviseurs de a et à ranger ces diviseurs dans une liste. Prenons un exemple : soit a = 180.

- On cherche successivement les diviseurs premiers de 180 avec « ordre de multiplicité ».
  Ici, 2^0, 2 et 2^2 sont des diviseurs de 180.
- On réalise alors une liste contenant ces premiers diviseurs : {1, 2, 4}.
- On réalise une $2^{ème}$ liste avec le nombre premier suivant et ses puissances, diviseurs de 180.
  Ici : {1, 3, 9} sont diviseurs de 180.
- On « multiplie » ces deux listes, élément par élément, pour en obtenir une troisième.
  Ici, {1, 2, 4} * {1, 3, 9} = {1, 2, 3, 4, 6, 9, 12, 18, 36}.
- Cette liste nous sert de base pour réaliser la liste suivante.

Avec 5 comme diviseur de 180, on obtient la liste : {1, 5} que l'on « multiplie » par la liste {1, 2, 3, 4, 6, 9, 12, 18, 36}.

On obtient alors la liste finale des diviseurs de 180 :

{1, 2, 3, 4, 6, 9, 12, 18, 36} * {1, 5} = {1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180}.

- **Algorithme**

L'algorithme qui suit est construit selon la méthode décrite à partir de l'exemple précédent.

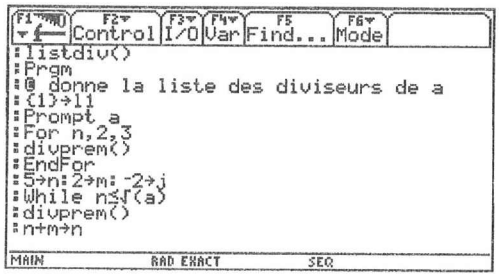
- On ouvre une liste {l1} pour y ranger les diviseurs de a.
- Boucle ** :
- On détermine si p premier est diviseur de a. S'il ne l'est pas, on passe au p suivant.
- On construit une liste : {1, p, p^2,..., p^k} des diviseurs de a que l'on multipliera avec la liste {l1}.
- On stocke cette liste dans {l1}.
- On reprend à ** tant que p est inférieur ou égal à $\sqrt{a}$.
- A la sortie de la boucle, {l1} contient la liste des diviseurs de a.

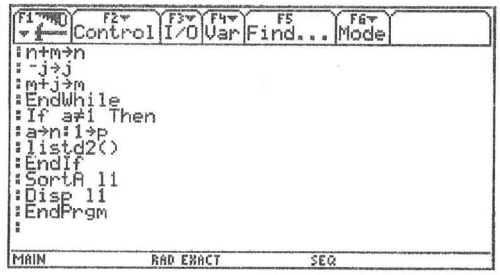
- **Programmes**

Le programme principal « listdiv » gère l'appel des deux sous-programmes :

- « divprem » qui recherche les nombres premiers diviseurs de a, avec leur ordre de multiplicité. ;
- « listd2 » qui établit la liste des diviseurs pour chaque facteur premier supplémentaire déterminé par « divprem ».

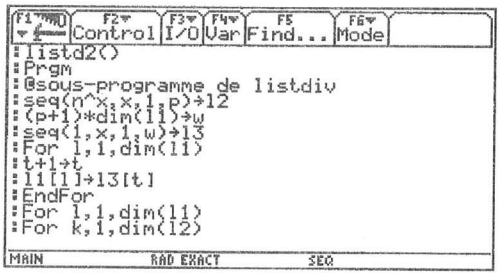
Programme principal « listdiv » :

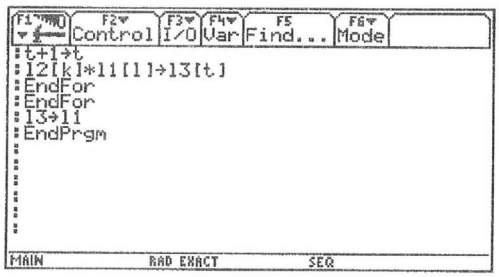




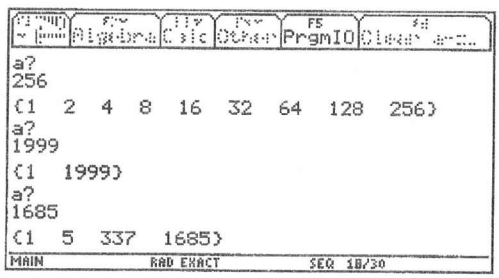
Premier sous-programme « divprem » :

Deuxième sous-programme « listd2 » :





- **Exemples**



V.2.5. Crible d'Eratosthène

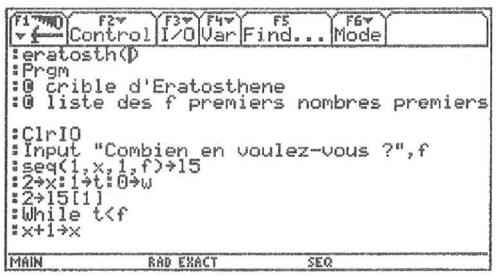
Eratosthène est un mathématicien grec de l'école d'Alexandrie (276 - 194 avant J.C.). Son « crible » permet de dresser la liste des nombres premiers compris entre 2 et N en barrant successivement les multiples des nombres entiers. Les nombres non barrés restants sont des nombres premiers.

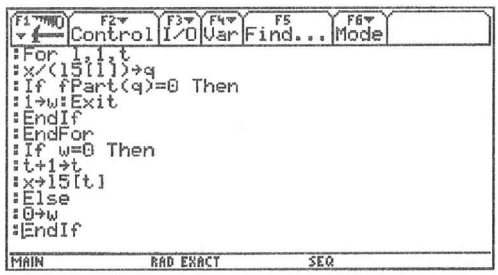
- **Problème**

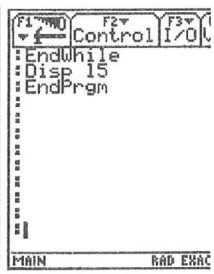
Soit à établir la liste des f nombres premiers, en utilisant le crible d'Eratosthène.

- **Algorithme**
  - On crée une liste {15} où l'on rangera les f premiers nombres premiers.
  - On range 2 comme premier élément de cette liste et on stocke 2 dans x.
  - Boucle ** :
  - On stocke x+1dans x et on teste si x divise les éléments de la liste {15} déjà rangés.
  - Si x ne les divise pas, on le range à la première place libre de {15}, sinon on retourne en **, sauf si on a déjà placé f valeurs dans la liste {15}.
  - A la sortie de la boucle, {15} contient les f premiers nombres premiers.

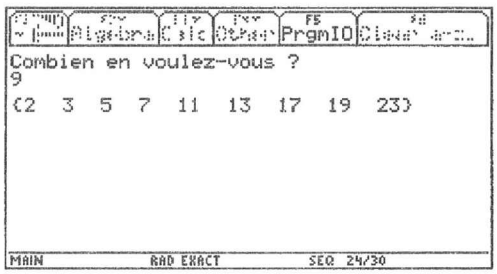
- **Programme**

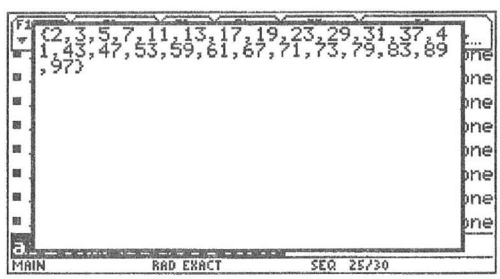






- **Exemples**





Remarque : Dans le deuxième écran des exemples, les 25 premiers nombres premiers ont été demandés. Ces nombres ont été stockés dans {15} (voir programme) puis affichés à l'écran en utilisant la commande « VAR-LINK » de la calculatrice.

V.2.6. Décomposition d'un nombre en facteurs premiers

La décomposition en facteurs premiers peut être obtenue directement avec la TI-92 en utilisant la fonction « factor » du menu Algèbre.

Ce programme permet d'obtenir un programme adaptable à d'autres types de calculatrices ou encore de comprendre comment fonctionne un algorithme de décomposition d'un nombre en facteurs premiers.

- **Problème**

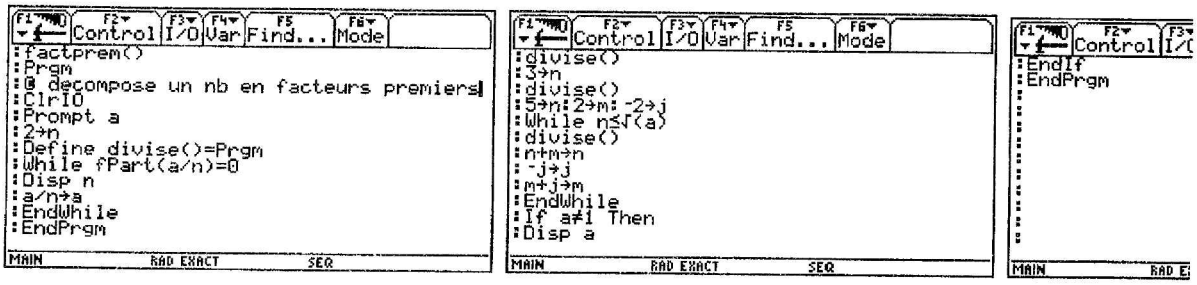
Soit un nombre entier a. Nous cherchons à déterminer sa décomposition en facteurs premiers.

- **Algorithme**
  - On initialise à p = 2.
  - Boucle ** : **tant que** $p \leq \sqrt{a}$:
  - Si a est n'est pas divisible par p, on passe au nombre premier suivant et on retourne à **.
  - Si a est divisible par p, on affiche p et on stocke a/p dans a, puis on retourne en **.
  - **Fin de boucle.**
  - A la sortie de la boucle, les facteurs premiers de a sont affichés à l'écran.

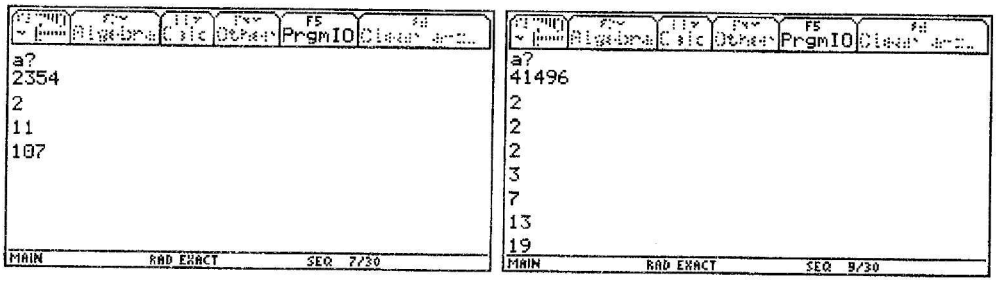
Remarque : Pour déterminer les nombres premiers p, on utilise la méthode décrite en introduction du V.2.4.

- **Programme**

Programme principal « factprem » incluant le sous-programme « divise » :



- **Exemples**



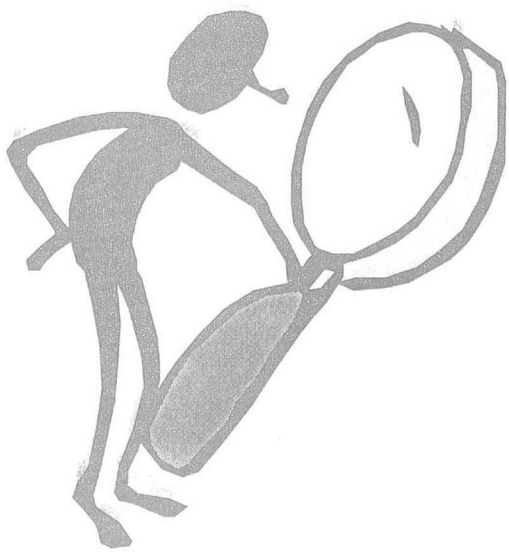
V.3. En guise de conclusion ...

Nous sommes maintenant à la fin de cette présentation de l'algorithmique. Nous espérons avoir à la fois éclairé notre lecteur sur les principes de cette science et lui avoir permis d'imaginer une utilisation possible en classe, avec les élèves.

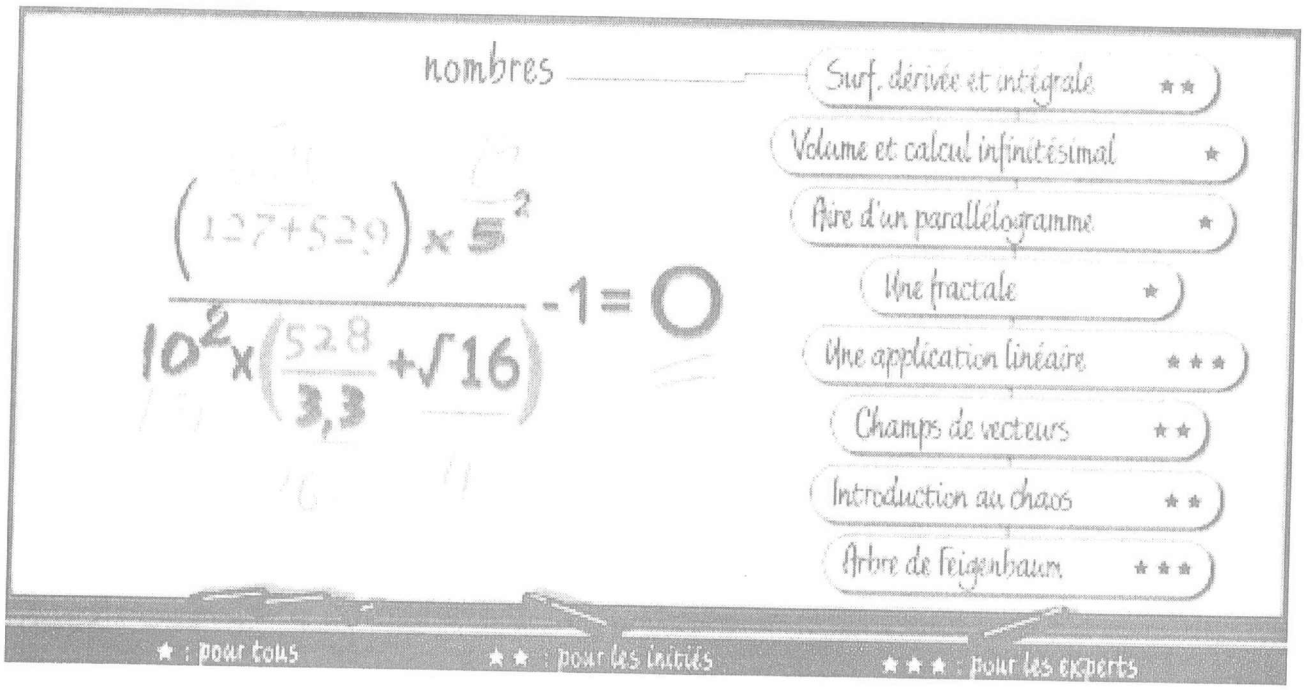
La programmation spécifique à chaque calculatrice ne devrait pas être un frein à cette démarche car d'une part, les langages des calculatrices sont très proches et d'autre part, l'usage d'un langage ou d'un autre permet simplement de traduire en instructions opérationnelles la démarche que l'on a explicité.

Voici quelques autres pistes pour d'autres programmes : PGCD et PPCM de plusieurs nombres, détermination de la primalité d'un nombre, programmation des premiers nombres parfaits ...

A vous de jouer !



VI. Des nombres sur lesquels on s'interroge



VI.1. Nombres pythagoriques

On appelle nombres pythagoriques, les entiers (> 0) qui vérifient l'équation $x^2 + y^2 = z^2$ *(appelée équation de Pythagore). Il existe au moins une solution* $(x,y,z) \in \mathbb{N}^3$ *bien connue des élèves : le triplet (3, 4, 5).*

Comment déterminer toutes les solutions ? Nous allons ci-dessous décrire trois méthodes.

VI.1.1. Méthode basée sur la parité (un peu laborieux)

A. Solutions primitives : ce sont les triplets (x, y, z) solutions où x, y et z sont premiers entre eux 2 à 2.

Si (x, y, z) est solution alors quel que soit λ entier positif non nul, (λx, λy, λz) est aussi solution.

On peut donc limiter la recherche à celle des x, y, z solutions qui sont premiers entre eux dans leur ensemble, ce qui est ici équivalent à premiers entre eux deux à deux.

- si d est un diviseur commun à x et y, x = dx' et y = dy' entraînent $d^2(x'^2 + y'^2) = z^2$, et d divise z.
- si d est un diviseur commun à x et z, x = dx' et z = dz' entraînent $d^2(z'^2 - x'^2) = y^2$, et d divise y.
- si d est un diviseur commun à y et z, ...)

Les solutions primitives permettent de trouver ensuite toutes les solutions.

B. Dans une solution primitive, x et y n'ont pas la même parité et z est impair.

- Soit z pair, alors x et y sont impairs (sinon les trois nombres ne sont pas premiers 2 à 2). Par exemple :

$x = 2n + 1$ et $y = 2m + 1$ et $x^2 + y^2 = (2n+1)^2 + (2m+1)^2 = 4n^2 + 4n + 4m^2 + 4m + 2$. Le reste de la division de z^2 par 4 serait 2, or le carré d'un nombre pair a pour reste 0 dans la division par 4, contradiction.

- Soit z impair, et x et y de même parité.

Le carré de z est aussi impair et les carrés de x et y ont aussi même parité, la somme de deux nombres de même parité est toujours paire, d'où contradiction.

On recherche les solutions primitives sous la forme, x, y, z premiers 2 à 2, x pair et y et z impairs (x et y ayant des rôles symétriques, on prendra x pair).

C. Théorème : Toutes les solutions primitives sont de la forme (à l'ordre près des deux premiers termes) : $x = 2ab$; $y = a^2 - b^2$; $z = a^2 + b^2$ où $a > b > 0$ et a et b premiers entre eux de parité différente.

On a : $x^2 = z^2 - y^2 = (z-y)(z+y)$

Comme z+y et z-y sont pairs, $z+y = 2k$ et $z-y = 2l$ où k et l sont des nombres premiers entre eux (si on a $\alpha z + \beta y = 1$ alors $(\alpha+\beta)k + (\alpha-\beta)l = 1$).

Soit $x^2 = 4\,kl$ avec k et l premiers entre eux, donc k et l sont des carrés parfaits de nombres premiers entre eux, soit $k = a^2$ et $l = b^2$ avec $a > b > 0$ (puisque $z + y = 2k > z - y = 2l$) et a et b premiers entre eux (puisque leurs carrés le sont).

Le système $\begin{cases} z+y = 2\,a^2 \\ z-y = 2\,b^2 \\ x^2 = 4\,a^2b^2 \end{cases}$ admet comme solution : $x = 2ab$ $\quad y = a^2 - b^2$ $\quad z = a^2 + b^2$.

De plus si a et b avaient la même parité, z et y seraient tous deux pairs, donc a et b de parité différente.

VI.1.2. Méthode basée sur les points rationnels du cercle unité, (plus géométrique).

> *Mais... $x^2 + y^2 = z^2$ équivaut si $z \neq 0$ à $(\frac{x}{z})^2 + (\frac{y}{z})^2 = 1$ et les solutions entières de l'équation de Pythagore correspondent géométriquement aux points à coordonnées rationnelles du cercle unité.*

Soit (C) le cercle unité (d'équation $x^2 + y^2 = 1$), A(-1 ; 0) est un point rationnel (à coordonnées rationnelles) de (C). Considérons les droites D_r d'équation $y = r(x+1)$ où r rationnel que nous appellerons droite rationnelle passant par A.

A. Il y a correspondance bijective entre les droites rationnelles passant par A et les points rationnels du cercle (C).

On associe à la droite D_r le point d'intersection (distinct de A) où elle coupe (C), ses coordonnées sont : $x = \frac{1-r^2}{1+r^2}$ et $y = \frac{2r}{1+r^2}$ (obtenu sans problème en factorisant l'équation obtenue par x+1).

Par ailleurs, la bijection réciproque est obtenue en associant à M(a,b) point rationnel du cercle (C), la droite (AM) qui est une droite rationnelle passant par A de coefficient directeur $\frac{b}{a+1}$.

Pour avoir bijection, il faut tout de même convenir que l'on associe à la tangente à (C) en A le point A lui-même.

Ainsi, en dehors de (-1 ; 0), tout point rationnel M(a, b) du cercle (C) à pour coordonnées :

$a = \frac{1-r^2}{1+r^2}$ et $b = \frac{2r}{1+r^2}$ où r rationnel. Si on pose $r = \frac{m}{n}$ (forme irréductible, donc m et n premiers entre eux) où $m \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ alors, $a = \frac{m^2-n^2}{m^2+n^2}$ et $b = \frac{2mn}{m^2+n^2}$.

B. Retour à Pythagore.

Si (x, y, z) solution non nulle de l'équation $x^2 + y^2 = z^2$, alors $z \neq 0$ et (x/z,y/z) est point rationnel du cercle (C).

Inversement, si M(a,b) est un point rationnel du cercle (C), on a : $a = \frac{m^2-n^2}{m^2+n^2}$ et $b = \frac{2mn}{m^2+n^2}$, (on fera attention si l'on ne veut pas écrire deux fois le même point à prendre m et n premiers entre eux et de parité différente, sinon s'ils sont tous les deux impairs, les formes de a et b sont simplifiables par 2 et on obtient le même point à coordonnées rationnelles du cercle).

On peut associer à M une infinité de solutions de l'équation de Pythagore. Il suffit de prendre : $x = k(m^2-n^2)$; $y = k2mn$; $z = k(m^2+n^2)$ où k est entier relatif.

En fait, on peut établir qu'il y a correspondance bijective entre l'ensemble des points rationnels du quart supérieur droit cercle (C) et l'ensemble des solutions primitives de l'équation de Pythagore ce qui donne comme condition supplémentaire $m > n > 0$ et $k = 1$.

Et on retrouve le théorème précédent.

VI.1.3. Méthode de Diophante (rapide...)

> *En fait Diophante cherche des solutions rationnelles à ses équations (en général) mais cela permet de trouver (ici) les solutions entières.*

$x^2 + y^2 = z^2$, on recherche y sous la forme $y = \alpha x - z$.

On a donc : $x^2 + (\alpha x - z)^2 = z^2$

$$x\,[(1 + \alpha^2)x - 2\,\alpha z] = 0$$

Si $x \neq 0$, on doit avoir $x = \frac{2\alpha z}{1 + \alpha^2}$ et $y = \alpha x - z = \frac{2\alpha^2 z}{1 + \alpha^2} - z = \frac{\alpha^2 - 1}{\alpha^2 + 1} z$.

Si $\alpha = \frac{p}{q}$ irréductible (p et q premiers entre eux) alors :

$x = \frac{2pq}{p^2 + q^2} z$ et $y = \frac{p^2 - q^2}{p^2 + q^2} z$.

On retrouve les solutions entières de $x^2 + y^2 = z^2$, si $z = p^2 + q^2$.

VI.2. Nombres rationnels et périodes maximales

On s'intéresse aux nombres rationnels du type n/d, où n et d sont des nombres entiers tels que n/d irréductible[30].

VI.1.1. Développement décimal.

Théorème 1

Toute fraction rationnelle n/d a un développement décimal périodique. Réciproquement, si un nombre a un développement décimal périodique, c'est un nombre rationnel n/d.

Ce développement décimal peut être fini ou infini.

- Fractions ayant un développement décimal fini

Exemple :

$$\frac{9}{16} = \frac{3^2}{2^4} = 0{,}5625$$

$$\frac{17}{250} = \frac{17}{2 \times 5^3} = 0{,}068$$

Si le développement est fini, on dit que la période est nulle.

Lorsqu'on multiplie ces nombres par une puissance de 10 assez grande, on trouve un entier.

Une fraction n/d a un développement décimal fini si son dénominateur est de la forme : $d = 2^i \times 5^j$.

Si d contient d'autres facteurs que 2 et 5, l'écriture décimale est infinie.

- Fractions à développement décimal infini

Exemple :

$$\frac{30578}{2475} = 12{,}35474747....$$

On notera : 12,35474747.... sous la forme : 12,35[47], 47 s'appelle la période du nombre.

---

30 On pourra consulter sur ce sujet l'article de Robert Ferreol « Quand les nombres font des cycles » dans Secrets de nombres, Tangente, [Ferreol,1998]. Egalement celui de Jean Paul Delahaye « Les fractions et leur mystère » dans Pour la science, [Delahaye, 1998].

- Démonstration du théorème

Sens direct :

Quand on divise par d, il n'y a que d restes possibles : de 0 à d -1.

Si la division " ne tombe pas juste ", le reste 0 n'est pas possible et la fraction rationnelle aura un développement décimal illimité et périodique.

On obtient de plus le résultat suivant :

La période de n/d, si elle n'est pas nulle, comporte au maximum d-1 chiffres.

Sens réciproque :

Soit un nombre N= $a_1a_2...a_n$, $b_1b_2...b_m$ $[c_1c_2...c_p]$ comportant n chiffres avant la virgule, m chiffres après la virgule différents des p chiffres qui se répètent ensuite.

$$N = \frac{a_1a_2...a_nb_1b_2...b_m}{10^m} + \frac{c_1c_2...c_p}{10^m(10^p - 1)}$$

On obtient cette forme en remarquant que : $N.10^m = a_1a_2...a_nb_1b_2...b_m + 0,[c_1c_2...c_p]$.

Si on pose $N' = 0,[c_1c_2...c_p]$, on a $N'.10^p = c_1c_2...c_p + N'$.

D'où le résultat précédent et N est bien une fraction de deux entiers.

- Irrationnels naturels et artificiels

Racine carrée

On sait que $\sqrt{\frac{n}{d}}$ n'est pas un rationnel dès que n et d ne sont pas des carrés parfaits.

Par exemple, $\sqrt{2}$ est un irrationnel naturel et ses décimales ne sont donc pas périodiques.

Irrationnels artificiels

Si on invente des nombres dont la partie décimale n'est pas périodique, ce ne sont pas des rationnels.

Exemples :

0,12112111211112...

0,123456789101112... : nombre de Champernowne

0,23571113.. : suite des nombres premiers

Ils sont appelés irrationnels artificiels.

VI.2.2. Périodes des nombres rationnels

On ne s'intéresse ici qu'aux nombres rationnels de dénominateur d différent de $2^i \times 5^j$ car nous avons vu qu'ils ont alors tous comme période 0.

- Quelques exemples

1/3 = 0,[3]
2/3 = 0,[6]

1/6 = 0,1[6]
5/6 = 0,8[3]

1/9 = 0,[1]
2/9 = 0,[2]
4/9 = 0,[4]
5/9 = 0,[5]
7/9 = 0,[7]
8/9 = 0,[8]

1/7 = 0,[142857]
2/7 = 0,[285714]
3/7 = 0,[428571]
4/7 = 0,[571428]
5/7 = 0,[714285]
6/7 = 0,[857142]

1/11 = 0,[09]
2/11 = 0,[18]
3/11 = 0,[27]
4/11 = 0,[36]
5/11 = 0,[45]
6/11 = 0,[54]
7/11 = 0,[63]
8/11 = 0,[72]
9/11 = 0,[81]
10/11 = 0,[90]

1/13 = 0,[076923]
2/13 = 0,[153846]
3/13 = 0,[230769]
4/13 = 0,[307692]
5/13 = 0,[384615]
6/13 = 0,[461538]
7/13 = 0,[538461]
8/13 = 0,[615384]
9/13 = 0,[692307]
10/13 = 0,[769230]
11/13 = 0,[846153]
12/13 = 0,[923076]

Théorème 2

Toutes les fractions irréductibles de même dénominateur d ont la même longueur de période.

- Démonstration

Préliminaires

Soit n/d une fraction irréductible, avec $n < d$, et $x_1x_2 \ldots x_i \ldots$la suite les chiffres successifs de sa partie décimale.

On a les égalités suivantes avec les restes successifs r_i de la division de n par d :

$10\ n = d\ x_1 + r_1$

$10\ r_1 = d\ x_2 + r_2$

.....

$10\ r_i = d\ x_{i+1} + r_{i+1}$

On en déduit :

$10^2\ n = d\ (10^1\ x_1 + x_2\ ) + r_2$..... ,puis :

$10^i\ n = d\ (10^{i-1}\ x_1 + \ldots + 10\ x_{i-1} + x_i\ ) + r_i$

On obtient r_i, reste de 10^i n par d, soit : $10^i\ n \equiv r_i\ [d]$.

Cas où n/d, fraction irréductible avec n < d

On a : $n/d = 0,b_1b_2...b_m\ [c_1c_2...c_p]$.

Pour tout chiffre après la virgule de rang $i \geq m$, on a $r_i = r_{i+p}$ puisque les quotients c_{i+1} et c_{i+p+1} de $10\ r_i$ et $10\ r_{i+p}$ par d doivent être les mêmes.

Ainsi : $10^i\ n \equiv 10^{i+p}\ n\ [d]$.

Ce qui s'écrit encore $(10^{i+p} - 10^i)n \equiv 0\ [d]$.

Comme d et n sont premiers entre eux, d divise $(10^{i+p} - 10^i)$ soit $10^{i+p} - 10^i \equiv 0\ [d]$ ou encore $10^{i+p} \equiv 10^i\ [d]$.

On obtient un résultat indépendant de n donc toutes les fractions irréductibles de même dénominateur d ont bien un développement ayant la même période.

On a un résultat supplémentaire :

m étant la plus petite valeur de i pour laquelle $10^{i+p} \equiv 10^i\ [d]$ est réalisée (sinon la période ne commencerait pas au rang m+1), **la période de toutes les fractions irréductibles de même dénominateur d commencent au même rang après la virgule.**

Cas où n/d, fraction irréductible avec n > d.

On se ramène sans problème au cas précédent puisque qu'on pourra écrire $n/d = e + n'/d$ avec e partie entière de n/d et $n' < d$.

- Exemples :

Si l'on considère les fractions irréductibles de dénominateur 7.

On a : $10^0 \equiv 1\ [7]$
$10^1 \equiv 3\ [7]$
$10^2 \equiv 2\ [7]$
$10^3 \equiv 6\ [7]$
$10^4 \equiv 4\ [7]$
$10^5 \equiv 5\ [7]$
$10^6 \equiv 1\ [7]$

Elles ont une période de 6 chiffres qui commencent au premier rang après la virgule. On peut le vérifier dans le tableau de calculs précédent.

Si l'on considère les fractions irréductibles de dénominateur 6.

On a : $10^0 \equiv 1\ [6]$
$10^1 \equiv 4\ [6]$
$10^2 \equiv 4\ [6]$

Elles ont une période de 1 chiffre qui commencent au deuxième rang après la virgule.

Si l'on considère les fractions irréductibles de dénominateur 11.

On a : $10^0 \equiv 1\ [11]$
$10^1 \equiv 10\ [11]$
$10^2 \equiv 1\ [11]$

Elles ont une période de 1 chiffre qui commencent au premier rang après la virgule.

- Résultat complémentaire

En reprenant : $10^{i+p} \equiv 10^i$ [d], si nous posons de plus que 2 et 5 ne divisent pas d, alors 10 et d sont premiers entre eux, ainsi que 10^i et d.

Ainsi comme $10^i (10^p - 1) \equiv 0$ [d], d divise $10^p - 1$, soit $10^p \equiv 1$ [d].

Théorème 3

Si d est un nombre non divisible par 2 et par 5, alors toutes les fractions irréductibles n/d (n < d) ont un développement décimal périodique commençant au premier chiffre après la virgule et la longueur de la période est le plus petit p vérifiant $10^p \equiv 1$[d].

VI.2.3. Périodes maximales

Etant donné n/d une fraction irréductible (on supposera d < n, puisque qu'on peut toujours s'y ramener en isolant la partie entière du rationnel que l'on considère), on a vu que sa période comporte au maximum d - 1 chiffres.

Problème : pour quelle valeur de d a-t-on une période maximale de d-1 chiffres ?

Comme nous avons vu que pour tout dénominateur d, les n/d ont la même longueur de période, nous observerons seulement les cas 1/d.

- Rang d'apparition d'une période maximale

Soit $1/d = 0,b_1b_2...b_m\,[c_1c_2...c_p]$, notons que si l'on a cette situation $0 \leq m \leq d - 1 - p$, puisqu'il y a seulement d-1 restes différents possibles. Ainsi, si la période de 1/d est maximale, elle commence nécessairement au premier rang après la virgule, p = d-1 et m = 0.

On a $1/d = 0,[c_1c_2...c_{d-1}]$.

Théorème 4

Si d n'est pas premier alors 1/d a une période strictement inférieure à d-1.

- Lemme :

Si 1, 2, ..., d-1 ont un inverse modulo d alors d premier.

Définition : y inverse de x modulo n $\Leftrightarrow$ $xy \equiv 1$ [d]

Remarque : si x et y inversibles, leur produit aussi.

- De façon rapide : $\mathbb{Z}/d\mathbb{Z}$ est un corps si et seulement si d est premier.

- Ou encore : $\mathbb{Z}/d\mathbb{Z}$ est un anneau intègre si et seulement si d est premier, Tout anneau intègre fini est un corps.

- En explicitant autrement :

Soit x non multiple de n alors $x \equiv 1$ ou 2 ou ... n-1 [d]

Donc x admet un inverse y modulo d et on a $xy = 1 + k\,d$ où $k \in \mathbb{Z}$.

Soit : $xy - kd = 1$ (Bezout) $\Rightarrow$ x et d premiers entre eux.

Mais alors d premier avec tout entier qu'il ne divise pas, en particulier avec tous les 1, 2, ..., d-1, donc d premier.

- Démonstration du théorème :

Nous montrerons la contraposée : **si 1/d a une période maximale alors d premier.**
Si la période est maximale, a un moment donné, on trouve forcément le nombre 1 comme reste possible parmi les d-1 premiers restes (puisque que la période commence au premier rang après la virgule).

Donc, il existe un j_1 de 1 à d-1 tel que $10^{j1} \equiv r_{j_1} \equiv 1$ [d]

$\Rightarrow$ 10 et 1 sont inversibles, ainsi que toutes les puissances de 10 dans $\mathbb{Z}/d\mathbb{Z}$.

Mais, de la même façon, il existe $j_2, j_3, \ldots j_{d-1}$ de 1 à d-1 tels que $10^{ji} \equiv i$ [d] puisque tous les nombres de 1 à d-1 sont atteints comme restes,

$\Rightarrow$ tous les i de 1 à d-1 sont inversibles

$\Rightarrow$ d premier (par application du lemme).

- La réciproque du théorème précédent est fausse.

Il suffit de prendre d = 11 pour s'en convaincre.

- Remarques

En fait on a même démontré plus :
Si 1/d à période maximale, alors d est premier et pour tout i de 1 à d-1, il existe j de 1 à d-1 tel que $10^j \equiv i$ [d].

Ce qui est d'ailleurs équivalent à : d-1 est le plus petit entier non nul tel que $10^{d-1} \equiv 1$ [d].

- Equivalence

(A) Pour tout i de 1 à d-1, il existe j de 1 à d-1 tel que $10^j \equiv i$ [d] équivaut à

(B) d-1 est le plus petit entier non nul tel que $10^{d-1} \equiv 1$ [d].

Sens direct (Non (B) $\Rightarrow$ Non (A))

S'il existe $k < d-1$ avec $10^k \equiv 1$ [d], $10^{k+1} \equiv 10$ [d], et tous les i de 1 à d-1 ne pourraient être obtenus en prenant les restes de toutes les puissances de 10 modulo d puisque on aurait (au minimum) deux valeurs de i identiques pour 10 et 10^{k+1}.

Réciproque (Non (A) $\Rightarrow$ Non (B))

S'il existe deux puissances de 10 différentes congrues au même i modulo d,

$10^j \equiv i$ [d] et $10^{j'} \equiv i$ [d] (on supposera $j < j'$)

Alors la succession des restes des puissances de 10 modulo d entre 10^j et $10^{j'}$ va se retrouver entre $10^{j'}$ et $^{10j'+(j'-j)}$. On va voir ainsi un cycle qui apparaître.
Dans ce cycle, soit 1 est atteint, mais alors il l'est pour une puissance de 10 inférieure à d-1, soit 1 n'est pas atteint et il ne pourra alors jamais être atteint.

Nous pouvons alors énoncer le théorème suivant.

Théorème 5

1/d a une période maximale si et seulement si :

- d premier

- d-1 est le plus petit entier non nul tel que $10^{d-1} \equiv 1$ [d].

- Démonstration

Sens direct

C'est le théorème précédent.

Réciproque

Notons que la deuxième condition, équivalente à pour tout i de 1 à d-1, il existe j de 1 à d-1 tel que $10^j \equiv i$ [d] exclu les nombres premiers 2 et 5 pour avoir une période maximale puisque $10 \equiv 0$ [2] et $10 \equiv 0$ [5].

Et puisque les $10^j \equiv i$ [d] pour i de 1 à d-1 représentent les « restes » de 1/d, on a bien d-1 restes différents successivement, donc bien une période de d-1 chiffres.

- Remarques :

Ce dernier théorème ne contredit pas le résultat du paragraphe II :
si d non multiple de 2 et 5, alors la période de 1/d est donnée par le plus petit entier p tel que $10^p \equiv 1$ [d].

Notons aussi que le théorème de Fermat nous assure que si d premier et 10 non divisible par d alors $10^{d-1} \equiv 1$ [d], mais il n'assure pas que d-1 soit le plus petit entier qui vérifie cela...

Théorème 6

Soit d premier différent de 2 et 5 et 3, d-1 est le plus entier non nul tel que : $10^{d-1} \equiv 1$ [d], si et seulement si d ne divise aucun des $a_k = 111...111$ (k chiffres 1) avec k diviseur propre de d-1.

- Démonstration

Sens direct (Non (B) $\Rightarrow$ Non (A))

S'il existe un diviseur propre k de d-1 (on a donc $1< k < d-1$) tel que d divise a_k.

On a : $a_k \equiv 0$ [d]

$9\, a_k \equiv 0$ [d]

$9.\ 111...111 \equiv 0$ [d]

$10^k - 1 \equiv 0$ [d]

Et donc d-1 n'est pas le plus petit non nul tel que $10^{d-1} \equiv 1$ [d].

Réciproque (Non (A) $\Rightarrow$ Non (B))

Soit k le plus petit entier non nul et strictement inférieur à d-1 tel que $10^k \equiv 1$ [d], en remontant les égalités précédentes, on aura, si d différent de 3, d qui divise a_k.
Montrons que s'il en est ainsi k est un diviseur propre de d-1.

En effet, on aura aussi $10^{2k} \equiv 1$ [d], $10^{3k} \equiv 1$ [d], ...

Et les restes modulo d des puissances de 10 vont former des cycles entre 10^k, 10^{2k}, 10^{3k}, ... Cycle qui sera d'ailleurs le même que celui entre 10^0 et 10^k. Ce cycle ne contiendra donc pas de reste 1, puisque nous avons pris le plus petit k non nul tel que $10^k \equiv 1$ [d].

Or, d étant premier différent de 2 et 5, on est sûr que $10^{d-1} \equiv 1$ [d] (Fermat).

Cette condition ne pourra être réalisée que si il existe q tel d-1 = qk, et k sera bien diviseur propre de d-1.

- Exemple

  $a_6 = 111111 = 3 \times 7 \times 11 \times 13 \times 37$,

  1/13 n'est pas à période maximale puisque 13 divise a_6 avec 6 diviseur propre de 12,

  de même pour 1/37 puisque 37 divise a_6 avec 6 diviseur propre de 36.

Conclusion : Pour déterminer si un d convient, il faut écrire tous les a_k où k diviseur propre de d-1 et vérifier si d divise ces a_k.

Pour 7 par exemple, 6 a pour seuls diviseurs propres 2 et 3, on écrit $a_2 = 11$ et $a_3 = 3 \times 37$,

comme 7 ne divise ni a_2, ni a_3, 1/7 est bien à période maximale.

- Disposition pratique : factorisation des $10^p - 1$

N'oublions pas que si d est un nombre non divisible par 2 et 5, la longueur de la période est le plus petit p vérifiant $10^p \equiv 1$ [d]. C'est vrai aussi pour les nombres premiers différents de 2 et 5, ainsi en écrivant successivement les factorisations de $10^p - 1$, la longueur de la période de 1/d, ou d premier, sera donnée par le rang de la ligne où d apparaît pour la première fois.

$10^1 - 1 = 9 = 3^2$
$10^2 - 1 = 99 = 3^2.11$
$10^3 - 1 = 999 = 3^2.37$
$10^4 - 1 = 9999 = 3^2.11.101$
$10^5 - 1 = 99999 = 3^2.41.271$
$10^6 - 1 = 999999 = 3^3.7.11.13.37$
$10^7 - 1 = 9999999 = 3^2.239.4649$
$10^8 - 1 = 99999999 = 3^2.11.73.101.137$
$10^9 - 1 = 999999999 = 3^4.37.333667$
$10^{10} - 1 = 9999999999 = 3^2.11.41.271.9091$

Les nombres premiers tels que leur inverse a une période maximale sont appelés nombres premiers longs.

Les " premiers " nombres premiers longs sont :

7 ; 17 ; 19 ; 23 ; 29 ; 47 ; 59 ; 61 ; 97 ; 109 ; 113 ; 131 ; 149 ; 167

Il y a environ 37% de nombres premiers qui sont longs ....

VI.2.4. Relation entre périodes

Nous avons vu que toute les fractions irréductibles de même dénominateur d ont la même longueur de période qui commence au même rang après la virgule, nous avons aussi vu a quelle condition 1/d est à période maximale, période qui commence alors au premier rang après la virgule. Quelle relation existe-t-il entre la période de 1/d et n/d si 1/d est à période maximale ?

Théorème 7

Si 1/d est à période maximale, alors tous les n/d (n < d) ont la même période à une permutation circulaire près.

En effet, si 1/d a une période maximale, alors pour tout i de 1 à d-1, il existe j de 1 à d-1 tel que $10^j \equiv i$ [d]. En particulier pour n < d, il existe j tel que $10^j \equiv n$ [d],

Ce qui permet d'écrire $10^k\, n \equiv 10^{k+j}$ [n].

En appelant : (r) et (x) les suites d'entiers (reste et chiffre de la période) définies précédemment pour 1/d,

et (r') et (x') les suites d'entiers correspondantes pour n/d.

La congruence précédente permet d'écrire $r'_k = r_{k+j}$ et $x'_k = x_{k+j}$.

- Un exemple pour d = 7

On a : 1/7 = 0,[142857]. Si nous voulons trouver la période de 3/7. On sait que $10 \equiv 3$ [7]. Donc k = 1, ainsi on aura pour le premier chiffre de la période de 3/7 (j = 1), $x'_1 = x_{1+1} = x_2 = 4$. Et ainsi de suite, d'où 3/7 = 0,[428571].

Comme $10^2 \equiv 2$ [7], pour 2/7, décalage de 2 chiffres : 2/7 = 0,[285714].

$10^3 \equiv 6$ [7], pour 6/7, décalage de 3 chiffres : 6/7 = 0,[857142].

$10^4 \equiv 6$ [7], pour 4/7, décalage de 4 chiffres : 4/7 = 0,[571428].

$10^5 \equiv 5$ [7], pour 5/7, décalage de 5 chiffres : 5/7 = 0,[714285].

Le nombre N = 142857 formé des chiffres de la période de 1/7 possède les mêmes propriétés de permutation.

En effet : on a : $10^6 \cdot \frac{1}{7} = N + \frac{1}{7}$ $\quad 10^6 \cdot \frac{3}{7} = 3N + \frac{3}{7}$ $\quad \Rightarrow 3N = 428571$

$10^6 \cdot \frac{2}{7} = 2N + \frac{2}{7}$ $\quad \Rightarrow 2N = 285714$ etc...

Ce qui nous donne d'autres façons de trouver la période.

Pour calculer celle de N de $\frac{1}{7}$, on calcule $N = \frac{10^6 - 1}{7}$. Ensuite si l'on veut celle de $\frac{5}{7}$, on calcule 5N, on trouve bien 714285.

- Autre exemple avec d =17

Pour trouver la période de $\frac{1}{17}$, on calcule $\frac{10^{16} - 1}{17}$, une calculatrice de base ne donnera pas le nombre exact mais avec une calculatrice symbolique on peut l'obtenir :
N = 588235294117647 (ne pas se laisser abuser par le fait qu'il n'y ait que 15 chiffres et non 16... La période commence par un 0 qui n'apparaît pas).

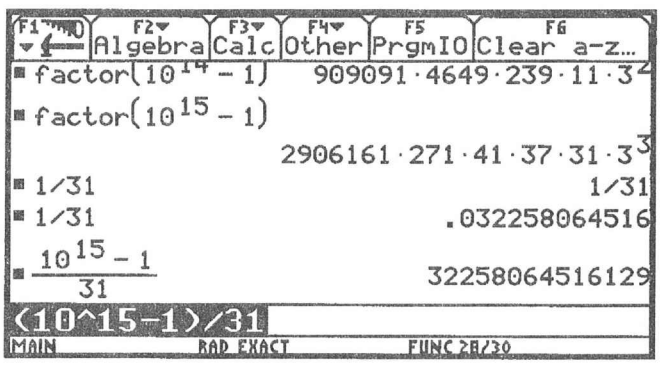
Ainsi : $\frac{1}{17}$ = 0,[0588235294117647] et on a donc 2N = 1176470588235294, soit $\frac{2}{17}$ = 0,[1176470588235294], et d'ailleurs on peut en déduire inversement que $10^{10} \equiv 2$ [17], puisque on a « décalé » de 10 chiffres, facilement vérifiable avec la calculatrice...

On peut continuer 3N = 1764705882352941 soit $\frac{3}{17}$ = 0,[1764705882352941] et $10^{11} \equiv 3$ [17], puisque on a « décalé » de 11 chiffres.

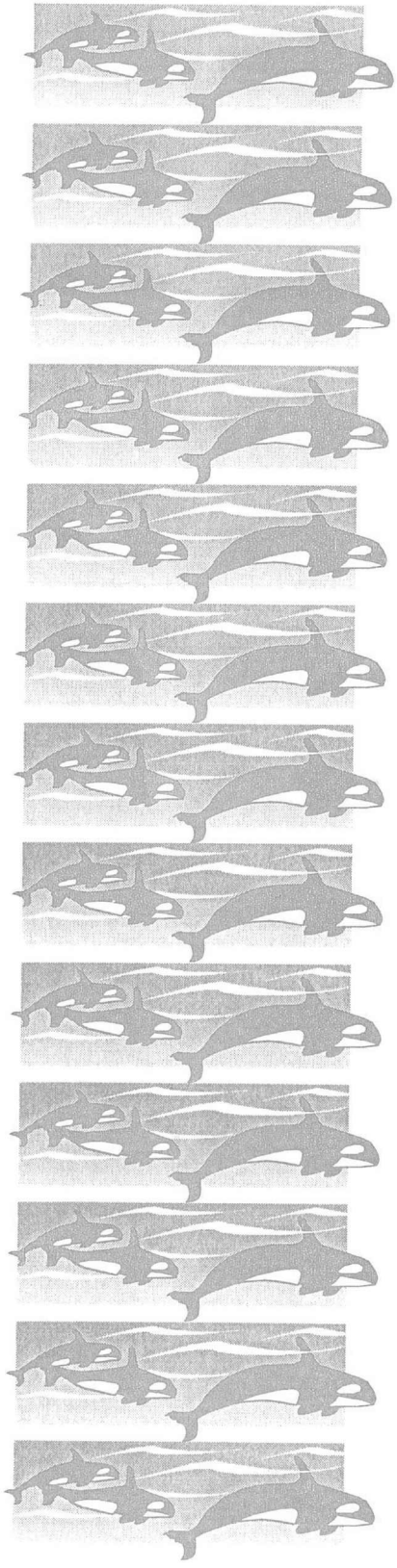
- Remarque

Si 1/d n'est pas a période maximale, d différent de 2 et 5, nous savons que le plus petit p tel que $10^p \equiv 1$ [d] représente la longueur de la période. Ainsi pour la déterminer il suffit de calculer :

$N = \frac{10^p - 1}{d}$ car les calculs précédents restent valables et pour avoir la période de n/d, on multiplie N par n. Ce qui change est qu'il n'y a pas de permutation. On peut ainsi « s'amuser »... 31 apparaît pour la première fois dans la décomposition de $10^p - 1$ en facteurs premiers lorsque p = 15. Sa période comporte donc 15 chiffres. En mode approché, il n'est pas possible de « voir » cette période puisque il y a seulement 12 chiffres significatifs, mais le calcul de $\frac{10^{15} - 1}{31}$ permet de la visualiser.



Conclusion



Nous voici arrivés au terme de ce petit voyage à l'intérieur des nombres.

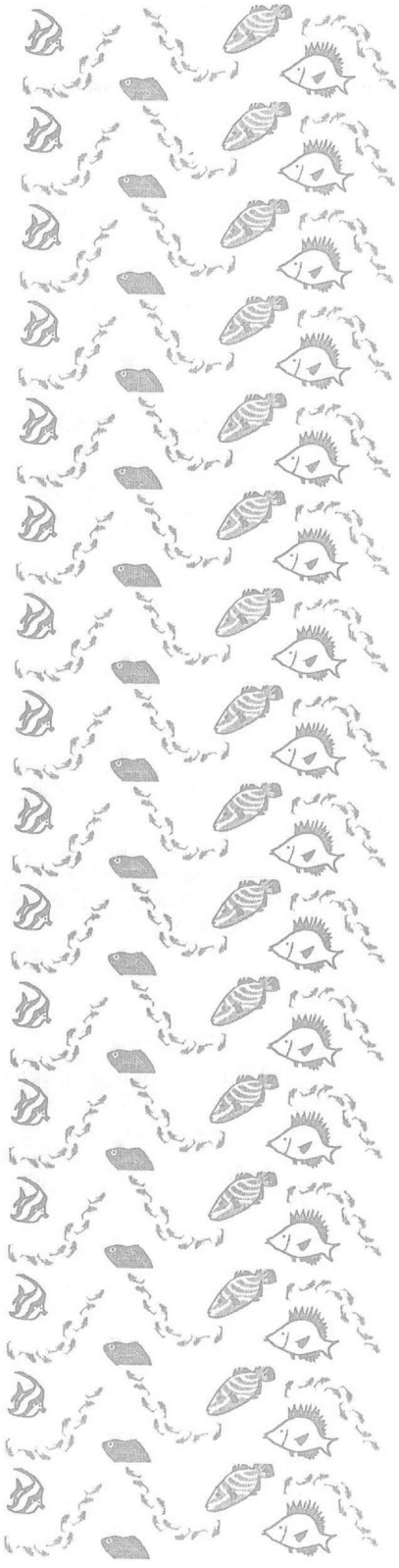
Nous espérons que le lecteur aura eu le même plaisir que nous à l'entreprendre.

Nous avions achevé notre précédent ouvrage de 1995 par un souhait, celui du retour effectif de l'arithmétique au lycée. Ce souhait a été partiellement exaucé.

Terminons cet ouvrage par un souhait complémentaire : celui que l'enseignement de l'arithmétique, élément de base de la culture mathématique, ne soit pas réservé à l'enseignement de spécialité, en terminale, mais soit généralisé, sous des formes adaptées, à toutes les sections du lycée.

Rendez-vous au prochain millénaire pour faire le point !

Les auteurs



Bibliographie

Structures algébriques

CONDAMINE & VISSIO. 1967. Tome 1- Mathématiques terminale C et T - DELAGRAVE.

D. GUIN. 1997. Algèbre. De la licence à l'agrégation. Belin.

LELONG-FERRAND & ARNAUDIES. 1978. Tome 1 - Cours de mathématiques - DUNOD.

PERRIN. 1995 - Cours d'algèbre - ELLIPSES.

MAC LANE & BIRKHOFF. 1970 - Tome 1 - Structures fondamentales - GAUTHIER-VILLARS.

Cryptographie

B. BECKETT. 1990 - Introduction aux méthodes de la Cryptologie- MASSON

D.DENNING. 1983 - Cryptography and Data Security - ADDISON-WESLEY

D.KAHN. 1966 - The Codebreakers -WEIDENFELD AND NICHOLSON.

H. KATZMAN. 1977 - The Standard Data Encryption Algorithm - PETROCELLI.

E. KRANAKIS. 1986 - Primality and Cryptography - JOHNWILEY.

La descente infinie

D. GUEDJ. 1998 - Le théorème du perroquet - ROMAN SEUIL.

H. LEHNING. 1998 - La méthode de descente infinie - In Tangente, Secrets de nombres, hors série n°6 - Editions ARCHIMEDE.

Discret et continu

R. BERNARD, C. FAURE, M. NOGUES, Y. NOUAZE, L. TROUCHE. 1995a - Des fonctions et des graphes - IREM de MONTPELLIER.

R. BERNARD, C. FAURE, M. NOGUES, Y. NOUAZE, L. TROUCHE. 1995b - Arithmétique le retour - IREM de MONTPELLIER.

R. BERNARD, C. FAURE, M. NOGUES, Y. NOUAZE, L. TROUCHE. 1998 - Pour une prise en compte des calculatrices symboliques au lycée - IREM de MONTPELLIER.

ENCYCLOPEDIE UNIVERSALIS. 1998 - Rubrique « discret et continu » -

L. TROUCHE. 1998 - Expérimenter et prouver, faire des mathématiques au lycée avec des calculatrices symboliques - IREM de MONTPELLIER.

Algorithmique et programmation

BERLIOUX et BIZARD. 1983 - Construction, preuve et évaluation des programmes - DUNOD.

ENCYCLOPEDIA UNIVERSALIS. 1998 - Rubrique « algorithmique » -

LIVERCY. 1978 - Théorie des programmes - DUNOD.

MEYER et BAUDOIN. 1984 - Méthodes de programmation - EYROLLES.

Nombres rationnels

R. FERREOL. 1998 - Quand les nombres font des cycles - IN Tangente, Secrets de nombres, hors série n°6 - Editions ARCHIMEDE.

J. P. DELAHAYE. 1998 - Les fractions et leur mystère - IN Pour la science, n°246.

TITRE
FRAGMENTS D'ARITHMETIQUE

AUTEURS
R. BERNARD - N. BRIANT - C. FAURE – J. FONTANA – M. NOGUES – L. TROUCHE

DATE
SEPTEMBRE 1999

EDITEUR
IREM DE MONTPELLIER

MOTS CLES
ARITHMETIQUE - ALGORITHMIQUE – DISCRET – CONTINU – DIVISIBILITE - NOMBRES PHYTAGORIQUES – NOMBRES RATIONNELS.

RESUME
A la suite de la réintroduction de l'arithmétique en classe de Terminale S (spécialité mathématique), notre équipe a été amenée à reprendre une réflexion déjà engagée sur cette partie des mathématiques lors de stages de formation. Nous reprenons ici les différents thèmes qui ont été abordés lors de ces stages : divisibilité, discret continu, nombres rationnels…

NOMBRE DE PAGES
112 PAGES

ISBN : 2-909916-37-5