UNIVERSITÉ LOUIS PASTEUR STRASBOURG

Institut de
Recherches sur l'
Enseignement des
Mathématiques

7, rue René Descartes
F - 67084 STRASBOURG CEDEX
Pour brochures :
Tél. : 03 88 41 64 40
Fax : 03 88 41 64 49
e-mail : bibirem@math.u-strasbg.fr
http://irem.u-strasbg.fr

POURQUOI PAS ? DES MATHÉMATIQUES

2000

Conçu à l'origine pour des étudiants sortant de terminales et se dirigeant vers des études scientifiques à dominante mathématique, ce petit livre nous semble à présent pouvoir être profitable à un public bien plus large. Avant son entrée en Deug science, le futur étudiant y apprendra à lire des mathématiques, découvrira et approfondira sous un jour nouveau des notions qu'il sera amené à manier dans ses futures études. L'étudiant plus avancé (2ième année de Deug, voire licence) trouvera l'occasion, malheureusement rare de nos jours, de lire et découvrir les mathématiques qu'il étudie sous un jour que nous espérons différent. Avoir du mal à lire seul des mathématiques, à trouver ainsi les informations souhaitées dans l'écrit est sans doute actuellement une des grandes difficultés que rencontrent les étudiants préparant le Capes.

Un des objectifs de ce petit fascicule pourrait être de vous convaincre que rien n'est plus simple que les mathématiques. Mais comme vous avez pu le constater dans votre vie de tous les jours, souvent rien n'est plus difficile à pénétrer que la vraie simplicité, tant nous sommes compliqués et tordus.

Aussi pour pénétrer ces textes qui suivent, leur simplicité cachée et suivre leur fil mathématique, il va vous falloir procéder à une lecture particulièrement active. Armés d'un stylo, de papier, nous vous conseillons d'écrire, de visualiser les définitions, les enchaînements, les petites démonstrations que nous vous proposons. Ecrivez, dessinez, couvrez de graffiti des pages blanches. Il vous faut, autant par l'écrit que par la lecture stimuler, chacun à votre manière, votre imagination. De cette façon, sans trop se rebeller, vos neurones pourront intégrer progressivement les emboîtements de notions constituant ces petits textes.

La présente brochure comprend quatre parties qui peuvent être lues indépendamment et développent les thèmes suivants :

- applications et fonctions vues à travers divers domaines,
- lecture accompagnée d'un texte mathématique sur les suites récurrentes et application logistique
- l'arithmétique,
- la notion d'espace vectoriel.

Entre chacune de ces parties vous trouverez quelques récréations logiques .

Ces chapitres qui diffèrent les uns des autres non seulement par le contenu thématique mais aussi par le style et le niveau d'approfondissement apportés, devraient vous faire découvrir des objets, voire vous familiariser, avec des notions incontournables au cours d'études nécessitant des mathématiques.

Nous espérons par ce petit écrit permettre à celui qui le souhaite d'augmenter sa capacité à lire des mathématiques d'une quantité epsilon strictement positive, aussi petite soit-elle.

LOGIQUE DE TOUS LES JOURS ET LOGIQUE MATHEMATIQUE

Le langage courant se sert souvent des mêmes mots que les mathématiciens (à moins que ce ne soit l'inverse...), mais la logique de tous les jours ne procède pas de la même rationalité que le raisonnement mathématique. Il importe de bien sentir ces nuances pour traquer efficacement les erreurs « dites » de logique. En voici quelques exemples.

C'est l'exception qui confirme la règle !
En mathématiques un seul contre-exemple suffit à montrer qu'une proposition est fausse !

Fromage ou dessert.
Boire ou conduire, il faut choisir !
La conjonction « ou » a souvent un sens exclusif (=« ou bien »). En logique le connecteur ou est inclusif c'est à dire qu'il signifie l'un ou l'autre **ou les deux**.
Une logicienne vient d'accoucher. A son mari qui, au téléphone, lui demande si c'est une fille ou un garçon, elle répond oui.

Si tu es sage alors tu auras du chocolat.
Une telle phrase, prononcée par un papa ou une maman, signifie implicitement que si l'enfant n'est pas sage il n'aura pas de chocolat c'est à dire que la réciproque de l'implication énoncée est vraie également. En mathématique, une implication n'est pas une équivalence et on ne peut sous-entendre une réciproque.

P'têt ben qu'oui, p'têt ben qu'non...
En mathématiques une assertion est vraie ou fausse c'est le principe du **tiers exclu**.

C'est faux, c'est l'inverse, c'est le contraire, c'est tout le contraire
En logique il y a une seule négation, le vrai c'est du non faux.

C'est vérifié dans beaucoup de cas donc c'est vrai
Des exemples (non exhaustifs) ne peuvent démontrer une assertion générale

Il y a toujours un médecin de garde à l'hôpital
Il y a un médecin qui est toujours de garde à l'hôpital
Ces deux phrases nous rappellent bien qu'il ne faut pas permuter des quantificateurs distincts. Elles se reformulent ainsi :
Quel que soit le jour il existe un médecin qui est de garde à l'hôpital.
Il existe un médecin qui, quel que soit le jour, est de garde à l'hôpital.

On affirme tout et le contraire de tout.
La phrase sous-entend bien le peu de crédit que l'on peut accorder à ce qui est dit.
L'ambition première des mathématiciens est d'éviter les absurdités. Le principe du raisonnement par l'absurde est le refus des contradictions.

Des arguments convergents renforcent la conviction.
Une seule démonstration suffit, deux démonstrations ne rendent pas un énoncé plus vrai.

PETITES ENIGMES PLAISANTES

QUE DE MENTEURS

A) Quatre amis (?) visitent un musée avec seulement trois billets d'entrée. Ils rencontrent un gardien qui veut savoir lequel n'a pas payé son entrée.
« Ce n'est pas moi » dit Paul.
« C'est Jean » dit Jacques.
« C'est Pierre » dit Jean .
« Jacques a tort » dit Pierre.
Un seul d'entre eux ment ! Quel est le resquilleur ?
(Rallye du Centre 1988)

B) André, Bernard, Claudine, Dominique, Laure et Sonia sont les six concurrents classés en tête d'une même épreuve. A l'issue de la course, chacun d'eux a fait une déclaration.
André : « Dominique est arrivé après Laure .»
Bernard : « André est arrivé après Laure. »
Claudine : « Sonia est arrivée après Laure »
Dominique : « Bernard est arrivé avant moi. »
Laure : « Claudine est arrivée après Sonia. »
Sonia : « Je suis arrivée troisième. »
Les concurrent(e)s arrivé(e)s après Laure ont tou(te)s menti. Les autres ont dit la vérité.
Retrouvez le classement de l'épreuve.
(1/2 finale FFJM 1991)

DEMONSTRATION PAR RECURRENCE.

Trouvez l'erreur !

Dans une boîte de crayons de couleurs, tous les crayons sont forcément de la même couleur. En effet notons n le nombre de crayons de la boîte et démontrons le résultat par récurrence :
1. si n=1 la boîte ne contient qu'un seul crayon et l'assertion est vraie.
2. Supposons l'assertion vraie pour toutes les boîtes de n crayons et montrons que l'assertion est vraie pour une boîte de n+1 crayons. Soit $c_1,..,c_n,c_{n+1}$ les crayons. Je prends les n crayons $c_2,..,c_n,c_{n+1}$ et je les range dans une même boîte. D'après l'hypothèse de récurrence ils sont de la même couleur. Je prends alors les n crayons $c_1,..,c_{n-1},c_n$. D'après l'hypothèse de récurrence ils sont de la même couleur. Les crayons sont donc nécessairement de la même couleur.

A CHACUN SON SPORT

Albert, Benoît et Charles pratiquent chacun un et un seul des sports suivants : pêche, karting et roller. On sait que :
1. Si Albert fait de la pêche alors c'est Benoît qui fait du karting.
2. Si Albert fait du karting alors c'est Benoît qui fait du roller.
3. Si Benoît ne fait pas de pêche alors Charles fait du karting.
4. Si Charles fait du roller alors Albert fait du karting.

Peut-on retrouver la spécialité de chacun ?

QUE DE MENTEURS.

A) Il n'y a que 4 cas possibles qu'il suffit d'examiner tous les quatre pour démontrer qu'il n'y a qu'une solution :
1) si le resquilleur est Paul :
Paul ment et Jacques ment ce qui fait déjà trop de menteurs !
2) si le resquilleur est Jean :
Paul dit vrai, Jacques dit vrai, Jean ment et Pierre ment ce qui fait encore trop de menteurs !
3) si le resquilleur est Jacques :
Paul dit vrai, Jacques ment, Jean ment ce qui fait encore trop de menteurs !
4) si le resquilleur est Pierre :
Paul dit vrai, Jacques ment, Jean dit vrai, Pierre dit vrai ! C'est l'unique possibilité.

B)
Il y a, pour six concurrents, 6!=720 classements possibles qu'il est hors de question d'examiner tous. Il faut trouver plus économique.

On peut, par exemple raisonner sur le rang de Laure qui sépare les menteurs des autres :

Si Laure était première, tous (sauf Laure) auraient menti, en particulier André ce qui signifierait que Dominique est avant Laure ce qui est impossible. Laure n'est donc pas première.
Si Laure était seconde, il y a au moins deux menteurs parmi A, B et C ce qui placerait deux concurrents avant Laure ce qui est impossible. Laure n'est pas seconde...etc.

Une autre procédure serait d'envisager les deux cas : Sonia ment - Sonia ne ment pas. Cette entrée est assez efficace dans la mesure où Sonia donne un renseignement très précis la concernant elle même.

L'ordre d'arrivée :

Bernard Dominique Sonia Laure Claudine André

est conforme aux affirmations de l'énoncé, mais est-ce la seule solution ?

Autour de la notion d'application

Le but de ce petit paragraphe est de revenir sur des notions déjà rencontrées pour en préciser le sens, se familiariser avec elles, se rendre compte combien elles sont naturelles et simples. Ces notions qui tournent autour des mots "applications, fonctions, injective, surjective, bijective, vous poursuivront tout au long de votre cursus en mathématique, tant en algèbre qu'en analyse.

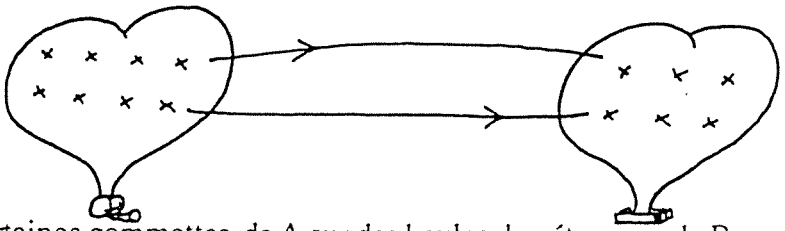
applications, fonctions

Partons d'un sac de p gommettes aimantées de couleurs différentes , appelons A ce sac et $g_1, g_2, g_3, \ldots\ldots, g_p$ les gommettes qu'il contient.

Par ailleurs (ou un peu à coté!), considérons un ensemble de q boules de pétanques distinctes, appelons B cet ensemble et $b_1, b_2, b_3, \ldots\ldots, b_q$ les boules de pétanques de B.

Et bien sûr, comme on s'y attend à ce stade de cette ridicule histoire, on plonge sa main dans le sac de gommettes et on va coller des gommettes sur des boules de pétanques. (J'espère pour vous que vous les avez choisies métalliques sinon cette histoire ne tient pas !)

L' ensemble "de départ " A (les gommettes) et l'ensemble "d'arrivée" B (les boules de pétanques) étant des ensembles finis (c'est à dire n'ayant qu'un nombre fini d'éléments) Le dessin précédent peut être schématisé de la façon suivante :



Aller coller certaines gommettes de A sur des boules de pétanques de B donne ce que l'on appelle une fonction de A dans B, on la note f et on la représente alors classiquement par une flèche :

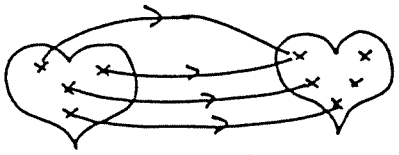
$f : A \to B$ ou $A \xrightarrow{f} B$

$f(g_i)$ désigne la boule sur laquelle se trouve collée la gommette g_i, on dira que $f(g_i)$ est l'image de g_i pour la fonction f. On utilise aussi la notation $f : g_i \to f(g_i)$, sans doute pour signifier que g_i est "transporté" par la fonction f. On appelle image de f, notée f(A) le sous ensemble de l'ensemble d'arrivé B constitué des boules ayant reçu une ou plusieurs gommettes.

Il est ainsi clair que la fonction f est définie par la donnée des images des éléments de A envoyés dans B. (Dans cette phrase on a perdu les gommettes et les boules, comme dans les notations introduites précédemment!, mais qu'importe.)
Remarquez bien que un élément de A ne peut aller que sur un élément de B. Cela peut vous paraître évident avec les gommettes, et pourtant!

Tout ce qui précède nous donne une idée intuitive de ce qu'est une fonction entre deux ensembles A et B.
Partant de cette notion intuitive de fonction, examinons

quelles sont les différents types de situations qui peuvent se produire :

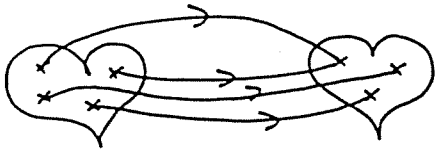


• Toutes les gommettes
sont utilisées et donc envoyées sur une boule,
la fonction est alors appelée une application :

Une fonction d'un ensemble A dans un ensemble B qui envoie chaque élément de A sur un élément de B est appelé une application de A dans B.

> Dans cette phrase on a jeté les gommettes et les boules qui ne servent qu'à illustrer le propos et on considère la notion d'application entre des ensembles A et B. Les définitions sont mises en italique.

Restons à présent parmi les fonctions qui sont des applications :

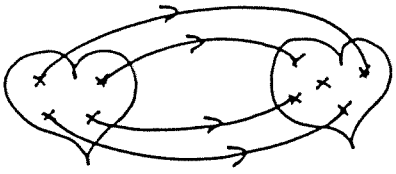


• Toutes les boules
ont reçu au moins une gommette,
l'application est alors dite surjective.

Une application de A dans B est dite surjective si tous les éléments de B sont dans l'image de l'application f c'est à dire f(A) = B.

autrement dit :
Pour tout élément y appartenant à l'ensemble B il existe un élément x appartenant à l'ensemble A tel que f(x)=y.

ce qui en langage symbolique nous donne :
$\forall y \in B \; \exists x \in A$ *tel que* $f(x) = y$



• Toute boule qui a reçu
une gommette, n'en a reçu qu'une,
l'application est alors dite injective.

Une application de A dans B est dite injective si deux éléments distincts de A sont envoyés sur deux éléments distincts de B.

autrement dit :
Pour tout x_1, x_2 appartenant à A tels que x_1 est différent de x_2,
on a $f(x_1)$ différent de $f(x_2)$.

ce qui en langage symbolique nous donne :
$\forall x_1, x_2 \in A$ *tels que* $x_1 \neq x_2$, *on a* $f(x_1) \neq f(x_2)$

ou encore (contraposé de la proposition précédente)*
$f(x_1)$ égal à $f(x_2)$ implique x_1 égal x_2.
ce qui en langage symbolique nous donne :
$\forall x_1, x_2 \in A,\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

• Chaque boule est munie
d'une (splendide) gommette et d'une seule,
l'application est alors dite bijective.

Une application de A dans B est dite bijective si elle est injective et surjective.

On a vu dans ce qui précède (en particulier dans les dessins précédents) que les gommettes et les boules n'ont bien sur rien à voir dans cette histoire.
Vous pouvez habiller A et B, des ensembles finis, avec ce que vous voulez, numéroter les élément de A, puis ceux de B, vos applications et leurs propriétés pourront être représentées de la même façon par les dessins précédents.

Pour pouvoir faire des dessins on a pris des ensembles A et B n'ayant qu'un nombre fini d'éléments, mais il est clair (?) que les définitions données à chaque fois après les dessins (en italique) ne dépendent pas du fait que les ensembles A et B soient finis.

Avant de rejoindre les nombreux exemples de fonctions, d'applications que vous connaissez et avez maniés de longue date, restons si vous le voulez bien un instant encore sur cette notion d'application dans le cas particulier des ensembles finis :
A à p éléments (ce que vous voulez, des pommes, des clefs, des poires, des montagnes .....ou tout simplement les éléments de A numérotés de 1 à p) et B à q éléments.

Ainsi si A={1, 2, 3, ..., p} et B={1, 2, 3, ..., q} (quelqu'en soit l'habillage), une application f : A $\rightarrow$B est déterminée par la donnée des images des éléments 1, 2, ..., p.
Une façon possible et pratique de se donner et de représenter une telle application est la suivante :

$$\begin{pmatrix} 1\ 2\ 3\ 4\ \ .....i.....p \\ 7\ 2\ 7\ q\ .....f(i).....7 \end{pmatrix}$$

on écrit l'image par f des chiffres de la première ligne sur la seconde, dans cet exemple f(1)=7, f(2)=2, f(3)=7, .., f(i), .., f(p)=7, i désignant ainsi classiquement un entier quelconque, ici pris entre 1 et p.

Par exemple, avec cette notation listons toutes les applications possibles entre deux ensembles A et B ayant chacun deux éléments :

$$\begin{pmatrix} 1\ 2 \\ 1\ 1 \end{pmatrix} \quad \begin{pmatrix} 1\ 2 \\ 1\ 2 \end{pmatrix} \quad \begin{pmatrix} 1\ 2 \\ 2\ 2 \end{pmatrix} \quad \begin{pmatrix} 1\ 2 \\ 2\ 1 \end{pmatrix}$$ on en a quatre

---

* {P implique Q} est équivalent à {(non Q) implique (non P)}
cela vous rapelle-t-il quelque chose? (allez voir page ?)

parmi celles-ci, cherchons celles qui sont bijectives :

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Faite de même, poursuivez le jeu, pour A ayant 3 éléments, B en ayant 2, donnez toutes les applications entre A et B. Pour A et B ayant 3 éléments chacun quelles sont toutes les applications possibles, quelles sont celles qui sont bijectives et pour 4 éléments...?

Quelques propriétés dans le cas particulier d'applications entre des ensembles finis.

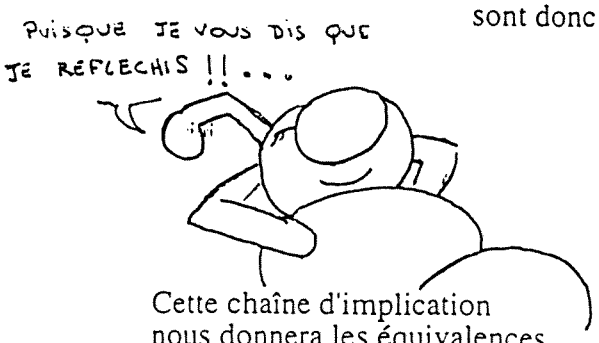
Soient A et B deux ensembles finis ayant un même nombre d'éléments et f : A → B une application. Les propriétés suivantes sont équivalentes :

(a) f est une application injective
(b) f est une application surjective
(c) f est une application bijective

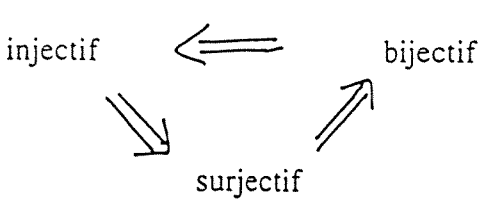
C'est écrit en italique et pourtant ce n'est de tout évidence pas une définition.
C'est une proposition. Il nous (ou vous) faut donc la démontrer.
Avant d'en faire la démonstration, essayons de nous convaincre de la véracité de ces affirmations (et si elles étaient fausses, peut être allons nous rencontrer un contre exemple !).

Revenons à un ensemble A de p gommettes et un ensemble B de p boules de pétanques.

f est injective	⇒	f est surjective	⇒	f est bijective	⇒	f est injective
deux gommettes distinctes vont sur deux boules distinctes	⇒	il y a même nombre de boules que de gommettes toutes les boules sont donc atteintes	⇒	Toutes les boules sont atteintes. Il y a même nombre de boules que de gommettes. Deux gommettes distinctes vont donc sur deux boules distinctes. On a surjectif et injectif.	⇒	bien sûr!



Cette chaîne d'implication nous donnera les équivalences souhaitées par le parcours circulaire :



On "voit" clairement la nécessité de l'hypothèse "même nombre de boules que de gommettes" :
Il manque une gommette, il est alors impossible d'atteindre toutes les boules.
Il manque une boule, qui empêchera deux gommettes d'aller sur la même boule.

Bien, à présent il nous (vous) faut faire la démonstration de cette proposition, sans boules ni gommettes.

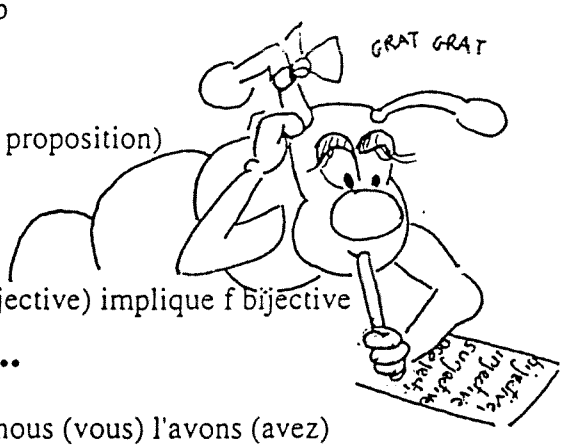
.....

Démonstration :
On va en fait démontrer que :
"f injective est équivalent à f surjective"

f est injective ainsi
pour tout x_i, x_j , $x_i \neq x_j$ appartenant à A on a $f(x_i) \neq f(x_j)$.
L'ensemble A ayant p éléments, son image f(A) dans B aura p éléments
Or B ayant p éléments, on a donc f(A)=B,
f est donc surjective

Il nous faut à présent montrer que f surjective implique f injective,
il est plus simple de montrer ici que si f n'est pas injective alors f n'est pas surjective*

si f n'est pas injective
il existe x_i et x_j , $x_i \neq x_j$ appartenant à A tels que $f(x_i) = f(x_j)$
f(A) a un nombre d'éléments strictement inférieur p
f(A) est strictement inclue dans B
donc f n'est pas surjective



Vous venez de montrer que (sous l'hypothèse de la proposition)
f injective est équivalent à f surjective.

Ceci nous permet de conclure :

f injective implique f surjective (équivalent ici à injective) implique f bijective

.....

Voilà, après avoir raconté cette petite proposition, nous (vous) l'avons (avez) démontrée.
Il en est très souvent ainsi en mathématiques, il faut d'abord, au moyen de dessins, du langage naturel, se convaincre, comprendre une situation, la décortiquer avant de pouvoir la démontrer. Ce travail préliminaire ne devant pas être confondu avec la démonstration elle même.

Venons en à présent à ce que vous connaissez et maniez depuis longtemps, les fonctions de R dans R et plus particulièrement celles qui sont définies par une formule par exemple :

$$f(x) = \sqrt{1-x^2},\ f(x) = x^2,\ f(x) = \sqrt{x},\ f(x) = \cos(x),\ f(x) = \frac{1}{1+x}$$

Vous avez bien sûr, dans vos neurones un énorme bestiaire de telles objets mathématiques. De plus, vous savez faire plein de choses avec ces bestioles, les étudier sous toutes les coutures (domaine de définitions, dérivées, tableau de variation, graphe .....).

En particulier revenons sur une propriété des fonctions continues dérivables que vous avez démontrée dans votre cursus précédent :
"Une fonction continue, dérivable, monotone sur un intervalle est bijective sur son image"

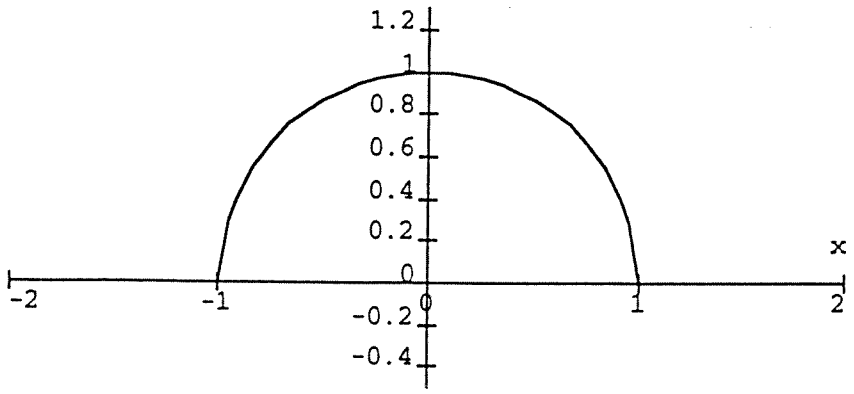
---

* {P implique Q} est équivalent à {(non Q) implique (non P)}

Pour être bijective, allez vous me dire, il faut qu'elle soit injective et surjective :
- "sur son image" nous donne naturellement la surjectivité
- "monotone" implique l'injectivité

Pour illustrer ceci suivons un instant l'étude de $f(x) = \sqrt{1-x^2}$ (que vous venez certainement de faire sur votre papier ou de faire faire à votre calculatrice!)

Commençons à l'envers, par recopier le graphe que vous avez tracé (ou fait tracer par votre calculette) :



• Cette fonction n'est pas définie sur tout **R**, il faut se restreindre à l'intervalle [-1 1]. C'est une **application**

$$[-1\ \ 1] \xrightarrow{f} \mathbf{R}$$

(aucun point en dehors de cet intervalle n'est transporté)

Notez que nous appelons toujours f cette application, restriction de la fonction f à l'intervalle [-1 1]. C'est un "abus de langage" que nous allons utiliser allègrement.

• Cette application n'atteint pas tous les points de **R**,
elle n'est **pas surjective**
cependant elle nous définit une nouvelle application que nous notons toujours f :

$$[-1\ \ 1] \xrightarrow{f} [0\ \ 1]$$

qui elle est **surjective.**
(on a restreint l'ensemble d'arrivée aux points atteints par f)

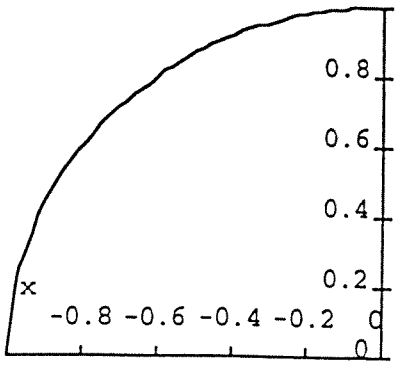
On reste fidèle au principe de "l'abus de langage précédent".

• Cette dernière application n'est **pas injective**, f(-1) = f(1) = 0, plus généralement pour tout x de [-1 1], f(-x) = f(x), c'est une fonction paire, son graphe est symétrique par rapport à l'axe des y.
Cependant nous pouvons "réduire" son ensemble de départ pour la rendre **injective** soit à [-1 0], soit à [0 1], et nous
noterons toujours f cette nouvelle application.) :

$$[-1\ \ 0] \xrightarrow{f} [0\ \ 1] \text{ ou } [0\ \ 1] \xrightarrow{f} [0\ \ 1]$$

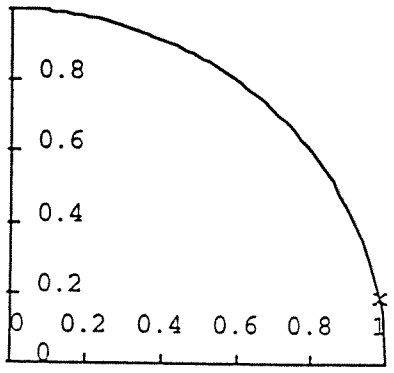
f est à présent **injective et surjective** donc **bijective.**

En ayant "abusé" de plus en plus, on a pour f les deux possibilités d'applications bijectives suivantes :



$[-1\ 0] \xrightarrow{f} [0\ 1]$

ou



$[0\ 1] \xrightarrow{f} [0\ 1]$

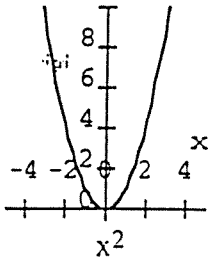
En fait comme vous l'aviez vu sur l'étude que vous aviez faite de cette fonction avant d'en tracer le graphe(?), de [-1 0] dans [0 1] elle est strictement monotone croissante et surjective donc elle est bijective. De même de [0 1] dans [0 1] elle est strictement monotone décroissante donc bijective.

Ainsi pour les fonctions de **R** dans **R** l'étude des variations nous fournit un outil permettant de déterminer les intervalles de l'ensemble de départ sur lesquels l'application est injective.

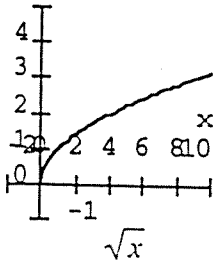
Faites de même, réduisez ensembles de départ et d'arrivée pour que les fonctions de **R** dans **R** suivantes "deviennent" des applications bijectives :

$$f(x) = x^2,\ f(x) = \sqrt{x}\ ,\ f(x) = \cos(x),\ f(x) = \tan(x)\ ,\ f(x) = \frac{1}{1+x}$$

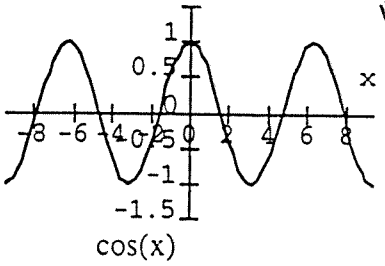
Ce qui sur un dessin vous donne:



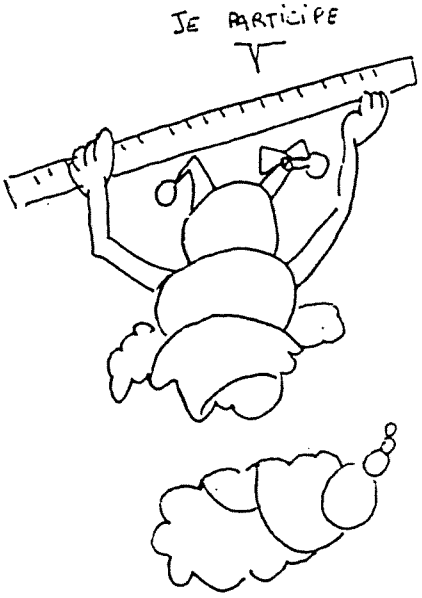
x^2

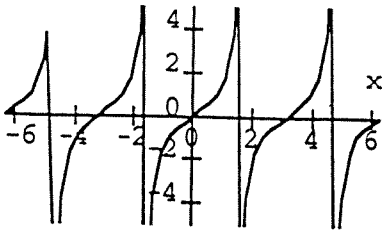


$\sqrt{x}$

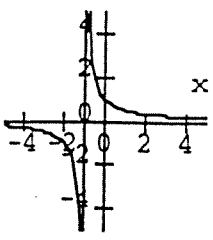


cos(x)



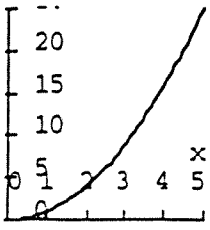


tan(x)

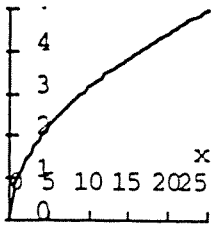


1/(1+x)

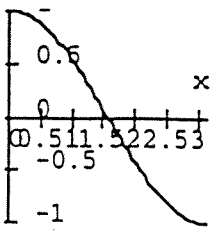
les mêmes "rendues" bijectives par restriction des intervalles de départ et arrivée, portant "abusivement" les mêmes noms:



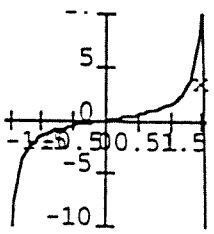
x^2



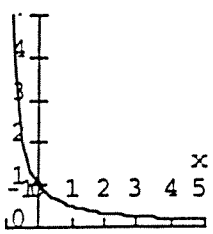
$\sqrt{x}$



cos(x)



tan(x)



1/(1+x)

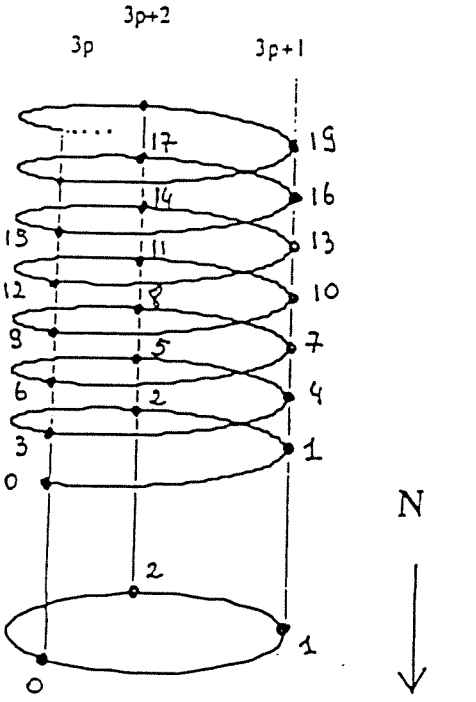
Il n'y a bien sûr pas que les fonctions de R dans R comme fonctions entre ensembles non forcément finis. Vous aurez l'occasion d'en rencontrer de toutes sortes. En voici deux exemples :

• f : N $\rightarrow$ {0, 1, 2}, une application des entiers naturels dans un ensemble à trois éléments définie de la façon suivante :

Soit n un entier, on le divise par 3 et on considère le reste de cette division que l'on note r_n

Ainsi, - si n = 3p, $r_n = 0$
- si n = 3p+1, $r_n = 1$
- si n = 3p+2, $r_n = 2$

f est définie par $n \mapsto r_n$ sur un dessin :



Dans ce dessin on a "enroulé" R^+ au dessus d'un cercle
N est un ensemble de points dans R et {0, 1, 2} des points sur le cercle.
La projection verticale nous permet de "visualiser" l'application f.

Cette application est **surjective** et **non injective**

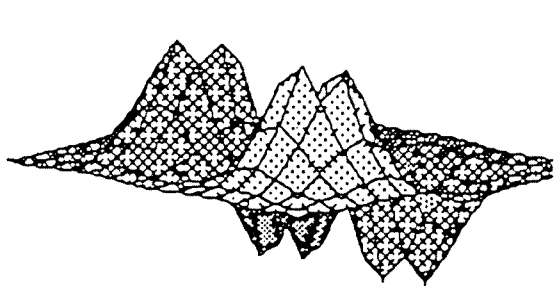
• f : R^2 $\rightarrow$ R, à tout point (x,y) du plan R^2 on associe un nombre réel z = f(x, y).

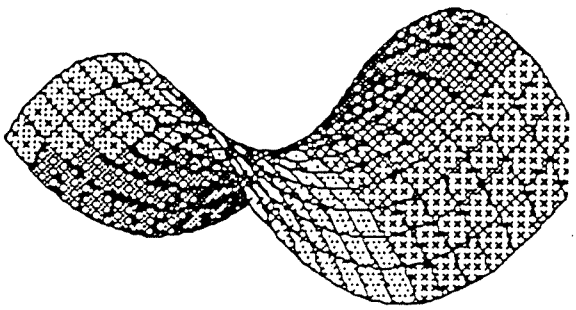
La valeur de ce nombre z qui dépend des valeurs des variables x et y peut comme dans le cas d'une variable être donné par une formule.
Par exemple :

$$f_1(x,y) = xy^2\exp[-(x^2+y^2)/4], \qquad f_2(x,y) = x^2-y^2$$

ainsi $f_1 : R^2 \rightarrow R$ est définie par $(x,y) \mapsto z = xy^2\exp[-(x^2+y^2)/4]$
et $f_2 : R^2 \rightarrow R$ est définie par $(x,y) \mapsto z = x^2-y^2$

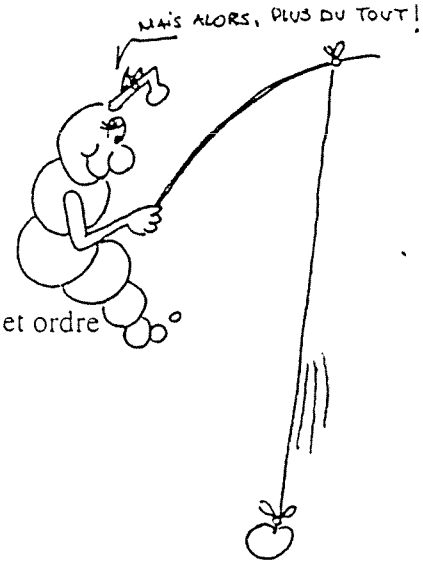
Pour les fonctions de $\mathbf{R}^2 \to \mathbf{R}$ on a un graphe qui va se trouver dans l'espace $\mathbf{R}^3$.
Ce graphe est une "surface" obtenue dans $\mathbf{R}^3$ en prenant au-dessus de chaque point (x,y) du plan xOy un point à la "hauteur" $z = f(x,y)$.
Pour les exemples f_1 et f_2 on obtient les surfaces suivantes :





$f_1(x,y) = xy^2\exp(-(x^2+y^2)/4)$

$z = x^2-y^2$



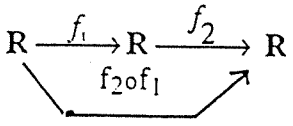
Composition, application réciproque

Composons des fonctions de R dans R :

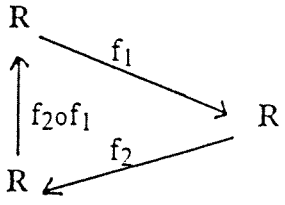
$f_1 : \mathbf{R} \to \mathbf{R}$ et $f_2 : \mathbf{R} \to \mathbf{R}$ nous donnent, prises dans cet ordre

$f_2 \circ f_1 : \mathbf{R} \to \mathbf{R}$, $x \mapsto f_2(f_1(x))$

Ce que l'on représentera parfois par les "diagrammes" suivants :



ou



Dans cet esprit, on suit les flèches représentant les fonctions pour "transporter" les éléments; un élément x de R est d'abord "transporté" sur $f_1(x)$, puis $f_1(x)$ pris en charge par f_2 est tranquillement transporté sur $f_2(f_1(x))$.

Notez bien que dans la notation en flèches $\mathbf{R} \xrightarrow{f_1} \mathbf{R} \xrightarrow{f_2} \mathbf{R}$, on a d'abord f_1, alors que dans l'écriture du résultat $f_2(f_1(x))$, comme dans celle de la composition $f_2 \circ f_1$, c'est f_2 que l'on est amené a écrire en premier.

Prenons quelques exemples dans le bestiaire des fonctions que vous connaissez, les fonctions de R dans R définies par une formule:

$$f_1(x) = \frac{1}{x} \text{ et } f_2(x) = \sin(x) \text{ alors } f_2 \circ f_1(x) = \sin(\frac{1}{x})$$

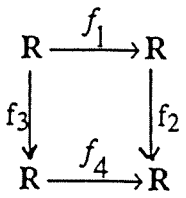
(qui n'a bien sur rien a voir avec $f_1 \circ f_2(x) = \dfrac{1}{\sin(x)}$)

On ne se soucie pas des ensembles de définition, si nécessaire, on enlèvera à R ce qu'il faut, là où il le faut, pour avoir des applications qui se composent.

A présent prenez $f_1(x) = 2x$, $f_2(x) = \exp(x) = f_3(x)$, $f_4(x) = x^2$ et vérifiez que vous avez pour ces fonctions la relation:

$$f_2 \circ f_1 = f_4 \circ f_3 \quad \text{car} \quad \exp(2x) = (\exp(x))^2$$

Sur un diagramme:



quand on transporte x par un coté ou par l'autre, en suivant les flèches de ce diagramme, on arrive sur le même élément $f_2 \circ f_1(x) = f_4 \circ f_3(x)$

une telle situation sera appelée " diagramme commutatif"

Revenons à l'exemple de l'application $f : \mathbf{N} \to \{0, 1, 2\}$ définie par les restes de la division par trois qui nous avait donné la belle spirale précédente.

Poursuivons le jeux et considérons les quatre applications suivantes :

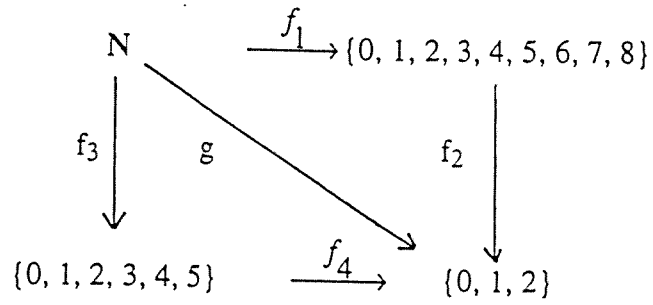
$f_1 : \mathbf{N} \to \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$,
$n \to$ le reste de la division de n par 9

$f_2 : \{0, 1, 2, 3, 4, 5, 6, 7, 8\} \to \{0, 1, 2,\}$
$n \to$ le reste de la division de n par 3

$f_3 : \mathbf{N} \to \{0, 1, 2, 3, 4, 5\}$,
$n \to$ le reste de la division de n par 6

$f_4 : \{0, 1, 2, 3, 4, 5\} \to \{0, 1, 2,\}$
$n \to$ le reste de la division de n par 3

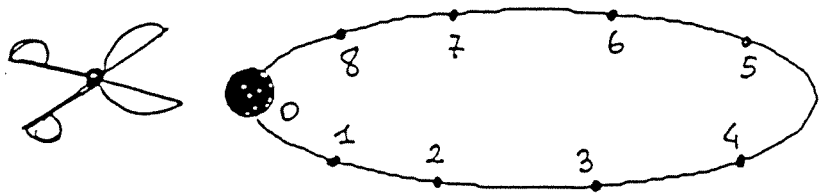
Vous savez faire des divisions dans les entiers, vérifiez que le diagramme



est commutatif c'est à dire que $f_2 \circ f_1 = f_4 \circ f_3 = g$

L'application g est elle même définie par les restes de la division par 3.

Tout cela pour faire deux pages de petits dessins:



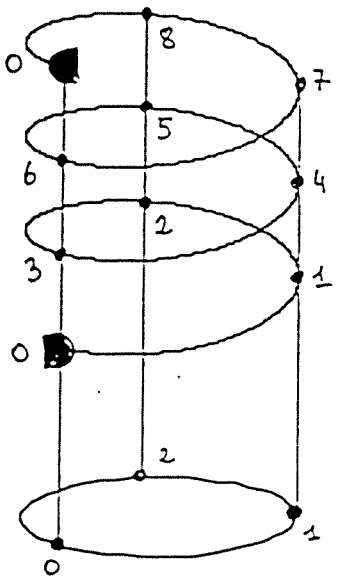
Voila un beau cercle avec neuf gros points (surtout 0!)

{0, 1, 2, 3, 4, 5, 6, 7, 8}

On coupe avec des ciseaux le point 0 en deux (il est assez gros pour cela!)

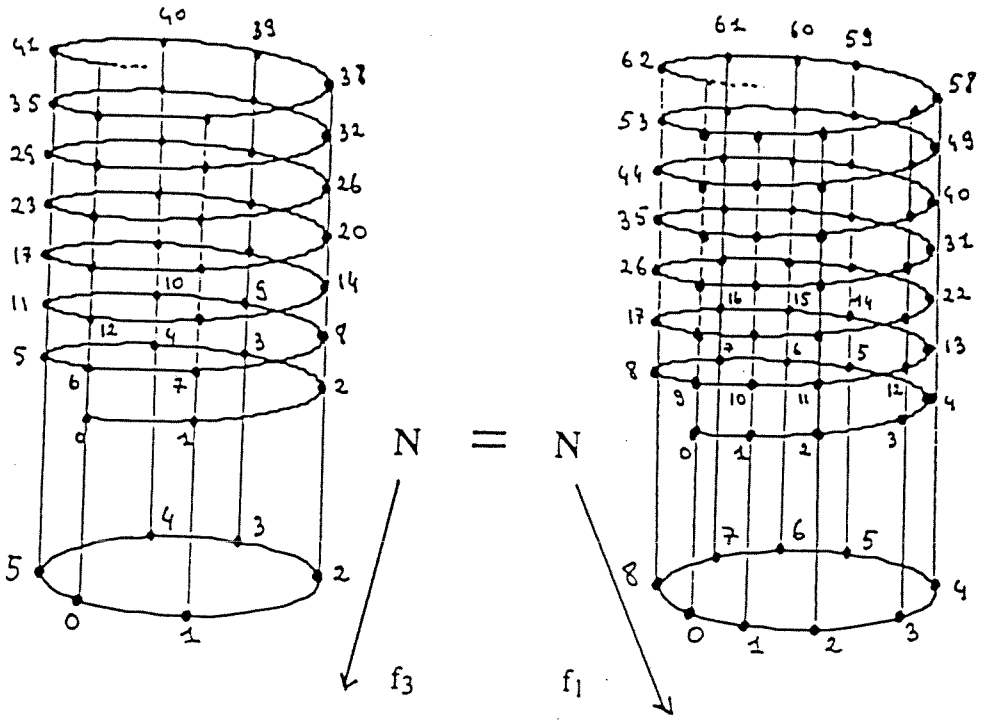
On "spirale" le tout et on projette sur un cercle avec trois points.

Le point 0 étant à deux endroit à la fois on a une représentation de l'application f_2.

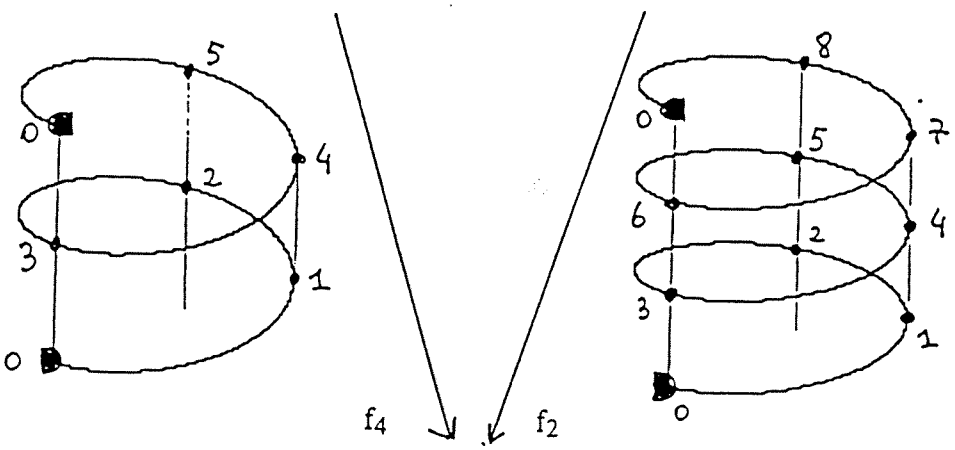


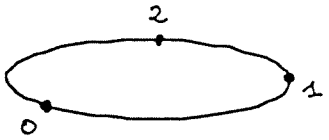
{0, 1, 2}

Cette vision des choses nous donne pour notre diagramme commutatif la représentation graphique suivante :



cercles identiques, après "découpage", aux spirales suivantes :





Retour aux applications entre ensembles finis :
(une histoire pleine de la lettre grecque sigma, des petits σ et un grand Σ)

Souvenez vous, vous avez tout à l'heure fait la liste de toutes les applications bijectives entre deux ensembles à trois éléments, vous avez trouvées les six applications suivantes que l'on notera $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6$. Notons Σ_3 l'ensemble de ces six bijections, c'est l'ensemble des permutations de trois éléments :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

σ_1 est bien particulière, elle laisse tout fixe, c'est l'application identité, dans la suite on notera id à la place de σ_1.

Pour composer deux de ces applications, ce n'est pas sorcier, on les écrits l'une en dessous de l'autre et on suit "le parcourt" de chaque élément par exemple :

σ_2 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

σ_5 $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

d'où $\sigma_5 \circ \sigma_2$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

! attention, on a d'abord "fait" σ_2 puis σ_5 pour avoir $\sigma_5 \circ \sigma_2$!

$\sigma_5 \circ \sigma_2$ est aussi un élément de Σ_3 , en fait $\sigma_5 \circ \sigma_2 = \sigma_6$
Vous pouvez par ce procédé construire une "table de composition" des éléments de Σ_3:

.	id	σ_2	σ_3	σ_4	σ_5	σ_6
id	id	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_3	id	σ_6	σ_4	σ_5
σ_3	σ_3	id	σ_2	σ_5	σ_6	σ_4
σ_4	σ_4	σ_5	σ_6	id	σ_2	σ_3
σ_5	σ_5	σ_6	σ_4	σ_3	id	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	id

dans ce tableau l'élément $\sigma_i \circ \sigma_j$ est dans la i-ème ligne et dans la j-ième colonne

	σ_4
σ_5	$\sigma_5 \circ \sigma_4$

avec $\sigma_5 \circ \sigma_4 = \sigma_3$

Vérifiez ce tableau, ayez la même attitude que celle que vous avez dans la vie courante, ne croyez pas ce que l'on vous dit, ce qui est écrit, chaque fois que cela est possible, vérifiez par vous même!

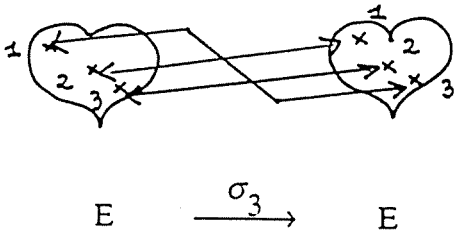
Pour première utilisation de ce tableau, considérez τ (la lettre grec tau) un des éléments de Σ_3, celui que vous voulez mais une fois choisi fixez le.
A présent on définit une application T_τ de Σ_3 dans Σ_3 par la composition des éléments de Σ_3 par l'application τ que vous avez choisie :

$$T_\tau : \Sigma_3 \to \Sigma_3 , \ \sigma \to \tau \circ \sigma$$

Montrons (ou plutôt montrez) que cette application est une bijection de Σ_3 sur Σ_3 :

- l'image de T_τ est l'ensemble des éléments de la ligne du tableau correspondant à l'élément τ que vous avez choisi. Chacune des lignes du tableau précédent contient tous les éléments de Σ_3. Quelque soit l'élément τ choisi, T_τ est donc une *application surjective*.
- Les ensembles de départ et d'arrivé Σ_3 étant des *ensembles finis ayant même nombre d'éléments*, T_τ est *bijective*. (vous avez démontré cette propriété tout à l'heure)

Ces applications sont de plus toutes des bijections de l'ensemble E = {1 2 3} sur lui même par exemple :



$$\begin{array}{ccc} 1 & 2 & 3 \\ \updownarrow & \updownarrow & \updownarrow \\ 3 & 1 & 2 \end{array}$$

$$E \xrightarrow{\sigma_3} E$$

Le flèches dessinées le sont toutes avec deux pointes; ceci pour bien indiquer que, l'application étant bijective, on peut "faire le parcourt dans les deux sens".

Chaque élément y de E étant l'image par σ_3 d'un unique élément x de E ($\sigma_3(x)=y$) on peut considérer la nouvelle application de E dans E envoyant l'élément y sur x.
C'est par définition *l'application inverse de σ_3 que l'on note σ_3^{-1} ($\sigma_3^{-1}(y)=x$)*.

Bien sur, ce qui est écrit en italique est vrai pour toute application f bijective d'un ensemble E dans un ensemble F (non nécessairement finis) et définit l'application inverse de f notée f^{-1} de F dans E par :

$$f^{-1}(y) = x \iff y = f(x)$$

Toutes ces applications, éléments de Σ_3, sont des bijections, elles ont donc chacune une application inverse qui est un des éléments de Σ_3.

A présent toutes ces applications f de l'ensemble E dans l'ensemble F défini ci dessus sont bijectives, elles ont donc une application réciproque notée f^{-1} de F dans E définie par :

$$f^{-1}(y) = x \quad \Leftrightarrow \quad y = f(x)$$

Parfois cette application réciproque porte naturellement son nom :

pour $f(x) = x^2$ on a $f^{-1}(x) = \sqrt{x}$

pour $f(x) = \sqrt{x}$ on a $f^{-1}(x) = x^2$

Dans d'autre cas, ce n'est pas une fonction déjà répertoriée, il faut lui inventer un nom :

pour $f(x) = \cos(x)$ on nomme $f^{-1}(x) = \arccos(x)$

pour $f(x) = \tan(x)$ on nomme $f^{-1}(x) = \arctan(x)$

Enfin dans certain cas il faut, à partir de sa définition, calculer l'expression de cette application réciproque en termes de fonctions classiques :

$$f(x) = y = \frac{1}{1+x} \quad \Leftrightarrow \quad 1+x = \frac{1}{y} \quad \Leftrightarrow \quad x = \frac{1}{y} - 1 = f^{-1}(y)$$

$$\text{ainsi } f^{-1}(x) = \frac{1}{x} - 1$$

Bien sûr, ces applications réciproques ne sont définies que pour les intervalles sur lesquels la fonction f considérée est bijective :

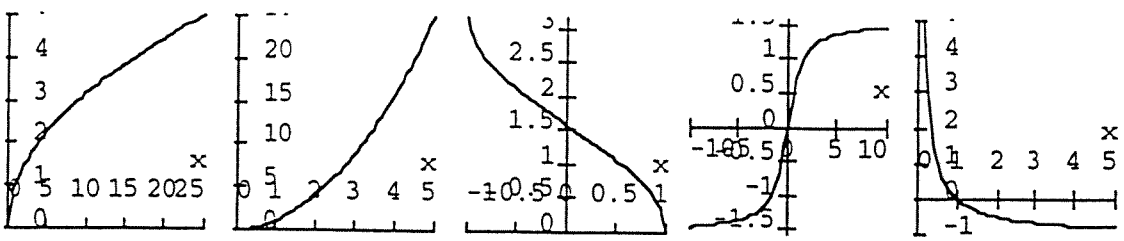
$$E \xrightarrow{f} F \quad \text{alors} \quad F \xrightarrow{f^{-1}} E$$

Ce qui dans les cas présentés ici nous donne :

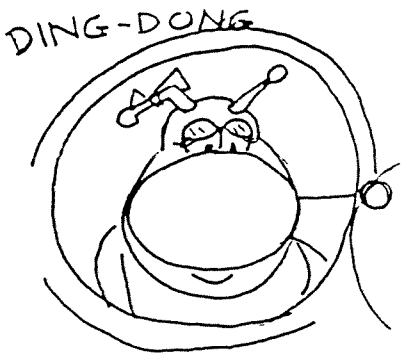
$$[0 \ \infty[\xrightarrow{\sqrt{x}} [0 \ \infty[\qquad [0 \ \infty[\xrightarrow{x^2} [0 \ \infty[\qquad [-1 \ 1] \xrightarrow{\arccos(x)} [0 \ \pi]$$

$$R \xrightarrow{\arctan(x)}]-\pi/2 \ \pi/2[\qquad]0 \ \infty[\xrightarrow{\frac{1}{x}-1} [-1 \ \infty[$$

Ainsi que leurs graphes respectifs :



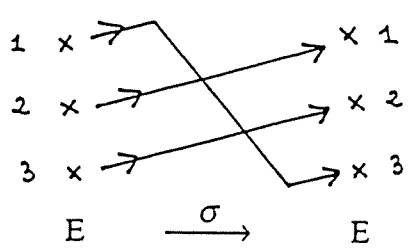
$\sqrt{x}$ $\quad x^2$ $\quad \arccos(x)$ $\quad \arctan(x)$ $\quad \frac{1}{x} - 1$

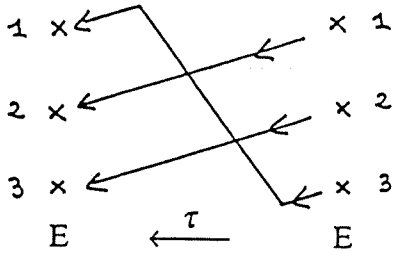


Ainsi pour un élément σ de Σ_3, on a un élément τ de Σ_3 qui est "la lecture à l'envers" de σ ($\tau = \sigma^{-1}$ et $\sigma = \tau^{-1}$). Par exemple pour :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

lecture à l'envers:





$$\text{soit } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

En faisant allègrement "l'aller retour" on a toujours l'identité, c'est à dire :

$$\sigma \circ \tau = \tau \circ \sigma = id$$

Par cette propriété en vous servant de la table de composition précédente il vous suffit pour chaque élément de repérer dans sa ligne (ou dans sa colonne si vous préférez) où se trouve l'élément id pour en déterminer l'inverse, ainsi :

$$(\sigma_2)^{-1} = \sigma_3 \text{ et } (\sigma_3)^{-1} = \sigma_2, \quad (\sigma_4)^{-1} = \sigma_4, \quad (\sigma_5)^{-1} = \sigma_5, \quad (\sigma_6)^{-1} = \sigma_6$$

Voilà, vous venez de faire "à la main" une description complète de Σ_3 que l'on appelle "le groupe de permutation de trois éléments". Et pour quatre, cinq, ... , et plus d'éléments me direz vous.

Les choses se compliquent très vite, en fait pour n éléments, Σ_n a n! éléments.

(Σ_4 a 24 éléments, ce qui ferait une table de composition de 576 éléments, Σ_5 a 120 éléments, Σ_6 720.....)

Revenons un instant aux fonctions de la page 7. Vous vous souvenez, ce sont celles qui après avoir été fortement réduite, avec moults abus de langage, ont fini par devenir des applications bijectives. Vous les aviez étudiées, vous aviez réduit les intervalles de départ et d'arrivé jusqu'à obtenir une application bijective qui, par abus de langage, portait le même nom que la fonction prise au départ :

$$[0 \ \infty[\xrightarrow{x^2} [0 \ \infty[\qquad [0 \ \infty[\xrightarrow{\sqrt{x}} [0 \ \infty[\qquad [0 \ \pi] \xrightarrow{\cos(x)} [-1 \ 1]$$

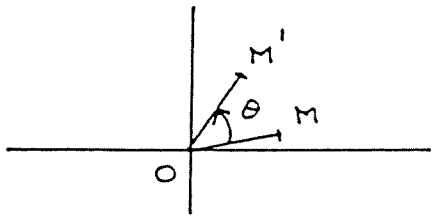
$$]-\pi/2 \ \pi/2[\xrightarrow{\tan} \mathbb{R} \qquad]-1 \ \infty[\xrightarrow{\frac{1}{(1+x)}} [0 \ \infty[$$

Il y a un autre ensemble d'applications bijectives que vous connaissez bien, ce sont les isométries, souvenez vous, ces applications du plan dans le plan, qui conservent les longueurs. Mais ceci est une histoire que nous allons parcourir dans le petit passage suivant.

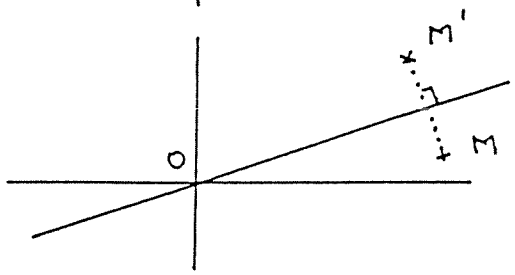
Un peu de géométrie :

Prenons pour ensemble de départ et d'arrivée le plan **P** rapporté à un repère orthonormé d'origine O. Notons, comme vous en avez l'habitude, $[M_1M_2]$ le segment d'extrémités les points M_1 et M_2, segment dont la longueur est notée M_1M_2.

Pour un angle fixé θ, vous connaissez la rotation de centre O d'angle θ , que nous noterons $R(\theta)$; on fait "tourner d'un angle θ autour du point O un point M pour obtenir son image M' " :

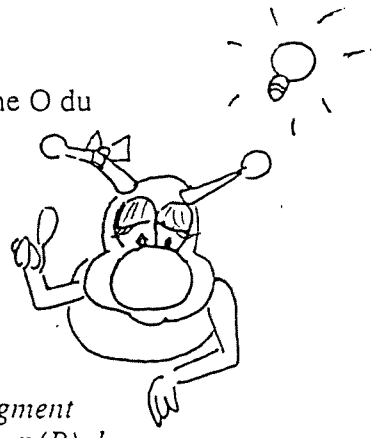


En prenant D une droite passant par l'origine O , vous avez de même la symétrie orthogonale par rapport à cette droite, que l'on notera S_D :



Ces différentes applications bijectives du plan dans le plan sont des applications qui conservent les distances, on dit que ce sont des isométries.

Soit $\varphi : \mathbf{P} \longrightarrow \mathbf{P}$ une isométrie, on a donc $\varphi(M_1)\,\varphi(M_2) = M_1M_2$



Ici nous allons nous restreindre aux isométries qui de plus conservent l'origine O du repère considéré. Notons Iso l'ensemble de ces isométries :

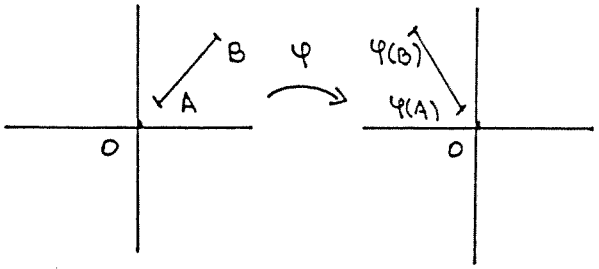
$$\text{Iso} = \{\, \varphi : \mathbf{P} \longrightarrow \mathbf{P} \mid \varphi \text{ est une isométrie et } \varphi(O) = O \}$$

Ainsi si $\varphi \in$ Iso on aura $O\,\varphi(M) = OM$.

Le fait de "conserver la distance" entraîne l'amusante propriété suivante :

Propriété
Soit φ une isométrie et [AB] un segment du plan P.
Pour tout point M du segment [AB], l'image de M, $\varphi(M)$, appartient au segment $[\varphi(A)\,\varphi(B)]$ et est uniquement déterminée par M et par les images $\varphi(A)$ et $\varphi(B)$ des points A et B.

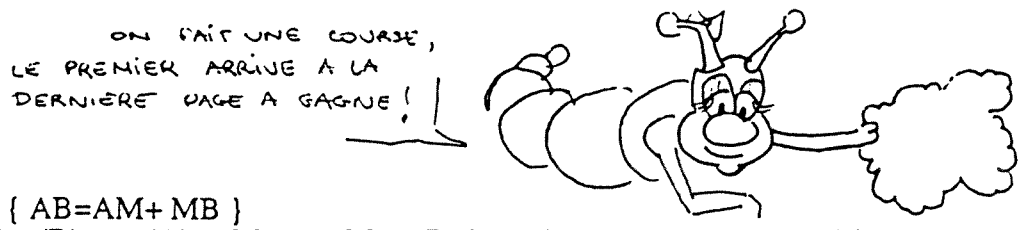
(Ainsi l'image d'un segment est un segment de même longueur)



Démonstration :
Montrons d'abord la petite propriété:

$$\{\, AB = AM + MB \,\} \Leftrightarrow \{\, M \in [AB] \,\}$$

Si M appartient au segment, on a bien cette relation de longueur.
Si M n'appartient pas au segment l'inégalité triangulaire nous donne la relation de longueur $AB < AM + MB$.
on a donc bien cette équivalence.
A présent en utilisant la propriété $\varphi(M_1)\,\varphi(M_2) = M_1M_2$ on a:



$\{ M \in [AB] \} \Leftrightarrow \{ AB = AM + MB \}$
$\Rightarrow \{ \varphi(A)\varphi(B) = \varphi(A)\varphi(M) + \varphi(M)\varphi(B) \} \Leftrightarrow \{ \varphi(M) \in [\varphi(A)\varphi(B)] \}$
Ainsi pour tout point M du segment [AB], l'image de M, $\varphi(M)$, appartient au segment $[\varphi(A)\varphi(B)]$.

Pour la dernière partie de notre propriété, on a :
$M \in [AB]$, alors $\exists k \in [01]$ tel que $AM = kAB$
φ est une isométrie d'où $\varphi(A)\varphi(M) = k\varphi(A)\varphi(B)$
le point $\varphi(M)$ est donc déterminé par k et les points $\varphi(A)$ et $\varphi(B)$.

En essayant de détailler un peu plus, si ce qui précède vous parait ténébreux;
Le nombre k est uniquement déterminé par la position du point M sur le segment d'extrémités A et B. Ainsi $\varphi(M)$ est le point du segment $[\varphi(A)\varphi(B)]$ défini par la relation de distance :

$$\varphi(A)\varphi(M) = k\varphi(A)\varphi(B)$$

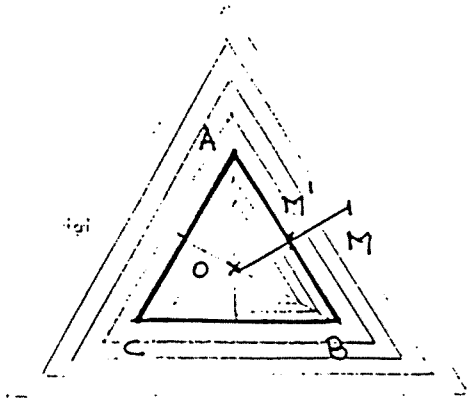
Ceci achève la démonstration de cette propriété.

Pour poursuivre notre propos, fixons nous dans le plan **P** un joli triangle équilatéral T de sommets les points A, B et C. Supposons de plus que l'origine O est le centre de gravité de ce magnifique triangle.

La propriété précédente nous donne la proposition :

Proposition
Soient $M \in P$ et $\varphi \in Iso$ alors
$\varphi(M)$ est uniquement déterminé par M et par $\varphi(A)$, $\varphi(B)$ et $\varphi(C)$.

(Autrement dit, une isométrie $\varphi \in$ Iso est uniquement déterminée par sa valeur sur les trois points A, B et C.)
Le petit dessin suivant va nous mettre gracieusement sur la piste de la démonstration de cette proposition :



Pour tout point M du plan, la demi droite OM coupe l'un des côtés du triangle en un point que nous appellerons M'

Ainsi on aura :
$\varphi(M)$ sera déterminé par $\varphi(M')$, lui même déterminé par $\varphi(A)$ et $\varphi(B)$
(car sur ce dessin le point M' est entre les points A et B)

En fait, quand on connaît l'image du triangle T, $\varphi(T)$, les triangles homothétiques de T (déssinés sur la figure) dans un rapport k, s'envoient par φ sur les triangles homothétiques dans un rapport k du triangle $\varphi(T)$.

Écrivons à présent proprement la démonstration de cette proposition.

démonstration :
Soit $M \in \mathbf{P}$, $M \neq O$, supposons que la demi droite d'origine O passant par M coupe le segment [AB] en un point M'. alors
$\exists k \in [0 \infty[$ tel que $OM = kOM'$,
de plus $\varphi \in$ Iso d'où $O\varphi(M) = kO\varphi(M')$.
Le point $\varphi(M)$ est donc déterminé k et par le point $\varphi(M')$.
Par la propriété précédente le point $\varphi(M')$ est déterminé par la position de M' entre A et B et par les points $\varphi(A)$ et $\varphi(B)$.
On procède de la même manière si la demi droite d'origine O coupe l'un des deux autres côtés du triangle T.
Ainsi l'application φ est déterminée par sa valeur sur les points A, B et C.

Et si le triangle T n'avait pas envie de bouger ? Si les points de T s'y trouvaient bien, peut-être comme vous en Alsace, après "avoir fait φ" , ils veulent toujours être dans T, quels sont les applications φ de Iso qui permettent cela ?

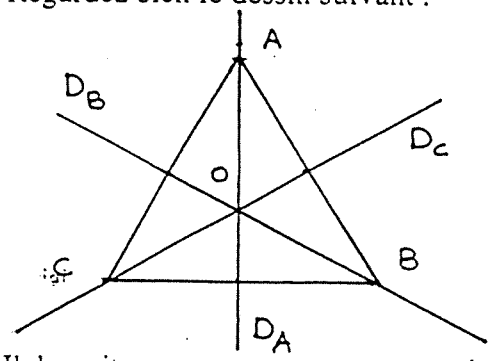
Précisément, quelles sont les isométries de Iso qui laissent globalement invariant le triangle T. C'est à dire déterminer l'ensemble :

$$\text{Iso}(T) = \{ \varphi \in \text{Iso} \mid \varphi(T) = T \}$$

L'ensemble Iso(T) est appelé l'ensemble des isométries du triangle équilatéral.
C'est la question qui va nous occuper un instant.

Drôle d'occupation me direz vous, mais ça ou la télévision! l'être humain ne sachant quasiment jamais laisser ses neurones au repos, voilà sans doute une amusante façon de les agiter.

Regardez bien le dessin suivant :



D_A, D_B et D_C désigne les droites passant par O et respectivement par les points A, B et C.
Dans le triangle T, on a de plus les angles suivants :

$$(\bar{OA}, \bar{OB}) = 2\pi/3 \text{ et } (\bar{OA}, \bar{OB}) = 4\pi/3$$

Il devrait vous permettre, sans trop de difficultés, d'identifier des éléments de Iso(T) :

- En tournant :

  • l'angle $(\bar{OA}, \bar{OB}) = 2\pi/3$, si donc on fait tout tourner autour du point O d'un angle de $2\pi/3$, le triangle T "tournera" sur lui-même, c'est la rotation d'angle $2\pi/3$.

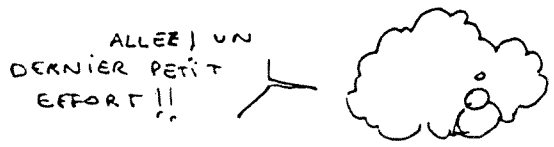
  Ainsi $R(2\pi/3) \in \text{Iso}(T)$

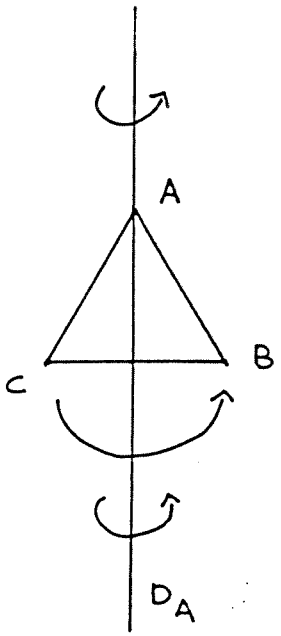
  • en "rotant" à nouveau de $2\pi/3$ le triangle T "tourne" encore sur lui même de $2\pi/3$, il aura tourné en tout de $4\pi/3$.

  Ainsi $R(4\pi/3) \in \text{Iso}(T)$

  • "rotons" toujours de $2\pi/3$, là le triangle T est retombé sur ses pieds, dans sa position initiale. C'est la rotation d'angle $6\pi/3=2\pi$, c'est l'application identité notée id.

  Ainsi, bien sûr, $\text{id} \in \text{Iso}(T)$





- En retournant, "flip-flap", autour des droites D_A, D_B et D_C, le triangle T se retourne sur lui même. Pour faire "flip-flap", (comme sur le dessin ci contre avec D_A) il nous faudrait une troisième dimension, on n'y a pas droit car on ne s'occupe ici que des applications du plan **P** dans le plan **P**. Ce sont donc les symétries orthogonales par rapport à ces droites D_A, D_B et D_C, qui nous donnerons ce triangle T envoyé sur lui même tout retourné, ainsi :

$$S_{D_A} \in \text{Iso(T)}$$
$$S_{D_B} \in \text{Iso(T)}$$
$$S_{D_C} \in \text{Iso(T)}$$

On a, grâce à ces petits dessins, identifiés 6 éléments de Iso(T).

Une angoissante question se présente alors à vous :

"les a-t-on bien trouvées toutes?"

Ou bien reste-t-il tout au fond de Iso(T) des éléments que l'on a pas réussi à détecter.

Pour vous apaiser et répondre à cette question, nous vous proposons la démarche suivante:

"envoyez Iso(T) dans Σ_3"

Mais que peut donc vouloir dire ce charabia? Regardez bien :

Une isométrie envoie un segment sur un segment, $\varphi \in$ Iso(T) envoie ainsi chaque sommet de T sur un sommet de T.
L'application φ définie une permutation de l'ensemble des sommets {A, B, C} sur lui même.
Et si A s'appelle 1
B s'appelle 2
C s'appelle 3
l'isométrie φ nous définit ce que l'on a appelé tout à l'heure une permutation de trois éléments (voir page 12), notée :

$$\sigma_\varphi = \begin{pmatrix} 1 & 2 & 3 \\ \varphi(1) & \varphi(2) & \varphi(3) \end{pmatrix}$$

Nous avons notés Σ_3 l'ensemble de ces permutations de trois éléments.

Le sens exacte du charabia précédent est donc :

Il y a une application naturelle :
Ψ : Iso(T) $\longrightarrow$ Σ_3 définie par $\Psi(\varphi) = \sigma_\varphi$

La réponse à la question "les a-t-on bien toutes" est alors une conséquence quasi immédiate de :

Proposition
Ψ est une bijection

démonstration

- Montrons que Ψ est injective :

(reportez vous a la page 2 pour trouver la définition de injective utilisée ici)

Soient φ_1, $\varphi_2 \in$ Iso(T), telles que $\Psi(\varphi_1) = \Psi(\varphi_1)$

Ainsi $\varphi_1(A) = \varphi_2(A)$, $\varphi_1(B) = \varphi_2(B)$ et $\varphi_1(C) = \varphi_2(C)$

Or on a démontré que φ_1 et φ_2 sont déterminés par leurs valeurs sur les sommets A, B, C du triangle T.

D'où $\varphi_1 = \varphi_2$ et donc Ψ est injective.

(Petit commentaire pour aider à suivre ce qui précède: la lettre φ représente les isométries du triangle T, ces isométries font bouger les trois sommets, ce sont les permutation $\Psi(\varphi) = \sigma_\varphi$. Si deux telles isométries φ_1 et φ_2 font bouger de la même manière les sommets A, B et C du triangle T , elles sont égales car on a vu qu'elles étaient déterminées par leurs valeurs sur ces sommets.)

- Montrons que Ψ est surjective :

Nous avons vu que Iso(T) a au moins 6 éléments distincts,

l'application Ψ étant injective, ces 6 éléments sont envoyés sur les 6 éléments de Σ_3,

Ψ est donc surjective.

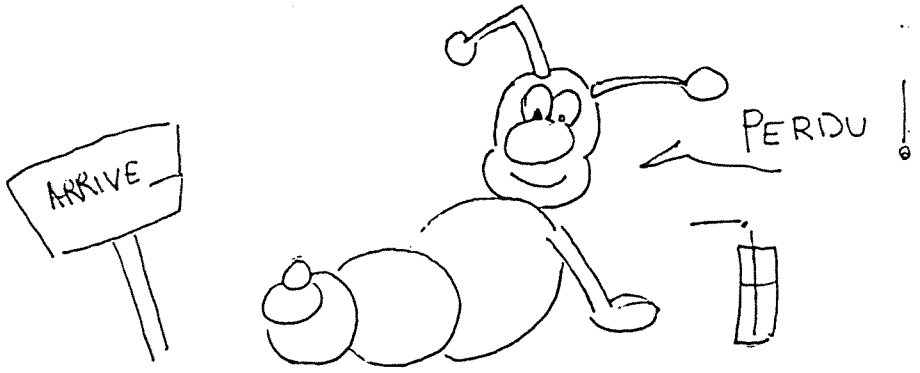
L'application Ψ étant injective et surjective est bijective.

L'ensemble Iso(T) a donc 6 éléments qui sont ceux décrits précédemment.

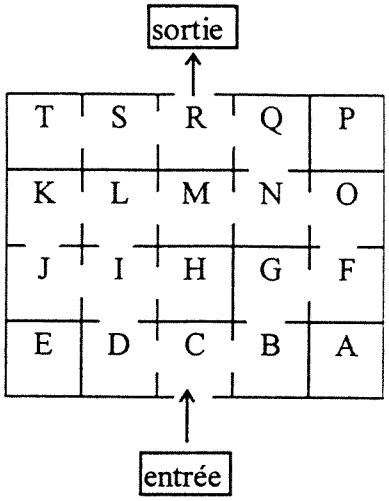
Si vous le souhaitez, ce petit jeu peut ne pas s'arrêter là.

Quand vous composez deux de ces isométries, vous restez dans l'ensemble Iso(T).

Comme vous l'avez fait à la page 13 pour l'ensemble Σ_3 vous pouvez construire une table de composition de Iso(T). Vérifiez alors que ces deux tables se "correspondent" par l'application Ψ. Plus tard dans vos études vous direz, dans une telle situation , que Iso(T) et Σ_3 sont des groupes et que Ψ est un homomorphisme de groupe. Mais cela est une autre histoire qui vous sera racontée plus tard dans vos études et en détail, par d'autres.



LE FIL D'ARIANE[1]



Voici un labyrinthe.

Une personne que nous appellerons X, a traversé ce labyrinthe de l'entrée à la sortie sans jamais être passée deux fois par la même porte.

Les pièces sont nommées A, B, C... comme indiqué sur la figure.

Pour chacune des phrases suivantes, dire si elle est vraie, si elle est fausse ou si on ne peut pas savoir.

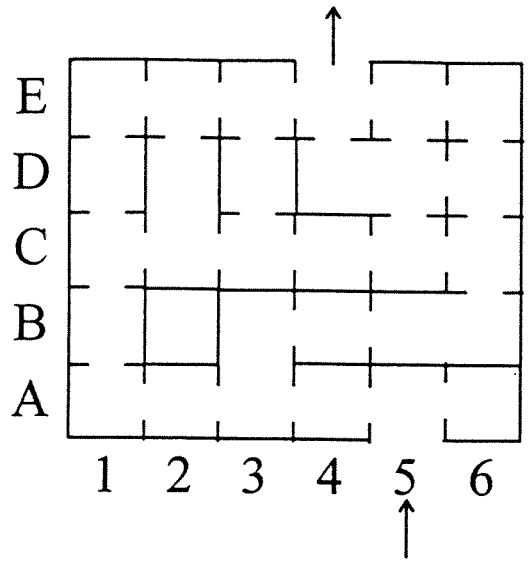
Une phrase sera déclarée vraie si on peut en être tout à fait certain. Par exemple, la phrase « X est passé par R » est vraie (c'est la seule case par laquelle X a pu sortir).
Il en est de même pour une phrase déclarée fausse. Par exemple, la phrase « X est passé par E » est fausse (il n'y a ni entrée ni sortie possible pour la case E).
Dans le cas de la phrase « X est passé par D », on ne peut pas savoir car tous les chemins qui vont de l'entrée à la sortie ne passent pas par D. Seule la personne X serait en mesure de trancher.
On peut donc éventuellement substituer aux trois réponses proposées « vrai », « faux », « on ne peut pas savoir », les réponses « oui », « non » et « peut-être ».

Phrase 0 : « X est passé par C »
Phrase 1 : « X est passé par P »
Phrase 2 : « X est passé par N »
Phrase 3 : « X est passé par M »
Phrase 4 : « Si X est passé par O, alors X est passé par F »
Phrase 5 : « Si X est passé par K, alors X est passé par L »
Phrase 6 : « Si X est passé par L, alors X est passé par K »
Phrase 7 : « X est passé deux fois par I »

En logique mathématique les propositions sont vraies ou fausses. Parmi ces phrases, il en est pour lesquelles **nous** ne pouvons pas savoir si elles sont vraies ou fausses. En revanche, **la personne X**, qui sait par où elle est passée, peut décider. Ces phrases sont donc des propositions logiques acceptables.

Dans la présentation ci-dessous, il n'est plus question d'une seule personne et de son trajet particulier, mais de l'ensemble de tous les chemins possibles. C'est ce qui justifie la présence de l'un ou l'autre des quantificateurs « pour tout » ou « il existe » dans leur libellé.

[1] Ariane remit à Thésée une pelote de fil pour lui permettre de ne pas s'égarer dans le Labyrinthe.



Voici un autre labyrinthe.

Soit U l'ensemble de tous les chemins qui traversent ce labyrinthe de l'entrée à la sortie sans jamais passer deux fois par la même porte.

Pour chacune des phrases suivantes, dire si elle est vraie, si elle est fausse ou si on ne peut pas savoir.

Phrase 1 : tout chemin de U passe par A5.

Phrase 2 : tout chemin de U passe par E2.

Phrase 3 : il existe un chemin de U passant par E2.

Phrase 4 : il existe un chemin de U ne passant pas par E2.

Phrase 5 : il existe un chemin de U passant par A6.

Phrase 6 : il existe un chemin de U ne passant ni par E2 ni par C3.

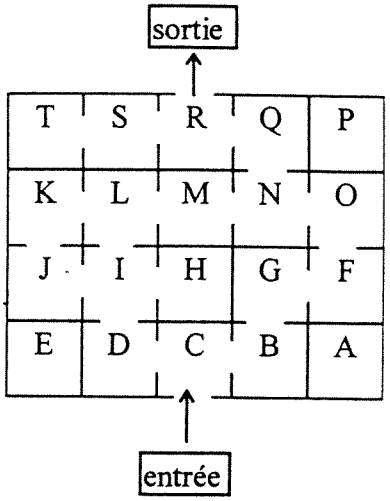
Phrase 7 : pour tout chemin t de U, si t passe par E5 alors t passe par E6.

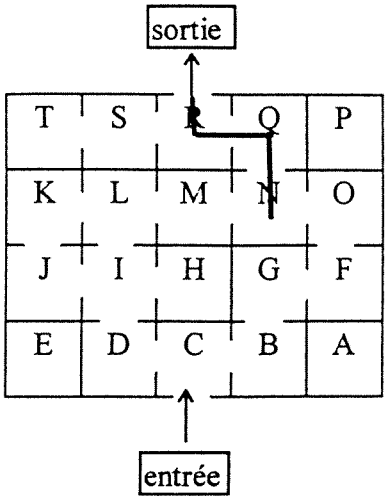
Phrase 8 : pour tout chemin t de U, si t passe par E6 alors t passe par E5.

Phrase 9 : pour tout chemin t de U, si t passe par A6 alors t passe par B2.

Phrase 10 : il existe un chemin de U qui passe deux fois par E4.

RETROUVONS LE FIL D'ARIANE





La fin du parcours de X

Phrase 0 : « X est passé par C »
C'est vrai, la case C est la seule entrée possible dans le labyrinthe.

Phrase 1 : « X est passé par P »
C'est faux, il n'y a ni entrée ni sortie pour la case A.

Phrase 2 : « X est passé par N »
C'est vrai. En raisonnant à partir de la sortie : X est passé par R, il n'est pas passé par S (pas d'entrée dans T). X est donc passé par Q et il est entré dans Q par N.

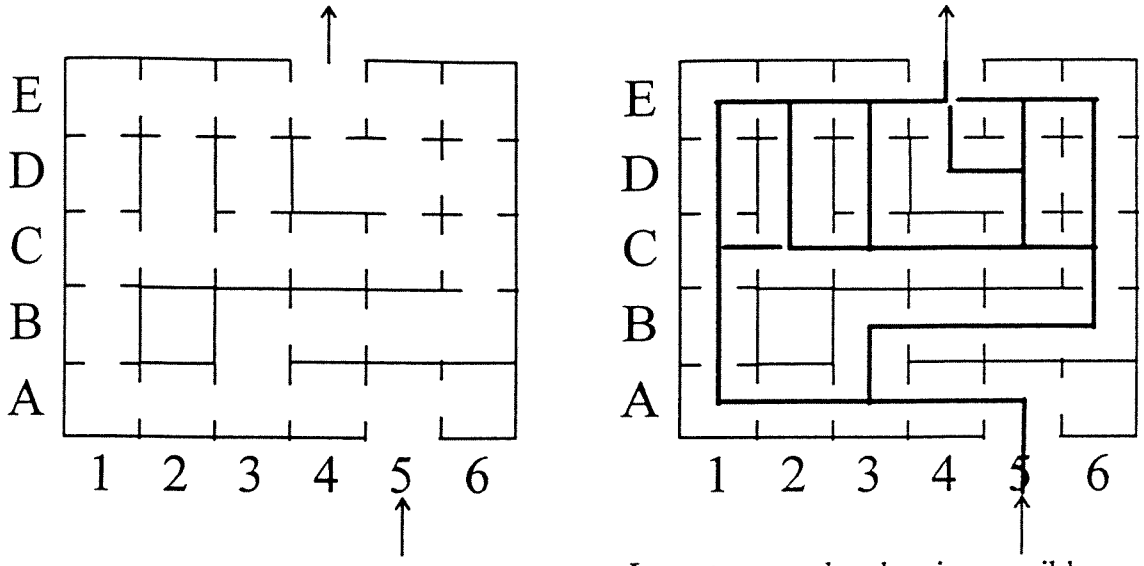
Phrase 3 : « X est passé par M »
On ne peut pas savoir. On peut accéder à la case N par M ou par O.

Phrase 4 : « Si X est passé par O, alors X est passé par F »
C'est vrai.
Si X est passé par O, il est entré dans O et ressorti par une autre porte, on peut donc affirmer qu'il est passé par F (et par N)

Phrase 5 : « Si X est passé par K, alors X est passé par L »
C'est vrai. Le raisonnement est analogue à celui ci-dessus.

Phrase 6 : « Si X est passé par L, alors X est passé par K »
On ne peut pas savoir, car les deux cases I et L permettent d'accéder à K.
C'est la réciproque de la phrase 5.

Phrase 7 : « X est passé deux fois par I »
C'est faux.
Il y a bien 4 portes pour I, donc a priori, deux passages possibles mais l'une des portes donne sur H qui est une impasse.



Les « traces » des chemins possibles.

L'un des procédés permettant de répondre aux questions posées est de décrire « en extension » l'ensemble U de tous les chemins qui vont de l'entrée à la sortie sans repasser deux fois par la même porte. Cet ensemble est fini mais il a suffisamment d'éléments pour rendre ce procédé exhaustif pénible d'autant que mettre en évidence les traces des chemins sur le labyrinthe ne donne pas une représentation très claire (en particulier pour ce qui concerne les sens de parcours).
Il vaut mieux se montrer plus astucieux.
Pour démontrer qu'une phrase comportant le quantificateur « il existe » est vraie, il suffit d'exhiber un chemin répondant aux contraintes.
Pour montrer qu'une phrase comportant le quantificateur « tout » est fausse, il suffit d'exhiber un contre-exemple, c'est à dire un chemin ne vérifiant pas les propriétés exigées.

Phrase 1 : tout chemin de U passe par A5.
C'est vrai car A5 est la seule case d'entrée dans le labyrinthe.

Phrase 3 : il existe un chemin de U passant par E2.
C'est vrai, en voilà un : entrée→A5→A1→E1→E4→sortie

Phrase 4 : il existe un chemin de U ne passant pas par E2.
C'est vrai, en voilà un : entrée→A5→A1→C1→C3→E3→E4→sortie

Phrase 2 : tout chemin de U passe par E2.
C'est faux puisqu'il s'agit de la négation de la phrase 4 et le chemin donné ci-dessus est un contre-exemple.

Phrase 5 : il existe un chemin de U passant par A6.
C'est faux, la case A6 ne comporte qu'une seule porte. On ne peut donc y entrer et en ressortir sans passer deux fois la même porte.

Phrase 6 : il existe un chemin de U ne passant ni par E2 ni par C3.
C'est vrai, en voilà un : entrée→A5→A3→B3→B6→E6→E4→sortie

Phrase 10 : il existe un chemin de U qui passe deux fois par E4.

C'est vrai, en voilà un :
entrée→A5→A3→B3→B6→E6→E3→C3→C5→D5→D4→E4→sortie

Phrase 7 : pour tout chemin t de U, si t passe par E5 alors t passe par E6.
C'est faux. Pour le démontrer il suffit de trouver un chemin de U qui passe par E5 sans passer par E6.
entrée→A5→A3→B3→B6→C6→C5→E5→D4→E4→sortie

Phrase 8 : pour tout chemin t de U, si t passe par E6 alors t passe par E5.
C'est vrai. La case E6 n'a que deux portes. Tout chemin passant par E6 entre par l'une de ces portes et sort par l'autre. Tout chemin passant par E6 passe par E5 (et D6).

Phrase 9 : pour tout chemin t de U, si t passe par A6 alors t passe par B2.
Cette phrase est vraie. Comme il n'y a aucun chemin de U passant par A6, il n'y a rien à vérifier ! Au niveau de la structure logique on peut rapprocher cette phrase de certaines autres comme :
« Si je gagne au loto je t'offre une voiture » qui est forcément vraie si elle est prononcée par quelqu'un qui ne joue jamais au loto, ou encore :
« Si tu es le roi alors je suis le pape ! » qui est vraie (si l'interpellé n'est pas le roi).
Ces trois phrases sont vraies d'un point de vue logique, mais inutiles (elles n'apportent aucune information). Ce qui est inutile n'est pas forcément faux.

On notera qu'ici il n'y a plus de phrase pour laquelle « on ne peut pas savoir ». L'ensemble de référence U étant défini avec précision et les phrases étant quantifiées, on peut décider si elles sont vraies ou fausses. Une situation analogue serait :
x est un réel
« $x^2 = 4$ » est une phrase dont on ne peut pas savoir si elle est vraie ou fausse alors que :
« $\forall x \in R, x^2 = 4$ » est faux et « $\exists x \in R, x^2 = 4$ » est vrai.

LOGIQUE ET QUANTIFICATEURS

IDENTITE REMARQUABLE ?

Parmi les commentaires suivants concernant l'égalité :

$$(x+y)^2 = x^2 + y^2$$

lesquels sont vrais ?

a) C'est vrai pour tout couple de réels (x,y).
b) C'est faux pour tout couple de réels (x,y).
c) C'est vrai uniquement si x et y sont nuls.
d) C'est vrai si x ou y est nul.
e) C'est vrai uniquement si x ou y est nul.
f) C'est vrai uniquement si les deux membres sont nuls.
g) C'est vrai pour un nombre fini de couples de réels (x,y).
h) C'est vrai si $x=y$.
i) C'est vrai pour une infinité de couples de réels (x,y).
j) La différence des deux membres tend vers 0 lorsque x (ou y) tend vers l'infini.
k) La différence des deux membres tend vers 0 lorsque x et y tendent vers l'infini.

TRIGONOMETRIE

Parmi les commentaires suivants concernant l'égalité :

$$\cos(x+y) = \cos(x) + \cos(y)$$

lesquels sont vrais ?

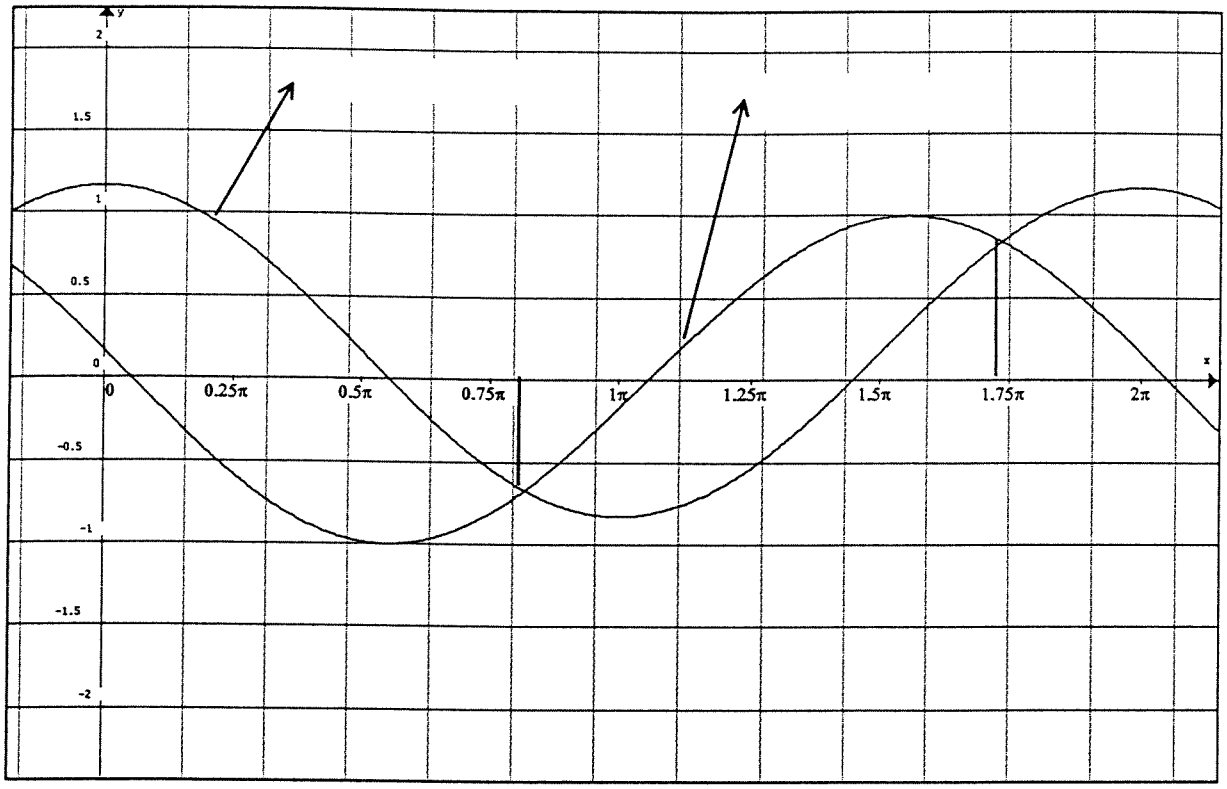
a) C'est vrai pour tout couple de réels (x,y).
b) C'est faux pour tout couple de réels (x,y).
c) C'est vrai uniquement si x et y sont nuls.
d) C'est vrai uniquement si x ou y est nul.
e) C'est faux si x ou y est nul.
f) C'est vrai uniquement si les deux membres sont nuls.
g) C'est vrai pour un nombre fini de couples de réels (x,y) avec x et y compris entre 0 et 2π.
h) C'est vrai si $x=y$.
i) C'est vrai pour une infinité de couples de réels (x,y) avec x et y compris entre 0 et 2π.
j) C'est vrai pour tout couple de réels (x,y) tel que $x = (2k+1)\frac{\pi}{2}$ (k entier).
k) La différence des deux membres tend vers 0 lorsque x (ou y) tend vers l'infini.
l) La différence des deux membres tend vers 0 lorsque x et y tendent vers l'infini.

(d'après concours Kangourou 1992)

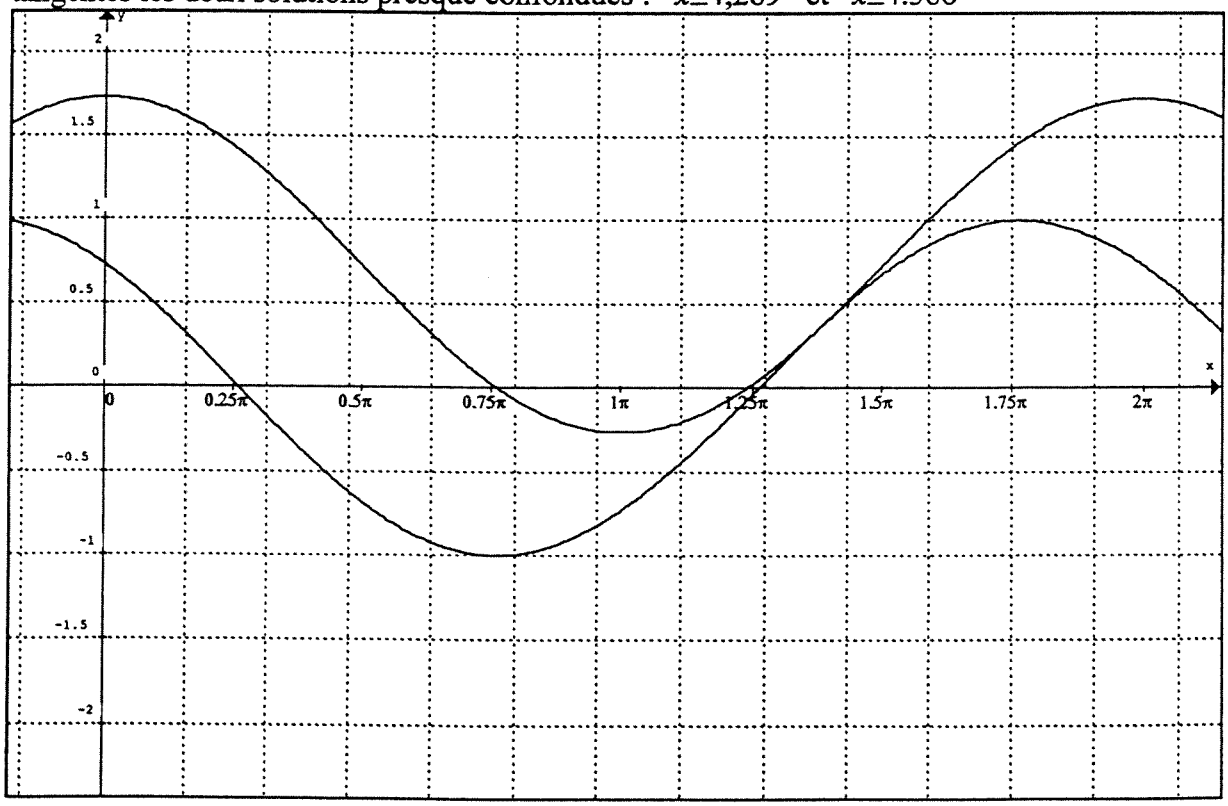
INDICATIONS DE SOLUTIONS

TRIGONOMETRIE

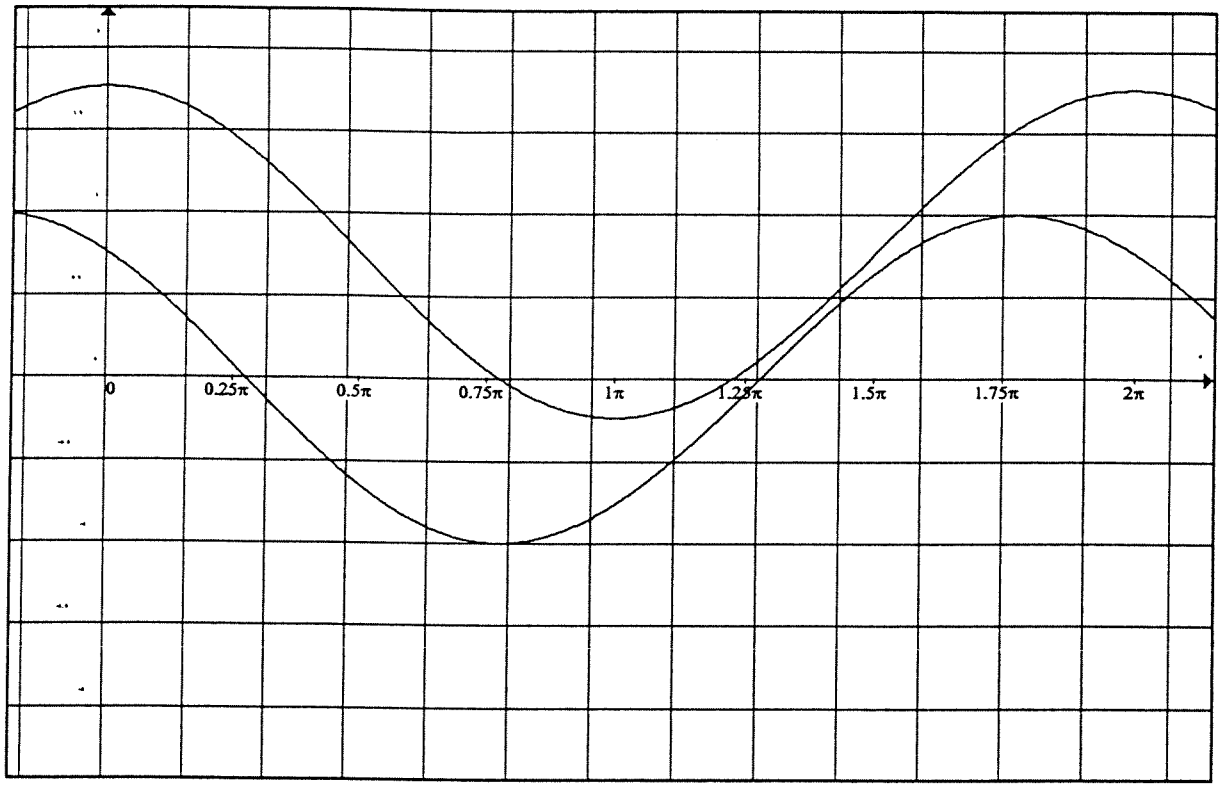
Exemple de l'équation $\cos(x+1,4)=\cos(x)+\cos(1,4)$ qui a deux solutions $x\cong 2,57$ et $x\cong 5,45$.



Exemple de l'équation $\cos(x+0,75)=\cos(x)+\cos(0,75)$: les deux courbes sont pratiquement tangentes les deux solutions presque confondues : $x\cong 4,289$ et $x\cong 4.386$



Pour $\cos(x+0,7)=\cos(x)+\cos(0,7)$ il n'y a plus de solution.



On remarque que pour tout λ compris entre 0,75 et $\frac{\pi}{2}$ l'équation $\cos(x+\lambda)=\cos(x)+\cos(\lambda)$ aura deux solutions dans l'intervalle $[0, 2\pi]$: l'une des courbes se décale horizontalement et l'autre verticalement.

L'équation d'inconnue x : $\cos(x+y)= \cos(x)+\cos(y)$ a donc une infinité de solutions dans l'intervalle $[0, 2\pi]$ (il y a, en particulier 2 solutions pour chaque valeur de y comprise entre 0,75 et $\frac{\pi}{2}$).

Analyse de texte – Analyse mathématique.

La lecture de textes mathématiques est un aspect non négligeable du travail à fournir dans l'enseignement supérieur. Contrairement à la lecture d'un roman, où seule une compréhension du fil directeur est nécessaire pour suivre l'histoire, il est souvent nécessaire de rentrer dans les détails d'un texte scientifique pour bien percevoir sa signification. Cela dépendra bien entendu de la nature du texte étudié et de ce que l'on cherchera à en retirer. Pour vous familiariser avec ce type de travail, nous vous proposons la lecture, suivie de l'analyse d'un texte du mathématicien Ian Stewart, extrait de son livre: "Dieu joue-t-il aux dés?"(Edition Flammarion, collection Nouvelle bibliothèque scientifique 1992)

Lecture du texte

Lire, plusieurs fois si nécessaire le texte proposé.
Essayer de bien comprendre les divers schémas et représentations graphiques proposés par l'auteur.
Essayer de suivre les consignes de l'auteur en analysant à l'aide d'une calculatrice ou d'un ordinateur le comportement à long terme de la suite (essayer dans chaque cas plusieurs valeurs de x_0).
Ne pas perdre le fil .

Extraits choisis du livre : "Dieu joue-t-il aux dés?"

Application logistique

Considérez un segment de droite de longueur unitaire. Un point sur ce segment de droite est représenté par un nombre x compris entre 0 et 1, qui exprime sa distance par rapport à l'extrémité gauche. L'application logistique est: $x \mapsto kx(1-x)$ où k est une constante comprise entre 0 et 4. Si nous itérons l'application, nous obtenons le système dynamique discret[1] suivant: $x_{t+1} = kx_t(1-x_t)$

Nous pouvons considérer que t représente le temps, mais maintenant le temps doit avancer par étapes saccadées d'un nombre entier à l'autre, 0, 1, 2, 3... Dans ce cas, x est la valeur de la variable x au temps *t*.

Géométriquement, l'application logistique étire ou comprime le segment de droite d'une manière non uniforme, puis le plie en deux. Par exemple, prenez $k = 3$, de sorte que $x_t = x$ se transforme en: $x_{t+1} = 3x(1-x)$

Les nombres compris entre 0 et 0,5 sont appliqués sur les nombres compris entre 0 et 0,75. Par exemple, 0,5 s'applique sur $3 \times 0{,}5 \times (1-0{,}5) = 0{,}75$. Les nombres compris entre 0,5 et 1 s'appliquent sur les nombres compris entre 0,75 et 0: le même intervalle dans le sens inverse. De sorte que l'effet de l'application est d'étirer le segment initial pour qu'il recouvre *deux fois* le segment compris entre 0 et 0,75.

En général, pour un k donné, l'application replie l'intervalle et le dépose par-dessus l'intervalle compris entre 0 et k/4. Si k est petit, il s'agit d'une compression plutôt que d'un étirement; et nous verrons une différence dans la dynamique. Si k est plus grand que 4, l'intervalle surgit hors de lui-même sous l'effet de l'itération, et certaines valeurs de x se projettent rapidement vers l'infini. Ceci n'est pas très agréable à constater au point où on en est, ce qui explique pourquoi j'ai supposé que k était compris entre 0 et 4. Pour étudier la dynamique de l'application logistique, nous devons observer son comportement à long terme - ses attracteurs. C'est-à-dire que nous voulons itérer l'application de nombreuses fois et observer ce qui arrive à x. Mais il y a une couche structurelle supplémentaire: nous souhaitons le faire pour diverses valeurs de k, et observer comment le schéma change lorsque k varie.

Ainsi k est le « bouton» sur la boîte noire, et l'équation ci-dessus décrit le circuit interne. Vous pouvez explorer ce qui se passe quand on donne à k diverses valeurs en utilisant une calculatrice de poche ou un ordinateur; et je

[1] En mathématiques, on parle plutôt de suite récurrente.

vous recommande vivement de vérifier tout ce que je dis. Cependant, je décrirai ce qui se produit: en partie pour ceux qui n'ont pas accès à de telles machines, et en partie pour souligner les éléments les plus intéressants.

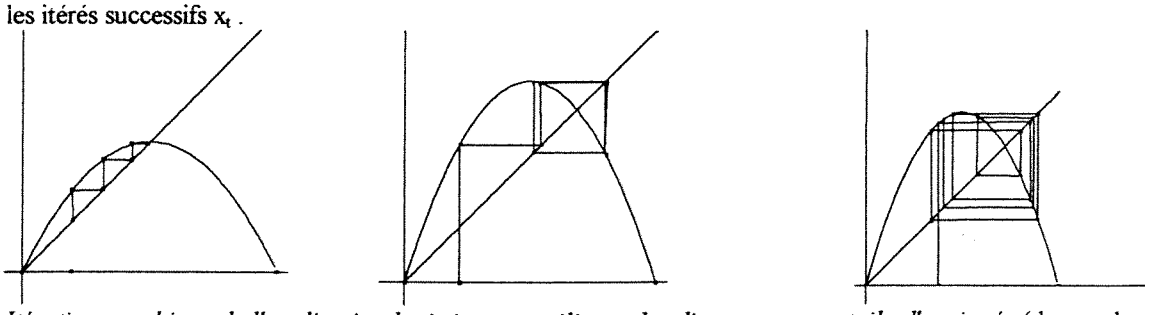
Régime stationnaire

L'intervalle des valeurs de k comprises entre 0 et 3 est appelé le *régime stationnaire*, le moins intéressant du point de vue de la dynamique. Choisissez k dans cet intervalle, disons k = 2, et itérez l'application. Par exemple, prenez x_o = 0,9. Puis, en appliquant la formule de manière répétée avec *t = 0, 1,* 2... nous trouvons une séquence[2] de valeurs:

$x_0 = 0,9$ $x_1 = 0,18$ $x_2 = 0,2952$
$x_3 = 0,41161$ $x_4 = 0,4859$ $x_5 = 0,4996$
$x_6 = 0,4999$ $x_7 = 0,5$ $x_8 = 0,5$

et elle s'installe là. Il y a un attracteur ponctuel, un état stationnaire stable, pour x = 0,5. Vous pouvez très facilement vérifier qu'il s'agit d'un état stationnaire: si x = 0,5, alors 2x (1-x) = 0,5 aussi. L'itération ne modifie pas la valeur 0,5.

On peut aussi vérifier la stabilité par le calcul, mais vous pouvez la constater géométriquement en traçant ce que les économistes mathématiciens appellent un *diagramme en toile d'araignée* (figure en bas de page). C'est une méthode graphique d'itération. Tracez d'abord un graphique de la formule y = 2x (1-x), obtenant ainsi une parabole inversée. Tracez la diagonale y = x sur le même diagramme. Pour itérer une valeur initiale x_0 , tracez une toile d'araignée verticale à partir de x_0 et observez où elle touche la parabole. Puis tracez une toile d'araignée horizontale qui touche la diagonale. La coordonnée horizontale de ce point est x_1 . Répétez, formant ainsi un « escalier » entre la parabole et la diagonale. Les coordonnées des « contremarches» successives de l'escalier sont les itérés successifs x_t .



Itération graphique de l'application logistique en utilisant des diagrammes en toile d'araignée (de gauche à droite): *état stationnaire, point périodique. chaos (reproduit avec la permission de John Wiley & Sons Ltd.).*

Quand k = 2, la toile d'araignée erre vers le haut de la diagonale puis tourne en spirale vers l'intérieur en se dirigeant vers le point où la parabole croise la diagonale. C'est le point fixe; et la stabilité en découle parce que la toile d'araignée tourne en spirale *vers l'intérieur.* Si elle tournait en spirale vers l'extérieur, vous auriez un point fixe instable. Si vous faites l'expérience, vous découvrirez que la toile d'araignée tourne en spirale vers l'intérieur, à condition que k soit inférieur à 3. De sorte que pour k compris entre 0 et 3 vous obtenez un point fixe unique stable, et la dynamique à long terme est de ne faire absolument rien. La position du point fixe bouge légèrement quand vous « augmentez un peu le volume » avec le bouton k, mais rien d'autre ne se produit.

Une cascade de doublements de période.

Lorsque k est exactement égal à 3, le point fixe est « marginalement stable »: la convergence vers lui est *extrêmement* lente. C'est le signe que nous approchons de quelque chose de terrible. En effet, lorsque k > 3, le point fixe devient instable, et la toile d'araignée tourne en spirale *vers l'extérieur.*

Chaque fois que vous connaissez une solution à un système dynamique, et que celle-ci devient instable, vous devez vous demander: « Où va-t-il se diriger maintenant? » En pratique, il ne va pas rester dans un état instable, même si cela satisfait les équations. Il va s'en aller et faire autre chose. Souvent cette autre chose est beaucoup moins évidente, et donc plus intéressante, que l'état instable d'où vous êtes parti. C'est une manière facile d'apprendre un certain nombre de choses nouvelles, cela s'appelle la *théorie de la bifurcation.* Dans cet esprit où va l'état stationnaire de l'application logistique lorsque k est plus grand que 3, lorsqu'il est égal à 3,2 par exemple?

Si vous tracez des diagrammes en toile d'araignée, vous découvrirez que la spirale dirigée vers l'extérieur ralentit et finit par converger vers une boucle carrée. La valeur de x_t oscille alternativement entre deux nombres distincts.

[2] Suite numérique.

C'est un *cycle de période deux*. Ainsi l'état stationnaire perd sa stabilité et devient périodique. En d'autres termes, le système commence à osciller.....

.....Si vous augmentez k jusqu'à environ 3,5, l'attracteur de période deux devient lui aussi instable, et un cycle de période quatre apparaît.... Pour 3,56 la période a doublé encore jusqu'à huit; pour 3,567 elle a atteint 16, et ensuite vous obtenez une séquence rapide de doublements jusqu'à des périodes de 32, 64, 128... (Si vous faites l'expérience sur votre ordinateur personnel, gardez s'il vous plaît en mémoire l'avertissement donné dans le chapitre 1 concernant les différentes marques d'ordinateurs qui donnent des résultats différents. Il en va de même pour tout ce qui suit.)
Cette *cascade de doublements de période* est si rapide que quand k = 3,58 ou à peu près, tout est terminé. La période a doublé un nombre infini de fois. A ce point, ayant fait de son mieux pour rester périodique en le payant par des périodes de plus en plus longues, l'application logistique devient chaotique.....

L'ordre dans le chaos

A partir de ce point, la musique devient de plus en plus chaotique. Pour la valeur maximale k = 4, l'air s'aventure densément à travers toute l'octave des notes disponibles. C'est-à-dire que, étant donné une trajectoire - une séquence de valeurs de x avec un point de départ donné -, il va passer aussi près que vous le désirez de tous les points de l'intervalle. L'intervalle tout entier s'est transformé en attracteur.
Tout cela a donc l'air assez simple. A mesure que k se déplace de 0 à 4, vous obtenez un accroissement régulier de la complexité du comportement dynamique:

stationnaire → périodique → chaotique

où la cascade de doublements de période est le mécanisme par lequel le chaos s'installe. Le « bouton de réglage » k ne fait que tout compliquer davantage à mesure que vous le tournez. Oh, ce n'est pas aussi simple que cela! Essayez, par exemple, la valeur k = 3,835, bien à l'intérieur du régime chaotique. Pour les cinquante premières itérations environ, tout a l'air bien comme il faut et chaotique, comme vous vous y attendez. Mais ensuite l'air change: *mi-sol-si-mi-sol-si...* se répétant indéfiniment. Période *trois* (figure 2). D'où *cela* provient-il?
D'après mon ordinateur, le cycle est:

0,1520744 → 0,4945148 → 0,9586346

Si vous augmentez k *très* doucement les périodes deviennent alors 6, 12, 24, 48, 96..... dans une nouvelle cascade de doublements de période!
Plus étonnant encore est ce qui se produit pour k = 3,739. Dans ce cas vous obtenez un cycle de période *cinq* (figure 3):

08411372 → 0,4996253 → 0,9347495 → 0,2280524 → 0,6582304

répété indéfiniment. Oui, à côté de cela vous trouverez des périodes 10, 20, 40, 80.....

Ce n'est pas une situation très confortable. Le bouton k n'est pas qu'un simple « générateur de chaos ». Il est faux de dire que le fait d'augmenter k rend toujours la dynamique plus compliquée. Au contraire, enterrées à l'intérieur du régime chaotique se trouvent de petites « fenêtres » de comportement régulier.
D'où viennent ces fenêtres? C'est une histoire compliquée, mais que l'on comprend bien maintenant. Nous savons même dans quel ordre les périodes surviennent. Le théorème fondamental fut démontré par un mathématicien russe, A.N. Sharkovski. Ecrivez les nombres entiers dans l'ordre suivant:

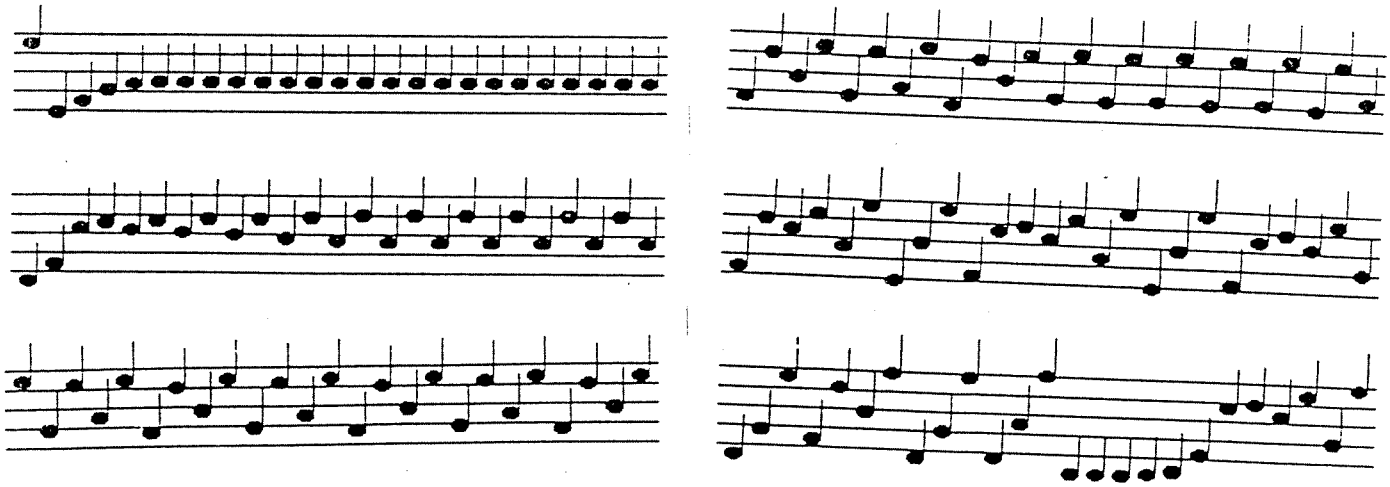
$$3 \rightarrow 5 \rightarrow 7 \rightarrow 9 \rightarrow 11 \rightarrow \ldots.$$
$$\rightarrow 6 \rightarrow 10 \rightarrow 14 \rightarrow 18 \rightarrow 22 \rightarrow \ldots.$$
$$\rightarrow 12 \rightarrow 20 \rightarrow 28 \rightarrow 36 \rightarrow \ldots\ldots$$
$$3 \times 2^n \rightarrow 5 \times 2^n \rightarrow 7 \times 2^n \rightarrow 9 \times 2^n \rightarrow \ldots\ldots$$
$$2^m \rightarrow 2^{m-1} \rightarrow \ldots\ldots \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1$$

D'abord, les nombres impairs en ordre *croissant*. Puis leurs doubles, quadruples, octuples... finalement les puissances de 2 en ordre *décroissant*. *Si*, pour une valeur donnée de k, l'application logistique a un cycle de période p, elle a dû avoir aussi des cycles de période *q* pour tout *q* tel que p → *q* dans ce classement. Ainsi les premiers cycles à apparaître ont des périodes 1, 2, 4, 8... - la cascade de doublements de période-. La période 17, par exemple, apparaît *avant* la période 15; mais avant celles-ci, la période 34 est apparue, et avant celle-ci des périodes telles que 44 ou 52 qui sont des multiples impairs de 4, et avant celles-ci 88 ou 104 ou 808 qui sont des multiples impairs de 8...
Mais ce qui confond vraiment l'imagination, c'est que ce même classement bizarre s'applique non seulement à des itérations de l'application logistique, mais aussi à des itérations de *n'importe quelle* application sur l'intervalle

unitaire à une seule bosse. Ce résultat fut le premier indice que quelques-uns des schémas du chaos pourraient être *universels*, à savoir non spécifiques d'exemples individuels mais représentatifs de *classes* entières de systèmes.

Grandes puces, petites puces...

Mais les fenêtres périodiques de l'application logistique ont un aspect encore plus étrange.
Il existe un moyen d'obtenir d'un seul coup un aperçu de tout le comportement dynamique de l'application logistique pour toutes les valeurs de k. Ce moyen est connu sous le nom de *diagramme de bifurcation*. Une bifurcation est un changement quelconque dans la forme qualitative de l'attracteur d'un système dynamique; et l'application logistique est tout simplement envahie de bifurcations.
Voici la manière de l'obtenir. Tracez un graphique avec k en abscisses et x en ordonnées. En regard de chaque valeur de k, tracez les valeurs de x qui se trouvent sur l'attracteur pour ce k donné. Chaque tranche verticale donne alors une image, dans l'intervalle compris entre 0 et 1, de l'attracteur correspondant. Ainsi, par exemple, quand k est inférieur à 3, il n'existe qu'un seul attracteur ponctuel, et vous ne devez marquer qu'une seule valeur de x. Cela donne une courbe.
Ceux qui possèdent un ordinateur personnel aimeraient peut-être faire l'expérience, avant de continuer à lire. Imaginez un graphique où k, en abscisses, va de 0 à 4 par étapes de 0,2 par exemple. Tracez x en ordonnées, entre 0 et 1. (Vous devrez élargir les échelles pour voir quelque chose.) Pour chaque valeur de k, itérez x pour quelques centaines d'étapes *sans* tracer de points, puis continuez encore pour une vingtaine d'étapes supplémentaires, traçant les valeurs de x au-dessus du k choisi.



La musique du chaos (k=2 - k=3,2 - k=3,56 - k=3,6 - k=3,8 - k=4)

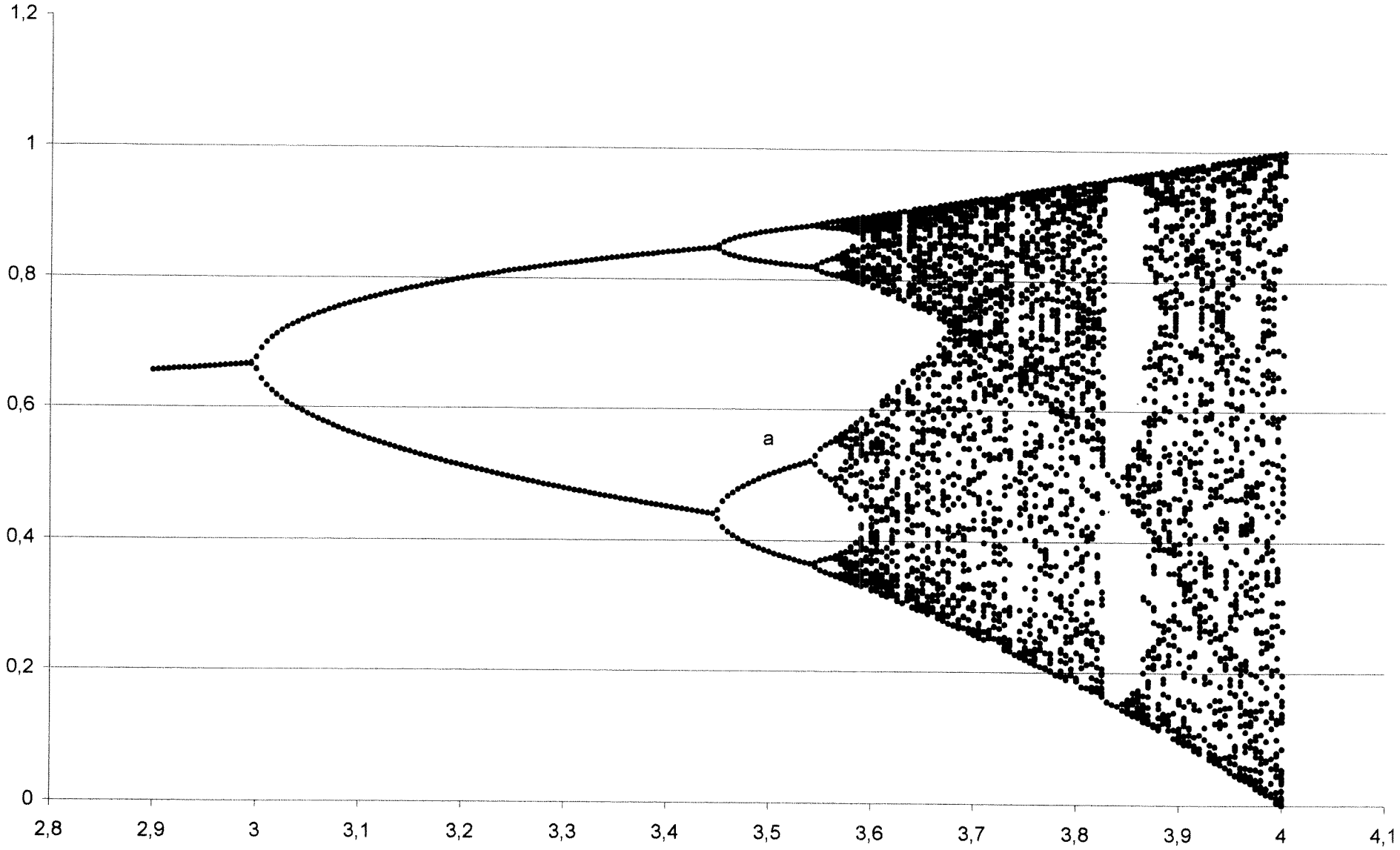


Diagramme de bifurcation

Première approche de la situation présentée

Il s'agit dans cette activité de vérifier un certain nombre d'affirmations de l'auteur en revenant sur quelques théorèmes importants d'analyse

1. Paragraphe d'introduction:

Etudier la fonction f_k définie sur [0;1] par $f_k(x) = kx(1-x)$ et vérifier toutes les affirmations du paragraphe. Vérifier également que f_k a deux points fixes[1] pour $1< k \leq 4$: 0 et $\frac{k-1}{k}$.

2. Régime stationnaire. (On choisira toujours pour x_0 un réel de]0;1[ )

a) Etude du cas $0 < k < 1$.

Posons I= [0;1]

Démontrer par récurrence que pour tout n, $x_n \in I$.

Démontrer que pour tout $x \in I$ on a $|f'(x)| \leq k$. En déduire à l'aide de l'inégalité des accroissements finis que pour tout n, $|x_{n+1}| \leq k|x_n|$ puis que $|x_n| \leq k^n$

Montrer que (x_n) converge vers 0.

L'étude que nous venons de faire et celles qui suivent sont basées sur l'utilisation de l'inégalité des accroissement finis:

Si f est dérivable sur un intervalle I, que pour tout x de I $|f'(x)| \leq \lambda$ *alors pour tout* α *et* β *de I on a* $|f(\beta) - f(\alpha)| \leq \lambda|\beta - \alpha|$.

On applique l'inégalité avec α *point fixe de f et* $\beta = x_n$. *Il convient donc de choisir un intervalle I contenant* α *et tous les termes de la suite (sauf peut-être les premiers). On démontre ensuite par récurrence que* $|x_n - \alpha| \leq \lambda^n|x_0 - \alpha|$ *qui implique la convergence de la suite vers* α *dès que* $\lambda<1$.

Finalement le choix de l'intervalle I doit répondre à trois conditions:

1. $\alpha \in I$.
2. *A partir d'un certain rang, pour tout n,* $x_n \in I$.
3. *pour tout x de I* $|f'(x)| \leq \lambda < 1$.

b) Etude du cas: k= 1,5. L'étude de f nous permettra de choisir par exemple $I = \left[\frac{1}{4};\frac{1}{2}\right]$

c) Etude du cas: k=2,5. L'étude de f nous permettra de choisir par exemple $I = \left[\frac{11}{20};\frac{13}{20}\right]$

d) Etude d'un cas particulier: k=2

Que pensez vous des affirmations de l'auteur qui dit que dans le cas où k=2 et x_o=0,9 on a x_7=0,5 ? x_8=0,5 ?

Démontrer que $\left|x_n - \frac{1}{2}\right| = \frac{1}{2}\left(2\left|x_0 - \frac{1}{2}\right|\right)^{2^n}$. Démontrer que la suite converge.

[1] Les points fixes de f sont les solutions de l'équation f(x)=x.

La méthode utilisée dans les questions précédentes est imparfaite dans la mesure où la présence d'un intervalle "attracteur" (l'intervalle I) ne garantit pas la convergence dans le cas où $x_0 \notin I$. Pour cela il nous faudra utiliser deux nouveaux arguments:

Premier théorème:
Toute suite croissante et majorée de nombres réels est convergente dans $\mathbb{R}$ (de même toute suite décroissante et minorée converge dans $\mathbb{R}$).

Ce théorème est lié à la structure de l'ensemble des nombres réels (on dit que $\mathbb{R}$ est complet). Il est mis en défaut si on se place dans Q l'ensemble des rationnels. On montre par exemple que les nombres $v_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots\ldots + \frac{1}{n!}$ *qui sont tous rationnels tendent vers le nombre e qui lui est irrationnel.*

Dans les cas qui nous intéressent, ce théorème s'avère insuffisant car il ne donne pas d'indication sur la limite éventuelle de la suite. Il convient de l'associer au

Deuxième théorème:
f étant une fonction continue (ce qui est le cas de toute fonction dérivable)sur un intervalle J et à valeurs dans J.La suite (u_n) étant définie par $u_0 \in J$ et pour tout n, $u_{n+1}=f(u_n)$.
Si (u_n) converge vers α, alors $f(\alpha)=\alpha$.

Ce deuxième théorème indique que les seules limites possibles sont les points fixes de la fonction f, or nous les connaissons tous.

Examinons le cas $1<k<2$.

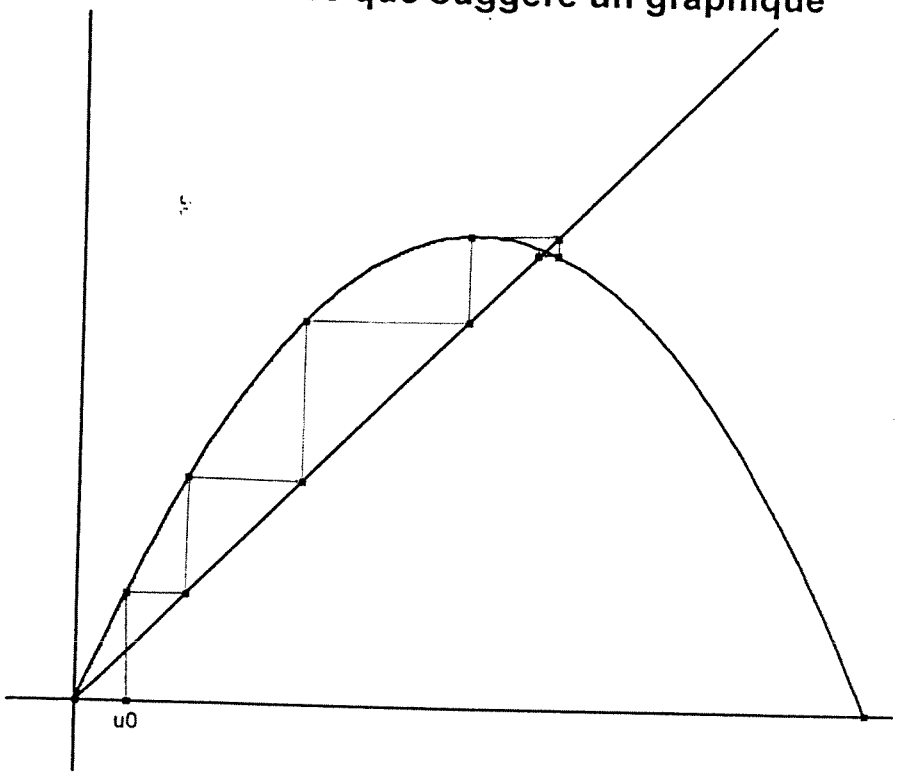
Le point fixe $\alpha_k = \frac{k-1}{k}$ de f_k est dans l'intervalle [0;0,5].

a) $0 < x_0 \leq \alpha_k$. Démontrer que la suite (x_n) est croissante et majorée. Conclure.

b) $\alpha_k \leq x_0 \leq \frac{1}{2}$. Démontrer que la suite (x_n) est décroissante et minorée. Conclure.

c) $\frac{1}{2} \leq x_0 < 1$. Démontrer que $0 < x_1 \leq \frac{1}{2}$. Conclure.

Démontrer ce que suggère un graphique



On a tracé la courbe représentative (C) de la fonction f définie sur [0;1] par $f(x) = kx(1-x)$ pour k=2,4 ainsi que la droite (D), d'équation y=x. Les abscisses des points construits sont les termes successifs de la suite $(u_n)_{n\in N}$ définie par $u_{n+1} = f(u_n)$ et u_0 donné.

Décrire et justifier cette construction.

Dans les deux premières parties, on conserve la valeur k=2,4.

Partie 1: Description et analyse graphique

Comme le titre de cette partie l'indique, il ne s'agit pas ici de démontrer des résultats, mais seulement de les découvrir et les préciser.

1. On constate que les premiers termes de la suite vont en croissant jusqu'à un certain rang p (p=4 pour la valeur de u_0 choisie sur la figure), puis semblent osciller autour d'une valeur limite α. Calculer α.
2. a) Prenez d'autres valeurs de u_0 dans l'intervalle [0;0,5]. Quel semble être le comportement de la suite ?
   b) Calculer b=f(0,5).
   c) Que se passe-t-il si on choisit $u_0 \in [0,5;b]$?
   d) Que se passe-t-il si on choisit $u_0 \in [b;1]$?

Partie 2: Justification des résultats

A partir de maintenant il ne s'agit plus simplement de regarder ce qui se passe, mais de démontrer ce qui a été mis en évidence.

1. $u_0 \in [0,5;b]$.
   a) Quel théorème d'analyse permet de comparer $|u_{n+1} - \alpha|$ et $|u_n - \alpha|$?
   b) Quelles sont les hypothèses nécessaires à une bonne application de ce théorème?

c) Vérifier que pour tout n, $u_n \in [0,5;0,6]$ et que pour tout $x \in [0,5;0,6]$, on a $|f'(x)| \leq 0,48$.

d) Montrer que $|u_n - \alpha| \leq 0,1 \times (0,48)^n$. Conclure.

2. $u_0 \in]0;0,5]$

L'étude graphique faite dans la première partie nous conduit à conjecturer qu'il existe un rang n_0 pour lequel on a $u_{n_0} \in [0,5;0,6]$. Nous allons démontrer cette propriété par l'absurde.

Pour cela supposons que pour tout n on a $u_n \in]0;0,5]$.

Montrer que dans ce cas la suite est croissante et majorée. Que peut-on en déduire? Pourquoi y a-t-il une contradiction avec l'hypothèse?

A ce stade de notre travail, nous savons qu'il existe un entier n_0 pour lequel $u_{n_0} \in [0,5;0,6]$.

Nous pouvons donc appliquer les résultats de la question 1. à la suite obtenue en choisissant comme premier terme u_{n_0} ce qui démontre la convergence vers α.

3. Etudier le cas : $u_0 \in [b;1[$.

Partie 3 : Recherche des valeurs de k pour lesquelles la situation reste identique.

1. Etudier les variations de f et la position de sa courbe représentative par rapport à la droite d'équation y=x lorsque $k \in [0;1]$. Démontrer que pour toute valeur de $u_0 \in]0;1[$ la suite est décroissante et minorée. Quelle est sa limite ?

2. Etudier les variations de f et la position de sa courbe représentative par rapport à la droite d'équation y=x lorsque $k \in [1;2]$. Etudier graphiquement le comportement de la suite en fonction de la valeur de u_0.

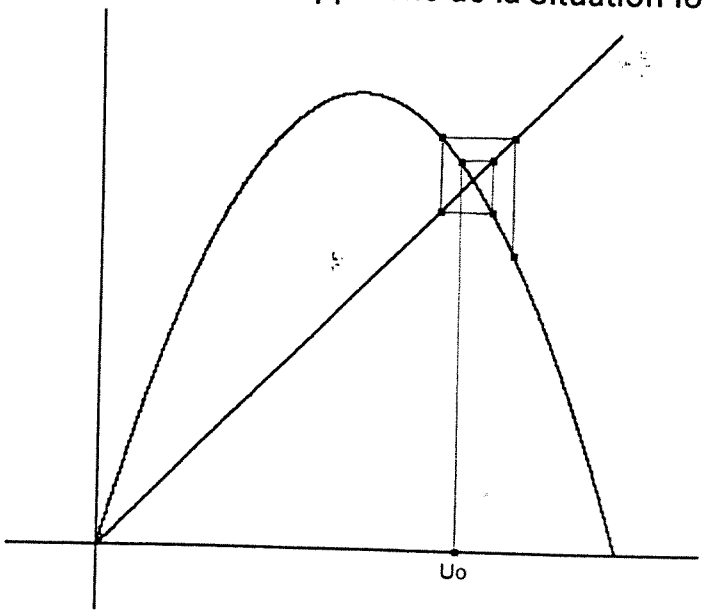
3. $k \in [2;4]$.

a) Vérifier que $f\left(\frac{1}{2}\right) = \frac{k}{4}$ et que $f\left(\frac{k}{4}\right) \leq \frac{k}{4}$.

b) Montrer que les conditions $f\left(\frac{k}{4}\right) \geq \frac{1}{2}$ et $\left|f'\left(\frac{k}{4}\right)\right| < 1$ sont suffisantes pour que l'on puisse conclure de la même manière que dans la partie 2.

c) Quelles sont les valeurs de k qui vérifient simultanément $f\left(\frac{k}{4}\right) \geq \frac{1}{2}$ et $\left|f'\left(\frac{k}{4}\right)\right| < 1$. (on pourra remarquer que 2 est solution de l'équation $x^2(1-x/4)=2$).

Partie 4: Première approche de la situation lorsque k>3



Pour k= 3,5 l'étude graphique montre qu'en choisissant un premier terme de la suite proche du point fixe α les termes suivant de la suite semblent s'en éloigner. Il n'y a donc apparemment pas convergence dans cette situation. La justification de cette propriété réside à nouveau dans l'inégalité des accroissements finis:

a) Démontrer que si $3<k<4$ on a $|f'(\alpha)|>1$.

Dans ce cas on peut choisir un intervalle I centré sur α et un réel λ tel que pour tout $x \in I$ on a $|f'(x)| \geq \lambda > 1$.[1]

b) Démontrer que si $u_n \in I$ $u_n \neq \alpha$ on a $|u_{n+1} - \alpha| \geq \lambda |u_n - \alpha|$.

Cette dernière inégalité montre bien que les termes de la suite s'éloignent de α. Dés lors pour qu'il y ait convergence (α est la seule limite possible) il faudrait qu'à partir d'un certain rang, on ait $u_n = \alpha$.

c) Résoudre l'équation $f(x)= \alpha$. Résoudre l'équation $f(x)= 1/k$. Démontrer qu'il existe une infinité de valeur de u_0 pour lesquelles la suite définie par u_0 et $u_{n+1}=f(u_n)$ est constante à partir d'un certain rang.

Pour visualiser cette dernière propriété, on peut "dérouler la toile d'araignée" à partir de α.

Bien que l'on puisse trouver une infinité de points de départ nous donnant une suite constante à partir d'un certain rang, on démontre que si l'on choisit "au hasard" un réel de l'intervalle [0;1] la probabilité que la suite soit divergente est égale à 1.

On peut également imaginer d'autres situations "pathologiques". En particulier, la fonction pourrait fournir des suites périodiques. C'est ce cas que nous allons étudier dans l'activité suivante.

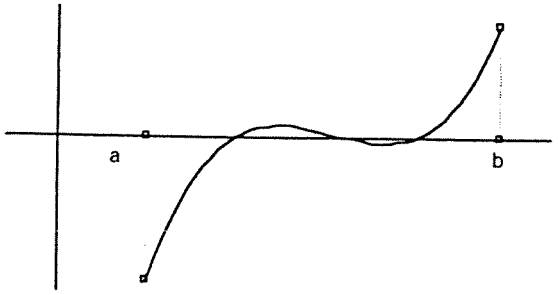
[1] Cette propriété que nous admettrons ici résulte de la continuité de f'.

Cycles d'une fonction

Pour traiter la partie suivante, nous aurons besoin d'une propriété des fonctions continues: Le théorème des valeurs intermédiaires.

***Weierstrass**(1815/1897) fut le premier à introduire le concept de fonction continue (nous n'en donnerons pas la définition ici) de manière rigoureuse. Notons simplement que toute fonction dérivable sur un intervalle est continue sur cet intervalle*[1]*. Ainsi toutes les fonctions définies sur un intervalle que vous avez rencontrées durant vos études étaient des fonctions continues (car elles étaient dérivables).*

***Théorème des valeurs intermédiaires** (version simplifiée):*
Soit f une fonction continue sur un intervalle [a,b] à valeurs dans $\mathbb{R}$.
Si f(a) et f(b) sont de signes contraires alors l'équation f(x)=0 admet (au moins) une solution dans [a,b].



Soit f une fonction définie et continue sur [0;1] qui prend ses valeurs dans l'intervalle [0;1], c'est à dire que, pour tout $x\in[0;1]$, $f(x)\in[0;1]$.

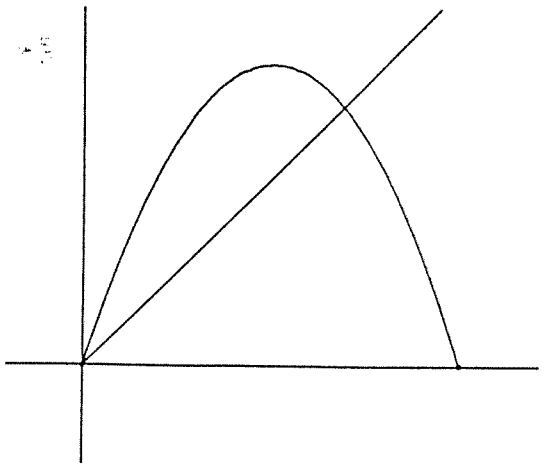
1. On veut montrer que l'équation f(x)=x admet au moins une solution α dans [0;1].
a) Interpréter graphiquement ce résultat.
b) Soit h la fonction définie par h(x)=f(x)-x. Démontrer que l'équation h(x)=0 admet au moins une solution sur [0;1]. Conclure.

2. On suppose qu'il existe deux réels distincts x_1 et x_2 de l'intervalle [0;1] tels que
$f(x_1) = x_2$ et $f(x_2) = x_1$.
a) Interpréter graphiquement cette condition.
b) On pose $g(x) = f \circ f(x)$. Calculer $g(x_1)$, $g(x_2)$ et $g(\alpha)$.
c) On suppose en plus que f est dérivable sur [0;1].
Montrer que g est dérivable sur [0;1], que $g'(x_1) = g'(x_2)$ et que
$$g'(\alpha) = (f'(\alpha))^2$$
d) Construire une courbe représentant une fonction g ayant toutes ces propriétés.
(commencer par placer le point d'abscisse α et la tangente en ce point.)

3. Dans cette question $f(x) = kx(1-x)$ avec $x\in[0;1]$ et $k\in[0;4]$.
a) Démontrer que les solutions de l'équation f(x)=x sont aussi solution de l'équation g(x)=x. Résoudre cette équation .On pourra vérifier que:
$$g(x) = x \Leftrightarrow x(kx+1-k)(k^2x^2-(k+k^2)x+(1+k)) = 0$$
Pour quelles valeurs de k cette équation a-t-elle quatre solutions réelles distinctes ?
d) Représenter graphiquement f et g pour k=3,2

[1] Attention la réciproque est fausse. Il existe des fonctions continues qui ne sont pas dérivables.

4. Dans cette question on suppose que f est dérivable et admet une représentation graphique du type suivant:



a) Expliquer pourquoi :

$0 < x < \alpha \Rightarrow f(x) > x$

$x > \alpha \Rightarrow f(x) < \alpha < x$

On suppose en plus qu'il existe trois réels a, b, c distincts de l'intervalle [0;1] vérifiant f(a)=b; f(b)=c et f(c)=a et on définit la fonction φ par $\varphi = f \circ f \circ f$.

a) Calculer φ (a), φ(b) et φ (c).

b) Montrer que φ est dérivable et que $\varphi'(a) = \varphi'(b) = \varphi'(c)$.

c) Démontrer qu'il existe x_1 et x_2 distincts tels que $f(x_1)=x_2$ et $f(x_2)=x_1$.

L'étude des itérées de la fonction f donne des informations sur le comportement de la suite (u_n). En effet, les données de u_0 et de $g = f \circ f$ permettent de calculer tous les termes de rang pair de la suite $(u_{n+2} = g(u_n))$. De même avec la donnée de u_1, on connaît les termes de rang impair. Prenons par exemple le cas étudié à la fin de la question 3. La courbe tracée (correspondant à k=3,2) a trois points d'intersection avec la droite d'équation y=x. L'un d'entre eux (celui du milieu) correspond à la valeur α. En ce point la tangente a un coefficient directeur supérieur à 1, ce qui nous permet de constater qu'il n'y a pas convergence $(g'(\alpha) > 1$ et $g'(\alpha) = (f'(\alpha))^2$ implique $|f'(\alpha)| > 1)$. Les deux autres points d'abscisses β et γ sont attractifs $(|g'(\beta)| = |g'(\gamma)| < 1)$: les sous-suites (u_{2n}) et (u_{2n+1}) vont converger l'une vers β, l'autre vers γ. Ces constatations, faites sur un graphique, nécessitent bien sur des justifications (que nous ne donnerons pas ici) mais l'une des plus importantes conséquences vient du fait que ces phénomènes ne dépendent que de la forme de la représentation graphique de f. Autrement dit, toute autre fonction ayant les mêmes propriétés que f fournira des suites de même nature. C'est là le phénomène universel dont parle Ian Stewart. Dans la dernière activité, nous allons voir que l'on peut construire la courbe représentant $f \circ f = g$ à partir de celle de f et étudier certaines situations rencontrées.

Construction de la représentation graphique de g=fof à partir de celle de f.

La fonction f considérée est une fonction définie sur [0;1] et à valeurs dans [0;1].
On pourra pour les constructions, utiliser les courbes données en annexe.

1. Symétries

La courbe représentative de f admet la droite d'équation $x = \frac{1}{2}$ comme axe de symétrie.

Démontrer que c'est aussi le cas pour la courbe représentative de g.

2. Premier cas

La fonction f est croissante sur $\left[0;\frac{1}{2}\right]$ et $m = f\left(\frac{1}{2}\right) \leq \frac{1}{2}$.

a) Démontrer que g est croissante sur $\left[0;\frac{1}{2}\right]$.

b) En utilisant la droite d'équation y=x, construire le point de coordonnées $\left(\frac{1}{2};g\left(\frac{1}{2}\right)\right)$.

c) Compléter la représentation graphique de g.

3. Deuxième cas.

La fonction f est strictement croissante sur $\left[0;\frac{1}{2}\right]$ et $m = f\left(\frac{1}{2}\right) > \frac{1}{2}$.

a) Démontrer qu'il existe un unique réel $\beta \in \left[0;\frac{1}{2}\right]$ tel que $f(\beta) = \frac{1}{2}$.

b) Démontrer que g est croissante sur $[0; \beta]$ et décroissante sur $\left[\beta,\frac{1}{2}\right]$.

c) Construire la courbe représentative de g

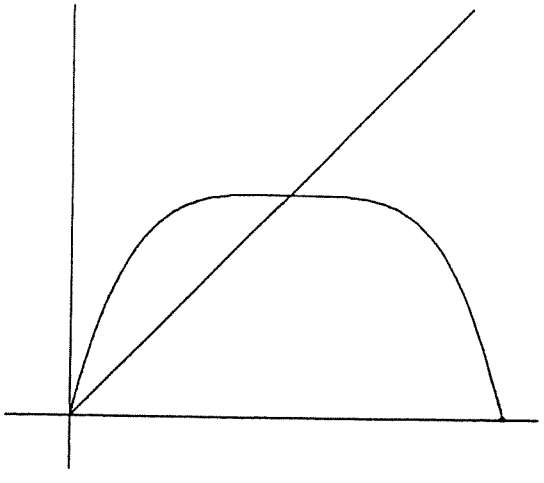
4. Courbes et équations

On suppose ici que $f(x) = kx(1-x)$ avec $k \in [0;4]$.

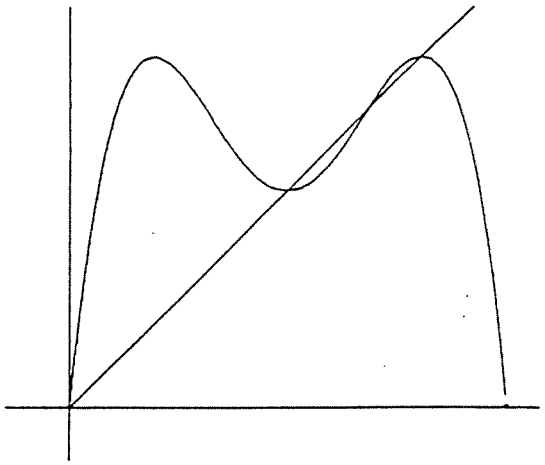
a) Exprimer m en fonction de k.

b) Pour $k \in]2;4]$, exprimer β en fonction de k.

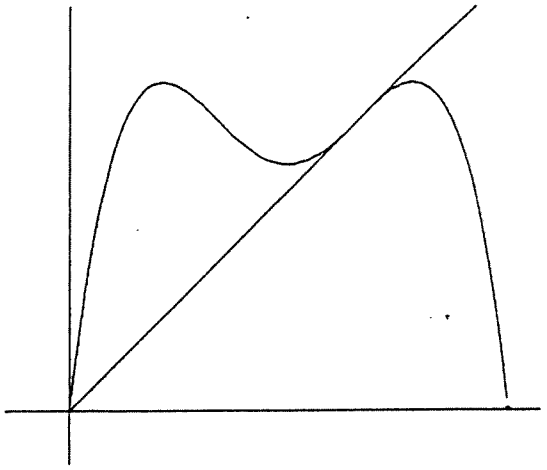
c) On donne une première courbe représentant g. La droite d'équation y=x coupe la courbe au point d'abscisse 0,5.
Déterminer la valeur correspondante de k.
On visualise bien dans ce cas la convergence des termes pairs et impairs vers la même valeur.



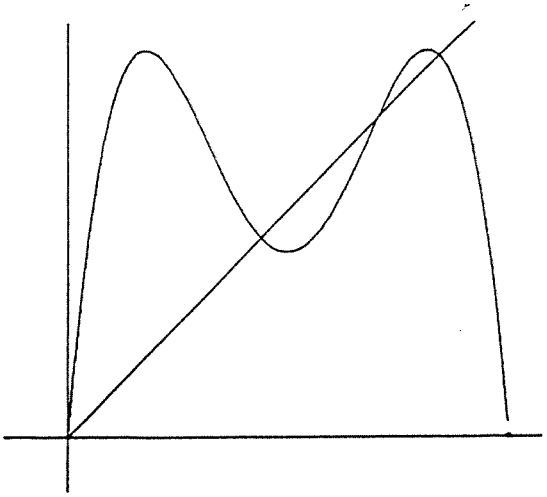
d) Ici également la droite d'équation y=x coupe la courbe de g au point d'abscisse 0,5.
Déterminer k .
Montrer que $g(1-\beta) = 1-\beta$ et que $g'(1-\beta) = 0$
Quel sera le comportement de la suite (u_n) ?
Vérifier ce résultat à l'aide d'une calculatrice en choisissant différentes valeurs de u_0.



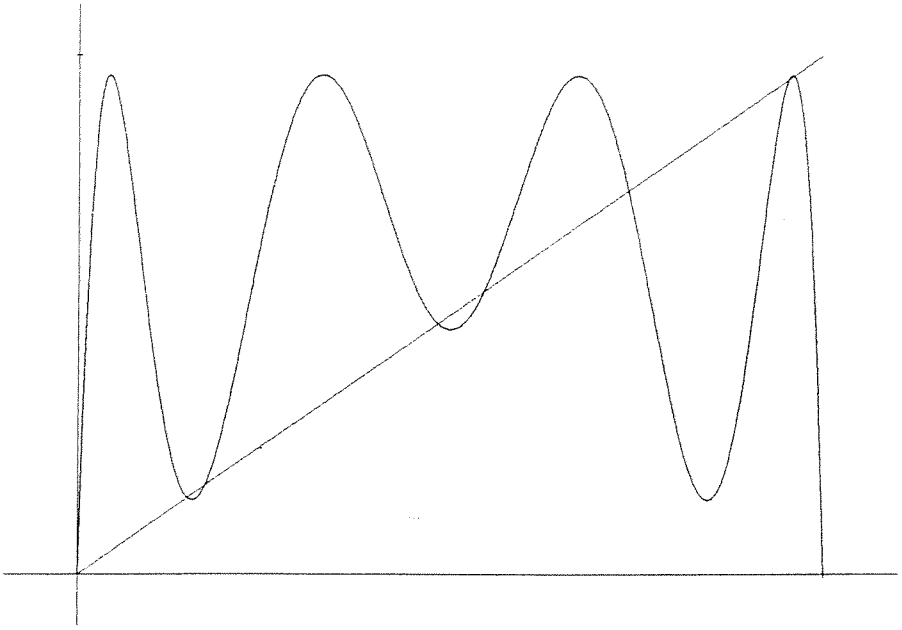
e) Ici la droite d'équation y=x est tangente à la courbe représentative de g.
Déterminer k.

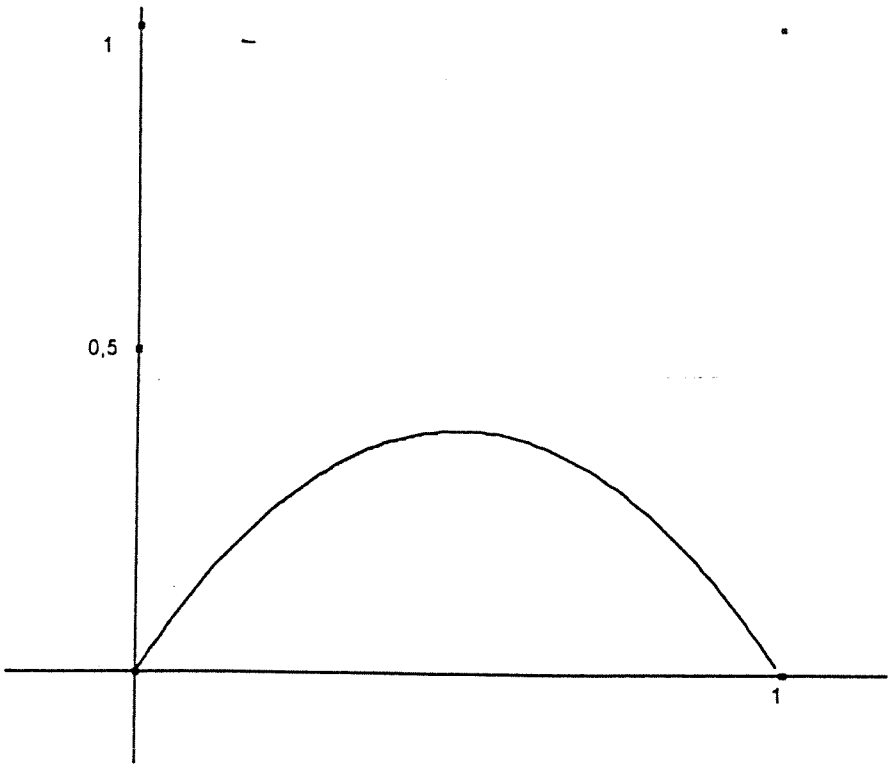


f) Ici la tangente en deux des points d'intersection a comme coefficient directeur (-1).
Déterminer k.

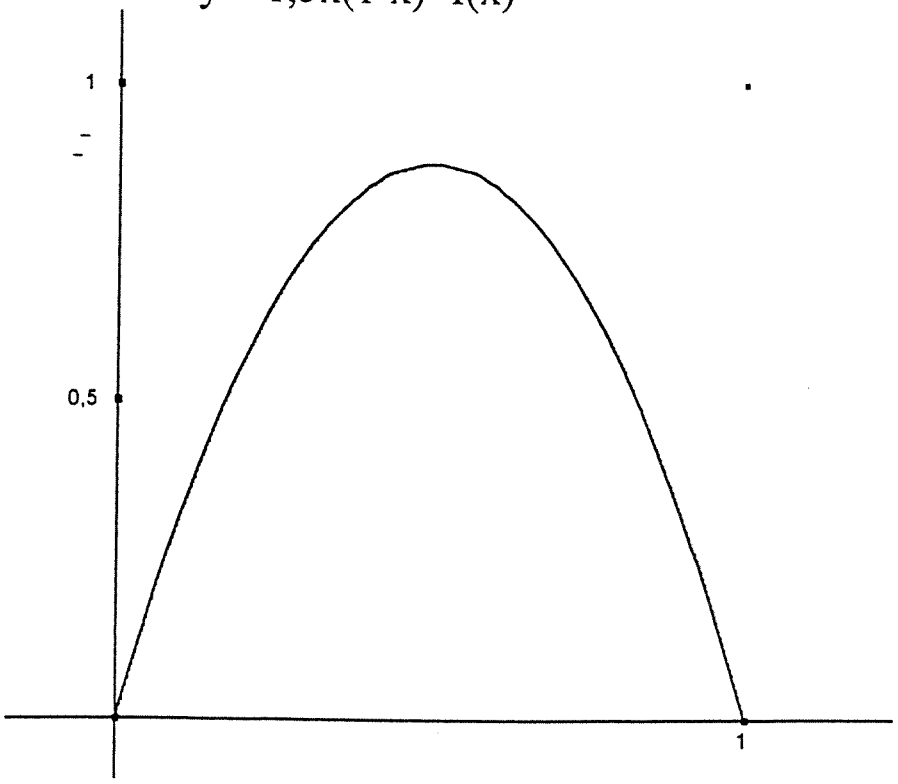


g) On a représenté $y = f \circ f \circ f(x)$ ci-dessous pour k=3,845. Quel va être le comportement de la suite (u_n) ?





$y = 1{,}5x(1-x)=f(x)$



$y = 3{,}5\ x\ (1-x) = f(x)$

Indications de solutions

Première approche:

1. $f'_k(x) = k(1-2x)$ s'annule et change de signe en x=1/2, donc f_k admet un maximum pour x=1/2 égal à k/4. Pour $k \in [0;4]$, et $x \in [0;1]$,on a $f_k(x) \in [0;1]$.

$f_k(x) = x \Leftrightarrow kx(1-x) - x = 0 \Leftrightarrow x(k - kx - 1) = 0$ qui a deux racines , 0 et $\frac{k-1}{k}$.

2. a) $0<k<1$.

$x_0 \in$ I. Si $x_n \in$ I, d'après la question précédente $x_{n+1}=f(x_n) \in$I. Ceci démontre bien que pour tout n, $x_n \in$ I.

D'autre part $f'_k(x) = k(1-2x)$ est affine décroissante donc sur I $f'_k(0) \geq f'_k(x) \geq f'_k(1)$. On en tire que $-k \leq f'_k(x) \leq k$ et donc que $|f'(x)| \leq k$. D'après l'inégalité des accroissements finis, pour tout a et b dans I $|f(b) - f(a)| \leq k|b-a|$. On peut choisir $b=x_n$ et $a=0$ car ils sont tous deux dans I ce qui donne: pour tout n, $|x_{n+1}| \leq k|x_n|$. Enfin, on en déduit, par récurrence que $|x_n| \leq k^n$. Comme k^n tend vers 0 à l'infini ($0<k<1$), (x_n) converge vers 0.

b) k=1,5. $I = \left[\frac{1}{4};\frac{1}{2}\right]$. $x_0 \in$I. Dans la suite f_k est notée f. f est croissante sur I , f(1/4)=9/32 $\in$I , f(1/2)=3/8 $\in$I donc si $x \in$I , $f(x) \in$I. Par récurrence, on obtient que pour tout n, $x_n \in$I. Le point fixe (k-1)/k=1/3 $\in$I. D'autre part, f' est décroissante, f'(1/4)=3/4, f'(1/2)=0 donc $|f'(x)| \leq \frac{3}{4}$ pour tout x de I. L'inégalité des accroissements finis appliquée à x_n et 1/3 donne: $\left|x_{n+1} - \frac{1}{3}\right| \leq \frac{3}{4}\left|x_n - \frac{1}{3}\right|$ et par récurrence on obtient : $\left|x_n - \frac{1}{3}\right| \leq \left(\frac{3}{4}\right)^n \left|x_0 - \frac{1}{3}\right| \leq \left(\frac{3}{4}\right)^n \times \frac{1}{2}$.

Ceci nous prouve que x_n converge vers 1/3.

c) k=2,5. $I = \left[\frac{11}{20};\frac{13}{20}\right]$. Ici f décroît sur I. f(11/20)=495/800 $\in$I , f(13/20)=455/800 $\in$I. On démontre toujours de la même manière que $x_n \in$I. Le point fixe est ici 3/5 ($\in$I). Le calcul de f' donne $-\frac{3}{4} \leq f'(x) \leq -\frac{1}{4}$ donc $|f'(x)| \leq \frac{3}{4}$ pour tout x de I. L'inégalité des accroissements finis appliquée à x_n et 3/5 suivie d'une récurrence nous donne $\left|x_n - \frac{3}{5}\right| \leq \frac{1}{10}\left(\frac{3}{4}\right)^n$ ce qui montre la convergence de x_n vers 3/5.

d) k=2. Il n'est pas possible qu'il y ait égalité x_n=0,5 sans que x_{n-1}=0,5 ce qui nous conduirait à x_0=0,5. Cependant, dans cette situation, la convergence de la suite vers 0,5 est tellement rapide que pour une calculatrice la suite devient très rapidement stationnaire.

$$\left|x_{n+1} - \frac{1}{2}\right| = \left|2x_n(1-x_n) - \frac{1}{2}\right| = \left|-\frac{4x_n^2 - 4x_n + 1}{2}\right| = 2\left|x_n - \frac{1}{2}\right|^2 = \frac{1}{2}\left(2\left|x_n - \frac{1}{2}\right|\right)^2 . \quad (*)$$

En appliquant le résultat (*) pour n=0, on trouve que la propriété est fondée.

Supposons que pour n fixé, on ait $\left|x_n - \frac{1}{2}\right| = \frac{1}{2}\left(2\left|x_0 - \frac{1}{2}\right|\right)^{2^n}$, alors

$$\left|x_{n+1}-\frac{1}{2}\right| = \frac{1}{2}\left(2\left|x_n-\frac{1}{2}\right|\right)^2 = \frac{1}{2}\left(2\frac{1}{2}\left(2\left|x_0-\frac{1}{2}\right|\right)^{2^n}\right)^2 = \frac{1}{2}\left(2\left|x_0-\frac{1}{2}\right|\right)^{2\times 2^n} = \frac{1}{2}\left(2\left|x_0-\frac{1}{2}\right|\right)^{2^{n+1}}$$

La propriété est bien démontrée par récurrence. Comme $x_0 \in]0\ ;1[$, $2\left|x_0-\frac{1}{2}\right| < 1$ qui démontre la convergence de x_n vers ½.

De plus, en posant $e_n = \left|x_n-\frac{1}{2}\right|$. (*) nous donne $e_{n+1} = 2(e_n)^2$. Donc

$e_n < 10^{-k} \Rightarrow e_{n+1} < 2.10^{-2k}$ qui montre que le nombre de décimales exactes dans l'approximation de ½ par x_n double pratiquement à chaque étape du calcul.

Le cas : $1<k<2$

a) La fonction f est croissante sur [0;0,5] donc sur $[0;\alpha_k]$. Par hypothèse $0 < x_0 \le \alpha_k$. De plus, si $0 < x_n \le \alpha_k$ alors $f(0) < f(x_n) \le f(\alpha_k)$ puisque f croît et donc $0 < x_{n+1} \le \alpha_k$ ce qui démontre par récurrence que (x_n) est majorée.

D'autre part, comme $1<k$ on a $f(x) \ge x$ pour tout x de l'intervalle $[0;\alpha_k]$. Cette remarque permet d'établir par récurrence que (x_n) est croissante. Finalement la suite est croissante et majorée donc convergente. Sa limite est un point fixe de f supérieur à x_0. C'est donc α_k.

b) Le même argument que précédemment permet d'établir que (x_n) est minorée par α_k. La croissance de f implique ici la décroissance de (x_n). En effet, $x_0 > \alpha_k$ implique $f(x_0) < x_0$ et donc $x_1 < x_0$. Si $x_n < x_{n-1}$, par croissance de f, $f(x_n) < f(x_{n-1})$ soit $x_{n+1} < x_n$. (Ceci montre par récurrence la décroissance de (x_n)). La suite est décroissante et minorée donc convergente vers un point fixe de f qui ne peut être dans ce cas que α_k.

c) $\frac{1}{2} \le x_0 < 1$. L'étude de f montre que l'image de l'intervalle [0,5;1] est une partie de l'intervalle [0;0,5]. Donc $0 \le x_1 \le 0,5$. On est donc ramené à l'un des deux cas précédents qui impliquent tous deux la convergence vers α_k.

Démontrer ce que suggère un graphique

partie 2

1.a) et b) Il s'agit de l'inégalité des accroissements finis. Pour pouvoir l'appliquer, il faut déterminer un intervalle contenant α ($\alpha = f(\alpha)$) et tous les termes de la suite (u_n) sur lequel la valeur absolue de la dérivée de f est majorée.

c) $b = 0,6 = f(0,5)$.

La fonction f est décroissante sur I=[0,5;0,6] donc

pour $0,5 \le x \le 0,6$, on a $f(0,5) \ge f(x) \ge f(0,6)$.

Finalement $0,556 \le f(x) \le 0,6$. Ceci montre que $f(I) \subset I$. On peut alors facilement démontrer par récurrence que pour tout n, $u_n \in I$ (car $u_0 \in I$).

La dérivée f' est négative sur I (et décroissante) donc $|f'(x)| \le |f'(0,6)| = 0,48$.

En appliquant l'inégalité des accroissements finis à f, on obtient $|u_{n+1}-\alpha| \le 0,48 \times |u_n-\alpha|$.

On démontre alors par récurrence que : $|u_n-\alpha| \le 0,1 \times (0,48)^n$. Le deuxième membre tend vers 0 donc (u_n) tend vers α.

2. $u_0 \in [0;0,5]$.

On suppose que pour tout n, $u_n \in [0;0,5]$. D'une part la suite u est bornée. D'autre part, pour tout $x \in [0;0;5]$, on a $f(x) \geq x$ ce qui permet de démontrer par récurrence que la suite est croissante. Toute suite croissante et majorée converge donc u converge vers une limite a avec $0 < a \leq 0,5$

De plus $f(a)=a$. Il y a donc bien contradiction puisque l'équation $f(x)=x$ n'a pas de solution dans l'intervalle]0;0,5]. Il existe donc un rang n_0 pour lequel $u_{n_0} \geq 0,5$ et comme b est le maximum de f sur [0;1] on a $u_{n_0} \in [0,5;b]$.

3. $u_0 \in [b;1]$.

Dans ce cas $u_1 \in [0;b]$. Ainsi quitte à oublier u_0 et à renuméroter les termes de la suite, on se ramène à l'un des deux cas étudiés précédemment.

Partie 3:

1. Pour $k \in [0;1]$, $f(x) \leq x$ pour tout $x \in [0;1]$. On démontre alors par récurrence que la suite est décroissante et minorée par 0. Elle converge donc vers la seule limite possible (solution de $f(x)=x$) qui est 0.

2. $f(x) \leq x \Leftrightarrow x \geq \alpha$ donc la courbe est située en dessous de la droite d'équation y=x si et seulement si $x \geq \alpha$.Pour $k \in [1;2]$, $\alpha \leq 0,5$. Si $x \leq \alpha$, $x \leq f(x) \leq \alpha$.

Donc si $u_0 \leq \alpha$, la suite est croissante et majorée donc convergente vers α (seule limite possible). Si $u_0 > \alpha$ alors $u_1 \leq \alpha$ et donc la suite est croissante et majorée par α (à partir du rang 1) et donc à nouveau convergente vers α.

3. $k \in [2;4]$.

a) $f(1/2)=k/4$. Le maximum de f est atteint en 1/2 donc $f(k/4) \leq f(1/2)=k/4$.

b) Le même raisonnement que dans la partie 2 permet d'affirmer qu'il existe un rang n_0 pour lequel $u_{n_0} \in [0,5;k/4]$. Plaçons-nous dès lors sur l'intervalle $I=\left[\frac{4-k}{4};\frac{k}{4}\right]$. Le milieu de cet intervalle est 1/2 donc pour des raisons de symétrie, la valeur absolue de la dérivée est strictement majorée par 1 (puisque $|f'(k/4)| < 1$). De plus, pour tout $x \in I$, $f(x) \in I$. On peut donc appliquer l'inégalité des accroissements finis à u_n ($n > n_0$) et à α. Ceci démontrera la convergence de u_n vers α.

c) $f(k/4) \geq 1/2$ nous donne $k \geq 2$. Donc $f'(k/4)=k-k^2/2$ est négatif. La condition devient $k-k^2/2>-1 \Leftrightarrow k^2-2k-2>0$. Finalement $k \in [2\ ;1+\sqrt{3}]$.

Partie 4:

a) $f'(\alpha) = k - 2k\alpha = 2 - k < -1$ pour $3<\mathbf{k}<4$.

b) Encore l'inégalité des accroissements finis.

c) $f(x)= \alpha \Leftrightarrow x=1/k$ ou $x=\alpha$.

$f(x)=1/k \Leftrightarrow x = \frac{k \pm \sqrt{k^2-4}}{2k}$. Appelons α_1 le plus petit de ces deux nombres : $\alpha_1 \in]0;0,5[$.

L'équation $f(x)=\alpha_1$ a une solution α_2 sur $]0;\alpha_1[$. On définit ainsi par récurrence une suite strictement décroissante de réels strictement positifs et donc une infinité de réels α_i. Si nous définissons la suite u en choisissant comme premier terme α_1, elle sera constante ($=\alpha$) à partir du terme de rang i+2 .

Cycles d'une fonction

1. Soient A et B de coordonnées $(0;f(0))$ et $(1;f(1))$. Pour relier A et B par une courbe continue, intérieure au carré unité, il faut nécessairement couper la droite d'équation y=x. $h(0) \geq 0$ et $h(1) \leq 0$. Il existe donc d'après le théorème des valeurs intermédiaires une solution α de l'équation $h(x)=0$. Or $h(\alpha)=0 \Leftrightarrow f(\alpha)=\alpha$.

2. Les points $(x_1;x_2)$ et $(x_2;x_1)$ sont symétriques par rapport à la droite d'équation y=x et situés tous deux sur la courbe de f. $g(x_1)=x_1$. $g(x_2)=x_2$ et $g(\alpha)=\alpha$.
La fonction f étant dérivable sur [0;1] et à valeurs dans [0;1], on en déduit par dérivation des fonctions composées que g est dérivable sur [0;1] et que $g'(x)=f'(x)\,f'(f(x))$.
$g'(x_1)=f'(x_1)\,f'(f(x_1))=f'(x_1)\,f'(x_2)$. De même $g'(x_2)=g'(x_1)$ et $g'(\alpha)=[f'(\alpha)]^2$.

3. Si β est tel que $f(\beta)=\beta$, alors $g(\beta)=f(f(\beta))=f(\beta)=\beta$. Dès lors $g(x)=x$ a deux racines "naturelles" 0 et $\alpha=(k-1)/k$. On peut donc factoriser comme indiqué dans l'énoncé. Le discriminant vaut $\Delta = k^2(k+1)(k-3)$. Il y a donc deux racines dans [0;1] qui ne sont ni nulles ni égales à α dés que $k>3$. $x_{1,2} = \dfrac{1+k \pm \sqrt{(k+1)(k-3)}}{2k}$.

4. Sur $]0;\alpha[$, la courbe (C) est au dessus de la droite D d'équation y=x donc si $0<x<\alpha$ alors $f(x)>x$.
Sur $]\alpha;1[$, f est décroissante donc $f(x)<f(\alpha)=\alpha<x$.

$\varphi(a)=a$. $\varphi(b)=b$ $\varphi(c)=c$.
$\varphi'(x)=f'(x)\,f'(f(x))\,f'(f(f(x)))$ (par dérivation des fonctions composées)
Appliqué à a, b et c on obtient $\varphi'(a)=\varphi'(b)=\varphi'(c)=f'(a)\,f'(b)\,f'(c)$.
Sans restreindre le problème, on peut considérer que c est le plus grand des trois nombres a, b, c. Si $c<\alpha$ alors $f(c)=a>c$ ce qui est impossible.
Donc $\underline{c>\alpha}$. (car $c\neq\alpha$ sinon $c=\alpha$ et $a=f(c)=\alpha$)
Ainsi $f(c)=a<\alpha$ donc $f(a)=b>a$. Comme il est impossible que $b>\alpha$ car alors $f(b)=c<\alpha$, on en déduit que $\underline{0<a<b<\alpha<c<1}$.
Considérons $L(x)=g(x)-x$.
$L(a)=c-a>0$ $L(b)=a-b<0$. D'après le théorème des valeurs intermédiaires, il existe x_1 dans $]a;b[$ tel que $L(x_1)=0$ et ainsi $g(x_1)=x_1$. Comme $\alpha \in]b;c[$, $x_1\neq\alpha$. Posons $x_2=f(x_1)$, on trouve alors que $f(x_2)=x_1$. De plus $x_1\neq x_2$ car α est la seule solution de $f(x)=x$ sur $]0;1[$.

Construction de la courbe de g

1. La symétrie se traduit par $f(1/2-h)=f(1/2+h)$ pour tout $h \in [0;1/2]$.
Ainsi $g(1/2-h)=f(f(1/2-h))=f(f(1/2+h))=g(1/2+h)$. La courbe de g présente donc la même symétrie.

2. Si $0<a<b<1/2$, par croissance de f: $0<f(a)<f(b)<f(1/2)<1/2$. Et encore par croissance de f, nous obtenons $g(a)<g(b)$ et donc que g est croissante sur [0;1/2].

3. On applique le théorème des valeurs intermédiaires à $f(x)-1/2$ ce qui démontre l'existence de β. La croissance stricte de f montre que β est unique. La suite se traite comme la question précédente.

4. a) et b) On trouve $m=k/4$ et $\beta = \dfrac{k-\sqrt{k^2-2k}}{2k}$ seule solution inférieure à 1/2.

c) $m=1/2$ donc $k=2$.
d) Il y a 4 solutions à $g(x)=x$ donc $k>3$. 1/2 n'est pas fixe par f et 1/2 est le plus petit point fixe différent de 0 de g donc :

x_1=1/2 or $x_1 = \dfrac{1+k-\sqrt{(k+1)(k-3)}}{2k}$ d'où on tire que $k = 1+\sqrt{5}$

e) $g'(\alpha)$=1 donc $f'(\alpha)= \pm 1$ Ici $f'(\alpha)$=-1 (sinon k=1 ce qui n'est visiblement pas le cas) et donc $k=3$.

f) Ici $g'(x_1)$=-1. Or $g'(x_1)=f'(x_1)\,f'(x_2) = k^2\,(1-2x_1)(1-2x_2)=k^2(1-2(x_1+x_2)+4x_1x_2)$

$$x_1 + x_2 = \frac{1+k}{k} \qquad \text{et} \qquad x_1x_2 = \frac{(k+1)^2-(k+1)(k-3)}{4k^2} = \frac{k+1}{k^2}$$

Après calcul, on trouve $k = 1+\sqrt{6}$.

On peut remarquer que si $3 < k < 1+\sqrt{6}$, la courbe de g sera moins "creuse", la pente des tangentes en x_1 et x_2 sera plus faible et ainsi les points fixes de g formeront un cycle limite pour la suite u.

En revanche lorsque $k > 1+\sqrt{6}$ la pente en x_1 et x_2 sera plus forte et alors, le cycle sera instable. Il est possible d'analyser la courbe représentant $g \circ g$ pour des valeurs proches de $1+\sqrt{6}$. On constatera alors que passée cette valeur, il y a apparition de quatre nouveaux points fixes pour $g \circ g$, c'est-à-dire un cycle limite d'ordre 4 pour u.

g) Il y a 8 points d'intersection avec la droite d'équation y=x. Pour 3 d'entre eux la dérivée (négative) est, en valeur absolue, strictement plus petite que 1. Sauf cas particulier dépendant du premier terme de la suite choisi, à partir d'un certain rang, les termes u_n de la suite vont "sauter" du voisinage de l'un au voisinage du suivant. Les 5 autres sont 0, α et un cycle instable (car la dérivée en ces points est plus grande que 1) d'ordre 3.

On pourra vérifier ce phénomène à l'aide d'une calculatrice ou d'un ordinateur en choisissant "au hasard" un premier terme de la suite (u_n). Sur ce point, même en choisissant comme premier terme $x_1 = \dfrac{1+k-\sqrt{(k+1)(k-3)}}{2k}$, l'ordinateur nous donnera le même cycle limite ce qui semble contredire la théorie. En fait, comme il ne peut travailler que sur des valeurs approchées, la non stabilité au voisinage de x_1 (et x_2) va engendrer des erreurs qui s'accumulent, et rapidement les résultats obtenus n'auront plus aucun rapport avec la réalité.

VRAI OU FAUX, DU BON USAGE DES CONTRE-EXEMPLES

La négation de $\forall x, P(x)$ est $\exists x, \overline{P}(x)$, ou, en des termes moins formalisés : pour montrer qu'une propriété *P(x)* n'est pas vraie pour toutes les valeurs de x, il suffit de montrer qu'il existe au moins un x pour lequel *P(x)* est fausse (c'est à dire $\overline{P}(x)$ vraie), c'est ce que l'on appelle un "contre-exemple".
Un contre-exemple célèbre est le ruban de Moebius[3] qui montre que l'affirmation :
"toute boucle obtenue en collant ensemble les deux extrémités d'une bande de papier a une face interne et une face externe" est fausse. Réalisez une telle boucle en tournant une fois l'une des extrémités avant de coller et tentez de colorier l'une des faces. Un ruban de Moebius a bien d'autres propriétés étonnantes. Essayez par exemple de le couper en deux dans le sens de la "longueur". Refaites l'expérience en coupant au 1/3 de la largeur.
Pour chacune des affirmations suivantes, donnez une démonstration pour montrer qu'elle est vraie ou un contre-exemple pour montrer qu'elle est fausse. (Indication : les dix premières affirmations sont toutes fausses, pour les autres il faudra vous faire votre propre opinion.

1) Deux quadrilatères ayant leurs quatre côtés deux à deux égaux sont isométriques.
2) Un polygone convexe ayant un nombre impair de côtés a un nombre impair de diagonales.
3) Un polygone convexe ayant un nombre impair de diagonales a un nombre impair de côtés.
4) Tout quadrilatère ayant deux côtés parallèles et deux côtés égaux est un parallélogramme.
5) Pour tout réel x non nul, $\frac{1}{x} \leq x$.
6) Toute fonction qui n'admet pas de maximum sur l'intervalle I admet un minimum sur I.
7) Pour tout réel positif x, $x < x^2$.
8) Toute fonction non croissante sur $[a,b]$ est décroissante sur $[a,b]$.
9) Si la fonction g définie par $g(x) = (f(x))^2$ est paire alors la fonction f est paire.
10) $\forall x \in R, -x < x^2$
11) Si f est une fonction définie et strictement croissante sur R alors $\lim\limits_{x \to +\infty} f(x) = +\infty$
12) Si *P(x)* est un polynôme qui n'a que des coefficients entiers, alors il ne prend que des valeurs entières pour toutes les valeurs entières de x.
13) Si *P(x)* est un polynôme qui ne prend que des valeurs entières pour toutes les valeurs entières de x, alors *P(x)* n'a que des coefficients entiers.
14) $\forall x \in R^+, x > -x^2$
15) $\exists x \in R, -x > x^2$
16) $\forall x \in R, \exists y \in R, y > x$.
17) $\exists y \in R, \forall x \in R, y > x$.
18) $\forall x \in R, \exists y \in R, x + y = x^3 + y^3$
19) $\exists y \in R, \forall x \in R, x + y = x^3 + y^3$
20) Si la fonction g définie par $g(x) = (f(x))^2$ est paire alors la fonction f est paire ou impaire.

[3]Augustus Ferdinand Möbius (1790-1868) astronome à l'observatoire de Leipzig en Allemagne a grandement contribué aux recherches concernant les propriétés topologiques des figures ainsi qu'au développement de la géométrie projective. Son nom reste attaché au ruban qui n'a qu'une face dont il est question ici.

Arithmétique et autres propos.

Arithmétique du grec ἀριθμός, nombre et aussi science des nombres... Mais de quels nombres s'agit-il au juste? naturels, rationnels, réels ou complexes?

Dans une première partie, nous partons redécouvrir tous ces nombres, insistant sur leurs différences (ou différentes propriétés), exhibant leurs emboîtements, poussant (le vice?) jusqu'à les "construire" les uns à partir des autres, des plus naturels aux plus complexes.

Dans une deuxième partie, nous explorons une petite parcelle du vaste domaine qu'est l'arithmétique. Nous partons de quatre problèmes "historiques" et nous nous dirigeons dans deux directions différentes : division euclidienne et congruences. Nous atteignons en fin de parcours une première application pratique de cette arithmétique.

Le (la) lecteur(trice) est libre de nous suivre dès la première page ou seulement à partir de la deuxième partie, juste après la récréation mét(h)éo(rique), quitte à revenir fouiller dans les pages précédentes.

Première partie.

Des nombres

Pour commencer parlons des plus simples dans le sens des plus anciennement et universellement utilisés. Pour cela, ils sont dits **naturels**. Ce sont ceux qui servent à compter les objets sur une table ou les grains de sable sur la plage ou ... : $1, 2, 3, 4, \ldots$ sans oublier 0 qui, comme le montre son histoire n'a rien de très naturel.

Que pouvons-nous faire de ces entiers naturels? D'abord les mettre dans un ensemble que l'on note $\mathbf{N}$ [1]. Puis en prendre plusieurs et les additionner (ou les multiplier) entre eux : nous obtenons un des leurs. On dit donc que $\mathbf{N}$ est *stable pour l'addition* (ou *la multiplication*).

Nous avons la liberté d'effectuer ces calculs en prenant les entiers dans l'ordre qui nous plaît, en les regroupant comme il nous convient, ce qui s'écrit mathématiquement (dans le cas de l'addition) :

pour tous n et m de $\mathbf{N}$, $n+m = m+n$ et pour tous n, m et p de $\mathbf{N}$, $(n+m)+p = n+(m+p)$ (et dans le cas de la multiplication?).

Dans le premier cas, nous faisons "commuter" les deux entiers... et on parle d'*opération commutative*. Dans le deuxième cas, nous les associons de toutes les manières possibles sans changer le résultat... on parle alors d'*opération associative*.

[1] Vous connaissez mieux la notation $\mathbb{N}$ qui n'est autre que la version manuscrite de $\mathbf{N}$. Il en est de même de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ que la machine écrit $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$.

Qu'en est-il de la soustraction et de la division? Attention il y a *trois* propriétés à étudier. Voyons...

MORCEAUX D'ENFANTS (extrait, fidèle par son contenu mais non par sa forme, du "*Triparty en la science des nombres*" de Nicolas Chuquet, 1484).

Il est un homme qui a des enfants dont le nombre est inconnu. Et il a certains deniers en son coffre dont le nombre ne se dit point. Et cet homme dit au premier de ses enfants : "Va en le coffre et prends le septième des deniers que tu y trouveras plus deux". Au second il dit : " Va en le coffre et après que ton frère aura pris sa portion prends le septième de ce que tu y trouveras plus 4". Et au troisième il dit qu'il prenne le septième et 6 et conséquemment aux autres jusqu'au dernier auquel il dit qu'il prenne tout ce que ses frères lui auront laissé. En ce faisant ils ont autant de deniers l'un que l'autre. Allez savoir la quantité d'enfants, de deniers qu'aura chacun d'eux et aussi de deniers dans le coffre?

Réponse : Ils sont 6 enfants. Chaque enfant a 14 d. En le coffre il y avait 84 d.

(...) Autre histoire comme dessus. Excepté que le premier doit prendre le septième de ce qui est dans le coffre plus 3. Le second le septième plus 8. Le troisième plus 13 etc. L'on demande comme dessus.

Réponse : 6 2/5 le nombre d'enfants. 224 deniers en le coffre.

Combien de réponses sont acceptables? Est-on sûr du nombre d'enfants ou de deniers dans le premier problème? i.e. est-ce l'unique solution? (Si la première question tient du bon sens, la seconde nécessite un petit travail mathématique, plus précisément une mise en équation du problème [2]... suivie de sa résolution! [3])

Que dire du deuxième problème?... Et de l'intérêt de respecter la nature des solutions? "2/5 d'enfants ça n'existe pas!" (2/5 n'existe pas dans N). Il est clair (ou raisonnable) que le nombre d'enfants soit un entier naturel or il n'y a pas d'entiers solutions. Ce problème est donc sans solution.

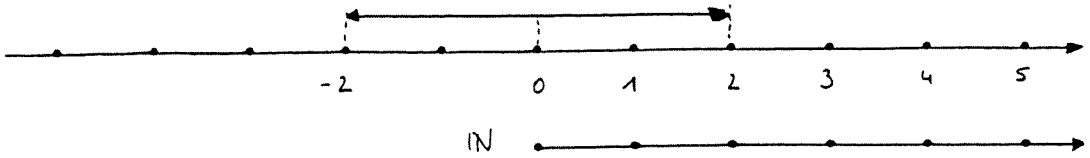
Revenons à la soustraction et à la division dans N. Elles ne sont pas possibles pour n'importe quel couple d'entiers, par exemple 2-3=?, 2:5=?. Ce qui nous conduit à considérer d'autres nombres.

Occupons-nous des **entiers** dits **relatifs** qui vont nous permettre de soustraire à notre aise. Intuitivement, nous prenons tous les entiers naturels et nous ajoutons toutes les différences entre un entier naturel et un autre qui lui est supérieur. Ces dernières sont des quantités *négatives*, c'est-à-dire celles *qui, dans une représentation géométrique des grandeurs (ou des quantités) par segments mesurés à partir d'une même origine sur une droite orientée,*

[2] une feuille de papier, un crayon et allons-y! Dressons la liste de nos inconnues : le nombre d'enfants (désignons-le par N), le nombre total de deniers dans le coffre (soit X) et le nombre de deniers de chacun des enfants (appelé x). Maintenant, écrivons les relations entre ces inconnues : pour le premier enfant, $x = \frac{X}{7} + 2$; pour le second, $x = \frac{X-x}{7} + 4$; pour le troisième, $x = \frac{X-2x}{7} + 6$; et ainsi de suite jusqu'à l'avant-dernier. Pour le dernier, $x = X - (N-1)x$.

[3] A l'aide des deux premières équations, on calcule X, puis x. La dernière équation fournit alors la valeur de N. Mais ce n'est pas fini! Nous avons négligé certaines équations et il convient de vérifier que notre précédente solution est encore solution de ces équations.

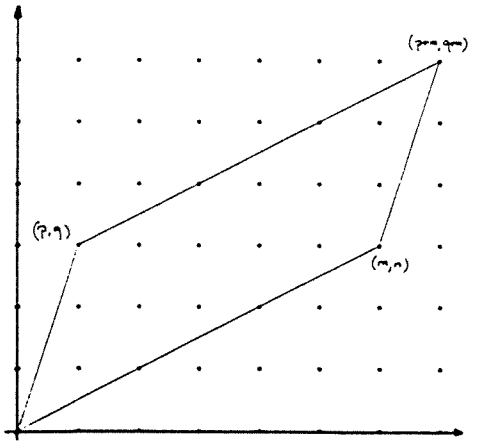
correspond à un déplacement dans la direction (le sens dans le langage mathématique) *inverse de l'axe* (Petit Robert 1). Graphiquement :



Des mots, des dessins... Mais quelle construction mathématique cachent-ils? Suivons donc la démarche du (de la) mathématicien(ne).

Des entiers naturels aux entiers relatifs.

Pour le moment, il (elle) ne connaît que N muni de son addition + et guidée par son intuition, il (elle) s'intéresse aux "différences" de deux entiers naturels. Il (elle) prend donc tous les couples (m, n) d'entiers naturels, comme $(2, 3), (5, 0), (0, 5)$ (les deux derniers sont bien distincts... cf. fig) plutôt que $m - n$. Pourquoi? Car si $2 - 3$ n'a pas encore de signification, $(2, 3)$ en a une. L'ensemble de tous ces couples est noté $\mathbf{N} \times \mathbf{N}$. Représentons-le ci-dessous.



Sur cet ensemble, nous pouvons définir une addition $+'$, à la manière de l'addition vectorielle : $(m, n) +' (p, q) = (m + p, n + q)$ pour tous $(m, n), (p, q)$ dans $\mathbf{N} \times \mathbf{N}$. Cette définition est satisfaisante a priori car nous souhaitons que $(m - n) + (p - q) = (m + p) - (n + q)$ (N'oublions pas que le couple (m, n) joue le rôle de $m - n$, comme (p, q) celui de $p - q$). Le couple $(0, 0)$ joue le même rôle que 0 dans N puisque $(m, n) + (0, 0) = (m, n)$.

Encore un petit moment, laissons-nous guider par notre "intuition". Par rapport à ce que nous attendons, il y a trop d'éléments : une multitude de couples représente une même différence. En effet,

$1 = 1 - 0 = 2 - 1 = 3 - 2 = ... = 903 - 902 = ...,$

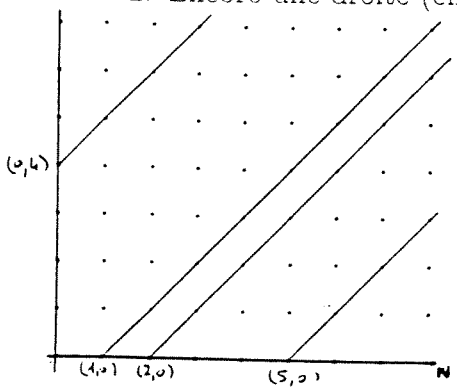
$2 = 2 - 0 = 3 - 1 = 4 - 2 = ... = 905 - 903 = ..., 3 = ...,$etc

Que peut-on dire géométriquement, des couples $(1, 0), (2, 1), (3, 2), ..., (903, 902), ...$ d'une part, et des couples $(2, 0), (3, 1), ...(905, 903), ...$ d'autre part?

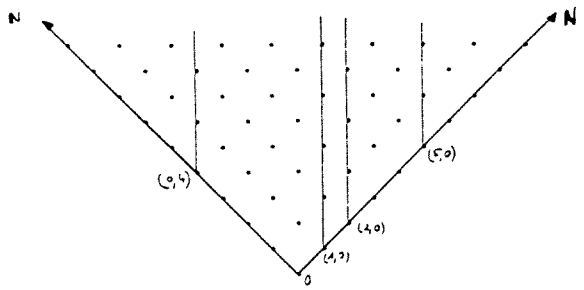
Notons (m, n) un couple quelconque parmi $(1, 0), (2, 1), (3, 2), ..., (903, 902), ...$ On remarque que dans tous les cas $n = m - 1$. N'est-ce pas là l'équation d'une droite? Oui mais (m, n) sont dans un quart de plan, donc sur la demi-droite $y = x - 1$ et $x, y \geq 0$.

Passons à $(2, 0), (3, 1), ...(905, 903), ...$ Cette fois-ci, si (m, n) est un des couples, alors

$n = m - 2$. Encore une droite (en fait demi-droite)! ... et de même pente!!!



ou

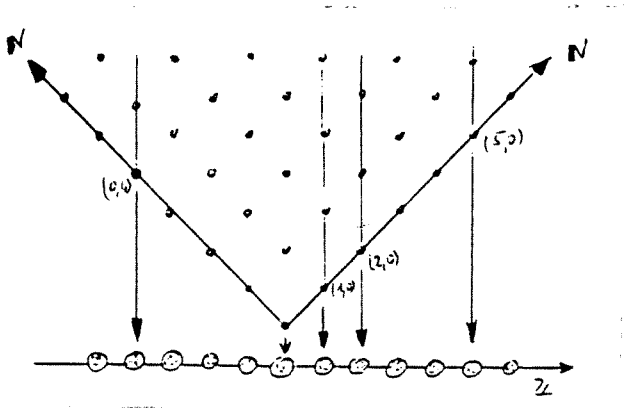


Plus généralement, deux couples (m, n) et (p, q) dont les composantes sont pareillement différentes (c'est-à-dire $m - n = p - q$, autrement dit $m + q = n + p$) appartiennent à une même demi-droite de pente 1 dans N × N. Pour le remarquer, observer la figure suffit mais pour convaincre (surtout les sceptiques) un petit calcul est nécessaire.

Prenons donc, au hasard, deux couples (m, n) et (m', n') de N × N dont les composantes sont pareillement différentes. Notons $k = m - n = m' - n'$. Alors $n = m - k$ et $n' = m' - k$. Les deux couples (m, n) et (m', n') vérifient donc l'équation de droite $y = x - k$. Toutes les composantes étant positives, ils sont même sur la demi-droite $y = x - k$ et $x, y \geq 0$.
Ainsi, la demi-droite qui joint deux tels couples est de pente 1.

Ceci en tête, retournons auprès du (de la) mathématicien(ne) au travail.

Celui-ci (celle-ci) considère à la place des couples de N × N, les demi-droites de pente 1 qui contiennent de tels couples, c'est-à-dire celles qui ont pour origine un couple $(m, 0)$ ou $(0, n)$. Ne connaissant que l'addition dans N, une telle demi-droite est définie comme l'ensemble des couples (x, y) de N × N tels que $m + y = x$ si elle est d'origine $(m, 0)$, $y = n + x$ si elle est d'origine $(0, n)$.



Et pour ne pas s'embarasser, il (elle) "empile" chaque demi-droite sur son point d'origine (ou dans le deuxième dessin sur le point situé en-dessous).

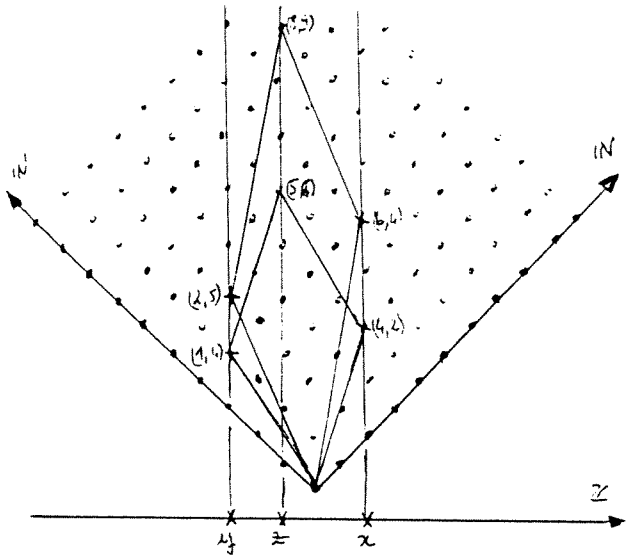
Il (elle) obtient donc un nouvel ensemble qu'il nomme Z. Chaque élément z de Z est un paquet de couples de N × N ayant la propriété d'être tous sur une même demi-droite de pente 1. Nous dirons qu'un couple de z est "*un représentant de* z" ou qu'il "*représente* z".

QUE DEVIENT L'ADDITION $+'$ SUR Z?

Donnons-nous deux éléments x et y de Z. Prenons un représentant de chacun d'eux dans N × N. Additionnons-les. Ceci nous donne un couple qui représente un élément z de Z.

Recommençons l'opération avec un autre représentant de x et un autre de y. Leur somme représente-t-elle encore z ou non?

Par exemple, supposons que (4,2) représente x et (1,4) y. Alors z est représenté par $(4,2)+'(1,4) = (5,6)$. Mais (6,4) représente encore x et (2,5) y. Or $(6,4) +' (2,5) = (8,9)$. Nous voyons bien que (5,6) et (8,9) sont sur la même demi-droite de pente 1 : ils représentent bien le même élément z!



Qu'en est-il en général?

Nous allons montrer que ce résultat subsiste pour tout x et tout y.

Appelons (m,n) un premier représentant de x et (m',n') n'importe quel autre. De même, appelons (p,q) un premier représentant de y et (p',q') n'importe quel autre. Nous savons que $(m,n) +' (p,q) = (m+p, n+q)$ représente z. Le couple $(m',n') +' (p',q') = (m'+p', n'+q')$ représente le même z s'il appartient à la même demi-droite de pente 1 que $(m+p, n+q)$, c'est-à-dire si $(m+p)+(n'+q') = (n+q)+(m'+p')$. Or

$$\begin{aligned} (m+p)+(n'+q') &= m+(p+n')+q' && \text{(associativité)} \\ &= m+(n'+p)+q' && \text{(commutativité)} \\ &= (m+n')+(p+q') && \text{(pourquoi?)} \end{aligned}$$

Rappelons-nous maintenant que (m,n) et (m',n') d'une part, et (p,q) et (p',q') d'autre part, sont sur une même demi-droite de pente 1 donc que $m+n' = n+m'$ et $p+q' = p'+q$. Nous poursuivons donc notre calcul par :

$$\begin{aligned} (m+p)+(n'+q') &= (m+n')+(p+q') &&= (n+m')+(p'+q) \\ &= \ldots = \ldots = \ldots && \text{(à complèter)} \\ &= (n+q)+(m'+p'). \end{aligned}$$

En conclusion, les points x et y étant donnés, la somme d'un représentant quelconque de x et d'un représentant quelconque de y représente le même élément z de $\mathbf{Z}$. Nous pouvons donc définir une addition sur notre ensemble $\mathbf{Z}$ (que nous noterons comme celle de $\mathbf{N}$) par : $x+y=z$.

Plus concrètement : si o est représenté par $(0,0)$ et y par $(2,3)$. Alors $o+y$ est représenté par le couple $(0,0) +' (2,3) = (0+2, 0+3) = (2,3)$ donc $o+y = y$. Qu'en est-il de $y+o$? de la somme de o avec n'importe quel autre élément de $\mathbf{Z}$? Si x est représenté par $(1,0)$ et y par $(0,1)$, que vaut $x+y$?

Si nous choisissons de représenter chaque élément de $\mathbf{Z}$ par un des couples $(n,0)$ ou $(0,n)$ (pourquoi est-ce possible?), quel est le représentant de

i) $(n,0) +' (n',0)$?

ii) $(0,n) +' (0,n')$?

iii) $(n,0) +' (0,n)$? et

iv) $(n,0) +' (0,n')$? (Attention les composantes sont dans N).

Si $n \in \mathbf{N}$, identifions n à l'élément de $\mathbf{Z}$ représenté par $(n,0)$. Alors l'addition dans N ou dans $\mathbf{Z}$ donne le même résultat. Notons $-n$ l'élément de $\mathbf{Z}$ représenté par $(0,n)$. Les résultats précédents se récrivent : $\mathbf{Z} = \{n, -n/n \in \mathbf{N}\}$ et pour tous $n, n' \in \mathbf{N}$,

ii) $(-n) + (-n') = -(n+n')$

iii) $n + (-n) = 0$

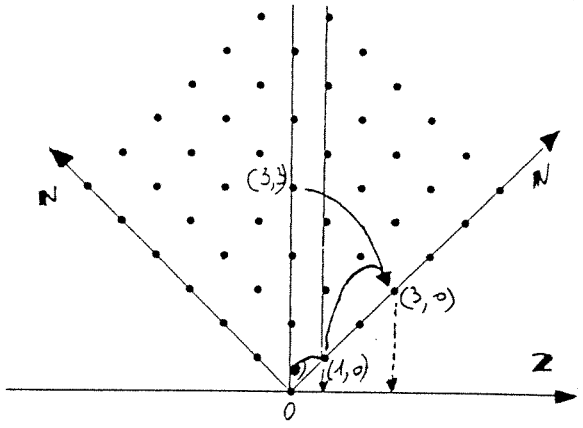
iv) $n + (-n') = n - n'$ si $n > n'$; $-(n'-n)$ si $n \leq n'$.

N'est-ce pas là l'ensemble $\mathbf{Z}$ bien connu?

Qu'en est-il de la multiplication? [4]

Comme pour l'addition, on cherche d'abord une opération $\times$ dans $\mathbf{N} \times \mathbf{N}$ puis on en déduit une sur $\mathbf{Z}$. Pour cela, il faut que cette opération "conserve" les paquets de $\mathbf{Z}$ ce qui signifie que si (m,n) et (m',n') sont des représentants d'un élément x de $\mathbf{Z}$ et si (p,q) et (p',q') d'un élément y de $\mathbf{Z}$, nous devons obtenir que $(m,n) \times (p,q)$ et $(m',n') \times (p',q')$ représentent le même élément de $\mathbf{Z}$.

La première idée de $\times$ sur $\mathbf{N} \times \mathbf{N}$ est la multiplication composante par composante, c'est-à-dire $(m,n) \times (p,q) = (mp, nq)$ où m,n,p,q désignent des entiers naturels. Mais alors $(0,0) \times (1,0) = (0,0)$ et $(3,3) \times (1,0) = (3,0)$. Or $(0,0)$ et $(3,3)$ sont dans le même "paquet" tandis que $(0,0)$ et $(3,0)$ non. Cette opération ne peut donc pas convenir car elle mélange les "paquets".



Cherchons une autre idée. Rappelons-nous que (m,n) est représenté par $m-n$ et (p,q) par $p-q$ et que nous voudrions que $(m-n) \times (p-q) = mp + nq - mq - np$, ce qui s'écrit aussi (en suivant nos conventions) $(m,n) \times (p,q) = (mp+nq, mq+pn)$. Soit! Prenons donc cette égalité comme définition d'une multiplication dans $\mathbf{N} \times \mathbf{N}$(Remarquez que cette expression n'est pas si éloignée de celle de la multiplication de deux nombres complexes quand on les représente par le couple (partie réelle, partie imaginaire).). Est-ce vraiment sensé?... oui car comme nous allons le voir, cette opération jouit de toutes les propriétés bien connues et utiles de la multiplication.

En premier lieu, le produit $(m,n) \times (p,q)$ ainsi défini fournit un nouveau couple de $\mathbf{N} \times \mathbf{N}$. En deuxième lieu, $(m,n) \times (p,q)$ et $(p,q) \times (m,n)$ donnent le même couple de $\mathbf{N} \times \mathbf{N}$, à savoir le couple $(mp+nq, mq+pn) = (pm+qn, pn+mq)$: ce produit est commutatif. En

[4] Par souci de complètude, on termine notre construction de $\mathbf{Z}$. Si cela vous "effraie", n'hésitez pas à abandonner le chantier et reprendre au paragraphe suivant.

troisième et dernier lieu.

$$\begin{aligned}((m,n)\times(p,q))\times(r,s) &= (mp+nq,mq+pn)\times(r,s)\\ &= ((mp+nq)r+(mq+pn)s,(mp+nq)s+r(mq+pn))\\ &= (m(pr+qs)+n(qr+ps),m(ps+rq)+(qs+pr)n)\\ &= (m,n)\times((p,q)\times(r,s))\end{aligned}$$

pour tout couple (m,n), (p,q) et (r,s) de $\mathbf{N}\times\mathbf{N}$: ce produit est également associatif.

Est-il distributif par rapport à l'addition, c'est-à-dire avons-nous pour tous couples (m,n), (p,q) et (r,s) de $\mathbf{N}\times\mathbf{N}$, l'égalité :

$$(m,n)\times((p,q)+(r,s))=(m,n)\times(p,q)+(m,n)\times(r,s)?$$

Nous avons donc sur $\mathbf{N}\times\mathbf{N}$ une (deuxième) multiplication. *Pouvons-nous en déduire une multiplication sur* $\mathbf{Z}$*?* (Il faut s'assurer que cette multiplication ne maltraite pas les "paquets" en s'inspirant du cas de l'addition.)

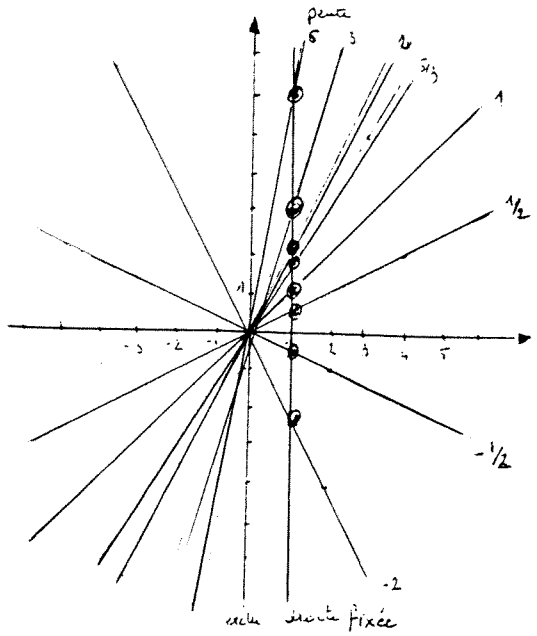
Et maintenant, retrouvez les règles du produit de deux éléments de $\mathbf{Z}$. **

Nous voilà donc en possession de $\mathbf{Z}$ et rassurés d'y retrouver nos "bons vieux" savoirs. Et en particulier, si nous savons que soustraire est sans danger, nous savons également que diviser n'est pas toujours possible. Grâce à ces impossibilités, il existe dans $\mathbf{Z}$ une notion de *reste dans une division* et de *nombres premiers*, deux sources de l'arithmétique qui seront explorées (très partiellement) dans la deuxième partie. Si la curiosité vous pique, vous pouvez faire un saut d'une dizaine de pages. Ici, nous poursuivons nos considérations sur les nombres.

... Encore des nombres!

Nous en arrivons maintenant à $\mathbf{Q}$, l'ensemble de tous les quotients *possibles* de deux entiers relatifs, celui des **nombres** dits **rationnels**. Un élément r de $\mathbf{Q}$ est donc *représenté* par une *fraction* $\frac{a}{b}$ où a et b sont des éléments de $\mathbf{Z}$ et $\mathbf{Z}^*$ respectivement. En fait, une infinité de fractions vont représenter r. Par exemple : si $r=0$, $r=\frac{0}{1}=\frac{0}{2}=\frac{0}{-1}=\ldots$ ou si $r=\frac{-1}{5}$, $r=\frac{1}{-5}=\frac{-2}{10}=\frac{-3}{15}=\ldots$

Comment dessiner $\mathbf{Q}$ à partir de $\mathbf{Z}\times\mathbf{Z}$?



On interprète un quotient $\frac{a}{b}$ comme un couple (b, a) que nous représentons graphiquement par le point de coordonnées (b, a). Attention ce couple appartient à $\mathbb{Z}^* \times \mathbb{Z}$! Il convient donc d'exclure l'axe des y.

Supposons que deux quotients $\frac{a}{b}$ et $\frac{c}{d}$ soient égaux. Les points M et N qui les représentent sur le dessin ne sont pas toujours confondus. mais toujours sur une même droite issue de l'origine (celle de pente $\frac{a}{b} = \frac{c}{d}$!) puisque la condition d'égalité s'écrit aussi $c = \frac{a}{b} \cdot d$.

Supposons maintenant que les points de coordonnées (b, a) et (d, c) soient sur une même droite passant par l'origine. En calculant la pente de cette droite de deux manières différentes, nous obtenons l'égalité entre $\frac{a}{b}$ et $\frac{c}{d}$.

Ainsi, dans $\mathbb{Z}^* \times \mathbb{Z}$, un rationnel r correspond à un "paquet" de couples représentés sur le dessin par tous les points à coordonnées entières de la droite de pente r et passant par l'origine. Pour obtenir une représentation plus proche du "sens commun", nous choisissons un point particulier sur chacune de ces droites, par exemple celui d'intersection avec une droite parallèle à l'axe des y fixée (cf. dessin). Puis nous tassons chaque droite sur son point particulier. Ces points "très particuliers" représentent alors les nombres rationnels.

Tout ceci n'est pas sans rappeler la "construction" précédente de $\mathbb{Z}$ à partir de $\mathbb{N}$. C'est en fait, par cette voie-là, que le (la) mathématicien(ne) obtient $\mathbb{Q}$ à partir de $\mathbb{Z}$.

Suivons, sans nous attarder, sa démarche. On considère tous les couples de $\mathbb{Z}^* \times \mathbb{Z}$ que l'on regroupe en paquets suivant la "règle" : (a, b) et (c, d) sont dans un même "paquet" si $ad = bc$. On "étiquette" le paquet contenant le couple (a, b) par le symbole $\frac{a}{b}$. On dit que deux "étiquettes" $\frac{a}{b}$ et $\frac{c}{d}$ sont égales si elles sont attachées au même paquet, c'est-à-dire si $ad = bc$. Bien évidemment, on ne peut pas faire ceci en choisissant n'importe quelle règle. On s'attend à ce que [5] :

(i) (a, b) soit toujours dans le même paquet que lui-même;

(ii) si (a, b) est dans le même paquet que (c, d), (c, d) soit dans le même paquet que (a, b);

(iii) si (a, b) est dans le même paquet que (c, d) et (c, d) est dans le même paquet que (e, f) alors (a, b) et (e, f) soient dans le même paquet.

A vous de vérifier qu'avec la règle choisie, ces trois propriétés sont satisfaites.

On appelle $\mathbb{Q}$ l'ensemble des paquets que l'on désigne par leurs "étiquettes".

Il reste à ajouter le vocabulaire mathématique qui accompagne cette démarche. La "règle" servant à former les paquets est dite *relation*. Quand elle satisfait les conditions (i), (ii) et (iii), elle est qualifiée de *relation d'équivalence*. Dans ce cas, les paquets prennent le nom de *classes d'équivalence* (comprendre un paquet = une classe d'équivalence). Un élément (a, b) d'une classe d'équivalence est appelé un *représentant* de cette classe.

L'ensemble $\mathbb{Q}$ est muni de deux opérations $+$ et $\times$ qui possèdent des propriétés bien connues. Enumérons-les.

[5] *Réfléchir sur la règle : (a, b) et (c, d) sont dans un même "paquet" si $a + b < c + d$.*

- pour l'addition :

(i) + est associative et commutative[6].

(ii) il y a un 0, c'est-à-dire un élément qui additionné avec tout autre élément ne change pas cet élément. En termes mathématiques : pour tout $r \in \mathbf{Q}$, $r + 0 = 0 + r = r$. Pour cette raison, il est appelé *élément neutre* pour l'addition.

(iii) tout élément a un opposé, c'est-à-dire pour tout élément r, il existe un élément r' tel que $r + r'$ soit l'élément neutre.

- pour la multiplication : sensiblement la même chose en remplaçant + par $\times$.

(iv) $\times$ est associative et commutative.

(v) il existe un élément neutre pour la multiplication, à savoir 1 (on a bien $r \times 1 = 1 \times r = r$ pour tout rationnel r).

(vi) tout élément a un inverse sauf 0. (c'est bien l'analogue de (iii)).

Et une autre propriété très utile dans les calculs,

(vii) distributivité de la multiplication par rapport à l'addition : pour tous $r, r', r'' \in \mathbf{Q}$, $(r + r')r'' = rr'' + r'r''$.

Ouvrons une parenthèse!

Connaissez-vous d'autres ensembles munis de deux opérations ayant toutes les propriétés précédentes?... Bien évidemment! Celui des **nombres réels** noté **R**, celui des **nombres complexes**, le fameux ensemble **C**. Et il y en a encore d'autres que vous rencontrerez plus tard. Vu la fréquence de telles situations, on a décidé de donner un nom à ces ensembles. On nomme *corps commutatif* un ensemble qui possède deux opérations ayant les propriétés (i) à (vii). Ainsi parle-t-on de *corps des nombres rationnels* pour désigner **Q**, de *corps des nombres réels* pour désigner **R** ou de *corps des nombres complexes* pour désigner **C**, ce qui signifie qu'en plus d'un ensemble d'éléments, il y a deux opérations avec toutes les propriétés ci-dessus.

On **ne** parlera **pas** de corps des entiers relatifs car nous savons que la propriété (vi) est fausse et donc que **Z** n'est pas un corps. Reprenons en détail ce raisonnement.

Pour démontrer que **Z** n'est pas un corps, il suffit de montrer qu'une des sept propriétés (i),...,(vii) n'est pas satisfaite.

Dans notre cas, seule la propriété (vi) n'est pas vérifiée. Montrons-le donc. Pour ce faire, il suffit de trouver (au moins) un entier relatif non nul qui n'a pas d'inverse (c'est la négation de (vi)). par exemple 2. Dire que 2 n'a pas d'inverse dans **Z** signifie qu'il n'existe pas d'entier z tel que $2z = 1$ ou encore que pour tout entier z, $2z \neq 1$. Vérifions la dernière propriété.

Si $z > 0$, alors puisqu'il est entier, $z \geq 1$ et $2z \geq 2$ donc $2z \neq 1$; si $z \leq 0$, alors $2z \leq 0$ donc $2z \neq 1$.

Par conséquent, 2 n'a pas d'inverse dans **Z** donc **Z** ne vérifie pas la propriété (vi) et donc **Z** n'est pas un corps.

Remarque : On peut également montrer que **N** n'est pas un corps. Dans ce cas, plusieurs des propriétés (i) à (vii) ne sont pas satisfaites (pouvez-vous préciser lesquelles?) mais pour

[6] Reportez-vous à la première page pour une définition de ces termes

la démonstration, il suffit d'en trouver une seule (au choix).

Il est temps de fermer notre parenthèse et de dire...

Quelques mots sur les nombres réels.

Comme déjà dit, $\mathbf{R}$ est un corps commutatif contenant $\mathbf{Q}$. Il possède en outre beaucoup d'éléments qui ne sont pas dans $\mathbf{Q}$. En voici quelques exemples.

PREMIER EXEMPLE très simple (et historique...) :

Prendre un carré de côté 1 et mesurer la longueur de sa diagonale. La mesure obtenue est-elle un nombre rationnel?

Par le théorème de Pythagore (bien connu), la longueur de la diagonale est $\sqrt{2}$. Si elle est rationnelle, elle s'écrit $\frac{p}{q}$ avec $p \in \mathbf{Z}^*$ et $q \in \mathbf{Z}^*$. Mais alors, $2q^2 = p^2$ donc p est pair. Ecrivons donc $p = 2p_1$ où $p_1 \in \mathbf{Z}^*$. Alors $2q^2 = p^2 \Leftrightarrow q^2 = 2p_1^2$ donc q est pair : $q = 2q_1, q_1 \in \mathbf{Z}^*$ et $2q_1^2 = p_1^2$. Nous avons donc trouver un autre couple d'entiers (p_1, q_1) vérifiant la même équation que (p, q) avec p_1 (resp. q_1) *strictement* plus petit que p (resp. q). Nous recommençons aussi souvent que nous voulons... au moins $(p-1)$ fois. Nous obtenons alors p entiers $p_1, p_2, ..., p_p$ tels que $p > p_1 > p_2 > ... > p_p > 0$. Or entre p et 0, il n'y a que $(p-1)$ entiers distincts. Cette situation ne peut donc pas se produire et $\sqrt{2}$ n'est pas rationnel.

Nous venons de raconter la démonstration de l'*irrationnalité* de $\sqrt{2}$, c'est-à-dire du fait que $\sqrt{2}$ n'appartient pas à $\mathbf{Q}$. Dans le langage plus formel du (de la) mathématicien(ne), ceci donne :

Démonstration : Raisonnons par l'absurde. Nous supposons donc que $\sqrt{2}$ est rationnel, c'est-à-dire qu'il existe deux entiers, p et q non nul, tels que $\sqrt{2} = \frac{p}{q}$. On en déduit que $(*)\ 2q^2 = p^2$, autrement dit que (p, q) est solution de l'équation (E) $2y^2 = x^2$ où x et y sont les inconnues.

Or, la relation $(*)$ implique que 2 divise p, c'est-à-dire qu'il existe $p_1 \in \mathbf{Z}^*$ tel que $p = 2p_1$. Nous avons donc (en remplaçant dans $(*)$) : $q^2 = 2p_1^2$. D'où 2 divise q, c'est-à-dire qu'il existe q_1 tel que $q = 2q_1$. L'égalité $(*)$ devient donc $2q_1^2 = p_1^2$.

Nous avons donc trouvé une autre solution (p_1, q_1) de (E) avec $p > p_1$ et $q > q_1$. En raisonnant de même à partir de (p_1, q_1) au lieu de (p, q), nous obtenons une troisième solution (p_2, q_2) de (E) avec $p_1 > p_2$ et $q_1 > q_2$. Et en recommençant ainsi, nous obtenons une infinité de solutions de (E) dont les composantes sont entières, positives et de plus en plus petites. Or, entre p et 0, comme entre q et 1, il n'existe qu'un nombre fini d'entiers. Il y a donc contradiction et notre hypothèse initiale est fausse : $\sqrt{2}$ n'est pas rationnel.

Cette méthode de démonstration est dite *de descente infinie*. Elle est due à Pierre de Fermat, célèbre mathématicien du XVII ième siècle. Elle ne s'applique que sur $\mathbf{Z}$ car il est nécessaire d'avoir qu'un nombre fini d'éléments compris entre deux éléments donnés, ce qui n'est pas vrai sur $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$.

Nous pouvons montrer de manière analogue que les autres racines carrées d'entiers naturels qui ne sont pas des carrés sont aussi *irrationnelles*, c'est-à-dire dans $\mathbf{R}$ mais non dans

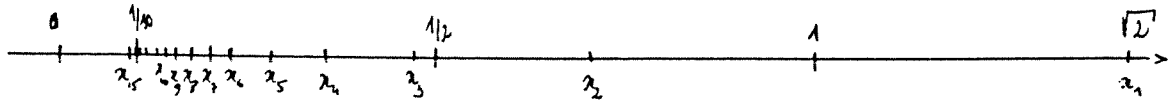
Q. Plus généralement, beaucoup de solutions d'équations polynômiales à coefficients dans Q ont des racines irrationnelles.

DEUXIÈME EXEMPLE : les nombres π et e ($1 = \ln(e)$).

Nous omettons les démonstrations. Disons simplement que ces questions ont fait couler beaucoup d'encre et ne furent résolues qu'au XVIII^e siècle par des méthodes analytiques élaborées (travaux de J.H. Lambert et L. Euler).

Ajoutons que ni π, ni e ne sont solutions d'une équation polynômiale à coefficients rationnels, résultats démontrés à la fin du siècle dernier (par F. Lindemann et Ch. Hermite respectivement). De tels réels sont appelés *nombres transcendants*. Leur étude est une branche de l'arithmétique que nous n'atteindrons pas.

Comment cohabitent rationnels et irrationnels dans **R**?
Il est facile de voir qu'entre deux rationnels se glisse toujours des irrationnels. Par exemple, considérons 0 et $\frac{1}{10}$:



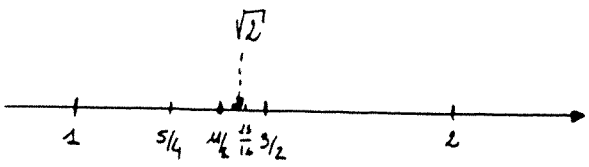
Les $x_n = \frac{\sqrt{2}}{n}$, $n \in \mathbf{N}$, sont des irrationnels (sinon $x_n \in \mathbf{Q}$ et $\sqrt{2} = nx_n \in \mathbf{Q}$ ce qui est faux) et x_{15} est inférieur à $\frac{1}{10}$.

Pour un raisonnement général, considérons deux rationnels distincts a et b et cherchons un irrationnel compris entre a et b. Nous pouvons supposer (et supposerons donc) que $a < b$. Alors $b - a$ est un rationnel strictement positif : $b - a = \frac{p}{q}$, $p \in \mathbf{N}$ et $q \in \mathbf{N}^*$. Nous avons les inégalités suivantes : $\sqrt{2} < 2 \leq 2p = 2q(b-a)$ d'où $\sqrt{2} < n(b-a)$ avec $n = 2q$ ou encore $a + \frac{\sqrt{2}}{n} < b$. Il est clair que $a + \frac{\sqrt{2}}{n} > a$ puisque $\frac{\sqrt{2}}{n} > 0$ et $a + \frac{\sqrt{2}}{n} \notin \mathbf{Q}$ sinon $\sqrt{2} \in \mathbf{Q}$.

Remarque : si nous prenons n'importe quel entier m strictement plus grand que n, alors $a < a + \frac{\sqrt{2}}{m} < a + \frac{\sqrt{2}}{n} < b$ et nous obtenons une infinité d'irrationnels compris entre a et b.

Que se passe-t-il autour d'un irrationnel? Fixons notre attention, par exemple, sur de petits intervalles centrés en $\sqrt{2}$:
- celui de longueur 1 contient un rationnel (au moins), par exemple 1.
En effet, $1 < \sqrt{2} < 2$ puisque $1^2 < 2 < 2^2$ et la fonction racine carrée est strictement croissante.
- celui de longueur 10^{-1} contient encore un rationnel (au moins), par exemple $\frac{11}{8}$.
La démonstration est analogue et est laissée au (à la) lecteur(trice).
- celui de longueur 10^{-2} contient encore un rationnel (au moins), par exemple $\frac{181}{128}$ qui est aussi contenu dans celui de longueur 10^{-3}...

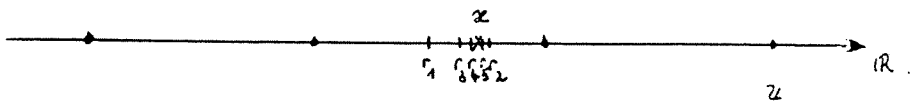
Nous pouvons continuer ainsi en divisant la longueur de l'intervalle par 10 à chaque étape et nous trouvons toujours (au moins) un rationnel dans l'intervalle. Pourquoi?



Nous avons vu que $1 < \sqrt{2} < 2$, autrement dit $\sqrt{2}$ appartient à l'intervalle $]1,2[$; divisons ce dernier en deux en son milieu $r_1 = \frac{3}{2}$. Nous avons deux intervalles de longueur moitié, à savoir $]1,\frac{3}{2}[$ et $]\frac{3}{2},2[$. Nécessairement, $\sqrt{2}$ est dans l'un des deux, plus précisément dans $]1,\frac{3}{2}[$ (puisque $2 < (\frac{3}{2})^2 = \frac{9}{4}$). Ainsi, $\sqrt{2}$ est distant du milieu $r_2 = \frac{5}{4}$ d'au plus la moitié de la longueur de l'intervalle, c'est-à-dire $\frac{1}{2}\cdot\frac{1}{2} = (\frac{1}{2})^2 = \frac{1}{4}$. Nous recommençons l'opération avec l'intervalle $]1,\frac{3}{2}[$ que nous coupons en $\frac{5}{4}$. Cette fois-ci $\frac{5}{4} < \sqrt{2}$ d'où $\sqrt{2}$ appartient à $]\frac{5}{4},\frac{3}{2}[$. Le milieu $r_3 = \frac{11}{8}$ est alors distant d'au plus $\frac{1}{2}\cdot\frac{1}{4} = (\frac{1}{2})^3 = \frac{1}{8}$.

Et ainsi de suite... Nous obtenons une suite de rationnels $(r_n)_n$ telle que, pour chaque n, $|\sqrt{2} - r_n| < (\frac{1}{2})^n$. Comme $(\frac{1}{2})^n$ tend vers 0 quand n devient grand, r_n est de plus en plus proche de $\sqrt{2}$ et nous trouvons près de $\sqrt{2}$ une accumulation de r_n, et plus généralement de rationnels.

Nous pouvons imaginer qu'en remplaçant $\sqrt{2}$ par un irrationnel arbitraire x et en procédant de même, nous obtiendrions (au moins en théorie...) une suite de rationnels allant, lentement mais sûrement, "s'écraser" sur x. (Pour bien voir la particularité de cette situation, pensez à $\mathbf{Z}$ dans $\mathbf{Q}$)



En conséquence, comment obtenir $\mathbf{R}$ à partir de $\mathbf{Q}$?... grâce aux suites de rationnels (bien sûr?) mais nous voilà bien loin de nos propos.

Et pour finir cette première partie, parlons un peu...

Des nombres complexes.

Il s'agit là de toutes les solutions d'équations polynômiales à coefficients réels. Tout d'abord, celles de l'équation $x^2 + 1 = 0$ notées traditionnellement i et $-i$, puis celles de $x^2 + x + 1 = 0$ par exemple qui s'expriment à l'aide de réels et de i (ce sont $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$), puis encore celles de $ax^2 + bx + c = 0$ ($a, b, c \in \mathbf{R}$ arbitraires) qui s'expriment encore à l'aide de réels et de i (*Quelles sont-elles?* [7]). Nous admettrons que les équations de degré supérieur n'apportent rien de nouveau et que, par conséquent, tout nombre complexe est de la forme $\alpha + i\beta$, $\alpha, \beta \in \mathbf{R}$.

Inversement, de quelle équation à coefficients réels, de degré 2 par exemple, $z = \alpha + i\beta$ est-il solution? [8]

[7] La réponse se trouve dans votre cours de terminale...

[8] La réponse précédente vous fournit la deuxième solution z' de l'équation cherchée... Vous connaissez donc une forme factorisée d'une équation ayant z et z' pour solutions. Développez et concluez. Si nécessaire, vous trouverez plus de détails à la note 1.

REMARQUE : de par nos constructions successives, tous les éléments de $\mathbf{N}$ sont des éléments de $\mathbf{Z}$, de $\mathbf{Q}$, de $\mathbf{R}$ et de $\mathbf{C}$; tous ceux de $\mathbf{Z}$ sont dans $\mathbf{Q}$, $\mathbf{R}$,$\mathbf{C}$, ceux de $\mathbf{Q}$ dans... ce qui s'écrit : $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$.

Mais où se cachent les **nombres décimaux**?

Les nombres décimaux sont ceux de la forme $\frac{a}{10^n}$ où a est un entier relatif ($a \in \mathbf{Z}$) et n un entier naturel ($n \in \mathbf{N}$). Ils s'écrivent tous sous forme décimale avec un nombre fini de chiffres après la virgule. Certains, ceux qui n'ont pas trop de décimales, apparaissent sur un cadran de machine à calculer. Ils sont utilisés pour les valeurs approchées, fort souvent en physique, chimie, biologie... mais fort peu en mathématiques. En effet, beaucoup de mathématiques, en particulier l'arithmétique, ne s'encombrent pas de valeurs approchées.

On note $\mathbf{D}$ l'ensemble de tous les nombres décimaux.

1) $\frac{1}{2}$ *est-il dans* $\mathbf{D}$*?*

2) $\frac{1}{3}$ *est-il dans* $\mathbf{D}$*?* On pourra à l'occasion réfléchir sur le "tiers mathématique", c'est-à-dire $\frac{1}{3}$ et le "tiers de toute machine à calculer", c'est-à-dire $0,33333333$. En mathématique, il s'agit de deux nombres différents.

3) *Montrer que* $\mathbf{D}$ *n'est égal à aucun des ensembles précédemment étudiés.*
(Il suffit d'exhiber un élément qui est dans l'un mais pas dans l'autre. Par exemple $\frac{1}{10}$ est dans $\mathbf{D}$ mais pas dans $\mathbf{N}$ donc $\mathbf{D}$ est différent de $\mathbf{N}$.)

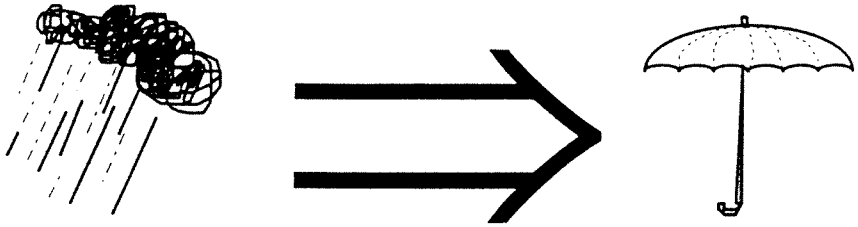
4) *Nous avons vu que* $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$. *Pouvez-vous intercaler* $\mathbf{D}$ *dans cette suite d'inclusions?*

5) *Peut-on parler de corps des nombres décimaux?* (Cf. la parenthèse trois, quatre pages avant)

MET(H)EO(RIE)

On considère la phrase :

P0 : S'il pleut alors j'ai un parapluie !



Parmi les phrases qui suivent il y a celles qui sont synonymes de la phrases P0, celles qui sont en contradiction avec P0 et ... les autres.
Pouvez-vous les répartir dans ces trois catégories (S = synonyme de P0, C = en contradiction avec P0, A = autres)

1. Si je n'ai pas de parapluie, il ne pleut pas.
2. Il suffit qu'il pleuve pour que j'aie un parapluie
2. J'ai un parapluie s'il pleut.
4. J'ai un parapluie.
5. Il pleut et je n'ai pas de parapluie.
6. Il suffit que j'aie un parapluie pour qu'il pleuve.
7. Il est nécessaire qu'il pleuve pour que j'aie un parapluie.
8. S'il ne pleut pas, je n'ai pas de parapluie.
9. Il ne pleut pas ou j'ai un parapluie.
10. Il faut qu'il pleuve pour que j'aie un parapluie.
11. Après la pluie le beau temps.
12. Je n'ai pas de parapluie et il pleut.
13. Il pleut.

Solution :

Une aide précieuse peut être de présenter les 4 situations envisageables par les cases d'un tableau à double entrée en distinguant les situations compatibles (situations dans lesquelles la phrase P0 est vraie) de celles qui sont incompatible avec P0.

ET	il pleut	il ne pleut pas
j'ai un parapluie	compatible	compatible
je n'ai pas de parapluie	**incompatible**	compatible

1. Si je n'ai pas de parapluie, il ne pleut pas.

synonyme : car s'il pleuvait j'aurais un parapluie. C'est ce que l'on appelle la forme contraposée de la phrase de départ.

2. Il suffit qu'il pleuve pour que j'aie un parapluie.

synonyme : la pluie est une condition suffisante pour que j'aie un parapluie. Dans le tableau, la seule case «compatible » de la colonne « il pleut » est dans la ligne « j'ai un parapluie ».

3. J'ai un parapluie s'il pleut.

synonyme : c'est une autre formulation de la phrase de départ P0.

4. j'ai un parapluie

autres : s'il ne pleut pas il est possible que je n'aie pas de parapluie. Dans le tableau, il y a un « compatible » dans la ligne « je n'ai pas de parapluie »

5. Il pleut et je n'ai pas de parapluie.

en contradiction : c'est exactement la situation incompatible du tableau.

6. Il suffit que j'aie un parapluie pour qu'il pleuve.

autres : avoir un parapluie alors qu'il ne pleut pas ne contredit pas P0.

7. Il est nécessaire qu'il pleuve pour que j'aie un parapluie.

autres : je peux avoir un parapluie alors qu'il ne pleut pas.

8. S'il ne pleut pas, je n'ai pas de parapluie.

autres : avoir un parapluie alors qu'il ne pleut pas ne contredit pas P0.

9. Il ne pleut pas ou j'ai un parapluie.

synonyme : ou il ne pleut pas, ou il pleut et alors j'ai un parapluie.

10. Il faut qu'il pleuve pour que j'aie un parapluie.

autres : c'est une autre formulation de la phrase 7.

11. Après la pluie le beau temps.

autres : cette affirmation n'a bien sûr aucun rapport avec la phrase P0.

12. Je n'ai pas de parapluie et il pleut.

en contradiction : car s'il pleut j'ai un parapluie.
C'est une phrase équivalente à la 5 car en logique le « et » est commutatif..

13. Il pleut.

autre : s'il pleut j'ai un parapluie n'affirme en rien qu'il pleut (une phrase analogue serait « si je gagne au Loto j'achète une voiture »). Dans le tableau il y a « compatible » dans la colonne « il pleut »

Des exemples de problèmes célèbres en arithmétique.

Les problèmes d'arithmétique dont nous allons parler portent sur l'étude des propriétés des nombres rationnels ou des entiers relatifs, par exemple les propriétés liées à la divisibilité dans **Z**. Un thème très important est la résolution (dans **Q** bien sûr) d'équations polynômiales, à une ou plusieurs inconnues, à coefficients rationnels (ou entiers), celles que l'on nomme *équations diophantiennes*, du nom de Diophante d'Alexandrie, mathématicien grec du IVème siècle ap. J.C.

Problème des triplets de Pythagore (Pythagore, VIème siècle av. J.C.) : *Trouver tous les triangles rectangles.*

Cela consiste à déterminer la longueur des côtés de tous les triangles rectangles. En termes d'équations (les longueurs étant appelées x, y, z), cela se traduit par : trouver toutes les solutions de $x^2 + y^2 = z^2$ où x, y, z sont les inconnues. Les triplets solution sont appelés "*triplets de Pythagore*".

C'est facile, direz-vous... En fait, ce n'est pas si simple car, Pythagore comme tous les arithméticiens même actuels, ne s'intéressent qu'aux solutions *rationnelles* (c'est-à-dire formées de nombres rationnels; par exemple, il n'y a pas de solution avec $x = 1$ et $y = 1$). Se restreindre aux solutions rationnelles est une difficulté plus ou moins surmontable.

Comment fabriquer (astucieusement) des triplets de Pythagore?

Tout d'abord, montrez que si la somme de deux entiers consécutifs est un carré, alors la différence de leurs carrés est encore un carré.

Puis, déduisez-en des triplets de Pythagore avec les valeurs suivantes de x : $x = 3$, puis 5. puis 11 et 101. (solution 1)

Pour les fabriquer tous, il nous faut persévérer...

Puisqu'extraire des racines carrées est très délicat dans **Q**, il vaut mieux l'éviter. Comment? Grâce à l'astuce... Mais en quoi consiste-t-elle au juste?

A poser $z = x + 1$ et à choisir y comme paramètre. Ce qui donne : $z^2 = x^2 + y^2 \Leftrightarrow 2x + 1 = y^2$... une équation en x du premier degré qui se résoud dans **Q** sans encombre : $x = \frac{y^2-1}{2}$, $z = \frac{y^2+1}{2}$, $y \in \mathbf{Q}$.
Généralisons. La différence entre z et x peut a priori prendre toutes les valeurs. Posons donc $z - x = b$, $b \in \mathbf{Q}$. Alors l'équation $z^2 = x^2 + y^2$ devient $2bx + b^2 = y^2$. Nous retrouvons une équation du premier degré en x avec deux paramètres (cette fois) à savoir b et $a = y$... que nous résolvons aisément :

$$x = \frac{a^2 - b^2}{2b}, \quad y = a, \quad z = \frac{a^2 + b^2}{2b}, \quad a, b \in \mathbf{Q}.$$

Voici donc une description de tous les triplets de Pythagore.

Problème des équations dites de Fermat, c'est-à-dire celles de la forme : $x^n + y^n = z^n$ pour un $n \in \mathbf{N}^*$ fixé.

Pour $n = 2$, nous retrouvons le problème précédent. Pour $n = 3$ ou 4, sa résolution est due à Pierre de Fermat (vous en trouverez un aperçu dans la fin du chapitre). Mais il a fallu presque 350 ans de plus pour résoudre le cas général. C'est le "grand théorème de Fermat" qui affirme que *si $n > 2$, l'équation $x^n + y^n = z^n$ n'a pas de solution rationnelle avec x, y et z non nuls.* Sa démonstration fut terminée en 1993 et utilise des méthodes faisant appel tant à la géométrie, qu'à l'analyse ou l'algèbre mais qui dépassent amplement nos ambitions.

Un problème de Diophante : *Trouver trois nombres qui soient en égale différence et tels que, pris deux à deux, ils forment un carré.*
Ici, *nombres* signifie nombres rationnels. Ces trois nombres a, b et c sont *en égale différence* si $c - b$ et $b - a$ sont égaux au même nombre rationnel r et *forment deux à deux un carré* si la somme de deux d'entre eux est un carré.

Ce problème se formule également ainsi : Trouver $a, b, c \in \mathbf{Q}$ tels que (1) $c - b = b - a$ et (2) il existe $A, B.C \in \mathbf{Q}$ tels que $b + c = A^2$, $c + a = B^2$ et $a + b = C^2$.

Si nous notons $r = c - b = b - a$, la connaissance de a et r nous permet de déterminer b et c ($b = a + r, c = a + 2r$) et la condition (2) devient : il existe $A, B, C \in \mathbf{Q}$ tels que $2a + 3r = A^2$, $2a + 2r = B^2$ et $2a + r = C^2$. Ce qui nous conduit naturellement à un autre problème :

Problème-variation[9] : *Trouver trois carrés en progression arithmétique.*

Aucun doute, ces deux problèmes sont différents mais leurs solutions semblent cependant liées. Regardons-les de plus près.

Soit a, b, c une solution du problème de Diophante, c'est-à-dire que $b - a = c - b = r$ et $a + b, b + c$ et $a + c$ sont des carrés dans $\mathbf{Q}$. D'après ce qui précède, $a + b$, $a + c$ et $c + b$ sont alors trois carrés en progression arithmétique. Ainsi nous obtenons une solution du problème-variation.

Inversement, si A^2, B^2, C^2 est une solution du problème-variation, comment obtenir une solution du problème de Diophante? *Examinez les calculs précédents* (avec les yeux mais aussi le stylo...cela ne marchera peut-être pas du premier coup) *et donnez l'expression d'une solution du problème de Diophante à l'aide de A, B, C.* (*Si vous perdez pied, voici une bouée : l'examen des calculs précédents nous montre que la différence $r = b - a = c - b$ d'une solution au problème de Diophante est égale à la raison de la progression arithmétique formée par A^2, B^2, C^2 et que le plus petit terme vaut $2a + r$. Posons donc $r = C^2 - B^2 = B^2 - A^2$ et $2a + r = A^2$. On obtient alors a, $b = a + r$ et $c = a + 2r$ en fonction de A, B, C. Les résultats précis sont (après un peu de bricolage) : $a = \frac{A^2+B^2-C^2}{2}, b = \frac{A^2-B^2+C^2}{2}, c = \frac{-A^2+B^2+C^2}{2}$. On vérifie que ces valeurs sont bien solution du problème de Diophante.*)

Que faisons-nous en fait? Nous avons les ensembles des solutions de deux problèmes, disons $\mathcal{S}_1$ et $\mathcal{S}_2$. A un élément de $\mathcal{S}_1$, nous associons un élément de $\mathcal{S}_2$ (*gommettes et boules de pétanques...*). Nous avons donc une application de $\mathcal{S}_1$ dans $\mathcal{S}_2$. A un élément de $\mathcal{S}_2$, nous

[9] ou variation sur un problème...

associons un élément de S_1. Nous avons donc une autre application, de S_2 dans S_1 cette fois. *Calculez les deux composées de ces applications. Que constatez-vous?* (Si nécessaire, les réponses se trouvent en note 2.)

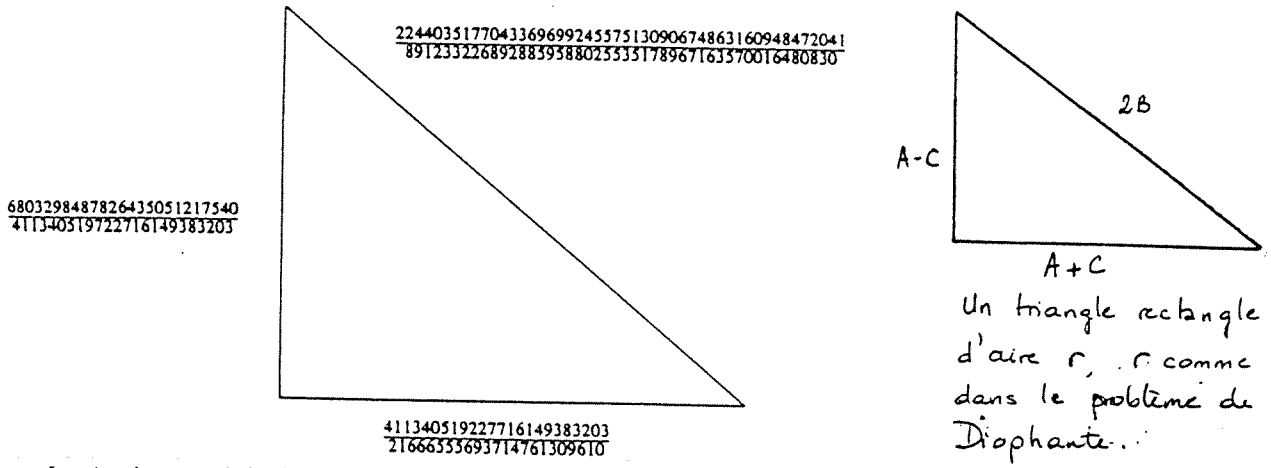
Nous avons donc une bijection de S_1 sur S_2. Autrement dit, si on connaît toutes les solutions du problème de Diophante, on en déduit toutes celles du problème-variation **et inversement**, si on connaît toutes les solutions de celui-ci, on en déduit toutes celles de celui-là. Par conséquent, si nous résolvons l'un des deux, nous aurons résolu les deux. Pour cette raison, les deux problèmes précédents sont dits *équivalents.*

Résolution du problème de Diophante : Il suffit de voir qu'il est équivalent au problème des triplets de Pythagore. Comme il est équivalent au problème-variation, montrons que le problème-variation et celui des triplets de Pythagore sont équivalents. A votre tour!...

(*A ne lire qu'en cas de panne d'idée : dans le sens "problème de Diophante" vers celui des triplets de Pythagore, l'ingrédient est les identités remarquables du carré, ou plus exactement la combinaison de deux d'entre elles, à savoir* $(x+y)^2+(x-y)^2=2(x^2+y^2)$. *Si c'est la noyade, prenez la bouée 1*)

Problème des nombres congruents[10].

Est appelé *nombre congruent* un nombre rationnel qui représente l'aire d'un triangle rectangle à côtés rationnels. Par exemple, 6 est un nombre congruent : l'aire du triangle de côtés (3,4,5) est 6. De même 5 est congruent (c'est l'aire du triangle rectangle de côtés $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$) et 157 aussi. Dans le problème de Diophante, le nombre r est congruent; dans le problème-variation, la raison de la progression arithmétique est un nombre congruent (voir ci-dessous).



Le triangle rectangle le plus "simple" dont l'aire est 157 (D. Zagier)

Plus généralement, nous connaissons tous les triangles rectangles à côtés rationnels. Nous savons calculer leur aire à partir des côtés. Nous pouvons donc déterminer tous les nombres congruents.

1. *En reprenant la description des triplets de Pythagore, montrer qu'un entier congruent* n *qui n'est pas divisible par un carré s'écrit sous la forme* $n=\frac{ab(a^2-b^2)}{c^2}$ *où* a, b *et* c *sont des*

[10] Malgré une éthymologie commune avec les termes *congru* et *congruence*, sa signification n'a rien de commun avec les leurs.

entiers bien choisis.

Ainsi.vous pouvez obtenir une liste d'entiers congruents : pour chaque valeur m de a, faites varier b de 1 à $m-1$ (*pourquoi?*), calculez $ab(a^2-b^2)$ puis divisez par le plus grand carré possible.

2. *Quitte à vous aider d'une machine à calculer, dressez le début de la liste (au moins jusqu'à $a=6$...et au plus jusqu'à lassitude.)*

Comme vous pouvez le constater les nombres obtenus n'ont pas d'ordre particulier. S'il vous est aisé d'affirmer que 15, 210 ou 330 sont congruents, que pouvez-vous dire de 1, 14, 17, 34, 70. 209 ou 429? Si vous poussez plus loin vos calculs, vous verrez apparaître 70, puis 14 puis 34 puis 429 ... Mais pourquoi 1, 17 et 209 n'apparaissent-ils pas? Est-ce vos calculs qui s'arrêtent trop vite ou ces nombres n'apparaitront-ils jamais? Impossible de répondre par cette méthode! D'où

Enoncé : Comment reconnaître parmi tous les rationnels ceux qui sont congruents?

Il faut avouer que la réponse n'est pas encore entièrement connue. Plus précisément, un critère a été établi en 1983 mais sa démonstration utilise un résultat *conjectural* [11]. C'est un exemple de problème très ancien, pas encore entièrement résolu, qui s'est transformé au cours des siècles en donnant naissance à de nouvelles théories qui à leur tour, ont posé de nouveaux problèmes dont la résolution peut avoir exigé de nouvelles théories... et ainsi se font les mathématiques!

Il y a bien d'autres exemples de problèmes, certains aussi vieux, d'autres plus récents, voire très récents, qui n'ont pas de solutions ou des solutions partielles.

Des nombres dits premiers.[12]

On dit qu'un entier b *divise* un entier a (ou que b est un *diviseur de* a ou encore que a est un multiple de b) s'il existe un entier q tel que $a=bq$. Si b divise a, on note $b|a$. Par exemple, $2|6$, $3|9$ mais $4 \not| 41$.

Cette relation "divise" possède un certain nombre des propriétés simples que nous énonçons et démontrons ci-après.

PROPRIÉTÉS : (1) Pour tout entier a, $a|a$ et $1|a$.

(2) Soient a et b deux entiers non nuls. Si $b|a$ et $a|b$, alors $a=\pm b$.

(3) Soient a, b et c trois entiers non nuls. Si $c|b$ et $b|a$, alors $c|a$.

(4) Soient a, b et c trois entiers non nuls. Si $c|b$ et $c|a$, alors $c|a+b$.

Démonstration : (1) est claire puisque $a=a\cdot 1=1\cdot a$.

(2) Par définition, si $b|a$ et $a|b$ alors il existe deux entiers q et q' tels que $a=bq$ et $b=aq'$. En substituant la valeur de b de la deuxième égalité dans la première, nous obtenons $a=(aq')q=a(q'q)$ (par associativité) d'où $q'q=1$. Ceci entraîne que $q=q'=\pm 1$

[11] On entend par *résultat conjectural* ou *conjecture* un résultat qu'on espère vrai (car de nombreux indices vont dans le sens de ce résultat) mais dont la démonstration nous échappe.

[12] De façon délibérée, nous avons choisi un style plus concis l'instant de deux pages. Nous n'y rappelons que des résultats vus en terminale... ce qui vous donne la liberté de les passer sans perdre le fil.

(sinon, la valeur absolue de q ou q' est supérieure à 2 donc $|qq'| \geq 2 > 1$). Autrement dit, $a = b \cdot (\pm 1) = \pm b$.

(3) Si $c|b$ et $b|a$, alors il existe q et q' tels que $b = cq$ et $a = bq'$. On en déduit que $a = (cq)q' = c(qq')$, c'est-à-dire que $c|a$.

(4) Si $c|b$ et $c|a$, alors il existe q et q' tels que $b = cq$ et $a = cq'$. On en déduit que $a + b = cq + cq' = c(q + q')$ donc que $c|a + b$. ◇

Pour simplifier, nous ne considèrerons dans la suite que des entiers **naturels**, c'est-à-dire positifs. Ainsi, dans ce paragraphe, un *entier* désignera toujours un entier **naturel**.

D'après la définition, un diviseur d'un entier a non nul est toujours au plus égal à a (car q est un entier). Par conséquent, chaque entier non nul possède un nombre fini de diviseurs (car ce sont des entiers).

D'après (1), tous les entiers au moins égaux à 2, possèdent au moins deux diviseurs distincts, à savoir 1 et lui-même. Seuls les entiers qui n'en possèdent pas d'autres ne peuvent être écrits comme produit d'entiers plus petits. Pour cela, ces nombres jouent un rôle particulier en arithmétique.

DÉFINITION : Un entier p est dit *premier* s'il est supérieur ou égal à 2 et si ses seuls diviseurs sont 1 et p.

Exemples : 2 et 3 sont des nombres premiers.

et

Contre-exemples : 1 n'est pas premier car inférieur strictement à 2. 4 n'est pas premier car il possède 3 diviseurs, à savoir 1,2,4; etc...

Aucun entier de la forme n^3+1 où n est un entier n'est premier sauf $2 = 1^3+1$. Pourquoi?
(Il convient de trouver suffisamment de diviseurs de $n^3 + 1$ alors... pensez à factoriser!)

THÉORÈME (EUCLIDE) : *Il existe une infinité de nombres premiers.*

Démonstration : Tout d'abord, nous établissons un résultat préliminaire.[13]

Lemme : Tout entier $n \neq 1$ possède un diviseur premier.

Démonstration : On raisonne par récurrence sur n avec l'hypothèse au rang n : tout entier compris entre 2 et n, possède un diviseur premier.

L'hypothèse au rang 2 est vraie : 2 est le seul entier concerné et possède 2 comme diviseur premier.

Si l'hypothèse au rang n est vraie, c'est-à-dire si tout entier $m \leq n$ possède un diviseur premier, montrons qu'il en va de même au rang $n+1$, c'est-à-dire que tout entier $m \leq n+1$ possède un diviseur premier.

Considérons m un entier plus petit que $n + 1$. Si $m < n + 1$ alors $m \leq n$ et m possède un diviseur premier d'après l'hypothèse de récurrence au rang n. Si $m = n + 1$, deux cas peuvent se produire. Soit $n+1$ possède un diviseur autre que 1 et lui-même, alors ce diviseur est inférieur ou égal à n et possède un diviseur premier par hypothèse de récurrence qui est aussi un diviseur premier de $n+1$ d'après la propriété (3); soit $n+1$ ne possède pas d'autres

[13] On nomme classiquement *lemme* un tel résultat.

diviseurs que 1 et lui-même, alors $n+1$ est premier donc possède encore un diviseur premier (lui-même). Ainsi, dans tous les cas, $n+1$ possède un diviseur premier.

L'hypothèse au rang $n+1$ est donc vérifiée. Par conséquent, l'hypothèse est vraie pour tout $n \geq 2$. Ceci termine la démonstration du lemme.

Démontrons maintenant le théorème d'Euclide par l'absurde. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers et notons-les p_1, p_2,..., p_k. Considérons l'entier $n = p_1p_2...p_k + 1$. D'après ce qui précède, n possède un diviseur premier, nécessairement l'un des p_i grâce à notre hypothèse. Notons p ce diviseur. Mais alors p divise $p_1p_2...p_k$ et n donc il divise $n - p_1p_2...p_k = 1$ donc $p = 1$. Or p est premier et 1 ne l'est pas. C'est absurde! L'hypothèse de départ est donc erronée. $\Diamond$

On déduit du lemme précédent le

LEMME : *Tout entier supérieur ou égal à 2 peut être écrit comme un produit de nombres premiers.*

Démonstration : Il s'agit d'une démonstration par récurrence, semblable à celle du lemme précédent. Elle est donc laissée au (à la) lecteur(trice). Autrement dit, en exercice...

Nous venons de démontrer l'existence de la décomposition d'un entier naturel en produit de facteurs premiers. Nous savons, en outre, que

LEMME : *La décomposition d'un entier naturel en produit de facteurs premiers est unique à l'ordre des facteurs près.*

Cela signifie simplement qu'en choisissant d'ordonner les facteurs premiers (par exemple par ordre croissant... ou par ordre décroissant) l'écriture est unique.

Nous admettons ce résultat faute d'outils suffisants pour la démonstration.

Et sur ces mots, **terminons notre petit passage "studieux"** et retournons fouiner dans les problèmes du paragraphe précédent voir si nos connaissances (actuelles) nous permettent de progresser vers une solution.

Plus précisément, penchons-nous sur la résolution des équations de Fermat. Il s'agit de montrer que l'équation (E_n) $x^n + y^n = z^n$ où $n > 2$ est un entier, n'a pas de solutions rationnelles avec x, y, z non nuls. A défaut de résoudre ce problème, nous allons le *réduire...Qu'est-ce à dire*? Trouver un autre problème plus simple qui une fois résolu, nous permet de résoudre le problème initial.

Pour s'exprimer plus aisément, nous qualifierons de *triviale* une solution rationnelle (x, y, z) dont l'une des composantes est nulle.

Soit n un entier. Il s'écrit comme produit de facteurs premiers. Soit p l'un d'entre eux et notons $n = pm$. Alors, l'équation (E_n) à résoudre s'écrit : $(x^m)^p + (y^m)^p = (z^m)^p$. Ainsi, si (a, b, c) désigne une solution de (E_n) alors (a^m, b^m, c^m) est une solution de (E_p). Supposons que toute solution rationnelle de (E_p) soit triviale. Dans ce cas, le triplet (a^m, b^m, c^m) a une composante nulle donc a, b ou c est nul et la solution (a, b, c) de (E_n) est triviale. Par conséquent, si toute solution rationnelle de (E_p) est triviale, toute solution de (E_n) l'est aussi.

On en déduit que si nous montrons le résultat pour chaque équation (E_p) où p est un entier premier, nous aurons en fait tout démontré. Il nous *suffit* donc de considérer les cas où n est premier.

MAIS il y a un problème... Par exemple si $n = 4$, le seul diviseur premier est 2. Or (E_2) a beaucoup de solutions rationnelles non triviales (Voir le problème des triplets de Pythagore). Nous **ne** pouvons **pas** conclure (et certainement pas, que (E_4) a aussi des solutions rationnelles non triviales...(c'est l'histoire de la pluie et du parapluie qui précède cette partie)). Il faut donc étudier le cas $n = 4$.

Et maintenant, si nous savons que (E_4) et les (E_p) où p est un nombre premier impair (c'est-à-dire autre que 2) n'ont que des solutions rationnelles triviales, pouvons-nous le déduire pour toutes les équations (E_n), $n > 2$? (bouée 2)

Imaginez maintenant que nous possèdions une "formule", à la rigueur compliquée, décrivant la suite des nombres premiers... Nous aurions alors un plan d'attaque (par récurrence) pour l'étude des équations (E_p). MAIS... une telle description n'existe pas.

PIS! Vous connaissez une manière de savoir si un nombre est premier ou non : le crible d'Erathostène... Si l'entier en question est "vraiment très grand", c'est très, très laborieux, tellement laborieux que même les ordinateurs n'y arrivent pas en un temps raisonnable. Et il a fallu développer des tests de plus en plus sophistiqués, faisant appel à des résultats théoriques assez poussés (encore du travail pour les mathématiciens!), pour décider si un entier donné est premier ou non. Malgré tout, il y a encore des nombres (à plus de 1000 chiffres) dont on ne peut que supposer qu'ils soient premiers... sans le prouver.

Un problème voisin est celui de la factorisation d'un entier n. S'il est facile d'imaginer une méthode d'obtenir une factorisation de n (par exemple, en effectuant les divisions de n par tous les entiers entre 2 et $n-1$), la mettre à exécution prend un temps énorme (même avec l'aide d'un ordinateur!). Là aussi, des mathématiciens déploient, encore de nos jours, toute leur ingéniosité pour trouver des méthodes très performantes.

Ces deux problèmes, test de primalité et factorisation, sont intimement liés aux questions de codage et décodage de messages, ce que l'on nomme la *cryptographie*[14].

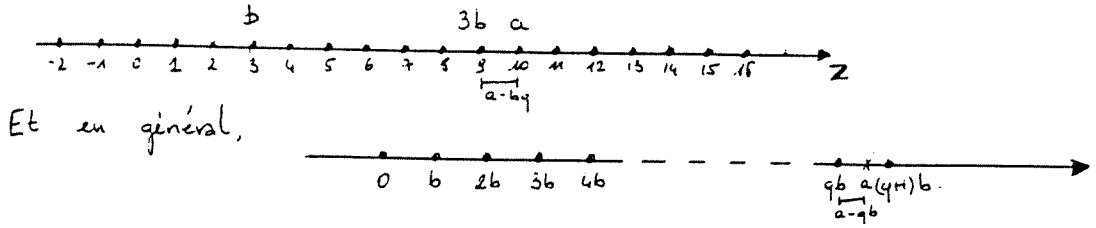
Pour conclure ce paragraphe, disons que depuis Euclide, l'étude des nombres premiers a été la source de nombreux travaux de mathématiciens et cette source n'est pas encore tarie. Voici quelques questions qui font toujours chercher les mathématiciens :

- **Conjecture des nombres premiers jumeaux** : Deux nombres premiers sont dits *jumeaux* si leur différence vaut ± 2. Par exemple, 3 et 5 sont jumeaux, ainsi que 5 et7, 11 et 13, 17 et 19,... Existe-t-il une infinité de couples de nombres premiers jumeaux? La conjecture des nombres premiers jumeaux affirme que la réponse est positive.
- **Conjecture de Goldbach** (question posée par C. Goldbach à Euler en 1742) : Tout entier pair autre que 2 s'écrit comme somme de deux nombres premiers.
- Existe-t-il une infinité de nombres premiers p tels que $p-1$ soit un carré?
- Entre deux carrés, existe-t-il un nombre premier?

[14] Vous trouverez un exemple à la dernière page.

De la division dans Z et de ses conséquences.

Comme déjà dit plus haut, parler de la fraction $\frac{a}{b}$ pour n'importe quel entier a et b (b non nul) n'a pas toujours de sens dans Z, par exemple [15] si $a = 13$ et $b = 3$. Rien ne nous empêche, par contre, de considérer le plus grand *multiple* de b qui soit inférieur à a (*Dans l'exemple, il s'agit de 12*). Notons-le qb (*donc , q vaut 4*). La plupart du temps, il est différent de a (*C'est notre cas!*). Que pouvons-nous dire de la différence $a - qb$? (*Elle vaut 1....*) Elle est positive (puisque qb est plus petit que a). Elle est *strictement* inférieure à b. Pourquoi? $(q + 1)b$ est nécessairement plus grand que a sinon qb ne serait pas le plus grand multiple de b qui soit inférieur à a (*Nous sommes d'accord!*).



Notons $r = a - qb$. Nous obtenons alors : $a = bq + r$ avec $0 \leq r < b$ (*$10 = 3 \cdot 3 + 1$*). Vous reconnaissez la formule de la *division euclidienne* de a par b où q s'appelle le quotient et r le reste. *Existe-t-il d'autres entiers q' et r' répondant aux mêmes conditions?* (cf. note 3)

Le reste est nul si et seulement si b divise a.

Si $b > a$, le quotient de a par b est 0 et le reste est a. En particulier, on retrouve que tout diviseur de a est plus petit que a.

Un premier exemple d'application.

Prenons un nombre premier p différent de 2 et 3. Montrer que p est de la forme $6n - 1$ ou $6n + 1$, $n \in \mathbf{N}^*$. (Vous pouvez remarquer que 6n - 1= 6(n -1) + 5 et que ces deux expressions ressemblent à la division euclidienne de p par 6. Alors... étudiez le cas de chaque reste puis concluez. Nous parlerons d'une solution de ce problème à la fin du chapitre, solution 2.) *Que dire de la réciproque?*

Vous venez d'obtenir un premier critère (assez grossier[16]) permettant de savoir que certains entiers ne sont pas premiers : ceux de la forme $6n + 2$ et différents de 2, $6n + 3$ et autres que 3, $6n + 4$ et bien sûr $6n$.

Un deuxième exemple d'application.

Prenons deux entiers, $a = 54$ et $b = 35$.

---

[15] *Nous suivrons la démarche sur cet exemple en indiquant les résultats dans cette écriture, aussi petite et penchée.* Vous pouvez également choisir vos propres exemples.

[16] En fait, ce critère équivaut à n'exclure que les multiples de 2 et 3.

Effectuons la division euclidienne de a par b : $54 = 35 \cdot 1 + 19$

puis de b par le reste obtenu précédemment $35 = 19 \cdot 1 + 16;$

puis de ce dernier par le deuxième reste obtenu $19 = 16 \cdot 1 + 3;$

et ainsi de suite... jusqu'à épuisement? $16 = 3 \cdot 5 + 1,$

$3 = 1 \cdot 3 + 0.$

Non. cela se termine puisque nous obtenons un reste nul.

Recommençons en changeant a et b : $a = 2574$, $b = 309$; $a = 159$, $b = 86$; ou d'autres de votre choix... Nous arrivons à chaque fois à un reste nul en un nombre fini d'étapes. Nous affirmons qu'en fait, cela se produit pour tous a et b (non nul).

Argumentons notre affirmation.

Prenons donc a et b quelconques, pas tout à fait puisque b doit être non nul et plus petit que a. Et recommençons notre "manipulation": $a = bq_1 + r_1$ avec $0 \leq r_1 < b$; $b = r_1q_2 + r_2$ avec $0 \leq r_2 < r_1$; $r_1 = r_2q_3 + r_3$ avec $0 \leq r_3 < r_2$, etc...tant que le reste obtenu n'est pas nul. Les restes r_i forment une suite strictement décroissante d'entiers tous positifs et strictement inférieurs à b: $b > r_1 > r_2 > r_3 > \ldots \geq 0$. Nous voulons montrer que cette suite est finie (puisqu'elle s'arrête quand le reste s'annule). Or, il n'y a que b entiers positifs et strictement inférieurs à b et les termes de notre suite sont deux à deux distincts. Donc cette suite a au plus b termes et est bien finie.

Ainsi, notre manipulation mène toujours à 0. Elle est connue sous le nom d'*algorithme d'Euclide* et est un outil arithmétique puissant comme nous le montrent les deux paragraphes suivants.

Nous partons donc de deux entiers a et b et de la suite d'égalités (A.E.) suivante :

$$\begin{array}{lllll} a & = & bq_1 & + & r_1 \\ b & = & r_1q_2 & + & r_2 \\ r_1 & = & r_2q_3 & + & r_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{n-2} & = & r_{n-1}q_{n-1} & + & r_n \\ r_{n-1} & = & r_nq_n. & & \end{array}$$

(Armez-vous de vos stylos!)

LE PGCD

Arrêtons-nous à l'avant-dernière étape. Que pouvons-nous dire du dernier reste non nul, c'est-à-dire de r_n?

Remontons la suite d'égalités précédente : $r_{n-2} = r_{n-1}q_{n-1} + r_n$ et $r_{n-1} = r_nq_n + 0$. Ainsi r_n divise r_{n-1} donc il divise $r_{n-1}q_{n-1} + r_n = r_{n-2}$. De l'étape d'avant, nous déduisons

que r_n divise r_{n-3} et... ainsi de suite jusqu'aux deux premières étapes dont nous déduisons que r_n divise a et b. Le nombre r_n est un *diviseur commun à a et b.*

Redescendons l'algorithme avec un diviseur d commun à a et b : puisque $a = bq_1 + r_1$, c'est-à-dire $r_1 = a - bq_1$, d divise r_1... et il divise encore b donc il divise r_2... et ainsi de suite jusqu'à l'avant dernière étape : d divise r_n. Ainsi r_n est divisible par tout diviseur commun à a et b. Il est donc supérieur à tous les diviseurs communs de a et b.

En conclusion, le dernier reste non nul dans l'algorithme d'Euclide appliqué à deux entiers a et b est le *plus grand diviseur commun à a et b.* Par ce fait, on le baptise le pgcd (reconnaître les initiales de "plus grand commun diviseur") de a et b noté $\text{pgcd}(a, b)$. Quand le pgcd de deux nombres est 1, on dit que ces deux nombres sont *premiers entre eux.*

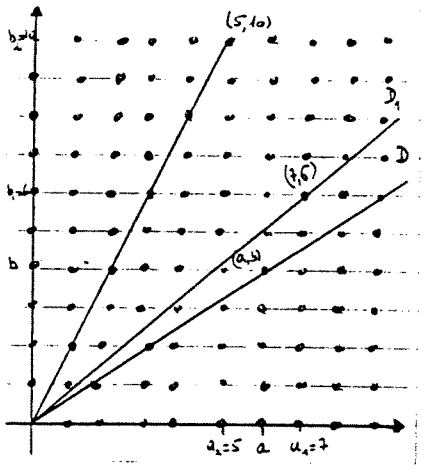
Exemples de calcul. (détaillés en solution 3.)

0) Calculons le pgcd de 154 et 88. Pour cela, effectuons la suite de divisions euclidiennes avec $a = 154$ et $b = 88$: $154 = 1 \cdot 88 + 66$, $88 = 1 \cdot 66 + 22$, $66 = 3 \cdot 22 + 0$: le dernier reste non nul est 22. D'où $\text{pgcd}(154, 88) = 22$.

1) Quel est $\text{pgcd}(a, b)$ *si* $a = 2574$ *et* $b = 309$ *d'une part, si* $a = 159$ *et* $b = 86$ *d'autre part.*

2) Calculer le pgcd *de* 2835 *et* 1960. *Pouvez-vous déterminer deux entiers u et v tels que* $2835u + 1960v = 35$? (sinon, fouiller la suite à la recherche d'une idée!)

3) Faisons un peu de géométrie. Interprétons a et b comme les coordonnées d'un point du plan (puisqu'au nombre de deux). Pour ce faire, donnons-nous un repère du plan (voir ci-contre). Représentons tous les points dont les coordonnées sont entières : ce sont les points d'intersection d'un "quadrillage" régulier et plaçons notre point à l'intersection de la a-ième ligne verticale et de la b-ième ligne horizontale (si les expressions "a-ième" et "b-ième" vous dérangent, remplacez a par 3, 5 ou ce qui vous plaît et b par quelque chose du même style). Traçons la droite D joignant l'origine au point (a, b). Comment déterminer $\text{pgcd}(a, b)$ *à partir de ce dessin? Où se cache-t-il?*



Aidons-nous de notre raisonnement et nos savoirs. Notons $d = \text{pgcd}(a, b)$ (n'hésitez pas à donner des valeurs à a et b, pas trop grandes pour le dessin et à regarder ce qui se passe. Bien sûr cela n'est qu'un guide, non un résultat général!). Alors $a = da'$ et $b = db'$. Le point (a', b') est à coordonnées entières. Se situe-t-il sur D? Prenons celui de coordonnées $(2a', 2b')$. Se situe-t-il sur D? Plus généralement, si n est un entier naturel, où se situe le point de coordonnées (na, nb)? Maintenant, comptez sur votre dessin tous les points de D situés sur le quadrillage (c'est-à-dire à coordonnées entières) compris entre l'origine (exclue) et le point (a, b), variez les valeurs de a et b : que constatez-vous? Reste maintenant à établir ce résultat pour a et b quelconques.

4) Nous pouvons aussi nous intéresser au plus grand diviseur commun de 3 nombres, par exemple 78,182 et 273. Comment le calculer?

Il y a encore une méthode graphique... mais elle nécessite un peu d'imagination car le

dessin est dans l'espace (3 coordonnées cette fois-ci!)

L'ALGORITHME D'EUCLIDE ET UNE CASCADE DE RÉSULTATS...

Repartons de nos deux entiers a et b et de la suite d'égalités (A.E) :

$$\begin{array}{ccccc} a & = & bq_1 & + & r_1 \\ b & = & r_1q_2 & + & r_2 \\ r_1 & = & r_2q_3 & + & r_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{n-2} & = & r_{n-1}q_{n-1} & + & r_n \\ r_{n-1} & = & r_nq_n. & & \end{array}$$

Prenons la première, multiplions-la par q_2 et substituons $b - r_2$ à r_1q_2 (grâce à la seconde). Prenons cette nouvelle égalité, multiplions par q_3 et faisons disparaître r_2q_3 à l'aide de la troisième égalité. Et poursuivons ainsi jusqu'à l'apparition de r_n, autrement dit de pgcd(a, b). Qu'obtenons-nous? La très célèbre *identité de Bézout* qui affirme :

Si a et b sont deux entiers, d leur pgcd *alors il existe deux entiers u et v tels que $au + bv = d$.*

Et comme un résultat peut en cacher d'autres, persévérons :

Théorème de Gauss : Soient a, b et c trois entiers. Si c divise ab et c est premier avec a alors c divise b.

Pourquoi? La condition "c est premier avec a" signifie que le pgcd(a, c) est 1. Appliquons l'identité de Bézout : il existe u et v tels que $au+cv = 1$. Multiplions par b : $abu+cbv = b$. Or c divise abu (grâce à l'hypothèse) et c divise cbv (clair!) donc il divise la somme, c'est-à-dire b. Etes-vous convaincu(e)?

Lemme d'Euclide : Soient a, b et c trois entiers. On suppose que a et b sont premiers entre eux. Si a et b divisent c alors ab divise c.

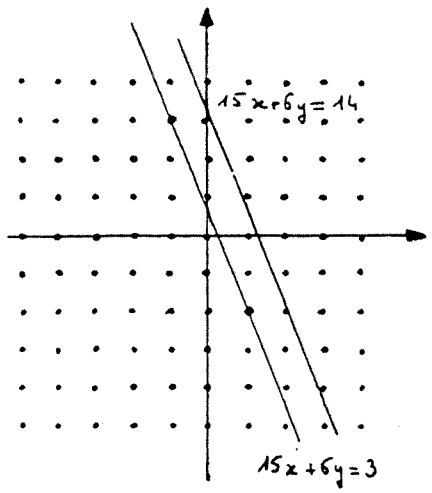
C'est une conséquence du théorème de Gauss. En effet, puisque a divise c, c s'écrit $c = ac'$ où c' est entier. Puisque b divise $c = ac'$ et b est premier à a, par le théorème de Gauss, b divise c'. La fin du raisonnement se déroule rapidement.

Nos premières équations diophantiennes...

1. Trouver les entiers relatifs x et y solutions de l'équation $15x + 6y = 3$ (d'abord en trouver une (x_1, y_1), puis en déduire les autres en remarquant que si (x_2, y_2) est aussi solution $(x, y) = (x_1 - x_2, y_1 - y_2)$ vérifie $15x + 6y = 0$.)

2. Résoudre dans $\mathbf{Z}^2$ l'équation $5x + 4y = 3$.

3. On affirme qu'une équation de la forme $ax + by = c$, $a, b, c \in \mathbf{Z}$, possède des solutions dans $\mathbf{Z}$ si et seulement si pgcd(a, b) *divise c. Etes-vous d'accord?*



Cherchons un" petit coup de pouce" dans la version géométrique du problème. Considérons la première équation. C'est l'équation d'une droite dans le plan. Représentons-la (cf. ci-contre). Sur le même dessin, représentons tous les points dont les coordonnées sont entières (...le "quadrillage" régulier). Où sont les solutions? Elles sont représentées par les points d'intersection du quadrillage et de notre droite. Regardons maintenant la droite d'équation $15x + 6y = 14$. Contient-elle des points du quadrillage? Visiblement non... et par démonstration, non plus : 3 divise 15 et 6 donc il divise $15x + 6y$ pour tous les entiers x et y tandis que 3 ne divise pas 14.

Enhardissons-nous.

4. Trouver trois entiers x, y, z tels que $78x + 182y + 273z = 13$. Trouver tous les triplets d'entiers (x, y, z) tels que $78x + 182y + 273z = 13$ (améliorer la méthode des équations précédentes est une bonne voie...)

5. Prenons deux nombres entiers a et b, premiers entre eux. Supposons que leur produit ab soit un carré, c'est-à-dire qu'il existe un entier c tel que $ab = c^2$. Montrer que a et b sont déjà des carrés (comment reconnaît-on un carré d'après l'écriture en produit de nombres premiers?).

Plus généralement, si a et b sont premiers entre eux et leur produit est une puissance $n^{\text{ième}}$, alors a et b sont aussi des puissances $n^{\text{ièmes}}$.

L'équation de Fermat [17]: (E_4) $x^4 + y^4 = z^4$.

Il s'agit ici de montrer que les seules solutions de cette équation sont les triplets dont l'une (au moins) des composantes est nulle, solutions qualifiées de *triviales*.

Nota bene : Par commodité de langage, nous appellerons *solution entière* de (E_4) une solution de (E_4) dont toutes les composantes sont des entiers relatifs et *solution rationnelle* une solution de (E_4) dans $\mathbf{Q}^3$.

Commençons par QUELQUES REMARQUES SIMPLIFICATRICES.

1. Vérifiez que si (a, b, c) est une solution rationnelle de (E_4), $(-a, b, c)$, $(-a, -b, c)$ et $(-a, -b, -c)$ sont des solutions de (E_4). Pouvez-vous en citer d'autres?

2. Vérifiez que si (a, b, c) est une solution de (E_4) et si $\alpha \in \mathbf{Q}^*$ alors $(\alpha a, \alpha b, \alpha c)$ est aussi solution de (E_4).

3. Déduisez-en qu'une solution rationnelle quelconque de (E_4) s'obtient en multipliant une solution entière par un nombre rationnel.

Poussons un peu plus loin cette dernière remarque.

4. Soit maintenant (x, y, z) une solution entière de (E_4). Montrez qu'un diviseur commun à x et y (en particulier le plus grand) divise aussi z. Déduisez-en que si le pgcd de x et y est différent de 1, la solution (x, y, z) est multiple d'une solution entière (x', y', z') dont les deux

[17] Attention passage difficile ! Poste de secours en solution 5.

premières composantes x' et y' sont premières entre elles. Montrez que z' est premier avec x' et y'.

Ainsi, déterminer les solutions rationnelles de (E_4) se réduit à déterminer les solutions entières, à composantes positives et deux à deux premières entre elles. Baptisons-les *solutions particulières.*

En effet, si nous connaissons toutes les solutions particulières de (E_4), nous obtenons toutes les solutions rationnelles en multipliant les solutions particulières par un rationnel quelconque et en changeant les signes d'autant de composantes que nous voulons. Remarquons alors qu'une solution triviale ne "donne naissance" qu'a des solutions rationnelles triviales. Nous avons donc **simplifier** le problème en

montrer que (E_4) ne possède pas de solutions particulières non triviales.

Dans la suite, nous nommons *très particulière* une solution particulière non triviale.

MAIS en quoi avons-nous simplifier notre problème? En nous ramenant à rechercher des solutions dont les composantes sont des entiers sur lesquels nous pouvons user des outils arithmétiques que nous avons acquis dans les pages précédentes. En particulier, nous pouvons utiliser la *méthode de descente infinie de Fermat.* Rappelons-en le principe.

On raisonne par l'absurde et on suppose donc l'existence d'une solution très particulière (et notre but est de trouver une contradiction). On met sur l'ensemble de ces solutions un ordre, c'est-à-dire que l'on donne un sens à l'expression $(x', y', z') < (x, y, z)$, par exemple $(x', y', z') < (x, y, z)$ peut signifier que $z' < z$ (relation $<$ habituelle dans $\mathbf{Z}$). On invente alors un procédé qui à partir d'une solution très particulière (x, y, z) construit une solution très particulière (x', y', z') strictement plus petite. On obtient ainsi une suite infinie de solutions, de plus en plus petites... et si le nombre de "places" est fini, on aboutit à une contradiction.

Nous allons mettre en œuvre ce principe avec une équation (E') plus simple que (E_4)... bien choisie pour que nous puissons en déduire le résultat espéré sur (E_4).

NOUVELLE RÉDUCTION DU PROBLÈME. Soit l'équation $(E') : x^4 + y^4 = z^2$.

5. Montrez qu'une solution (très) particulière de (E_4) fournit une solution toute aussi particulière de (E').

Concluons en remarquant que si (E') ne possède pas de solutions très particulières l'équation (E_4) non plus. Il suffit donc de

montrer que (E') ne possède pas de solutions très particulières.

MISE EN ŒUVRE DU PRINCIPE.

Nous dirons qu'une solution (x', y', z') est strictement plus petite qu'une autre solution (x, y, z) si $z' < z$ (signification habituelle).

Soit (a, b, c) une solution très particulière de (E'). Construisons une solution très particulière (a_1, b_1, c_1) telle que $c_1 < c$.

6. Montrez que a et b sont de parité différente, c'est-à-dire que 2 divise l'un des deux mais pas les deux...

Comme a et b jouent des rôles symétriques dans l'équation, c'est-à-dire que (a, b, c) et $(b. a. c)$ sont simultanément solutions ou non solutions de (E'), nous pouvons donc supposé que a est impair et b est pair donc c est nécessairement impair.

Ecrivons que (a, b, c) est solution de (E') : $a^4 + b^4 = c^2$ ou $b^4 = c^2 - a^4 = (c - a^2)(c + a^2)$.

7. Montrez que $\text{pgcd}(c - a^2, c + a^2) = 2$.

Comme 2 divise b, 16 divise $(c - a^2)(c + a^2)$. D'après ce qui précède, l'un des facteurs de ce produit est divisible par 2 mais non par 4. L'autre facteur est donc divisible par 8. Deux cas se présentent :

cas 1 : $\begin{cases} c - a^2 = 2\alpha^4 \\ c + a^2 = 8\beta^4 \end{cases}$ où $\alpha, \beta > 0$, α est impair, α et β sont premiers entre eux;

cas 2 : $\begin{cases} c - a^2 = 8\beta^4 \\ c + a^2 = 2\alpha^4 \end{cases}$ où $\alpha, \beta > 0$, α est impair, α et β sont premiers entre eux.

8. Examinons le premier cas. Montrez que $a^2 + \alpha^4 = 4\beta^4$ *mais que 4 ne peut pas diviser* $a^2 + \alpha^4$.

Seul le cas 2 peut donc se produire. Examinons-le.

9. Montrez que le système devient :

$$\begin{cases} c = \alpha^4 + 4\beta^4 \\ 4\beta^4 = (\alpha^2 - a)(\alpha^2 + a) \end{cases}.$$

10. Calculez le pgcd de $\alpha^2 - a$ *et* $\alpha^2 + a$. *Déduisez-en l'existence de deux entiers* γ *et* δ *strictement positifs tels que* $\alpha^2 - a = 2\gamma^4$ *et* $\alpha^2 + a = 2\delta^4$.

11. Posons $a_1 = \gamma$, $b_1 = \delta$ *et* $c_1 = \alpha$. *Montrez que* (a_1, b_1, c_1) *est une solution très particulière de* (E') *et que* $c_1 < c$.

Nous avons donc décrit un procédé (de 6. à 11.) qui nous permet de construire à partir de (a, b, c) une solution très particulière (a_1, b_1, c_1) strictement plus petite. En appliquant ce même procédé à (a_1, b_1, c_1), nous obtenons une troisième solution (a_2, b_2, c_2) toute aussi particulière telle que $c_2 < c_1$ à laquelle nous pouvons appliquer le prodédé pour obtenir une quatrième solution très particulière, etc. Nous obtenons donc une suite infinie de solutions très particulières $((a_n, b_n, c_n))_{n \in \mathbf{N}^*}$ telle que, pour tout $n \in \mathbf{N}^*$, $0 < c_{n+1} < c_n < c$. Mais tous les c_n sont des entiers : il y a donc une contradiction... comme souhaité!

En conclusion, nous avons établi que l'équation (E') ne possède que des solutions triviales. Par suite, l'équation (E_4) ne possède que des solutions triviales.

Interlude. Vous connaissez, de longue date, les fractions rationnelles, c'est-à-dire les quotients d'entiers. Il y a une infinité de couples d'entiers qui donnent le même rationnel, par exemple $\frac{247}{741} = \frac{19}{57} = \frac{1}{3}$ et bien d'autres encore. Parmi toutes ces fractions, une est privilégiée : celle qu'on ne peut pas simplifier davantage (ici, $\frac{1}{3}$) appelée pour cela *fraction irréductible.* Comment reconnaître une fraction irréductible parmi les autres? Etant donné un rationnel, comment trouver son écriture comme fraction irréductible?

Regardons un exemple, $\frac{253}{55}$.

Première réponse : calculons le pgcd du numérateur 253 et du dénominateur 55. D'une manière ou d'une autre, nous trouvons 11. Ainsi $\frac{253}{55} = \frac{11 \cdot 23}{11 \cdot 5} = \frac{23}{5}$. La fraction $\frac{23}{5}$ est irréductible car il n'y a plus de diviseurs communs aux numérateur et dénominateur.

En général, une fraction est irréductible si son numérateur et son dénominateur sont premiers entre eux. Pour obtenir une fraction irréductible, il suffit de diviser numérateur et dénominateur par leur pgcd.

Deuxième réponse : $\frac{253}{55} = \frac{253}{55} = \frac{253}{55} = \frac{23}{5}$. Qu'en pensez-vous?

Voici deux exemples pour étayer votre réflexion :

1) $\frac{980}{392} = \frac{980}{392} = \frac{80}{32}$ et $\frac{890}{932} = \frac{890}{932} = \frac{80}{32}$;

2) $\frac{640}{641} = \frac{640}{641} = \frac{0}{1}$!!!....

Si la première réponse convient pour toutes les fractions, la seconde donne le bon résultat que pour certaines fractions appelées *fractions magiques*. En voici quelques unes supplémentaires :

$\frac{392}{49} = \frac{392}{49} = \frac{32}{4}$,

$\frac{640}{160} = \frac{640}{160} = \frac{4}{1} = 4$,

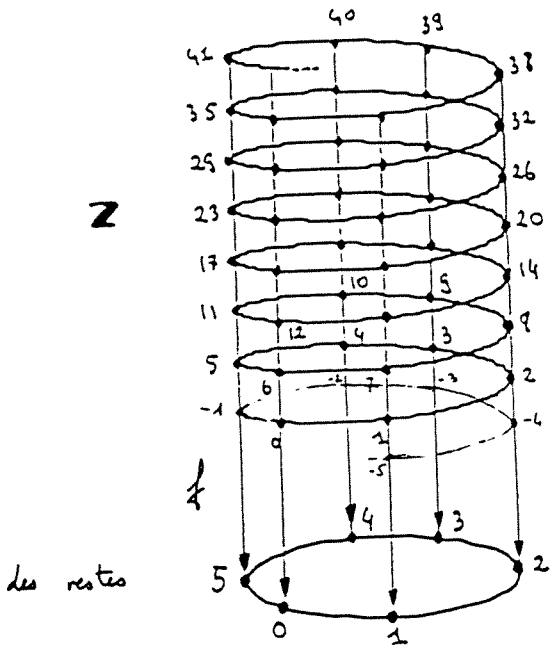
$\frac{99999}{51154948845} = \frac{99999}{51154948845} = \frac{99999}{51154948845} = \ldots = \frac{9999}{5115448845}$.

Des restes dans Z et des congruences.

Fixons un entier b strictement positif. Que pouvons-nous faire des restes de la division euclidienne par b?...

Dans l'esprit de ce chapitre, nous sommes tentés de les additionner ou les multiplier (finalement ce ne sont que des entiers!). Qu'obtenons-nous alors?... A priori, rien d'intéressant : tous les restes sont compris entre 0 et $b-1$ or, à les multiplier ou les additionner, nous pouvons obtenir un entier très grand (plus grand que b) qui ne sera donc pas un reste.

Dans les pages d'un autre chapitre, vous avez rencontré une application qui à chaque entier, associe son reste dans la division par b, et un beau dessin : (Prenons par exemple $b = 6$ et notons ici f l'application notée f_3 là-bas.)



Pourquoi ne pas utiliser f pour "ramener" nos résultats entre 0 et $b-1$? Ainsi, si r_1 et r_2 sont deux restes par la division par 6, on définit la somme et la multiplication de r_1 et r_2 par : $r_1 +_6 r_2 = f(r_1 + r_2)$ et $r_1 \cdot_6 r_2 = f(r_1 \cdot r_2)$, ce qui en clair donne :

$r_1 +_6 r_2$ = le reste dans la division par 6 de $r_1 + r_2$ et

$r_1 \cdot_6 r_2$ = le reste dans la division par 6 de $r_1 \cdot r_2$

(nous avons distingué les opérations dans l'ensemble des restes, $+_6$ et $\cdot_6$, de celles dans Z).

A l'aide de la spirale, dressez les tables d'addition et de multiplication dans l'ensemble des restes de la division euclidienne par 6.

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

×	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Remarques :

1) Nous constatons la présence de 0 dans la deuxième table hors de la première ligne et de la première colonne. Par exemple, nous obtenons que $2 \times 3 = 0$! Ceci a pour conséquence par exemple que l'équation $2x = 0$ a pour solution $x = 0$ et $x = 3$. Voilà une situation à laquelle nous ne sommes guère habitués!

Autre conséquence : il n'existe pas d'éléments x dans cet ensemble de restes tels que $2 \times x = 1$ (voir la table). Ainsi, l'équation $2x = 4$ n'entraîne pas $x = 2$ (voir la table encore), ce qui signifie qu'il existe un élément x tel que $2x = 2 \cdot 2$ et $x \neq 2$.

2) Nous pouvons faire la même chose en prenant n'importe quelle autre valeur de b... par exemple avec $b = 3$ ou $b = 8$.

UNE AUTRE VISION DE L'ENSEMBLE DES RESTES.

Nous allons cette fois-ci utiliser la totalité de la spirale, et même la prolonger indéfiniment vers les entiers négatifs. Ceci revient à considérer l'application g définie pour tout entier relatif par : si $n \in \mathbf{Z}$, $g(n) =$ le reste de la division par b de n. Une façon de "mimer" cette application est de comprimer la spirale-ressort sur le disque... Voilà une pratique mathématique déjà rencontrée ("empilement de droites"). Décrivons-la en termes mathématiques.

- Un seul ingrédient : une relation ayant les bonnes propriétés (Il faut remonter loin... dans la première partie juste au-dessus de la parenthèse). *Laquelle?*[18] (reprenons $b = 6$)
- Mettre tous les entiers en relation dans un même paquet. *Combien y a-t-il de paquets?*
- Les étiqueter pour s'y retrouver. Par exemple, nous désignerons par $\overline{a}$ le paquet contenant a. (Ainsi, $\overline{a} = \overline{c}$ si et seulement si a et c ont le même reste par la division euclidienne par b, ou si et seulement si b divise $a - c$.)

On note $\mathbf{Z}/b\mathbf{Z}$ l'ensemble des paquets[19].

Pouvons-nous additionner ou multiplier des paquets?

Prenons a et a' deux entiers (dans $\mathbf{Z}$). Notons r le reste a dans la division euclidienne par b et r' celui de a'. Nous pouvons donc écrire :

[18] En cas de besoin, cherchez une bouée quelque part dans la suite du texte.

[19] Une remarque sur la notation. Tout d'abord, $b\mathbf{Z}$ désigne l'ensemble des entiers de la forme ba où a parcourt $\mathbf{Z}$, c'est-à-dire de tous les multiples de b. La relation précédente revient à négliger tous les multiples de b puisque nous ne faisons plus la différence entre les entiers d'un même paquet. D'où la notation sous forme de quotient et l'appellation de l'ensemble des paquets par *ensemble quotient.*

$a = bq + r$ et $a' = bq' + r'$ où q et q' désignent les quotients des divisions. Alors $a + a' = (bq + r) + (bq' + r') = b(q + q') + (r + r')$.

Ainsi, le reste dans la division euclidienne par b de $a + a'$ et de $r + r'$ sont égaux donc $a + a'$ et $r + r'$ sont dans un même paquet. Par conséquent, nous pouvons additionner deux paquets en extrayant un élément de chacun d'eux (on monte dans la spirale), en additionnant ces derniers (dans $\mathbb{Z}$), et en prenant le paquet contenant le résultat (on redescend).

Pour la multiplication, nous procédons de façon analogue en remarquant que $aa' = (bq + r)(bq' + r') = b(bqq' + qr' + rq') + rr'$.

ETUDE D'UN EXEMPLE [20] : $\mathbb{Z}/3\mathbb{Z}$.

On construit $\mathbb{Z}/3\mathbb{Z}$ comme précédemment (cas où $b = 3$). On note $\overline{0}$, $\overline{1}$ et $\overline{2}$ les trois éléments de $\mathbb{Z}/3\mathbb{Z}$ contenant respectivement 0,1,2.

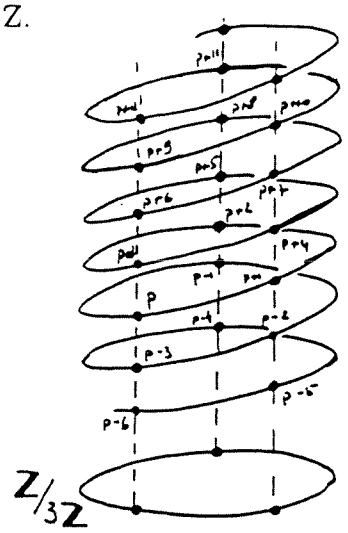
1) *Ecrivez les tables d'addition et de multiplication dans* $\mathbb{Z}/3\mathbb{Z}$.

2) Nous avons parlé de l'intérêt sucité par les nombres premiers jumeaux, c'est-à-dire les couples de nombres premiers de la forme $(p, p + 2)$. Nous pouvons nous poser la question analogue pour des triplets $(p, p + 2, p + 4)$ de nombres premiers, comme (3,5,7).

Combien de nombres premiers trouve-t-on dans le paquet $\overline{0}$*?*

Prenons un nombre premier p *différent de 3. En utilisant la table d'addition dans* $\mathbb{Z}/3\mathbb{Z}$*, montrez que* $p + 2$ *ou* $p + 4$ *est dans le paquet* $\overline{0}$*. Le triplet* $(p, p + 2, p + 4)$ *est-il formé de trois nombres premiers?*

Déduisez-en la liste des triplets $(p, p + 2, p + 4)$ *de nombres premiers.*



3) Donnons suite à la dernière remarque. Dans ce cas, les zéros dans la table de multiplication sont bien rangés dans les premières colonne et ligne. Ainsi, si $\overline{a} \neq \overline{0}$, $\overline{a}x = \overline{0}$ entraîne $x = \overline{0}$. Nous trouvons également un $\overline{1}$ dans chaque colonne (ou ligne) : l'équation $\overline{a}x = \overline{1}$ a toujours exactement une solution. Voilà qui devient beaucoup plus banal que le cas $b = 6$!... Cela est même tout à fait banal car vous pouvez retrouver toutes les propriétés énoncées pour $\mathbb{Q}$ (Si nécessaire, recherchez-les dans le paragraphe sur les nombres rationnels de la première partie). Ainsi, $\mathbb{Z}/3\mathbb{Z}$ est un *corps à trois éléments.*

4) Quelques particularités de ce tout petit corps. Remarquez d'abord que $\overline{1} + \overline{1} + \overline{1} = \overline{0}$, ce qui s'écrit $3 \cdot \overline{1} = \overline{0}$. Ensuite, calculez $\overline{1}^2$, $\overline{2}^2$, $\overline{1}^3$, $\overline{2}^3$, $\overline{a}^n$ où $n \in \mathbb{N}$ (N'oubliez pas que n est pair ou impair.) ...

5) Ce que nous pouvons faire à l'aide de ce tout petit corps : *soit à résoudre dans* $\mathbb{Q}^2$ *l'équation* (E') : $x^4 + y^4 + x^2y^2 + xy^3 = 0$. Le couple $(0, 0)$ est bien évidemment solution. En existe-t-il d'autres?

1. *Montrez que s'il existe une solution dans* $\mathbb{Q}^2$*, il y en a une dans* $\mathbb{Z}^2$.

[20] Pour certains passages difficiles, des bouées sont à disposition à la fin du chapitre.

2. *Soit (a, b) une solution dans* $\mathbf{Z}$: $a^4 + b^4 + a^2b^2 + ab^3 = 0$. *Alors* $a^4 + b^4 + a^2b^2 + ab^3$ *et* 0 *ont le même reste dans la division par* 3, *autrement dit* $\overline{a^4 + b^4 + a^2b^2 + ab^3} = \overline{0}$ *dans* $\mathbf{Z}/3\mathbf{Z}$. *Nous sommes donc ramenés à calculer dans* $\mathbf{Z}/3\mathbf{Z}$.

En utilisant la définition des opérations, montrez que $\overline{a}^4 + \overline{b}^4 + \overline{a}^2\overline{b}^2 + \overline{a}\overline{b}^3 = \overline{0}$, *puis que* $(\overline{0}, \overline{0})$ *est l'unique solution (remarquez qu'il n'y a qu'un nombre fini de valeurs pour* $\overline{a}$ *et* $\overline{b}$*).* Mais, ce n'est pas fini!

3. Maintenant, il nous faut revenir à $\mathbf{Z}$ (remonter dans la spirale). Nous déduisons de ce qui précède que a et b sont multiples de 3. Soit! Divisons-les tous les deux par 3. Nous obtenons a_1 et b_1, encore solution de (E') donc divisibles par 3. Ceci nous donne a_2 et b_2, encore solution de (E') donc divisibles par 3... et ainsi de suite autant de fois que nous voulons. Mais, le seul entier qui puisse être divisé par une puissance quelconque de 3 est 0. Ainsi $a = 0$ et $b = 0$.

En conclusion $(0, 0)$ est l'unique solution rationnelle de (E').

QUELQUES NOTATIONS ET APPELATIONS CONSACRÉES.

La relation précédemment utilisée joue un rôle très importante en arithmétique et a donc le privilège d'avoir un nom "universel".

Deux entiers a et a' ayant le même reste dans la division par b sont dits *congrus modulo* b. On le note $a \equiv a' \ [b]$.

Ainsi $1 \equiv 4 \equiv 7 \equiv -2 \equiv -5$ [3] et $1 \equiv 5 \equiv 9 \equiv -3$ [4].

Comme suggéré ci-dessus, nous pouvons faire varier les a et a' ou le b suivant le problème posé. A b fixé, on parle de *congruences modulo* b. Quand b n'est pas fixé, on parle de *congruences* (dans $\mathbf{Z}$).

Les classes de congruences modulo b ne sont autres que les éléments de $\mathbf{Z}/b\mathbf{Z}$. Nous pouvons donc traduire en termes de congruences les résultats obtenus dans $\mathbf{Z}/b\mathbf{Z}$. Voici un petit dictionnaire :

dans $\mathbf{Z}$	dans $\mathbf{Z}/b\mathbf{Z}$
$a \equiv a' \ [b]$	$\overline{a} = \overline{a'}$
Si $a \equiv a' \ [b]$ et $c \equiv c' \ [b]$, alors $a + c \equiv a' + c' \ [b]$ et $a \cdot c \equiv a' \cdot c' \ [b]$	Si $\overline{a} = \overline{a'}$ et $\overline{c} = \overline{c'}$, alors $\overline{a} + \overline{c} = \overline{a'} + \overline{c'}$ et $\overline{a} \cdot \overline{c} = \overline{a'} \cdot \overline{c'}$

Petits exercices sur les congruences et leurs opérations.

1) Montrez que le reste dans la division euclidienne par 3 d'un entier est égal à celui de la somme de ses chiffres. (Remarquez que $10 \equiv 1$ [3] et que $15 = 1 \times 10 + 5$ tout comme $489 = 4 \times 10^2 + 9 \times 10 + 8$, etc...) *Déduisez-en un critère de divisibilité par 3.*

2) Trouvez un critère de divisibilité par 9.

3) Soit n un entier positif. Que vaut 10^n modulo 11? Déduisez-en un critère de divisibilité par 11.

4) Montrez que pour tout entier $n \in \mathbf{N}$, $3^{2n} - 2^n$ est divisible par 7.

5) Rappelons qu'un nombre premier est congru à 1 ou -1 modulo 6. Existe-t-il une infinité de nombres premiers congrus à -1 modulo 6? *Si vous supposez qu'il n'en existe qu'un nombre fini, notez-les* $p_1, p_2, \ldots, p_r$ *et considérez l'entier* $n = 6\prod_{i=1}^{r} p_i - 1$. *Que vaut* n *modulo 6? n est-il premier? Que dire de ses facteurs premiers (modulo 6)? N'y a-t-il pas une contradiction?*

(solution 6)

LE PETIT THÉORÈME DE FERMAT.[21]

Enoncé : Soit p un nombre premier et n un entier. On suppose que p ne divise pas n (c'est-à-dire que $n \not\equiv 0\ [p]$ ou $\overline{n} \neq \overline{0}$ dans $\mathbf{Z}/p\mathbf{Z}$). Alors $n^{p-1} \equiv 1\ [p]$ (ou $\overline{n}^{p-1} = \overline{1}$ dans $\mathbf{Z}/p\mathbf{Z}$) .

Vous pouvez vérifier ceci pour $p = 3$ à l'aide de la table. Vous pouvez également essayer de remplacer p par un entier non premier (6 par exemple) : que constatez-vous alors?

Une démonstration de ce théorème.

1) En utilisant le théorème de Gauss, montrez que n, $2n$, $3n$, ...,$(p-1)n$ *ne sont pas congrus à 0 modulo p (autrement dit ne sont pas divisibles par p).* Il faudra établir que tout entier m plus petit strictement que p est premier à p.

2) En utilisant (1), montrez que n, $2n$, $3n$, ...,$(p-1)n$ *ne sont pas deux à deux congrus modulo p (autrement dit que la différence de deux d'entre eux n'est pas divisible par p).*

Passons du côté de $\mathbf{Z}/p\mathbf{Z}$. D'une part, $\overline{n}$, $\overline{2n}$, $\overline{3n}$, ...,$\overline{(p-1)n}$ sont différents de 0 (1) et deux à deux distincts (2). D'autre part, $\mathbf{Z}/p\mathbf{Z}$ a p éléments, à savoir $\overline{0}$, $\overline{1}$, $\overline{2}$,...,$\overline{p-1}$, dont $p-1$ distincts de $\overline{0}$. Par suite, nous avons écrit tous éléments de $\mathbf{Z}/p\mathbf{Z}$ autres que $\overline{0}$ de deux façons différentes. Nous avons donc deux manières d'écrire le produit de tous les éléments de $\mathbf{Z}/p\mathbf{Z}$ autres que $\overline{0}$, sans changer le résultat bien sûr. Nous obtenons ainsi :

$$\overline{n} \cdot \overline{2n} \cdot \overline{3n} \cdot \ldots \cdot \overline{(p-1)n} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1}.$$

3) En partant de l'égalité précédente et en utilisant les propriétés de la multiplication, montrez que $\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1} \cdot \overline{n}^{p-1} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1}$.

Notons déjà que si $p = 2$, le terme de gauche se réduit à $\overline{n}^{p-1}$ tandis que celui de droite vaut $\overline{1}$. C'est le résultat voulu. Dans ce cas, la vérification directe est suffisante...

Prenons maintenant un nombre premier p différent de 2. Pour conclure, il convient de simplifier par $\overline{1}$ puis $\overline{2}$ puis ... puis $\overline{p-1}$. Pour $\overline{1}$, c'est immédiat. Passons à $\overline{2}$.

4) Vérifiez que $\frac{p-1}{2}$ *est entier et que* $2 \cdot \frac{p-1}{2} \equiv 1[p]$. *Déduisez-en que* $\overline{3} \cdot \ldots \cdot \overline{p-1} \cdot \overline{n}^{p-1} = \overline{3} \cdot \ldots \cdot \overline{p-1}$.

Pouvons-nous faire de même avec 3, 4, etc... ? Malheureusement, cela devient beaucoup plus difficile de trouver (explicitement) un entier u qui satisfasse $3 \cdot u \equiv 1\ [p]$ ou $4 \cdot u \equiv 1\ [p]$ ou $5 \cdot u \equiv 1\ [p]$ ou etc... Simplifions donc le problème.

Remarquons que nous pouvons nous passer de la valeur exacte de u, qu'il nous suffit d'en connaître l'existence. Fixons $m = 3, 4, \ldots$ ou $p-1$ et écrivons ce que u doit satisfaire :

[21] *petit* par opposition au *grand théorème de Fermat* (cf. la première page de cette partie) mais pas par son importance. Pour un aperçu de ses applications, tournez la page.

$m \cdot u \equiv 1\ [p] \Leftrightarrow$ il existe $v \in \mathbf{Z}$ tel que $mu = 1 + pv$ (dans $\mathbf{Z}$) ou encore $mu - pv = 1$ $(*)$. Nous sommes donc amenés à montrer l'existence de deux entiers u et v tels que $nu - pv = 1$.

5) Que vous rappelle ce problème?...une certaine identité célèbre...dans le chapitre sur la division euclidienne.

Déduisez-en, grâce à la célèbre identité, l'existence de u et v vérifiant $(*)$.

6) La conclusion est laissée à l'initiative du (de la) lecteur(trice). ◇

En fait, la démonstration est entièrement rédigée à la note 4. Vous y trouverez des éléments de réponses.

QUELQUES APPLICATIONS DU PETIT THÉORÈME DE FERMAT. (solution 7)

Tout d'abord **les ludiques** :

1) Déterminez le reste dans la division euclidienne par 17 de 14^{256}.

2) Déterminez le reste dans la division euclidienne par 7 de $1798^{1998} + 1998^{1798}$.

3) Soit n un entier. Quelles sont les valeurs possibles de $\overline{n}^5$ dans $\mathbf{Z}/11\mathbf{Z}$? Vous chercherez au préalable les éléments de $\mathbf{Z}/11\mathbf{Z}$ dont le carré vaut $\overline{1}$.

Puis une plus sérieuse : le petit théorème de Fermat comme **test de non-primalité**. En effet, nous pouvons formuler l'énoncé de ce thèorème de la manière suivante :

S'il existe un entier n non divisible par p tel que $n^{p-1} \not\equiv 1[p]$ alors p n'est pas premier.[22]

On vérifie facilement que 6 n'est pas premier : $2^5 \equiv 2^3 \cdot 2^2 \equiv 2 \cdot 4 \equiv 2 \not\equiv 1[6]$.

1) Les entiers 21 et 10 ne sont pas premiers. Trouvez un entier n pour appliquer le critère précédent.

2) Montrez que 1073 n'est pas premier (par exemple, considérez n=3).

3) 1037 est-il premier? (solution 8)

Vous constatez certainement que ne rien savoir de l'entier n n'est pas agréable... Cela devient même très désagréable quand on sait que n peut ne pas exister bien que p ne soit pas premier [23] (que de calculs inutiles!) C'est par exemple le cas quand $p = 561 = 3 \times 11 \times 17$ ou $p = 1729 = 7 \times 13 \times 19$.

Et pour finir, une très sérieuse... qui peut redevenir ludique : **codage et décodage de messages.**

Pour coder un message, il convient de transformer chaque lettre en un autre symbole[24]. Par exemple, nous pouvons simplement remplacer chaque lettre par son rang dans l'alphabet et attribuer 27 à l'espace entre les mots. Ainsi, *théorème de fermat* devient *20 8 5 15 18 5 13 5 27 4 5 27 6 5 18 13 1 20.*

Pour décoder, il suffit d'appliquer la même règle en sens inverse. C'est très simple... beaucoup trop simple pour être efficace : un bon code doit être indéchiffrable sauf par son destinataire.

---

[22] Nous laissons le (la) lecteur(trice) s'assurer de l'exactitude de cet énoncé.

[23] Autrement dit, notre énoncé a le défaut d'être à sens unique : il existe un entier n tel que $n^{p-1} \not\equiv 1[p]$ $\Rightarrow$ p n'est pas premier (sens autorisé); p n'est pas premier $\not\Rightarrow$ il existe un entier n tel que $n^{p-1} \not\equiv 1[p]$ (sens interdit).

[24] En réalité, pour plus de fiabilité, on transforme un groupe de lettres en un symbole. La version proposée ici est très, très simplifiée.

Avec vos yeux de mathématiciens, vous avez reconnu que "coder" correspond à une bijection qui dans notre exemple, est définie de l'ensemble $\mathcal{L} = \{a, b, c, ..., z, \ \}$ dans l'ensemble $\mathcal{N} = \{1, 2, ..., 27\}$. Notons-la f. "Décoder" consiste alors à utiliser l'application réciproque. Pour rendre plus efficace notre codage, il suffit donc de compliquer la règle de codage, c'est-à-dire f. Et pour ce faire, nous utiliserons les congruences.

Un exemple : Choisissons un entier $n = 33$. Regarder les entiers de $\mathcal{N}$ modulo 33 ne les changent pas puisque 33 est strictement plus grand que chacun d'entre eux. Désormais, nous travaillerons modulo 33. Elevons chacun des nombres à la puissance 7 (et réduisons-les modulo 33). L'exemple précédent devient : 5 31 14 27 6 14 7 14 3 16 14 3 30 14 6 7 1 5. (N'oubliez pas dans la suite que ces entiers sont écrits modulo 33)

Voilà qui mélange bien les nombres. Mais comment décoder?...

A la recherche de la "clé" de décodage...

Prenons deux entiers premiers p et q, par exemple $p = 3$ et $q = 11$. D'après le petit théorème de Fermat, si un entier a est premier à p alors $a^{p-1} \equiv 1[p]$. Nous supposons a premier à p et q.

1. Calculez $(u-1)(u^{n-1}+u^{n-2}+...+u+1)$ *où* $u \in \mathbf{R}$ *et* n *un entier naturel. Déduisez-en que* $(a^{p-1}-1)$ *divise* $(a^{(p-1)(q-1)}-1)$.

2. Montrez que $(a^{q-1}-1)$ *divise aussi* $(a^{(p-1)(q-1)}-1)$.

3. En vous aidant d'un résultat d'Euclide, montrez que pq *divise* $(a^{(p-1)(q-1)}-1)$. *Autrement dit,* $a^{(p-1)(q-1)} \equiv 1[pq]$.

4. Montrez que pour tout entier a *(non nécessairement premier à* p *et* q*) nous avons* $a^{(p-1)(q-1)+1} \equiv a[pq]$.

5. On rappelle que l'on a codé le message lettre par lettre en élevant son rang à la puissance 7 et en réduisant modulo 33. Quelle est la clé de décodage? (Au pire, vous la découvrirez avec la bouée 4.)

Notes, bouées et solutions.

Commençons par les notes.

Note 1.

Il a été vu que les deux solutions d'une équation de degré 2 à coefficients réels sont réelles ou complexes conjuguées. Ainsi, $z' = \overline{z}$. La forme factorisée dont il est question peut être (ce choix n'est pas le seul) : $(x - z)(x - \overline{z}) = 0$ (elle est bien de degré 2 et a les bonnes racines). Une fois développée, cette équation devient : $x^2 + (z + \overline{z})x + z\overline{z} = 0$. Le coefficient de x est le double de la partie réelle de z donc est réel; le coefficient constant est le carré du module de z donc est réel. Cette équation convient.

Note 2.

L'application de $\mathcal{S}_1$ dans $\mathcal{S}_2$ est : $\begin{cases} \mathcal{S}_1 & \to & \mathcal{S}_2 \\ (a,b,c) & \mapsto & (a+b, a+c, b+c) \end{cases}$. Baptisons-la ϕ. L'autre application de $\mathcal{S}_2$ dans $\mathcal{S}_1$ que nous noterons ψ, est : $\begin{cases} \mathcal{S}_2 & \to & \mathcal{S}_1 \\ (A^2,B^2,C^2) & \mapsto & (\frac{A^2+B^2-C^2}{2}, \frac{A^2-B^2+C^2}{2}, \frac{-A^2+B^2+C^2}{2}) \end{cases}$.

Les deux composées sont $\phi \circ \psi$ et $\psi \circ \phi$. La première est une application de $\mathcal{S}_2$ dans lui-même tandis que la seconde est une application de $\mathcal{S}_1$ dans lui-même. Elles ne sont donc pas égales!

Calculons $\phi \circ \psi$. Prenons (A^2, B^2, C^2) un élément de $\mathcal{S}_2$. Alors

$$\phi \circ \psi((A^2,B^2,C^2)) = \phi((\frac{A^2+B^2-C^2}{2}, \frac{A^2-B^2+C^2}{2}, \frac{-A^2+B^2+C^2}{2})) = (A^2,B^2,C^2).$$

Par suite, $\phi \circ \psi = \mathrm{id}_{\mathcal{S}_2}$.

Un calcul analogue montre que $\psi \circ \phi == \mathrm{id}_{\mathcal{S}_1}$.

On en déduit que ϕ et ψ sont des bijections, réciproques l'une de l'autre.

Note 3. Unicité de q et r.

Prenons (q,r) et (q',r') deux couples d'entiers vérifiant les conditions, c'est-à-dire $(*)$ $a = bq+r = bq'+r'$ avec $0 \leq r < b$ et $0 \leq r' < b$. On aura prouvé l'unicité de q et r si l'on montre que $q = q'$ et $r = r'$.

De $(*)$, on déduit que $b(q-q') = r'-r$ ou (pour ne pas s'embarrasser de signe : $|b(q-q')| = |r'-r|$ ou encore, puisque $b > 0$.) $b|q-q'| = |r'-r|$. Donc, b divise $|r-r'|$. Comme $|r-r'| < b$ (c'est la longueur d'un intervalle strictement contenu dans $[0,b]$), $|r-r'| = 0$; et par suite $|q-q'| = 0$. Ceci dit exactement que $r = r'$ et $q = q'$. $\Diamond$

Note 4. Démonstration du petit théorème de Fermat.

Soit k un entier compris entre 1 et $p-1$. Puisque k est strictement plus petit que p (et non nul), k n'est pas divisible par p. De plus, par hypothèse, p ne divise pas n. Grâce au théorème de Gauss (formulé sous une forme différente, laquelle?), on sait que p ne divise pas le produit kn.

Prenons deux entiers l et l', tous deux compris entre 1 et $p-1$. Alors $ln-l'n = (l-l')n$ et $0 \leq l-l' < p-1$. D'après ce qui précède, p ne divise pas $(l-l')n$, autrement dit $(l-l')n \not\equiv 0$ $[p]$ ou encore $ln \not\equiv l'n$ $[p]$.

En conséquence, les éléments $\overline{n}$, $\overline{2n}$, $\overline{3n}$,..., $\overline{(p-1)n}$ de $\mathbf{Z}/p\mathbf{Z}$ sont deux à deux distincts et représentent donc ses $(p-1)$ éléments non nuls. On a l'égalité :

$$\overline{n} \cdot \overline{2n} \cdot \overline{3n} \cdot \ldots \cdot \overline{(p-1)n} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1}.$$

Les facteurs des deux produits précédents sont les mêmes mais pas nécessairement "rangés" dans le même ordre, on utilise donc que la multiplication de $\mathbf{Z}/p\mathbf{Z}$ est commutative.

En utilisant la définition de la multiplication de $\mathbf{Z}/p\mathbf{Z}$, on récrit cette égalité sous la forme :

$$\overline{n} \cdot \overline{2} \cdot \overline{n} \cdot \overline{3} \cdot \overline{n} \cdot \ldots \cdot \overline{p-1} \cdot \overline{n} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1}.$$

et en ordonnant grâce à la commutativité de la multiplication de $\mathbf{Z}/p\mathbf{Z}$,

$$\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1} \cdot \overline{n}^{p-1} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1}.$$

Or, tout entier non nul strictement plus petit que p est premier à p (puisqu'il n'est pas divisible par p et que p est premier) donc d'après l'identité de Bézout, pour chaque entier k compris entre 1 et $p-1$, il existe deux entiers

u_k et v_k (Que les choses soient claires, les entiers u_k et v_k varient si l'on change de k!) tels que $ku_k + pv_k = 1$ donc en réduisant modulo p, pour chaque k compris entre 1 et $p-1$, il existe un entier u_k tel que $ku_k \equiv 1\ [p]$ i.e. $\overline{k} \cdot \overline{u}_k = \overline{1}$. En multipliant les deux membres de la dernière égalité successivement par $u_1, u_2, \ldots, u_{p-1}$, on obtient : $\overline{n}^{p-1} = \overline{1}$. ◇

Poursuivons par les bouées.

Bouée 1.

Supposons que A^2, B^2 et C^2 soient en progression arithmétique. La raison de cette progression est $B^2 - A^2$ et $C^2 - B^2$. On en déduit l'égalité : $2B^2 = A^2 + C^2$. Comparons-la avec l'identité donnée. Pour ce faire, écrivons $A = x - y$ et $C = x + y$ (ceci est toujours possible. Il suffit de prendre $x = \frac{A+C}{2}$ et $y = \frac{C-A}{2}$). Alors $2B^2 = A^2 + C^2 = 2(x^2 + y^2)$ d'où $B^2 = x^2 + y^2$. Nous avons donc obtenu un triplet de Pythagore (x, y, B).

Ainsi, au trois carrés A^2, B^2, C^2 en progression arithmétique, nous associons le triplet de Pythagore $(\frac{A+C}{2}, \frac{C-A}{2}, B)$.

Réciproquement, si (x, y, z) est un triplet de Pythagore, le calcul précédent nous suggère de prendre $B = z, A = x - y, C = x + y$. On vérifie que $(x-y)^2$, $z^2 = x^2 + y^2$, $(x+y)^2$ sont en progression arithmétique (de raison $2xy$). C'est une solution du problème-variation.

Notons $\mathcal{S}$ l'ensemble des triplets de Pythagore. On a deux applications :

$$\Phi : \begin{cases} \mathcal{S}_2 & \to & \mathcal{S} \\ (A^2, B^2, C^2) & \mapsto & (\frac{A+C}{2}, \frac{A-C}{2}, B) \end{cases} \quad \text{et} \quad \Psi : \begin{cases} \mathcal{S} & \to & \mathcal{S}_2 \\ (x, y, z) & \mapsto & (x - y, z, x + y) \end{cases}$$

et on vérifie que $\Phi \circ \Psi = \mathrm{id}_{\mathcal{S}}$ et $\Psi \circ \Phi = \mathrm{id}_{\mathcal{S}_2}$.

Résolution du problème de Diophante : En composant les bijections ψ et Ψ, on obtient toutes les solutions du problème de Diophante à partir des triplets de Pythagore. En effet, pour toute solution du problème de Diophante (a, b, c), il existe un triplet de Pythagore (x, y, z) tel que $\psi \circ \Psi((x, y, z)) = (a, b, c)$ (c'est la surjectivité de $\psi \circ \Psi$). En explicitant, les solutions du problème de Diophante sont de la forme : $(\frac{z-2y}{2}, \frac{2x-z}{2}, \frac{z+2y}{2})$ où (x, y, z) est un triplet de Pythagore.

Bouée 2.

Soit $n > 2$. Si n est divisible par un nombre premier impair p, écrivons $n = pm$. Comme (E_p) n'a que des solutions triviales (c'est l'hypothèse), (E_n) également (les détails du raisonnement se trouvent dans le texte).

Supposons que n ne soit divisible par aucun nombre premier impair. Dans ce cas, n est une puissance de 2 (2 est le seul facteur premier possible!). Ecrivons $n = 2^k$ où $k \geq 2$ est un entier (n est strictement plus grand que 2). Ecrivons $n = 4m$. Si (a, b, c) est une solution de (E_n) alors (a^m, b^m, c^m) est une solution de (E_4) donc est triviale par hypothèse. Par conséquent, (a, b, c) est triviale et toutes solutions de (E_n) sont triviales.

La réponse est donc : oui.

Bouées 3. Quelques mots sur $\mathbf{Z}/3\mathbf{Z}$.

1 et 2) C'est une bouée percée : tout se lit sur la spirale. La liste est réduite à : $(3, 5, 7)$.

4) On obtient (grâce à la table ou la spirale) que $\overline{1}^2 = \overline{2}^2 = \overline{1}$ et $\overline{1}^3 = \overline{1}$, $\overline{2}^3 = \overline{2}$.

Pour $\overline{a}^n$, on voit de suite que si $\overline{a} = \overline{0}$ alors $\overline{a}^n = \overline{0}$. Et de même, si $\overline{a} = \overline{1}$ alors $\overline{a}^n = \overline{1}$. Reste le cas où $\overline{a} = \overline{2}$. Si n est pair, c'est-à-dire $n = 2m$ alors $\overline{a}^n = \overline{a}^{2m} = (\overline{a}^2)^m = \overline{1}^m = \overline{1}$. Si n est impair, on procède de manière analogue (à moins d'utiliser le résultat précédent) et on obtient que $\overline{a}^n = \overline{a}$.

5) 1. Si (A, B) est une solution avec A et B rationnels, alors en multipliant A et B par le produit de leur dénominateur, on obtient un couple (a, b) d'entiers. Est-ce une solution?

2. Résolution dans $\mathbf{Z}/3\mathbf{Z}$: on s'arme de patience et on essaie toutes les possibilités. On peut présenter ceci sous forme de tableau : les valeurs de $\overline{a}$ sur le côté gauche, celles de $\overline{b}$ en haut, celles de $\overline{a}^4 + \overline{b}^4 + \overline{a}^2\overline{b}^2 + \overline{a}\overline{b}^3$ dans les cases.

$\bar{a}$ \ $\bar{b}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{1}$	$\bar{2}$	$\bar{1}$

On peut être plus rapide : si $\bar{a} = \bar{0}$ alors l'équation devient $\bar{b}^4 = \bar{0}$ soit $\bar{b} \cdot \bar{b}^3 = \bar{0}$ ou $\bar{b} = \bar{0}$ (d'après la table). Donc $(\bar{0}, \bar{0})$ est l'unique solution avec $\bar{a} = \bar{0}$.

Si $\bar{a} = \bar{1}$, l'équation devient $\bar{1}^4 + \bar{b}^1 + \bar{b}^2 + \bar{b}^3 = \bar{0}$ ce qui s'écrit $\bar{b}^2(\bar{1} + \bar{b} + \bar{b}^2) = \overline{-1} = \bar{2}$. D'après la table, les seuls produits égaux à $\bar{2}$ sont $\bar{1} \cdot \bar{2}$ et $\bar{2} \cdot \bar{1}$. Donc soit $\bar{b}^2 = \bar{1}$ et $\bar{1} + \bar{b} + \bar{b}^2 = \bar{2}$, soit $\bar{b}^2 = \bar{2}$ et $\bar{1} + \bar{b} + \bar{b}^2 = \bar{1}$. Or encore d'après la table (voir la diagonale), aucun carré ne vaut $\bar{2}$: cela exclut la deuxième possibilité. Quant à la première, elle donne $\bar{b}^2 = \bar{1}$ et $\bar{1} + \bar{b} + \bar{1} = \bar{2}$ c'est-à-dire $\bar{b} = \bar{0}$. Or $(\bar{1}; \bar{0})$ n'est pas solution. Il n'y a donc pas de solution avec $\bar{a} = \bar{1}$. L'étude du cas où $\bar{a} = \bar{2}$ est laissée au lecteur.

Bouée 4. La clé de décodage.

1) Le produit $(u-1)(u^{n-1} + u^{n-2} + \ldots + u + 1)$ n'est autre que $u^n - 1$. Prenons $u = a^{p-1}$ et $n = q - 1$. L'identité précédente s'écrit : $(a^{p-1} - 1)((a^{p-1})^{(q-1)-1} + (a^{p-1})^{(q-1)-2} + \ldots + (a^{p-1}) + 1) = (a^{p-1})^{(q-1)} - 1 = a^{(p-1)(q-1)} - 1$. Ceci prouve que $(a^{p-1} - 1)$ divise $a^{(p-1)(q-1)} - 1$.

2) En échangeant les rôles de p et q dans le calcul précédent, on montre de même que $(a^{p-1} - 1)$ divise $a^{(p-1)(q-1)} - 1$.

3) Le résultat d'Euclide qui peut être utile ici est le lemme d'Euclide (Si besoin est, recherchez-le dans la cascade de résultats, une dizaine de pages avant). Il réduit le problème à regarder si p et q divisent $a^{(p-1)(q-1)} - 1$ séparément. Mais alors, le petit théorème de Fermat dit que p divise $a^{p-1} - 1$ (a est premier à p) qui divise $a^{(p-1)(q-1)} - 1$ d'après 1). Donc, p divise $a^{(p-1)(q-1)} - 1$. De même, q divise $a^{(p-1)(q-1)} - 1$ (il suffit d'utiliser 2)). Comme p et q sont premiers entre eux, pq divise $a^{(p-1)(q-1)} - 1$ par le lemme d'Euclide.

4) Si a est premier à p et q, il suffit de multiplier les deux membres de la congruence de la question 3) par a (ce qui conserve la congruence) et on obtient le résultat voulu.

Le cas où a est divisible par pq est évident puisque les deux membres de la congruence sont alors nuls. Reste les cas où a est divisible par l'un mais pas par l'autre. Regardons le cas où $a = p$.

Il est clair que $a^{(p-1)(q-1)+1} - a$ est divisible par p et le même argument qu'en 2) (a est premier à q) montre qu'il est divisible par q. Donc par le lemme d'Euclide, il est divisible par pq.

Regardons maintenant le cas où $a = p^r a'$ avec a' premier à p. On a
$a^{(p-1)(q-1)+1} = p^{r((p-1)(q-1)+1)} a'^{(p-1)(q-1)+1} = (p^{(p-1)(q-1)+1})^r a'^{(p-1)(q-1)+1}$.
On applique alors les résultats précédents et on trouve $a^{(p-1)(q-1)+1} \equiv a\,[pq]$.

Nous avons donc examiné tous les cas où p divise a. Il reste à voir le cas où q divise a mais pas p. Il suffit de faire comme pour p.

5) D'après ce qui précède, $a \equiv a^{(p-1)(q-1)+1}\,[pq]$. En prenant $p = 3$ et $q = 11$ (puisque $n = 33$), on obtient : $a^{2 \cdot 10 + 1} \equiv a\,[33]$, c'est-à-dire $a^{7 \cdot 3} \equiv a\,[33]$ ou encore $(a^7)^3 \equiv a\,[33]$. Et voilà la clé ! Il nous arrive a^7 et en l'élevant au cube on retrouve a.

Et terminons par les solutions.

Solution 1.

Soit n un entier. Son successeur est $n + 1$. L'hypothèse se traduit par : $n + (n + 1) = 2n + 1$ est un carré, ce qui s'écrit aussi : il existe un entier a tel que $2n + 1 = a^2$.

Supposons ceci vérifié et étudions la différence des carrés $(n + 1)^2 - n^2$. En développant, on obtient : $(n + 1)^2 - n^2 = 2n + 1 = a^2$, ce qu'il fallait établir.

Sous la même hypothèse, on a $(n + 1)^2 = n^2 + a^2$. Les triplets $(a, n, n + 1)$ et $(n, a, n + 1)$ sont donc des triplets de Pythagore. Une façon de construire un triplet de Pythagore avec un x imposé est d'identifier x à a ou n dans les triplets précédents.

Si l'on se donne $n = x$, il faut calculer a à partir de n. Or on ne connaît que l'expression de a^2 en fonction de n : on ne peut pas toujours extraire une racine carrée dans Q. Il y a donc un problème.

Par contre, si l'on se donne $a = x$ (impair), le calcul de n est aisé : $n = \frac{a^2-1}{2}$ et on obtient pour tout x impair le triplet de Pythagore $(x, \frac{x^2-1}{2}, \frac{x^2+1}{2})$. Ainsi, pour $x = 3$, on obtient le célèbre $(3, 4, 5)$; pour $x = 5$, $(5, 12, 13)$; pour $x = 11$, $(11, 60, 61)$; pour $x = 101$, $(101, 5100, 5101)$.

Solution 2.

Comme indiqué, effectuons la division euclidienne de p par 6 : $p = 6q + r$ où $0 \leq r < 6$. Et toujours comme indiqué, étudions chaque cas.

Si $r = 0$, 6 divise p et p n'est pas premier. Donc le reste ne peut pas être 0.

Si $r = 1$, on a $p = 6q + 1$(c'est un des cas que nous voulons conserver... Passons!)

Si $r = 2$ alors $p = 6q + 2 = 2(3q + 1)$: p est divisible par 2. Mais p est premier et différent de 2 . Il y a donc une contradiction. Le reste ne peut pas être 2.

Si $r = 3$ alors $p = 3(2q + 1)$... Impossible! (c'est comme ci-dessus en changeant 2 en 3.)

Si $r = 4$ alors $p = 2(3q + 2)$... Impossible! (reprendre mot à mot le cas $r = 2$.)

Si $r = 5$... on passe (voir le cas $r = 1$.)

En résumé, si p est premier différent de 2 et 3, les seuls restes possibles dans la division euclidienne de p par 6 sont 1 et 5, c'est-à-dire $p = 6q + 1$ ou $p = 6q + 5 = 6(q + 1) - 1$.

Enoncé de la réciproque : tous les entiers de la forme $6n + 1$ ou $6n - 1$ sont premiers.

Qu'en dire? Autrement dit, est-elle vraie ou fausse? Elle est fausse. Pour s'en convaincre, calculez les nombres $6n + 1$ et $6n - 1$ jusqu'à des valeurs suffisamment grandes de n.

Solution 3. Calculs de pgcd.

1) On applique l'algorithme d'Euclide :

$$\begin{array}{rcrcrcr} 2574 & = & 309 & \cdot & 8 & + & 102 \\ 309 & = & 102 & \cdot & 3 & + & 3 \\ 102 & = & 3 & \cdot & 34. & & \end{array}$$

Le dernier reste non nul est donc 3. Le pgcd de 2574 et 309 est 3.

2) Comme ci-dessus. On obtient $\text{pgcd}(2835, 1960) = 35$. Pour la suite, écrivons les divisions euclidiennes successives :

$$\begin{array}{rcrcrcr} 2835 & = & 1960 & \cdot & 1 & + & 875 \\ 1960 & = & 875 & \cdot & 2 & + & 210 \\ 875 & = & 210 & \cdot & 4 & + & 35 \\ 210 & = & 35 & \cdot & 6. & & \end{array}$$

De la troisième, on déduit que (1) $35 = 875 - 210 \cdot 4$. La seconde donne 210 en fonction de 1960 et 875 : (2) $210 = 1960 - 875 \cdot 2$; tandis que la première exprime 875 grâce à 2835 et 1960 : (3) $875 = 2835 - 1960$. En mettant tout cela bout à bout, on obtient :

$$35 \overset{(1)}{=} 875 - 210 \cdot 4 \overset{(2)}{=} 875 - (1960 - 875 \cdot 2) = 875 \cdot 3 - 1960 \overset{(3)}{=} (2835 - 1960) \cdot 3 - 1960 = 3 \cdot 2835 - 4 \cdot 1960.$$

3) Il s'agit de montrer que le pgcd d de a et b est égal au nombre de points à coordonnées entières sur le segment I d'extrémités l'origine (exclue) et le point de coordonnées (a, b) (inclus).

Soit (x, y) un point de I, c'est-à-dire (1) $y = \frac{b}{a}x$ (Le point (x, y) est situé sur la droite contenant l'origine et (a, b).) et (2) $0 < x \leq a$ et $0 < y \leq b$ (en tenant compte des bornes). De plus x et y sont entiers.

Avec les notations du texte, le point de coordonnées (a', b') vérifie les conditions (1) et (2) ainsi que tous ceux dont les coordonnées sont de la forme (na', nb') où n est un entier compris entre 0 (exclu) et d (compris) (par (2)). On compte ainsi d points à coordonnées entières sur I.

Il reste à s'assurer que nous les avons bien tous compter. Pour cela, il nous faut un résultat de la page suivante... Poursuivez donc un peu votre lecture et reprenez après.

Soit (x, y) un point de I. La condition (1) s'écrit : $ya' = b'x$. Or a' et b' sont premiers entre eux. Donc par le théorème de Gauss, puisque a' divise $b'x$, a' divise x; et puisque b' divise ya', b' divise y. Ainsi, $x = qa'$ et $y = q'b'$ avec q et q' convenables. En revenant à (1), on voit que $q = q'$. Notons-les n pour la peine! Le couple (x, y) s'écrit donc (na', nb') et a donc été compté.

Nous pouvons maintenant affirmer qu'il y a exactement d points à coordonnées entières sur I.

4) On remarque que le pgcd δ de 78, 182 et 273 est un diviseur commun à 78 et 182. Il divise donc le pgcd d de 78 et 182. Calculons d comme ci-dessus : $d = 26$. Nous savons donc que δ divise 26 et 273, c'est-à-dire leur pgcd qui vaut 13. En fait $\delta = 13$ car tout diviseur de 273 et du pgcd de 78 et 182 est un diviseur de 78.182 et 273.

Imaginons une méthode graphique. Nous choisissons trois axes de coordonnées dans l'espace, nommons O l'origine, plaçons le point A de coordonnées de $(78, 182, 273)$ et traçons le segment $]O, A]$. Nous comptons alors les points de ce segment à coordonnées entières : leur nombre est le pgcd cherché...L'imagination de l'auteur ne permet pas d'avoir un résultat plus précis. Et la vôtre?

Solution 4. Equations diophantiennes.

1) Il est clair que (1,-2) est solution de l'équation (par exemple). Soit (x, y) une autre solution. On a $15 \cdot 1 - 6 \cdot 2 = 3 = 15x + 6y$ d'où $15(x - 1) + 6(y + 2) = 0$ ce qui s'écrit aussi $5(x - 1) = -2(y + 2)$. Par le théorème de Gauss, 5 divise $(y + 2)$ et 2 divise $(x - 1)$. Il existe donc k, k' entiers tels que $x = 2k + 1$, $y = 5k' - 2$ (divisibilité). En revenant à l'équation, on voit que $k = k'$. Ainsi, les solutions de l'équation sont : $x = 2k + 1$, $y = 5k - 2$, $k \in \mathbf{Z}$.

2) Cherchons une solution. Comme $5 - 4 = 1$, $5 \cdot 3 - 4 \cdot 3 = 3$. Le couple $(3, -3)$ est une solution.

Si (a, b) est une autre solution alors $(a - 3, b + 3)$ est solution de $5x + 4y = 0$. Résolvons cette équation. Elle s'écrit : $5x = -4y$. D'où, grâce au théorème de Gauss (et puisque 5 et 4 sont premiers entre eux), 5 divise y et 4 divise x : $x = 4x'$ et $y = 5y'$. Ce couple (x, y) n'est solution que si $x' = -y'$.

L'ensemble des solutions de $5x + 4y = 0$ est donc $\{(4k, -5k), k \in \mathbf{Z}\}$. Celui de $5x + 4y = 3$ est $\{(4k + 3, -5k - 3), k \in \mathbf{Z}\}$.

3) Notons d le pgcd de a et b. Considérons une solution (x_0, y_0) de l'équation. Comme d divise a et b, d divise $ax_0 + by_0$ qui n'est autre que c. Nous venons de montrer que si une équation de la forme $ax + by = c$ a des solutions dans $\mathbf{Z}$ alors $\text{pgcd}(a, b)$ divise c.

Regardons la réciproque. Supposons que $d = \text{pgcd}(a, b)$ divise c et écrivons $c = dc'$, $a = da'$, $b = db'$. L'équation $ax + by = c$ est équivalente à $a'x + b'y = c'$. Comme a' et b' sont premiers entre eux, l'identité de Bézout assure l'existence d'entiers u et v tels que $a'u + b'v = 1$. Alors $(c'u, c'v)$ est une solution de notre équation. Par suite, si $\text{pgcd}(a, b)$ divise c alors l'équation de la forme $ax + by = c$ a des solutions dans $\mathbf{Z}$. La réciproque est vraie.

En conséquence, nous sommes d'accord!

4) On a $78 = 13 \cdot 6$, $182 = 13 \cdot 14$ et $273 = 13 \cdot 21$. L'équation est équivalente à : $6x + 14y + 21z = 1$. Le triplet $(-1, -1, 1)$ est solution évidente.

Déterminons toutes les solutions. Si (x, y, z) est solution alors

$$(1) \quad 6(x + 1) + 14(y + 1) + 21(z - 1) = 0.$$

En écrivant (1) sous la forme $3[2(x + 1) + 7(z - 1)] = -14(y + 1)$ et en appliquant le théorème de Gauss, on voit que 3 divise $(y + 1)$ (car 3 est premier à 14) : il existe un entier l tel que $y = 3l - 1$.

Un raisonnement analogue avec 7 puis 2 au lieu de 3 montre qu'il existe deux entiers k et m tels que $x = 7k - 1$ et $z = 2m + 1$.

Les solutions de l'équation sont donc à chercher parmi les triplets $(7k - 1, 3l - 1, 2m + 1)$ où k, l, m sont des entiers. Prenons un tel triplet. Il est solution si et seulement si $k + l + m = 0$ (On l'a "rentré" dans l'équation (1) puis on a divisé le tout par 42).

En conclusion, les solutions sont : $(7k - 1, 3l - 1, 1 - 2(k + l))$ avec $k, l \in \mathbf{Z}$.

5) On écrit a et b comme produit de nombres premiers : $a = \prod_{i=1}^{n} p_i^{r_i}$ et $b = \prod_{j=1}^{m} q_j^{s_j}$ où $r_i, s_j \in \mathbf{N}^*$ et les p_i (resp. q_j) sont des nombres premiers distincts. Puisque a et b sont premiers entre eux, un nombre premier qui apparaît dans l'écriture de a n'apparaît pas dans celle de b et inversement : $p_i \neq q_j$ pour tous i, j.

L'écriture en produit de nombres premiers de ab est le produit de celles de a et de b : $ab = \prod_{i=1}^{n} p_i^{r_i} \prod_{j=1}^{m} q_j^{s_j}$ (tous les nombres premiers intervenant sont distincts).

Par hypothèse, ab est un carré donc tous les nombres premiers dans son écriture en facteurs premiers sont à une puissance paire : $r_i = 2r'_i$, $s_j = 2s'_j$, $r'_i, s'_j \in \mathbf{N}^*$. D'où $a = \prod_{i=1}^{n} p_i^{r_i} = \prod_{i=1}^{n} p_i^{2r'_i} = (\prod_{i=1}^{n} p_i^{r'_i})^2$ et $b = (\prod_{j=1}^{m} q_j^{s'_j})^2$: a et b sont des carrés.

Solution 5. Résolution de l'équation $x^4 + y^4 = z^4$.

Remarques simplificatrices : on remarque que si l'on change le signe d'une ou plusieurs composante d'une solution, on obtient une nouvelle solution (on n'a pas changé la valeur des "bicarrés" (terme contemporain de Fermat désignant les puissances quatrièmes)). On construit ainsi 7 solutions en plus. Mais surtout, cela nous permet de nous intéresser qu'aux solutions dont toutes les composantes sont positives.

De plus, si l'on multiplie chaque composante d'une solution par un rationnel α, on multiplie alors les deux membres de l'équation par α^4 et l'égalité est conservée : on obtient encore une solution. Par suite, si (x, y, z) est une solution rationnelle et si q est le produit des dénominateurs de x, y et z, (qx, qy, qz) est une solution (x', y', z') entière et $(x, y, z) = \frac{1}{q}(x', y', z')$.

Soit (x, y, z) une solution entière de (E_4). Si d est un diviseur de x, y, et z alors $x = dx'$, $y = dy'$ et $z = dz'$ avec x', y', z' des entiers et $x^4 + y^4 = z^4$ implique que $d^4(x'^4 + y'^4) = d^4 z'^4$ puis que $x'^4 + y'^4 = z'^4$. Ainsi, (x', y', z') est une solution de (E_4). En particulier, si d est le pgcd de x, y et z, x' et y' n'ont pas de diviseurs communs autre que 1 donc x' et y' sont premiers entre eux. De plus, si un entier premier p divise x' et z', il divise $z'^4 - x'^4 = y'^4$ donc il divise y' : ceci est exclu. Un raisonnement analogue montre que z' et y' sont premiers entre eux. Ainsi, x', y' et z' sont deux à deux premiers entre eux.

Nouvelle réduction du problème : il est immédiat que si (a, b, c) est une solution de (E_4), (a, b, c^2) est une solution de (E'). Si, de plus, (a, b, c) est entière (resp. à composantes positives, à composantes deux à deux premières entre elles, non triviale), la solution (a, b, c^2) de (E') est entière (resp. à composantes positives, à composantes deux à deux premières entre elles, non triviale). Par conséquent, si (a, b, c) est (très) particulière, (a, b, c^2) l'est tout autant.

Mise en œuvre du principe : Soit (a, b, c) une solution très particulière de (E'). Alors a et b sont premiers entre eux donc l'un des deux est impair. Si a et b sont impairs, écrivons-les sous la forme : $a = 2k + 1$ et $b = 2l + 1$. Nous avons : $a^4 + b^4 = 4(4k^4 + 8k^3 + 6k^2 + 2k + 4l^4 + 8l^3 + 6l^2 + 2l) + 2 = c^4$. Donc 2 divise c^4 mais pas 4 : impossible!!! Par suite, a et b ne sont pas tous les deux impairs. Nécessairement, l'un est pair, l'autre impair.

Supposons désormais a impair et b pair. Dire que (a, b, c) est solution de (E') équivaut à dire que $b^4 = (c - a^2)(c + a^2)$. Ainsi, 16 divise $(c - a^2)(c + a^2)$ (*).

Comme c et a sont impairs, $c - a^2$ et $c + a^2$ sont pairs : leur pgcd est divisible par 2. De plus, si p est un entier qui divise $c - a^2$ et $c + a^2$, p divise leur somme $2c$ et leur différence $2a^2$. Mais c et a (ou a^2) sont premiers entre eux ((a, b, c) est particulière) donc p divise 2, c'est-à-dire $p = 1$ ou 2. Par conséquent, le pgcd de $c - a^2$ et $c + a^2$ vaut 2 (**).

De (*) et (**), on déduit que l'un des facteur $c - a^2$ ou $c + a^2$ est divisible par 2, l'autre par 8.

Premier cas : 2 divise $c - a^2$ (mais non 4) et 8 divise $c + a^2$, c'est-à-dire $c - a^2 = 2u$ et $c + a^2 = 8v$ où $u, v \in \mathbf{N}^*$, u est impair (sinon 4 divise $c - a^2$), u et v sont premiers entre eux (par (**)). En écrivant $b = 2b'$, (*) devient : $b'^4 = uv$ et d'après l'exercice précédent, u et v sont des "bicarrés" : $u = \alpha^4$ et $v = \beta^4$. D'où $c - a^2 = 2\alpha^4$ et $c + a^2 = 8\beta^4$.

En soustrayant la première équation à la seconde, on obtient : $2a^2 = 2(-\alpha^4 + 4\beta^4)$ d'où $a^2 = -\alpha^4 + 4\beta^4$ ou $a^2 + \alpha^4 = 4\beta^4$. Or a et α sont impairs donc $a^2 + \alpha^4$ ne peut pas être divisible par 4 (si nécessaire, voir l'idée de la démonstration ci-dessus). Ce cas ne peut donc pas se produire. Nécessairement,

Deuxième cas : 8 divise $c - a^2$ et 2 divise $c + a^2$ (mais non 4), c'est-à-dire $c - a^2 = 8\beta^4$ et $c + a^2 = 2\alpha^4$ (***) où $\alpha, \beta \in \mathbf{N}^*$, α est impair, α et β sont premiers entre eux (par (**) et le raisonnement précédent). Alors

$$\begin{cases} c - a^2 = 8\beta^4 \\ c + a^2 = 2\alpha^4 \end{cases} \Leftrightarrow \begin{cases} 2c = 2(\alpha^4 + 4\beta^4) \\ c + a^2 = 2\alpha^4 \end{cases} \Leftrightarrow \begin{cases} c = \alpha^4 + 4\beta^4 \\ \alpha^4 + 4\beta^4 + a^2 = 2\alpha^4 \end{cases} \Leftrightarrow \begin{cases} c = \alpha^4 + 4\beta^4 \\ 4\beta^4 = (\alpha^2 - a)(a^2 + a) \end{cases}$$

Comme α et a sont impairs, $\alpha^2 - a$ et $\alpha^2 + a$ sont pairs : leur pgcd est divisible par 2. De plus il divise leur somme $2\alpha^2$ et leur différence $2a$. Or α et a sont premiers entre eux car leur pgcd divise c (par (***)) donc divise le pgcd de a et c qui vaut 1. Par conséquent, le pgcd de $\alpha^2 - a$ et $\alpha^2 + a$ divise 2 : c'est donc 2.

En raisonnant comme ci-dessus, on en déduit l'existence de deux entiers positifs γ et δ tels que $\alpha^2 - a = 2\gamma^4$ et $\alpha^2 + a = 2\delta^4$ (****). On remarque que

(i) si γ est nul, $\alpha^2 = a$ et (***) entraine que $c = \alpha^4 = a^2$ donc que $b = 0$. Or la solution (a, b, c) n'est pas triviale donc c'est impossible : γ est non nul. On montre de même que δ est strictement positif;

(ii) γ et δ sont premiers entre eux car le pgcd de $\alpha^2 - a$ et $\alpha^2 + a$ est 2.

En additionnant les deux équations de (****), on obtient : $\gamma^4 + \delta^4 = \alpha^2$ donc (γ, δ, α) est une solution de (E'). Par (***), $\alpha < c$; par (i) et (ii), c'est une solution très particulière.

Solution 6. Les congruences.

Les critères de divisibilité par 3, 9 ou 11 : Traduisons ce que nous voulons établir en termes de congruences. Pour cela, nous avons besoin du reste de n dans la division euclidienne par 3 et des chiffres de n. Notons donc r le reste, a_0 le chiffre des unités de n, a_1 celui des dizaines, a_2 celui des centaines, etc... (Ainsi si n a s chiffres, n s'écrit $a_{s-1}...a_1a_0$.) Notre problème revient alors à montrer que $r \equiv a_0 + a_1 + ... + a_{s-1}\,[3]$.

Mais, d'après la division euclienne, il existe un entier q tel que $n = 3q + r$ donc $r \equiv 3q + r \equiv n\,[3]$. Il suffit donc d'établir que $n \equiv a_0 + a_1 + ... + a_{s-1}\,[3]$.

Or on a l'égalité : $n = a_0 + a_1 \times 10 + a_2 \times 10^2 + ... + a_{s-1} \times 10^{s-1}$ d'où $n \equiv a_0 + a_1 \times 10 + a_2 \times 10^2 + ... + a_{s-1} \times 10^{s-1} \equiv a_0 + a_1 \times 1 + a_2 \times 1^2 + ... + a_{s-1} \times 1^{s-1}\,[3]$ (car $10 \equiv 1\,[3]$) ou plus simplement $n \equiv a_0 + a_1 + ... + a_{s-1}\,[3]$. C'est ce que nous voulions!

Pour obtenir le critère, il suffit de remarquer que "n est divisible par 3" signifie que son reste est congru à zéro modulo 3 donc aussi la somme de ses termes. Par conséquent :
Un entier est divisible par 3 si et seulement si la somme de ses termes l'est.

Comme 10 est aussi congru à 1 modulo 9, on obtient (par le même raisonnement) qu'un entier n est divisible par 9 si et seulement si la somme de ses chiffres l'est.

Par contre 10 est congru à -1 modulo 11 donc 10^2 est congru à $(-1)^2 = 1$ modulo 11 et 10^3 est congru à $(-1)^3 = -1$ modulo 11 etc... Par conséquent $n \equiv a_0 - a_1 + a_2 - ... + (-1)^s a_s\,[3]$. Le même raisonnement que précédemment fournit alors le critère suivant : *un entier est divisible par 11 si et seulement si la somme alternée de ses termes l'est.*

4) utilise la remarque suivante $3^2 = 9 \equiv 2\,[7]$. Ainsi $3^{2n} - 2^n \equiv 2^n - 2^n\,[3]$ mais $2^n - 2^n = 0$.

5) Regardons n modulo 6. Puisque $n = 6\prod_{i=1}^{r} p_i - 1$, $n \equiv -1\,[6]$. Comme $n \neq p_i$ pour tout $i \in \{1, 2, ..., r\}$, n ne peut être premier (à cause de notre hypothèse).

Prenons p un facteur premier de n. Il est différent de 2 car si 2 divise n, 2 divise $n - 6\prod_{i=1}^{r} p_i$ c'est-à-dire -1. Il est différent de 3 et de tous les p_i, $i \in \{1, 2, ..., r\}$ (Raisonnez comme pour 2) autrement dit de tous les entiers premiers congrus à -1 modulo 6 (notre hypothèse). Mais alors, p doit être congru à 1 modulo 6 (l'argument est en solution 2). Par conséquent, tous les facteurs premiers de n sont congru à 1 modulo 6... et n aussi! (comme produit d'entiers tous congrus à 1 modulo 6) Il y a donc une contradiction et notre hypothèse de départ est fausse.

Il existe donc une infinité de nombres premiers congrus à -1 modulo 6.

Solution 7.

1) L'entier 17 étant premier et ne divisant pas 14, nous pouvons utiliser le petit théorème de Fermat. Nous savons donc que : $14^{16} \equiv 1\,[17]$. Or $256 = 16^2$ donc $14^{256} \equiv 14^{16^2} \equiv (14^{16})^2 \equiv 1\,[17]$. Le reste de la division euclidienne de 14^{256} par 17 est donc 1.

2) On procède comme en 1). L'entier 7 est premier et premier à 1998 et 1798. Par le petit théorème de Fermat, on a : $1998^6 \equiv 1\,[7]$ et $1798^6 \equiv 1\,[7]$. Mais d'une part, $1998 \equiv 3\,[7]$ et $1798 \equiv -1\,[7]$; d'autre part $1998 \equiv 0\,[6]$ et $1798 \equiv 4\,[6]$. D'où $1798^{1998} + 1998^{1798} \equiv (-1)^0 + 3^4 \equiv 4\,[7]$. Le reste demandé est donc 4.

3) Encore une fois, on va appliquer le petit théorème de Fermat puisque 11 est premier. Mais n est quelconque et peut donc ne pas être premier à 11. Distingons donc deux cas :

- n n'est pas premier à 11, c'est-à-dire, puisque 11 est premier, n est divisible par 11. Alors toute puissance de n est divisible par 11, en particulier la cinquième. Ceci se traduit dans $\mathbb{Z}/11\mathbb{Z}$ par $\overline{n}^5 = \overline{0}$.

- n est premier à 11. Dans ce cas, on peut appliquer le petit théorème de Fermat : $\overline{n}^{10} = \overline{1}$. Or $\overline{n}^{10} = (\overline{n}^5)^2$. Ainsi, $\overline{n}^5$ est de carré 1. Déterminons donc les éléments de $\mathbb{Z}/11\mathbb{Z}$ de carré $\overline{1}$:

$\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{4}$, $\overline{3}^2 = \overline{9}$, $\overline{4}^2 = \overline{5}$, $\overline{5}^2 = \overline{3}$, $\overline{6}^2 = \overline{-5}^2 = \overline{3}$, $\overline{7}^2 = \overline{5}$, $\overline{8}^2 = \overline{9}$, $\overline{9}^2 = \overline{4}$, $\overline{10}^2 = \overline{1}$.

Les seuls éléments de carré 1 sont donc $\overline{1}$ et $\overline{-1}$.

Revenons à $\overline{n}$. Nous savons donc que $\overline{n}^5 = \pm 1$ dans $\mathbf{Z}/11\mathbf{Z}$. Il ne reste plus qu'à vérifier que 1 et -1 sont bien les puissances cinquièmes de certains $\overline{n}$ dans $\mathbf{Z}/11\mathbf{Z}$: $\overline{1}^5 = \overline{1}$ et $\overline{-1}^5 = \overline{-1}$.

En conclusion, les valeurs possibles de $\overline{n}^5$ sont : $\overline{0}$, $\overline{1}$,$\overline{-1}$.

Solution 8.

1) Dans le cas de 21, prenons le plus petit n, c'est-à-dire $n = 2$. Il n'est pas divisible par 21. Calculons 2^{20} modulo 21 : $2^2 \equiv 4$, $2^4 \equiv (2^2)^2 \equiv 16 \equiv -5$, $2^{16} \equiv ((2^4)^2)^2 \equiv 4^2 \equiv -5$ et $2^{20} \equiv 2^{16}2^4 \equiv (-5)(-5) \equiv 4 \not\equiv 1\,[21]$. L'entier 2 convient.

Pour 10, 2 convient aussi.

Dans les deux cas, l'entier n n'est pas unique. Vous pouvez donc en trouver d'autres qui conviendront aussi bien.

2) Il suffit de calculer $n^{1072}\,[1073]$... Allons-y! Remarquons que $1072 = 4 \cdot 67 = 4(2^6 + 3)$. Calculons : $3^4 = 81$, $3^8 = (3^4)^2 = 123$,...$3^{64} = -225$ d'où $3^{67} = 3^{64}3^3 = 363$ (Tous ces calculs sont faits dans $\mathbf{Z}/1073\mathbf{Z}$). Ainsi $3^{1072} = (3^{67})^4 = 107 \neq 1$ et 1073 n'est donc pas premier.

3) On procède comme ci-dessus... sauf que si l'on prend $n = 3$, $n^{1036} = 1$ mod 1037. Il faut donc en prendre un autre.

CONTRE-EXEMPLES EN ARITHMETIQUE

Pour chacune des affirmations suivantes, donnez une démonstration pour montrer qu'elle est vraie ou un contre-exemple pour montrer qu'elle est fausse.

1) Parmi trois nombres entiers consécutifs, deux au moins sont pairs.

2) Parmi trois nombres entiers consécutifs, deux au moins sont de même parité.

3) Le carré d' un nombre impair est impair.

4) La somme de deux nombres premiers est un nombre premier.

5) Le produit de deux nombres premiers est un nombre premier.

6) Si a, b et c sont trois entiers tels que $c=ab$ et si c est divisible par 24 alors a ou b est divisible par 24.

7) Un entier divisible par 3 et par 6 est divisible par 18.

8) Pour tout entier $n>0$, $6n+1$ et $6n-1$ sont premier.

9) Pour tout entier $n>0$, $6n+1$ ou $6n-1$ est premier.

10) Pour tout entier premier $p>3$, il existe un entier n tel que $p=6n+1$ ou $p=6n-1$.

11) Parmi 6 nombres entiers consécutifs, il y en a au moins un qui est premier avec tous les autres.

12) Parmi 7 nombres entiers consécutifs, il y en a au moins un qui est premier avec tous les autres.

13) Pour tout entier premier $p>3$, il existe un entier n tel que $p=30n+1$ ou $p=30n-1$ ou $p=30n+7$ ou $p=30n-7$ ou $p=30n+11$ ou $p=30n-11$ ou $p=30n+13$ ou $p=30n-13$.

14) Pour tout entier naturel n, $n^2 + n + 41$ est un nombre premier.

15) Pour tout entier naturel n, $n^2-79n+1601$ est un nombre premier.

16) 131 est le plus petit nombre premier à trois chiffres tel que toute permutation de ses chiffres donne aussi un nombre premier.

17) Tous les multiples à 5 chiffres de 41 donnent des multiples de 41 par permutation cyclique de leurs chiffres.

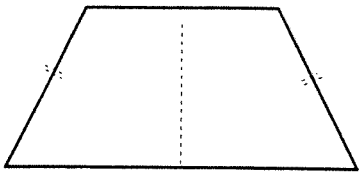
18) Le carré de tout nombre entier se terminant par 538 se termine par 444.

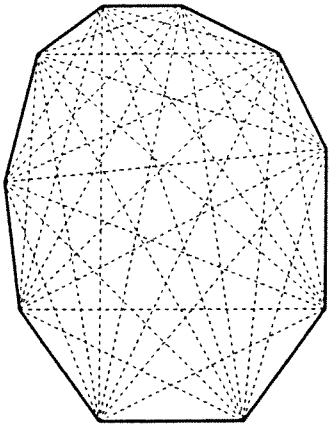
19) Tout nombre entier est somme d'au plus 4 carrés.

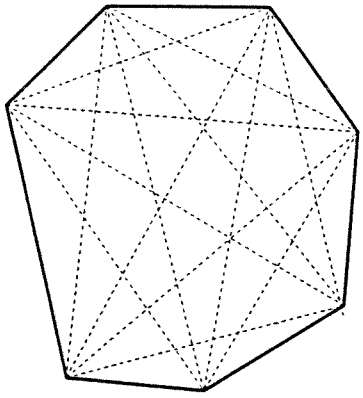
CONTRE-EXEMPLES EN VRAC

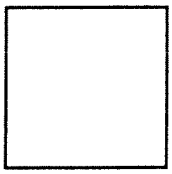
$g(x) = (x)^2$

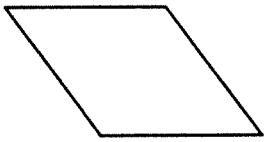
$\left(\frac{1}{2}\right)^2 < \frac{1}{2}$











$\frac{1}{0,25} > 0,25$

$f(x) = \tan(x) \qquad I = \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$

$f(x) = \sin(x) \quad [a,b] = [0,4\pi]$

$-\left(-\frac{1}{2}\right) > \frac{1}{4}$

$$f(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

$$P(x) = \frac{x(x+1)}{2} = \frac{1}{2}x^2 + \frac{1}{2}x$$

$$f(x) = \begin{cases} x \ si \quad x \in Z \\ x^2 \ si \quad x \notin Z \end{cases}$$

C'est Euler qui a proposé la formule $n^2 + n + 41$ qui donne 40 nombres premiers pour les valeurs de n allant de 0 à 39. Aucune formule du second degré $n^2 + an + b$ avec a et b positifs inférieurs à 10000 ne produit une suite plus longue de nombres premiers.

LES BONS MOTS[2]

On dispose d'un **alphabet** formé des 3 symboles M, I, U.

Les **mots** sont formés par juxtaposition de ces trois lettres (par exemple UMIUM, UUU,...)

Les **bons mots** sont obtenus en respectant les 5 règles suivantes :

Règle 0 : MI est un bon mot.

Les quatre autres règles permettent, en partant d'un bon mot, d'obtenir d'autres bons mots :

Règle 1 : En ajoutant U à la fin d'un bon mot se terminant par I, on obtient un bon mot

Nous abrégerons la règle 1 en écrivant :

R1 : xI → xIU

où x est un mot quelconque éventuellement vide.

Avec des notations analogues on définit les trois autres règles de production de bons mots :

Soit x et y des mots quelconques éventuellement vides.

R2 : xIIIy → xUy

R3 : Mx → Mxx

R4 : xUUy → xy

Questions :

a) Montrer que MIIU est un bon mot.
b) Montrer que le mot MIIII....III qui commence par « M » et se termine par 1024 « I » est un bon mot.
c) Déterminer les onze bons mots que l'on peut obtenir à partir de MI en appliquant successivement au maximum trois règles de production.
d) Montrer que tous les bons mots commencent par M.
e) Le mot vide est-il un bon mot ?
f) MU est-il un bon mot ?
Indication : examiner l'effet de chacune des règles de production sur le nombre de "I" du mot et en déduire qu'il n'y a pas de bons mots sans « I ».
g) Y a-t-il un nombre fini de bons mots ?

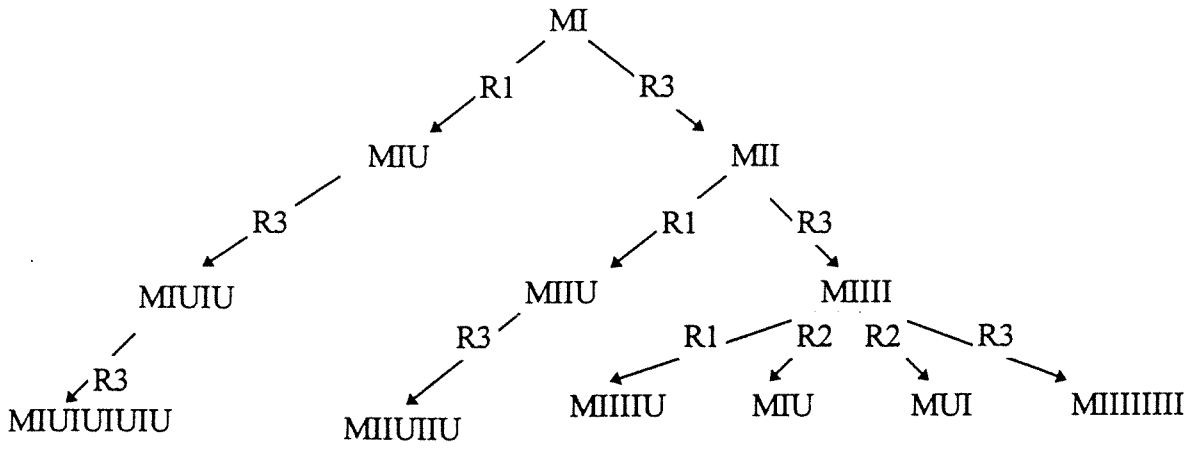
[2] D'après « L'énigme MU » dans Gödel, Escher, Bach par Douglas Hofstadter

LE DERNIER MOT A PROPOS DES BONS MOTS

a) MI $\xrightarrow{R3}$ MII $\xrightarrow{R1}$ MIIU

b) A partir de MI, chaque application de la règle R3 double le nombre de I qui terminent le mot. Comme $1024 = 2^{10}$, en appliquant 10 fois la règle R3 on obtiendra le bon mot demandé.

c) En appliquant, à partir de MI toutes les règles possibles on peut établir l'arbre ci-dessous dont les nœuds représentent les bons mots obtenus en enchaînant au plus trois règles successivement.



d) Le premier bon mot MI commence par M. Aucune des quarte règles de production ne modifie la première lettre d'un bon mot. Tous les bons mots commencent donc par M.

e) Le mot vide ne commence pas par M. Le résultat précédent permet donc de conclure que ce n'est pas un bon mot.

f) Si on note n(c) le nombre de I contenus dans un mot, on remarque que :
n(MU)=0
n(MI)=1
Les règles R1 et R4 laisse n(c) invariant.
La règle R2 diminue n(c) de 3.
La règle R3 multiplie n(c) par 2. (2*0=0 ; 2*1=2 ; 2*2=4)
En raisonnant modulo 3 on voit que toutes les règles transforment une chaîne pour laquelle n(c) est non nul (modulo 3) en une chaîne avec n(c) non nul (modulo 3). Ceci démontre qu'en partant de MI, on ne peut pas aboutir à MU.

g) L'application n fois répétée de la règle R3 en partant de MI permet d'engendrer des bons mots formés d'un « M » suivi de 2^n « I » qui sont en nombre infini.

DES CARRÉS MAGIQUES...

AUX ESPACES VECTORIELS.

1. Espaces vectoriels : exemples et définition

En mathématiques on a souvent des problèmes à résoudre ! Malheureusement, pour la plupart d'entre eux nous n'arrivons pas à décrire leur(s) solution(s) de manière simple. Mais lorsqu'on trouve un problème pour lequel c'est possible, il est naturel d'en chercher la structure essentielle qui fait que cette description simple existe. Ainsi, on saura que les solutions de tout autre problème possédant cette structure pourront être décrites de la même manière.

Dans cette section nous allons regarder quelques problèmes bien choisis et nous allons (à la main) les résoudre complètement, ce qui veut dire que nous allons trouver toutes leurs solutions. Nous verrons que dans chaque exemple, bien qu'il y ait une infinité de solutions, il sera possible de trouver un nombre fini de ces solutions tel que toute solution s'écrive de manière simple à partir de celles-ci. Cette observation motivera la définition de ce que l'on appelle un espace vectoriel.

Exemple 1

Un carré magique de taille 2×2 est un 'carré'

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

tel que la somme des nombres dans chaque ligne et la somme des nombres dans chaque colonne est la même : autrement dit, tel que

$$a + b = c + d = a + c = b + d. \tag{1.1}$$

Par exemple, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}$ sont des carrés magiques de somme 0 et 7 respectivement. Le problème que l'on se pose est de trouver tous les carrés magiques.

Normalement, pour résoudre ce problème il faut résoudre les équations (1.1) ci-dessus. Mais avant de faire cela, nous allons voir que, même sans connaître le moindre exemple explicite de carré magique, nous pouvons dire des choses intéressantes sur les propriétés des carrés magiques.

Supposons que l'on ait un carré magique $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Si on le multiplie par un nombre réel λ suivant la règle

$$\lambda . \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$$

on obtient de nouveau un carré magique car la somme des nombres dans une colonne (ou ligne) de $\begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$ est égale à λ fois la somme des nombres dans la colonne (ou ligne) correspondante de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Nous avons là une méthode pour 'fabriquer de nouveaux carrés magiques à partir d'anciens' : la multiplication par un nombre réel. Par exemple, $\begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}$ est un carré magique de somme 7 et si on le multiplie par 5 on obtient $\begin{pmatrix} 15 & 20 \\ 20 & 15 \end{pmatrix}$ qui est un carré magique de somme 35.

Il y a une deuxième méthode pour 'fabriquer de nouveaux carrés magiques à partir d'anciens'. Supposons cette fois-ci que l'on ait deux carrés magiques : $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Les additionner selon la règle suivante :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix},$$

donne aussi un nouveau carré magique. Vérifions que la somme des nombres dans la première colonne est égale à la somme des nombres dans la première ligne. La somme des nombres dans la première colonne est égale à $(a+a')+(c+c')=(a+c)+(a'+c')$, et cela vaut $(a+b)+(a'+b')$ (car $a+c=a+b$ et $a'+c'=a'+b'$), ce qui est égale à $(a+a')+(b+b')$ - la somme des nombres dans la première ligne.

Exercice : Vérifier que la somme des nombres de chaque colonne est égale à la somme des nombres de chaque ligne.

Nous avons donc trouvé une deuxième méthode pour 'fabriquer de nouveaux carrés magiques à partir d'anciens' : les additionner.

En combinant ces deux méthodes pour trouver des carrés magiques, on peut en trouver beaucoup. Car, si la somme de deux carrés magiques est un troisième carré magique, la somme du troisième avec le premier sera un quatrième , et la somme du quatrième avec le deuxième sera un cinquième, et puis ... on peut continuer ad infinitum. Muliplier chacun de ces carrés magiques par un nombre réel donne encore d'autres carrés magiques. Mais alors une question cruciale se pose : peut-on obtenir tous les carrés magiques de cette façon ? Plus précisément :

(QUESTION A) Peut-on trouver un ensemble fini de carrés magiques tel que tous les autres carrés magiques s'obtiennent à partir de ceux-là par nos deux méthodes : multiplication par un réel et addition ?

S'il s'avère que l'on peut trouver un tel ensemble, nous dirons que cet ensemble de carrés magiques *engendre* tous les carrés magiques. Comme il n'y a aucune raison de supposer que de tels ensembles sont uniques, il est naturel de se demander (pour des raisons d'économie) :

(QUESTION B) Quel est le plus petit nombre de carrés magiques qui engendrent tous les carrés magiques ?

Nous allons maintenant revenir à notre problème de départ, le résoudre et essayer de répondre à ces deux questions.

Pour cela considérons un carré magique $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ quelconque. De par la définition même des carrés magiques on a les équations (voir (1.1) ci-dessus) :

$$a+b=c+d=a+c=b+d.$$

On va essayer d'exprimer c et d en fonction de a et b. De $a+b=a+c$ on a $b=c$, et de $a+b=b+d$ on a $a=d$. En résumé, nous avons démontré que si $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est un carré magique de somme 0, alors $c=b$ et $d=a$. Autrement dit, notre carré magique est de la forme $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ et nous avons complètement résolu notre problème de départ : si a et b sont des réels quelconque, $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ est un carré magique et tous les carrés magiques sont de cette forme.

Revenons maintenant aux questions A et B ci-dessus. Comme on peut écrire le carré magique général $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ sous la forme

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} = a.\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b.\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

nous voyons que les carrés magiques $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ engendrent tous les carrés magiques, et la réponse à la question A est 'oui'. En ce qui concerne la question B – quel est le plus petit nombre de carrés magiques qui engendrent tous les carrés magiques ? – la réponse est 'deux' mais nous ne le démontrerons pas avant d'avoir un plus d'outils théoriques à notre disposition.

Remarque. — Comme

$$a.\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \frac{a}{2}.\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix} \qquad \text{et} \qquad b.\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \frac{b}{2}.\begin{pmatrix}0 & 2\\ 2 & 0\end{pmatrix},$$

on voit que les deux carrés magiques $\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$ et $\begin{pmatrix}0 & 2\\ 2 & 0\end{pmatrix}$ engendrent tous les autres.

Exemple 2

Dans l'exemple précédent on a trouvé tous les carrés magiques de taille 2×2, c'est-à-dire qui ont deux lignes et deux colonnes et dont la somme de chaque ligne est égale à la somme de chaque colonne. Qu'en est-il pour des carrés magiques de taille 3×3, c'est-à-dire qui ont trois lignes et trois colonnes ? Les trouver tous est certainement un problème bien plus compliqué et pour simplifier nous n'allons regarder que les carrés magiques de 'somme 0'. Le problème que l'on se pose est donc de trouver tous les carrés

$$\begin{pmatrix}a & b & c\\ d & e & f\\ g & h & j\end{pmatrix}$$

tels que la somme des nombres dans chaque ligne et la somme des nombres dans chaque colonne soit égale à 0. Mais quelles sont les ressemblances entre ce problème et le problème de l'exemple précédent ?

D'abord, si l'on a un carré magique

$$\begin{pmatrix}a & b & c\\ d & e & f\\ g & h & j\end{pmatrix},$$

le carré

$$\lambda.\begin{pmatrix}a & b & c\\ d & e & f\\ g & h & j\end{pmatrix} = \begin{pmatrix}\lambda a & \lambda b & \lambda c\\ \lambda d & \lambda e & \lambda f\\ \lambda g & \lambda h & \lambda j\end{pmatrix} \tag{1.2}$$

obtenu en le multipliant par un nombre réel λ reste un carré magique car la somme des nombres dans chaque ligne et chaque colonne est toujours égale à 0 (à vérifier en exercice). Ensuite, la somme de deux carrés magiques, définie par la formule

$$\begin{pmatrix}a & b & c\\ d & e & f\\ g & h & j\end{pmatrix} + \begin{pmatrix}a' & b' & c'\\ d' & e' & f'\\ g' & h' & j'\end{pmatrix} = \begin{pmatrix}a+a' & b+b' & c+c'\\ d+d' & e+e' & f+f'\\ g+g' & h+h' & j+j'\end{pmatrix}, \tag{1.3}$$

est un carré magique (à vérifier en exercice). Donc on peut dire que, comme dans l'exemple 1, on a toujours deux méthodes pour 'fabriquer de nouveaux carrés magiques à partir d'anciens' : la multiplication par un nombre réel et l'addition. Du coup, cela a un sens de se poser les questions A et B :

(QUESTION A) Peut-on trouver un ensemble fini de carrés magiques de taille 3×3 *tel que tous les autres carrés magiques s'obtiennent à partir de ceux-là par multiplication par un nombre réel et par addition ?*

(QUESTION B) Quel est le plus petit nombre de carrés magiques qui engendrent tous les carrés magiques ?

Nous allons maintenant revenir à notre problème de départ, le résoudre et répondre à ces deux questions (presque !)

Pour cela prenons un carré magique quelconque

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix}.$$

Comme la somme des nombres dans chaque ligne et chaque colonne est égale à 0, nous avons les équations :

$$\begin{aligned} a+b+c=0 \quad (1) \qquad & a+d+g=0 \quad (4) \\ d+e+f=0 \quad (2) \qquad & b+e+h=0 \quad (5) \\ g+h+j=0 \quad (3) \qquad & c+f+j=0 \quad (6). \end{aligned}$$

Essayons de résoudre ces équations en imitant la méthode de l'Exemple 1.

Rappelons que dans l'Exemple 1 on a montré que si on fixait deux des coefficients (c'étaient a et b) d'un carré magique

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

les autres coefficients c et d étaient entièrement déterminés en fonction de a et b.

Montrons que si on fixe les quatre coefficients a, b, d, e du carré magique

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix}$$

les autres coefficients (c'est-à-dire c, f, g, h et j) sont entièrement déterminés :
d'après l'équation (1) on a $c = -a - b$;
d'après l'équation (2) on a $f = -d - e$;
d'après l'équation (4) on a $g = -a - d$;
d'après l'équation (5) on a $h = -b - e$;
d'après l'équation (6) on a $j = -c - f = -(-a - b) - (-d - e) = a + b + d + e$.

Autrement dit, **tout** carré magique de taille 3 x 3 et de somme 0 est de la forme

$$\begin{pmatrix} a & b & -a-b \\ d & e & -d-e \\ -a-d & -b-e & a+b+d+e \end{pmatrix}, \tag{1.4}$$

où a, b, d et e peuvent être choisis arbitrairement. C'est la solution complète au problème que l'on s'est posé au départ.

Revenons maintenant aux questions A et B. Parmi les carrés magiques de taille 2 x 2 nous avons vu qu'il était possible d'en trouver deux tel que tous les autres en fussent une combinaison linéaire. Qu'en est-il pour les carrés magiques de taille 3 x 3 de somme 0 ? Remarquons que l'on peut écrire le carré magique général (2) sous la forme

$$a.\begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix} + b.\begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & -1 & 1 \end{pmatrix} + d.\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix} + e.\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix}. \tag{1.5}$$

Exercice : A l'aide de 1.2 et 1.3 vérifier que le carré magique de 1.4 est effectivement égale au carré magique de 1.5.

Cela montre que tout carré magique de somme 0 est une somme de multiples des 4 carrés magiques de somme 0 :

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix}.$$

On peut donc dire que ces 4 carrés magiques de somme 0 de taille 3×3 engendrent tous les autres et on a la réponse (positive) à la question A.

Pour répondre à la question B, il faut calculer le nombre minimal de carrés magiques de taille 3×3 nécessaires pour engendrer tous les autres. Nous savons que ce nombre est au plus 4, mais ne serait-il pas possible d'engendrer tous les carrés magiques de somme 0 à partir de seulement 3 carrés magiques de somme 0, voire à partir de 2? Non, ce n'est pas possible : il en faut au moins quatre. Ce résultat sera démontré plus tard quand on aura plus d'outils théoriques.

Exemple 3

Une suite de nombres réels

$$(u_1, u_2, u_3, u_4, u_5 \cdots)$$

est dite arithmétique si la différence entre deux termes consécutifs, appelée la raison, est constante. Par exemple,

$$(1, 2, 3, 4, 5, \cdots) \quad \text{et} \quad (5, 3, 1, -1, -3, -5, \cdots)$$

sont des suites arithmétiques. Le problème que l'on se pose est de trouver **toutes** les suites arithmétiques possibles. A première vue, ce problème est d'aspect bien différent des exemples précédents et pourtant, il leur est tout à fait semblable.

En effet, on peut multiplier une suite arithmétique de raison r

$$(u_1, u_2, u_3, u_4, u_5 \cdots)$$

par un nombre réel λ suivant la règle

$$\lambda.(u_1, u_2, u_3, u_4, u_5 \cdots) = (\lambda u_1, \lambda u_2, \lambda u_3, \lambda u_4, \lambda u_5 \cdots), \tag{1.6}$$

et on vérifie que la nouvelle suite est arithmétique de raison λr.

De même, si $(u_1, u_2, u_3, u_4, u_5 \cdots)$ et $(u'_1, u'_2, u'_3, u'_4, u'_5 \cdots)$ sont deux suites arithmétiques de raison respectives r et r', la somme définie par

$$(u_1, u_2, u_3, u_4, u_5 \cdots) + (u'_1, u'_2, u'_3, u'_4, u'_5 \cdots) = (u_1 + u'_1, u_2 + u'_2, u_3 + u'_3, u_4 + u'_4, u_5 + u'_5 \cdots) \tag{1.7}$$

est aussi une suite arithmétique, de raison $r + r'$ (à vérifier en exercice). Donc, comme dans les deux exemples précédents, nous avons deux méthodes pour 'fabriquer du nouveau à partir de l'ancien' : la multiplication par un nombre réel et l'addition. De nouveau on peut se poser les questions A et B :

(QUESTION A) Peut-on trouver un ensemble fini de suites arithmétiques tel que toutes les suites arithmétiques s'obtiennent à partir de celles-là par nos deux méthodes : multiplication par un réel et addition ?

(QUESTION B) Quel est le plus petit nombre de suites arithmétiques qui engendrent toutes les suites arithmétiques ?

Etudions la question A. Il est clair qu'il suffit de connaître deux nombres pour décrire une suite arithmétique : son premier terme et la raison. Car, si on connaît le premier terme u_1 et la raison r, on sait que la suite ne peut être que

$$(u_1, u_1 + r, u_1 + 2r, u_1 + 3r, u_1 + 4r, \cdots).$$

D'après 1.6 et 1.7, cette suite arithmétique peut s'écrire

$$(u_1, u_1, u_1, u_1, u_1, \cdots) + (0, r, 2r, 3r, 4r, \cdots),$$

qui est aussi égale à

$$u_1.(1, 1, 1, 1, 1, \cdots) + r.(0, 1, 2, 3, 4, \cdots).$$

Cela montre que toute progression arithmétique peut s'écrire comme une somme de multiples des deux progressions arithmétiques

$$(1, 1, 1, 1, 1, \cdots) \quad \text{et} \quad (0, 1, 2, 3, 4, \cdots),$$

et on peut donc dire que ces deux progressions engendrent toutes les progressions arithmétiques. Nous avons répondu positivement à la question A.

Nous répondrons à la question B lorsqu'on aura plus d'outils techniques. On peut dès maintenant soupçonner que le plus petit nombre de suites arithmétiques qu'il faut pour engendrer toutes les suites arithmétiques est deux.

Discussion

Pour chacun des problèmes considérés dans les exemples 1,2 et 3, nous avons vu qu'il est possible de trouver un nombre fini de solutions telles que toutes les autres solutions s'obtiennent à partir de celles-là en faisant des additions et des multiplications. Ce qui est commun aux trois problèmes - et ce qui permet finalement cette description simple de leurs solutions - est l'existence de ces opérations d'addition et de multiplication. Les objets que l'on manipule dans les trois cas ne sont pas les mêmes - un carré magique n'est pas une suite arithmétique - mais les opérations que l'on leur fait subir sont très semblables. L'idée qui motive l'introduction de la notion d'espace vectoriel est de chercher un cadre où l'on peut étudier pour elles-mêmes les opérations d'addition et de multiplication sans se préoccuper de la nature des objets additionés et multipliés. Bien d'autres ensembles d'objets que ceux des exemples précédents sont des espaces vectoriels, en particulier l'ensemble des vecteurs du plan (ou de l'espace).

Les espaces vectoriels

Nous allons maintenant donner la définition d'un espace vectoriel en procédant par étapes.

Il faudra d'abord un ensemble E où il est possible d'additionner deux éléments et de multiplier un élément par un nombre réel. Qu'est-ce que cela signifie au juste ? Cela veut dire que l'on a :

— une opération '+' qui à deux éléments v, w de E associe un troisième élément $v + w$ de E ;

— une multiplication '$\bullet$' qui à un nombre réel λ et à un élément v de E associe un élément $\lambda \bullet v$ de E.

Revenant aux exemples 1,2 et 3, nous avons déjà vu que l'ensemble de carrés magiques (de taille 2×2 de somme quelconque ou 3×3 de somme 0) et l'ensemble de suites arithmétiques ont une opération '+' et une multiplication '$\bullet$'. Sur ces exemples on remarque que les opérations '+' et '$\bullet$' satisfont à certaines règles de calcul. Par exemple, la somme de deux carrés magiques (ou de deux progressions arithmétiques) ne dépend pas de l'ordre des termes mais il y a d'autres règles de calcul, plus ou moins cachées, qu'il faut aussi mettre dans la définition d'un espace vectoriel. La pratique a montré que ces règles de calcul sont :

(I) $v + w = w + v$ (commutativité de $+$) ;

(II) $(v + w) + u = v + (w + u)$ (associativité de $+$) ;

(III) Il existe un élément zéro dans E, c'est-à-dire il existe un élément de E, noté 0, tel que $v + 0 = v$ quel que soit v dans E ;

(IV) Pour chaque v dans E il existe un unique v' dans E tel que $v + v' = 0$ et on le note $-v$;

(V) $1 \bullet v = v$ pour tout v dans E ;

(VI) $\lambda \bullet (\mu \bullet v) = (\lambda\mu) \bullet v$ pour tous λ, μ dans $\mathbb{R}$ et tout v dans E ;

(VII) $(\lambda + \mu) \bullet v = \lambda \bullet v + \mu \bullet v$ pour tout λ, μ dans $\mathbb{R}$ et tout v dans E ;

(VIII) $\lambda \bullet (v + w) = \lambda \bullet v + \lambda \bullet w$ pour tout λ dans $\mathbb{R}$ et tous v, w dans E.

Nous laissons au lecteur (ou à la lectrice) le soin de vérifier que ces propriétés sont bien satisfaites dans les exemples 1,2 et 3.

Ceci étant nous pouvons maintenant donner la définition précise d'un espace vectoriel :

DÉFINITION

Un espace vectoriel est un ensemble non vide E muni d'une opération $+ : E \times E \to E$ et d'une multiplication $\bullet : \mathbb{R} \times E \to E$ tel que les propriétes (I) jusqu'a (VIII) sont satisfaites. On appelle les éléments de E des vecteurs.

2. Dépendance et Indépendance Linéaire

Le but de cette section est d'introduire les outils théoriques nécéssaires pour pouvoir répondre à la question B de la première section. Elle est plus abstraite que celle qui la précède et celle qui la suit. Lors d'une première lecture vous pourriez regarder seulement le Corollaire 5 ci-dessus et ensuite passer directement à la section suivante. En effet, seul le Corollaire 5 sera utilisé dans la dernière section pour répondre à la question B.

Soit E un espace vectoriel. Des éléments de E, c'est-à-dire des vecteurs, seront toujours désignés par les lettres romaines avec ou sans indice (par exemple u, u_1, v, v_1 etc) et des nombres réels par des lettres grecques avec ou sans indice (par exemple λ, λ_1 etc). Soient maintenant $u_1, u_2, \cdots, u_k$ des vecteurs de E. On peut toujours fabriquer de nouveaux vecteurs de E à partir de $u_1, u_2, \cdots, u_k$ en faisant des additions et en multipliant par des scalaires. On notera $< u_1, u_2, \cdots, u_k >$ l'ensemble de tous les vecteurs que l'on peut obtenir de cette manière :

$$< u_1, u_2, \cdots, u_k >= \{\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_k u_k : \quad \lambda_1, \lambda_2, \cdots \lambda_k \in \mathbb{R}\}.$$

Nous appelerons $< u_1, u_2, \cdots, u_k >$ le sous-espace de E engendré par les vecteurs $u_1, u_2, \cdots, u_k$ et nous appelerons une expression de la forme $\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_k u_k$ une combinaison linéaire des vecteurs $u_1, u_2, \cdots, u_k$.

Exercice (A) : Montrer que si u et v appartiennent à $< u_1, u_2, \cdots, u_k >$ et λ est un nombre réel, alors $u + v$ et λu appartiennent à E.

Dans cette section nous allons supposer que l'espace vectoriel E a la propriété suivante :

(*) *il existe une famille de vecteurs* $v_1, v_2, \cdots, v_n$ *de* V *tels que* $V =< v_1, v_2, \cdots, v_n >$.

Autrement dit, nous allons supposer que la question (A) du premier chapitre admet une réponse positive pour l'espace vectoriel E. Comme on l'a déjà vu, tous les exemples de la section précédente ont cette propriété. Donc toute autre propriété de E que l'on pourrait déduire à partir de (*) par des 'raisonnements abstraits' sera vraie dans chacun des exemples. C'est cela tout l'interet d'avoir dégagé la structure mathématique commune à tous ces exemples. En particulier, nous allons démontrer une propriété des espaces vectoriels, le Corollaire 5 ci-dessous, qui nous permettra, comme déjà dit, de répondre à la question B pour les exemples 1,2 et 3 de la section précédente.

Considérons donc un espace vectoriel E qui a la propriété (*). Les vecteurs $v_1, v_2, \cdots, v_n$ engendrent E mais il est naturel de se demander (cf. la question (B)) s'il ne serait pas possible d'engendrer E de manière plus économe, c'est-à-dire avec moins de vecteurs. Les familles de vecteurs engendrant E et qui sont les plus économes possibles méritent un nom :

1 DÉFINITION

On dira que les vecteurs $u_1, u_2, \cdots, u_k$ *forment une base de* E *si* (*i*) E *est engendré par* $u_1, u_2, \cdots, u_k$ *et si* (*ii*) *aucune sous-famille de* $u_1, u_2, \cdots, u_k$ *n'engendre* E.

Existe-t-il des bases de E? Considérons les sous-familles de la famille $v_1, v_2, \cdots, v_n$. Une sous-famille engendre ou n'engendre pas E, donc parmi les sous-familles qui engendrent, une qui contient le moins de vecteurs est certainement une base. Mais attention : a priori rien empêche une autre sous-famille qui engendre E et qui contient plus de vecteurs d'être aussi une base.

Une fois que l'on sait que des bases existent comment fait-on pour les trouver? Si $u_1, u_2, \cdots, u_k$ forment une base, les vecteurs $u_1, u_2, \cdots, u_k$ ont-ils quelque chose de spécial? La proposition suivante met en evidence une propriété importante d'une famille de vecteurs formant une base de E.

2 PROPOSITION

Soit $u_1, u_2, \cdots, u_k$ *une base de* E. *Soient* $\lambda_1, \lambda_2, \cdots, \lambda_k$ *des nombres réels tels que*

$$\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_k u_k = 0.$$

Nous avons alors $\lambda_1 = \lambda_2 = \cdots = \lambda_k = 0$.

Démonstration. Supposons pour avoir une contradiction que l'on puisse trouver des nombres réels $\lambda_1, \lambda_2, \cdots, \lambda_k$ dont au moins un, disons λ_s, est différent de zéro tels que

$$\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_s u_s + \cdots + \lambda_k u_k = 0.$$

Comme $\lambda_s \neq 0$, on a le droit de diviser par λ_s et on peut alors exprimer u_s en termes des autres vecteurs de la base $u_1, u_2, \cdots, u_k$:

$$u_s = -\frac{\lambda_1}{\lambda_s} u_1 - \frac{\lambda_2}{\lambda_s} u_2 - \cdots - \frac{\lambda_{s-1}}{\lambda_s} u_{s-1} - \frac{\lambda_{s+1}}{\lambda_s} u_{s+1} - \cdots - \frac{\lambda_k}{\lambda_s} u_k. \tag{2.1}$$

Cela veut dire que toute combinaison linéaire des k vecteurs $u_1, u_2, \cdots, u_k$ est en fait une combinaison linéaire des $k-1$ vecteurs de la sous-famille obtenue en enlevant u_s : chaque fois que u_s apparaît dans

une telle combinaison linéaire on le remplace par 2.1. Comme la famille $u_1, u_2, \cdots, u_k$ engendre E, cette sous-famille aussi. Mais $u_1, u_2, \cdots, u_k$ est une base ce qui fait qu'aucune sous-famille ne peut engendrer E d'où une contradiction. L'hypothèse de départ est donc fausse (puisqu'elle mène à une contradiction) et la proposition est démontrée. □

La proposition nous dit que si $u_1, u_2, \cdots, u_k$ forment une base de E, la seule combinaison de ces vecteurs qui donne 0 est la combinaison 'triviale', c'est-à-dire celle où tous les coefficients sont 0. Donnons un nom à cette propriété :

3 DEFINITION
On dira que les vecteurs $u_1, u_2, \cdots, u_k$ de E sont :
- liés s'il existe des nombres réels $\lambda_1, \lambda_2, \cdots \lambda_k$ dont au moins un est différent de 0 tels que

$$\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_k u_k = 0.$$

- indépendants si

$$\left.\begin{array}{r} \lambda_1, \lambda_2, \cdots \lambda_k \in \mathbb{R} \\ \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_k u_k = 0 \end{array}\right\} \Rightarrow \lambda_1 = \lambda_2 = \cdots = \lambda_k = 0.$$

D'après la Proposition 2, les vecteurs $u_1, u_2, \cdots, u_k$ ne peuvent constituer une base de E que s'ils sont indépendants.

Exercice (B) : Montrer que toute famille de vecteurs contenant le vecteur nul est liée.

Exercice (C) : Montrer qu'une famille de vecteurs qui contient une famille de vecteurs liés est liée.

Nous pouvons maintenant énoncer le résultat clé de ce chapitre. Ce qu'il affirme c'est que si l'on veut engendrer un espace vectoriel avec le moins de vecteurs possibles il faut prendre des vecteurs indépendants.

4 THÉORÈME
Toute famille de $k+1$ vecteurs appartenant à l'espace engendré par k vecteurs de E est liée.

Démonstration. Nous allons démontrer ce résultat par récurrence sur k. L'hypothèse de récurrence au cran n est :

Toute famille de $n+1$ vecteurs de l'espace engendré par n vecteurs de E est liée. (H_n)

Nous devons donc : (i) vérifier que (H_1) est vraie et (ii) montrer que pour tout entier $n \geq 1$, (H_n) est vraie implique que (H_{n+1}) est vraie.

Vérifions d'abord (H_1). Pour cela il faut montrer que si w_1 est un vecteur de E , alors deux vecteurs quelconques appartenant à $< w_1 >$, disons x_1 et x_2, sont liés.

Si $w_1 = 0$, comme tout multiple de 0 est également 0, nous avons $x_1 = x_2 = 0$ et les vecteurs x_1 et x_2 sont liés par l'Exercice B. Supposons donc que $w_1 \neq 0$.

Remarquons d'abord que si un des vecteurs x_1, x_2 est nul alors les deux sont liés (par l'Exercice (B) ci-dessus) donc pour démontrer (H_1) il suffit de traiter le cas où les deux vecteurs sont non-nuls.

Comme les éléments de $< w_1 >$ sont par définition tous de la forme λw_1 pour λ un nombre réel, il existe $\lambda_1 \neq 0$ et $\lambda_2 \neq 0$ dans $\mathbb{R}$ tels que

$$x_1 = \lambda_1 w_1 \quad \text{et} \quad x_2 = \lambda_2 w_1.$$

Cela implique que

$$\lambda_2 x_1 - \lambda_1 x_2 = 0$$

et cette équation dit exactement que x_1 et x_2 sont liés. Nous avons demontré que (H_1) est vérifiée.

Maintenant supposons que (H_n) est vraie pour un entier $n \geq 1$. Il faut montrer que ceci implique que (H_{n+1}) est vraie.

Soit donc $x_1, x_2, \cdots, x_{n+2}$ une famille de $n+2$ vecteurs appartenant à $< w_1, w_2, \cdots, w_{n+1} >$ où $w_1, w_2, \cdots, w_{n+1}$ sont des vecteurs arbitraires de E. Si un des $x_1, x_2, \cdots, x_{n+2}$ est nul, on sait qu'ils sont liés donc pour démontrer (H_{n+1}) il suffit de traiter le cas où $x_i \neq 0$ pour $1 \leq i \leq n+2$.

Comme tout élément de $< w_1, w_2, \cdots, w_{n+1} >$ est par définition une combinaison linéaire des w_i, il existe des nombres réels $\lambda_{a,b}$ (avec $1 \leq a \leq n+2$ et $1 \leq b \leq n+1$) tels que :

$$\begin{aligned} x_1 &= \lambda_{1,1}w_1 + \lambda_{1,2}w_2 + \cdots + \lambda_{1,n+1}w_{n+1} \\ x_2 &= \lambda_{2,1}w_1 + \lambda_{2,2}w_2 + \cdots + \lambda_{2,n+1}w_{n+1} \\ &\text{etc} \\ x_{n+2} &= \lambda_{n+2,1}w_1 + \lambda_{n+2,2}w_2 + \cdots + \lambda_{n+2,n+1}w_{n+1}. \end{aligned}$$

Nous avons supposé que $x_1 \neq 0$ donc un des coefficients $\lambda_{1,1}, \lambda_{1,2}, \cdots \lambda_{1,n+1}$ dans l'équation

$$x_1 = \lambda_{1,1}w_1 + \lambda_{1,2}w_2 + \cdots + \lambda_{1,n+1}w_{n+1}$$

est différent de zéro et, quitte à renuméroter les vecteurs $w_1, w_2, \cdots, w_{n+1}$, on peut supposer que $\lambda_{1,1} \neq 0$.

Considérons maintenant les $n+1$ vecteurs

$$\lambda_{1,1}x_2 - \lambda_{2,1}x_1, \quad \lambda_{1,1}x_3 - \lambda_{3,1}x_1, \quad \cdots, \quad \lambda_{1,1}x_{n+2} - \lambda_{n+2,1}x_1.$$

On voit que chacun de ces $n+1$ vecteurs est une combinaison linéaire des n vecteurs $w_2, \cdots, w_{n+1}$ car il n'y a pas de terme en w_1. D'après l'hypothèse au cran n cela veut dire que les vecteurs $\lambda_{1,1}x_2 - \lambda_{2,1}x_1$, $\lambda_{1,1}x_3 - \lambda_{3,1}x_1$, $\cdots$, $\lambda_{1,1}x_{n+2} - \lambda_{n+2,1}x_1$ sont liés, c'est-à-dire qu'il existe des nombres réels $\mu_2, \mu_3, \cdots, \mu_{n+2}$ dont au moins un, disons μ_k, est différent de zéro tels que

$$\mu_2(\lambda_{1,1}x_2 - \lambda_{2,1}x_1) + \mu_3(\lambda_{1,1}x_3 - \lambda_{3,1}x_1) + \cdots + \mu_{n+2}(\lambda_{1,1}x_{n+2} - \lambda_{n+2,1}x_1) = 0.$$

Mais quand on enlève les parenthèses du membre de gauche de cette équation on a une combinaison linéaire des $x_1, x_2, \cdots, x_{n+2}$ et le coefficient de x_k est $\mu_k\lambda_{1,1}$ qui est différent de zéro. Comme cette combinaison linéaire est égale au vecteur nul, nous avons bien démontré que $x_1, x_2, \cdots, x_{n+2}$ sont liés. □

5 COROLLAIRE

L'espace $< u_1, u_2, \cdots, u_k >$ engendré par k vecteurs indépendants $u_1, u_2, \cdots, u_k$ ne peut être engendré par r vecteurs si $r < k$.

Démonstration. Si $< u_1, u_2, \cdots, u_k >$ était engendré par r vecteurs, toute famille de $r+1$ vecteurs appartenant à $< u_1, u_2, \cdots, u_k >$ serait liée d'après le Théorème 4. Mais la famille $u_1, u_2, \cdots, u_k$ contient au moins $r+1$ vecteurs car $r < k$ et donc serait liée d'après l'Exercice C. C'est une contradiction. □

6 COROLLAIRE

Deux bases de E ont le même nombre de vecteurs.

Démonstration. Soient $y_1, y_2, \cdots, y_n$ et $w_1, w_2, \cdots w_m$ deux bases de E. Les vecteurs $w_1, w_2, \cdots w_m$ engendrent $E =< y_1, y_2, \cdots, y_n >$ et comme $y_1, y_2, \cdots, y_n$ sont indépendants on a $m \geq n$ d'après le Corollaire 5. De même, les vecteurs $y_1, y_2, \cdots, y_n$ engendrent $E =< w_1, w_2, \cdots w_m >$ et comme

$w_1, w_2, \cdots w_m$ sont indépendants on a $n \geq m$ d'après le Corollaire 5. Puisque $m \geq n$ et $n \geq m$, nous avons $m = n$. □

3. Retour aux exemples

Maintenant nous allons voir que le Corollaire 5 permet de répondre à la question B pour les exemples 1,2 et 3 de la première section. Rappelons que nous y avions vu que :

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ engendrent tous les carrés magiques de taille 2×2;

$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix}$ engendrent tous les carrés magiques de taille 3×3 de somme 0;

$(1,1,1,1,1,\cdots)$ et $(0,1,2,3,4,\cdots)$ engendrent toutes les suites arithmétiques.

Considérons l'exemple 1. Si les deux carrés magiques

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

sont indépendants, le Corollaire 5 entraîne que tous les carrés magiques de taille 2×2 ne peuvent être engendrés par moins de deux carrés magiques. Autrement dit, et c'est la reponse à la question B, le plus petit nombre de carrés magiques de taille 2×2 qui engendrent tous les carrés magiques de taille 2×2 est deux. Vérifions que $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ sont effectivement indépendants. Pour cela il faut montrer que si

$$\lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \mu \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

alors $\lambda = \mu = 0$. Or, l'équation ci-dessus s'écrit

$$\begin{pmatrix} \lambda & \mu \\ \mu & \lambda \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

ce qui implique $\lambda = \mu = 0$.

Considérons l'exemple 2. Le Corollaire 5 entraîne que, si les trois carrés magiques

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix}$$

sont indépendants, le plus petit nombre de carrés magiques de taille 3×3 de somme 0 qui engendrent tous les carrés magiques de taille 3×3 de somme 0 est quatre. Vérifions l'indépendance de ces quatre carrés magiques. Supposons que

$$\lambda \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix} + \mu \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & -1 & 1 \end{pmatrix} + \nu \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix} + \rho \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Cette équation s'écrit

$$\begin{pmatrix} \lambda & \mu & -\lambda-\mu \\ \nu & \rho & -\nu-\rho \\ -\lambda-\nu & -\mu-\rho & \lambda+\mu+\nu+\rho \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

D'après l'égalité des deux premières lignes on a $\lambda = 0$ et $\mu = 0$, et d'après l'égalité des deux deuxièmes lignes on a $\nu = 0$ et $\rho = 0$. Donc les quatre carrés magiques sont bien indépendants.

Nous laissons au lecteur (ou à la lectrice) le soin de vérifier que les deux suites arithmétiques

$$(1, 1, 1, 1, 1, \cdots) \quad \text{et} \quad (0, 1, 2, 3, 4, \cdots)$$

sont indépendantes, ce qui montre, de nouveau par le Corollaire 5, que le plus petit nombre de suites arithmétiques qui engendrent toutes les suites arithmétiques est deux.

En conclusion, nous avons pu répondre à la question B pour les trois exemples de la première section. Cela s'est fait, non sans peine, en exploitant la notion abstraite d'indépendance linéaire des vecteurs.

Titre : Pourquoi pas ? des Mathématiques

Auteurs : Groupe IREM «Liaison Lycée-DEUG» :
WEIL Dominique - SLUPINSKI Markus -
KOCH Bernard - DIDIERJEAN André -
BLASCO Laure - ATLAGH Mohamed.

Mots-clés : Liaison lycée-université - Logique - Analyse -
Arithmétique - Algèbre linéaire

Date : 2000

Editeur : I.R.E.M. de Strasbourg (**S. 179**)

ISBN : 2-911446-14-3

Public concerné : Lycéens en fin de terminale scientifique
& Etudiants en DEUG

Résumé :
Cette brochure est conçue pour être lisible par un élève à sa sortie de terminale scientifique.

Elle l'invite à une lecture active de petits textes mathématiques lui présentant des notions incontournables au cours d'études scientifiques.

Ce fascicule comprend quatre parties pouvant être lues indépendamment et développant les thèmes suivants :

. application et fonctions vues à travers divers domaines,
. lecture accompagnée d'un texte mathématique sur les suites récurrentes et l'application logistique,
. arithmétique,
. notion d'espace vectoriel.

Entre chacune de ces parties se trouvent quelques récréations logiques.

Prix : 55 F + port.