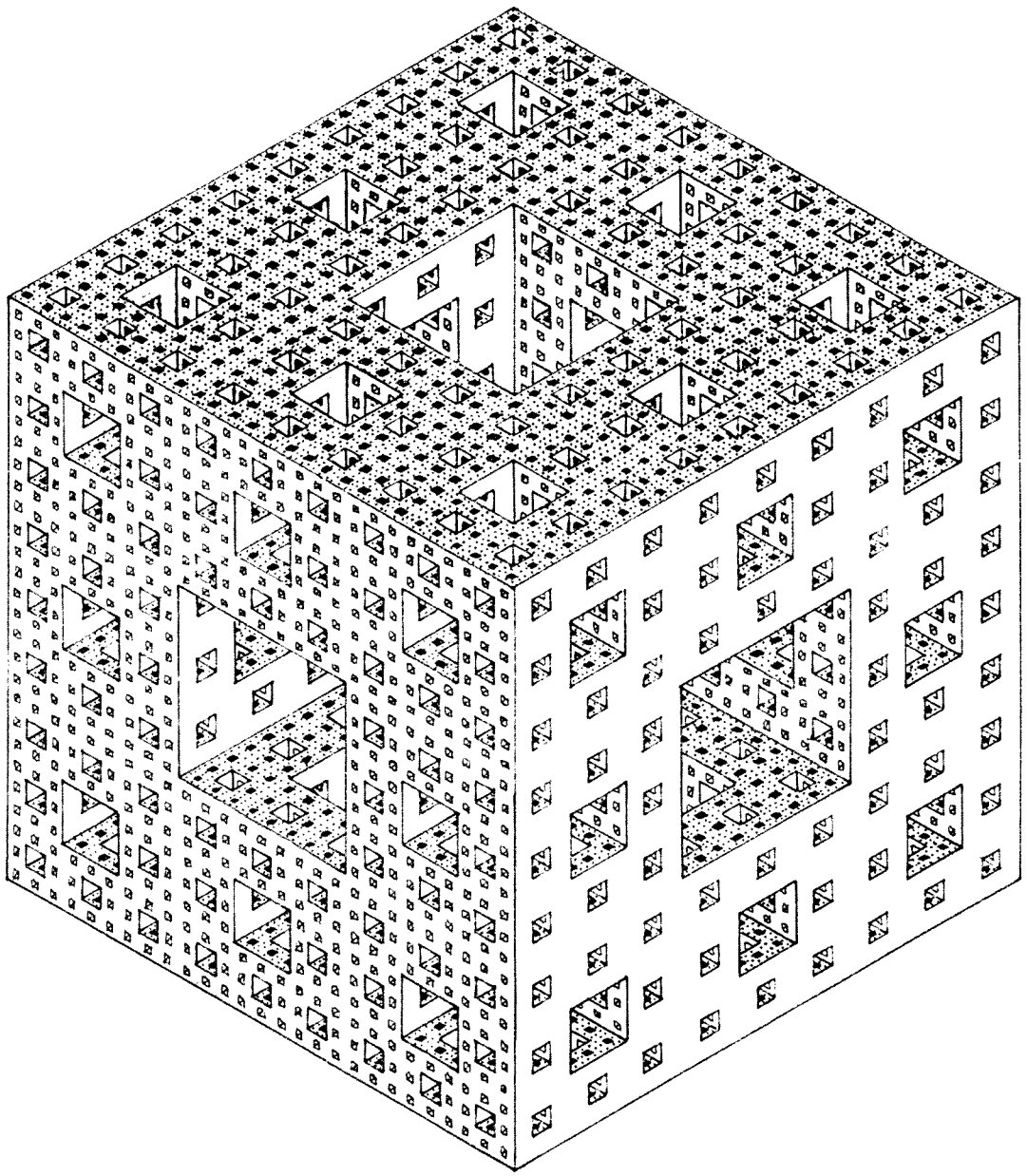
l'ouvert n°18

ORGANE D'INFORMATION ET D'ECHANGE
DE LA REGIONALE APMEP D'ALSACE ET
DE L'IREM DE STRASBOURG - MAI 79



NOTRE COUVERTURE : Une éponge de Sierpinski. Partant d'un cube d'arête unité, on le divise en $3^3 = 27$ petits cubes identiques. On enlève le cube central ainsi que les six qui lui sont adjacents. On recommence l'opération sur les vingt cubes restants et ainsi de suite jusqu'à l'infini. L'ensemble obtenu a beaucoup de parenté avec l'ensemble triadique de Cantor. En particulier on peut lui attribuer une dimension fractale de 2,7268... (voir l'article page 33 et suivantes).

SOMMAIRE

Dévaluation

Il est de bon ton de se plaindre du niveau des élèves qui baisse d'année en année et il ne manque pas de collègues pour vous citer l'exemple de tel exercice qu'ils donnaient à résoudre en quatrième il y a vingt ans et qu'il est difficile de faire passer en seconde actuellement. C'est enfoncer des portes ouvertes que de dénoncer la dévaluation des examens et des diplômes ; on parlera avec nostalgie du Certificat d'Etude d'antan.

Mais dès qu'on aborde le niveau de recrutement des enseignants, quelle levée de boucliers corporatistes! Et pourtant, il n'y a aucune raison que le CAPES, l'agrégation, le doctorat... aient échappé à la dévaluation générale des diplômes. Et effectivement, une comparaison rapide des thèses soutenues actuellement et de celles soutenues il y a quelques dizaines d'années démontre sans ambiguïté ce fait. Malheureusement, à côté de cette baisse du niveau des formations traditionnelles, les ministres successifs ont instauré des sous-formations, ce qui a un avantage financier évident (plus d'heures de cours pour un salaire moindre, quelle aubaine !)

Il n'est pas du tout surprenant de constater que l'extension de la scolarité des élèves a coïncidé avec une baisse générale du niveau tant de ceux-ci que des enseignants. De tout temps les meilleurs maîtres ont été réservés à l'élite. Il ne s'est jamais vu qu'un I.G. ayant félicité un professeur de Terminale C lui propose comme promotion de prendre en charge à la rentrée une 5ème spéciale (ex-CPPN). En raison du nivellement par la base qui a été effectué dans les différentes classes, on reporte la sélection des élites au moment du bac ou même après.

Il est alors clair que la démocratisation de l'enseignement dont on nous rabâche les oreilles n'est qu'une pseudo-démocratisation. Les enfants des milieux défavorisés doivent rester plus longtemps à l'école, ce qui entraîne une lassitude et un dégoût vis-à-vis d'une institution qui ne leur est pas destinée et finalement ils n'en retireront aucun bénéfice car le diplôme final qu'ils pourront obtenir aura été dévalué en proportion plus grande. A cela il faudra ajouter l'effort financier des parents qui ne pourra pas être maintenu assez longtemps.

Ces quelques réflexions font mieux comprendre le lent glissement de l'école obligatoire vers la garderie. Pour l'Administration, la seule chose qui compte c'est que l'emploi du temps indique que les 4ème 3 ont mathématiques le mardi de 8 à 9 avec monsieur X et que ce professeur prenne en charge ces élèves à l'heure indiquée et

remette en temps utile liste des notes et liste des absents. Que monsieur X enseigne soi-disant les mathématiques après une titularisation lors d'un match de basket n'a aucune importance puisque cet enseignant ne s'adresse pas à la future élite que sont les enfants des milieux socio-culturels favorisés. Et si des parents se plaignent, on pourra toujours accuser les mathématiques modernes.

On va me dire : "Que vous voilà pessimiste ! Tout cela est entrain de changer. La preuve : Le ministère vient de revaloriser de façon appréciable la formation des instituteurs." Voire ! Nous arrivons dans les classes démographiques creuses et par les vertus du redéploiement il n'est guère besoin de recruter de nouveaux maîtres. Cela enlève beaucoup à la noblesse des intentions du gouvernement. Nous attendons une formation continue digne de ce nom. Le sort réservé aux IREM nous montre ce qu'il en sera.

Jean Lefort

L'importance des interactions entre les différents secteurs mathématiques, (...) ne caractérise pas spécialement la période récente. Souvent au contraire, cette convergence des théories mathématiques (vers un foyer qu'on peut situer du côté de la théorie des nombres) échappe à beaucoup de mathématiciens trop pris dans leur spécialité. Les difficultés de carrière, qui s'aggravent rapidement depuis quelques années, rendent la concurrence plus vive et poussent les jeunes mathématiciens à se spécialiser plus étroitement pour produire plus vite ; ces difficultés découragent les étudiants de tenter la voie de la recherche mathématique (où la France fait encore bonne figure sur le plan international) et on peut craindre que cette activité ne soit étouffée à brève échéance. Parallèlement, l'enseignement secondaire va se dégrader de façon catastrophique avec l'asphyxie des IREM et les désastreux projets ministériels sur la formation des maîtres.

Ch. Houzel : "Les mathématiciens retournent au concret" La Recherche nº 100.

Quelques problèmes posés par la phyllotaxie

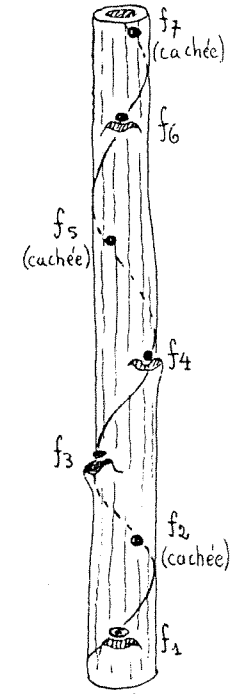
I. QU'EST-CE QUE LA PHYLLOTAXIE ?

La phyllotaxie est l'étude de la disposition des feuilles sur la tige d'une plante ($\varphi\upsilon\lambda\lambda o\nu$ = feuille). Dans ce qui va suivre nous allons nous intéresser à l'un des aspects de cette science donnant de curieux résultats liés à des problèmes d'arithmétique. L'observation est très facile et il n'est pas nécessaire d'avoir recours à des plantes rares : quelques pommes de pin et d'épicéa, une tête d'artichaut, quelques marguerites ou mieux encore des dahlias ; la fleur de tournesol est idéale mais difficile à trouver et non indispensable.

Lorsque les feuilles sont alternes, c'est-à-dire insérées isolément sur la tige, elles sont disposées suivant une hélice de sorte que de chacune d'elles à la suivante il y ait une fraction déterminée de tour. Cette fraction constante pour la plante donnée porte le nom de divergence. Si les feuilles sont largement espacées l'observation est aisée et on trouve pour valeurs les plus fréquentes de la divergence :

$$\frac{1}{2}\ ,\ \frac{1}{3}\ ,\ \frac{2}{5}\ ,\ \frac{3}{8}\ ,\ \frac{5}{13}\ \cdots$$

Ex : orme : $\frac{1}{2}$, aulne : $\frac{1}{3}$, cerisier : $\frac{2}{5}$.



Rameau à feuilles alternes dépouillé de ses feuilles

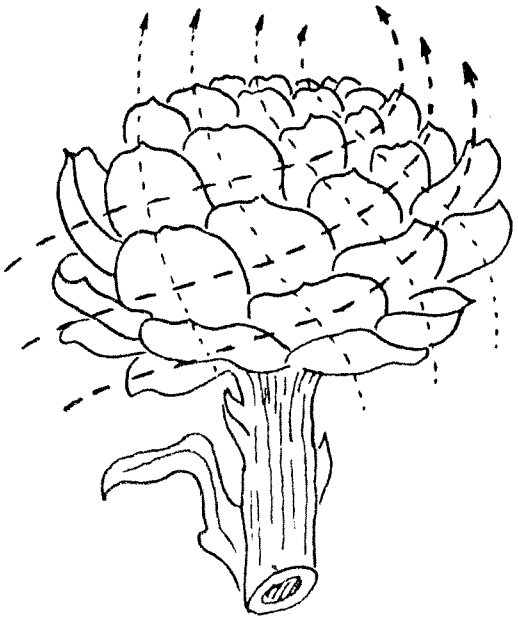
Lorsque les feuilles sont très rapprochées comme pour l'artichaut par exemple, l'étude devient beaucoup plus difficile. Mais on remarque qu'en joignant chaque feuille à la feuille supérieure immédiatement voisine on peut tracer sur l'artichaut 8 rangées tordues en hélices montant dans un sens et 5 montant dans l'autre. Une étude minutieuse donnerait pour divergence $\frac{5}{13}$. Les hélices sont particulièrement visibles sur une pomme d'épicéa (5 dans un sens et 8 dans l'autre et sur une pomme de pin, 8 et 13). La disposition des graines dans une fleur suit en général la même règle.

Nous avons observé dans un dahlia 21 spirales dans un sens et 34 dans l'autre. On trouve des valeurs encore plus élevées pour les fleurs de tournesol (55 et 89 par exemple).

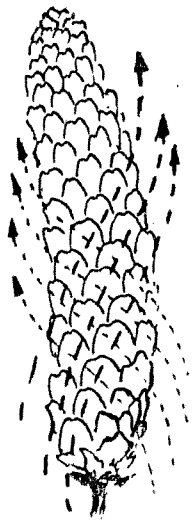
Invariablement les mêmes conclusions s'imposent :

a) La divergence est une fraction $\frac{a}{b}$ telle que $a = u_k$ et $b = u_{k+2}$, les u_i étant des termes de la suite de Fibonacci : 1, 1, 2, 3, 5, 8, 13, 21 ... définie par $u_n = u_{n-1} + u_{n-2}$ et $u_o = u_1 = 1$.

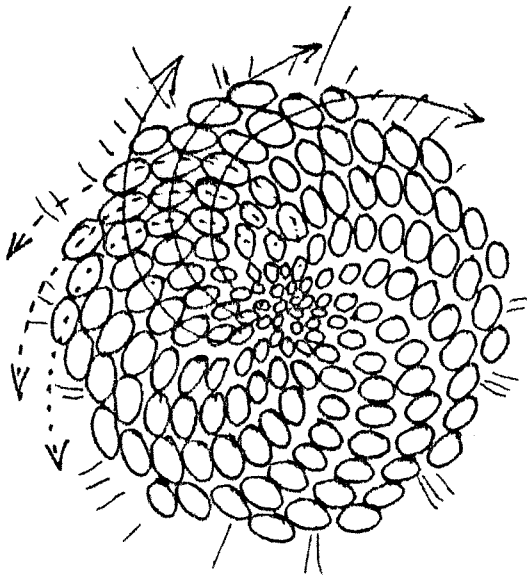
b) Si la divergence vaut $\frac{u_k}{u_{k+2}}$ alors les feuilles ou les graines, lorsqu'elles sont très rapprochées semblent disposées suivant u_k spirales (ou hélices) tournant dans un sens et u_{k+1} spirales tournant dans l'autre sens.



Artichaut : $\alpha = \frac{5}{13}$



Pomme d'épicea : $d = \frac{5}{13}$



Graines dans une fleur de tournesol

Essayons d'expliquer de façon plausible ces résultats moyennant certaines hypothèses. Mais auparavant il nous faut reprendre quelques propriétés classiques de la suite de Fibonacci.

II. SUITE DE FIBONACCI ET NOMBRE D'OR

La suite de Fibonnaci est donc définie par la relation de récurrence :

$\forall n \quad u_n = u_{n-1} + u_{n-2}$ avec $u_o = u_1 = 1$.

u_0	u_1	u_2	u_3	u_4	u_5	u_6	u_7	.....
1	1	2	3	5	8	13	21	.....

Quelques propriétés

a) Appelons $\delta(a,b)$ le pgcd de a et b. On peut écrire :

$$\delta(u_n, u_{n+1}) = \delta(u_{n+1} - u_n, u_n) = \delta(u_{n-1}, u_n) = \ldots\ldots\ldots = \delta(1,1) = 1$$

D'autre part :

$$\delta(u_n, u_{n+2}) = \delta(u_n, u_{n+2} - u_n) = \delta(u_n, u_{n+1}) = 1$$

$\forall n$ $\boxed{\begin{array}{l} u_n \text{ et } u_{n+1} \text{ sont premiers entre eux} \\ u_n \text{ et } u_{n+2} \text{ sont premiers entre eux.} \end{array}}$

b) $u_{n+1} \cdot u_{n-1} - u_n^2 = (u_n + u_{n-1})u_{n-1} - u_n(u_{n-1} + u_{n-2})$

$$= u_n \cdot u_{n-1} + u_{n-1}^2 - u_n \cdot u_{n-1} - u_n \cdot u_{n-2} = u_{n-1}^2 - u_n \cdot u_{n-2}$$

et comme $u_2 \cdot u_0 - u_1^2 = 1$

$$\boxed{u_{n+1} \cdot u_{n-1} - u_n^2 = (-1)^{n+1}}$$

$$u_{n+1} \cdot u_{n-2} - u_n \cdot u_{n-1} = (u_n + u_{n-1})u_{n-2} - u_n(u_{n-2} + u_{n-3})$$

$$= u_{n-1} \cdot u_{n-2} - u_n \cdot u_{n-1}$$

Donc

$$\boxed{u_{n+1} \cdot u_{n-2} - u_n \cdot u_{n-1} = (-1)^n}$$

On trouve de la même façon

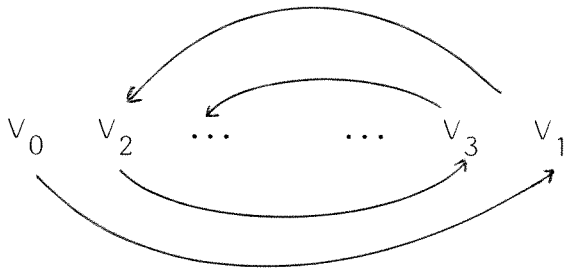
$$\boxed{u_{n-2} \cdot u_{n+2} - u_n^2 = (-1)^n}$$

c) Considérons la suite $V_n = \dfrac{u_{n+1}}{u_n}$

$$V_n - V_{n-1} = \frac{u_{n+1} \cdot u_{n-1} - u_n^2}{u_n \cdot u_{n-1}} = \frac{(-1)^{n+1}}{u_n \cdot u_{n-1}}$$

Comme la suite des u_n est croissante et que $u_n \longrightarrow +\infty$ lorsque $n \longrightarrow +\infty$ le terme $V_n - V_{n-1} \longrightarrow 0$ lorsque $n \longrightarrow +\infty$ et la suite des V_n est croissante pour les n pairs et décroissante pour les n impairs.

On a donc la disposition suivante :



Donc lorsque $n \longrightarrow +\infty$ V_n tend vers une limite que nous appellerons Φ .

$$\Phi = \lim_{n \to +\infty} \frac{u_{n+1}}{u_n}$$

Calculons Φ $\quad u_{n+1} = u_n + u_{n-1}$

$$\frac{u_{n+1}}{u_n} = 1 + \frac{u_{n-1}}{u_n} = 1 + \frac{1}{\frac{u_n}{u_{n-1}}}$$

$$\lim_{n \to +\infty} \frac{u_{n+1}}{u_n} = 1 + \frac{1}{\lim\limits_{n \to +\infty} \frac{u_n}{u_{n-1}}} \quad \Longleftrightarrow \quad \Phi = 1 + \frac{1}{\Phi}$$

Φ est la solution positive de l'équation $\Phi^2 - \Phi - 1 = 0$

$$\boxed{\Phi = \frac{1 + \sqrt{5}}{2} \simeq 1{,}618}$$ (Φ = nombre d'or)

Développement en fraction continue

$$\Phi = 1 + \frac{1}{\Phi} = 1 + \frac{1}{1 + \frac{1}{\Phi}} = 1 + \frac{1}{1 + \frac{1}{1 + ..}}$$

Les premières réduites sont $\frac{1}{1}$, $\frac{2}{1}$, $\frac{3}{2}$, $\frac{5}{3}$, ...

Supposons que la $n^{ième}$ résuite soit $\frac{u_n}{u_{n-1}}$

La $(n+1)^{ième}$ réduite est alors $1 + \frac{1}{\frac{u_n}{un-1}} = \frac{u_n + u_{n-1}}{u_n} = \frac{u_{n+1}}{u_n}$

Donc : la $n^{ième}$ réduite de Φ est $\frac{u_n}{u_{n-1}}$

d) Le nombre $\Psi = \frac{1}{\Phi^2}$

Ce nombre va jouer un rôle important dans la disposition des feuilles et des graines.

La décomposition de Ψ en fraction continue est immédiate

$$\Phi^2 = 1 + \Phi \implies \Psi = \frac{1}{1+\Phi} = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \ldots}}}$$

Les premières réduites sont cette fois : $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{5}$, $\frac{3}{8}$, ...

Supposons que la $n^{ième}$ réduite soit $\frac{u_{n-1}}{u_{n+1}}$. Soit x la $(n+1)^e$ réduite.

On a : $\cfrac{u_{n-1}}{u_{n+1}} = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\ddots 1}}}$ donc $\cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots 1}}} = \cfrac{1}{\cfrac{u_{n+1}}{u_{n-1}} - 1}$

et par conséquent :

$$x = \cfrac{1}{2 + \cfrac{1}{\cfrac{u_{n+1}}{u_{n-1}} - 1}} = \cfrac{1}{2 + \cfrac{u_{n-1}}{u_n}} = \frac{u_n}{u_n + u_n + u_{n-1}}$$

$$= \frac{u_n}{u_n + u_{n+1}} = \frac{u_n}{u_{n+2}}$$

Conclusion : les fractions $\frac{u_k}{u_{k+2}}$ que nous avons rencontrées à propos de la divergence des feuilles ne sont autres que les résuites de : $\Psi = \frac{1}{\Phi^2}$ ($\simeq 0{,}382$).

III. INTERPRETATION MATHEMATIQUE DES PHENOMENES OBSERVES

Dans ce dernier paragraphe nous allons essayer de répondre à deux questions :

- Pourquoi la divergence prend-elle des valeurs $d = \frac{u_k}{u_{k+2}}$?
- Pourquoi, si $d = \frac{u_k}{u_{k+2}}$, voit-on apparaître u_k spirales tournées dans un sens et u_{k+1} tournées dans l'autre ?

1) La divergence vaut $d = \frac{u_k}{u_{k+2}}$

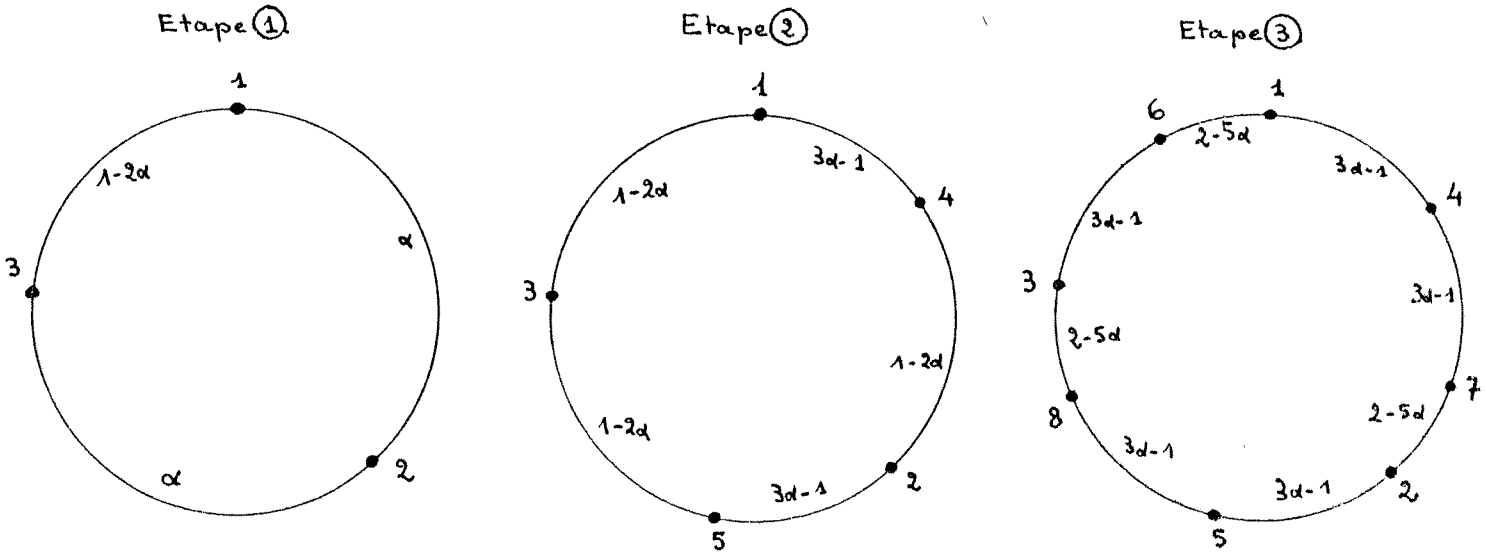
Représentons la section de la tige par un cercle et l'arc correspondant à la divergence par un arc α . La divergence étant par définition une fraction de circonférence nous allons prendre le cercle entier comme unité de mesure des arcs. Pour faire cette étude il est indispensable de recourir à des figures aussi exactes que possible. Comme $d = \frac{5}{13}$ et $d' = \frac{8}{21}$ correspondent à des valeurs voisines de

0,38 prenons cette valeur pour nos constructions (ceci correspond à un arc d'environ 137°). Plaçons sur le cercle des points numérotés représentant les bases des feuilles dans l'ordre de leur croissance. La figure confirme alors immédiatement l'hypothèse que nous retiendrons et qui est préconisé par certains auteurs (cf. par exemple : "les formes dans la nature" de P. Stevens) :

> Lorsqu'une nouvelle feuille n° c vient se placer entre deux feuilles n° a et n° b (a < b) elle se place plus près de la feuille la plus âgée n° a que de la plus jeune n° b.

Cette hypothèse est assez naturelle quand on songe que de cette façon les feuilles les plus jeunes et en pleine croissance, b et c en l'occurence, se gênent le moins possible dans leur développement.

Examinons maintenant en 3 étapes l'apparition des 8 premières feuilles.



① La feuille 3 est plus près de 1 que de 2.

② La feuille 4 vient entre 1 et 2 mais plus près de 1 que de 2.
La feuille 5 vient entre 2 et 3 mais plus près de 2 que de 3.

③ La feuille 6 vient entre 1 et 3 mais plus près de 1 que de 3.
La feuille 7 vient entre 2 et 4 mais plus près de 2 que de 4.
La feuille 8 vient entre 3 et 5 mais plus près de 3 que de 5.

En tenant compte du fait que l'arc séparant deux feuilles consécutives vaut toujours α on constate qu'à chaque étape le cercle est subdivisé en grands arcs et petits arcs respectivement égaux entre eux. A l'étape suivante les points se placeront sur les grands arcs qu'ils subdiviseront de sorte que les nouveaux grands arcs soient égaux aux anciens petits arcs conformément au tableau suivant.

	1ère étape		2° étape		3° étape			n^ième étape	
	Nombre	Valeur	Nbre	Valeur	Nbre	Valeur		Nombre	Valeur
Petits arcs	1	$1-2\alpha$	2	$3\alpha-1$	3	$2-5\alpha$	....	u_n	$(-1)^n(u_{n+1}\alpha - u_n)$
Grands arcs	2	α	3	$1-2\alpha$	5	$3\alpha-1$	....	u_{n+1}	$(-1)^n(u_{n-1} - u_n\alpha)$

Par récurrence, à l'étape n+1 :

nombre de petits arcs = nombre de grands arcs de l'étape antérieure

$= u_{n+1}$

nombre de grands arcs = nombre de petits arcs + nombre de grands arcs de l'étape antérieure = $u_{n+1} + u_n = u_{n+2}$.

Valeur des grands arcs : $(-1)^n(u_{n+1}\alpha - u_{n-1}) = (-1)^{n+1}(u_{n-1} - u_{n+1}\alpha)$

Valeur des petits arcs : $\dfrac{1 - u_{n+2}(-1)^{n+1}(u_{n-1} - u_{n+1}\alpha)}{u_{n+1}}$

$$= (-1)^{n+1}\alpha u_{n+2} + \frac{1 - (-1)^{n+1} u_{n+2}\cdot u_{n-1}}{u_{n+1}}$$

$$= (-1)^{n+1}\alpha u_{n+2} + \frac{1 - (-1)^{n+1}\left[(-1)^{n+1} + u_{n+1}\cdot u_n\right]}{u_{n+1}} = (-1)^{n+1}\alpha u_{n+2} - (-1)^{n+1} u_n$$

$$= (-1)^{n+1}(\alpha u_{n+2} - u_n)$$

Ceci démontre donc les résultats du tableau concernant la n^ième étape. Théoriquement la divergence α, si notre hypothèse se trouve réalisée de façon absolue, doit donc satisfaire aux conditions :

$1 - 2\alpha < \alpha \quad \Longrightarrow \alpha > \frac{1}{3}$

$3\alpha - 1 < 1 - 2\alpha \Longrightarrow \alpha < \frac{2}{5}$

$2 - 5\alpha < 3\alpha - 1 \Longrightarrow \alpha > \frac{3}{8}$

.....

$(-1)^n(u_{n+1}\alpha - u_n) < (-1)^n(u_{n-2} - u_n\alpha) \Longrightarrow \alpha < \dfrac{u_k}{u_{k+2}}$ indices pairs

$\alpha > \dfrac{u_k}{u_{k+2}}$ indices impairs

$$\Rightarrow \frac{u_1}{u_3} < \frac{u_3}{u_5} < \frac{u_5}{u_7} < \ldots\ldots < \alpha < \ldots\ldots \frac{u_4}{u_6} < \frac{u_2}{u_4} < \frac{u_0}{u_2}$$

$\Rightarrow$ $\alpha = \Psi = \frac{1}{\Phi^2}$ (puisque les fractions sont les réduites de Ψ).

$\Rightarrow$ La divergence idéale serait $\alpha = \Psi = \frac{1}{\Phi^2}$ où Φ est le nombre d'or.

On trouve $\Psi = \frac{1}{\left(\frac{1+\sqrt{5}}{2}\right)^2} = \frac{3-\sqrt{5}}{2} \simeq 0{,}381966.$

Le nombre Ψ est irrationnel, or les divergences sont des fractions. Mais les valeurs rencontrées dans la nature ne sont autres que les réduites de Ψ c'est-à-dire de toutes les fractions celles qui approchent le mieux la valeur idéale $\alpha = \frac{1}{\Phi^2}$.

Il est curieux aussi de constater que les premières réduites (celles où l'approximation est la moins bonne) se rencontrent surtout sur les tiges à feuilles largement espacées. Par contre pour les plantes à feuilles (ou grains) serrées on rencontre des réduites d'un ordre plus élevé.

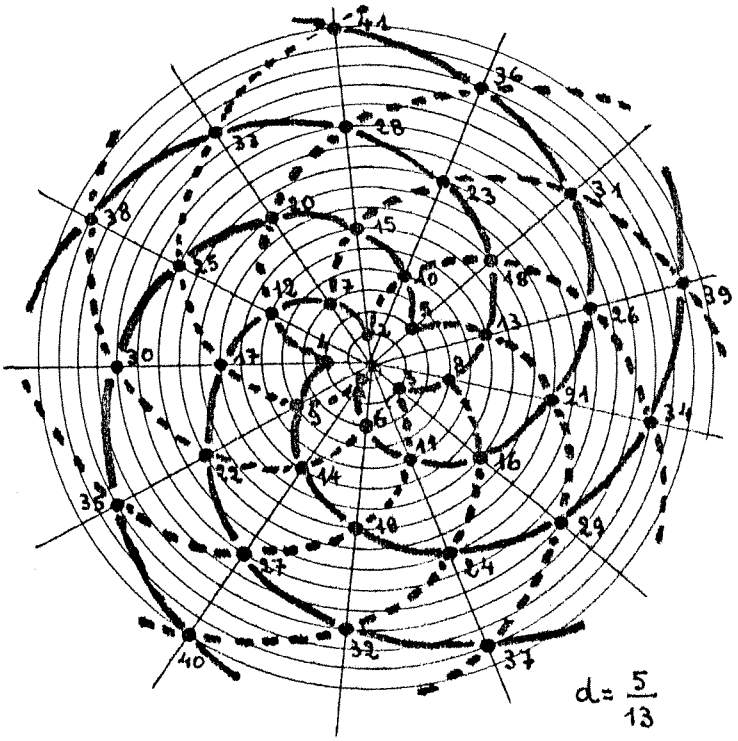
Ex. si $d = \frac{5}{13}$ (artichaut, épicéa) l'approximation est inférieure à 1° ce qui est remarquable compte-tenu de la grosseur des feuilles.

Pour $d = \frac{89}{233}$ (certaines fleurs de tournesol) la précision est de l'ordre de 10" ce qui est vraiment stupéfiant !

2) Le nombre de spirales

Lorsque $d = \frac{u_n}{u_{n+2}}$ les points sont tous placés sur l'un des u_{n+2} rayons. Lorsque le point k est situé sur un rayon x le point k+1 est situé sur le rayon $x + u_n \pmod{u_{n+2}}$. On peut faire passer un grand nombre de spirales par les points mais les seules qui soient vraiment apparentes sont celles qui joignent les points situés sur des rayons consécutifs.

Cherchons donc h tel que k et k + h soient situés sur deux rayons consécutifs. Il en sera alors de même pour k' et k' + h.



Cela conduit à l'une des équations :

$$h \times u_n \equiv 1 \pmod{u_{n+2}} \quad \text{ou} \quad h \times u_n \equiv -1 \pmod{u_{n+2}}$$

ou encore

$$\begin{cases} h \times u_n - p\, u_{n+2} = 1 & (1) \\ h \times u_n - p\, u_{n+2} = -1 & (2) \end{cases}$$ (équations diophantiennes linéaires)

Les relations suivantes (cf. § III) nous donnent une solution :

$$u_n^2 - u_{n-2} \cdot u_{n+2} = (-1)^{n+1}$$

$$u_{n+1} \cdot u_n - u_{n-1} \cdot u_{n+2} = (-1)^n$$

Comme l'inconnue h seule nous intéresse nous voyons que

$h = u_n$ est solution de l'une des équations (1) ou (2),

$h = u_{n+1}$ est solution de l'autre.

La solution générale étant $h = u_n + l\, u_{n+2}$ (l entier)

dans un cas et $h = u_{n+1} + l'\, u_{n+2}$ dans l'autre,

on s'aperçoit que les plus petites solutions positives sont $h = u_n$ et $h = u_{n+1}$ puisque $u_n < u_{n+2}$ et $u_{n+1} < u_{n+2}$.

a) Si $h = u_n$ les points $1,\ 1 + u_n,\ 1 + 2u_n$ ..... sont sur une spirale

$2,\ 2 + u_n,\ 2 + 2u_n$ ..... sont sur une 2° spirale

$\vdots$

$u_n,\ 2u_n,\ 3u_n \cdots$ sont sur une spirale.

Il y a donc autant de spirales qu'il y a des classes résiduelles modulo u_n c'est-à-dire u_n.

b) Si $h = u_{n+1}$ il y a de la même façon u_{n+1} spirales.

Comme le 2° membre des équations (1) et (2) est tantôt 1 tantôt -1 les spirales a) sont tournées dans un sens et les spirales b) dans l'autre.

La figure ci-dessus nous donne une illustration dans le cas où $d = \frac{5}{13}$.

Nous n'avons abordé que quelques aspects du problème de la phyllotaxie. Ces quelques exemples nous font néanmoins comprendre que la morphologie des êtres vivants est soumise à de véritables lois mathématiques comparables à celles de la physique.

F. Stoltz

Multiplions-nous !

La notion de groupe ne figure plus aux programmes 1978 pour les classes de 4° et 3°. C'est un fait, et mon but n'est pas de porter un jugement. S'il est vrai qu'on a souvent demandé aux élèves un niveau d'abstraction de la structure dont ils n'étaient pas capables, on risque maintenant de tomber dans l'excès contraire. A la fin du premier cycle, les élèves n'auront jamais opéré avec d'autres êtres mathématiques que les nombres et auront (à bon droit) l'idée que les propriétés des opérations sont tout à fait générales. Or chacun sait que tous les ensembles n'ont pas une structure de corps totalement ordonné.

Il est vrai que rien n'empêche de considérer les opérations ensemblistes ou la composition des applications dans la même optique. Mais on se heurtera très vite au problème de l'abstraction. C'est pourquoi je suggère une activité qui a provoqué l'enthousiasme de ma classe de 4° et qui a eu des retombées bénéfiques sur d'autres points du programme. Il s'agit d'une étude de l'anneau $\mathbb{Z}/24\mathbb{Z}$, dont l'originalité est de réduire le plus possible l'abstraction.

Le principe est très simple: donner à la classe une structure d'anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Evidemment, les résultats pratiques sont plus ou moins intéressants suivant les valeurs de n. Ma classe de 4° ayant 23 élèves, nous avons ajouté un élève imaginaire: $\mathbb{Z}/24\mathbb{Z}$ a des propriétés plus étonnantes que $\mathbb{Z}/23\mathbb{Z}$ qui est un corps. Cette adjonction n'a troublé personne.

Tout le travail a été effectué en fait sur les classes d'équivalences, mais aussitôt transposé par isomorphisme à la classe elle-même. Evidemment, on n'a jamais prononcé le mot de classe d'équivalence, et l'ensemble a été noté: $\mathbb{Z}_{24} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23\}$.

Les opérations d'addition et de multiplication ont été définies ainsi: pour multiplier deux éléments de $\mathbb{Z}_{24}$, on fait leur produit en tant que nombres entiers, puis on retranche autant de fois 24 qu'il est nécessaire pour obtenir un résultat compris entre 0 et 23. Il m'est apparu que cette phrase était plus accessible que "rechercher le reste de la division par 24". Idem pour l'addition. Remarque: les tables gagnent à être faites à la maison: elles sont très longues (576 cases chacune), et les élèves les remplissent sans méthode, même lorsqu'ils ont constaté des moyens d'abréger le calcul. Elles sont données en annexe.

Il suffit ensuite d'attribuer un numéro à chaque élève pour obtenir l'isomorphisme. Pour fixer les idées, je donne l'exemple de mes élèves:

0: Raymond;	1: Martine;	2: Dominique;
3: Encarnacion;	4: Evelyne;	5: Nathalie;
6: Marie-Line;	7: Corine;	8: Sylvie;
9: Patricia;	10: Gilles;	11: Christine;
12: Catherine;	13: Sophie;	14: Christian;
15: Astride;	16: Paule;	17: Sandrine;
18: Dietmar;	19: Antonia;	20: Brigitte;
21: Frédéric;	22: Christophe;	23: Marielle.

Sitôt prêtes les tables, les élèves ont commencé à s'additionner et à se "multiplier". Ainsi, on remarque que Gilles + Christophe = Sylvie, que Astride + Patricia = Raymond, que Antonia x Dietmar = Marie-Line, etc... Toutefois, il est certain que les élèves se lassent assez vite si on ne leur propose pas du nouveau; faire ce travail pour en rester là serait un peu stérile. C'est pourquoi je vous propose quelques pistes que j'ai expérimentées avec mes élèves; la plupart se généralisent bien à un nombre quelconque d'élèves; pour la clarté de l'exposé,

je resterai dans le cadre de $\mathbb{Z}/24\mathbb{Z}$.

1. Propriétés de l'addition.

$(\mathbb{Z}/24\mathbb{Z}, +)$ est un groupe abélien, d'élément neutre $\overline{0}$; l'opposé de $\overline{n}$ est $\overline{24-n}$. Après isomorphisme, (C, +) est donc aussi un groupe abélien, dont l'élément neutre est Raymond (qu'un élève a proposé d'écrire Raymond, sans aucune allusion). Chacun s'est amusé à chercher son opposé, ce qui a parfois déclenché d'homériques fous-rires, surtout quand un garçon découvre être l'opposé d'une fille qu'il drague ouvertement dans la cour du collège... La structure additive étant "sans surprises", il ne me paraît pas indispensable d'insister beaucoup plus.

2. Propriétés de la multiplication.

On repère très vite l'élément neutre (Martine), l'élément absorbant (Raymond), la commutativité. Inutile d'insister sur l'associativité ni sur la distributivité de la multiplication par rapport à l'addition, qu'on suppose vraies sans démonstration.

L'intérêt est ici dans la présence de nombreux diviseurs de 0. A vrai dire, ce fait n'a pas paru surprendre outre mesure les élèves; ils en ont pourtant remarqué les effets néfastes: Gilles x Marie-Line = Gilles x Dietmar = Catherine: la régularité n'est pas au rendez-vous.

Il y a 8 nombres inversibles: dans ce cas particulier, ils sont leurs propres inverses (car si p est premier avec 6, p^2 est congru à 1 modulo 24). Les élèves inversibles sont donc Martine, Nathalie, Corine, Christine, Sophie, Sandrine, Antonia et Marielle (c'est un hasard s'il n'y a que des filles). Il est facile de constater qu'ils forment un sous-ensemble stable pour la multiplication, dont la table d'opération est la suivante:

	1	5	7	11	13	17	19	23
1	1	5	7	11	13	17	19	23
5	5	1	11	7	17	13	23	19
7	7	11	1	5	19	23	13	17
11	11	7	5	1	23	19	17	13
13	13	17	19	23	1	5	7	11
17	17	13	23	19	5	1	11	7
19	19	23	13	17	7	11	1	5
23	23	19	17	13	11	7	5	1

Il s'agit du groupe de Klein à 8 éléments, dont on aura d'autres exemples avec l'ensemble $(\mathbb{Z}/2\mathbb{Z})^3$, muni de l'addition (la table d'addition de cet ensemble est facile à réaliser) ou avec l'ensemble des parties d'un ensemble de trois éléments muni de la différence symétrique.

S'il ne pose pas de problème aux élèves de chercher leurs opposés dans la table d'addition, il leur est plus difficile de repérer les nombres inversibles en cherchant les 1 dans la table de multiplication. Par contre, la présence des 0 au milieu de la table est rapidement repérée.

3. Relation d'ordre.

Je n'ai pas abordé cet aspect en classe. On pourrait considérer plusieurs types de relations; le classement n'a aucune chance d'être compatible avec les opérations (et comme je n'en fais pas, c'était de toutes façons exclu); une inégalité naturelle est le classement à partir des numéros; mais il n'est pas non plus totalement compatible: par exemple, Catherine (12) est inférieure à Frédéric (21), mais Catherine + Corine (12 + 7) est supérieur à Frédéric + Corine (21 + 7). De plus, établir une telle relation nécessiterait un choix de vocabulaire soigné (il pourrait être déplaisant de dire que tel élève est "supérieur" ou "avant" tel autre).

4. Valeur absolue.

Piste inexplorée aussi. Même si on ne parle pas de relation d'ordre, on peut dire que deux élèves ont même valeur absolue s'ils sont opposés. La valeur absolue aurait par contre davantage d'intérêt dans un corps.

5. Puissances.

Il est très facile de calculer les puissances successives des élèves. Elles déclenchent également pas mal de fous-rires, par exemple quand un garçon constate que son carré est une fille. On remarque vite que certains éléments jouent un rôle important et que la plupart des puissances sont rapidement cycliques. En particulier, les huit inversibles ont comme carré l'élément neutre (Martine); donc, si a est inversible, on a:

$$a^{2n} = \text{Martine}; \quad a^{2n+1} = a .$$

De plus, si a est divible par 6, son carré est donc divisible par 36: il est donc égal à Raymond ou à Catherine; la puissance 4 sera automatiquement égale à Raymond. On obtient le tableau suivant:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
0	-	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	...
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	...
2	1	2	4	8	16	8	16	8	16	8	16	8	16	8	16	8	...
3	1	3	9	3	9	3	9	3	9	3	9	3	9	3	9	3	...
4	1	4	16	16	16	16	16	16	16	16	16	16	16	16	16	16	...
5	1	5	1	5	1	5	1	5	1	5	1	5	1	5	1	5	...
6	1	6	12	0	0	0	0	0	0	0	0	0	0	0	0	0	...
7	1	7	1	7	1	7	1	7	1	7	1	7	1	7	1	7	...
8	1	8	16	8	16	8	16	8	16	8	16	8	16	8	16	8	...
9	1	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	...
10	1	10	4	16	16	16	16	16	16	16	16	16	16	16	16	16	...
11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	...
12	1	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	...
13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	...
14	1	14	4	8	16	8	16	8	16	8	16	8	16	8	16	8	...
15	1	15	9	15	9	15	9	15	9	15	9	15	9	15	9	15	...
16	1	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	...
17	1	17	1	17	1	17	1	17	1	17	1	17	1	17	1	17	...
18	1	18	12	0	0	0	0	0	0	0	0	0	0	0	0	0	...
19	1	19	1	19	1	19	1	19	1	19	1	19	1	19	1	19	...
20	1	20	16	8	16	8	16	8	16	8	16	8	16	8	16	8	...
21	1	21	9	21	9	21	9	21	9	21	9	21	9	21	9	21	...
22	1	22	4	16	16	16	16	16	16	16	16	16	16	16	16	16	...
23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	...

On remarque sur ce tableau un certain nombre de relations (auxquelles les élèves ne pensent pas seuls), comme par exemple:

$$a^{2n} = (-a)^{2n} \quad ; \qquad (-a)^{2n+1} = -(a^{2n+1}) \quad .$$

On remarque également que les seuls carrés sont 0, 1, 4, 9, 16, comme on pouvait s'y attendre,et 12. Il y a trois éléments nilpotents (6 = Marie-Line, 12 = Catherine et 18 = Dietmar), et quatre éléments idempotents (0 = Raymond, 1 = Martine,

9 = Patricia et 16 = Paule). Enfin, les éléments 2 (Dominique), 4 (Evelyne), 6 (Marie-Line), 10 (Gilles), 12 (Catherine), 14 (Christian), 18 (Dietmar), 20 (Brigitte) et 22 (Christophe) ne peuvent être candidats à une puissance supérieure à 3. Les élèves "impairs" sont donc en général "plus puissants" que les élèves "pairs".

6. Racines carrées.

Même en quatrième, il est très facile d'envisager le problème inverse du précédent; tout raisonnement est inutile, il suffit de regarder la table de multiplication. On a déjà constaté que les seuls nombres qui possèdent une racine carrée sont 0, 1, 4, 9, 12 et 16. Toutefois, il y a de notables différences par rapport à ce qui se passe dans $\mathbb{R}$:

- 0 a deux racines carrées: 0 et 12.
- 1 a huit racines carrées, opposées deux à deux, et qui sont les huit éléments inversibles.
- 4 a quatre racines carrées, opposées deux à deux: 2 et 22, 10 et 14.
- 9 a quatre racines carrées, opposées deux à deux: 3 et 21, 9 et 15.
- 12 a deux racines carrées opposées, 6 et 18.
- 16 a quatre racines carrées opposées deux à deux: 4 et 20, 8 et 16.

7. Sous-structures.

On atteint ici un niveau d'abstraction qui risque de poser quelques problèmes. Il est certain qu'on ne peut parler de "sous-groupe" ou de "partie engendrée" par un élément, encore-moins de sous-anneau ou d'idéal. Toutefois, une petite incursion dans ce domaine m'a montré que l'aspect numérique restait abordable, et que l'aspect jeu motivait les petites recherches nécessaires.

Voici les sous-groupes additifs de la classe engendrés par les éléments:

<Raymond> = {Raymond} ;

Martine, Nathalie, Corine, Christian, Sophie, Sandrine, Antonia et Marielle, qui sont inversibles, engendrent toute la classe (une telle phrase est susceptible de faire de l'effet sur une classe!)

<Dominique> = {Raymond, Dominique, Evelyne, Marie-Line, Sylvie, Gilles, Catherine, Christian, Paule, Dietmar, Brigitte, Christophe} (sous-groupe isomorphe à $\mathbb{Z}/12\mathbb{Z}$).

<Encarnacion> = {Raymond, Encarnacion, Marie-Line, Patricia, Catherine, Astride, Dietmar, Frédéric} (sous-groupe isomorphe à $\mathbb{Z}/8\mathbb{Z}$).

<Evelyne> = {Raymond, Evelyne, Sylvie, Catherine, Paula, Brigitte} (sous-groupe isomorphe à $\mathbb{Z}/6\mathbb{Z}$).

<Marie-Line> = {Raymond, Marie-Line, Catherine, Dietmar} (sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}$)

<Sylvie> = {Raymond, Sylvie, Paule} (sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z}$).

<Catherine> = {Raymond, Catherine}. (sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$)

Les sous-groupes engendrés par Gilles, Christian, Astride, Paule, Dietmar, Brigitte, Frédéric et Christophe, sont déjà écrits; le lecteur les reconnaîtra aisément parmi les sous-groupes ci-dessus.

La structure de groupe attachée à ces sous-ensembles est évidente. Je n'ai pas jugé bon de pousser le détail à ce sujet trop loin en classe.

Il est facile de se convaincre que l'on a obtenu ainsi tous les ensembles stables par l'addition.

On sait que tous ces sous-ensembles seront aussi des sous-anneaux et même des idéaux. On peut par contre rechercher lesquels ont une structure de corps.

Il n'est pas inintéressant de s'intéresser de plus près aux structures multiplicatives de ces ensembles, en particulier à cause des nombreux diviseurs de zéro qu'ils contiennent. Ils fournissent en effet l'un ou l'autre cas pathologique.

Notons pour commencer qu'un idéal contenant Catherine (dont le carré est égal à Raymond, c'est-à-dire nul), n'a aucune chance d'avoir une structure de corps. L'idéal engendré par Sylvie est donc le seul candidat acceptable. Voici sa table de multiplication:

$<$ Sylvie$>$ = {Raymond, Sylvie, Paule}.

$<8>$ = {0, 8, 16}

	0	8	16
0	0	0	0
8	0	16	8
16	0	8	16

On remarque que 16 est élément neutre, que 8 est son propre symétrique: l'idéal engendré par Sylvie est bien un corps isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Voilà un exemple d'une sous-structure dont l'élément neutre n'est pas celui de la structure initiale.

L'idéal engendré par Catherine donne un exemple d'ensemble dans lequel tous les produits sont nuls. Celui engendré par Marie-Line et celui engendré par Evelyne sont des exemples d'ensembles sans élément neutre, mais possédant en revanche deux éléments absorbants:

$<$Marie-Line$>$ = {Raymond, Marie-Line, Catherine, Dietmar}.

$<6>$ = {0, 6, 12, 18}

	0	6	12	18
0	0	0	0	0
6	0	12	0	12
12	0	0	0	0
18	0	0	0	0

$<4>$ = {0, 4, 8, 12, 16, 20}.

	0	4	8	12	16	20
0	0	0	0	0	0	0
4	0	16	8	0	16	8
8	0	8	16	0	8	16
12	0	0	0	0	0	0
16	0	16	8	0	16	8
20	0	8	16	0	8	16

$<$Evelyne$>$ = {Raymond, Evelyne, Sylvie, Catherine, Paule, Brigitte.}

L'idéal engendré par Dominique possède la même propriété.

On peut aussi s'intéresser aux sous-ensembles multiplicatifs engendrés par chaque élément. Mis à part les éléments 0 et 1, on obtient:

(Dominique) = {Dominique, Evelyne, Sylvie, Paule}.

(Encarnacion) = {Encarnacion, Patricia}.

(Marie-Line) = {Raymond, Marie-Line, Catherine}.

(Sylvie) = {Sylvie, Paule}.

(Gilles) = {Evelyne, Gilles, Paule}.

(Catherine) = {Raymond, Catherine}.

(Christian) = {Evelyne, Sylvie, Christian, Paule.}

(Astride) = {Patricia, Astride}.

(Dietmar) = {Raymond, Catherine, Dietmar}.

(Brigitte) = {Sylvie, Paule, Brigitte}.

(Frédéric) = {Patricia, Frédéric}.

(Christophe) = {Evelyne, Paule, Christophe.}

Les quatre éléments idempotents (Raymond, Martine, Patricia et Paule) n'engendrent pas

d'autre élément; les huit éléments inversibles engendrent un sous ensemble qui contient, en plus d'eux, l'unité (Martine).

De ces sous-ensembles, seul (Catherine) est stable par addition.

8. Divisibilité.

On peut chercher les ensembles de "multiples" d'un élève donné. On aura reconnu la recherche précédente des sous-ensembles stables par addition. Ici encore, la recherche effectuée sur les nombres est motivée par les résultats transposés à la classe. Il ne fait ni chaud ni froid de savoir que 4 est un multiple de 2 ou que 7 divise 6 (quoique ce dernier résultat n'ait rien d'évident a priori). Il est par contre fort amusant de dire que Evelyne est un multiple de Dominique et que Corine divise Marie-Line.

Nous avons vu que les élèves inversibles engendrent toute la classe: tout élève est donc leur multiple; un élève inversible divise donc tout élève, ce qui implique qu'il faudra revoir une éventuelle définition d'"élèves premiers": tout élève a au moins huit diviseurs.

Dire que a divise b, c'est dire que $< a >$ contient $< b >$. Mis à part les éléments inversibles et eux-mêmes, voici les diviseurs de chaque élève:

- Raymond est divisible par tout élève;
- Martine, de même que les élèves inversibles, n'est divisible par personne d'autre. Remarquer que le résultat est aussi vrai dans $\mathbb{Z}$, où les éléments inversibles 1 et -1 ne sont divisibles que par eux mêmes, et ne doivent pas être considérés comme premiers pour sauvegarder l'unicité de la factorisation en nombres premiers.
- Dominique, Gilles, Christian, Christophe (2, 10, 14, 22), ainsi que Encarnacion, Astride et Frédéric (3, 15, 21), ne sont divisibles que par eux-mêmes et par les élèves inversibles: on pourra les considérer comme des "élèves premiers".
- Evelyne (4) est divisible par Dominique, Gilles, Christian et Christophe.
- Sylvie (8) est divisible par les précédents et par Evelyne et Brigitte.
- Paule (16) est divisible par les précédents et par Sylvie.
- Brigitte (20) a les mêmes diviseurs qu'Evelyne.
- Marie-Line (6) est divisible par Dominique, Gilles, Christian, Christophe, Encarnacion, Astride et Frédéric, ainsi que par Patricia et Dietmar.
- Patricia (9) et Dietmar (18) ont les mêmes diviseurs qu'Encarnacion.
- Enfin, Catherine (12) est divisible par tout élève, sauf par Raymond, Sylvie et Paule.

Comme on l'a dit, on pourra appeler élève premier tout élève qui n'est divisible que par lui-même et par les nombres inversibles, à condition qu'il ne soit pas inversible. On peut alors se poser le problème de la décomposition en produit de facteurs premiers, qui ne sera de toutes façons unique qu'au produit par le carré d'un élève inversible près; mais on s'assure rapidement qu'il n'y a aucun espoir d'unicité même à ce prix. Par exemple:

Evelyne = Dominique^2 = Gilles^2 = Christian^2 = Christophe^2.

On se convainc rapidement que les 8 élèves non premiers et non inversibles ont au moins une décomposition en produit de facteurs premiers:

Evelyne = Dominique^2 ; Marie-Line = Dominique x Encarnacion ;

Sylvie = Dominique^3 ; Patricia = Encarnacion^2 ; Paule = Dominique^4 ;

Catherine = Dominique^2 x Encarnacion ; Dietmar = Dominique x Encarnacion^2 ;

Brigitte = Dominique x Gilles.

On pourra éventuellement chercher pour chaque élève toutes ses factorisations premières (exception faite des modifications apportées par les élèves inversibles).

Cette absence d'unicité de la factorisation première rend illusoire des recherches de PGCD ou de PPCM; aussi ne m'y suis-je pas aventuré avec les élèves. L'absence de relation d'ordre naturelle compatible avec la structure d'anneau est ici relayée par la relation d'inclusion des sous-ensembles engendrés par les éléments. A titre d'exemple, Sylvie (8) et Catherine (12) admettent comme PGCD Evelyne et Brigitte, si l'on excepte les élèves inversibles. La confusion ici risque d'être préjudiciable à la recherche.

9. Polynômes.

Il est bien sûr possible de construire à partir de l'anneau (C,+,x) un anneau de polynomes (ou de fonctions polynomes); les calculs seront effectués dans $\mathbb{Z}/24\mathbb{Z}[x]$ et leurs résultats transportés dans C[x]. L'expérience m'a prouvé que le temps passé à additionner ou à multiplier de tels polynomes n'a pas été du temps perdu: l'apprentissage des opérations sur les polynomes de $\mathbb{R}[x]$ a été grandement facilité; encore une fois, la référence à la classe a été très motivante pour une recherche dont les principes étaient les mêmes que ceux que les élèves ont à connaître mais amènent d'autres résultats. On objectera que les polynomes ne sont plus au programme du premier cycle; cela ne me paraît pas être une raison suffisante de les négliger.

J'ai distingué polynomes (suites d'éléments de C nulles à partir d'un certain rang) et fonctions polynomes (fonctions associées à ces suites), tout d'abord parce que j'ai constaté que l'apprentissage du mécanisme des opérations est facilité sur les polynomes et étendu ensuite sans difficultés aux fonctions, ensuite parce que si la confusion est sans danger dans $\mathbb{R}[x]$, il n'en est pas de même dans C[x]: un polynome peut ne pas avoir même degré que la fonction polynome associée, du fait de la non-intégrité de l'anneau C.

On a ainsi choisi quelques polynomes, dont on a calculé les valeurs, c'est-à-dire les images par la fonction polynome associée pour quelques éléments de C. Par exemple:

f = (Dietmar, Catherine, Brigitte, Sandrine, Raymond, ...)

$f(x)$ = Dietmar + Catherine . x + Brigitte . x^2 + Sandrine . x^3

f(Raymond) = Dietmar ;

f(Dominique) = Dietmar + Catherine.Dominique + Brigitte.Dominique^2
+ Sandrine.Dominique^3 = Dietmar + Catherine.Dominique
+ Brigitte.Evelyne + Sandrine.Sylvie = Dietmar + Raymond + Sylvie
+ Paule = Dietmar.

On constate ici que Raymond et Dominique ont la même image qui est Dietmar.

f(Corine) = Dietmar + Catherine.Corine + Brigitte.Corine^2 + Sandrine.Corine^3
= Dietmar + Catherine.Corine + Brigitte.Martine + Sandrine.Corine
= Dietmar + Catherine + Brigitte + Marielle = Martine.

Il est assez facile de constater que ce polynome de degré 3 n'a pas de racine (car $20x^2 + 17x^3$ n'est jamais congru à 6 modulo 24). On peut donc aussi essayer de trouver des polynomes ayant un nombre de racines supérieur au degré, voire des polynomes non nuls tels que la fonction associée soit identiquement nulle ou des polynomes distincts tels que les fonctions associées soient égales. Ici, la recherche ne peut pas être faite par les élèves et n'est que prétexte à calcul; mais ce calcul se fait dans le cadre motivant de l'application à la classe.

Ainsi, il est tout à fait clair que le polynome (0,12,12,0...) de degré 2 est associé à la fonction polynome $12x^2 + 12x$, qui est identiquement nulle. Ce fait apparaît très vite aux bon élèves, qui n'ont besoin que de quelques essais pour le démontrer (si x est pair, x^2 est pair, 12a est nul; si x est impair, x^2 l'est aussi, 12a=12, et 12+12=0). Mais on peut proposer d'autres exemples moins évidents et qui pourront être à l'origine de calculs numériques.

On pourra ainsi s'assurer que le polynome de dégré 4:

(Raymond, Dominique, Christine, Gilles, Martine, Raymond...)

est associé à la fonction polynome:

$\text{Martine}.x^4 + \text{Gilles}.x^3 + \text{Christine}.x^2 + \text{Dominique}.x + \text{Raymond}$

qui est identiquement nulle. Evidemment, les calculs sont faits sur la fonction polynome correspondante de $\mathbb{Z}/24\mathbb{Z}$, en utilisant les tables d'opération, ou en faisant le calcul dans $\mathbb{Z}$, en constatant après coup que le résultat est divisible par 24. On peut trouver d'autres exemples, en remplaçant des coefficients par leurs opposés. Ainsi, le polynome:

$\text{Martine}.x^4 - \text{Christian}.x^3 - \text{Sophie}.x^2 + \text{Dominique}.x + \text{Raymond}$

est égal au précédent. On pourra obtenir d'autres polynomes de degré 4 associés à la fonction nulle:
le polynome $ax^4 + bx^3 + cx^2 + dx + e$ est de ce type si les conditions suivantes sont réalisées:

$e = 0$; b et d pairs ; $c + \frac{d}{2}$ pair ; $2a + b$ et $2a + d$ multiples de 4 ; $a + c$ et $b + d$ congrus à 12 modulo 24.

Bien sûr, toutes les classes ne saisiront pas la différence qu'il peut y avoir entre polynome et fonction polynome. Même s'il n'est pas possible d'insister dans ce domaine, il ne me semble pas inutile qu'ils aient rencontré des cas où tout ne se passe pas aussi joliment que dans $\mathbb{R}$.

On peut aussi s'intéresser aux racines d'un polynome. C'est souvent un travail long, si on choisit le polynom e au hasard, mais les élèves le font pour le but ultime de la conversion des résultats chiffrés en résultats-élèves. On peut aussi choisir des cas plus simples, comme par exemple (Raymond, Raymond, Sylvie, Encarnacion, Raymond...) qui dans $\mathbb{Z}/24\mathbb{Z}$ s'écrit (0, 0, 6, 3, 0...) et sous forme de fonction:

dans C: $\text{Encarnacion}.x^3 + \text{Sylvie}.x^2$

dans $\mathbb{Z}/24\mathbb{Z}$: $3x^3 + 6x^2$

Ce polynome de degré 3 admet 12 racines, tous les multiples de 2.

Pour une telle recherche, il est évidemment plus agréable de choisir un polynome ayant de nombreuses racines:chaque nouvelle découverte est un facteur de motivation pour la suite de la recherche; il peut aussi être intéressant de choisir un exemple où une méthode générale donne le résultat: certains bons élèves cherchent une telle méthode après quelques essais; on peut aussi choisir dans cette optique une fonction paire ou impaire.

10. Identités remarquables.

On sait qu'on a ici: $(a + b)^{24} = a^{24} + b^{24}$. Toutefois, une telle relation est trop difficile à démontrer en 4e. Il ne manque pas non plus d'exemples où $(a + b)^2 = a^2 + b^2$. Mais le terrain m'a paru mouvant, car trop d'élèves restent persuadés de la généralité d'une telle relation pour qu'on aille leur en montrer des exemples. J'ai donc renoncé à une incursion dans ce domaine, me contentant de faire effectuer des produits et des sommes de polynomes. Rien n'empêche de donner des exemples où les produits sont nuls, l'anneau $\mathbb{C}[x]$ n'étant pas plus intègre que C. On pourra inventer de nombreux exemples dont le produit est "directement" nul (par exemple:

$(6x^2 + 12x + 6)(4x^2 + 16x + 8) = 0$, car tous les produits de coefficients sont nuls). Plus intéressant, on vérifiera par exemple que:
$(x^2 + 3x + 2)(x^2 + 7x + 12) = x^4 + 10x^3 + 11x^2 + 2x$ (polynome associé à la fonction nulle, voir ci-dessus). En général, on a:
$C_n^p = \frac{n(n-1)\ldots(n-p+1)}{p(p-1)\ldots 2.1}$; en particulier: $C_n^4 = \frac{n(n-1)(n-2)(n-3)}{24}$; le produit de 4 nombres consécutifs est divisible par 24. Donc, le produit des polynomes $(x + a)(x + a + 1)(x + a + 2)(x + a + 3)$ est donc un polynome de degré 4 associé à la fonction polynome nulle.

11. Equations.

Si on maîtrise bien les polynomes, on peut résoudre de nombreuses équations de degré supérieur ou égal à 1. Nous l'avons fait sans le dire dans bien des cas. On constatera qu'une équation de degré n n'a pas forcément n solutions. Par exemple, l'équation de degré 4 :

$$(x + 5)(x + 6)(x + 7)(x + 8) = (x + 15)(x + 16)(x + 17)(x + 18)$$

est indéterminée et vérifiée quel que soit x dans $\mathbb{Z}/24\mathbb{Z}$. Au contraire, l'équation du premier degré $6x + 17 = 0$ n'a aucune solution.

Ici encore, tous les calculs sont faits dans $\mathbb{Z}/24\mathbb{Z}$, mais l'énoncé du problème et des résultats dans C éveille largement l'intérêt des élèves.

Les exemples ne manqueront pas suivant le résultat cherché, même si on se borne au premier degré.

12. ...

On peut sûrement trouver bien d'autres activités en partant de l'anneau $\mathbb{Z}/n\mathbb{Z}$, en établissant un isomorphisme avec une classe... Mon but n'était pas de refaire ici la théorie des anneaux ni de dresser une liste complète. Je serais heureux que des collègues complètent la liste de ces activités. Je me suis volontairement borné aux études faites en classe. Comme je l'ai déjà dit, les élèves les ont fort bien accueillies, sans doute à cause de leur aspect inhabituel; il m'a semblé que certains se sentaient plus impliqués à partir du moment où ils travaillaient "sur eux-mêmes". Il se trouvera peut-être un psychologue pour me dire que c'était une opération néfaste, mais tant pis: ils ont effectué sans rechigner des calculs que je n'aurais peut-être pas osé leur imposer dans le cadre traditionnel, et l'entraînement qu'ils ont ainsi effectué a eu des effets bénéfiques par la suite. Tant pis si on juge que ce type d'activité est un peu artificiel. Les élèves, eux, en ont redemandé.

Depuis toujours, j'essaye d'introduire une étude sur les groupes cycliques en 4°, avec par exemple $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/6\mathbb{Z}$. Les élèves réagissent toujours en blasés qui ne s'étonnent de rien (en math, tout est possible!). C'est la première fois que je les vois s'intéresser ainsi à un problème sortant de l'ordinaire. Pour que l'information soit complète, j'ajouterai que la classe de 4° est très moyenne (voire même faible, à cinq ou six exceptions près), mais que personne ne s'est trouvé à la traîne. Enfin, un début d'étude a été également fait en 3°, où il avait été également très bien accueilli, mais n'a pu être développé faute de temps.

On pourra objecter qu'il est inutile que des élèves de 4° aient déjà rencontré des "cas pathologiques" et qu'ils ont assez de mal à assimiler les résultats obtenus dans $\mathbb{R}$. Je ne partage pas cette opinion; une vue un peu plus globale des choses ne me paraît pas contradictoire avec un apprentissage correct, et il est bon de mettre un frein à une faculté de généralisation galopante qui aura tôt fait de régler tous les problèmes avec l'unique machine qu'ils connaissent. Il me paraît bon au contraire qu'ils soient conscients très tôt qu'il n'y a pas de méthode générale. Même les structures n'auront pas tout unifié en mathématiques, et c'est bien heureux!

Alain BONNET

Table d'addition

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
18	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
20	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
21	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
22	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
23	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

Table de multiplication

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2	0	2	4	6	8	10	12	14	16	18	20	22	0	2	4	6	8	10	12	14	16	18	20	22
3	0	3	6	9	12	15	18	21	0	3	6	9	12	15	18	21	0	3	6	9	12	15	18	21
4	0	4	8	12	16	20	0	4	8	12	16	20	0	4	8	12	16	20	0	4	8	12	16	20
5	0	5	10	15	20	1	6	11	16	21	2	7	12	17	22	3	8	13	18	23	4	9	14	19
6	0	6	12	18	0	6	12	18	0	6	12	18	0	6	12	18	0	6	12	18	0	6	12	18
7	0	7	14	21	4	11	18	1	8	15	22	5	12	19	2	9	16	23	6	13	20	3	10	17
8	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16	0	8	16
9	0	9	18	3	12	21	6	15	0	9	18	3	12	21	6	15	0	9	18	3	12	21	6	15
10	0	10	20	6	16	2	12	22	8	18	4	14	0	10	20	6	16	2	12	22	8	18	4	14
11	0	11	22	9	20	7	18	5	16	3	14	1	12	23	10	21	8	19	6	17	4	15	26	13
12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12	0	12
13	0	13	2	15	4	17	6	19	8	21	10	23	12	1	14	3	16	5	18	7	20	9	22	11
14	0	14	4	18	8	22	12	2	16	6	20	10	0	14	4	18	8	22	12	2	16	6	20	10
15	0	15	6	21	12	3	18	9	0	15	6	21	12	3	18	9	0	15	6	21	12	3	18	9
16	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8	0	16	8
17	0	17	10	3	20	13	6	23	16	9	2	19	12	5	22	15	8	1	18	11	4	21	14	7
18	0	18	12	6	0	18	12	6	0	18	12	6	0	18	12	6	0	18	12	6	0	18	12	6
19	0	19	14	9	4	23	18	13	8	3	22	17	12	7	2	21	16	11	6	1	20	15	10	5
20	0	20	16	12	8	4	0	20	16	12	8	4	0	20	16	12	8	4	0	20	16	12	8	4
21	0	21	18	15	12	9	6	3	0	21	18	15	12	9	6	3	0	21	18	15	12	9	6	3
22	0	22	20	18	16	14	12	10	8	6	4	2	0	22	20	18	16	14	12	10	8	6	4	2
23	0	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Transmission de messages secrets grâce à l'arithmétique

(d'après R.L. Rivest, A. Shamir, L. Adleman)

Les discours secrets doivent être regardés comme des pensées.
Voltaire (Pol. et lég. Relat. mort de la Barre)

L'oeuf qui a reçu une quantité appropriée de chaleur se transforme en poussin, mais la chaleur ne peut transformer une pierre en poussin, car leurs bases sont différentes.
Mao Tsé-Toung (De la Contradiction, août 1937, oeuvres choisies, tome I)

I. La notion de système cryptographique à clef publique.

Ce schéma a été introduit par Diffie et Hellman [1] . On considère un ensemble d'individus i, j, k ... qui veulent communiquer entre eux. Mais, lorsque j envoie un message à i , seul i doit pouvoir le déchiffrer.

A chaque individu i correspondent deux procédures, l'une E_i (1) qui est publique, l'autre D_i , secrète, connue seulement de i (en principe !). La liste des procédures E_i figure tout simplement sur un annuaire.

Si l'individu j veut envoyer un message M à l'individu i , il procède ainsi : Il consulte l'annuaire pour trouver la procédure E_i . Il calcule $M' = E_i(M)$ et envoie M' à i . Pour déchiffrer M' , i calcule $D_i(M')$.

Ce schéma est caractérisé par les propriétés suivantes :

a) Décodage : Pour tout i et tout message M, on a $D_i(E_i(M)) = M$. En calculant $D_i(M') = D_i(E_i(M) = M$, i déchiffre le message qui lui est destiné.

b) Simplicité : Le travail de codage et décodage imposé par les procédures E_i et D_i n'est pas trop compliqué.

c) Secret : La connaissance de E_i ne permet pas de découvrir facilement la procédure D_i.

Ainsi, seul i peut déchiffrer le message qui lui est envoyé. Mais un plaisantin ou un individu malveillant peut lui communiquer de fausses nouvelles. Donc, dans de nombreux cas, on souhaite que l'expéditeur du message puisse être identifié avec certitude : le message doit être signé. Ceci est réalisé, de façon élégante, si la propriété suivante a lieu.

d) Signature : On suppose de plus $E_i [D_i(M)] = M$, pour tout i et tout M.

Supposons que j veuille faire parvenir à i un message M "signé". Il calcule $S = D_j(M)$, puis $S' = E_i(S)$. Il envoie S' à i. Alors i calcule $S = D_i(S')$, puis $E_j(S) = E_j [D_j(M)] = M$. (2)

Quiconque a connaissance de S et de M peut se convaincre que l'expéditeur est bien j, en vérifiant la relation $E_j(S) = M$.

Le papier de Diffie et Hellman ne comportait qu'un seul défaut, il ne proposait aucun exemple de telles procédures E_i et D_i. Un tel exemple a été fourni par Rivest, Shamir et Adleman, nous l'étudierons dans un prochain paragraphe.

II. Interlude arithmétique.

Les quelques faits élémentaires suivants nous seront utiles.

LEMME 1. - Soit p un nombre premier. Soit k un entier congru à 1 modulo (p-1). Alors tout entier x vérifie la congruence

$$x^k \equiv x \pmod{p} .$$

> Lorsque p divise x c'est banal, puisque les deux membres sont alors congrus à zéro modulo p. Si p ne divise pas x, le petit théorème de Fermat [2], énoncé en 1640, affirme que l'on a

$$x^{p-1} \equiv 1 \mod p ,$$

donc, comme k est de la forme $\ell(p-1)+1$, on a bien

$$x^k = (x^{p-1})^{\ell} x \equiv x \pmod{p} .<$$

LEMME 2 (Théorème chinois). - Soient a et b deux entiers premiers entre eux, alors il existe un isomorphisme naturel entre les anneaux $\mathbb{Z}_{/ab\mathbb{Z}}$ et $\mathbb{Z}_{/a\mathbb{Z}} \times \mathbb{Z}_{/b\mathbb{Z}}$.

> Ce résultat était connu, au langage près, des astronomes chinois de l'Antiquité. En voici une preuve.

Considérons l'application naturelle

$$\mathbb{Z} \to \mathbb{Z}_{/a\mathbb{Z}} \times \mathbb{Z}_{/b\mathbb{Z}}$$

qui a un entier x fait correspondre le couple $(x \bmod a,\ x \bmod b)$. Du fait que l'on peut ajouter et multiplier des congruences membre à membre, il s'agit d'un homorphisme d'anneaux. Son noyau est constitué par les entiers congrus à zéro modulo a et modulo b, donc par les multiples de ab. D'où un homomorphisme injectif

$$\mathbb{Z}_{/ab} \to \mathbb{Z}_{/a\mathbb{Z}} \times \mathbb{Z}_{/b\mathbb{Z}} .$$

Pour conclure qu'il s'agit en fait d'une bijection, il suffit de noter que les ensembles de départ et d'arrivée comptent tous deux ab éléments. <

THEOREME 1. - Soient $p_1, \ldots, p_\ell$ des nombres premiers distincts et $n = p_1 \cdots p_h$. On pose $\varphi(n) = (p_1 - 1) \ldots (p_h - 1)$. Soit k un entier congru à 1 modulo $\varphi(n)$. Alors, tout entier x vérifie

$$x^k \equiv x \pmod{n} . \qquad (3)$$

>Par application répétée du lemme 2, on voit que les anneaux $\mathbb{Z}_{/n\mathbb{Z}}$ et $\mathbb{Z}_{/p_1\mathbb{Z}} \times \cdots \times \mathbb{Z}_{/p_h\mathbb{Z}}$ sont isomorphes ; par conséquent, il suffit de vérifier que l'on a toujours

$$x^k \equiv x \pmod{p_i} \quad \text{pour} \quad i = 1, \ldots, h .$$

Ces congruences résultent immédiatement du lemme 1.<

III. L'exemple de Rivest-Shamir-Adleman ([4]).

A chaque individu i, associons des entiers e_i, d_i, n_i tels que e_i et n_i figurent dans l'annuaire, tandis que d_i est tenu secret, seul i le connaît. Les messages M envoyés à i sont des entiers modulo n_i (ce qui n'ôte rien à la généralité de cette méthode). Les procédures E_i et D_i sont définies par

$$E_i(M) = M^{e_i} \quad \text{modulo } n_i ,$$
$$D_i(C) = C^{d_i} \quad \text{modulo } n_i .$$

Chaque entier n_i est le produit de deux nombres premiers distincts p_i et q_i. Le choix des entiers d_i et e_i sera précisé plus loin.

Oublions les indices i provisoirement.

1 - Pour réaliser la condition a), il faut que l'on ait

$$D(E(M)) = (M^e)^d = M^{ed} \equiv M \pmod{n} .$$

Le théorème 1 montre que cette condition a lieu lorsque e et d vérifient

$$ed \equiv 1 \pmod{\varphi(n)} , \quad \text{où} \quad \varphi(n) = (p-1)(q-1) .$$

2 - C'est un truc bien connu des informaticiens que le calcul de x^k nécessite au plus $2 \log_2(k)$ multiplications. La preuve formelle est la suivante : on écrit k en base deux,

$$k = \sum_{i=0}^{\ell} \epsilon_i 2^i \quad (\text{avec } \ell \leq \log_2 k) ,$$

et on a

$$x^k = x^{\Sigma \epsilon_i 2^i} = \prod_{i=0}^{\ell} (x^{2^i})^{\epsilon_i} . \qquad (4)$$

Ceci prouve que les temps de calcul de E et D sont polynomiaux en fonction de Log n , donc possibles même pour de très grandes valeurs de n .

3 - La condition c est-elle réalisée ?

On suppose que p et q sont deux grands nombres premiers secrets. On calcule alors $n = p\,q$ et $\varphi(n) = (p-1)(q-1)$. On choisit ensuite un entier d secret,assez grand et premier avec $\varphi(n)$ (il suffit de prendre d premier $> \max\{p, q\}$) . Grâce à l'algorithme d'Euclide du calcul du p. g. c. d de d et $\varphi(n)$, on calcule ensuite e tel que $ed \equiv 1 \mod \varphi(n)$. Le temps de ce calcul est encore polynômial en fonction de Log n . Comme nous l'avons déjà vu, cette congruence assure que la condition a) est vérifiée.

Rappelons que seuls n et e sont publics. Dans ces conditions, comment peut-on trouver d ?

. Si on sait factoriser n , on trouvera p et q , puis $\varphi(n)$ et enfin la clef d en résolvant $ed \equiv 1 \mod \varphi(n)$. Mais - à ce jour - personne

ne sait factoriser rapidement un entier arbitraire. La méthode élémentaire en quelques $\sqrt{n}$ opérations a été améliorée, cependant même avec les meilleures méthodes connues on estime que la factorisation d'un entier de l'ordre de 10^{100} nécessite en général 75 ans de calcul avec les ordinateurs les plus puissants et celle d'un entier de l'ordre de 10^{200} nécessite 4 millions d'années ! On choisit donc p et q supérieurs à 10^{50}.

. La factorisation de n n'est pas nécessaire, il "suffit" de calculer $\varphi(n)$. Mais, c'est aussi difficile que de factoriser n, puisque la connaissance de $\varphi(n) = n-(p+q)+1$ et $n = pq$ permet de retrouver facilement p et q.

. Aucune procédure efficace de résolution de l'équation

$$x^e \equiv a \pmod{n}$$

ne semble connue pour un entier e général.

4 - Du fait que les entiers n_i sont distincts, la condition d) n'est réalisée que dans "la moitié" des cas. En effet, pour $n_j > n_i$, le domaine de définition des fonctions D_j et E_j n'est pas contenu dans celui de E_i et D_i. On trouvera dans [4] deux suggestions simples pour remédier à cet inconvénient. Mais L. M. Kohnfelder [3] a proposé une solution plus élégante à ce problème. Supposons que j veuille envoyer à i un message M signé.

- Si n_j vérifie $n_j < n_i$ alors j procède comme indiqué au premier paragraphe.

- Si n_j vérifie $n_j > n_i$, cette fois j envoie $T = D_j(E_i(M))$ et i décode le message en calculant $M = D_i(E_j(T))$. Pour authentifier le message, il suffit de vérifier que l'on a $E_j(T) = E_i(M)$.
- Cette procédure n'est pas ambigüe puisque les entiers n_i et n_j sont connus, n'importe qui peut donc les comparer.

IV. Remarques.

. Le théorème 1 montre qu'il n'est pas nécessaire de choisir des entiers n égaux au produit de deux entiers premiers distincts, il suffit que n ne soit pas divisible par le carré d'un nombre premier. (5)

. Dans [4], le théorème 1 n'est démontré que pour $h = 2$. De plus, la démonstration donnée ici évite l'étude de cas qui figure dans [4].

Références.

[1] W. Diffie, M. Hellman. - New directions in cryptography, I.E.E.E. Trans. Inform. Theory IT-22, nov. 1976, n°6, p. 644-654.

[2] P. de Fermat. - Oeuvres, ii. 209.

[3] L. M. Kohnfelder. - On the signature reblocking problem in public-key cryptosystems, Com. A.C.M., fev. 1978, v.21, n°2, p. 179.

[4] R. L. Rivest, A. Shamir, L. Adleman. - A method for obtaining digital signatures and Public-Rey cryptosystems, Com. A.C.M., fev. 1978, v.21, n°2, p. 120-126.

Maurice Mignotte
Centre de Calcul
7, rue René Descartes
67084 STRASBOURG Cédex

N O T E S : Il a semblé nécessaire à la rédaction de l'ouvert d'ajouter quelques notes au texte de M. Mignotte pour une meilleure compréhension.

(1) E pour "encodage" et D pour "décodage".

(2) M est un message quelconque ou un simple mot du message. On peut toujours supposer après remplacement des lettres par un nombre à deux chiffres correspondant à leur rang dans l'alphabet, que M est un nombre entier.

(3) Ce théorème n'est qu'une généralisation du théorème bien connu des élèves de terminale C : $x^{p-1} \equiv 1 \pmod p$ où p est un nombre premier. (Théorème de Fermat).

(4) Par exemple, pour calculer x^{15} on calcule successivement : x^2 , x^4 , x^8 , $x^{8+4} = x^{12}$, $x^{12+2} = x^{14}$ et enfin x^{15} ce qui nécessite finalement 6 multiplications.

(5) En effet, si $n = p^2q$, en prenant $M = pq$ on voit que $M^2 \equiv 0 \pmod n$ et par suite M et 0 ont la même image ce qui prouve que le codage n'est pas bijectif (ce qui est source d'incompréhension !)

UN EXEMPLE :

Prenons $n = 3\,691 \times 3\,989 = 14\,723\,399$
alors $\varphi(n) = 3\,690 \times 3\,988 = 14\,715\,720 = 2^3 \times 3^2 \times 5 \times 41 \times 997$
choisissons comme valeur de d : 1 999 qui étant premier et plus grand que le plus grand facteur de $\varphi(n)$ est premier avec lui.

Il nous faut trouver e tel que :

$$ed \equiv 1 \pmod{\varphi(n)}$$

Comme d et $\varphi(n)$ sont premier entre eux, d'après le théorème de Bezout, il existe deux constantes e et f telles que :

$$ed + f\varphi(n) = 1$$

En prenant les reste modulo $\varphi(n)$ des deux membres de cette égalité, on voit que e est bien le nombre cherché.

Voici la construction de e pour $d = 1\,999$ et $\varphi(n) = 14\,715\,720$; l'application de l'algorithme d'Euclide donne :

14 715 720	=	7 361	x	1 999 + 1 081	- 233
1 999	=	1	x	1 081 + 918	+ 126
1 081	=	1	x	918 + 163	- 107
918	=	5	x	163 + 103	+ 19
163	=	1	x	103 + 60	- 12
103	=	1	x	60 + 43	+ 7
60	=	1	x	43 + 17	- 5
43	=	2	x	17 + 9	+ 2
17	=	1	x	9 + 8	- 1
9	=	1	x	8 + 1	

Dans la colonne de droite on a choisi, à partir du bas, des coefficients multiplicatifs de manière à pouvoir effectuer les simplifications indiquées après addition membre à membre des différentes égalités. Il vient alors :

$$-233 \times 14\,715\,720 + 126 \times 1\,999 = -233 \times 7\,361 \times 1\,999 + 1$$

Soit encore :

$$-233 \times 14\,715\,720 + 1\,715\,239 \times 1\,999 = 1$$

D'où la valeur de e :

$$e = 1\,715\,239$$

Nous laissons le soin aux ordinateurs pour encoder ou décoder les messages !

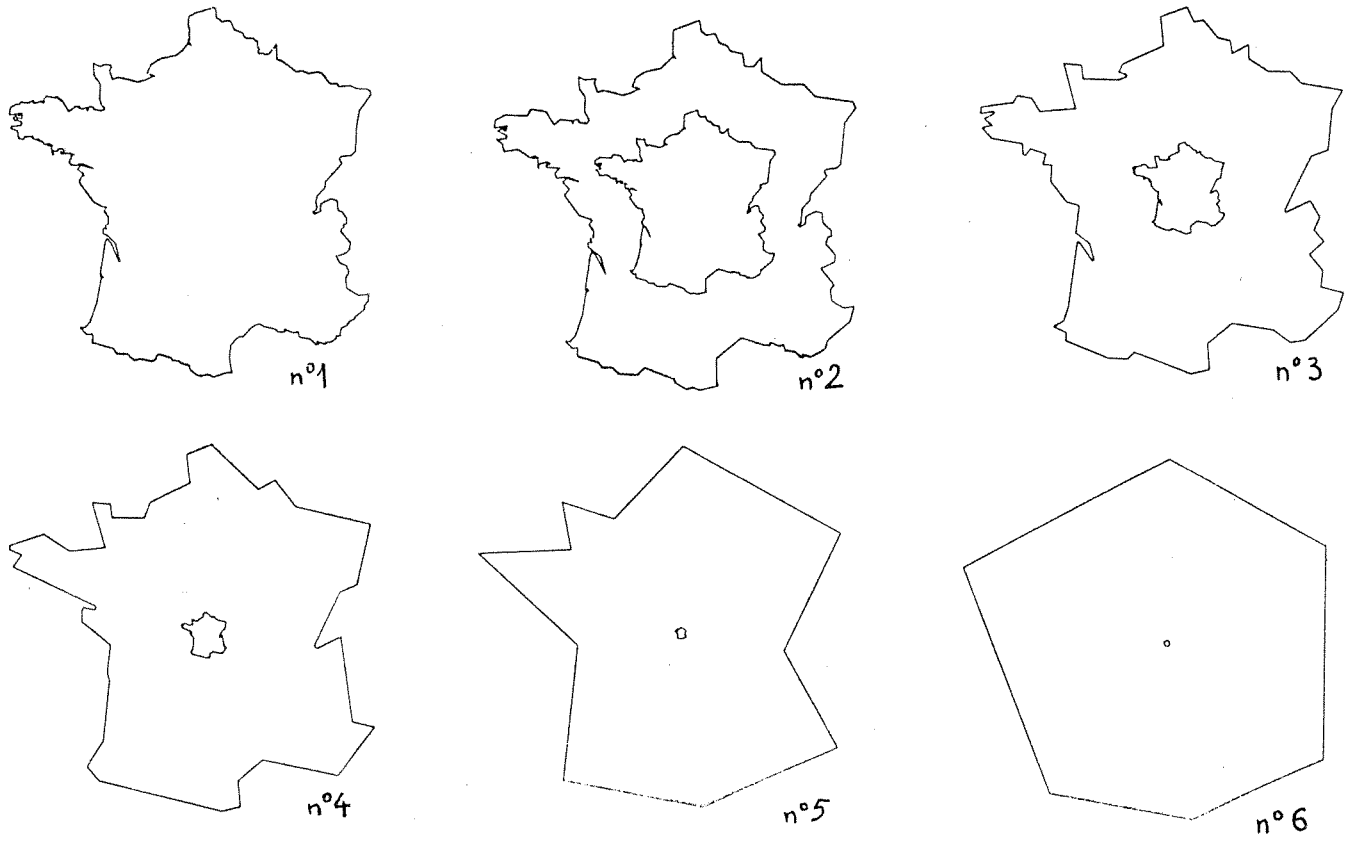
L ' O U V E R T : responsable de la publication : Jean Lefort
24, rue A Schweitzer
Wintzenheim 68000 Colmar

impression : Irem de Strasbourg
10, rue du général Zimmer
67084 Strasbourg Cédex

Un livre : Les objets fractals par Mandelbrot

En 1967, Mandelbrot publiait dans la revue "Science" un texte intitulé : "Combien mesure la côte de la Bretagne ?" Ce texte, ainsi que bien d'autres publications de l'auteur, est largement commenté dans le petit ouvrage publié chez Flammarion en 1975 : "Les objets fractals".

En quoi la longueur de la côte de la Bretagne (ou la longueur des frontières tant terrestres que maritimes d'un pays quelconque) a-t-elle à voir avec les mathématiques ? Le graphique ci-dessous (extrait de la revue du Palais de la Découverte nº 33) qui représente des cartes de la France continentale permet de comprendre les motivations de l'auteur. Quand l'échelle double, la longueur des frontières fran-



D'une carte à l'autre, l'échelle est diminuée de moitié, mais on a représenté un agrandissement de chaque carte à l'échelle initiale de façon à faire apparaître la perte des détails.

çaises augmente. Ainsi sur le dessin nº 6 la longueur est de 153 mm, sur le nº 5 elle est de 167 mm, sur le nº 4 de 193 mmm .... Imaginons que nous continuions à agrandir l'échelle de la carte. A chaque agrandissement nous pouvons prendre en compte des

détails, des anfractuosités qui n'apparaissent pas sur la carte précédente et qui vont se traduire par une augmentation de la longueur totale.

Au lieu d'utiliser le processus d'une carte à différentes échelles, nous pouvons, et cela revient au même, modifier notre instrument de mesure : avec une "règle" de 1 km de long dont nous posons les extrémités en des points du rivage (ou de la frontière) nous obtiendrons une longueur moindre qu'avec une règle de 1 hm, ou de 1 dam .... Nous pouvons continuer jusqu'au centimètre, ce qui nous oblige à contourner chaque caillou, puis jusqu'au dixième de millimètre ce qui nous fait mesurer les détails sur un grain de sable ... Il n'y a aucune raison de nous arrêter et la longueur mesurée croit indéfiniment. (Mandelbrot explique dans son livre comment faire abstraction des marées). Finalement il semble que personne ne soit capable de donner la mesure de la longueur des côtes de Bretagne.

En 1953, Richardson a eu l'idée de reporter sur un graphique en coordonnées bilogarithmiques la longueur $L(\eta)$ de différentes frontières ou portions de rivage en fonction de η longueur de l'instrument de mesure utilisé. Il remarqua que les points obtenus s'alignaient sensiblement suivant des droites distinctes selon l'objet considéré et dont les pentes sont négatives. On peut donc écrire :

$$L(\eta) = A.\ \eta^{1-D}$$

avec $D \geqslant 1$ et de l'ordre de $1,3$. $D = 1$ correspond à la droite, au cercle,... bref, à des objets mathématiques usuels dont la longueur est bien connue et constante. (d'où l'intérêt de la notation $1-D$). Il est tentant d'interpréter D comme une dimension; la droite et le cercle ont bien la dimension 1. Mais qu'est-ce qu'une dimension <u>fractale</u> pour reprendre le mot forgé par Mandelbrot sur"fraction" ?

Pour mieux comprendre ce phénomène, nous allons nous intéresser à des cas beaucoup plus théoriques, mais aussi beaucoup plus simples.

<u>1) Vers la dimension d'homothétie</u>

Tout le monde est persuadé qu'un segment a la dimension 1, le rectangle la dimension 2, le cube 3 ...

* Considérons le segment $[0\ ,\ 1]$. Il peut être pavé par exactement $N = n$ parties de la forme $\left[\frac{k-1}{n},\ \frac{k}{n}\right]$. Chaque partie de longueur $1/n$ est homothétique au segment initial dans le rapport $r(N) = 1/n$.
* Considérons le rectangle $[0\ ,\ X] \times [0\ ,\ Y]$. Il peut être pavé par exactement $N = n^2$ parties de la forme $\left[\frac{k-1}{n}x,\ \frac{k}{n}x\right] \times \left[\frac{k-1}{n}y,\ \frac{k}{n}y\right]$. Chaque partie d'aire XY/n^2 est homothétique au rectangle initial dans le rapport $r(N) = 1/n$.
* On généralise sans peine au cas du parallèlépipède qui est pavé par $N = n^3$ parties homothétiques au tout dans le rapport $r(N) = 1/n$.

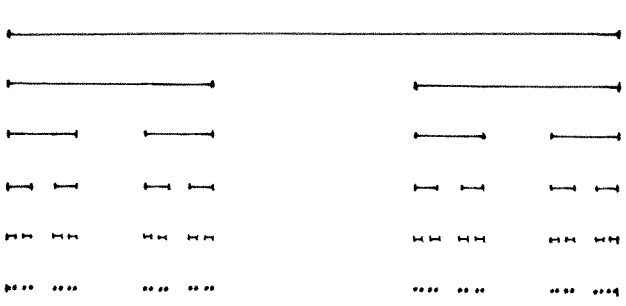
* Dans ces trois cas, on voit que la dimension peut être donnée par la formule :

$$D = - \frac{\text{Log } N}{\text{Log } r(N)} = \text{Log } N \ / \ \text{Log} \frac{1}{r}$$

Nous allons appliquer cette définition à différents ensembles qui se verront attribuer une valeur non entière comme dimension D.

2) Application à l'ensemble de Cantor

L'ensemble triadique de Cantor s'obtient de la façon suivante : On part du segment $[0 , 1]$ dont on ôte le tiers central $]1/3 , 2/3[$. On recommence le même procédé sur les deux segments restants et on itère indéfiniment le processus. On obtient alors un ensemble C d'intérieur vide dont tous les points sont des points d'accumulation (aucun point n'est isolé).



On peut facilement remarquer que $C \cap [0 , 1/3]$ est homothétique de C dans le rapport $1/3$ mais qu'il faut deux telles parties pour paver C . En conclusion on posera :

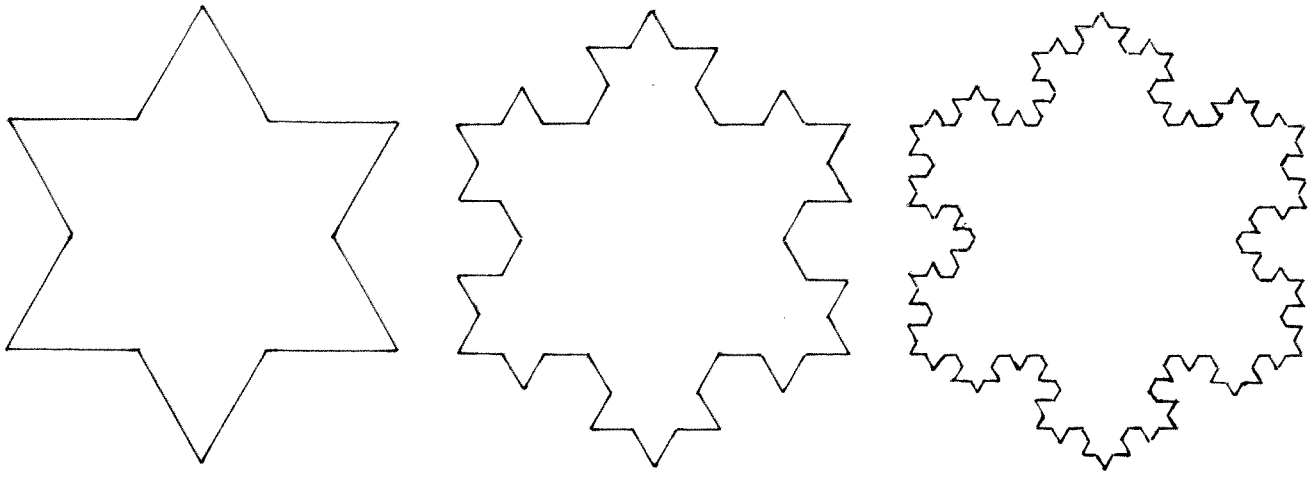
$$D(C) = \text{Log } 2 \ / \ \text{Log } 3 = 0,6309...$$

3) L'éponge de Sierpinski

Il existe différentes formes de cette "éponge". Celle de la couverture est obtenue de la façon suivante : Partant d'un cube d'arête unité, on le divise en $3^3 = 27$ petits cubes identiques. On enlève le petit cube central ainsi que les six autres adjacents par une face. On recommence l'opération sur les 20 petits cubes restants et ainsi de suite. Chaque partie enlevée est un ensemble ouvert (c-à-d ne contenant pas le bord). A la limite on obtient un ensemble infiniment feuilleté, connexe (d'un seul tenant) qui a une grande parenté avec l'éponge naturelle ou avec le gruyère : quelques gros trous, beaucoup de trous plus petits, encore plus de mini-trous ... La principale différence provenant de la régularité de l'éponge de Sierpinski, ce qui lui donne sans ambiguïté la dimension fractale de $\text{Log}20/\text{Log } 3 = 2,7268...$ Il faut en effet, à partir du cube initial, 20 petits cubes déduits du grand cube par une homothétie de rapport $1/3$ pour le recouvrir complètement.

L'intersection du cube par une diagonale ou une diagonale de face est un ensemble triadique de Cantor. Une face peut d'ailleurs être interprétée comme un modèle grossier des cratères de la Lune.

On trouvera dans le livre de Mandelbrot bien d'autres ensembles frac-



tals réguliers :

* Courbes de Von Koch généralisées (avec différentes valeurs de D). On trouve ci-dessus la reproduction de son célèbre flocon. ($D = \text{Log}\,4 / \text{Log}\,3 = 1{,}2618$).
* Courbes de Peano qui remplissent tout le plan et pour lesquelles D vaut 2.
* Des schémas du poumon avec une dimension $D = \dfrac{1}{2\cos(\pi/4 - \varepsilon/2)}$ et ε très petit.

4) Le rôle du hasard

Dans la réalité on ne peut pas se satisfaire d'une homothétie régulière. Mandelbrot explique comment on peut définir la dimension fractale dans ce cas. L'idée consiste à analyser statistiquement l'auto-homothétie des courbes ou surfaces obtenues. Une simulation du hasard sur ordinateur permet effectivement d'obtenir des courbes qui ressemblent à s'y méprendre à un contour de côte ou à des surfaces imitant parfaitement un relief imaginaire. Ces essais sur ordinateur conduisent à dire que la dimension d'un rivage est d'environ 1,3 , celle d'un paysage montagneux environ 2,3 , sans que les chiffres soient impératifs, certaines zones n'ayant pas la même dimension que d'autres.

Cette intervention du hasard, l'auteur la développe à travers de nombreux exemples tirés du quotidien :

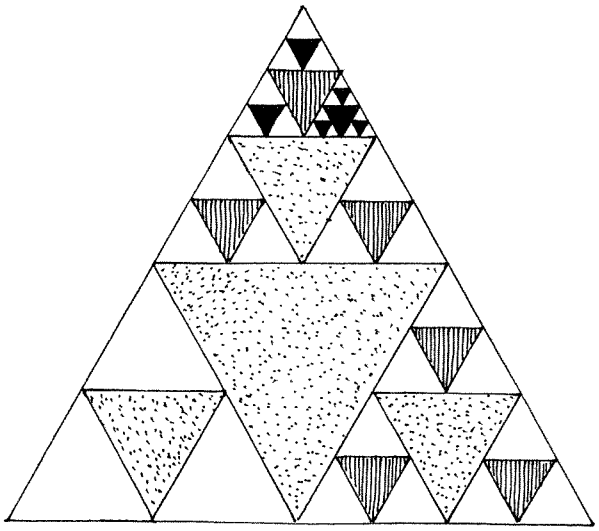
-- Les erreurs dans les transmissions téléphoniques.

-- La distribution des cratères de la Lune, où l'auteur améliore le modèle que représente une face de l'éponge de Sierpinski en supposant que les cratères s'effacent avec le temps et surtout que tout cratère peut en chevaucher d'autres.

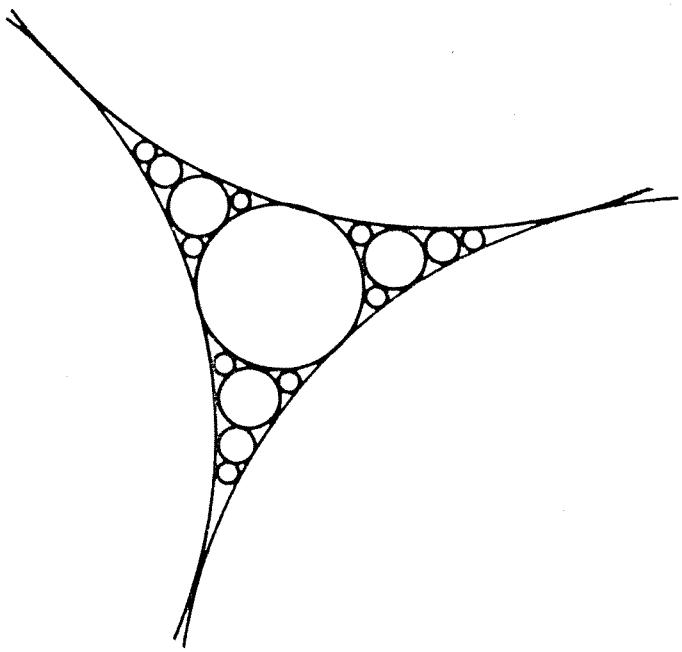
-- La distribution de la matière stellaire qui est nécessairement non uniforme sinon le ciel aurait la même luminosité de jour comme de "nuit" (paradoxe d'Olbers). De nombreuses réflexions théoriques conduisent à penser que la dimension fractale de l'Univers est sans doute 1 (!) et de toute façon inférieure à 1,77. Des simulations

dans le cas D = 1 conduisent à des résultats tout à fait acceptables (D = 1 et les étoiles ne sont pas sur une même courbe !)

-- La structure du savon qui fait intervenir le bourrage de cône dans le même esprit que le bourrage des triangles ou des cercles ci-dessous :



Bourrage d'un triangle pointe en haut par des triangles pointe en bas. On vérifie que la dimension vaut $\frac{\text{Log } 3}{\text{Log } 2}$ (dimension d'homothétie)



Bourrage appolonien de cercles ; la dimension de Hausdorff (inconnue) vaut environ 1,307

-- La géométrie de la turbulence (écoulement fluide).

-- Les arrangements de composants d'ordinateur

-- La loi de fréquence des mots (encore ne faut-il pas généraliser aux mots rares auxquels il est difficile, voire impossible, d'attribuer une fréquence ; un mot tel que "fourchette" doit déjà être considéré comme rare).

5) Généralisation de la notion de dimension

Le livre se termine par deux chapitres indépendants qui regroupent :

a) L'un des esquisses de biographies de personnes ayant d'une façon ou d'une autre imaginé la dimension fractale. A ces biographies il faudrait ajouter celle de J. Perrin longuement cité dans l'introduction.

b) L'autre des notes techniques montrant qu'il n'y a pas une dimension fractale mais plusieurs qui ne conduisent pas aux mêmes valeurs de D sauf dans les cas classiques connus d'Euclide.

Généralisation de la dimension d'homothétie au cas où interviennent plusieurs rapport r_i. D est alors défini par $\sum r_i^D = 1$.

La dimension de Hausdorff ou dimension de contenu (qui s'applique parfaitement au cas du bourrage appolonien de cercles).

La dimension de Minkowski . . . . . .

Les définitions de ces différents termes sont données de façon très claire en quelques lignes. Comme dans tout son livre, Mandelbrot évite les développements mathématiques complexes et vulgarise à merveille des notions inhabituelles qui donnent encore lieu à des recherches en mathématiques avancées.

P.S. Le livre : "Les objets fractals , forme, hasard et dimension" de Mandelbrot peut être consulté et emprunté à la bibliothèque de l'I.R.E.M.

Jean Lefort

UNE HIERARCHIE "OPPRESSIVE" ? Or l'enseignant est seul. "On est lâché dans la nature sans savoir à qui parler". Dans l'établissement c'est parfois le vide.(...) Par ailleurs, il y a toute la hiérarchie, qui, à tort ou à raison, est ressentie comme une structure oppressive par nature. Le proviseur, les inspecteurs ne pourraient donc être des interlocuteurs et des aides ("ils jugent et ils notent").

Ceux qui ont eu la chance d'assister à des mini-stages ou journées pédagogiques n'en n'ont pas tiré tout le profit escompté. Ces rencontres "verticales" n'offrent guère, selon eux, que l'occasion pour la hiérarchie de faire des discours.

L' EXPERIENCE DE CHACUN AU SERVICE DE TOUS. Au contraire l'échange "horizontal" d'expériences réelles, entre collègues, le professeur de mathématiques l'a trouvé dans les Instituts de recherche pour l'enseignement des mathématiques (IREM). A son avis cette expérience représente le modèle le plus réussi d'une formation continue. Chacun parle à ses égaux de son expérience et la confronte à celle de ses collègues. Ainsi l'expérience individuelle est mise au service de tous.

La formation des enseignants

table ronde au lycée Emile Zola de Wattrelos

le courrier de l'éducation : nº 79 / avril 79

Orientation en fin de Seconde

"Qui décide du passage d'un élève de Seconde C en Première C ou Première D, d'un élève de Seconde AB en Première B ou en Première G ?" est une question souvent posée entre collègues et dans l'esprit de beaucoup, la réponse semble varier d'un établissement à l'autre. Pour en avoir le coeur net ; nous avons consulté les textes officiels ; de ceux-ci ressortent les différents points suivants :

1. En fin d'année scolaire, le conseil de classe formule des propositions. Ces propositions portent soit sur le passage dans la classe supérieure du même type d'enseignement ou sur le redoublement, soit sur le passage vers un type d'enseignement différent de celui dans lequel se trouve l'élève.* Ces propositions sont portées à la connaissance des familles.**

2. Chaque type d'enseignement est composé comme suit :
   - enseignement des classes de Seconde et de Première A ;
   - enseignement des classes de Seconde A et B et de Première B et B.Tn (G) ;
   - enseignement des classes de Seconde C et de Première C, D, H ;
   - enseignement des classes de Seconde T et de Première E, H et B.Tn (F) ;
   - enseignement des classes préparatoires aux B.E.P. ;
   - enseignement des classes préparatoires aux B.T..**

3. Si la proposition du conseil de classe est conforme aux voeux de la famille, ou acceptée par elle, elle prend valeur de décision d'orientation. Si la proposition du conseil de classe n'est pas conforme aux voeux de la famille ou n'est pas acceptée par elle, ou encore si celle-ci n'a pas émis d'opinion, le chef d'établissement prend toutes initiatives pour engager ou poursuivre avec la famille un échange d'informations.

En cas de désaccord persistant, la famille peut opter entre deux solutions :
   - s'en remettre à l'arbitrage de la commission d'appel (...) ;
   - demander que l'élève soit soumis à un examen organisé par l'inspecteur d'Académie.

La décision d'orientation est alors déterminée par le résultat de l'examen.
Toutefois, en cas de proposition de redoublement, la famille ne peut recourir qu'à l'arbitrage de la commission d'appel.*

4. L'affectation des élèves se fait sous la responsabilité de l'inspecteur d'Académie, en fonction des décisions d'orientation et des choix offerts par la carte scolaire.
Pour l'enseignement technologique, ces mesures d'affectation tiennent compte de l'ordre de préférence entre les sections ou les spécialités établi par les familles.
Si l'orientation d'un élève n'entraîne pas un changement d'établissement ou de cycle, les mesures d'affectation sont prises par le chef d'établissement. *

5. La commission d'appel comprend des membres permanents et "des membres qui participent à une partie des travaux, selon les dossiers présentés :

le professeur principal (...) de la classe à laquelle appartient l'élève dont le cas est examiné ;

le conseiller d'orientation de l'établissement." **

Il semble donc que la réponse à la question posée au départ soit la suivante : si le conseil de classe a à se prononcer sur le passage d'un élève de 2°C en 1° (C ou D ou H) ou d'un élève de 2°AB en 1° (B ou G_1 ou G_2 ou G_3), ce n'est ni lui ni la famille qui choisiront la section, mais l'administration ! (en l'occurence, le plus souvent, le chef d'établissement).

La note n° 1962 du 25 mai 1976 (collèges : Bureau DC 12) "Applications des procédures d'orientation" dans laquelle on lit "Il est rappelé que la proposition définitive du conseil de classe ne peut mentionner que le ou les types d'enseignement. Les appels formulés par les familles ne sont recevables que s'ils portent sur un type d'enseignement (...) la décision d'orientation (...) ne peut porter que sur le ou les types d'enseignement (...), l'affectation (...) se fait sous la responsabilité de l'inspecteur d'Académie, en fonction des décisions d'orientation et des choix offerts par la carte scolaire", confirme cette analyse.
A titre de documentation, on trouvera ci-après une information chiffrée sur les taux de redoublement et de passage de Seconde en Première.

* Décret n° 73-129 du 12 février 1973 (Premier Ministre, Education Nationale.)
** Arrêté du 12 février 1973 (Education Nationale)
tous deux : "Procédures d'orientation dans le Second degré de l'Enseignement Public".

Passage de Seconde en Première à la fin de l'année scolaire 1976-77, dans les lycées du département du Bas-Rhin.

ETABLISSEMENTS	Effectifs 2°A	% RA	% 1°A	Effectifs 2°AB	% RAB	% 1°B	% 1°G	Effectifs 2°C	% RC	% 1°C	% 1°D	% 1°(mD)
Marie - Curie	40	17,5	40	107	20	6	36	118	14,5	26,5	35,5	62
Kléber	56	3,5	86	48	17	52	31	289	15	46,5	25,5	72
Pasteur *	30	13,5	80					110	15,5	45,5	29	74,5
Fustel *	120	4	82,5	58	9	46,5	22	168	6,5	55	26	81
Pontonniers	52	15	71	94	19	30	48	71	10	52	27	79
Neudorf	35	0	88,5	106	8,5	33	52	174	8,5	35,5	38	73,5
Bouxwiller *	27	18,5	66,5					62	11	35,5	47	82,5
Saverne	17	6	53	65	4,5	35	52	76	4	56,5	26,5	83
Barr *	20	0	65	26	0	8	85	34	9	38	41	79
Sélestat *	30	13	70	94	1	1	87	119	7,5	49,5	33,5	83
Bischwiller	6	16,5	83,5	54	4	18,5	48	44	7	38,5	36,5	75
Haguenau	33	3	63,5	166	2,5	20,5	69	146	4	55,5	27,5	83
Wissembourg	22	0	100	76	4	39,5	68,5	56	5,5	41	28,5	69,5
Molsheim *	35	3	83	78	6,5	2,5	60	91	5,5	36,5	49,5	86
Obernai	20	0	95	41	5	53,5	24,5	41	2	49	39	88
Schoch *				127	6		83					
BASRHIN	543	7	76	1140	8	20	58	1599	9,5	45	32,5	77,5

RA, RAB, RC signifient respectivement redoublement en 2°A, en 2°AB, en 2°C.

* Etablissement n'ayant pas en 1977-78 de classes de 1° B.

Les statistiques ne sont pas tout. Une anecdote :

Une élève de 2° T4 demande à la fin de l'année scolaire, après en avoir parlé avec certains de ses professeurs, à passer en 1°D. Le conseil de classe, de fin d'année, présidé par un représentant de l'administration, en parle longuement et convient de la solution suivante : le professeur principal contactera la famille pour l'informer des avantages et des risques pour l'avenir du passage de cette élève en 1°F8 ou en 1°D et la famille choisira. Les membres de ce conseil ignoraient manifestement les textes officiels. Quelques jours après, avant que le professeur principal n'ait eu le temps de faire quoi que ce soit, ils apprennent que la commission d'appel a décidé d'orienter cette élève en 1°D.
On avait ainsi remplacé une solution humaine par une solution administrative ! Comment ne pas le regretter !

M. de Cointet