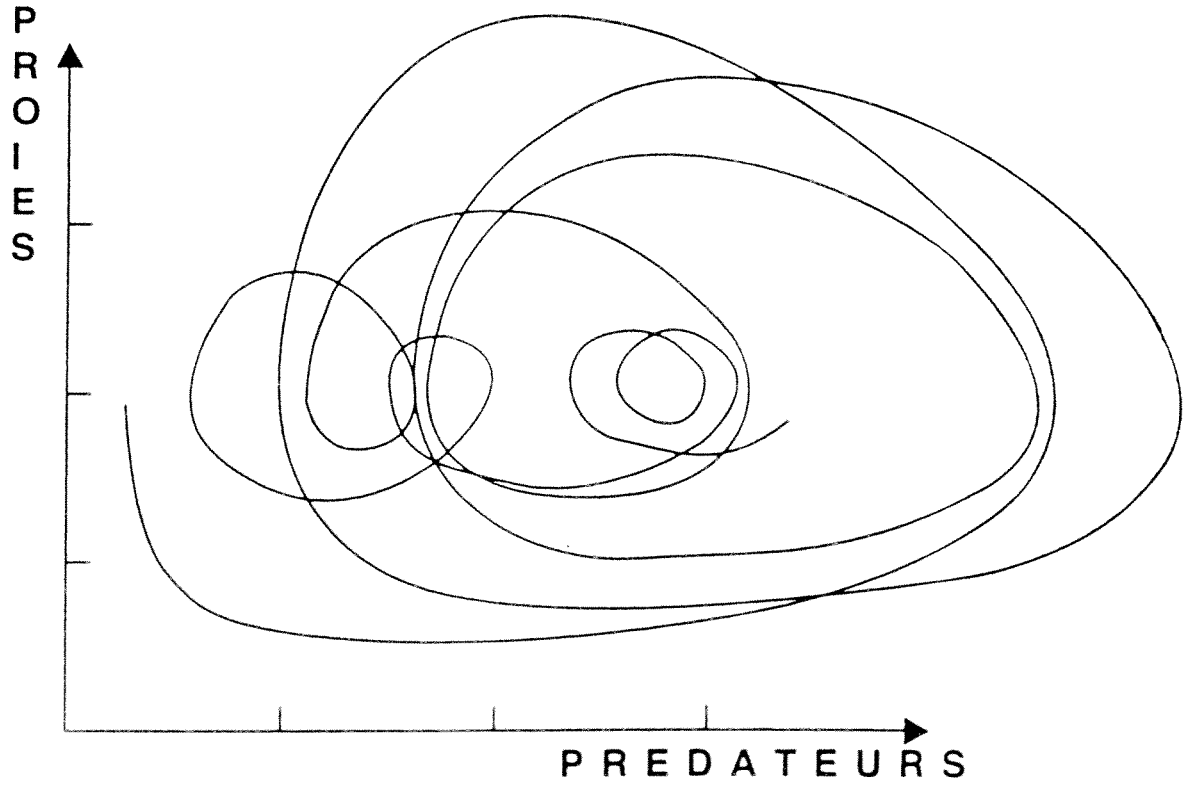
Société des Enseignants Neuchâtelois de Sciences



bulletin n° 17, avril 1994

Une conférence, un livre, une réaction d'élève sont susceptibles d'intéresser d'autres collègues. Pourquoi de pas faire figurer cette information dans le bulletin ?

Edition: Société des enseignants neuchâtelois de sciences (SENS).

Comité de la SENS: Christian Bazzoni (vice-président, délégué coll. informatique), Christian Berger, Pierre-André Bolle (caissier), Michel Favez (délégué coll. physique), Michel Favre (président, délégué coll. mathématique), François Goetz, Françoise Jeandroz, Jean-Pierre Launaz (secrétaire), Willy Reichenbach (délégué coll. biologie), Denis Sermet.

Equipe de rédaction du Bulletin: Jacques-André Calame, Michel Favre, François Jaquet, Françoise Jeandroz, Jacques Méry, Luc-Olivier Pochon.

A collaboré à ce numéro: Bruno Vitale.

Couverture: Evolution de deux populations; extrait de l'article de Bruno Vitale.

Délai pour transmettre vos contributions au prochain numéro: 15 juin 1994

didactique

Modélisation qualitative et quantitative: Un exemple d'intégration de l'informatique à la pratique pédagogique: les bases de la pensée écologique [1]

B.Vitale [2]

Il y a tellement de modélisations...

Un article récent sur Informatique-Information (voir la rubrique Lu pour vous de ce Bulletin) a présenté les concepts de "modèle mathématique" et de "simulation", en les définissant dans le contexte d'une utilisation scolaire de l'informatique à l'aide de logiciels de modélisation-simulation (en particulier, STELLA). Je désire élargir ici cette présentation, en explorant plus en détail trois dimensions pertinentes:

- du côté des **modèles** (et non seulement des "modèles mathématiques"), en introduisant des nuances entre "modèles qualitatifs" et "modèles quantitatifs", "modèles descriptifs" et "modèles explicatifs";

- du côté de la **psychopédagogie** et de la **pratique pédagogique**, en situant l'activité de modélisation et de simulation dans le contexte de l'apprentissage de la mathématique et des sciences, au delà du stricte domaine de l'informatique;

---

[1] Les considérations présentées dans cet article sont le fruit d'une longue collaboration et d'intenses discussions avec C.Béguin, J.-L.Gurtner, O.de Marcellus, M.Denzler et A.Tryphon.

[2] En congé sabbatique de l'Institut de physique théorique, Université de Naples; collaborateur au CRPP, Genève.

- du côté des **simulations**, en plaidant la cause - peu populaire de nos jours, il est vrai! - de l'importance de la programmation directe, de la part des élèves, par rapport à l'utilisation de logiciels de modélisation-simulation.

Je prendrai comme exemple et je décrirai les premiers résultats d'une expérience de modélisation-simulation qui continue, depuis plusieurs années, dans des classes de 7e du Cycle d'orientation et dans le cadre assez large et transdisciplinaire des cours d'Observation scientifique, de Biologie et d'Informatique. Thème général: **les processus de croissance et de changement**. Cette expérience prépare les bases pour une possible extension de l'activité (en 8e et en 9e) vers **l'exploration de l'"espace écologique"**: c'est-à-dire, vers le domaine de la modélisation relative à l'interaction entre deux ou plus grandeurs variables dans le temps. Dans ce qui suit, es modèles seront tous, formellement, des modèles continus paramétrisés par le temps (transformés en modèles discrets seulement pour en permettre l'intégration par l'ordinateur).

Language observationnel commun: la nouvelle approche vers l'activité d'observation scientifique dans les classes de 7e; language informatique commun: LOGOwriter.

Observation scientifique et modélisation

Le cours d'Observation scientifique en 7e est en train d'abandonner le cadre de référence assez limité dans lequel il s'était développé au début, celui de l'enseignement et de l'apprentissage de "la méthode scientifique" d'observation - générale et non contextuelle - des phénomènes naturels, une méthode qui n'était pas censé amener à l'établissement de règles, de régularités quantitatives, de modèles pour les phénomènes étudiés.

Au contraire, la nouvelle approche demande explicitement un élargissement de la pratique expérimentale dans des cadres interprétatifs (voir, par exemple, (2)). En d'autres mots: on reconnait que l'action même d'observer et de créer des situations expérimentales qui se prêtent à l'observation, demande la présence - quelquefois implicite, et que les enseignants essaient de rendre explicite - de **modèles informels** ou **qualitatifs**. Ces modèles informels ou qualitatifs se retrouvent dans le choix des expériences, de la région de variation des paramètres définie pour chaque expérience, des variables considérées comme pertinentes et de celle dont on néglige la mesure dans le temps, etc.

La définition de "modèle" est ici évidemment différente de celle, plus stricte, de "modèle mathématique"; mais tous les modèles participent, d'un point de vue cognitif, d'une commune nature, et devraient être traités par une démarche compréhensive, capable de mettre en évidence leur essentielle homogénéité.

Parmi les phénomènes de croissance et de changement étudiés: la croissance du corps propre des élèves (dans ses aspects globaux - grandeur des élèves à partir de leur enfance - et différentiels - variations dans les rapports entre les différents parties du corps pendant le développement); la croissance d'une jeune tige florale d'amaryllis; le réchauffement et le refroidissement de différents liquides; l'évolution de l'épidémique du SIDA.

Parmi les phénomènes que nous voudrions être en mesure d'étudier: le développement d'une population isolée (bactéries? fourmis?); le développement de deux populations capables d'interagir entre elles.

Technique d'observation de cette pratique pédagogique: suivi de la part des enseignants; observations dans la classe et ensuite entretiens cliniques avec des couples d'élèves de la part des chercheurs.

L'intérêt de la modélisation qualitative: aspects gestuels, verbaux, graphiques

Les activités de "représentation" et de "modélisation qualitative" participent, ensemble, à l'apprentissage d'une certaine maîtrise des phénomènes observés et étudiés dans un laboratoire. On doit apprendre pour ça à observer comment les élèves **parlent** de leur expérience et réussissent à la **décrire** à l'expérimentateur; à la **spatialiser** par leurs gestes; à la **représenter** (par un tableau, un graphique, etc.).

Dès que la réflexion sur les données de l'expérience (ou des "séries historiques", comme dans le cas du SIDA) commence, la présence de certains **modèles qualitatifs et globaux** devient évidente: par une phrase rapide, par un geste de la main un phénomène est qualitativement et globalement décrit ("ça baisse tout le temps"; "ça fait des vagues").

Mais, à une analyse plus fine, la présence de plusieurs modèles qualitatifs et **locaux** (c'est-à-dire, qui impliquent l'observation d'un très petit intervalle temporel) peut être mise en évidence. Il s'agit ici, par exemple, de modèles locaux d'**interpolation** (comment faire une hypothèse sur la valeur d'une variable à un moment donné, si l'expérience a été faite seulement un peu

plus tôt et un peu plus tard?; on retrouve un paradigme assez constant de **régularité** et de **linéarité**, avec un modèle local assez trouble de "moyenne"); ou de modèles moins locaux d'**extrapolation** (comment prévoir le comportement asymptotique d'une variable en évolution, si la mesure s'est arrêtée après un certain temps?).

Il faut donc apprendre à tenir compte d'une première relation dialectique entre les modèles qualitatifs globaux (qui semblent précéder tous les autres, à niveaux représentatif) et les modèles qualitatifs locaux.

L'importance des modèles quantitatifs locaux: règles, invariants et symétries

Tous ces modèles sont, au début, qualitatifs; même la "moyenne" cité ci-dessus est bien plus qualitative et symbolique et beaucoup moins computationnelle de ce que l'on pourrait s'attendre. Mais il faut tenir compte d'une autre relation dialectique, celle entre les modèles qualitatifs et les modèles quantitatifs; la réflexion et l'observation sur les données expérimentales donnent lieu rapidement à un glissement d'une appréciation purement qualitative ("la température change plus rapidement au début, et toujours plus lentement après, à parité d'intervalle temporel, quand un liquide se refroidi") vers une appréciation et une tentative d'évaluation quantitative ("plus le liquide est chaud, plus il perd de chaleur; peut-être le changement de température est proportionnel à la température du liquide"). C'est à partir de ces modèles quantitatifs locaux qu'une intégration du modèle (par itération manuelle ou par ordinateur) est possible.

Et encore une troisième relation dialectique, souvent ignorée: celle entre les modèles descriptifs et les modèles explicatifs (comment souvent les enseignants disent "maintenant, je vous explique", alors que, au plus, on pourrait dire "maintenant, je vous décris"). Les modèles qualitatifs locaux dont a été question jusqu'à présent sont purement descriptifs; on constate, par exemple, que la perte de chaleur est proportionnelle à la température du liquide; on peut pas l'expliquer (faute de connaissance en thermodynamique). On verra ci-dessous comment ce dernier modèle devient un modèle local explicatif lors de l'intégration vers un modèle quantitatif global. (La boucle **semble** se fermer: on est parti d'un modèle qualitatif global, et se retrouve avec un modèle quantitatif global; pendant cette trajectoire en spirale, on a appris par mal de choses...).

C'est dans la construction de ces modèles quantitatifs locaux que des concepts nouveaux deviennent essentiels: en particulier, ceux de régularité, linéarité = proportionnalité, symétrie (voir, par exemple, (3) à (6)).

L'intégration de l'informatique à la pratique pédagogique: programmation et modèles quantitatifs globaux.

Le passage d'un modèle quantitatif local, décrit en général par un certain nombre de paramètres libres (à fixer par la confrontation des prévisions du modèle avec l'expérience), à un modèle quantitatif global peut être obtenu, souvent, par des moyens analytiques (solution d'une équation différentielle ou d'un système d'équations différentielles); mais ces moyens sont au delà des possibilités des élèves du Cycle et, dans certains cas, des enseignants eux-mêmes.

Reste la possibilité d'intégration manuelle par itération (presque jamais possible, ou au moins limitée à quelques itérations); celle d'intégration graphique (possible seulement dans des cas très simples de dépendance fonctionnelle du modèle local); et enfin celle de l'intégration par la programmation et par l'utilisation de l'ordinateur.

J'ai longtemps et très en détail présenté, dans la série de cahiers (7), les raisons pour lesquelles je considère fortement préférable, pour les premières classes de l'école secondaire, l'utilisation de la programmation (dans nos classes, en LOGOwriter, le dialecte LOGO enseigné maintenant à tous les élèves de 7e) à la place des logiciels de modélisation-simulation (type STELLA). J'y renvoie le lecteur. En quelques mots:

- l'ordinateur est, lui aussi, un **objet de connaissance** pour les élèves; laissons que le rapport des élèves avec l'ordinateur soit le plus transparent possible, et que le dialogue soit le plus possible proche du dialogue naturel;

- le language de programmation est, lui aussi, un **objet de connaissance** pour les élèves; laissons que les élèves maîtrisent les analogies et les différences entre un langage naturel et un langage formel;

- l'intégration pédagogique de l'ordinateur passe par sa présence continue dans la réflexion des élèves, des enseignants et de la classe entière; et non seulement dans les classes de 7e, mais dans tous les espaces transdisciplinaires que l'on pourra dénicher dans les classes de 8e et de 9e; pour que ce but soit réaliste, il faut que les élèves puissent autonomement programmer de manière flexible l'ordinateur pour réaliser leurs projets,

sans être à tout moment dépendants (et esclaves) de la présence ou non d'une logiciel adéquat.

Et la pensée écologique?

Pour moi, la construction d'un espace cognitif et représentatif adéquat pour l'élaboration d'une pensée écologique en classe, dans l'école secondaire obligatoire, passe par tous les points qui précédent: expérimentation, observation, représentation, explicitation des modèles locaux, intégration vers un modèle global.

Dans le cas particulier de la pensée écologique (voir, pour plus de détail, le cahier 5 cité dans (7)), l'intégration de très simples modèles de développement d'une population et la modélisation quantitative locale d'interaction entre deux populations permet de faire prendre conscience aux élèves du rôle joué par un certain nombre de concepts fondamentaux et tout à fait transdisciplinaires: l'importance des états d'**équilibre statique**; la présence d'une forme différente (et beaucoup plus fréquente en nature) d'équilibre, l'**équilibre dynamique** entre un certain nombre de variables; la présence, pour plusieurs systèmes, d'un certains nombre d'états d'équilibre doués d'une nouvelle caractéristique: celle d'être **attracteurs** ou **répulseurs**. C'est la description même du monde, des phénomènes de croissance et de changement, qui de cette manière s'enrichi.

Un tel début de réflexion écologique peut aussi permettre de discuter les effets différents que peut avoir sur un système le fait d'être soumis à un régime de **compétition**, ou au contraire de **symbiose** et/ou de **collaboration** (Figs.1 à 3). Dans un monde tellement compétitif, peut-être les avantages de la coopération serons ressentis positivement par les élèves...

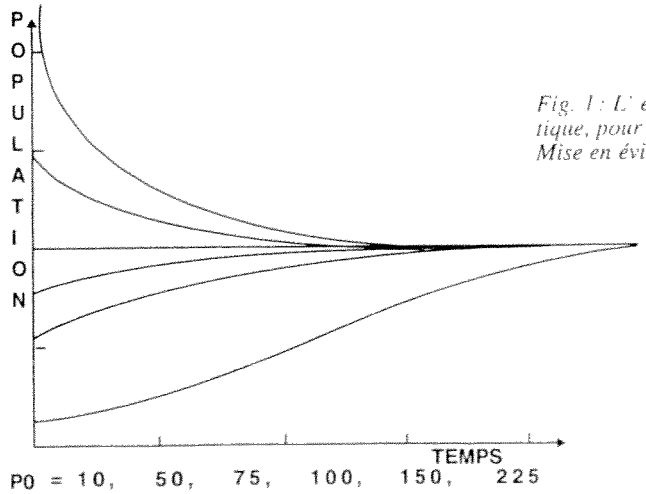


Fig. 1 : L' évolution d'une population, dans le modèle logistique, pour des valeurs différentes de la population à temps 0. Mise en évidence d'un état d'équilibre statique et attracteur.

Fig. 1

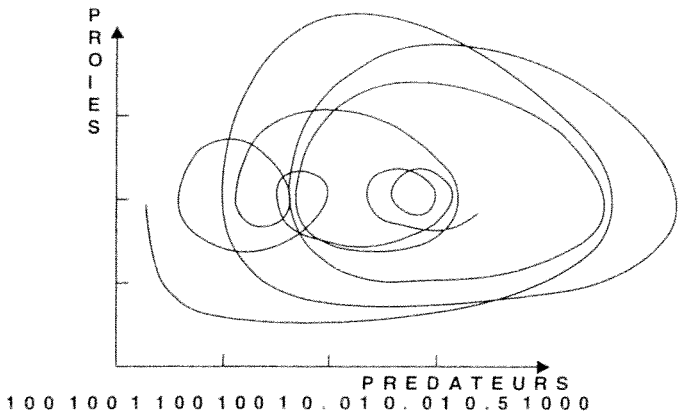


Fig. 2

Fig. 2 : L'évolution de deux populations, chacune des deux décrite par le modèle logistique avec pertubation périodique et avec une très simple interaction entre les deux du type "compétition" (prédateur-proie), pour la valeur (100,100) des deux populations à temps 0. Il n'y a plus d'états d'équilibre statique, ni d'attracteurs.

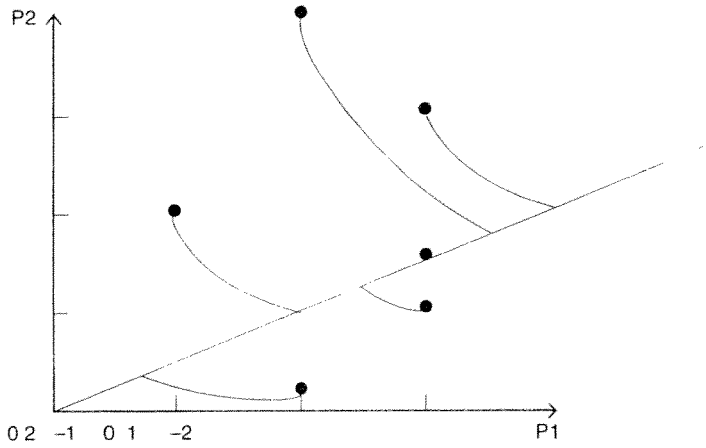


Fig. 3

*Fig. 3 : L'évolution de deux populations, chacune des deux décrite par le modèle logistique et avec une très simple interaction entre les deux du type "coopération" (symbiose), pour des valeurs différentes des deux populations à temps 0. Il y a une ligne (P1 = 2 * P2) de points d'équilibre statique, tous attracteurs.*

Références:

(1) J.-C.Cortésy: Modèles mathématiques et simulation. **Informatique-Information**, octobre 1993.

(2) B.Vitale: Pratiques et perspectives nouvelles de la stratégie expérimentale; Elargissement de la pratique expérimentale dans des cadres interprétatifs (Séminaire de formation pour l'enseignement d'Observation scientifique, Genève, 1991). **Cahiers d'OS**, no.5, septembre 1991, pp.50-60.

(3) J.-L.Gurtner and B.Vitale: Why modeling? Pupils interpretation of the activity of modeling in mathematical education (Proceedings of the 15th International conference on Psychology in Mathematical Education, PME-15). Assisi, 1991, vol.II, pp.101-108.

(4) J.-L.Gurtner, C.León, R.Nuñez Errazuriz et B.Vitale: Representation and modelisation of change over time by 12-13 year old children in a school context. **Cahiers des Archives J.Piaget**, 1994.

(5) J.-L.Gurtner, C.León, R.Nuñez Errazuriz and B.Vitale: The representation, understanding and mastering of experience; Modelling and programming in a school context, dans J.de Lange, Ch.Keitel, J.Huntley and M.Niss: **Innovation in maths education by modelling and applications**. New York: Horwood, 1993, pp.63-68.

(6) B.Vitale: Processes; A dynamical integration of informatics into mathematical education, in C.Hoyles and R.Noss (eds.): **Learning mathematics and LOGO**. Cambridge (USA): MIT University Press, 1992, pp.279-318.

(7) B.Vitale: L'intégration de l'informatique à la pratique pédagogique. Genève: CRPP-DIP, 1990-1993:
volume 1: Considérations générales pour une approche transdisciplinaire.
volume 2: Les projets:
cahier 1: Le laboratoire "jeux";
cahier 2: Le laboratoire "arbres et arborescences";
cahier 3: Le laboratoire "croissance et changement";
cahier 4: Le laboratoire "la construction de l'espace musical";
cahier 5: Le laboratoire "les bases de la pensée écologique".

Cet article a aussi paru dans Informatique-Informations n° 23, février 1994

mathématique

A propos de codage

L.-O. Pochon, CPLN

Le codage de l'information est un thème qui soulève plusieurs problèmes et qui fait appel à de nombreux domaines : traitement du contenu informationnel, correction des erreurs, cryptage, etc.

Le but de cette note est de présenter une technique de cryptage particulière, faisant appel à une méthode dite à *clef révélée*, c'est-à-dire une méthode où l'on peut donner l'algorithme de cryptage, sans permettre à son utilisateur de décrypter des messages utilisant le même procédé. On en voit bien l'utilité : une société X peut proposer à ces clients une façon de crypter les messages (téléphoniques, informatiques, ...) sans que personne (à moins de travaux gigantesques) ne puisse les remettre en clair (sauf ladite société, cela va sans dire). Une des méthodes les plus simples ne fait appel qu'à quelques principes simples d'arithmétique avec des classes de restes.

Ce sera aussi l'occasion de réfléchir aux concepts fondamentaux de mathématiques mis en oeuvre dans des résolutions de problèmes assistées par ordinateur.

Quelques principes

Les opérations *div* et *mod*

La notation "a *div* b" désignera la division euclidienne (entière) de a par b. div sera aussi désigné par la suite par FLOOR. Quant à la notation "a *mod* b", elle désigne le reste de la division de a par b.

Classes de restes

On dit que *a et b sont congruents modulo n* (notation: $a \equiv b \pmod n$) si a mod n = b mod n. Cela signifie que les divisions de a et b par n ont le même reste. Exemple: $106 \equiv 71 \pmod 5$. A l'aide de cette relation on peut définir une partition de Z en classes d'équivalence, les classes de restes. Z/nZ est l'ensemble quotient. Exemple: $Z/4Z = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}\}$ où chaque nombre représente toute une classe. $\underline{1}$ représente {... -7, -3, 1, 5, 9, ... }. Z/nZ est un groupe additif.

L'indicateur d'Euler

Pour un nombre entier n, $\varphi(n)$ représente le nombre de nombres premiers avec n (y compris 1) inférieurs à n.

$\varphi(3) = 2$ (les diviseurs de 3 inférieurs à 3 sont 1 et 2)
$\varphi(4) = 2$ (les diviseurs de 4 inférieurs à 4 sont 1 et 3)
$\varphi(5) = 4$ (les diviseurs de 5 inférieurs à 5 sont 1, 2, 3 et 4)
$\varphi(6) = 2$ (les diviseurs de 6 inférieurs à 6 sont 1 et 5)
$\varphi(p) = p-1$ (p est premier)
$\varphi(pq) = (p-1)(q-1)$ (si p et q sont deux nombres premiers)
$\varphi(10) = 4$ (10 = 2*5)

La formule pour $\varphi(pq)$ se généralise: $\varphi(n*m) = \varphi(n) * \varphi(m)$ si n et m sont deux nombres premiers entre eux. De plus on a : $\varphi(p^r) = p^{r-1}(p-1)$.

On peut aussi multiplier deux éléments de Z/nZ. On considère Z/nZ* le groupe des éléments de Z/nZ qui possèdent un inverse, c'est-à-dire des éléments a tels que
il existe m avec am = 1 ou
am ≡ 1 (mod n) ou encore
s'il existe a et b tels que am + bn = 1.

Selon le théorème de Bezout, cette dernière relation existe si et seulement si m et n sont premiers entre eux. $\varphi(n)$ est donc aussi le nombre d'éléments du groupe multiplicatif Z/nZ* des classes de restes modulo n.

Si a est un élément de Z/nZ* alors: $\{ax \mid x \in Z/nZ^*\} = Z/nZ^*$. Par conséquent le produit de tous les membres de chacun de ces deux ensembles sont égaux:

$$\prod_{x \in Z/nZ^*} ax \equiv \prod_{x \in Z/nZ^*} x \pmod n \quad \text{donc} \quad a^{\varphi(n)} \prod x \equiv \prod x \pmod n$$

Par conséquent $a^{\varphi(n)} \equiv 1 \pmod n$ si a et n sont premiers entre eux. Ce résultat est connu sous le nom de théorème d'Euler. Exemple: $a^4 \equiv 1 \pmod{10}$ pour tout nombre a premier avec 10 (3, 7, 9, ...).

Cette formule généralise le 'petit' théorème de Fermat: si p est un nombre premier et a n'est pas divisible par p : $a^{p-1} \equiv 1 \pmod p$. Exemple: $a^4 \equiv 1 \pmod 5$ pour a non divisible par 5.

Le théorème d'Euler nous dit que si la décomposition de n en facteurs premiers est n = pq, et que si M est premier avec n (ce qui est le cas si M est inférieur à p ou q) on a : $M^{\varphi(n)} = M^{(p-1)(q-1)} \equiv 1 \pmod n$ ou $M^{\varphi(n)} \bmod n = 1$.

Par ailleurs le théorème de Bezout permet de dire que si e est premier avec $\varphi(n)$, il existe s tel que $es \equiv 1 \pmod{\varphi(n)}$.

Méthode de codage

Sur cette base une méthode de codage simple peut être construite: (n,e) est la clef révélée du système de codage (ces nombres sont en principe enfouis dans un programme d'ordinateur); s en est la clef secrète qui permet le décryptage !

Le principe de codage est le suivant : le message est représenté sous la forme d'un nombre que l'on découpe en tranches inférieures à n. Pour une tranche M, on effectue le calcul suivant :

$C = M^e \bmod n$. C est le message codé !

Il paraît qu'il est difficile de retrouver s sans retrouver p et q, ce qui serait en principe possible de réaliser en factorisant n. Mais ce travail (si les nombres premiers p et q sont grands) est quasiment impossible à réaliser dans un temps raisonnable !

Pour décoder il suffit de faire :

$C^s \bmod n$.

En effet $C^s \bmod n = M^{es} \bmod n = M^{(a\,\varphi(n)\,+\,1)} \bmod n = (M^{a\,\varphi(n)} \bmod n)\ (M \bmod n) = M \bmod n = M$.

On notera que e et s jouent un rôle symétrique. s est la clef secrète de la clef révélée (n,e). Mais e peut aussi être la clef secrète de la clef (n,s).

Exemple réduit

$n = 221\ (= 13*17)$; $\varphi(n) = 12*16 = 192$
$e = 35$; $s = 11$ (on vérifie que $e*s \equiv 1 \pmod{192}$, puisque $11*35 = 2*192+1$)

On prend le 'message' $M = 12$.

Le message codé est alors : $C = 12^{35} \bmod 221 = 181$.

Pour accélérer le calcul de C, il suffit de calculer préalablement 12 à la puissance 2^i et réduire mod n au fur et à mesure. On trouve: $12^2 = 144$, $12^4 \equiv 183 \pmod{221}$, $12^8 \equiv 118 \pmod{221}$, $12^{16} \equiv 1 \pmod{221}$, $12^{32} \equiv 1 \pmod{221}$ et donc
$12^{35} = 12^{32} * 12^2 * 12 \equiv 12*144 = 1728 \equiv 181 \pmod{221}$.

Décodage :

Le décodage s'opère par le calcul $C^s \bmod n = 181^{11} \bmod 221 = 12$. Il s'agit bien du message initial.

Ce calcul s'effectue après avoir calculé les puissances 2e, 4e et 8e de 181 réduites mod n. Elles valent respectivement: 53, 157, 118.

Un exemple plus compliqué

Voici une clef révélée :
n = 14923696918500106370820048199173565630921138635885734898108859571174 3
e = 7719068319927551

Pouvez-vous m'envoyer des messages ? Saurez-vous décoder le message
C = 553158717909856679607693767493057799388932503530911255062977692502 92 ?

Problèmes annexes

Signature

Un problème peut exister de savoir si un message envoyé de l'expéditeur A à B provient effectivement de A. Pour cela une technique consiste à introduire une signature au message, codée à l'aide de la clef secrète de A, et reconstituée par B à l'aide de la clef révélée de A. Le fait de retrouver la signature de A grâce à sa clef révélée prouve l'origine de l'émetteur du message.

Problème de calcul

Cette technique pose le problème du calcul avec de grands nombres. Dans la pratique tous les nombres utilisés p, q, e, s sont de l'ordre de 10^{200}. Se confronter avec des grands nombres augmente les difficultés. La perception globale est plus difficile, les manipulations plus lentes. Par conséquent, il est plus facile de perdre le fil du travail. Les lois ne paraissent plus tout à fait les mêmes ! Cela permet d'imaginer pourquoi les jeunes élèves éprouvent de la peine à résoudre des problèmes avec des 'grands' nombres, alors qu'ils peuvent les maîtriser sur des jeux de nombres plus petits.

L'usage de DERIVE

Outil simple, DERIVE est un programme de moins de 300 kB, qui permet de nombreuses manipulations de mathématique formelle. En particulier, la façon de réaliser des fonctions est très dynamique. Ainsi que le montre la réalisation de m^e mod n (avec réductions successives).

Principe

$$m^e \bmod n = \begin{cases} \text{si } e = 1: m \bmod n \\ \text{sinon} \begin{cases} \text{si e est pair: } (m\text{^}2 \bmod n)\text{^}(e/2) \bmod n \\ \text{sinon: } (m * m\text{^}(e-1) \bmod n) \bmod n \end{cases} \end{cases}$$

Code

```
PMOD(m,e,n) := IF(e=1,
                  MOD(m,n),
                  IF(MOD(e,2)=0,
                      PMOD(MOD(m^2,n),e/2,n),
                      MOD(m*PMOD(m,e-1,n),n)))
```

Le mode programmation incite aussi à réaliser des opérations en un seul "passage". Ainsi, pour trouver les coefficients du théorème de Bezout (a et b tels que an + bm = 1) à l'aide de l'algorithme d'Euclide on cherche simultanément la suite des restes r_n, celle des quotients q_n et celles des coefficients a_n et b_n.

Plus précisément, en supposant n>m cet algorithme commence par chercher q et r tels que: n = qm + r (division euclidienne). Si r vaut 1 le processus s'arrête et on a n - qm = 1. Sinon on recommence le processus avec m et r.

On pose donc: $n = r_0$, $m = r_1$
La formule de récurrence liant r_n est: $r_{n-1} = q_{n+1}\, r_n + r_{n+1}$

La décomposition de r_n en r_0 et r_1 permet de définir a_n et b_n par: $r_n = a_n\, r_0 + b_n\, r_1$

La relation: $r_{n+1} = r_{n-1} - q_{n+1}\, r_n = \underbrace{(a_{n-1} - q_{n+1}\, a_n)}_{a_{n+1}}\, r_0 + \underbrace{(b_{n-1} - q_{n+1}\, b_n)}_{b_{n+1}}\, r_1$

donne les valeurs de:

Toutes ces informations sont mises sous la forme d'un vecteur :

$v_n = [r_n, r_{n+1}, q_{n+1}, a_n, a_{n+1}, b_n, b_{n+1}]$

Avec $v_0 = [r_0, r_1, *, 1, 0, 0, 1]$ et

$v_{n+1} = [r_{n+1}, \mathrm{MOD}(r_n,r_{n+1}), q_{n+2} := \mathrm{FLOOR}(r_n,r_{n+1}),$
$a_{n+1}, (a_n - q_{n+2}\, a_{n+1}), b_{n+1}, (b_n - q_{n+2}\, b_{n+1})]$

```
BEZOUT(r1,r2,q2,a1,a2,b1,b2) := IF (r2=0,
                  [r1,a1,b1],
                  BEZOUT(r2,MOD(r1,r2),q2:=FLOOR(r1,r2),a2,a1-q2*a2,b2,b1-q2*b2)
```

Ou, si on se contente de faire des soustractions :

```
BEZOUTS(r1,r2,a1,a2,b1,b2) := IF (r2=0,
                  [r1,a1,b1],
                  IF (r2<=r1,
                      BEZOUTS(r1-r2,r2,a1-a2,a2,b1-b2,b2),
                      BEZOUTS(r2,r1,a2,a1,b2,b1)))
```

L'appel: *BEZOUTS(100,33,1,0,0,1)* donne la solution *[1,1,-3]*. Ce qui correspond à la décomposition de Bezout: 100 - 3*33 = 1.

Pour terminer, on laisse le soin au lecteur de méditer ces formules trouvées au hasard des exemples proposés par les créateurs du système :

MOD(a,b) := LIM(b/2-b*ATAN(COT(pi*x/b))/pi,x,a,1)
INVERSE(u,x) := ITERATE(u,x,x,-1) (inverse de l'opérateur u selon la variable x)

Pour conclure

Il est intéressant de noter que si une partie de l'informatique numérique se consacre à des algorithmes et à tendance a rejeter ce formulaire classique (la formule de Cramer est un désastre en temps de calcul), les systèmes formels, les systèmes parallèles auraient eux tendance à y faire un recours plus fréquent. Jean Beiner, dans sa présentation de 'comment bien programmer' fait ainsi allusion à la mise de processus sous forme linéaire, en particulier dans les systèmes de dessins assistés par ordinateur.

Références

Robert, A. (1984). Note de la séance du groupe Gonseth du 25 septembre 1984 sur les mathématiques et leur utilisation.

Hellmann (1980). Les mathématiques de la cryptographie à clef révélée. In: Les progrès des mathématiques. Paris: Bibliothèque pour la Science.

Sigrist, F. (1992). Les codes correcteurs d'erreurs. Bulletin no 12, avril 1992. Neuchâtel: Société des enseignants neuchâtelois en Sciences.

Delahaye, F. (1994) Une "puce" américaine menace le secret bancaire. L'Hebdo, 10 février 1994.

compte rendu

MATHÉMATIQUES 93, un colloque romand à suivre

F. Jaquet
Directeur de "Mathématiques 93"

Après "Allemand 89" et "Français 91", "Mathématiques 93" était le troisième colloque organisé par la Conférence intercantonale des chefs des Départements de l'instruction publique de la Suisse romande et du Tessin, le premier dans sa discipline. Vingt ans exactement après l'introduction généralisée des programmes romands de mathématiques, l'occasion était à saisir, le rendez-vous à ne pas manquer. Le colloque était accompagné d'activités parallèles auxquelles la SENS s'était associée.

Il semble opportun, dans l'élan de l'événement, d'en rappeler certains enjeux et de faire connaître les premières impressions de ses participants.

Une rencontre de maîtres en charge d'enseignement

"Mathématiques 93" devait réunir des enseignants titulaires de classes de mathématiques. Cette condition de participation clairement exprimée par les organisateurs de la rencontre a été largement respectée: la très grande majorité des 84 participants réunis à la Chaux-de-Fonds les 18 et 19 novembre 1993 étaient en prise directe sur les problématiques abordées, au vu de leur engagement quotidien en classe de mathématiques.

Se rencontrer sur des pratiques communes

Pour le premier jour du colloque, l'enjeu était de se retrouver sur une activité commune conduite au préalable, dans leurs classes respectives, par tous les membres d'un même groupe de travail. Chaque animateur avait soigneusement préparé et défini son thème et ses modalités pratiques avant de les présenter aux participants. Ces derniers sont entrés dans le jeu, pleinement. Ils y ont passé beaucoup de temps. Ils sont venus avec des travaux d'élèves, des remarques, des résultats expérimentaux témoignant d'une large pratique des activités proposées.

Un double enseignement est à tirer de ce type d'organisation: il est possible de faire "faire des mathématiques" à des classes de degrés, sections et cantons différents à propos d'un même thème et il est évident que les maîtres qui se retrouvent dans ce dispositif ont des choses à se dire!

En corollaire, on relève une frustration manifeste: celle de ne pas avoir eu plus de temps pour exploiter la somme de données acquises lors des travaux préparatoires.

Créer une dynamique

Les activités proposées par "Mathématiques 93" ont été conçues pour être reproduites ou poursuivies, dans différents contextes. Toutes les conditions sont remplies pour ces futurs développements: il reste une grande quantité de résultats à analyser, les textes de préparation sont disponibles, les animateurs sont devenus des formateurs et sont disposés à contribuer à la poursuite des travaux ébauchés.
Les groupes de travail du second jour ont fait émerger les grandes problématiques de l'enseignement des mathématiques dans notre période de transformations accélérées, comme l'ont fait également les discussions de coulisses, intenses et animées, renforcées par la diversité de nos contextes cantonaux. Des liens se sont tissés. Des questions communes sont ouvertes. Les conditions sont réunies pour que le mouvement esquissé vers la recherche de leur solution se poursuive.

Le temps des ouvertures

Il y avait des enseignants de tous les degrés à la Chaux-de-Fonds. Certains travaux ont pu être conduits à la fois dans des classes primaires et secondaires, avec quelques adaptations. On a pu constater que, d'un degré à l'autre, certaines constantes se retrouvent: dans les conceptions didactiques, dans la façon de considérer l'erreur dans la gestion de situations mathématiques, etc. Pour beaucoup, c'était l'occasion d'un premier regard vers l'aval ou vers l'amont de l'enseignement de sa discipline.
L'ouverture transfrontalière s'est révélée fructueuse. Les invités étrangers sont eux aussi entrés dans le jeu du colloque. Ils se sont montrés intéressés et actifs. Ils nous ont apporté leurs éclairages. Les questions qu'ils se posent, qu'ils nous posent, ne sont pas fondamentalement différentes des nôtres. Par leurs contributions, on mesure l'intérêt à voir au-delà de nos frontières, non seulement cantonales, mais nationales.
Une semaine de portes ouvertes sur les mathématiques et leur enseignement, était organisée à la Chaux-de-Fonds à l'occasion du colloque: expositions, films, conférences, concert, concours, atelier de formation permanente. L'ouverture était orientée, là, vers la population entière d'une région, au-delà des murs de l'école. L'intérêt suscité montre que ces pistes sont à explorer et qu'on peut faire quelque chose pour changer l'image des mathématiques, pour ouvrir son enseignement sur l'extérieur.

Vers un élargissement des champs de réflexion

Dans sa "conférence interactive", Marc Legrand, a démontré non seulement qu'un véritable échange est possible dans un auditoire d'une centaine de personnes, mais encore que le débat peut être approfondi et conduit scientifiquement. Aucun des participants ne le démentira, même si le thème du vrai et du faux est parfois dérangeant lorsqu'on est coiffé de l'autorité du maître de mathématiques.
Et ce thème du vrai et du faux nous contraint à élargir notre réflexion, à remonter aux finalités essentielles de notre enseignement des mathématiques, à redéfinir ses objectifs dans une perspective systémique où interviennent les besoins de la société, les rapports de pouvoir, l'affectivité, l'éthique.
Va-t-on remettre en question le calcul littéral? Le discours ex-catedra a-t-il encore sa place dans nos classes de mathématiques? Les épreuves communes et autres dispositifs de notation ou de sélection scolaire sont-ils incontournables? La dimension des objectifs généraux (et généreux) des plans d'études dépassera-t-elle celle du texte législatif ou du discours d'intentions?

La formation des maîtres

Si le bilan n'est encore prématuré on peut toutefois affirmer, sans risque de se tromper, que toute innovation future passera inexorablement par la formation des maîtres. Que ce soit dans le domaine de l'évaluation, de la gestion des situations-problèmes, de la prise de conscience des représentations de l'élève, de l'amélioration des connaissances mathématiques de base ou de tout autre aspect de l'apprentissage et de l'enseignement, on retrouve la même nécessité: les conceptions du maître de mathématiques devront évoluer, au même rythme que celui de la science, des techniques ou de la société en général.

Cette évolution est synonyme de formation continue et permanente. Non pas de "cours de recyclage" isolés ou d'enseignements stéréotypés. A l'image de ce que propose la didactique des mathématiques, il faudra certainement faire intervenir dans ce processus le travail d'équipe et ses interactions, l'esprit de recherche ou de découverte illustré par les "problème ouverts", les phases de mise en commun, l'idée de "contrat de formation", etc.

Les conditions sont remplies pour que, dès 1994, "Mathématiques 93" prenne sa véritable vitesse de croisière. Le chemin n'est pas aisé car les obstacles sont encore nombreux. Le colloque, préparé au mieux par ses responsables, commission et animateurs, s'est conclu par un appel aux participants: "la balle est dans votre camp!"

Ce camp n'est pas celui de la centaine d'heureux élus qui ont eu la chance de représenter leurs collègues. C'est celui de tous ceux qui sont concernés par l'enseignement des mathématiques: maîtres, élèves, autorités scolaires, associations d'enseignants, parents et société dans son ensemble.

agenda

Introduction à la pensée et à l'action systémique

Cours d'introduction à la pensée et à la pratique systémique. Institut de physique, rue A.L. Breguet 1, Moyen auditoire (3e étage). Début: jeudi 21 avril 12h15.

Les colloques ont lieu le mercredi tous les quinze jours à 17h15, salle D63, Bâtiment principal de l'Université, av. du premier Mars 26.

4 mai:	La modélisation par la dynamique des systèmes. Un exemple d'application: Y a-t-il une relation entre le chômage et le niveau du prélévement fiscal? (U. LaRoche, Zürich)
18 mai:	Le management du futur: Hiérarchie ou auto-organisation. De l'organisation à l'organisme (M. Gerber, Zürich)
1 juin:	L'avenir du travail (H. Ruh, Zürich)
14 septembre:	**L'organisation névrosée (P. Watzlawick, Palo Alto)**

Des séminaires-ateliers ont lieu certains mercredis à 17h15, salle D63. Prochaines séances : 27 avril, 11 mai, 8 juin.

Renseignements : Eric Schwarz, CIES, Université de Neuchâtel, 26, av. du 1er Mars, Tél. 038 25 38 51.

* * *

lu pour vous

Cortésy, J.-C. (1993) Modèles mathématiques et simulation. *Informatique, informations no 22*. Genève: Département de l'Instruction publique.

Cet article donne quelques informations sur l'utilisation des modèles mathématiques basés sur l'intégration numérique. Les domaines cités sont variés: biologie (croissance des plantes et des animaux, ...), économie (les fluctuations boursières, ...), physique (systèmes oscillants, ...), chimie (réactions oscillantes), géographie (démographie, ...). L'intérêt pédagogique de tels modèles se trouve principalement, pour l'auteur, dans le côté interdisciplinaire. A part le sujet lui-même, qui peut concerner toutes les branches du curriculum, il faut faire appel aux mathématiques, à l'informatique et ... aux langues pour consulter la documentation des systèmes informatiques (le système mentionné est STELLA).

Kuhn, T.S. (1983). *La structure des révolutions scientifiques*. Paris: Flammarion. (la première édition date de 1962).

Dans cet ouvrage déjà classique, Kuhn, physicien de formation, étudie la façon dont la science évolue. Il constate que, loin d'être un processus continu, l'accroissement des connaissances scientifiques procède par bonds, en évoluant d'un "paradigme" à un autre. Un paradigme (appelé "matrice disciplinaire" dans une nouvelle version de sa théorie) est constitué de plusieurs éléments dont:

- les généralisations symboliques, qui sont les règles facilement formalisables, par exemple: *action égale réaction*.
- les paradigmes métaphysiques, qui sont des croyances ou des heuristiques. Par exemple: *la chaleur est l'énergie cinétique des parties constituantes des corps*. Ou encore: *un circuit électrique peut être considéré comme un circuit hydrodynamique en état d'équilibre.*
- les valeurs: *les prédictions quantitatives sont préférables aux prédictions qualitatives*.
- les exemples qui sont les solutions concrètes de problèmes souvent simples mais très explicites: *problème du plan incliné*.

Un groupe scientifique s'identifie par un paradigme donné. Un étudiant commencera par étudier les exemples et à travers eux s'initiera aux autres élements du paradigme, ce qui lui permettra de s'identifier à un groupe. Un scientique s'occupera rarement de deux paradigmes différents (la naissance d'un nouveau paradigme est donc l'affaire de jeunes chercheurs) et son travail consistera principalement à tirer le plus possible parti d'un paradigme en épuisant le maximum de problèmes que l'on peut résoudre grâce à lui. L'idée de Popper que la science doit procéder par falsification des théories est donc fortement remise en cause par l'analyse réelle du processus du travail scientifique proposée par Kuhn. Plus même, il semble très rare qu'un paradigme soit véritablement remis en cause. La théorie de Newton continue à subsister à côté de celle d'Einstein. Et la mort d'un paradigme suit souvent celle des acteurs (théorie du phlogistique pour expliquer les réactions en chimie).

Pouquoi parler de révolution et non d'évolution ? L'analyse de Kuhn montre que l'adoption d'un nouveau paradigme ne suit pas toujours des critères d'efficacité objective démontrée. Si un nouveau paradigme permet de résoudre des problèmes nouveaux dont d'autres paradigmes ne peuvent rendre compte, il est très rare que lors de son adoption on sache si, globalement, il est plus efficace pour traiter les problèmes déjà résolus.

Serre, M. (1993). *La légende des Anges*. Paris: Flammarion.

L'évocation à travers un musée imaginaire du monde des messages. Comment traduire par un résumé l'atmosphère poétique de l'ouvrage, le message sur le message ? Voici ce qu'en dit l'auteur en page quatre de couverture:

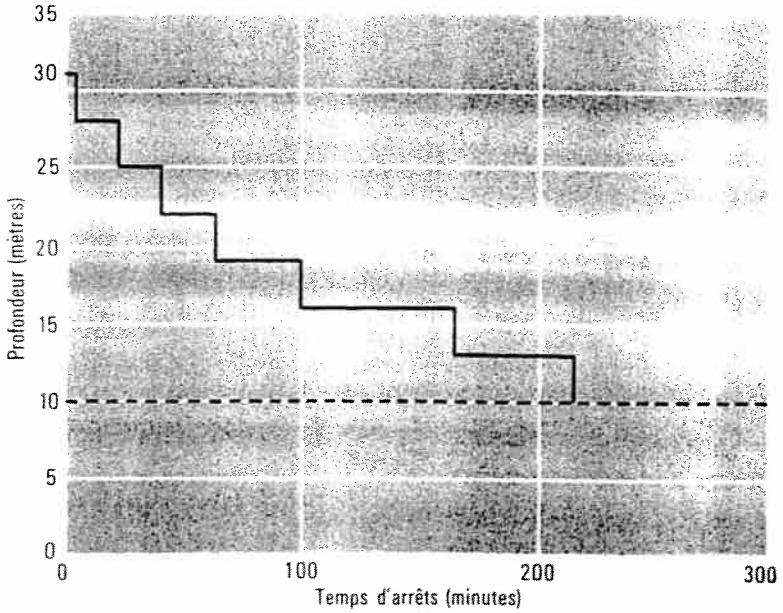
"Pour les religions monothéistes comme dans les anciennes légendes, l'Ange porte des messages.
Or nos sciences et nos techniques produisent cent métiers de communication, autant de réseaux mondiaux, une ville sans limites, d'incessants déplacements qui dessinent la carte d'un nouvel univers et induisent des problèmes planétaires, portés sans cesse vers nous par mille messagers.
Mais cette messagerie universelle s'accompagne d'indicibles injustices, d'une misère croissante, de famines et de guerres, d'une révoltante inégalité.
Voyons-nous, réalisée, partout, autour de nous, une nouvelle Légende des Anges, avec échangeurs et annonceurs, réseaux et passages, chutes et Démons, Puissances et Dominations, quête de miséricorde...?
Construisons-nous, sans la voir, une culture neuve qui convoque, ensemble, sciences, droits et religions, c'est-à-dire notre raison, nos exigences de justice et nos blessures d'amour ?"

Table de décompression

La remontée des plongeurs en mer profonde se fait toujours sous la menace du « mal des caissons » provoqué par la formation de bulles à partir de l'azote dissous dans les tissus pendant la descente. Ce mal peut ne pas être seulement douloureux mais aussi paralysant et même fatal. La remontée se fait donc assez lentement, pour que l'azote se dépose sans formation de bulles. Peut-être l'avez-vous vu au cinéma. Le plongeur s'arrête à différentes profondeurs lors de la remontée. Où croyez-vous qu'ait lieu la station la plus longue : près de la surface où le plongeur est presque à la pression atmosphérique, près du fond, ou à une profondeur intermédiaire ?

J'avais éliminé immédiatement la première possibilité, mais la table de décompression de la figure 3.9 me contredit : les stations les plus longues sont près de la surface. Pourquoi ?

Quelle est la profondeur maximum à laquelle vous pouvez plonger sans être obligé de vous arrêter pendant la remontée ?

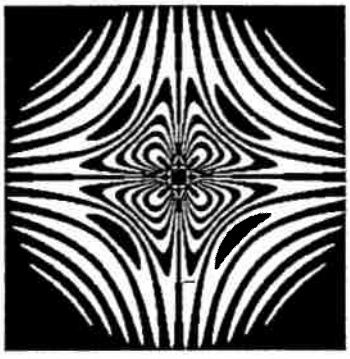


Tiré de J. Walker, Le carnaval de la physique. Pour la problématique générale, adressez-vous à P.-A. Bolle.

S O M M A I R E , No 17

Pour vous abonner au bulletin (10 Frs pour une année) ou pour demander votre adhésion à la Société des enseignants neuchâtelois de sciences adressez-vous à son président:

Michel Favre, rte de la Jonchère 13a, 2208 Les Hauts Geneveys (038/ 53 38 81)



sens