CONVERGENCES...

A.P.M.E.P.
Régionale de Lille

Le journal qui a de la suite dans les idées...
...Sans être monotone et borné !...

terme de rang 15 (mai 2002)

Responsable de la publication :
Pierre STEPHAN
34 Avenue des lilas 59800 LILLE.

Sommaire

A l'heure où nous éditons ce numéro 15 de CONVERGENCES, deux faits me semblent propulsés sur l'avant-scène des informations mathématico-politiques : la pétition de l'APMEP sur le maintien des horaires de mathématiques qui circule toujours, encore et encore, et la nomination de Luc Ferry comme Ministre de la Jeunesse, de l'Éducation Nationale et de la Recherche.
Je salue que " jeunesse " s'accorde avec " éducation " , cela marque la responsabilité endossée par notre génération pour que s'effectue son propre renouvellement : que filles et garçons puissent se détacher de ce qui les a faits tout en sachant d'où ils viennent . L'avenir dira ce qui est mis sous cet affichage, mais je voudrais revenir rapidement sur les deux points cités.

La pétition de l'APMEP peu explicative n'est pas corporatiste, elle ne vient pas de professeurs crispés sur leurs positions acquises, elle est le fait de professeurs , intellectuels d'abord , qui connaissent l'effort de concentration nécessaire à tout travail scientifique, qui savent qu'il faut du temps pour toute conceptualisation , et qui ont été piégés par leur propre générosité. Avoir insisté sur l'attention individuelle aux élèves, sur la prise en compte des progrès différenciés des uns et des autres, sur la nécessaire ouverture de la discipline a abouti à une mise en œuvre institutionnelle du " soutien " et de " l'interdisciplinarité " à travers aide individualisée, travaux croisés et autres TPE , tout cela, à moyens constants, c'est à dire en rognant sur les heures de cours et de TD.

Généralement, les conditions de mise en oeuvre de ces travaux interdisciplinaires ont exalté l'initiative de l'élève , refusant aux professeurs le droit de cadrer les choses en fonction de leurs intérêts , de ce qu'ils connaissent de leurs élèves à un niveau donné, mettant en difficulté leur savoir et leur culture . Cela en fin de compte n'a pas permis une dynamique des disciplines entre elles, a souvent envoyé les élèves dans des questions trop difficiles , contournées par des pratiques d'évitement et a crée un malaise chez les professeurs de mathématiques, dont la discipline est peu visible dans les questions de société proposées.

Finalement, au lycée, on a sorti de la classe de mathématiques, de physique et de SVT ce qui aurait pu être du travail d'un groupe de professeurs : mettre en résonance le contenu de leurs enseignements avec un champ de problèmes accessibles qui engagent des objets de connaissance communs. Pourquoi a-t-il fallu inventer un nouvel objet et bercer d'illusions les élèves ?

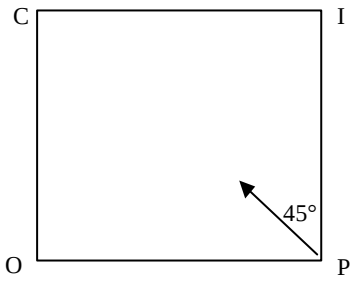
De l'autre côté voilà venir Luc Ferry, le président du CNP, philosophe médiatique, déconstructeur des déconstructions opérées par Foucault, Deleuze, Derrida, artisan créateur de l'allégement des programmes et des pôles dis ciplinaires au collège. Les mathématiques, avait-il écrit, sont à mettre dans le pôle " expression " et dans le pôle " connaissance du monde " et dans un moment d'agacement sans doute au delà de sa pensée, il s'est laissé aller à dire que les mathématiciens avaient encore à faire la preuve " de la légitimité de l'enseignement des mathématiques dans le secondaire ".

Nous verrons la suite mais nous répétons , que les mathématiques concourent à la formation de l'esprit, qu'elles sont une langue commune universellement répandue mais que leur interaction efficace avec les autres sciences et leur utilité les rend vulnérables. Il y a danger à renoncer à l'universalité des mathématiques et à les diviser suivant la nature actuelle de leurs applications sans souci des interactions possibles, elles seront d'autant plus précieuses qu' on préservera leur spécificité . A l'enseignement de savoir s'échapper d'une exposition séquentielle de mathématiques coupées du monde, à l'enseignement , quelque soit le niveau , de montrer par le discours, l'exercice , l'expérimentation, comment les mathématiques procèdent, s'emparant de concepts venus d'ailleurs , les travaillant, les rendant aussi simples et généraux que possible et de ce fait utilisables , de façon imprévisible bien loin du champ qui leur avait donné naissance. Les mathématiques dites élémentaires enseignées dans le secondaire offrent de nombreux exemples.

Anne-Marie MARMIER

Problèmes du numéro 15

Le billard



Une boule de billard part de l'angle P d'un billard rectangulaire de 2002 mm sur 2001 mm, avec pour trajectoire initiale la bissectrice de l'angle P.
Puis elle poursuit sa route sans perdre d'énergie.

La boule s'arrêtera t-elle en P, I, C ou O ou bien ne s'arrêtera t-elle jamais ?

Partager un triangle en deux

Soit un triangle ABC et soit un point P situé sur l'un des côtés du triangle.

Comment tracer une droite passant par P et partageant ABC en 2 surfaces de même aire ?

(problème issu de Géométriquement vôtre *Dunod*)

Un peu de cryptographie

Décryptez les deux messages suivants:

1°) EQPXGTIGPEGU NG OCICBKPG SWK C FG NC UWKVG FCPU NGU KFGGU

2°) RO HFUURHZRG WV KIVMWIV MLGIV ZOKSZYVG Z O ' VMEVIH.

RESSOURCES MATHEMATIQUES
En NORD PAS de CALAIS

Partant de la question " qu'est-ce que j'aurais aimé trouver en débutant dans l'enseignement ? " l'APMEP - Régionale de LILLE lance le projet de constitution d'un vade-mecum des ressources locales en mathématiques.
Cela prendra la forme d'un numéro spécial de Convergences à la rentrée 2002, massivement distribué aux PLC2 de cette nouvelle cohorte de matheux *(partant du principe que ce seraient des hors-académie mutés dans notre belle région).*

D'ici le mois de juin 2002, nous avons donc besoin de répertorier tout ce qu'il serait pertinent d'y mentionner : outre les grandes institutions (IREM de Lille, Apmep Nationale et Régionale) que nous connaissons bien, il existe des "niches" mathématiques mal connues et réparties dans la région. Par exemple des antennes du CRDP, des centres de culture scientifique locaux ne dédaignant pas les maths, les bibliothèques des centres IUFM ou des universités, certaines bibliothèques municipales sont bien dotées en ouvrages mathématiques.

Au sommaire également : un calendrier des manifestations mathématiques (Journées IREM ou organisées par certaines universités, Journées des éditeurs, rallye, …), un panorama de ce que peuvent proposer nos amis belges, un annuaire de clubs mathématiques existant (clubs Evariste, structures math en Jeans, …).
Le vade-mecum comportera également des références de sites particulièrement utiles pour dépanner ou fournir des idées : sites de mutualisation des documents (Sesamath en est l'exemple le plus pertinent), des sites académiques ou personnels.

C'est le travail de chaque adhérent que de collationner les renseignements utiles : modalités d'inscription, de participation si nécessaire, personne à contacter…
Chacun a sans doute déjà des pistes qu'il utilise régulièrement : faites-en profiter vos futurs collègues, et aussi les collègues plus anciens qui seraient passés à côté !
Le travail de collecte se fait essentiellement à distance, centralisé par Dominique CAMBRESY :
1 rue Basselart 59260 Hellemmes
(dcambresy@nordnet.fr).

Le document final sera rédigé en Juin par le Bureau de la Régionale, le site (http://www2.ac-lille.fr/apmep/) devrait relayer les avancées des travaux. Toutes les bonnes volontés sont bienvenues, pour rédiger ou distribuer le vade-mecum.

Dominique Cambrésy

CRYPTOGRAPHIE

Nous vous proposons sur plusieurs numéros de Convergences d'en connaître un peu plus sur diverses techniques historiquement mises en œuvre pour coder ou décoder, la place des mathématiques dans ces techniques, une bibliographie et une webographie commentées.

L'histoire de la cryptographie, c'est l'histoire d'une guerre. La guerre qui oppose, depuis des siècles, ceux qui ont quelque chose à cacher (qu'ils soient militaires, scientifiques, politiciens, financiers ou même amants illégitimes) et ceux qui aimeraient bien savoir ce qu'on leur cache (les ennemis, les concurrents, les espions, les escrocs et même les maris jaloux).

Les deux camps se livrent une lutte sans merci. Dés que l'un a trouvé un nouveau moyen de chiffrer ses messages, le second se dépêche de trouver un moyen de les décrypter. Et, jusqu'à présent, il y parvient toujours. Ce n'est qu'une question de temps et de moyens.

Cultivée depuis l'antiquité, la cryptographie (du grec *kruptos*, caché, et *graphein*, écrire) est plusieurs fois millénaire. Dans la Chine antique on utilisait déjà la stéganographie, c'est à dire l'art de dissimuler un message secret dans un texte d'aspect anodin. En Inde, le célèbre «Kàma-Sùtra» recommandait aux femmes d'apprendre - entre autres choses - l'art des écritures secrètes qui doit leur permettre de dissimuler leurs liaisons. En Mésopotamie, une autre grande civilisation de l'antiquité, on remplaçait des mots par des nombres. En Grèce, on utilisait un instrument appelé «*scytale*» pour mélanger les lettres d'un message...

Fondamentalement, il existe deux méthodes de cryptage, qui sont d'ailleurs toujours utilisées de nos jours. Les confusions qui mélangent l'ordre des symboles contenus dans le message (transpositions) et les substitutions qui remplacent un symbole par un autre. Bien sûr, sur la base de ces deux techniques, une multitudes de variantes, plus ou moins complexes, plus ou moins efficaces, ont été inventées.

Webographie Part I

http://lwh.free.fr/index.html

Ce site est consacré à l'algorithmique et à la programmation. Il propose de nombreuses démos d'algorithmes fondamentaux (tris, jeux, cryptographie...), un langage Logo, des cours à télécharger et un support pédagogique pour les étudiants préparant la Valeur d'Accueil et de Reconversion à l'Informatique du Camos/Cnam.

Pour la partie cryptographie, le gros inconvénient est qu'il propose des mises en œuvre d'algorithmes inspirés des modèles : par exemple l'alphabet des "Hommes dansants" n'est pas conforme à celui de Conan Doyle. A manier avec cette restriction en tête.

http://www.vectorsite.net/ttcode.html

Ce site en anglais est fort bien documenté et va des techniques antiques jusqu'aux raffinements informatiques actuels

http://mantis.free.fr/main.htm

Ce site est consacré à la stéganographie et à la cryptographie : marquage de textes, tatouages d'images sont bien abordés. Une bibliographie fournie permet d'aller plus loin après les aperçus.

http://www.chez.com/nopb/crypto.html#menu

Ce document numérique a trois ambitions principales: La première est d'expliquer et de clarifier ce qu'est le chiffrement tout en mettant en valeur ce qu'il peut apporter dans notre vie de tous les jours. Le second est de permettre à toute personne non spécialiste en Informatique ou en Mathématiques, donc à un large public, de découvrir rapidement ses différents aspects essentiels : principales méthodes utilisables, techniques de base et vulnérabilité ou non de ces dernières. Enfin il se veut faire un point rapide mais précis sur les réglementations relatives à la cryptographie en vigueur en France aujourd'hui.

http://titan.glo.be/tsf/ : Un petit site par la taille qui présente clairement quelques techniques.
http://janus81.free.fr/: Un site clair et bien documenté avec des exemples pratiques, sur les méthodes artisanales**.**

Dominique Cambrésy

Dans le prochain numéro : "Cryptographie et Littérature", "Analyse de fréquences" et la suite des biblio-webo-graphies.

Le Bloc-notes...

Prochaines réunions du groupe de travail « ***mathématiques et autres disciplines*** »:
Mercredi 22 mai à partir de 14 heures
Lycée J.B Corot
133 rue St Vaast Douai

Au programme :
Introduction de la fonction exponentielle à partir du phénomène de la radioactivité.
Présentation des programmes de physique de collège.

Du côté de l'IREM :

- Il est tout juste encore temps de s'inscrire au ***rallye mathématique*** des collèges, dont la finale a lieu le Samedi 8 juin.
- Une nouvelle brochure IREM est disponible : « ***Vie des mathématiciens*** », recueil de 40 notices biographiques (1,5 euros). Contact: 03 0 43 41 81, *irem@univ-lille1.fr*

A noter :

- 3 nouvelles brochures APMEP (voir le dernier BGV) et le projet d'une demi-journée de rentrée de l'APMEP régionale dur le thème des TPE et des itinéraires de découverte le 16 octobre 2002.

- Le mercredi 5 juin 2002, ***l'ARPAM*** (association pour la réalisation du parc d'activités mathématiques) organise à l'université de Valenciennes une journée de formation pédagogique à l'intention des enseignants de l'académie de Lille.

Renseignements : ARPAM : 15 av de Vaularon 91940 Gometz-le-Chatel
tel 01.69.07.08.91

Thème de la journée : "***Comment la Nature remplit-elle l'Espace*** ? 1 : Frises, Pavages"

Dans les nouvelles parutions

" Deux livres brochés, humbles et riches, concernant les mathématiques, viennent de paraître aux éditions Odile Jacob . Il faut les lire absolument et les mettre en interaction avec notre enseignement des mathématiques à quelque niveau que ce soit, et quelque soit le fond de déprime dont il s'échappe :

L'Enseignement des sciences mathématiques
Il s'agit du rapport au Ministre, sous la direction de J.P Kahane, qui regroupe les travaux de la Commission de réflexion sur l'enseignement des mathématiques. Les thèmes abordés sont : l'Informatique, les Statistique et Probabilités , la Géométrie, le Calcul , ils sont suivis de recommandations et suggestions.

L'Université de tous les savoirs - les Mathématiques - Vol 13
Différentes contributions par les plus grands noms des mathématiciens actuels sont présentées : fondements, énigmes, relation avec la société, géométrie, finance et économie, perspectives sur les recherches actuelles. "

Le système R.S.A.

A l'heure du développement de l'informatique, des réseaux, du commerce et du courrier électronique, préserver la confidentialité des informations est devenue indispensable.
Le système RSA assure la confidentialité d'un message, et garantit également son authenticité. Nous verrons en effet qu'il garantit l'envoi du message sans que ni l'émetteur ni le récepteur puissent nier la transaction. En outre il est accessible à tous, sous réserve de posséder un ordinateur et un logiciel adapté au système RSA..
Le système R.S.A. du nom de ses créateurs Rivest, Shamir et Adleman (1977) est basé sur le principe suivant:

Soit un message *M*.
M est constitué d'une série d'entiers, chacun d'eux étant inférieur à un entier N (de l'ordre de 10^{100}).
Par exemple, « bonjour » donnerait 02151410152118 si chaque lettre est codé par sa position dans l'alphabet.
Si le message est trop long, il est découpé en plusieurs tronçons de taille inférieure à N.
Toute personne utilisant le système RSA possède deux clefs symétriques (ce sont des entiers) : une clef publique (connue de tous) et une clef privée (connue d'elle seule).
Bernard veut donc envoyer son message *M* à Sophie.
Il connaît la clef publique de Sophie, avec laquelle il code son message *M* qui devient alors *M'*.
Le message *M'* n'a alors plus aucun sens. Seule, la clef symétrique, c'est à dire la clef privée de Sophie, peut transformer M' en M. Comme seule Sophie connaît sa clef privée, elle seule peut décoder le message envoyé par Bernard.
Le système RSA est un algorithme dit asymétrique: la clef servant au chiffrement est différente de celle servant au déchiffrement.

Le fonctionnement du système RSA est basé sur la proposition suivante :

Proposition

Soit un entier $M < N = p\,q$ (p et q sont premiers), tel que M ne soit ni multiple de p, ni multiple de q.
Soit C_1 un entier tel que PGCD (C_1 ; (p-1)(q-1)) = 1.
Soit C_2 l'entier le plus petit telque $C_2C_1 = 1 \bmod [\,(p-1)(q-1)\,]$
On a alors: $M^{C1} = M' \bmod (N)$ ssi $M'^{C2} = M \bmod (N)$

Démonstration de la proposition

D'après le théorème de Bézout, il existe C_2 entier naturel et a entier relatif tels que $C_2C_1 + a(p-1)(q-1) = 1$
On choisit pour C_2 l'entier le plus petit possible.
On a donc également PGCD (C_2 ; (p-1)(q-1)) = 1.
et enfin $C_2C_1 = 1 \bmod [\,(p-1)(q-1)\,]$
$M'^{C2} - M^{C1C2} = (M' - M^{C1})(M'^{C2-1} + M^{C1}M'^{C2-2} + \ldots + M^{C1(C2-1)})$
Donc $N / M'^{C2} - M^{C1C2}$ car $N / M' - M^{C1}$.
Comme l'entier premier p ne divise pas M, d'après le théorème de Fermat on a : $p / M^{p-1} - 1$.
De même, $q / M^{q-1} - 1$.
Remarquons que $(X^{ab} - 1) = (X^a - 1)(X^{a(b-1)} + X^{a(b-2)} + \ldots + 1)$ (*)
D'où $p / M^{p-1} - 1 / M^{(p-1)(q-1)} - 1$ et $q / M^{q-1} - 1 / M^{(p-1)(q-1)} - 1$
D'où $N = p\,q / M^{(p-1)(q-1)} - 1$.
$M^{C1C2} - M = M^{1 + k(p-1)(q-1)} - M = M(M^{k(p-1)(q-1)} - 1) = M(M^{(p-1)(q-1)} - 1)(M^{(p-1)(q-1)(k-1)} + \ldots + 1)$ d'après (*)
Donc $N / M^{C1C2} - M$.
$M'^{C2} - M = (M'^{C2} - M^{C1C2}) + (M^{C1C2} - M)$
Donc $N / M'^{C2} - M$.
Finalement $M'^{C2} = M \bmod (N)$.

Exemple
N = 13 x 7 = 91.
C_1 = 5. PGCD (72 ;5) = 1. C_2 = 29.
C_1C_2 = 145 = 1 mod (72)
Soit M = 88 , ni multiple de 13, ni multiple de 7.
On a : $88^5 = 30 \bmod (91)$ et $30^{29} = 88 \bmod (91)$

Dans un "annuaire" , que consulte Bernard, figure [Sophie, N, C_1]. C_1 est la clef publique de Sophie.
Bernard veut envoyer un message M à Sophie.
Il détermine M' tel que $M^{C1} = M' \bmod (N)$. Puis il envoie M' à Sophie.
Puis Sophie retrouve M à l'aide de $M'^{C2} = M \bmod (N)$. C_2 est sa clef privée.

En reprenant l'exemple précédent, 5 et 29 sont les deux clefs de Sophie.
Bernard code son message à l'aide de la clef publique de Sophie 5 , et Sophie décode le message reçue à l'aide de sa clef privée 29.
En réalité les clefs sont des entiers de l'ordre de 2^{256} (256 bits).

Si un espion intercepte le message M', il ne peut pas le décoder car bien que connaissant [Sophie, N, C_1] il lui est impossible de déterminer C_2 puisque C_2 est calculée à l'aide des deux facteurs premiers p et q inconnus. Et comme N est très grand, il ne sait pas le factoriser. Dans le cas contraire, RSA perdrait toute sa fiabilité.
En effet, si un ordinateur puissant peut décider de la primalité d'un entier d'une centaine de chiffres en quelques minutes, décomposer un tel nombre entier en facteurs premiers est pratiquement impossible. Cependant des progrès importants en théorie des nombres et/ou une augmentation conséquente de la puissance de calcul des ordinateurs peuvent remettre en cause tout le système.

Signature du message M.

Soit un message M. Il existe des fonctions mathématiques qui transforment M en un entier s(M) bien plus petit appelé signature de M, le "caractérisant".
S(M) constitue en quelque sorte une empreinte unique du message M.

Ces fonctions sont d'ailleurs intégrées dans les navigateurs du web.

Reprenons la situation précédente :

Après avoir déterminé M', Bernard calcule s(M').
Puis, à l'aide de sa clef privée (!), transforme s(M') en M''.
Enfin il envoie M' et M'' à Sophie.
Quand Sophie reçoit le message, elle commence par déterminer s(M')=M1, signature du message reçu.
A l'aide de C2, sa clef privée, Sophie transforme M' en M.
A l'aide de la clef publique de Bernard, elle transforme M'' en
s(M')=M2 signature du message original.
(En effet, étant donné le caractère des deux clefs, on peut coder un message avec sa clef privée, auquel cas, la clef publique étant connue de tous, chacun, dès lors qu'il en connaît l'expéditeur, peut décoder le message).
Si M1<>M2 alors cela signifie que le message a été altéré (lors de son voyage sur le web par exemple)
Si M1=M2 alors

1) Le message n'a pas été altéré.

2) Le message est réellement envoyé par Bernard, car seule la clef publique de Bernard permet d'inverser le codage effectué avec sa clef privée, que seul il connaît. Ainsi, Bernard ne pourra pas nier l'envoi du message.

Cette méthode est fondamentale pour les relations fournisseurs-clients, banques-particuliers etc.…

Vous pouvez consulter les pages consacrées aux problèmes de codages dans :

- Cours d'algèbre - primalité, divisibilité, codes - *M.Demazure*, Ed Cassini , Paris 1997.
- Merveilleux nombres premiers - *J.P Delahaye*, Belin Pour la Science, Paris 2000.

Dans la revue REPERES IREM , des articles généraux :

- N° 37 Oct. 1999 : Arithmétique et cryptographie - *R.Noirfalise* , Irem de Clermont Ferrand
- N° 46 Janv. 2002 : Du chiffrement de César à la mathématique de la carte bancaire -
  D.J Mercier - IUFM Antilles Guyane, centre Guadeloupe.

Le livre suivant est particulièrement intéressant et donne une vue globale des techniques de la cryptographie, de son histoire et ses enjeux:

- Histoire de codes secrets de Simon SINGH chez J.C Lattès

Dans les bulletins de l'APMEP consacrés à l'arithmétique N° 432, 433, 434 de Janv. 2001 à Juin 2001, plus particulièrement l'article du N° 432 : Quelques activités arithmétiques liées aux codes correcteurs et à la cryptographie - R.Rolland, Irem de Marseille.