CONVERGENCES

terme de rang 20 (Octobre 2004)

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

Responsable de Publication
Thérèse Le Chevalier
1153 Boulevard de la République
59500 DOUAI
lechevalier@wanadoo.fr

A.P.M.E.P – Régionale de Lille

Sommaire

Editorial

Thérèse Le Chevalier.

Réunion de rentrée
Mercredi 13 Octobre à 14h30, Villeneuve d'Ascq, bâtiment M1

L'enseignement en spirale

Il est intéressant pour un enseignant d'explorer non seulement les matières au programme de sa classe mais aussi celles d'avant et d'après, puisque l'éducation mathématique forme un tout. On voit apparaître alors, dans le cursus collège-lycée des idées ou notions qui peuvent soutenir un enseignement en spirale puisque, de classe en classe, elles reviennent dans des contextes divers et éclairent des questions de plus en plus vastes.
Nous nous proposons d'illustrer ce propos en travaillant en atelier sur un(des) exemple(s).

1 Cryptographie et littérature (suite)

Dominique Cambresy – *dcambresy@nordnet.fr*

Les romans policiers ou d'espionnage actuels évoquent de plus en plus des thèmes liés à la cryptographie :

Dans « **Une vie d'espion** » d'Henry Porter (Balland 2003), c'est une photo compromettante pour un tortionnaire serbe qui est dissimulée sous forme de « bruit » dans un disque de musique classique, tandis qu'une bande de « pirates » fait passer via les ondes radio des révélations sur les turpitudes des services secrets occidentaux.

Dans « **Sacrifier une Reine** » de Laurie R King, c'est un Sherlock Holmes vieillissant associé à une jeune surdouée qui se trouve confronté à un jeu de piste sanglant. Un des indices est dissimulé dans des lacérations perpétrées dans la banquette d'un fiacre, formant une suite de traits dans laquelle il reconnaît des chiffres romains :

XVXVIIXXIIXIIXXIIXXIVXXXI.

Pour décoder ce message, une petite aide : un alphabet à base d'octal (base 8) est utilisé et voici sa correspondance :

1	2	3	4	5	6	7	10	11	12	13	14	15	16	17	20	21	22	23	24	25	26	27	30	31	32
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Il ne vous reste plus qu'à retrouver les espaces entre les nombres romains pour retrouver le nom de la personne responsable de ces méfaits. Notons que cette touche « crypto » n'apporte pas grand chose à l'action romanesque : l'indice pourrait être obtenu d'une autre façon, sans recours quelconque à un code, et d'ailleurs on peut utiliser le code sans lire le roman, la preuve !

Dans « **Red Rabbit** » de Tom Clancy, nous avons droit à une nouvelle aventure de Jack Ryan, agent de la C.I.A. immortalisé au cinéma sous les traits de Alec Baldwin dans « **A la poursuite d'Octobre Rouge** », puis par deux fois ceux d'Harrison Ford, et dernièrement ceux de Ben Affleck dans « **La somme de toutes les peurs** ». Au début de sa carrière, il est mêlé à l'extraction d'un fonctionnaire des services secrets soviétiques révolté par le projet d'Andropov d'assassiner le Pape. Epoque oblige, pas de téléphone portable ni d'ordinateur ultra-perfectionné mais d'antiques masques jetables, dont le fonctionnement laborieux nous est décrit : des classeurs renferment des listes créÂées aléatoirement : une antenne hypersensible étant reliée à un télex, le récepteur placé entre les deux écoutait le bruit de fond atmosphérique et le télex interprétait ces « signaux » en une succession de lettres morses, que la machine à côté imprimait scrupuleusement. En fait, plusieurs de ces machines étaient interconnectées de façon que le caractère aléatoire du bruit de fond atmosphérique soit à nouveau brouillé pour aboutir à un charabia rigoureusement imprévisible. C'est de ce charabia qu'étaient composés les masques jetables qui étaient censés donner des cribles de transposition totalement aléatoires qu'aucune formule mathématique ne pouvait prédire et par conséquent décrypter. Le chiffrement par masque jetable était universellement considéré comme le système de cryptage le plus sûr. A condition de ne pas utiliser deux fois le même masque, d'où le nom de « jetable », sinon des correspondances peuvent être établies.

Le roman « **Enigma** » de Robert Harris, adapté au cinéma dans le film éponyme, ainsi que la BD « **Le Théorème de Morcom** » de Goffin et Peeters nous plongent dans la Seconde Guerre Mondiale, à Bletchley Park, là où a été cassé le code produit par la machine Enigma. Autour du mathématicien Alan Turing, une équipe d'experts composée de scientifiques, de linguistes et d'historiens est chargée de décrypter les messages interceptés par les Alliés et codés par une machine électro-mécanique utilisée sur tous les sous-marins et postes de commandement allemands. Cette machine permettait de brouiller toute recherche par analyse de fréquences en étant équipée de plusieurs rotors : à chaque frappe le rotor tourne d'un cran donc l'alphabet est décalé et si l'on retape la même lettre plusieurs fois, le résultat change. Chaque rotor ayant 26 positions, une machine équipée de 3 rotors permet $26 \times 26 \times 26$ possibilités. Les investigations pour casser un tel code étant hors de portée du calcul humain, l'équipe d'Alan Turing a mis au point un des premiers calculateurs, qui allaient ensuite devenir nos ordinateurs actuels.

Le roman est le plus intéressant car on suit les aventures d'un proche assistant de Turing dans les divers services, ainsi que les affres des décodeurs quand les allemands durcissent leur code. La BD propose une enquête sur la mort d'un obscur mathématicien qui se révèle être un des principaux décrypteurs d'Enigma, mais cette enquête gêne beaucoup certains services secrets...

Signalons tout de même que le fait pour les Alliés de pouvoir décoder les messages allemands sans que ceux-ci ne s'en doutent a permis selon les spécialistes de gagner la guerre avec au moins une année de moins. De lourdes pertes humaines ont été ainsi épargnées.

Un autre roman a pour « personnage » la machine Enigma : le volumineux « **Cryptonomicon** » de Neal Stephenson. Nous y suivons plusieurs intrigues ayant lieu en des époques différentes mais impliquant aujourd'hui les descendants des protagonistes de l'époque de la Seconde Guerre Mondiale. D'un côté l'armée américaine parvient à casser l'équivalent japonais de l'Enigma, tandis qu'une équipe de militaires est spécialement mise en place en Europe pour dissimuler aux Allemands que leur précieuse machine est une grande source de renseignements pour les Alliés. De l'autre côté une bande d'informaticiens tente de créer un paradis numérique, à l'instar des paradis fiscaux. Le tout est lié par la quête d'un trésor fabuleux... Un code est détaillé dans le roman, « **l'algorithme du Solitaire** » , utilisant des cartes à jouer. Aux dernières nouvelles, il n'aurait toujours pas été « cassé » , même s'il est peu pratique d'utilisation. Un article de Jean-Paul Delahaye dans « **Pour la Science** » n°284 de juin 2001 lui est consacré.

Dans « **Da Vinci Code** » de Dan Brown, nous avons droit à un roman dont le principal ressort est la cryptographie : ça commence quand un tueur s'étant introduit dans le Louvre pour tuer le Conservateur, on trouve sur le sol des marques invisibles écrites par la victime avant sa mort. Enigmatiques, elles offrent plusieurs niveaux de signification : suite de Fibonacci, référence à une société secrète, facéties de Léonard de Vinci dans ses tableaux, révélations sur la famille du Christ, luttes d'influence entre le Vatican et l'Opus Dei et une grosse dose d'ésotérisme, rien ne nous est épargné, mais pour une fois que la crypto est à l'honneur, ne boudons pas notre plaisir ! Lors du prochain salon des jeux et de la culture mathématiques à Paris (en juin), n'oubliez pas de visiter l'église Saint-Sulpice toute proche en guise de pèlerinage cryptographique...
Un indicateur du succès de ce roman est l'effervescence qui s'est emparée de nombreux forums de discussion quant à l'existence des carnets de Léonard de Vinci donnant les plans de son ingénieux « cryptex ». Beaucoup d'amateurs seraient prêts à financer la réalisation de cette machine, si seulement quelqu'un pouvait en fournir les plans !
Néanmoins un article du numéro de « **Science & Avenir** » d'août 2004 pointe un certain nombre d'erreurs et d'approximations, ce qui devrait refroidir les ambitions de bon nombre de ses aficionados !
Notons que ce gros succès en librairie va être porté à l'écran l'an prochain sous la houlette de Ron Howard, avec Russel Crowe dans le rôle principal. Un nouveau film à mettre dans notre filmographie crypto, après « **Windtalkers** » qui nous faisait découvrir l'utilisation d'Indiens Navajos dans les transmissions américaines dans la guerre contre le Japon, leur langue étant un des rares dialectes inconnus des Japonais, et après « **U 571** » qui nous racontait la prise d'une machine Enigma à bord d'un sous-marin allemand par les Alliés, les courageux Anglais d'origine étant ici supplantés par des Américains sans doute plus « télégéniques »...
Tant que nous sommes dans les images animées, notons également que des documentaires existent bien que difficilement trouvables : « **La saga des communications secrètes** » en 3 volets nous vient du Canada, tandis que la BBC a produit une série en Angleterre. J'en profite pour passer une annonce : si quelqu'un a une copie de ces merveilles, qu'elle nous fasse signe !

Dans « **Le cercle de la croix** » d'Iain Pears, nous assistons à une enquête dans l'Angleterre du XVII^{e} siècle, à peine sortie de la période troublée de la guerre civile. L'un des protagonistes est le mathématicien John Wallis, célèbre entre autres pour ses travaux sur π et fondateur de la Royal Society, mais également maître-espion au service de la Couronne, comme avait pu l'être François Viète un siècle auparavant en France.
Le récit est très intéressant dans sa construction : quatre protagonistes racontent leur version autour d'un même meurtre, et la vérité émerge de ces entrecroisements. La cryptographie n'est pourtant pas l'élément essentiel : des lettres codées ont servi à faire accuser un des personnages et la technique de codage utilisée nécessite un livre précis, dans une édition suffisamment rare pour ne pas risquer trop de se voir découvert ! En voici un extrait, où le docteur Wallis nous détaille un peu son travail :

> *Le décodage est un art compliqué et c'était l'époque où il le devenait de plus en plus. Souvent il ne s'agissait que de deviner comment une lettre ou un groupe de lettres étaient remplacés par une autre lettre ou groupe de lettres : on déchiffre par simple substitution que (par exemple) « a » remplace « the » ; 4 signifie « king », d=l, f=d, h=on, g=i, v=s, c=n ; et il est assez facile d'en déduire que a4gvgcdhfh veut dire : « The king is in London. » Vous noterez que le procédé (très utilisé par le royaliste pendant la guerre, des âmes simples, il faut bien l'avouer) consistant à substituer une lettre par une autre est peu complexe, alors que celui qui consiste à substituer parfois une lettre à une autre lettre, mais parfois à une syllabe ou un mot, est plus difficile. Néanmoins il ne présente guère de problème. Ce qui est plus compliqué, c'est lorsque la valeur des lettres change constamment, selon une méthode proposée pour la première fois en Angleterre par lord Bacon, mais qui, paraît-il, avait été inventée, en fait, par un Florentin il y a plus de cent ans. Les Français en réclament aujourd'hui la paternité, ce peuple insolent ne supportant pas que quelque chose ne vienne pas de chez lui. Ils volent ce qui ne leur appartient pas : j'en ai moi-même pâti lorsqu'un misérable petit clerc du nom de Fermat osa déclarer que mes découvertes sur les nombres premiers lui revenaient.*
> *Je vais essayer d'expliquer le procédé. L'essence de la méthode c'est que l'expéditeur et le destinataire doivent avoir le même texte. Le message commence avec un groupe de chiffres : par exemple, 124,5 ; ce qui signifie que la clef commence page 124, au cinquième mot, de ce texte. Supposons que la page commence par « So Hatach went forth to Mordecai unto the street of the city, which was before the king's gate. » (Esther 4, 6 ...) Le cinquième mot, « to » , constitue votre point de départ, et vous substituez 't' à 'a', ce qui donne l'alphabet suivant :*
>
> *abcdefghijklmnopqrstuvwxyz*
> *tuvwxyzabcdefghijklmnopqrs*
>
> *si bien que votre message : « The king is in London. » devient « maxdbgzblbgehgwhg » . L'important c'est que, après un nombre de lettres donné, normalement 25, on passe au mot suivant, dans le cas présent « Mordecai », et on recommence, de telle sorte que m=a, n=b, etc. Il existe des variations sur cette méthode, bien sûr, mais l'essentiel c'est de s'assurer que la valeur des lettres change assez souvent pour qu'il devienne presque impossible de la deviner si l'on ne possède pas le texte sur lequel elle se fonde.*

Le romancier Ken Follett, spécialiste des romans d'espionnage, nous propose un intéressant exemple de code quasi parfait dans « **Le Code Rebecca** » : en 1942, au Caire, un espion nazi communique des renseignements à son

Etat-Major à l'aide d'un livre et d'une clef. Comment fonctionne ce système de codage ? Laissons Ken Follett nous l'expliquer lui-même :

> *« Wolff s'approcha du buffet où il dissimulait l'émetteur radio. Il prit le roman anglais et la feuille de papier sur laquelle était inscrit le chiffre du code. Il l'étudia. On était aujourd'hui le 28 mai. Il fallait ajouter 42 -le chiffre de l'année- à 28 pour arriver au numéro de la page du roman qu'il devait utiliser pour coder son message. Mai était le cinquième mois de l'année, aussi allait-il supprimer une lettre sur cinq dans la page. (...) » « Il décida d'envoyer comme message SUIS ARRIVE. M'INSTALLE. ACCUSEZ RECEPTION. Commençant en haut de la page 70 du livre, il chercha la lettre S. En supprimant une lettre sur cinq, le S était le dixième caractère de la page. Dans son code, il serait donc représenté par la dixième lettre de l'alphabet, le J. Il lui fallait ensuite un U. Dans le livre, la troisième lettre après le S était un U. Le U de SUIS serait donc représenté par la troisième lettre de l'alphabet, le C. Il y avait des façons particulières pour représenter les lettres rares, comme le X, par exemple. » « Ce type de code était une variation de la feuille unique de bloc, la seule forme de code indéchiffrable en théorie comme en pratique. Pour décoder le message, il fallait avoir tout à la fois le livre et la clef. »*

Ken Follett a effectivement raison ; un tel système est indécryptable si l'on en possède pas tous les éléments : livre et clef. Même si l'on doit garder à portée de main le livre au risque de se le faire voler, il ne sert pas à grand chose si l'adversaire ne dispose pas de la clé. Parmi les nombreuses aventures (romans d'espionnage, BD...) où un livre est utilisé comme moyen de transmettre un message de façon cachée, c'est le seul qui le rende quasi-incassable par l'adjonction d'une clé.

(*à suivre*)

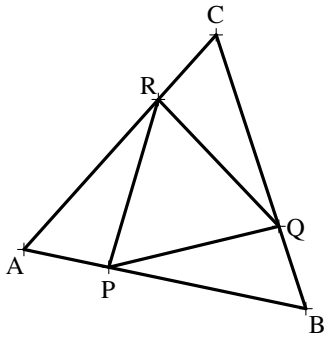
2 Annonces diverses

– **Histoire des Mathématiques à l'I.R.E.M.** – « Groupe E.M.T.A : Enseignement des Mathématiques et lecture de Textes Anciens. »
Avec le 0, le 1, les radicaux, les négatifs... les erreurs des élèves et les écueils sont nombreux ;mais les enseignants aussi, éprouvent des difficultés à enseigner l'algèbre au collège et au lycée : de la résolution des problèmes avec des nombres à celle avec des lettres, les équations, les règles d'opérations...
Le groupe E.M.T.A., s'engage à partir de la rentrée 2004, dans un nouveau projet d'acquisition de connaissances en histoire des mathématiques ; le thème général reste toujours compris dans la question : « La lecture de textes historiques, manuscrits ou traités, est-elle une ressource pour penser l'enseignement du calcul algébrique élémentaire ? »
Il s'agit d'abord de retourner à l'histoire pour y suivre comment concepts et outils s'élaborent et interviennent par nécessité. Ahmed Djebbar guidera le groupe dans l'élaboration de son programme de travail, dans le choix de textes et leur lecture commentée ; il a fait un exposé général de cadrage historique sur le sujet le vendredi 17 septembre.
Le groupe est ouvert à toutes celles et tous ceux que ce sujet nouveau intéresse.
Les prochaines séances auront lieu les vendredi 15 octobre (tradition grecque), vendredi 19 novembre (Egypte et Mésopotamie) et vendredi 10 décembre (exposé d'Ahmed Djebbar sur le traité de Al Kwarizmi

– **Groupe Jeux**
Lors de l'Assemblée Générale de la Régionale en mai dernier, il a été décidé l'activation (ou réactivation ?) d'un groupe « Jeux ». Les possibilités sont vastes, aussi pouvons-nous déjà lister quelques pistes de travail :
- mise en place d'une compétition amicale en fin d'année scolaire, à destination des enseignants : des énigmes mathématiques bien sûr, mais pas seulement : pourquoi ne pas s'entourer de collègues d'autres matières et proposer une compétition par équipes, par exemple de 4, avec des questions portant sur diverses disciplines ?
- création en dur de jeux issus des brochures « Jeux » de l'A.P.M.E.P. et d'autres revues : cela permettrait de les pratiquer, de les faire connaître aux adhérents présents et à venir lors de Journées Régionales ou d'autres manifestations. Le public visé irait alors des enfants aux adultes, enseignants ou non.
- recensement de jeux du commerce ayant un lien avec les mathématiques : jeux anciens ou encore disponibles, solitaires ou non, jeux pour enfants ou pour joueurs confirmés... Ce travail pourrait être effectué en liaison avec le groupe national qui poursuit également ce but (voir leurs dernières présentations dans le B.G.V.).
- création d'une exposition plus centrée sur un thème ludique et mathématique : les puzzles plans ou spatiaux, les labyrinthes, les jeux littéraires (oulipo et autres), les carrés magiques... La liste est longue et il est facile de proposer aux spectateurs des manipulations pour les rendre acteurs. L'exemple de la Régionale de Lorraine dans ce domaine est particulièrement intéressant.

3 Le coin des problèmes

La figure ci-contre vous est sans doute familière :
ABC est un triangle.
On a placé P sur [AB], Q sur [BC] et R sur [CA], de sorte que AP = BQ = CR.
On ne manque pas de méthodes pour montrer que,
si ABC *est un triangle équilatéral,* PQR *est un triangle équilatéral.*
Mais que pensez-vous de la réciproque :
Si PQR *est équilatéral, alors* ABC *l'est également ?*



Envoyez-nous vos solutions.

4 Adhésion

Le bulletin d'adhésion ci-dessous concerne l'année civile 2005. Il n'est pas destiné au réabonnement : si vous êtes à jour de votre adhésion en 2004, vous recevrez un bulletin de réadhésion en temps utile. Il n'est pas non plus destiné aux stagiaires qui bénéficient de conditions particulières, ni aux établissements. Il est prévu pour de nouveaux adhérents titulaires, contractuels ou vacataires, avec tous les avantages qu'il y a à adhérer avant janvier (les numéros non encore parus de l'année 2004 sont envoyés)
Si vous souhaitez des renseignements supplémentaires, (ou des bulletins complets) écrivez à T. Le Chevalier

Bulletin à retourner à APMEP 26 rue Duméril 75013 PARIS

Rappel des formules :
- « Tout APMEP » (Les 6 BGV, les 4 PLOT, les 6 Bulletins Verts, deux brochures à choisir dans la liste ci-contre)
- Adhésion seule : 27€ (Code **C2**)
- Adhésion + BGV : 32 € (Code **C5**)
- Abonnement au BGV : 20€ (Code **E4**)
- Abonnement à PLOT : 35€ (Code **E1**)
- Abonnement au Bulletin Vert : 70€ (Code **E2**)

Dans le cas du « Tout APMEP »

Mettre une croix (ou mieux un numéro d'ordre) face aux brochures choisies
☐ Deux numéros de Plot (Année 2003-2004)
☐ Jeux 6, niveau collège ou CM – n°144
☐ Olympiades Maths, niveau 1ères Sc. – n°158
☐ Un enseignement problématisé des mathématiques au lycée, tome 1 – n°150

Ecrivez **très lisiblement** *en majuscules, au stylo noir de préférence, et, dans votre intérêt, remplissez* **toutes** *les rubriques.*

M. ☐ Mme. ☐ **NOM, Prénom** Adresse personnelle : _____ _____ Code Postal :_____ Ville :_____ PAYS : _____ Téléphone : _____ E-mail : _____	*Etablissement d'exercice :* Collège ☐, LGT ☐,LP ☐, CPGE ☐, Université ☐. Nom de cet établissement : _____ _____ Adresse : _____ _____ Code Postal :_____ Ville :_____ PAYS : _____

Votre tarif d'adhésion-abonnements et son code :

⋆**« Le TOUT APMEP »**	Code A1	Tarif	44€
Eventuellement, adhésion simple de votre conjoint	Code C1	Tarif	13€

⋆ **SINON**, indiquez ci-dessous la formule choisie (C2, C5, E1, E2, E4), le tarif et le code correspondant :
Formule : _____ Code_____ Tarif_____ €

⋆ **Dans tous les cas** d'envoi de brochures gratuites, contribution au frais de port _____ 4,50€

Total_____ €

Date Signature

5 La vie de la Régionale

Nos rendez-vous de cette année

- L'enseignement en spirale le mercredi 13 octobre à Villeneuve-d'Ascq :
  voir présentation en page 1
- LaTeX (vaste sujet qui reste encore à délimiter) au collège de Beuvrages le mercredi 23 février.
- Nous envisageons de vous emmener à la Citadelle de Lille pour traiter du thème « les fortifications ». La date actuellement prévue est le samedi 28 mai. Mais rien n'est encore définitif.

Le bloc-notes

- L'Association pour la création de la **Cité des Géométries** organise un colloque :

  ARCHITECTURES, URBANISME ET GEOMETRIES

  « Des mesures pour l'Homme, l'Homme dé-mesuré ? »

  les 7 et 8 octobre 2004 à Maubeuge - Théâtre du manège
  Renseignements : Sandrine Labar - tél/fax 03.27.67.76.51 - citedesgeometries@free.fr
  http ://www.citedesgeometries.com

- **L'U.S.T.L. Culture** organise à l' Aeronef - av Willy Brandt , Euralille un colloque international

  « A PROPOS DE LA CULTURE »

  conférences et tables rondes alterneront pendant trois jours les 2, 3, 4 novembre prochain pour mettre en questions l'ambition démocratique d'une plus large ouverture à la culture.

  mardi 2 novembre :
  à partir de 14H : « La construction européenne au risque de ses cultures »
  en soirée : dialogue avec Taslima Nasreen

  mercredi 3 novembre :
  à partir de 9h : « Universalité et particularité »
  à partir de 14h30 :« Culture et barbarie »

  jeudi 4 novembre :
  à partir de 9h : « Instrumentalisation de la culture »
  à partir de 14h30 : « Transmission et création »

  contact : http ://www.univ-lille1.fr/culture/
  tél : 03 20 43 69 09

- **L'IREM de Lille** organise cette année, à Arras, le 1er décembre 2004, à Lille, le 12 janvier 2005, à Valenciennes le 26 janvier 2005 et à Calais, le 9 mars 2005 une journée consacrée à l'enseignement des mathématiques à l'école primaire et à l'articulation école-collège intitulée « Comment contribuer à améliorer l'articulation école-collège dans le cadre des apprentissages mathématiques ? »
  contact : IREM de Lille – tél : 03 20 43 41 81, 03 20 43 41 82
  http ://www.univ-lille1.fr/irem/ – irem@univ-lille1.fr

- Les **Journées Académiques** de l'**IREM de Lille** auront lieu les jeudi 7 et vendredi 8 avril sur le thème : « Apports des TICE dans l'enseignement scientifique »

- En droite ligne de la création d'un Groupe Jeu, nous rappelons que le **CIJM** (Comité International des Jeux Mathématiques) anime pendant plusieurs jours au mois de juin un **Salon des Jeux Mathématiques** à Paris (place Saint-Sulpice), destinée au grand public comme aux matheux, avec diverses compétitions et la présence de nombreux éditeurs.
  http ://cijm.org/

- La finale du **Rallye des Collèges** aura lieu le samedi 11 juin 2005, sur le campus de Villeneuve d'Ascq.

- Un colloque dont le tire provisoire est « La géométrie à travers les classes et les âges (de la liaison école-collège à la liaison collège-lycée) » devrait être organisé à Villeneuve d'Ascq les 20, 21 et 22 juin par les **commissions Inter-IREM Premier cycle** et **Géométrie**.