ANNEXES

IREM
123 Avenue Albert Thomas
87060 Limoges cedex

http://www.unilim.fr/irem

Université de Limoges

IREM Institut de Recherche
sur l'Enseignement des Mathématiques

Limoges, le Jeudi 28 août 2008

Le Directeur

aux

Animateurs de l'IREM

Affaire suivie par
Martine Guerletin

08/IREM/AN/MG/752

Téléphonne. 05 55 45 72 49
Télécopie 05 55 45 73 20
Mél irem@unilim.fr

Cher (e) ami (e) ,

La prochaine Journée Animateurs de l'IREM aura lieu le :

Jeudi 11 Septembre 2008 à 13h45.

Ordre du jour :

- Compte-rendu de l'ADIREM et du Séminaire de juin 2008 à Limoges.
- Préparation de l'année 2008-2009 (calendrier des stages et ERR, formation des groupes, fonctionnement, etc.).
- Divers.

A. Nezey.

ANIMATIONS DANS LE DOMAINE DES MATHEMATIQUES (IREM)

(En partenariat avec le Tournoi de Mathématiques du Limousin, le CIJM et Récréasciences)

Site de LIMOGES, *Espace Jules Noriac – Limoges*
du 19 au 21 novembre 2008 de 9h à 12h et de 14h à 18h

Jeux et manipulations mathématiques :
- *Atelier de pavages avec les triangles d'or et d'argent et les calissons.*
- *Atelier de jeux de grilles autour du sudoku avec les gratte ciel et immeubles et jardins.*
- *Jeux classiques (tour de Hanoï, puzzles, etc.).*
- *Arts et mathématiques, utilisation du pliage.*

Exposition « Les graphes »

Conférence-spectacle : Xavier VIENNOT, directeur de recherche au LaBRI, Université de Bordeaux. D'une lettre oubliée d'Euler (1707-1783) à la combinatoire et à la physique contemporaine le **18 novembre** au Conseil Régional du Limousin.

Site de GUERET, *grande salle de la Mairie – Guéret*
du 19 au 21 novembre 2008 de 9h à 12h et de 14h à 17h

Exposition ***« Les graphes »***

Jeux et manipulations mathématiques

Site de TULLE, *salle de l'Auzelou, avenue du Lieutenant Colonel Farot – Tulle du 20 au 21 novembre 2008.*

Jeux et manipulations mathématiques. Stand sur le Rubik's cube animé par Jérôme Dufour et ses élèves du collège Cabanis

Pour tout renseignement *:*
MARTINE GUERLETIN IREM
123 av A. Thomas - 87 060 LIMOGES Cedex
Tél : 05 55 45 72 49
Courriel : irem@unilim.fr

Université de Limoges
IREM Institut de Recherche sur l'Enseignement des Mathématiques

D'une lettre oubliée d'Euler (1707-1783) à la combinatoire et à la physique contemporaine

Conférence-spectacle

Vidéos, musique et textes

organisée par l'IREM de Limoges le

18 novembre 2008 à 19h30
au Conseil Régional du Limousin, 27 bd de la Corderie à Limoges

avec : Marcia Pig Lagos (textes), Xavier Viennot* (rétro et vidéo)

La « conférence-spectacle » sur la vie et l'œuvre de Leonhard Euler s'adresse à un large public et est accompagnée par deux violonistes et une conteuse.
Leonhard Euler grand savant universel et exceptionnel, mathématicien, physicien, astronome, ingénieur et philosophe, vécut à Bâle, Saint-Pétersbourg, Berlin et à nouveau Saint-Pétersbourg.
Il fut européen avant l'heure à l'époque du siècle des lumières. Il a été aussi membre étranger de l'Académie de Paris.

Entrée libre et gratuite

Au violon : extraits d'œuvres de J. S. Bach, Ch. De Bériot, A. Ponchielli, J. M. Leclair, P. I. Tchaikovsky,, L. Boccherini, J. F. Mazas, W. A. Mozart et J. W. Kalliwoda.

La conteuse Marcia raconte quelques épisodes ou péripéties de la vie d'Euler qui se déroule en cinq périodes. Chacune de ces périodes est introduite par un morceau d'époque au violon qui rappelle le pays où l'histoire va se dérouler. Ces « tranches de vie » personnelles sur Euler alternent avec l'exposé mathématique et scientifique relatif à son œuvre.

Contact : *IREM de Limoges*
05 55 45 72 49
irem@unilim.fr

* Xavier Viennot est directeur de recherche au CNRS au laboratoire de recherche en informatique de l'université de Bordeaux I.

Séminaire IREM-IUFM

Conférence

Mercredi 10 décembre 2008
à 18h30 au Conseil Régional du Limousin
27 bd de la Corderie à Limoges
Salle Lac du Causse (rez-de-chaussée du bâtiment A)

Université de Limoges
IREM Institut de Recherche sur l'Enseignement des Mathématiques

« Petite histoire de la monstruosité : les monstres ont-ils encore quelque chose à nous dire ? »

Michel Salamon
Professeur de Philosophie chargé de cours à l'Université de Limoges
Ancien chargé de mission à l'Observatoire d'Astronomie de Strasbourg

Entrée libre et gratuite

Contact : IREM de Limoges
05 55 45 72 49
irem@unilim.fr

S'il existe toujours une part de fantasme dans le regard que nous portons sur les monstres, il faut bien distinguer les monstres imaginaires – véritables stars du grand écran, de la littérature de science-fiction et des bandes dessinées américaines - et les monstres réels qui sont généralement éliminés après dépistage par les techniques contemporaines de diagnostique prénatal.
Les « monstres humains » sont par conséquent emblématiques de deux questions essentielles. Tout d'abord, comment ne pas voir à quel point ils demeurent, aujourd'hui comme autrefois, emblématiques de la question éthique fondamentale de l'acceptation de la différence et du handicap ? Mais aussi, si on considère les formes monstrueuses telles qu'elles se perpétuent dans notre imaginaire, les monstres révèlent l'essentielle problématicité de notre époque : si on les replace dans le contexte nouveau qui découle de la seconde guerre mondiale, ils annoncent « la fin de l'homme ».

Séminaire IREM - IUFM*

Jeudi 11 Décembre 2008

IUFM, 209 boulevard de Vanteaux, Limoges

9h	Accueil et informations diverses Valérie **LEGROS** (Directrice de l'IUFM) Abdelkader **NECER** (Directeur IREM) Michel **HAREL** (Directeur du département de Mathématiques de l'IUFM)
9h30	Exposé par Abdelkader **NECER**, (Directeur de l'IREM de Limoges) *« L'IREM dans la formation initiale et continue en mathématiques dans l'Académie »*
10h	Pause – Café
10h30	Conférence donnée par Marie-José **PESTEL** (Présidente du CIJM, animatrice IREM) *« Jeux et énigmes mathématiques : un outil pédagogique ** »*
12h	Repas
14h	**Ateliers tournants**
16h30	Bilan de la journée

** ouvert à tous les enseignants*

*** Les jeux mathématiques permettent d'avoir un regard différent sur l'apprenant : comment pourrait-il intervenir en évaluation ? Les jeux mathématiques « redistribuent les cartes » et redonnent une chance : ils devraient intervenir en remédiation. Les jeux et les énigmes mathématiques sont d'excellents « accélérateurs de neurones » pour tous !*

123, Avenue Albert Thomas – 87060 LIMOGES CEDEX
Tél. : 05 55 45 72 49 – Fax : 05 55 45 73 20 - Mél : irem@unilim.fr
url : www.unilim.fr/irem/

ATELIERS

N°	INTITULÉS	ANIMATEURS	CONTENU
1	Chercher et conjecturer avec les TICE	Colette CHAUPRADE et des membres de l'ERR « Mathématique au lycée »	Élaborer des activités pour développer chez les élèves la capacité à mobiliser les TICE pour résoudre un problème mathématique.
2	Utilisation du TBI	Jean-Louis BALAS	Initiation à l'utilisation du TBI, quelques exemples d'activités
3	Liaison 3^{e} – 2^{nd}	Groupe IREM « Liaison 3^{e}-2^{nd} »	QCM et démonstration dans les différents domaines des mathématiques dans l'optique de la liaison 3^{e}-2^{nd}.
4	RADIO IREM	Michel LAFONT	Un professeur de collège, animateur de l'IREM répond aux questions des stagiaires sur - la gestion de la classe, - la correction de devoirs, - les classes hétérogènes, - …..
5	Jeux mathématiques	Des membres de l'ERR « Mathématiques et Jeux »	Une promenade dans les jeux du Tournoi Mathématique du Limousin : jeux numériques, logiques ou géométriques. Des jeux pour tous car «il faut commencer tôt pour aller loin ». Des jeux qui sont de vrais outils pour devenir « acteur dans la construction de son savoir ».

123, Avenue Albert Thomas – 87060 LIMOGES CEDEX
Tél. : 05 55 45 72 49 – Fax : 05 55 45 73 20 - Mél : irem@unilim.fr
url : www.unilim.fr/irem/

IREM
123 Avenue Albert Thomas
87060 Limoges cedex

http://www.unilim.fr/irem

Université de Limoges

IREM Institut de Recherche
sur l'Enseignement des Mathématiques

Limoges, le vendredi 5 décembre 2008

Le Directeur

aux

Animateurs de l'IREM

Affaire suivie par
Martine Guerletin

08/IREM/AN/MG/775

Téléphonne. 05 55 45 72 49
Télécopie 05 55 45 73 20
Mél irem@unilim.fr

Cher (e) ami (e) ,

La prochaine Journée Animateurs de l'IREM aura lieu le :

Jeudi 18 décembre 2008 à 14h.

Ordre du jour :

14h : Informations sur la

- Mastérisation.
- Réforme du lycée.

14h30 : Quelles mathématiques dans l'Université numérique ?

15 h : Préparation des journées académiques, départementale et maths pour tous.

- Préparation du PAF 2009-2010.

16h45 : Assemblée Générale de l'Association des Amis de l'IREM (A.A.I.).

A. Nelep.

Le **C**omité **I**nternational des **J**eux **M**athématiques, le **T**ournoi **M**athématique du **L**imousin et l'**A**ssociation des **P**rofesseurs de **M**athématiques de l'**E**nseignement **P**ublic, l'**I**nstitut de **R**echerche sur l'**E**nseignement des **M**athématiques vous invitent à la 4e édition de la journée

Mathématiques pour tous

Université de Limoges
IREM Institut de Recherche sur l'Enseignement des Mathématiques

Mercredi 28 janvier 2009

De 14h à 17h30 : *« Jeux et manipulations »*

Activités destinées au grand public et inspirées de sujets du Tournoi Mathématique du Limousin ou d'autres compétitions de jeux mathématiques.

à la Bibliothèque Francophone Multimédia de Limoges (BFM), espace jardin d'hiver

À 18h : conférence

« Jeux et énigmes mathématiques dans la construction des savoirs »

Marie-José PESTEL, présidente du Comité International des Jeux Mathématiques, animatrice IREM

au Conseil Régional du Limousin, salle lac du Causse

Entrée libre et gratuite

Contact : IREM de Limoges - 05 55 45 72 49 - irem@unilim.fr

Université de Limoges

IREM Institut de Recherche sur l'Enseignement des Mathématiques

JOURNÉE DÉPARTEMENTALE de la CORRÈZE

Jeudi 19 février 2009

Lycée Edmond Perrier à Tulle

9h – 9h45	Accueil et informations diverses par Gérard **LAGARDE**, proviseur du lycée Abdelkader **NECER**, directeur de l'IREM
9h45 – 10h30	Béatrice **QUELET**, IA-IPR de Mathématiques
10h30 – 10h45	Michel **LAFONT**, enseignant au collège Clémenceau à Tulle et le groupe de Tulle Liaison 3e-2e « *Informations sur les nouveaux programmes au collège* »
10h45 – 11h	Pause
11h00 – 12h45	Pascal Kossivi **ADJAMAGBO**, Professeur à l'Université Pierre et Marie Curie (Paris 6) « *La nature, l'essence et la finalité des mathématiques à la lumière du papyrus de Rhind* »
13h00 – 14h30	Repas
14h30 – 17h	Ateliers tournants (voir page suivante)

123, Avenue Albert Thomas – 87060 LIMOGES CEDEX
Tél. : 05 55 45 72 49 – Fax : 05 55 45 73 20 - Mél : irem@unilim.fr
url : www.unilim.fr/irem/

ATELIERS

N°	INTITULÉS	ANIMATEURS
1	Histoire et opérations arithmétiques	Pascale SÉNÉCHAUD
2	Logiciels de mathématiques et tableau blanc interactif	Samuel ADABIA
3	Échanges sur les problèmes spécifiques de l'enseignement des mathématiques au collège	Michel LAFONT Madeleine MCHARD
4	Activités mathématiques en relation avec le domaine technique et professionnel	Monique VARLET

123, Avenue Albert Thomas – 87060 LIMOGES CEDEX
Tél. : 05 55 45 72 49 – Fax : 05 55 45 73 20 - Mél : irem@unilim.fr
url : www.unilim.fr/irem

Conférence

Mercredi 11 mars 2009
à 14h30 au Conseil Régional du Limousin
27 bd de la Corderie à Limoges
Salle Lac du Causse (rez-de-chaussée du bâtiment A)

Université de Limoges
IREM Institut de Recherche sur l'Enseignement des Mathématiques

« L'univers a-t-il une forme ? »

Roland LEHOUCQ
Astrophysicien au Service d'Astrophysique du Commissariat à l'Énergie Atomique (CEA) de Saclay

S'il est possible d'apprécier la forme d'une galaxie ou d'un amas de galaxies, celle de l'Univers nous reste difficilement accessible. Les notions géométriques sont généralement intuitives lorsqu'il s'agit du plan ou de la sphère car nous pouvons mentalement les plonger dans notre espace à trois dimensions pour se les représenter comme "vue de l'extérieur". Mais, privés d'intuition géométrique directe d'un espace à quatre dimensions, nous avons les plus grandes peines à imaginer l'infinie variété des domaines à trois dimensions qui pourraient décrire notre univers. Ce biais nous conduit à utiliser les représentations les plus simples, imaginant par exemple l'univers comme un espace à trois dimensions ayant les mêmes propriétés que le plan à deux dimensions. Pourtant, nous n'avons pas plus de raisons de croire que notre univers est ainsi fait que les anciens n'en avaient de croire que la Terre était plate. Au cours de cette conférence, je montrerai qu'il n'est pas contradictoire pour un espace à trois dimensions d'être à la fois limité et dépourvu de bords et que l'aspect infini de notre univers ne pourrait être qu'une illusion imposée par sa forme particulière. Il faut donc tenir compte des univers modèles, munis de topologie étrange pour notre intuition commune, pour lesquels l'univers observable est plus grand que l'univers réel. Je montrerai qu'il semble aujourd'hui possible de tester expérimentalement cette hypothèse en en cherchant des traces dans le rayonnement diffus cosmologique.

RECRE@SCIENCES CCSTI Limousin

culture et jeux mathématiques CIJM

Cnam CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Entrée libre et gratuite

Contact : IREM
de Limoges
05 55 45 72 49
irem@unilim.fr

Conférence*

Mercredi 1er avril 2009
à 18h00 au Conseil Régional du Limousin
27 bd de la Corderie à Limoges
Salle Lac du Causse (rez-de-chaussée du bâtiment A)

Université de Limoges
IREM Institut de Recherche sur l'Enseignement des Mathématiques

La formation du citoyen en France à la lumière des études internationales

Le cas des mathématiques et l'étude PISA

Antoine BODIN
Professeur agrégé de mathématiques – Chercheur associé à l'INRP
Fondateur et responsable de l'Observatoire EVAPM de 1987 à 2007

Entrée libre et gratuite

Contact : IREM de Limoges
05 55 45 72 49
irem@unilim.fr

À intervalles réguliers, les médias font état de la place de la France dans les évaluations internationales. Le public entend ainsi parler de TIMSS, de PISA, de PIRLS, etc. Il s'agit dans tous ces cas d'études visant à comparer, à travers le monde, ou au moins pour l'ensemble des pays développés, les acquis des élèves à tel ou tel âge (10 ans, 13 ans, 15 ans, ...), en lecture, en mathématiques, en sciences et dans quelques autres domaines.
La plupart de ces études cherchent à évaluer les compétences nécessaires pour une entrée réussie dans la vie adulte, pour l'insertion des jeunes dans le monde social et dans le monde du travail, mais aussi susceptibles de servir de base à des études ultérieures et à l'apprentissage tout au long de la vie.
La population visée par ces études est l'ensemble des jeunes, indépendamment des orientations qu'ils seront amenés à prendre ultérieurement. De ce fait il s'agit bien de l'éducation du citoyen et les compétences en question sont à rapprocher de celles qui constituent le socle commun de connaissances et de compétences.
Dans ce cadre, le public apprend que, pour la France, le niveau ainsi mesuré n'est pas brillant et, pire, qu'il ne cesse de baisser de façon absolue (par rapport à des normes fixes), comme de façon relative (par rapport à d'autres pays).
La conférence aura pour objet de présenter le cadre général et les objectifs de ces études et, en ce qui concerne les mathématiques d'en présenter les résultats d'une façon à permettre à l'auditeur de se faire une idée correcte leur signification. Cela signifie que les questions posées seront présentées et discutées et que les modes de traitement des résultats seront explicités.
Les résultats médiocres de la France ne seront pas niés, mais, mis en contexte ; ils seront relativisés et seront source de questionnement sur le fonctionnement de notre système éducatif et de propositions pour une meilleure prise en compte des enseignements que l'on peut tirer des études internationales.
Le lien sera fait avec les études d'évaluation menées par l'association des professeurs de mathématiques et l'institut national de la recherche pédagogique (EVAPM) ainsi qu'avec les évaluations menées par le ministère de l'éducation nationale (DEPP).

* organisée en marge de la Journée académique du 2 avril 2009 à la Faculté des Sciences et Techniques

Université de Limoges
IREM Institut de Recherche sur l'Enseignement des Mathématiques

Programme

Journée « Enseignement des mathématiques en Limousin »

Jeudi 2 avril 2009

Faculté des Sciences et Techniques (Limoges)

Amphi Couty

8h30 – 9h00	Accueil
9h – 9h45	Informations diverses par : Béatrice **QUELET**, IA-IPR de Mathématiques Abdelkader **NECER**, directeur de l'IREM
9h45 – 11h00	Antoine **BODIN*** *, professeur agrégé de mathématiques, chercheur associé à l'INRP, responsable de l'Observatoire EVAPM *« **Dissonances et convergences évaluatives*** *de l'évaluation dans la classe aux évaluations internationales »*
11h00 – 11h15	Pause
11h15 – 12h30	Jean-Claude **YAKOUBSOHN***, professeur de mathématiques à l'Université de Toulouse « ***Le pendule simple : un exemple pas si simple*** »
12h45 – 14h15	Repas
14h15– 15h45	Ahmed **DJEBBAR***, mathématicien et historien des sciences, Université de Lille *« **De la culture aux mathématiques*** *l'exemple de l'analyse combinatoire en pays d'Islam »*
15h45 – 17h15	Ateliers (voir détail page suivante)

* Résumé des conférences, voir page suivante.

** En marge de cette journée, Antoine Bodin donnera une conférence grand public le **mercredi 1er avril** à 18h au Conseil Régional du Limousin sur *« **La formation du citoyen en France : à la lumière des études internationales*** »

123, Avenue Albert Thomas – 87060 LIMOGES CEDEX
Tél. : 05 55 45 72 49 – Fax : 05 55 45 73 20 - Mél : irem@unilim.fr
url : www.unilim.fr/irem/

Résumé de l'exposé d'Antoine BODIN : L'évaluation est aujourd'hui omniprésente dans tous les systèmes éducatifs. Toutefois la lecture et la mise en relation des faits d'évaluation n'est évidente ni pour les enseignants, ni pour les élèves, ni pour aucune catégorie d'acteurs concernés. Par évaluation, nous entendons aussi bien celle qui est pratiquée, au

quotidien dans les classes que celle qui se fait dans le cadre des examens ou encore celle qui est pratiquée sur les personnels ou sur le système lui-même (EVAPM, PISA, IGEN…).
Des voix s'élèvent à l'interne comme à l'externe pour dénoncer la trop grande pression que l'évaluation met sur les élèves comme sur les enseignants. Ainsi il y aurait beaucoup trop d'évaluation dans notre système. À l'inverse, d'autres dénoncent la pauvreté des indicateurs relatifs aux acquis des élèves, ou encore la faible validité de nos examens (bac, brevet...).
Entre le regard évaluatif de l'enseignant dans sa classe et celui des divers « décideurs » ou « partenaires sociaux », la dissonance est manifeste. Peut-il y avoir davantage de cohérence ? Comment ? Cela est-il souhaitable ?
Dans quelle mesure, les actions d'évaluation convergent-elles pour faciliter les apprentissages, ou, du moins, pour ne pas les contrecarrer ? Dans quelle mesure, certains de leurs effets tendent-ils à se contrarier ? Si l'on veut éviter un schématisme réducteur, une vision systémique s'impose.
La communication reprendra le thème et le titre d'un article publié récemment dans le bulletin de l'APMEP (voir références). Le thème des études internationales (PISA et TIMSS) aura été développé la veille, et ne sera pas repris systématiquement dans cette intervention, mais des références aux questions et aux résultats de PISA seront faites.
La question de la problématique de évaluation du socle de connaissance et de compétences et de son rapport avec les études internationales sera aussi abordée en référence au travail effectué avec un groupe de l'IREM de Marseille.

Résumé de l'exposé de Jean-Claude YAKOUBSOHN : Le problème du pendule simple servira d'illustration au cours de l'exposé pour aborder les questions suivantes :
1- Comment modéliser automatiquement un problème physique ?
2- Pourquoi la modélisation fournit en général un problème du type F(x,x')=0 et non pas une équation différentielle x'=F(x) ?
3- Pourquoi l' équation F(x,x')=0 n'est pas dans la plupart des cas équivalente à une équation différentielle x'=f(x) ?
4- Quelle fut la réponse, oubliée et redécouverte depuis peu, que proposa Jacobi pour résoudre une équation du type F(x,x')=0 ?
5- Suite au traitement algébrique de Jacobi, quelles sont les méthodes qui permettent une résolution numérique d'une équation du type F(x,x')=0 ?
Aucun pré requis n'est besoin à priori pour suivre cet exposé.

Résumé de l'exposé d'Ahmed DJEBBAR : dans cette conférence, sera présenté un aspect peu connu des contributions des savants des pays d'Islam, celui du développement d'un chapitre d'analyse combinatoire en réponse, essentiellement, à un problème posé par les premiers linguistes arabes du VIII^{e}.
La conférence commencera par présenter les différentes tentatives des linguistes, métriciens et grammairiens de l'empire musulman pour répondre à des questions liées à la métrique et à la lexicographie arabes. Puis seront exposées quelques incursions dans le domaine combinatoire en vue de résoudre des problèmes posés dans le cadre de l'algèbre et de la théorie des nombres.
Dans une troisième partie seront présentées les contributions de mathématiciens du Maghreb dans l'établissement des premiers résultats combinatoires servant à résoudre un des problèmes posés par les linguistes et ouvrant la voie à de nouvelles pratiques combinatoires dans des domaines non-mathématiques.

ATELIERS

N°	INTITULÉS	ANIMATEURS IREM de Limoges
1	Arithmétique : histoire et opérations	Pascale SÉNÉCHAUD
2	Logiciels de mathématiques et tableau blanc interactif	Samuel ADABIA
3	Échanges sur les problèmes spécifiques de l'enseignement des mathématiques au collège	Michel LAFONT Madeleine MICHARD
4	Activités mathématiques en relation avec le domaine technique et professionnel	Monique VARLET

Dans le cadre de
l'Année Mondiale de l'Astronomie

la Société d'astronomie populaire de Limoges
et
l'Institut de Recherche sur l'Enseignement des Mathématiques

vous invitent à une nouvelle

conférence

Comment croire à l'invraisemblable expansion de l'Univers ?

par **Christian Magnan**, chercheur astrophysicien
au Collège de France et à l'Université de Montpellier

Jeudi 2 avril 2009 à 20h45

à l'amphithéâtre Billy, Faculté des Sciences et Techniques
de Limoges, 123, avenue Albert-Thomas

Plus que tout autre découverte, celle de l'expansion de l'Univers a profondément bouleversé la pensée humaine en nous apprenant que notre monde a une histoire vieille d'une quinzaine de milliards d'années. Mais comment les scientifiques sont-ils arrivés à une conclusion si ahurissante ?

Renseignements :
- 05 55 06 38 67 (répondeur)
- 05 55 50 20 29
- http://saplimoges.fr

Participation aux frais : 2 € (entrée gratuite pour les adhérents de la saplimoges)

Faculté des Sciences et Techniques
Juin 2009

TRAVAUX PRATIQUES

Arithmétique, RSA

A. NECER

I Pour se mettre en appétit

I.1 Des exercices apéritifs

Exercice 1 *Quel est le reste de la division euclidienne de* 11^{2008} *par 3 ? de* 10^{100} *par 27 ?*

Exercice 2 *Quels sont les deux derniers chiffres de* 5^{1000} *? de* 7^{2008} *?*

Exercice 3 *Par quel entier naturel faut-il multiplier 4 pour trouver 1 modulo 27 ?*

Exercice 4 *Aujourd'hui nous sommes mercredi 3 juin 2009. Quel jour de la semaine sera le 5 juillet 2009 ?*

I.2 Un vieux chiffrement à rendre à Jules César

Pour *chiffrer* ses messages, Jules César appliquait un décalage de trois lettres aux mots du texte qu'il envoyait à ses généraux : A était remplacé par D, B par E, C par F..... Z par C (voir le tableau 1 ci-dessous). Ainsi par exemple le mot "BAC" était chiffré par "EDF".

A	B	C	$\cdots$	Z
D	E	F	$\cdots$	C

Tableau 1.

Exercice 5 *Chiffrer par cette méthode « Le bac est dans la poche » (Les blancs sont chiffrés par des blancs).*
Comment le destinataire du message, déchiffre-*t-il le message reçu ?*
Si on intercepte un message chiffré par cette méthode, comment le décrypter *?*
En remplaçant A par 1, B par 2, ..., et Z par 26, comment traduire le chiffrement de Jules César modulo 26 ?

I.3 Et un chiffrement « linéaire »

Pour écrire les messages, on utilise les 26 lettres de l'alphabet et un 27^e symbole : le blanc ou l'espace. On *code* ou on *numérise* ces symboles par des nombres de 0 à 26 comme l'indique le tableau 2 suivant :

Lettre		A	B	C	D	E	F	G	H
Entier	00	01	02	03	04	05	06	07	08
Lettre	I	J	K	L	M	N	O	P	Q
Entier	09	10	11	12	13	14	15	16	17
Lettre	R	S	T	U	V	W	X	Y	Z
Entier	18	19	20	21	22	23	24	25	26

Tableau 2.

Par exemple, le mot « MATHS » sera codé par : 1301200819. Ce dernier sera chiffré par la procédure suivante : chaque nombre x (de 2 chiffres, à partir de la gauche) sera remplacé par $4x \pmod{27}$.
Ainsi 13 donne $4 \times 13 \pmod{27}$, 01 donne $4 \times 1 \pmod{27}$, etc.

Exercice 6 *Compléter le chiffrement de MATHS.*
Comment le destinataire du message, déchiffre-*t-il le message reçu ?*
Si on intercepte un message chiffré par cette méthode, comment le décrypter *?*

II Fermat, Euler et le chiffrement RSA

Le chiffrement dit RSA[1] est basé sur la difficulté de factoriser de grands nombres. Il utilise les théorèmes de Fermat et Euler.

II.1 Théorèmes de Fermat et d'Euler

Théorème 1 **(Petit Théorème de Fermat)** *Soit p un nombre premier. Pour tout entier a premier avec p, on a :*

$$a^{p-1} \equiv 1 \pmod{p}$$

On en déduit immédiatement :

Corollaire 1 *Soit p un nombre premier. Pour tout entier a (non nécessairement premier avec p), et pour tout entier positif k, on a :*

$$a^{k(p-1)+1} \equiv a \pmod{p}$$

Remarquons que l'hypothèse de primalité du module p est essentielle. Le théorème est en général faux si le module n'est pas premier. On peut cependant donner une formule analogue si le module est le produit de deux nombres premiers.

1. Rivest – Shamir – Adleman

Théorème 2 *(Euler) Soient p et q deux nombres premiers distincts et soit $n = pq$. Pour tout entier a premier avec n, on a :*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{n}$$

On en déduit le résultat :

Corollaire 2 *Soit $n = pq$ le produit de deux nombres premiers distincts. Pour tout entier a et pour tout entier positif k, on a :*

$$a^{k(p-1)(q-1)+1} \equiv a \pmod{n}$$

II.2 Principe du chiffrement RSA

Pour recevoir des messages (chiffrés par RSA), Bob choisit deux grands nombres premiers p et q dont il calcule le produit n (*le module du chiffrement*) et un nombre d premiers avec $(p-1)(q-1)$ (d sera appelé *clé de chiffrement*).
Il calcule ensuite e tel que

$$de \equiv 1 \pmod{(p-1)(q-1)}$$

Le nombre e sera appelé *clé de déchiffrement*.
Bob garde secrets p, q et e et rend public ses « coordonnées » n et d.
Alice veut envoyer un message à Bob. Elle regarde dans l'annuaire (public) et trouve les coordonnées n et d de Bob. Elle convertit son message en nombres plus petits que n et les chiffre, en utilisant la clé de chiffrement d, de la façon suivante : pour un mot, disons x, elle calcule

$$y = x^d \pmod{n}.$$

Elle envoie ensuite y à Bob.
Bob reçoit y. Il utilise sa clé de déchiffrement e pour calculer $y^e \pmod{n}$. Il obtient x et retrouve ainsi le mot envoyé par Alice. En effet,

$$\begin{aligned} y^e &\equiv (x^d)^e \pmod{n} \\ &\equiv x^{de} \pmod{n} \\ &\equiv x \pmod{n} \end{aligned}$$

La dernière congruence découle du fait que $de = 1 + k(p-1)(q-1)$, $k \in \mathbb{N}$

Remarques

1. Ce qui est secret : e, p et q ; ce qui est public : n et d.
2. La connaissance de p et q permet de retrouver facilement e et donc de décrypter le message.
3. La seule connaissance de n et de d et de ne permet pas de calculer e dans des délais raisonnables.

III Travail à faire

Après une rapide prise en main de Maple (voir page 5), on veillera à répondre aux questions ci-dessous en complétant les trous dans la page 6.

On utilise la numérisation (ou codage) donné par le tableau 2 ci-dessus.

1. Les lettres sont groupées par 3 : MATHS donne 130120 - 081900.
   On utilise les paramètres suivants $p = 373$, $q = 809$ et $d = 13$
   (a) Vérifier que p et q sont bien premiers que d est une clé de chiffrement.
   (b) Déterminez la clé de déchiffrement e.
   (c) Chiffrez le message "MATHS"
   (d) Déchiffrez le message 106127 - 289649.
2. Vous interceptez un message : 3294460797 - 685705689. Vous savez que les lettres sont groupées par 5 et que la clé de chiffrement publique utilisée est $d = 17$ et $n = 3450459293$.
   (a) Déterminez les deux facteurs premiers de n.
   (b) Déterminez la clé de déchiffrement e.
   (c) Décryptez le message !

   Visiblement, le nombre n choisi n'était pas assez grand.
3. Si le temps le permet, créez votre propre clé publique. Vous devez :
   (a) Déterminer les valeurs de p, q, n, d et e. La valeur de n doit être légèrement supérieure à la taille des entiers à chiffrer.
   (b) Rendre publiques les valeurs d et n.
   (c) Savoir déchiffrer un message chiffré avec votre clé publique.

IV Quelques commandes MAPLE

Les instructions se terminent par le caractère ; et s'exécutent en appuyant sur la touche Entrée.
Le résultat du dernier calcul effectué (pas forcément sur la ligne précédente !) peut être rappelé par le caractère %. Par exemple :

|> 2^3;

$$8$$

|> % + 5;

$$13$$

On peut définir des variables avec l'instruction " :=". Par exemple :

|> p := 373;

$$p := 373$$

|> p := 809;

$$q := 809$$

|> n := p * q;

$$n := 301757$$

Puissance et congruence :
on peut calculer rapidement $a^b \pmod c$, même si b est grand, avec l'instruction :

a&^b mod c

Par exemple :

|> 3&^12345678901234567890 mod 100 ;

Une liste de quelques fonctions utiles : isolve, isprime, nextprime, prevprime, ifactor,...
Pour avoir de l'aide sur ces fonctions (par exemple isolve), taper

|> ?isolve ;

V Travail à faire (à compléter)

1. (a) Équation à résoudre :

   Valeur de e : $e =$

   (b) Message à chiffrer

Lettres	MAT	HS
x	130120	081900
y		

   (c) Message à déchiffrer :

y	106127	289649
x		
Lettres		

2. (a) Valeur de p et q :

   Équation à résoudre :

   (b) Valeur de e : $e =$

   (c) Message à décrypter :

y	3294460797	685705689
x		
Lettres		

Université de Limoges

CONFÉRENCE

Contact : IREM de Limoges
TÉLÉPHONE 05 55 45 72 49
FAX 05 55 45 73 20

À l'occasion du lancement du séminaire « *Histoire des Sciences et Épistémologie* »

L'IUFM DU LIMOUSIN, L'IREM DE LIMOGES, LA MISSION « DIFFUSION DE LA CULTURE ET DES SAVOIRS » VOUS INVITENT À LA CONFÉRENCE

LE LIVRE SCIENTIFIQUE À LA RENAISSANCE

PAR

LAURENT PINON
Historien des Sciences
PROFESSEUR À L'ECOLE NORMALE SUPÉRIEURE DE PARIS

Date : vendredi 19 juin 2009

Lieu : Amphithéâtre Couty- Faculté des Sciences et Techniques

Heure : 11 heures

Résumé À la Renaissance, avant l'apparition des périodiques savants, le livre imprimé est l'un des principaux supports de communication scientifique. Cela explique qu'il ait été l'objet d'une attention particulière de la part des auteurs scientifiques, et qu'il soit aujourd'hui une source majeure pour l'histoire des sciences. J'aborderai ce thème à partir de deux études de cas.

La première concerne l'astronome danois Tycho Brahe qui imprime lui-même ses traités d'astronomie. Le bilan mitigé de cette entreprise d'auto-édition permettra de discuter des spécificités formelles des livres scientifiques et des difficultés propres à leur impression.

La présentation d'une enquête sur les livres scientifiques et techniques imprimés à Rome aux XVI^{e} siècle et XVII^{e} siècle permettra de discuter des apports de la bibliographie pour la compréhension de la culture scientifique dans la capitale pontificale et d'évoquer le livre scientifique comme source pour l'historien.

L. Pinon

Journée Mathématiques du 19 juin 2009 - (IUFM – IREM)

-- Matin *(au département de mathématiques IREM- FST)*

10 h 30 - Accueil

11 h – Conférence
Laurent PINON (ENS - Département d'histoire) :
Le livre scientifique à la Renaissance

12 h 15 - Débat.

12 h 45 [Pause déjeuner au restaurant de La Borie]

-- Après-midi *(à l'IUFM)*

14h 30. Atelier: Autour de l'*Arithmetica integra* de Michael STIFEL

14 h 30 - Introduction
François LOGET (Université Limoges - CESR Tours) :
L'Arithmetica Integra (1544) et l'algèbre de la Renaissance.

15 h - Conférence
Sabine ROMMEVAUX (CNRS - CESR Tours) :
Théorie des rapports et des proportionnalités dans l'algèbre de Stifel

15 h 45 - Conférence
Marie-Hélène LABARTHE (Université Perpignan) :
L'extraction des racines des nombres cossiques chez Stifel: une méthode unique pour les trois cas d'équations composées

16h 30 - Conférence
Odile KOUTEYNIKOFF (CHSPAM Paris) :
Les reprises de la règle AMASIAS de Michael Stifel par quelques contemporains et successeurs immédiats

17 h 15 - Table ronde animée par **Maryvonne SPIESSER** (Université Paul-Sabatier Toulouse III - Institut de mathématiques)

18h. Conclusion