UNIVERSITÉ DE FRANCHE-COMTÉ

INSTITUT DE RECHERCHE SUR

L'ENSEIGNEMENT DES MATHEMATIQUES

UNIVERSITÉ DE FRANCHE-COMTÉ

Histoire des Mathématiques **«** Mathématiques, mathématiciens et guerres **»**
Salle 316 B

Jeudi 23 janvier (matin) Christophe Delaunay (Université de Franche-Comté) : *Introduction à la cryptographie et problème du logarithme discret*

La cryptographie a connu de grandes avancées au cours des dernières décennies. En particulier, la cryptographie dite à "clé publique" s'est largement développée depuis la création du fameux système RSA (du nom de ses inventeurs : Rivest, Shamir, Adleman) dans les années 70. Dans cet exposé, nous rappellerons rapidement les principaux enjeux de la cryptographie moderne et les grands principes de la cryptographie à clé secrète et à clé publique. Puis, nous nous focaliserons sur le problème du "logarithme discret" et ses applications en cryptographie (par exemple, protocole de Diffie-Hellman). Notamment, nous expliciterons ce problème dans le cas du groupe multiplicatif du corps fini à *p* éléments et dans le cas du groupe des points d'une courbe elliptique définie sur un corps fini.

Jeudi 23 janvier (après-midi) Michèle Audin (Université de Strasbourg) : *Des guerres et des mathématiciens*

Il s'agira de raconter (j'insiste sur le terme « raconter » qui n'est pas un effet du hasard) l'histoire de différents mathématiciens et de leurs travaux pendant les deux guerres mondiales, de montrer comment ces guerres ont pu, de façons différentes, influencer leur vie et leurs recherches. Voici une première liste de personnes (en France) et de sujets dont il pourra être question : Pierre Fatou et Gaston Julia (et l'itération des fractions rationnelles), Jacques Feldbau (et la topologie), André Weil (et l'arithmétique sur les corps finis)... Le rôle joué par les institutions (Académie des sciences en France, notamment) sera aussi envisagé.

Vendredi 24 janvier (matin) Anne-Marie Aebischer et Hombeline Languereau (IREM, Université, de Franche-Comté) : *Servois ou la géométrie à l'école de l'artillerie*

Dans une atmosphère épaissie par la fumée des tirs, les troupes de la jeune République française sont clouées au sol par les tirs ennemis. On aperçoit au loin le rougeoiement du tir d'un canon ennemi qu'il faut absolument anéantir. Les munitions sont chères, il faut arriver à déterminer la distance à ce point de tir diablement inaccessible … Les constructions géométriques doivent tenir compte du contexte militaire. Dans cet exposé, nous étudierons quelques constructions et nous proposerons des activités de géométrie à mener avec des collégiens ou des lycéens.

Vendredi 24 janvier (fin de matinée - après-midi) Frédéric Métin (ESPE, Université de Bourgogne) *Artillerie et Fortifications au 17siècle*

Le premier 17^{e} siècle voit l'appropriation des nouvelles théories militaires par les ingénieurs du nord de l'Europe. Les nouvelles manières de fortifier sont d'origine italienne, tandis que ce sont les Espagnols qui sont passés maîtres dans l'artillerie (suivant cependant la théorie de Tartaglia) : c'est qu'on n'est pas encore bien sûr de la courbe modélisant la trajectoire des boulets de canon. La théorie du bastionnement et le profilage géométrique des enceintes des cités répondent néanmoins à des contraintes liées à ces trajectoires, car dans un plan horizontal, chacun s'accorde pour admettre que les canons tirent droit. Jusqu'à l'avènement de Vauban à la fin du siècle, artilleurs et fortificateurs s'affrontent sur le terrain comme dans les livres. Certains, comme Claude Flamand à Montbéliard, participent peu à la guerre mais travaillent comme ingénieurs civils au service des princes, d'autres comme Jean Errard sont actifs dans la tranchée. En tous les cas, c'est la géométrie qui emporte la conviction des élites et par là-même influe sur la stratégie. Lors de la demi-journée, un exposé général sera complété par un atelier qui permettra aux participants de s'approprier les tracés géométriques de l'époque.

IREM - Département de Mathématiques
UFR des Sciences et Techniques - 16, route de Gray - 25030 BESANÇON CEDEX
Téléphone : 03 81 66 62 25, Télécopie : 03 81 66 66 23, Adresse électronique : iremfc@univ-fcomte.fr