Plenary Lectures
Conférences plénières

GILLES BRASSARD, Montréal
Cryptography in a Quantum World

Although practised as an art and science for ages, cryptography had to wait until the mid-twentieth century before Claude Shannon gave it a strong mathematical foundation. However, Shannon's approach was rooted is his own information theory, itself inspired by the classical physics of Newton and Einstein. When quantum physics is taken into account, new vistas open up both for codemakers and codebreakers. Is this blessing or a curse for the protection of privacy? As we shall see, the jury is still out! No prior knowledge in cryptography or quantum physics will be assumed.

Reference: arXiv:1510.04256 [quant-ph] .

ANNA GILBERT, University of Michigan
Recent developments in the Sparse Fourier Transform

The Discrete Fourier Transform (DFT) is a fundamental component of numerous computational techniques in signal processing and scientific computing. The most popular means of computing the DFT is the Fast Fourier Transform (FFT). However, with the emergence of big data problems, in which the size of the processed data sets can easily exceed terabytes, the "Fast" in Fast Fourier Transform is often no longer fast enough. In addition, in many big data applications it is hard to acquire a sufficient amount of data in order to compute the desired Fourier transform in the first place. The Sparse Fourier Transform (SFT) addresses the big data setting by computing a compressed Fourier transform using only a subset of the input data, in time sub-linear in the data set size. The goal of this talk is to survey these recent developments, to explain the basic techniques with examples and applications in big data, to demonstrate trade-offs in empirical performance of the algorithms, and to discuss the connection between the SFT and other techniques for massive data analysis such as streaming algorithms and compressive sensing.

MARTIN HAIRER, Warwick, U.K.
On random rubber bands

A rubber band constrained to remain on a manifold evolves by trying to shorten its length, eventually settling on some minimal closed geodesic, or collapsing entirely. It is natural to try to consider a noisy version of such a model where each segment of the band gets pulled in random directions. Trying to build such a model turns out to be surprisingly difficult and generates a number of nice geometric insights, as well as some beautiful algebraic and analytical objects.

BERNARD HODGSON, Université Laval
History of mathematics as a component of university math education: reflections inspired by Archimedes' mathematical rhetoric

I wish in my presentation to discuss the role that history of mathematics could, or should, play in university mathematics education, including in the preparation of schoolteachers. After briefly commenting on some challenges that may be faced by faculty members who start being involved in the teaching of history of mathematics, I will concentrate on two results due to Archimedes—about the area of a circle and of a segment of parabola. I will examine in particular how the great Syracusan has, or may have, identified those results, and how he has proved them—in the latter case, not merely once, but three times!

(The presentation will involve both official languages of the CMS.)

L'histoire des mathématiques en tant que composante de la formation universitaire en mathématiques : réflexions inspirées par la rhétorique mathématique d'Archimède

Cette présentation porte sur le rôle que l'histoire des mathématiques peut, ou devrait, jouer dans l'enseignement des mathématiques à l'université, y compris dans le cadre de la formation des enseignants. Après de brefs commentaires à propos des défis que peuvent rencontrer ceux qui se lancent dans l'enseignement de l'histoire des mathématiques, je me concentrerai sur deux résultats dus à Archimède et portant sur l'aire du cercle et l'aire d'un segment de parabole. J'examinerai de façon particulière comment le grand Syracusain a, ou peut avoir, identifié ces résultats, et comment il les a démontrés — en ce qui concerne le segment parabolique, trois fois plutôt qu'une!

(La présentation se déroulera dans les deux langues officielles de la SMC.)

CAROLINE SERIES, University of Warwick

Boundaries of discreteness and hyperbolic 3-manifolds

Suppose given a finite collection of Moebius maps which depend holomorphically on some complex parameters. For which parameter values is the group they generate discrete? Inspired by Mandelbrot's work on iteration of quadratic polynomials, this question was investigated by David Mumford and David Wright in the 1980s. Their remarkable computer experiments suggested that the region of discreteness in parameter space has a complicated fractal-like boundary. I will explain how three dimensional hyperbolic geometry has shed light on this problem, making use of wonderful new concepts stemming from Thurston's revolutionary work on hyperbolic three manifolds. The talk will be illustrated with beautiful computer graphics which have played a crucial role in the discoveries.

JAMIE TAPPENDEN, University of Michigan

Styles of Mathematical Explanation. Why do Elliptic Functions have Two Periods?

In recent years, philosophers have devoted significant attention to the topic of explanation as a phenomenon within mathematics. There appear to be both differences and similarities in the patterns characteristic of mathematical explanations of mathematical events and causal explanations of physical events, but more study is needed to ascertain precisely what the differences are. This talk will present a historical case study illustrating that, among other things, mathematical explanations can exhibit the same interest-relativity and context-dependence that are found in explanations of physical events. The example is the explanation of the fact that elliptic functions are doubly periodic. (This way of describing the case involves seeing the elliptic functions in a nineteenth-century way via inverting elliptic integrals; today double periodicity is part of the definition of "elliptic function".) Two ways to address the fact – one using techniques characteristic of Bernhard Riemann (develop the Riemann surface then integrate on a torus) and another in the style of Karl Weierstrass (represent via the Weierstrass P-function and its derivative) reveal strikingly different mathematical virtues. The explanations are both "good ones", but for incommensurable reasons.