THE ACADEMY CORNER

No. 26

Bruce Shawyer

All communications about this column should be sent to Bruce Shawyer, Department of Mathematics and Statistics, Memorial University of Newfoundland, St. John's, Newfoundland, Canada. A1C 5S7

Abstracts • Résumés

Canadian Undergraduate Mathematics Conference 1998 — Part 4

The Dirichlet-to-Neumann Map

Scott MacLachlan
University of British Columbia

There are two classic problems in potential theory - the Dirichlet and Neumann problems. In most courses on partial differential equations the problems are treated separately; however there is a very elegant link between these problems that can be explored via Fourier analysis. The Dirichlet-to-Neumann map takes data for a Dirichlet problem and translates it into data for a Neumann problem without calculating a solution first. This map is useful in many areas, particularly in potential theory.

Systèmes de racines

Maciej Mizerski
McGill University

Un des plus beaux résultats de la théorie des groupes et algèbres de Lie est la classification des algèbres de Lie semi-simples. Cette classification se ramène à l'étude de la structure des systèmes de racines. Dans ma présentation, je vais introduire les systèmes de racines et survoler leur classification en utilisant les diagrammes de Dynkin. Aussi je vais tenter de faire le lien avec les groupes et les algèbres de Lie.

Cardan's Formulas for Solving Cubic Equations Revisited

Afroze Naqvi
University of Regina

This presentation offers a very brief history of Algebra and then proceeds to derive Cardan's Formulas for solving cubic equations. These formulas will be used to solve some cubic equations.

Mathematics of the Ancient Jews and Ancient Israel

Peter Papez
University of Calgary

As mathematicians we are well acquainted with the mathematics of the ancient Babylonians, Greeks and Egyptians. Even Ancient Chinese mathematicians have gained great notoriety in recent years. But the mathematics of ancient Israel is certainly noteworthy, if not impressive, and has not received the attention it deserves. The purpose of this discussion will be to introduce these impressive achievements and discuss some problems and the solutions obtained by ancient Jewish scholars. In order to facilitate the discussion, a brief overview of ancient Jewish history will be given. As well, the Talmud and Talmudic Law will be presented. The discussion will encompass the very beginning construction of numerals and numeracy within the ancient Jewish culture, proceed through the development of arithmetic, touch on important notions concerning science and logic, and conclude with a discussion of some fairly advanced developments in sampling and statistics. Various problems and their solutions, as derived by the ancient Jews, will be used to illustrate these developments and the entire discussion will be placed in a historical and Talmudic context.

Computing in the Quantum World

Christian Paquin
Université de Montréal

The current computing model is based on the laws of classical physics. But the world is not classical; it follows the laws of quantum mechanics. A quantum computer is a model of computation based on quantum mechanics. It has been proved that such a model is more powerful than its classical counterpart, meaning that it can do the same computations as a classical computer (in approximately the same time) but there exist some problems for which the quantum computer is much faster. In this paper I will explain what is quantum information, why a quantum computer would be useful, what are the problems to build a quantum computer and how it will work.

Wavelet Compression on Fractal Tilings

Daniel Piché
University of Waterloo

Over the last decade, wavelets have become increasingly useful for studying the behaviour of functions, and for compression. Though much remains to be investigated in this field, certain types of wavelets are fairly easy to construct, namely Haar wavelets. This paper ties together the theory of these wavelets with that of complex bases. An algorithm is proposed for doing wavelet analysis, with wavelets arising in this fashion. This will enable further study of the properties of these wavelets.

Introduction to Representation Theory

Evelyne Robidoux
McGill University

This paper provides an introduction to representation theory, with emphasis on representations of finite groups. The background required will be only a bit of group theory (that is, being familiar with the concepts of groups, homomorphisms, conjugacy classes) and linear algebra (vector spaces, linear transformations, inner products, direct sums). A classical reference for this material is the book by Serre, *Linear Representations of Finite Groups*, which I really recommend.

The Effect of Impurities in One-Dimensional Antiferromagnets

Alistair Savage
University of British Columbia

A brief overview of a paper to be published shortly with Ian Affleck of the University of British Columbia Department of Physics and Astronomy.

Authentication Codes Without Secrecy

Nelly Simões
Simon Fraser University

Suppose Alice wants to say something to Bob and cares only about the *authentication* of her message. Authentication makes it possible for Bob to receive Alice's message and be certain it came from her. Basically an authentication code without secrecy is a process in which a mathematical function transforms what Alice wants to say to Bob, we call this the *source state*, into what is called an *authentication tag* and adds it to the source state to form the *message*. We also suppose that Alice and Bob mutually trust each other. Alice wants to use an *unconditionally secure* method of authentication. She does not want anyone to be able to modify her message, not even a person with lots of computer power. This is why Alice decides to use a combinatorial method. We are going to explore an unconditionally secure way of authenticating Alice's message.

Integer Triangles With a Side of Given Length

Jill Taylor
Mount Allison University

This presentation will give a glimpse into the history of *Heronian triangles* (triangles with integer sides and integer area) and one special case of such triangles which I have researched this summer. However, the main focus will be a particular problem involving Heronian triangles with a given perimeter. The solution of this problem requires both number theory and basic geometrical concepts.

Convergence and Transcendence in the Field of p–adic Numbers

Sarah Sumner
Queen's University

We will first explore convergence properties of series in $\mathbb{Q}_p$, and then study instances when the series

$$\sum_{n=0}^{\infty} a_n p^n, \; a_n \in \mathbb{Q}_p$$

is transcendental over $\mathbb{Q}_p$. We will give a general result describing a large class of series of this type which are transcendental over $\mathbb{Q}_p$. Our result unfortunately does not resolve the transcendence of $\sum_{n=0}^{\infty} n!$ in $\mathbb{Q}_p$. However, our theorem applies to show transcendence of

$$\sum_{n=0}^{\infty} \zeta_n n!$$

where ζ_n is a primitive n-th root of unity if $(p, n) = 1$ and is 1 otherwise.

Random Number Generation

Renée Touzin
Université de Montréal

Nowadays, in many scientific fields, random number distributions are needed. Those distributions such as a binomial, a normal, an exponential are built from iid uniform $(0, 1)$ distributions. But this distribution does not really exist. In fact, it consists of a mathematical and deterministic algorithm that tries to behave stochastically.

The building of an efficient generator requires a strong knowledge of mathematics and computer science. A priori, a generator must follow certain theoretical criteria. A posteriori, those same generators must pass many statistical tests to be sure they look random even though they are deterministic. In this presentation, we will talk about different kinds of existing generators and the qualities of a good generator. We will give examples of good and bad generators and finally we will present a simple implementation in $\mathbb{C}$.

The Probabilistic Method: Proving Existence by Chance

Alexander Yong
University of Waterloo

The Probabilistic Method is based on a simple concept: in order to prove the existence of some mathematical object, construct an appropriate probability space and show that the object occurs with positive probability. We will investigate this powerful proof technique via three examples.