The Abdus Salam International Centre for Theoretical Physics
50th Anniversary 1964–2014

United Nations Educational, Scientific and Cultural Organization

IAEA International Atomic Energy Agency

School in Computational Algebra and Number Theory

5 - 10 December 2014
(Montevideo, Uruguay)

The Abdus Salam International Centre for Theoretical Physics (ICTP), Trieste, Italy, is organizing a School in Computational Algebra and Number Theory, to be held ***in Montevideo, Uruguay***, from ***5 – 10 December 2014.***

This school is a satellite of FoCM'14 https://www.fing.edu.uy/eventos/focm2014/

TOPICS AND FACULTY

Teresa Krick (Universidad de Buenos Aires)

Arithmetic Nullstellensätze and Applications

The purpose of these lectures is to introduce Hilbert's Nullstellensatz, a cornerstone in Algebraic Geometry, and comment on its effective aspects, including degree and height aspects when the defining field admits a notion of height. We will introduce the ingredients used to obtain sharp estimates, which can be useful on their own, and present some applications (by others) to problems on finite fields.

Christophe Ritzenthaler (Université Rennes 1)

Elliptic Curves and its Applications to Cryptography

The course will be a brief introduction to elliptic curves and its applications to cryptography and is divided into 4 lectures:

- definition(s) of an elliptic curve, group law, isomorphisms, torsion points, Weil pairing.
- elliptic curves over finite fields: two proofs of Hasse-Weil bound.
- elliptic curves over finite fields: how to count points? Overview of the different methods.
- application to cryptography: protocols, attacks and zoology of the existing models.

Peter Stevenhagen (Universiteit Leiden)

Algebraic Number Theory

- roots of the topic: Fermat, Euler, quadratic reciprocity.
- algorithmic requirements for the theory, e.g. in view of the number field sieve.
- working in number rings: integrality, (explicit) ideal factorization
- geometry of numbers, finiteness theorems (class group, Dirichlet unit theorem).
- Dedekind zeta function, computing fundamental number field invariants,
- local-global aspects: local fields, adeles, ideles.
- number field sieve.

PARTICIPATION

The workshop is open to researchers and students from all countries that are members of the United Nations, UNESCO, or IAEA. The principal objective of the ICTP is to help researchers from developing countries through a programme of training activities within a framework of international cooperation. Participants should have an adequate working knowledge of English. Due to budget limitations, every effort should be made by candidates to secure either total or partial support for their expenses. However, funds are available exclusively for a limited number of participants who are nationals of, and working in, countries from Latin America Participants are required to take part in all aspects of this activity for its entire duration. There is no registration fee.

HOW TO APPLY FOR PARTICIPATION

The application form can be accessed at the activity website **http://agenda.ictp.it/smr.php?2642**

Once in the website, comprehensive instructions will guide you step-by-step, on how to fill out and submit the application form. Closing date for receipt of the applications is: **15 October 2014**

Students who would like to extend their stay and attend FoCM'14, or just its workshop on Computational Number Theory, should explicitly mention this in their application.

E-mail: ***smr2642@ictp.it*** ***ICTP Home Page:*** **http://www.ictp.it/**

August 2014

DIRECTORS

***Gonzalo* Tornaría**
Universidad de la República
(Montevideo, Uruguay)

Teresa Krick
Universidad de Buenos Aires
(Buenos Aires, Argentina)

F. Rodriguez Villegas
ICTP, Trieste, Italy

Peter Stevenhagen
Universiteit Leiden
(Leiden, Netherlands)

SPEAKERS

Above Faculty &

John Cremona
University of Warwick
(Warwick, UK)

LOCAL ORGANIZER

Gonzalo Tornaría
Universidad de la República
(Montevideo, Uruguay)

DEADLINE
For requesting participation:

15 October 2014