German-Israeli Minerva School 2008

Arithmetic Geometry and Public Key Cryptography

Organizers: Prof. Dr. Moshe Jarden
School of Mathematics
Tel Aviv University, Israel
Director of the Hermann Minkowski Center for
Geometry, founded by the Minerva Foundation

Prof. Dr. Dr.h.c. Gerhard Frey
University of Duisburg-Essen, Germany
Chairman of the Advisory Council of the
Hermann Minkowski Center for Geometry,
founded by the Minerva Foundation

Conference venue and date: Tel Aviv University, 27 July — 5 August, 2008

Subject area: Arithmetic Geometry and Applications to Cryptology

The traditional focus of pure mathematics is on deciding whether certain mathematical objects exist or not. For instance, one wants to know if given equations have solutions, or whether structures with given properties exist. In the past few decades, an increasing need has become apparent for methods that actually construct these mathematical objects in case they exist.

This trend has not meant a shift from pure to applied mathematics, but it is rather changing the nature of pure mathematics itself: algorithmic thinking and the language of complexity theory are entering into pure mathematics.

There are two forces driving the trend towards explicit methods in the area of number theory and arithmetic geometry. The first is the desire of mathematicians to understand the mathematical universe in a more thorough way than before and to develop computer labs to allow computer experiments with mathematical objects of a greater variety than in traditional numerical computation.

Secondly, the vastly increased use and complexity of electronic communication and networking has created needs in data security and coding theory that are often met by applications of unexpected branches of number theory and arithmetic geometry. For instance algorithms for elliptic curves over finite fields have a profound impact on cryptology and especially on public key crypto systems which are crucial for constructing open networks like the internet.

To be more specific: Public key crypto systems rely on one way functions. For the construction of such functions one looks for ``hard computational problems'' and so number theory and the theory of varieties over finite fields enter the scene. The study of the action of the Frobenius automorphism plays a central role and a major attraction of public key cryptography for mathematicians is that the most beautiful and deepest results on the arithmetic of Galois representations lead to the most efficient algorithms both for constructing and attacking systems.

The **main topics to be addressed at the school** are:

Crypto-Protocols

The RSA –system and the factorization of numbers

Discrete Logarithms and their realizations as ideal class groups

Constructive and destructive applications of Galois Theory: efficient scalar multiplication, point counting, scalar restriction (Weil descent)

Duality theorems and the Tate-Lichtenbaum pairing

Role of the Brauer group of local and global fields for discrete logarithms

Applications in the world of communication

Preliminary programme

We plan to have 2 lectures in the morning of Sunday (27.7), 3 lectures of one hour each in the mornings Monday (28.7.) –Thursday (31.7.) and Sunday (3.8)--Monday (4.8). We plan to hold 5 series of lectures, 4 hours each. In addition the school will offer an excursion to its participants on Friday and Saturday (1.-2.8). Possible goals are Jerusalem (including the old city) on Friday and the Dead Sea and Massada on Saturday.

Lecturers:
C. Diem (Leipzig) (Index-Calculus Methods)

G. Frey (Duisburg-Essen) (Duality Theorems and Applications)

M. Jarden (Tel Aviv) (Arithmetic of Varieties over Finite Fields)

F. Vercauteren (Leuven) (Cohomological Methods for Point Counting)

U. Vishne (Bar Ilan) (Protocols, discrete logarithms)

In the afternoon of the lecture days the students will be time to solve exercises prepared by the lecturers (15-17.00) (with a possibility to contact the lecturers).
The solutions will be presented and discussed from 17.30-19.00.
Alternatively, talks will be given by invited speakers on recent results related to the subject of the school.

The school can offer about 30 spots.

Substantial support (travel, accomodation) will be available due to the funding by the Minerva Foundation and the Minkowski Center.

For more information and for application please contact

frey@exp-math.uni-due.de
or
jarden@post.tau.ac.il