06/10/2017

InterCity - seminar

Bern - Neuchâtel - **Fribourg/Freiburg**

7

Time	Speaker	Talk
14:00	Arthur Bik (Bern)	**Euclidean distance degrees of affine subvarieties of polar representations**
		Abstract: The Euclidean distance degree of an affine subvariety X of a space V counts the number of critical points on X of the distance function to a generic point of V. Drusvyatskiy, Lee, Ottaviani, and Thomas proved that the ED degree of an orthogonally invariant matrix variety X equals the ED degree of the set of diagonal matrices in X. In this talk, we generalize this result to orthogonally invariant subvarieties of polar representations.
15:30	Giulia Bianco (Neuchâtel)	**Index calculus for the discrete logarithm problem**
		Abstract: Cryptography ensures safe communication between parties, with the use of secret keys to protect the transmitted messages. In practice, the keys are elements of a cyclic group of prime order p, and their security is determined by the hardness of solving some mathematical problems in the group. One of the most important among these problems is the Discrete Logarithm Problem (DLP). It has been shown that generic algorithms for solving the DLP have complexity at least O(√p), which is achieved by the so called Pollard's rho method. Generic algorithms work in any group, independently of its particular structure. Therefore, in order to develop techniques that perform better than the Pollard's rho, one has to exploit the algebraic/ geometric structure of the group under consideration. In this talk, we speak about index calculus, that is one of the most popular among the non-generic strategies for the solution of the DLP. Such method can be applied to different structured groups that are used in cryptography, with the great potential to lower the generic complexity of the problem.

The talks will take place in Room 0.51 of the Physics building (Pérolles) of the University of Fribourg.

For further informations please refer to the seminar's webpage

www.combinatorialmethods.ch/intercity/

or contact the organisers:

Emanuele Delucchi (Fribourg) — Jan Draisma (Bern) — Elisa Gorla (Neuchâtel)