Prof. Philippe Michel
Chair of Analytic Number Theory (TAN)

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

SEMINAR OF MATHEMATICS

***Thursday March 2nd, 2017 at 10h15, CIB lecture hall* [BI A0 448]**

Prof. Dimitar Jetchev *(EPFL)*

will present a seminar entitled:

"CM-theoretic Aspects of the Birch and Swinnerton-Dyer Conjecture and Curve-Based Cryptography"

Abstract:

The theory of complex multiplication (CM theory) has found numerous applications in both modern number theory, arithmetic geometry and mathematical cryptology. In this talk, I will give a basic background on the BSD conjecture and outline the main ideas of the recent proof of the conjectural formula for elliptic curves of analytic rank 1. I will then explain how CM theory provides an algebraic model for the analytic side of the BSD conjecture via Euler systems and report on higher-dimensional constructions from special cycles on unitary Shimura varieties. These constructions are based on local analysis via Bruhat-Tits buildings of the corresponding unitary groups.

The seemingly unrelated problem of computing explicit isogenies for principally polarized abelian varieties plays a key role in the study of the discrete logarithm problem (DLP), the main computational hardness assumptions for most of the existing curve-based cryptographic schemes. I will review recent work on computing isogenies in higher dimensions via theta embeddings and CM theory, and comment on the implications of these to DLP and parameter selection. This requires establishing precise structural properties of certain graphs of isogenies of principally polarized abelian varieties - a problem that can be solved using similar local analysis on the Bruhat-Tits buildings for symplectic groups as the one used in the construction of Euler systems.

Lausanne, February 23, 2017 / mg

The seminars taking place at the Section of Mathematics are announced on internet address:
http://memento.epfl.ch/