istanbul matematiksel bilimler merkezi
istanbul center for mathematical sciences

Arithmetic properties of elliptic division polynomials and divisibility sequences

Paul Voutier (London)

Abstract

Binary linear recurrences such as the Lucas sequences, which have played an important role in number theory since its earliest days, are associated with twists of the multiplicative group, $\mathbb{G}_m$.

Similarly, one can associate sequences to other algebraic groups. An example is the algebraic group $E(\mathbb{Q})$ where $E/\mathbb{Q}$ is an elliptic curve. If $E(\mathbb{Q})$ is of positive rank, we take a non-torsion point, $P \in E(\mathbb{Q})$, put $[n]P = A_n/B_n^2$ with $(A_n, B_n) = 1$, $B_n \geq 1$ and consider $\{B_n\}_{n\geq 0}$. This sequence is called an *elliptic divisibility sequence* and is closely related to the *elliptic division polynomials*, Ψ_n.

These sequences provide us with much important information about the arithmetic geometry of the underlying curve, E and the point, P.

In this talk, we present new results on some arithmetic properties of these objects – in particular, on explicit valuations of the elliptic division polynomials and on primitive divisors of elliptic divisibility sequences.

This is joint work with Minoru Yabuta.

Date : Tuesday, October 31, 2017

Time: 15:00

Place: IMBM Seminar Room, Boğaziçi University South Campus