Boğaziçi
MATH COLLOQUIUM

One-way Algebra

Alexandre V. Borovik
University of Manchester

Abstract:

I will give a survey of recent results in probabilistic methods of computational algebra (and, more, specifically, group theory) concerned with the categories of explicitly defined finite algebraic structures (groups, rings, fields, projective spaces, etc.) and efficiently computable homomorphisms between them. The motivation for some results comes from cryptography, for others from needs of practical computations. This is an intriguing world where most natural morphisms are likely to be non-invertible, and where we do not know whether finite fields of prime order are unique up to (efficiently computable both ways!) isomorphisms. However, it is a surprisingly rich and beautiful theory with unexpected links with some classical areas of mathematics.

(Joint work with Şükrü Yalçınkaya)

Date : Wednesday, October 07, 2015
Time: 14:00
Place: TB 250, Boğaziçi University