Applied arithmetic geometry

Dr. Ambrus Pal
Imperial College London, United Kingdom.

The aim of this lecture series is to introduce some methods of arithmetic geometry which are applied in cryptographic research. Cryptography, including more sophisticated versions such as elliptic curve cryptography, allows for efficient protocols for information security, and is widely used in the banking sector including mobile money transfers, an industry in which Africa is a world leader. The methods presented can be used by African research groups to tackle a range of problems arising in technological challenges relevant to the African development context. Arithmetic geometry is a rather modern, highly prestigious and very developed area of pure mathematics, developed originally for studying Diophantine equations. I has very efficient methods to count points on algebraic varieties over finite fields which is closely related to the original motivating problem of finding rational points on varieties over number fields, a geometric reformulation of Diophantine equations. The former problem is very important in cryptography and related areas of secure communication, network building and hash functions. The lecture series will cover the necessary background on cryptography and point counting, and will introduce such tools as p-adic numbers, differential forms and Monsky-Washnitzer cohomology, from the ground up.

Keywords: Arithmetic geometry; cryptography; p-adic numbers; differential forms; Monsky-Washnitzer cohomology