MARCO POLLANEN, Trent University, Peterborough, ON K9J 7B8
Algebraic Curves for Non-Uniform Pseudo-Random Sequence Generation

Pseudo-random numbers are a critical part of modern computing, especially for use in simulations and cryptography, and consequently there are a myriad of algorithms for creating uniform pseudo-random sequences. However, many simulations ultimately require non-uniform random sequences. In this talk we introduce a new method to directly generate, without transformation of rejection, some non-uniform pseudo-random sequences. This method is a group-theoretic analogue of linear congruential pseudo-random number generation. We provide examples of such sequences, involving computations in Jacobian groups of plane algebraic curves, that have both good theoretical and statistical properties.