Pseudorandom numbers from curves of genus 2

Vishnupriya Anupindi
RICAM, Austrian Academy of Sciences, Austria
vishnupriya.anupindi@oeaw.ac.at

Pseudorandom sequences, that is, sequences which are generated with deterministic algorithms but look random, have many applications, for example in cryptography, in wireless communication or in numerical methods.

In this poster, we briefly recall the group law on genus 2 hyperelliptic curves and discuss some properties of pseudorandomness of sequences derived from these curves. In particular, we look at two different ways of generating sequences, that is, the linear congruential generator and the Frobenius endomorphism generator over hyperelliptic curves of genus 2. We show that these sequences possess good pseudorandom properties in terms of linear complexity.

Joint work with László Mérai (RICAM, Austrian Academy of Sciences).