RANDOM POLYNOMIALS IN LEGENDRE SEQUENCES

Katalin Gyarmati (Eötvös Loránd University)

Abstract: It is crucial in pseudorandomness cryptographic applications that the smaller key used as a seed can be generated at random. Thus, if the Legendre sequence based on a polynomial (as proposed by Hoffstein and Lieman) is used, that is

$$\left\{\left(\frac{f(1)}{p}\right),\left(\frac{f(2)}{p}\right),\left(\frac{f(3)}{p}\right),\dots,\left(\frac{f(p)}{p}\right)\right\},$$

it is important to choose the polynomial f at random. Goubin, Mauduit, and Sárközy presented some non-restrictive conditions on the polynomial f, but these conditions may not be satisfied if we choose a truly random polynomial. However, how can it be ensured that the sequence's pseudo-random measures are always low for nearly "random" polynomials? These semirandom polynomials will be constructed with as few modifications as necessary from a truly random polynomial. This is a joint work with Károly Müllner.