Séminaire de théorie des nombres

Le 22 octobre 2018 à 14h (Jussieu)

Drinfeld Modules, Hasse Invariants and Factoring Polynomials over Finite Fields

Exposé de Anand Kumar Narayanan
(IMJ-PRG)

Résumé : We present three novel algorithms to factor polynomials in one variable over finite fields using the arithmetic of Drinfeld modules. The first algorithm estimates the degree of an irreducible factor of a polynomial from Euler-Poincare characteristics of random Drinfeld modules. Knowledge of a factor degree allows one to rapidly extract all factors. The second algorithm is a random Drinfeld module analogue of Berlekamp's algorithm, partly inspired by Lenstra's elliptic curve method for integer factorization. The third algorithm employs Drinfeld modules with complex multiplication and will be the primary focus of the talk. The main idea is to compute a lift of the Hasse invariant with Deligne's congruence playing a critical role. We will discuss practical implementations and complexity theoretic implications of the algorithms.