SOME TOOLS FOR PRIMALITY PROVING ALGORITHMS AND JACOBIANS VARIETIES

Tony EZOME
Université des Sciences et Techniques de Masuku (USTM)
Franceville - Gabon

Abstract

That is a talk in two parts. The first one is about algorithms for determining whether a given integer n is prime or composite. The simplest algorithms, namely the Miller-Rabin test and the PocKlington-Lehmer algorithm, use properties of $\mathbb{Z}/n\mathbb{Z}$. However $\mathbb{Z}/n\mathbb{Z}$-algebras play an important role in the construction of powerfull primality tests. We will recall a few properties of Galois ring extensions of $\mathbb{Z}/n\mathbb{Z}$. And then we will describe how we use them for primality testing algorithms.
The second part of the talk will be concerned with the problem of computing the quotient of the Jacobian variety J of an hyperelliptic curve C by a certain subgroup. We will start from the genus one case (with elliptic curves).

Date: September 11, 2015.