RENATE SCHEIDLER, University of Calgary

Efficient Divisor Reduction on Hyperelliptic Curves

A key ingredient in hyperelliptic curve arithmetic is divisor reduction. Standard reduction methods take as input a non-reduced divisor in Mumford representation and iteratively generate a sequence of divisors until a reduced one is obtained. In this computationally expensive process, the degrees of the intermediate Mumford coefficients gradually decrease down to the genus of the curve. This talk will illustrate how to replace this costly procedure by the computation of just two linear recurrences which allow the recovery of the Mumford polynomials of the reduced target divisor at the end. The two scenarios under consideration are a large input divisor that could have been obtained via an inexpensive tupling procedure for example, and an input divisor that is the sum of two reduced divisors, as encountered in scalar multiplication using non-adjacent form.