



CONGRESO DE JÓVENES INVESTIGADORES

Real Sociedad Matemática Española

Universidad de Murcia, del 7 al 11 de Septiembre de 2015

Halve-and-add in genus 2 type II curves over binary fields

Ricard Garra Oronich¹

We give a method to compute multiples kD of a divisor in the Jacobian variety of a curve of genus 2 in characteristic 2 based on halving algorithms. Our method is competitive compared to the classic algorithms based on double-and-add, and also compared to analogous for other curves over binary fields. We show explicit halving formulas for each possible divisor class for type II curves (with $h(x) = x$), detailing all the process to obtain them.

This is a joint work with Josep M. Miret and Jordi Pujolàs.

¹Departament de matemàtica
Universitat de Lleida
garra@matematica.udl.cat