Publicacions més rellevants de la línia de recerca:

Problemes computacionals amb corbes el.líptiques i hiperel.líptiques

---

Referència: Miret, J., Moreno, R., Pujolàs, J. and Rio, A. Halving for the 2-Sylow subgroup of genus 2 curves over binary fields. *Finite Fields Appl.*, **15(5)** (2009), pp. 569–579.

Abstract: We give a deterministic polynomial time algorithm to find the structure of the 2-Sylow subgroup of the Jacobian of a genus 2 curve over a finite field of characteristic 2. Our procedure starts with the points of order 2 and then performs a chain of successive halvings while such an operation makes sense. The stopping condition is triggered when certain polynomials fail to have roots in the base field, as previously shown by I. Kitamura, M. Katagi and T. Takagi. The structure of our algorithm is similar to the already known case of genus 1 and odd characteristic.

Referència: Miret, J., Moreno, R., Rio. A. and Valls, M. Computing the ℓ-power torsion of an elliptic curve over a finite field. *Math. Comp.*, **78(267)** (2009), pp. 1767–1786.

Abstract: The algorithm we develop outputs the order and the structure, including generators, of the ℓ-Sylow subgroup of the group of rational points of an elliptic curve defined over a finite field. To do this, we do not assume any knowledge of the group order. We are able to choose points in such a way that a linear number of successive ℓ-divisions leads to generators of the subgroup under consideration. After the computation of a couple of polynomials and their resultant, each division step relies on finding rational roots of polynomials of degree ℓ. We specify in complete detail the case $\ell = 3$, when the complexity of each trisection is given by the computation of cubic roots in finite fields.

Referència: Miret, J., Moreno, R., Sadornil, D., Tena, J. and Valls, M. Computing the height of volcanoes of l-isogenies of elliptic curves over finite fields. *Appl. Math. Comp.*, **196(1)** (2008), pp. 67–76.

Abstract: The structure of the volcano of ℓ–isogenies, ℓ prime, of elliptic curves over finite fields has been extensively studied over recent years. Previous works present some results and algorithms concerning the height of such volcanoes in the case of isogenies whose kernels are generated by

a rational point. The main goal of this paper is to extend such works to the case of ℓ–isogenies whose kernels are defined by a rational subgroup. In particular, the height of such volcanoes is completely characterized and can be computationally obtained.