3rd European Congress of Mathematics
Poster sessions

Section 06: Discrete Mathematics and Computer Science | Poster number 110

Invariants of Hyperelliptic Curves of Genus 2 over Finite Fields

L. Hernández Encinas*, Dpto. de Matemáticas, Universidad de Salamanca.
J. Muñoz Masqué, Instituto de Física Aplicada, C.S.I.C., Madrid, Spain.

ABSTRACT

Let $\mathbb{F}$ be a finite field. As it is well-known ([3]), every hyperelliptic curve H of genus 2 defined over $\mathbb{F}$ can be given by an equation of the form $H\colon v^2 + h(u)v = f(u)$, where $h(u)$ is a polynomial of degree 2, and $f(u)$ is a monic polynomial of degree 5, *i.e.*,

$$H\colon v^2 + \left(a_1u^2 + a_3u + a_5\right) v = u^5 + a_2u^4 + a_4u^3 + a_6u^2 + a_8u + a_{10}, \qquad \forall a_i \in \mathbb{F}. \tag{1}$$

This equation is unique up to a change of coordinates of the form ([1, Proposition 1.2]):

$$(u, v) \mapsto \left(\alpha^2 u + \gamma, \alpha^5 v + \alpha^4 \epsilon u^2 + \alpha^2 \beta u + \delta\right), \qquad \alpha \in \mathbb{F}^*, \quad \beta, \gamma, \delta, \epsilon \in \mathbb{F}. \tag{2}$$

In order to classify non-singular hyperelliptic curves of genus 2 in a similar way as elliptic curves are classified ([4, III.§1], [2, 2.3]), we define some quantities, which only depend on the original coefficients of the curve, called the j–invariants. In this poster these quantities are proved to be invariants and they are computed explicitly in $\mathrm{char}(\mathbb{F}) \neq 2, 5$. Setting in 2:

$$\begin{array}{lll} \alpha = 1/10, & \beta = -a_3/2 + a_1a_2/5 + a_1^3/20, & \gamma = -a_2/5 - a_1^2/20, \\ \delta = -a_5/2 + a_3a_2/10 + a_3a_1^2/40 - a_1a_2^2/50 - a_2a_1^3/100 - a_1^5/800, & & \epsilon = -a_1/2, \end{array}$$

we obtain the reduced equation for H:

$$v^2 = u^5 + 2 \cdot 5^3 c_4 u^3 + 2^2 \cdot 5^4 c_6 u^2 + 5^3 c_8 u + 2^2 \cdot 5^5 c_{10}.$$

Let Δ be the discriminant of the non-hyperelliptic curve, H ([1]), then its *j-invariants* are:

$$j_1 = c_4^{10}/\Delta, \qquad j_2 = c_8^5/\Delta, \qquad j_3 = c_{10}^4/\Delta, \qquad j_4 = c_6^{20}/\Delta^3.$$

Theorem *The quantities j_i, $1 \le i \le 4$, are invariants under the change of coordinates of type 2.*

References

[1] P. Lockhart, On the discriminant of a hyperelliptic curve, *T. Am. Math. Soc.* **342**, 2 (1994), 729–752.

[2] A. Menezes, Elliptic curve public key cryptosystems, Kluwer Academic Publishers, Boston, 1993.

[3] N. Koblitz, Algebraic aspects of Cryptography, ACM 3, Springer-Verlag, New York, 1998.

[4] J. Silverman, The arithmetic of elliptic curves, GTM 106, Springer-Verlag, New York, 1986.

Keywords: *Hyperelliptic curves, Invariants of curves, Genus of a curve, Finite fields, Cryptology.*

Mathematics Subject Classification: *11G20, 11G30, 14H45, 94A60*

Contact Address: encinas@gugu.usal.es