Some Computational Aspects of Jacobians of Curves in the Family $y^3 = \gamma x^5 + \delta$ Over $\mathbb{F}_p$.

Régis Blache[*], Jean-Pierre Cherdieu.[†] Jorge Estrada Sarlabous.[‡]

January 19, 2004

Abstract

In this paper, we study the Jacobian varieties of certain diagonal curves of genus four : we first give the structure of the Jacobian, showing that it is simple over the prime field in most cases, then we give a reduction algorithm, suitable for calculations in the group of its rational points.

AMS Subject Classification:

14H45, 14H40, 14H05, 14Q05, 14Q20, 11G10, 11T71.

Keywords:

Diagonal curve, Jacobi sum, Jacobian Variety, Reduction Algorithm .

Introduction

During the last decade, much work has been done to study the Jacobian varieties of curves of genus 2 (hyperelliptic) or 3 (hyperelliptic or Picard). Two questions arise naturally : the first is to determine the structure of the Jacobian variety, the second is to represent its points in order to perform efficiently computations in the group of its rational points. In this paper, we study the Jacobians of certain diagonal genus 4 curves from this point of view.

[*]Département de Mathématiques et Informatique. Université des Antilles et de la Guyane. Campus de Fouillole, F97159 Pointe-à-Pitre CEDEX. e-mail: rblache@univ-ag.fr

[†]Département de Mathématiques et Informatique. Université des Antilles et de la Guyane. Campus de Fouillole, F97159 Pointe-à-Pitre CEDEX. e-mail: jpcherdi@univ-ag.fr

[‡]Department of Geometry. ICIMAF, Calle E No. 309, esquina 15, Vedado, La Habana, Cuba. e-mail: jestrada@icmf.inf.cu

We first recall well known facts. Let C be a curve of genus g defined over a finite field k. Its *Jacobian variety* $J(C)$ is an abelian variety of dimension g ; in particular its rational points $J(C)(k)$ form a group. An important tool in the study of J_C is the characteristic polynomial of the action of the Frobenius endomorphism of $J(C)$ relative to k. It is well known (cf. [Tate] for instance) that the decomposition of $J(C)$ as a product of simple abelian varieties corresponds to the factorisation of the characteristic polynomial over $\mathbb{Q}$. In the case of diagonal curves, the roots of this polynomial are Jacobi sums ; we use this fact, as well as arithmetic information on Jacobi sums (mainly Stickleberger theorem) to make explicit the structure of $J(C)$.

The second part of this work is devoted to finding a representation of the elements of $J(C)(k)$, suitable for performing computations in this group. Earlier works on this subject follow two directions : in the first one, an isomorphism between $J(C)(k)$ and the ideal class group of a ring of regular functions on C is used ; in the second, more geometric, one tries to generalize the "chord and tangent" method for elliptic curves to higher genus curves. We shall adopt the second one. In order to do this, we shall work with the canonical model of the curve C in $\mathbb{P}^3$, and consider its intersections with quadrics ; the method is a generalisation of the one in [EstReiChe].

The paper is organized as follows : in section I, we calculate explicitely the roots of the characteristic polynomial of the action of the Frobenius of $J(C)$ in terms of Jacobi sums. Then we use arithmetic information on these sums to obtain informations on the structure of $J(C)$. The second section is devoted to a reduction algorithm : we first give a bijection between the points in $J(C)(k)$ and certain divisors on the curve C, using the canonical model of C, then we study the intersection of C with quadrics to give the algorithm.

1 The structure of the Jacobian.

1.1 General facts.

If $C(\mathbb{F}_q)$ is a complete non-singular curve of genus g, one important tool for studying its Jacobian variety $J(C)$ is Weil's theorem:

Theorem 1.1 *There exist complex numbers $\alpha_1, \alpha_1, \ldots, \alpha_{2g}$ such that,*

$$N_r = \#C(\mathbb{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} {\alpha_i}^r \tag{1}$$

for $r > 0$, or equivalently, the power series

$$Z(C,T) = \exp(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}) \in \mathbb{C}[[T]]$$

represents a rational function, with numerator

$$L(C,T) = \prod_{i=1}^{2g}(1-\alpha_i T)$$

and denominator $(1-T)(1-qT)$. *Moreover,* $L(C,T)$ *has integer coefficients and the complex numbers* α_i *have absolute value* $q^{1/2}$.

$Z(C,T)$ and $L(C,T)$ are called the zeta function and the L-polynomial of $C/\mathbb{F}_q$, respectively. We have also

$$L(C,T) = T^{2g}P(1/T)$$

where $P(\lambda)$ is the characteristic polynomial of the Frobenius endomorphism π of $J(C)$ relative to $\mathbb{F}_q$. Thus, the computation of $Z(C,T)$ reduces to the computation of $P(\lambda)$. It is also well known that the number of $\mathbb{F}_q$-rational points of $J(C)$ is equal to :

$$|J(C)(\mathbb{F}_q)| = L(C,1) = P(1).$$

1.2 Diagonal Curves and their Zeta Functions

First recall that a *diagonal curve* over $\mathbb{F}_q$ is a curve having an affine equation of the form $y^{m_1} = ax^{m_2} + b$, with $m_1, m_2 \geq 2$ integers prime to q, and a, b in $\mathbb{F}_q^*$. Such a curve has genus :

$$g = \frac{1}{2}\left((m_1-1)(m_2-1) - gcd(m_1,m_2) + 1\right).$$

In the following, we restrict our attention to the diagonal curves C of genus 4 in the family :

$$D(3,5;\gamma,\delta) \ : \ y^3 = \gamma x^5 + \delta, \ \gamma, \ \delta \in \mathbb{F}_q^*.$$

We first determine the number N_i of $\mathbb{F}_{q^i}$-rational points on C. Set $d = \gcd(5, q-1)$ and $e = \gcd(3, q-1)$, and let χ be a character of order de of the multiplicative group $\mathbb{F}_q^*$, extended to $\mathbb{F}_q$ by setting $\chi(0) = 0$; from a classical result on the number of solutions of diagonal equations [Small], we have :

$$N_1 = 1 + \sum_{i=0}^{d-1}\sum_{j=0}^{e-1}\chi^{ei}(-\gamma^{-1})\chi^{ei+dj}(\delta)j_{\mathbb{F}_q}\left(\chi^{ei},\chi^{dj}\right),$$

where

$$j_{\mathbb{F}_q}(\chi^{ei},\chi^{dj}) = \sum_{x\in\mathbb{F}_q}\chi^{ei}(x)\chi^{dj}(1-x)$$

is the *Jacobi sum* over $\mathbb{F}_q$, attached to the characters χ^{ei} and χ^{dj}, and the number 1 corresponds to the point at infinity (the blowing up of the singular point $P_\infty(0:1:0)$ of the plane model gives a single point since the exponents 3 and 5 are coprime integers). Noting that the Jacobi sum with $i = j = 0$ is q, and the ones with $i = 0,\ j \neq 0$ or $i \neq 0,\ j = 0$ are zero, we can rewrite this expression as follows:

$$\begin{aligned} N_1 &= q + 1 + \sum_{x \in \mathbb{F}_q} \sum_{i=1}^{d-1} \sum_{j=1}^{e-1} \chi^{ei}(-\gamma^{-1}) \chi^{ei+dj}(\delta) \chi^{ei}(x) \chi^{dj}(1-x) \\ &= q + 1 + \sum_{i=1}^{d-1} \sum_{j=1}^{e-1} \chi^{ei}(-\gamma^{-1}) \chi^{ei+dj}(\delta) j_{\mathbb{F}_q}(\chi^{ei}, \chi^{dj}) \end{aligned}$$

In order to write down the zeta function of C over $\mathbb{F}_q$, we only have to compute the N_i. If the residue of q^i modulo 15 is not one, then at least one of the integers d, e will be 1, and the preceding formula gives us that $N_i = q^i + 1$. We are reduced to studying the remaining cases: let f be the order of q in the multiplicative group $G = (\mathbb{Z}/15\mathbb{Z})^*$. Let χ_1 be a character of order 15 of $\mathbb{F}_{q^f}^*$; we know that if we set for every $l \geq 1 :\ \chi_l := \chi_1 \circ N_{\mathbb{F}_{q^{fl}}/\mathbb{F}_{q^f}}$, with $N_{\mathbb{F}_{q^{fl}}/\mathbb{F}_{q^f}}$ the norm from $\mathbb{F}_{q^{fl}}$ to $\mathbb{F}_q$, then χ_l is a character of order 15 of the group $\mathbb{F}_{q^{fl}}^*$. Since in our case $d = 5$ and $e = 3$, we get :

$$\begin{aligned} N_{fl} &= q^{fl} + 1 + \sum_{i=1}^{4} \sum_{j=1}^{2} \chi_l^{3i}(-\gamma^{-1}) \chi_l^{3i+5j}(\delta) j_{\mathbb{F}_{q^{fl}}}(\chi_l^{3i}, \chi_l^{5j}) \\ &= q^{fl} + 1 + \sum_{i \in G} \chi_l^{3i}(-\gamma^{-1}) \chi_l^{8i}(\delta) j_{\mathbb{F}_{q^{fl}}}(\chi_l^{3i}, \chi_l^{5i}) \\ &= q^{fl} + 1 + \sum_{i \in G} \left(\chi_1^{3i}(-\gamma^{-1}) \chi_1^{8i}(\delta) j_{\mathbb{F}_{q^f}}(\chi_1^{3i}, \chi_1^{5i}) \right)^l \end{aligned}$$

the last equality coming from the Hasse Davenport relation, and from the fact that, since $a, b \in \mathbb{F}_{q^f}$, we have $\chi_l(a) = \chi_1(a)^l$ and $\chi_l(\delta) = \chi_1(\delta)^l$. On the other hand, since $x \mapsto x^q$ is an automorphism of $\mathbb{F}_{q^f}$, we have the following for the Jacobi sums involved in the last equality :

$$j_{\mathbb{F}_{q^f}}(\chi_1^{3q}, \chi_1^{5q}) = j_{\mathbb{F}_{q^f}}(\chi_1^3, \chi_1^5).$$

Thus we see that if H is the subgroup of order f of G, generated by q, then the Jacobi sum $j_{\mathbb{F}_{q^f}}(\chi_1^{3i}, \chi_1^{5i})$ is independent of the choice

of i in a coset of H in G ; for this reason we introduce Q, the quotient group G/H, say of order g. With these notations, and since a and b are elements of $\mathbb{F}_q$ fixed by the automorphism $x \mapsto x^q$, we get the relation :

$$N_{fl} = q^{fl} + 1 + f \sum_{i \in Q} \left(\chi_1^{3i}(-\gamma^{-1}) \chi_1^{3i+5j}(\delta) j_{\mathbb{F}_{q^f}}(\chi_1^{3i}, \chi_1^{5i}) \right)^l$$

Now if π_j, $1 \leq j \leq 8$ are the reciprocal roots of the numerator of the zeta function of C, we can write for any $i \geq 1$:

$$N_i = q^i + 1 + \sum_{j=1}^{8} \pi_j^i$$

Comparing the two results, we get, for all $k \geq 1$:

$$q^k + 1 + \sum_{j=1}^{8} \pi_j^k = \begin{cases} q^k + 1 \text{ if } k \text{ is not a multiple of } f \\ q^{fl} + 1 + f \sum_{i \in K} \left(\chi_1^{3i}(-\gamma^{-1}) \chi_1^{8i}(\delta) j_{\mathbb{F}_{q^f}}(\chi_1^{3i}, \chi_1^{5i}) \right)^l \text{ if } k = fl. \end{cases}$$

Thus we get :

$$\pi_j^f = \chi_1^{3i}(-\gamma^{-1}) \chi_1^{8i}(\delta) j_{\mathbb{F}_{q^f}}(\chi_1^{3i}, \chi_1^{5i}) \quad \text{for some } i \in Q$$

and the reciprocal roots are exactly the f-roots of these algebraic integers.

Now we can write down the numerator of the zeta function of C over $\mathbb{F}_q$:

Proposition 1.1 *Let q be a power of a prime p, f be the order of the residue of q in $G = (\mathbb{Z}/15\mathbb{Z})^*$, and χ_1 a character of order 15 of $\mathbb{F}_{q^f}^*$. If $Q = G/H$, $H =< q >$, then the numerator of the zeta function of the curve C defined over $\mathbb{F}_q$ is :*

$$P(T) = \prod_{i \in Q} (1 - \chi_1^{3i}(-\gamma^{-1}) \chi_1^{8i}(\delta) j_{\mathbb{F}_{q^f}}(\chi_1^{3i}, \chi_1^{5i}) T^f).$$

1.3 Jacobi Sums and the structure of the Jacobian

In order to study the structure of the Jacobian of C, we have to study the L-polynomial of C ; this is the aim of this section : we give well-known arithmetic properties of the Jacobi sums that are the reciprocal roots of this polynomial, then we deduce the structure of the Jacobian from the factorisation of this polynomial in the case where q is prime.

Computation of the Jacobi sums Assume first that $q = p$ is a prime number such that $p \equiv 1 \bmod 15$. If we denote $\mathfrak{D} = \mathbb{Z}[\zeta_{15}]$, the ideal $p\mathfrak{D}$ completely splits in $\mathfrak{D}$. Let $\mathfrak{p}$ be a fixed prime ideal of $\mathfrak{D}$ lying over p. Then $\mathfrak{D}/\mathfrak{p}$ is isomorphic to $\mathbb{F}_p$. Let $\chi_\mathfrak{p}$ be the $15-th$ power residue symbol modulo $\mathfrak{p}$, which means that $\chi_\mathfrak{p}$ is a multiplicative character of order 15 (cf. [Lidl-Nied] p. 205) that sends a nonzero x in $\mathfrak{D}$ to

$$\chi_\mathfrak{p}(x) = \left(\frac{x}{\mathfrak{p}}\right)_{15} \equiv x^{(p-1)/15} \pmod{\mathfrak{p}},$$

the unique 15-th root of unity in $\mathfrak{D}$ congruent to $x^{(p-1)/15}$ modulo $\mathfrak{p}$.

For any integers a and b we set

$$j(a,b) := j_\mathfrak{p}(\chi_\mathfrak{p}^a, \chi_\mathfrak{p}^b) = \sum_{\substack{x,y \in (\mathfrak{D}/\mathfrak{p})^\times \\ x+y=1}} \chi_\mathfrak{p}(x)^a \chi_\mathfrak{p}(y)^b.$$

We have the following congruence of Iwasawa (cf. [Yui] p.113):

$$j(a,b) \equiv \chi_\mathfrak{p}^{15-(a+b)}(-1) \bmod (1-\zeta_{15})^2.$$

Moreover, we have **Stickelberger Relation** cf. [Lang] thm. IV.11, p.98) : for positive integers a, b such that 15 doesn't divide $a+b$, we have the equality of ideals of $\mathfrak{D}$:

$$\left(j_\mathfrak{p}(\chi_\mathfrak{p}^a, \chi_\mathfrak{p}^b)\right) = \mathfrak{p}^{\theta(a,b)},$$

where

$$\theta(a,b) = \sum_{n \in (\mathbb{Z}/15\mathbb{Z})^*} \left(\left[\frac{(a+b)n}{15}\right] - \left[\frac{an}{m}\right] - \left[\frac{bn}{m}\right] \right) \sigma_n^{-1},$$

(and σ_n is the automorphism of $Gal(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$ defined by $\zeta_{15} \mapsto \zeta_{15}^n$).

In our case, we obtain :

$$\left(j_\mathfrak{p}(\chi_\mathfrak{p}^3, \chi_\mathfrak{p}^5)\right) = \mathfrak{p}^{\sigma_8}\mathfrak{p}^{\sigma_4}\mathfrak{p}^{\sigma_2}\mathfrak{p}^{\sigma_{14}}.$$

Since $\mathbb{Z}[\zeta_{15}]$ is a principal ideal domain, if we denote by β a generator of $\mathfrak{p}$, then : $(j_\mathfrak{p}(\chi_\mathfrak{p}^3, \chi_\mathfrak{p}^5)) = (\beta)^{\theta(3,5)}$. Thus $j_\mathfrak{p}(\chi_\mathfrak{p}^3, \chi_\mathfrak{p}^5) = u\beta^{\theta(3,5)}$, for some u in $\mathfrak{D}^*$; moreover all the conjugates of u over $\mathbb{Q}$ have complex absolute value 1, thus from a well-known result u is a root of unity. Since the only roots of unity in $\mathbb{Z}[\zeta_{15}]$ are the $\pm\zeta_{15}^s$ with $0 \le s \le 14$ (cf. [Be-Ev-W] thm. 2.1.13 p.64), we get :

$$j_\mathfrak{p}(\chi_\mathfrak{p}^a, \chi_\mathfrak{p}^b) = \pm\zeta_m^s \beta^{\theta(a,b)}.$$

So the computation of the exact value of the Jacobi sum is reduced to the determination of the sign, the exponent s, and of the generator β of the ideal $\mathfrak{p}$. The computation of the generator β is known as the "Principal ideal problem" (cf. [Coh] p. 354 6.5.5) and can be solved using algorithm 6.5.10 (cf. [Coh] p. 355).

Example :

- $p = 1500015015015150004531$

  $\mathfrak{p} = 1500015015015150004531\mathbb{Z}[\zeta]+(575895549308087764 4+\zeta)\mathbb{Z}[\zeta]$,

  and

  $$\beta = 49 + 287\zeta - 33\zeta^2 + 292\zeta^3 + 101\zeta^4 + 15\zeta^5 - 66\zeta^6 + 93\zeta^7.$$

The answer is very quick even for "large" prime numbers. To find the sign $r \in \pm 1$, and the exponent s we follow Buhler and Koblitz (cf. [Buh-Kob] p.150) and use the Iwasawa congruence,

$$j(3,5) \equiv \chi^7(-1) \bmod (1-\zeta)^2,$$

in the ring $\mathbb{Z}[\zeta_{15}]$. We set $\beta^{\theta(3,5)} = \sum_{j=0}^{7} a_j \zeta^j$ and $\pi = \zeta - 1$. So we have $\zeta^k = (1+\pi)^k \equiv 1 + k\pi \bmod \pi^2$, and

$$\begin{aligned} j(3,5) &\equiv r(1+s\pi)\textstyle\sum_{j=0}^{7} a_j(1+j\pi) \bmod \pi^2 \\ &\equiv r\left(\sum_0^7 a_j + \left(s\sum_0^7 a_j + \sum_0^7 j a_j\right)\pi\right) \equiv \chi^7(-1) \bmod \pi^2. \end{aligned}$$

Note that if $p = 15f+1$, then $\chi^7(-1) = (-1)^f$. We will choose the sign r such that $(-1)^f \equiv r\sum_0^7 a_j \bmod 15$, and set $s \equiv r\sum_0^7 j a_j \bmod 15$.

Structure of the Jacobian : The aim of this paragraph is to check whether the Jacobian $J(C)$ of C is $\mathbb{F}_p$-simple, depending on the residue of p modulo 15. Recall that the characteristic polynomial of Frobenius of $J(C)$ relative to $\mathbb{F}_p$ is given by :

$$P(T) = \prod_{i \in K} (T^f - \chi_1^{3i}(-\gamma^{-1})\chi_1^{8i}(\delta) j_{\mathbb{F}_{p^f}}(\chi_1^{3i}, \chi_1^{5i})),$$

where f is the order of p in $\mathbb{Z}/15\mathbb{Z}^*$. If the polynomial $P(T) = T^{2g}L(C, 1/T)$ is $\mathbb{Q}$-irreducible, then the Jacobian $J(C)$ is $\mathbb{F}_p$-simple (cf [Tate] Theorem 2.(e)).

Let us study the degrees as algebraic integers of the roots of $P(T)$, depending on the residue of p modulo 15 :

1) $p \equiv 1 \bmod 15$:

Here $f = 1$, the decomposition subfield of the prime p in $\mathbb{Q}(\zeta_{15})$ is the whole field $\mathbb{Q}(\zeta_{15})$, and the roots of P are the eight algebraic integers :

$$\chi_1^{3i}(-\gamma^{-1})\chi_1^{8i}(\delta) j_{\mathbb{F}_p}(\chi_1^{3i}, \chi_1^{5i}),\ i \in G$$

Since the term $\chi_1^{3i}(-\gamma^{-1})\chi_1^{8i}(\delta)$, being a root of unity, does not change the prime ideal decomposition, we see that the ideals generated by these eight algebraic integers have distinct prime decompositions in the integer ring of $\mathbb{Q}(\zeta_{15})$. Since they are conjugate under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$, we see that they must be algebraic integers of degree 8 over $\mathbb{Q}$, and that P must be their minimal polynomial, hence irreducible.

2) $p \equiv 2, 8 \bmod 15$:

We study these two cases together, since 2 and 8 generate the same subgroup of G. Here the decomposition field k_p of p is a quadratic extension of $\mathbb{Q}$. In fact, we can write in its integers ring : $(p) = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1$, $\mathfrak{p}_2$ being two prime ideals, fixed by the elements $\sigma_2, \sigma_4, \sigma_8$ of G, and permuted by $\sigma_7, \sigma_{11}, \sigma_{13}, \sigma_{14}$. The decomposition of the ideal generated by the Jacobi sum is then : $(j) = \mathfrak{p}_1^3\mathfrak{p}_2$.

Thus the two Jacobi sums must be algebraic integers of degree 2 over $\mathbb{Q}$, and the roots of P are the fourth roots of these sums. To conclude in this case, we remark that since the ring of integers $\mathbb{Z}[\zeta_{15}]$ of $\mathbb{Q}(\zeta_{15})$ is a principal domain, the ring of integers of k_p is a principal domain too, and we can apply Eisenstein criterion to the polynomial (over this ring)

$$T^4 - \chi_1^{3i}(-\gamma^{-1})\chi_1^{8i}(\delta) j_{\mathbb{F}_{p^4}}(\chi_1^{3i}, \chi_1^{5i})$$

and to the prime $\mathfrak{p}_2$. We get that this last polynomial is irreducible over k_p, and that its roots are algebraic integers of degree 8.

3) $p \equiv 7, 13 \bmod 15$:

Here we can rewrite what we have done in the preceding case, to obtain the same result.

4) $p \equiv 4 \bmod 15$:

We have $f = 2$, and the decomposition subfield of p is a degree four extension of $\mathbb{Q}$. We get four primes in the decomposition of (p): $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, each one being fixed by σ_4, $\mathfrak{p}_1^{\sigma_2} = \mathfrak{p}_2$, $\mathfrak{p}_1^{\sigma_{14}} = \mathfrak{p}_3$, $\mathfrak{p}_1^{\sigma_7} = \mathfrak{p}_4$. The ideal generated by the Jacobi sum $j_{\mathbb{F}_{p^2}}(\chi_1^3, \chi_1^5)$ has the form $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3$. Considering the action of $\mathrm{Gal}(k_p/\mathbb{Q})$ on this decomposition, we get that the Jacobi sum is an algebraic integer of degree 4 over $\mathbb{Q}$.

Here again we can apply Eisenstein's criterion to the polynomial

$$T^2 - \chi_1^{3i}(-\gamma^{-1})\chi_1^{8i}(\delta) j_{\mathbb{F}_{p^2}}(\chi_1^{3i}, \chi_1^{5i})$$

and to one of the primes $\mathfrak{p}_1, \mathfrak{p}_3$ in the integer ring of k_p, and we get the desired result.

5) $p \equiv 11 \bmod 15$:
We can rephrase here what we have just said, and we get the same result.

6) $p \equiv 14 \bmod 15$:
Here we get that the prime decomposition of the ideal generated by the Jacobi sum is $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 = (p)$, and that the Jacobian is supersingular.

Finally we obtain the :

Proposition 1.2 *The Jacobian of the curve C, defined over the prime field $\mathbb{F}_p$, is $\mathbb{F}_p$-simple if the residue of p modulo* 15 *belongs to the set* $\{1, 2, 4, 7, 8, 11, 13\}$*; it is supersingular if* $p \equiv 14 \bmod 15$.

Example :

Let $p = 181$, we find

$$\begin{aligned} P(T) \quad &= 1073283121T^8 - 41508187T^7 + 3865798T^6 \\ &+116021T^5 - 9545T^4 + 641T^3 + 118T^2 - 7T + 1, \end{aligned}$$

and,

$$\#J(C)(\mathbb{F}_{181}) = 1035747961, \text{ a prime.}$$

2 A reduction algorithm for curves $y^3 = p_5(x)$

We give a reduction algorithm for a slightly more general class of curves, namely the plane projective curves defined by an equation $C : Y^3Z^2 = Z^5 p_5(\frac{X}{Z})$ over $k = \mathbb{F}_q$, a field of characteristic different from 3. We assume the point at infinity $P_\infty = (0 : 1 : 0)$ to be the only singular point, i.e. that the affine plane curve of equation $y^3 = p_5(x)$ is nonsingular. Note this is equivelant to asking the polynomial $p_5(X) := a_5X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ to be separable over $\mathbb{F}_q$.

2.1 Representing the points of the Jacobian by affine divisors

We will make extensive use of the **Riemann-Roch theorem** : let D be any divisor on C, a curve of genus g, then we have :

$$l(D) = l(K - D) + \deg D + 1 - g,$$

where K is the canonical divisor on C.

Since C has genus 4, any point of $J(C)(k)$ can be represented by a degree 0 divisor on C of the form $D - dP_\infty$, $d \leq 4$, and D effective, affine (its support doesn't meet P_∞). We will see here to what extent this representation is unique, and find a subset of the set of affine effective divisors of degree less than 4 on C such that the map $D \mapsto D - \deg(D)P_\infty$ is one-to-one.

Assume that we have $D_1 - d_1 P_\infty \equiv D_2 - d_2 P_\infty$, D_1, D_2 two affine effective divisors of degrees d_1, d_2 such that $d_1 \leq d_2$. We get that $D_1 + (d_2 - d_1)P_\infty - D_2 \equiv 0$, i.e. there is a function f in $K(C)$, the function field of C, such that $< f >= D_1 + (d_2 - d_1)P_\infty - D_2$. We are reduced to classifying the functions in $K(C)$ whose polar divisor is affine of degree less than 4. The quantity $l(K - D)$ has the following geometric interpretation: it is the dimension of the space of hyperplanes in $\mathbb{P}^{g-1}$ passing through the points of D on the canonical model of C. For this reason, it is more convenient here to work with the canonical model of C; since C has genus four, its canonical model is the intersection of a quadric and a cubic in $\mathbb{P}^3 = \mathrm{Proj}\,(k[X_0, X_1, X_2, Y])$, given by the following homogeneous equations :

$$\begin{cases} Y^3 & = & a_5 X_2^2 X_1 + a_4 X_2^2 X_0 + a_3 X_1^3 + a_2 X_1^2 X_0 + a_1 X_1 X_0^2 + a_0 X_0^3 \\ X_2 X_0 & = & X_1^2 \end{cases}$$

We want to study the dimensions of the spaces $l(D)$, D an affine effective divisor of degree $d_2 \leq 4$:

i) if $d_2 = 1, 2$ that is $D = P$ or $D = P + Q$, since K is very ample (C is not hyperelliptic) we know that $l(K - P) = l(K) - 1$, and $l(K - P - Q) = l(K) - 2$ for any P, Q (cf [Har] for instance). Thus Riemann-Roch theorem ensures us that $l(P) = l(P + Q) = 1$, these spaces contain only the constant functions.

ii) if $d_2 = 3$, from the geometric interpretation of the Riemann-Roch theorem, we get that $l(P + Q + R) = 1$ or 2 depending on whether the points P, Q, R are in general position or collinear in $\mathbb{P}^3$. This last case only happens in a very peculiar configuration :

Lemma 2.1 *If three affine points P, Q, R of the canonical model of C are collinear in $\mathbb{P}^3$, then there exists $a \in \bar{k}$ such that :*

$$P(1 : a : a^2 : b)\ ;\ Q(1 : a : a^2 : c)\ ;\ R(1 : a : a^2 : d),$$

where b, c, d are the three solutions of $y^3 = p_5(a)$.

Proof: The equations of the affine hyperplanes $H(x_1, y, x_2)$ in $\mathbb{P}^3$ can take the following forms :

1) $x_1 = a$,

2) $y = ax_1 + b$,

3) $x_2 = ay + bx_1 + c$.

First we just try to solve the system $H_1(x_1, y, x_2) = H_2(x_1, y, x_2) = 0$ and $x_2 = x_1^2$.

If $H_1(x_1, y, x_2) = x_2 - ay - bx_1 - c$ and $H_2(x_1, y, x_2) = x_2 - dy - ex_1 - f$ are two hyperplanes of the third type, then if $a \neq d$, y can be expressed as a linear function of x_1, we get a degree two equation on x_1 that cannot have three solutions. If $a = d \neq 0$, then x_1 is fixed by the equations of the hyperplanes, it gives x_2 and y, and there is at most one solution. If $a = d = 0$, then x_1 is fixed, $x_2 = x_1^2$ too ; finally y is not given by these three equations, but it must satisfy the remaining one, that is : $y^3 = p_5(x_1)$. Thus we are in the situation described in the lemma.

The study of the remaining cases is straightforward. ■

iii) if $d = 4$, again from the geometric interpretation of Riemann-Roch theorem, we get that $l(P + Q + R + S) = 1$ or 2, depending on whether P, Q, R, S are in general position or coplanar in $\mathbb{P}^3$ (note that from the preceding lemma they can't be all four collinear).

From these results we can deduce the following : assume as above that $D_1 - d_1 P_\infty \equiv D_2 - d_2 P_\infty$ with $d_2 \geq d_1$; we have :

i) if $d_2 \leq 2$, we have equality : $D_1 - d_1 P_\infty = D_2 - d_2 P_\infty$;

ii) if $d_2 = 3$ and the three points are not as in the lemma, we have again equality ; if they are as in the lemma then we can choose $D_1 = 0$ and $d_1 = 0$ since $D_2 - 3P_\infty$ is the divisor of the function $x_1 - a$;

iii) if $d_2 = 4$ and the four points are not coplanar, then we have equality ; if they are coplanar, we can choose D_1 such that $d_1 \leq 3$, since we can find a function f in $\mathcal{L}(P + Q + R + S)$ such that $f(P_\infty) = 0$.

This study motivates the following definition :

Definition 2.1 *Let $Div^*(C)$ be the set of affine effective divisors of degree less than or equal to four on C such that if* $\deg D = 3$ *(*resp. $\deg D = 4$*) the three (*resp. *four) points of D are not collinear (*resp. *coplanar) in the canonical model of C in $\mathbb{P}^3$.*

From this definition and the preceding discussion we get immediately :

Proposition 2.1 *The map :*

$$\begin{array}{rccc} \phi & : & Div^*(C) & \to & J(C)(k) \\ & & D & \mapsto & D - \deg(D) P_\infty \end{array}$$

is a bijection. ■

2.2 A coordinate system for the points of the Jacobian

From now on we work over the plane model $Y^3Z^2 = Z^5 p_5(\frac{X}{Z})$ of C. Note that the morphism $\mathbb{P}^3 \to \mathbb{P}^2$ given by $X_0 \mapsto Z$, $X_1 \mapsto X$, $X_2 \mapsto X^2$, and $Y \mapsto Y$ restricts to a birational morphism from the canonical model to the plane model, and to an isomorphism of the two affine models of $C\backslash\{P_\infty\}$.

We begin by pointing out two automorphisms of the rational function field of C $K(C)/k(x)$, namely $\sigma : y \mapsto \zeta y$ and σ^2, where ζ stands for a primitive cubic root of unity. Note that to any affine point $P = (x, y)$ of C correspond the points $(x, \zeta y)$ and $(x, \zeta^2 y)$, we denote respectively by σP and $\sigma^2 P$. Note that if P, Q, R are points as in lemma 2.1, their images by the former isomorphism must be of the form $P, \sigma P, \sigma^2 P$.

We begin with some definitions.

Definition 2.2 *The* weight *of a monomial in $k[x, y]$, $x^i y^j$, is the integer $3i + 5j$. The* weight *of a polynomial in $k[x, y]$ is the maximum of the weights of its monomials. A polynomial in $k[x, y]$ is* monic *if the coefficient of its term of greatest weight is* 1.

Let D be an affine effective divisor. We denote by v_D the monic element in $k[x, y]$ with minimum weight such that $< v_D >_0 \succeq D$. We call it the interpolating function of D.

Example : For a generic divisor D of degree 3, we get $v_D = a_{00} + a_{10}x + a_{01}y + a_{20}x^2$, for a generic divisor D of degree 4, $v_D = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy$, and for a generic divisor D of degree 5, $v_D = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{30}x^3$.

Remark:

- Note that the weight of a polynomial in $k[x, y]$ is just the pole order of the function it represents on the plane model of C.
- From the definition of v_D and the isomorphism between the affine parts of the canonical model and of the plane model, we can give conditions so that D does not contain the images of three collinear points or four coplanar points in the canonical model of C.

  i) If $\deg D = 3$, then D contains the images of three collinear points in the canonical model if and only if v_D writes $x + a_{00}$.

  ii) If $\deg D = 4$, then D contains the images of four collinear points in the canonical model if and only if v_D writes $x^2 + a_{01}y + a_{10}x + a_{00}$.

Now we associate to each D in $Div^*(C)$ a coordinate system : let $D = P_1 + \ldots + P_k$, $P_i(x_i, y_i)$ be in $Div^*(C)$. We associate to D the functions :

i) $u_D = \prod_{i=1}^{k}(x - x_i)$;

ii) the interpolating function v_D ;

iii) $w_D = \prod_{i=1}^{k}(y - y_i)$.

Let us show that this coordinate system is "good", i.e. that it defines a bijection. To do this, we need to get rid of certain divisors.

Definition 2.3 *We denote by* $\mathrm{Div}^{*,i}(C)$ *the set of affine effective divisors of degree* i *on* C*, and :*

$$\mathrm{Div}_0^{*,5}(C) = \{D \in \mathrm{Div}^{*,5}(C), \forall P, Q \in C, \{P, \sigma P, Q, \sigma Q\} \notin Supp(D)\}.$$

Let $\mathcal{D}(5) = \cup_{i=0}^{5}\mathrm{Div}^{*,i}(C)$, $\mathcal{D}_0(5) = Div^*(C) \cup \mathrm{Div}_0^{*,5}(C)$.

Proposition 2.2 *The map:*

$$\begin{array}{rccc} \Phi & : & \mathcal{D}_0(5) & \to & k[x] \times k[x,y] \times k[y] \\ & & D & \mapsto & (u_D, v_D, w_D) \end{array}$$

is a bijection from $\mathcal{D}_0(5)$ *to its image.*

The proof of this proposition is very similar to that of lemma 4 of [EstReiChe].

2.3 A reduction algorithm

We have seen that if $J(C)$ is the Jacobian of C, then every point of $J(C)(k)$ can be represented by $D - dP_\infty$, $D \in Div^*(C)$. The aim of a reduction algorithm is to solve the following problem :

from a divisor $D - dP_\infty$, $d \in \mathbb{N}$*, find a linearly equivalent divisor* $D_0 - d_0P_\infty$*, with* $D_0 \in Div^*(C)$.

Such an algorithm allows us to make additions in the Jacobian of C: starting from two points of $J(k)$ $D_1 - d_1P_\infty$ and $D_2 - d_2P_\infty$, we apply the algorithm to $D_1 + D_2 - (d_1 + d_2)P_\infty$ and find a representative of the required form. It is also possible to estimate the order of the former group computing multiples of a point $P - P_\infty$ of $J(C)(k)$.

We can describe a first reduction algorithm. Let $D - dP_\infty$, $n \geq 0$ a divisor of degree 0. Write $D = D_0 + E_1 + \ldots + E_k$, with $\deg D_0 = 5$; the divisor of the interpolating function $v_{D_0} = v_1$ can be written as: $< v_1 >= D_0 + D_1 - nP_\infty$ with $n \leq 9$, since $v_{P_\infty}(v_0) \leq v_{P_\infty}(x^3) = 9$, and we get :

$$D_0 - 5P_\infty \equiv -D_1 + (n-5)P_\infty.$$

Applying the same process to D_1, we get $v_{D_1} = v_1$ such that $< v_1 >= D_1 + D_2 - n_1P_\infty$, with $n_1 \leq n - 1$, and finally:

$$D_0 - 5P_\infty \equiv D_2 - n_2P_\infty, \qquad n_2 \leq 4.$$

Now choose $E_1 \preceq D - D_0$, with degree $5 - \deg D_2 > 0$, and we apply the preceding process to $D_3 = D_2 + E_1$, etc... In this way we get a (finite) sequence of divisors $(D_0, D_1, \ldots, D_{3k+2})$, and $D_{3k+2} - d_{3k+2}P_\infty$ is the reduction of D.

Unfortunately this algorithm needs to factor several polynomials, first to obtain D_1 from v_0, then to obtain D_2 from v_1, etc...; its complexity is high. Thus we now give a second algorithm, relying on the use of the resultant, and which performs the reduction mostly by solving 5×5 linear systems.

The coordinate system allows us to modify the preceding algorithm in such a way that we avoid most of the factorizations. Let us first roughly describe the principal steps of the new algorithm. We keep the same notations as in the former algorithm, and we set $\Phi(D_n) = (u_n, v_n, w_n)$.

Let D be an affine effective divisor of degree n. If $n < 5$, there is nothing to do. If $n \geq 5$, choose $D_0 \preceq D$, $\deg D_0 = 5$, and compute $\Phi(D) = (u_0, v_0, w_0)$ if possible. ¿From it, we will (generally) obtain $\Phi(D_1)$ and $\Phi(D_2)$, solving 5×5 linear systems, without regard to the supports of D_1 or D_2 (this would lead us to factorizations). Then from $\Phi(D_2)$ and E_1, we compute $\Phi(D_3)$, $D_3 = D_2 + E_1$ solving 5×5 linear systems, etc... .

In this way we get a sequence $(\Phi(D_0), \ldots, \Phi(D_{3k+2}))$, and it remains to obtain D_{3k+2} from $\Phi(D_{3k+2})$, with just one factorization : it is the reduction of D.

We now make precise what we have just claimed.

Lemma 2.2 *Let $D_0 \in \mathrm{Div}^{*,5}(C)$. We can compute :*
i) $\Phi(D_0)$ if $D_0 \in \mathrm{Div}_0^{*,5}(C)$;
ii) $\Phi(D_1)$ and $\Phi(D_2)$ else.

Proof: Let $D_0 = P_1 + \ldots + P_5$, $P_i(x_i, y_i)$. We consider two cases depending on whether D_0 is in $\mathrm{Div}_0^{*,5}(C)$ or not:

i) We compute directly : $u_0 = \prod_{i=1}^5 (x - x_i)$, and $w_0 = \prod_{i=1}^5 (y - y_i)$; finally we get v_0 solving the system $v_0(P_i) = 0,\ 1 \leq i \leq 5$, with v_0 of minimum weight.

ii) If $D_0 = P_1 + \sigma P_1 + P_2 + \sigma P_2 + P_3$.

Let us choose $v_0 = (x - x_1)(x - x_2)(x - x_3)$; we obtain $D_1 = \sigma^2 P_1 + \sigma^2 P_2 + \sigma P_3 + \sigma^2 P_3$; from this we deduce directly u_1 and w_1, and $v_1 = r(x - x_3)$, with r the equation of the line $(\sigma^2 P_1 \sigma^2 P_2)$. If we now set $v_2 = v_1$, we get the last two coordinates by the equations :

$$u_2 = \left(\frac{\mathrm{Res}_y(v_1, C)}{u_1} \right)^m \quad ; \quad w_2 = \left(\frac{\mathrm{Res}_x(v_1, C)}{w_1} \right)^m, \qquad (1)$$

where Res_y stands for the resultant with respect to y, $C : y^3 - p_5(x) = 0$ the equation of C, and $(*)^m$ means that we make the polynomial $*$ monic.

■

Lemma 2.3 *From $\Phi(D_0)$, we can compute :*
i) $\Phi(D_1)$, $\Phi(D_2)$;
ii) or D_2 explicitly.

In the proof, we will need to consider several cases, depending on the form of v_0 ; the aim of the following lemma is to give equivalent conditions for v_0 to have a linear factor.

Lemma 2.4 *Let $D_0 \in \mathrm{Div}_0^{+,5}(C)$; the following conditions are equivalent :*
i) $v_0 = a_{00}+a_{10}x+a_{20}x^2+a_{30}x^3+a_{01}y+a_{11}xy$ has a linear factor;
ii) either $D_0 \succeq P_1 + P_2 + P_3 + P_4$, with P_j four colinear points, or $D_0 \succeq P_1 + \sigma P_1$;
iii) $\mathrm{Res}(a_{00} + a_{10}x + a_{20}x^2 + a_{30}x^3, a_{01} + a_{11}x) = 0$.

Proof: (of lemma 2.3) : We make cases depending on v_0 :
1) if v_0 is linear (i.e. $a_{20} = a_{30} = a_{11} = 0$), then $< v_0 >= D_0 - 5P_\infty \equiv 0$, and there is nothing to do : $D_1 = D_2 = 0$;
2) if v_0 has a linear factor, we consider separately the two cases in ii) of lemma 2.4 :
a) if D_0 contains four collinear points, $v_0 = (x - x_5)r$, with r the equation of the line through the four points. Let M be the fifth intersection point of $r = 0$ with C. Then x_M is the root of the linear polynomial :

$$L_M = \frac{\mathrm{Res}_y(r, C)(x - x_5)}{u_0}.$$

If r depends on x, we get y_M solving $r(x_M, y) = 0$, and y_5 is the root of the linear polynomial :

$$L_5 = \frac{w_0(y - y_M)}{\mathrm{Res}_x(r, C)}.$$

If this is not so, $r = y - y_0$, $y_M = y_0$ and y_5 is the only root of $w_0/(y - y_0)^4$ linear.
Finally, once we have M and P_5 explicitly, we clearly know $D_1 = M + \sigma P_5 + \sigma^2 P_5$ and $D_2 = \sigma M + \sigma^2 M + P_5$ explicitly.
b) else $D_0 \succeq P_1 + \sigma P_1$, and $v_0 = c_1(x - x_1)$; we obtain u_1 and w_1 from formulae (1) and (2), $\sigma^2 P_1(x_1, \zeta^2 y_1)$, and $\zeta^2 y_1$ is a root of:

$$L = \frac{w_1}{gcd(\mathrm{Res}_x(c_1, C), w_1)}$$

if the denominator has degree 3. If its degree is less than 3, we must have $c_1(\sigma^2 P_1) = 0$, and we get $\zeta^2 y_1$ solving the (linear with respect to

y) equation $c_1(x_1, y) = 0$. Once we know $\sigma^2 P_1$, we obtain v_1 solving the system :

$$\begin{cases} v_1(\sigma^2 P_1) = 0 \text{ up to order n} \\ \frac{\text{Res}_y(v_1, c_1)}{(x-x_1)^{n-1}} = \lambda \frac{u_1}{(x-x_1)^n} \end{cases}$$

with $n-1$ the multiplicity of $\sigma^2 P_1$ on c_1, and λ a non zero constant making v_1 monic.

Finally, $v_2 = v_1$ and we get u_2 and w_2 from (1).

3) if v_0 has no linear factor

a) if $a_{30} = a_{11} = 0$, $v_0 = a_{00} + a_{10}x + a_{20}x^2 + a_{01}y$, thus v_0 has to meet C at a sixth point P_6 we get from (1) : we must have $u_1 = x - x_6$ and $w_1 = y - y_6$ on the one hand and $v_1 = u_1$ on the other. Thus $D_1 = P_6$, $D_2 = \sigma P_6 + \sigma^2 P_6$ and we get D_2 explicitely this way.

b) else the resultant in lemma 2.4 is non zero, and it is the determinant of the linear (since the interpolating functions are linear in y) system :

$$\text{Res}_y(v_0, v_1) = \lambda u_1.$$

Note that if v_0 has no term x^3, it suffices to look for v_1 among the polynomials $b_{00}+b_{10}x+b_{20}x^2+b_{01}y$, and the system has four equations in this case. Finally we get $u_1,\ u_2,\ w_1,\ w_2$ with the help of formulae (1).

■

We can now justify the last step :

Lemma 2.5 *Suppose we know also D_2 and E_1, or $\Phi(D_1)$, $\Phi(D_2)$ and E_1 explicitly; then we can compute $\Phi(D_3)$, $D_3 = D_2 + E_1$, or $\Phi(D_4)$ and $\Phi(D_5)$.*

Proof: Suppose we know D_2 explicitly ; we just have to solve the following 5×5 linear system :

$$v_3(P_i) = 0, \quad P_i \in \text{Supp}(D_3)$$

the same way as to obtain $\Phi(D_0)$ from D_0 ; if $D_3 \notin \text{Div}_0^{*,5}(C)$, we get $\Phi(D_4)$ and $\Phi(D_5)$ directly.

Anyway, if $E_1 = Q_1 + \ldots + Q_k$, we have :

$$u_3 = u_2 \prod_{i=1}^{k} (x - x_{Q_i}), \qquad w_3 = w_2 \prod_{i=1}^{k} (y - y_{Q_i}).$$

In the second case, we have to solve :

$$\begin{cases} v_3(Q_i) = 0 \quad 1 \le i \le k \\ \text{Res}_y(v_2, v_3) = \lambda u_2 \end{cases}$$

λ chosen to obtain v_3 monic.

If $v_2(Q_i) \neq 0$, this system is invertible and we solve it. Else we get two cases :

$$v_2(Q_1) = 0 \Rightarrow u_2(x_{Q_1}) = 0 \quad \text{or} \quad u_1(x_{Q_1}) = 0.$$

In the first case, we add the equation $v_3(Q_i) = 0$ *up to order* 2, and we divide the two parts of the second equation by $x - x_{Q_1}$:

$$\begin{cases} v_3(Q_1) = 0 \quad \text{up to order 2} \\ v_3(Q_i) = 0 \quad 2 \leq i \leq k \\ \frac{\text{Res}_y(v_2, v_3)}{x - x_{Q_1}} = \lambda \frac{u_2}{x - x_{Q_1}} \end{cases}$$

In the second case, we get rid of equation $v_3(Q_1) = 0$, and we multiply the second part of the second equation by $(x - x_{Q_1})$:

$$\begin{cases} v_3(Q_i) = 0 \quad 2 \leq i \leq k \\ \text{Res}_y(v_2, v_3) = \lambda u_2 (x - x_{Q_1}) \end{cases}$$

following this process with $u_1 := \frac{u_1}{x - x_{Q_1}}$ until u_1 has no more zero at one of the Q_i. ■

Example : Let $p = 31$,

$$P_1 := [23, 27],\ P_2 := [7, 18],\ P_3 := [14, 28]$$

and $C : y^3 = x^5 - 1$. The reduction of the following divisor

$$D = 2(P_1 + P_2 + P_3)$$

is

$$D' = Q_1 + Q_2 + Q_3 + Q_4,$$

where

$$Q_1 = [\alpha, 21\alpha^3 + \alpha^2 + 11\alpha + 13],$$
$$Q_2 = [2\alpha^3 + \alpha^2 + 22\alpha + 11, 28\alpha^3 + 8\alpha^2 + 10\alpha + 16]$$
$$Q_3 = [3\alpha^3 + 6\alpha^2 + 10\alpha + 4, 7\alpha^3 + 20\alpha^2 + 10\alpha + 6]$$
$$Q_4 = [26\alpha^3 + 24\alpha^2 + 29\alpha + 7, 6\alpha^3 + 2\alpha^2 + 23],$$

and where α is a root of

$$x^4 + 9x^3 + 23x^2 + 18x + 25.$$

References

[Be-Ev-W] Berndt B. C., Evans R.J.,Williams K.S. Gauss and Jacobi Sums. Canadian Math. Society, Series of Monographs and Advanced Texts, Vol. 21, Wiley-Interscience Publication, (1997).

[Buh-Kob] Buhler, J., Koblitz, N., *Lattices basis reduction, Jacobi sums and hyperelliptic cryptosystems.* Bull. Australian Math. Soc., Vol. 58, pp.147-154,(1998).

[Coh] Cohen, H. A Course in Computational Number Theory. Graduate Texts in Math., vol. 138, Springer, New-York,(1993).

[Che] Cherdieu, J.-P. *Remarks on the Zeta function of some diagonal hyperelliptic curves.* to appear in Journal of Pure and Applied Algebra.

[Est1] Estrada Sarlabous. J, *On the JacobianVarieties of Picard Curves Defined over Fields of Characteristic p,.* Math. Nachr. 152 (1991), 329-340.

[Est2] Estrada Sarlabous. J., *A finiteness theorem for Picard curves with good reduction,.* Appendix I of *Ball models and some Hilbert Problems* by R.-P. Holzapfel. Lectures in Mathematics. Birkhäuser-Verlag, (1995).

[EstReiPi] Estrada Sarlabous. J, Reinaldo Barreiro. E, Piñeiro Barceló. J.A., *On the JacobianVarieties of Picard curves: explicit Addition Law and Algebraic Structure,* Math. Nachrichten 208 (1999), pp. 149-166

[EstReiChe] Estrada-Sarlabous, J., Reinaldo-Barreiro, E., Cherdieu, J-P. *Efficient Reduction on the JacobianVariety of Picard Curves* in: Coding Theory, Cryptography and Related Areas. *Proceedings of the ICCC-98*, J. Buchmann, T. Hohold, H. Stichtenoth, H. Tapia-Recillas (eds.), pp.13-28, Springer-Verlag, 2000.

[ECRH] Estrada Sarlabous, J., Cherdieu, J.-P., Reinaldo, E., Holzapfel, R.-P. *The Emergence of Picard Jacobians in Cryptography*, Proceedings IV ITLA, 2001, pp. 266-275 , ISBN: 959-7056-13-5.

[Har] Hartshorne, R., Algebraic geometry Springer Verlag GTM 52

[Lang] Lang S., Algebraic Number Theory, Graduate Texts in Math., vol. 110, Springer, New-York, (1991).

[Lidl-Nied] Lidl, R., Niederreiter H., Finite fields. Volume 20 of Encyclopedia of Mathematics and its applications. Cambridge University Press, (1983).

[Mum] Mumford, D., Tata Lectures on Theta II. Jacobian theta functions and differential equations. Progress in Math, Vol.42, Birkhäuser Verlag (1984).

[Small] Small, C. Arithmetic of finite fields, Pure and applied mathematics 148, Marcel Dekker, New York (1991)

[Tate] Tate, J.*Endomorphisms of Abelian varieties over finite fields,* Invent. Math. 2, pp.134-144 (1966).

[Weil] Weil A., *Jacobi sums as "Grössencharaktere",* Bull. Amer. Math. Soc., VI. 73, pp.487-495; =œuvres Scientifiques[1952d], vol. II, pp. 63-71.

[Yui] Yui, N. *Norms of algebraic numbers.* Journal of Number Theory, vol. 47 pp.106-129 (1994).