ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Pure and Applied Algebra 190 (2004) 31–43

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Remarks on the zeta function of some diagonal hyperelliptic curves[☆]

Jean-Pierre Cherdieu

Département de Mathématiques Informatique Equipe, Applications de l'Algébre et de l'Arithmétique, Université des Antilles et de la Guyane, Campus de Fouillole, Pointe-Pitre, Cedex F97159, France

Received 26 January 2000; received in revised form 16 March 2003
Communicated by M.-F. Roy

Abstract

We compute the Jacobi sums and the zeta functions associated to the family of diagonal curves defined over $\mathbb{F}_p$ by $y^2 = \gamma x^5 + \delta$ (with $\gamma\delta \neq 0$), then we prove that their Jacobians are simple. We discuss about the hardness of the associated discrete logarithm problem with respect to known attacks and we show that our family is suitable for cryptographic purpose.

MSC: 11T4; 11T71

1. Introduction

Many public key protocols use the hardness of the discrete logarithm problem on well chosen abelian groups. As subexponential algorithms exist for $\mathbb{Z}/N\mathbb{Z}$ and for the additive group of a finite field, we need some other groups. A good candidate is the Jacobian variety $J(X)$ of a curve X, since it is an abelian group with group law given by the addition in the divisor class group. Such secure Diffie–Hellman-type cryptosystem have been constructed for some hyperelliptic curves [8] and also for elliptic curves [7]. But $J(X)$ is suitable only if the cardinality of one of its cyclic subgroups is a large prime ($\sim 2^{180}$).

Let p be a prime. Let us denote by $Z(X,T)$ the Zeta function of the curve X defined over $\mathbb{F}_p$. Set $P(X,T) = Z(X,T)(1-T)(1-pT)$, we know that

$$|J(X)| = P(X,1).$$

[☆] This work was partially supported by the Conseil Régional de la Guadeloupe.

E-mail address: jean-pierre.cherdieu@univ-ag.fr (J.P. Cherdieu).

0022-4049/$ - see front matter © 2003 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2003.10.017

Using the Jacobi sums, Koblitz gives in [8] conditions for the irreducibility of the numerator of the zeta function in the case of hyperelliptic curves family $y^2 + y = x^d$ over $\mathbb{F}_p$ where $d = 2g + 1$ is not divisible by p.

In the case of diagonal curves a precise computation of associated Jacobi sums can be performed. Hence, motivated by the Koblitz's result, we try to obtain similar explicit necessary conditions for the irreducibility of the numerator of the Zeta function corresponding to the special families of diagonal curves of small genus.

More precisely if e and f are two positive integers the special families of curves $X = D(e, f; \gamma, \delta)$ with affine equation defined over $k = \mathbb{F}_p$ given by

$$y^e = \gamma x^f + \delta,$$

where

$$2 \leqslant e \leqslant f, \;\; \gcd(p, e) = \gcd(p, f) = 1, \;\; \gamma \in k^\times = k - \{0\}, \;\; \delta \in k^\times$$

is called a diagonal curve.

Using the result of Honda [6, Theorem 2, p. 193], we show that the Jacobian is simple. We also compute explicitly $P(D, T)$. The key step is the computation of some Jacobi sums. All the general results on these sums, the diagonal curves and their related Zeta function are given in Section 2. More precise results on the Jacobi sums, for the hyperelliptic diagonal curves, are in Section 3. In Section 4 we give some numerical examples with large numbers which could be suitable for cryptosystems. We terminate this paper by discussing on the construction of a hyperelliptic cryptosystem, and also testing its resistance against some known attacks.

2. Diagonal curves

2.1. The $\mathfrak{G}$ group

Let e and f be two positive integers, and let

$$d = \gcd\ (e, f), \;\; m = \operatorname{lcm}\ (e, f).$$

We set $\zeta = \zeta_m = e^{2i\pi/m}$, and denote by $K = \mathbb{Q}(\zeta)$ the mth cyclotomic field. For any positive integer n dividing m, we will use the letter μ_n to denote the group of nth roots of unity in K. We also set

$$\mathfrak{G} = \mu_f \times \mu_e = \{g = (\xi, \eta) \mid \xi \in \mu_f, \eta \in \mu_e\}$$

and

$$\hat{\mathfrak{G}} = \mathbb{Z}/f\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z} = \{\mathbf{a} = (a, b) \mid a \in \mathbb{Z}/f\mathbb{Z}, \;\; b \in \mathbb{Z}/e\mathbb{Z}\}.$$

The main properties of these groups can be found in [16,9]. The map

$$\hat{\mathfrak{G}} \times \mathfrak{G} \to K$$

defined for any $g \in \mathfrak{G}$ and $\mathbf{a} \in \hat{\mathfrak{G}}$ by

$$< g, \mathbf{a} > = \xi^a \eta^b$$

allows us to identify $\hat{\mathfrak{G}}$ with the group of the characters of $\mathfrak{G}$.

On the other hand, we introduce the following subsets of $\hat{\mathfrak{S}}$:

- $\mathfrak{A}$ the image of $(a,b) \in \mathbb{Z}^2$ such that
$$1 \leqslant a \leqslant f-1,\ 1 \leqslant b \leqslant e-1,\ \frac{a}{f}+\frac{b}{e} \not\equiv 0\,(\mathrm{mod}\,1);$$
- $\mathfrak{B}$ the image of $(a,b) \in \mathbb{Z}^2$ such that
$$1 \leqslant a \leqslant f-1,\ 1 \leqslant b \leqslant e-1,\ \frac{a}{f}+\frac{b}{e} \equiv 0\,(\mathrm{mod}\,1);$$
- $\mathfrak{C}$ the image of $(a,b) \in \mathbb{Z}^2$ such that
$$(a,0)(a \neq 0), \quad (0,b)(b \neq 0).$$

We thus obtain a partition of $\hat{\mathfrak{S}}$

(1) $\hat{\mathfrak{S}} = \mathfrak{A} \sqcup \mathfrak{B} \sqcup \mathfrak{C} \sqcup \{0\}$, and
(2) $|\mathfrak{B}| = d-1$.

From which we deduce,

Corollary 2.1. *We have*
$$|\mathfrak{A}| = (e-1)(f-1)-(d-1).$$

Proof. Let $\mathfrak{B}_0$ be the set of $(x,y) \in \mathbb{Z}^2$ such that
$$1 \leqslant x \leqslant d-1,\ 1 \leqslant y \leqslant d-1,\ x+y \equiv 0\,(\mathrm{mod}\,d).$$

Suppose that $e = de'$ and $f = df'$ and consider the injective map $f : \mathfrak{B}_0 \to \hat{\mathfrak{S}}$ defined by $f(x,y) = (xf', ye')$. Then,
$$\frac{xf'}{f}+\frac{ye'}{e} = \frac{x}{d}+\frac{y}{d} \equiv 0\,(\mathrm{mod}\,1),$$
hence, f maps $\mathfrak{B}_0$ into $\mathfrak{B}$. If $(a,b) \in \mathfrak{B}$, we have
$$0 < \frac{1}{f}+\frac{1}{e} \leqslant \frac{a}{f}+\frac{b}{e} \leqslant \frac{f-1}{f}+\frac{e-1}{e} < 2$$
then,
$$\frac{a}{f}+\frac{b}{e} = 1.$$

The first assertion implies $ae+bf = ef$, so $f \mid ae$, and since $\gcd(f',e') = 1$, we have $f' \mid a$. Thus, $a = xf'$. In the same way, one gets $b = ye'$, hence, f is surjective from $\mathfrak{B}_0$ onto $\mathfrak{B}$. Finally, we have
$$|\mathfrak{B}| = |\mathfrak{B}_0| = d-1. \qquad \square$$

2.2. Jacobi sums

Let $k=\mathbb{F}_q$ be a finite field with q elements and denote by $\mathbb{X}=\mathbb{X}(k^\times)$ its group of multiplicative characters. The identity element of that group will be denoted by ε. It is the trivial multiplicative character and satisfies $\varepsilon(x)=1$ for all $x\in k^\times$. Following the notation introduced by Weil [16], we set

Definition 2.1. The Jacobi sum associated to the couple $(\chi,\lambda)\in\mathbb{X}^2$ is

$$j(\chi,\lambda)=-\sum_{x+y=1}\chi(x)\lambda(y),$$

where x and y belong to $k^\times$.

Remark. If $(\chi,\lambda)\in\hat{\mathfrak{S}}$, the sum $j(\chi,\lambda)$ is in the ring $\mathbb{Z}[\zeta]$ of integers of $\mathbb{Q}(\zeta)$.

Let e, f and m be as in the previous section, and suppose that

$$m\mid q-1.$$

Let ψ be an element of $\mathbb{X}$ of order m. The homomorphism

$$(a,b)\mapsto(\psi^a,\psi^b)$$

from $\hat{\mathfrak{S}}$ into $\mathbb{X}\times\mathbb{X}$ is injective. In order to simplify the notations, we will denote its image by the same notation, hence we can write

$$\hat{\mathfrak{S}}=\hat{\mathfrak{S}}(k^\times)=\{(\chi,\lambda)\in\mathbb{X}(k^\times)\times\mathbb{X}(k^\times)\mid\chi^f=\varepsilon,\quad\lambda^e=\varepsilon\}.$$

Lemma 2.1. *Let k_s be the extension of degree s of k, and let N_s be the norm of the extension k_s/k. If $q\equiv 1\bmod m$, then the map β*

$$(\chi,\lambda)\mapsto(\chi\circ N_s,\lambda\circ N_s)$$

from $\hat{\mathfrak{S}}(k^\times)$ to $\hat{\mathfrak{S}}(k_s^\times)$ is an isomorphism. Furthermore, if $\chi\neq\varepsilon,\lambda\neq\varepsilon$ and $\lambda\chi\neq\varepsilon$, then we have the Hasse–Davenport relation [10, Theorem 5.26, p. 210],

$$j(\chi\circ N_s,\lambda\circ N_s)=j(\chi,\lambda)^s.$$

Remark. Let us note that if the classical $(-1)^{s-1}$ does not appear in this formula, it comes from the choice of Weil to define the Jacobi's sum with a minus sign.

Proof. The crucial point is to prove that the map β is onto. For that let us recall that a multiplicative character χ' of k_s is of the form $\chi\circ N_s$ if and only if $\chi'^{q-1}=\varepsilon$. For (χ',λ') in $\hat{\mathfrak{S}}(k_s^\times)$ this condition is verified because $f\mid m=\operatorname{lcm}(e,f)$, and $m\mid q-1$. □

Assume now that $q=p$ is a prime number and that $p\equiv 1\bmod m$. If we note $\mathfrak{D}=\mathbb{Z}[\zeta_m]$, then the ideal $p\mathfrak{D}$ completely splits in $\mathfrak{D}$. Let $\mathfrak{p}$ be a fixed prime ideal of $\mathfrak{D}$ lying over p. We have $N(\mathfrak{p})=p$ and $\mathfrak{D}/\mathfrak{p}$ is isomorphic to $\mathbb{F}_p$. Let $\psi_{\mathfrak{p}}$ be the mth power residue symbol modulo $\mathfrak{p}$, which means that $\psi_{\mathfrak{p}}$ is the multiplicative character of order m such that ([16, p. 488] (or 64))

$$\psi_{\mathfrak{p}}(x) = \left(\frac{x}{\mathfrak{p}}\right)_m \equiv x^{(p-1)/m} \,(\mathrm{mod}\, \mathfrak{p}).$$

For all integers a and b we set

$$j_{\mathfrak{p}}(\psi_{\mathfrak{p}}^a, \psi_{\mathfrak{p}}^b) = -\sum_{\substack{x,y \in (\mathfrak{O}/\mathfrak{p})^\times \\ x+y=1}} \psi_{\mathfrak{p}}(x)^a \psi_{\mathfrak{p}}(y)^b.$$

2.3. Zeta function of the diagonal curves

Let us first recall the result of Aubry and Perret [2, Theorem 2.1, p. 2].

Theorem 2.1. *Let $\tilde{X}$ be the normalisation of X, and v the normalisation map from $\tilde{X}$ to X. Let d_P be the degree of the extension of the residue field of the point P over $\mathbb{F}_q$. If S is the (finite) set of singular points of X, then*

$$Z(X,T) = \frac{P(X,T)}{(1-T)(1-qT)},$$

where

$$P(X,T) = P(\tilde{X},T) \prod_{P \in S} \left(\frac{\prod_{Q \in v^{-1}(P)} (1 - T^{d_Q})}{1 - T^{d_P}} \right)$$

and where $P(\tilde{X},T)$ is the numerator of the zeta function $Z(\tilde{X},T)$ of $\tilde{X}$.

For any nonsingular irreducible curve V, of genus $g = g(V)$, defined over $k = \mathbb{F}_q$, we denote by $Z(V,T)$ the zeta function of V. We set

$$P(V,T) = Z(V,T)(1-T)(1-qT)$$

with

$$\deg P(V,T) = 2g.$$

Let $Y = D(e, f; \gamma, \delta)$ be the affine curve defined over k by

$$y^e = \gamma x^f + \delta,$$

where

$$2 \leqslant e \leqslant f, \;\; \gcd(q,e) = \gcd(q,f) = 1, \;\; \gamma \in k^\times, \;\; \delta \in k^\times.$$

This affine curve is clearly smooth. We assume that

$$m = \mathrm{lcm}(e,f) \,|\, q-1$$

and for any $(\chi, \lambda) \in \hat{\mathfrak{S}}$, we set

$$c(\chi,\lambda) = (\chi\lambda)(\delta)\chi(-\gamma^{-1}) = \lambda(\delta)\chi(-\delta\gamma^{-1}),$$

$$\alpha(\chi,\lambda) = c(\chi,\lambda) j(\chi,\lambda).$$

Theorem 2.2. *Let Y be the projective nonsingular model of X. Then*

$$P(Y,T)=\prod_{(\chi,\lambda)\in\mathfrak{u}}(1-\alpha(\chi,\lambda)T).$$

In particular,

$$2g(Y)=|\mathfrak{A}|=(e-1)(f-1)-(d-1).$$

Proof. Let $N(k)$ (resp. $N(k_s)$) be the number of points of $Y(k)$ (resp. of $Y(k_s)$), where k_s is the extension of k of degree s. Since Y is given by a diagonal equation, we may use the method of Weil [15, p. 103], and we get

$$N(Y)=\sum_{(\chi,\lambda)\in\hat{\mathfrak{S}}}(\chi\lambda)(\delta)\chi(-\gamma^{-1})\sum_{u+v=1}\chi(u)\lambda(v).$$

Hence

$$N(Y)=-\sum_{(\chi,\lambda)\in\hat{\mathfrak{S}}}c(\chi,\lambda)j(\chi,\lambda)=-\sum_{(\chi,\lambda)\in\hat{\mathfrak{S}}}\alpha(\chi,\lambda).$$

Using the Davenport–Hasse relation, we obtain

$$\begin{aligned}N_s(Y)&=-\sum_{(\chi,\lambda)\in\hat{\mathfrak{S}}}\alpha(\chi,\lambda)^s\\&=-\sum_{(\chi,\lambda)\in\{0\}}\alpha(\chi,\lambda)^s-\sum_{(\chi,\lambda)\in\mathfrak{B}}\alpha(\chi,\lambda)^s-\sum_{(\chi,\lambda)\in\mathfrak{C}}\alpha(\chi,\lambda)^s-\sum_{(\chi,\lambda)\in\mathfrak{A}}\alpha(\chi,\lambda)^s.\end{aligned}$$

Observe that for $d>1$, the elements of $\mathfrak{B}$ are those of the form (χ,χ^{-1}), where χ is a nontrivial character of order d. Then

$$\begin{aligned}\sum_{(\chi,\lambda)\in\mathfrak{B}}\alpha(\chi,\lambda)^s&=\sum_{\chi}\chi(\delta^{-1})^s\chi(-\delta\gamma^{-1})^s\chi(-1)^s\\&=\sum_{\chi}\chi(\gamma^{-1})^s=\sum_{\chi}\chi(\gamma)^s.\end{aligned}$$

So, we have

$$N_s(Y)=q^s+1-\sum_{(\chi,\lambda)\in\mathfrak{A}}\alpha(\chi,\lambda)^s-\sum_{\chi^d=1}\chi(\gamma)^s$$

and by a standard computation

$$P(Y,T)=\prod_{(\chi,\lambda)\in\mathfrak{A}}(1-\alpha(\chi,\lambda)T)\prod_{\chi^d=1}(1-\chi(\gamma)T).$$

Using the result of Aubry and Perret we obtain the desired result. □

3. The hyperelliptic curves $D(2, 5; \gamma, \delta)$

Assume $k = \mathbb{F}_p$ is such that $char(k) \neq 2$. The curve $D(2, 2g+1; \gamma, \delta)$, defined over k, and given by

$$y^2 = \gamma x^{2g+1} + \delta$$

is of genus g according to Theorem 2.2.

3.1. *The associated Jacobi sums*

From now, we will only be concerned by the projective curve of genus 2 with affine equation

$$y^2 = \gamma x^5 + \delta.$$

This curve is hyperelliptic [14]. Here, $m = 10$, $\zeta = \zeta_{10} = \exp(2i\pi/10)$, and we assume $p \equiv 1 (\mathrm{mod}\, 10)$. The smooth projective model of $D(2, 5; \gamma, \delta)$ has only one point at the infinity and its number of points is given by

$$N_p = p + 1 - \alpha(\eta, \chi) - \alpha(\eta, \chi^2) - \alpha(\eta, \chi^3) - \alpha(\eta, \chi^4),$$

where η is the Legendre character, and χ is a character of order 5. As in Section 2, we have

$$c(\eta, \chi) = (\eta\chi)(\delta)\chi(-\gamma^{-1}) = \eta(\delta)\chi(-\delta\gamma^{-1}),$$

$$\alpha(\eta, \chi) = c(\eta, \chi) j(\eta, \chi).$$

Lemma 3.1. *Let* $\varphi = \zeta + \bar{\zeta} = \frac{1+\sqrt{5}}{2}$, *then* $\{1, \zeta, \varphi, \varphi\zeta\}$ *is a basis of the* $\mathbb{Z}$ *module* $\mathbb{Z}[\zeta]$.

Proof. We just check that

$$\begin{aligned} \zeta^2 &= -1 + \varphi\zeta, & \zeta^6 &= -\zeta, \\ \zeta^3 &= -\varphi + \varphi\zeta, & \zeta^7 &= 1 - \varphi\zeta, \\ \zeta^4 &= \zeta - \varphi, & \zeta^8 &= \varphi - \varphi\zeta, \\ \zeta^5 &= -1, & \zeta^9 &= -\zeta + \varphi. \qquad \Box \end{aligned}$$

We denote by G the Galois group of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Then,

$$G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/10\mathbb{Z})^\times = \{1, 3, -3, -1\} \simeq \mathbb{Z}/4\mathbb{Z}.$$

We define an isomorphism $\tau : (\mathbb{Z}/10\mathbb{Z})^\times \to G$, by

$$\tau(n).\zeta = \zeta^n, \quad n \in (\mathbb{Z}/10\mathbb{Z})^\times.$$

We set $\sigma = \tau(3)$, hence

$$G = \{1, \sigma, \sigma^2, \sigma^3\}.$$

In order to introduce the following result, notice that the two elements

$$\mathrm{i}\sqrt{5+2\sqrt{5}} = \zeta - \bar{\zeta} + \zeta^2 - \overline{\zeta^2}, \quad \mathrm{i}\sqrt{5-2\sqrt{5}} = -\zeta + \bar{\zeta} + \zeta^2 - \overline{\zeta^2}.$$

form a basis of K over $\mathbb{Q}(\varphi)$.

Theorem 3.1. (Cf. [Berndt et al. [3, Theorem 3.7.2, p. 125]]). *Let $p \equiv 1 (\mathrm{mod}\, 10)$, and ψ a character of order 10. Then,*

$$\eta(-1)K(\psi) = a + b\sqrt{5} + \mathrm{i}c\sqrt{5+2\sqrt{5}} + \mathrm{i}d\sqrt{5-2\sqrt{5}},$$

where $K(\psi) = \psi(4)j(\psi,\psi) = \psi(4)j(\psi)$, and

(1) $a \equiv -1 \,(\mathrm{mod}\, 5)$,
(2) $a^2 + 5b^2 + 5c^2 + 5d^2 = p$,
(3) $ab = d^2 - c^2 - cd$.

The solutions $\pm\{a,b,c,d\}$ are "essentially unique" in the sense that the only other solutions in integers are the conjugate solutions $\pm\{a,b,-c,-d\}$ and $\pm\{a,-b,d,-c\}$.

Theorem 3.2. (Cf. [Berndt et al. [3, Theorem 3.7.3, p. 127]]). *If g is a primitive root mod p, and let $h = g(p-1)/10$. Define $(|a|,|b|,|c|,|d|)$ by the previous theorem, then they are uniquely determined by the equations in the previous theorem together with the congruences,*

(1) $a + b(2h^2 - 2h^3 + 1) + c(h + h^2 + h^3 + h^4) + d(h^2 + h^3 - h - h^4) \equiv 0 \bmod p$
(2) $5b^2 - a^2 \equiv (2h^2 - 2h^3 + 1)(c^2 - d^2 - 4cd) \bmod p$

Examples.

(1) If $p = 11$, with $g = 2$, and
$$j(\eta,\psi) = -1 + \sqrt{5} + \mathrm{i}\sqrt{5+2\sqrt{5}} = -3 + 2\zeta + 2\varphi\zeta.$$
(2) If $p = 31$, with $g = 3$, and
$$j(\eta,\psi) = -1 + \sqrt{5} + 2\mathrm{i}\sqrt{5-2\sqrt{5}} - \mathrm{i}\sqrt{5-2\sqrt{5}} = 3 + 2\varphi - 6\zeta - 2\varphi\zeta,$$
(3) If $p = 41$, with $g = 6$, and
$$j(\eta,\psi) = -4 - \sqrt{5} - 2\mathrm{i}\sqrt{5-2\sqrt{5}} = -1 - 2\varphi + 4\zeta - 4\varphi\zeta.$$
(4) If $p = 61$, with $g = 2$, and
$$j(\eta,\psi) = 4 + \sqrt{5} + 2\mathrm{i}\sqrt{5+2\sqrt{5}} - 2\mathrm{i}\sqrt{5-2\sqrt{5}} = 3 - 2\varphi + 8\zeta.$$

Proposition 3.1. *Let $p \equiv 1\,(\mathrm{mod}\ 10), \eta$ the Legendre character, and ψ a character of order 5. If we set*

$$A = a - b - c - d, \; B = 2b - 2c, \; C = 2c - 2d, \; D = 2c + 2d,$$

then

$$j(\eta,\psi)=A+B\varphi+C\zeta+D\varphi\zeta,$$

where

(1) $A+\frac{B}{2}+\frac{C}{4}+\frac{3D}{4}\equiv -1\,(\text{mod } 5)$,
(2) $A^2+AB+3B^2/2+AC/2+3BC/2+C^2+3AD/2+2BD+CD+3D^2/2=p$,
(3) $AB/2+B^2/4+AC/4+BC/4-C^2/8+AD/4+BD/2+CD/2+D^2/4=0$.

3.2. *Zeta function of $D(2,5;\gamma,\delta)$*

If

$$Z(X,T)=\frac{P(X,T)}{(1-T)(1-qT)}$$

is the Zeta function of the curve X, we obtain, using the results of the previous section, and a standard computation:

$$P(X,T)=(1-\alpha(\eta,\chi)T)(1-\alpha(\eta,\chi^2)T)(1-\alpha(\eta,\bar{\chi})T)(1-\alpha(\eta,\bar{\chi}^2)T),$$

i.e.,

$$P(X,T)=\prod_{\lambda\in G}(1-\alpha(\eta,\chi)^{\lambda}T).$$

Recall that $\alpha(\eta,\chi)^{\lambda}\in\mathbb{Z}[\zeta]$. Hence, one of the three following cases may occur:

(1) $\alpha(\eta,\chi)\in\mathbb{Z}$. Then $P(X,T)$ is a product of four factors of degree 1.
(2) $\alpha(\eta,\chi)\in\mathbb{Z}[\varphi]-\mathbb{Z}$. In this case $P(X,T)$ is the square of a quadratic irreducible polynomial in $\mathbb{Z}[T]$.
(3) $\alpha(\eta,\chi)\in\mathbb{Z}[\zeta]-\mathbb{Z}[\varphi]$. Then $P(X,T)$ is irreducible.
    In order to obtain a nice result , let us recall the following result of Yui [17, Theorem 3.2, p. 390].

Theorem 3.3. *If $J(X)$ is simple and ordinary then $P(X,T)$ is $\mathbb{Q}$-irreducible.*

A direct computation of the Hasse–Witt matrix of X shows that $J(X)$ is ordinary.

As $p\equiv 1$ mod 10, then the least natural number f such that $p^f\equiv 1$ mod 5 is $f=1$, hence we can apply the result of Honda [6, Theorem 2, p. 193] which implies that the Jacobian is simple. Note that

- the decomposition field of p in $\mathbb{Q}(\zeta_5)$ is precisely $\mathbb{Q}(\zeta_5)$, which is totally imaginary.
- The endomorphism algebra of $J(X)$ coincides with its center.
- All the ramified prime ideals of the endomorphism algebra of $J(X)$ divide p, moreover since $\mathbb{Q}(\zeta_5)$ is totally imaginary, no infinite place is ramified in the endomorphism algebra of $J(X)$.
- The characteristic polynomial of the Frobenius endomorphism of $J(X)$ has p-adic roots with p-adic values equal to 0 or 1, since $J(X)$ is ordinary.

- All the invariants of the endomorphism algebra of $J(X)$ at its ramified prime ideals are integers,

Hence, the endomorphism algebra of $J(X)$, its center, the decomposition field of p and $\mathbb{Q}(\zeta_5)$ are all equal and $J(X)$ is a simple abelian variety. So we have,

Theorem 3.4. *The polynomial $P(X,T)$ is $\mathbb{Q}$-irreducible, and if*

$$j(\eta,\psi) = A + B\varphi + C\zeta + D\varphi\zeta,$$

then

$$\begin{aligned} P(X,T) = p^2T^4 &+ (-4A-2B-C-3D)pT^3 \\ &+(-10B^2-10BC-5C^2-10BD-5CD-5D^2+6p)T^2 \\ &+(-4A-2B-C-3D)T+1 \end{aligned}$$

and

$$\begin{aligned} P(X,1) = 1-4A-2B-10B^2-C-10BC-5C^2-3D-10BD-5CD-5D^2 \\ +(6-4A-2B-C-3D)p+p^2. \end{aligned}$$

Proof. It is an application of the above theorem. □

Example. Let us consider $X = D(2,5;1,1)$ its equation is

$$y^2 = x^5 + 1,$$

where η is the Legendre character and ψ a character of order 5. So we have

$$\psi(-\delta\gamma^{-1}) = 1,\ \ \eta(1) = 1.$$

In particular

p	$P(X,T)$	$P(X,1) = \lvert\mathfrak{J}(X)\rvert$
11	$121T^4 - 44T^3 + 6T^2 - 4T + 1$	$80 = 2^4.5$
31	$961T^4 - 124T^3 + 46T^2 - 4T + 1$	$880 = 2^4.5.11$
41	$1681T^4 + 656T^3 + 126T^2 + 16T + 1$	$2480 = 2^4.5.31$
61	$3721T^4 + 976T^3 + 166T^2 + 16T + 1$	$4880 = 2^4.5.61$
71	$5041T^4 - 284T^3 + 126T^2 - 4T + 1$	$4880 = 2^4.5.61$

4. Some more examples

A condition to construct an efficient cryptosystem which is secure against all known attacks is that "the number of points of the Jacobian must be divisible by a large prime" [4, p. 148]. Here are some suitable examples. We denote by $lng\ p$ the size of the prime p, $Ing(fJ)$ the number of digit of the greatest prime factor of $\#J(X)$, and a, b, c, d are, as previously, the solutions of the system of Theorem 2.4.1. For example, we have found

$$p = 47430895079011576853874359579591 \quad lng(p) = 32,$$

$$a = -1, b = 3079964125733011, c = -65872481, d = 15478794,$$

$$\#J(X) = 2^4 12285061.513524984252777671$$

$$.222876235122895735521824705738542031 21,$$

$$Ing(fJ) = 38,$$

$$p = 4217726215989637430569115140062500822778 91 \quad lng(p) = 43,$$

$$a = -1, b = -918447191295137825471, c = -658724581, d = 29985478776,$$

$$\#J(X) = 2^4.104739002006047351$$

$$.10615204277019918159103541977137312669645346704161379714595164312551,$$

$$lng(fJ) = 68.$$

5. Application

5.1. An hyperelliptic cryptosystem

Throughout this section we suppose that p is a large prime number as in the previous section.

Our family of diagonal hyperelliptic curves is suitable for a cryptosystem. In [8,5] Koblitz and Cantor give an efficient algorithm for the addition of divisors in the Jacobian of hyperelliptic curves. This algorithm may be used to implement the group law of the Jacobian of genus two diagonal curves. Seyen [13] gives a simplification of the reduction algorithm which is preferable for small genus hyperelliptic curves.

5.2. Resistance against some classical attacks

(1) *The smooth-divisor attack*: The smooth-divisor attack of Adleman et al. [1] for hyperelliptic curves over $\mathbb{F}_p$ will not be effective, because it supposes that the genus verifies

$$2g + 1 > ln(p).$$

But our genus is 2, and we have supposed that p is large enough.

(2) *Baby-step giant-step and Pohligh–Hellman attacks*: The choice of a sufficiently large p with also a large $lng(fJ)$ preserve us from the baby-step giant-step attack [12], and also from the Pohlig–Hellman attack, because running times of both methods are of order $\sqrt{lng(fJ)}$.

(3) *The speeding up factor*: The order of the group of automorphisms is small, hence the speeding up factor for the discrete log computation proposed in [11] is not substantial.

6. Open problem and concluding remarks

The Jacobi sums associated to the special families of diagonal curves of genus two is explicitly computed.

Under some conditions the special family of diagonal curves studied in this paper happens to have a $\mathbb{Q}$-irreducible Zeta polynomial and the explicit computation of the coefficients of Zeta polynomial is reduced to the decomposition of a prime number as (weighted) sum of four squares. For large prime numbers, this problem is still open, there is not known algorithm to find the integers $\{a,b,c,d\}$ of Theorem 3.1. Our method only allows us to find numbers verifying these conditions with $p \equiv 1 (\mathrm{mod}\, 10)$.

References

[1] L.M. Adleman, J. DeMarais, M. Huang, A subex-ponential algorithm for discrete logarithm over the rational subgroup of the Jacobians of large hyperelliptic curves over finite fields, Proceedings of ANTS1, Lecture Notes in Computer Science, Vol. 877, Springer, Berlin, 1994, pp. 28–40.

[2] Y. Aubry, M. Perret, A Weil Theorem for singular curves, in: Arithmetic, Geometry and Coding Theory -4, Marseille-Luminy, De Gruyter, Berlin, 1996, pp. 1–7.

[3] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums. Canadian Mathematical Society, Series of Monographs and Advanced Texts, Vol. 21, Wiley-Interscience Publication, New York, 1997.

[4] J. Buhler, N. Koblitz, Lattices basis reduction, Jacobi sums and hyperelliptic cryptosystems, Bull. Austral. Math. Soc. 58 (1998) 147–154.

[5] D.G. Cantor, Computing in the Jacobian of an hyperelliptic curve, Math. Comput. 24 (177) (1970) 95–101.

[6] T. Honda, On the Jacobian variety of the algebraic curve $y^2 = 1 - x^1$ over a fixed of characteristic $p > 0$, Osaka J. Math. 3 (1966) 189–194.

[7] N. Koblitz, Elliptic curve cryptosystems, Math. Comput. 48 (1987) 203–209.

[8] N. Koblitz, Hyperelliptic crypstosystems, J. Cryptol. 1 (1989) 139–150.

[9] G. Lachaud, Courbes diagonales et courbes de Picard, Prétirage N. 97–30. IML-France. 1997.

[10] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, Vol. 20, Cambridge University Press, Cambridge, 1983.

[11] F. Morain, I. Duursma, P. Gaudry, Speeding up the discrete log computation on curves with automorphisms, in: A. Odlyzko, G. Walsh, H. Williams (Eds.), Proceedings of the Conference on the Mathematics of Public Key Cryptography, Toronto, 1999.

[12] A. Odlyzko, Discrete logarithm and their cryptographic significiance, Advances in Cryptology-Eurocrypto'84, Springer, Berlin, 1985, pp. 224–314.

[13] M. Seysen, A probabilistic factorization algorithm with quadraticforms of negative discriminant, Math. Comput., to appear.

[14] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Universitext, 1993.

[15] A. Weil, Number of solutions of equations in finite fields, Bull. Amer. Math. Soc. 55 (1949) 497–508; =Œuvres Scientifiques (1949b), Vol. I, pp. 399–410.

[16] A. Weil, Jacobi sums as "Grossencharaktere", Trans. Amer. Math. Soc. 73 (1952) 497–508; =Œuvres Scientifiques (1952d), Vol. II, pp. 63–71.

[17] N. Yui, On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, J. Algebra 52 (1978) 378–410.