

# Some remarks on the Picard curves over a finite field

Yoh Takizawa

## Abstract

Let  $C$  be a smooth projective curve of genus 3 defined over a finite field  $k = \mathbb{F}_p$  with an affine model:

$$C : y^3 = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0, \quad a_i \in k.$$

It is called a Picard curve.

We show that for some concrete Picard curves the corresponding Jacobian variety is isomorphic to a product of supersingular elliptic curves.

And we get some curves of genus 3 such that the number of the rational points attain the Weill bound.

1991 Mathematics Subject Classification. Primary 11G20; Secondary 14G40, 14H45, 14G10, 14G15

## 1 Introduction

In this paper we study some special curves of genus 3 defined over finite field  $\mathbb{F}_p$ , where  $p$  is a rational prime with  $p > 3$ .

Let  $C$  be a smooth projective over  $\mathbb{F}_p$ . If the Jacobian variety of  $C$  is isogenous to a product of supersingular elliptic curves,  $C$  is called supersingular.

For hyperelliptic curves, there is a criterion for supersingularity in Yui[10]. In genus 2 case, Ibukiyama, Katsura and Oort[4] gave a detailed study on supersingular curves. Especially they listed up the supersingular curves of genus 2 for some finite fields.

In genus 3 case, Estrada-Sarlabous[1] gave a criterion for supersingularity of Picard curves using differential 1 forms and Cartier operators. In this paper, we use a basis of  $H^1(C, \mathcal{O}_C)$  and the Frobenius endomorphisms. This method is simply a dual version of [1].

We obtain some special curves, such that the Jacobian is isomorphic to a product of supersingular elliptic curves. Moreover we show that some of these curves attain the Weil bound.

## 2 The geometry of Picard curves over finite field

Let  $k = \mathbb{F}_p$  be a finite field with a rational prime  $p > 3$ , and  $\bar{k}$  be its algebraic closure. Let  $C$  be a smooth projective curve over  $k$  with an affine model:

$$y^3 = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0, \quad a_i \in k.$$

where  $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$  has no multiple root. It is called a Picard curve.

We choose a system of basis of  $H^1(C, \mathcal{O}_C)$  as

$$\{y/x, y^2/x^2, y^2/x\}.$$

Let  $\sigma : C \rightarrow C$  be the  $p$ -th power Frobenius morphism. Then  $\sigma$  induces a map

$$\sigma' : H^1(C, \mathcal{O}_C) \rightarrow H^1(C, \mathcal{O}_C)$$

on cohomology. This map is not linear, but it is  $p$ -linear, namely;

$$\sigma(\lambda f) = \lambda^p \sigma(f), \quad \lambda \in k, f \in H^1(C, \mathcal{O}_C).$$

If  $\{z_1, z_2, z_3\}$  is a system of basis of  $H^1(C, \mathcal{O}_C)$ , the action of  $\sigma$  can be represented by a matrix  $A = (a_{ij})$ , whose entries are defined by

$$\sigma(z_i) = \sum_{j=1}^3 a_{ij} z_j, \quad a_{ij} \in k$$

The matrix  $A$  is called the Hasse-Witt matrix of  $C$  with respect to the basis  $\{z_1, z_2, z_3\}$ .

Let  $J(C)$  be the Jacobian variety of  $C$ . We may assume that  $J(C)$  and its canonical embedding  $C \rightarrow J(C)$  are also defined over  $k$ . Let  $P_{\sigma'}(t)$  be the characteristic polynomial of  $\sigma'$ .

The zeta function of  $C$  is equal to;

$$Z(C, t) = \frac{F(t)}{(1-t)(1-pt)},$$

where  $F(t) = \sum_{i=0}^6 b_i t^i$  is the polynomial in  $\mathbb{Z}[t]$ . And the coefficients  $b_i$  of  $F(t)$  can be computed with the number of  $k^r$ -rational points on  $C$ .

Let  $N_r$  be the number of  $k^r$ -rational points on  $C$ . The coefficients of  $F(t)$  are represented as follows;

$$\begin{aligned} b_6 &= 1, b_5 = N_1 - 1 - p, b_4 = (N_2 - 1 - p^2 + b_5^2)/2, \\ b_3 &= (N_3 - 1 - p^3 + b_5^2 + 3b_4b_5)/3, \\ b_2 &= pb_4, b_1 = p^2b_5, b_0 = p^3. \end{aligned}$$

We have the following well known equality;

$$P_{\sigma'}(t) = t^6 F(1/t).$$

### 3 The superspecial Picard curves

Let  $k^m$  be a finite field of characteristic  $p > 0$  with  $q = p^m (m \leq 1)$  elements and  $\bar{k}$  its algebraic closure. The following theorem is well known:

**Theorem 1.** *Let  $X$  be a curve defined over  $k$ . Then the Jacobian  $J(X)$  is isomorphic to a product of supersingular elliptic curves if and only if the Cartier operator  $\mathcal{C} : H^0(X, \Omega_X^1) \rightarrow H^0(X, \Omega_X^1)$  vanishes.*

Let  $X$  be a curve over  $k$ .  $X$  is called supersingular, if the Jacobian  $J(X)$  is isogenous to a product of supersingular elliptic curves.  $X$  is called superspecial, if the Jacobian  $J(X)$  is isomorphic to a product of supersingular elliptic curves.

By the Serre duality this is equivalent to vanishing of the Frobenius  $\sigma' : H^1(X, \mathcal{O}_X^1) \rightarrow H^1(X, \mathcal{O}_X^1)$ . We compute some examples, we get these results by explicit computing.

**Theorem 2.** *Let  $p$  be a rational prime with  $p > 5$ .*

1. *If  $p \equiv 8 \pmod{9}$ , then the Jacobian variety of a Picard curve defined over  $\mathbb{F}_p$  with an affine equation;*

$$y^3 = x^4 - x$$

*is superspecial.*

2. *If  $p \equiv 11 \pmod{12}$ , then the Jacobian variety of a Picard curve defined over  $\mathbb{F}_p$  with an affine equation;*

$$y^3 = x^4 - 1$$

*is superspecial.*

*Proof.* 1. Assume  $p = 9r + 8$ ,  $r \in \mathbb{Z}$  and  $y^3 = x^4 - x$ .

$$\begin{aligned} (y/x)^p &= (y^3)^{3r+2} y^2 / x^p \\ &= (x^4 - x)^{3r+2} y^2 / x^p \\ &= \sum \binom{3r+2}{k} (-1)^{3r+2-k} x^{3r+3k+2} (y^2 / x^{9r+8}) \\ &= \sum \binom{3r+2}{k} (-1)^{3r+2-k} x^{3(k-2r-2)} (y^2) \\ &\equiv 0 \pmod{H^1(C, \mathcal{O}_C)}. \end{aligned}$$

By the same argument,

$$\begin{aligned} (y^2/x^2)^p &= (y^3)^{6r+5} y / x^{2p} \\ &= \sum \binom{6r+5}{k} (-1)^{6r+5-k} x^{3(k-2r-3)-2} (y^2) \\ &\equiv 0 \pmod{H^1(C, \mathcal{O}_C)}. \end{aligned}$$

$$\begin{aligned} (y^2/x)^p &= (y^3)^{6r+5} y / x^p \\ &= \sum \binom{6r+5}{k} (-1)^{6r+5-k} x^{3(k-r-1)} (y^2) \\ &\equiv 0 \pmod{H^1(C, \mathcal{O}_C)}. \end{aligned}$$

2. Assume  $p = 12r + 11$ ,  $r \in \mathbb{Z}$  and  $y^3 = x^4 - 1$ .

$$\begin{aligned}
(y/x)^p &= (y^3)^{4r+3} y^2/x^p \\
&= (x^4 - 1)^{4r+3} y^2/x^p \\
&= \sum \binom{4r+3}{k} (-1)^{4r+3-k} x^{4k} (y^2/x^{12r+11}) \\
&= \sum \binom{4r+3}{k} (-1)^{4r+3-k} x^{4(k-3r-2)-3} (y^2) \\
&\equiv 0 \pmod{H}^1(C, \mathcal{O}_C).
\end{aligned}$$

By the same argument,

$$\begin{aligned}
(y^2/x^2)^p &= (y^3)^{8r+7} y/x^{2p} \\
&= \sum \binom{8r+7}{k} (-1)^{8r+7-k} x^{4(k-6r-5)-2} (y^2) \\
&\equiv 0 \pmod{H}^1(C, \mathcal{O}_C).
\end{aligned}$$

$$\begin{aligned}
(y^2/x)^p &= (y^3)^{8r+7} y/x^p \\
&= \sum \binom{8r+7}{k} (-1)^{8r+7-k} x^{4(k-3r-2)-3} (y^2) \\
&\equiv 0 \pmod{H}^1(C, \mathcal{O}_C).
\end{aligned}$$

So our Frobenius map is 0-map. That assures our assertions.  $\square$

## 4 Some examples of Picard curves with many rational points

Let  $X$  be a smooth projective curve of genus  $g$  defined over  $\mathbb{F}_q$ , with  $q = p^r$  for a rational prime  $p$  and a positive integer  $r$ . Let  $N_m$  be the number of  $\mathbb{F}_{q^m}$  rational points of  $X$ . It holds

$$1 + q^m - 2gq^{m/2} \leq N_m \leq 1 + q^m + 2gq^{m/2}.$$

This is called the Weil bound.

Let  $C$  be a superspecial curve defined over  $\mathbb{F}_p$ , the number of rational points of  $C$  attains the Weil bound.

In the preceding section, we have two examples of superspecial Picard curves. we computed the zeta functions of these curves for some rational primes.

**Example 1.** Let  $p = 17$ , and  $C$  be the curve over  $\mathbb{F}_{17}$  with affine model:

$$C : y^3 = x^4 - x.$$

$\sharp C(\mathbb{F}_p) = 18$ ,  $\sharp C(\mathbb{F}_{p^2}) = 392 = 1 + 172 + 2 \cdot 3i7$  and  $\sharp C(\mathbb{F}_{p^3}) = 4914$ . The zeta function of  $C/\mathbb{F}_{17}$  is:

$$Z(C, t) = \frac{(1 + 17t^2)^3}{(1 - t)(1 - 17t)}.$$

The number of the rational points  $N_m = \#C(\mathbb{F}_{p^m})$  is:

$$N_m = 1 + 17^m - 3(\sqrt{-17^m} + (-\sqrt{-17})^m).$$

For  $e \in \mathbb{N}$ ,

$$N_{2e} = 1 + 17^{2e} - 6 \cdot (-17)^e.$$

**Example 2.** Let  $p = 11$ , and  $C$  be the curve over  $\mathbb{F}_{11}$  with affine model:

$$C : y^3 = x^4 - 1.$$

$\#C(\mathbb{F}_p) = 12$ ,  $\#C(\mathbb{F}_{p^2}) = 188 = 1 + 112 + 2 \cdot 3i11$  and  $\#C(\mathbb{F}_{p^3}) = 1332$ . The zeta function of  $C/\mathbb{F}_{11}$  is:

$$Z(C, t) = \frac{(1 + 11t^2)^3}{(1 - t)(1 - 11t)}.$$

The number of the rational points  $N_m = \#C(\mathbb{F}_{p^m})$  is:

$$N_m = 1 + 11^m - 3(\sqrt{-11^m} + (-\sqrt{-11})^m).$$

For  $e \in \mathbb{N}$ ,

$$N_{2e} = 1 + 11^{2e} - 6 \cdot (-11)^e.$$

## References

- [1] J.Estrada-Sarlabous: On the Jacobian varieties of Picard curves defined over fields of characteristic  $p > 0$ . Math.Nachr. 152 (1991), 329-340.
- [2] R. P. Holzapfel and F. Nicolae: Arithmetic on a family of Picard curves. preprint.
- [3] T. Ibukiyama, T. Katsura and F. Oort: Supersingular curves of genus two and class numbers. Compos. Math. 57 (1986), 127-152.
- [4] Y. I. Manin: The Hasse-Witt matrix of an algebraic curve. AMS Trans. Ser. 2, Vol. 45 (1965), 245-264.
- [5] J. S. Milne: Abelian varieties. Arithmetic Geometry, Springer-Verlag, New York (1986), 103-150.
- [6] J. S. Milne: Jacobian varieties. Arithmetic Geometry, Springer-Verlag, New York (1986), 167-211.
- [7] N. Nygaard: Slopes of powers of Frobenius on crystalline cohomology. Ann. Sci. Ecole. Norm. Sup. 14 (1981), 369-401.
- [8] N. Yui: On the Jacobian varieties of hyperelliptic curves over fields of characteristic  $p > 2$ . Joun. of alg. 52 (1978), 378-410.