

Some remarks on the Picard curves over a finite field II

Yoh Takizawa

Abstract

In this paper we classify the Newton polygons of the L -polynomial $L(t)$ associated to the Picard curve over \mathbb{F}_p obtained from the curve

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

over \mathbb{Z} by reduction modulo p . Our main result is stated in Theorem 3.1.

1 Curves over finite fields

Let k denote the field of $q = p^m$ elements with a rational prime p , and let \bar{k} denote its algebraic closure. Let k_r denote the algebraic extension of k with $[k_r : k] = r$. Let C/k be a smooth projective curve of genus g , and let N_r denote the number of k_r -rational points.

The zeta function of C over $k = \mathbb{F}_q$ is the formal power series

$$Z(C; t) = \exp\left(\sum_{i=1}^{\infty} N_i \frac{t^i}{i}\right).$$

Proposition 1.1. 1. $Z(C; t)$ is a rational function of t and it is given in the form

$$Z(C; t) = \frac{L_C(t)}{(1-t)(1-qt)},$$

where $L_C(t) = \sum_{i=0}^{2g} a_i t^i \in \mathbb{Z}[t]$, $a_0 = 1$, $a_{2g} = q^g$.

2. $Z(C; t)$ satisfies the functional equation

$$Z\left(C; \frac{1}{qt}\right) = q^{1-g} t^{2-2g} Z(C; t).$$

3. Let $L_C(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$ be the decomposition in linear factors in $\mathbb{C}[t]$, it holds

$$|\alpha_i| = q^{1/2}, \quad 1 \leq i \leq 2g.$$

Proof. Milne[5],[6]. □

The polynomial $L_C(t)$ is called the L -polynomial of C .

Corollary 1.1. 1. For the L -polynomial $L_C(t) = \sum_{i=0}^{2g} a_i t^i$, we have

$$a_i = q^{i-g} a_{2g-i}, \quad 0 \leq i \leq g$$

2. For the linear decomposition $L_C(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$ over \mathbb{C} , it holds

$$N_r = 1 + q^r - \sum_{i=1}^{2g} \alpha_i^r.$$

Let $J = J(C)$ be the jacobian variety associated to C/k . If $N_1 \neq 0$, we may assume that J and the canonical embedding $C \rightarrow J$ are defined over k . (Hindry and Silverman [8].) Let l be a rational prime with $l \neq p$ and let $T_l J$ denote the Tate module of J , and let $(T_l J)^\vee$ denote its dual.

Proposition 1.2. *Let $H^n(C_{\text{et}}, \mathbb{Z}_l)$ and $H^n(J_{\text{et}}, \mathbb{Z}_l)$ be l -adic cohomologies of C and J , respectively. It holds*

$$H^1(C_{\text{et}}, \mathbb{Z}_l) \cong H^1(J_{\text{et}}, \mathbb{Z}_l) \cong (T_l J)^\vee.$$

Proof. Milne [5],[6]. □

Let $\pi : J \rightarrow J$ be the Frobenius endomorphism relative to k , and let $P(t)$ is the characteristic polynomial of π acting on $T_l J$. Then we have

$$P(t) = t^{-2g} L_C(1/t).$$

Theorem 1.1. *Let A and B be abelian varieties over k . Let $P_A(t)$ and $P_B(t)$ be the characteristic polynomials of the Frobenius, respectively. A is isogenous to B if and only if $P_A(t) = P_B(t)$.*

Proof. Tate [10]. □

Let $H^n(C, \mathcal{O}_C)$ be the coherent cohomology relative to the Zariski topology. If we choose a basis $\{f_1, \dots, f_g\}$ of $H^1(C, \mathcal{O}_C)$, the Frobenius morphism π is represented by a matrix:

$$\pi \begin{pmatrix} f_1 \\ \vdots \\ f_g \end{pmatrix} = A \begin{pmatrix} f_1 \\ \vdots \\ f_g \end{pmatrix},$$

where A is a $(g \times g)$ matrix with elements in k .

$$A_\pi = A \cdot A^{(p^2)} \dots A^{(p^{g-1})}$$

is called the Hasse-Witt matrix of C relative to the basis $\{f_1, \dots, f_g\}$.

Theorem 1.2.

$$P(t) \equiv (-1)^{gt^g} \det(A_\pi - tI_g) \pmod{p}.$$

Proof. Manin [3],[4]. □

The following theorem is well known:

Theorem 1.3. *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.*

Proof. Nygaard [7]. □

This means $J(C)$ is isomorphic to a product of the supersingular elliptic curves if and only if the Frobenius endomorphism $\pi : H^1(C, \mathcal{O}_C) \rightarrow H^1(C, \mathcal{O}_C)$ vanishes.

2 Picard curves over a finite field

Let $k = \mathbb{F}_p$ be a finite field with a rational prime $p > 3$, And let C be a smooth projective curve over k with an affine model:

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

here it is supposed $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ has no multiple root. It is called a Picard curve.

The L -polynomial of C is equal to;

$$L_C(t) = \sum_{i=0}^6 b_i t^i.$$

Let N_r be the number of k^r -rational points on C . The coefficients of $L_C(t)$ are given by

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

Proposition 2.1. *Let C be a Picard curve over a finite field \mathbb{F}_q . If $q^m \equiv 2 \pmod{3}$, then*

$$N_m = q^m + 1.$$

Proof. Estrada [1] Holzapfel-Nicolae[2]. □

The projective model of C is:

$$Y^3 = X^4 + a_3X^3Z + a_2X^2Z^2 + a_1XZ^3 + a_0Z^4.$$

To find a basis of $H^1(C, \mathcal{O}_C)$, we consider the standard affine covering of C

$$V_0 = C \cap \{Z \neq 0\}, \quad V_1 = \{X \neq 0\}.$$

Let δ be the coboundary map :

$$\delta : \Gamma(V_0, \mathcal{O}_C) \times \Gamma(V_1, \mathcal{O}_C) \rightarrow \Gamma(V_0 \cap V_1),$$

$$\delta(f_0, f_1) = f_0 - f_1|_{V_0 \cap V_1}.$$

Because $\{V_0, V_1\}$ is an affine covering of C , the Cech cohomology is isomorphic to $H^i(C, \mathcal{O}_C)$. In particular

$$H^1(C, \mathcal{O}_C) \cong \Gamma(V_0 \cap V_1, \mathcal{O}_C) / \text{Im } \delta.$$

Set $P_\infty = [X : Y : Z] = [0 : 1 : 0]$, $P_i = [0 : \beta_i : 1]$ ($i = 1, 2, 3$), where β_i 's are the roots of the equation $y^3 = a_0$ and $Q_j = [\alpha_j : 0 : 1]$ ($j = 1, 2, 3, 4$), where α_j 's are the roots of the equation $f(x) = 0$.

If $\varphi \in \Gamma(V_0 \cap V_1, \mathcal{O}_C)$, then φ is regular except $\{P_1, P_2, P_3, P_\infty\}$. On the other hand, we have the Weierstrass gap values 1, 2, 5 at P_∞ .

We denote the principal divisor of the function φ by (φ) . The divisors of coordinate functions $x = X/Z$ and $y = Y/Z$ are given by

$$\begin{aligned} (x) &= P_1 + P_2 + P_3 - 3P_\infty, \\ (y) &= Q_1 + Q_2 + Q_3 + Q_4 - 4P_\infty. \end{aligned}$$

Similarly we have

$$(y/x) = \sum_{i=1}^4 Q_i - \sum_{j=1}^3 P_j - P_\infty$$

$$(y^2/x^2) = 2 \sum_{i=1}^4 Q_i - 2 \sum_{j=1}^3 P_j - 2P_\infty$$

$$(y^2/x) = 2 \sum_{i=1}^4 Q_i - \sum_{j=1}^3 P_j - 5P_\infty.$$

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

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

Proposition 2.2. *We have*

$$y/x^n = 0 \text{ in } H^1(C, \mathcal{O}_C)$$

for $n \neq 1$, and

$$y^2/x^m = 0 \text{ in } H^1(C, \mathcal{O}_C)$$

for $m \neq 1, 2$.

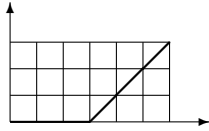
Proof. We have

$$(y/x^n) = \sum_{i=1}^4 Q_i - n \sum_{j=1}^3 P_j + (3n - 4)P_\infty \quad (n \in \mathbb{Z}).$$

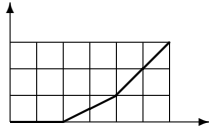
If $n \leq 0$, then y/x^n has a pole only at P_∞ . This means $y/x^n \in \Gamma(V_0, \mathcal{O}_C)$, and $\delta(y/x^n, 0) = y/x^n$. If $n \geq 2$, y/x^n has a pole at P_1, P_2, P_3 . This means $y/x^n \in \Gamma(V_1, \mathcal{O}_C)$, and $\delta(0, y/x^n) = y/x^n$. So the first assertion follows.

We obtain the second by the same argument. \square

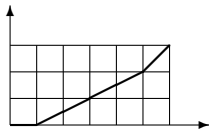
Let v_p be the p -adic valuation of \mathbb{Q}_p . By the Newton polygon of $L_C(t) = \sum_{i=0}^6 b_i t^i$ we mean the lower convex envelope of the set of points $\{(i, v_p(b_i)) : 0 \leq i \leq 2g\} \subset \mathbb{R}^2$. Let $L_C(t) = \sum_{i=1}^{2g} a_i t^i$ be a L -polynomial of a Picard curve. We have five possibilities for the Newton polygons given by the following figures.



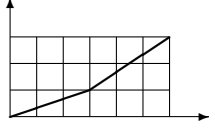
Type I : ordinary



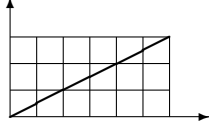
Type II



Type III



Type IV



Type V : supersingular

3 Curve $C : y^3 = x^4 - 1$ over \mathbb{F}_p

Theorem 3.1. *Let p be a rational prime with $p > 3$ and let $k = \mathbb{F}_p$. For the Picard curve*

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

over k , the Newton polygon takes the shape of

$$\left\{ \begin{array}{ll} \text{Type V} & \text{for } p \equiv 11 \pmod{12} \\ \text{Type I} & \text{for } p \equiv 1 \pmod{12} \\ \text{Type II} & \text{for } p \equiv 5 \pmod{12} \\ \text{Type III} & \text{for } p \equiv 7 \pmod{12}. \end{array} \right.$$

Proof. (1) Assume $p = 12r + 11$, $r \in \mathbb{Z}$. So

$$\begin{aligned} (y/x)^p &= (y^3)^{4r+3} y^2 / x^p \\ &= (x^4 - 1)^{3r+2} y^2 / x^p \\ &= \sum (-1)^{4r+3-k} \binom{4r+3}{k} y^2 / x^{p-4k}, \end{aligned}$$

with

$$\begin{aligned} p - 4k &= 12r + 11 - 4k \\ &= 4(3r - k + 2) + 3 \\ &\neq 1, 2. \end{aligned}$$

By Proposition 2.2, we obtain

$$(y/x)^p \equiv 0 \pmod{H^1(C, \mathcal{O}_C)}.$$

We have

$$\begin{aligned} (y^2/x^2)^p &= (y^3)^{8r+7} y / x^{2p} \\ &= \sum (-1)^{8r+7-k} \binom{8r+7}{k} y / x^{2p-4k}, \end{aligned}$$

with

$$\begin{aligned} 2p - 4k &= 24r + 22 - 4k \\ &= 4(6r - k + 5) + 2 \\ &\neq 1. \end{aligned}$$

By Proposition 2.2, we obtain

$$(y^2/x^2)^p \equiv 0 \pmod{H^1(C, \mathcal{O}_C)}.$$

And we have

$$\begin{aligned} (y^2/x)^p &= (y^3)^{8r+7} y/x^p \\ &= \sum (-1)^{8r+7-k} \binom{8r+7}{k} y/x^{p-4k}, \end{aligned}$$

with

$$\begin{aligned} p - 4k &= 4(3r - k + 2) + 3 \\ &\neq 1. \end{aligned}$$

By Proposition 2.2, we obtain

$$(y^2/x)^p \equiv 0 \pmod{H^1(C, \mathcal{O}_C)}.$$

So our Frobenius map is 0-map. By Theorem 1.3,

$$P(t) \equiv (-1)^3 t^3 (-t^3) \equiv t^6 \pmod{p},$$

and

$$L_C(t) \equiv 1 \pmod{p}.$$

We conclude $L_C(t)$ belongs to Type V.

(2) Assume $p = 12r + 1$, $r \in \mathbb{Z}$. So

$$\begin{aligned} (y/x)^p &= (y^3)^{4r} y/x^p \\ &= (x^4 - 1)^{4r} y/x^p \\ &= \sum (-1)^{4r-k} \binom{4r}{k} y/x^{p-4k}, \end{aligned}$$

with

$$\begin{aligned} p - 4k &= 12r + 1 - 4k \\ &= 4(3r - k) + 1. \end{aligned}$$

By Proposition 2.2, it remains only the term $k = 3r$. So we obtain

$$(y/x)^p \equiv (-1)^r \binom{4r}{3r} y/x \pmod{H^1(C, \mathcal{O}_C)}.$$

We have

$$\begin{aligned} (y^2/x^2)^p &= (y^3)^{8r} y^2/x^{2p} \\ &= \sum (-1)^{8r-k} \binom{8r}{k} y^2/x^{2p-4k}, \end{aligned}$$

with

$$\begin{aligned} 2p - 4k &= 24r + 2 - 4k \\ &= 4(6r - k) + 2. \end{aligned}$$

By Proposition 2.2, it remains only the term $k = 6r$. So we obtain

$$(y^2/x^2)^p \equiv (-1)^{2r} \binom{8r}{6r} y^2/x^2 \pmod{H^1(C, \mathcal{O}_C)}.$$

And we have

$$\begin{aligned} (y^2/x)^p &= (y^3)^{8r} y^2/x^p \\ &= \sum (-1)^{8r-r} \binom{8r}{k} y/x^{p-4k}, \end{aligned}$$

with

$$\begin{aligned} p - 4k &= 12r + 1 - 4k \\ &= 4(3r - k) + 1. \end{aligned}$$

By Proposition 2.2, it remains only the term $k = 3r$. So we obtain

$$(y^2/x)^p \equiv (-1)^{5r} \binom{8r}{3r} y^2/x \pmod{H^1(C, \mathcal{O}_C)}.$$

The matrix associated to the Frobenius map is:

$$A = \begin{pmatrix} (-1)^r \binom{4r}{3r} & 0 & 0 \\ 0 & (-1)^{2r} \binom{8r}{6r} & 0 \\ 0 & 0 & (-1)^{5r} \binom{8r}{3r} \end{pmatrix},$$

and the Hasse-Witt matrix of C is

$$A_\pi = \begin{pmatrix} c_1 & 0 & 0 \\ 0 & c_2 & 0 \\ 0 & 0 & c_3 \end{pmatrix},$$

where $c_1 = (-1)^{r+p+p^2} \binom{4r}{3r} \binom{4r}{3r}^p \binom{4r}{3r}^{p^2}$, $c_2 = (-1)^{2r+p+p^2} \binom{8r}{6r} \binom{8r}{6r}^p \binom{8r}{6r}^{p^2}$ and $c_3 = (-1)^{5r+p+p^2} \binom{8r}{3r} \binom{8r}{3r}^p \binom{8r}{3r}^{p^2}$. By Theorem 1.2, we obtain

$$\begin{aligned} P(t) &\equiv -t^3(c_1 - t)(c_2 - t)(c_3 - t) \\ &\equiv t^6 - (c_1 + c_2 + c_3)t^5 + (c_1c_2 + c_2c_3 + c_3c_1)t^4 - c_1c_2c_3t^3 \pmod{p}, \end{aligned}$$

and

$$L_C(t) \equiv 1 - (c_1 + c_2 + c_3)t + (c_1c_2 + c_2c_3 + c_3c_1)t^2 - c_1c_2c_3t^3 \pmod{p},$$

with $v_p(c_1c_2c_3) = 0$. So $L_C(t)$ belongs to Type I.

(3) Assume $p = 12r + 5$, $r \in \mathbb{Z}$. So

$$\begin{aligned} (y/x)^p &= (y^3)^{4r+1} y^2/x^p \\ &= (x^4 - 1)^{4r+1} y^2/x^p \\ &= \sum (-1)^{4r+1-k} \binom{4r+1}{k} y^2/x^{p-4k}, \end{aligned}$$

with

$$\begin{aligned} p - 4k &= 12r + 5 - 4k \\ &= 4(3r - k + 1) + 1. \end{aligned}$$

By Proposition 2.2, it remains only the term $k = 3r + 1$. So we obtain

$$(y/x)^p \equiv (-1)^r \binom{4r+1}{3r+1} y^2/x \pmod{H^1(C, \mathcal{O}_C)}.$$

We have

$$\begin{aligned} (y^2/x^2)^p &= (y^3)^{8r+3} y/x^{2p} \\ &= \sum (-1)^{8r+3-k} \binom{8r+3}{k} y/x^{2p-4k}, \end{aligned}$$

with

$$\begin{aligned} 2p - 4k &= 24r + 10 - 4k \\ &= 4(6r - k + 2) + 2 \\ &\neq 1. \end{aligned}$$

By Proposition 2.2, we obtain

$$(y^2/x^2)^p \equiv 0 \pmod{H^1(C, \mathcal{O}_C)}.$$

And we have

$$\begin{aligned} (y^2/x)^p &= (y^3)^{8r+3} y/x^p \\ &= \sum (-1)^{8r+3-k} \binom{8r+3}{k} y/x^{p-4k}, \end{aligned}$$

with

$$p - 4k = 4(3r - k + 1) + 1.$$

By Proposition 2.2, it remains only the term $k = 3r + 1$. So we obtain

$$(y^2/x)^p \equiv (-1)^{5r+2} \binom{8r+3}{3r+1} y/x \pmod{H^1(C, \mathcal{O}_C)}.$$

The matrix associated to Frobenius map is;

$$A = \begin{pmatrix} 0 & 0 & (-1)^r \binom{4r+1}{3r+1} \\ 0 & 0 & 0 \\ (-1)^{5r+2} \binom{8r+3}{3r+1} & 0 & 0 \end{pmatrix},$$

and the Hasse-Witt matrix of C is

$$A_\pi = \begin{pmatrix} 0 & 0 & \alpha \\ 0 & 0 & 0 \\ \beta & 0 & 0 \end{pmatrix},$$

where $\alpha = (-1)^{5r+2+r^p+(5r+2)^{p^2}} \binom{4r+1}{3r+1}^p \binom{8r+3}{3r+1}^{p^2+1}$ and $\beta = (-1)^{r+(5r+2)^p+r^{p^2}} \binom{8r+3}{3r+1}^p \binom{4r+1}{3r+1}^{p^2+1}$.

By Theorem 1.2, we obtain

$$\begin{aligned} P(t) &\equiv (-1)^3 t^3 (-t^3 + \alpha\beta t) \\ &\equiv t^6 - \alpha\beta t^4 \pmod{p}, \end{aligned}$$

and

$$L(t) \equiv 1 - \alpha\beta t^2 \pmod{p}$$

with

$$v_p(\alpha\beta) = 0.$$

We conclude $L_C(t)$ belongs to Type II.

(4) Assume $p = 12r + 7$, $r \in \mathbb{Z}$. So

$$\begin{aligned} (y/x)^p &= (y^3)^{4r+2} y/x^p \\ &= (x^4 - 1)^{4r+2} y/x^p \\ &= \sum (-1)^{4r+2-k} \binom{4r+2}{k} y/x^{p-4k}, \end{aligned}$$

with

$$\begin{aligned} p - 4k &= 12r + 7 - 4k \\ &= 4(3r - k + 1) + 3 \\ &\neq 1, 2. \end{aligned}$$

By Proposition 2.2, we obtain

$$(y/x)^p \equiv 0 \pmod{H^1(C, \mathcal{O}_C)}.$$

We have

$$\begin{aligned} (y^2/x^2)^p &= (y^3)^{8r+4} y^2/x^{2p} \\ &= \sum (-1)^{8r+4-k} \binom{8r+4}{k} y^2/x^{2p-4k}, \end{aligned}$$

with

$$\begin{aligned} 2p - 4k &= 24r + 14 - 4k \\ &= 4(6r - k + 3) + 2. \end{aligned}$$

By Proposition 2.2, it remains only the term $k = 6r + 3$. So we obtain

$$(y^2/x^2)^p \equiv (-1)^{2r+1} \binom{8r+4}{6r+3} y^2/x^2 \pmod{H^1(C, \mathcal{O}_C)}.$$

And we have

$$\begin{aligned} (y^2/x)^p &= (y^3)^{8r+4} y^2/x^p \\ &= \sum (-1)^{8r+4-k} \binom{8r+4}{k} y^2/x^{p-4k}, \end{aligned}$$

with

$$\begin{aligned} p - 4k &= 4(3r - k + 1) + 3 \\ &\neq 1, 2. \end{aligned}$$

By Proposition 2.2, we obtain

$$(y^2/x)^p \equiv 0 \pmod{H^1(C, \mathcal{O}_C)}.$$

The matrix associated to Frobenius map is;

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & (-1)^{2r+1} \binom{8r+4}{6r+3} & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and the Hasse-Witt matrix of C is

$$A_\pi = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \gamma & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

where $\gamma = (-1)^{2r+1+(2r+1)^p+(2r+1)^{p^2}} \binom{8r+4}{6r+3}^{1+p+p^2}$.

By Theorem 1.2, we obtain

$$\begin{aligned} P(t) &\equiv (-1)^3 t^3 t^2 (\gamma - t) \\ &\equiv -t^6 + \gamma t^5 \pmod{p}, \end{aligned}$$

and

$$L(t) \equiv 1 - \gamma t \pmod{p},$$

with

$$v_p(\gamma) = 0.$$

We conclude $L_C(t)$ belongs to Type III. □

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. Holzappel and F. Nicolae: Arithmetic on a family of Picard curves. preprint.
- [3] Y. I. Manin: The theory of commutative formal groups over fields of finite characteristic. Russian Math Surveys 18 (1963), 3-90.
- [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] M. Hindy and J. Silverman: Diophantine Geometry. Springer-Verlag, New York (2000).
- [9] Y. Takizawa: Some remarks on Picard curves over a finite field. Tech. Report Chiba U. no. 19 (2003).
- [10] J. Tate : Endomorphisms of Abelian Varieties over finite fields. Invent Math. 2 (1966), 134-144.
- [11] N. Yui: On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. Joun. of alg. 52 (1978), 378-410.