NAOSITE: Nagasaki University's Academic Output SITE



| | |
|---|---|
| Title | L-Functions of Algebraic Function Fields defined by y2=x5+a over GF(p) |
| Author(s) | Washio, Tadashi |
| Citation | 長崎大学教育学部自然科学研究報告. vol.34, p.15-19; 1983 |
| Issue Date | 1983-02-28 |
| URL | http://hdl.handle.net/10069/32560 |
| Right | |

This document is downloaded at: 2018-11-14T18:18:21Z

http://naosite.lb.nagasaki-u.ac.jp

Sci. Bull. Fac. Educ., Nagasaki Univ., No. 34, pp. 15~19 (1984)

# $L$-Functions of Algebraic Function Fields defined by $y^2 = x^5 + a$ over $GF(p)$

Tadashi WASHIO

Department of Mathematics, Faculty of Education,
Nagasaki University, Nagasaki
(Received Oct. 31, 1982)

Abstract

Let $K=F(x, y)$ be an algebraic function field over a finite prime field $F$ defined by an equation $y^2=x^5+a$ ($a\neq 0$, $a\in F$). Then, under the assumption $p\equiv 1 \bmod 5$, the $L$-function of $K$ is computed by relating it to the Hasse-Witt matrix of $K$.

1. Introduction. Let $F=GF(p)$ be a finite prime field of characteristic $p\neq 2$. Let $K=F(x, y)$ be an algebraic function field over $F$ defined by an equation $y^2=x^5+a$ ($a\neq 0$, $a\in F$). We wish to study the numerator

$$L(u)=1+a_1u+a_2u^2+pa_1u^3+p^2u^4$$

of the zeta-function of $K$.

We have already discussed the particular case of $p\equiv 2, 3, 4 \bmod 5$ in [4], [5]. In fact, if $p\equiv 2,3 \bmod 5$, then

$$L(u)=1+p^2u^4,$$

and if $p\equiv 4 \bmod 5$, then

$$L(u)=1+2pu^2+p^2u^4.$$

Thus, in this note, we will go further to discuss the remaining case, that is, $p\equiv 1 \bmod 5$. Let $N_1$ be the number of prime divisors of degree one of $K$. Moreover, we will denote a constant field extension of $K$ of degree two by $K_2$ and also the number of prime divisors of degree one of $K_2$ by $N_1^{(2)}$. Applying the general theory in Hasse [1] to our case, we can immediately obtain the following formulae

$$N_1=p+1+c_1, \quad N_1^{(2)}=p^2+1+c_2,$$

where $c_1$ and $c_2$ mean the so-called error terms and they satisfy the inequalities

(1) $\qquad |c_1|\leqq 4\sqrt{p}, \quad |c_2|\leqq 4p.$

Then, the coefficients $a_1$ and $a_2$ are given by

(2) $\qquad a_1=c_1, \quad 2a_2=c_1^2+c_2.$

On the other hand, let $A$ be the Hasse-Witt matrix of $K$. Then, we have already proved that

$$\begin{cases} \text{Trace } A = \overline{1-N_1}, \\ \text{Trace } A^{p+1} = \overline{1-N_1{}^{(2)}}, \end{cases}$$

where the notation $\overline{m}$ means the residue class modulo $p$ represented by an integer $m$. ([3]).

It follows that

$$(3) \qquad \begin{cases} \overline{c_1} = -\text{Trace } A \\ \overline{c_2} = -\text{Trace } A^2. \end{cases}$$

Thus, in order to determine error terms, we will use information about the Hasse-Witt matrix, which is carried out in 2. In 3, we give explicit expressions for the coefficients of the $L$-function.

2. Hasse-Witt matrices. The Hasse-Witt matrices of a hyperelliptic function field has been discussed by Miller [2]. In this note, we limite ourselves only to the case where a hyperelliptic function field $K=F(x, y)$ is defined by

$$y^2=x^5+a, \quad (a\neq 0, a\in F),$$

over a finite prime field $F=GF(p)$ with characteristic $p$. Throughout this note, we will always assume that $p\equiv 1 \bmod 5$.

Let $A_{u,v}$ $(0\leqq u, v\leqq 1)$ be the coefficient of $x^{v+1}$ in the following polynomial

$$\Psi((x^5+a)^{\frac{p-1}{2}}x^{u+1}) = \Psi\Big(\sum_{0\leqq i\leqq\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i} a^{\frac{p-1}{2}-i} x^{5i+u+1}\Big)$$

where $\Psi$ means the $p^{-1}$−linear operator satisfying

$$\Psi(x^w) = \begin{cases} 0 & \text{if } (p, w)=1, \\ x^{\frac{w}{p}} & \text{otherwise.} \end{cases}$$

Then, the square matrix $A=(A_{u,v})$ is called the Hasse-Witt matrix of $K$. Because of the fact that the solutions $(u, v, i)$ of the equation

$$5i+u+1=p(v+1), \quad (0\leqq u, v\leqq 1,\ 0\leqq i\leqq \frac{p+1}{2})$$

are given by $(0, 0, \frac{p-1}{5})$ and $(1, 1, \frac{2p-2}{5})$, we have

$$A_{0,1}=A_{1,0}=0, \quad A_{0,0}=\binom{\frac{p-1}{2}}{\frac{p-1}{5}} a^{\frac{3p-3}{10}}, \quad A_{1,1}=\binom{\frac{p-1}{2}}{\frac{2p-2}{5}} a^{\frac{p-1}{10}}.$$

This implies that

$$(4)\quad \begin{cases} \text{Trace } A=A_{0,0}+A_{0,0}=\binom{\frac{p-1}{2}}{\frac{p-1}{5}}a^{\frac{3p-3}{10}}+\binom{\frac{p-1}{2}}{\frac{2p-2}{5}}a^{\frac{p-1}{10}}, \\ \text{Trace } A^2=A_{0,0}{}^2+A_{1,1}{}^2=\binom{\frac{p-1}{2}}{\frac{p-1}{5}}^2 a^{\frac{3p-3}{5}}+\binom{\frac{p-1}{2}}{\frac{2p-2}{5}}^2 a^{\frac{p-1}{5}}. \end{cases}$$

THEOREM 1. *We will conveniently denote the representative in* Z *of* $a\in F$ *by the same letter* $a$. *Let* $s_1$, $s_2$ *be, respectively the integers satisfying*

$$(5)\quad \begin{cases} s_1\equiv\binom{\frac{p-1}{2}}{\frac{p-1}{5}}a^{\frac{3p-3}{10}}+\binom{\frac{p-1}{2}}{\frac{2p-2}{5}}a^{\frac{p-1}{10}} \bmod p,\ |s_1|<\frac{p}{2}, \\ s_2\equiv\binom{\frac{p-1}{2}}{\frac{p-1}{5}}^2 a^{\frac{3p-3}{5}}+\binom{\frac{p-1}{2}}{\frac{2p-2}{5}}^2 a^{\frac{p-1}{5}} \bmod p,\ |s_2|<\frac{p}{2}. \end{cases}$$

*Then,* $c_1$ *and* $c_2$ *can be expressed in the form*

$$(6)\quad \begin{cases} c_1=pt-s_1, & (-1\leqq t\leqq 1), \\ c_2=pt'-s_2, & (-4\leqq t'\leqq 4). \end{cases}$$

*Especially, if* $p\geqq 71$ *then* $c_1=-s_1$.

PROOF. Combining (3),(4) and (5) gives us

$$\bar{c_1}=-\bar{s_1} \quad \text{and} \quad \bar{c_2}=-\bar{s_2}.$$

Moreover, because of $p\equiv 1 \bmod 5$, we can easily obtain $\frac{3}{2}p>4\sqrt{p}$. So the inequalities (1) lead to

$$|c_1|<\frac{3}{2}p \quad \text{and} \quad |c_2|\leqq 4p.$$

Therefore, inequalities $|s_1|<p/2$ and $|s_2|<p/2$ lead to the desired results (6). If $p\geqq 71$, then it is clear that $p/2>4\sqrt{p}$ and so $|c_1|<p/2$. Thus we get $c_1=-s_1$. This completes the proof of the theorem.

3. Error terms $c_1$ and $c_2$. We will now determine $t$ and $t'$ in Theorem 1. Let $\psi$ and $\psi_2$ be the quadratic characters of $F=GF(p)$ and $F_2=GF(p^2)$ respectively. Then, the error terms $c_1$ and $c_2$ are given by

$$(7)\quad c_1=\sum_{\alpha\in F}\psi(\alpha^5+a), \qquad c_2=\sum_{\beta\in F_2}\psi_2(\beta^5+a).$$

LEMMA 1. *If* $p\equiv 1 \bmod 5$, *then* $c_1\equiv\left(\frac{a}{p}\right) \bmod 5$

*where* $\left(\frac{a}{p}\right)$ *means the Legendre symbol, that is,* $\left(\frac{a}{p}\right)=\psi(a)$.

PROOF. Let us denote by $r$ a generating element of the cyclic group $F-\{0\}$. Then, by the definition (7) of $c_1$, we have

$$\begin{aligned} c_1 &= \psi(a) + \sum_{1\leqq i\leqq p-1} \psi(r^{5i}+a) \\ &= \left(\frac{a}{p}\right) + 5 \sum_{1\leqq i\leqq (p-1)/5} \psi(r^{5i}+a) \\ &\equiv \left(\frac{a}{p}\right) \bmod 5. \end{aligned}$$

LEMMA 1. *If* $p\equiv 1 \bmod 5$, *then*

$$c_2 \equiv \begin{cases} 6 \bmod 10 & \text{if } \chi_5(a)=1, \\ 1 \bmod 10 & \text{otherwise.} \end{cases} \tag{8}$$

*where* $\chi_5$ *means a multiplicative character of order* 5 *of* $F$.

PROOF. Let us denote by $\sigma$ a generating element of the cyclic group $F_2-\{0\}$. Then, by the definition (7) of $c_2$ and of $\psi_2(a)=1$, we have

$$c_2 = 1 + 5 \sum_{1\leqq i\leqq (p^2-1)/5} \psi_2(\sigma^{5i}+a). \tag{9}$$

If $\chi_5(a)=1$, then $\sigma^{5i}+a=0$ $(1\leqq i\leqq (p^2-1)/5)$ has one solution $i$ and if $\chi_5(a)\neq 1$, then $\sigma^{5i}+a\neq 0$ $(1\leqq i\leqq (p^2-1)/5)$.

This implies that

$$\sum_{1\leqq i\leqq (p^2-1)/5} \psi_2(\sigma^{5i}+a) \equiv \frac{p^2-1}{5} - \begin{cases} 1 \\ 0 \end{cases} \equiv \begin{cases} 1 \bmod 2 & \text{if } \chi_5(a)=1, \\ 0 \bmod 2 & \text{otherwise.} \end{cases}$$

Therefore, in view of the formula (9), we see the desired congruence (8).

THEOREM 2. *Let* $p\equiv 1 \bmod 5$. *Let the integers* $s_1$ *and* $s_2$ *be as in Theorem* 1. *Moreover, let* $t_1$ *and* $t_2$ *be, respectively, the integers satisfying*

$$t_1 \equiv s_1 + \left(\frac{a}{p}\right) \bmod 5, \qquad (-1\leqq t\leqq 1),$$

$$t_2 \equiv s_2 + \begin{cases} 6 \bmod 10 & \text{if } \chi_5(a)=1, \\ 1 \bmod 10 & \text{otherwise,} \end{cases} \qquad (-4\leqq t_2\leqq 4).$$

*Then, we have*

$$\begin{cases} c_1 = pt_1 - s_1, \\ c_2 = pt_2 - s_2. \end{cases} \tag{10}$$

PROOF. By making use of Theorem 1, $c_1$ and $c_2$ can be expressed in the form

$$\begin{cases} c_1 \equiv pt - s_1, & (-1\leqq t\leqq 1), \\ c_2 \equiv pt' - s_2, & (-4\leqq t'\leqq 4). \end{cases}$$

So, because of $p\equiv 1 \bmod 5$ and of $p\equiv 1 \bmod 10$, we have

$$\begin{cases} c_1 \equiv t - s_1 \bmod 5, \\ c_2 \equiv t' - s_2 \bmod 10. \end{cases}$$

Thus, Lemma 1 and Lemma 2 lead to

$$\begin{cases} t \equiv s_1 + c_1 \equiv s_1 + \left(\dfrac{a}{p}\right) \mod 5, \\ t' \equiv s_2 + c_2 \equiv s_2 + \begin{cases} 6 & \mod 10 \quad \text{if } \chi_5(a) = 1, \\ 1 & \mod 10 \quad \text{otherwise.} \end{cases} \end{cases}$$

Therefore, $t$ and $t'$, respectively, coincide with $t_1$ and $t_2$ and so we have the desired assertions (10).

Substiuting (10) in the formulae (2) gives us the following result.

COROLLARY. *If* $p \equiv 1 \mod 5$, *then*

$$\begin{cases} a_1 = pt_1 - s_1, \\ 2a_2 = (pt_1 - s_1)^2 + pt_2 - s_2. \end{cases}$$

## References


[1] H. Hasse, *The Riemann Hypothesis in Algebraic Function Fields over a Finite Constants Field*, The Pennsylvania State University, (1968), p. 235.

[2] L. Miller, *Curves with Invertible Hasse-Witt Matrix*, Math. Ann., **197** (1972), 123-127.

[3] T. Washio, *A Remark on the Trace Formula for an Inseparable Correspondence in an Algebraic Function Field*, Mem. Fac. Sci., Kyushu Univ., Ser. A **24** (2) (1970), 231-237.

[4] T. Washio, *On Class Numbers of Hyperelliptic Function Fields*, Sci. Bull. Fac. Educ., Nagasaki Univ., **29** (1978), 1-3.

[5] T. Washio, *On Class Numbere of Hyperelliptic Function Fields*, II, Sci. Bull. Fac. Educ., Nagasaki Univ., **31** (1980), 1-4.