Sci. Bull. Fac. Educ., Nagasaki Univ., No. 48, pp. 1~4 (1993)

Note on explicit formulas of L-funcitons of some hyperelliptic curves

Dedicated to Professor Katsumi Shiratani on his 60th birthday

Tadashi WASHIO and Tetsuo KODAMA*

Department of Mathematics, Faculty of Education,
Nagasaki University, Nagasaki 852, Japan

(Received Oct. 30, 1992)

Abstract

Let $\mathbb{F}=GF(p)$ be a prime field of characteristic $p>2$. Let $P(x)$ and $P'(x)$ be polynomials over $\mathbb{F}$ satisfying $P'(x) \mid P(x)$. Denote by $K=\mathbb{F}(x,y)$ and $K'=\mathbb{F}(x,y)$ hyperelliptic function fields defined by $y^2=P(x)$ and $y^2=P'(x)$ over $\mathbb{F}$ respectively. Then we give a condition for $P(x)$ and $P'(x)$ such that the L-function of K is divisible by the one of K'.

1. Introduction

Let $\mathbb{F}=GF(p)$ be a prime field of characteristic $p>2$. Let g be a positive integer. Denote by $P(x)$ a polynomial over $\mathbb{F}$ of the form $P(x)=x^{2g+1}+1$ where $(2g+1, p)=1$ or of the form $P(x)=x(x^{2g}+1)$ where $(2g, p)=1$ and by $K=\mathbb{F}(x, y)$ a hyperelliptic function field defined by $y^2=P(x)$ over $\mathbb{F}$. Assume that, in the case $P(x)=x^{2g+1}+1$, there exists $m \in \mathbb{N}$ satisfying $p^m \equiv -1 \pmod{4g+2}$ and that, in the case $P(x)=x(x^{2g}+1)$, there exists $m \in \mathbb{N}$ satisfying $p^m \equiv -1$ or $1+2g \pmod{4g}$.

Then, in [3, 4, 6], we have studied the L-function $L(u)$ of K and shown that $L(u)$ is given by

$$L(u)=\prod_{j=1}^{\alpha}\{1+(pu^2)^{n_j/2}\}^{b_j}$$

for suitable positive integers α, b_j, and even n_j.

As is well-known, the class number h of K is given by $h=L(1)$, (see Eichler [1] , and Hasse [2]). So we can get

$$h=\prod_{j=1}^{\alpha}\{1+p^{n_j/2}\}^{b_j}.$$

In this note, as the application of these formulas to both the L-function relation and the class number relation, we will prove the following theorems.

---

* Department of Mathematics, College of General Education, Kyushu University, Fukuoka 810, Japan

THEOREM 1. *Let g be a positive integer such that $(f, p)=1$ where $f=2g+1$. Assume that there exists $m \in \mathbb{N}$ such that $p^m \equiv -1 \pmod{2f}$ and that there exists $n \in \mathbb{N}$ such that $(p^n-1, 2f)=2(p^n-1, f)>2$. Put $f'=(p^n-1, f)$. Denote by $K=\mathbb{F}(x, y)$ and $K'=\mathbb{F}(x, y)$ hyperelliptic function fields defined by $y^2=x^f+1$ and $y^2=x^{f'}+1$ over $\mathbb{F}$ respectively. Then the L-function of K is divisible by the one of K'.*

THEOREM 2. *Let g be a positive integer such that $(f, p)=1$ where $f=2g$. Assume that there exists $m \in \mathbb{N}$ such that $p^m \equiv -1$ or $1+2g \pmod{2f}$ and that there exists $n \in \mathbb{N}$ such that $(p^n-1, 2f)=2(p^n-1, f)>2$. Put $f'=(p^n-1, f)$. Denote by $K=\mathbb{F}(x, y)$ and $K'=\mathbb{F}(x, y)$ hyperelliptic function fields defined by $y^2=x(x^f+1)$ and $y^2=x(x^{f'}+1)$ over $\mathbb{F}$ respectively. Then the L-function of K is divisible by the one of K'.*

The following result follows at once from Theorems 1 and 2.

COROLLARY. *Notations and assumtions being same as in Theorem 1 or 2, the class number of K is divisible by the one of K'.*

Remark. Madan [5] has got the divisibility relation between L-functions in Galois extension of algebraic function fields. In our case of Theorem 1, K is an algebraic (not necessarily Galois) extension of K' and our consideration is done without relating to him because we treat very special type of algebraic function fields. Also, in our case, the quotient of the L-function of K divided by the one of K' is given explicitely and so is the quotient of the class numbers.

2. Notations and Some Lemmas

In this section we will review some notations and their properties which were obtained in [6]. Let g be a positive integer and p a prime number. Put $f=2g+1$ or $f=2g$. Then we assume that there exists $m \in \mathbb{N}$ satisfying $p^m \equiv -1 \pmod{2f}$ for $f=2g+1$ or that there exists $m \in \mathbb{N}$ satisfying $p^m \equiv -1$ or $1+f \pmod{2f}$ for $f=2g$. Moreover denote by k the minimum of such m's.

We write, for every $n \in \mathbb{N}$,

$$\varepsilon_n=(p^n-1, 2f), \quad \delta_n=(p^n-1, f),$$

and set

$$D=\{\delta_n ; n \in \mathbb{N}, \varepsilon_n=2\delta_n>2\}$$

and $\alpha=\#D$ (the cardinal number of the set D).

Furthermore, for each $d_j \in D$, we denote by n_j the minimum of n's such that $\varepsilon_n=2\delta_n=2d_j$. By renumbering, we may assume that

$$n_1 < n_2 < \cdots < n_\alpha$$

and we put

$$N=\{n_1, n_2 \cdots, n_\alpha\}, \quad D=\{d_1, d_2, \cdots, d_\alpha\},$$

where $d_j=\delta_{n_j}$, These definitions lead to the following lemmas.

LEMMA 1. (i) *If* $n_j \in N$ *then* $2 \mid n_j$ *and* n_j *is the minimum of* n*'s satisfying* $p^n \equiv 1 \pmod{2d_j}$.

(ii) *Let* $d_i, d_j \in D$; *then* $d_i \mid d_j \Leftrightarrow n_i \mid n_j$.

(iii) *Let* $d_j \in D$ *and* $n \in \mathbb{N}$; *then* $d_j \mid \delta_n \Leftrightarrow n_j \mid n$.

LEMMA 2. (i) *If* $p^k \equiv -1 \pmod{2f}$ *then* $p^{n_j/2} \equiv -1 \pmod{2d_j}$ *for all* $n_j \in N$.

(ii) *If* $f=2g$ *and* $p^k \equiv 1+f \pmod{2f}$ *then* $p^{n_j/2} \equiv 1+d_j \pmod{2d_j}$ *for all* $n_j \in N$.

3. Proofs of Theorems

Let the assumptions and notations be same as in Theorem 1 or 2 and in § 2. Since $(p^n-1, 2f)=2(p^n-1, f)>2$ and $f'=(p^n-1, f)$, there exist $d_l \in D=\{d_1, d_2, \cdots, d_\alpha\}$ and $n_l \in N=\{n_1, n_2, \cdots, n_\alpha\}$ satisfying $f'=d_l=(p^{n_l}-1, f)$. We will put $k'=n_l/2$.

Then Lemma 1 shows that $2k'$ is the minimum of n's satisfying $p^n \equiv 1 \pmod{2f'}$ and Lemma 2 also shows that if $p^k \equiv -1 \pmod{2f}$ then $p^{k'} \equiv -1 \pmod{2f'}$ and if $p^k \equiv 1+f \pmod{2f}$ then $p^{k'} \equiv 1+f' \pmod{2f'}$. So we can define ε'_n, δ'_n, D' and N' in place of ε_n, δ_n, D and N as follows.

We write $\varepsilon'_n=(p^n-1, 2f')$, $\delta'_n=(p^n-1, f')$ for every $n \in \mathbb{N}$ and put

$$D'=\{\delta'_n ; n \in \mathbb{N}, \varepsilon'_n=2\delta'_n>2\}=\{d'_1, d'_2, \cdots, d'_\beta\}.$$

where $\beta=\#D'$.

For $d'_t \in D'$ $(1 \leqq t \leqq \beta)$, we denote by n'_t the minimum of n's such that $\varepsilon'_n=2\delta'_n=2d'_t$. By renumbering, we put

$$N'=\{n'_1, n'_2, \cdots, n'_\beta\}$$

where $n'_1<n'_2<\cdots<n'_\beta$ and $d'_t=\delta'_{n'_t}=(p^{n'_t}-1, f')$. Moreover we set

$$N(n_j)=\{n_i \in N ; n_i \mid n_j\} \quad \text{and} \quad D(d_j)=\{d_i \in N ; d_i \mid d_j\}.$$

Then, from Lemma 1, we can easily prove the following lemma.

LEMMA 3. *The sets* N' *and* D' *coincide with the sets* $N(n_l)$ *and* $D(d_l)$ *respectively.*

PROOF of THEOREM 1. Let $L(u)$ be the L-function of K. Then we get

$$L(u)=\prod_{j=1}^{\alpha}\{1+(pu^2)^{n_j/2}\}^{b_j}$$

where $b_j=\frac{1}{n_j}\sum_{n_i \in N(n_j)}\mu(n_i, n_j)(d_i-1)$ $(j=1, 2, \cdots, \alpha)$

and $\mu(x, y)$ means the Möbius function on N, i.e., $\mu(x, y)$ is defined by

(i) $\mu(x, y)=1$ $(x \in N)$

(ii) $\mu(x, y)=0$ $(x, y \in N, x \nmid y)$

(iii) $\sum_{z\in N:\, x\mid z\mid y} \mu(x, z)=0 \quad (x, y\in N, x\mid y, x\neq y)$.

Moreover let $L'(u)$ be the L-function of K' and $\mu'(x, y)$ the Möbius function on N'. Then we also obtain

$$L'(u)=\prod_{j=1}^{\beta}\{1+(pu^2)^{n'_j/2}\}^{b'_j}$$

where $b'_j=\frac{1}{n'_j}\sum_{n'_i\in N'(n'_j)}\mu'(n'_i, n'_j)(d'_i-1)$ $(j=1, 2, \cdots, \beta)$

and $N'(n')=\{n'_i\in N' ; n'_i \mid n'\}$.

Lemma 3 leads to $\mu'(x, y)=\mu(x, y)$ on N' and $N'(n'_j)=N(n'_j)$.
So we see

$$\{b'_1, b'_2, \cdots, b'_\beta\}\subset\{b_1, b_2, \cdots, b_\alpha\}.$$

Therefore we have $L'(u) \mid L(u)$. This completes the proof.

The proof of Theorem 2 is same as the above except for replacing d_i-1 and d'_i-1 by d_i and d'_i.

References

1. M. Eichler, "*Introduction to the theory of algebraic numbers and functions,*" Academic Press, New York-London, 1966.
2. H. Hasse, "*The Riemann hypothesis in algebraic function fields over a finite constants field,*" Pennsylvania, 1968.
3. T. Kodama and T. Washio, *On class numbers of hyperellipitic function fields with Hasse-Witt-invariant zero,* Arch. Math., **49** (1987), 208-213.
4. T. Kodama and T. Washio, *A family of hyperelliptic function fields with Hasse-Witt-invariant zero,* J. Number Theory, **36** (1990), 187-200.
5. M. L. Madan, *Class number relations in fields of algebraic functions,* J. Reine Angew. Math., **238** (1969), 89-92.
6. T. Washio and T. Kodama, *Explicit formulas of L-functions of some hyperelliptic curves,* Sci. Bull. Fac. Educ., Nagasaki Univ., **47** (1992), 1-9.