Sci. Bull. Fac. Educ., Nagasaki Univ., No. 47, pp. 1 ~ 9 (1992)

Explicit formulas of L-functions of some hyperelliptic curves

To the Memory of Professor Koichi Yamamoto

Tadashi WASHIO and Tetsuo KODAMA*

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

(Received Feb. 29, 1992)

Abstract

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 $n\in\mathbb{N}$ satisfying $p^n\equiv -1 \pmod{4g+2}$ and that, in the case $P(x)=x(x^{2g}+1)$, there exists $n\in\mathbb{N}$ satisfying $p^n\equiv -1$ or $1+2g \pmod{4g}$.

Then, it is shown that the L-function $L(u)$ of K 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.

The proof is done by calculations of the number of points on the curves in suitable constant field extentions of K and by the Möbius's inversion formula instead of using the techniques of Weil.

1. INTRODUCTION

Let $\mathbb{F}=GF(q)$ be a finite field of characteristic $p>2$. Let K be an algebraic function field of genus $g>0$ over $\mathbb{F}$. We will denote by $L(u)$ its L-function, i.e., the numerator of its zeta-function $Z(s)$. Then it is put in the form

$$\begin{aligned}L(u)&=a_0+a_1u+a_2u^2+\cdots+a_{2g}u^{2g}\\&=(1-\omega_1u)(1-\omega_2u)\cdots(1-\omega_{2g}u)\end{aligned}$$

where $a_i\in\mathbb{Z}$, $a_0=1$, $a_{2g-i}=q^{g-i}a_i$ $(i=0,\ldots g)$ and $\omega_i\in\mathbb{C}$ $(i=1,\ldots,2g)$.

The so-called Riemann hypothesis means that ω_i can be written as

---

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

$\omega_i=\gamma_i q^{1/2}$, $|\gamma_i|=1$ $(i=1,2,\ldots,2g)$ (see Eichler [1], Ch. V, § 4 and Hasse [2], Ch. IV).

Let us assume that $K=\mathbb{F}(x,y)$ is a hyperelliptic function feld defined by $y^2=P(x)$ where $P(x)$ is a polynomial over $\mathbb{F}$ of the form

$$P(x)=x^{2g+1}+a \text{ with } (2g+1,p)=1 \text{ and } a\in\mathbb{F}^\times \text{ or}$$
$$P(x)=x(x^{2g}+a) \text{ with } (2g,p)=1 \text{ and } a\in\mathbb{F}^\times.$$

Then, in [7], we have proved that all γ_1, $\gamma_2,\ldots,\gamma_{2g}$ are roots of unity if and only if there exists $n\in\mathbb{N}$ satisfying $p^n\equiv -1 \pmod{4g+2}$ in the case $P(x)=x^{2g+1}+a$ or satisfying $p^n\equiv -1$ or $1+2g \pmod{4g}$ in the case $P(x)=x(x^{2g}+a)$.

We will study the explicit formulas of the $L(u)$'s for these cases which have a decomposition with integral polynomial factors and are useful to calculate the class number of K. In this paper, we will determine such formulas in the essential case of $q=p$ and $a=1$. These formulas are 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.

In [9], A. Weil has already considered curves of the form $y^e=\gamma x^f+\delta$, where γ, $\delta\in GF(p^m)$ satisfying $p\nmid ef$, and shown

$$L(u)=\prod_{a,b}L_{a,b}(u), \qquad \text{where } L_{a,b}(u)=1+\zeta j\, u^d$$

with a root of unity ζ and a Jacobi sum j for suitable integers a,b,d. Our proof is done by calculations of the number of points on the curves in suitable constant field extentions of K and by using the Möbius's inversion formula instead of using the techniques of Weil.

To do so, we will state several notaions and some lemmas concerned at them in § 2 and prepare some lemmas for the Jacobi sums in § 3. The desired results about $L(u)$'s for $P(x)=x^{2g+1}+1$ and $P(x)=x(x^{2g}+1)$ will be given in §§ 4 and 5 respectively.

2. Notations and Some Lemmas

In this section we will give some notations and their properties which will be used in §§ 4 and 5. 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; thus $2k$ means the order of p modulo $2f$. We write, for every $n\in\mathbb{N}$,

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

It is clear that if $n \equiv m \pmod{2k}$ or $n=(m, 2k)$ then $\varepsilon_n = \varepsilon_m$ and $\delta_n = \delta_m$. Moreover the equality $\varepsilon_n = 2\delta_n$ is equivalent to $\mathrm{ord}_2(p^n-1) > \mathrm{ord}_2 f$, where $\mathrm{ord}_2 z$ means the number of times 2 dividing z.

Now we set

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

and $\alpha = \#\mathrm{D}$ (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

$$n_1 < n_2 < \ldots < n_\alpha$$

and we put

$$N = \{n_1, n_2, \ldots, n_\alpha\} \text{ and } D = \{d_1, d_2, \ldots, d_\alpha\}, \text{ where } d_j = \delta_{n_j} \quad (1 \leqq j \leqq \alpha).$$

Clearly $n_j \mid 2k$, $d_j \mid f$, $n_\alpha = 2k$ and $d_\alpha = f$. These definitions lead to the following lemma.

LEMMA 2.1. (i) *If $n_j \in N$ then 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 $d_j \mid \delta_n \Leftrightarrow n_j \mid n$.*

Since we can easily prove that $n_j \mid 2k$ and $2n_j \nmid 2k$ for $n_j \in N$, we see the following lemma.

LEMMA 2.2. $\mathrm{ord}_2 n_j = \mathrm{ord}_2 2k$ *for all $n_j \in N$; especially $2 \mid n_j$.*

LEMMA 2.3. (i) *If $p^k \equiv -1 \pmod{2f}$ then $p^{n_j/2} \equiv -1 \pmod{2d_j}$ and $\varepsilon_{n_j/2} = 2$ for all $n_j \in N$.*

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

PROOF. Because of $2n_j \nmid 2k$, we can put $2k = 2n_j u + 2v$ ($u, v \in \mathbb{Z}$, $0 < v < n_j$). From $n_j \mid 2k$ we get $n_j \mid 2v$ and so $v = n_j/2$; consequently $p^k \equiv p^{n_j/2} \pmod{2d_j}$.

Case (i) Obviously $p^{n_j/2} \equiv -1 \pmod{2d_j}$. Also, since $n_j/2 \mid k$ and $\varepsilon_k = 2$, we have $\varepsilon_{n_j/2} = 2$.

Case (ii) Evidently $p^{n_j/2} \equiv 1 + f \pmod{2d_j}$. Since $d_j \mid f$ and n_j is the minimum of n's such that $p^n \equiv 1 \pmod{2d_j}$ we get $p^{n_j/2} \equiv 1 + d_j \pmod{2d_j}$. Thus we see $d_j \mid \delta_{n_j/2} \mid \delta_{n_j}$ and hence $d_j = \delta_{n_j/2}$

We will now define the notation $N(n)$ for $n \in \mathbb{N}$ by

$$N(n) = \{n_j \in N; \ n_j \mid n\}.$$

Then the following lemma follows from Lemma 2.1.

LEMMA 2.4. *If $N(n) \neq \emptyset$ and n_j is the largest number contained in $N(n)$ then $d_j = \delta_n$ and $N(n) = N(n_j)$.*

We can regard the set $N = (n_1, n_2, \ldots, n_\alpha)$ as a partially ordered set with respect to the divisibility relation and so we can define the Möbius function $\mu(x,y)$ on N, i.e.,

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

(ii) $\mu(x,y) = 0 \quad (x,y \in N,\ x \not| y)$,

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

Then, by making use of the Möbius's inversion formula, we obtain the following lemma.

LEMMA 2.5. *Let $d_1', d_2', \ldots, d_\alpha'$ be α given real numbers. Then the solution $(x_1, x_2, \ldots, x_\alpha)$ of a system of linear equations*

$$\sum_{n_i \in N(n_j)} n_i x_i = d_j' \quad (j = 1,2,\ldots,\alpha)$$

is given by

$$x_j = \frac{1}{n_j} \sum_{n_i \in N(n_j)} \mu(n_i, n_j)\, d_i' \quad (j = 1,2,\ldots,\alpha)$$

3. Jacobi Sums

In this section we will give some lemmas for the Jacobi sums. Let $\mathbb{K}$ be a finite field. Then a Jacobi sum in $\mathbb{K}$ with respect to multiplicative characters σ and ν of $\mathbb{K}$ is given by

$$J(\sigma,\nu) = \sum_{u+v=1} \sigma(u)\nu(v)$$

with the summation extended over all pairs (u, v) of elements of $\mathbb{K}$ satisfying $u+v=1$.

The general theory of the Jacobi sums may be found in B.C. Berndt and R.J. Evans [1], H. Davenport and H. Hasse[2], K. Ireland and M. Rosen[5] and R. Lidl and H. Niederreiter[8]. In [7], we have known the following results. ([7],p.192 and p.196).

LEMMA 3.1. *Let p be a prime number and n a positive integer. Let $\mathbb{K} = GF(p^{2n})$. Suppose that $d>1$ is an odd integer satisfying $p^n \equiv -1 \pmod{2d}$. If λ is a multiplicative character of order d of $\mathbb{N}$ then*

$$J(\lambda^j, \lambda^j) = p^n \text{ for } j = 1,2,\ldots,\ d-1.$$

LEMMA 3.2. *Let p be a prime number and n a positive integer. Let $\mathbb{K} = GF(p^{2n})$. Suppose that $d>1$ is an even integer satisfying $p^n \equiv -1$ or $1+d \pmod{2d}$. If λ is*

a multiplicative character of order $2d$ and η is the quadratic character of $\mathbb{K}$ then

$$\lambda^{2j+1}(-1)\,J(\lambda^{2j+1},\eta)=p^n \quad \textit{for } j=0,1,\ldots,\ d-1.$$

4. L-Function for $P(x)=x^f+1$

Let $\mathbb{F}=GF(p)$ be a prime field of characteristic $p>2$ and $K=\mathbb{F}(x,y)$ a hyperelliptic function field defined by $y^2=x^f+1$ where $f=2g+1$ and $(f,\ p)=1$. We will denote by $L(u)$ its L-function and put

$$L(u)=(1-\omega_1 u)\ (1-\omega_2 u)\ \cdots\ (1-\omega_{2g}u).$$

Let $L_n(u)=a_0^{(n)}+a_1^{(n)}u+a_2^{(n)}u^2+\cdots+a_{2g}^{(n)}u^{2g}$ be the L-function of the constant field extension of K of degree n. Then it is well-known that

$$L_n(u)=(1-\omega_1{}^n u)\ (1-\omega_2{}^n u)\cdots(1-\omega_{2g}{}^n u)\ \text{(see [3], [4])}.$$

Now we assume that there exists $m\in\mathbb{N}$ such that $p^m\equiv -1 \pmod{2f}$ and denote by k the minimum of such m's.

LEMMA 4.1. *Let notations be same as in § 2 and let $n\in\mathbb{N}$.*

(i) *If $N(n)=\emptyset$ then $a_1^{(n)}=0$.*

(ii) *If $N(n)\neq\emptyset$ then $a_1^{(n)}=(-1)^{n/m-1}(d-1)\ p^{n/2}$,*

where m is the largest number contained in $N(n)$ and $d=\delta_m$.

PROOF. Put $q=p^n$ and $\mathbb{K}=GF(q)$. Then, as is well known, $a_1^{(n)}$ is given by

$$a_1^{(n)}=\sum_{v\in\mathbb{P}_1}\eta(v^f+1)=\sum_{j=1}^{d-1}\lambda^j(-4)J(\lambda^j,\lambda^j)$$

where η is the quadratic character of $\mathbb{K}$ and λ is a multiplicative character of $\mathbb{K}$ of order $d=\delta_n$. Clearly, if $N(n)=\emptyset$ then $d=1$ and so $a_1^{(n)}=0$.

Suppose that $N(n)\neq\emptyset$. Since Lemma 2.4 leads to $d=\delta_m=\delta_n$ we obtain

$$J(\lambda^j,\lambda^j)=(-1)^{n/m-1}\ J(\sigma^j,\sigma^j)^{n/m},$$

where σ is a multiplicative character of $GF(p^m)$ of order d such that σ is lifted to λ ; $\lambda=\sigma\circ\mathrm{Norm}$.

Then, from Lemmas 2.2 and 2.3, we see $2\mid m$ and $p^{m/2}\equiv -1 \pmod{2d}$. So it follows from Lemma 3.1 and $\sigma^j(-4)=1$ that

$$\sigma^j(-4)\ J(\sigma^j,\sigma^j)=p^{m/2}.$$

Therefore we get

$$\begin{aligned}\lambda^j(-4)J(\lambda^j,\lambda^j) &= (-1)^{n/m-1}\{\sigma^j(-4)J(\sigma^j,\ \sigma^j)\}^{n/m}\\ &= (-1)^{n/m-1}\ p^{n/2}\end{aligned}$$

and hence

$$a_1^{(n)}=(-1)^{n/m-1}(d-1)\ p^{n/2}.$$

THEOREM 1. *Let* $\mathbb{F}=GF(p)$ *be a prime field of characteristic* $p>2$ *and* $K=\mathbb{F}(x, y)$ *a hyperelliptic function field defined by* $y^2=x^f+1$ *where* $f=2g+1$ *and* $(f, p)=1$. *Assume that there exists* $m\in\mathbb{N}$ *such that* $p^m\equiv -1 \pmod{2f}$. *Let notations*

$$N=\{n_1, n_2,\ldots, n_\alpha\} \text{ and } D=\{d_1, d_2,\ldots, d_\alpha\}$$

be same as in §2. *Then the L-function of K is given by*

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

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

PROOF. From Lemma 3.5 and the definition of b_i, we see

$$\sum_{n_i\in N(n_j)} b_i n_i=d_j-1 \quad (j=1,2\ldots,\alpha).$$

For $n\in\mathbb{N}$ we will define c_n by

$$c_n=\begin{cases} 0 & \text{if } N(n)=\emptyset, \\ p^{n/2}\sum_{n_i\in N(n)}(-1)^{n/n_i-1}b_i n_i & \text{if } N(n)\neq\emptyset. \end{cases}$$

In the case $N(n)\neq\emptyset$, if we denote by n_j the largest number contained in $N(n)$, then, from Lemma 2.4, we have $N(n)=N(n_j)$. Since Lemma 2.2 leads to $\mathrm{ord}_2 n_i=\mathrm{ord}_2 n_j$ for $n_i\in N(n_j)$ we get $n/n_i\equiv n/n_j \pmod 2$. Thus

$$\begin{aligned} c_n &= (-1)^{n/n_j-1}p^{n/2}\sum_{n_i\in N(n_j)} b_i n_i \\ &= (-1)^{n/n_j-1}(d_j-1)p^{n/2}. \end{aligned}$$

Thus Lemma 4.1 shows that $c_n=a_1^{(n)}$ for $n\in\mathbb{N}$. Hence it follows that

$$\begin{aligned} \log L(u) &= -\sum_{n=1}^{\infty}(\omega_1{}^n+\cdots+\omega_{2g}{}^n)u^n/n \\ &= \sum_{n=1}^{\infty} a_1^{(n)}u^n/n=\sum_{n=1}^{\infty} c_n u^n/n \\ &= \sum_{j=1}^{\alpha}\sum_{s=1}^{\infty}(-1)^{s-1}b_j n_j(p^{n_j/2}u^{n_j})^s/sn_j \\ &= \sum_{j=1}^{\alpha}\log\{1+(pu^2)^{n_j/2}\}^{b_j}, \end{aligned}$$

and so we have the desired formula.

The notations being as in Theorem 1, the following results follow at once from the straightforward calculations.

Numerical example. Let $g=269$ and $p=61$. Then $f=539$, $k=105$, $\alpha=5$, $N=\{6, 10,$

30, 42, 210}, $D=\}$, $D=\{7, 11, 77, 49, 539\}$, and so

$$L(u)=(1+p^3u^6)\ (1+p^5u^{10})\ (1+p^{15}u^{30})^2\ (1+p^{21}u^{42})\ (1+p^{105}u^{210})^2.$$

COROLLARY 1. *If* $k=2^r\ (r\geqq 0)$, *then* $\alpha=1$, $N=\{2k\}$, $D=\{f\}$, *and*

$$L(u)=\{1+(pu^2)^k\}^{g/k}.$$

COROLLARY 2. *If* f *is a prime number satisfying* $f\neq p$ *and the order of* p *modulo* $2f$ *is even, then* k *is the half order of* p *modulo* $2f$, $\alpha=1$, $N=\{2k\}$, $D=\{f\}$, *and*

$$L(u)=\{1+(pu^2)^k\}^{g/k}.$$

COROLLARY 3. *If* $f=\ell^r\ (\ell:$ *odd prime,* $r>0)$ *and* p *is a primitive root modulo* $2f$, *then* $k=(\ell-1)\ell^{r-1}/2$, $\alpha=r$, $N=\{\ell-1,\ldots,\ (\ell-1)\ell^{j-1},\ldots,\ 2k\}$, $D=\{\ell,\ldots,\ \ell^j,\ \ldots,\ f\}$ *and*

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

where $n_j=(\ell-1)\ell^{j-1}$.

5. L-Function for $P(x)=x(x^f+1)$

Let $\mathbb{F}=GF(p)$ be a prime field of characteristic $p>2$ and $K=\mathbb{F}(x,y)$ a hyperelliptic function field defined by $y^2=x(x^f+1)$ where $f=2g$ and $(f,\ p)=1$, We will denote by $L(u)$ its L-function.

Let $L_n(u)=a_0^{(n)}+a_1^{(n)}u+a_2^{(n)}u^2+\cdots+a_{2g}^{(n)}u^{2g}$ be the L-function of the constant field extension of K of degree n.

Throughout this section, we assume that there exists $m\in\mathbb{N}$ such that $p^m\equiv -1$ or $1+f\ (\mathrm{mod}\ 2f)$ and denote by k the minimum of such m's.

LEMMA 5.1. *Let notations be same as in* § 2 *and let* $n\in\mathbb{N}$.

(i) *If* $N(n)=\emptyset$ *then* $a_1^{(n)}=0$.

(ii) *If* $N(n)\neq\emptyset$ *then* $a_1^{(n)}=(-1)^{n/m-1}\,d\,p^{n/2}$,

where m *is the largest number contained in* $N(n)$ *and* $d=\delta_n$.

PROOF. Put $q=p^n$ and $\mathbb{K}=GF(q)$. Then, as is well known, $a_1^{(n)}$ is given by the Jacobsthal sum

$$a_1^{(n)}=\sum_{v\in\mathbb{K}}\eta\,(v(v^f+1))$$

where η is the quadratic character of $\mathbb{K}$. Thus if $N(n)=\emptyset$ then $a_1^{(n)}=0$ and if $N(n)\neq\emptyset$ then

$$a_1^{(n)}=\sum_{j=0}^{d-1}\lambda^{2j+1}(-1)J(\lambda^{2j+1},\eta).$$

where λ is a multiplicative character of $\mathbb{K}$ of order $2d=2\delta_n$.

In the case $N(n)\neq\emptyset$, Lemma 2.4 gives us $d=\delta_m=\delta_n$ and so we have

$$J(\lambda^{2j+1},\eta)=(-1)^{n/m-1}J(\sigma^{2j+1},\nu)^{n/m},$$

where ν is the quadratic character and σ is a multiplicative character of $GF(p^m)$ of order $2d$ such that σ is lifted to λ ; $\lambda=\sigma\circ$ Norm.

Then, from Lemmas 2.2 and 2.3, we see $2|m$ and $p^{m/2}\equiv-1$ or $1+d \pmod{2d}$. So Lemma 3.2 leads to

$$\sigma^{2j+1}(-1)\,J(\sigma^{2j+1},\nu)=p^{m/2}.$$

Therefore we obtain

$$\begin{aligned}\lambda^{2j+1}(-1)\,J(\lambda^{2j+1},\eta) &= (-1)^{n/m-1}\{\sigma^{2j+1}(-1)\,J(\sigma^{2j+1},\nu)\}^{n/m}\\ &= (-1)^{n/m-1}p^{n/2}\end{aligned}$$

and so we get the desired assertion

$$a_1^{(n)}=(-1)^{n/m-1}\,d\,p^{n/2}.$$

The proof of the following theorem is same as the proof of Theorem 1 with the exception of replacing Lemma 4.1 by Lemma 5.1.

THEOREM 2. *Let $\mathbb{F}=GF(p)$ be a prime field of characteristic $p>2$ and $K=\mathbb{F}(x,y)$ a hyperelliptic function field defined by $y^2=x(x^f+1)$ where $f=2g$ and $(f,\ p)=1$. Assume that there exists $m\in\mathbb{N}$ such $p^m\equiv-1$ or $1+f \pmod{2f}$. Let the notations*

$$N=\{n_1,\ n_2,\ldots,\ n_\alpha\}\ \text{and}\ D=\{d_1,\ d_2,\ldots,\ d_\alpha\}$$

be same as in §2. Then the L-function of K is given by

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

where $b_j=\dfrac{1}{n_j}\displaystyle\sum_{n_i\in N(n_j)}\mu(n_i,\ n_j)\,d_i\quad(j=1,2,\ldots,\alpha)$.

Let the notations be as in Theorem 2. Then we can also get easily the following results.

COROLLARY 1. *If $k=2^r(r\geqq0)$, then $\alpha=1$, $N=\{2k\}$, $D=\{f\}$, and*

$$L(u)=\{1+(pu^2)^k\}^{g/k}.$$

COROLLARY 2. *If $2g=p^{2^r}-1$, $(r>0)$, then $k=2^r$ and*

$$L(u)=\{1+(pu^2)^k\}^{g/k}.$$

COROLLARY 3. *If $g=\ell$ (ℓ : odd prime) and $k>1$ then, $\alpha=2$, $N=\{2,\ 2k\}$, $D=\{2,\ f\}$, and*

$$L(u)=(1+pu^2)\{1+(pu^2)^k\}^{(g-1)/k}.$$

COROLLARY 4. *If* $2g=p^{\ell^r}-1$, (ℓ : *odd prime*, $r>0$), *then* $k=\ell^r$, $\alpha=r+1$, $N=\{2, 2\ell^i,\ldots, 2k\}$, $D=\{p-1,\ldots, p^{\ell^i}-1,\ldots f\}$, *and*

$$L(u)=\prod_{i=0}^{r}\{1+(pu^2)^{\ell^i}\}^{b_i},$$

where $b_i=(p^{\ell^i}-p^{\ell^{i-1}})/2\ell^i$.

Remark. The fact that the numbers b_j ($j=1,2,\ldots, \alpha$) which appear in Theorems 1 and 2 are positive integers follows from the fact that $L(u)$ is a polynomial and from induction on α.

References

1. B.C. Berndt and R.J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory **11** (1979), 349-398.
2. H. Davenport and H. Hasse, *Die Nullstellen der kongruenzzeta-funktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151-182.
3. M. Eichler, "*Introduction to the theory of algebraic numbers and functions*," Academic Press, New York-London, 1966.
4. H. Hasse, "*The Riemann hypothesis in algebraic function fields over a finite constants field*," Pennsylvania, 1968.
5. K. Ireland and M. Rosen, "*A classical introduction to modern number theory*," Springer, New York-Heidelberg-Berlin, 1982.
6. T. Kodama and T. Washio, *On class numbers of hyperelliptic function fields with Hasse-Witt-invariant zero*, Arch. Math. **49** (1987), 208-213.
7. T. Kodama and T. Washio, *A family of hyperelliptic function fields with Hasse-Witt-invariant zero*, J. Number Theory **36** (1990), 187-200.
8. R. Lidl and H. Niederreiter, "*Finite fields*," Addison-Wesley, Reading, MA, 1983.
9. A. Weil, *Jacobi sums as "Grössencharaktere"*, Trans. Amer. Math. Soc. **73** (1952), 487-495 .