On Class Numbers of Hyperelliptic Function Fields, II

Tadashi WASHIO

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

(Received Oct. 31, 1979)

Abstract

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 $y^2 = x^n - a$ ($a \neq 0, a \in F$), where $n$ means an odd number so that $n > 1$ and $p \nmid n$. Let $h$ be the class number of $K$ and $g$ the genus of $K$. Then, it is obvious that $h = p + 1$ if $n = 3$ and $p \equiv 2 \mod 3$. This particular fact can be generally expressed as follows:

Given $n$, there exists an integer $c$ such that $h = (p + 1)g$ whenever $p \equiv c \mod n$.

In this note, it is shown that this generalization is true in the particular case of $n = 5$ and of $n = 7$.

1. Introduction. Let $F = GF(p)$ be a finite prime field of characteristic $p \neq 2$. Let $n$ be an odd number satisfying $n > 1$ and $p \nmid n$. Throughout this note, $K = F(x, y)$ means an algebraic function field over $F$ defined by an equation $y^2 = x^n - a$ ($a \neq 0, a \in F$). If we denote by $g$ the genus of $K$, it is obvious that $g = (n-1)/2$.

Let $h$ be the class number of $K$, i.e., the order of the finite group of divisor classes of degree zero. We will then discuss the following question:

Does there exist an integer $c$ which depends only on $n$ such that $h = (p + 1)g$ whenever $p \equiv c \mod n$?

In the case of $n = 3$, we had an answer in the affirmative. ([5], Theorem 1 (i)). When $h = p^e + 1$ then the similar question was discussed. ([6]). In this note, we wish to give an answer only in the case of $n = 5$ and of $n = 7$. In doing so, we will recall a method of estimating class numbers of algebraic function fields without proofs but with references.

Let $L(u) = 1 + a_1 u + a_2 u^2 + \cdots + p^{e-1} a_{e-1} u^{e-1} + p^e a_0 u^e$ be the $L$-function of $K$. Then it is obvious that $h = L(1)$. As is well known, the explicit expression for coefficients $a_i$, $a_2$ and $a_3$ can be put in the form
\[ \begin{align*}
2a_t &= N_t - (2p+1)N_t + 2N_t + 2p \\
6a_t &= N_t - 3(p+1)N_t + (3p-1)N_t - 6(p+1)N_t + 6N_t + 6N_t
\end{align*} \]

where \( N_d \) means the number of prime divisors of degree \( d \) of \( K \). (M.L.Madan and C.S.Queen [2], p. 427).

Thus, for our present purpose, it is enough to compute \( N_d \). Since \( N_d \) depends on the number of prime divisors of degree one in some constant field extensions of \( K \), in § 2 we will investigate the number \( N(K_d) \) of prime divisors of degree one of an algebraic function field \( K_d \) over a finite field \( F_d \). In § 3, we will compute \( h \) in the case of \( n=5 \) and of \( n=7 \).

### 2. The number of prime divisors of degree one.

Let \( K_d \) be the constant field extension of \( K \) of degree \( d \) and let \( F_d \) be the finite field \( GF(p^d) \) with \( p^d \) elements. Let us denote by \( N(K_d) \) the number of prime divisors of degree one of \( K_d \). We will then consider \( N(K_d) \) under the assumption \( p \equiv -1 \mod n \).

**THEOREM 1.** If \( d \equiv 1 \mod 2 \) and \( p \equiv -1 \mod n \), then the equality \( N(K_d) = p^d + 1 \) holds.

**PROOF.** By the definition of \( N(K_d) \), we have

\[ N(K_d) = 1 + \# \{(a, \beta) \in F_d \times F_d ; \beta^3 = a^a - a \} \]

So we need to estimate the last term in this formula. Since our assumptions \( d \equiv 1 \mod 2 \) and \( p \equiv -1 \mod n \) lead to \( (p^d - 1, n) = 1 \), we can get \( F_d^* = F_d \) in view of the fact that \( F^* = F_d - \{0\} \) is a cyclic group of order \( p^d - 1 \). This implies that

\[ \# \{(a, 0) \in F_d \times F_d ; a^a = a \} = 1 \]

and

\[ \# \{(a, \beta) \in F_d \times F_d ; \beta \neq 0, \beta^3 = a^a - a \} = p^d - 1. \]

Therefore we have \( N(K_d) = 1 + 1 + p^d - 1 = p^d + 1 \).

We will now consider \( N(K_d) \) in the case of \( d = 2 \).

**THEOREM 2.** If \( p \equiv -1 \mod n \) and \( n = 2g + 1 \), then \( N(K_2) = p^2 + 2gp + 1 \) holds.

We will prepare some lemmas for the proof of this theorem. The following lemma will be proved on the basis of the properties of Hasse-Witt matrices of the algebraic function field \( K_d \) over \( F_d \).

**LEMMA 1.** If \( p \equiv -1 \mod n \), then \( N(K_d) \equiv 1 \mod p \) for an arbitrary positive integer \( d \).

**PROOF.** For \( 0 \leq u, v \leq g - 1 \), let \( A_{u,v} \) be the coefficient of \( x^{v+1} \) in the following polynomial

\[ \psi((x-a)(x+1)^r x^{u+1}) = \psi(\sum \binom{(p-1)}{r} \binom{(p-1)}{r} \binom{(p-1)}{r} (-a)^{(p-1)/2} x^{nr+u+1}) \]

where \( \psi \) means the \( p^{-1} \)-linear operator satisfying

\[ \psi(x^w) = \begin{cases} 
\frac{x^w}{p} & \text{if } p \mid w \\
0 & \text{otherwise.}
\end{cases} \]

The matrix \( A = (A_{u,v}) \) is called the Hasse-Witt matrix. (L.Miller [3]). Since it is easy in our case to show that \( nr + u + 1 \neq p(v+1) \) for every \( 0 \leq u, v \leq g - 1 \), we
have $A_n=0$ i.e., $A=0$. Therefore the desired assertion $N(K_2)\equiv 1 \mod p$ follows at once from $A=0$.([4], Theorem).

**LEMMA 2.** If $p\equiv -1 \mod n$, then $N(K_2)\equiv 0 \mod 2$ and $N(K_2)\equiv 3 \mod n$ hold.

**PROOF.** Since $(p-1,n)=1$, we get $\#\{\alpha \in F_1=GF(p) : \alpha^n=a\} = 1$. This lead to $\#\{\alpha \in F_1 : \alpha^n=a\} = n$, because $F_1$ contains, in our case, an $n$th primitive root of unity.

Moreover, it is clear that $\#\{\alpha, \beta \in F_1 \times F_1 : \beta^2=\alpha^n-a, \beta \neq 0\} \equiv 0 \mod 2$. Hence we get the first part of the lemma as follows.

$$N(K_2) = 1 + \#\{(\alpha, \beta) \in F_1 \times F_1 : \beta^2=\alpha^n-a\} \equiv 1 + n \equiv 0 \mod 2.$$

We will now prove the second assertion. Since $F_1$ contains an $n$th primitive root of unity, we have

$$\#\{\alpha, \beta \in F_1 \times F_1 : \alpha^n=\beta^2+a, \alpha \neq 0\} \equiv 0 \mod n.$$

Therefore, because of $\#\{\beta \in F_1 : \beta^2=-a\} = 2$, we get

$$N(K_2) = 1 + \#\{(0, \beta) \in F_1 \times F_1 : \beta^2=-a\} + \#\{(\alpha, \beta) \in F_1 \times F_1 : \alpha \neq 0, \beta^2=\alpha^n-a\} \equiv 1 + 2 = 3 \mod n.$$

This completes the proof of the lemma.

Now let us turn to the proof of Theorem 2.

**PROOF of Theorem 2.** As is well known, the inequalities $p^2+1-2gp \leq N(K_2) \leq p^2+1+2gp$ hold. ([M. Eichler[1], p. 306]. Therefore Lemma 1 and the first part of Lemma 2 lead to

$$N(K_2) = p^2 + 1 + mp \ (m=0, \pm 2, \pm 4, \ldots, \pm 2g).$$

Using the second part of Lemma 2, we have $p^2+1+mp \equiv 3 \mod n$. Therefore we can easily get $m=2g$ because of our assumptions $p \equiv -1 \mod n$ and $n=2g+1$. Hence we have our assertion $N(K_2) = p^2+1+2gp$.

3. Results. Let us now consider the question in §1 only in the case of $n=5$ and $n=7$. In fact, we can answer our question in the case of $n=5$ in the affirmative as follows.

**THEOREM 3.** Let $F=GF(p)$ be a finite prime field of characteristic $p \neq 2$. Let $K=F(x,y)$ be a hyperelliptic function field over $F$ defined by an equation $y^2=x^3-a \ (a \neq 0, a \in F)$. Denote by $h$ the class number of $K$. If $p \equiv 4 \mod 5$, then $h=(p+1)^3$ and $L(u)=1+2pu^2+p^2u^3$. 

**PROOF.** Applying Theorem 1 to $d=1$ we have $N_i = N(K_i) = p+1$. Moreover, applying Theorem 2 to $g=2$, we have $N(K_i) = p^2+4p+1$. So we get $N_i = p(p+3)/2$ in view of the fact that the relation among $N_i$, $N_2$ and $N(K_2)$ is given by $N(K_2) = N_i+2N_2$. Therefore, by making use of the formula (1), we can easily obtain $a_i=0, a_2=2p, L(u)=1+2pu^2+p^2u^3$ and $h=L(1)=(p+1)^3$.

Finally we will give an affirmative answer to our question in the case of $n=7$.

**THEOREM 4.** Let $F=GF(p)$ be a finite prime field of characteristic $p \neq 2$. Let $K=F(x,y)$ be a hyperelliptic function field over $F$ defined by an equation $y^2=x^3-a \ (a \neq 0, a \in F)$. Denote by $h$ the class number of $K$. If $p \equiv 6 \mod 7$, then $h=(p+1)^3$.
and \( L(u) = 1 + 3pu^3 + 3p^2u^4 + p^3u^6 \).

**Proof.** As applications of Theorem 1 to \( d=1 \) and \( d=3 \), we have \( N_1 = N(K_1) = p+1 \) and \( N(K_3) = p^3+1 \). Consequently the formula \( N(K_2) = N_1 + 3N_2 \) leads to \( N_2 = (p^3-p)/3 \). Similarly, applying Theorem 2 to \( g = 3 \), we have \( N(K_3) = p^3 + 6p + 1 \). Therefore the formula \( N(K_2) = N_1 + 2N_2 \) also leads to \( N_2 = (p^3 + 5p)/2 \).

Hence, by means of the formula (1), it is easy to check on \( a_i = a_3 = 0, a_1 = 3p, L(u) = 1 + 3pu^3 + 3p^2u^4 + p^3u^6 \) and \( h = L(1) = (p+1)^3 \). This completes the proof of the theorem.

**References**