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 \( F = \text{GF}(p) \) 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 \( F = \text{GF}(p) \) 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 \( h = p^g + 1 \) 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 \( L(u) = 1 + a_1 u + a_2 u^2 + \cdots + p^{g-1} a_g u^{g-1} + p^g a_g u^g \) be the \( L \)-function of \( K \). Then it is obvious that \( h = L(1) \). As is well known, the explicit expression for coefficients \( a_1, a_2 \) and \( a_g \) can be put in the form
\begin{align}
\begin{cases}
a_1 &= N_1 - (p+1) \\
2a_2 &= N_1^2 - (2p+1)N_1 + 2N_2 + 2p \\
6a_3 &= N_1^3 - 3pN_1^2 + (3p-1)N_1 - 6(p+1)N_2 + 6N_3 + 6N_4
\end{cases}
\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

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

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

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

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 \( N(K_g) = p^g + 2gp + 1 \) 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 \( x^{u+v} \) in the following polynomial

\[
\psi((x-a)(x^{-1})^{p^u}x^{u+v}) = \psi(\sum_{r=0}^{(p-1)/2} r^{(p-1)/2} r^{(p-1)/2} (-a)^{r^2} x^{r^2 u+v})
\]

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

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

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 $A_{u,v} = 0$ i.e., $A = 0$. Therefore the desired assertion $N(K_d) = 1 \mod p$ follows at once from $A = 0$ ([4], Theorem).

**Lemma 2.** If $p = -1 \mod n$, then $N(K_3) = 0 \mod 2$ and $N(K_4) = 3 \mod n$ hold.

**Proof.** Since $(p-1,n) = 1$, we get $\#(x \in F_4; x = a) = 1$. This leads to $\#(x \in F_4; x = a) = n$, because $F_4$ contains, in our case, an $n$th primitive root of unity.

Moreover, it is clear that $\#(x \in F_4; x = a) = n$, because $F_4$ contains an $n$th primitive root of unity.

We will now prove the second assertion. Since $F_4$ contains an $n$th primitive root of unity, we have

$$\#(x \in F_4; x = a) = n,$$

Therefore, because of $\#(x \in F_4; x = a) = n$, we get

$$N(K_3) = 1 + \#(x \in F_4; x = a) = 1 + n = 0 \mod 2.$$

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 $p^2 + 1 - 2g \leq N(K_3) \leq p^2 + 1 + 2g p$ hold ([M. Eichler [1], p. 306]). Therefore Lemma 1 and the first part of Lemma 2 lead to

$$N(K_3) = p^2 + 1 + mp \quad (m = 0, \pm 2, \pm 4, \ldots, \pm 2g).$$

Using the second part of Lemma 2, we have $p^2 + 1 + mp \equiv 0 \mod n$. 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 $N(K_3) = p^2 + 1 + 2g p$.

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 $y^2 = x^3 - a \quad (a \neq 0, a \in F)$. Denote by $h$ the class number of $K$. If $p \equiv 4 \mod 5$, then $h = (p+1)^3$ and $L(u) = 1 + 2pu + p^3$.

**Proof.** Applying Theorem 1 to $d = 1$ we have $N_1 = N(K_3) = p + 1$. Moreover, applying Theorem 2 to $g = 2$, we have $N(K_3) = p^2 + 4p + 1$. So we get $N_1 = p(p+3)/2$ in view of the fact that the relation among $N_1$, $N_2$ and $N(K_3)$ is given by $N(K_3) = N_1 + 2N_2$. Therefore, by making use of the formula (1), we can easily obtain $a_1 = 0$, $a_2 = 2p$, $L(u) = 1 + 2pu + p^3$ 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 $y^2 = x^3 - a \quad (a \neq 0, a \in F)$. Denote by $h$ the class number of $K$. If $p \equiv 6 \mod 7$, then $h = (p+1)^3$.
and \( L(u) = 1 + 3pu^2 + 3pu'u + p'u'. \)

PROOF. As applications of Theorem 1 to \( d = 1 \) and \( d = 3 \), we have \( N_i = N(K_i) = p + 1 \) and \( N(K_3) = p^3 + 1 \). Consequently the formula \( N(K_3) = N_i + 3N_3 \) leads to \( N_i = \frac{(p^3 - p)}{3} \). Similarly, applying Theorem 2 to \( g = 3 \), we have \( N(K_3) = p^3 + 6p + 1 \). Therefore the formula \( N(K_3) = N_i + 2N_3 \) also leads to \( N_i = \frac{(p^3 + 5p)}{2} \).

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

References