ACTA ARITHMETICA
102.3 (2002)

Class numbers of cyclotomic function fields

by

Sunghan Bae and Pyung-Lyun Kang (Taejon)

0. Introduction. Let $\mathbb{A} = \mathbb{F}_q[T]$ be the ring of polynomials over a finite field $\mathbb{F}_q$ with q elements, and $k = \mathbb{F}(T)$. We assume that $q > 2$. For each $M \in \mathbb{A}$ one uses the Carlitz module to construct a field extension $k(M)$, called the *Mth cyclotomic function field*, and its real subfield $k^+(M)$. It is well known that the divisor class number $h(M)$ of $k(M)$ is divisible by the class number $h^+(M)$ of $k^+(M)$. Write $h^-(M) = h(M)/h^+(M)$. We call $h^-(M)$ the *first factor* or *relative class number*, and $h^+(M)$ the *second factor* or *real class number* of $k(M)$.

In a recent paper Guo and Shu [GS] studied $h^-(P^n)$ and $h^+(P^n)$, where P is an irreducible polynomial in $\mathbb{A}$. Shu obtained very useful formulas for these factors as products of character sums. We use these formulas to obtain upper bounds for these factors in the case of prime cyclotomic function fields, modifying the method of Feng [F].

In the classical case there are certain matrices, called the Maillet matrix and Dem'yanenko matrix, whose determinants are very closely related to the first factor of the class number. We define some matrices analogous to those matrices, which are easy to define and easy to handle. Adopting the ideas of Wang [W] and Hazama [H] and using the formulas of Shu we can express $h^-(P^n)$ and $h^+(P^n)$ as the determinants of those matrices. The matrices are useful to compute the class numbers in many cases. We use them to improve the lower bound of [GS, Theorem 3.1].

In the final section we find all the possible polynomials M with $h^-(M) = 1$ when q is odd. The cases of $h(M)$ and $h^+(M)$ are given in [KM].

1. Basic facts and notations. Let M be a polynomial in $\mathbb{A}$. It is well known that the Galois group G of $k(M)$ over k is isomorphic to $(\mathbb{A}/M)^*$. Thus characters on G can be regarded as characters on $(\mathbb{A}/M)^*$. A character

2000 *Mathematics Subject Classification*: 11R58, 11R29.

χ is called *real* if its restriction to $\mathbb{F}_q^*$ is trivial, and *nonreal* otherwise. For a polynomial $N \in \mathbb{A}$ we let $\mathcal{N}_N$ (resp. $\mathcal{M}_N$) be the set of all polynomials (resp. monic polynomials) in $\mathbb{A}$ with degree less than the degree of N and prime to N. Let $\phi(N) = |\mathcal{N}_N|$. It is known that (cf. [GS])

$$h^-(M) = \prod_{\chi\ \mathrm{nonreal}} \Big(\sum_{A \in \mathcal{M}_{f_\chi}} \chi(A) \Big), \tag{1}$$

$$h^+(M) = \prod_{\chi\ \mathrm{real},\, \chi \neq \mathrm{id}} \Big(- \sum_{A \in \mathcal{M}_{f_\chi}} \deg A \chi(A) \Big), \tag{2}$$

where f_χ is the conductor of χ. When $M = P^n$, a power of an irreducible P, then the formulas can be written as

$$h^-(P^n) = \prod_{\chi\ \mathrm{nonreal}} \Big(\sum_{A \in \mathcal{M}} \chi(A) \Big), \tag{3}$$

$$h^+(P^n) = \prod_{\chi\ \mathrm{real},\, \chi \neq \mathrm{id}} \Big(- \sum_{A \in \mathcal{M}} \deg A \chi(A) \Big), \tag{4}$$

where $\mathcal{M} = \mathcal{M}_M$.

From the formulas (1) and (2), we see that if $M \mid N$, then $h^-(M) \mid h^-(N)$ and $h^+(M) \mid h^+(N)$.

2. Upper bounds for prime cyclotomic function fields. In this section we follow the method of [F] to obtain upper bounds for $h^-(P)$ and $h^+(P)$, where P is an irreducible polynomial of degree d. Further, $\mathcal{M} = \mathcal{M}_P$.

THEOREM 1. *Let $r = |\mathcal{M}| = (q^d - 1)/(q-1)$. We have*

$$h^-(P) \le r^{(q-2)r/2}$$

and

$$h^+(P) \le \bigg(\sum_{A \in \mathcal{M}} (\deg A)^2 - \frac{1}{r-1} \sum_{A, B \in \mathcal{M},\, A \neq B} \deg A \cdot \deg B \bigg)^{(r-1)/2}.$$

Proof. Let χ_0 be any generator of the group of characters of $(\mathbb{A}/P)^*$. We write characters of $(\mathbb{A}/P)^*$ in the form $\chi = \chi_0^{(q-1)i+k}$, $1 \le i \le r$, $0 \le k \le q-2$. Let $A, B \in \mathcal{M}$. For $0 \le k \le q-2$,

$$\sum_{i=1}^{r} \chi_0^{(q-1)i-k}(A) \overline{\chi}_0^{(q-1)i-k}(B) = \eta^{-k} \sum_{i=1}^{r} \eta^{q-1} = \begin{cases} r\eta^{-k} & \text{if } \eta^{q-1} = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where $\eta = \chi_0(A/B)$. Thus

$$\sum_{\chi\,\text{nonreal}} \chi(A)\overline{\chi}(B) = \begin{cases} r\sum_{k=1}^{q-2}\eta^{-k} & \text{if } \eta^{q-1}=1,\\ 0, & \text{otherwise,}\end{cases}$$
$$= \begin{cases} r(q-2) & \text{if } \eta = 1,\\ -r & \text{if } \eta^{q-1}=1 \text{ and } \eta\neq 1,\\ 0 & \text{otherwise.}\end{cases}$$

Then

$$\begin{aligned} h^-(P)^{2/(r(q-2))} &= \prod_{\chi\,\text{nonreal}} \Big|\sum_{A\in\mathcal{M}} \chi(A)\Big|^{2/(r(q-2))}\\ &= \prod_{\chi\,\text{nonreal}} \Big(\sum_{A,B\in\mathcal{M}} \chi(A)\overline{\chi}(B)\Big)^{1/(r(q-2))}\\ &\le \frac{1}{r(q-2)} \sum_{\chi\,\text{nonreal}} \Big(\sum_{A,B\in\mathcal{M}} \chi(A)\overline{\chi}(B)\Big)\\ &= \frac{1}{r(q-2)} rr(q-2) = r. \end{aligned}$$

The equality in the last line of above equation comes from the fact that there is no element in $\mathcal{M}$ whose order in $(\mathbb{A}/P)^*$ is $q-1$. Hence

$$h^-(P) \le r^{(q-2)r/2}.$$

For h^+ we proceed as follows. As for h^-, we have

$$\sum_{\chi\,\text{real},\,\chi\neq\text{id}} \chi(A)\overline{\chi}(B) = \begin{cases} r-1 & \text{if } \eta^{q-1}=1,\\ -1 & \text{otherwise.}\end{cases}$$

Then

$$\begin{aligned} h^+(P)^{2/(r-1)} &\le \frac{1}{r-1} \sum_{A,B\in\mathcal{M}} \deg A\cdot\deg B \sum_{\chi\,\text{real},\,\chi\neq\text{id}} \chi(A)\overline{\chi}(B)\\ &= \sum_{A\in\mathcal{M}} (\deg A)^2 - \frac{1}{r-1}\sum_{A,B\in\mathcal{M},\,A\neq B} \deg A\cdot\deg B, \end{aligned}$$

which implies the result.

Corollary. (i) *If* $\deg P = 1$, *then* $h^-(P)=1$ *and* $h^+(P)=1$.
(ii) *If* $\deg P = 2$, *then* $h^+(P)=1$.

Proof. (i) is trivial. If $d=2$, then $r=q+1$. Then

$$\sum_{A\in\mathcal{M}} (\deg A)^2 - \frac{1}{r-1}\sum_{A,B\in\mathcal{M},\,A\neq B} \deg A\cdot\deg B = q - \frac{q(q-1)}{q} = 1.$$

3. Determinant formulas for $h^-(P^n)$ and $h^+(P^n)$. In this section we let $M = P^n$, $e = nd$ the degree of M, and $r = \phi(M)/(q-1)$. Let $\mathcal{N} = \mathcal{N}_M$ and $\mathcal{M} = \mathcal{M}_M$. Write

$$\mathcal{M} = \{A_1, \ldots, A_r\}.$$

For each polynomial A prime to M, define $\operatorname{sgn}(A)$ to be the leading coefficient of A and $\operatorname{sgn}_M(A) = \operatorname{sgn}(B)$, where $B \equiv A \bmod M$ with $\deg B < e$. Define $\delta(A) \in \mathbb{Z}$ to be 1 if $\operatorname{sgn}_M(A) = 1$ and 0 otherwise. We denote by A' an inverse of A modulo M. Define $r \times r$ matrix

$$K = (\operatorname{sgn}_M(A_i A_j')).$$

Fix a character $\psi : \mathbb{F}_q^* \to \mathbb{C}$ of order $q-1$. For each $k = 1, \ldots, q-2$ define

$$K^{(k)} = \overline{\psi}^k(K),$$

and a $(q-2)r \times (q-2)r$ matrix

$$\mathcal{K} = \begin{pmatrix} K^{(1)} & 0 & & 0 \\ 0 & K^{(2)} & & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & K^{(q-2)} \end{pmatrix}.$$

THEOREM 2. $h^-(M) = \det \mathcal{K} = \prod_{k=1}^{q-2} \det K^{(k)}$.

Proof. For each k with $1 \le k \le q-2$, let $\{\chi_1^{(k)}, \ldots, \chi_r^{(k)}\}$ be the set of all the characters of $(\mathbb{A}/M)^*$ whose restriction to $\mathbb{F}_q^*$ is equal to ψ^k. Let

$$\Omega^{(k)} = \frac{1}{\sqrt{r}}(\chi_i^{(k)}(A_j)), \qquad \Omega = \begin{pmatrix} \Omega^{(1)} & 0 & & 0 \\ 0 & \Omega^{(2)} & & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & \Omega^{(q-2)} \end{pmatrix}.$$

From the orthogonality relation among characters we can see that Ω is a unitary matrix. Then we have

$$\det \mathcal{K} = \det(\Omega \mathcal{K} \Omega^*) = \prod_{k=1}^{q-2} \det\left(\frac{1}{r} x_{ij}^{(k)}\right),$$

where

$$x_{ij}^{(k)} = \sum_{A \in \mathcal{M}} \sum_{B \in \mathcal{M}} \chi_i^{(k)}(A) \overline{\psi}^{(k)}(\operatorname{sgn}_M(AB')) \overline{\chi}_j^k(B).$$

Note that

$$\begin{aligned}
&\sum_{A\in\mathcal{N}}\sum_{B\in\mathcal{N}}\chi_i^{(k)}(A)\delta(AB')\overline{\chi}_j^{(k)}(B)\\
&\quad=\sum_{C\in\mathcal{N}}\sum_{B\in\mathcal{N}}\chi_i^{(k)}(CB)\delta(C)\overline{\chi}_j^{(k)}(B)\\
&\quad=\Big(\sum_{B\in\mathcal{N}}\chi_i^{(k)}(B)\overline{\chi}_j^{(k)}(B)\Big)\Big(\sum_{C\in\mathcal{N}}\delta(C)\chi_i^{(k)}(C)\Big)=\delta_{ij}\phi(M)\sum_{A\in\mathcal{M}}\chi_i^{(k)}(A).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\sum_{A\in\mathcal{N}}\sum_{B\in\mathcal{N}}\chi_i^{(k)}(A)\delta(AB')\overline{\chi}_j^{(k)}(B)\\
&\quad=\sum_{A\in\mathcal{M}}\sum_{B\in\mathcal{M}}\Big(\sum_{\alpha\in\mathbb{F}_q^*}\sum_{\beta\in\mathbb{F}_q^*}\psi^k(\alpha)\overline{\psi}^k(\beta)\delta(\alpha\beta^{-1}AB')\Big)\chi_i^{(k)}(A)\overline{\chi}_j^{(k)}(B)\\
&\quad=(q-1)\sum_{A\in\mathcal{M}}\sum_{B\in\mathcal{M}}\chi_i^{(k)}(A)\overline{\psi}^k(\mathrm{sgn}_M(AB'))\overline{\chi}_j^{(k)}(B)=(q-1)x_{ij}^{(k)}.
\end{aligned}$$

Therefore we have

$$x_{ij}^{(k)}=\delta_{ij}r\sum_{A\in\mathcal{M}}\chi_i^{(k)}(A).$$

Then

$$\det\mathcal{K}=\prod_{k=1}^{q-2}\det\Big(\delta_{ij}\sum_{A\in\mathcal{M}}\chi_i^{(k)}(A)\Big)=\prod_{\chi\text{ nonreal}}\sum_{A\in\mathcal{M}}\chi(A)=h^-(M).$$

This theorem gives an easy way of computing the relative class numbers.

EXAMPLE 1. Let $q=3$ and $M=T^2+1$. Then with $\mathcal{M}=\{1,T,T+1,T-1\}$ we have

$$K=\begin{pmatrix}1&-1&1&1\\1&1&-1&1\\1&-1&1&-1\\1&1&1&1\end{pmatrix}$$

and $h^-(M)=\det\mathcal{K}=8$.

EXAMPLE 2. Let $q=4$ and $M=T^2+\alpha T+1$ where α is a generator of $\mathbb{F}_4^*$. Then

$$K=\begin{pmatrix}1&1&1+\alpha&1&1+\alpha\\1&1&1+\alpha&\alpha&\alpha\\1&1&1&1+\alpha&1\\1&\alpha&\alpha&1&1+\alpha\\1&1+\alpha&1&1&1\end{pmatrix},$$

$\det K^{(1)} = \frac{9}{2} + \frac{27\sqrt{3}}{2}i$, $\det K^{(2)} = \frac{9}{2} - \frac{27\sqrt{3}}{2}i$, and $h^-(M) = \det \mathcal{K} = 567 = 3^4 \cdot 7$.

We will see from the Corollary to Theorem 4 below that the irreducible polynomials in the above examples are regular.

Example 3. Let $q = 5$ and $M = T^2 + T + 1$. Then

$$K = \begin{pmatrix} 1 & -1 & -1 & -2 & -2 & 2 \\ 1 & 1 & 1 & -2 & 1 & -1 \\ 1 & -1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 2 & 1 & 1 & 2 \\ 1 & -2 & -1 & -1 & 1 & -2 \\ 1 & 2 & -2 & 2 & -2 & 1 \end{pmatrix},$$

$\det K^{(1)} = 92 + 60i$, $\det K^{(3)} = 92 - 60i$, $\det K^{(2)} = 160$, and $h^-(M) = \det \mathcal{K} = 2^{10} \cdot 5 \cdot 13 \cdot 29$. Thus M is irregular.

Example 4. Let $q = 3$ and $M = T^3 + T^2 - 1$. Then $h^-(M) = 2^{12} \cdot 5 \cdot 79$.

For the prime ℓ dividing $q-1$, we improve the lower bound for the ℓ-part of the relative class number given in [GS, Theorem 3.1].

Theorem 3. *Let ℓ be a prime factor of $q-1$ and ℓ^c be the highest power of ℓ dividing $q-1$. Then $\ell^{c(r-1)}$ divides $h^-(M)$, and so $(q-1)^r$ divides $h^-(M)$.*

Proof. Write $q - 1 = \ell^c m$. Let ζ be a primitive ℓ^cth root of 1. Then the entries of $K^{(\ell^i km)}$, with $0 \le i \le c$, $(k, \ell) = 1$ and $0 < k < \ell^{c-i}$, are the powers of ζ^{ℓ^i} and the first column of $K^{(\ell^i km)}$ is $(1, \dots, 1)^t$. If we subtract the first column from the other columns, then the entries in the other columns are divisible by $1 - \zeta^{\ell^i}$, whose absolute value is ℓ^a, where $a = 1/(\ell^{c-i} - \ell^{c-i-1})$, since ℓ is totally ramified in $\mathbb{Q}(\zeta^{\ell^i})$. Then $\det K^{(\ell^i km)}$ is divisible by $\ell^{a(r-1)}$. Multiplying all these we conclude that $\det \mathcal{K}$ is divisible by $\ell^{c(r-1)}$, since there are $\ell^{c-i} - \ell^{c-i-1}$ such k's.

Remark. In the examples above $\ell^{c(r-1)}$ is the highest power of ℓ dividing $h^-(M)$. It is interesting to know whether this fact is always true as is mentioned in [IS].

Corollary. $h^-(P^n) = 1$ *if and only if* $\deg P = 1$ *and* $n = 1$.

The second factor can be treated similarly. We keep the notations as before. For each polynomial $A \in \mathbb{A}$, prime to M we define $\deg_M(A)$ to be the degree of the polynomial B which is congruent to A modulo M with degree less than the degree of M. Define an $r \times r$ matrix

$$L = (\deg_M(AB'))_{A,B \in \mathcal{M}}.$$

Let $\{\chi_1, \dots, \chi_r\}$ be the set of all the real characters modulo M with $\chi_1 = \mathrm{id}$ and let

$$\Lambda = \frac{1}{\sqrt{r}}(\chi_i(A_j)).$$

Let

$$d(M) = \sum_{A \in \mathcal{M}} \deg_M(A) = \sum_{A \in \mathcal{M}} \chi_1(A) \deg_M(A).$$

A similar process to that for the first factor replacing Ω by Λ, $h(AB')$ by $\deg_M(AB')h(AB')$ will give

THEOREM 4. $h^+(M) = \frac{1}{d(M)}|\det L|$.

Note that Theorem 4 also holds for $q = 2$, in which case $h(M) = h^+(M)$.

COROLLARY. *If* $\deg P = 2$, *then* $h^+(P) = 1$.

Proof. One can see easily that the matrix L is a $(q+1) \times (q+1)$ matrix such that its diagonal entries are 0 and all the other entries are 1. By elementary row and column operations we can see that $\det L = (-1)^q q$. Since $d(P) = q$, we get the result.

EXAMPLE 5. Let $q = 3$ and $P = T^3 - T + 1$. Then with

$$\mathcal{M} = \{1, T, T+1, T-1, T^2, T^2+1, T^2-1, T^2+T, T^2+T+1, \\ T^2+T-1, T^2-T, T^2-T+1, T^2-T-1\}$$

we have

$$L = \begin{pmatrix}
0 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 2 & 2 \\
1 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 1 & 2 \\
1 & 2 & 0 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 2 & 2 & 2 \\
1 & 2 & 2 & 0 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 \\
2 & 1 & 2 & 2 & 0 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 2 \\
2 & 2 & 2 & 2 & 2 & 0 & 1 & 2 & 2 & 2 & 2 & 1 & 1 \\
2 & 2 & 1 & 1 & 2 & 2 & 0 & 2 & 2 & 1 & 2 & 2 & 2 \\
2 & 1 & 1 & 2 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 1 \\
2 & 2 & 2 & 1 & 2 & 2 & 2 & 1 & 0 & 2 & 2 & 1 & 2 \\
2 & 2 & 2 & 2 & 1 & 1 & 2 & 1 & 2 & 0 & 2 & 2 & 2 \\
2 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 0 & 2 & 2 \\
2 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 1 & 0 & 2 \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 0
\end{pmatrix},$$

$\det L = 3^{10} \cdot 7$ and $d(P) = 21$. Thus $h^+(P) = 3^9$.

Similarly, for $P = T^3 + T^2 - 1$, $h^+(P) = 53 \cdot 313$.

REMARK. It is mentioned in [IS] that a computer program to calculate the class numbers of the subfields of $k(P)$ has been devised by R. D. Small. From Theorems 2 and 4 one can construct another program to calculate $h^+(P^n)$ and $h^-(P^n)$.

4. Polynomial M with $h^-(M) = 1$. In this section we assume that q is odd. From the Corollary of Theorem 3, $h^-(M) = 1$ only if M is square-free and divisible only by irreducible polynomials of degree 1.

PROPOSITION 5. *If three distinct irreducibles divide M, then $2 \mid h^-(M)$.*

Proof. Let P_1, P_2 and P_3 be distinct irreducible polynomials of degree 1 dividing M. Let χ_i be the quadratic character modulo P_i and $\chi = \chi_1\chi_2\chi_3$. Then χ is a nonreal character with conductor $N = P_1P_2P_3$. Now consider

$$\sum_{A\in\mathcal{M}_N} \chi(A).$$

Each term in the sum is either 1 or -1 and there are $|\mathcal{M}_N| = (q-1)^2$ terms, which is an even number. Thus $\sum_{A\in\mathcal{M}_N} \chi(A)$ is even and nonzero, and we get the result.

COROLLARY. *Suppose that q is odd. Then $h^-(M) = 1$ if and only if M is one of the following types*:

(i) $M = P$, *where P is an irreducible polynomial of degree* 1.

(ii) $q = 3$ *and* $M = P_1P_2$, *where P_1 and P_2 are distinct irreducible polynomials of degree* 1.

Proof. From Proposition 5 we only have to consider the case $M = P_1P_2$ with $\deg P_1 = \deg P_2 = 1$. When $q = 3$, one can compute easily from the formula (1) that $h^-(M) = 1$. Now assume that $q > 3$. From [KM, Theorem 3(b)], $h^+(M) = 1$, but from [KM, Theorem 4(c)], $h(M) > 1$. Thus $h^-(M) > 1$ in this case.

PROPOSITION 6. *Assume that $q \equiv 1 \bmod 4$ and $M = P_1P_2$ with $P_1 \neq P_2$, $\deg P_1 = \deg P_2 = 1$. Then $h^-(M)$ is divisible by* 2.

Proof. Let χ_i be a generator of the group of characters modulo P_i. Let $q - 1 = 4m$ and

$$\chi = \chi_1^m\chi_2^m.$$

Then χ is nonreal with conductor M. The values of χ lie in the set $\{\pm1, \pm i\}$ and there are $q - 1$ elements in $\mathcal{M}$. For each $a \in \{\pm1, \pm i\}$ let m_a be the number of $A \in \mathcal{M}$ with $\chi(A) = a$. Then

$$\sum_{A\in\mathcal{M}} \chi(A) = (m_1 - m_{-1}) + (m_i - m_{-i})i.$$

Since $m_1 + m_{-1} + m_i + m_{-i} = q-1$, which is even, $m_1 - m_{-1}$ and $m_i - m_{-i}$ must have the same parity. Thus 2 must divide $|\sum_{A\in\mathcal{M}} \chi(A)|^2$, and so 2 divides $h^-(M)$.

References

[F] K. Feng, *On the first factor of the class number of cyclotomic field*, Proc. Amer. Math. Soc. 84 (1982), 479–482.

[GS] L. Guo and L. Shu, *Class numbers of cyclotomic function fields*, Trans. Amer. Math. Soc. 351 (1999), 4445–4467.

[H] F. Hazama, *Demjanenko matrix*, *class numbers*, *and Hodge group*, J. Number Theory 34 (1990), 174–177.

[IS] K. F. Ireland and R. D. Small, *Class numbers of cyclotomic function fields*, Math. Comp. 46 (1986), 337–340.

[KM] M. Kida and N. Murabayashi, *Cyclotomic function fields with divisor class number one*, Tokyo J. Math. 14 (1991), 45–56.

[W] K. Wang, *On Maillet determinant*, J. Number Theory 18 (1984), 306–312.

Department of Mathematics
KAIST
Taejon 305-701, South Korea
E-mail: shbae@mathx.kaist.ac.kr

Department of Mathematics
Chungnam National University
Taejon 305-764, South Korea
E-mail: plkang@math.chungnam.ac.kr

Received on 21.3.2000
and in revised form on 12.7.2001 (3782)