ACTA ARITHMETICA
138.3 (2009)

A determinant formula for congruence zeta functions of maximal real cyclotomic function fields

by

DAISUKE SHIOMI (Nagoya)

1. Introduction. Let k be a field of rational functions over a finite field $\mathbb{F}_q$ with q elements. Fix a generator T of k, and let $R = \mathbb{F}_q[T]$ be the polynomial subring of k. Let M be a monic polynomial in R, and Λ_M be the M-torsion of the Carlitz module. The field k_M obtained by adding the points of Λ_M to k is called the Mth cyclotomic function field. For the definition of the Carlitz module and basic facts on cyclotomic function fields, see Section 2 below. Let k_M^+ be a "maximal real subfield" of k_M which is the decomposition field of the infinite prime of k in k_M/k.

Define $h_{k_M^+}$ to be the order of the divisor class group of degree 0 for k_M^+. Bae and Kang obtained a determinant formula for $h_{k_M^+}$ in [1]. For the field k_M^+, the congruence zeta function $\zeta(s, k_M^+)$ is expressed by

$$\zeta(s, k_M^+) = \frac{P_{k_M^+}(q^{-s})}{(1-q^{-s})(1-q^{1-s})} \tag{1}$$

where $P_{k_M^+}(X)$ is a polynomial with integral coefficients, and $P_{k_M^+}(1) = h_{k_M^+}$ (cf. [5, p. 130]).

The purpose of this paper is to give a determinant formula for $P_{k_M^+}(X)$ (see Section 3). Since $P_{k_M^+}(1) = h_{k_M^+}$, our formula is a generalization of the determinant formula for $h_{k_M^+}$. As an application, we calculate some low coefficients of $P_{k_M^+}(X)$ by using the first and second derivatives of a determinant (see Section 4).

2. Basic facts. In this section, we recall some basic properties of cyclotomic function fields and their congruence zeta functions. For details, see [2, 3, 4].

2000 *Mathematics Subject Classification*: 11M38, 11R60.
Key words and phrases: congruence zeta function, cyclotomic function fields.

DOI: 10.4064/aa138-3-3

2.1. *Cyclotomic function fields.* Let $\mathrm{End}(k^{\mathrm{ac}})$ be the $\mathbb{F}_q$-algebra of endomorphisms of the additive group of the algebraic closure k^{ac} of k. The Frobenius automorphism φ $(x \mapsto x^q)$ and the T-multiplication μ_T $(x \mapsto T \cdot x)$ are elements of $\mathrm{End}(k^{\mathrm{ac}})$. We define

$$x^M := M(\varphi + \mu_T)(x) \tag{2}$$

for $x \in k^{\mathrm{ac}}$ and $M \in R$. Then k^{ac} becomes an R-module with the above action.

For a monic polynomial $M \in R$, let Λ_M be the set of all x satisfying $x^M = 0$, which is a cyclic R-submodule of k^{ac}. We have the following isomorphism of R-modules:

$$R/M \to \Lambda_M \ (A \bmod M \mapsto \lambda^A) \tag{3}$$

where λ is one of the generators of Λ_M.

Let $(R/M)^\times$ be the group of units of R/M. Let $\Phi(M)$ be the order of $(R/M)^\times$. By using the previous isomorphism, we see that $\Phi(M)$ is the number of generators of Λ_M.

Let k_M be the field obtained by adding the elements of Λ_M to k, which is called the Mth *cyclotomic function field*. Then k_M is an abelian extension of k. Fix a generator λ of Λ_M. We get the following isomorphism:

$$(R/M)^\times \to \mathrm{Gal}(k_M/k) \ (A \bmod M \mapsto \sigma_{A \bmod M}) \tag{4}$$

where $\mathrm{Gal}(k_M/k)$ is the Galois group of k_M/k, and $\sigma_{A \bmod M}$ is the isomorphism given by $\sigma_{A \bmod M}(\lambda) = \lambda^A$. The extension degree of k_M/k is $\Phi(M)$. We see that $\mathbb{F}_q^\times$ is contained in $(R/M)^\times$, and let k_M^+ be the subfield of k_M corresponding to $\mathbb{F}_q^\times$. We call k_M^+ the *maximal real subfield* of k_M. The extension degree of k_M^+/k is $\Phi(M)/(q-1)$. If M is a monic polynomial of degree 1, then $k_M^+ = k$.

For a monic polynomial $M \in R$, let X_M be the group of all primitive Dirichlet characters of $(R/M)^\times$. We call χ the *real character* if $\chi(a) = 1$ for any $a \in \mathbb{F}_q^\times$. Let X_M^+ be the set of real characters contained in X_M. Let $\mathbb{D}$ be the group of all primitive Dirichlet characters. Put

$$\tilde{k} := \bigcup_M k_M \tag{5}$$

where M runs through all monic polynomials in R. By the same argument as in Chapter 3 of [4], we have a one-to-one correspondence between finite subgroups of $\mathbb{D}$ and finite subextension fields of $\tilde{k}/k$, and X_M, X_M^+ corresponds to k_M, k_M^+ respectively.

THEOREM 2.1 (cf. [4, Theorem 3.7]). *Let X be a finite subgroup of $\mathbb{D}$, and L the associated field. For an irreducible monic polynomial $P \in R$, put*

$$Y := \{\chi \in X \mid \chi(P) \neq 0\}, \qquad Z := \{\chi \in X \mid \chi(P) = 1\}.$$

Then

$$\begin{aligned} X/Y &\simeq \textit{the inertia group of } P \textit{ for } L/k, \\ Y/Z &\simeq \textit{the cyclic group of order } f_P, \\ X/Z &\simeq \textit{the decomposition group of } P \textit{ for } L/k, \end{aligned}$$

where f_P is the residue class degree of P in L/k.

2.2. *The congruence zeta function for k_M^+.* For a monic polynomial $M \in R$, let $\mathcal{O}_{k_M^+}$ be the integral closure of R in the field k_M^+. We define $\zeta(s, \mathcal{O}_{k_M^+})$ by

$$\zeta(s, \mathcal{O}_{k_M^+}) := \prod_{\mathcal{P}} \left(1 - \frac{1}{\mathcal{N}\mathcal{P}^s}\right)^{-1} \tag{6}$$

where $\mathcal{P}$ runs through all primes of $\mathcal{O}_{k_M^+}$, and $\mathcal{N}\mathcal{P}$ denotes the number of elements of the residue field of $\mathcal{P}$. By the same argument as in the case of number fields, we have the following proposition.

Proposition 2.1 (cf. [4, Theorem 4.3]).

$$\zeta(s, \mathcal{O}_{k_M^+}) = \prod_{\chi \in X_M^+} L(s, \chi) \tag{7}$$

where the L-function is defined by

$$L(s, \chi) := \prod_{P} \left(1 - \frac{\chi(P)}{\mathcal{N}P^s}\right)^{-1}$$

with P running through all monic irreducible polynomials of R.

The congruence zeta function of k_M^+ is defined by

$$\zeta(s, k_M^+) := \prod_{\mathcal{P}} \left(1 - \frac{1}{\mathcal{N}\mathcal{P}^s}\right)^{-1}$$

where $\mathcal{P}$ runs through all primes of k_M^+. Let P_∞ be the infinite prime of k determined by the unique pole of T. Let e_∞, f_∞, g_∞ be the ramification index in k_M^+/k, the residue class degree, and the number of primes lying above P_∞, respectively. Then we obtain

$$\zeta(s, k_M^+) = \zeta(s, \mathcal{O}_{k_M^+})(1 - q^{-sf_\infty})^{-g_\infty}.$$

Since P_∞ splits completely in k_M^+/k, we get

$$\zeta(s, k_M^+) = \zeta(s, \mathcal{O}_{k_M^+})(1 - q^{-s})^{-\Phi(M)/(q-1)}. \tag{8}$$

3. The determinant formula for $P_{k_M^+}(X)$. The goal of this section is to give a determinant formula for $P_{k_M^+}(X)$.

For a monic polynomial $M \in R$ of degree d ($d \geq 2$), we define $\mathcal{R}_M := (R/M)^\times/\mathbb{F}_q^\times$. For $\alpha \in (R/M)^\times$, let r_α be the element of R satisfying

$$r_\alpha \equiv \alpha \bmod M, \qquad \deg r_\alpha < d,$$

where $\deg A$ denotes the degree of the polynomial A. We define

$$\mathrm{Deg}(\alpha) = \deg r_\alpha. \tag{9}$$

We can easily see that Deg is a function over $\mathcal{R}_M$.

Let $N = \Phi(M)/(q-1) - 1$. We put

$$\mathcal{R}_M = \{1, \alpha_1, \ldots, \alpha_N\},$$

and

$$\begin{aligned} d_i &= \mathrm{Deg}(\alpha_i) && (i = 1, \ldots, N), \\ d_{ij} &= \mathrm{Deg}(\alpha_i \alpha_j^{-1}) && (i, j = 1, \ldots, N). \end{aligned}$$

We define

$$J_{k_M^+}(X) := \prod_{\substack{\chi \in X_M^+ \\ \chi \neq 1}} \prod_{Q \mid M} (1 - \chi(Q) X^{\deg Q}), \tag{10}$$

where Q runs through all irreducible monic polynomials dividing M. We put

$$D_{k_M^+}(X) := \left(\frac{X^{d_{ij}} - X^{d_i}}{1 - X} \right)_{i,j=1,\ldots,N}. \tag{11}$$

Proposition 3.1.

$$J_{k_M^+}(X) = \prod_{Q \mid M} \frac{(1 - X^{f_Q \deg Q})^{g_Q}}{1 - X^{\deg Q}} \tag{12}$$

where Q is an irreducible monic polynomial dividing M and f_Q, g_Q are the residue class degree in k_M^+/k and the number of primes lying over Q, respectively.

Proof. Let Q be an irreducible monic polynomial dividing M, and put

$$Y_Q^+ := \{\chi \in X_M^+ \mid \chi(Q) \neq 0\}, \qquad Z_Q^+ := \{\chi \in X_M^+ \mid \chi(Q) = 1\}.$$

From Theorem 2.1,

$$\begin{aligned}\prod_{\chi\in X_M^+}(1-\chi(Q)X^{\deg Q}) &= \prod_{\chi\in Y_Q^+}(1-\chi(Q)X^{\deg Q})\\ &= \prod_{\chi\in Y_Q^+/Z_Q^+}\prod_{\psi\in Z_Q^+}(1-\chi\psi(Q)X^{\deg Q})\\ &= \Big(\prod_{\chi\in Y_Q^+/Z_Q^+}(1-\chi(Q)X^{\deg Q})\Big)^{g_Q}.\end{aligned}$$

Since Y_Q^+/Z_Q^+ is a cyclic group of order f_Q, we have

$$\prod_{\chi\in Y_Q^+/Z_Q^+}(1-\chi(Q)X^{\deg Q}) = 1-X^{f_Q\deg Q}.$$

Hence we obtain

$$\prod_{\chi\in X_M^+}(1-\chi(Q)X^{\deg Q}) = (1-X^{f_Q\deg Q})^{g_Q}.$$

From the above equality, the desired result follows. ■

From Proposition 3.1, $J_{k_M^+}(X)$ is a polynomial with integral coefficients. Now we can prove the main result of the present paper.

THEOREM 3.1. *Let $M\in R$ be a monic polynomial of degree not less than 2. Then*

$$\det D_{k_M^+}(X) = P_{k_M^+}(X)J_{k_M^+}(X). \tag{13}$$

Proof. For any $\chi\in X_M^+$, let f_χ be the conductor of χ. Define $\tilde\chi$ by

$$\tilde\chi=\chi\circ\pi_\chi$$

where $\pi_\chi:(R/M)^\times\to(R/f_\chi)^\times$ is the natural homomorphism. Then we can easily see that

$$L(s,\tilde\chi)=L(s,\chi)\cdot\prod_{Q|M}(1-\chi(Q)q^{-s\deg Q}).$$

Hence we have

$$\prod_{\substack{\chi\in X_M^+\\ \chi\neq1}}L(s,\tilde\chi)=\Big(\prod_{\substack{\chi\in X_M^+\\ \chi\neq1}}L(s,\chi)\Big)\cdot J_{k_M^+}(q^{-s})=\zeta(s,\mathcal{O}_{k_M^+})(1-q^{1-s})J_{k_M^+}(q^{-s}).$$

By the same argument as in Lemma 3 in [2], if $\chi\neq1$,

$$L(s,\tilde\chi)=\sum_{k=0}^{d-1}\sum_{\substack{\deg A=k\\ A\,\mathrm{monic}}}\tilde\chi(A)q^{-ks}=\sum_{\alpha\in\mathcal{R}_M}\tilde\chi(\alpha)q^{-\operatorname{Deg}(\alpha)s}.$$

Since $\tilde{\chi}$ is real, $\tilde{\chi}$ is a character of $\mathcal{R}_M$. Notice that $\tilde{\chi}$ runs through all characters of $\mathcal{R}_M$ when χ runs through all characters of X_M^+. By the Frobenius determinant formula (cf. [4, Lemma 5.26]),

$$\prod_{\substack{\chi\in X_M^+\\ \chi\neq 1}} L(s,\tilde{\chi}) = \prod_{\substack{\chi\in X_M^+\\ \chi\neq 1}} \sum_{\alpha\in\mathcal{R}_M} \tilde{\chi}(\alpha) q^{-\mathrm{Deg}(\alpha)s} = \det\,(q^{-sd_{ij}} - q^{-sd_i})_{i,j=1,\dots,N}.$$

Since P_∞ splits completely in k_M^+/k, we have

$$\det\left(\frac{q^{-sd_{ij}} - q^{-sd_i}}{1-q^{-s}}\right)_{i,j} = P_{k_M^+}(q^{-s}) J_{k_M^+}(q^{-s}).$$

Putting $X = q^{-s}$, we obtain the desired result. ∎

By applying L'Hôpital's rule, we calculate

$$\left.\frac{X^{d_{ij}} - X^{d_i}}{1-X}\right|_{X=1} = d_i - d_{ij}. \tag{14}$$

We can now use our theorem to rederive the class number formula of Bae and Kang.

Corollary 3.1 (Bae–Kang [1]). *In the notations of Proposition* 3.1, *we have*

$$\det\,(d_i - d_{ij})_{i,j=1,\dots,N} = W_{k_M^+} h_{k_M^+} \tag{15}$$

where

$$W_{k_M^+} = \begin{cases} \prod_{Q\mid M} f_Q & \text{if } g_Q = 1 \text{ for every prime } Q \text{ dividing } M,\\ 0 & \text{otherwise.}\end{cases} \tag{16}$$

Proof. We can calculate

$$\det D_{k_M^+}(X)|_{X=1} = \det\,(d_i - d_{ij})_{i,j=1,\dots,N}, \tag{17}$$

and $W_{K_M^+} = J_M^+(1)$ by Proposition 3.1. Since $P_{k_M^+}(1) = h_{k_M^+}$, we obtain the desired result. ∎

Remark. The corollary applies, in particular, when $M = Q^d$ is a prime power. Since Q is totally ramified in k_M^+/k, we have $g_Q = 1$ and $f_Q = 1$. It follows, in this case, that $h_{k_M^+} = \det\,(d_i - d_{ij})$.

Corollary 3.2. *Let $M \in R$ be a monic polynomial of degree* 2. *Then* $P_{k_M^+}(X) = 1$.

Proof. We have

$$d_i = 1, \qquad d_{ij} = \begin{cases} 0 & \text{if } i = j,\\ 1 & \text{if } i \neq j.\end{cases}$$

It follows that $D_{k_M^+}(X) = I_N$. By Theorem 3.1, $P_{k_M^+}(X) = 1$. ∎

I would like to thank the referee for suggesting the following alternative proof of Corollary 3.2. Using the Riemann–Hurwitz formula, we find that k_M^+ has genus zero in the case of $\deg M = 2$. Thus, we also obtain $P_{K_M^+}(X) = 1$.

We give some examples of $P_{k_M^+}(X)$.

EXAMPLE 3.1. Let $q = 2$ and $M = T^3 \in \mathbb{F}_q[T]$. We put

$$\mathcal{R}_M = \{1,\, \alpha_1 = T+1,\, \alpha_2 = T^2+1,\, \alpha_3 = T^2+T+1\}.$$

As M is a power of an irreducible polynomial, $P_{k_M^+}(X) = \det D_{k_M^+}(X)$. Hence

$$P_{k_M^+}(X) = \det D_{k_M^+}(X) = \begin{vmatrix} 1 & -X & -X \\ X & 1+X & 0 \\ 0 & X & 1+X \end{vmatrix} = 1 + 2X + 2X^2.$$

EXAMPLE 3.2. Let $q = 2$ and $M = T^2(T+1)^2 \in \mathbb{F}_q[T]$. We put

$$\mathcal{R}_M = \{1,\, \alpha_1 = T^2+T+1,\, \alpha_2 = T^3+T+1,\, \alpha_3 = T^3+T^2+1\}.$$

Then

$$\det D_{k_M^+}(X) = \begin{vmatrix} 1+X & -X^2 & -X^2 \\ 0 & 1+X+X^2 & X^2 \\ 0 & X^2 & 1+X+X^2 \end{vmatrix}$$
$$= (1+X+2X^2)(1+X)^2,$$

and

$$J_{k_M^+}(X) = (1+X)^2.$$

Thus, we get

$$P_{k_M^+}(X) = 1 + X + 2X^2.$$

4. Calculating the coefficients of $\det D_{k_M^+}(X)$**.** In this section, we will give a formula for the coefficients of low degree for $\det D_{k_M^+}(X)$.

Let $M \in R$ be a monic polynomial of degree d. Since $\det D_{k_M^+}(0) = 1$, we can write

$$\det D_{k_M^+}(X) = 1 + a_1X + a_2X^2 + \cdots, \tag{18}$$

where a_i $(i = 1, 2, \dots)$ are integers. For $0 \le i < d$, put

$$s_i = \#\{\alpha \in \mathcal{R}_M \mid \deg \alpha = i\}, \qquad t_i = \#\{\alpha \in \mathcal{R}_M \mid \deg \alpha \le i\},$$

where $\#A$ is the number of elements of the set A. We have the following result.

Proposition 4.1. *If* $\deg M \geq 3$, *then*

$$a_1 = \frac{\Phi(M)}{q-1} - t_1, \tag{19}$$

$$a_2 = \frac{1}{2}\left\{\frac{\Phi(M)}{q-1} - 2t_2 + \left(\frac{\Phi(M)}{q-1} - t_1\right)^2 + t_1^2\right\}. \tag{20}$$

To prove this proposition, we first state the following lemma, which can be shown by simple calculations.

Lemma 4.1. *Let* $F(X) = (f_{ij}(X))_{i,j}$ *be a matrix-valued function of one variable. If* $F(X)$ *is twice differentiable and invertible for* $X = X_0$, *then*

$$\left.\frac{d\det F(X)}{dX}\right|_{X=X_0} = \det F(X_0)\cdot \mathrm{Tr}\left(F(X_0)^{-1}\frac{dF}{dX}(X_0)\right),$$

$$\begin{aligned}\left.\frac{d^2\det F(X)}{dX^2}\right|_{X=X_0} = \det F(X_0)\cdot\Bigg\{&\mathrm{Tr}\left(F(X_0)^{-1}\frac{d^2F}{dX^2}(X_0)\right)\\ &-\mathrm{Tr}\left(F(X_0)^{-1}\frac{dF}{dX}(X_0)F(X_0)^{-1}\frac{dF}{dX}(X_0)\right)\\ &+\mathrm{Tr}\left(F(X_0)^{-1}\frac{dF}{dX}(X_0)\right)^2\Bigg\},\end{aligned}$$

where $\mathrm{Tr}(A)$ *is the trace of the matrix* A.

Proof of Proposition 4.1. The matrix $D_{k_M^+}(0)$ is the unit matrix I_N, and

$$D_{k_M^+}(0)^{-1} = I_N, \qquad \frac{dD_{k_M^+}}{dX}(0) = (c_{ij})_{i,j=1,\dots,N},$$

where

$$c_{ij} = \begin{cases} 0 & \text{if } i=j,\ d_i = 1,\\ 1 & \text{if } i=j,\ d_i \neq 1,\\ 1 & \text{if } d_{ij}=1,\ d_i>1,\\ -1 & \text{if } d_{ij}>1,\ d_i=1,\\ 0 & \text{otherwise}.\end{cases} \tag{21}$$

From Lemma 4.1, we obtain

$$a_1 = \mathrm{Tr}((c_{ij})_{i,j}) = \frac{\Phi(M)}{q-1} - t_1,$$

and

$$2a_2 = \mathrm{Tr}\left(\frac{d^2D_{k_M^+}}{dX^2}(0)\right) - \mathrm{Tr}\left(\left(\frac{dD_{k_M^+}}{dX}(0)\right)^2\right) + \mathrm{Tr}\left(\frac{dD_{k_M^+}}{dX}(0)\right)^2.$$

By straightforward calculations, we get

$$\mathrm{Tr}\biggl(\frac{d^2D_{k_M^+}}{dX^2}(0)\biggr)=2\biggl(\frac{\Phi(M)}{q-1}-t_2\biggr),\qquad \mathrm{Tr}\biggl(\frac{dD_{k_M^+}}{dX}(0)\biggr)^2=\biggl(\frac{\Phi(M)}{q-1}-t_1\biggr)^2.$$

From (21),

$$\begin{aligned}\mathrm{Tr}\biggl(\biggl(\frac{dD_{k_M^+}}{dX}(0)\biggr)^2\biggr)&=\sum_{i=1}^{N}\sum_{j=1}^{N}c_{ij}c_{ji}\\&=\sum_{i=1}^{N}c_i^2+\sum_{\substack{d_i=1<d_{ij}\\ d_j=1<d_{ji}}}1+\sum_{\substack{d_{ij}=1<d_i\\ d_{ji}=1<d_j}}1-\sum_{\substack{d_i=1<d_{ij}\\ d_{ji}=1<d_j}}1-\sum_{\substack{d_j=1<d_{ji}\\ d_{ij}=1<d_i}}1.\end{aligned}$$

Since $\deg M\geq 3$, we can easily see that

$$\sum_{i=1}^{N}c_i^2=\frac{\Phi(M)}{q-1}-t_1,\qquad \sum_{\substack{d_i=1<d_{ij}\\ d_j=1<d_{ji}}}1=s_1^2-s_1,$$

$$\sum_{\substack{d_{ij}=1<d_i\\ d_{ji}=1<d_j}}1=0,\qquad \sum_{\substack{d_i=1<d_{ij}\\ d_{ji}=1<d_j}}1=\sum_{\substack{d_j=1<d_{ji}\\ d_{ij}=1<d_i}}1=s_1^2.$$

It follows that

$$\mathrm{Tr}\biggl(\biggl(\frac{dD_{k_M^+}}{dX}(0)\biggr)^2\biggr)=\frac{\Phi(M)}{q-1}-t_1^2.$$

Hence (20) follows. ∎

We give some examples for Proposition 4.1.

Example 4.1. Let $M\in R$ be an irreducible monic polynomial of degree 3. Then

$$t_1=q+1,\qquad t_2=\frac{\Phi(M)}{q-1}=q^2+q+1.$$

By Proposition 4.1,

$$P_{k_M^+}(X)=\det D_{k_M^+}(X)=1+q^2X+\frac{q(q^3+1)}{2}X^2+\cdots.$$

Example 4.2. We put $M=T^n$ $(n\geq 3)$. Then

$$t_1=q,\qquad t_2=q^2,\qquad \frac{\Phi(M)}{q-1}=q^{n-1}.$$

Hence

$$\begin{aligned}P_{k_M^+}(X)&=\det D_{k_M^+}(X)\\&=1+(q^{n-1}-q)X+\frac{q^{n-1}(q^{n-1}-2q+1)}{2}X^2+\cdots.\end{aligned}$$

Acknowledgements. I would like to thank Prof. Kohji Matsumoto and the referee for their valuable comments.

References

[1] S. H. Bae and P.-L. Kang, *Class numbers of cyclotomic function fields*, Acta Arith. 102 (2002), 251–259.
[2] S. Galovich and M. Rosen, *The class number of cyclotomic function fields*, J. Number Theory 13 (1981), 363–375.
[3] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. 189 (1974), 77–91.
[4] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.
[5] A. Weil, *Basic Number Theory*, Springer, New York, 1967.

Graduate School of Mathematics
Nagoya University
Chikusa-ku, Nagoya 464-8602
Japan
E-mail: m05019e@math.nagoya-u.ac.jp

Received on 18.4.2008
and in revised form on 10.3.2009 (5689)