Nihonkai Math. J.
Vol.16(2005), 77-84

On the Number of Places of Function Fields and Congruence Zeta Functions

Takehiro HASEGAWA

Abstract

In the first half, we determine completely the numbers of any prime degree places of maximal function fields in the Hasse-Weil sense, and we present a new characterization of the Hermitian function field. In the latter half, in fact we count such numbers for three algebraic function fields. The first and the second examples are generalizations of the Hermitian function field, which are maximal. The last example is the Klein Quartic function field over the field of two elements. This is not maximal.

Key words and phrases: algebraic function field, congruence Zeta function

2000 Mathematics Subject Classifications: 11G20, 11R58

1 Introduction

Let q be a power of a prime number and $\mathbb{F}_q$ the finite field of size q. We consider an algebraic function field F of one variable with full constant field $\mathbb{F}_q$. Let $N(F)$ be the number of rational places (i.e., places of degree one) of $F/\mathbb{F}_q$, and let $B_n = B_n(F)$ be the number of places of degree n of $F/\mathbb{F}_q$. Of course $N(F)$ is equal to $B_1(F)$. Let $g = g(F)$ be the genus of an algebraic function field F. It is well-known (for example, [4] Hasse-Weil Bound) that

$$|N(F) - (q+1)| \leq 2g(F) \cdot \sqrt{q}.$$

One is often interested in algebraic function fields with many rational places. So we introduce the following notion.

Definition. An algebraic function field $F/\mathbb{F}_q$ is called maximal (resp. minimal) if

$$N(F) = q + 1 + 2g(F) \cdot \sqrt{q} \quad (\text{resp.} \quad N(F) = q + 1 - 2g(F) \cdot \sqrt{q}).$$

In this paper, we show the following theorem and corollary.

Theorem. Assume that F is a maximal function field over $\mathbb{F}_{q^2}$ of genus g. Then,

(1)
$$B_2(F) = \frac{q(q+1)(q^2-q-2g)}{2}$$

(2)
$$B_l(F) = \frac{q(q^{l-1}-1)(q^l+q+2g)}{l} \qquad \text{for every odd prime number } l.$$

By the theorem, it is clear that the number $B_l(F)$ is not zero for any maximal function field F and any odd prime number l. We have the following corollary for $l = 2$.

Corollary. A maximal function field $F/\mathbb{F}_{q^2}$ has the number $B_2(F) = 0$ if and only if $F/\mathbb{F}_{q^2}$ is isomorphic to the Hermitian function field over $\mathbb{F}_{q^2}$.

This corollary characterizes the Hermitian function field, and states that the Hermitian function field is a special maximal function field.

In the next section, we give an elementary proof for a special case of an explicit formula in the textbook of H. Stichtenoth ([4], p 178 (2.23)) by only using fundamental facts of the algebraic function field theory. This proof is completely different from his one. In the third section, we recall the facts of the Zeta functions and L-polynomials, and we prove the theorem and the corollary. The last section has three examples. The first and the second are generalizations of the Hremitian function field, which are maximal. The last is the Klein Quartic function field over the field of two elements, which is not maximal. It is interesting to count the numbers of nonrational places, because these imply the numbers of monic irreducible polynomials over finite fields and a special case of Fermat's theorem. Little attention has been given to compute the numbers of nonrational places of algebraic function fields.

2 Preliminaries

Let n be a positive integer and $\mathbb{F}_{q^n}$ the n-th cyclic Galois extension of $\mathbb{F}_q$. We fix an algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$. By Galois Theory, there exists $\xi \in \bar{\mathbb{F}}_q$ such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\xi)$. Assuming that $\varphi(T)$ is the minimal polynomial of the element ξ over $\mathbb{F}_q$, then the degree of $\varphi(T)$ is equal to n. Let m be a positive integer. Note that if m and n are coprime then the fields $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$ are linearly disjoint over $\mathbb{F}_q$, therefore the intersection of $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$ is equal to $\mathbb{F}_q$.

Let F be an algebraic function field over $\mathbb{F}_q$ of genus g, and let $\mathbb{P}_F$ be the set of places of F. We fix the constant field extension $F\bar{\mathbb{F}}_q$ of F and set F_n the compositum $F\mathbb{F}_{q^n} \subseteq F\bar{\mathbb{F}}_q$ of the fields F and $\mathbb{F}_{q^n}$. Then F_n is the algebraic function field with full constant field $\mathbb{F}_{q^n}$, and its genus $g(F_n)$ is equal to g (see, [4] Proposition III.6.1 and Theorem III.6.3). It is clear that $F_n = F(\xi)$ and $[F_n : F] = n$ by Galois Theory. Let P be a place of $F/\mathbb{F}_q$, and $\mathcal{O}_P$ its discrete valuation ring. Since $\mathbb{F}_q \subseteq \mathcal{O}_P$ and $\mathbb{F}_q \cap P = \{0\}$, the residue class map

$$\mathcal{O}_P \to \mathcal{O}_P/P, \qquad c \mapsto \bar{c} := c + P$$

induces a canonical embedding of the finite field $\mathbb{F}_q$ into the residue class field $\mathcal{O}_P/P$ of P. By the embedding map, if $\psi(T) = c_0 + c_1T + \cdots + c_sT^s$ is a polynomial over $\mathcal{O}_P$ then $\bar{\psi}(T) := \bar{c}_0 + \bar{c}_1T + \cdots + \bar{c}_sT^s$ is a polynomial over $\mathcal{O}_P/P$. In particular, if $\psi(T)$ is a polynomial over $\mathbb{F}_q$, then $\bar{\psi}(T)$ can be regarded as $\psi(T)$, that is, $\bar{\psi}(T) = \psi(T)$.

The next is very useful when one investigates the ramification of nonrational places.

Definition. Let P be a place of F, and let F' be a finite algebraic extension of F. We call the place P totally inert in the extension F'/F if there exists only one extension P' of P in F' and the relative degree $f(P'|P)$ is equal to the degree $[F' : F]$.

Now we show the proposition:

Proposition. Let l be a prime number, and F an algebraic function field over the finite field $\mathbb{F}_q$. Let $F_l \subseteq F\bar{\mathbb{F}}_q$ be the compositum of the fields F and $\mathbb{F}_q$. Then we have

$$N(F) + l \cdot B_l(F) = N(F_l).$$

This proposition is a special case for any prime number of an explicit formula in the textbook of Stichtenoth ([4], p 178 (2.23)). His proof requires some deep results from the constant field

extension theory (confer, [4] Chapter III.6). Here we give a very elementary proof without using it. This proposition follows from the following two lemmas, which we can prove by only using Galois Theory and the Kummer's Theorem (see, [4] Theorem III.3.7).

Lemma 1. Let P be a place of F. Assume that m is greater than n.

(1) If P is rational (i.e., of degree one), then P is totally inert in the extension F_n/F and the extension of P in F_n is also rational.

(2) If P is of degree n, then P splits completely in F_n/F and n extensions of P in F_n are rational.

(3) If P is of degree m, then each extension of P in F_n is not rational.

Proof. (1) Assuming that a place P is rational of F, then its residue class field $\mathcal{O}_P/P$ is the finite field $\mathbb{F}_q$ and the minimal polynomial $\varphi(T)$ of the element ξ over $\mathbb{F}_q$ is irreducible over $\mathcal{O}_P/P$. By using the Kummer's Theorem, there exists $P' \in \mathbb{P}_{F_n}$ satisfying $P'|P$ and $f(P'|P) = n$. Hence we obtain $\deg P' = 1$ because

$$n \cdot \deg P' = [\mathcal{O}_{P'}/P' : \mathbb{F}_{q^n}] \cdot [\mathbb{F}_{q^n} : \mathbb{F}_q] = f(P'|P) \cdot \deg P = n.$$

(2) If P is a place of degree n in F, then $\mathcal{O}_P/P = \mathbb{F}_{q^n}$ and $\varphi(T) = (T - \xi_1) \cdots (T - \xi_n)$ in the polynomial ring $\mathcal{O}_P/P[T]$, where $\xi_1 := \xi$. Then, for $1 \leq i \leq n$, there are $P_i \in \mathbb{P}_{F_n}$ satisfying $P_i|P$ and $f(P_i|P) = 1$. Moreover, $P_i \neq P_j$ for $i \neq j$. Thus $\deg P_i = 1$ for all i.

(3) Let P be a place of degree m in F, and let P' be an extension of P in F_n. Then

$$\deg P' = [\mathcal{O}_{P'}/P' : \mathbb{F}_{q^n}] = \frac{f(P'|P) \cdot \deg P}{n} > 1,$$

and the proof is complete. □

Lemma 2. Suppose that n is prime to m. If P is a place of degree m in F, then P is totally inert in the extension F_n/F, and the degree of the extension of P in F_n is equal to m.

Proof. If P is a place of degree m in F, then $\mathcal{O}_P/P = \mathbb{F}_{q^m}$. Since m and n are coprime, then the fields $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$ are linearly disjoint over $\mathbb{F}_q$, and we know that

$$m = [\mathbb{F}_{q^m} : \mathbb{F}_q] = [\mathbb{F}_{q^m}(\xi) : \mathbb{F}_{q^n}].$$

Suppose that $\varphi(T) = \varphi_1(T) \cdot \varphi_2(T)$, where $\varphi_1(T)$ and $\varphi_2(T)$ are polynomials over $\mathbb{F}_{q^m}$. Without loss of generality, we can assume that $\varphi_1(\xi) = 0$. Then we obtain

$$m \cdot \deg \varphi(T) = [\mathbb{F}_{q^m}(\xi) : \mathbb{F}_q] \leq \deg \varphi_1(T) \cdot m, \quad \text{so} \quad \deg \varphi(T) \leq \deg \varphi_1(T).$$

Hence $\varphi(T)$ is irreducible over $\mathcal{O}_P/P$. By the Kummer's Theorem, there exists $P' \in \mathbb{P}_{F_n}$ satisfying $P'|P$ and $f(P'|P) = n$. Hence we obtain $\deg P' = m$. □

Proof of Proposition. By Lemma 1 (1), any rational place of F has only one extension of degree one in F_l. Next, assuming that P is a place of degree l, the place P has l extensions of degree one in F_l from Lemma 1 (2). Lastly, suppose that P is a place as in Lemma 1 (3) or Lemma 2. Any extension of the place P in F_l is not rational, and the proof is complete. □

3 Proofs

In the section, we prove the theorem and the corollary. Firstly, we recall some facts about the Zeta functions and L-polynomials of algebraic function fields over finite fields.

Definition. Let F be an algebraic function field over the finite field $\mathbb{F}_q$. The Zeta function $Z_F(t)$ (resp. L-polynomial $L_F(t)$) of F is defined as follows:

$$Z_F(0) := 1 \qquad \text{and} \qquad Z_F(t) := \sum_{n=1}^{\infty} N(F_n)t^{n-1};$$

$$(\text{resp.} \qquad L_F(t) := (1-t)(1-qt) \cdot Z_F(t)).$$

By the difinitions, we obtain (confer, [4] Corollary V.1.17)

$$\begin{aligned} \frac{d}{dt}\log L_F(t) &= \frac{d}{dt}\log Z_F(t) - \frac{1}{1-t} - \frac{q}{1-qt} \\ &= \sum_{n=1}^{\infty} N(F_n)t^{n-1} - \sum_{n=1}^{\infty} t^{n-1} - \sum_{n=1}^{\infty} q^n t^{n-1} \\ &= \sum_{n=1}^{\infty} \Big(N(F_n) - (q^n+1)\Big)t^{n-1}. \end{aligned} \tag{1}$$

It is well-known that F is an maximal (resp. minimal) function field over $\mathbb{F}_q$ if and only if

$$L_F(t) = (1+\sqrt{q}t)^{2g(F)} \qquad (\text{resp.} \quad L_F(t) = (1-\sqrt{q}t)^{2g(F)}).$$

Secondly, we show the following by using the above facts.

Lemma 3. Let F be an algebraic function field over $\mathbb{F}_q$, and let F_n be the compositum of the fields F and $\mathbb{F}_{q^n}$ (note that F_n is an algebraic function field over $\mathbb{F}_{q^n}$).

(i) Assume that F is maximal. If n is an odd (resp. even) integer, then F_n is maximal (resp. minimal); $N(F_n) = q^n + 1 + 2g(F) \cdot \sqrt{q^n}$ (resp. $N(F_n) = q^n + 1 - 2g(F) \cdot \sqrt{q^n}$).

(ii) If F is minimal, then the compositum F_n is also minimal for each n.

Proof. (i) Since F is maximal, then we have $L_F(t) = (1+\sqrt{q}t)^{2g(F)}$ by the above fact, so

$$\begin{aligned} \sum_{n=1}^{\infty} \Big(N(F_n) - (q^n+1)\Big)t^{n-1} &= \frac{d}{dt}\log L_F(t) \\ &= 2g(F)\sqrt{q}\sum_{n=1}^{\infty}(-\sqrt{q}t)^{n-1} \end{aligned}$$

by the equation (1). Contrasting the both sides for each n, we obtain the desired results. The claim (ii) is the same as the proof of the claim (i). This finishes the proof of Lemma 3. □

Now, we compute the numbers of any prime degree places in maximal function fields.

Proof of Theorem. (1) Fix $l = 2$. By Lemma 3 (i), the algebraic function field F_2 over $\mathbb{F}_{q^4}$ is minimal, that is, $N(F_2) = q^4 + 1 - 2gq^2$. Hence, from Proposition, we get

$$B_2(F) = \frac{N(F_2) - N(F)}{2} = \frac{q(q+1)(q^2-q-2g)}{2}.$$

(2) We know, from Lemma 3 (i) that the algebraic function fields F_l over $\mathbb{F}_{q^{2l}}$ are maximal, namely, $N(F_l) = q^{2l} + 1 - 2gq^l$. Therefore we obtain by Proposition

$$B_l(F) = \frac{N(F_l) - N(F)}{l} = \frac{q(q^{l-1} - 1)(q^l + q + 2g)}{l}.$$

Now the integers q, $q^{l-1} - 1$ and $q^l + q + 2g$ are positive, thus $B_l(F)$ are not zero for all l. □

Next, we prove the corollary.

Proof of Corollary. Suppose that F is a maximal function field over $\mathbb{F}_{q^2}$, and $B_2(F) = 0$. Then the genus g of F is equal to $g = q(q-1)/2$ by Theorem (1). Hence it follows that F is isomorphic to the Hermitian function field over $\mathbb{F}_{q^2}$ from the main theorem in the paper [3] of H. G. Rüch and H. Stichtenoth. The converse is trivial, and the proof is complete. □

4 Examples

Let us begin with the definition of q-polynomials (see, [2] Chapter 3.4).

Definition. Polynomials

$$f(T) = \sum_{i=0}^{m} a_i T^i \qquad \text{and} \qquad f^*(T) = \sum_{i=0}^{m} a_i T^{q^i}$$

over $\mathbb{F}_{q^n}$ are called q-associates of each other.

We can interpret f^* as a linear map over $\mathbb{F}_q$ from the algebraically closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$ to itself, that is, $f^*(\alpha+\beta) = f^*(\alpha)+f^*(\beta)$ and $f^*(c\alpha) = cf^*(\alpha)$ for all $\alpha, \beta \in \bar{\mathbb{F}}_q$ and all $c \in \mathbb{F}_q$. Suppose that

$$f(T) = \sum_{i=0}^{m} a_i T^i \qquad \text{and} \qquad g(T) = \sum_{j=0}^{n} b_j T^j$$

are polynomials over $\mathbb{F}_q$. Since the product of f and g is given by

$$fg(T) = \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i b_j \Big) T^k,$$

then we obtain

$$(fg)^*(T) = \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i b_j \Big) T^{q^k} = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j T^{q^{i+j}} = f^*(g^*(T)). \tag{2}$$

It follows, from the equation (2) that the next algebraic function field is maximal.

Example 1. Let us consider the algebraic function field

$$H = \mathbb{F}_{q^{2r}}(x, y) \qquad \text{with} \quad y^q + y = x^{q^r+1},$$

where r is an odd integer. Note that this is the Hermitian function field when r is equal to one. Let Q be the infinite place (i.e., the simple pole of x) of the rational function field $\mathbb{F}_{q^{2r}}(x)$. As the place Q is totally ramified in the extension $H/\mathbb{F}_{q^{2r}}(x)$, the full constant field of H is

also the finite field $\mathbb{F}_{q^{2r}}$. Firstly, we know that the genus of H is equal to $q^r(q-1)/2$ (see, [4] Proposition VI.4.1 (e)). Next, we count the number of rational places in H. Assuming that

$$\rho(T) = \sum_{i=0}^{r-1}(-1)^i T^{r-i-1} \qquad \text{and} \qquad \tau(T) = (T+1)(T^r-1)$$

are polynomials over $\mathbb{F}_{q^{2r}}$, their linearized q-associates are given by

$$\rho^*(T) = \sum_{i=0}^{r-1}(-1)^i T^{q^{r-i-1}} \qquad \text{and} \qquad \tau^*(T) = (T^q+T)^{q^r} - (T^q+T)$$

from the equation (2). Therefore we get an equation $T^{q^{2r}} - T = \rho^*(\tau^*(T))$ over $\mathbb{F}_{q^{2r}}$. Suppose that an element β in an algebraically closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$ is a root of the equation $T^q + T = \alpha^{q^r+1}$ for a element $\alpha \in \mathbb{F}_{q^{2r}}$. Then

$$\tau^*(\beta) = (\beta^q+\beta)^{q^r} - (\beta^q+\beta) = (\alpha^{q^r+1})^{q^r} - (\alpha^{q^r+1}) = 0,$$

thus $\beta^{q^{2r}} - \beta = \rho^*(\tau^*(\beta)) = \rho^*(0) = 0$, so the element β is in $\mathbb{F}_{q^{2r}}$. Hence, for each $\alpha \in \mathbb{F}_{q^{2r}}$ the equation $T^q + T = \alpha^{q^r+1}$ has q distinct roots in $\mathbb{F}_{q^{2r}}$, and $N(H) = q^{2r+1}+1$ (see, [1]). In consequence, we see that the algebraic function field H over $\mathbb{F}_{q^{2r}}$ is maximal, that is,

$$N(H) - (q^{2r}+1) = q^{2r+1} - q^{2r} = q^r(q-1)\cdot\sqrt{q^{2r}} = 2g(H)\cdot\sqrt{q^{2r}}.$$

Combining Proposition and Lemma 3 (i), we obtain the following results:

(1) If $l = 2$, then we obtain

$$B_2(H) = \frac{q^{2r+1}(q^{r-1}-1)(q^r+1)}{2};$$

(2) If l is an odd prime number, then we obtain

$$B_l(H) = \frac{q^{2r+1}(q^{(l-1)r}-1)(q^{(l-1)r-1}+1)}{l}.$$

We deal with a subfield of the Hermitian function field.

Example 2. Assume that $s \mid q+1$. Let us consider the algebraic function field

$$H = \mathbb{F}_{q^2}(x,y) \qquad \text{with} \quad y^q + y = x^s.$$

Since $g(H) = (q-1)(s-1)/2$ and $N(H) = 1 + q(1+(q-1)s)$, the algebraic function field H over $\mathbb{F}_{q^2}$ is maximal (for example, [4] Example VI. 4.2). Combining Proposition and Lemma 3 (i), we obtain the following results:

(1) If $l = 2$, then we obtain

$$B_2(H) = \frac{q(q-1)(q+1)(q+1-s)}{2};$$

(2) If l is an odd prime number, then we obtain

$$B_l(H) = \frac{(q^l-q)(q^l+q+(q-1)(s-1))}{l}.$$

Remark. When $s = 1$, this example is interesting. Because it show that $B_l(H)$ is equal to the number of monic irreducible polynomials of degree l in $\mathbb{F}_{q^2}[T]$ (confer, [2] Chapter 3.2).

For an algebraic function field F over the finite field $\mathbb{F}_q$, the Serre Bound (for example, [4] Theorem V.3.1) is given by $|N(F) - (q+1)| \leq [2g(F) \cdot \sqrt{q}]$, where $[r]$ denotes the integer part of the real number r.

The algebraic function fields in the above examples is maximal. Thus the numbers B_l are given by the theorem if the genus is known. Next, we present such numbers of a nonmaximal function field. Since this is not maximal, we can not apply the theorem.

Example 3. We consider the Klein Quartic function field $K = \mathbb{F}_2(x, y)$ defined by the affine equation $y^3 + x^3y + x = 0$. It is well-known (for example, [4] Example VI.3.8) that

$$[K : \mathbb{F}_2(x)] = 3, \qquad g(K) = 3 \qquad \text{and} \qquad N(K) = 3,$$

and the L-polynomial of the Klein Quartic is given by $L_K(t) = 1 + 5t^3 + 8t^6$. After a technical computation, we obtain the power series expansion of the logarithmic derivative of L_K:

$$\begin{aligned} \frac{d}{dt}\log L_K(t) &= 3t^2(5+16t^3) \cdot \frac{1}{1+5t^3+8t^6} \\ &= 3t^2(5+16t^3) \cdot \frac{32}{7+(5+16t^3)^2} \\ &= \frac{2^5 \cdot 3}{7} t^2 \cdot \sum_{n=0}^{\infty} \left(\frac{-1}{7}\right)^n (5+16t^3)^{2n+1}; \qquad (3) \\ &= 15t^2 - 27t^5 + 15t^8 + 141t^{11} - 825t^{14} + 2997t^{17} + \cdots . \end{aligned}$$

First, fix $l = 3$. It follows from the equation (1) and the series (3) that

$$N(K_3) - (2^3 + 1) = 15, \qquad \text{so} \qquad N(K_3) = 24.$$

Thus we get $B_3(K) = 7$ by Proposition. Next, we fix a prime number l and $l \neq 3$. Note that the number l is not divisible by 3. It follows that $N(K_l) = 2^l + 1$ from the equation (1) and the series (3). So we have $B_l(K) = (2^l - 2)/l$ by Proposition. In conclusion, we obtain

$$B_3(K) = 7 \qquad \text{and} \qquad B_l(K) = \frac{2^l - 2}{l} \quad \text{for any prime number } l, l \neq 3.$$

Remark. (1) The algebraic function field K_3 over the field of eight elements is maximal for Serre Bound. It is for this reason that $l = 3$ is the special case.

(2) For any prime number $l \neq 3$, the number $B_l(K)$ is equal to the number of monic irreducible polynomials of degree l in $\mathbb{F}_2[T]$ (confer, [2] Chapter 3.2).

5 Acknowledgments

The author thanks Professor Ken Sawada and the referee for valuable comments on the first version of this paper.

References

[1] S. Kondo, T. Katagiri, and T. Ogihara, Automorphism groups of one-point codes from the curves $y^q + y = x^{q^r+1}$, IEEE Trans. Inform. Theory **47** (2001) 2573–2579.

[2] R. Lidl and H. Niederreiter, *Finite fields* (With a foreword by P. M. Cohn, Second edition, Encyclopedia of Mathematics and its Applications **20**), Cambridge, 1997.

[3] H. G. Rüch and H. Stichtenoth, A Characterization of Hermitian function fields over finite fields, J. reine angew. Math. **457** (1994) 185–188.

[4] H. Stichtenoth, *Algebraic function fields and codes* (Universitext), Springer-Verlag, 1993.

Present Address: Department of Mathematics, School of Education,
Waseda University, Nishi-Waseda, Shinjuku-ku, Tokyo 169-8050, Japan
E-mail:thasegawa@suou.waseda.jp

Received 17 March, 2005 Revised 6 May, 2005