J. Korean Math. Soc. **35** (1998), No. 2, pp. 341–360

THE ARITHMETIC OF CARLITZ POLYNOMIALS

SUNGHAN BAE

ABSTRACT. Some interesting properties of Carlitz cyclotomic polynomials analogous to those of classical cyclotomic polynomials are given.

0. Introduction

The analogies between number fields and function fields have many interesting aspects in the recent development of number theory. The Carlitz polynomial $\rho_M(X)$ plays a very important role in the study of function fields as does the equation $X^m - 1$ in the study of number fields. The cyclotomic polynomial $\Phi_m(X)$, which is a certain factor of $X^m - 1$, has been studied for a long time.

One can define the Carlitz cyclotomic polynomial $\Phi_M(X)$ as a factor of the Carlitz polynomial $\rho_M(X)$ in a similar way. In this article the resultant of Carlitz cyclotomic polynomials is calculated explicitly, and criterions for the reducibility or solvabilty of a Carlitz cyclotomic polynomials modulo certain ideals are given. Finally an analogue of the theorem of Bang and Zsigmondy on the primitive factors of the value $B^{q^{\deg M}}\rho_M(\frac{A}{B})$, which can be thought as the analogue of the numbers $a^m - b^m$, is given. The results and proofs here are very similar to those in the classical case replacing integers by polynomials. The main difference arises from the fact that there can be more than one irreducible polynomial with the same absolute value at infinity.

Let $\mathbb{F}_q[T]$ be a polynomial ring over a finite field $\mathbb{F}_q$, where q is a power of a prime number p. Throughout the paper the letters A, B

Received September 30, 1997.

1991 Mathematics Subject Classification: 12E05, 11A51.

Key words and phrases: Carlitz Module, cyclotomic polynomial, resultant, primitive factor.

Partially supported by Non Directed Research Fund, Korea Research Foundation, 1996.

denote polynomials, M, N, D monic polynomials, and P, Q monic irreducible polynomial in $\mathbb{F}_q[T]$. The greatest common divisor (M, N) is defined to be the monic generator of the ideal generated by M and N.

1. Preliminaries

Let ρ be the Carlitz module, that is, ρ is the rank 1 Drinfeld module on $\mathbb{F}_q[T]$ defined by

$$\rho_T(X) = TX + X^q.$$

For a polynomial N in $\mathbb{F}_q[T]$ a *primitive N-th root* λ_N of ρ is defined to be a root of $\rho_N(X)$ which is not a root of $\rho_M(X)$ for any proper divisor M of N. Let $\Phi_N(X)$ be the minimal polynomial of any primitive N-th root of ρ over $\mathbb{F}_q(T)$. Let $\phi(N)$ denote the Euler phi function, that is, the number of polynomials which are prime to N and have degree less than $\deg N$. Then $\deg \Phi_N(X) = \phi(N)$.

PROPOSITION 1.1. ([3], Proposition 1.2)

a) $\rho_N(X) = \prod_{D|N} \Phi_D(X)$.

b) *If P is a monic irreducible polynomial of degree d in $\mathbb{F}_q[T]$, then*

$$\Phi_P(X) = P + A_1 X^{q-1} + \cdots + A_{d-1} X^{q^{d-1}-1} + X^{q^d-1},$$

with $A_i \in \mathbb{F}_q[T]$ and $P \mid A_i$ for every i. Moreover,

$$\Phi_{P^r}(X) = \Phi_P(\rho_{P^{r-1}}(X)).$$

c) *If P_i's are distinct irreducible polynomials in $\mathbb{F}_q[T]$, then*

$$\Phi_{P_1^{r_1} \cdots P_s^{r_s}}(X) = \Phi_{P_1 \cdots P_s}(\rho_{P_1^{r_1-1} \cdots P_s^{r_s-1}}(X)).$$

d) *If $P \nmid N$, then*

$$\Phi_{P^e N}(X) = \Phi_N(\rho_{P^e}(X)) \,/\, \Phi_N(\rho_{P^{e-1}} X).$$

If $P \mid N$, then

$$\Phi_{P^e N}(X) = \Phi_N(\rho_{P^e}(X)).$$

e) $\Phi_N(X) = \prod_{D|N} \big(\rho_{N/D}(X)\big)^{\mu(D)}$
where μ is the Möbius function.

COROLLARY 1.2.

a) $\Phi_N(X)$ *is a polynomial in* X^{q-1} *with coefficients in* $\mathbb{F}_q[T]$ *for* $\deg N \geq 1$.

b)

$$\Phi_N(0) = \begin{cases} P & \text{if } N \text{ is a power of a prime } P \\ 1 & \text{otherwise.} \end{cases}$$

c)

$$\Phi_{P^eN}(X) \equiv \begin{cases} \Phi_N(X)^{\phi(P^e)} \pmod{P} & \text{if } P \nmid N \\ \Phi_N(X)^{q^{e \deg P}} \pmod{P} & \text{if } P \mid N. \end{cases}$$

d)

$$\Phi_N(\rho_R(X)) = \begin{cases} \Phi_{NR}(X) \\ \qquad \text{if every prime factor of } R \text{ divides } N, \\ \Phi_N(\rho_S(X))\Phi_{NP}(\rho_S(X)) \\ \qquad \text{if } R = PS \text{ and } P \nmid N \text{ for some prime } P. \end{cases}$$

2. Resultant of cyclotomic polynomials

For two polynomials F and G in one variable X with coefficients in $\mathbb{F}_q(T)$, we write $R(F,G)$ the *resultant* of F and G. The fundamental properties of $R(F,G)$ are

PROPOSITION 2.1. ([1], §2) *Let* $F(X) = a_n \prod_{k=1}^{n}(X - \alpha_k)$, *and* $G(X) = b_m \prod_{j=1}^{m}(X - \beta_j)$. *Then we have*

a) $R(F(X),G(X)) = a_n^m b_m^n \prod_{k=1}^{n} \prod_{j=1}^{m}(\alpha_k - \beta_j)$,
b) $R(F(X),G(X)) = (-1)^{mn} R(G,F)$,
c) $R(F(X),G(X)) = b_m^n \prod_{j=1}^{m} F(\beta_j)$
d) $R(F(X),G(X)H(X)) = R(F(X),G(X))R(F(X),H(X))$,
e) $F(X)$ *and* $G(X)$ *have a root in common if and only if* $R(F(X),G(X)) = 0$.

Thus we see easily that $R(\Phi_1(X),\Phi_M(X)) = \Phi_M(0)$ and $R(\Phi_M(X),\Phi_N(X)) = R(\Phi_N(X),\Phi_M(X))$ for $M \neq N$.

THEOREM 2.2. (cf; [2], Theorem 1) *Let a and b be elements in an extension field of $\mathbb{F}_q(T)$. Then we have*

$$R(\Phi_M(a+X),\Phi_N(b+X)) = \prod_{D|N} \Phi_{\frac{M}{D'}}(\rho_D(a-b))^{\mu(\frac{N}{D})\frac{\phi(M)}{\phi(\frac{M}{D'})}},$$

where $D' = (M, D)$.

Proof. Denote by λ_M a primitive M-th root of ρ. Then all the roots of $\Phi_M(a+X) = 0$ are $\rho_K(\lambda_M) - a$, for $(K, M) = 1$ and $\deg K < \deg M$. Then

$$\begin{aligned}
&R(\Phi_M(a+X), \rho_D(b+X)) \\
&= \prod_{(K,M)=1, \deg K < \deg M} (\rho_D(\rho_K(\lambda_M) + b - a)) \quad \text{(by Proposition 2.1, c)} \\
&= \prod (\rho_{DK}(\lambda_M) + \rho_D(b-a)) \\
&= \left[\prod_{(K, \frac{M}{D'})=1} (\rho_{\frac{DK}{D'}}(\lambda_{\frac{M}{D'}}) + \rho_D(b-a)) \right]^{\frac{\phi(M)}{\phi(\frac{M}{D'})}} \\
&= \left(\Phi_{\frac{M}{D'}}(\rho_D(b-a)) \right)^{\frac{\phi(M)}{\phi(\frac{M}{D'})}}.
\end{aligned}$$

Thus

$$\begin{aligned}
R(\Phi_M(a+X),\Phi_N(b+X)) &= \prod_{D|N} R(\Phi_M(a+X), \rho_D(b+X))^{\mu(\frac{N}{D})} \\
&= \prod_{D|N} \Phi_{\frac{M}{D'}}(\rho_D(b-a))^{\mu(\frac{N}{D})\frac{\phi(M)}{\phi(\frac{M}{D'})}}.
\end{aligned}$$

□

COROLLARY 2.3. (cf; [1], Theorem 2)

$$R(\Phi_M(X),\Phi_N(X)) = \prod_{D,P} P^{\mu(N/D)\phi(M)/\phi(P^a)}$$

where $D \mid N$ and P is a prime such that $M/(M, D) = P^a, a \geq 1$.

Proof. This follows from Theorem 2.2 and Corollary 1.2, taking $a = b = 0$. □

COROLLARY 2.4. (cf; [1], Theorem 3) *If* $\deg M \geq \deg N > 0$ *and* $(M, N) = 1$, *then* $R(\Phi_M(X), \Phi_N(X)) = 1$.

PROPOSITION 2.5. (cf; [1], Theorem 4) *If* $\deg M \geq \deg N > 0$ *and* $(M, N) \neq 1$, *then*

$$R(\Phi_M(X), \Phi_N(X)) = \begin{cases} P^{\phi(N)} & \text{if } M/N \text{ is a power of } P, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. The proof is exactly the same as the proof of [1] Theorem 4, and we omit the proof. However we note that in the proof of [1], Theorem 4 d' should range through the square free divisors of n', not of $k'n'$. □

COROLLARY 2.6. (cf; [9], Satz 2) *Let* $M = P^e N$ *and* λ *be a primitive* M*-th root of* ρ. *Put* $\psi(P^e)$ *to be* $\phi(P^e)$ *if* $P \nmid N$ *and* $q^{e \deg P}$ *otherwise. Let* $g(X) \in \mathbb{F}_q[T][X]$ *be defined by*

$$\Phi_N(X) = \Phi_M(X)^{\psi(P^e)} + Pg(X).$$

Then $g(\lambda)$ *is a unit in* $\mathbb{F}_q[T][\lambda]$.

Proof. The existence of $g(X)$ follows from Corollary 1.3. Then the result follows from Proposition 2.1, e) and Proposition 2.5. □

Now we will compute the resultant $R(\Phi_M(\rho_R(X)), \Phi_N(\rho_S(X)))$ for some monic polynomials R and S. For this we need the following notion of order of an element of an $\mathbb{F}_q[T]$-module. Let $\mathcal{M}$ be an $\mathbb{F}_q[T]$-module, and α be an element of $\mathcal{M}$. We define the order $ord(\alpha)$ of α to be the monic generator of the ideal $Ann(\alpha)$, the annihilator of α. Then, as in abelian groups, we have;

LEMMA 2.7. *Let* $A \in \mathbb{F}_q[T]$ *be monic. Then we have*

$$ord(A\alpha) = \frac{ord(\alpha)}{(A, ord(\alpha))} = \frac{[A, ord(\alpha)]}{A},$$

where (A,B) denotes the greatest common divisor of A and B, and $[A,B]$ the least common multiple of A and B.

Now viewing the algebraic closure $\overline{\mathbb{F}_q(T)}$ of $\mathbb{F}_q(T)$ as an $\mathbb{F}_q[T]$-module via ρ, we have

PROPOSITION 2.8. (cf; [6], Lemma 1) *For monic polynomials A and B, we have*

$$\Phi_A(\rho_B(X)) = \prod_{[M,B]=AB, M\ monic} \Phi_M(X).$$

For two monic polynomials A and B in $\mathbb{F}_q[T]$ we define $< A,B >$ by

$$< A,B >= \prod_{P, v_P(A)>0} P^{v_P(AB)},$$

where $v_P(A)$ is the P-adic valuation of A. Then following the same lines as in [6] taking Proposition 2.7 into account, we get

THEOREM 2.9. (cf;[6], Theorem 17) *Let M,N,R and S be monic polynomials in $\mathbb{F}_q[T]$. Let*

$$G = \left(\frac{MR}{< M,R >}, \frac{NS}{< N,S >}\right)$$

and for each irreducible polynomial P, let $u(P) = v_P((MR,NS)) - v_P(< M,R >)$, $v(P) = v_P((MR,NS)) - v_P(< N,S >)$. Then

$$R(\Phi_M(\rho_R(X)), \Phi_N(\rho_S(X))$$

$$= \begin{cases} 0 & \\ & \text{if } < M,R > \mid NS \text{ and } < N,S > \mid MR, \\ P^{\phi((MR,NS))\frac{q^{u(P)\deg P}}{\phi(P^{u(P)})}\frac{q^{\deg G}}{\phi(G)}} & \\ & \text{if } < M,R > \mid NS \text{ and } \frac{<N,S>}{(<N,S>,MR)} = P^e, \\ P^{\phi((MR,NS))\frac{q^{v(P)\deg P}}{\phi(P^{v(P)})}\frac{q^{\deg G}}{\phi(G)}} & \\ & \text{if } < N,S > \mid MR \text{ and } \frac{<M,R>}{(<M,R>,NS)} = P^e, \\ 1 & \\ & \text{otherwise.} \end{cases}$$

REMARK. The term $(-1)^{\phi(M)\phi(N)q^{\deg RS}}$ disappears in our case because the exponent is always even for odd characteristic, and $-1 = 1$ for even characteristic.

3. Reducibility

In this section we discuss reducibility properties of Carlitz cyclotomic polynomials modulo certain ideals. We begin with the reducibility of the polynomial $\Phi_M(\rho_R(X))$.

PROPOSITION 3.1. (cf;[7], Theorem 1) *$\Phi_M(\rho_R(X))$ is irreducible over $\mathbb{F}_q[T]$ if and only if every prime factor of R is also a prime factor of M.*

Proof. This follows easily from Corollary 1.4. □

LEMMA 3.2. *Let M be a monic polynomial in $\mathbb{F}_q[T]$. The group $U = (\mathbb{F}_q[T]/M)^*$ of units is a cyclic group if and only if one of the followings holds;*

i) *M is an irreducible polynomial $P(T)$, in which case $U \simeq \mathbb{Z}/(q^d - 1)$.*
ii) *$q = p$ a prime number and $M = P(T)^2$ with $\deg P(T) = 1$, in which case $U \simeq \mathbb{Z}/(p(p-1))$.*
iii) *$q = 2$, besides i) and ii), we have, with $P(T)$ a monic irreducible polynomial of degree $d > 1$,*

(a) $M = T(T+1)$, in which case U is trivial,

(b) $M = T(T+1)^2$, or, $T^2(T+1)$, in which case $U \simeq \mathbb{Z}/2$

(c) $M = T^3$, $(T+1)^3$, $T(T+1)^3$, or $(T+1)T^3$, in which case $U \simeq \mathbb{Z}/4$,

(d) $M = TP(T)$, $(T+1)P(T)$, or $T(T+1)P(T)$,
in which case $U \simeq \mathbb{Z}/(2^d - 1)$,

(e) $M = T^2P(T)$, $(T+1)^2P(T)$, $T^2(T+1)P(T)$, or $T(T+1)^2P(T)$,
in which case $U \simeq \mathbb{Z}/(2(2^d - 1))$,

(f) $M = T^3P(T)$, $(T+1)^3P(T)$, $T^3(T+1)P(T)$, or $T(T+1)^3P(T)$,
in which case $U \simeq \mathbb{Z}/(4(2^d - 1))$,

Proof. It is clear that if one of i), ii) and iii) holds, U is cyclic. Now suppose that U is cyclic. Assume that M is a power of an irreducible polynomial $P(T)$, say, $M = P(T)^s$ with $\deg P(T) = d$. If $s = 1$, then U is cyclic. Now assume that $s \geq 2$. Let α be a primitive root modulo $P(T)$. Then there is a primitive root modulo $P(T)^s$ of the form

$$\alpha + P(T)A(T)$$

for some polynomial $A(T)$. Let $q = p^r$, where p is a prime number. Then we must have

$$(\alpha + P(T)A(T))^{(p^{rd}-1)p^{rd(s-1)-1}} \not\equiv 1 \mod P(T)^s,$$

since $\alpha + P(T)A(T)$ is a primitive root. But

$$(\alpha + P(T)A(T))^{(p^{rd}-1)p^{rd(s-1)-1}} = 1 - P(T)^{p^{rd(s-1)-1}}B(T),$$

for some polynomial $B(T)$. Hence we must have

$$p^{rd(s-1)-1} < s,$$

which implies that $s \leq 3$ since $2^{s-2} \geq s$ for $s > 3$. For $s = 2$, we have $p^{rd-1} < 2$ which implies that $rd = 1$ and we get ii). For $s = 3$, we have $p^{2rd-1} < 3$ which implies that $rd = 1$ and $p = 2$. If M is not a power of a prime, then we must have $q = 2$. For $q = 2$ and $\deg P(T) = 1$, $(\mathbb{F}_2[T]/P(T)^s)^*$ is trivial, $\mathbb{Z}/2$, or $\mathbb{Z}/4$ if $s = 1$, 2, or 3, respectively. Now the result follows because the only polynomials of degree 1 in $\mathbb{F}_2[T]$ are T and $T + 1$. □

It is known from [8] that the Galois group of the cyclotomic polynomial $\Phi_M(X)$ over $\mathbb{F}_q(T)$ is $(\mathbb{F}_q[T]/M)^*$. Thus following [7] by taking the above lemma into account, we get;

PROPOSITION 3.3. (cf; [7], Theorem 3) *$\Phi_M(\rho_R(X))$ is reducible modulo Q for every prime Q in $\mathbb{F}_q[T]$, except in the following cases:*

i) *$M = 1$ and $R = 1$,*
ii) *$M = P(T)$ and $R = 1$ for some prime $P(T)$.*
iii) *$q = p$, a prime number and $RM = P(T)^2$, $M \neq 1$ with $\deg P(T) = 1$.*

iv) $q = 2$ *and* (R, M) *is one of the following;*
(T, T^2), (T^2, T), $(T+1, (T+1)^2)$, $((T+1)^2, T+1)$, $(T, T(T+1))$, $(T+1, T(T+1))$, $(T, T^2(T+1))$, $(T^2, T(T+1))$, $(T+1, T(T+1)^2)$, $((T+1)^2, T(T+1))$, $(T, TP(T))$, $(T, T(T+1)P(T))$, $(T+1, (T+1)P(T))$, $(T+1, T(T+1)P(T))$, $(T, T^2P(T))$, $(T^2, TP(T))$, $(T, T^2(T+1)P(T))$, $(T^2, T(T+1)P(T))$, $(T+1, (T+1)^2P(T))$, $((T+1)^2, (T+1)P(T))$, $(T+1, T(T+1)^2P(T))$, $((T+1)^2, T(T+1)P(T))$, *where* $\deg P(T) > 1$.

Now let K be a finite extension of $\mathbb{F}_q(T)$ and $\mathcal{O}_K$ be the integral closure of $\mathbb{F}_q[T]$ in K. We will give criterions for the solvability of the equation

$$\Phi_M(X) \equiv 0 \mod \mathfrak{a}$$

for some ideal $\mathfrak{a}$ of $\mathcal{O}_K$. By the Chinese Remainder Theorem we may assume that $\mathfrak{a} = \mathfrak{q}^b$ for some prime ideal $\mathfrak{q}$. Let f be the inertial degree of $\mathfrak{q}$ in $K/\mathbb{F}_q(T)$. We need the following facts whose proofs are straightforward.

LEMMA 3.4. *Let* Q *be the monic irreducible polynomial generating the ideal* $\mathfrak{q} \cap \mathbb{F}_q[T]$.

i) *Let* M *be a polynomial in* $\mathbb{F}_q[T]$. *Then* $Q^f \equiv 1 \mod M$, *if and only if* $\mathfrak{q}$ *splits completely in* $K(\lambda_M)$.
ii) $\mathcal{O}_K/\mathfrak{q}$ *with* $\mathbb{F}_q[T]$*-module structure via* ρ, *is isomorphic to* $\mathbb{F}_q[T]/(Q^f - 1)$ *with usual* $\mathbb{F}_q[T]$*-module structure.*
iii) *Let* $\beta \in \mathcal{O}_K$. *Then*

$$\rho_{Q^{(b-1)f}(Q^f-1)}(\beta) \equiv 0 \mod \mathfrak{q}^b.$$

In fact, $\rho_{Q^{(b-1)}(Q^f-1)}(\beta) \equiv 0 \mod \mathfrak{q}^b$.

THEOREM 3.5. (cf; [11], Theorem 2.1) *Suppose that* $M = P_1^{a_1} P_2^{a_2} \cdots P_r^{a_r}$ *with* $a_i > 0$ *and* $\deg P_i \leq \deg P_{i+1}$. *Assume that we have chosen* P_r *so that* a_r *is maximal among* a_j*'s where* $\deg P_j = \deg P_r$. *Assume further that* $a_r \geq f$, *and that* P_r *is unramified in* K. *Let* $M_0 = \frac{M}{P_r^{a_r}}$. *Suppose that, if* M_0 *is nonconstant,* $\lambda_{M_0} \notin K$. *If* $M = P_1^{a_1} P_2^{a_2}$ *with* $P_2 = P_1 - 1$, *we also assume that* $\lambda_{P_2^{a_2}} \notin K$. *If* $q = 2$, *we assume that* $\deg P_r \geq 2$. *Then the following are equivalent;*

i) $\Phi_M(\beta) \equiv 0 \mod \mathfrak{q}^b$ *for some* $\beta \in \mathcal{O}_K$.

ii) *Either* $\mathfrak{q}$ *splits completely or is ramified in* $K(\lambda_M)$. *In the latter case,* $\mathfrak{q} \mid P_r$, *and* $\mathfrak{q}$ *splits completely in* $K(\lambda_{M_0})$ *and* $b = 1$, *or* $M = P_1^{a_1} P_2^{a_2}$ *with* $P_2 = P_1 - 1$, $\mathfrak{q} \mid P_1$, $\mathfrak{q}$ *splits completely in* $K(\lambda_{P_2^{a_2}})$, *and* $b = 1$.

Proof. Assume that $\Phi_M(\beta) \equiv 0 \mod \alpha$. Let $D = P_1^{c_1} P_2^{c_2} \cdots P_r^{c_r} \in \mathbb{F}_q[T]$ be the order of β in $\mathcal{O}_K/\mathfrak{q}^b$ as $\mathbb{F}_q[T]$-module via ρ. Then $D \mid Q^{(b-1)}(Q^f - 1)$ by Lemma 3.4. If $P_j \neq Q$ for any $j = 1, 2, \ldots, r$, then D divides $Q^f - 1$. If $c_j < a_j$ for some j, then let $H = \frac{M}{P_j^{(a_j - c_j)}}$. Then

$$\frac{\rho_M(\beta)}{\rho_H(\beta)} = \Phi_M(\beta) \prod_{R \neq M, P_j^{c_j+1} \mid R} \Phi_R(\beta) \equiv 0 \mod \mathfrak{q}^b.$$

But since $\rho_H(\beta) \equiv 0 \mod \mathfrak{q}^b$, we have

$$\frac{\rho_M(\beta)}{\rho_H(\beta)} = \frac{\rho_{\frac{M}{H}}(\rho_H(\beta))}{\rho_H(\beta)} \equiv \frac{M}{H} \mod \mathfrak{q}^b.$$

Thus $Q \mid P_j$ which is a contradiction, so $D = M$. Hence $Q^f - 1 \equiv 1 \mod M$, and so $\mathfrak{q}$ splits completely in $K(\lambda_M)$.

If $Q_i = P_j$ for some j, the as before $c_k = a_k$ for all $k \neq j$. If $\deg P_j < \deg P_r$, then $Q_i^f = P_j^f \equiv 1 \mod \prod_{k \neq j} P_k^{a_k}$. Thus $\deg P_r^f > \deg P_j^f \geq \deg P_r^{a_r}$, which is a contradiction to the assumption that $a_r \geq f$. Hence $\deg P_j = \deg P_r$. If $j = r$, we easily get $\mathfrak{q}$ splits completely in $K(\lambda_{M_0})$. If $j \neq r$, then from the preceding argument, we must have $P_j^f \equiv 1 \mod \prod_{k \neq j} P_k^{a_k}$, which can happen only when $r = 2$, $j = 1$ and $f = a_r$. That is, $M = P_1^{a_1} P_2^{a_2}$ with $\deg P_1 = \deg P_2$, and $P_1^{a_2} - 1$ is divisible by $P_2^{a_2}$. But then $P_1^{a_2} - 1 = (P_1 - 1)(P_1^{a_2 - 1} + \cdots + 1)$, $P_2 = P_1 - 1$.

We know that

$$\begin{aligned} \rho_M(\beta) &= \rho_{P_r}(\rho_{\frac{M}{P_r}}(\beta)) \\ &= P_r\{\rho_{\frac{M}{P_r}}(\beta) + \gamma(\rho_{\frac{M}{P_r}}(\beta))^q\} + (\rho_{\frac{M}{P_r}}(\beta))^{q^{\deg P_r}} \end{aligned}$$

for some $\gamma \in \mathcal{O}_K$. Since P_r is unramified in K, we have $v_{\mathfrak{q}}(P_r) = 1$. Hence if $v_{\mathfrak{q}_i}(\rho_{\frac{M}{P_r}}(\beta)) > 0$, then we have

$$v_{\mathfrak{q}}(\rho_M(\beta)) = v_{\mathfrak{q}_i}(\rho_{\frac{M}{P_r}}(\beta)) + 1$$

unless $q = 2$ and $\deg P_r = 1$. Then the rest of the proof is almost the same as in the classical case. But we must note that the condition that P_r is unramified in $K/\mathbb{Q}$ is necessary in the proof of Theorem 2.1 of [11] too. □

The remaining case is that $q = 2$ and $\deg P_r = 1$, that is, essentially M is equal to $T^{a_1}(T+1)^{a_2}$ with $0 \leq a_1 \leq a_2$.

THEOREM 3.6. *Let $q = 2$ and $M = T^{a_1}(T+1)^{a_2}$ with $0 \leq a_1 \leq a_2$. Assume that $\lambda_{T^{a_1}} \notin K$ if $a_1 > 1$ and $\lambda_{(T+1)^{a_2}} \notin K$ if $a_2 > 1$.*

If $a_2 = 1$, then $\Phi_M(X) \equiv 0 \mod \mathfrak{q}^b$ always has a solution.

If $a_1 > 1$, and T and $T+1$ are unramified in K, then the followings are equivalent;

i) $\Phi_M(\beta) \equiv 0 \mod \mathfrak{q}^b$ *for some* $\beta \in \mathcal{O}_K$.

ii) *Either* $\mathfrak{q}$ *splits completely or is ramified in* $K(\lambda_M)$. *In the latter case,* $\mathfrak{q} \mid T$ ($\mathfrak{q} \mid (T+1)$, *respectively*) *and* $\mathfrak{q}$ *splits completely in* $K(\lambda_{(T+1)^{a_2}})$ ($K(\lambda_{T^{a_1}})$, *respectively*) *and* $b = 1$.

If $a_1 = 0$, $a_2 > 1$, and $(T+1)$ is unramified in $K/\mathbb{F}_q(T)$, then the followings are equivalent;

i) $\Phi_M(\beta) \equiv 0 \mod \mathfrak{q}^b$ *for some* $\beta \in \mathcal{O}_K$.

ii) *Either* $\mathfrak{q}$ *splits completely or is ramified in* $K(\lambda_M)$. *In the latter case,* $\mathfrak{q} \mid (T+1)$, *and* $b = 1$.

Proof. The first assertion follows from the fact that $\Phi_{T(T+1)}(X) = X + 1$. Let $\mathfrak{q} \mid T$ and $\rho_{T^{a_1}(T+1)^{a_2}}(\beta) \equiv 0 \mod \mathfrak{q}$. Then $v_{\mathfrak{q}}(\beta) > 0$. Thus $v_{\mathfrak{q}}(\rho_{T^{a_1-1}(T+1)^{a_2}}(\beta)) > 1$ if $a_1 - 1 > 0$. Hence if $a_1 > 1$,

$$v_{\mathfrak{q}}(\rho_M(\beta)) = v_{\mathfrak{q}}(\rho_{\frac{M}{T}}(\beta)) + 1.$$

Now the second assertion is exactly the same as Theorem 3.5. The method just given works for the third assertion. □

COROLLARY 3.7. *Let $N = Q_1^{b_1}Q_2^{b_2}\cdots Q_s^{b_s}$ for distinct irreducible polynomials in $\mathbb{F}_q[T]$. Suppose that $q > 2$ or $\deg P_r \geq 2$ in case $q = 2$. Then the following are equivalent;*

i) $\Phi_M(A) \equiv 0 \mod N$ *for some* $A \in \mathbb{F}_q[T]$.

ii) $Q_i \equiv 1 \mod M$ *or* $Q_i = P_r \equiv 1 \mod M_0$ *and* $b = 1$.

Similar arguments give the following variant of Theorem 3.5.

THEOREM 3.8. *Notations are as in the* Theorem 3.5. *Suppose that* $q > 2$ *and all the* P_i*'s are unramified in* K *and that* $\lambda_{P_i^{a_i}} \notin K$, *for each* i. *Then the following are equivalent;*

i) $\Phi_M(\beta) \equiv 0 \mod \mathfrak{q}^b$ *for some* $\beta \in \mathcal{O}_K$.

ii) *Either* $\mathfrak{q}$ *splits completely or is ramified in* $K(\lambda_M)$. *In the latter case,* $\mathfrak{q} \mid P_i$ *for some* i, $\mathfrak{q}$ *splits completely in* $K(\lambda_{\frac{M}{P_i^{a_i}}})$ *and* $b = 1$.

4. Primitive Factors

In this section we consider the function field analogue of the equation $X^n - Y^n$. For a polynomial M of degree m in $\mathbb{F}_q[T]$, we define

$$\mathcal{P}_M(X,Y) = Y^{q^m}\rho_M(X/Y),$$

$$\mathcal{Q}_M(X,Y) = \mathcal{P}_M(X,Y)/X,$$

and

$$\mathcal{F}_M(X,Y) = Y^{\phi(M)}\Phi_M(X/Y).$$

REMARK. 1. If we replace $\Phi_M(X)$ by $\mathcal{F}_M(X,Y)$ and $\rho_M(X)$ by $\mathcal{P}_M(X,Y)$, Proposition 1.1 also holds.

2. One can think $\rho_M(X)$ as an analogue of the classical cyclotomic polynomial $X^m - 1$. Thus $\mathcal{P}_M(X,Y)$ (resp. $\mathcal{Q}_M(X,Y)$) can be thought as an analogue of the equation $X^n - Y^n$ (resp. $(X^n - Y^n)/(X - Y)$) of the classical case, since $X^n - Y^n = Y^n((\frac{X}{Y})^n - 1)$.

PROPOSITION 4.1. *Let* M *and* N *be two monic polynomials in* $\mathbb{F}_q[T]$ *of degree* m *and* n, *respectively.*

a)

$$\mathcal{P}_{MN}(X,Y) = \mathcal{P}_M(\mathcal{P}_N(X,Y), Y^{q^n}) = \mathcal{P}_N(\mathcal{P}_M(X,Y), Y^{q^m}),$$

and

$$\mathcal{Q}_{MN}(X,Y) = \mathcal{Q}_M(X\mathcal{Q}_N(X,Y), Y^{q^n})\mathcal{Q}_N(X,Y).$$

Thus we have

$$\mathcal{P}_M(X,Y) \mid \mathcal{P}_{MN}(X,Y) \qquad \text{and} \qquad \mathcal{Q}_M(X,Y) \mid \mathcal{Q}_{MN}(X,Y).$$

b) *If* $m > n$, *then*

$$\mathcal{P}_{M+N}(X,Y) = \mathcal{P}_M(X,Y) + Y^{q^m-q^n}\mathcal{P}_N(X,Y),$$

and

$$\mathcal{Q}_{M+N}(X,Y) = \mathcal{Q}_M(X,Y) + Y^{q^m-q^n}\mathcal{Q}_N(X,Y).$$

c)

$$\prod_{c\in\mathbb{F}_q} \mathcal{P}_{MT+c}(X,Y) = \mathcal{P}_{MT}^q(X,Y) - Y^{(q^{m+1}-1)(q-1)}X^{q-1}\mathcal{P}_{MT}(X,Y),$$

and

$$\prod_{c\in\mathbb{F}_q} \mathcal{Q}_{MT+c}(X,Y) = \mathcal{Q}_{MT}^q(X,Y) - Y^{(q^{m+1}-1)(q-1)}\mathcal{Q}_{MT}(X,Y).$$

Proof. The properties for $\mathcal{Q}$ follows from those of $\mathcal{P}$. a) follows from the facts that $\rho_{MN}(X) = \rho_M(\rho_N(X))$ and $\mathcal{P}_N(X,Y) = Y^{q^n}\rho_N(X/Y)$. b) follows from $\rho_{M+N} = \rho_M + \rho_N$, c) follows from b).□

PROPOSITION 4.2. *If* $\mathcal{P}_M(A,B)$ *is prime to* N, *then* $\frac{\mathcal{P}_{MN}(A,B)}{\mathcal{P}_M(A,B)}$ *is prime to* $\mathcal{P}_M(A,B)$.

Proof. By Proposition 4.1, a)

$$\frac{\mathcal{P}_{MN}(A,B)}{\mathcal{P}_M(A,B)} \equiv NB^{q^{m+n}-q^m} \mod \mathcal{P}_M(A,B),$$

where $m = \deg M$, $n = \deg N$. Since $(B, \mathcal{P}_M(A,B)) = 1$ from the definition, we get the result. □

PROPOSITION 4.3. (cf; [12], P1.2) *Let* P *denote a monic irreducible polynomial.*

a) *If* $(M,N) = D$, *then*

$$\big(\mathcal{P}_M(A,B), \mathcal{P}_N(A,B)\big) = \mathcal{P}_D(A,B),$$

and

$$\big(\mathcal{Q}_M(A,B), \mathcal{Q}_N(A,B)\big) = \mathcal{Q}_D(A,B).$$

b) $\prod_{P|N} \mathcal{Q}_P(A,B)$ *divides* $\mathcal{Q}_N(A,B)$.
c) $\big(\mathcal{Q}_N(A,B), A\big) = (N,A)$.
d) *If* $P^e \parallel A$, *and* $N = P^r M$ *with* $P \nmid M$, *then* $P^{e+r} \parallel \mathcal{P}_N(A,B)$.
e) *If* $P \mid A$, *then* $P^e \parallel N$ *if and only if* $P^e \parallel \mathcal{Q}_N(A,B)$. *In particular, if* $P \mid A$, *then* $P^2 \nmid \mathcal{Q}_P(A,B)$.

Proof. a) follows from the methods of [10] using Euclidean algorithm and b), c) of Proposition 4.1. b) is an easy consequence of a). For c), let

$$\rho_N(X) = \sum_{i=0}^{n} C_i X^{q^i}$$

with $C_0 = N$. Then

$$\begin{aligned}\mathcal{Q}_N(A,B) &= \sum C_i A^{q^i-1} B^{q^d-q^i} \\ &\equiv C_0 B^{q^d-1} \mod A.\end{aligned}$$

Thus $\big(\mathcal{Q}_N(A,B), A\big) = (N,A)$, since $(A,B) = 1$. Now d) follows from c) and e) from d). □

Now we let A and B be two relatively prime polynomials in $\mathbb{F}_q[T]$, and N a polynomial of degree $n > 0$. A prime divisor of $\mathcal{P}_N(A,B)$, which is prime to $\mathcal{P}_M(A,B)$ for all divisor M of N not equal to N, is called a *primitive factor*. Then we have the following analogue of Euler's.

PROPOSITION 4.4. (cf; [4], Theorem I, [12], P1.4) *Let* P *be a monic prime in* $\mathbb{F}_q[T]$. *Then the followings are equivalent.*

i) P *is a primitive factor of* $\mathcal{P}_N(A,B)$.
ii) $P \mid \mathcal{F}_N(A,B)$ *and* $P \equiv 1 \mod N$.
iii) $P \mid \mathcal{F}_N(A,B)$ *and* $P \nmid N$.

Proof. Let P be a primitive factor. Then $P \nmid \mathcal{P}_1(A,B) = A$. Hence $P \nmid B$ also. Choose $C \in \mathbb{F}_q[T]$ so that $A \equiv BC \mod P$. Then

$$\begin{aligned}\mathcal{P}_N(A,B) &\equiv B^{q^n}\rho_N(BC/B) \mod P \\ &\equiv B^{q^n}\rho_N(C) \mod P.\end{aligned}$$

Since $(B,P) = 1$, P must divide $\rho_N(C)$. It is well-known that $P \mid \rho_{P-1}(C)$. View $\mathcal{M} = \mathbb{F}_q[T]/(P)$ as an $\mathbb{F}_q[T]$-module via ρ. From the primality, $ord(C) = N$ in $\mathcal{M}$, hence N must divide $P-1$. Thus i) implies ii). ii) implies iii) is clear. The proof that iii) implies i) is exactly the same as the proof of (P1.4), [12]. □

Now let $\mathcal{P}_N(A,B) = P_1^{\alpha_1}\cdots P_k^{\alpha_k}$ be the factorization of $\mathcal{P}_N$, with $P_1,\ldots P_s$ all distinct prime primitive divisors of $\mathcal{P}_N$. Put

$$\mathbf{P}_N(A,B) = \prod_{i=1}^{s} P_i^{\alpha_i},$$

and call $\mathbf{P}(N)$ the *arithmetic primitive factor* of $\mathcal{P}_N$. From Proposition 1.1, e), we have

$$\mathcal{F}_N(X,Y) = \prod_{D|N} \mathcal{P}_{N/D}(X,Y)^{\mu(D)},$$

and so by the Möbius inversion formula,

$$\mathcal{P}_N(X,Y) = \prod_{N'|N} \mathcal{F}_{N'}(X,Y).$$

We call $\mathcal{F}_N(A,B)$ the *algebraic primitive factor* of $\mathcal{P}_N(A,B)$. Let

$$\omega = \frac{\mathcal{F}_N(A,B)}{\mathbf{P}_N(A,B)}$$

THEOREM 4.5. (cf; [4], Theorem IV) *If* $\deg N > 0$, *then* $\omega = 1$, *unless* $\mathbf{P}_{N'}(A,B) \equiv 0 \mod P$, *where* $N = P^\alpha N'$, *and* $P \nmid N'$. *In the latter case, if* q *is odd,* $\omega = P$, *and if* q *is even,* $\omega = P(P-1)$ *when* $(B,N) = 1$, $N = P(P-1)$ *with* P, $P-1$ *primes, and* $\omega = P$ *otherwise.*

Proof. Note that

$$\mathcal{F}_N(A,B) = \frac{\mathcal{F}_{N'}(\mathcal{P}_{P^\alpha}, B^{q^{\alpha \deg P}})}{\mathcal{F}_{N'}(\mathcal{P}_{P^{\alpha-1}}, B^{q^{(\alpha-1)\deg P}})},$$

if $N = P^\alpha N'$ with $P \nmid N'$. Since $\mathcal{P}_{P^\alpha} \equiv A^{q^{\alpha \deg P}} \mod P$, we have

$$\mathcal{F}_{N'}(\mathcal{P}_{P^\alpha}, B^{q^{\alpha \deg P}}) \equiv \mathcal{F}_{N'}(A,B)^{q^{\alpha \deg P}} \mod P.$$

Now one can follow the proof of [4], Theorem IV by replacing $V(n)$ by $\mathcal{P}_N$ and $F(n)$ by $\mathcal{F}_N$. However the fact that $P \equiv 1 \mod N'$ implies only that $\deg P \geq \deg N'$. If q is odd, such a prime P is unique. When q is even, then there can exist another prime Q so that $N = PQ$ and $Q = P - 1$. In this case, $\mathcal{F}_{P-1}(A,B) \equiv B^{q^{\deg P - 1}} - 1 \mod P$ and $\mathcal{F}_P(A,B) \equiv B^{q^{\deg P - 1}} - 1 \mod (P-1)$. Thus $\mathcal{F}_{P-1} \equiv 0 \mod P$ and $\mathcal{F}_P \equiv 0 \mod (P-1)$ if and only if $(B,N) = 1$. The rest of the proof is the same as that of Theorem IV of [4]. □

LEMMA 4.6. *Write* $n = \deg N$, $a = \deg A$, *and* $b = \deg B$. *Then, if* $q > 2$,

$$\deg \mathcal{P}_N(A,B) = \begin{cases} aq^n, & \text{if } a > b \\ bq^n + q^{n+a-b-1}, & \text{if } 0 \leq b-a < n \\ bq^n + n + a - b, & \text{if } b - a \geq n. \end{cases}$$

Proof. Write $\mathcal{P}_N = \sum_{i=0}^{n} A_i A^{q^i} B^{q^n - q^i}$. Then we know from Proposition 1.1 of [7] that $\deg A_i = (n-i)q^i$. Thus

$$r_i = \deg A_i A^{q^i} B^{q^n - q^i} = (n + a - b - i)q^i + bq^n.$$

Consider the function $f(x) = (n + a - b - x)q^x + bq^n$. $f(x)$ attains its maximum at $x = n + a - b - \frac{1}{\log q}$. Now an easy calculation gives the result. □

For the case $q = 2$ we need the following lemma.

LEMMA 4.7. *Let* $\rho_{T^k}(X) = \sum_i a_i^{(k)} X^{q^i}$. *Then*

$$a_i^{(k)} = T^{q^i(k-i)} + T^{q^i(k-i)-q^{i-1}} + \text{lower terms.}$$

Hence for a monic polynomial N *of degree* n *write* $\rho_N(X) = \sum a_i X^{q^i}$, *we have*

$$a_i = T^{q^i(n-i)} + T^{q^i(n-i)-q^{i-1}} + \text{lower terms.}$$

Proof. Easy induction on k gives the result. □

LEMMA 4.8. *Let* $q = 2$. *Then*

$$\deg \mathcal{P}_N(A,B) = \begin{cases} a2^n, & \text{if } a > b+1 \\ b2^n + 2^{n+a-b-1} - 2^{n+a-b-3}, & \text{if } 0 \le b-a < n-2 \\ b2^n + n + a - b, & \text{if } b-a \ge n-1. \end{cases}$$

Proof. The difference from the proof of Lemma 4.6 is that $\frac{1}{2} < \log 2 < 1$ and that $r_{n-k-1} = r_{n-k-2}$ for $0 \le k = b-a < n-1$. But Lemma 4.7 fills the gap. □

We want to know whether $\mathcal{P}_N(A,B)$ possesses a primitive factor other than units if $\deg N > 0$. To do this it suffices to show that $\deg \mathbf{P}_N(A,B) > 0$.

PROPOSITION 4.9. *Suppose that* $q > 2$. *We have*

$$\deg \mathcal{F}_N(A,B) > n,$$

except the following cases

i) $n = 1$ *and* $a = b = 0$, *in which case* $\deg \mathcal{F}_N = 1$,
ii) $n = 2$, $N = P^2$ *and* $a = b = 0$, *in which case* $\deg \mathcal{F}_N = 2$,
iii) $n = 2$, $N = PQ$ *a product of distinct primes,* $a = b = 0$, *in which case* $\deg \mathcal{F}_N = 1$.

Proof. From e) of Proposition 1.1 $\deg \mathcal{F}_N = \sum_{D|N} \mu(D) \deg \mathcal{P}_{\frac{N}{D}}$. If $a > b$, then from Lemma 4.6 we see that $\deg \mathcal{F}_N = a\phi(N)$. Since $a > 0$, $a\phi(N) \geq (q-1)^n > n$, as desired. Now assume that $b \geq a$. Then

$$\begin{aligned}
&\deg \mathcal{F}_N(A,B) \\
&= \sum_{D|N} \mu(D) \deg \mathcal{P}_{\frac{N}{D}}(A,B) \\
&= \sum_{D|N} \mu(D)(bq^{\deg \frac{N}{D}} + q^{\deg \frac{N}{D}+a-b-1}) \\
&+ \sum_{D|N, \deg \frac{N}{D} \leq b-a} \mu(D)\{bq^{\deg \frac{N}{D}} + \deg \frac{N}{D} \\
&\qquad + a - b - bq^{\deg \frac{N}{D}} - q^{\deg \frac{N}{D}+a-b-1}\} \\
&= (b + q^{a-b-1})\phi(N) \\
&+ \sum_{D|N, \deg \frac{N}{D} \leq b-a} \mu(D)(\deg \frac{N}{D} + a - b - q^{\deg \frac{N}{D}+a-b-1}).
\end{aligned}$$

For $D \neq N$ and $\deg \frac{N}{D} + a - b \leq 0$, we have

$$|deg \frac{N}{D} + a - b - q^{\deg \frac{N}{D}+a-b-1}| < b - a - 1 + \frac{1}{q},$$

and for $D = N$,

$$|deg \frac{N}{D} + a - b - q^{\deg \frac{N}{D}+a-b-1}| < b - a + \frac{1}{q}.$$

Thus

$$\begin{aligned}
&\sum_{D|N, \deg \frac{N}{D} \leq b-a} \mu(D)(\deg \frac{N}{D} + a - b - q^{\deg \frac{N}{D}+a-b-1}) \\
&< (b - a - 1 + \frac{1}{q})(\text{number of monic divisors of } N) + 1 \\
&\leq (b - a - 1 + \frac{1}{q})2^n + 1.
\end{aligned}$$

Then

$$\begin{aligned}\deg \mathcal{F}_N(A,B) &> (b+q^{a-b-1})(q-1)^n - (b-a-1+\frac{1}{q})2^n - 1\\ &\geq (b+q^{a-b-1})2^n - (b-a-1+\frac{1}{q})2^n - 1\\ &= \{(1+a) - \frac{1}{q}(1-q^{a-b})\}2^n - 1\\ &> (1-\frac{1}{q})2^n - 1\end{aligned}$$

But $(1-\frac{1}{q})2^n - 1 < n$ only if $n = 1$ or $n = 2$, $q = 3$. For $n = 1$, $\deg \mathcal{F}_N(A,B) = (q-1)b + 1$, so we get i). Now assume $n = 2$ and $q = 3$. If $N = P$ a prime, then

$$\deg \mathcal{F}_N(A,B) = \begin{cases} 9b+3-a, & \text{if } b-a=0\\ 9b+1-a, & \text{if } b-a=1\\ 9b+2-b, & \text{if } b-a\geq 2.\end{cases}$$

If $N = P^2$, then

$$\deg \mathcal{F}_N(A,B) = \begin{cases} 6b+2, & \text{if } b-a=0\\ 6b+1, & \text{if } b-a\geq 1.\end{cases}$$

If $N = PQ$ a product of distinct primes, then

$$\deg \mathcal{F}_N(A,B) = \begin{cases} 3b+1+a, & \text{if } b-a=0 \text{ or } 1\\ 4b & \text{if } b-a\geq 2.\end{cases}$$

Therefore we get the result. □

Now we can get easily from Proposition 4.7 and Theorem 4.5 the following analogue of the theorem of Bang and Zsigmondy.

THEOREM 4.10. (cf; [4], Theorem V) *Suppose that $q > 2$. If $\deg N > 0$, then $\mathcal{P}_N(A,B)$ possesses at least one primitive factor other than units, except in the case $q = 3$, $N = (T+\alpha)(T+\alpha+1)$, and $A = \pm 1$, $B = \pm 1$. In this case*

$$\mathcal{P}_{(T+\alpha)(T+\alpha+1)}(\pm 1, \pm 1) = \pm(T+\alpha+1)^2(T+\alpha-1),$$

and

$$\mathcal{P}_{(T+\alpha)}(\pm 1, \pm 1) = \pm(T+\alpha+1), \mathcal{P}_{(T+\alpha 1)}(\pm 1, \pm 1) = \pm(T+\alpha-1).$$

REMARK. When $q = 2$, above method works for $b - a < -1$ or $b - a > n - 2$. However we do not know in general because of the indeterminacy for the case $b - a = n - 2$ in Lemma 4.8.

References

[1] Apostol, T. M., *Resultant of Cyclotomic Polynomials*, Proc. Amer. Math. Soc. **24** (1970), 457–463.

[2] ———, *Resultant of Cyclotomic Polynomials $F_m(ax)$ and $F_n(bx)$*, Math. Comp. **29** (1975), 1-6.

[3] Bae, S. and Hahn, S., *On the Ring of Integers of Cyclotomic Function Fields*, Bull. of KMS **29** (1992), 153–163.

[4] Birkhoff, G. D. and Vandiver, H. S., *On the integral divisors of $a^n - b^n$*, Ann. Math. **5** (1904), 173-180.

[5] Carlitz, L., *A Class of Polynomials*, Trans. Amer. Math. Soc. **43** (1938), 167–182.

[6] Cheng, C. C., McKay, J. H., and Wang, S. S., *Resultants of Cyclotomic Polynomials*, Proc. Amer. Math. Soc. **123**, (1995), 1053-1059.

[7] Golomb, S. W., *Cyclotomic Polynomials and Factorization Theorems*, Math. Monthly **85** (1978), 734-737.

[8] Hayes, D., *Explicit Class Field Theory in Rational Function Fields*, Trans. Amer. Math. Soc. **189** (1974), 77-91.

[9] Lünenburg, H., *Resultanten von Kreisteilungspolynomen*, Arch. Math. **42** (1984), 139-144.

[10] Möller, K., *Untere Schranke für die Anzahl der Primzahlen, aus denen x, y, z der Fermatschen Gleichung $x^n + y^n = z^n$ bestehen muss*, Math, Nachr. **14** (1955), 25-28.

[11] Mollin, R. A., *On the Cyclotomic Polynomials*, Journal of Number Th. **17** (1983), 165-175.

[12] Ribenboim, P., *Catalan's Conjecture*, Academic Press, 1994.

Department of Mathematics
KAIST
Taejon 305-701, Korea