Math. J. Okayama Univ. 37(1995), 27-36

ON VALUES OF CYCLOTOMIC POLYNOMIALS. II

KAORU MOTOSE

Let q be a prime divisor of a Mersenne number $2^p - 1$ where p is prime. Then p is the order $|2|_q$ of $2 \bmod q$. Thus p is a divisor of $q-1$ and $q > p$. This shows that there exist infinitely many prime numbers. In this argument, $p = |2|_q$ is most important. We generalized this to the next theorem in the recent paper [1]. In this paper, we shall use this freely without references.

$\Phi_n(x)$ represents the cyclotomic polynomial and all Latin letters represent natural numbers. The p-part of the natural number m means the largest power of a prime p dividing m.

Theorem A. *We set $n, a \geq 2$ and $|a|_p$ is the order of $a \bmod p$ for a prime p. Then p is a prime divisor of $\Phi_n(a)$ if and only if $(a,p) = 1$ and $n = p^e|a|_p$ where $e \geq 0$. A prime divisor p of $\Phi_n(a)$ for $n \geq 3$ has the property such that $n = |a|_p$ or p is the p-part of $\Phi_n(a)$ according as $e = 0$ or not.*

1. Square free divisors of cyclotomic numbers. The prime numbers p satisfying $2^{p-1} \equiv 1 \bmod p^2$ are 1093 or 3511 for $p < 6 \times 10^9$. The prime numbers p satisfying $3^{p-1} \equiv 1 \bmod p^2$ are 11 or 1006003 for $p < 10^7$. This fact together with the next shows $\Phi_n(2)$ and $\Phi_n(3)$ are almost square free.

Theorem 1.1. *Assume $r \geq 2$. Then p^r divides $\Phi_d(a)$ for some d if and only if $a^{p-1} \equiv 1 \bmod p^r$.*

Proof. If p^r divides $\Phi_d(a)$ then d is the order of $a \bmod p$ and so d divides $p-1$. Thus $a^d - 1$ divides $a^{p-1} - 1$. This implies our assertion since $\Phi_d(a)$ divides $a^d - 1$. Conversely, if $a^{p-1} \equiv 1 \bmod p^r$, then p^r divides $a^{p-1} - 1 = \prod_{d|p-1} \Phi_d(a)$ and $d = |a|_p$ for the only divisor d of $p-1$. Thus we have the assertion.

The prime numbers p satisfying $10^{p-1} \equiv 1 \bmod p^2$ are 3 or 487 for $p < 10^6$.

Example 1.1. Cyclotomic numbers $\Phi_{364}(2), \Phi_{1755}(2), \Phi_5(3), \Phi_{486}(10)$ have divisors $1093^2, 3511^2, 11^2, 487^2$, respectively.

The next shows that Fermat numbers and Mersenne numbers are almost square free.

Corollary 1.1. *Assume that p and q are primes. If p^2 divides $2^{2^n}+1$ or 2^q-1, then $2^{p-1} \equiv 1 \bmod p^2$. If p^2 divides $(10^q-1)/9$, then $10^{p-1} \equiv 1 \bmod p^2$.*

Proof. Theorem implies our assertion from

$$2^{2^n}+1 = \Phi_{2^{n+1}}(2), \quad 2^q - 1 = \Phi_q(2) \text{ and } \frac{10^q-1}{9} = \Phi_q(10).$$

The next needs later. It is easy to see $np = |a+p|_{p^2}$ from the conditions of this proposition.

Proposition 1.2. *If p^2 divides $\Phi_n(a)$ for $n \geq 3$, then p is the p-part of $\Phi_n(a+p)$.*

Proof. The condition implies that $n = |a+p|_p$ and $(a+p)^n \equiv npa^{n-1}+1 \not\equiv 1 \bmod p^2$. This means p is the p-part of $\Phi_n(a+p)$.

Example 1.2. We know a cyclotomic number $\Phi_5(3) = 11^2$ and so we can find that $55 = |14|_{11^2}$ and 11 is the 11-part of $\Phi_5(14)$.

We can consider from the table in [3-5] that almost cyclotomic numbers are square free and all cyclotomic numbers are qubic free. But the next shows this is incorrect.

Proposition 1.3. *If p is a divisor of $\Phi_n(a)$ and p is not a divisor of n, then p^r is a divisor of $\Phi_n(a^{p^{r-1}})$.*

Proof. Since $\Phi_n(a)$ is a divisor of $a^n - 1$, we have $a^n \equiv 1 \bmod p$ and so $a^{np^{r-1}} \equiv 1 \bmod p^r$. It follows from the equation $(a^{p^{r-1}})^n - 1 = \prod_{d|n} \Phi_d(a^{p^{r-1}})$ that p is a divisor of $\Phi_d(a^{p^{r-1}})$ for the only divisor d of n. Thus we have our assertion from the equation $d = |a^{p^{r-1}}|_p = |a|_p = n$.

Example 1.3. $\Phi_6(3^{7^3})$ has a divisor 7^4 by $\Phi_6(3) = 7$.

2. Primitive roots. As was stated in [1], it is easy to see that n is a divisor of $\Phi_{n-1}(a)$ if and only if n is a prime and a is a primitive root of p. So we can restate Artin's conjecture: For the integer $b \geq 2$, the set $A(b) = \{n\colon n|\Phi_{n-1}(b)\}$ is infinite.

In this point of view, we shall give a new proof of the existence of the primitive root for every prime.

Theorem 2.1. *There exists an integer a with $|a|_p = p-1$ for every prime p.*

Proof. We set $f(x) = \prod_{b=1}^{p-1}(x-b)$ and P is a prime ideal, containing p, in the ring of the algebraic integers. Then we have $f(x) \equiv x^{p-1} - 1 \bmod P$ and so $f(\zeta_{p-1}) \equiv 0 \bmod P$ where ζ_{p-1} is a primitive $(p-1)$-th root of 1. On the other hand $\prod_{b=1}^{p-1} \Phi_{p-1}(b)$ has a factor $f(\zeta_{p-1})$ and hence $\prod_{b=1}^{p-1} \Phi_{p-1}(b) \in P \cap \mathbf{Z} = p\mathbf{Z}$. Thus p divides $\Phi_{p-1}(b)$ for some b and our assertion follows.

We shall also give a new proof of the existence of a primitive root for every odd prime power.

Theorem 2.2. *There exists an integer a with $|a|_{p^r} = \phi(p^r)$ for every odd prime power p^r.*

Proof. There exists an integer a such that p is a divisor of $\Phi_{p-1}(a)$ by the above theorem. We may assume from Proposition 1.2 that p is the p-part of $\Phi_{p-1}(a)$. We set $m = |a|_{p^r}$. Then m is a multiple of $p-1$ by $p-1 = |a|_p$ and m is a divisor of $\phi(p^r) = p^{r-1}(p-1)$. Thus we can obtain $m = (p-1)p^s$ where $s \leq r-1$ and $\prod_{d|m} \Phi_d(a) = a^m - 1 \equiv 0 \bmod p^r$. It follows from $|a|_p = p-1$ that

$$\prod_{k=0}^{s} \Phi_{(p-1)p^k}(a) \equiv 0 \bmod p^r.$$

This equation implies $r \leq s+1$ since p is the p-part of $\Phi_{(p-1)p^k}(a)$ for $k \geq 1$. Hence the proof is complete from $s = r-1$.

Theorem 2.1 together with Proposition 1.3 shows that every prime power p^r for a prime $p > 3$ can be a factor of $\Phi_n(a)$ for $n \geq 3$. But $4, 6, 14, 22, \cdots$ and $9, 15, 33, \cdots$ can not be divisors of $\Phi_n(a)$ for $n \geq 3$. So, we shall present the next theorem.

Theorem 2.3. *We set $m, a \geq 2$, $n \geq 3$ and p is the maximal prime divisor of n. Then a composite number m is a divisor of $\Phi_n(a)$ if and only if $a^n \equiv 1 \bmod m$, $n = |a|_q$ for every prime divisor q of m different from p, and $n = p^{\ell_p}|a|_p$ in case p is a divisor of m.*

Proof. Necessity follows easily from Theorem A. So, we assume the sufficient condition. Then, in case $p|m$, p is a divisor of $\Phi_n(a)$ and p is p-part of m. It follows from $n = |a|_q$ that q divides $a^n - 1 = \prod_{d|n} \Phi_d(a)$. Hence q divides only $\Phi_n(a)$ by virtue of $n = |a|_q$. This shows also that every q-part of m is a divisor of $\Phi_n(a)$. We have our assertion.

3. Common divisors of cyclotomic numbers. The next shows cyclotomic numbers of distinct degrees are almost relatively prime.

Theorem 3.1. *Assume $m > n \geq 2$. Then the following are equivalent.*

(1) *p is a common prime divisor of $\Phi_m(a)$ and $\Phi_n(a)$.*
(2) *$(\Phi_m(a), \Phi_n(a)) = p$ is prime.*
(3) *$(m, \Phi_m(a)) = p$ is prime and m/n is a power of p.*
(4) *$m = p^\alpha |a|_p$ and $n = p^\beta |a|_p$ for some prime p and $\alpha \geq 1$.*

Proof. It follow from (1) that $m = p^\alpha |a|_p$ and $n = p^\beta |a|_p$ and so $m = p^\gamma n$ for $\gamma \geq 1$ by $m > n$. Thus (1) is equivalent to (4). Other equivalence's follow easily from the same argument.

Example 3.1. For example, $p = 3$, $\Phi_{54}(2) = 3 \cdot 87211$, $\Phi_{18}(2) = 3 \cdot 19$ has the property of the above theorem.

The next shows the characterization in order to that cyclotomic numbers of the same degree have the common divisor.

Theorem 3.2. *Assume $n, a, b \geq 2$ and an odd prime p does not divide n. Then the following are equivalent.*

(1) *p^s is the common divisor of $\Phi_n(a)$ and $\Phi_n(b)$.*
(2) *$n = |a|_p$, $a^n \equiv 1$ and $b \equiv a^k \bmod p^s$ for $(k, n) = 1$.*
(3) *$\Phi_n(a) \equiv 0$ and $b \equiv a^k \bmod p^s$ for $(k, n) = 1$.*

Proof. (1) implies that $a^n \equiv b^n \equiv 1 \bmod p^s$, $n = |a|_p = |b|_p$ and so $n = |a|_{p^s} = |b|_{p^s}$. Thus (1) is equivalent to (2) from Theorem 2.2. It is easy to see the equivalence of (2) and (3).

Remark 3.2. In the above theorem, we can see

$$\Phi_n(x) \equiv \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (x - a^k) \bmod p.$$

Corollary 3.2.1. *Assume $n, a \geq 2$ and $(n, \Phi_n(a)) = 1$. Then $\Phi_n(a)$ divides properly $\Phi_n(a^k)$ for $k \geq 2$ and $(k, n) = 1$.*

Proof. Theorem implies that every prime part of $\Phi_n(a)$ is a divisor of $\Phi_n(a^k)$ and $\Phi_n(a^k) > \Phi_n(a)$ (see [1, Corollary 1]).

Example 3.2.1. $\Phi_{10}(2) = 11$ is a divisor of $\Phi_{10}(2^k)$ for $k = 3, 7, 9, \cdots$. $\Phi_5(3) = 11^2$ is a divisor of $\Phi_5(3^k)$ for $k = 2, 3, 4, 6, \cdots$.

Corollary 3.2.2. *Assume $a^k \equiv b \neq 1$ and $\Phi_n(a) \equiv 0 \bmod p$, where $n, a, k \geq 2$, $(k, n) = 1$ and $(n, \Phi_n(a)) = 1$. Then p is a divisor of $\Phi_n(b)$. If $b < a$, then $\Phi_n(a)$ is composite. If $b > a$, then $\Phi_n(b)$ is composite.*

Proof. Theorem together with [1, Corollary 1] implies our corollary.

Example 3.2.2. We can see that $\Phi_{10}(7) = 11 \cdot 191$, $7^3 \equiv 2 \bmod 11$, $7^3 \equiv 152 \bmod 191$, $\Phi_{10}(2) = 11$, and $\Phi_{10}(152)$ has a divisor 191.

4. Cyclotomic composite numbers. We can obtain cyclotomic composite numbers from Corollaries 3.2.1 and 3.2.2. The next is easy to know from some numerical examples. For example, $\Phi_{18}(2) = 3 \cdot 19$.

Theorem 4.1. *Assume that $(n, \Phi_n(a)) > 1$ where $n \geq 3$, $a \geq 2$ and $(n, a) \neq (6, 2)$. Then $\Phi_n(a)$ is composite.*

Proof. We can see $(n, \Phi_n(a))$ is a prime p from Theorem 3.1. If $p = \Phi_n(a)$, then we have the next inequality as in [1, Corollary 2]

$$p = \Phi_n(a) > a^{\phi(n)-1} \geq 2^{p-2}.$$

So we have $(n, a) = (6, 2)$.

The next is the generalization of the well known result for Mersenne numbers. The proof in P. Ribenboim's book [2] is incorrect.

Theorem 4.2. *Assume that p is an odd prime, $q = 2p + 1$ and $q \geq a > 1$. Then q is prime and $\left(\frac{a}{q}\right) = 1$ if and only if q is a divisor of $\Phi_p(a)$. In this case, p is a Sophie Germain prime and q is the smallest prime divisor of $\Phi_p(a)$.*

Proof. If q is prime and $\left(\frac{a}{q}\right) = 1$, then $a^p = a^{(q-1)/2} \equiv \left(\frac{a}{q}\right) = 1 \bmod q$ and $q \geq a$ is a divisor of $a^p - 1 = \Phi_p(a)(a-1)$. Thus we have q

is a divisor of $\Phi_p(a)$. Conversely, if q is a divisor of $\Phi_p(a)$ and r is a prime divisor of q, then $p = |a|_r$ and $kp+1 = r$ is a divisor of $q = 2p+1$ for some $k \geq 1$. Thus we have $q = r$ is prime and $\left(\frac{a}{q}\right) \equiv a^{(q-1)/2} = a^p \equiv 1 \bmod q$.

Example 4.2. 1. In case $a = 2$, this is well known for Mersenne numbers. If $p > 3$ is Sophie Germain prime and $p \equiv -1 \bmod 4$, then $\Phi_p(2) = 2^p - 1$ has a proper prime divisor $2p+1$. For example, $2^{11} - 1$ has a divisor 23.

2. In case $a = 3$, if $p > 2$ is Sophie Germain prime and $p \equiv -1 \bmod 3$, then $\Phi_p(3) = (3^p - 1)/2$ has a proper prime divisor $2p + 1$. For example, $(3^{83} - 1)/2$ has a divisor 167.

3. In case $a = 5$, if $p > 2$ is Sophie Germain prime and $p \equiv -1 \bmod 5$, then $\Phi_p(5) = (5^p - 1)/4$ has a proper prime divisor $2p + 1$. For example, $(5^{179} - 1)/4$ has a divisor 359.

4. In case $a = 10$, if $p > 2$ is Sophie Germain prime and $p \equiv \pm 1, -7 \bmod 20$, then $\Phi_p(10) = (10^p - 1)/9$ has a proper prime divisor $2p+1$. For example, repunits $(10^{41} - 1)/9$, $(10^{359} - 1)/9$ and $(10^{53} - 1)/9$ have divisors 83, 719, and 107, respectively.

5. Pocklington's theorem. The next is the Pocklington's theorem. This is useful for the factorization of the number N such that $N - 1$ has the known factorization. In this section, we shall give a proof using the cyclotomic numbers.

Theorem 5.1. *If N divides $\Phi_d(a)$ for an integer $a > 1$ and a divisor d of $N - 1$, then d is a divisor of $p - 1$ for each prime p of N.*

Proof. It follows from the condition that $d = |a|_p$ is a divisor of $p - 1$.

Corollary 5.2. *Assume that $N - 1 = FR$, where $(F, R) = 1$, B is a number such that $FB \geq \sqrt{N}$, and R has no prime factors less than B. Assume that there exists integers $a = a(q) > 1$ for every prime divisor q of F and $b > 1$ such that*

$$\begin{aligned} \textit{for} \quad a^{\frac{N-1}{q}} &\equiv s(q) = s \neq 1 \quad \textit{and} \quad b^F \equiv t \neq 1 \bmod N, \\ s^q &\equiv 1 \bmod (s-1)N \quad \textit{and} \quad t^R \equiv 1 \bmod (t-1)N. \end{aligned}$$

Then N is prime.

Proof. Let p be a prime divisor of N. By the assumptions, we have $0 \equiv \Phi_q(s) \equiv \Phi_q(u^{q^{e-1}}) = \Phi_{q^e}(u) \bmod N$ where q^e is the q-part of F and

$$u \equiv a^{\frac{N-1}{q^e}} \bmod N.$$

Thus $q^e = |u|_p$ is a divisor of $p-1$ and hence F is a divisor of $p-1$. On the other hand, p is a divisor of $(t^R-1)/(t-1) = \prod_{d|R, d>1} \Phi_d(t)$ and so $d = |t|_p$ is a divisor of $p-1$ for a divisor $d > 1$ of R. Hence dF is a divisor of $p-1$. Thus $p > dF \geq BF \geq \sqrt{N}$.

6. a-pseudoprime. The next shows that divisors of $\Phi_n(a)$ are almost a-pseudoprimes.

Theorem 6.1. *If D is a divisor of $\Phi_n(a)$ and D is not divided by the maximal prime divisor of n, then $a^{D-1} \equiv 1 \bmod D$.*

Proof. Let p be a prime divisor of D and so of $\Phi_n(a)$. Then $n = |a|_p$ is a divisor of $p-1$, equivalently, $p \equiv 1 \bmod n$. Hence $D \equiv 1 \bmod n$. Since $a^n \equiv 1 \bmod D$, we have our result.

Example 6.1. Theorem together with Example 1.1 shows that 1093^2 and 3511^2 are square (2-)pseudoprimes.

The next contains the result of M. Cipolla (see [2]) for a prime n.

Corollary 6.1. *If $a \geq 2$, $n \geq 2$ is odd and $(n, \Phi_n(a^2)) = 1$, then $\Phi_n(a^2)$ is a-pseudoprime.*

Proof. It follows from Corollary 3.2.1 to see $\Phi_n(a^2)$ is composite. We have that $\Phi_n(a^2)$ is odd and $\Phi_n(a^2) \equiv 1 \bmod n$ as in the proof of theorem. Thus we have $\Phi_n(a^2) \equiv 1 \bmod 2n$ which implies our assertion.

The next contains the result of M. Cipolla (see [2]) for Fermat numbers.

Proposition 6.2. *Let $a > 1$, let M be the finite set of distinct natural numbers $d > 1$ with $(d, \Phi_d(a)) = 1$, let ℓ be the least common multiple of the numbers in M and let $N = \prod_{d \in M} N_d$ where $N_d > 1$ is a divisor of $\Phi_d(a)$. Then $a^{N-1} \equiv 1 \bmod N$ if and only if ℓ divides $N-1$.*

Proof. We can easily see d is the order of $a \bmod N_d$. It follows from $(d, \Phi_d(a)) = 1$ that $\Phi_d(a)$ and $\Phi_{d'}(a)$ are relatively prime for distinct numbers d, $d' \in M$. Thus $\ell = |a|_N$ and so we have the assertion.

The next contains the result of E. Malo [2] for $a = 2$.

Proposition 6.3. *$(a^n - 1)/(a-1)$ is a-pseudoprime whenever $n > 1$ is a-pseudoprime with $(n, a-1) = 1$.*

Proof. Let M be the set of divisors of n different from 1. Then the assumption $(n, a-1) = 1$ is equivalent to $(n, a^n - 1) = 1$ since n is a-pseudoprime. This implies that $(d, \Phi_d(a)) = 1$ for $d|n$. Theorem together with the equation $N = (a^n - 1)/(a-1) = \prod_{d \in M} \Phi_d(a)$ shows our assertion since $N \equiv 1 \bmod n$.

7. Lucas Test. The purpose of this section is to show that Pepin's test is the same as the Lucas test and a new proof for these tests.

Let P, Q be nonzero integers, let α, β be distinct roots of the quadratic equation $X^2 - PX + Q = 0$ and $D = P^2 - 4Q$. Then $P = \alpha + \beta$, $Q = \alpha\beta$, and $D = (\alpha - \beta)^2$. We set

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n.$$

The next is a preparation for the proof of Pepin's test and Lucas' test.

Proposition 7.1. *Assume n is an odd prime and $(QD, n) = 1$. Then we have the following*

(1) $2V_{n+1} = PV_n + DU_n$ *and* $2QV_{n-1} = PV_n - DU_n$.

(2) $V_n \equiv P \bmod n$ *and* $U_n \equiv \left(\frac{D}{n}\right) \bmod n$.

(3) $V_{n-(\frac{D}{n})} \equiv 2Q^{(1-(\frac{D}{n}))/2} \bmod n$.

(4) $V_{(n-(\frac{D}{n}))/2} \equiv 0 \bmod n$ *if and only if* $\left(\frac{Q}{n}\right) = -1$.

Proof. (1) is clear. The first of (2) follows from $V_n \equiv (\alpha + \beta)^n \equiv P^n \equiv P \bmod n$. It is easy to see from $(D, n) = 1$ that $(\alpha - \beta) \bmod n$ has the inverse in O/nO, where O is the ring of algebraic integers in $\mathbf{Q}(\alpha)$, and so the second of (2) follows from

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \equiv \frac{(\alpha - \beta)^n}{\alpha - \beta} = D^{\frac{n-1}{2}} \equiv \left(\frac{D}{n}\right) \bmod n.$$

(3) follows from (1) and (2). (4) follows from

$$V^2_{\frac{n-(\frac{D}{n})}{2}} = V_{n-(\frac{D}{n})} + 2Q^{\frac{n-(\frac{D}{n})}{2}} \equiv 2Q^{\frac{1-(\frac{D}{n})}{2}}\left(1 + \left(\frac{Q}{n}\right)\right) \bmod n.$$

The proof of the next Theorems 7.2 and 7.3 is different from the usual one.

Theorem 7.2. *$M_q = 2^q - 1$ is prime and $\left(\frac{D}{M_q}\right) = \left(\frac{Q}{M_q}\right) = -1$ if and only if $(QD, M_q) = 1$ and $V_{(M_q+1)/2} \equiv 0 \bmod M_q$.*

Proof. It is enough from the above to prove the necessity. Let O be the ring of algebraic integers in $\mathbf{Q}(\alpha)$, and let $\mathcal{P}$ be a prime ideal of O containing M_q. Then $\mathcal{P} \cap \mathbf{Z} = p\mathbf{Z}$ and p is a prime divisor of M_q. It follows from $(Q, M_q) = 1$ that $\beta \bmod \mathcal{P}$ has an inverse element in the residue field $O/\mathcal{P}$. Thus there exists an element γ in O with $\gamma^{(M_q+1)/2} \equiv -1 \bmod \mathcal{P}$ and $M_q + 1$ is the order of $\gamma \bmod \mathcal{P}$. Since the order of the residue field $O/\mathcal{P}$ is p or p^2, we have $p^2 - 1 = k(M_q + 1) \geq k(p+1)$ for some k. Thus $k \equiv -1 \bmod p$ and $k \leq p - 1$ which implies $k = p - 1$ and $p = M_q$.

Pepin's test can be proved more easily but the proof of the next is the same as in the above theorem.

Theorem 7.3. *$F_m = 2^{2^m} + 1$ is prime, $\left(\frac{D}{F_m}\right) = 1$ and $\left(\frac{Q}{F_m}\right) = -1$ if and only if $(DQ, F_m) = 1$ and $V_{(F_m-1)/2} \equiv 0 \bmod F_m$.*

If we set $P = 2$, $Q = -2$ and $S_k = (V_{2^{k+1}})/2^{2^k}$ $(k = 0, 1, \ldots)$, then we have $S_0 = 4$ and $S_{k+1} = S_k^2 - 2$. Thus it follows form the above that $M_q = 2^q - 1$ is prime if and only if M_q divides S_{q-2}.

On the other hand if we set $P = 4$, $Q = 3$, then $3^{(F_m-1)/2} + 1 = V_{(F_m-1)/2} \equiv 0 \bmod F_m$ if and only if F_m is prime.

REFERENCES

[1] K. MOTOSE: On values of cyclotomic polynomials, Math. J. Okayama Univ. **35** (1993), 35–40.

[2] P. RIBENBOIM: The little book of big primes, Springer, 1991.

[3] M. MORIMOTO and Y. KIDA: Factorization of cyclotomic numbers, Sophia Kokyuroku in Mathematics **26** (1987), (in Japanese).

[4] M. MORIMOTO, Y. KIDA and M. SAITO: Factorization of cyclotomic numbers II, Sophia Kokyuroku in Mathematics **29** (1989), (in Japanese).

[5] M. MORIMOTO, Y. KIDA and M. KOBAYASHI: Factorization of cyclotomic numbers III, Sophia Kokyuroku in Mathematics **35** (1992), (in Japanese).

Department of Mathematics
Faculty of Science
Hirosaki University
Hirosaki 036, Japan

(*Received January 23, 1996*)