JOURNAL OF NUMBER THEORY 17, 165–175 (1983)

On the Cyclotomic Polynomial

R. A. MOLLIN*,†

Mathematics Department, Queen's University, Kingston, Ontario K7L 3N6, Canada

Communicated by A. E. Ross

Received October 10, 1981

For a given positive integer m and an algebraic number field K necessary and sufficient conditions for the mth cyclotomic polynomial to have K-integral solutions modulo a given integer of K are given. Among applications thereof are: that the solvability of the cyclotomic polynomial mod an integer yields information about the class number of related number fields; and about representation of integers by binary quadratic forms. The latter extends previous work of the author. Moreover some information is obtained pertaining to when an integer of K is the norm of an integer in a given quadratic extension of K. Finally an explicit determination of the pqth cyclotomic polynomial for distinct primes p and q is provided, and known results in the literature as well as generalizations thereof are obtained.

1. NOTATION AND PRELIMINARIES

The symbol $\mathbb{Q}$ will denote the rational number field, and $\mathbb{Z}$ will denote the rational integers. For a given algebraic number field K, O_K will denote the ring of integers of K, and $h(K)$ will denote its class number. For a given positive integer m we let ε_m denote a primitive mth root of unity. The symbol $\prod$ is used to denote a product and when confusion cannot arise we will eliminate the indexing variable for convenience sake. Finally $(*/*)$ denotes the Legendre symbol.

2. SOLVABILITY MODULO INTEGERS

The minimum polynomial of ε_m over $\mathbb{Q}$ is $\phi_m(x) = \prod_{(k,m)=1} (x - \varepsilon_m^k)$, which is the mth cyclotomic polynomial. Moreover $x^m - 1 = \prod_{d \mid m} \phi_d(m)$.

First we provide a result which is of independent interest in that for a given positive $m \in Z$ and a given number field K it provides necessary and sufficient conditions for $\phi_m(x)$ to have K-integral solutions modulo a given $\alpha \in O_K$.

* The author's research is supported by N.S.E.R.C. Canada.

† Current address: Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta T2N1N4, Canada.

0022-314X/83 $3.00

641/17/2-3

THEOREM 2.1. *Let K be an algebraic number field with $\alpha \in O_K$ such that $(\alpha) = \wp_1^{b_1}\wp_2^{b_2}\cdots\wp_s^{b_s}$ for distinct K-primes $\wp_i$, where $b_i > 0$. Suppose $m = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, where $p_1 < p_2 < \cdots < p_r$ are distinct rational primes; and if $m_0 = m/p_r^{a_r} > 1$, then ε_{m_0} is not in K. We assume that $a_r \geqslant f_i$ for all $i = 1, 2, \ldots, s$, where f_i is the inertial degree of $\wp_i$ in $K/\mathbb{Q}$. Furthermore if $p_r = 2$, then we assume that 2 is unramified in K. Then the following are equivalent*:

(1) $\phi_m(\beta) \equiv 0 \pmod{(\alpha)}$ *for some* $\beta \in O_K$.

(2) *Each $\wp_i$ for $i = 1, 2, \ldots, s$, is either completely split or ramified in $K(\varepsilon_m)$. In the latter case $\wp_i \mid p_r$, $\wp_i$ is completely split in $K(\varepsilon_{m_0})$, and $b_i = 1$ for $p_r > 2$ (respectively, $a_r = 1$ or $b_i = 1$ for $p_r = 2$).*

Proof. Assume $\phi_m(\beta) \equiv 0 \pmod{(\alpha)}$ for some $\beta \in O_K$. Then $\phi_m(\beta) \equiv 0 \pmod{\wp_i^{b_i}}$ for each $i = 1, 2, \ldots, s$. Let $d = p_1^{c_1}p_2^{c_2}\cdots p_r^{c_r}$ be the order of β modulo $\wp_i^{b_i}$. By the generalized Euler criterion we have that d divides $q_i^{f_i(b_i-1)}(q_i^{f_i} - 1)$, where $\wp_i \cap \mathbb{Z} = q_i$. If $p_j \neq q_i$ for any $j = 1, 2, \ldots, r$, then we have $q_i^{f_i} \equiv 1 \pmod{d}$. If $c_j < a_j$ for any $j = 1, 2, \ldots, r$, then consider: $\phi_m(\beta)\prod \phi_k(\beta) = (\beta^m - 1)/(\beta^t - 1) = \beta^{t(m/t-1)} + \beta^{t(m/t-2)} + \cdots + \beta^t + 1$, where the product ranges over all $k \neq m$ such that $p_j^{c_j+1}$ divides k; and $t = m/p_j^{a_j-c_j}$. But $\beta^t \equiv 1 \pmod{\wp_i^{b_i}}$ so $(\beta^m - 1)/(\beta^t - 1) \equiv p_j^{a_j-c_j} \pmod{\wp_i^{b_i}}$. Thus $\wp_i \mid p_j$; which implies $p_j = q_i$, a contradiction. Hence $q_i^{f_i} \equiv 1 \pmod{m}$; that is, $\wp_i$ is completely split in $K(\varepsilon_m)$.

Now, if $q_i = p_j$ for some $j = 1, 2, \ldots, r$, then by the same argument as above we obtain that $c_k = a_k$ for all $k \neq j$. If $j < r$, then since $q_i^{f_i} = p_j^{f_i} \equiv 1 \pmod{\prod_{k\neq j} p_k^{a_k}}$ we have $p_r^{f_i} > p_j^{f_i} > p_r^{a_r}$, a contradiction since $a_r \geqslant f_i$ by hypothesis. Therefore $j = r$; that is, $\wp_i$ is completely split in $K(\varepsilon_{m/p_r^{a_r}})$.

Now, if $\wp_i \mid p_r = 2$, then we claim that either $b_i = 1$ or $a_r = 1$. If not, then $\phi_{2^{a_r}}(\beta) = \beta^{2^{a_r-1}} + 1 \equiv 0 \pmod{\wp_i^{b_i}}$. Therefore -1 is a square modulo $\wp_i^2$. This implies by [6, 6C, p. 278] and the fact that 2 is unramified in K, that $\wp_i$ is unramified in $K(\sqrt{-1})$. Therefore we have that $\hat{\wp}_i$ is unramified in $K(\sqrt{-1})$ over $\mathbb{Q}$, where $\hat{\wp}_i$ is a $K(\sqrt{-1})$-prime above $\wp_i$. But $\hat{\wp}_i \cap \mathbb{Q}(\sqrt{-1})$ is ramified over $\mathbb{Q}$, a contradiction. Therefore $b_i = 1$ or $a_r = 1$.

If $K(\varepsilon_m) = K$, then trivially $\wp_i$ is completely split in $K(\varepsilon_m)$ so we assume henceforth that $K(\varepsilon_m) \neq K$ and $\wp_i \mid p_r > 2$. If $\beta = \varepsilon_{m/p_r}^k$ for some $k \in \mathbb{Z}$, then as previously $p_r \equiv (\beta^m - 1)/(\beta^t - 1) \equiv 0 \pmod{\wp_i^{b_i}}$, where $t = m/p_r$. However, since $p_r \in \wp_i$, then $p_r^{b_i} \equiv 0 \pmod{\wp_i^{b_i}}$ so $b_i = 1$. We assume now that $\beta \neq \varepsilon_{m/p_r}^k$ for any $k \in \mathbb{Z}$. Now since $\phi_m(\beta) = \phi_{m_0}(\beta^{p_r^{a_r}})/\phi_{m_0}(\beta^{p_r^{a_r-1}})$, where $m_0 = m/p_r^{a_r}$, then it suffices to show that if $\phi_{m_0}(\beta^{p_r^{a_r-1}})$ is divisible by exactly $\wp_i^l$, say, then $\phi_{m_0}(\beta^{p_r^{a_r}})$ is exactly divisible by $\wp_i^{l+1}$. Since $\phi_{m_0}(\beta^{p_r^{a_r-1}})$ is divisible by the same power of $\wp_i$ as $\beta^{m/p_r} - 1 \neq 0$, then $(\beta^{m/p_r} - 1) \in \wp_i^l$. Thus

$$
\begin{aligned}
(\beta^{m/p_r}-1)^{p_r} &= \beta^m - \beta_{p_r}^{m/p_r(p_r-1)}\binom{p_r}{1} + \beta^{m/p_r(p_r-2)}\binom{p_r}{2} \\
&\quad - \cdots + \beta_{p_r}^{m/p_r}\binom{p_r}{p_r-1} - 1 \\
&= \beta^m + \alpha\beta^{m/p_r}p_r - 1,
\end{aligned}
$$

where ( ) denotes the binomial coefficient, where α is relatively prime to $\wp_i$ since $p_r > 2$. Thus $\beta^m - 1$ is exactly divisible by $\wp_i^{l+1}$. Since $\phi_{m_0}(\beta^{p_r^{a_r}})$ is divisible by exactly the same power of $\wp_i$ as $\beta^m - 1$ we have accomplished that $b_i = 1$. Thus we have shown that (1) implies (2).

Conversely assume (2). By the Chinese remainder theorem it suffices to show that $\phi_m(\beta_i) \equiv 0 \pmod{\wp_i^{b_i}}$ for $i = 1, 2,..., s$, where $\beta_i \in O_K$. If $\wp_i$ is completely split in $K(\varepsilon_m)$, then we may choose an element of order m modulo $\wp_i^{b_i}$. By the choice of β_i we have $\phi_k(\beta_i) \not\equiv 0 \pmod{\wp_i}$ for any proper divisor k of m. Therefore $\phi_m(\beta_i) \equiv 0 \pmod{\wp_i^{b_i}}$. If $\wp_i \mid p_r = 2$, then $a_r = 1$ or $b_i = 1$. If $a_r = 1$, then $\phi_m(-1) \equiv 0 \pmod{\wp_i^{b_i}}$. If $b_i = 1$, then $\phi_m(1) \equiv 0 \pmod{\wp_i}$. Now assume $\wp_i \mid p_r > 2$. Choose $\beta_i \in O_K$ of order $m_0 = m/p_r^{a_r}$ modulo $\wp_i$. We have $\phi_m(\beta_i) = \phi_{m_0}(\beta_i^{p_r^{a_r}})/\phi_{m_0}(\beta_i^{p_r^{a_r-1}})$. If $\phi_{m_0}(\beta_i^{p_r^{a_r-1}}) = 0$, then $\beta_i^{p_r^{a_r-1}} = \varepsilon_{m_0}$ which implies ε_{m_0} is in K. Therefore by hypothesis $m_0 = 1$. In this case $\phi_m(\beta_i) = p_r \equiv 0 \pmod{\wp_i}$, and since $b_i = 1$ we have the result. If $\phi_{m_0}(\beta_i^{p_r^{a_r-1}}) \neq 0$, then $\phi_m(\beta_i) \equiv 0 \pmod{\wp_i}$ since $b_i = 1$ and $\phi_{m_0}(\beta_i^{p_r^{a_r-1}})$ is divisible by exactly one lower power of $\wp_i$ than $\phi_{m_0}(\beta_i^{p_r^{a_r}})$. Q.E.D.

The following result which is immediate from Theorem 2.1 yields [5, Theorem 2.4] as a special case.

COROLLARY 2.2. *Let* $n = q_1^{b_1}q_2^{b_2}\cdots q_s^{b_s}$ *for distinct rational primes* q_i. *Then the following are equivalent*:

(1) $\phi_m(x) \equiv 0 \pmod{n}$ *for some* $x \in \mathbb{Z}$.

(2) *All* q_i *are such that* $q_i = p_r \equiv 1 \pmod{m_0}$ *and* $b_i = 1$ *for* $p_r > 2$ (*respectively*, $a_r = 1$ *or* $b_i = 1$ *for* $p_r = 2$); *or* $q_i \equiv 1 \pmod{m}$.

Continuing to maintain the above notation we obtain information in the following result, pertaining to the class number of $\mathbb{Q}(\varepsilon_{mq})$ for each $q \mid n$ with $q \nmid m$. This generalizes [5, Corollary 2.5].

COROLLARY 2.3. *If* $\phi_m(r) \equiv 0 \pmod{n}$ *for some* $r \in \mathbb{Z}$, $m > 2$, *and if* $q_i > 2$ *does not divide* m, *then for each* $j = 1, 2,..., r$, *we have that* $p_j^{(\phi(m)/2)-1}$ *divides* $h(\mathbb{Q}(\varepsilon_{mq_i}))$ *and if* $p_j = 2$, *then* $2^{(\phi(m)/2)-1}$ *divides* $h(\mathbb{Q}(\varepsilon_m, \sqrt{q_i^*}))$, *where* $q_i^* = (-1)^{(q_i-1)/2}\, q_i$.

Proof. By Theorem 2.1 we have that the hypothesis of [5, Theorem 1.1] is satisfied. The result follows. Q.E.D.

We note that if 2 ramifies in K, then the theorem fails. For example, if

$K = \mathbb{Q}(\sqrt{7})$, then $\phi_4(\sqrt{7}) \equiv 0 \pmod{\wp^2}$, where $(2) = \wp^2$ in K. However, $a_r > 1$ and $b_i > 1$ contradicting Theorem 2.1.

Also if $a_r < f_i$ for some $i = 1, 2, \ldots, s$, then the theorem fails. For example, if $K = \mathbb{Q}(\varepsilon_5)$, then $\phi_{15}(\varepsilon_5) \equiv 0 \pmod{\wp}$, where $(3) = \wp$ in K. If $m = 15$, then $a_r = 1 < f = 4$, where f is the inertial degree of 3 in K. However, $\wp \nmid 5 = p_r$ contradicting Theorem 2.1.

The stage is now set to provide a generalization of [5, Theorem 2.6]. In what follows $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} > 2$ for distinct primes p_i with $p_1 < p_2 < \cdots < p_r$ and

$$
\begin{aligned}
m^* &= \pm \prod_{i=1}^{r} p_i, && \text{if } p_1 > 2, \\
&= \pm \prod_{i=2}^{r} p_i, && \text{if } p_1 = 2 \text{ and } r > 1, \\
&= -1, && \text{if } p_1 = 2, r = 1 \text{ and } a_1 = 2, \\
&= -2, && \text{if } p_1 = 2, r = 1 \text{ and } a_1 > 2.
\end{aligned}
$$

The "$\pm$" signs for the first two values of m^* indicate that either sign is admissible in the theorem.

THEOREM 2.3. *Let $n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s} > 1$, where the q_i's are distinct primes such that $b_i \equiv 0 \pmod 2$ whenever $q_i \equiv 3 \pmod 4$. If $h(\mathbb{Q}(\sqrt{m^*})) = 1$, then whenever $\phi_m(x) \equiv 0 \pmod n$ for some $x \in \mathbb{Z}$, then $n = a^2 - m^* b^2$ for some $a, b \in \mathbb{Z}$.*

Proof. It suffices to show that $q_i = a^2 - m^* b^2$ for $i = 1, 2, \ldots, s$ since we have that $(c^2 - m^* d^2)(e^2 - m^* f^2) = (ce - m^* df)^2 - m^*(de - cf)^2$. For $q_i \equiv 3 \pmod 4$ we have $q_i = (q_i^{a_i/2})^2 - m^* \cdot 0^2$ so we assume $q_i \equiv 1 \pmod 4$ or $q_i = 2$. Since $\phi_m(x) \equiv 0 \pmod n$ has an integer solution then by Theorem 2.1 we have $q_i \equiv 1 \pmod m$ or $q_i \mid m$. If $q_i \equiv 1 \pmod m$, then for $p_1 > 2$ or $r > 1$ we have that $(m^*/q_i) = \prod_j (p_j/q_i) = \prod_j (q_i/p_j) = 1$. If $p_1 = 2$ and $r = 1$, then $(m^*/q_i) = (-1/q_i) = 1$, whenever $a_1 = 2$; and if $a_1 > 2$, then $(m^*/q_i) = (-2/q_i) = 1$. Thus q_i is completely split in $\mathbb{Q}(\sqrt{m^*})$ or q_i ramifies in $\mathbb{Q}(\sqrt{m^*})$. In either case $q_i = N(\wp_i)$, where $\wp_i$ is a $\mathbb{Q}(\sqrt{m^*})$ – prime above q_i. Moreover since $h(\mathbb{Q}(\sqrt{m^*})) = 1$, then $q_i = N(\wp_i) = N(a + \sqrt{m^*}\, b)$, where $a + \sqrt{m^*}\, b$ is an element of $O_{\mathbb{Q}(\sqrt{m^*})}$. Hence $q_i = a^2 - m^* b^2$. Now if $m^* \equiv 2, 3 \pmod 4$, then a and b are integers. If $m^* \equiv 1 \pmod 4$, then $2a$ and $2b$ are integers. In this case let $a = c/2$ and $b = d/2$, where c and d are integers. Therefore if $q_i \equiv 1 \pmod m$, then we have $4 \equiv 4q_i \equiv c^2 \pmod{4m^*}$ which implies that c is even and so d is even. In any case we have the result for any $q_i \equiv 1 \pmod m$. If $q_i \mid m$, then $q_i = p_r$, where $p_r > p_i$ for all $i < r$, by

Theorem 2.1 and $q_i \equiv 1 \pmod{\prod_{i=1}^{r-1} p_i}$. Therefore if $r > 1$, then as in the above argument we have the result. The only remaining case is $r = 1$ and $p_r = q_i$. We are assuming that either $q_i = 2$ or $q_i \equiv 1 \pmod 4$. If $q_i \equiv 1 \pmod 4$, then there are integers a and b such that $b^2 - q_i a^2 = -1$. Therefore $q_i = (q_i a)^2 - q_i b^2$. If $q_i = 2$ and $a_1 = 2$, then $2 = 1^2 + 1^2$. If $q_i = 2$ and $a_1 > 2$, then $2 = 0^2 + 2 \cdot 1^2$. Q.E.D.

We note that if we remove the restriction $h(\mathbb{Q}(\sqrt{m^*})) = 1$ in Theorem 2.3, then the theorem fails to hold. For example, if $m = 79 = m^*$ and $n = 317$, then $h(\mathbb{Q}(\sqrt{79})) = 3$. Since $317 \equiv 1 \pmod{79}$, then by Theorem 2.1 we have $\phi_{79}(x) \equiv 0 \pmod{317}$ has an integer solution. Moreover $317 \equiv 1 \pmod 4$. However, it can be shown that $317 \neq a^2 - 79b^2$ for any $a, b \in Z$.

Furthermore, if we remove the restriction on n that all q_i dividing n appear to an even power if $q_i \equiv 3 \pmod 4$, then the theorem fails to hold. For example, if $n = 23$ and $m = 11$, then $m^* = 11$ and $h(Q(\sqrt{11})) = 1$. Moreover since $23 \equiv 1 \pmod{11}$, then $\phi_{11}(x) \equiv 0 \pmod{23}$ has a solution $x \in Z$. However, since 23 is inert in $Q(\sqrt{11})$, then $23 \neq a^2 - 11b^2$ for any $a, b \in Z$.

However, what is of interest here is that if we relax our demands on the conclusion we can generalize the result. Suppose we only want that n is a norm of an integer from $\mathbb{Q}(\sqrt{m^*})$. Then as we shall see not only may we eliminate the restriction on n but we may also proceed from Q to any number field K. We do however have to restrict m^* somewhat. We define $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} > 2$, where $p_1 < p_2 < \cdots < p_r$ are distinct primes and we define

$$
\begin{aligned}
m^* &= \prod_1^r p_i, && \text{if } \prod_1^r p_i \equiv 1 \pmod 4 \text{ or } p_1 = 2 \text{ and } a_1 > 2,\\
&= -\prod_1^r p_i, && \text{if } \prod_1^r p_i \equiv 3 \pmod 4,\\
&= \prod_2^r p_i, && \text{if } p_1 = 2,\ a_1 \leqslant 2 \text{ and } \prod_2^r p_i \equiv 1 \pmod 4,\\
&= -\prod_2^r p_i, && \text{if } p_1 = 2,\ a_1 \leqslant 2 \text{ and } \prod_2^r p_i \equiv 3 \pmod 4.
\end{aligned}
$$

THEOREM 2.4. *Let K be an algebraic number field and let $\alpha \in O_K$ with $(\alpha) = \wp_1^{b_1} \wp_2^{b_2} \cdots \wp_s^{b_s}$, where $\wp_i \mid q_i$ in $K/\mathbb{Q}$. If $m_0 = m/p_r^{a_r} > 1$, then ε_{m_0} is not in K, and we assume that $a_r \geqslant f_i$ for all $i = 1, 2, \ldots, s$, where m, a_r, and f_i are as above. Furthermore if $p_r = 2$, then we assume that 2 is unramified in K. Now if $h(K(\sqrt{m^*})) = 1 = h(K)$, then whenever $\phi_m(\beta) \equiv 0 \pmod{(\alpha)}$ for some*

$\beta \in O_K$, then $\alpha = N(\gamma)$ for some $\gamma \in O_{K(\sqrt{m^*})}$, where N is the norm map in $K(\sqrt{m^*})/K$.

Proof. By the fact that $h(K) = 1$, then $\mathscr{q}_i = (\alpha_i)$ for some $\alpha_i \in O_K$ for $i = 1, 2, \ldots, s$. By the multiplicativity of the norm map it suffices to show that $\alpha_i = N(\gamma_i)$ for some $\gamma_i \in O_{K(\sqrt{m^*})}$. Since $h(K(\sqrt{m^*})) = 1$, then if we can show that each $\mathscr{q}_i$ is completely split or ramified in $K(\sqrt{m^*})$, then we have that $N((\gamma_i)) = N(\hat{\mathscr{q}}_i) = \mathscr{q}_i = (\alpha_i)$, where $\hat{\mathscr{q}}_i \mid q_i$ in $K(\sqrt{m^*})/K$. But by hypothesis we may invoke Theorem 2.1 to get that each $\mathscr{q}_i$ is completely split or ramified in $K(\varepsilon_m)$. Moreover by the choice of m^* we have $K(\sqrt{m^*}) \subseteq K(\varepsilon_m)$. This secures the theorem. Q.E.D.

We note that it is important to have conditions, even under as restrictive a hypothesis as Theorem 2.4, to determine when an algebraic integer is the norm of an algebraic integer from a given quadratic extension. It is possible, even in the simplest cases, to have an algebraic integer which is a norm from a quadratic extension but *not* the norm of an algebraic integer. One may for example use the product formula for the local norm residue symbol to determine whether or not an integer is a norm, but we cannot determine by those methods whether or not it is the norm of an integer.

For example, if $F = \mathbb{Q}(\sqrt{79})$, then $N((19 + 2\sqrt{79})/3) = 5$. However, using the norm residue symbol we get $N(\alpha) \neq 5$ for any $\alpha \in O_F$. One reason for this is that the F-ideals above 5 are not principal.

We now return to a discussion of Theorem 2.3 which has implications for the theory of representations of numbers by binary quadratic forms, as the following applications indicate.

Applications of Theorem 2.3

(1) By taking $m = 8$ we get that all primes of the form $8k + 1$ are representable in the form $x^2 + 2y^2$ for $x, y \in Z$. Fermat proved this result in 1654.

More generally we have that all integers of the form $n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$, where all $q_i \equiv 1 \pmod 8$, or $n = 2$, are representable in the form $x^2 + 2y^2$.

(2) We have Fermat's two-square theorem; viz. if $\phi_4(x) \equiv 0 \pmod n$ is solvable for $x \in \mathbb{Z}$, then $n = a^2 + b^2$. In other words if $n = q_1^{b_1} \cdots q^{b_s}$, where $b_i \equiv 0 \pmod 2$ if $q_i \equiv 3 \pmod 4$, and $q_i \leqslant 1$ if $q_i = 2$, then $n = a^2 + b^2$.

(3) If p is an odd prime, then $x^2 - py^2$ represents all primes of the form $1 + 4pt$ (e.g., $x^2 - 3y^2$ represents all $q \equiv 1 \pmod{12}$).

The converse of Theorem 2.3 fails, as the following examples indicates. If $m^* = m = 7$ and $n = 53$, then $53 = 9^2 - 7.2^2$. Moreover $h(\mathbb{Q}(\sqrt{7})) = 1$ and $53 \equiv 1 \pmod 4$. However, $53 \not\equiv 1 \pmod 7$ and so by Theorem 2.1

$\phi_7(x) \not\equiv 0 \pmod{53}$ for any $x \in \mathbb{Z}$. The converse even fails for $m = 2, 3$. For example, if $n = 2^2 + 2^2$, and $m = 4$, then by Theorem 2.1, $\phi_4(x) \not\equiv 0 \pmod 8$ for any $x \in \mathbb{Z}$. Also if $n = 4 = 4^2 - 3.2^2$ and $m = 3$, then $\phi_3(x) \not\equiv 0 \pmod 4$ since $2 \not\equiv 1 \pmod 3$. However, with minor restrictions on a given $n \in \mathbb{Z}$ we can get the converse of Theorem 2.3 to hold for $m = 2, 3$ as shown in [5, Lemma 2.7].

The latter result leads us into an interesting conjecture made by Chowla in [3]; viz. If $g(x, y)$, $h(x, y) \in Z[x, y]$ are primitive irreducible polynomials which represent the same numbers, then g and h are equivalent by a unimodular transformation. However, Schinzel in [7] gave the following counterexample: $f(x, y) = x^2 + 3y^2$ and $g(t_1, t_2) = t_1^2 + t_1 t_2 + t_2^2$ have the same set of values but they are not equivalent by a unimodular transformation. Now in [5] we showed that given $n = a^2 + 3b^2$ with $(a, b) = 1$ and $2 \mid a$, then $\phi_3(x) \equiv 0 \pmod n$ is solvable for $x \in \mathbb{Z}$. Moreover we have an explicit determination of those integer solutions.[1] We now give a more palatable analog of this method using the form of $g(t_1, t_2)$. Let $e = a - b$ and $f = 2b$, then $n = a^2 + 3b^2 = e^2 + ef + f^2$ with $(e, f) = 1$. Thus there exist $c, d \in \mathbb{Z}$ such that $fd - ce = 1$. Now consider the following matrix $A = \begin{pmatrix} f & -e \\ -c & d \end{pmatrix}$ and the following matrix product:

$$A \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} A^{-1} = \begin{pmatrix} -df - ed - fc & -ef - e^2 - f^2 \\ cd + d^2 + c^2 & ce + ed + fc \end{pmatrix}$$

$$= \begin{pmatrix} -df - ed - fc & -ef - e^2 - f^2 \\ cd + d^2 + c^2 & -1 + df + ed + fc \end{pmatrix}$$

$$= \begin{pmatrix} k & -n \\ h & -1 - k \end{pmatrix}.$$

However, the determinant of the latter matrix must clearly be 1. Therefore $-k(1 + k) + nh = 1$; that is, $k^2 + k + 1 \equiv 0 \pmod n$. Thus $k = -df - ed - fc$ is a solution of $\phi_3(x) \equiv 0 \pmod n$.

Example. Let $n = 4339$, a prime. Then $n = 64^2 + 3.9^2 = 55^2 + 18.55 + 18^2$. Thus $a = 64$, $b = 9$, $e = 55$, $f = 18$, and $c = -1$ while $d = -3$. Therefore $k = 237$; that is, $\phi_3(237) \equiv 0 \pmod{4339}$.

3. The pq-th Cyclotomic Polynomial

$\phi_{pq}(x)$ has been studied by Ivanov [4], Carlitz [2], Beiter [1], and Zeitlin [8] among others. We provide herein an explicit determination of $\phi_{pq}(x)$ from which we obtain much of the above as well as some generalizations thereof.

[1] Note that in [5, Theorem 2.8] m should be $(-1 + 3bc + ad)/2$. Also, in the subsequent example, m should be $-((p^2 - p + 14)/4)$.

THEOREM 3.1. *Let $q < p$ be primes, and let l_i be the quadratic residue of $-pi$ modulo q, where $0 \leqslant l_i < q$ for $i = 1, 2, \ldots, q-1$. Then* $\phi_{pq}(x) = 1 + \sum_{j=1}^{q-1} \sum_{i=1}^{k_j} (x^{(q-j)p-qi+1} - x^{(q-j)p-qi})$, *where* $k_j = ((q-j)p - l_j)/q$.

Proof. Let $f(x)$ denote the above polynomial for the moment so as not to prejudice the situation. We now verify that $\phi_1(x)\,\phi_p(x)\,\phi_q(x) f(x) = x^{pq} - 1$. We have $\phi_1(x)\,\phi_p(x)\,\phi_q(x) = x^{p+q-1} + x^{p+q-2} + \cdots + x^p - x^{q-1} - x^{q-2} \cdots 1$. Now $x^{p+q-i}f(x)$ has all of its positive terms, except x^{p+q-i}, cancel with all of the negative terms of $x^{p+q-i+1}f(x)$ for $i = 2, 3, \ldots, q$. Moreover all of the positive terms of $x^{p+q-1}f(x)$, except $x^{pq} + x^{pq-p} + \cdots + x^{2p} + x^{p+q-1}$, cancel with all of the negative terms of $x^p f(x)$, except $-x^{p+l_1} - x^{p+l_2} - \cdots - x^{p+l_{q-1}}$. Thus $(x^{p+q-1} + x^{p+q-2} + \cdots + x^p) f(x) = x^{p+q-2} + x^{p+q-3} + \cdots + x^p + x^{pq} + x^{pq-p} + \cdots + x^{2p} + x^{p+q-1} - x^{p+l_1} - x^{p+l_2} - \cdots - x^{p+l_{q-1}}$. Furthermore $-x^{q-i}f(x)$ has all of its negative terms except $-x^{q-i}$ cancel with all of the positive terms of $-x^{q-i+1}f(x)$ for $i = 2, 3, \ldots, q$. Moreover $-x^{q-1}f(x)$ has all of its negative terms, except $-x^{pq-p} - x^{pq-2p} - \cdots - x^p - x^{q-1}$, cancel with all of the positive terms of $-f(x)$, except $x^{l_1} + \cdots + x^{l_{q-1}}$. Thus $-(x^{q-1} + x^{q-2} + \cdots + 1) f(x) = -x^{q-2} - x^{q-3} - \cdots - 1 - x^{pq-p} - x^{pq-2p} - \cdots - x^p - x^{q-1} + x^{l_1} + x^{l_2} + \cdots + x^{l_{q-1}}$. Hence we have in total that

$$\begin{aligned}
&\phi_1(x)\,\phi_p(x)\,\phi_q(x) f(x)\\
&\quad = x^{p+q-2} + x^{p+q-3} + \cdots + x^{p+1} + x^p\\
&\qquad + x^{pq} + x^{pq-p} + \cdots + x^{2p} + x^{p+q-1} - x^{p+l_1} - x^{p+l_2}\\
&\qquad - \cdots - x^{p+l_{q-1}} - x^{q-2} - x^{q-3} - \cdots - 1 - x^{pq-p} - x^{pq-2p}\\
&\qquad - \cdots - x^p - x^{q-1} + x^{l_1} + x^{l_2} + \cdots + x^{l_{q-1}},\\
&\quad = x^{p+q-1} + x^{p+q-2} + \cdots + x^{p+1} + x^{pq} - x^{q-1} - x^{q-2}\\
&\qquad - \cdots - x - 1 + x^{l_1} + x^{l_2} + \cdots + x^{l_{q-1}} - x^{p+l_1} - x^{p+l_2}\\
&\qquad - \cdots - x^{p+l_{q-1}},\\
&\quad = (x^{pq} - 1) + (x^p - 1)(x^{q-1} + x^{q-2} + \cdots + x)\\
&\qquad - (x^p - 1)(x^{l_1} + x^{l_2} + \cdots + x^{l_{q-1}}),\\
&\quad = x^{pq} - 1 \qquad \text{since } \phi_q(x) = x^{l_1} + x^{l_2} + \cdots + x^{l_{q-1}}.
\end{aligned}$$

Q.E.D.

APPLICATIONS OF THEOREM 3.1

(i) For arbitrary $p > 2 = q$ we have that $\phi_{2p}(x) = x^{p-1} - x^{p-2} + \cdots - x + 1$. Also we have as examples

$$\phi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 + x^3 - x^4 - x + 1,$$

and

$$\phi_{35}(x) = x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1.$$

(ii) For $0 < j,\ h < q$ and $0 < i \leqslant k_j;\ 0 < m \leqslant k_h$ we have $(q-j)p - qi = (q-h)p - qm$ if and only if $h = j$ and $i = m$. Thus the only coefficients of $\phi_{pq}(x)$ are $0, \pm 1$. This was first obtained by V. Ivanov [4].

(iii) The following result was first obtained by Carlitz in [2, Theorem, p. 980]. We now show how the result may be obtained from Theorem 3.1.

THEOREM 3.2. *Let p and q be arbitrary primes with $q < p$, and let u be defined by $pu = -1 + qt$ with $0 < u < q$. If $\theta_0(pq)$ denotes the number of terms with positive coefficient in $\phi_{pq}(x)$, then $\theta_0(pq) = (q-u)(pu+1)/q$.*

Proof. For $i = 1, 2, ..., q-1$ define j_i by $(q-i)p = l_i + qj_i$, where l_i is as in Theorem 3.1. If we have cancellation of terms in the form of $\phi_{pq}(x)$ as given in Theorem 3.1, then for some set of integers i, k, l, m with $0 < i, k < q$ and $1 \leqslant l \leqslant j_k;\ 1 \leqslant m \leqslant j_i$ we have $(q-i)p - qm = (q-k)p - ql + 1$; that is, $q(l-m) - p(i-k) = 1$. There are only two possible sets of solutions for this equation.

Case 1. $m = l - t$ and $k = i - u$ in which case $i = u+1, ..., q-1$ which implies $k = 1, 2, ..., q-u-1$ and $l = t+1, ..., t+j_i$ which implies $m = 1, ..., j_i$. Thus for Case 1 there are $\sum_{i=u+1}^{q-1} j_i$ cancellations.

Case 2. For $u \geqslant 2$ set $k = i - (u-q)$ and $j = l - (t-p) = l + j_u$ in which case $i = 1, ..., u-1$ which implies $k = q-u+1, ..., q-1$ and $l = j_1 - j_u = j_{q-u+1}, ..., j_{q-u+i}$ which implies $m = j_1, ..., j_i$. Thus there are $\sum_{c=q-u+1}^{q-1} j_c$ cancellations in Case 2.

Hence the number of terms in $\phi_{pq}(x)$ with positive coefficient is

$$\theta_0(pq) = 1 + \sum_{b=1}^{q-1} j_b - \sum_{c=u+1}^{q-1} j_c - \sum_{d=q-u+1}^{q-1} j_d$$

$$= 1 + \sum_{b=1}^{u} j_b - \sum_{c=q-u+1}^{q-1} j_c.$$

We now show that this equals $(q-u)(pu+1)/q$.

$$\begin{aligned}1+\sum_{1}^{u} j_b-\sum_{q-u+1}^{q-u} j_b &= 1+pu-\frac{pu(u+1)}{2q}-\sum_{b=1}^{u}\frac{l_b}{q}-\sum_{b=1}^{u-1}\frac{(q-(q-u+b))p-l_b}{q}\\ &=\frac{(q-u)(pu+1)+u+(\sum_{b=1}^{u-1} l_{q-u+b}-\sum_{b=1}^{u} l_b)}{q}.\end{aligned}$$

It now suffices to show that $\sum_1^{u-1} l_{q-u+b}-\sum_1^u l_b=-u$. First we prove the following:

Claim. $l_{q-u+b}=l_b-1$ and $j_{q-u+b}=j_b-j_u$. We have $(l_b-l_u)+q(j_b-j_u)=(q-b)p-(q-u)p=(q-(q-u+b))=l_{q-u+b}+qj_{q-u+b}$. But since $l_u+j_uq=(q-u)p=qp-pu=qp+1-qt=1+q(p-t)$, then $l_u=1$ and so $l_b-1=l_{q-u+b}$ and $j_{q-u+b}=j_b-j_u$. This completes the proof of the claim.

Therefore $\sum_1^{u-1} l_{q-u+b}-\sum_1^u l_b=\sum_1^u (l_b-1)-\sum_1^u l_b=\sum_1^{u-1} l_b-(u-1)-\sum_1^u l_b=-(u-1)-l_u=-(u-1)-1=-u$. Q.E.D.

It is interesting to note that Carlitz [2, p. 981] mentions that the value of $\theta_0(pq)$ depends strongly on the residue of p modulo q. We can see from the above why this is the case.

Now let $d=\phi(pq)=(p-1)(q-1)$. As the above proof indicates, cancellations occur in a symmetric fashion about $x^{d/2}$. Thus we have the following which is [8, Lemma 4, p. 978]:

COROLLARY 3.3. *If $\theta_0(pq)$ is odd, then the coefficient of $x^{d/2}$ in $\phi_{pq}(x)$ is* 1 *and it is* -1 *otherwise.*

Furthermore we have the following result which generalizes [8, Lemma 5, p. 978]:

COROLLARY 3.4. *Let $p=a+q^k$ for primes p and q, and let $q\equiv b \pmod a$ for $0<b<a$, with $r=$ the order of b modulo a. Then if $b^{r-1}q\equiv 1 \pmod{2a}$, then the coefficient of $x^{d/2}$ in $\phi_{pq}(x)$ is* 1. *Otherwise the coefficient is* -1.

ACKNOWLEDGMENTS

The author welcomes the opportunity to thank the University of Victoria Mathematics Department for their hospitality during May 1981 when this research was begun. Moreover thanks must go to colleagues at Queen's University for providing an excellent working environment for the completion of this research.

REFERENCES

1. M. BEITER, The midterm coefficient of the cyclotomic polynomial, *Amer. Math. Monthly* **71** (1964), 769–770.
2. L. CARLITZ, The number of terms in the cyclotomic polynomial $F_{pq}(x)$, *Amer. Math. Monthly* **73** (1966), 979–981.
3. S. CHOWLA, Some problems of elementary number theory, *J. Reine Angew. Math.* **222** (1966), 71–74.
4. V. IVANOV, On properties of the coefficients of the irreducible equation for the partition of the circle, *Uspekhi Mat. Nauk* **9** (1941), 313–317. [Russian]
5. R. MOLLIN, Class numbers and a generalized Fermat theorem, *J. Number Theory*, in press.
6. P. RIBENBOIM, "Algebraic Numbers," Wiley–Interscience, New York, 1972.
7. A. SCHINZEL, On the relation between two conjectures on polynomials, *Acta Arith.* **38** (1980), 285–322.
8. D. ZEITLIN, On coefficient identities for cyclotomic polynomials $F_{pq}(x)$, *Amer. Math. Montly* **75** (1968), 976–980.