Arch. Math. 78 (2002) 386–396
0003-889X/02/050386-11 $ 3.70/0

Sonderdruck aus
Archiv der Mathematik

A note on a conjecture of Borwein and Choi

By

R. THANGADURAI

Abstract. A polynomial $P(X)$ with coefficients $\{\pm 1\}$ of odd degree $N-1$ is cyclotomic if and only if

$$P(X) = \pm\Phi_{p_1}(\pm X)\Phi_{p_2}(\pm X^{p_1})\cdots\Phi_{p_r}(\pm X^{p_1 p_2\cdots p_{r-1}})$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes, not necessarily distinct, and where $\Phi_p(X) := (X^p-1)/(X-1)$ is the $p-$th cyclotomic polynomial. This is a conjecture of Borwein and Choi [1]. We prove this conjecture for a class of polynomials of degree $N-1 = 2^r p^\ell - 1$ for any odd prime p and for integers $r, \ell \geqq 1$.

1. Introduction. Let

$$\Phi_n(z) = \prod_{a=1,(a,n)=1}^{n} \left(z - e^{\frac{2\pi a i}{n}}\right)$$

denote the $n-$th cyclotomic polynomial. This polynomial is monic with integral coefficients, irreducible, of degree $\phi(n)$, and its roots are the primitive $n-$th roots of unity. More generally, we call a monic polynomial $P(z)$ *cyclotomic* if it has integral coefficients and its roots lie on the unit circle $|z| = 1$. A classical theorem of Kronecker says that an algebraic integer having all its conjugates absolute value 1, then it is a root of unity. (See for instance, L. Washington [6], Chap. 1). Since any root of our cyclotomic polynomial $P(z)$ is an algebraic integer and by the definition all its conjugates have absolute value 1, by the above Kronecker's theorem it is a root of unity. Thus all the roots of $P(z)$ are some roots of unity and hence it justified the name. Consequently, a cyclotomic polynomial $P(z)$ is simply a product of the irreducible polynomials Φ_n.

The main object is to characterise these cyclotomic polynomials in some way. The question of characterising these polynomials arises naturally when one considers the problem of listing all monic polynomials $K(X) \in \mathbb{Z}[X]$ of degree N whose Mahler measure lies below a given bound. Since the cyclotomic polynomials will fall in such a class, the number of cyclotomic polynomials provides a trivial lower bound for the computational complexity of the task (See for instance [3]). Moreover, in [1] Borwein and Choi used this characterization to count the explict number of cyclotomic Littlewood polynomials of even degree having odd coefficients. Thus this number provides a trivial lower bound for the same; but for the smaller class.

Mathematics Subject Classification (2000): Primary 11T22; Secondary 11R18.

Here we are interested to study the cyclotomic polynomials whose coefficients are just ± 1. More generally, the polynomials with coefficients ± 1 are called *Littlewood polynomials* as Borwein [2] calls. Recently, Borwein and Choi [1] proved the following theorem.

Theorem 1.1 (Borwein and Choi). *A polynomial $P(X)$ with coefficients ± 1 of even degree $N-1$ is cyclotomic if and only if*

$$P(X) = \pm\Phi_{p_1}(\pm X)\Phi_{p_2}(\pm X^{p_1})\cdots\Phi_{p_r}(\pm X^{p_1 p_2\cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_{r-1} p_r$ and the p_i are primes, not necessarily distinct.

Indeed, using this characterisation, Borwein and Choi [1] counted the number of such polynomials of even degree explicitly. Now, the question is left unanswered for the odd degree cyclotomic Littlewood polynomials. In fact, in the same paper they conjectured that $P(X)$ will be of the same form when $N-1$ is odd. More precisely, they conjectured

Conjecture. A polynomial $P(X)$ with coefficients ± 1 of odd degree $N-1$ is cyclotomic if and only if

$$P(X) = \pm\Phi_{p_1}(\pm X)\Phi_{p_2}(\pm X^{p_1})\cdots\Phi_{p_r}(\pm X^{p_1 p_2\cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_{r-1} p_r$ and the p_i are primes, not necessarily distinct.

Borwein and Choi [1] proved this conjecture when $N = 2^\ell$ for any $\ell \geqq 1$ and they have checked this conjecture for those polynomials degree upto 210 except for the degree $N = 192$.

We would like to use, for the rest of this article, the following properties of $n-$th cyclotomic polynomials $\Phi_n(X)$ which can be seen, for instance, in [4] and [5].

Lemma 1.2.

(i) $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$.
(ii) *If* $(2, n) = 1$, *then* $\Phi_{2n}(X) = \Phi_n(-X)$.
(iii) *We have,* $\Phi_{p^s m}(X) = \Phi_m(X^{p^s})/\Phi_m(X^{p^{s-1}})$ *whenever* $p \nmid m$, $s \geqq 1$. *In other words,*

$$\Phi_m(X^{p^s}) = \Phi_{p^s m}(X)\Phi_m(X^{p^{s-1}}) = \Phi_{p^s m}(X)\Phi_{p^{s-1}m}(X)\cdots\Phi_{pm}(X)\Phi_m(X),$$

whenever $p \nmid m$ *and* $s \geqq 1$.
(iv) *We have* $\Phi_{pm}(X) = \Phi_m(X^p)$ *whenever* $p|m$.

In the same paper mentioned above, Borwein and Choi [1] proved the following theorem.

Theorem 1.3 [1]. *Let $N = 2^t M$ with $t \geqq 0$ and M is odd. A polynomial $P(X)$ with odd coefficients of degree $N-1$ is cyclotomic if and only if*

$$P(X) = \prod_{d|M} \Phi_d^{e_d}(X)\Phi_{2d}^{e_{2d}}(X)\cdots\Phi_{2^{t+1}d}^{e_{2^{t+1}d}}(X),$$

where $e_\ell \geqq 0$ integers satisfying the following relation

$$e_d + \sum_{i=1}^{t+1} 2^{i-1} e_{2^i d} = \begin{cases} 2^t & \text{for } d|M,\ d > 1 \\ 2^t - 1 & \text{for } d = 1. \end{cases}$$

For the illustration of Theorem 1.3, let us consider the case $N = 2p$ for an odd prime p. In this case, our cyclotomic polynomial

$$P(X) = \Phi_1^{e_1}(X)\Phi_2^{e_2}(X)\Phi_4^{e_4}(X)\Phi_p^{e_p}(X)\Phi_{2p}^{e_{2p}}(X)\Phi_{4p}^{e_{4p}}(X)$$

where e_i satisfy $e_1 + e_2 + 2e_4 = 1$ and $e_p + e_{2p} + 2e_{4p} = 2$. Since e_i are non-negative, we have $(e_1, e_2, e_4) = (1, 0, 0)$ or $(0, 1, 0)$ and $(e_p, e_{2p}, e_{4p}) = (1, 1, 0)$ or $(0, 0, 1)$ or $(2, 0, 0)$ or $(0, 2, 0)$. Therefore, any cyclotomic polynomial $P(X)$ of degree $2p - 1$ will be equal to $\Phi_1(X)\Phi_p(X)\Phi_{2p}(X)$ or $\Phi_1(X)\Phi_{4p}(X)$ or $\Phi_1(X)\Phi_p^2(X)$ or $\Phi_1(X)\Phi_{2p}^2(X)$ or $\Phi_2(X)\Phi_p(X)\Phi_{2p}(X)$ or $\Phi_2(X)\Phi_{4p}(X)$ or $\Phi_2(X)\Phi_p^2(X)$ or $\Phi_2(X)\Phi_{2p}^2(X)$.

Remark 1.4. In the above illustration, the case when at least one of the e_i's such that $e_i \geqq 2$, we have $P(X) = \Phi_1(X)\Phi_p^2(X)$ or $P(X) = \Phi_1(X)\Phi_{2p}^2(X)$ or $P(X) = \Phi_2(X)\Phi_p^2(X)$ or $P(X) = \Phi_2(X)\Phi_{2p}^2(X)$. Thus, in this situation our cyclotomic polynomial $P(X)$ is not the product of distinct factors of irreducible $d-$th cyclotomic polynomials.

Remark 1.5. In the Theorem 1.3, the e_i's are non-negative integers. If we restrict ourself e_i to either 0 or $+1$, then the cyclotomic polynomial $P(X)$ will be the product of distinct factors of d-th irreducible cyclotomic polynomials $\Phi_d(X)$ as remarked in Remark 1.4. More precisely, as in the notations of Theorem 1.3, we have

$$P(X) = \prod_{d|M} \Phi_d^{e_d}(X)\Phi_{2d}^{e_{2d}}(X)\cdots\Phi_{2^{t+1}d}^{e_{2^{t+1}d}}(X),$$

where e_i belongs to $\{0, +1\}$ and satisfy the relation

$$e_d + \sum_{i=1}^{t+1} 2^{i-1} e_{2^i d} = \begin{cases} 2^t & \text{for } d|M, d > 1 \\ 2^t - 1 & \text{for } d = 1. \end{cases}$$

Definition. A cyclotomic Littlewood polynmial $P(X)$ is said to be *square-free* if $P(X)$ can be written as a product of distinct factors of d-th irreducible cyclotomic polynomials $\Phi_d(X)$.

For example, consider $P(X) = X^5 + X^4 + X^3 + X^2 + X + 1$ which is clearly a cyclotomic Littlewood square-free polynomial, since $P(X)$ is equal to the product of $\Phi_2(X)\Phi_3(X)\Phi_6(X)$. On the other hand, if we consider $P(X) = X^5 + X^4 + X^3 - X^2 - X - 1$ is a cyclotomic Littlewood polynomial, since $P(X) = \Phi_1(X)\Phi_p^2(X)$; but not square free.

In this small note, we shall prove the following theorems.

Theorem 1. *Let $N = 2^r p^\ell$ for any odd prime p and for any integers $\ell, r \geqq 1$. Let $P(X)$ be a square-free cyclotomic Littlewood polynomial of degree $N - 1$. Then if we write $p_1 = p_2 = \ldots = p_r = 2$ and $p_{r+1} = p_{r+2} = \ldots = p_{r+\ell} = p$, then we have,*

$$P(X) = \pm\Phi_{p_1}(\pm X)\Phi_{p_2}(X^{p_1})\cdots\Phi_{p_r}(X^{p_1 p_2\cdots p_{r-1}})\cdots\Phi_{p_{r+\ell}}(\pm X^{p_1 p_2\cdots p_{r+\ell-1}}).$$

Theorem 2. *Let $N = 2p$ for any odd prime p. Let $P(X)$ be the cyclotomic Littlewood polynomial of degree $N - 1$. Then, the conjecture is true.*

2. Proof of Theorem 1.

A Key Lemma. *Let $N = 2^r p^\ell$ for an odd prime p and for any integers $r, \ell \geqq 1$. Let $P(X)$ be a square-free cyclotomic Littlewood polynomial of degree $N-1$. Also, assume that the conjecture is true for $P(X)$. Then,*

$$P(X) = \pm\Phi_2(\pm X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})\Phi_p(\pm X^{2^r})\cdots\Phi_p(\pm X^{2^r p^{\ell-1}}).$$

Proof. Given that $P(X)$ is a square-free cyclotomic Littlewood polynomial of degree $N-1$ where $N = 2^r p^\ell$ for an odd prime p and for an integer $\ell \geqq 1$. Let $\mathscr{C}$ be a collection of polynomials such that

$$\mathscr{C} = \left\{\pm\Phi_2(\pm X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})\Phi_p(\pm X^{2^r})\cdots\Phi_p(\pm X^{2^r p^{\ell-1}})\right\}.$$

Claim 1. If $P(X) \in \mathscr{C}$, then $P(X)$ is a square-free cyclotomic Littlewood polynomial. That is, in the view of Theorem 1.3, this polynomial $P(X)$ will have the e_i's which are belonging to $\{0, +1\}$. To prove this claim first let us observe the following;

(1) For each $i = 1, 2, \ldots, r$ and for each $j = 1, 2, \ldots, \ell-1$, we have

$$\begin{aligned}\Phi_p(X^{2^i p^j}) &= \Phi_{p^{j+1}}(X^{2^i}) \text{ (by Lemma 1.2(ii))}\\ &= \Phi_{2^i p^{j+1}}(X)\Phi_{p^{j+1}}(X^{2^{i-1}}) \text{ (by Lemma 1.2(iii))}\\ &= \Phi_{2^i p^{j+1}}(X)\Phi_{2^{i-1}p^{j+1}}(X)\Phi_{p^{j+1}}(X^{2^{i-2}}) \text{ (by Lemma 1.2(iii))}\\ &= \cdots\cdots\cdots\\ &= \Phi_{2^i p^{j+1}}(X)\Phi_{2^{i-1}p^{j+1}}(X)\cdots\Phi_{2p^{j+1}}(X)\Phi_{p^{j+1}}(X).\end{aligned}$$

(2) For each $i = 1, 2, \ldots, r-1$ and for each $j = 1, 2, \ldots, \ell-1$ we have

$$\Phi_p(-X^{2^i p^j}) = \Phi_{p^{j+1}}(-X^{2^i}) = \Phi_{2p^{j+1}}(X^{2^i}) = \Phi_{2^{i+1}p^{j+1}}(X)$$

by Lemma 1.2(ii) and (iv).

(3) For each $i = 2, 3, \ldots, r$ we have

$$\Phi_2(-X^{2^i}) = \Phi_{2^{i+1}}(-X) = \Phi_{2^{i+1}}(X)$$

and

$$\Phi_2(X^{2^i}) = \Phi_{2^{i+1}}(X).$$

Observe that if $P(X) \in \mathscr{C}$, then it is a cyclotomic Littlewood polynomial. Let $P(X) \in \mathscr{C}$ be of the form, for instance, (the other cases are similar)

$$\begin{aligned}P(X) &= -\Phi_2(-X)\Phi_2(X^2)\Phi_2(-X^{2^2})\cdots\Phi_p(-X^{2^r})\Phi_p(-X^{2^r p})\cdots\\ &\quad\cdots\Phi_p(-X^{2^r p^{\ell-2}})\Phi_p(X^{2^r p^{\ell-1}})\\ &= \Phi_1\Phi_{2^2}\Phi_{2^3}\cdots\Phi_{2^r}\Phi_{2^{r+1}p}\Phi_{2^{r+1}p^2}\cdots\Phi_{2^{r+1}p^{\ell-1}}\Phi_{2^r p^\ell}\Phi_{2^{r-1}p^\ell}\cdots\Phi_{2p^\ell}\Phi_{p^\ell}\end{aligned}$$

using the observations (1), (2) and (3). Therefore, in this case, in the view of Theorem 1.3, $P(X)$ has irreducible factors which are determined by the e_i's as follows;

$$(e_1, e_2, e_{2^2}, \ldots, e_{2^{r+1}}) = (1, 0, \underbrace{1, 1, \ldots, 1}_{r-1\ 1's}, 0),$$

$$(e_{p^i}, e_{2p^i}, e_{2^2p^i}, \ldots, e_{2^r p^i}, e_{2^{r+1}p^i}) = (\underbrace{0, 0, \ldots, 0}_{r+1\ 0's}, 1)$$

for all $i = 1, 2, \ldots, \ell - 1$ and

$$(e_{p^\ell}, e_{2p^\ell}, e_{2^2p^\ell}, \ldots, e_{2^rp^\ell}, e_{2^{r+1}p^\ell}) = (\underbrace{1, 1, \ldots, 1}_{r+1 \ \ 1's}, 0).$$

Thus, $P(X)$ is a square-free cyclotomic Littlewood polynomial as we have claimed.

Claim 2. The number of square-free cyclotomic Littlewood polynomials is equal to the cardinality of the set $\mathscr{C}$.

Note that it is fairly clear that the cardinality of the set $\mathscr{C}$ is $2^{\ell+2}$.

Now let us count the number of square-free cyclotomic Littlewood polynomials. Theorem 1.3 gives a clue how to count this number. More precisely, Theorem 1.3 says that if we let $N = 2^tM$ with $t \geqq 0$ and M is odd, then a polynomial $P(X)$ with odd coefficients of degree $N - 1$ is cyclotomic if and only if

$$P(X) = \prod_{d|M} \Phi_d^{e_d}(X)\Phi_{2d}^{e_{2d}}(X) \cdots \Phi_{2^{t+1}d}^{e_{2^{t+1}d}}(X),$$

where $e_\ell \geqq 0$ integers satisfying the following relation

$$e_d + \sum_{i=1}^{t+1} 2^{i-1}e_{2^id} = \begin{cases} 2^t & \text{for } d|M, d > 1 \\ 2^t - 1 & \text{for } d = 1. \end{cases}$$

In our case $t = r$ and $M = p^\ell$ for an odd prime p. Also $P(X)$ has to have coefficients ± 1 and it is square-free. Therefore, those non-negative integers e_i should be either 0 or $+1$ for all i satisfying the following relations;

$$e_1 + e_2 + 2e_{2^2} + 2^2e_{2^3} + \cdots + 2^{r-1}e_{2^r} + 2^re_{2^{r+1}} = 2^r - 1$$

and for each $i = 1, 2, \ldots, \ell$

$$e_{p^i} + e_{2p^i} + 2e_{2^2p^i} + \cdots + 2^{r-1}e_{2^rp^i} + 2^re_{2^{r+1}p^i} = 2^r.$$

Since e_i's belongs to $\{0, +1\}$ and they are satisfying the above relations, it is enough to count the number of possible cases of e_i satisfying these relations. Since there are $\ell + 1$ equations each of them having 2 choices, the total number of choices forming different sets of solutions of the above equations with the condition that $e_i \in \{0, +1\}$ is $2^{\ell+1}$. For the total number of square-free cyclotomic polynomials, we have to multiply 2 with $2^{\ell+1}$ because if by letting $Q(X) = -P(X)$, then $Q(X)$ is not counted in that. Thus as we claimed, the number of square-free cyclotomic polynomials with odd coefficients is equal to $2^{\ell+2}$ which is the cardinality of the set $\mathscr{C}$.

By Claim 1, we have $\mathscr{C}$ is a subset of the set of square-free cylotomic Littlewood polynomials. By Claim 2, it is clear that the cardinality of the both above mentioned sets are equal. Thus, the set $\mathscr{C}$ exhaust all the square-free cyclotomic Littlewood polynomials. Hence the lemma. □

We shall prove the Theorem 1 inductively as follows. For our convenience, we shall define a statement $A(r, \ell)$ as follows;

$A(r, \ell)$: If $P(X)$ is a square-free cyclotomic Littlewood polynomial of degree $N - 1$ where $N = 2^rp^\ell$ for any odd prime p and for any integers $r, \ell \geqq 1$, then

$$P(X) = \pm\Phi_{p_1}(\pm X)\Phi_{p_2}(X^{p_1}) \cdots \Phi_{p_r}(X^{p_1p_2\cdots p_{r-1}}) \cdots \Phi_{p_{r+\ell}}(\pm X^{p_1p_2\cdots p_{r+\ell-1}}),$$

where $p_1 = p_2 = \ldots = p_r = 2$ and $p_{r+1} = p_{r+2} = \ldots = p_{r+\ell} = p$.

Lemma 2.1. *The statement $A(r, 1)$ is true for all integer $r \geqq 1$.*

Proof. Let $P(X)$ be a square-free cyclotomic Littlewood polynomial of degree $N-1$ where $N = 2^r p$ for any odd prime p and any integer $r \geqq 1$. In the view of Theorem 1.3, we have

$$P(X) = \Phi_1^{e_1}\Phi_2^{e_2}\Phi_{2^2}^{e_{2^2}}\cdots\Phi_{2^{r+1}}^{e_{2^{r+1}}}\Phi_p^{e_p}\Phi_{2p}^{e_{2p}}\Phi_{2^2p}^{e_{2^2p}}\cdots\Phi_{2^{r+1}p}^{e_{2^{r+1}p}}$$

where $e_1 + e_2 + \sum_{i=1}^{r} 2^i e_{2^{i+1}} = 2^r - 1$ and $e_p + e_{2p} + \sum_{i=1}^{r} 2^i e_{2^{i+1}p} = 2^r$. Since $e_i \in \{0, +1\}$, there are only four cases as follows.

Case 1. $(e_1, e_2, \ldots, e_{2^{r+1}}) = (1, 0, \underbrace{1, 1, \ldots, 1}_{r-1\ 1's}, 0)$ and $(e_p, e_{2p}, \ldots, e_{2^{r+1}p}) = (\underbrace{1, 1, \ldots, 1}_{r\ 1's}, 0)$.

In this case, we have

$$P(X) = \Phi_1\Phi_{2^2}\Phi_{2^3}\cdots\Phi_{2^r}\Phi_p\Phi_{2p}\cdots\Phi_{2^r p}.$$

Since, $\Phi_1(X)\Phi_{2^2}(X)\Phi_{2^3}(X)\cdots\Phi_{2^r}(X) = -\Phi_2(-X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})$ using Lemma 1.2(i) and (iv) and since

$$\begin{aligned}\Phi_p(X)\Phi_{2p}(X)\cdots\Phi_{2^r p}(X) &= \Phi_p(X)\big(\Phi_p(X^2)/\Phi_p(X)\big)\cdots\big(\Phi_p(X^{2^r})/\Phi_p(X^{2^{r-1}})\big)\\ &= \Phi_p(X^{2^r}),\end{aligned}$$

we have

$$P(X) = -\Phi_2(-X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})\Phi_p(X^{2^r})$$

which is of desired form.

Case 2. $\big((e_1, e_2, \ldots, e_{2^{r+1}}) = (1, 0, \underbrace{1, 1, \ldots, 1}_{r-1\ 1's}, 0)$ and $e_{2^{r+1}p} = 1$ with $e_{2^i} = 0$ for $i = 0, 1, \ldots, r$.

In this case, we have

$$P(X) = \Phi_1\Phi_{2^2}\Phi_{2^3}\cdots\Phi_{2^r}\Phi_{2^{r+1}p}.$$

Since, as in the Case 1,

$$\Phi_1(X)\Phi_{2^2}(X)\Phi_{2^3}(X)\cdots\Phi_{2^r}(X) = -\Phi_2(-X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})$$

using Lemma 1.2(i) and (iv) and since $\Phi_{2^{r+1}p}(X) = \Phi_p(-X^{2^r})$, we have

$$P(X) = -\Phi_2(-X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})\Phi_p(-X^{2^r})$$

as desired.

Case 3. $\big((e_1, e_2, \ldots, e_{2^{r+1}}) = (0, \underbrace{1, 1, \ldots, 1}_{r-1\ 1's}, 0)$ and $e_{2^{r+1}p} = 1$ with $e_{2^i} = 0$ for $i = 0, 1, \cdots, r$.

In this case, we have

$$P(X) = \Phi_2\Phi_{2^2}\Phi_{2^3}\cdots\Phi_{2^r}\Phi_{2^{r+1}p}.$$

Since, as in the Case 1,

$$\Phi_2(X)\Phi_{2^2}(X)\Phi_{2^3}(X)\cdots\Phi_{2^r}(X) = \Phi_2(X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})$$

using Lemma 1.2(i) and (iv) and since $\Phi_{2^{r+1}p}(X) = \Phi_p(-X^{2^r})$, we have

$$P(X) = \Phi_2(X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})\Phi_p(-X^{2^r})$$

as desired.

Case 4. $(e_1, e_2, \ldots, e_{2^{r+1}}) = (0, \underbrace{1, 1, \ldots, 1}_{r-1\ 1's}, 0)$ and $((e_p, e_{2p}, \ldots, e_{2^{r+1}p}) = (\underbrace{1, 1, \ldots, 1}_{r\ 1's}, 0)$.

In this case, we have

$$P(X) = \Phi_2\Phi_{2^2}\Phi_{2^3}\cdots\Phi_{2^r}\Phi_p\Phi_{2p}\cdots\Phi_{2^rp}.$$

Since, as in the Case 1,

$$\Phi_2(X)\Phi_{2^2}(X)\Phi_{2^3}(X)\cdots\Phi_{2^r}(X) = \Phi_2(X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})$$

using Lemma 1.2(i) and (iv) and since $\Phi_p(X)\Phi_{2p}(X)\cdots\Phi_{2^rp}(X) = \Phi_p(X)\left(\Phi_p(X^2)/\Phi_p(X)\right)\cdots\left(\Phi_p(X^{2^r})/\Phi_p(X^{2^{r-1}})\right) = \Phi_p(X^{2^r})$, we have

$$P(X) = \Phi_2(X)\Phi_2(X^2)\Phi_2(X^{2^2})\cdots\Phi_2(X^{2^{r-1}})\Phi_p(X^{2^r})$$

as desired. Thus the statement $A(r, 1)$ is true for every integer $r \geqq 1$. □

Lemma 2.2. *If the statement $A(r, \ell)$ is true for some integer $\ell \geqq 1$, then $A(r, \ell+1)$ is also true.*

Proof. Suppose the statement $A(r, \ell)$ is true. Let $P(X)$ be a square-free cyclotomic Littlewood polynomial whose degree is $N-1$ where $N = 2^r p^{\ell+1}$. Since $P(X)$ is square-free, we have,

$$P(X) = \Phi_1^{e_1}\Phi_2^{e_2}\Phi_{2^2}^{e_{2^2}}\cdots\Phi_{2^{r+1}}^{e_{2^{r+1}}}\prod_{i=1}^{\ell+1}\left(\Phi_{p^i}^{e_{p^i}}\Phi_{2p^i}^{e_{2p^i}}\Phi_{2^2p^i}^{e_{2^2p^i}}\cdots\Phi_{2^{r+1}p^i}^{e_{2^{r+1}p^i}}\right),$$

where $e_1 + e_2 + \sum_{i=1}^{r} 2^i e_{2^{i+1}} = 2^r - 1$ and $e_{p^i} + e_{2p^i} + \sum_{j=1}^{r} 2^j e_{2^{j+1}p^i} = 2^r$ for every $i = 1, 2, \ldots, \ell+1$ and $e_i \in \{0, +1\}$ for all i.

Let $Q(X)$ be the polynomial defined by

$$Q(X) = \Phi_1^{e_1}\Phi_2^{e_2}\Phi_{2^2}^{e_{2^2}}\cdots\Phi_{2^{r+1}}^{e_{2^{r+1}}}\prod_{i=1}^{\ell}\left(\Phi_{p^i}^{e_{p^i}}\Phi_{2p^i}^{e_{2p^i}}\Phi_{2^2p^i}^{e_{2^2p^i}}\cdots\Phi_{2^{r+1}p^i}^{e_{2^{r+1}p^i}}\right),$$

where $e_1 + e_2 + \sum_{i=1}^{r} 2^i e_{2^{i+1}} = 2^r - 1$ and $e_{p^i} + e_{2p^i} + \sum_{j=1}^{r} 2^j e_{2^{j+1}p^i} = 2^r$ for every $i = 1, 2, \ldots, \ell$ and $e_i \in \{0, +1\}$ for all i. Let $H(X)$ be the polynomial defined as

$$H(X) = \Phi_{p^{\ell+1}}^{e_{p^{\ell+1}}}\Phi_{2p^{\ell+1}}^{e_{2p^{\ell+1}}}\Phi_{2^2p^{\ell+1}}^{e_{2^2p^{\ell+1}}}\cdots\Phi_{2^{r+1}p^{\ell+1}}^{e_{2^{r+1}p^{\ell+1}}},$$

where $e_{p^{\ell+1}} + e_{2p^{\ell+1}} + \sum_{j=1}^{r} 2^j e_{2^{j+1}p^{\ell+1}} = 2^r$ and $e_i \in \{0, +1\}$ for all i.

Now, let us compute the degree of the polynomial $H(X)$. To do that we have to check which e_i's are 0 and which are 1. Because of their relation, there are two cases as follows; The case (1) is $(e_{p^{\ell+1}}, e_{2p^{\ell+1}}, \ldots, e_{2^{r+1}p^{\ell+1}}) = (\underbrace{0, 0, \ldots, 0}_{r+1\ 0's}, 1)$ and the case (2) is $(e_{p^{\ell+1}}, e_{2p^{\ell+1}}, \ldots, e_{2^{r+1}p^{\ell+1}}) = (\underbrace{1, 1, \ldots, 1}_{r+1\ 1's}, 0)$. In the first case, the degree of $H(X) = \Phi_{2^{r+1}p^{\ell+1}}(X)$ is $\phi(2^{r+1}p^{\ell+1}) = 2^r p^{\ell}(p-1)$. In the second case, the degree of $H(X) = \Phi_{p^{\ell+1}}\Phi_{2p^{\ell+1}}\cdots\Phi_{2^r p^{\ell+1}}$ is $p^{\ell}(p-1)(1+1+2+\cdots+2^{r-1}) = 2^r p^{\ell}(p-1)$. Thus in the both the cases the degree of $H(X)$ is $2^r p^{\ell}(p-1)$.

Now, the degree of $Q(X)$ is the degree of $P(X)$ minus the degree of $H(X)$. That is, the degree of $Q(X)$ is $2^r p^{\ell+1} - 1 - 2^r p^{\ell}(p-1) = 2^r p^{\ell} - 1$. Also note that $Q(X)$ is a square-free cyclotomic Littlewood polynomial of degree $2^r p^{\ell} - 1$ with $e_i \in \{0, +1\}$. Since by assumption, the statement $A(r, \ell)$ is true, $Q(X)$ is of desired form.

To prove the result it is enough to prove that $H(X)$ is of desired form and if so, by glueing together $Q(X)$ and $H(X)$ we get $P(X)$ is of desired form and hence the statement $A(r, \ell+1)$ is true.

Case 1. $(e_{p^{\ell+1}}, e_{2p^{\ell+1}}, \ldots, e_{2^{r+1}p^{\ell+1}}) = (\underbrace{0, 0, \ldots, 0}_{r+1\ 0's}, 1)$.

In this case,

$$H(X) = \Phi_{2^{r+1}p^{\ell+1}}(X) = \Phi_{2p}(X^{2^r p^{\ell}}) = \Phi_p(-X^{2^r p^{\ell}})$$

as desired. Here we are using Lemma 1.2 (ii), (iii) and (iv).

Case 2. $(e_{p^{\ell+1}}, e_{2p^{\ell+1}}, \ldots, e_{2^{r+1}p^{\ell+1}}) = (\underbrace{1, 1, \ldots, 1}_{r+1\ 1's}, 0)$.

In this case,

$$H(X) = \Phi_{p^{\ell+1}}(X)\Phi_{2p^{\ell+1}}(X)\cdots\Phi_{2^r p^{\ell+1}}(X).$$

By Lemma 1.2 (iii) we have

$$\Phi_{2^i p^{\ell+1}}(X) = \Phi_p(X^{2^i p^{\ell}})/\Phi_p(X^{2^{i-1}p^{\ell}})$$

for each $i = r, r-1, \ldots, 2, 1$. Clearly, for i and $i+1$ we have,

$$\begin{aligned}\Phi_{2^i p^{\ell+1}}(X)\Phi_{2^{i+1}p^{\ell+1}}(X) &= \left(\Phi_p(X^{2^i p^{\ell}})/\Phi_p(X^{2^{i-1}p^{\ell}})\right)\left(\Phi_p(X^{2^{i+1}p^{\ell}})/\Phi_p(X^{2^i p^{\ell}})\right)\\ &= \Phi_p(X^{2^{i+1}p^{\ell}})/\Phi_p(X^{2^{i-1}p^{\ell}})\end{aligned}$$

for $i = r-1, r-2, \ldots, 1$. Therefore, clearly,

$$H(X) = \Phi_p(X^{2^r p^{\ell}})$$

as desired. □

Proof of the Theorem 1. Let $P(X)$ be a square-free cyclotomic Littlewood polynomial of degree $N-1$ where $N = 2^r p^{\ell}$ for some odd prime p and for any integer $r, \ell \geqq 1$. Since by Lemma 2.1 the statement $A(m, 1)$ is true for all integer $m \geqq 1$, in paritícular, the statement $A(r, 1)$ is true. Now we apply Lemma 2.2 to get the statement $A(r, 2)$ is true and hence by applying Lemma 2.2 recursively $\ell - 1$ times, we get the statement $A(r, \ell)$ is true. Thus $P(X)$ is of desired form. □

3. Proof of Theorem 2.

Theorem 2. *Let $N = 2p$ for an odd prime p. Let $P(X)$ be a cyclotomic Littlewood polynomial whose degree is $N - 1 = 2p - 1$. Then*

$$P(X) = \pm\Phi_2(\pm X)\Phi_p(\pm X^2) \text{ or } \pm\Phi_p(\pm X)\Phi_2(\pm X^p).$$

Proof. As in the notations of Theorem 1.3, in this case, we have $t = 1$ and $M = p$. Therefore,

$$P(X) = \Phi_1^{e_1}(X)\Phi_2^{e_2}(X)\Phi_4^{e_4}(X)\Phi_p^{e_p}(X)\Phi_{2p}^{e_{2p}}(X)\Phi_{4p}^{e_{4p}}(X)$$

satisfying $e_1 + e_2 + 2e_4 = 1$ and $e_p + e_{2p} + 2e_{4p} = 2$. Since e_i are non-negative integers, there arise eight different cases as follows.

Case i. $((e_1, e_2, e_4) = (1, 0, 0)$ and $(e_p, e_{2p}, e_{4p}) = (1, 1, 0))$.

In this case, the cyclotomic polynomial $P(X)$ looks like

$$P(X) = \Phi_1(X)\Phi_p(X)\Phi_{2p}(X).$$

Since $\Phi_1(X) = X - 1 = -(-X + 1) = -\Phi_2(-X)$ and as $(2, p) = 1$, $\Phi_{2p} = \Phi_p(X^2)/\Phi_p(X)$ (using Lemma 1.2(iii)), we have

$$P(X) = -\Phi_2(-X)\Phi_p(X)\Phi_p(X^2)/\Phi_p(X) = -\Phi_2(-X)\Phi_p(X^2)$$

as desired.

Case ii. $((e_1, e_2, e_4) = (1, 0, 0)$ and $(e_p, e_{2p}, e_{4p}) = (0, 0, 1))$.

Since $\Phi_{4p}(X) = \Phi_{2p}(X^2) = \Phi_p(-X^2)$ and $\Phi_1(X) = -\Phi_2(-X)$, in this case we get

$$P(X) = \Phi_1(X)\Phi_{4p}(X) = -\Phi_2(-X)\Phi_{2p}(X^2) = -\Phi_2(-X)\Phi_p(-X^2)$$

as desired.

Case iii. $((e_1, e_2, e_4) = (1, 0, 0)$ and $(e_p, e_{2p}, e_{4p}) = (2, 0, 0))$.

Since $\Phi_p(X) = \Phi_{2p}(-X)$ and $\Phi_1(X) = -\Phi_2(-X)$, we have

$$\Phi_1(X)\Phi_p(X)\Phi_p(X) = -\Phi_2(-X)\Phi_{2p}(-X)\Phi_p(X) = -\Phi_p(X)\Phi_2(-X^p)$$

as desired.

Case iv. $((e_1, e_2, e_4) = (1, 0, 0)$ and $(e_p, e_{2p}, e_{4p}) = (0, 2, 0))$.

Since $\Phi_1(X)\Phi_{2p}^2(X)$ is a cyclotomic polynomial but not a Littlewood polynomial, since,

$$P(X) = X^{2p-1} - 3X^{2p-2} + 5X^{2p-3} - \cdots - 5X^2 + 3X - 1.$$

Therefore in this case we may not expect the desired form.

For the other cases, we simply write the result, since they are similar in nature.

(v) In this case, $(e_1, e_2, e_4) = (0, 1, 0)$ and $(e_p, e_{2p}, e_{4p}) = (1, 1, 0)$. Therefore

$$\Phi_2(X)\Phi_p(X)\Phi_{2p}(X) = \Phi_2(X)\Phi_p(X^2).$$

(vi) In this case, $(e_1, e_2, e_4) = (0, 1, 0)$ and $(e_p, e_{2p}, e_{4p}) = (0, 0, 1)$. Therefore

$$\Phi_2(X)\Phi_{4p}(X) = \Phi_2(X)\Phi_p(-X^2).$$

(vii) In this case, $(e_1, e_2, e_4) = (0, 1, 0)$ and $(e_p, e_{2p}, e_{4p}) = (0, 2, 0)$. Therefore,

$$\Phi_2(X)\Phi_{2p}^2(X) = \Phi_p(X)\Phi_2(X^p).$$

(viii) In this case, $(e_1, e_2, e_4) = (0, 1, 0)$ and $(e_p, e_{2p}, e_{4p}) = (2, 0, 0)$. But the polynomial $\Phi_2(X)\Phi_p^2(X)$ contains coefficients other than ± 1 and hence it is not a Littlewood polynomial, since,

$$\Phi_2(X)\Phi_p^2(X) = 1 + 3X + 5X^2 + \cdots + 5X^{2p-3} + 3X^{2p-2} + X^{2p-1}.$$

Thus we have exhausted all the cases, in which all cyclotomic Littlewood polynomials have the desired form. □

4. Concluding remarks. Let us consider the case when $N = 2pq$ where $p < q$ are two odd primes. Let $P(X)$ be the cyclotomic Littlewood polynomial whose degree is $N - 1$. Then if we assume that $P(X)$ is of one of the following forms

$$P(X) = \pm\Phi_2(\pm X)\Phi_p(\pm X^2)\Phi_q(\pm X^{2p}),$$

then $P(X)$ is a product of distinct factors of irreducible cyclotomic polynomials.

(1) $\pm\Phi_2(X)\Phi_p(X^2)\Phi_q(X^{2p}) = \pm\Phi_2(X)\Phi_p(X)\Phi_{2p}(X)\Phi_q(X)\Phi_{2q}(X)\Phi_{pq}\Phi_{2pq}(X)$ by the Lemma 1.2(iii). In these cases, $(e_1, e_2, e_4) = (0, 1, 0)$, $(e_p, e_{2p}, e_{4p}) = (1, 1, 0)$, $(e_q, e_{2q}, e_{4q}) = (1, 1, 0)$, and $(e_{pq}, e_{2pq}, e_{4pq}) = (1, 1, 0)$. Clearly,

$$\pm\Phi_2(X)\Phi_p(X^2)\Phi_q(X^{2p}) = \pm(1 + X + X^2 + \cdots + X^{2p-2} + X^{2p-1}).$$

(2) $\pm\Phi_2(X)\Phi_p(X^2)\Phi_q(-X^{2p}) = \pm\Phi_2(X)\Phi_p(X)\Phi_{2p}(X)\Phi_{4q}(X)\Phi_{4pq}(X)$ by Lemma 1.2(ii), (iii) and (iv). In these cases, $(e_1, e_2, e_4) = (0, 1, 0)$, $(e_p, e_{2p}, e_{4p}) = (1, 1, 0)$, $(e_q, e_{2q}, e_{4q}) = (0, 0, 1)$, and $(e_{pq}, e_{2pq}, e_{4pq}) = (0, 0, 1)$.

(3) $\pm\Phi_2(X)\Phi_p(-X^2)\Phi_q(X^{2p}) = \pm\Phi_2(X)\Phi_{4p}(X)\Phi_q(X)\Phi_{2q}(X)\Phi_{pq}\Phi_{2pq}(X)$ by Lemma 1.2(ii), (iii) and (iv). In these cases, $(e_1, e_2, e_4) = (0, 1, 0)$, $(e_p, e_{2p}, e_{4p}) = (0, 0, 1)$, $(e_q, e_{2q}, e_{4q}) = (1, 1, 0)$, and $(e_{pq}, e_{2pq}, e_{4pq}) = (1, 1, 0)$.

(4) $\pm\Phi_2(X)\Phi_p(-X^2)\Phi_q(-X^{2p}) = \pm\Phi_2(X)\Phi_{4p}(X)\Phi_{4q}(X)\Phi_{4pq}(X)$ using Lemma 1.2(ii), (iii) and(*iv*). In these cases, $(e_1, e_2, e_4) = (0, 1, 0)$, $(e_p, e_{2p}, e_{4p}) = (0, 0, 1)$, $(e_q, e_{2q}, e_{4q}) = (0, 0, 1)$, and $(e_{pq}, e_{2pq}, e_{4pq}) = (0, 0, 1)$.

(5) $\pm\Phi_2(-X)\Phi_p(X^2)\Phi_q(X^{2p}) = \mp\Phi_1(X)\Phi_p(X)\Phi_{2p}(X)\Phi_q(X)\Phi_{2q}(X)\Phi_{pq}\Phi_{2pq}(X)$ by the Lemma 1.2(i) and (iii). In these cases, $(e_1, e_2, e_4) = (1, 0, 0)$, $(e_p, e_{2p}, e_{4p}) = (1, 1, 0)$, $(e_q, e_{2q}, e_{4q}) = (1, 1, 0)$, and $(e_{pq}, e_{2pq}, e_{4pq}) = (1, 1, 0)$.

(6) $\pm\Phi_2(-X)\Phi_p(X^2)\Phi_q(-X^{2p}) = \mp\Phi_1(X)\Phi_p(X)\Phi_{2p}(X)\Phi_{4q}(X)\Phi_{4pq}(X)$ by Lemma 1.2(i), (ii), (iii) and (iv). In these cases, $(e_1, e_2, e_4) = (1, 0, 0)$, $(e_p, e_{2p}, e_{4p}) = (1, 1, 0)$, $(e_q, e_{2q}, e_{4q}) = (0, 0, 1)$, and $(e_{pq}, e_{2pq}, e_{4pq}) = (0, 0, 1)$.

(7) $\pm\Phi_2(-X)\Phi_p(-X^2)\Phi_q(X^{2p}) = \mp\Phi_1(X)\Phi_{4p}(X)\Phi_q(X)\Phi_{2q}(X)\Phi_{pq}\Phi_{2pq}(X)$ by Lemma 1.2(i), (ii), (iii) and (iv). In these cases, $(e_1, e_2, e_4) = (1, 0, 0)$, $(e_p, e_{2p}, e_{4p}) = (0, 0, 1)$, $(e_q, e_{2q}, e_{4q}) = (1, 1, 0)$, and $(e_{pq}, e_{2pq}, e_{4pq}) = (1, 1, 0)$.

(8) $\pm\Phi_2(-X)\Phi_p(-X^2)\Phi_q(-X^{2p}) = \mp\Phi_1(X)\Phi_{4p}(X)\Phi_{4q}(X)\Phi_{4pq}(X)$ by Lemma 1.2(ii), (iii) and (iv). In these cases, $(e_1, e_2, e_4) = (1, 0, 0)$, $(e_p, e_{2p}, e_{4p}) = (0, 0, 1)$, $(e_q, e_{2q}, e_{4q}) = (0, 0, 1)$, and $(e_{pq}, e_{2pq}, e_{4pq}) = (0, 0, 1)$.

Thus when $N = 2pq$ where $p < q$ are odd primes, if any cyclotomic Littlewood polynomial $P(X)$ satisfying the Conjecture and which is of one of the above the above forms, then $P(X)$ is a square-free cyclotomic Littlewood polynomial.

Let $\mathscr{C}$ be a collection of polynomials defined as

$$\mathscr{C} = \left\{\pm\Phi_2(\pm X)\Phi_p(\pm X^2)\Phi_q(\pm X^{2p})\right\}.$$

Clearly, the cardinality of $\mathscr{C}$ is $2^4 = 16$. All these 16 polynomials which we have discussed above belong to $\mathscr{C}$. As we have seen above, these polynomials are square-free. As in the Key Lemma in Section 2, can we expect this set $\mathscr{C}$ to exhaust all square-free cyclotomic Littlewood polynomials? The answer is NO. In this case, unlike the Key Lemma in Section 2, $\mathscr{C}$ can not exhaust all the square-free cyclotomic Littlewood polynomials. For example, consider the case when $(e_1, e_2, e_4) = (0, 1, 0)$, $(e_p, e_{2p}, e_{4p}) = (1, 1, 0)$, $(e_q, e_{2q}, e_{4q}) = (0, 0, 1)$, and $(e_{pq}, e_{2pq}, e_{4pq}) = (1, 1, 0)$. That is, we are considering the following polynomial

$$\Phi_2(X)\Phi_p(X)\Phi_{2p}(X)\Phi_{4q}(X)\Phi_{pq}(X)\Phi_{2pq}(X) = \Phi_2(X)\Phi_q(-X^2)\Phi_p(X^{2q}).$$

This case was not covered in any of the above 16 cases.

References

[1] P. BORWEIN and K.-K. S. CHOI, On Cyclotomic polynomials with ± 1 coefficients. Experimental Math. **8**, No. 4, 399–407 (1999).
[2] P. BORWEIN, Paul Erdös and Polynomials. Preprint.
[3] D. W. BOYD and H. L. MONTGOMERY, Cyclotomic Partitions. In: Number theory (Banff, AB, 1988), 7–25. Berlin 1990.
[4] P. RIBENBOIM, Fermat's last theorem for amateurs. New York 1999.
[5] R. THANGADURAI, On the coefficients of cyclotomic polynomials. To appear in the Proceedings on "Cyclotomic Fields", Pune 1999.
[6] L. WASHINGTON, Introduction to cyclotomic fields, Second edition. Graduate Texts in Math. **83**, New York 1997.

Eingegangen am 6. 7. 2000

Anschrift des Autors:

R. Thangadurai
The Institute of Mathematical Sciences
C.I.T. Campus, Taramani
Chennai 600 113
India
thanga@@imsc.ernet.in

Current address:
R. Thangadurai
Stat-Math Division
Indian Statistical Institute
203, B.T. Road
Kolkata – 700108
India
thanga_v@isical.ac.in