ON THE LITTLEWOOD CYCLOTOMIC POLYNOMIALS

SHABNAM AKHTARI AND STEPHEN K. CHOI

Abstract. In this article, we study the cyclotomic polynomials of degree $N-1$ with coefficients restricted to the set $\{+1,-1\}$. By a cyclotomic polynomial we mean any monic polynomial with integer coefficients and all roots of modulus 1. By a careful analysis of the effect of Graeffe's root squaring algorithm on cyclotomic polynomials, P. Borwein and K.K. Choi gave a complete characterization of all cyclotomic polynomials with odd coefficients. They also proved that a polynomial $p(x)$ with coefficients ± 1 of even degree $N-1$ is cyclotomic if and only if $p(x) = \pm\Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1})\dots\Phi_{p_r}(\pm x^{p_1p_2\cdots p_{r-1}})$, where $N = p_1p_2\dots p_r$ and the p_i are primes, not necessarily distinct. Here $\Phi_p(x) := \frac{x^p-1}{x-1}$ is the pth cyclotomic polynomial. Based on substantial computation, they also conjectured that this characterization also holds for polynomials of odd degree with ± 1 coefficients. We consider the conjecture for odd degree here. Using Ramanujan's sums, we solve the problem for some special cases. We prove that the conjecture is true for polynomials of degree $2^\alpha p^\beta - 1$ with odd prime p or separable polynomials of any odd degree.

1. Introductory Remarks and Statements of Results

We are interested in studying polynomials with coefficients restricted to the set $\{+1,-1\}$. This particular set of polynomials has drawn much attention and there are a number of difficult old questions concerning it (e.g. see [1]). Littlewood raised a number of these questions in [11] and so we call these polynomials **Littlewood polynomials**. A Littlewood polynomial of degree $N-1$ has L_2 norm on the unit circle equal to $\sqrt{N}$. Many of the questions raised concern comparing the behavior of these polynomials in other norms to the L_2 norm. One of the older and more intriguing of these asks whether such polynomials can be "flat". Specifically, do there exist two positive constants C_1 and C_2 so that for each N there is Littlewood polynomial $P(z)$ of degree $N-1$ with

$$C_1\sqrt{N} < |p(z)| < C_2\sqrt{N}$$

for each z of modulus 1?

The size of the L_p norm of Littlewood polynomials has been studied from a number of points of view. The problem of minimizing the L_4 norm has also attracted a lot of attention. (e.g. see [3] - [6])

Mahler raised the question of maximizing the Mahler measure of Littlewood polynomials. The Mahler measure is the limit of the L_p norm on the circle as

Date: April 3, 2007.

2000 *Mathematics Subject Classification.* Primary: 11R09; Secondary: 11Y99.

Key words and phrases. Cyclotomic polynomial, Littlewood polynomial, Separable polynomial, Newton's identity, Ramanujan's sum.

Research of Stephen Choi was supported by NSERC of Canada.

$p \to 0^+$ and one would expect this to be closely related to the minimizing problem for the L_4 norm above (see [9]).

Let $P(x)$ be a cyclotomic polynomial of degree $N-1$, that is

$$P(x) = a_0 + a_1 x + \cdots + a_{N-1}x^{N-1}, \quad a_i \in \mathbb{Z}$$

and all the roots of $P(x)$ are of modulus one. For convenience, we also let $n = N-1$ so that n is the degree and N is the length of the polynomial $P(x)$. Let $\Phi_m(x)$ be the mth irreducible cyclotomic polynomial, that is,

$$\Phi_m(x) := \prod_{\substack{j=1 \\ (j,m)=1}}^{m} \left(x - \xi_m^j\right)$$

whose roots are the primitive mth roots of unity. Here $(j,m) = \gcd(j,m)$ and $\xi_m := e^{2\pi i/m}$.

By a classical result of Kronecker, polynomials with integer coefficients having minimal Mahler measure 1 are precisely cyclotomic polynomials, or x^n.

In [2], P. Borwein and K.K. Choi addressed the question of characterizing the cyclotomic Littlewood polynomials of even degree and showed that all cyclotomic polynomials with **odd coefficients** are characterized as follows.

Theorem 1.1. *Let $N = 2^t M$ with $t \geq 0$ and $(2, M) = 1$. A polynomial, $P(x)$, with odd coefficients of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \pm \prod_{d|M} \Phi_d^{e(d)}(x)\Phi_{2d}^{e(2d)}(x)\cdots\Phi_{2^{t+1}d}^{e(2^{t+1}d)}(x),$$

and the $e(d)$'s satisfy the condition

$$e(d) + \sum_{i=1}^{t+1} 2^{i-1}e(2^i d) = \begin{cases} 2^t & \text{for } d \mid M,\ d > 1; \\ 2^t - 1 & \text{for } d = 1. \end{cases}$$

Furthermore, if N is odd, then any polynomial, $P(x)$, with odd coefficients of even degree $N-1$ is cyclotomic if and only if

$$P(x) = \pm \prod_{d|N, d>1} \Phi_d^{e(d)}(\pm x)$$

where the $e(d)$'s are non-negative integers.

They also gave an explicit formula for the number of such polynomials. Their analysis in [2] was based on a careful treatment of Graeffe's root squaring algorithm. It transpires that all cyclotomic Littlewood polynomials of fixed degree have the same fixed point on iterating Graeffe's root squaring algorithm. This gives a characterization of all cyclotomic polynomials with odd coefficients.

Among the polynomials with odd coefficients, we are particularly interested in Littlewood polynomials, i.e., with ± 1 coefficients. As a corollary of Theorem 1.1, Borwein and Choi obtained the characterization of all Littlewood cyclotomic polynomials of even degree.

Theorem 1.2. *Suppose N is odd. A Littlewood polynomial, $P(x)$, of 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.

The authors in [2] conjectured that Theorem 1.2 also holds for polynomials of odd degree. They computed up to degree 210 (except for the case $n = 191$). The computation was based on computing all cyclotomic polynomials with odd coefficients of a given degree and then checking which were actually Littlewood and checking that this set matched the set generated by the conjecture. For example, for $n = 143$ there are 6773464 cyclotomic polynomials with odd coefficients of which 416 are Littlewood.

Conjecture 1.3. *A Littlewood polynomial, $P(x)$, of degree $N-1$ is cyclotomic if and only if*

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

where $N = p_1p_2\cdots p_r$ and all p_i are primes, not necessarily distinct.

In this article, we prove the conjecture is true for polynomials of degree $n = 2^\alpha p^\beta - 1$ with odd prime p or for separable polynomials of any odd degree.

Theorem 1.4. *Conjecture 1.3 is true for separable Littlewood cyclotomic polynomials.*

Theorem 1.5. *Conjecture 1.3 is true for the Littlewood cyclotomic polynomials of degree $N-1$ where $N = 2^\alpha p^\beta$ and p is an odd prime.*

Here we recall that a separable polynomial is a polynomial with no repeated roots.

In [12], R. Thangadurai proves that Conjecture 1.3 is true for separable polynomials of degree $n = 2^r p^l - 1$. There is apparently a typographical error in the abstract of [12] where the word "separable" is forgotten to be written and the separability in fact is assumed in his proof. Our results improve Thangadurai's result.

2. Separable Polynomials

Let $P(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_i = \pm 1$ and $N = n+1 = 2^tM$ with $2 \nmid M$ be a Littlewood polynomial of degree $N-1$. We also assume that $P(x)$ is a product of cyclotomic polynomials. Without loss of generality, assume $a_0 = a_1 = +1$, by replacing by $-P(x)$ or $P(-x)$ if necessary. Now consider

$$\begin{aligned} Q(x) &= -\Phi_1(x)P(x) \\ &= (1-x)P(x) \\ &= a_0 + (a_1-a_0)x + \cdots + (a_{N-1}-a_{N-2})x^{N-1} - a_{N-1}x^N \\ &:= b_0 + b_1x + \cdots + b_Nx^N \end{aligned} \tag{2.1}$$

with $b_0 = a_0 = 1$ and $b_N = -a_{N-1} = \pm 1$ but $b_1, b_2, \ldots, b_{N-1} \in \{-2, 0, 2\}$ because $a_i = \pm 1$. Also since $a_1 = 1$, so $b_1 = 0$. We now suppose that

$$a_0 = a_1 = \cdots = a_{i-1} = 1 \quad \text{and} \quad a_i = -1$$

for some $i \geq 2$ (If such i does not exist, the result becomes trivial because $P(x) = 1 + x + \cdots + x^n$). This corresponds to

$$b_0 = 1,\ b_1 = \cdots = b_{i-1} = 0 \quad \text{and} \quad b_i = -2. \tag{2.2}$$

By Theorem 1.1, we have the factorization of $Q(x)$ into cyclotomic polynomials

$$Q(x) = \prod_{d|M} \prod_{l=0}^{t+1} \Phi_{2^l d}^{e(2^l d)}(x)$$

where for any $d|M$

$$e(d) + e(2d) + 2e(4d) + \cdots + 2^t e(2^{t+1}d) = \sum_{l=0}^{t+1} \phi(2^l) e(2^l d) = 2^t. \tag{2.3}$$

Let S_j be the sum of the jth power of all the roots of $Q(x)$. Since the sum of the jth power of all the roots of $\Phi_m(x)$ is

$$c_m(j) = \sum_{\substack{h=1 \\ (h,m)=1}}^{m} \xi_m^{hj}$$

where $c_m(j)$ is the Ramanujan's sum, so

$$S_j = \sum_{d|M} \sum_{l=0}^{t+1} e(2^l d) c_{2^l d}(j). \tag{2.4}$$

Since $P(x)$ is a product of cyclotomic polynomials, it follows that $x^{N-1}P(x) = \pm P\left(\frac{1}{x}\right)$ and consequently we may write Newton's identity (e.g. p.5 of [8]) as

$$S_j + b_1 S_{j-1} + \cdots + b_{j-1} S_1 + j b_j = 0$$

for $j \leq n$.

For $j = 1$, we have $S_1 + b_1 = 0$. However, $b_1 = 0$ and hence $S_1 = 0$.

For $i > 2$ and $j = 2$, we have $b_1 = b_2 = 0$ and so

$$S_2 = -b_1 S_1 - 2b_2 = 0.$$

Inductively, we have

$$S_1 = \cdots = S_{i-1} = 0. \tag{2.5}$$

For $j = i$, we have

$$S_i = -i b_i = 2i. \tag{2.6}$$

In order to prove Conjecture 1.3 for our cases, we aim to obtain some "periodic" properties for S_j.

The following two lemmas are elementary results about the greatest common divisor which are useful later.

Lemma 2.1. *Let N and k be positive integers. Then for any $d|N$, we have*

$$(d, k) = (d, (N, k)).$$

Proof. For any $d \mid N$, we first see that since $(N, k) \mid k$, so

$$(d, (N, k)) \mid (d, k).$$

On the other hand, since $d|N$ so $(d, k)|(N, k)$. Thus $(d, k)|(d, (N, k))$. This proves the lemma. □

For the remainder of this section, we write the length N of $P(x)$ as $N = 2^t M$ with M odd.

Lemma 2.2. *If $2^{t+1} \nmid k$, then $(2^{t+1}d, k) = (2^{t+1}d, (N, k))$ for any $d \mid M$.*

Proof. Let $d|M$. Since $(N,k)|k$, we first have

$$(2^{t+1}d,(N,k)) \mid (2^{t+1}d,k).$$

It remains to prove that

$$(2^{t+1}d,k) \mid (2^{t+1}d,(N,k)). \tag{2.7}$$

Let p be an odd prime. If $p^\alpha \mid (2^{t+1}d,k)$ then $p^\alpha \mid (d,k)$. Clearly, $p^\alpha \mid (N,k)$. Thus $p^\alpha \mid (2^{t+1}d,(N,k))$.

If $2^\alpha \mid (2^{t+1}d,k)$ then $2^\alpha \mid k$. Because $2^{t+1} \nmid k$ we get $\alpha \le t$. Since $N = 2^t M$, so $2^\alpha \mid N$ and hence $2^\alpha \mid (N,k)$. Therefore, $2^\alpha \mid (2^{t+1}d,(N,k))$. This proves (2.7). □

It is well known (e.g. Theorem 272 of [10]) that

$$c_q(m) = \mu\left(\frac{q}{(m,q)}\right)\phi(q)\left(\phi\left(\frac{q}{(m,q)}\right)\right)^{-1}. \tag{2.8}$$

where $\mu(n)$ is the Möbius function and $\phi(n)$ is Euler's totient function. We note from (2.8) that if $(q,m_1) = (q,m_2)$ then

$$c_q(m_1) = c_q(m_2). \tag{2.9}$$

We next establish some "periodic" properties for S_j.

Lemma 2.3. *If $2^{t+1} \nmid k$, then we have*

$$S_k = S_{(N,k)}.$$

Proof. In view of Lemma 2.1 (for $0 \le j \le t$) and Lemma 2.2 (for $j = t+1$), if $2^{t+1} \nmid k$, then $(2^j d,k) = (2^j d,(N,k))$ for $j = 0,1,\cdots,t+1$ and $d \mid M$. Hence from (2.4) we have

$$\begin{aligned} S_k &= \sum_{d|M}\sum_{l=0}^{t+1} e(2^l d)c_{2^l d}(k) \\ &= \sum_{d|M}\sum_{l=0}^{t+1} e(2^l d)c_{2^l d}((N,k)) \\ &= S_{(N,k)}. \end{aligned}$$

□

Lemma 2.4. *If $2^{t+1} \mid k$ and $k \le N-1$, then $S_k = 0$.*

Proof. Let $k = 2^{t+1}k'$. Then for any $0 \le j \le t+1$ and $d \mid M$, we have

$$\begin{aligned} c_{2^j d}(k) &= \mu\left(\frac{2^j d}{(2^j d,k)}\right)\phi(2^j d)\left(\phi\left(\frac{2^j d}{(2^j d,k)}\right)\right)^{-1} \\ &= \mu\left(\frac{d}{(d,k)}\right)\phi(2^j)\phi(d)\left(\phi\left(\frac{d}{(d,k)}\right)\right)^{-1} \\ &= c_d(k)\phi(2^j). \end{aligned}$$

It thus follows that from (2.4) that

$$\begin{aligned} S_k &= \sum_{d|M}\sum_{j=0}^{t+1} e(2^j d)c_{2^j d}(k) \\ &= \sum_{d|M}\sum_{j=0}^{t+1} e(2^j d)\phi(2^j)c_d(k) \\ &= \sum_{d|M} c_d(k)\sum_{j=0}^{t+1} e(2^j d)\phi(2^j) \\ &= 2^t \sum_{d|M} c_d(k) \end{aligned}$$

by (2.3). We note that $k \not\equiv 0 \pmod{M}$; otherwise $N|k$ and $k \geq N$. The lemma now follows from the fact that $\sum_{d|M} c_d(k) = 0$ for $k \not\equiv 0 \pmod{M}$. □

Lemma 2.5. *For the integer i defined in* (2.2)*, we have $i \mid N$.*

Proof. Since $S_i = 2i \neq 0$, by Lemma 2.4, $2^{t+1} \nmid i$. By Lemma 2.3, $S_i = S_{(N,i)}$. If $(N,i) < i$ then $S_{(N,i)} = 0 \neq S_i$ by (2.2). Hence $(N,i) = i$ and $i \mid N$. □

We end this section by proving Theorem 1.4.

Proof of Theorem 1.4. Suppose $P(x)$ is a separable cyclotomic Littlewood polynomial of degree $N-1$ with $N = 2^t M$, $t \geq 1$ and odd integer M (for the case $t = 0$, the result follows from Theorem 1.2). Then

$$P(x) = \prod_{d|M} \Phi_d^{e(d)}(x)\Phi_{2d}^{e(2d)} \cdots \Phi_{2^{t+1}d}^{e(2^{t+1}d)}$$

where $e(l)$ is either 0 or 1 (because $P(x)$ is separable) and satisfies

$$e(d) + \sum_{i=1}^{t+1} 2^{i-1} e(2^i d) = \begin{cases} 2^t & \text{if } d \mid M, d > 1; \\ 2^t - 1 & \text{if } d = 1. \end{cases}$$

For $d = 1$, we have

$$e(1) + e(2) + 2e(4) + \cdots + 2^t e(2^{t+1}) = 2^t - 1.$$

Since $e(j)$ is either 0 or 1, so we must have $e(2^{t+1}) = 0$ and

$$e(1) + e(2) = e(4) = e(8) = \cdots = e(2t) = 1.$$

Hence by the well-known property of $\Phi_n(x)$ that for $k \geq 1$,

$$\Phi_{2^k}(x) = \Phi_2(x^{2^{k-1}}),$$

we have

$$\begin{aligned} \Phi_1^{e(1)}(x)\Phi_2^{e(2)}(x)\cdots\Phi_{2^{t+1}}^{e(2^{t+1})}(x) &= \Phi_1^{e(1)}(x)\Phi_2^{e(2)}(x)\Phi_4(x)\cdots\Phi_{2^t}(x) \\ &= \Phi_2(\pm x)F_1(x^2) \end{aligned}$$

for some polynomial $F_1(x)$ in $\mathbb{Z}[x]$. For $d > 1$, we have

$$e(d) + e(2d) + 2e(4d) + \cdots + 2^t e(2^{t+1}d) = 2^t.$$

So we have either

$$e(2^{t+1}d) = 1 \text{ and } e(d) = \cdots = e(2^t d) = 0$$

or

$$e(2^{t+1}d) = 0 \text{ and } e(d) = \cdots = e(2^t d) = 1.$$

So $\Phi_d^{e(d)}(x)\Phi_{2d}^{e(2d)}(x)\cdots\Phi_{2^{t+1}d}^{e(2^{t+1}d)}(x)$ is either

$$\Phi_{2^{t+1}d}(x) = \Phi_{2d}(x^{2^t})$$

or

$$\Phi_d(x)\Phi_{2d}(x)\cdots\Phi_{2^t d}(x) = F_2(x^2)$$

for some $F_2(x)$ in $\mathbb{Z}[x]$. In either case, it is in the form of $F_2(x^2)$ for some $F_2(x)$ in $\mathbb{Z}[x]$. Therefore,

$$P(x) = \Phi_2(\pm x)F(x^2)$$

for some polynomial $F(x)$ in $\mathbb{Z}[x]$. Hence induction applies to $F(x)$ and this proves Theorem 1.4. □

3. The case of $N = 2^\alpha p^\beta$ and Proof of Theorem 1.5

As we mention in §2, we aim to obtain some "periodic" properties for S_j. We wish to show that (c.f. (2.5))

$$\begin{gathered} S_1 = \cdots = S_{i-1} = 0 \\ S_{i+1} = \cdots = S_{2i-1} = 0 \\ \vdots \\ S_{(N/i-1)i+1} = \cdots = S_{N-1} = 0 \end{gathered}$$

i.e.

$$S_j = 0 \text{ for all } j \not\equiv 0 \pmod{i}. \tag{3.10}$$

Suppose (3.10) is proved. Then we claim that

$$b_j = 0 \text{ for all } j \not\equiv 0 \pmod{i}. \tag{3.11}$$

If (3.11) holds then one can easily observe that the coefficients of $P(x)$ are equal in runs of length i, which implies that the polynomial $(1 + x + \cdots + x^{i-1})$ can be factored out and this gives

$$P(x) = (1 + x + \cdots + x^{i-1})P_1(x^i)$$

for some cyclotomic Littlewood polynomial $P_1(x)$ of degree $N/i - 1$. Hence from this, we can apply the induction to $P_1(x)$ on the degree.

To prove the claim (3.11) from (3.10), by Newton's identity, if $j \not\equiv 0 \pmod{i}$, then we have

$$S_j + \sum_{l=1}^{j-1} b_l S_{j-l} + jb_j = 0.$$

For $1 \le l \le j-1$, either $l \not\equiv 0 \pmod{i}$ or $j - l \not\equiv 0 \pmod{i}$ because $j \not\equiv 0 \pmod{i}$. By (3.10) and the induction assumption, we have $b_l S_{j-l} = 0$ for $1 \le l \le j-1$. Hence $S_j + jb_j = 0$. From (3.10) again, $b_j = 0$. This proves the claim (3.11).

From now on, we may assume the set

$$E := \{0 \le k < N : S_k \neq 0, i \nmid k\} \tag{3.12}$$

is non-empty and let j be the least positive integer in this set. From the definition of j, we have, if there exists $l < j$ such that $S_l \neq 0$, then $i|l$.

Lemma 3.1. *Let i be defined in* (2.2) *and j be the least positive integer of the set E defined in* (3.12)*. Then we have*

(i) $j \mid N$,
(ii) $b_k = 0$, *for any* $k < j$ *and* $i \nmid k$,
(iii) $S_j = -jb_j$,
(iv) $S_{i+j} \neq 0$,
(v) $(i+j) \mid N$.

Proof. (i) Since $S_j \neq 0$, so $2^{t+1} \nmid j$ by Lemma 2.4 and hence by Lemma 2.3, $S_j = S_{(j,N)}$. So, if $(j,N) < j$ then by the definition of j, we have $i \mid (j,N)$. It follows that $i \mid j$ which contradicts the definition of j. Therefore, $(j,N) = j$ and hence $j \mid N$.

(ii) For any $k < j$ and $i \nmid k$, by the definition of j, we have $S_k = 0$. By Newton's identity,

$$S_k + b_1 S_{k-1} + \cdots + b_{i-1} S_{k-(i-1)} + b_i S_{k-i} + b_{i+1} S_{k-(i+1)} + \cdots + b_{k-1} S_1 + k b_k = 0.$$

Since $i \nmid k$, so either $i \nmid l$ or $i \nmid k-l$. That is either $b_l = 0$ or $S_{k-l} = 0$ by the definition of j and the induction assumption. So $S_k + k b_k = 0$ and hence $b_k = 0$.

(iii) By Newton's identity, we have

$$S_j + \sum_{l=1}^{j-1} b_l S_{j-l} + j b_j = 0$$

and by (ii), so

$$S_j + \sum_{1 \le l \le (j-1)/i} b_{il} S_{j-il} + j b_j = 0.$$

But $i \nmid j - il$ because $i \nmid j$, so $S_{j-il} = 0$. Thus $S_j + j b_j = 0$ and hence $S_j = -j b_j$.

(iv) We first note that $i + j < N$ from (i). By Newton's identity, we have

$$S_{i+j} + \sum_{l=1}^{i-1} b_l S_{i+j-l} + b_i S_j + \sum_{l=1}^{j-i-1} b_{i+l} S_{j-l} + b_j S_i + \sum_{l=1}^{i-1} b_{j+l} S_{i-l} + (i+j) b_{i+j} = 0.$$

Now we note that since $b_1 = \cdots = b_{i-1} = 0$, so

$$\sum_{l=1}^{i-1} b_l S_{i+j-l} = 0.$$

For $1 \le l \le j-i-1$, then $i + l < j$. If $i \nmid l$, then we have $b_{i+l} = 0$ by (ii). If $i|l$ then $i \nmid j - l$ and by the definition of j, we have $S_{j-l} = 0$. Thus we have

$$\sum_{l=1}^{j-i-1} b_{i+l} S_{j-l} = 0.$$

For $1 \le l \le i-1$, we have $i \nmid i - l$ and hence $S_{i-l} = 0$. We conclude that

$$S_{i+j} + b_j S_i + b_i S_j + (i+j) b_{i+j} = 0.$$

Since $S_i = 2i$ and $S_j = -jb_j$ by (2.6) and (iii), we get

$$S_{i+j} = -(i+j)(2b_j + b_{i+j}).$$

Suppose $S_{i+j} = 0$. Then $2b_j + b_{i+j} = 0$. Since $b_N = \pm 1$, so $i + j \neq N$ and hence $b_{i+j} \in \{-2, 0, +2\}$. Because $b_j \neq 0$, so $b_{i+j} \neq 0$ and hence

$$b_{i+j} = \pm 2 \equiv 2 \pmod 4.$$

Therefore,

$$\begin{aligned} 0 &\equiv b_{i+j} + 2b_j \pmod 4 \\ &\equiv 2 + 2b_j \pmod 4. \end{aligned}$$

It follows that $1 + b_j \equiv 0 \pmod 2$ and hence $b_j \equiv 1 \pmod 2$. This contradicts $b_j \in \{-2, 0, +2\}$.

(v) Since $S_{i+j} \neq 0$ and $i + j < N$, we have $2^{t+1} \nmid (i + j)$ by Lemma 2.4 and $S_{i+j} = S_{(N,i+j)}$ by Lemma 2.3. If $k = (N, i+j) < i+j$ then since $i+j < 2j$, every proper divisor of $i+j$ is less than j. In particular, $k < j$ but $S_k = S_{i+j} \neq 0$ by the definition of j. So $i|k$ and hence $i|j$. This contradiction shows that $k = (N, i+j) = i + j$ and $(i + j)|N$. □

Proof of Theorem 1.5. Let i and j be as above. Since $i, j \mid N$, we have $i = 2^{\alpha_1}p^{\beta_1}$ and $j = 2^{\alpha_2}p^{\beta_2}$ where $0 \leq \alpha_1, \alpha_2 \leq \alpha$ and $0 \leq \beta_1, \beta_2 \leq \beta$. Since $i \nmid j$, either "$\alpha_1 > \alpha_2$ and $\beta_2 > \beta_1$" or "$\alpha_2 > \alpha_1$ and $\beta_1 > \beta_2$". In both cases, one finds that $i + j$ has a factor of the form $2^r + p^s$ with r and s positive. By Lemma 3.1 (v), $(i+j) \mid N$, but $(2^r + p^s) \nmid 2^\alpha p^\beta$. This is a contradiction. Thus we conclude that the set E defined in (3.12) is empty and as we explained before, $P(x)$ can be written as

$$P(x) = (1 + x + \cdots + x^{i-1})P_1(x^i)$$

for some cyclotomic Littlewood polynomial $P_1(x)$ of degree $N/i - 1$. So one can complete the proof of Conjecture 1.3 for $N = 2^\alpha p^\beta$ by induction. This proves Theorem 1.5. □

Acknowledgement. The authors would like to thank the referee for his/her careful reading and suggestion of the manuscript.

References

[1] P. Borwein, *Computational Excursions in Analysis and Number Theory,* Springer-Verlag, 2002.

[2] P. Borwein and K.K. Choi, *On Cyclotomic Polynomials with ±1 Coefficients*, Experiment. Math. **8** (1999), no. 4, 399–407.

[3] P. Borwein and K.K. Choi, *Merit factors of character polynomials,* J. London Math. Soc. (2), **61** (2000), no. 3, 706–720.

[4] P. Borwein and K.K. Choi *Merit factors of polynomials formed by Jacobi symbols*, Canad. J. Math., **53** (2001), no. 1, 33–50.

[5] P. Borwein and K.K. Choi, *Explicit merit factor formulae for Fekete and Turyn Polynomials*, Trans. Amer. Math. Soc. , **354** (2002), 219–234.

[6] P. Borwein and K.K. Choi, *The average norm of polynomials of fixed height,* Trans. Amer. Math. Soc. **359** (2007) 923–936.

[7] P. Borwein, K.K. Choi and R. Ferguson, *Norm of Littlewood Cyclotomic Polynomials,* Mathematical Proceedings Cambridge Philosophical Society, **138** (2005) 315–326.

[8] P. Borwein and T. Erdelyi, Polynomials and Polynomial Inequalities, GTM 161, Springer-Verlag, New York, 1995.

[9] K.K. Choi and M. Mossinghoff, *Mahlers Measure and Lp Norms of Polynomials with Restricted Coefficients*, in preparation (2007).

[10] G. Hardy and E. Wright, An Introduction to the Theory of Numbers, 5th Ed., Oxford Science Publications, 1979.
[11] J.E. Littlewood, *Some Problems in Real and Complex Analysis,* Heath Mathematical Monographs, Lexington, Massachusetts, 1968.
[12] R. Thangadurai, *A note on the conjecture of Borwein and Choi*, Arch. Math. (Basel) **78** (2002), no. 5, 386–396.

Department of Mathematics, University of British Columbia, Vancouver, British Columbia V6T 1Z2, CANADA
E-mail address: akhtari@math.ubc.ca

Department of Mathematics, Simon Fraser University, Burnaby, British Columbia V5A 1S6, CANADA
E-mail address: kkchoi@cecm.sfu.ca