Spectra of Certain Types of Polynomials
and Tiling of Integers
with Translates of Finite Sets

Sergei Konyagin
Izabella Laba

Spectra of certain types of polynomials and tiling of integers with translates of finite sets

Sergei Konyagin and Izabella Laba

January 30, 2004

1 Introduction

Definition 1.1 Let \( A(x) \in \mathbb{Z}[x] \) be a polynomial. We say that \( \{\theta_1, \theta_2, \ldots, \theta_{N-1}\} \) is an \( N \)-spectrum for \( A(x) \) if the \( \theta_j \) are all distinct and

\[
A(\epsilon_{jk}) = 0 \quad \text{for all} \quad 0 \leq j, k \leq N - 1, \quad j \neq k,
\]

where

\[
\epsilon_{jk} = e^{2\pi i (\theta_j - \theta_k)}, \quad \theta_0 = 0.
\]

Definition 1.1 is motivated by a conjecture of Fuglede [2], which asserts that a measurable set \( E \subset \mathbb{R}^n \) tiles \( \mathbb{R}^n \) by translations if and only if the space \( L^2(E) \) has an orthogonal basis consisting of exponential functions \( \{e^{2\pi i \lambda \cdot x}\}_{\lambda \in \Lambda} \); the set \( \Lambda \) is called a spectrum for \( E \). For recent work on Fuglede’s conjecture see e.g. [4], [5], [6], [7], [8], [9], [11], [12], [13], [14], [15], [16], [18], [20], [21], [22]. In the special case when \( E \subset \mathbb{R} \) is a union of \( N \) intervals of length 1, Fuglede’s conjecture was proved in [8] (see also [18], [17], [15], [20]) to be equivalent to the following.

Conjecture 1.2 Let \( A(x) \) be a polynomial whose all coefficients are nonnegative integers. Then the following are equivalent:

(T) There is a finite set \( A \subset \{0, 1, 2, \ldots\} \) such that \( A(x) = \sum_{a \in A} x^a \). Moreover, the set \( A \) tiles \( \mathbb{Z} \) by translations, i.e., there is a set \( B \subset \mathbb{Z} \) (called the translation set) such that every integer \( n \) can be uniquely represented as \( n = a + b \) with \( a \in A \) and \( b \in B \);

(S) \( A(x) \) has an \( N \)-spectrum with \( N = A(1) \).

If (T) holds for some \( B \), we will write \( A \oplus B = \mathbb{Z} \). Throughout this paper we will always assume that \( 2 \leq \#A < \infty \).
We will also address the question of characterizing finite sets $A$ which tile $\mathbb{Z}$ by translations. This problem has been considered by several authors and is closely related to many questions concerning factorization of finite groups, in particular periodicity and replacement of factors; see e.g. [1], [3], [17], [18], [19], [23], [24], [25]. In particular, the following conditions were formulated in [1]. Let $\Phi_s(x)$ denote the $s$-th cyclotomic polynomial, defined inductively by
\[ x^n - 1 = \prod_{s \mid n} \Phi_s(x). \] (1.1)

We define $S_A$ to be the set of prime powers $p^a$ such that $\Phi_{p^a}(x)$ divides $A(x)$.

**Conjecture 1.3** A tiles $\mathbb{Z}$ by translations if and only if the following two conditions hold:

(T1) $A(1) = \prod_{s \in S_A} \Phi_s(1)$,

(T2) if $s_1, \ldots, s_k \in S_A$ are powers of different primes, then $\Phi_{s_1 \ldots s_k}(x)$ divides $A(x)$.

It is proved in [1] that (T1)-(T2) imply (T), (T) implies (T1), and that (T) implies (T2) under the additional assumption that $\#A$ has at most two distinct prime factors. It is not known whether (T) always implies (T2); a partial result in the three-prime case was obtained in [3].

Conjecture 1.3, if true, implies one part of Conjecture 1.2, since (T1)-(T2) imply (S) with the spectrum
\[ \left\{ \sum_{s \in S_A} \frac{k_s}{s} : 0 \leq k_s < p \text{ if } s = p^a, \text{ p prime} \right\} \setminus \{0\} \]
(see [15]). In particular, we have (T) $\Rightarrow$ (S) if $\#A$ has at most two distinct prime factors.

Conjectures 1.2 and 1.3 have been verified in several other special cases. They are both true under the assumption that the degree of $A(x)$ is less than $\frac{3N}{2} - 1$, where $N = \#A$ [15]. It also follows from the results of [14] that Conjecture 1.2 is true for polynomials of the form
\[ A(x) = \frac{x^k - 1}{x - 1} + x^m \frac{x^n - 1}{x - 1} = 1 + x + \ldots + x^{k-1} + x^m + x^{m+1} + \ldots + x^{m+n-1} \]
with $m \geq k$. It is also known [22] that if a set $A$ tiles the nonnegative integers by translations, then (S) holds (in fact the result of [22] applies to more general sets $E \subset [0, \infty)$). Finally, it is proved in [15] that if $A(x)$ has degree less than $\frac{3N}{2} - 1$, where $N = \#A$, then an N-spectrum must be rational.

The results of this paper are as follows.

**Theorem 1.4** Conjectures 1.2 and 1.3 are true if $A(x)$ is assumed to be irreducible. Furthermore, if $A(x)$ is irreducible, then (T), (S) hold if and only if $\#A = p$ is prime and $A(x) = 1 + x^{p^a-1} + x^{2p^a-1} + \ldots + x^{(p-1)p^a-1}$ for some $\alpha \in \mathbb{N}$. 

2
Our next two theorems concerns polynomials of the form

\[ A(x) = \prod_{i=1}^{N} A_i(x), \quad A_i(x) = 1 + x^{m_i} + \ldots + x^{m_i(n_i-1)} = \frac{x^{m_i n_i} - 1}{x^{m_i} - 1}. \]  

(1.2)

Note that each factor \( A_i \) is the characteristic polynomial of the set \( \{0, m_i, 2m_i, \ldots, (n_i - 1)m_i\} \), which tiles \( \mathbb{Z} \) with the translation set \( \{0, 1, \ldots, m_i - 1\} + m_i n_i \mathbb{Z} \). Furthermore, \( A_i(1) = n_i \) and each \( A_i \) has an \( n_i \)-spectrum \( \{k/n_i m_i : k = 1, 2, \ldots, n_i - 1\} \). It follows from Corollary 2.3 that \( A(x) \) cannot have an \( M \)-spectrum with \( M = n_1 \ldots n_N = A(1) \) unless all coefficients of \( A(x) \) are 0 or 1, i.e. \( A(x) \) is a characteristic polynomial of a set \( A \subseteq \mathbb{Z} \).

**Theorem 1.5** Conjectures 1.2 and 1.3 are true for polynomials of the form (1.2) with \( N = 2 \).

**Theorem 1.6** Conjecture 1.3 is true for polynomials of the form (1.2) for all \( N \geq 2 \).

## 2 Preliminaries

It is well known (see e.g. [19]) that all tilings of \( \mathbb{Z} \) by finite sets are periodic: if \( A \) is finite and \( A \oplus C = \mathbb{Z} \), then \( C = B \oplus M \mathbb{Z} \) for some finite set \( B \) such that \( \#A \cdot \#B = M \). Equivalently, \( A \oplus B \) is a complete residue system modulo \( M \), with \( M \) as above. We can rewrite it as

\[ A(x)B(x) = 1 + x + \ldots + x^{M-1} \pmod{x^M - 1}, \]  

(2.1)

where \( B(x) = \sum_{b \in B} x^b \). By (1.1), this is equivalent to

\[ A(1)B(1) = M \text{ and } \Phi_s(x) \mid A(x)B(x) \text{ for all } s \mid M, \ s \neq 1. \]  

(2.2)

The following lemma is due to A. Granville (unpublished).

**Lemma 2.1** If \( A \) tiles \( \mathbb{Z} \) by translations, then it admits a tiling whose period divides the number

\[ L = \text{lcm}\{s : \Phi_s(x) \mid A(x)\}. \]

**Proof.** Fix \( A \), and let \( A \oplus B = \mathbb{Z}_M \pmod{M} \). Replacing \( B \) by \( \{c \in \{0, 1, \ldots, M - 1\} : c = b \pmod{M} \text{ for some } b \in B\} \) if necessary, we may assume that \( B \subseteq \{0, \ldots, M - 1\} \). Let \( l = (L, M) \). If \( d \mid M \) but \( d \nmid L \) then

\[ \Phi_d(x) \mid \frac{x^M - 1}{x - 1} \mid A(x)B(x) \]
but $\Phi_d(x) \not| A(x)$, hence $\Phi_d(x) \mid B(x)$. Therefore

$$\frac{x^M - 1}{x^l - 1} = \prod_{d \mid M, d \not| l} \Phi_d(x) \mid B(x).$$

Let $P(x) = B(x)(x^i - 1)/(x^M - 1) = \sum_{j=0}^{i-1} p_j x^j$. Then

$$B(x) = \frac{x^M - 1}{x^l - 1} P(x) = \sum_{j=0}^{i-1} p_j (x^j + x^{j+l} + \ldots + x^{j+M-l}).$$

Thus the polynomial $P(x)$ has the form $P(x) = R_0(x)$, where $B_0 = \{b \in B : 0 \leq b \leq i - 1\}$.

Then $A(x)B_0(x) = \frac{x^M - 1}{x^l - 1} (\text{mod } (x^i - 1))$ and $A(x)B_0(x) = Z_l (\text{mod } l)$. ■

We will need the following well known property of cyclotomic polynomials:

$$\Phi_s(1) = \begin{cases} 
0 & \text{if } s = 1, \\
p & \text{if } s = p^e, \ p \text{ prime}, \\
1 & \text{otherwise}. 
\end{cases} \quad (2.3)$$

Finally, we will need the following lemma.

**Lemma 2.2** Suppose that $A(x) \in \mathbb{Z}[x]$ has nonnegative coefficients. Then $A(x)$ cannot have an $N$-spectrum for any $N$ greater than the number of non-zero coefficients of $A$.

**Proof.** The proof is a simple modification of an argument of [8]. Let $A(x) = \sum_{j=1}^{M} a_j x^n_j$, where $a_j > 0$ for all $j$. Let $\{\theta_j : j = 1, \ldots, N - 1\}$ be an $N$-spectrum for $A(x)$, $\theta_N = 0$, $\epsilon_j = e^{2\pi i \theta_j}$ and $\epsilon_{jk} = e^{2\pi i (\theta_j - \theta_k)}$. Then the condition $A(\epsilon_{jk}) = 0$ means that the vectors

$$u_j = (\epsilon_j^{a_{j1}}, \ldots, \epsilon_j^{a_{jM}})$$

are mutually orthogonal in $\mathbb{C}^M$ with respect to the inner product

$$(v, w) = \sum a_k v_k w_k, \ v = (v_1, \ldots, v_M), \ w = (w_1, \ldots, w_M).$$

Since there can be at most $M$ such vectors, it follows that $N \leq M$. ■

**Corollary 2.3** Assume that $A(x) \in \mathbb{Z}[x]$ has nonnegative coefficients, and that it satisfies either (T1)-(T2) or (S). Then all non-zero coefficients of $A(x)$ are 1.

**Proof.** If $A(x)$ satisfies (T1)-(T2), then it also satisfies (S) [15]. Thus it suffices to consider the case when (S) holds. But then the corollary is an immediate consequence of Lemma 2.2. ■
3 Proof of Theorem 1.4

Throughout this section we assume that \( A(x) \) is irreducible. Assume that \( A \) files \( \mathbb{Z} \) by translations. Then (T1) holds, and it follows from the irreducibility of \( A(x) \) and (2.3) that \( A(x) = \Phi_{p^n}(x) \) for some prime \( p \). Hence \( N = A(1) = p \) and the set \( \{jp^{-\alpha} : j = 1, 2, \ldots, p^\alpha - 1 \} \) is an \( N \)-spectrum for \( A \).

Suppose now that \( A(x) \) has an \( N \)-spectrum. Let \( \epsilon(u) = e^{2\pi i u} \),
\[
A(x) = \sum_{k=0}^{N-1} a_k x^k, \quad a_0 = M > a_1 > \ldots > a_{N-1} = 0,
\]
let \( \{\theta_1, \ldots, \theta_{N-1}\} \subset (0, 1) \) be a spectrum for \( A(x) \),
\[
\epsilon_j = \epsilon(\theta_j - \theta_k), \quad \theta_0 = 0,
\]
and let \( z_1, \ldots, z_M \) be the roots of the polynomial \( A(x) \). The matrix \((\epsilon(\theta_j a_j))_{i,j=0}^{N-1} \) is orthogonal. Therefore, for \( j \neq k \)
\[
\sum_{i=0}^{N-1} \epsilon(\theta_i (a_j - a_k)) = 0,
\]
or
\[
\sum_{i=1}^{N-1} \epsilon(\theta_i (a_j - a_k)) = -1. \tag{3.1}
\]

Denote
\[
S_j = \sum_{i=1}^{M} z_i^j.
\]

Let \( G \) be the Galois group of \( A(x) \). Then, by (3.1), for any \( \sigma \in G \)
\[
\sum_{i=1}^{N-1} \sigma(\epsilon(\theta_i))^{a_j - a_k} = -1.
\]

Averaging over \( \sigma \), we get
\[
S_{a_j - a_k} = -M/(N - 1). \tag{3.2}
\]

By Newton’s identities, if
\[
A(x) = \sum_{j=0}^{M} b_j x^j,
\]
then
\[
S_j + b_{M-1} S_{j-1} + \ldots + b_{M-j+1} S_1 + j b_{M-j} = 0. \tag{3.3}
\]

Taking consequently \( j = 1, \ldots, M - a_1 - 1 \), and using that all coefficients \( b_i \) in (3.3) are zeros, we get
\[
S_1 = \ldots = S_{M-a_1-1} = 0. \tag{3.4}
\]
Furthermore, for \( j = M - a_1 \) Newton’s identity gives
\[
S_{M-a_1} + (M - a_1) = 0. \tag{3.5}
\]
On the other hand, \( S_{M-a_1} = -M/(N - 1) \) by (3.2). Therefore,
\[
M - a_1 = M/(N - 1). \tag{3.6}
\]

We claim that
\[
a_{j-1} - a_j \geq M/(N - 1), \quad j = 1, \ldots, N - 1. \tag{3.7}
\]
Indeed, suppose the contrary. Then, by (3.4), \( S_{a_{j-1}-a_j} = 0 \), but this equality does not agree with (3.2). Hence,
\[
M = \sum_{j=1}^{N-1} (a_{j-1} - a_j) \geq \sum_{j=1}^{N-1} M/(N - 1) = M.
\]
Thus, the inequalities in (3.7) are actually equalities, and we have
\[
a_j = M - jM/(N - 1), \quad j = 1, \ldots, N - 1,
\]
and
\[
A(x) = \sum_{j=0}^{N-1} x^{jM/(N-1)} = \frac{x^{MN/(N-1)} - 1}{x^{M/(N-1)} - 1}.
\]
In particular, all roots of \( A(x) \) are roots of unity. Since \( A(x) \) is irreducible, \( A(x) = \Phi_s(x) \) for some \( s \in \mathbb{N} \); moreover, \( A(1) = N > 1 \) implies that \( N = p \) and \( s = p^a \) for some prime \( p \). Hence \( A(x) = (x^{p^a} - 1)/( (x^{p^a-1} - 1) \) and
\[
A = \{0, p^a-1, 2p^a-1, \ldots, (p-1)p^a-1\}.
\]
It is easy to see that \( A \) tiles \( \mathbb{Z} \) with the translation set \( B = \{0,1,\ldots,p^a-1\} + p^a \mathbb{Z} \).

4 Proof of Theorem 1.6

We will consider polynomials of the form
\[
A(x) = \prod_{i=1}^{N} A_i(x), \quad A_i(x) = 1 + x^m_i + \ldots + x^{m_i(n_i-1)} = \frac{x^{m_in_i} - 1}{x^{m_i} - 1}. \tag{4.1}
\]
It suffices to prove Theorem 1.6 under the assumption that
\[
(m_1, \ldots, m_N) = 1. \tag{4.2}
\]
Indeed, suppose that \( (m_1, \ldots, m_N) = d > 1 \), and let \( A' = A/d, m'_i = m_i/d \). Then \( A' \) has the form (4.1) and satisfies (4.2). Furthermore, \( A \) tiles \( \mathbb{Z} \) if and only \( A' \) tiles \( \mathbb{Z} \), and \( A \) satisfies (T1)-(T2) if and only if so does \( A' \) (see [1]).
Assume for now that \( m_i, n_j \) are chosen so that \( A(x) \) has 0,1 coefficients. (By Theorem 1.6, (4.3) below is a sufficient condition.)

Let \( m = (m_1, \ldots, m_N) \in \mathbb{R}^N \). Consider the projection \( \pi : \mathbb{R}^N \to \mathbb{R} \) given by
\[
\pi : (u_1, \ldots, u_N) = u \to \langle u, m \rangle = u_1 m_1 + \cdots + u_N m_N.
\]
Let
\[
\mathcal{A} = \{(j_1, \ldots, j_N) : j_k = 0, 1, \ldots, n_k - 1\}
\]
so that \( \pi(\mathcal{A}) = A \), and
\[
W = \{(w_1, \ldots, w_N) : w_i \in \mathbb{Z}, \langle w, m \rangle = 0\}.
\]
If \( A \) tiles \( \mathbb{Z} \) with the translation set \( B \), we will write
\[
B = \{(u_1, \ldots, u_N) : \langle u, m \rangle \in B\} = \pi^{-1}(B).
\]
Finally, we will denote \( d_{ij} = (m_i, m_j) \). We will sometimes identify \( \mathcal{A} \) with the rectangular box \( \{x \in \mathbb{R}^N : 0 \leq x_j < n_j\} \).

**Lemma 4.1** Assume that \( A \oplus B = \mathbb{Z} \), then:

(i) \( A \oplus B \) is a tiling of \( \mathbb{Z}^N \);

(ii) \( B \) is invariant under all translations by vectors in \( W \).

**Proof.** Let \( w \in \mathbb{Z}^N \), then \( \pi(w) = a + b \) for unique \( a \in A, b \in B \). Let \( u = \pi^{-1}(a) \); we are assuming that \( \pi \) is one-to-one on \( \mathcal{A} \), hence \( u \) is uniquely determined. Let also \( v = w - u \). Then \( \pi(v) = \pi(w) - \pi(u) = b \), hence \( v \in B \). This shows that each \( w \) can be represented as \( u + v \) with \( u \in \mathcal{A}, v \in B \). Furthermore, for any such representation we must have \( \pi(u) = a \) and \( \pi(v) = b \), so that the above argument also shows uniqueness. \( \square \)

**Remark** We also have the following converse of Lemma 4.1. Let a tiling \( A \oplus B = \mathbb{Z}^N \) be given, where \( \mathcal{A} \) and \( B \) are as above. We claim that if (ii) holds, then \( A \oplus B = \mathbb{Z} \), where \( A = \pi(\mathcal{A}) \) and \( B = \pi(B) \). Indeed, by (4.2) \( \pi \) is onto. Let \( x \in \mathbb{Z} \) and pick a vector in \( \pi^{-1}(x) \); this vector can be written as \( u + v \), where \( u \in \mathcal{A} \) and \( v \in B \). Therefore \( x = a + b \) with \( a = \pi(u) \in A \) and \( b = \pi(v) \in B \). It remains to verify that this representation is unique. Indeed, suppose that \( x = \pi(w) = \pi(w') \), then \( \pi(w - w') = 0 \) so that \( w - w' \in W \). By (ii), the tiling \( \mathcal{A} \oplus B \) is invariant under the translation by \( w - w' \). Hence if we write \( w = u + v, w' = u' + v' \) with \( u, u' \in \mathcal{A}, v, v' \in B \), it follows that \( u = u' \) and consequently \( a = \pi(u) = \pi(u') \) is uniquely determined. This also determines \( b = x - a \).
Lemma 4.2 Let $w_{ij}$ be the vector whose $i$-th coordinate is $m_j / d_{ij}$, $j$-th coordinate is $-m_i / d_{ij}$, and all other coordinates are 0. Then

$$ W = \{ \sum_{i,j} k_{ij} w_{ij} : k_{ij} \in \mathbb{Z} \}. $$

Proof. Denote the set on the right by $W'$. Since $w_{ij}$ have integer coordinates and $\langle w_{ij}, m \rangle = 0$, it is clear that $W' \subset W$. We will now prove the converse using induction in $N$. The inductive step will not necessarily preserve the property (4.2). However, if the lemma is proved for some $N$ under the assumption (4.2), it also holds for the same $N$ without this assumption. Indeed, suppose that $(m_1, \ldots, m_N) = d > 1$, then $d$ divides each $d_{ij}$, so that we may replace each $m_j$ by $m'_j = m_j / d$ and apply the version of the lemma in which (4.2) is assumed.

The case $N = 1$ is trivial since $\langle w, m \rangle = 0$ in dimension 1 only if $w = 0$. Suppose that the lemma has been proved for $N - 1$. We will show that any $w \in W$ can be written as $w = w' + w''$, where $w' \in W'$ and $w'' \in W$, $w'' = 0$; then the claim will follow by induction. It suffices to prove that

$$ w_1 = \sum_{j=2}^{N} k_j \frac{m_j}{d_{1j}}, $$

for some choice of integers $k_j$; in other words, that $(\frac{m_2}{d_{21}}, \ldots, \frac{m_N}{d_{N1}})$ divides $w_1$. Since $\langle w, m \rangle = 0$, we have

$$ m_1 w_1 = -m_2 w_2 - \ldots - m_N w_N. $$

Hence $(m_2, \ldots, m_N)$ divides $m_1 w_1$. By (4.2), it must in fact divide $w_1$. It only remains to observe that $(\frac{m_2}{d_{21}}, \ldots, \frac{m_N}{d_{N1}})$ divides $(m_2, \ldots, m_N)$. \[\blacksquare\]

Theorem 4.3 Let $A$ be as in (4.1). Then the following are equivalent:

(i) $A$ tiles $\mathbb{Z}$ by translations;

(ii) $A$ satisfies (T1)–(T2);

(iii) there is a labelling of the factors $A_i$ for which the following holds:

$$ m_1 | (\frac{m_2}{d_{21}}, \ldots, \frac{m_N}{d_{N1}}), $$

$$ n_2 | (\frac{m_3}{d_{32}}, \ldots, \frac{m_N}{d_{N2}}), $$

$$ \ldots, $$

$$ n_{N-1} | \frac{m_N}{d_{N-1,N}}. $$

(4.3)

Recall that we are assuming (4.2) throughout this section, including the proof that follows; however, it is easy to see that the theorem remains true without this assumption (see the remark after (4.2)).
Proof of Theorem 4.3. We will prove that (i) $\Rightarrow$ (iii) $\Rightarrow$ (ii); the implication (ii) $\Rightarrow$ (i) is proved (for more general $A$) in [1].

(i) implies (iii): We will say that a set $V \subset \mathbf{R}^N$ has Keller’s property if for each $v \in V$, $v \neq 0$, we have $v_i \in \mathbf{Z} \setminus \{0\}$ for at least one $i$. Let $L$ be the linear transformation on $\mathbf{R}^N$ defined by

$$L(u_1, \ldots, u_N) = \left( \frac{u_1}{n_1}, \ldots, \frac{u_N}{n_N} \right).$$

If we identify $A$ with the rectangular box $\{x \in \mathbf{R}^N : 0 \leq x_j < n_j\}$, then $L(A)$ is the unit cube $Q$ in $\mathbf{R}^N$, and by Lemma 4.1(i) $Q \oplus L(A)$ is a tiling of $\mathbf{R}^N$. We now use the following theorem of Keller on cube tilings [10].

Theorem 4.4 [10] If $Q \oplus V$ is a tiling of $\mathbf{R}^N$, then the set $V - V := \{v - v' : v, v' \in V\}$ has Keller’s property.

It follows that $L(A) - L(B)$ has Keller’s property; in particular, since $W \subset B - B$, $L(W)$ has Keller’s property.

We first claim that Keller’s property for $W$ implies the first equation in (4.3) for some labelling of $A_i$. Indeed, suppose that the first equation in (4.3) fails for all such labellings. Then for each $i \in \{1, \ldots, N\}$ there is a $\sigma(i) \neq i$ such that $n_i \not\mid \frac{m_{\sigma(i)}}{d_{\sigma(i),i}}$. We may find a cycle $i_1, \ldots, i_r$ such that $i_{j+1} = \sigma(i_j)$, with $i_{r+1} = i_1$. We thus have

$$n_{i_j} / \frac{m_{i_{j+1}}}{d_{i_{j+1}, i_{j+1}}},$$

for $j = 1, \ldots, r$.

Define $w_{i,j}$ as in Lemma 4.2. If there is a $j$ such that

$$n_{i_{j+1}} / \frac{m_{i_{j}}}{d_{i_{j+1}, i_{j+1}}},$$

then by (4.4), (4.5) Keller’s property fails for $w_{i_{j+1}}$. If on the other hand (4.5) fails for all $j$, then this together with (4.4) implies that Keller’s property fails for $\sum_{j=1}^r w_{i_{j+1}}$. This completes the proof of the claim.

The remaining equations in (4.3) can now be obtained by induction in $N$. Indeed, consider the set

$$W_1 = \{(w_2, \ldots, w_N) : (0, w_2, \ldots, w_N) \in W\} \subset \mathbf{R}^{N-1}.$$

This set (as a subset of $\mathbf{R}^{N-1}$) has Keller’s property, hence the previous argument with $W$ replaced by $W_1$ implies the second equation in (4.3). Similarly we obtain the rest of (4.3).

(iii) implies (ii): By the definition of $A_i(x)$,

$$\Phi_i(x) | A_i(x) \text{ if and only if } s | m_i n_i, \ s / m_i.$$  

(4.6)
We first prove (T1). By the definition of $A_i(x)$, all its irreducible factors are distinct cyclotomic polynomials, so that by (2.3) (T1) holds for each $A_i(x)$. It therefore suffices to prove that if (4.3) holds, then any prime power cyclotomic polynomial can divide at most one $A_i(x)$.

Let $p$ be a prime such that $\Phi_{p^\alpha}(x)$ divides $A_i(x)$ for some $\alpha, i$; it suffices to prove that $\Phi_{p^\alpha}(x)$ cannot divide $A_j(x)$ for any $j > i$. Let $p^{\beta_k} | n_k$ and $p^{\gamma_k} | m_k$ for $k = 1, \ldots, N$, then
\[
\Phi_{p^\alpha}(x) | A_k(x) \text{ if and only if } \beta_k < \alpha \leq \beta_k + \gamma_k. \tag{4.7}
\]

In particular, it follows that $\gamma_i \neq 0$.

Let $j > i$. By (4.3) we have $n_i = n_i(m_i, m_j) | m_j$. Thus $\gamma_i + \min(\beta_i, \beta_j) \leq \beta_j$. Note that we cannot have $\min(\beta_i, \beta_j) = \beta_j$, since then $\gamma_i$ would be 0. Hence $\min(\beta_i, \beta_j) = \beta_i$ and $\alpha \leq \beta_i + \gamma_i \leq \beta_j$. This and (4.7) imply that $\Phi_{p^\alpha}(x) / A_j(x)$, as claimed.

We note for future reference that we have also proved the following:
\[
\text{if } \Phi_{p^\alpha}(x) | A_i(x) \text{ for some } \alpha, \text{ then } \beta_i + \gamma_i \leq \beta_j \text{ for all } j > i. \tag{4.8}
\]

It remains to prove (T2). We must prove that if $s > 1$ is an integer such that $\Phi_{p^\alpha}(x) | A(x)$ for every $p^\alpha | s$, then $\Phi_{s}(x) | A(x)$. We will in fact show that $\Phi_{s}(x) | A_j(x)$, where
\[
j = \max\{k : \Phi_{p^\alpha}(x) | A_i(x) \text{ for some } p^\alpha | s\}.
\]

By (4.6), it suffices to prove that $s | m_j n_j$ and $s / m_j$.

For every $p^\alpha | s$ we have $\Phi_{p^\alpha}(x) | A_k(x)$ for some $k \leq j$. Therefore $p^\alpha | m_j n_j$; this follows from (4.6) if $k = j$, and from (4.8) if $k < j$. Hence $s | m_j n_j$. On the other hand, by the definition of $j$ there is at least one prime power $p^\alpha | s$ such that $\Phi_{p^\alpha}(x) | A_j(x)$. By (4.6) we have $p^\alpha / m_j$, so that $s / m_j$. 

## 5 Proof of Theorem 1.5

In this section we will assume that $A(x)$ is as in (1.2). Denote also $d = (m_1, m_2)$. We will prove that, under the above hypotheses, each of (T), (S), (T1)-(T2) is equivalent to the statement that one of the following holds:
\[
m_1 \mid \frac{m_2}{d}, \tag{5.1}
\]
\[
n_2 \mid \frac{m_1}{d}. \tag{5.2}
\]

We record for future reference that $\Phi_{s}(x) | A(x)$ if and only if
\[
s | m_i n_i, \quad s / m_i \text{ for at least one of } i = 1, 2. \tag{5.3}
\]
By Theorem 4.3 and the remark following it, the statement that one of (5.1), (5.2) holds is equivalent to (T) and to (T1)-(T2). In light of [15], Theorem 1.5, this also implies (S). It remains to show that (S) implies one of (5.1), (5.2).

Suppose that \( A(x) \) has an \( N \)-spectrum \( \{\theta_j : j = 1, \ldots, N - 1\} \). Let \( \theta_N = 0, \epsilon_j = e^{2\pi i \theta_j} (j = 1, \ldots, N - 1), \epsilon_N = 1 \). Then the numbers
\[
\epsilon_j / \epsilon_k = e^{2\pi i (\theta_j - \theta_k)}
\]
are roots of \( A(x) \) for all \( j \neq k, j \leq N, k \leq N \).

We will first prove that one of the following must hold:
\[
\forall j \ m_1 n_1 \theta_j \in \mathbb{Z}, \quad (5.4)
\]
\[
\forall j \ m_2 n_2 \theta_j \in \mathbb{Z}. \quad (5.5)
\]
Indeed, suppose that (5.4) and (5.5) fail. Then there exist \( j \) and \( k \) such that
\[
m_1 n_1 \theta_j \not\in \mathbb{Z}, \quad (5.6)
\]
\[
m_2 n_2 \theta_k \not\in \mathbb{Z}. \quad (5.7)
\]
Since \( \epsilon_j \) is a root of \( A(x) \), we get from (5.6) that
\[
m_2 n_2 \theta_j \in \mathbb{Z}. \quad (5.8)
\]
Similarly,
\[
m_1 n_1 \theta_k \in \mathbb{Z}. \quad (5.9)
\]
The conditions (5.6)-(5.9) imply
\[
m_1 n_1 (\theta_j - \theta_k) \not\in \mathbb{Z},
\]
\[
m_2 n_2 (\theta_j - \theta_k) \not\in \mathbb{Z}.
\]
Thus, \( \epsilon_j / \epsilon_k \) is not a root of \( A(x) \). This contradiction shows that our supposition cannot occur. Without loss of generality, we will assume that (5.4) holds.

For \( l = 0, \ldots, n_1 - 1 \) denote
\[
J_l = \{ j : m_1 n_1 \theta_j \equiv l \ (\text{mod} \ n_1) \}.
\]
For \( j, k \in J_l, j \neq k \), the number \( \epsilon_j / \epsilon_k \) is not a root of \( A_1(x) \). Hence, it is a root of \( A_2(x) \). This means that, for \( j, k \in J_l, j \neq k \), the numbers \( m_2 n_2 (\theta_j - \theta_k) \) are integers not divisible by \( n_2 \). This yields \( |J_l| \leq n_2 \). On the other hand, the equality
\[
N = n_1 n_2 = \sum_{l=0}^{n_1-1} |J_l|
\]
demonstrates that actually \( |J_l| = n_2 \) for all \( l \), and, moreover, for a fixed \( k \in J_l \), the numbers \( m_2 n_2 (\theta_j - \theta_k) \) run over the complete residue system modulo \( n_2 \).
In particular, there exists \( j \in J_0 \) such that
\[
m_2 n_2 \theta_j \equiv 1 \pmod{n_2}.
\]
Therefore,
\[
\frac{m_1 m_2 n_2 \theta_j s}{s} \equiv \frac{m_1}{s} \pmod{n_2}.
\] (5.10)
On the other hand, the condition \( j \in J_0 \) means \( m_1 \theta_j \in \mathbb{Z} \). Therefore,
\[
m_1 n_2 \theta_j \equiv 0 \pmod{n_2}
\]
and
\[
\frac{m_1 m_2 n_2 \theta_j s}{s} \equiv 0 \pmod{n_2}.
\] (5.11)
Comparing (5.10) and (5.11), we obtain (5.2).

Acknowledgement. The first author was supported by Grants 02-01-00248 and 00-15-96109 from the Russian Foundation for Basic Research. The second author was supported by the NSERC Grant 22R80520.

References


12


**Department of Mechanics and Mathematics, Moscow State University, Moscow 11992, Russia**

E-mail address: kcon@mech.math.msu.su

**Department of Mathematics, University of British Columbia, Vancouver, B.C. V6T 1Z2, Canada**

E-mail address: ilaba@math.ubc.ca