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

Sergei Konyagin and Izabella Łaba

September 16, 2002

1 Introduction

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

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

where

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

Definition 1.1 is motivated by a conjecture of Fuglede [2], which asserts that a measurable set $E \subset \mathbf{R}^n$ tiles $\mathbf{R}^n$ 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 Λ 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 $E \subset \mathbf{R}$ 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 $\mathbf{Z}$ by translations, i.e., there is a set $B \subset \mathbf{Z}$ (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 $A \oplus B = \mathbf{Z}$. 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 $\mathbf{Z}$ 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

$$x^n - 1 = \prod_{s\,|\,n} \Phi_s(x). \tag{1.1}$$

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

Conjecture 1.3 *A tiles $\mathbf{Z}$ 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

$$\Big\{ \sum_{s\in S_A} \frac{k_s}{s} :\ 0 \le k_s < p \text{ if } s = p^\alpha,\ p \text{ prime} \Big\} \setminus \{0\}$$

(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 $m \ge k$. 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 $\frac{5N}{2} - 1$, 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 $A(x) = 1 + x^{p^{\alpha-1}} + x^{2p^{\alpha-1}} + \ldots + x^{(p-1)p^{\alpha-1}}$ for some $\alpha \in \mathbf{N}$.*

Our next two theorems concerns polynomials of the form

$$A(x) = \prod_{i=1}^{N} A_i(x),\ \ A_i(x) = 1 + x^{m_i} + \ldots + x^{m_i(n_i-1)} = \frac{x^{m_i n_i} - 1}{x^{m_i} - 1}. \tag{1.2}$$

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 $\mathbf{Z}$ with the translation set $\{0, 1, \ldots, m_i - 1\} + m_i n_i \mathbf{Z}$. 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 $A \subset \mathbf{Z}$.

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 $\mathbf{Z}$ by finite sets are periodic: if A is finite and $A \oplus C = \mathbf{Z}$, then $C = B \oplus M\mathbf{Z}$ 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

$$A(x)B(x) = 1 + x + \ldots + x^{M-1} \ (\mathrm{mod}\,(x^M - 1)), \tag{2.1}$$

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

$$A(1)B(1) = M \text{ and } \Phi_s(x) \,|\, A(x)B(x) \text{ for all } s \,|\, M,\ s \neq 1. \tag{2.2}$$

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

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

$$L = lcm\{s :\ \Phi_s(x) \,|\, A(x)\}.$$

Proof. Fix A, and let $A \oplus B = \mathbf{Z}_M \ (\mathrm{mod}\, M)$. Replacing B by $\{c \in \{0, 1, \ldots, M-1\} : c = b \ (\mathrm{mod}\, M)$ for some $b \in B\}$ if necessary, we may assume that $B \subset \{0, \ldots, M-1\}$. Let $l = (L, M)$. If $d \,|\, M$ but $d \not| L$ then

$$\Phi_d(x) \,\Big|\, \frac{x^M - 1}{x - 1} \,\Big|\, A(x)B(x)$$

but $\Phi_d(x) \nmid A(x)$, hence $\Phi_d(x) \mid B(x)$. Therefore

$$\frac{x^M - 1}{x^l - 1} = \prod_{d \mid M, d \nmid l} \Phi_d(x) \Big| B(x).$$

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

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

Thus the polynomial $P(x)$ has the form $P(x) = B_0(x)$, where $B_0 = \{b \in B: \ 0 \le b \le l-1\}$. Then $A(x)B_0(x) = \frac{x^l-1}{x-1} \pmod{(x^l - 1)}$ and $A(x)B_0(x) = \mathbf{Z}_l \pmod{l}$. ∎

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

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

Finally, we will need the following lemma.

Lemma 2.2 *Suppose that $A(x) \in \mathbf{Z}[x]$ 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 $A(x) = \sum_{j=1}^{M} a_j x^{\alpha_j}$, 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

$$\mathbf{u}_j = (\epsilon_j^{\alpha_1}, \ldots, \epsilon_j^{\alpha_M})$$

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

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

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

Corollary 2.3 *Assume that $A(x) \in \mathbf{Z}[x]$ 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 tiles $\mathbf{Z}$ by translations. Then (T1) holds, and it follows from the irreducibility of $A(x)$ and (2.3) that $A(x) = \Phi_{p^\alpha}(x)$ 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 $e(u) = e^{2\pi i u}$,

$$A(x) = \sum_{k=0}^{N-1} x^{a_k}, \ a_0 = M > a_1 > \ldots > a_{N-1} = 0,$$

let $\{\theta_1, \ldots, \theta_{N-1}\} \subset (0,1)$ be a spectrum for $A(x)$,

$$\epsilon_{jk} = e(\theta_j - \theta_k), \ \theta_0 = 0,$$

and let $z_1, \ldots, z_M$ be the roots of the polynomial $A(x)$. The matrix $(e(\theta_i a_j))_{i,j=0}^{N-1}$ is orthogonal. Therefore, for $j \neq k$

$$\sum_{i=0}^{N-1} e(\theta_i(a_j - a_k)) = 0,$$

or

$$\sum_{i=1}^{N-1} e(\theta_i(a_j - a_k)) = -1. \tag{3.1}$$

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 $\sigma \in G$

$$\sum_{i=1}^{N-1} \sigma(e(\theta_i))^{a_j - a_k} = -1.$$

Averaging over σ, 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

$$a_{j-1} - a_j \geq M/(N-1),\ j = 1, \ldots, N-1. \tag{3.7}$$

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

$$a_j = M - jM/(N-1),\ j = 1, \ldots, N-1,$$

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 $s \in \mathbf{N}$; moreover, $A(1) = N > 1$ implies that $N = p$ and $s = p^\alpha$ for some prime p. Hence $A(x) = (x^{p^\alpha} - 1)/((x^{p^{\alpha-1}} - 1)$ and

$$A = \{0, p^{\alpha-1}, 2p^{\alpha-1}, \ldots, (p-1)p^{\alpha-1}\}.$$

It is easy to see that A tiles $\mathbf{Z}$ with the translation set $B = \{0, 1, \ldots, p^{\alpha-1} - 1\} + p^\alpha \mathbf{Z}$.

4 Proof of Theorem 1.6

We will consider polynomials of the form

$$A(x) = \prod_{i=1}^{N} A_i(x),\ A_i(x) = 1 + x^{m_i} + \ldots + x^{m_i(n_i-1)} = \frac{x^{m_i n_i} - 1}{x^{m_i} - 1}. \tag{4.1}$$

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 $\mathbf{Z}$ if and only A' tiles $\mathbf{Z}$, and A satisfies (T1)-(T2) if and only if so does A' (see [1]).

Assume for now that m_i, n_i are chosen so that $A(x)$ has $0,1$ coefficients. (By Theorem 1.6, (4.3) below is a sufficient condition.)

Let $m = (m_1, \dots, m_N) \in \mathbf{R}^N$. Consider the projection $\pi : \mathbf{R}^N \to \mathbf{R}$ given by

$$\pi : \ (u_1, \dots, u_N) = u \to \langle u, m \rangle = u_1 m_1 + \dots + u_N m_N.$$

Let

$$\mathcal{A} = \{(j_1, \dots, j_N) : \ j_k = 0, 1, \dots, n_k - 1\}$$

so that $\pi(\mathcal{A}) = A$, and

$$W = \{(w_1, \dots, w_N) : \ w_i \in \mathbf{Z}, \ \langle w, m \rangle = 0\}.$$

If A tiles $\mathbf{Z}$ with the translation set B, we will write

$$\mathcal{B} = \{(u_1, \dots, u_N) : \ \langle u, m \rangle \in B\} = \pi^{-1}(B).$$

Finally, we will denote $d_{ij} = (m_i, m_j)$. We will sometimes identify $\mathcal{A}$ with the rectangular box $\{x \in \mathbf{R}^N : \ 0 \le x_j < n_j\}$.

Lemma 4.1 *Assume that $A \oplus B = \mathbf{Z}$, then:*

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

(ii) $\mathcal{B}$ is invariant under all translations by vectors in W.

Proof. Let $w \in \mathbf{Z}^N$, then $\pi(w) = a + b$ for unique $a \in A, b \in B$. Let $u = \pi^{-1}(a)$; we are assuming that π 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 $v \in \mathcal{B}$. This shows that each w can be represented as $u + v$ with $u \in \mathcal{A}, v \in \mathcal{B}$. Furthermore, for any such representation we must have $\pi(u) = a$ and $\pi(v) = b$, so that the above argument also shows uniqueness. ∎

Remark We also have the following converse of Lemma 4.1. Let a tiling $\mathcal{A} \oplus \mathcal{B} = \mathbf{Z}^N$ be given, where $\mathcal{A}$ and $\mathcal{B}$ are as above. We claim that if (ii) holds, then $A \oplus B = \mathbf{Z}$, where $A = \pi(\mathcal{A})$ and $B = \pi(\mathcal{B})$. Indeed, by (4.2) π is onto. Let $x \in \mathbf{Z}$ and pick a vector in $\pi^{-1}(x)$; this vector can be written as $u + v$, where $u \in \mathcal{A}$ and $v \in \mathcal{B}$. 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 $\mathcal{A} \oplus \mathcal{B}$ is invariant under the translation by $w - w'$. Hence if we write $w = u + v$, $w' = u' + v'$ with $u, u' \in \mathcal{A}$, $v, v' \in \mathcal{B}$, 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*

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

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 $(m_1, \dots, m_N) = d > 1$, 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 $w'' \in W$, $w''_1 = 0$; 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 $(\frac{m_2}{d_{12}}, \dots, \frac{m_N}{d_{1N}})$ divides w_1. Since $\langle w, m\rangle = 0$, we have

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

Hence $(m_2, \dots, m_N)$ divides $m_1 w_1$. By (4.2), it must in fact divide w_1. It only remains to observe that $(\frac{m_2}{d_{12}}, \dots, \frac{m_N}{d_{1N}})$ divides $(m_2, \dots, m_N)$. ∎

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

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

(ii) A satisfies (T1)–(T2);

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

$$\begin{aligned} &n_1 | (\tfrac{m_2}{d_{12}}, \dots, \tfrac{m_N}{d_{1N}}), \\ &n_2 | (\tfrac{m_3}{d_{23}}, \dots, \tfrac{m_N}{d_{2N}}), \\ &\dots, \\ &n_{N-1} | \tfrac{m_N}{d_{N-1,N}}. \end{aligned} \tag{4.3}$$

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

$$L(u_1, \dots, u_N) = (\frac{u_1}{n_1}, \dots, \frac{u_N}{n_N}).$$

If we identify $\mathcal{A}$ with the rectangular box $\{x \in \mathbf{R}^N : \ 0 \leq x_j < n_j\}$, then $L(\mathcal{A})$ is the unit cube Q in $\mathbf{R}^N$, and by Lemma 4.1(i) $Q \oplus L(\mathcal{B})$ 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 $L(\mathcal{B}) - L(\mathcal{B})$ has Keller's property; in particular, since $W \subset \mathcal{B} - \mathcal{B}$, $L(W)$ 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 $i \in \{1, \dots, N\}$ there is a $\sigma(i) \neq i$ such that $n_i \not| \frac{m_i}{d_{i\sigma(i)}}$. We may find a cycle $i_1, \dots, i_r$ such that $i_{j+1} = \sigma(i_j)$, with $i_{r+1} = i_1$. We thus have

$$n_{i_j} \not| \frac{m_{i_{j+1}}}{d_{i_j, i_{j+1}}} \tag{4.4}$$

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

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

$$n_{i_{j+1}} \not| \frac{m_{i_j}}{d_{i_j, i_{j+1}}}, \tag{4.5}$$

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

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

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 $A_i(x)$,

$$\Phi_s(x) \,|\, A_i(x) \text{ if and only if } s \,|\, m_i n_i, \ s \not| m_i. \tag{4.6}$$

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 α, i; it suffices to prove that $\Phi_{p^\alpha}(x)$ cannot divide $A_j(x)$ for any $j > i$. Let $p^{\beta_k} || m_k$ and $p^{\gamma_k} || n_k$ for $k = 1, \dots, N$, 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 $n_i \,|\, \frac{m_j}{d_{ij}}$, i.e. $n_i(m_i, m_j) \,|\, m_j$. 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 γ_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 $\Phi_{p^\alpha}(x) \not| A_j(x)$, 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

$$j = \max\{k : \ \Phi_{p^\alpha}(x) \,|\, A_k(x) \text{ for some } p^\alpha || s\}.$$

By (4.6), it suffices to prove that $s \,|\, m_j n_j$ and $s \not| m_j$.

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 $p^\alpha \not| m_j$, so that $s \not| m_j$. ■

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:

$$n_1 \,|\, \frac{m_2}{d}, \tag{5.1}$$

$$n_2 \,|\, \frac{m_1}{d}. \tag{5.2}$$

We record for future reference that $\Phi_s(x) \,|\, A(x)$ if and only if

$$s \,|\, m_i n_i, \ \ s \not| m_i \text{ for at least one of } i = 1, 2. \tag{5.3}$$

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:

$$\forall j \ m_1 n_1 \theta_j \in \mathbf{Z}, \tag{5.4}$$

$$\forall j \ m_2 n_2 \theta_j \in \mathbf{Z}. \tag{5.5}$$

Indeed, suppose that (5.4) and (5.5) fail. Then there exist j and k such that

$$m_1 n_1 \theta_j \notin \mathbf{Z}, \tag{5.6}$$

$$m_2 n_2 \theta_k \notin \mathbf{Z}. \tag{5.7}$$

Since ϵ_j is a root of $A(x)$, we get from (5.6) that

$$m_2 n_2 \theta_j \in \mathbf{Z}. \tag{5.8}$$

Similarly,

$$m_1 n_1 \theta_k \in \mathbf{Z}. \tag{5.9}$$

The conditions (5.6)–(5.9) imply

$$m_1 n_1 (\theta_j - \theta_k) \notin \mathbf{Z},$$

$$m_2 n_2 (\theta_j - \theta_k) \notin \mathbf{Z}.$$

Thus, ϵ_j/ϵ_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

$$J_l = \{j : m_1 n_1 \theta_j \equiv l \ (\mathrm{mod} n_1)\}.$$

For $j, k \in J_l$, $j \neq k$, the number ϵ_j/ϵ_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

$$m_2 n_2 \theta_j \equiv 1 \ (\mathrm{mod} n_2).$$

Therefore,

$$\frac{m_1 m_2 n_2}{s} \theta_j \equiv \frac{m_1}{s} \ (\mathrm{mod} n_2). \tag{5.10}$$

On the other hand, the condition $j \in J_0$ means $m_1 \theta_j \in \mathbf{Z}$. Therefore,

$$m_1 n_2 \theta_j \equiv 0 \ (\mathrm{mod} n_2)$$

and

$$\frac{m_1 m_2 n_2}{s} \theta_j \equiv 0 \ (\mathrm{mod} n_2). \tag{5.11}$$

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

[1] E. Coven, A. Meyerowitz: *Tiling the integers with translates of one finite set*, J. Algebra 212 (1999), 161–174.

[2] B.Fuglede: *Commuting self-adjoint partial differential operators and a group-theoretic problem*, J. Funct. Anal. 16 (1974), 101–121.

[3] A. Granville, I. Łaba, Y. Wang: *A characterization of finite sets that tile the integers*, preprint, 2001.

[4] A. Iosevich, N. H. Katz, S. Pedersen: *Fourier bases and a distance problem of Erdös*, Math. Res. Lett. 6 (1999), 251–255.

[5] A. Iosevich, N. H. Katz, T. Tao: *Convex bodies with a point of curvature do not have Fourier bases*, Amer. J. Math. 123 (2001), 115–120.

[6] A. Iosevich, N. H. Katz, T. Tao: *Fuglede conjecture holds for convex planar domains*, preprint, 2001.

[7] A. Iosevich, S. Pedersen: *Spectral and tiling properties of the unit cube*, Internat. Math. Res. Notices 16 (1998), 819–828.

[8] P. Jorgensen, S. Pedersen: *Fractal Geometry and Stochastics*, in: Progress in Probability, vol. 17, Birkhäuser, Basel, 1995, 191–219.

[9] P. Jorgensen, S. Pedersen: *Spectral pairs in Cartesian coordinates*, J. Fourier Anal. Appl. 5 (1999), 285–302.

[10] O. H. Keller: *Über die lückenlose Einfüllung des Raumes mit Würfeln*, J. Reine Angew. Math. 163 (1930), 231–248.

[11] M. Kolountzakis: *Non-symmetric convex domains have no basis of exponentials*, Illinois J. Math. 44 (2000), 542–550.

[12] M. Kolountzakis: *Packing, tiling, orthogonality, and completeness*, Bull. London Math. Soc. 32 (2000), 589–599.

[13] M. Kolountzakis, M. Papadimitrakis: *A class of non-convex polytopes that admit no orthogonal basis of exponentials*, preprint, 2001.

[14] I. Łaba: *Fuglede's conjecture for a union of two intervals*, Proc. AMS 129 (2001), 2965–2972.

[15] I. Łaba: *The spectral set conjecture and multiplicative properties of roots of polynomials*, J. London Math. Soc. 65 (2002), 661–671.

[16] J. C. Lagarias, J. A. Reed, Y. Wang: *Orthonormal bases of exponentials for the n-cube*, Duke Math. J. 103 (2000), 25–37.

[17] J. C. Lagarias, S. Szabó: *Universal spectra and Tijdeman's conjecture on factorization of cyclic groups*, J. Fourier Anal. Appl. 7 (2001), 63–70.

[18] J. C. Lagarias, Y. Wang: *Spectral sets and factorizations of finite abelian groups*, J. Funct. Anal. 145 (1997), 73–98.

[19] D.J. Newman: *Tesselation of integers*, J. Number Theory 9 (1977), 107–111.

[20] S. Pedersen: *Spectral sets whose spectrum is a lattice with a base*, J. Funct. Anal. 141 (1996), 496–509.

[21] S. Pedersen: *The dual spectral set conjecture*, preprint, 2002.

[22] S. Pedersen, Y. Wang: *Universal spectra, universal tiling sets, and the spectral set conjecture*, Math. Scand. 88 (2001), 246–256.

[23] A. Sands: *On Keller's conjecture for certain cyclic groups*, Proc. Edinburgh Math. Soc. 2 (1979), 17–21.

[24] A. Sands: *Replacement of factors by subgroups in the factorization of abelian groups*, Bull. London Math. Soc. 32 (2000), 297–304.

[25] R. Tijdeman: *Decomposition of the integers as a direct sum of two subsets*, in *Number Theory (Paris 1992–1993)*, London Math. Soc. Lecture Notes, vol. 215,261–276, Cambridge Univ. Press, Cambridge, 1995.

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

E-mail address: `kon@mech.math.msu.su`

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

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