On finite sets which tile the integers

Andrew Granville, Izabella Łaba, and Yang Wang

December 19, 2001

1 Introduction

A set of integers A is said to *tile the integers* if there is a set $C \subset \mathbf{Z}$ such that every integer n can be written in a unique way as $n = a + c$ with $a \in A$ and $c \in C$. Throughout this paper we will assume that A is finite. It is well known (see [7]) that any tiling of $\mathbf{Z}$ by a finite set A must be periodic: $C = B + M\mathbf{Z}$ for some finite set $B \subset \mathbf{Z}$ such that $|A|\,|B| = M$. W then write $A \oplus B = \mathbf{Z}/M\mathbf{Z}$.

Newman [7] gave a characterization of all sets A which tile the integers and such that $|A|$ is a prime power. Coven and Meyerowitz [1] found necessary and sufficient conditions for A to tile $\mathbf{Z}$ if $|A|$ has at most two prime factors. To state their result we need to introduce some notation. Without loss of generality we may assume that $A, B \subset \{0, 1, \dots\}$ and that $0 \in A \cap B$. Define the characteristic polynomials

$$A(x) = \sum_{a \in A} x^a, \;\; B(x) = \sum_{b \in B} x^b.$$

Then $A \oplus B = \mathbf{Z}/M\mathbf{Z}$ is equivalent to

$$A(x)B(x) = 1 + x + \ldots + x^{M-1} \; (\mathrm{mod}\, (x^M - 1)). \tag{1.1}$$

Let $\Phi_s(x)$ be the s-th cyclotomic polynomial, i.e. the monic, irreducible polynomial whose roots are the primitive s-th roots of unity, so that $x^n - 1 = \prod_{s|n} \Phi_s(x)$. Then (1.1) holds if and only if

$$|A||B| = M \text{ and } \Phi_s(x) \mid A(x)B(x) \text{ for all } s|M, \;\; s \neq 1. \tag{1.2}$$

Let S_A be the set of prime powers p^α such that $\Phi_{p^\alpha}(x)$ divides $A(x)$. Then the Coven-Meyerowitz conditions are:

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

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

It is proved in [1] that:

- if A satisfies (T1), (T2), then it tiles $\mathbf{Z}$;
- if A tiles $\mathbf{Z}$ then (T1) holds;

- if A tiles $\mathbf{Z}$ and $|A|$ has at most two prime factors, then (T2) holds.

The first two statements are relatively simple to prove and hold regardless of the size of A; the main difficulty is in proving the third one. The proof given by Coven and Meyerowitz relies crucially on a result of Sands [8]: if $A \oplus B = \mathbf{Z}/M\mathbf{Z}$ and M has at most two prime divisors, then one of A, B must be contained in a subgroup of $\mathbf{Z}_M$. A theorem of Tijdeman [10] implies that if A tiles the integers, then there exists a tiling $A \oplus B$ such that $|B|$ has the same prime factors as $|A|$. Therefore if $|A|$ has at most two prime factors, there is a tiling to which Sands' result applies; the authors then decompose this tiling and proceed by induction in $|A|$.

It seems very hard to verify whether (T2) holds for all sets which tile the integers. There is no analogue of Sands' result if M has three or more prime factors, as shown in [9], [4]; hence the methods of Coven and Meyerowitz do not extend to more general sets. The purpose of this paper is to settle, for the first time, a three-prime case.

Theorem 1.1 *Let A, B be two sets of integers such that $|A| = p^\alpha q^\beta r^\gamma$ and $|B| = pqr$, where p, q, r are distinct primes. Assume that $A \oplus B = \mathbf{Z}/M\mathbf{Z}$, where $M = |A|\,|B|$. If $\Phi_p(x), \Phi_q(x), \Phi_r(x)$ divide $A(x)$, then so do $\Phi_{pq}(x), \Phi_{pr}(x), \Phi_{qr}(x), \Phi_{pqr}(x)$.*

Equivalently, if the elements of A are equi-distributed modulo p, q, and r, then they are also equi-distributed modulo pqr. Observe that this reformulation of (T2) does not require the elements of A to be nonnegative.

We remark that by the results of [5], [6], [3], proving (T2) for all finite sets which tile the integers would essentially resolve one part of Fuglede's spectral set conjecture [2] in dimension 1.

Our main tool in proving Theorem 1.1 is the following identity.

Theorem 1.2 *For any finite $A, B \subset \mathbf{Z}$, let*

$$A_m = \#\{(a, a') \in A \times A : \ (a - a', N) = m\}, \ B_m = \#\{(b, b') \in B \times B : \ (b - b', N) = m\}.$$

Then

$$\sum_{m|N} \frac{A_m B_m}{\phi(N/m)} = \frac{1}{N} \sum_{d|N} \frac{\mathcal{A}_d \mathcal{B}_d}{\phi(d)}, \tag{1.3}$$

where

$$\mathcal{A}_d = \sum_{\xi : \Phi_d(\xi)=0} |A(\xi)|^2, \ \mathcal{B}_d = \sum_{\xi : \Phi_d(\xi)=0} |B(\xi)|^2.$$

Here, as usual, $\phi(n)$ is the Euler function and (m, n) denotes the greatest common divisor of m and n. We adopt the convention that $(n, 0) = n$ for any $n \neq 0$.

We also observe that Theorem 1.2 extends the following result of Sands [8].

Theorem 1.3 *[8] Let A, B be two subsets of $\mathbf{Z}$ such that the elements of each of them are distinct modulo M. Define $D_A = \{(a - a', M) : \ a, a' \in A, \ a \neq a'\}$ and $D_B = \{(b - b', M) : b, b' \in B, \ b \neq b'\}$. Then $A \oplus B = \mathbf{Z}/M\mathbf{Z}$ if and only if $|A|\,|B| = M$ and $D_A \cap D_B = \emptyset$.*

Our Theorem 1.2 provides an alternative proof of Theorem 1.3; furthermore, it implies Theorem 1.4 below.

Theorem 1.4 *Define A, B, D_A, D_B as in Theorem 1.3. If $D_A \cap D_B = \emptyset$, then $|A|\,|B| \le M$; the equality holds if and only if $A \oplus B = \mathbf{Z}/M\mathbf{Z}$.*

2 Proof of Theorems 1.2–1.4

Proof of Theorem 1.2. Fix $A, B \subset \mathbf{Z}$ and $N \in \mathbf{N}$. As usual, $\mu(n)$ is the Möbius function and $e(t) = e^{2\pi i t}$. Let $d|N$, then for any $t \in \mathbf{Z}$

$$\frac{1}{d} \sum_{\substack{j=0 \\ \frac{N}{d} \mid j}}^{N-1} e\Big(\frac{t_j}{N}\Big) = \begin{cases} 1 & \text{if } d \mid t, \\ 0 & \text{if } d \nmid t. \end{cases} \tag{2.1}$$

Let χ_I denote the characteristic function of the set I. Then for $m|N$,

$$\begin{aligned} \chi_{(N,t)=m} = \chi_{m|t}\, \chi_{(\frac{N}{m}, \frac{t}{m})=1} &= \chi_{m|t} \sum_{l|\frac{N}{m},\ l|\frac{t}{m}} \mu(l) \\ &= \sum_{l|\frac{N}{m}} \mu(l) \chi_{lm|t} \\ &= \sum_{l|\frac{N}{m}} \frac{\mu(l)}{lm} \sum_{\substack{j=0 \\ \frac{N}{lm}|j}}^{N-1} e\Big(\frac{tj}{N}\Big) \\ &= \sum_{j=0}^{N-1} e\Big(\frac{tj}{N}\Big) \sum_{l|\frac{N}{m},\ \frac{N}{lm}|j} \frac{\mu(l)}{lm}, \end{aligned} \tag{2.2}$$

where we used (2.1) and that $\sum_{v|u} \mu(v) = \chi_{u=1}$. Taking $v = N/m$, we deduce that

$$\begin{aligned} A_m = \#\{(a,a') \in A \times A :\ (a-a', N) = m\} &= \sum_{a,a' \in A} \chi_{(a-a',N)=N/v} \\ &= \sum_{a,a' \in A} \sum_{j=0}^{N-1} e\Big(\frac{(a-a')j}{N}\Big) \sum_{l|v,\ \frac{v}{l}|j} \frac{\mu(l)}{l} \\ &= \frac{1}{N} \sum_{j=0}^{N-1} \Big| \sum_{a \in A} e\Big(\frac{aj}{N}\Big)\Big|^2 \sum_{d|v,\ d|j} d\mu(v/d), \end{aligned} \tag{2.3}$$

where we substituted $d = v/l$. Let

$$s_J = \Big|A\Big(e\Big(\frac{J}{N}\Big)\Big)\Big| = \Big|\sum_{a \in A} e\Big(\frac{aJ}{N}\Big)\Big|,\ t_J = \Big|B\Big(e\Big(\frac{J}{N}\Big)\Big)\Big| = \Big|\sum_{b \in B} e\Big(\frac{bJ}{N}\Big)\Big|,$$

then from (2.3) we have

$$\sum_{m|N} \frac{A_m\, B_m}{\phi(N/m)} = \sum_{v|N} \frac{1}{\phi(v)} \left(\frac{1}{N} \sum_{J=0}^{N-1} s_J^2 \sum_{d|v,\ d|J} d\mu(v/d) \right) \left(\frac{1}{N} \sum_{I=0}^{N-1} t_I^2 \sum_{e|v,\ e|I} e\mu(v/e) \right)$$

$$= \frac{1}{N^2} \sum_{I,J=0}^{N-1} s_J^2\, t_I^2 \left(\sum_{v|N} \frac{1}{\phi(v)} \sum_{d|v,\ d|J} d\mu(v/d) \sum_{e|v,\ e|I} e\mu(v/e) \right). \tag{2.4}$$

Let $g = (I, J, N)$, $r = (J, N)/g$, and $s = (I, N)/g$ so that $(r, s) = 1$. Then

$$\sum_{v|N} \frac{1}{\phi(v)} \sum_{d|v,\ d|J} d\mu(v/d) \sum_{e|v,\ e|I} e\mu(v/e) = \sum_{v|N} \frac{1}{\phi(v)} \sum_{d|(v,rg)} d\mu(v/d) \sum_{e|(v,sg)} e\mu(v/e)$$

$$= \prod_{p^\alpha || N} \left(\sum_{i=0}^{\alpha} \frac{1}{\phi(p^i)} \sum_{d|(p^i,rg)} d\mu\Big(\frac{p^i}{d}\Big) \sum_{e|(p^i,sg)} e\mu\Big(\frac{p^i}{e}\Big) \right), \tag{2.5}$$

since all the functions involved are multiplicative. Now

$$\sum_{d|(p^i,t)} d\mu\Big(\frac{p^i}{d}\Big) = \begin{cases} 1 & \text{if } i = 0, \\ p^i - p^{i-1} & \text{if } i \geq 1 \quad \text{and} \quad p^i \mid t, \\ -p^{i-1} & \text{if } i \geq 1 \quad \text{and} \quad p^{i-1} \mid\mid t, \\ 0 & \text{if } i \geq 1 \quad \text{and} \quad p^i \nmid t. \end{cases}$$

Write $p^\gamma || g$ and $p^\delta || rs$ so that $\gamma + \delta \leq \alpha$. Therefore

$$\sum_{i=0}^{\alpha} \frac{1}{\phi(p^i)} \sum_{d|(p^i,rg)} d\mu\Big(\frac{p^i}{d}\Big) \sum_{e|(p^i,sg)} e\mu\Big(\frac{p^i}{e}\Big)$$

$$= 1 + \sum_{i=1}^{\gamma} \frac{1}{\phi(p^i)} (p^i - p^{i-1})^2 + \begin{cases} 0 & \text{if } \gamma = a, \\ \frac{1}{\phi(p^{\gamma+1})} (-p^\gamma)^2 & \text{if } \gamma < \alpha \quad \text{and } \delta = 0, \\ \frac{1}{\phi(p^{\gamma+1})} (-p^\gamma)(p^{\gamma+1} - p^\gamma) & \text{if } \gamma < \alpha \quad \text{and } \delta \geq 1 \end{cases}$$

$$= \begin{cases} p^\gamma & \text{if } \gamma = a \quad \text{(hence } \delta = 0), \\ p^{\gamma+1}/(p-1) & \text{if } \gamma < \alpha \quad \text{and } \delta = 0, \\ 0 & \text{if } \gamma < \alpha \quad \text{and } \delta \geq 1. \end{cases}$$

We thus have a non-zero term in (2.5) if and only if $\delta = 0$ for all p, that is $r = s = 1$, in other words $(I, N) = (J, N) = g$. In this case our answer is $p^\gamma\, p^{\alpha-\gamma}/\phi(p^{\alpha-\gamma}) = p^\alpha/\phi(p^{\alpha-\gamma})$. Therefore (2.5) becomes

$$\prod_{p^\alpha || N} \frac{p^\alpha}{\phi(p^{\alpha-\gamma})} = \frac{N}{\phi(N/g)}.$$

Substituting this into (2.4) gives

$$\sum_{m|N} \frac{A_m\, B_m}{\phi(N/m)} = \frac{1}{N} \sum_{g|N} \frac{1}{\phi(N/g)} \Big(\sum_{\substack{I=0 \\ (I,N)=g}}^{N-1} s_I^2 \Big) \Big(\sum_{\substack{J=0 \\ (J,N)=g}}^{N-1} t_J^2 \Big). \tag{2.6}$$

Let $N/g = d$ and $I = gi$, so that $(i, N/g) = (i, d) = 1$. Then

$$\sum_{\substack{I=0 \\ (I,N)=g}}^{N-1} s_I^2 = \sum_{\substack{i=0 \\ (i,d)=1}}^{N-1} \Big| A(e(ig/N)) \Big|^2 = \sum_{\substack{i=0 \\ (i,d)=1}}^{N-1} \Big| A(e(i/d)) \Big|^2 = \mathcal{A}_d,$$

and similarly for $\sum t_J^2$. Hence the right side of (2.6) equals

$$\frac{1}{N} \sum_{d|N} \frac{1}{\phi(d)} \mathcal{A}_d\, \mathcal{B}_d.$$

The theorem follows. ∎

Proof of Theorems 1.3 and 1.4. Apply Theorem 1.2 with $M = N$. The term on the right side of (1.3) with $d = 1$ is $|A|^2\,|B|^2/M$, and, since all elements of A and B are distinct modulo M, the term on the left side of (1.3) with $m = M$ is $|A|\,|B| = M$. In particular, the left side of (1.3) is $\geq M$, since all the remaining terms are nonnegative.

We first deduce Theorem 1.3. We have $A \oplus B = \mathbf{Z}/M\mathbf{Z}$ if and only if $|A|\,|B| = M$ and $\Phi_d(x)$ divides $A(x)$ or $B(x)$ for all $d|M$, $d \neq 1$. This in turn is equivalent to $|A|\,|B| = M$ and $\mathcal{A}_d\,\mathcal{B}_d = 0$ for all $d|M$, $d \neq 1$. Thus $A \oplus B = \mathbf{Z}/M\mathbf{Z}$ if and only if $|A|\,|B| = M$ and the right side of (1.3) equals $|A|^2\,|B|^2/M = M$. But the left side of (1.3) equals M if and only if $A_m\, B_m = 0$ for all $m|M$, $m \neq M$, which in turn is equivalent to $D_A \cap D_B = \emptyset$.

Assume now that $D_A \cap D_B = \emptyset$. Then the left side of (1.3) equals M, therefore so does the right side. Using that the $d = 1$ term is $|A|^2\,|B|^2/M$ and that all other terms are nonnegative, we find that $M \geq |A|^2\,|B|^2/M$, hence $|A|\,|B| \leq M$ and equality holds if and only if all the terms with $d > 1$ on the right are zero. As above, the latter together with the equality $|A|\,|B| = M$ is equivalent to $A \oplus B = \mathbf{Z}/M\mathbf{Z}$. Theorem 1.4 is proved. ∎

Our proof of Theorem 1.1 will be based on the following corollary of Theorem 1.2.

Corollary 2.1 *Assume that $A \oplus B = \mathbf{Z}/M\mathbf{Z}$. Define A_m as in Theorem 1.2. Let $N|M$, $c \in \mathbf{Z} \setminus B$, and*

$$b_m = b_m(c) = \#\{b \in B :\ (b - c, N) = m\}.$$

Then the quantity

$$\sum_{m|N} \frac{b_m(c) A_m}{\phi(N/m)} \tag{2.7}$$

is independent of the choice of c.

Proof. Fix N such that $N|M$. Apply Theorem 1.2 with B replaced by $C = B \cup \{c\}$, where $c \in \mathbf{Z} \setminus B$ will be allowed to vary later on. Define $C(x)$ and $\mathcal{C}_d$ in the obvious way.

We first evaluate the terms on the right of (1.3). The term with $d = 1$ is $(|B|+1)^2|A|^2/N$. If $d \neq 1, d|N$, then $d|M$, hence $\Phi_d(x)$ divides at least one of $A(x)$ or $B(x)$. If it divides $A(x)$, then $\mathcal{A}_d = 0$. If it divides $B(x)$, then for all roots ξ of $\Phi_d(x)$ we have $|C(\xi)|^2 = |B(\xi)+\xi^c|^2 = |\xi^c|^2 = 1$, hence $\mathcal{C}_d = \#\{\xi : \Phi_d(\xi) = 0\} = \phi(d)$. Combining all this we find that the right-hand side of (1.3) equals

$$\frac{1}{N}(|B|+1)^2|A|^2 + \frac{1}{N}\sum_{d|N, d\neq 1} \mathcal{A}_d. \tag{2.8}$$

Observe that this is independent of the choice of c.

Next, we have $C_m = B_m + 2b_m$, hence the left side of (1.3) equals

$$\sum_{m|N} \frac{A_m B_m}{\phi(N/m)} + \sum_{m|N} \frac{2b_m A_m}{\phi(N/m)}. \tag{2.9}$$

Comparing (2.9) and (2.8) we obtain (2.7)

We remark that (2.7) can be computed explicitly if $N = M$. Namely, choose c so that $c = b + kN \in B + N\mathbf{Z}$. If $m|N, m \neq N$, then $b_m \neq 0$ implies that there is an $b' \in B$ such that $(c - b', M) = m$, hence $(b - b', M) = m$ and $m \in D_B$. By Theorem 1.4, $m \notin D_A$ and $A_m = 0$. It follows that $b_m A_m = 0$ for all $m \neq M$. Moreover $b_M = 1$ and $A_M = |A|$. Hence

$$\sum_{m|N} \frac{b_m(c) A_m}{\phi(N/m)} = |A| \text{ if } N = M. \ \blacksquare \tag{2.10}$$

3 The tiling result

In this section we prove Theorem 1.1. Let A, B, M be as in the statement of the theorem.

Throughout the proof we will assume that B is not contained in $d\mathbf{Z}$ for any $d|M, d \neq 1$, for otherwise we may decompose the tiling as in Lemma 2.5 of [1] and proceed by induction. More precisely, suppose that the theorem is true for all sets A' whose cardinality $|A'|$ divides, but is not equal to, $|A|$. Suppose further that $B \subset p\mathbf{Z}$. From Lemma 2.5 of [1] we have the decomposition

$$A(x) = \sum_{i=0}^{p-1} x^{a_0} \bar{A}^{(i)}(x^p),$$

where $A^{(i)} = \{a \in A : \ a \equiv i \pmod p\}$, $a_i = \min(A^{(i)})$, and $\bar{A}^{(i)} = \{a - a_i : \ a \in A^{(i)}\}/p$. Moreover, we have

$$|A^{(0)}| = |A^{(1)}| = \ldots = |A^{(0)}| = |A|/p, \tag{3.1}$$

$$\bar{A}^{(i)} \oplus p^{-1}B = \mathbf{Z}, \tag{3.2}$$

$$S_{\bar{A}^{(0)}} = S_{\bar{A}^{(1)}} = \ldots = S_{\bar{A}^{(p-1)}} \tag{3.3}$$

and

$$S_A = \{p\} \cup S_{p\bar{A}^{(0)}}. \tag{3.4}$$

Suppose that $\Phi_p(x), \Phi_q(x), \Phi_r(x)$ divide $A(x)$. By (3.4), $\Phi_q(x)$ and $\Phi_r(x)$ divide $\bar{A}^{(0)}(x^p)$. By Lemma 1.1(7) of [1], $\Phi_q(x)$ and $\Phi_r(x)$ divide $\bar{A}^{(0)}(x)$, hence also $\bar{A}^{(i)}(x)$ for all i by (3.3). Since $\bar{A}^{(i)}$ tiles $\mathbf{Z}$ by (3.2), it follows from the inductive assumption that $\Phi_{qr}(x)$ divides $\bar{A}^{(i)}(x)$ for each i. Using Lemma 1.1(7) of [1] again, we deduce that $\Phi_{pq}(x)$, $\Phi_{pr}(x)$, $\Phi_{qr}(x)$, $\Phi_{pqr}(x)$ divide $\bar{A}^{(i)}(x^p)$ for each i, hence they also divide $A(x)$. Thus if we assume A to be a set of the smallest cardinality for which the theorem fails, the corresponding B cannot be a subset of $p\mathbf{Z}$, $q\mathbf{Z}$, or $r\mathbf{Z}$.

The following notation will be used throughout this section. We denote by (i,j,k) the unique integer in $\{0,1,\dots,pqr-1\}$ which equals $i(\operatorname{mod} p), j(\operatorname{mod} q), k(\operatorname{mod} r)$, and write $[i,j,k] = (i,j,k) + pqr\mathbf{Z}$. We also write $[*,j,k] = \bigcup_i [i,j,k]$, $[*,*,k] = \bigcup_{i,j}[i,j,k]$, etc. One can think of the residues modulo p,q,r as three-dimensional "coordinates", so that for example $[i,j,k]$ is a point, $[i,j,*]$ is a vertical line, and $[*,*,k]$ is a horizontal plane.

Lemma 3.1 *Let $B \subset \mathbf{Z}$. Assume that $0 \in B$ and*

$$B - B \subset p\mathbf{Z} \cup q\mathbf{Z} \cup r\mathbf{Z}. \tag{3.5}$$

Then at least one of the following holds:

$$B \subset [*,j,k] \cup [i,*,k] \cup [i,j,*] \text{ for some } i,j,k, \tag{3.6}$$

$$B \subset [0,0,0] \cup [i,j,0] \cup [i,0,k] \cup [0,j,k] \text{ for some } i,j,k, \tag{3.7}$$

$$B \subset [*,*,0], \text{ or } B \subset [*,0,*], \text{ or } B \subset [0,*,*]. \tag{3.8}$$

Proof. Suppose that (3.6) and (3.8) fail. Then in particular there is an $b \in B$ which is not in the set on the right of (3.6) with $i = j = k = 0$, say $b \in [i,j,0]$ for some $i,j \neq 0$. From our assumptions we have $B - b \subset p\mathbf{Z} \cup q\mathbf{Z} \cup r\mathbf{Z}$. Hence

$$\begin{aligned} B &\subset \Big([*,*,0] \cup [0,*,*] \cup [*,0,*]\Big) \cap \Big([*,*,0] \cup [i,*,*] \cup [*,j,*]\Big) \\ &= [*,*,0] \cup [i,0,*] \cup [0,j,*]. \end{aligned}$$

From the failure of (3.8) we get that at least one of the following holds:

(a) there is a $b_1 \in B$ such that $b_1 \in [i,0,*] \setminus [*,*,0]$,

(b) there is a $b_2 \in B$ such that $b_2 \in [0,j,*] \setminus [*,*,0]$.

Suppose that (a) holds, then $B - b_1 \subset p\mathbf{Z} \cup q\mathbf{Z} \cup r\mathbf{Z}$, hence $B \cap [0,*,*] \subset [*,0,0] \cup [i,*,0]$. Thus we have (3.6) unless (a) and (b) both hold. In the latter case, $b_1 \in [i,0,k]$ and $b_2 \in [0,j,k']$ for some $k,k' \neq 0$. We then see from (3.5) that $k = k'$ and that (3.7) holds. ■

By Theorem 1.3, at least one of the sets D_A, D_B does not contain 1. We deduce that at least one of $A - A$, $B - B$ satisfies (3.5), hence at least one of A, B obeys the conclusions of Lemma 3.1. We will now show that A cannot obey these conclusions. Indeed, we are assuming that the elements of A are distributed uniformly $\operatorname{mod} p$, $\operatorname{mod} q$, and $\operatorname{mod} r$. Hence each plane $[i,*,*]$ contains exactly $|A|/p$ elements of A, etc. This immediately contradicts (3.7) and (3.8), since in both of these cases there are planes which do not contain any elements of A. Suppose now that (3.6) holds. Assume that $p < r$ and let $i' \neq i$. By uniformity $\bmod r$ and $\bmod p$, the planes $[*, *, k]$ and $[i', *, *]$ contain exactly $|A|/r$ and $|A|/p$ elements of A. But by (3.6), all the elements of A which belong to $[i', *, *]$ are in fact in $[i', j, k]$, hence in $[*, *, k]$. This implies $|A|/p \leq |A|/r$, which contradicts the assumption that $p < r$.

Thus B satisfies one of (3.6), (3.7) (recall that we assume that (3.8) fails).

We record a simple lemma.

Lemma 3.2 *Let $A \subset \mathbf{Z}$. Then for any m we have*

$$|\{(a, a') \in A \times A: \ m|a - a'\}| \geq \frac{|A|^2}{m},$$

with equality if and only if the elements of A are equi-distributed $\bmod m$.

Let $N = pqr$. For $m|N$, we write $\alpha_m = \dfrac{A_m}{\phi(N/m)}$. It suffices to prove that

$$\alpha_m = \alpha_{m'} \text{ for all } m, m'|N. \tag{3.9}$$

Indeed, (3.9) implies that

$$|A|^2 = \sum_{m|pqr} A_m = \sum_{m|pqr} \phi(\frac{pqr}{m}) A_{pqr} = pqr A_{pqr},$$

and the theorem follows by Lemma 3.2.

It remains to deduce (3.9) from Corollary 2.1.

Case 1a. Assume that B satisfies (3.7) and that $p, q, r > 2$. We may then choose I, J, K such that $I \neq 0, i$, $J \neq 0, j$, $K \neq 0, k$, and the planes $[I, *, *], [*, J, *], [*, *, K]$ contain no elements of B. We first compare (2.7) with $c \in [I, J, K]$ and $c' \in [0, J, K]$. We then have

$$b_1(c) = |B|, \ b_m(c) = 0 \text{ if } m \neq 1,$$

$$b_1(c') = |B \cap [i, *, *]|, \ b_p(c') = |B \cap [0, *, *]| \neq 0, \ b_m(c') = 0 \text{ if } m \neq 1, p.$$

Substituting this in (2.7) we see that

$$|B|\alpha_1 = |B \cap [i, *, *]|\alpha_1 + |B \cap [0, *, *]|\alpha_p,$$

hence $\alpha_1 = \alpha_p$. Repeating this argument with p replaced by q and r, we obtain

$$\alpha_p = \alpha_q = \alpha_r = \alpha_1. \tag{3.10}$$

With I, J, K as above, let $c'' \in [0, 0, K]$, then

$$b_{pq} = |B \cap [0, 0, 0]| \neq 0, \ b_{pr} = b_{qr} = b_{pqr} = 0.$$

Comparing (2.7) for c and c'', and using also (3.10), we find that $\alpha_{pq} = \alpha_1$. Similarly for α_{qr} and α_{pr}, hence

$$\alpha_1 = \alpha_{pq} = \alpha_{pr} = \alpha_{qr}. \tag{3.11}$$

It only remains to prove that $\alpha_{pqr} = \alpha_1$. But this follows by applying (2.7) and (3.10), (3.11) to c as above and $c''' \in [0,0,0]$.

Case 1b. Assume now that B satisfies (3.7) and that $p = 2$. Let

$$t = |B \cap [0,0,0]|,\ x = |B \cap [i,j,0]|,\ y = |B \cap [0,j,k]|,\ z = |B \cap [i,0,k]|.$$

Since the case when (3.6) holds will be considered below, we may now assume that (3.6) fails, and in particular that t, x, y, z are all nonzero. Choose J, K such that $J \neq 0, j,\ K \neq 0, k$, and the planes $[*, J, *], [*, *, K]$ contain no elements of B. We first evaluate (2.7) with $c \in [0, J, K],\ [0, J, 0], [0, J, k]$, and find that the following are all equal:

$$\begin{aligned}(t+y)\alpha_2 + (x+z)\alpha_1 \quad &= C,\\ t\alpha_{2r} + y\alpha_2 + x\alpha_r + z\alpha_1 \quad &= C,\\ y\alpha_{2r} + t\alpha_2 + x\alpha_r + z\alpha_1 \quad &= C.\end{aligned}$$

Therefore

$$\begin{aligned}t(\alpha_2 - \alpha_{2r}) + x(\alpha_1 - \alpha_r) \quad &= 0,\\ y(\alpha_2 - \alpha_{2r}) + z(\alpha_1 - \alpha_r) \quad &= 0.\end{aligned} \tag{3.12}$$

Similarly, by considering (2.7) with c in $[1, J, K],\ [1, J, 0],\ [1, J, k]$ we obtain that

$$\begin{aligned}x(\alpha_2 - \alpha_{2r}) + t(\alpha_1 - \alpha_r) \quad &= 0,\\ z(\alpha_2 - \alpha_{2r}) + y(\alpha_1 - \alpha_r) \quad &= 0.\end{aligned} \tag{3.13}$$

Combining the first equations in (3.12), (3.13) we deduce that $(x-t)(\alpha_2 - \alpha_{2r} - \alpha_1 + \alpha_r) = 0$. Similarly, combining the second equations we deduce that $(y-z)(\alpha_2 - \alpha_{2r} - \alpha_1 + \alpha_r) = 0$. It follows that

$$\alpha_2 - \alpha_{2r} = \alpha_1 - \alpha_r. \tag{3.14}$$

Indeed, if (3.14) fails, we must have $x = t$ and $y = z$, in which case B is equi-distributed mod 2 and $\Phi_2(\xi)$ divides both $A(\xi)$ and $B(\xi)$. This is easily seen to be impossible, e.g. by (T1). We now substitute (3.14) in the first equation in (3.13):

$$(t+x)(\alpha_2 - \alpha_{2r}) = (t+x)(\alpha_1 - \alpha_r) = 0.$$

Since $t + x > 0$, it follows that $\alpha_1 = \alpha_r$ and $\alpha_2 = \alpha_{2r}$. We now repeat the same argument with r replaced by q, and conclude that

$$\alpha_1 = \alpha_r = \alpha_q,\ \alpha_2 = \alpha_{2r} = \alpha_{2q}. \tag{3.15}$$

Next, we evaluate (2.7) for c in $[0,0,0]$, $[1,0,0]$, $[0,j,0]$, $[1,j,0]$, $[0,0,k]$, $[1,j,k]$. Using also (3.15), we obtain that

$$\begin{aligned}
t\alpha_{2qr} + x\alpha_r + y\alpha_2 + z\alpha_q &= t\alpha_{2qr} + (x+z)\alpha_1 + y\alpha_2 &&= C,\\
t\alpha_{qr} + z\alpha_{2q} + x\alpha_{2r} + y\alpha_1 &= t\alpha_{qr} + (x+z)\alpha_2 + y\alpha_1 &&= C,\\
t\alpha_{2r} + x\alpha_{qr} + y\alpha_{2q} + z\alpha_1 &= x\alpha_{qr} + (y+t)\alpha_2 + z\alpha_1 &&= C,\\
x\alpha_{2qr} + t\alpha_r + y\alpha_q + z\alpha_2 &= x\alpha_{2qr} + (y+t)\alpha_1 + z\alpha_2 &&= C,\\
t\alpha_{2q} + z\alpha_{qr} + y\alpha_{2r} + x\alpha_1 &= z\alpha_{qr} + (t+y)\alpha_2 + x\alpha_1 &&= C,\\
y\alpha_{qr} + x\alpha_{2q} + z\alpha_{2r} + t\alpha_1 &= y\alpha_{qr} + (x+z)\alpha_2 + t\alpha_1 &&= C.
\end{aligned} \tag{3.16}$$

From equations 2,6 we have $(t-y)(\alpha_{qr}-\alpha_1)=0$, and from equations 3,5 $(x-z)(\alpha_{qr}-\alpha_1)=0$. Suppose first that $t\neq y$ or $x\neq z$, hence $\alpha_{qr}=\alpha_1$. Then we deduce from equations 2,4 that $\alpha_2=\alpha_{2qr}$. Substituting this in equations 1 and 2, we find that

$$(x+z)\alpha_1 + (t+y)\alpha_2 = (x+z)\alpha_2 + (t+y)\alpha_1,$$

hence $(x+z-t-y)(\alpha_1-\alpha_2)=0$. Now $x+z\neq t+y$, since otherwise B would be equi-distributed mod 2 and we have already noted that this is impossible. Therefore $\alpha_1=\alpha_2$, hence all the α_m are equal and we are done.

It remains to consider the case when $t=y$ and $x=z$. Then we rewrite equations 1,2,3,5 in (3.16) as

$$\begin{aligned}
2x\alpha_1 &+t\alpha_2 & & +t\alpha_{2qr} &= C,\\
t\alpha_1 &+2x\alpha_2 &+t\alpha_{qr} & &= C,\\
2t\alpha_1 &+x\alpha_2 & & +x\alpha_{2qr} &= C,\\
x\alpha_1 &+2t\alpha_2 &+x\alpha_{qr} & &= C.
\end{aligned} \tag{3.17}$$

The determinant of the coefficient matrix is $-4(t^2-x^2)^2$. If it were 0, we would have $x=t=y=z$, and in particular $|B|=x+y+z+t=4t$ would be divisible by 4, which contradicts the assumption that $|B|=2qr$. Hence (3.17) has only the trivial solution $\alpha_1=\alpha_2=\alpha_{qr}=\alpha_{2qr}$. This together with (3.15) implies that all the α_m are equal, which completes the proof for Case 1b.

Case 2. Assume that B satisfies (3.6). Translating B if necessary, we may assume that (3.6) holds with $i=j=k=0$. Denote

$$t = |B\cap[0,0,0]|,$$

$$x_i = |B\cap[i,0,0]|,\ y_j = |B\cap[0,j,0]|,\ z_k = |B\cap[0,0,k]|,\ i,j,k>0,$$
$$X=\sum x_i,\ Y=\sum y_i,\ Z=\sum z_i.$$

Since we are assuming that (3.8) fails, we have $X,Y,Z\neq 0$.

Applying Corollary 2.1 to c in $[i,j,k]$, $[i,j,0]$, $[i,0,k]$, $[0,j,k]$, $[i,0,0]$, $[0,j,0]$, $[0,0,k]$, $[0,0,0]$, where $i,j,k \neq 0$, we obtain that the following are all equal (denote the right-hand side by C):

$$\begin{aligned}
(X - x_i + Y - y_j + Z - z_k + t)\alpha_1 + x_i\alpha_p + y_j\alpha_q + z_k\alpha_r &= C,\\
(X - x_i + Y - y_j + t)\alpha_r + x_i\alpha_{pr} + y_j\alpha_{qr} + Z\alpha_1 &= C,\\
(X - x_i + Z - z_k + t)\alpha_q + x_i\alpha_{pq} + z_k\alpha_{qr} + Y\alpha_1 &= C,\\
(Y - y_j + Z - z_k + t)\alpha_p + y_j\alpha_{pq} + z_k\alpha_{pr} + X\alpha_1 &= C,\\
x_i\alpha_{pqr} + (X - x_i + t)\alpha_{qr} + (Y + Z)\alpha_1 &= C,\\
y_j\alpha_{pqr} + (Y - y_j + t)\alpha_{pr} + (X + Z)\alpha_1 &= C,\\
z_k\alpha_{pqr} + (Z - z_k + t)\alpha_{pq} + (X + Y)\alpha_1 &= C,\\
t\alpha_{pqr} + X\alpha_{qr} + Y\alpha_{pr} + Z\alpha_{pq} &= C.
\end{aligned} \tag{3.18}$$

We have to prove that this is possible if and only if all the α_m are equal. We begin with a few lemmas.

Lemma 3.3 *Let $A \subset \mathbf{Z}$, $|A|^2 = pqrL$, $N = prq$. Define α_m as above. Assume that $\Phi_p, \Phi_q, \Phi_r, \Phi_{pr}$ divide $A(x)$. Then:*

$$(q-1)\alpha_{pr} + \alpha_{pqr} = qL, \tag{3.19}$$

$$(q-1)\alpha_r + \alpha_{qr} = (q-1)\alpha_p + \alpha_{pq} = qL, \tag{3.20}$$

$$(q-1)\alpha_1 + \alpha_q = qL. \tag{3.21}$$

Proof. We will first prove that if Φ_p, Φ_q, Φ_r divide $A(x)$, then:

$$\begin{aligned}
(q-1)(r-1)\alpha_p + (r-1)\alpha_{pq} + (q-1)\alpha_{pr} + \alpha_{pqr} &= qrL,\\
(p-1)(r-1)\alpha_q + (r-1)\alpha_{pq} + (p-1)\alpha_{qr} + \alpha_{pqr} &= prL,\\
(p-1)(q-1)\alpha_r + (q-1)\alpha_{pr} + (p-1)\alpha_{qr} + \alpha_{pqr} &= pqL,
\end{aligned} \tag{3.22}$$

and

$$\begin{aligned}
(q-1)(r-1)\alpha_1 + (r-1)\alpha_q + (q-1)\alpha_r + \alpha_{qr} &= qrL,\\
(p-1)(r-1)\alpha_1 + (r-1)\alpha_p + (p-1)\alpha_r + \alpha_{pr} &= prL,\\
(p-1)(q-1)\alpha_1 + (q-1)\alpha_p + (p-1)\alpha_q + \alpha_{pq} &= pqL.
\end{aligned} \tag{3.23}$$

Indeed, from Lemma 3.2 with $m = p$ we have

$$A_p + A_{pq} + A_{pr} + A_{pqr} = \frac{|A|^2}{p} = qrL,$$

and the first equation in (3.22) follows by converting the A_m to α_m. Also, since $\sum_{m|pqr} A_m = |A|^2$, from the displayed equation above we have

$$A_1 + A_q + A_r + A_{qr} = (1 - \frac{1}{p})|A|^2 = (p-1)qrL,$$

and the first equation in (3.23) follows. The remaining equations in (3.22), (3.23) are similar.

Assume now that also $\Phi_{pr}(x)|A(x)$. Applying Lemma 3.2 with $m = pr$, we obtain

$$A_{pr} + A_{pqr} = \frac{|A|}{pr} = qL,$$

which implies (3.19). (3.20) follows by combining (3.19) with the first and third equations in (3.22), and (3.21) by combining the first equation in (3.20) with the first equation in (3.23). ∎

Lemma 3.4 *Suppose that α_m solve (3.18) with $X, Y, Z \neq 0$, and that*

$$\alpha_1 = \alpha_p,\ \alpha_r = \alpha_{pr},\ \alpha_q = \alpha_{pq},\ \alpha_{qr} = \alpha_{pqr}. \tag{3.24}$$

Then the α_m are all equal.

Proof. Fix i, j, k. Plugging (3.24) into (3.18), we obtain

$$\begin{aligned}
(X + Y - y_j + Z - z_k + t)\alpha_1 + y_j\alpha_q + z_k\alpha_r &= C,\\
(X + Y - y_j + t)\alpha_r + y_j\alpha_{qr} + Z\alpha_1 &= C,\\
(X + Z - z_k + t)\alpha_q + z_k\alpha_{qr} + Y\alpha_1 &= C,\\
(Y - y_j + Z - z_k + t)\alpha_p + y_j\alpha_q + z_k\alpha_r + X\alpha_1 &= C,\\
(X + t)\alpha_{qr} + (Y + Z)\alpha_1 &= C,\\
y_j\alpha_{qr} + (Y - y_j + t)\alpha_r + (X + Z)\alpha_1 &= C,\\
z_k\alpha_{qr} + (Z - z_k + t)\alpha_q + (X + Y)\alpha_1 &= C,\\
(t + X)\alpha_{qr} + Y\alpha_r + Z\alpha_q &= C.
\end{aligned} \tag{3.25}$$

From equations 2 and 6 in (3.25) we have $X\alpha_r = X\alpha_1$, hence $\alpha_r = \alpha_1$. Similarly, from equations 3 and 7 we have $X\alpha_q = X\alpha_1$, hence $\alpha_q = \alpha_1$. We now have $\alpha_1 = \alpha_p = \alpha_q = \alpha_r = \alpha_{pr} = \alpha_{pq}$. Plugging this into equation 1 we obtain $(X + Y + Z + t)\alpha_1 = C$; this together with equation 5 yields that $(X + t)\alpha_{qr} = (X + t)\alpha_1$, hence $\alpha_{qr} = \alpha_1$. By the last part of (3.24) we also have $\alpha_{pqr} = \alpha_1$, which ends the proof. ∎

We now begin the proof of Theorem 1.1 under the assumption that B satisfies (3.6). It suffices to consider the case when

$$x_i = x,\ y_j = y,\ z_k = z \tag{3.26}$$

for some $x, y, z \neq 0$ and all $i, j, k \neq 0$. (Hence $X = (p-1)x, Y = (q-1)y, Z = (r-1)z$.) Indeed, suppose for instance that $x_i \neq x_{i'}$ for some i, i'. Fix some j, k, and apply (3.18) with i, j, k and i', j, k. From equations 1, 2, 3, 5 in (3.18) we find that (3.24) holds, hence by Lemma 3.4 all the α_m are equal and we are done.

Lemma 3.5 *Assume that B satisfies (3.6) and that (3.26) holds. Then:*

- *$\Phi_{pq}(\xi) | B(\xi)$ if and only if $t = x + y + z - zr$;*
- *$\Phi_{qr}(\xi) | B(\xi)$ if and only if $t = x + y + z - xp$;*
- *$\Phi_{pr}(\xi) | B(\xi)$ if and only if $t = x + y + z - yq$;*
- *$\Phi_{pqr}(\xi) | B(\xi)$ if and only if $t = x + y + z$.*

Proof. We have

$$\begin{aligned} B(\xi) = t &+ x(\xi^{qr} + \xi^{2qr} + \ldots + \xi^{(p-1)qr}) + y(\xi^{pr} + \xi^{2pr} + \ldots + \xi^{(q-1)pr}) \\ &+ z(\xi^{pq} + \xi^{2pq} + \ldots + \xi^{(r-1)pq}) \\ &= t + x(\Phi_p(\xi^{qr}) - 1) + y(\Phi_q(\xi^{pr}) - 1) + z(\Phi_r(\xi^{pq}) - 1). \end{aligned}$$

Hence

$$B(e^{2\pi i/pq}) = t + x\Phi_p(e^{2\pi i r/p}) + y\Phi_q(e^{2\pi i r/q}) + z\Phi_r(1) - x - y - z = t + zr - x - y - z,$$

and similarly

$$B(e^{2\pi i/qr}) = t - x - y - z + px,$$

$$B(e^{2\pi i/pr}) = t - x - y - z + qy,$$

$$B(e^{2\pi i/pqr}) = t - x - y - z.$$

The lemma follows. ■

Corollary 3.6 *Let B be as in Lemma 3.5.*

- *If $\Phi_{pqr}(\xi) | B(\xi)$, then none of $\Phi_{pq}(\xi), \Phi_{qr}(\xi), \Phi_{pr}(\xi)$ can divide $B(\xi)$.*
- *Assume that $|B| = pqr$, then at most one of $\Phi_{pq}(\xi), \Phi_{qr}(\xi), \Phi_{pr}(\xi)$ can divide $B(\xi)$.*

Proof. The first part is obvious from Lemma 3.5, since $x, y, z \neq 0$. Suppose now that $|B| = pqr$ and that Φ_{pq}, Φ_{qr} divide $B(\xi)$. By Lemma 3.5 we have $t = x + y + z - zr = x + y + z - px$, hence $px = zr$, and in particular $p|z$, $r|x$. Moreover, adding up the elements of B we obtain

$$|B| = pqr = t + (p-1)x + (q-1)y + (r-1)z = px + qy = qy + rz,$$

hence $qr|x$ and $pr|y$. But then $pqr = pqr\dfrac{x}{qr} + pqr\dfrac{y}{pr}$, therefore $x = 0$ or $y = 0$ – a contradiction. ■

We return to the proof of Theorem 1.1. If $\Phi_{pq}(x), \Phi_{qr}(x), \Phi_{pr}(x), \Phi_{pqr}(x)$ divide $A(x)$, we are done. Assume therefore that at least one of them divides $B(x)$. By Corollary 3.6, we only need to consider two cases.

Case 2a: $\Phi_{pq}(\xi)|B(\xi)$, $\Phi_{pr}(\xi)\Phi_{qr}(\xi)|A(\xi)$. From Lemma 3.5 we have $t = x + y - Z$, which we substitute in (3.18):

$$\begin{aligned}
(X+Y-z)\alpha_1 + x\alpha_p + y\alpha_q + z\alpha_r &= C,\\
(X+Y-Z)\alpha_r + x\alpha_{pr} + y\alpha_{qr} + Z\alpha_1 &= C,\\
(X+y-z)\alpha_q + x\alpha_{pq} + z\alpha_{qr} + Y\alpha_1 &= C,\\
(Y+x-z)\alpha_p + y\alpha_{pq} + z\alpha_{pr} + X\alpha_1 &= C,\\
x\alpha_{pqr} + (X+y-Z)\alpha_{qr} + (Y+Z)\alpha_1 &= C,\\
y\alpha_{pqr} + (Y+x-Z)\alpha_{pr} + (X+Z)\alpha_1 &= C,\\
z\alpha_{pqr} + (x+y-z)\alpha_{pq} + (X+Y)\alpha_1 &= C,\\
(x+y-Z)\alpha_{pqr} + X\alpha_{qr} + Y\alpha_{pr} + Z\alpha_{pq} &= C.
\end{aligned} \tag{3.27}$$

We also have from Lemma 3.3:

$$\begin{aligned}
Y\alpha_{pr} + y\alpha_{pqr} = Y\alpha_p + y\alpha_{pq} = Y\alpha_r + y\alpha_{qr} = Y\alpha_1 + y\alpha_q = qyL,\\
X\alpha_{qr} + x\alpha_{pqr} = X\alpha_q + x\alpha_{pq} = X\alpha_r + x\alpha_{pr} = X\alpha_1 + x\alpha_p = pxL,
\end{aligned} \tag{3.28}$$

where as before we denote $L = |A|^2/pqr$. Plugging (3.28) into (3.27), we obtain:

$$\begin{aligned}
z(\alpha_r - \alpha_1) + pxL + qyL &= C,\\
Z(\alpha_1 - \alpha_r) + pxL + qyL &= C,\\
z(\alpha_{qr} - \alpha_q) + pxL + qyL &= C,\\
z(\alpha_{pr} - \alpha_p) + pxL + qyL &= C,\\
(y-Z)\alpha_{qr} + (Y+Z)\alpha_1 + pxL &= C,\\
(x-Z)\alpha_{pr} + (X+Z)\alpha_1 + qyL &= C,\\
z\alpha_{pqr} + (x+y-z)\alpha_{pr} + (X+Y)\alpha_1 &= C,\\
Z(\alpha_{pq} - \alpha_{pqr}) + pxL + qyL &= C.
\end{aligned} \tag{3.29}$$

From equations 1,2 in (3.29) we have $\alpha_1 = \alpha_r$ and $C = pxL + qyL$. From equations 3,4,8 respectively we then have $\alpha_q = \alpha_{qr}$, $\alpha_p = \alpha_{pr}$, $\alpha_{pq} = \alpha_{pqr}$. Thus we may apply Lemma 3.4 (with p and r interchanged) and conclude that all the α_m are equal.

Case 2b. $\Phi_{pqr}(\xi)|B(\xi)$, $\Phi_{pq}(\xi)\Phi_{qr}(\xi)\Phi_{pr}(\xi)|A(\xi)$. By (3.19)–(3.21) we have

$$\begin{aligned}
&(p-1)\alpha_{qr} + \alpha_{pqr} = (p-1)\alpha_q + \alpha_{pq} = (p-1)\alpha_r + \alpha_{pr} = (p-1)\alpha_1 + \alpha_p = pL,\\
&(q-1)\alpha_{pr} + \alpha_{pqr} = (q-1)\alpha_p + \alpha_{pq} = (q-1)\alpha_r + \alpha_{qr} = (q-1)\alpha_1 + \alpha_q = qL,\\
&(r-1)\alpha_{pq} + \alpha_{pqr} = (r-1)\alpha_r + \alpha_{pr} = (r-1)\alpha_q + \alpha_{qr} = (r-1)\alpha_1 + \alpha_r = rL.
\end{aligned} \tag{3.30}$$

Thus we can compute all the α_m if $\alpha_1 = \alpha$ is given:

$$\begin{aligned}
\alpha_p &= pL - (p-1)\alpha,\\
\alpha_q &= qL - (q-1)\alpha,\\
\alpha_r &= rL - (r-1)\alpha,\\
\alpha_{pq} &= (p-1)(q-1)\alpha - (pq-p-q)L,\\
\alpha_{pr} &= (p-1)(r-1)\alpha - (pr-p-r)L,\\
\alpha_{qr} &= (q-1)(r-1)\alpha - (qr-q-r)L,\\
\alpha_{pqr} &= ((p-1)(q-1)(r-1)+1)L - (p-1)(q-1)(r-1)\alpha.
\end{aligned} \tag{3.31}$$

If Φ_{pqr} does not divide $A(\xi)$, by Lemma 3.2 with $m = pqr$ we have $A_{pqr} = \alpha_{pqr} > L$, hence (from the last equation above) $L > \alpha$. We have to show that this is impossible.

By Lemma 3.5 we have $t = x + y + z$. We substitute this in the last four equations in (3.18):

$$\begin{aligned}
x\alpha_{pqr} + (X+y+z)\alpha_{qr} + (Y+Z)\alpha_1 &= C,\\
y\alpha_{pqr} + (Y+x+z)\alpha_{pr} + (X+Z)\alpha_1 &= C,\\
z\alpha_{pqr} + (x+y+Z)\alpha_{pq} + (X+Y)\alpha_1 &= C,\\
(x+y+z)\alpha_{pqr} + X\alpha_{qr} + Y\alpha_{pr} + Z\alpha_{pq} &= C.
\end{aligned} \tag{3.32}$$

(the remaining equations are equivalent). We now plug in (3.30). From the last equation we have

$$xpL + yqL + zrL = C. \tag{3.33}$$

The remaining equations become

$$\begin{aligned}
xpL + (y+z)\alpha_{qr} + (Y+Z)\alpha_1 &= C,\\
yqL + (x+z)\alpha_{pr} + (X+Z)\alpha_1 &= C,\\
zrL + (x+y)\alpha_{pq} + (X+Y)\alpha_1 &= C.
\end{aligned} \tag{3.34}$$

This adds up to

$$xpL + yqL + zrL + (y+z)\alpha_{qr} + (x+z)\alpha_{pr} + (x+y)\alpha_{pq} + 2(X+Y+Z)\alpha_1 = 3C,$$

hence by (3.33)

$$(y+z)\alpha_{qr} + (x+z)\alpha_{pr} + (x+y)\alpha_{pq} = 2(pxL + qyL + rzL - X\alpha_1 - Y\alpha_1 - Z\alpha_1).$$

By (3.30), the left side equals

$$2(pxL - X\alpha_p + qyL - Y\alpha_q + rzL - Z\alpha_r).$$

But now we can use (3.31). If $L > \alpha$, we have

$$\alpha_p = pL - (p-1)\alpha > \alpha = \alpha_1$$

and similarly $\alpha_q > \alpha_1, \alpha_r > \alpha_1$, which clearly contradicts the above. ■

Acknowledgement. The first and third authors are supported in part by the NSF. The second author is supported in part by NSERC.

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] I. Łaba: The spectral set conjecture and multiplicative properties of roots of polynomials, preprint, 2000.

[4] J.C. Lagarias, S. Szabó: Universal spectra and Tijdeman's conjecture on factorization of cyclic groups, J. Fourier Anal. Appl., to appear.

[5] J.C. Lagarias, Y. Wang: Tiling the line with translates of one tile, Invent. Math. 124 (1996), 341–365.

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

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

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

[9] S. Szabó: A type of factorization of finite abelian groups, Discrete Math. 54 (1985), 121–124.

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

Department of Mathematics, University of Georgia, Athens, GA 30602, U.S.A.
E-mail address: andrew@math.uga.edu

Department of Mathematics, University of British Columbia, Vancouver, B.C. V6T 1Z2, Canada
E-mail address: ilaba@math.ubc.ca

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332, U.S.A.
E-mail address: wang@math.gatech.edu