2014

Tiling the Integers

Shasha Li
University of Central Florida

TILLING THE INTEGERS

by

SHASHA LI
B.S. Uppsala University, 2009
M.S. Malardalen University, 2011

A thesis submitted in partial fulfilment of the requirements
for the degree of Master of Science in Mathematical Science
in the Department of Mathematics
in the College of Sciences
at the University of Central Florida
Orlando, Florida

Spring Term
2014

Major Professor: Dorin Dutkay

ABSTRACT

A set tiles the integers if and only if the integers can be written as a disjoint union of translates of that set. Counterexamples based on finite Abelian groups show that Fuglede conjecture is false in high dimensions. A solution for the Fuglede conjecture in $\mathbf{Z}$ or all the groups $\mathbf{Z}_N$ would provide a solution for the Fuglede conjecture in R. Focusing on tiles in dimension one, we will concentrate on the analysis of tiles in the finite groups $\mathbf{Z}_N$. Based on the Coven- Meyerowitz conjecture, it has been proved that if any spectral set in $\mathbf{Z}$ satisfies the the Coven-Meyerowitz properties, then every spectral set in R is a tile. We will present some of the main results related to integer tiles and give a self-contained description of the theory with detailed proofs.

ACKNOWLEDGMENTS

This thesis would not have been possible without the help and support of a number of people. First and foremost, I would like to express my sincerest gratitude to my advisor, Dr. Dorin Dutkay, for the tremendous time, energy and wisdom he invested in my graduate education. His inspiring and constructive supervision has always been a constant source of encouragement for my study. I also want to thank my other thesis committee members, Dr. Qiyu Sun, and Dr. Deguang Han , for spending their time to review the manuscript and providing valuable comments.

I dedicate this thesis to my family: my parents Yong Li and Cuixiang Liu, my husband Jason Zhang, for all their love and encouragement through my life. Last but not least, I would also like to extend my thanks to my friends, who have cared and helped me, in one way or another. My graduate studies would not have been the same without them.

TABLE OF CONTENTS

LIST OF FIGURES vi

CHAPTER 1: INTRODUCTION 1

CHAPTER 2: PRELIMINARIES 5

2.1 Congruence Modulon 5

2.2 Fourier Transform 13

2.2.1 Characters 15

2.3 Cyclotomic Polynomials 18

CHAPTER 3: TILING RESULT 29

3.1 Basic Properties 29

3.2 Tijdeman's Theorem 36

3.3 Coven Meyerowitz 40

3.4 The Square-free Case 47

LIST OF REFERENCES 49

LIST OF FIGURES

Figure 2.1: Indices of Entries 18

CHAPTER 1: INTRODUCTION

In 1974 [5], Bent Fuglede was working on a problem posed by Segal, stemming from quantum mechanics: given a domain Ω in $\mathbf{R}^n$, under what conditions are there *commuting* self-adjoint extensions of the differential operators $-i\frac{\partial}{\partial x_j}$, $j = 1, \ldots, n$, on the Hilbert space $L^2(\Omega)$? Fuglede found a solution to this problem and proved that such commuting extension exist if and only if there exists a discrete subset Λ of $\mathbf{R}^n$ with the property that the set of corresponding exponentials $\{e^{2\pi i\lambda\cdot x} : \lambda \in \Lambda\}$ forms an orthogonal basis for $L^2(\Omega)$. Such sets, that have a orthogonal basis of exponentials, are now called *spectral sets*.

Definition For λ in $\mathbf{R}^n$, denote $e_\lambda(x) = e^{2\pi i\lambda\cdot x}$, $x \in \mathbf{R}^n$. Let Ω be a bounded Lebesgue measurable set, of non-zero measure. The set Ω is called a *spectral set* if there exists a set Λ in $\mathbf{R}^n$ with the property that

$$\{e_\lambda : \lambda \in \Lambda\}$$

forms an orthogonal basis for $L^2(\Omega)$. In this case Λ is called a *spectrum* for Ω.

In the same paper, in an effort to give a geometric description of the spectral condition, Fuglede proposed the following conjecture, which is now known as "Fuglede's conjecture":

Conjecture 1.0.1 *[5] Let Ω be a bounded measurable susbet of $\mathbf{R}^n$, of non-zero measure. Then Ω is a spectral set if and only if Ω tiles $\mathbf{R}^n$ by translation.*

Definition We denote by $|A|$, the Lebesgue measure of a subset A of $\mathbf{R}^n$. Let Ω be a Lebesgue measurable subset of $\mathbf{R}^n$. We say that Ω *tiles $\mathbf{R}^n$ by translations* if there exists a set $\mathcal{T}$ in $\mathbf{R}^n$ such that $(\Omega + t)_{t\in\mathcal{T}}$ is a partition of $\mathbf{R}^n$ up to measure zero, i.e., $|(\Omega + t) \cap (\Omega + t')| = 0$ for all $t \neq t'$ in $\mathcal{T}$ and $|\mathbf{R}^n \setminus \cup_{t\in\mathcal{T}}(\Omega + t)| = 0$.

Recently, Terrence Tao [13] gave a counterexample to disprove the conjecture on $d \geq 5$. It was eventually shown that the conjecture is false in both directions on $d \geq 3$ [7, 4, 10, 8]. All these counterexamples are based on the study of the Fuglede conjecture on finite Abelian groups and also on the integer lattice. At this moment, the Fuglede conjecture is still open in both directions in dimension one and two.

The Fuglede conjecture can be easily formulated in the larger context of locally compact Abelian groups.

Definition Let G be a locally compact Abelian group and $\widehat{G}$ its dual group. Let Ω be a subset of G of finite, non-zero Haar measure. A set $\Lambda \subset \widehat{G}$ is called a *spectrum* of $\Omega \subset G$ if the characters $\{\lambda\}_{\lambda\in\Lambda}$ form an orthonormal basis in $L^2(\Omega)$. Ω is called a *spectral set* of G. Ω is called a tile if there exists a *tiling set* $\mathcal{T}$ in G such that $\Omega \oplus \mathcal{T} = G$ (i.e. every element in G can be uniquely written as sum of elements in T and $\mathcal{T}$, up to Haar measure zero).

Conjecture 1.0.2 *[The Fuglede conjecture for G] Let G be a locally compact Abelian group. A measurable subset Ω of G is spectral if and only if it is a tile.*

The groups that reveceived most of the attention are $\mathbf{R}$, $\mathbf{Z}$ and $\mathbf{Z}_N$ and their multidimensional variants.

Following the work of Tao, Kolountzakis, Matolcsi et. al., Dutkay and Lai [3] proved that a solution for the Fuglede conjecture in $\mathbf{Z}$ or all the groups $\mathbf{Z}_N$ would provide a solution for the Fuglede conjecture in $\mathbf{R}$. In other words, if one proves the Fuglede conjecture for all the groups $\mathbf{Z}_N$ that this implies the Fuglede conjecture for $\mathbf{R}$. This remains true also for one side of the equivalence, so if one proves that every tile is spectral in all the groups $\mathbf{Z}_N$ then all the tiles are spectral in $\mathbf{R}$.

In this thesis we will focus on tiles in dimension one. It known [6, 2, 11] that every finite tile of $\mathbf{Z}$ must have a periodic tiling set. This means that the study of tilings of the set of integers can be immediately reduced to the study of tiling sets for the finite groups $\mathbf{Z}_N$. Thus, we will concentrate on the analysis of tiles in the finite group $\mathbf{Z}_N$.

At this moment, probably the most promising approach for the analysis of tiles in $\mathbf{Z}_N$ is through the work of Coven and Meyerowitz [1]. They introduced two algebraic properties for finite sets $A \subset \mathbf{Z}^+ \cup \{0\}$. Define *the mask polynomial* associated to A,

$$A(x) := \sum_{a \in A} x^a.$$

Recall that the cyclotomic polynomial $\Phi_s(x)$ is the minimal polynomial for the primitive s^{th} root of unity.

Definition Let A be a finite subset of $\mathbf{Z}^+ \cup \{0\}$ and let

$$\mathcal{S}_A = \{p^\alpha : p \text{ is a prime}, \alpha \geq 1 \text{ an integer and } \Phi_s(x) \text{ divides } A(x)\}.$$

We say that A (or $A(x)$) satisfies the Coven-Meyerowitz property (CM-property) if $A(x)$ satisfies

$(T1)$. $\#A = A(1) = \prod_{s \in \mathcal{S}_A} \Phi_s(1)$.

$(T2)$. If $s_1, \cdots, s_n \in \mathcal{S}_A$, then $\Phi_{s_1 \cdots s_n}(x)$ divides $A(x)$.

Coven and Meyerowitz showed that all tiles on $\mathbb{Z}$ must satisfy (T1) and they satisfy (T2) if the number of elements in the tiles contains at most 2 prime factors. They proposed the following conjecture:

Conjecture 1.0.3 *The Coven-Meyerowitz conjecture Every finite tile in* $\mathbf{Z}$ *satisfies the CM-property.*

Moreover, the work of Coven and Meyerowitz [1], in conjunction with the work of Łaba [9], tells us that:

Theorem 1.0.4 *(i)[1] If* $A \subset \mathbb{Z}^+ \cup \{0\}$ *satisfies the CM-property, then* A *is a tile of integers.*

(ii)[9] If $A \subset \mathbb{Z}^+ \cup \{0\}$ *satisfies the CM-property, then* A *is a spectral set of integers.*

Using these results, Dutkay and Lai [3] proved that if the Coven-Meyerowitz conjecture is true, then any tile is spectral in $\mathbf{R}$ and, if any spectral set in $\mathbf{Z}$ satisfies the CM-property, then every spectral set in $\mathbf{R}$ is a tile.

The main results that we will describe in this thesis appear in the work of Coven and Meyerowitz (cite their paper) and on Terrence Tao's blog. We will present a self-contained description of the theory with detailed proofs.

CHAPTER 2: PRELIMINARIES

2.1 Congruence Modulon

Definition If two numbers b and c have the property that their difference $b-c$ is integrally divisible by a number m, (i.e., $(b-c)/m$ is an integer) then b and c are said to be "*congruent modulo m*". The number m is called the modulus, and the statement "b is congruent to c (modulo m)" is written mathematically as $b \equiv c$ (mod m). If $b-c$ is not integrally divisible by m, then it is said that "b is not congruent to c (modulo m)," which is written $b \not\equiv c$ (mod m). The number c in the congruence $b \equiv c$ (mod m) is called the *residue* of b (mod m). The *residue classes* of a function $f(x)$ mod m are all possible values of the residue $f(x)$ (mod m). For example, the residue classes of x^2 (mod 6) are $0, 1, 3, 4$, since

$$0^2 = 0(mod6)$$

$$1^2 = 1(mod6)$$

$$2^2 = 4(mod6)$$

$$3^2 = 3(mod6)$$

$$4^2 = 4(mod6)$$

$$5^2 = 1(mod6)$$

are all the possible residues.

Definition The greatest common divisor, denoted *gcd*, of two numbers M and N is the largest number D such that $D|N$ and $D|M$. There is an efficient algorithm to compute D. It can be verified that D is equal to the product of P^i over all primes P that divide both M and N i times

(i.e. $P^i|N$, $P^i|M$ but it's not the case that $P^{i+1}|N$ and $P^{i+1}|M$). Two integers m and n are *relatively prime* if they share no common positive factors (divisors) except 1,which is $(m, n) = 1$. We say that M and N are co-prime if $gcd(N, M) = 1$. For example, if P, Q, R are distinct primes, $N = PQ^2R$ and $M = Q^2R$ then $gcd(N, M) = Q^2R$. A set of integers is said to be *pairwise co-prime* if a and b are co-prime for every pair (a, b) of different integers in it.

- If P and Q are co-prime and both $P|N$ and $Q|N$, then $PQ|N$.
- If $P|AB$ then either $P|A$ or $P|B$.

Let **Z** denote the integers and let n be a fixed positive integer. We define a relation on **Z** by $i \equiv j$(mod n) if and only if n divides $i - j$. A divides B, denoted $A|B$ if there's a K such that $KA = B$. Here both the symbol $\equiv$ and the (mod n) are used to denote the relation. This is an equivalence relation on the integers. Thus we obtain a natural choice for the equivalence class representative. The factor set would be $\{[0], [1], [2], ..., [n-2], [n-1]\}$ and by abuse of notation we write this as $\{0, 1, 2, ..., n-2, n-1\}$.

Theorem 2.1.1 *let n be a positive integer. For all $a, b, c \in$ **Z***

1. $a \equiv a$ *(mod n)*
2. $a \equiv b$ *(mod n)* $\Rightarrow b \equiv a$ *(mod n)*
3. $a \equiv b$ *(mod n) and $b \equiv c$ (mod n)* $\Rightarrow a \equiv c$ *(mod n).*

Proof 1. $a - a = 0$ and $n|0$, hence $a \equiv a$ (mod n).

2. $a \equiv b$ (mod n) means that $a - b = nk$ for some $k \in$ **Z**. Therefore, $b - a = -nk = n(-k)$; hence $b \equiv a$ (mod n).

3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then

$$a - b = nk$$

$$b - c = nk'$$

Adding these two equations yields

$$a - c = n(k + k')$$

and so $a \equiv c \pmod{n}$.■

Theorem 2.1.2 *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then*

1. $a + c \equiv b + d \pmod{n}$
2. $ac \equiv bd \pmod{n}$

Proof 1. By the definition of congruence, there are integers s and t such that $a - b = sn$ and $c - d = tn$. Therefore adding $b + d$ to both sides of this equation, we get

$$a + c = b + d + n(s + t)$$

Hence, $a + c \equiv b + d \pmod{n}$.

2. Using the fact that $-bc + bc = 0$ we have

$$\begin{aligned} ac - bd &= ac + 0 - bd \\ &= ac + (-bc + bc) - bd \\ &= c(a - b) + b(c - d) \\ &= c(sn) + b(tn) \\ &= n(cs + bt) \end{aligned} \tag{2.1}$$

and so $n|(ac - bd)$. Hence $ac \equiv bd$ (mod n). ■

Definition Let a and n be integers with $n > 0$. The *congruence class* of a modulo n, denoted $[a]_n$ is the set of all integers that are congruent to a modulo n; i.e.,

$$[a]_n = \{z \in \mathbf{Z} | a - z = kn \text{ for some } k \in \mathbf{Z}\} \tag{2.2}$$

A *ring* is a set R equipped with binary operations addition and multiplication satisfying the following eight axioms, called the ring axioms:

R is an Abelian group under addition, meaning:

1. $(a + b) + c = a + (b + c)$ for all a, b, c in R (+ is associative).
2. There is an element 0 in R such that $a + 0 = a$ and $0 + a = a$ (0 is the additive identity).
3. For each a in R there exists a in R such that $a + (a) = (a) + a = 0$ (a is the additive inverse of a).
4. $a + b = b + a$ for all a and b in R (+ is commutative).

R is a monoid under multiplication, meaning:

5. $(a \times b) \times c = a \times (b \times c)$ for all a, b, c in R ($\times$ is associative).

6. There is an element 1 in R such that $a \times 1 = a$ and $1 \times a = a$ (1 is the multiplicative identity).

Multiplication distributes over addition:

7. $a \times (b + c) = (a \times b) + (a \times c)$ for all a, b, c in R (left distributivity).

8. $(b + c) \times a = (b \times a) + (c \times a)$ for all a, b, c in R (right distributivity).

Theorem 2.1.3 *$\boldsymbol{Z}_N = \boldsymbol{Z}/N\boldsymbol{Z}$, the integers modulo N where $N \geq 2$ and $N \in \boldsymbol{Z}$, with the operation of addition and multiplication forms a ring.*

A *group* is an ordered pair $(G, *)$ where $*$ is a binary operation:

$$* : G \times G \to G$$

$$(a, b) \to a \times b$$

that satisfies:

1. (Associativity) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$

2. (Identity) There exists an element $1 \in G$ such that $a * 1 = 1 * a = a$ for all $a \in G$

3. (Inverses) For each $a \in G$, there exists $a^{-1} \in G$ such that $a^{-1} * a = e = a * a^{-1}$.

We denote $a^k = a \star \cdots \star a$ (k times). A *subgroup* is a subset H of a group G that is a group under the multiplication in G (we'll write $H \leq G$).

The group is *Abelian* (also known as *commutative*) if $a \star b = b \star a$ for all $a, b \in G$. The size of a group G, denoted $|G|$, is the number of elements in it. An *Abelian group* is a nonempty set A with a binary operation $+$ defined on A such that the following conditions hold:

1. (Associativity) for all $a, b, c \in A$, we have $a + (b + c) = (a + b) + c$;
2. (Commutativity) for all $a, b \in A$, we have $a + b = b + a$;
3. (Existence of an additive identity) there exists an element $0 \in A$ such that $0 + a = a$ for all $a \in A$;
4. (Existence of additive inverses) for each $a \in A$ there exists an element $-a \in A$ such that $-a + a = 0$.

Theorem 2.1.4 *If $m \in \boldsymbol{Z}_N$ is prime with N, then there exists $k, l \in \boldsymbol{Z}$ such that $mk + Nl = 1$.*

Proof Let $G = \{km + lN.\ k, l \in \mathbf{Z}\}$, then G is a subgroup of $\mathbf{Z}$. We need to prove $G = d\mathbf{Z}$ for $d \in \mathbf{Z}$.

Define $d := min\{g \in G, g > 0\}$, then $d \in G$ and $nd \in g \in G$ for $n \in \mathbf{Z}$. Therefore $d\mathbf{Z} \subset G$. Let $g = kd + l$ with $0 < l \leq d - 1$, then $l = g - kd \in G$. As d is the positive minimum in G, we get that $l = 0$ and $g = kd$. Hence $G \subset d\mathbf{Z}$ and $G = d\mathbf{Z}$. Let $m = dk_1$ and $N = dk_2$, as m is prime with N so $d = \pm 1$. As d is positive by definition so $d = 1$ and $G = \mathbf{Z}$. Since $1 \in \mathbf{Z}$, we have $1 \in G$ and $km + lN = 1$.■

Theorem 2.1.5 *Let $\mathbf{Z}_N^*$ be the set of elements in $\mathbf{Z}_N$ that have a multiplication inverse. Then $\mathbf{Z}_N^* = \{m \in \mathbf{Z}_N : \text{ m is prime with N}\}$ and $\mathbf{Z}_N^*$ is a group with the operation of multiplication.*

Proof First we will prove $\mathbf{Z}_N^* = \{m \in \mathbf{Z}_N : \text{ m is prime with N}\}$. To show this we first will show if there exists a $m \in \mathbf{Z}_N^*$, then $\{m \in \mathbf{Z}_N : \ m \text{ is prime with } N\}$. Let $m \in \mathbf{Z}_N^*$, then m is invertible, there exist a $q \in \mathbf{Z}$ such that $mq \equiv 1 \bmod N$, which means there exists a $k \in \mathbf{Z}$ such that $mq - 1 = kN$. If $d|m$ and $d|N$, then $d|(mq)$ and $d|(kN)$. Therefore $d|(mq)$ and $d|(mq-1)$ and $d|1$ which means $d = \pm 1$ and there is no other common divisor between m and N, so $gcd(m, N) = 1$. As $\mathbf{Z}_N^*$ is the set of elements in $\mathbf{Z}_N$, so $m \in \mathbf{Z}_N^* \subseteq \mathbf{Z}$. Next we will show if $m \in \mathbf{Z}_N$ and m is prime with N, then $m \in \mathbf{Z}_N^*$. As m is prime with N, then by Theorem 2.1.4, there exist $p, q \in \mathbf{Z}$ such that $mp + Nq = 1$. Hence $mp \equiv 1 \bmod N$ and m is invertible. As $m \in \mathbf{Z}_N$ and m has a multiplication inverse, we get $m \in \mathbf{Z}_N^*$.

Second we will show $\mathbf{Z}_N^*$ is a group with the operation of multiplication. As $\mathbf{Z}_N^*$ have multiplication inverse, let $a \in \mathbf{Z}_N^*$, then $a^{-1} \in \mathbf{Z}_N^*$ and $a \times a^{-1} = 1$. If $a, b \in \mathbf{Z}_N^*$, then $a^{-1}, b^{-1} \in \mathbf{Z}_N^*$ and $a \times b \in \mathbf{Z}_N^*$. Therefore $\mathbf{Z}_N^*$ is a group with the operation of multiplication.■

If there is an isomorphism $f : G \to H$, G and H are isomorphic, and we write $G \cong H$. Given two groups $(G, *)$ and $(H, \odot)$, a group isomorphism from $(G, *)$ to $(H, \odot)$ is a bijective group homomorphism from G to H. Spelled out, this means that a group isomorphism is a bijective function $f : G \to H$ such that for all u and v in G it holds that $f(u * v) = f(u) \odot f(v)$.

Theorem 2.1.6 *Let $N = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$ where $p_1, \dots, p_s$ are distinct prime numbers and $r_1, \dots, r_s > 0$. Then the map*

$$\Psi : \mathbf{Z}_N \to \mathbf{Z}_{p_1^{r_1}} \times \mathbf{Z}_{p_2^{r_2}} \times \cdots \times \mathbf{Z}_{p_s^{r_s}}, \quad \Psi(n) = (n \mod p_1^{r_1}, n \mod p_2^{r_2}, \dots, n \mod p_s^{r_s}), \text{ for } n \in \mathbf{Z}_N$$

is a group isomorphism.

Proof Suppose n and $n' \in \mathbf{Z}_N$, then $n \equiv n' \bmod N$ and $n' \equiv n \bmod N$, so Ψ is well defined and is obvious a group morphism. We will prove Ψ is one-to-one, or equivalently, that is has a trivial kernel $(\Psi(x) = 0)$. As $n \in \mathbf{Z}_{p_1^{r_1} \dots p_s^{r_s}}$, if $\Psi(n) = 0$ then $n \equiv 0 \mod p_i^{r_i}$ for all $i \in \{1, \dots, s\}$, so $n = k_i p_i^{r_i}$ and is divisible by all $p_i^{r_i}$. Since these primes are distinct it follows that n is divisible by their product which is N. Therefore f is one-to-one.■

Proposition 2.1.7 *Let $N = p_1 \dots p_s$ be a square-free number, $p_1, \dots, p_s$ are primes. Let $P = \{p_1, \dots, p_s\}$. Then*

1. *Any subgroup of $\prod_{p \in P} \mathbf{Z}_p$ is of the form $\prod_{p \in P'} \mathbf{Z}_p$, where P' is a subset of P.*
2. *For any subgroup H of $\mathbf{Z}_N$, there exists a subgroup $H^\perp$ such that $H \oplus H^\perp = \mathbf{Z}_N$.*

Proof Let H be a subgroup of $\prod_{p \in P} \mathbf{Z}_p$. Suppose $a = (a_1, \dots, a_s)$ is a non-zero element in H. We can assume, to simplify notation, that $a_1 \neq 0$. Then $p_2 p_3 \dots p_s \cdot a = (p_2 p_3 \dots p_s \cdot a_1, p_2 p_3 \dots p_s \cdot a_2, \dots, p_2 p_3 \dots p_s \cdot a_s)$. As in $\mathbf{Z}_p$, so $p_2 p_3 \dots p_s \cdot a_2, \dots, p_2 p_3 \dots p_s \cdot a_s = 0 \dots 0$. Since the primes p_i are distinct, the element $b_1 := p_2 \dots p_s \cdot a_1$ of $\mathbf{Z}_{p_1}$ cannot be zero, the order of a_1 being p_1. Thus H contains the element $(b_1, 0 \dots, 0)$ and this generates the entire subgroup $\mathbf{Z}_{p_1} \times \{0\} \times \dots \times \{0\}$. Thus if H contains an element $(a_1, \dots, a_s)$ with $a_i \neq 0$ then the subgroup $\mathbf{Z}_{p_i}$ is contained in H. This implies the first conclusion.

From the first part we see that any subgroup H of $\prod_{p \in P} \mathbf{Z}_p$ has a complement subgroup $H^\perp = \prod_{p \in P \setminus P'} \mathbf{Z}_p$. By Theorem 2.1.6, the group $\mathbf{Z}_N$ and $\mathbf{Z}_{p_1^{r_1}} \times \mathbf{Z}_{p_2^{r_2}} \times \dots \times \mathbf{Z}_{p_s^{r_s}}$ are isomorphic. Therefore $\mathbf{Z}_{p_1^{r_1}} \times \mathbf{Z}_{p_2^{r_2}} \times \dots \times \mathbf{Z}_{p_s^{r_s}}$ has a completement subgroup and the second statement follows.■

Theorem 2.1.8 *(Chinese remainder theorem) Let P and Q be two prime numbers (actually can be also just co-prime) and let $N = PQ$. Consider the following function from $\mathbf{Z}_N$ to $\mathbf{Z}_P \times \mathbf{Z}_Q$: $f(X) = \langle X \pmod P, X \pmod Q \rangle$. We claim the following properties of this function:*

1. *$f(\cdot)$ preserves addition: $f(X+X') = f(X)+f(X')$. (In the right hand side $f(X)+f(X')$ means that we add the first element of both pairs mod P and the second element mod Q. This follows from the fact that the modulo operation has this property.*
2. *$f(\cdot)$ preserves multiplication: $f(X \cdot X') = f(X) \cdot f(X')$. Again, this follows from the fact that the modulo operation has this property.*
3. *$f(\cdot)$ is one-to-one. Indeed, if there exist $X \neq X'$ with $f(X) = f(X')$ then $f(X - X') = \langle 0, 0 \rangle$. Which means that $P|X - X'$ and $Q|X - X'$ which implies $PQ = N|X - X'$ which can't happen for a number between 1 and $N - 1$.*
4. *$f(\cdot)$ is onto. This follows from the fact that $|\mathbf{Z}_N| = |\mathbf{Z}_P| \cdot |\mathbf{Z}_Q|$.*
5. *Note that the above properties also imply that f is an isomorphism from $\mathbf{Z}_N^*$ to $\mathbf{Z}_P^* \times \mathbf{Z}_Q^*$.*

2.2 Fourier Transform

Definition Let $f : \mathbf{Z}_N \to \mathbb{C}$, the Fourier transform of f is defined as the function $\widehat{f} : \mathbf{Z}_N \to \mathbb{C}$

$$\widehat{f}(k) = \frac{1}{\sqrt{N}} \sum_{n \in \mathbf{Z}_N} f(n) e^{2\pi i \frac{k \cdot n}{N}}, \quad (k \in \mathbf{Z}_N).$$

(Note that the definition does not depend on the choice of the representatives k, n of elements in $\mathbf{Z}_N$) The matrix of the Fourier transform is

$$\frac{1}{\sqrt{N}} \left(e^{2\pi i \frac{kn}{N}} \right)_{k,n \in \mathbf{Z}_N}.$$

Theorem 2.2.1 *The Fourier transform is unitary.*

Proof We are going to prove the matrix of the Fourier transform is unitary. Clearly $\frac{1}{\sqrt{N}}\left(e^{2\pi i\frac{kn}{N}}\right)_{k,n\in\mathbf{Z}_N}$ is a matrix with k is the row and n is the column. We are going to prove the rows are orthogonal. Take $k \neq k'$ in $\mathbf{Z}_N$. Then

$$\sum_{n\in\mathbf{Z}_N} e^{2\pi i\frac{(k-k')\cdot n}{N}} = \sum_{n=0}^{N-1}\left(e^{2\pi i\frac{k-k'}{N}}\right)^n = \frac{\left(e^{2\pi i\frac{k-k'}{N}}\right)^N - 1}{e^{2\pi i\frac{k-k'}{N}} - 1} = \frac{e^{2\pi i(k-k')} - 1}{e^{2\pi i\frac{k-k'}{N}} - 1} = \frac{1-1}{e^{2\pi i\frac{k-k'}{N}} - 1} = 0.$$

Hence they are orthogonal and the matrix of the Fourier transform is unitary.■

Theorem 2.2.2 *(Fourier inversion formula) Let $f : \mathbf{Z}_N \to \mathbb{C}$ and let $\widehat{f}$ be its Fourier transform. Then*

$$f(n) = \frac{1}{\sqrt{N}}\sum_{k\in\mathbf{Z}_N}\widehat{f}(k)e^{-2\pi i\frac{kn}{N}}, \quad (n \in \mathbf{Z}_N).$$

Proof Since the Fourier transform is unitary, its inverse is its transpose conjugate.■

Definition Let $f : \mathbf{Z}_N \to \mathbb{C}$, then $f(n) * g(n) = \frac{1}{N}\sum_{k\in\mathbf{Z}_N} f(n-k)g(k)$.

Theorem 2.2.3 $\widehat{f * g}(n) = \frac{1}{\sqrt{N}}\hat{f}(n)\hat{g}(n)$

Proof As Fourier transforms states that $\widehat{f}(k) = \frac{1}{\sqrt{N}}\sum_{n\in\mathbf{Z}_N} f(n)e^{2\pi i\frac{k\cdot n}{N}}, \quad (k \in \mathbf{Z}_N)$. Then by the definition of $f * g$, we have

$$\widehat{f * g}(n) = \frac{1}{\sqrt{N}}\sum_{k\in\mathbf{Z}_N} f * g(k)e^{2\pi i\frac{k\cdot n}{N}} = \frac{1}{\sqrt{N}}\sum_{k\in\mathbf{Z}_N}\frac{1}{N}\sum_{m\in\mathbf{Z}_N} f(k-m)g(m)e^{2\pi i\frac{((k-m)+m)n}{N}}$$

Let $k - m = l$, then

$$\widehat{f * g}(n) = \frac{1}{\sqrt{N}} \sum_{l \in \mathbf{Z}_N} f(l) e^{2\pi i \frac{ln}{N}} \frac{1}{\sqrt{N}} \cdot \frac{1}{\sqrt{N}} \sum_{m \in \mathbf{Z}_N} g(m) e^{2\pi i \frac{mn}{N}} = \frac{1}{\sqrt{N}} \hat{f}(n) \hat{g}(n)$$

.■

2.2.1 Characters

Definition Let $(G, +)$ be a finite Abelian group. A character on G is a function $\varphi : G \to \mathbf{T}$, where $\mathbf{T} = \{z \in \mathbb{C} : |z| = 1\}$, such that $\varphi(x + y) = \varphi(x)\varphi(y)$ for all $x, y \in G$. Clearly, if φ is a character, then $\varphi(0) = 1$. The set of characters is denoted $\widehat{G}$.

Proposition 2.2.4 *The set of characters $\widehat{G}$ is a group with the operation of pointwise multiplication. Any two distinct characters φ, φ' in $\widehat{G}$ are orthogonal in $L^2(G)$, i.e.,*

$$\sum_{g \in G} \varphi(g) \bar{\varphi}'(g) = 0 \tag{2.3}$$

Proof Checking that $\widehat{G}$ is a group is trivial. To see that φ, φ' are orthogonal, take $h \in G$ such that $\varphi(h) \neq \varphi'(h)$. Then

$$\sum_{g \in G} \varphi(g) \bar{\varphi}'(g) = \sum_{g \in G} \varphi(g + h) \bar{\varphi}'(g + h) = \varphi(h) \bar{\varphi}'(h) \sum_{g \in G} \varphi(g) \bar{\varphi}'(g).$$

Since $\varphi(h) \bar{\varphi}'(h) = \varphi(h) / \varphi'(h) \neq 1$, equation (2.3) follows.■

Proposition 2.2.5 *The characters of the group $G = \boldsymbol{Z}_{N_1} \times \cdots \times \boldsymbol{Z}_{N_s}$ are the maps of the form*

$$\varphi(n_1, \ldots, n_s) = e^{2\pi i \left(\frac{k_1 n_1}{N_1} + \cdots + \frac{k_s n_s}{N_s} \right)}, \quad ((n_1, \ldots, n_s) \in G),$$

where $(k_1, \ldots, k_s)$ is a fixed element in G. Therefore, for any finite Abelian group $\widehat{G}$ is isomorphic to G.

Proof Let φ be a character. Then $\varphi(1,0,\ldots,0)^{N_1} = \varphi(N_1 \cdot 1, 0, \ldots, 0) = \varphi(0) = 1$. Therefore $\varphi(1,0,\ldots,0)$ is a root of order N of unity; hence there exists $k_1 \in \mathbf{Z}_{N_1}$ such that $\varphi(1,0,\ldots,0) = e^{2\pi i \frac{k_1}{N_1}}$. We can do the same thing for the other components and obtain $k_2 \in \mathbf{Z}_{N_2}$ etc. The formula for φ follows directly from this.

For the converse, a simple check shows that any such map is a character on G.

Since any finite Abelian group is of the form $\mathbf{Z}_{N_1} \times \cdots \times \mathbf{Z}_{N_s}$, the last statement is clear.■

Definition Let G be a finite Abelian group of cardinality N. For a function $f : G \to \mathbb{C}$, the Fourier transform of f is the function $\widehat{f} : \widehat{G} \to \mathbb{C}$

$$\widehat{f}(\varphi) = \frac{1}{\sqrt{N}} \sum_{g \in G} f(g)\varphi(g).$$

The matrix of the Fourier transform is

$$\frac{1}{\sqrt{N}} \left(\varphi(g)\right)_{\varphi \in \widehat{G}, g \in G}.$$

Theorem 2.2.6 *The Fourier transform is a unitary transformation.*

Proof From Proposition 2.2.4 we see that the rows of the matrix of the Fourier transform are orthogonal. From Proposition 2.2.5, we see that $\widehat{G}$ has N elements. Thus the matrix is unitary.■

Remark Let $N = p_1 \ldots p_s$ where p_i are distinct primes and let $G = \prod_{i=1}^{s} \mathbf{Z}_{p_i}$. From Proposition 2.2.5, we see that the characters of G are of the form $(n_1, \ldots, n_s) \mapsto e^{2\pi i \left(\frac{k_1 n_1}{p_1} + \ldots \frac{k_s n_s}{p_s}\right)}$. However,

we can also use the isomorphism in Theorem 2.1.6 to produce characters on G and in this way, any character on G will be of the form $(n_1, \ldots, n_s) \mapsto e^{2\pi i \frac{\Psi^{-1}(n_1,\ldots,n_s)\cdot k}{N}}$, for some $k \in \mathbf{Z}_N$, or $(n_1, \ldots, n_s) \mapsto e^{2\pi i \frac{\Psi^{-1}(n_1,\ldots,n_s)\cdot \Psi^{-1}(k_1,\ldots,k_s)}{N}}$, for some $(k_1, \ldots, k_s) \in G$.

We can write the Fourier transform using both these forms, but note that we are making some identifications $\widehat{G}$ isomorphic to G and is isomorphic to $\mathbf{Z}_N$. The problem is that under these identifications the order in which the characters are listed might change and so the matrices of the Fourier transforms might be different. They will be obtain from one another by some permutation. Let us illustrate with one example.

Take $\mathbf{Z}_6 = \mathbf{Z}_2 \times \mathbf{Z}_3$. The isomorphism Ψ from Theorem 2.1.6 acts as follows: $0 \mapsto (0,0)$, $1 \mapsto (1,1)$, $2 \mapsto (0,2)$, $3 \mapsto (1,0)$, $4 \mapsto (0,1)$, $5 \mapsto (1,2)$.

When we write the Fourier transform using the group $\mathbf{Z}_6$, the (k,n) entry will be (omitting the $e^{2\pi i}$ part) $\frac{kn}{6}$. If $\Psi(k) = (k_1, k_2)$, $\Psi(n) = (n_1, n_2)$, and we write the Fourier transform using the group $\mathbf{Z}_2 \times \mathbf{Z}_3$, the corresponding entry will be $\frac{k_1 n_1}{2} + \frac{k_2 n_2}{3}$. The first rows and columns represent the indices of the entries. Figure 2.1 shows the details.

Note that the matrices can be obtained from each other by permutation of rows or columns. This shows also that if $f : \mathbf{Z}_2 \times \mathbf{Z}_3 \to \mathbb{C}$ then $\widehat{f} \circ \Psi \neq \widehat{f \circ \Psi}$, where the first Fourier tranform is taken using the group $\mathbf{Z}_2 \times \mathbf{Z}_3$ and the second Fourier tranform is using the group $\mathbf{Z}_6$. Indeed, for example take $f = \chi_{(0,2)}$. Then $f \circ \Psi = \chi_2$. For $\widehat{\chi}_2$ we use the first matrix and we have $\widehat{\chi}_2(1) = e^{2\pi i \frac{2}{6}}$ and for $\widehat{\chi}_{(0,2)}$ we use the second table and we have $\widehat{\chi}_{(0,2)}(\Psi(1)) = \widehat{\chi}_{(0,2)}(1,1) = e^{2\pi i \frac{4}{6}}$.

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	$\frac{1}{6}$	$\frac{2}{6}$	$\frac{3}{6}$	$\frac{4}{6}$	$\frac{5}{6}$
2	0	$\frac{2}{6}$	$\frac{4}{6}$	0	$\frac{2}{6}$	$\frac{4}{6}$
3	0	$\frac{3}{6}$	0	$\frac{3}{6}$	0	$\frac{3}{6}$
4	0	$\frac{4}{6}$	$\frac{2}{6}$	0	$\frac{4}{6}$	$\frac{2}{6}$
5	0	$\frac{5}{6}$	$\frac{4}{6}$	$\frac{3}{6}$	$\frac{2}{6}$	$\frac{1}{6}$

	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,0)	0	0	0	0	0	0
(1,1)	0	$\frac{5}{6}$	$\frac{4}{6}$	$\frac{3}{6}$	$\frac{2}{6}$	$\frac{1}{6}$
(0,2)	0	$\frac{4}{6}$	$\frac{2}{6}$	0	$\frac{4}{6}$	$\frac{2}{6}$
(1,0)	0	$\frac{3}{6}$	0	$\frac{3}{6}$	0	$\frac{3}{6}$
(0,1)	0	$\frac{2}{6}$	$\frac{4}{6}$	0	$\frac{2}{6}$	$\frac{4}{6}$
(1,2)	0	$\frac{1}{6}$	$\frac{2}{6}$	$\frac{3}{6}$	$\frac{4}{6}$	$\frac{5}{6}$

Figure 2.1: Indices of Entries

2.3 Cyclotomic Polynomials

Definition The *n-th cyclotomic polynomial* is

$$\Phi_n(x) = \prod \{(x-\omega) : \omega \text{ is a primitive } n\text{-}th \text{ root of 1 in } \mathbb{C}\} = \prod_{1 \le k \le n,\, k \text{ prime to } n} (x - e^{2\pi i \frac{k}{n}}).$$

By definition the cyclotomic polynomial $\Phi_n(x)$ is a polynomial over $\mathbb{C}$ but we will see that it actually has integer coefficients. It is clear that $\Phi_n(x)$ is a monic polynomial (i.e., is a polynomial

$c_n x^n + c_{n-1}x^{n-1} + \cdots + c_2 x^2 + c_1 x + c_0$ in which the leading coefficient c_n is equal to 1) of degree $\varphi(n)$ where φ is the Euler totient function that counts how many numbers k with $1 \leq k \leq n$ are relatively prime to n.

Note the factorization

$$x^n - 1 = \prod \{(x-\omega) : \omega \text{ is an } n\text{-}th \text{ root of } 1\} = \prod_{1 \leq k \leq n,\, k \text{ prime to } n} (x - e^{2\pi i \frac{k}{n}})$$

$$= \prod_{d|n} \prod \{(x-\omega) : \omega \text{ is a primitive } d\text{-}th \text{ root of } 1\} = \prod_{d|n} \Phi_d(x).$$

This relation can be used to compute $\Phi_n(x)$ recursively, by induction.

For example when $n = 1$, to make sure $d|n$, we have $d = 1$,so $\Phi_1(x) = x - 1$. When $n = 2$, then $d = 1, 2$, so $\Phi_1(x)\Phi_2(x) = x^2 - 1$ so $\Phi_2(x) = x + 1$. When $n = 3$, $d = 1, 3$, so $x^3 - 1 = \Phi_1(x)\Phi_3(x)$ so $\Phi_3(x) = x^2 + x + 1$. Similarly when $n = 4$, $d = 1, 2, 4$, then $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, etc.

Proposition 2.3.1 *For all n, the cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial with integer coefficients of degree $\varphi(n)$.*

Proof We just have to show that $\Phi_n(x)$ has integer coefficients. We will proceed by induction. When $n = 1$, we have $\Phi_1(x) = x - e^{2\pi i \frac{k}{1}}$(k is prime to 1) $= x - 1$. When $d < n$, fix $n > 1$ and let $f(x)$ be a monic polynomial with integer coefficients with

$$f(x) = \prod_{d|n, d<n} \Phi_d(x).$$

Then we have

$$\prod_{d|n} \Phi_d(x) = x^n - 1 = \Phi_n(x) \prod_{d|n, d<n} \Phi_d(x) = \Phi_n(x) f(x).$$

As $\prod_{d|n} \Phi_d(x)$ and $f(x)$ are both monic polynomial with integer coefficients, to show $\Phi_n(x)$ is also monic polynomial with integer coefficients, we will use the following lemma:

Lemma 2.3.2 *Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $Q(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$. Suppose $Q(x)$ and $P(x) \cdot Q(x)$ have integer coefficients. Then $P(x)$ has integer coefficients.*

Proof For convenience, let $a_n = 1$, $b_m = 1$ and $a_k = 0$ for $k > n$, $b_k = 0$ for $k > m$. We write the coefficients for $P(x) \cdot Q(x) = x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_0$:

$$c_{m+n-1} = a_n b_{m-1} + a_{n-1} b_m,$$

$$c_{m+n-2} = a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m,$$

$$\vdots$$

Suppose $P(x)$ does not have integer coefficients. Let k be the largest index such that a_k is not an integer. In the equations above, look at the first time a_k appears. let $n - l = k$, then $c_{m+n-l} = a_n b_{m-l} + a_{n-1} b_{m-l+1} + \cdots + a_{n-l} b_m$. As $b_m = 1$, we have $c_{m+k} = a_{k+l} b_{m-l} + a_{k+l-1} b_{m-l+1} + \cdots + a_k$. Because $i > k$ for $i \in \{k+1, \ldots, k+l\}$, so all the a_i's will be integers. Since all the c_i's and all the b_i's are integers, we have a_k must be integers. Therefore $P(x)$ has integer coefficients.■

By Lemma 2.3.2, $\Phi_n(x)$ has integer coefficients and it's a monic polynomial with integer coefficients of degree $\varphi(n)$.■

Definition For each $a \in \mathbf{Z}_N$, we define the equivalence class of a, denoted by $[a]$ to be the set

$[a] = \{x \in S | x \equiv y \bmod n\}$.

Lemma 2.3.3 *The following statements are equivalent:*

1. $\Phi_n(x)$ *is irreducible.*
2. *Let* ω *be a primitive* n*-th root of unity in* $\mathbb{C}$ *and let* f *be the minimal polynomial of* ω *over* **Q***, i.e., the monic polynomial over* **Q** *of lowest degree that has* ω *as a root. If* p *is a prime not dividing* n *then* ω^p *is a root of* f.
3. *Let* ω *be a primitive* n*-th root of unity in* $\mathbb{C}$ *and let* f *be a minimal polynomial of* ω *over* **Q***. If* r *is relatively prime to* n *then* ω^r *is a root of* f.

Proof (1) implies (2): Since $\Phi_n(x) = \prod\{(x - \omega) : \omega \text{ is a primitive } n\text{-}th \text{ root of } 1\}$, we have $\Phi_n(\omega) = 0$. As f is the minimal polynomial of ω over **Q**, it follows that $f(x)$ divides $\Phi_n(x)$. But since $\Phi_n(x)$ is irreducible, we get $\Phi_n(x) = f(x)$. If p is prime to n and $\omega = e^{2\pi i \frac{k}{n}}$, then $\omega^p = e^{2\pi i \frac{kp}{n}}$. As both k and p are prime to n, we have pk is prime to n and ω^p is a primitive n-th root of unity. So $f(\omega^p) = \Phi_n(\omega^p) = 0$.

(2) implies (3). Let r be relatively prime to n and r have a prime decomposition $r = p_1 p_2 \ldots, p_{k-1}$ containing only primes that do not divide n. As ω is a primitive n-th root of unity in $\mathbb{C}$ and f is the minimal polynomial of ω over **Q**, then applying (2) repeatedly, we obtain that $f(\omega^{p_1 p_2, \ldots, p_{k-1}}) = f(\omega^r) = 0$.

(3) implies (1): Since $\Phi_n(\omega) = 0$ it follows that $f(x)$ divides $\Phi_n(x)$. As $f(\omega^r) = f(e^{2\pi i \frac{rk}{n}}) = 0$, so $f(x)$ is divisible by $x - e^{2\pi i \frac{rk}{n}}$ for all r prime to n. So $f(x)$ is divisible by $\Phi_n(x)$. Therefore $\Phi_n(x) = f(x)$. If $f(x) = \Phi_n(x) = g(x)h(x)$ for some polynomials g, h of degree at least 1, then one of them, say g has ω as a root, which contradicts the minimality of f. Therefore $\Phi_n(x)$ is irreducible.■

Theorem 2.3.4 *(Fermat's Little Theorem) If p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p. In the notation of modular arithmetic, this is expressed as $a^p \equiv a \pmod{p}$. For example, if $a = 2$ and $p = 7$, $2^7 = 128$, and $128 - 2 = 7 \times 18$ is an integer multiple of 7. If a is not divisible by p, Theorem 2.3.4 is equivalent to the statement that $a^{p-1} - 1$ is an integer multiple of p: $a^{p-1} \equiv 1 \pmod{p}$. For example, if $a = 2$ and $p = 7$, $2^6 = 64$, and $64 - 1 = 63 = 7 \times 9$.*

Lemma 2.3.5 *(Gauss' lemma) A polynomial $P(x)$ is called primitive if the greatest common divisor of its coefficients is 1.*

1. *The product of primitive polynomials is primitive.*
2. *Let $P(x)$ be a polynomial over **Z**. Then $P(x)$ is irreducible over **Z** iff $P(x)$ is irreducible over **Q**.*

Proof (1) Let $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ be primitive polynomials and let $P(x) = f(x)g(x) = c_{n+m}x^{n+m} + \cdots + c_0$. We are going to show $P(x)$ is primitive. Let p be a prime number, then p cannot divide all the coefficients of $f(x)$. Let r be the largest number that p does not divide a_r. Similarly, let s be the largest number such that p does not divide b_s. We have

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j.$$

In this sum, we have the term $a_r b_s$ which is not divisible by p and for all the other terms either $i > r$ or $j > s$ so $a_i b_j$ is divisible by p. Therefore c_{r+s} is not divisible by p and, since p is an arbitrary prime, it follows that the greatest common divisor of the coefficients of $P(x)$ is 1. Therefore $P(x)$ is primitive.

(2) We will prove by contradiction. First we will show if $P(x)$ is irreducible over **Z**, then it is irreducible over Q. Suppose $P(x)$ is reducible over Q, $P(x) = f(x)g(x) = \frac{ac}{bd} f_1 g_1$. We can write $P(x) = eP_1(x)$, $f(x) = \frac{a}{b} f_1(x)$, $g(x) = \frac{c}{d} g_1(x)$ with P_1, f_1, g_1 primitive and $e \in$ **Z**, $a, b, c, d \in$ **Z**. Then $P(x) = eP_1(x) = \frac{ac}{bd} f_1 g_1$, by (1) we have $f_1(x)g_1(x)$ is primitive over **Z**. To show $P(x)$ is reducible over **Z**, we need to show $\frac{ac}{bd} = \pm e$ by the following lemma:

Lemma 2.3.6 *If $\frac{l}{n} P(x) = \frac{j}{k} Q(x)$ with $P(x)$ and $Q(x)$ primitive over **Z**, then $\frac{l}{n} = \frac{j}{k}$ or $\frac{l}{n} = -\frac{j}{k}$.*

Proof Let $P(x) = p_n x^n + \cdots + p_0$ and $Q(x) = q_n x^n + \cdots + q_0$. We have $\frac{lk}{nj} p_i = q_i$, for $i \in \{0, \ldots, n\}$. Since the greatest common divisor of the p_i's is 1, there exist numbers $m_0, \ldots, m_n$ such that $m_0 p_0 + \cdots + m_n p_n = 1$. Multiplying the previous equations by m_i and adding we obtain $\frac{lk}{jn} = q_0 m_0 + \cdots + q_n m_n \in$ **Z**. By symmetry we have also $\frac{jn}{lk} \in$ **Z**. Therefore $\frac{lk}{jn} \in \{1, -1\}$.■

As $e \in$ **Z** and can be written in $\frac{j}{k}$, so $P(x) = eP_1(x) = ef_1 g_1$ or $-ef_1 g_1$ which implies $P(x)$ is reducible over **Z**. By contradiction, $P(x)$ is irreducible over **Q** if $P(x)$ is irreducible over **Z**. Next we will show if $P(x)$ is irreducible over Q, then it is irreducible over **Z**. Suppose $P(x)$ is reducible over **Z**, let $p(x) = f(x)g(x)$ where $f, g \in$ **Z**, then $p(x) = f(x)g(x)$ where $f, g \in Q$ because every integer can be written in $\frac{a}{b}$ where $a, b \in$ **Z**. By contradiction, $P(x)$ is irreducible over **Z** if $P(x)$ is irreducible over **Q**.■

Theorem 2.3.7 *$\Phi_n(x)$ is irreducible over **Q**. It is the minimal polynomial of every primitive n-th root of unity.*

Proof Suppose $\Phi_n(x)$ is reducible that $\Phi_n(x) = f(x)g(x)$ with $f, g \in$ **Z**$[x]$ and f is irreducible. Let ω be a root of f in $\mathbb{C}$, thus ω is a root of Φ_n so it is a primitive n-th root of unity and f is the minimal polynomial of ω over **Q**. Let p be a prime not dividing n, if we can show ω^p is a root of f where p is a prime not dividing n, by Lemma 2.3.3, $\Phi_n(x)$ is irreducible over **Z**.

To show ω^p is a root of f, we will do by contradiction. Suppose ω^p is not a root of f. Then, as ω is a root of Φ_n and p is a prime,we have ω^p is a root of Φ_n. Therefore ω^p must be a root of g, or, equivalently ω is a root of $g(x^p)$. Then Φ_n divides $g(x^p)$. Since f is the minimal polynomial of Φ_n, it follows that f divides $g(x^p)$. If we reduce all the polynomials modulo p, then we get $\tilde{f}(x)$ divides $\tilde{g}(x^p)$. Next lemma will show that $\tilde{g}(x^p) = (\tilde{g}(x))^p$.

Lemma 2.3.8 *In* $\mathbf{Z}_p$ *we have* $(x+y)^p = x^p + y^p$. *This implies that* $\tilde{g}(x^p) = (\tilde{g}(x))^p$.

Proof $(x+y)^p = x^p + C_p^1 x^{p-1}y + \cdots + C_p^{p-1}xy^{p-1} + y^p$.The binomial coefficients are for $1 \leq k \leq p$:

$$\left(\begin{array}{c} p \\ k \end{array} \right) = \frac{(p-k)!}{k!} = \frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \ldots k}.$$

Since p is a prime and none of the terms in the denominator $(1 \ldots k)$ divides p except 1, however the numerator $(p(p-1)\ldots(p-k+1))$ divides p. So the binomial coefficients are divisible by p. Therefore in $\mathbf{Z}_p$ the only terms that remain in the binomial formula are $x^p + y^p$. Let $\tilde{g}(x) = a_0 + a_1 x + \cdots + a_n x^n$, then

$$\tilde{g}(x)^p = (a_0 + a_1 x + \cdots + a_n x^n)^p = a_0^p + a_1^p x^p + \cdots + a_n^p x^{np}$$

By Theorem 2.3.4, $a^p \equiv a \bmod p$, we have

$$\tilde{g}(x)^p = a_0^p + a_1^p x^p + \cdots + a_n^p x^{np} = a_0 + a_1 x^p + \cdots + a_n x^{np} = \tilde{g}(x^p)$$

. Therefore $\tilde{g}(x)^p = \tilde{g}(x^p)$.■

Returning to the proof of the theorem we obtain that $\tilde{f}$ divides $(\tilde{g}(x))^p$ which implies $\tilde{f}(x)$ and

$\tilde{g}(x)$ have a common factor $\tilde{f}_1$ with $deg(\tilde{f}_1) \geq 1$ over $\mathbf{Z}_p$. As $\Phi_n(x)$ divides $x^n - 1$ so

$$x^n - 1 = \tilde{f}(x)\tilde{g}(x) = \tilde{f}_1{}^2 \cdot \tilde{k}(x) \tag{2.4}$$

By derivation,

$$nx^{n-1} = 2\tilde{f}_1 \cdot \tilde{k}(x) + \tilde{f}_1{}^2 \cdot \tilde{k}'(x) = \tilde{f}_1(2\tilde{k}(x) + \tilde{f}_1 \cdot \tilde{k}'(x)) \tag{2.5}$$

Therefore $\tilde{f}_1|(x^n - 1)$ and $\tilde{f}_1|(nx^{n-1})$. Then $\tilde{f}_1|(n(x^n - 1))$ and $\tilde{f}_1|(nx^{n-1}x)$, subtract each other we get $\tilde{f}_1|n$. This shows $\tilde{f}_1$ is a constant polynomial, which contradicts that $deg(\tilde{f}_1) \geq 1$. Hence ω^p is a root of f, Lemma 2.3.3 implies $\Phi_n(x)$ is the minimal polynomial of $\Phi_n(\omega) = 0$ and $\Phi_n(x)$ is irreducible over **Z**. By Lemma 2.3.5 (2) we get that $\Phi_n(x)$ is irreducible over Q.■

Proposition 2.3.9 *Let p be a prime.*

1. *A polynomial $P(x) \in \boldsymbol{Z}[x]$ is divisible by $\Phi_s(x)$ if and only if $P(\omega) = 0$ for a primitive s-th root of unity ω.*

2. $1 + x + \cdots + x^{s-1} = \prod_{t>1, t|s} \Phi_t(x)$.

3. $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$ *and* $\Phi_{p^{\alpha+1}}(x) = \Phi_p(x^{p^\alpha})$.

4. $$\Phi_s(1) = \begin{cases} 0 & \text{if } s = 1 \\ q & \text{if } s \text{ is a power of a prime } q \\ 1 & \text{otherwise.} \end{cases}$$

5. $$\Phi_s(x^p) = \begin{cases} \Phi_{ps}(x) & \text{if } p \text{ is a factor of } s \\ \Phi_s(x)\Phi_{ps}(x) & \text{if } p \text{ is not a factor } s. \end{cases}$$

6. *If s and t are relatively prime, then $\Phi_s(x^t) = \prod_{r|t} \Phi_{rs}(x)$.*

7. *If $\bar{A}(x)$ is an integer polynomial and $A(x) = \bar{A}(x^p)$, then*

$$\{t : \Phi_t(x) \textit{ divides } A(x)\} = \{s' : \Phi_s(x) \textit{ divides } \bar{A}(x)\} \cup \{ps : \Phi_s(x) \textit{ divides } \bar{A}(x)\}$$

where $s' = ps$ or s according to p is or is not a factor of s.

Proof (1) First let's show if $P(\omega) = 0$ for a primitive $s\text{-}th$ root of unity ω, then $P(x)$ is divisible by $\Phi_s(x)$. Let $P(x) = Q(x)\Phi_s(x) + R(x)$ where $Q(x)$ and $R(x)$ have integer coefficients with $deg(R) < deg(\Phi_s)$. As $P(\omega) = 0$, it follows $Q(\omega)\Phi_s(\omega) + R(\omega) = 0$. As $\Phi_s(\omega) = 0$, it follows $R(\omega) = 0$, so by minimal polynomial, $R(x) = 0$ and $P(x) = Q(x)\Phi_s(x)$, which indicates $P(x)$ is divisible by $\Phi_s(x)$. Next we will show if $P(x)$ is divisible by $\Phi_s(x)$, then $P(\omega) = 0$ for a primitive $s\text{-}th$ root of unity ω. Since $P(x)$ is divisible by $\Phi_s(x)$, we have $P(x) = Q(x)\Phi_s(x)$ and $P(\omega) = Q(\omega)\Phi_s(\omega)$. As $\Phi_s(\omega) = 0$, it follows $P(\omega) = 0$.

(2) As we know $\prod_{t|s} \Phi_t(x) = x^s - 1 = (x-1)(1 + x + \cdots + x^{s-1})$ and $\Phi_1(x) = x - 1$, then $\prod_{t>1,t|s} \Phi_t(x) = \frac{\prod_{t|s} \Phi_t(x)}{\Phi_1(x)} = (1 + x + \cdots + x^{s-1})$

(3) As $\prod_{d|p} \Phi_d(x) = x^p - 1$ where p is a prime, then $\prod_{d|p} \Phi_d(x) = \Phi_1(x)\Phi_p(x)$. As $\Phi_1(x) = x - 1$ so $\Phi_p(x) = \frac{x^p-1}{x-1} = 1 + x + \cdots + x^{n-1}$. To prove $\Phi_{p^{\alpha+1}}(x) = \Phi_p(x^{p^\alpha})$ we have $\Phi_1(x)\prod_1^{\alpha+1} \Phi_{p^k}(x) = \prod_{s|p^{\alpha+1}} \Phi_s(x) = x^{p^{\alpha+1}} - 1 = (x-1)(x^{p^{\alpha+1}-1} + \cdots + x + 1)$ where $\Phi_1(x) = x - 1$, so $1 + x + \cdots + x^{p^{\alpha+1}-1} = \prod_1^{\alpha+1} \Phi_{p^k}(x) = \Phi_p(x)\Phi_{p^2}(x)\ldots\Phi_{p^\alpha}(x)\Phi_{p^{\alpha+1}}(x)$ so

$$\Phi_{p^{\alpha+1}}(x) = \frac{1 + x + \cdots + x^{p^{\alpha+1}-1}}{\Phi_p(x)\Phi_{p^2}(x)\ldots\Phi_{p^\alpha}(x)} = \frac{1 + x + \cdots + x^{p^{\alpha+1}-1}}{1 + x + \cdots + x^{p^\alpha-1}}$$

$$= \frac{(1 + x^{p^\alpha} + x^{2p^\alpha} + \cdots + x^{(p-1)p^\alpha})(1 + x + \cdots + x^{p^\alpha-1})}{1 + x + \cdots + x^{p^\alpha-1}} = 1 + x^{p^\alpha} + x^{2p^\alpha} + \cdots + x^{(p-1)p^\alpha} = \Phi_p(x^{p^\alpha})$$

.

(4) When $s = 1$, $\Phi_1(x) = x - 1$ and $\Phi_1(1) = 1 - 1 = 0$. When s is a power of a prime q, $\Phi_q(1) = 1 + 1 + \cdots + 1^{q-1} = q$ and according to (3), $\Phi_{q^s}(1) = \Phi_q(1^{q^{s-1}}) = \Phi_q(1) = q$. When s is otherwise, or has at least two primes in its decomposition, we proceed by induction on the length of the prime decomposition. From (2), letting $x = 1$ we have $s = \prod_{t>1,t|s} \Phi_t(1) = \Phi_s(1) \prod_{t= \text{ prime power},t|s} \Phi_t(1) \prod_{t= \text{ a product of at least two primes},t|s} \Phi_t(1)$.

Suppose all the other t's have a shorter prime decomposition that $\Phi_t(1) = 1$, then

$$\prod_{t= \text{ a product of at least two primes},t|s} \Phi_t(1) = 1.$$

Let s have a prime decomposition that $s = p_1^{r_1} \dots p_n^{r_n}$, so

$$\prod_{t= \text{ prime power},t|s} \Phi_t(1) = \prod_{j=1}^{n} \prod_{l=1}^{r_j} \Phi_{p_j^l}(1) = \prod_{j=1}^{n} \prod_{l=1}^{r_j} p_j^l = \prod_{j=1}^{n} p_j^{r_j} = s.$$

Therefore the product is $s\Phi_s(1) = s$ and $\Phi_s(1) = 1$.

(5) As ω is the root of $\Phi_s(x)$, then $\omega^{1/p} = e^{2\pi i \frac{k}{s} \frac{1}{p}}$ is the root of $\Phi_s(x^p)$ where k is relatively prime to s and $e^{2\pi i \frac{k}{ps}}$ is the root of $\Phi_{ps}(x)$ where k is relatively prime to ps. If p is a factor of s, then k is relatively prime to ps which indicates $\omega^{1/p} = e^{2\pi i \frac{k}{ps}}$ is the root of $\Phi_{ps}(x)$. Therefore $\Phi_s(x^p) = \Phi_{ps}(x)$.

If p is not a factor of s, then we have two cases: either k is prime to ps or k is a multiple of p, $k = pr$ with r prime to s. If k is prime to ps, we have the above result as $\Phi_s(x^p) = \Phi_{ps}(x)$; If k is a multiple of p, then k is prime to s which implies $e^{2\pi i \frac{k}{s}}$ is the root of $\Phi_s(x)$ and r prime to s which indicates $(e^{2\pi i \frac{r}{s}})^p$ is the root of $\Phi_s(x^p)$. Hence $\Phi_s(x^p) = \Phi_s(x)$ and $\Phi_s(x^p)$ has the same roots as $\Phi_s(x)\Phi_{ps}(x)$.

(6) Let $t = p_1 \dots p_m p_{m+1}$ where some of the primes can be repeated. We have from (5), since t and s are relatively prime:

$$\Phi_s(x^t) = \Phi_s(x^{p_1 \cdots p_{m+1}}) = \Phi_s\left((x^{p_1 \cdots p_m})^{p_{m+1}}\right) = \Phi_s(x^{p_1 \cdots p_m}) \Phi_{p_{m+1}s}(x^{p_1 \cdots p_m})$$

$$= \prod_{r|p_1 \dots p_m} \Phi_{rs}(x) \prod_{r|p_1 \dots p_m} \Phi_{r p_{m+1} s}(x) = \prod_{r|p_1 \dots p_{m+1}} \Phi_{rs}(x) = \prod_{r|t} \Phi_{rs}(x)$$

.

(7) First we will show if $\Phi_t(x)$ divides $A(x)$, then $t = s$ or ps and $\Phi_s(x)$ divides $\bar{A}(x^p)$. Let $\omega = e^{2\pi i/t}$, then $\omega^p = e^{2\pi i \frac{p}{t}} = e^{2\pi i \frac{k}{s}}$ is a primitive s-th root of unity for some s. From (5), if p is a factor of s and $\Phi_s(x^p) = \Phi_{ps}(x)$, then $\Phi_{ps}(\omega) = 0$ and since $\Phi_t(\omega) = 0$ it follows that $t = ps = s'$, so $t \in \{s', ps\} = \{ps\}$. If p is not a factor of s then $\Phi_s(\omega) = 0$ or $\Phi_{ps}(\omega) = 0$ so $t \in = \{s', ps\}\{s, ps\}$. As $\Phi_t(x)|A(x)$, we have $A(\omega_t) = 0$ and $\bar{A}(\omega_t^p) = 0$ where $\omega_t^p = e^{2\pi i \frac{k}{s}}$. Hence $\Phi_s(x)|\bar{A}(x)$.

Next we will show if $\Phi_s(x)$ divides $\bar{A}(x)$ then $\Phi_t(x)$ divides $A(x)$ for $s = t$ or $ps = t$. Let $\omega = e^{2\pi i/s}$ and s be such that $\Phi_s(x)|\bar{A}(x)$, then $\bar{A}(\omega) = \bar{A}(e^{2\pi i/s}) = 0$. Therefore $A(e^{2\pi i/ps}) = 0$ implies $\bar{A}(e^{2\pi ip/ps}) = 0$. If p is a factor of s, we have $\Phi_{ps}(e^{2\pi i/ps})|A(e^{2\pi i/ps})$ and $ps = \{t : \Phi_t(x)|A(x)\}$. Hence $\Phi_t(x)|A(x)$. If p is not a factor of s, then $e^{2\pi ip/s}$ is a primitive s-th root of 1. As $\Phi_s(x)|\bar{A}(x)$ and $\Phi_s(\omega) = 0$, we have $\Phi_s(\omega^p) = 0$ and $\bar{A}(\omega^p) = A(e^{2\pi ip/s}) = 0$. Therefore $A(e^{2\pi i/s}) = 0$ and $\Phi_s(x)|A(x)$ which implies $s = t : \{t : \Phi_t(x)|A(x)\}$. Hence the statement follows.■

CHAPTER 3: TILING RESULT

3.1 Basic Properties

Definition Let $G = (G, +)$ be a finite additive group, A *tiling pair* is a pair of non-empty subsets A, B such that every element of G can be written in exactly one way as a sum of an element of a of A and an element of b of B, in which case we can write $G = A \oplus B$. The sets A, B are then called *tiles*, with B be a *complementary tile* to A and vice versa.

Let $A \oplus B = \mathbf{Z}_N$ be a tiling pair for a cyclic group $\mathbf{Z}_N$ of cyclic order. Observe that the relationship $A \oplus B = \mathbf{Z}_N$ can be rewritten as $1_A * 1_B = 1$ where $1_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$ Then it is obvious for the cardinality identity

$$|A||B| = N \tag{3.1}$$

In particular, $|A|$ and $|B|$ are divisors of N, and thus are products of disjoint sets of prime factors of N.

For A and B sets or multi-sets of integers, we denote the multi-set $\{a + b : a \in A, b \in B\}$ by $A + B$. We write $A \oplus B$ when every element can be expressed uniquely $a + b$. For k an integer, we write kA for $\{ka : a \in A\}$, we call $\{k\} \oplus A$ as a *translate* of A, and when k is a factor of every $a \in A$, we write A/k for $\{a/k : a \in A\}$.

Proposition 3.1.1 *Suppose N be a positive integer and A, B are multi-sets of nonnegative integers. Let $A(x) = \sum_{a \in A} x^a$, we have $\#A = A(1)$. The following statements are equivalent:*

1. $A \oplus (B \oplus N\mathbf{Z}) = \mathbf{Z}$.

2. *$A \oplus B$ is a complete set of representatives of $\mathbf{Z}_N$; in other words $A \oplus B = \mathbf{Z}_N$, where addition is understood modulo N.*

3. $A(x)B(x) \equiv 1 + x + \cdots + x^{N-1} \mod (x^N - 1)$.

4. *$A(1)B(1) = N$ and for every factor $t > 1$ of N, the cyclotomic polynomial $\Phi_t(x)$ divides $A(x)$ or $B(x)$.*

Proof (1) implies (2) is trivial. As $A \oplus (B \oplus N\mathbf{Z}) = (A \oplus B) \oplus N\mathbf{Z} = \mathbf{Z}$, so $A \oplus B$ is the complete set of all the elements modulo $\mathbf{Z}_N$ which means $A \oplus B$ is a complete set of representatives of $\mathbf{Z}_N$.

(2) implies (3). For every $k \in \{0, \ldots, N-1\}$ there exists a unique $a_k \in A$, $b_k \in B$ and $m_k \in \mathbf{Z}$ such that $k = a_k + b_k + Nm_k$. Since $x^N \equiv 1 \mod (x^N - 1)$, by induction $x^{mN} - 1 = (x^N - 1)(x^{(m-1)N} + x^{(m-2)N} + \cdots + 1)$, so $x^{mN} \equiv 1 \mod (x^N - 1)$ we have

$$A(x)B(x) = \sum_{a \in A, b \in B} x^{a+b} \equiv \sum_{k=0}^{N-1} x^{a_k + b_k + Nm_k} \mod (x^N - 1) = \sum_{k=0}^{N-1} x^k.$$

Therefore $A(x)B(x) \equiv \sum_{k=0}^{N-1} x^k \mod (x^N - 1)$.

(3) implies (4). From (3) we have $A(x)B(x) = p(x)(x^N - 1) + (1 + x + \cdots + x^{N-1})$ for some integer polynomial $p(x)$. Then $A(1)B(1) = p(1)(1^N - 1) + (1 + 1 + \cdots + 1^{N-1}) = 1 + 1 + \cdots + 1^{N-1} = N$. For every factor $t > 1$ of N, the cyclotomic polynomial $\Phi_t(x)$ divides $1 + x + \cdots + x^{N-1}$. Since $\Phi_t(x)$ is irreducible it must divide either $A(x)$ or $B(x)$.

(4) implies (3). The hypothesis implies that $A(x)B(x)$ is divisible by the product of all $\Phi_t(x)$ with $t > 1$ factor of N. So it is divisible by $1 + x + \cdots + x^{N-1}$. We have also $A(x)B(x) = p(x)(x^N - 1) + q(x)$ for some integer polynomials $p(x), q(x)$ with $\deg(q) < N$. Since $q(x)$ has to be divisible by $1 + x + \cdots + x^{N-1}$ it follows that $q(x) = c(1 + x + \cdots + x^{N-1})$ where c is constant. Since $A(1)B(1) = q(1) = N$, we have $N = q(1) = c(1 + 1 + \cdots + 1^{N-1}) = cN$, which implies

$c = 1$ and $q(x) = 1 + x + \cdots + x^{N-1}$. Hence $A(x)B(x) - (1 + x + \cdots + x^{N-1}) = p(x)(x^N - 1)$ and $A(x)B(x) \equiv 1 + x + \cdots + x^{N-1} \mod (x^N - 1)$.

(3) implies (2). We have

$$1 + x + \cdots + x^{N-1} \equiv A(x)B(x) = \sum_{a \in A, b \in B} x^{a+b} \equiv \sum_{a \in A, b \in B} x^{a+b \mod N} \mod (x^N - 1).$$

This implies that $A \oplus B = \mathbf{Z}_N$.■

Remark For a subset of $\mathbf{Z}_N$, the Fourier transform of the characteristic function of A is related to the polynomial $A(x)$ that corresponds to A by the formula

$$\widehat{1}_A(k) = \frac{1}{\sqrt{N}} A(e^{2\pi i \frac{k}{N}}), \quad (k \in \mathbf{Z}_N). \tag{3.2}$$

So $\widehat{1}_A(k) = 0$ if and only if $A(e^{2\pi i \frac{k}{N}}) = 0$. If $e^{2\pi i \frac{k}{N}}$ is a primitive s-th root of unity, which means that $\frac{k}{N} = \frac{l}{s}$ with l and s co-prime, then $\widehat{1}_A(k) = 0$ if and only if the cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$.

For A, B, which $A \oplus B = \mathbf{Z}_N$, there is a physical space separation property

$$(A - A) \cap (B - B) = \{0\} \tag{3.3}$$

If two non-empty subsets A, B of $\mathbf{Z}_N$ obey both 3.1 and 3.3, then they must be a tiling pair, since the sums in $A + B$ are disjoint and have the same cardinality as $\mathbf{Z}_N$.

Now we use Fourier analysis to get more structural information. As $1_A * 1_B = 1$, we have $\widehat{1_A * 1_B} = \hat{1}$ where $\hat{1}(n) = \frac{1}{\sqrt{N}} \sum_{k \in \mathbf{Z}_N} 1(k) e^{2\pi i \frac{kn}{N}} = \begin{cases} \frac{N}{\sqrt{N}} & n = 0 \\ 0 & otherwise \end{cases}$ Therefore $\widehat{1_A * 1_B} = \frac{1}{\sqrt{N}} \hat{1}_A \hat{1}_B =$

$$\hat{1}(n) = \begin{cases} \sqrt{N} & n = 0 \\ 0 & otherwise \end{cases}$$

Hence $\hat{1}_A(k)\hat{1}_B(k) = N1_{k=0}$. Note that when $k = 0$,this case of identity is (3.1). The remaining cases of this identity can be reformulated equivalently as a frequency space separation property

$$supp(\hat{1}_A) \cap supp(\hat{1}_B) = \{0\} \tag{3.4}$$

where supp$(\hat{1}_A) := \{k \in \mathbf{Z}_N : \hat{1}_A(k) \neq 0\}$ is the support of $\hat{1}_A$. Conversely, if A, B obey both (3.4) and (3.1), then the above argument shows that $A \oplus B = \mathbf{Z}_N$.

Proposition 3.1.2 *The following statements are equivalent*

1. $A \oplus B = \mathbf{Z}_N$.
2. $1_A * 1_B = 1$ *(in* $\mathbf{Z}_N$*).*
3. $|A| \cdot |B| = N$ *and* $(A - A) \cap (B - B) = \{0\}$.
4. $|A| \cdot |B| = N$ *and the supports of the Fourier transforms satisfies the following relation* $\operatorname{supp} \widehat{1}_A \cap \operatorname{supp} \widehat{1}_B = \{0\}$.

Proof (2) is just a reformulation of (1).

(1) implies (3). Since $A \oplus B = \mathbf{Z}_N$ it follows that $|A| \cdot |B| = N$. To show $(A-A) \cap (B-B) = \{0\}$, we will do by contradiction. Suppose $(A-A) \cap (B-B) = \{k\}$, so $k \in A-A$ and $k \in B-B$ and there exists $a, a' \in A$ and $b, b' \in B$ such that $k = a - a' = b - b'$. This implies $a - a' = b - b'$ then $a + b' = a' + b$ so $a = a'$ and $b = b'$ with $k = a - a' = b - b' = 0$. Therefore $(A-A) \cap (B-B) = \{0\}$.

(3) implies (1). The map from $A \times B$ to $\mathbf{Z}_N$ defined by $(a, b) = a + b$ can be checked to be one-to-one from the hypothesis. Since the two sets have the same cardinality N, it follows that this map is also onto. This implies (1).

(2) implies (4). As $|A| \cdot |B| = N$ is obvious so we only need to show $\operatorname{supp} \widehat{1}_A \cap \operatorname{supp} \widehat{1}_B = \{0\}$. We will show by contradiction. Suppose $\operatorname{supp} \widehat{1}_A \cap \operatorname{supp} \widehat{1}_B = \{k\}$. By the definition of $\operatorname{supp} \widehat{1}_A$ we have $\widehat{1}_A(k) \neq 0 \neq \widehat{1}_B(k)$. This implies $\widehat{1}_A(k)\widehat{1}_B(k) \neq 0$. By Fourier transform and we obtained $\widehat{1}_A(k)\widehat{1}_B(k) = N1_{k=0}$, so $\widehat{1}_A(k)\widehat{1}_B(k) = N1_{k=0} \neq 0$ which implies $k = 0$. This gives $\operatorname{supp} \widehat{1}_A \cap \operatorname{supp} \widehat{1}_B = \{0\}$.

(4) implies (2). From the hypothesis we get that $\widehat{1}_A(k)\widehat{1}_B(k) = N1_{k=1}$. Taking the inverse of the Fourier transform , we get that $\sqrt{N}\widehat{1_A * 1_B} = \widehat{1}_A(k)\widehat{1}_B(k) = N1_{k=0} = N\frac{1}{\sqrt{N}}\widehat{1}$. Therefore $1_A * 1_B = 1$ (in $\mathbf{Z}_N$).■

Definition Let us call two elements a, b of $\mathbf{Z}_N$ *equivalent* if one has $a = mb$ for some m co-prime to N (or equivalently, if $(a, N) = (b, N)$).

Lemma 3.1.3 *$supp(\hat{1}_A)$ and $supp(\hat{1}_B)$ are unions of equivalence classes, with $\{0\}$ being the only equivalence class in common.*

Proof First we will show $supp(\hat{1}_A)$ and $supp(\hat{1}_B)$ are unions of equivalence classes. As $supp(\hat{1}_A) := \{k \in \mathbf{Z}_N : \hat{1}_A(k) \neq 0\}$, if we can find some m is co-prime to N such that $k = mk_1$, where $k_1 \in \mathbf{Z}_N$ and $(k, N) = (k_1, N)$, then to show $supp(\hat{1}_A)$ is the union of equivalence class, we only need to show that $\hat{1}_A(k) \neq 0$ if and only if $\hat{1}_A(km) \neq 0$. To show $\hat{1}_A(k) \neq 0$ if and only if $\hat{1}_A(km) \neq 0$, we will show $\hat{1}_A(k) = 0$ if and only if $\hat{1}_A(km) = 0$.

First we will show if $\hat{1}_A(k) = 0$, then $\hat{1}_A(mk) = 0$. Let $\omega = e^{2\pi i/n}$, since $\hat{1}_A(k) = \frac{1}{\sqrt{N}} \sum_{a \in A} \omega^{ka} = \frac{1}{\sqrt{N}} \sum_{a \in A} e^{2\pi i \frac{ka}{n}} = 0$, we have $A(e^{2\pi i \frac{k}{n}}) = 0$. Suppose $e^{2\pi i \frac{k}{n}}$ is primitive s-th root of 1 and $\frac{k}{n} = \frac{l}{s}$

where l, s are coprime. Then $\frac{km}{n} = \frac{lm}{s}$ where lm and s are coprime. Hence $\Phi_s(e^{2\pi i\frac{lm}{s}}) = 0$ and $\Phi_s(x)|A(x)$ imply $A(e^{2\pi i\frac{lm}{s}}) = 0$, then $\frac{1}{\sqrt{N}}\sum_{a\in A} e^{2\pi i\frac{lma}{s}} = 0$ implies $\frac{1}{\sqrt{N}}\sum_{a\in A} e^{2\pi i\frac{kma}{n}}$. Hence $\hat{1}_A(km) = 0$.

Next we will show if $\hat{1}_A(mk) = 0$, then $\hat{1}_A(k) = 0$. Let m, N be coprime, then m is invertible in $\mathbf{Z}_N$, so there exists a $l \in \mathbf{Z}_N$ such that $ml = 1$ mod N. Since $\hat{1}_A(km) = 0$ implies $\hat{1}_A(klm) = 0$, we have $\hat{1}_A(k) = 0$. it is the same to show $supp(\hat{1}_B)$ is unions of equivalence classes.

Second we will show $\operatorname{supp}\widehat{1}_A \cap \operatorname{supp}\widehat{1}_B = \{0\}$. By Proposition 3.1.2, the statement follows.■

Remark One can also obtain the above lemma from the theory of cyclotomic polynomials and unique factorisation, noting that the product of the generating polynomials $\sum_{n\in A} z^n$ and $\sum_{n\in B} z^n$ form a multiple of $(z^N - 1)/(z - 1) = \prod_{k|N} \Phi_k(z)$, and that each cyclotomic polynomial Φ_k is irreducible and has zeroes corresponding to a single equivalence class in $\mathbf{Z}_N$.

Corollary 3.1.4 *(strong physical space separation) The sets $(A - A) \setminus \{0\}$ and $(B - B) \setminus \{0\}$ lie in disjoint equivalence classes; thus any non-zero equivalence class may contain an element of $A - A$ or an element of $B - B$, but not both.*

Proof We will prove this by contradiction. Suppose any non-zero equivalence classes may contain an element of $A - A$ and $B - B$, let x be this non-zero element, so $x \in A - A$ and $x \in B - B$. As we know $(A - A) \cap (B - B) = \{0\}$, so $x \in \{0\}$ which contradicts that x is non-zero. Therefore any non-zero equivalence classes may contain an element of $A - A$ or $B - B$, but not both.■

Theorem 3.1.5 *[6, 2] Every tiling of $\mathbf{Z}$ by translates of a finite set is periodic, i.e., if A is a finite set and $A \oplus C = \mathbf{Z}$, then there exists a finite set B such that $C = B \oplus N\mathbf{Z}$, where $N = |A| \cdot |B|$.*

Proof Let $A := \{a_1, a_2, \ldots, a_k\}$ with $a_1 < a_2 < \cdots < a_k$. Consider the characteristic function 1_C (i,e, $l_C : x \to \{0, 1\}$ where $C \subset x$ and $1 \in C$, $0 \in x - C$)of the set C. We will prove that it is periodic.

Since $A \oplus C = \mathbf{Z}$, for each $n \in \mathbf{Z}$ there exists exactly one $j \in \{1, \ldots, k\}$ such that $n - a_j \in C$. This means that

$$1_C(n - a_1) + \cdots + 1_C(n - a_k) = 1 \text{ for all } n \in \mathbf{Z}. \tag{3.5}$$

Let $\tau := a_k - a_1$. Consider the τ-tuple

$$c_n := (1_C(n + 1), 1_C(n + 2), \ldots, 1_C(n + \tau)) \in \{0, 1\}^\tau.$$

We will prove that a c_n for some fixed n completely determines the function 1_C. We will do this by induction: we prove that c_n determines c_{n+1} and c_{n-1}. For this we have to prove that $1_C(n+\tau+1)$ and $1_C(n)$ are completely determined by c_n.

Take $m := a_1 + n + \tau + 1$. We have $n + \tau + 1 = m - a_1 > m - a_2 > \cdots > m - a_k = n + 1$. From (3.5) we have

$$1_C(n + \tau + 1) = 1 - \sum_{j=2}^{k} 1_C(m - a_j),$$

but all the numbers on the right appear in c_n, therefore $1_C(n + \tau + 1)$ is completely determined by c_n.

Now take $m = a_k + n$. We have $n + \tau = m - a_1 > m - a_2 > \cdots > m - a_k = n$. From (3.5) we have

$$1_C(n) = 1 - \sum_{j=1}^{k-1} 1_C(m - a_j),$$

but all the numbers on the right appear in c_n, therefore $1_C(n)$ is completely determined by c_n.

Since $c_n \in \{0,1\}^\tau$ for all n, and $|\{0,1\}^\tau| = 2^\tau$, there exist $n_1, n_2 \in \mathbf{Z}$ such that $0 < n = n_2 - n_1 \leq 2^\tau$ such that $c_{n_1} = c_{n_2}$. But then, by the argument above, $1_C(n_1 + k) = 1_C(n_2 + k)$ for all $k \in \mathbf{Z}$, which means that $1_C(k) = 1_C(n + k)$ for all $k \in \mathbf{Z}$, so $k \in C$ if and only if $k + n \in C$. Let $B = C \cap \{0, \ldots, N-1\}$. We have $C = B \oplus N\mathbf{Z}$ and this proves the theorem.

3.2 Tijdeman's Theorem

Lemma 3.2.1 *Let A and B be finite sets of nonnegative integers with corresponding polynomials $A(x)$ and $B(x)$ and let $N = A(1)B(1)$. If*

$$A(x)B(x) \equiv 1 + x + ... + x^{N-1} \mod (x^N - 1)$$

and p is a prime which is not a factor of A(1), then

$$A(x^p)B(x) \equiv 1 + x + ... + x^{N-1} \mod (x^N - 1).$$

Proof Since p is prime, $A(x^p) \equiv (A(x))^p$ (mod p), i.e., when the coefficients are reduced modulo p. Let $G_N(x) = 1 + x + ... + x^{N-1}$. Then

$$A(x^p)B(x) \equiv (A(x))^{p-1}A(x)B(x) = (A(x))^{p-1}G_N(x),$$

where $\equiv$ means the exponents are reduced modulo n and then the coefficients are reduced modulo p. Every $x^i G_N(x) \equiv G_N(x)$ mod $(x^n - 1)$ for $i \in N$, so

$$(a_0 + a_1 x + \cdots + a_k x^k)G_N(x) \equiv (a_0 + a_1 + \cdots + a_k)G_N(x) \text{ mod } (x^N - 1)$$

then

$$(A(x))^{p-1}G_n(x) \equiv (A(1))^{p-1}G_N(x) \bmod (x^N - 1).$$

By Theorem 2.3.4,$(A(1))^{p-1} \equiv 1$ (mod p). Therefore $A(x^p)B(x) \equiv G_N(x)$. Both $A(x^p)B(x)$ and $G_n(x)$ have nonnegative coefficients whose sum is n since $A(1)B(1) = G_n(1) = n$. Consider the following reductions.

$(R1)$ $A(x^p)B(x)$ is reduced modulo $x^n - 1$, yielding a polynomial $G^*(x)$.

$(R2)$ The coefficients of $G^*(x)$ are reduced modulo p, yielding $G_n(x)$.

$(R1)$ preserves the sum of the coefficients, but $(R2)$ reduces the sum by some nonnegative multiple of p. Because the sum of the coefficients of both $G^*(x)$ and $G_n(x)$ are n, that multiple is 0. Therefore $G^*(x) = G_n(x)$.■

Theorem 3.2.2 *(Tijdeman's Theorem) Suppose that A is finite, $0 \in A \cap C$, and $A \oplus C = \mathbf{Z}$. If r and $\#A$ are relatively prime, then $rA \oplus C = \mathbf{Z}$.*

Proof Let r have a prime decomposition such that $r = p_1 \dots p_k$ where p_i for $i \in \{1 \dots k\}$ does not divide $\#A$. By Theorem 3.1.5 $C = B + N\mathbf{Z}$ and $A \oplus B = \mathbf{Z}_N$, then by Proposition 3.1.2 we have $A(x)B(x) \equiv 1+x+\cdots+x^{N-1} \mod (x^N-1)$ and by Lemma 3.2.1 we have $A(x^{p_1})B(x) \equiv 1 + x + ... + x^{N-1} \mod (x^N - 1)$ where p_1 is a prime which is not a factor of $\#A$. Apply Lemma 3.2.1 repeatedly, we have $A(x^{p_1 \cdots p_k})B(x) \equiv 1 + x + ... + x^{N-1} \mod (x^N - 1)$ where $p_1 \dots p_k$ is prime which is not a factor of $\#A$. Therefore $A(x^r)B(x) \equiv 1 + x + ... + x^{n-1} \mod (x^n - 1)$. As $A(x^r) = (rA)(x)$ and by Proposition 3.1.2 we get $rA \oplus B = \mathbf{Z}_N$. Apply Proposition 3.1.2 again we have $rA \oplus (B \oplus N\mathbf{Z}) = \mathbf{Z}$ and $rA \oplus C = \mathbf{Z}$.■

Conjecture 3.2.3 *(Tijdeman-Sands conjecture) Let $A \oplus B = \mathbf{Z}_N$ be a tiling of a square-free cyclic group V_p, then at least one of A or B is contained in a coset of a proper subgroup of $\mathbf{Z}_N$.*

The following Corollary is the alternative proof of 3.2.2 for the case m is co-prime with N.

Corollary 3.2.4 *(Dilation invariance) Let $A \oplus B = \mathbf{Z}_N$ for some N. If m is an integer co-prime to N, then $A \oplus mB = \mathbf{Z}_N$, where $mB := \{mb : b \in B\}$ is the dilation of B by m.*

Proof From Lemma 3.1.3, we know that $supp(\hat{1}_B)$ is a union of equivalence classes, if m is an integer co-prime to N then $supp(\hat{1}_B) = supp(\hat{1}_{mB})$. As $A \oplus B = \mathbf{Z}_N$, we know $|A||B| = N$ and $supp(\hat{1}_A) \cap supp(\hat{1}_B) = \{0\}$. As $mB := \{mb : b \in B\}$, so mB is also a divisor of N and $|A||mB| = N$. Since $supp(\hat{1}_B) = supp(\hat{1}_{mB})$, we get that $supp(\hat{1}_A) \cap supp(\hat{1}_B) = \{0\}$, therefore by Proposition 3.1.2 $A \oplus mB = \mathbf{Z}_N$.■

Lemma 3.2.5 *If a finite set A tiles the integers, then there is a tiling by A whose period is a product of powers of the prime factors of $\#A$.*

Proof If $A \oplus C = \mathbf{Z}$ is a tiling of period n and $r > 1$ is a factor of n relatively prime to $\#A$, then by Theorem 3.2.2, $rA \oplus C = \mathbf{Z}$. Therefore $rA \oplus C_0 = r\mathbf{Z}$, where $C_0 = \{c \in C : c \equiv 0 \text{ (mod r)}\}$, and hence $A \oplus C_0/r = \mathbf{Z}$ is a tiling of period n/r.■

Lemma 3.2.6 *Let A and B be finite, $A, B \neq \{0\}$, and $A \oplus B$ a complete set of residues modulo $(\#A)(\#B)$. Then at least one of the following is true.*

1. *No number of $A - A$ is relatively prime to $\#B$.*
2. *No number of $B - B$ is relatively prime to $\#A$.*

Proof We will prove by contradiction. Let $N = (\#A)(\#B)$. By Proposition 3.1.1,

$$A(x)B(x) \equiv 1 + x + \cdots + x^{N-1} \mod (x^N - 1)$$

Suppose $0 < a_1 - a_2 = \delta'$ for $a_1, a_2 \in A$ is relatively prime to $\#B$ and $0 < b_1 - b_2 = \delta''$ for $b_1, b_2 \in B$ is relatively prime to $\#A$. Lemma 3.2.1 shows that

$$A(x^{\delta''})B(x^{\delta'}) \equiv 1 + x + \cdots + x^{N-1} \mod (x^N - 1)$$

so by Proposition 3.1.1 again, $\delta'' A \oplus \delta' B$ is a complete set of residues modulo N. But

$$(b_1 - b_2)a_1 + (a_1 - a_2)b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = (b_1 - b_2)a_2 + (a_1 - a_2)b_1$$

Thus it can be expressed $\delta'' a + \delta' b$ in two ways, which contradicts the tiling property that $a_1 = a_2$. Therefore the statement follows.■

Lemma 3.2.7 *[12] Let $A \oplus C = \mathbf{Z}$ be a tiling of period N such that A is finite, $0 \in A \cap C$, and N has one or two prime factors. Then there is a prime factor p of N such that either $A \subset p\mathbf{Z}$ or $C \subseteq p\mathbf{Z}$.*

Proof let $C = B \oplus N\mathbf{Z}$ and the prime factors of N be p and possibly q. Then Lemma 3.2.6 holds.

If 3.2.6(1) holds, and $0 \in A$then $A \subseteq A - A \subset p\mathbf{Z} \cup q\mathbf{Z}$. If neither $p\mathbf{Z}$ nor $q\mathbf{Z}$ contains A, then there exist $a_1, a_2 \in A$ such that $a_1 \in p\mathbf{Z} \setminus q\mathbf{Z}$ and $a_2 \in q\mathbf{Z} \setminus p\mathbf{Z}$. Hence $a_1 - a_2$ won't be divisible by $p\mathbf{Z}$ or $q\mathbf{Z}$, so it is relatively prime to $\#B$, which contradicts Lemma 3.2.6(1) holding. Therefore $A \subset p\mathbf{Z}$ or $A \subset q\mathbf{Z}$.

If 3.2.6(2) holds, the same argument shows that $B \subseteq p\mathbf{Z}$ or $B \subseteq q\mathbf{Z}$. As $C = B + N\mathbf{Z}$, so $C \subset p\mathbf{Z} + pq\mathbf{Z} = p\mathbf{Z}$ or $C \subset q\mathbf{Z} + pq\mathbf{Z} = q\mathbf{Z}$.■

Remark Translating A or C does not affect the conclusion. Thus the condition $0 \in A \cap C$ is not needed.

3.3 Coven Meyerowitz

Least common multiple (also called the lowest common multiple or smallest common multiple) of two integers a and b, usually denoted by $lcm(a, b)$, is the smallest positive integer that is divisible by both a and b.

Theorem 3.3.1 *Let A be a finite set of nonnegative integers with corresponding polynomial $A(x) = \sum_{a\in A} x^a$ and let S_A be the set of prime powers s such that the cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$. If*

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

$(T2)$ *If $s_1, ..., s_m \in S_A$ are powers of distinct primes, then $\Phi_{s_1,...s_m}(x)$ divides $A(x)$,*

then A tiles the integers.

Proof To show A tiles the integers, we can show $A \oplus B = \mathbf{Z}_N$. To show $A \oplus B = \mathbf{Z}_N$, we will use Proposition 3.1.1 (4). Therefore we will prove there exists a set B such that $\Phi_t(x)|B(x)$ or $\Phi_t(x)|A(x)$ and $A(1)B(1) = N$. Define $B(x) = \prod \Phi_s(x^{t(s)})$, where the product is taken over all prime power factors s of lcm(S_A) which are not in S_A and $t(s)$ is the largest factor of lcm(S_A) relatively prime to s. Since $s = p^\alpha \notin S_A$, we have $s = p^\alpha | lcm(S_A)$. Since every such s is a prime power, $B(x) = 1 + x^{p^\alpha - 1} + \cdots + x^{(x-1)p^\alpha - 1}$ has nonnegative coefficients. By Proposition 3.1.1(4) A, B are multi-sets nonnegative integers, we have B is a set that all the coefficients are 0 and 1.

Let $s > 1$ be a factor of $A(1)B(1)$ and write $s = s_1...s_m$ as a product of powers of distinct primes. If every $s_i \in S_A$, then by $(T2)$, $\Phi_s(x)$ divides $A(x)$. If some $s_i \notin S_A$, since $B(x) = \prod \Phi_s(x^{t(s)})$, we have $\Phi_{s_i}(x^{t(s_i)})$ divides $B(x)$ for $s = s_i$ and $t = t(s_i)$. Let $r = \frac{s}{s_i}$ be a factor of $t(s_i)$, as $\frac{s}{s_i}$ are all primes while $t(s_i)$ is the largest prime, then $r|t(s_i)$. By proposition 2.3.9(6) we know

$\Phi_s(x^t) = \prod_{r|t} \Phi_{rs}(x)$ for s and t are relatively prime, then $\Phi_{s_i} x^{t(s_i)} = \prod_{\frac{s}{s_i}|t(s_i)} \Phi_{rs_i}(x)$ and $\Phi_{rs_i}(x)$ divides $\Phi_{s_i}(x^{t(s_i)})$. Thus $\Phi_s(x)$ divides $B(x)$ since $rs_i = s_i$.

As $A(1) = \prod_{s \in S_A} \Phi_s(1)$ and $B(1) = \prod_{s \notin S_A, s|lcm(S_A)} \Phi_s(1)$, As $s = p^\alpha$ and $\Phi_s(x) = 1 + x^{p^{\alpha-1}} + \cdots + x^{(p-1)p^{\alpha-1}}$, so $\Phi_s(1) = p$. Let $lcm(S_A) = N$ have a prime decomposition that $lcm(S_A) = p_1^{r_1} \ldots p_e^{r_e}$, for $p_i^\alpha : 1 \leq \alpha \leq r_i$, if $p_i^\alpha \in S_A$, it's contribution with a p_i for $A(1)$; if $p_i \notin S_A$, it's contribution with a p_i for $B(1)$. Therefore $A(1)B(1) = \prod_{i=1}^{l} \prod_{\alpha=1}^{r_i} p_i = \prod_{i=1}^{l} p_i^{r_i} = N$. ■

Remark The set B constructed in the proof depends only on $S = S_A$ and not on A. Defining $C_S = B \oplus lcm(S)\mathbf{Z}$, $A \oplus C_S = \mathbf{Z}$ for all A with $S_A = S$ which satisfy $(T1)$ and $(T2)$. Then $C_S \subseteq p\mathbf{Z}$ for every prime $p \in S$, since p is a factor of n and every divisor $\Phi_s(x^{t(s)})$ of $B(x)$ is a polynomial in x^p. For either $t(s)$ is a multiple of p, or $s = p^{\alpha+1}$ with $\alpha \geqslant 1$ and $\Phi_s(x^{t(s)}) = \Phi_p(x^{t(s)p^\alpha})$, so every divisor $\Phi_s(x^{t(s)})$ of $B(x)$ os a polynomial in x^p.

Lemma 3.3.2 *Let $A(x)$ and $B(x)$ be polynomials with coefficients 0 and 1, $N = A(1)B(1)$, and R is the set of prime power factors of N. If $\Phi_t(x)$ divides $A(x)$ or $B(x)$ for every factor $t > 1$ of N, then*

1. *$A(1) = \prod_{s \in S_A} \Phi_s(1)$ and $B(1) = \prod_{s \in S_B} \Phi_s(1)$.*
2. *S_A and S_B are disjoint sets whose union is R.*

Proof For every factor $t > 1$ of N, $\Phi_t(x)$ divides $A(x)$ or $B(x)$, as $S_A = \{p^\alpha : p^\alpha | N \text{ and } \Phi_{p^\alpha}(x) | A(x)\}$ and similar for S_B, so if $p^\alpha = t \in R$, then $\Phi_t(x)|A(x)$ or $\Phi_t(x)|B(x)$. Hence $t = p^\alpha \in S_A$ or $t \in S_B$ and $R \subseteq S_A \cup S_B$ with $A(x) = k(x) \prod_{t \in S_A} \Phi_t(x)$ or $B(x) = k(x) \prod_{t \in S_B} \Phi_t(x)$. From $A(x) = k(x) \prod_{s \in S_A} \Phi_t(x)$, it follows that $A(1) = k(1) \prod_{s \in S_A} \Phi_t(1)$. But $k(x)$ has integer coefficients so $k(1)$ is an integer. Since $A(1) > 0$ and $\prod_{s \in S_A} \Phi_t(1) > 0$, we have $k(1) \geq 1$ so

$A(1) \geq \prod_{s \in S_A} \Phi_s(1)$ and the same for $B(1) \geq \prod_{s \in S_B} \Phi_s(1)$. Thus

$$N = A(1)B(1) \geq \prod_{s \in S_A} \Phi_s(1) \prod_{s \in S_B} \Phi_s(1) \geq \prod_{t \in R} \Phi_t(1)$$

As R is the set of prime power factors of n, then by Proposition 2.3.9 (4), $\prod_{t \in R} \Phi_t(1) = N$. Hence

$$N = A(1)B(1) \geq \prod_{s \in S_A} \Phi_s(1) \prod_{s \in S_B} \Phi_s(1) \geq \prod_{t \in R} \Phi_t(1) = N$$

and all the inequalities and containments above are actually equalities, so $\prod_{s \in S_A} \Phi_s(1) \prod_{s \in S_B} \Phi_s(1) = \prod_{s \in R} \Phi_t(1)$. But we know $R \subseteq S_A \cup S_B$, for $s \in S_A, S_B$ or R, s is a prime power, so $\Phi_s(1) = \Phi_{p^\alpha}(1) = p > 1$. We cannot have a $s = p^\alpha \in S_A \cap S_B$ because it will appear twice in the product $\prod_{s \in S_A} \Phi_s(1) \prod_{s \in S_B} \Phi_s(1)$ and only once in $\prod_{s \in R} \Phi_t(1)$, so the products could not be equal. Therefore S_A is disjoint from S_B. ■

Theorem 3.3.3 *Let A be a finite set of nonnegative integers with corresponding polynomial $A(x) = \sum_{a \in A} x^a$ and let S_A be the set of prime powers s such that the cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$. If A tiles the integers, then*

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

Proof By Proposition 3.1.1, we get $A(1)B(1) = N$ and $\Phi_s(x)|A(x)$ or $\Phi_s(x)|B(x)$, then by Lemma 3.3.2 (1), it follows directly.■

Remark $(T1)$ is not sufficient for A to tile the integers. $A = \{0, 1, 2, 4, 5, 6\}$ does not tile the integers because we cannot find a disjoint set containing $\{3\}$, but $A(x) = \Phi_3(x)\Phi_8(x)$ satisfies $(T1)$ because $\Phi_3(x) = 1 + x + x^2$ and $\Phi_8(x) = \Phi_{2^{(2+1)}}(x) = \Phi_2(x^4) = 1 + x^4$, so $S_A = \{3, 2^3\}$ and A(1)=6.

Conjecture 3.3.4 *(Coven-Meyerowitz conjecture, square-free case) Let N be square-free and let A be a tile of $\mathbf{Z}_N$. Then there exist a subgroup H of $\mathbf{Z}_N$ such that A consists of a single representative from each coset of H.*

Note that in the square-free case, every subgroup H of $\mathbf{Z}_N$ has a complementary subgroup $H^\perp$ (thus $\mathbf{Z}_N = H \oplus H^\perp$). In particular, H consists of a single representative from each coset of $H^\perp$.

Conjecture 3.3.5 *(Coven-Meyerowitz conjecture, general case) Let A be a finite subset of $\mathbf{Z}^+ \cup \{0\}$ and let*

$$\mathcal{S}_A = \{p^\alpha : p \text{ is a prime}, \alpha \geq 1 \text{ an integer and } \Phi_s(x) \text{ divides } A(x)\}.$$

Then every finite tile in $\mathbf{Z}$ satisfies: $(T1)$. $\#A = A(1) = \prod_{s \in \mathcal{S}_A} \Phi_s(1)$.

$(T2)$. *If $s_1, \cdots, s_n \in \mathcal{S}_A$ are powers of distinct primes, then $\Phi_{s_1 \cdots s_n}(x)$ divides $A(x)$.*

Lemma 3.3.6 *Suppose $A \oplus C = \mathbf{Z}$, where A is a finite set of nonnegative integers, $k > 1$, and $C \subseteq k\mathbf{Z}$. For $i = 0, 1, \ldots k-1$, let $A_i = \{a \in A : a \equiv i \mod k\}$, $a_i = min(A_i)$ and $\bar{A}_i = \{a - a_i : a \in A_i\}/k$. Then*

1. $A(x) = x^{a_0} \bar{A}_0(x^k) + x^{a_1} \bar{A}_1(x^k) + \cdots + x^{a_{k-1}} \bar{A}_{k-1}(x^k)$.
2. *Every $\bar{A}_i \oplus C/k = \mathbf{Z}$.*
3. *The elements of A are equally distributed modulo k — every $\#\bar{A}_i = (\#A)/k$.*
4. $S_{\bar{A}_0} = S_{\bar{A}_1} = \cdots = S_{\bar{A}_{k-1}}$.
5. *When k is prime, $S_A = \{k\} \cup S_{k\bar{A}_0}$ and if every $\bar{A}_i(x)$ satisfies (T2), then $A(x)$ satisfies (T2).*

Proof 1. As $A_i = \{a \in A : a \equiv i \mod k\}$, $a_i = min(A_i)$ and $\bar{A}_i = \{a - a_i : a \in A_i\}/k$, then $k\bar{A}_i + a_i = \{a : a \in A_i\} = A_i$. As $\bigcup_{i=0}^{k-1} A_i = A$, so $\bigcup_{i=0}^{k-1}(k\bar{A}_i + a_i) = \bigcup_{i=0}^{k-1} A_i = A$. Put into polynomial we have $A(x) = \sum_{i=0}^{k-1} x^{a_i}(k\bar{A}_i)(x) = \sum_{i=0}^{k-1} x^{a_i}\bar{A}_i(x^k) = x^{a_0}\bar{A}_0(x^k) + x^{a_1}\bar{A}_1(x^k) + \cdots + x^{a_{k-1}}\bar{A}_{k-1}(x^k)$.

2. As $A \oplus C = \mathbf{Z}$ and $C \subseteq k\mathbf{Z}$, look at the elements in $\mathbf{Z}$ congruent to i mod k, we get $A_i \oplus C = \{i\} \oplus k\mathbf{Z} = \{a_i\} \oplus k\mathbf{Z}$. Then $(A_i - a_i) \oplus C = k\mathbf{Z}$ and $(A_i - a_i)/k \oplus C/k = k\mathbf{Z}/k$. From (1) we have $k\bar{A}_i + a_i = A_i$, therefore $\bar{A}_i \oplus C/k = \mathbf{Z}$.

3. The translation set C/k has some period N, so there is a set $\bar{B}$ such that $\bar{A}_i \oplus (\bar{B} \oplus N\mathbf{Z}) = \mathbf{Z}$ and every $\bar{A}_i \oplus \bar{B}$ is a complete set of residues modulo N. Thus the $\#\bar{A}_i$ are equal.

4. Since by Lemma 3.3.2, every $S_{\bar{A}_i}$ is the complement of $S_{\bar{B}}$ in the set of prime power factors of N.

5. Write p in place of k. From Lemma 3.3.7 (2), $S_{p\bar{A}_i} = \{s' : s \in S_{\bar{A}_i}\}$, where $s' = ps$ or s according as p is or is not a factor of s. $p\bar{A}_i(x) = \sum_{a \in A_i} x^{pa} = \sum_{a \in A_i}(x^p)^a = \bar{A}_i(x^p)$. Define $S_{p\bar{A}_i} = \{p^\alpha : p \text{ is a prime}, a \geq 1 \text{ an integer and } \Phi_s(x) | \bar{A}(x)\}$, $t \in S_{p\bar{A}_i}$ implies $t = s'$ for some $s \in S_{\bar{A}_i}$. From (4), all the $S_{\bar{A}_i}$ are the same, then $S_{p\bar{A}}$ are the same. If $t \in S_{p\bar{A}_0}$, then $t \in S_{p\bar{A}}$ for any i. Hence $\Phi_t(x) | (p\bar{A}_i)(x) = \bar{A}_i(x^p)$ and $\Phi_t(x) | (x^{a_0}\bar{A}_0(x^p) + \cdots + x^{a_{k-1}}\bar{A}_{k-1}(x^k)) = A(x)$. Therefore $t \in S_A$ and $S_{p\bar{A}_0} \subseteq S_A$. Also $p \in S_A$, since if $\Phi_p(\omega) = 0$, then ω^p is the primitive root of unity so $\omega^p = 1$, $\omega^{a_i \equiv i \mod p}$ implies $\omega^{a_i - i} = \omega^{pk} = 1$, so $a_i - i = 0$ and $\omega^{a_i} = \omega^i$, and $A(\omega) = \sum_{i=0}^{p-1} \omega^i \bar{A}_i(1) = (\#A/k) \sum_{i=0}^{p-1} \omega^i = 0$, the next-to-last equality by (3). We have thus shown that $S_A \supseteq \{p\} \cup S_{p\bar{A}_0}$. Since A_0 and A tile the integers, $A_0(x)$ and $A(x)$ satisfy (T1) and $S_A = \{p\} \cup S_{p\bar{A}_0}$.

Now assume that every $\bar{A}_i(x)$ satisfies (T2). Condition (T2) for $A(x)$ is: if $s_1, \ldots, s_m \in S_{\bar{A}_0}$ are powers of distinct primes, then $\Phi_{s'_1 \ldots s'_m}(x)$ divides $A(x)$ and $\Phi_{ps_1 \ldots s_m}(x)$ divides $A(x)$. By (T2),

$\Phi_{s_1 \ldots s_m}(x)$ divides every $\bar{A}_i(x)$. hence by Proposition 2.3.9 (7), $\Phi_{s'_1 \ldots s'_m}$ and $\Phi_{ps_1 \ldots s_m}(x)$ divide all the $\bar{A}_i(x^p)$, so they divide $A(x)$ as well. ■

Lemma 3.3.7 *Let $k > 1$ and let $A = k\bar{A}$ be a finite set of nonnegative integers.*

1. *A tiles the integers if and only if $\bar{A}$ tiles the integers.*
2. *If p is prime, then $S_{p\bar{A}} = \{p^{\alpha+1} : p^\alpha \in S_{\bar{A}}\} \cup \{q^\beta \in S_{\bar{A}} : q \text{ prime}, q \neq p\}$.*
3. *$A(x)$ satisfies (T1) if and only if $\bar{A}(x)$ satisfies (T1).*
4. *$A(x)$ satisfies (T2) if and only if $\bar{A}(x)$ satisfies (T2).*

Proof (1) First we will show if $\bar{A}$ tiles the integers, then A tiles the integers. Let $\bar{A} \oplus C = \mathbf{Z}$. Then $k\bar{A} \oplus kC = k\mathbf{Z}$ and hence $A \oplus (\{0, 1, \ldots, k-1\} \oplus kC) = \{0, 1, \ldots, k-1\} \oplus (k\bar{A} \oplus kC) = \{0, 1, \ldots, k-1\} \oplus k\mathbf{Z} = \mathbf{Z}$. Next we will show if A tiles the integers, then $\bar{A}$ tiles the integers. Let $k\bar{A} \oplus D = \mathbf{Z}$. Then $k\bar{A} \oplus D_0 = k\mathbf{Z}$, where $D_0 = \{d \in D : d \equiv 0(\mod k)\}$, and hence $\bar{A} \oplus D_0/k = \mathbf{Z}$.

(2) From Proposition 2.3.9 (7) we have

$$\{t : \Phi_t(x) | A(x)\} = \{s' : \Phi_s(x) | \bar{A}(x)\} \cup \{ps : \Phi_s(x) | \bar{A}(x)\} \tag{3.6}$$

S_A and $S_{\bar{A}}$ contain prime power factors with $S_A =$ prime powers in the set of 3.6 and $S_{\bar{A}} = \{s = p^\alpha$ or q^β for q is a prime $q \neq p\}$, then we will have two cases:

Case 1: $s = p^\alpha$. When p is a factor of s, then $s' = ps = p^{\alpha+1}$.

Case 2: $s = q^\beta$. When p is not a factor of s, then $s' = s = q^\beta$; when p is a factor of s, then $s' = ps = pq^\beta$. As pq^β is not a prime power so it's not in $S_{\bar{A}}$.

(3) Suppose k is prime,, say $k = p$. Since $\#A = \#\bar{A}$, from (2) and Proposition 2.3.9 (4) we have

$$\bar{A}(1) \Leftrightarrow \prod_{p^\alpha \in S_{\bar{A}}} \Phi_{p^{\alpha+1}}(1) \prod_{q^\beta \in S_{\bar{A}}, q \neq p} \Phi_{q^\beta}(1) \Leftrightarrow \prod_{p^\alpha \in S_A} \Phi_{p^\alpha}(1) \prod_{q^\beta \in S_A, q \neq p} \Phi_{q^\beta}(1) \Leftrightarrow A(1)$$

(4) Let $s' = ps$ or s according as p is or is not a factor of s. let $s_1, \ldots, s_m$ be powers of distinct primes and $s = s_1 \ldots s_m$. Then $s'_1, \ldots, s'_m$ are powers of distinct primes and $s' = s'_1 \ldots s'_m$. Then $\bar{A}(x)$ satisfies $(T2) \Leftrightarrow s_i \in S_{\bar{A}}$ for $i \in \{1, \ldots, m\} \Leftrightarrow s'_i \in S_A = S_{p\bar{A}}$. From Proposition 2.3.9 (7), $\Phi_s(x)$ divides $\bar{A}(x) \Leftrightarrow \Phi_{s'}(x)$ divides $A(x)$. As $s_i \in S_{\bar{A}} \Leftrightarrow \Phi_{s_1 \ldots s_m}(x) | \bar{A}(x) \Leftrightarrow \Phi_s(x) | \bar{A}(x)$ and $s'_i \in S_A \Leftrightarrow \Phi_{s'_1 \ldots s'_m}(x) | A(x) \Leftrightarrow \Phi_{s'}(x) | A(x)$, so $\bar{A}(x)$ satisfies $(T2) \Leftrightarrow s_i \in S_{\bar{A}} \Leftrightarrow \Phi_s(x) | \bar{A}(x) \Leftrightarrow s'_i \in S_A \Leftrightarrow \Phi_{s'}(x) | A(x) \Leftrightarrow A(x)$ satisfies $(T2)$. ■

Remark B is not contained in $p\mathbf{Z}$ when $\Phi_p(x)$ divides $B(x)$ because if $B \subset p\mathbf{Z}$, then $B = p\bar{B}$, by (2) we get $S_B = S_{p\bar{B}} = \{p^{\alpha+1} : p^\alpha \in S_B\} \cup \{q^\beta \in S_{\bar{B}} : q \neq p\}$. However $\Phi_p(x) | B(x)$ indicates $p \in S_B$ and $\alpha \geq 1$ indicates $\alpha + 1 \geq 2$, then S_B contains only powers of p bigger than 2.

Theorem 3.3.8 *Let A be a finite set of nonnegative integers with corresponding polynomial $A(x) = \sum_{a \in A} x^a$ such that $\#A$ has at most two prime factors and let S_A be the set of prime powers s such that the cyclotomic polynomial $\Phi_s(x)$ divides $A(x)$. If A tiles the integers, then*

(T2) If $s_1, \ldots, s_m \in S_A$ are powers of distinct primes, then $\Phi_{s_1 \ldots s_m}(x)$ divides $A(x)$.

Proof From Lemma 3.3.7, there is no loss of generality in assuming that $gcd(A) = 1$ and $0 \in A$.

By Lemma 3.2.5 there is a tiling $A \oplus C = \mathbf{Z}$ whose period N is a product of powers of the prime factors of $\#A$. We complete the proof by induction on n. If $n = 1$, then $A = \{0\}$ and $A(x) \equiv 1$ satisfies (T2) vacuously. If $N > 1$, then by Lemma 3.2.7 there is a prime factor p of N such that $C \subseteq p\mathbf{Z}$. Then by Lemma 3.3.6, $A(x) = x^{a_0} \bar{A}_0 x^p + x^{a_1} \bar{A}_1 x^p + \cdots + x^{a_{p-1}} \bar{A}_{p-1}(x^p)$ and every

$\bar{A}_i \oplus C/p = \mathbf{Z}$ is a tiling of period N/p. Hence $\bar{A}_i$ tiles $\mathbf{Z}_{N/p}$ where $N/p < N$ also has only 2 prime factors. By the inductive hypothesis, every $\bar{A}_i(x)$ satisfies (T2), so by Lemma 3.3.6 (5), $A(x)$ satisfies (T2).■

Lemma 3.3.9 *Suppose A is finite, $0 \in A$, A tiles the integers with period N, and N has two prime factors, p and q. If neither $\Phi_p(x)$ nor $\Phi_q(x)$ is a divisor of $A(x)$, then $A \subset p\mathbf{Z}$ or $A \subset q\mathbf{Z}$.*

Proof Let $A \oplus (B \oplus N\mathbf{Z}) = \mathbf{Z}$ be a tiling of period N. By Proposition 3.1.1, $\Phi_p(x)$ and $\Phi_q(x)$ are divisors of $B(x)$ or $A(x)$. From the remark after Lemma 3.3.7, neither $p\mathbf{Z}$ nor $q\mathbf{Z}$ contains B. Then the conclusion follows by Lemma 3.2.7.■

Corollary 3.3.10 *If A is a finite set of integers and $C \subseteq k\mathbf{Z}$, then $A \oplus C = \mathbf{Z}$ if and only if $A = \bigcup_{i=0}^{k-1}(\{a_i\} \oplus k\bar{A}_i)$ for some complete set $\{a_0, a_1, \ldots, a_{k-1}\}$ of residues modulo k, and k sets $\bar{A}_i$, each of which satisfies min$(A_i) = 0$ and tiles the integers with translation set C/k.*

The decomposition is unique. We can have $gcd(A) = 1$ although this may not be true for the $\bar{A}_i$. If the $\bar{A}_i$ are equal, then the union is a direct sum, $A = \{a_0, a_1, \ldots, a_{k-1}\} \oplus k\bar{A}_0$. For some simple choices of translation set C, every tile has this form.

3.4 The Square-free Case

Theorem 3.4.1 *If $A \oplus B = \mathbf{Z}_N$ and N is square free, then A satisfies $(T1)$ and $(T2)$.*

Proof Suppose that $A \oplus B = \mathbf{Z}_N$ with N square-free. Let r be a prime dividing $|B|$, then as N is square-free so r does not divide $|A|$. By Theorem 3.2.2, $rA \oplus B = \mathbf{Z}_N$, then $B \oplus (rA \oplus N\mathbf{Z}) = \mathbf{Z}$. Let $C = rA \oplus N\mathbf{Z} \subseteq r\mathbf{Z}$ and $B' = B \cap r\mathbf{Z}$, then $|B'| = |B|/r$ and $B' = \{b \in B : b \equiv 0 \mod r\} =$

B_0. (this follows for example because $\Phi_r(x)$ divides $B(x)$, so that B has the same number of elements in each congruence class mod r). Then by Lemma 3.3.6 (2), $\bar{B}_0 \oplus (rA \oplus N\mathbf{Z})/r = \mathbf{Z}$, we get that $A \oplus B'' = \mathbf{Z}_{N/r}$, where $B'' = B'/r = \bar{B}_0$ and $|B''| = N/r$. Hence A tiles $\mathbf{Z}_{N/r}$, which iterates the procedure as long as we have primes in the tiling set $|B|$, we eventually get to the point when $|B| = 1$. Therefore $A \oplus 0 = \mathbf{Z}_{|A|}$, so A is a complete set of primes mod $|A|$ that $A(x) = 1 + x + \cdots + x^{|A|-1} \mod (x^{|A|} - 1)$, which implies $(T1)$ and $(T2)$ are satisfied.■

LIST OF REFERENCES

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

[2] N. G. de Bruijn. On bases for the set of integers. *Publ. Math. Debrecen*, 1:232–242, 1950.

[3] Dorin Ervin Dutkay and Chun-Kit Lai.

[4] Bálint Farkas, Máté Matolcsi, and Péter Móra. On Fuglede's conjecture and the existence of universal spectra. *J. Fourier Anal. Appl.*, 12(5):483–494, 2006.

[5] Bent Fuglede. Commuting self-adjoint partial differential operators and a group theoretic problem. *J. Functional Analysis*, 16:101–121, 1974.

[6] G. Hajós. Sur la factorisation des groupes abéliens. *Časopis Pěst. Mat. Fys.*, 74:157–162 (1950), 1949.

[7] Mihail N. Kolountzakis and Máté Matolcsi. Complex Hadamard matrices and the spectral set conjecture. *Collect. Math.*, (Vol. Extra):281–291, 2006.

[8] Mihail N. Kolountzakis and Máté Matolcsi. Tiles with no spectra. *Forum Math.*, 18(3):519–528, 2006.

[9] I. Łaba. The spectral set conjecture and multiplicative properties of roots of polynomials. *J. London Math. Soc. (2)*, 65(3):661–671, 2002.

[10] Máté Matolcsi. Fuglede's conjecture fails in dimension 4. *Proc. Amer. Math. Soc.*, 133(10):3021–3026, 2005.

[11] Donald J. Newman. Tesselation of integers. *J. Number Theory*, 9(1):107–111, 1977.

[12] A. D. Sands. On keller's conjecture for certain cyclic groups. *Proc. Edinburgh. Math. Soc.*, 22:17–21, 1997.

[13] Terence Tao. Fuglede's conjecture is false in 5 and higher dimensions. *Math. Res. Lett.*, 11(2-3):251–258, 2004.