Recent developments in the discrete Fuglede conjecture

Romanos Diogenes Malikiosis

Aristotle University of Thessaloniki

Codes and Expansions (CodEx) Seminar
August 10th, 2021

Fourier Analysis on domains $\Omega \subseteq \mathbb{R}^n$

Question

On which measurable domains $\Omega \subseteq \mathbb{R}^n$ with $\mu(\Omega) > 0$ can we do Fourier analysis, that is, there is an orthonormal basis of exponential functions $\left\{ \frac{1}{\mu(\Omega)} e^{2\pi i \lambda \cdot x} : \lambda \in \Lambda \right\}$ in $L^2(\Omega)$, where $\Lambda \subseteq \mathbb{R}^n$ discrete?

Definition

If Ω satisfies the above condition it is called *spectral*, and Λ is the *spectrum* of Ω.

Fourier Analysis on domains $\Omega \subseteq \mathbb{R}^n$

Question

On which measurable domains $\Omega \subseteq \mathbb{R}^n$ with $\mu(\Omega) > 0$ can we do Fourier analysis, that is, there is an orthonormal basis of exponential functions $\left\{ \frac{1}{\mu(\Omega)} e^{2\pi i \lambda \cdot x} : \lambda \in \Lambda \right\}$ in $L^2(\Omega)$, where $\Lambda \subseteq \mathbb{R}^n$ discrete?

Definition

If Ω satisfies the above condition it is called *spectral*, and Λ is the *spectrum* of Ω.

- The n-dimensional cube $C = [0, 1]^n$.

Fourier Analysis on domains $\Omega \subseteq \mathbb{R}^n$

Question

On which measurable domains $\Omega \subseteq \mathbb{R}^n$ with $\mu(\Omega) > 0$ can we do Fourier analysis, that is, there is an orthonormal basis of exponential functions $\left\{ \frac{1}{\mu(\Omega)} e^{2\pi i \lambda \cdot x} : \lambda \in \Lambda \right\}$ in $L^2(\Omega)$, where $\Lambda \subseteq \mathbb{R}^n$ discrete?

Definition

If Ω satisfies the above condition it is called *spectral*, and Λ is the *spectrum* of Ω.

- The n-dimensional cube $C = [0, 1]^n$.
- Parallelepipeds AC, where $A \in \mathrm{GL}(n, \mathbb{R})$.

Fourier Analysis on domains $\Omega \subseteq \mathbb{R}^n$

Question

On which measurable domains $\Omega \subseteq \mathbb{R}^n$ with $\mu(\Omega) > 0$ can we do Fourier analysis, that is, there is an orthonormal basis of exponential functions $\left\{ \frac{1}{\mu(\Omega)} e^{2\pi i \lambda \cdot x} : \lambda \in \Lambda \right\}$ in $L^2(\Omega)$, where $\Lambda \subseteq \mathbb{R}^n$ discrete?

Definition

If Ω satisfies the above condition it is called *spectral*, and Λ is the *spectrum* of Ω.

- The n-dimensional cube $C = [0, 1]^n$.
- Parallelepipeds AC, where $A \in \mathrm{GL}(n, \mathbb{R})$.
- Hexagons on $\mathbb{R}^2$.

Fourier Analysis on domains $\Omega \subseteq \mathbb{R}^n$

Question

On which measurable domains $\Omega \subseteq \mathbb{R}^n$ with $\mu(\Omega) > 0$ can we do Fourier analysis, that is, there is an orthonormal basis of exponential functions $\left\{ \frac{1}{\mu(\Omega)} e^{2\pi i \lambda \cdot x} : \lambda \in \Lambda \right\}$ in $L^2(\Omega)$, where $\Lambda \subseteq \mathbb{R}^n$ discrete?

Definition

If Ω satisfies the above condition it is called *spectral*, and Λ is the *spectrum* of Ω.

- The n-dimensional cube $C = [0,1]^n$.
- Parallelepipeds AC, where $A \in \mathrm{GL}(n, \mathbb{R})$.
- Hexagons on $\mathbb{R}^2$.
- Not n-dimensional balls! ($n \geq 2$) (Iosevich, Katz, Pedersen, '99)

Fourier Analysis on domains $\Omega \subseteq \mathbb{R}^n$

Question

On which measurable domains $\Omega \subseteq \mathbb{R}^n$ with $\mu(\Omega) > 0$ can we do Fourier analysis, that is, there is an orthonormal basis of exponential functions $\left\{\frac{1}{\mu(\Omega)} e^{2\pi i \lambda \cdot x} : \lambda \in \Lambda\right\}$ in $L^2(\Omega)$, where $\Lambda \subseteq \mathbb{R}^n$ discrete?

Definition

If Ω satisfies the above condition it is called *spectral*, and Λ is the *spectrum* of Ω.

- The n-dimensional cube $C = [0,1]^n$.
- Parallelepipeds AC, where $A \in \mathrm{GL}(n, \mathbb{R})$.
- Hexagons on $\mathbb{R}^2$.
- Not n-dimensional balls! $(n \geq 2)$ (Iosevich, Katz, Pedersen, '99)

Fuglede's conjecture

Definition

A set $\Omega \subseteq \mathbb{R}^n$ of positive measure is called *tile* of $\mathbb{R}^n$ if there is $T \subseteq \mathbb{R}^n$ such that $\Omega \oplus T = \mathbb{R}^n$.

Conjecture (Fuglede, 1974)

A set $\Omega \subseteq \mathbb{R}^n$ of positive measure is spectral if and only if it tiles $\mathbb{R}^n$.

Fuglede's conjecture

Definition

A set $\Omega \subseteq \mathbb{R}^n$ of positive measure is called *tile* of $\mathbb{R}^n$ if there is $T \subseteq \mathbb{R}^n$ such that $\Omega \oplus T = \mathbb{R}^n$.

Conjecture (Fuglede, 1974)

A set $\Omega \subseteq \mathbb{R}^n$ of positive measure is spectral if and only if it tiles $\mathbb{R}^n$.

Special cases

Theorem (Fuglede, '74)

Let $\Omega \subseteq \mathbb{R}^n$ be an open bounded set of measure 1 and $\Lambda \subseteq \mathbb{R}^n$ be a lattice with density 1. then $\Omega \oplus \Lambda = \mathbb{R}^n$ if and only if $\Lambda^\star$ is a spectrum of Ω.

Theorem (Lev, Matolcsi, '19)

Let $K \subseteq \mathbb{R}^n$ be a convex body; then K is spectral if and only if it tiles $\mathbb{R}^n$.

Special cases

Theorem (Fuglede, '74)

Let $\Omega \subseteq \mathbb{R}^n$ *be an open bounded set of measure* 1 *and* $\Lambda \subseteq \mathbb{R}^n$ *be a lattice with density* 1*. then* $\Omega \oplus \Lambda = \mathbb{R}^n$ *if and only if* $\Lambda^\star$ *is a spectrum of* Ω*.*

Theorem (Lev, Matolcsi, '19)

Let $K \subseteq \mathbb{R}^n$ *be a convex body; then* K *is spectral if and only if it tiles* $\mathbb{R}^n$*.*

Tao's counterexample

"A cataclysmic event in the history of this problem took place in 2004 when Terry Tao disproved the Fuglede Conjecture by exhibiting a spectral set in $\mathbb{R}^{12}$ *which does not tile."*
The Fuglede Conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$, Iosevich, Mayeli, Pakianathan, 2017.

Tao's counterexample

"A cataclysmic event in the history of this problem took place in 2004 when Terry Tao disproved the Fuglede Conjecture by exhibiting a spectral set in $\mathbb{R}^{12}$ which does not tile."
The Fuglede Conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$, Iosevich, Mayeli, Pakianathan, 2017.

Theorem (Tao, '04)

There are spectral subsets of $\mathbb{R}^5$ of positive measure that do not tile $\mathbb{R}^5$.

Tao's counterexample

"A cataclysmic event in the history of this problem took place in 2004 when Terry Tao disproved the Fuglede Conjecture by exhibiting a spectral set in $\mathbb{R}^{12}$ which does not tile."
The Fuglede Conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$, Iosevich, Mayeli, Pakianathan, 2017.

Theorem (Tao, '04)

There are spectral subsets of $\mathbb{R}^5$ of positive measure that do not tile $\mathbb{R}^5$.

Theorem (Farkas-Kolountzakis-Matolcsi-Mora-Revesz-Tao, '04-'06)

Fuglede's conjecture fails for $n \geq 3$ (both directions).

Tao's counterexample

"A cataclysmic event in the history of this problem took place in 2004 when Terry Tao disproved the Fuglede Conjecture by exhibiting a spectral set in $\mathbb{R}^{12}$ which does not tile."
The Fuglede Conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$, Iosevich, Mayeli, Pakianathan, 2017.

Theorem (Tao, '04)

There are spectral subsets of $\mathbb{R}^5$ of positive measure that do not tile $\mathbb{R}^5$.

Theorem (Farkas-Kolountzakis-Matolcsi-Mora-Revesz-Tao, '04-'06)

Fuglede's conjecture fails for $n \geq 3$ (both directions).

The conjecture is still open for $n \leq 2$. Tao's counterexample is a union of unit cubes. It comes from a spectral subset of $\mathbb{Z}_3^5$ of size 6.

Tao's counterexample

"A cataclysmic event in the history of this problem took place in 2004 when Terry Tao disproved the Fuglede Conjecture by exhibiting a spectral set in $\mathbb{R}^{12}$ which does not tile."
The Fuglede Conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$, Iosevich, Mayeli, Pakianathan, 2017.

Theorem (Tao, '04)

There are spectral subsets of $\mathbb{R}^5$ of positive measure that do not tile $\mathbb{R}^5$.

Theorem (Farkas-Kolountzakis-Matolcsi-Mora-Revesz-Tao, '04-'06)

Fuglede's conjecture fails for $n \geq 3$ (both directions).

The conjecture is still open for $n \leq 2$. Tao's counterexample is a union of unit cubes. It comes from a spectral subset of $\mathbb{Z}_3^5$ of size 6.

Tao's counterexample

Consider the standard basis of $\mathbb{Z}_3^6$, $e_1, \ldots, e_6$. Let $\omega = e^{2\pi i/3}$ and $\xi_1, \ldots, \xi_6$ be characters such that

$$[\xi_j(e_i)]_{1 \leq i,j \leq 6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ 1 & \omega & 1 & \omega^2 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 \end{pmatrix}$$

Tao's counterexample

Consider the standard basis of $\mathbb{Z}_3^6$, $e_1, \ldots, e_6$. Let $\omega = e^{2\pi i/3}$ and $\xi_1, \ldots, \xi_6$ be characters such that

$$[\xi_j(e_i)]_{1 \le i,j \le 6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ 1 & \omega & 1 & \omega^2 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 \end{pmatrix}$$

The above matrix is *Hadamard*, hence $\Lambda = \{\xi_1, \ldots, \xi_6\}$ is a spectrum of $\Omega = \{e_1, \ldots, e_6\}$. $\Omega - e_1$ then is contained in a hyperplane, thus showing the existence of a counterexample in $\mathbb{Z}_3^5$. Obviously, such a set cannot tile, since $6 \nmid 3^5$.

Tao's counterexample

Consider the standard basis of $\mathbb{Z}_3^6$, $e_1, \ldots, e_6$. Let $\omega = e^{2\pi i/3}$ and $\xi_1, \ldots, \xi_6$ be characters such that

$$[\xi_j(e_i)]_{1\leq i,j\leq 6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ 1 & \omega & 1 & \omega^2 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 \end{pmatrix}$$

The above matrix is *Hadamard*, hence $\Lambda = \{\xi_1, \ldots, \xi_6\}$ is a spectrum of $\Omega = \{e_1, \ldots, e_6\}$. $\Omega - e_1$ then is contained in a hyperplane, thus showing the existence of a counterexample in $\mathbb{Z}_3^5$. Obviously, such a set cannot tile, since $6 \nmid 3^5$.

Passage to finite groups

Definition

Let G be an Abelian group. We write **(S-T**(G)**)** if every bounded spectral subset of G is also a tile, and **(T-S**(G)**)** if every bounded tile of G is spectral.

Theorem

The following hold:

$$(\mathbf{T}\text{-}\mathbf{S}(\mathbb{Z}_n))\forall n \in \mathbb{N} \Leftrightarrow (\mathbf{T}\text{-}\mathbf{S}(\mathbb{Z})) \Leftrightarrow (\mathbf{T}\text{-}\mathbf{S}(\mathbb{R}))$$

and

$$(\mathbf{S}\text{-}\mathbf{T}(\mathbb{R})) \Rightarrow (\mathbf{S}\text{-}\mathbf{T}(\mathbb{Z})) \Rightarrow (\mathbf{S}\text{-}\mathbf{T}(\mathbb{Z}_n))\forall n \in \mathbb{N}.$$

Passage to finite groups

Definition

Let G be an Abelian group. We write **(S-T**(G)**)** if every bounded spectral subset of G is also a tile, and **(T-S**(G)**)** if every bounded tile of G is spectral.

Theorem

The following hold:

$$\textbf{(T-S}(\mathbb{Z}_n)\textbf{)}\forall n \in \mathbb{N} \Leftrightarrow \textbf{(T-S}(\mathbb{Z})\textbf{)} \Leftrightarrow \textbf{(T-S}(\mathbb{R})\textbf{)}$$

and

$$\textbf{(S-T}(\mathbb{R})\textbf{)} \Rightarrow \textbf{(S-T}(\mathbb{Z})\textbf{)} \Rightarrow \textbf{(S-T}(\mathbb{Z}_n)\textbf{)}\forall n \in \mathbb{N}.$$

Passage to finite groups

The last hold in both directions if every bounded spectral subset of $\mathbb{R}$ has a rational spectrum.

Theorem (Dutkay, Lai, '14)

If Fuglede's conjecture holds in $\mathbb{R}$, then every bounded spectral set has a rational spectrum.

Passage to finite groups

The last hold in both directions if every bounded spectral subset of $\mathbb{R}$ has a rational spectrum.

Theorem (Dutkay, Lai, '14)

If Fuglede's conjecture holds in $\mathbb{R}$, then every bounded spectral set has a rational spectrum.

Partial positive results on the rationality of spectrum have been proved by Łaba ('02), Bose & Madan ('17).

Passage to finite groups

The last hold in both directions if every bounded spectral subset of $\mathbb{R}$ has a rational spectrum.

Theorem (Dutkay, Lai, '14)

If Fuglede's conjecture holds in $\mathbb{R}$, then every bounded spectral set has a rational spectrum.

Partial positive results on the rationality of spectrum have been proved by Łaba ('02), Bose & Madan ('17).

Non-cyclic groups; negative results

The properties **(S-T**(G)**)** and **(T-S**(G)**)** are hereditary, that is, they hold for every subgroup of G.

It suffices then to examine groups of the form $\mathbb{Z}_N^d$. For $d \geq 2$ we get the following results:

Non-cyclic groups; negative results

The properties **(S-T(G))** and **(T-S(G))** are hereditary, that is, they hold for every subgroup of G.
It suffices then to examine groups of the form $\mathbb{Z}_N^d$. For $d \geq 2$ we get the following results:

- There is a spectral subset of $\mathbb{Z}_8^3$ that does not tile (Kolountzakis, Matolcsi, '06).

Non-cyclic groups; negative results

The properties **(S-T(G))** and **(T-S(G))** are hereditary, that is, they hold for every subgroup of G.
It suffices then to examine groups of the form $\mathbb{Z}_N^d$. For $d \geq 2$ we get the following results:

- There is a spectral subset of $\mathbb{Z}_8^3$ that does not tile (Kolountzakis, Matolcsi, '06).
- There is a tile of $\mathbb{Z}_{24}^3$ that is not spectral (Farkas, Matolcsi, Mora, '06).

Non-cyclic groups; negative results

The properties **(S-T(G))** and **(T-S(G))** are hereditary, that is, they hold for every subgroup of G.
It suffices then to examine groups of the form $\mathbb{Z}_N^d$. For $d \geq 2$ we get the following results:

- There is a spectral subset of $\mathbb{Z}_8^3$ that does not tile (Kolountzakis, Matolcsi, '06).
- There is a tile of $\mathbb{Z}_{24}^3$ that is not spectral (Farkas, Matolcsi, Mora, '06).
- There are spectral subsets of $\mathbb{Z}_p^4$ that do not tile for p odd (Ferguson, Sothanaphan; independently Mattheus '20); the same holds for $\mathbb{Z}_2^{10}$ (F-S, '20).

Non-cyclic groups; negative results

The properties **(S-T**(G)**)** and **(T-S**(G)**)** are hereditary, that is, they hold for every subgroup of G.
It suffices then to examine groups of the form $\mathbb{Z}_N^d$. For $d \geq 2$ we get the following results:

- There is a spectral subset of $\mathbb{Z}_8^3$ that does not tile (Kolountzakis, Matolcsi, '06).
- There is a tile of $\mathbb{Z}_{24}^3$ that is not spectral (Farkas, Matolcsi, Mora, '06).
- There are spectral subsets of $\mathbb{Z}_p^4$ that do not tile for p odd (Ferguson, Sothanaphan; independently Mattheus '20); the same holds for $\mathbb{Z}_2^{10}$ (F-S, '20).

Non-cyclic groups; negative results

The properties **(S-T**(G)**)** and **(T-S**(G)**)** are hereditary, that is, they hold for every subgroup of G.
It suffices then to examine groups of the form $\mathbb{Z}_N^d$. For $d \geq 2$ we get the following results:

- There is a spectral subset of $\mathbb{Z}_8^3$ that does not tile (Kolountzakis, Matolcsi, '06).
- There is a tile of $\mathbb{Z}_{24}^3$ that is not spectral (Farkas, Matolcsi, Mora, '06).
- There are spectral subsets of $\mathbb{Z}_p^4$ that do not tile for p odd (Ferguson, Sothanaphan; independently Mattheus '20); the same holds for $\mathbb{Z}_2^{10}$ (F-S, '20).

Non-cyclic groups; positive results

- Fuglede's conjecture holds in $\mathbb{Z}_p^2$, p prime (Iosevich, Mayeli, Pakianathan, '17).
- Fuglede's conjecture holds in $\mathbb{Z}_2^6$ (Ferguson, Sothanaphan, '20).

Non-cyclic groups; positive results

- Fuglede's conjecture holds in $\mathbb{Z}_p^2$, p prime (Iosevich, Mayeli, Pakianathan, '17).
- Fuglede's conjecture holds in $\mathbb{Z}_2^6$ (Ferguson, Sothanaphan, '20).
- Fuglede's conjecture holds in $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ (Shi, '20).

Non-cyclic groups; positive results

- Fuglede's conjecture holds in $\mathbb{Z}_p^2$, p prime (Iosevich, Mayeli, Pakianathan, '17).
- Fuglede's conjecture holds in $\mathbb{Z}_2^6$ (Ferguson, Sothanaphan, '20).
- Fuglede's conjecture holds in $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ (Shi, '20).
- Fuglede's conjecture holds in $\mathbb{Z}_p^2 \times \mathbb{Z}_q^2$, (Fallon, Kiss, Somlai, '21).

Non-cyclic groups; positive results

- Fuglede's conjecture holds in $\mathbb{Z}_p^2$, p prime (Iosevich, Mayeli, Pakianathan, '17).
- Fuglede's conjecture holds in $\mathbb{Z}_2^6$ (Ferguson, Sothanaphan, '20).
- Fuglede's conjecture holds in $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ (Shi, '20).
- Fuglede's conjecture holds in $\mathbb{Z}_p^2 \times \mathbb{Z}_q^2$, (Fallon, Kiss, Somlai, '21).
- Every tile of $\mathbb{Z}_p^3$ is spectral (Aten et al. '17).

Non-cyclic groups; positive results

- Fuglede's conjecture holds in $\mathbb{Z}_p^2$, p prime (Iosevich, Mayeli, Pakianathan, '17).
- Fuglede's conjecture holds in $\mathbb{Z}_2^6$ (Ferguson, Sothanaphan, '20).
- Fuglede's conjecture holds in $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ (Shi, '20).
- Fuglede's conjecture holds in $\mathbb{Z}_p^2 \times \mathbb{Z}_q^2$, (Fallon, Kiss, Somlai, '21).
- Every tile of $\mathbb{Z}_p^3$ is spectral (Aten et al. '17).
- Every spectral subset of $\mathbb{Z}_p^3$ is a tile, for $p \leq 7$ (Fallon, Mayeli, Villano, '19).

Non-cyclic groups; positive results

- Fuglede's conjecture holds in $\mathbb{Z}_p^2$, p prime (Iosevich, Mayeli, Pakianathan, '17).
- Fuglede's conjecture holds in $\mathbb{Z}_2^6$ (Ferguson, Sothanaphan, '20).
- Fuglede's conjecture holds in $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ (Shi, '20).
- Fuglede's conjecture holds in $\mathbb{Z}_p^2 \times \mathbb{Z}_q^2$, (Fallon, Kiss, Somlai, '21).
- Every tile of $\mathbb{Z}_p^3$ is spectral (Aten et al. '17).
- Every spectral subset of $\mathbb{Z}_p^3$ is a tile, for $p \leq 7$ (Fallon, Mayeli, Villano, '19).

Cyclic groups - Basic properties

Let $A \subseteq \mathbb{Z}_N$ and $e_\lambda(a) = e^{2\pi i \lambda \cdot a/N}$. Inner product on $L^2(A)$:

$$\langle f, g \rangle_A = \sum_{a \in A} f(a)\overline{g(a)}.$$

It holds $\langle e_\lambda, e_{\lambda'} \rangle_A = \widehat{\mathbf{1}_A}(\lambda' - \lambda)$.

Lemma

Λ is a spectrum of $A \subseteq \mathbb{Z}_N$ if and only if

$$\widehat{\mathbf{1}_A}(\lambda' - \lambda) = 0, \ \forall \lambda \neq \lambda', \lambda, \lambda' \in \Lambda$$

and $|A| = |\Lambda|$.

Cyclic groups - Basic properties

Let $A \subseteq \mathbb{Z}_N$ and $e_\lambda(a) = e^{2\pi i \lambda \cdot a/N}$. Inner product on $L^2(A)$:

$$\langle f, g \rangle_A = \sum_{a \in A} f(a)\overline{g(a)}.$$

It holds $\langle e_\lambda, e_{\lambda'} \rangle_A = \widehat{\mathbf{1}_A}(\lambda' - \lambda)$.

Lemma

Λ is a spectrum of $A \subseteq \mathbb{Z}_N$ if and only if

$$\widehat{\mathbf{1}_A}(\lambda' - \lambda) = 0, \ \forall \lambda \neq \lambda', \lambda, \lambda' \in \Lambda$$

and $|A| = |\Lambda|$.

The mask polynomial

Definition (Coven-Meyerowitz, '98)

Let $A \subseteq \mathbb{Z}_N$. The mask polynomial A is given by

$$\sum_{a \in A} X^a \in \mathbb{Z}[X]/(X^N - 1).$$

It holds

$$\widehat{\mathbf{1}}_A(d) = A(\zeta_N^d), \forall d \in \mathbb{Z}_N.$$

Λ is a spectrum of A if and only if $|A| = |\Lambda|$ and

$$A(\zeta_{\mathrm{ord}(\ell - \ell')}) = 0, \ \forall \ell, \ell' \in \Lambda, \ell \neq \ell'.$$

The mask polynomial

Definition (Coven-Meyerowitz, '98)

Let $A \subseteq \mathbb{Z}_N$. The mask polynomial A is given by

$$\sum_{a \in A} X^a \in \mathbb{Z}[X]/(X^N - 1).$$

It holds

$$\widehat{\mathbf{1}}_A(d) = A(\zeta_N^d), \forall d \in \mathbb{Z}_N.$$

Λ is a spectrum of A if and only if $|A| = |\Lambda|$ and

$$A(\zeta_{\mathrm{ord}(\ell-\ell')}) = 0,\ \forall \ell, \ell' \in \Lambda, \ell \neq \ell'.$$

Moreover, $A \oplus T = \mathbb{Z}_N$ if and only if

$$A(X)T(X) \equiv 1 + X + X^2 + \cdots + X^{N-1} \bmod (X^N - 1).$$

The mask polynomial

Definition (Coven-Meyerowitz, '98)

Let $A \subseteq \mathbb{Z}_N$. The mask polynomial A is given by

$$\sum_{a \in A} X^a \in \mathbb{Z}[X]/(X^N - 1).$$

It holds

$$\widehat{\mathbf{1}}_A(d) = A(\zeta_N^d), \forall d \in \mathbb{Z}_N.$$

Λ is a spectrum of A if and only if $|A| = |\Lambda|$ and

$$A(\zeta_{\mathrm{ord}(\ell - \ell')}) = 0, \ \forall \ell, \ell' \in \Lambda, \ell \neq \ell'.$$

Moreover, $A \oplus T = \mathbb{Z}_N$ if and only if

$$A(X)T(X) \equiv 1 + X + X^2 + \cdots + X^{N-1} \bmod (X^N - 1).$$

The properties (T1) and (T2)

Definition

Let $A(X) \in \mathbb{Z}[X]/(X^N - 1)$, and let

$$S_A = \{d \mid N : d \text{ prime power}, A(\zeta_d) = 0\}.$$

We define the following properties:

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

(T2) Let $s_1, s_2, \ldots, s_k \in S_A$ be powers of different primes. Then $\Phi_s(X) \mid A(X)$, where $s = s_1 \cdots s_k$.

Remark

When N is a prime power, (T2) holds vacuously. If $N = p^n q^m$, then (T2) is simply

$$A(\zeta_{p^k}) = A(\zeta_{q^\ell}) = 0 \Rightarrow A(\zeta_{p^k q^\ell}) = 0$$

The properties (T1) and (T2)

Definition

Let $A(X) \in \mathbb{Z}[X]/(X^N - 1)$, and let

$$S_A = \{d \mid N : d \text{ prime power}, A(\zeta_d) = 0\}.$$

We define the following properties:

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

(T2) Let $s_1, s_2, \ldots, s_k \in S_A$ be powers of different primes. Then $\Phi_s(X) \mid A(X)$, where $s = s_1 \cdots s_k$.

Remark

When N is a prime power, (T2) holds vacuously. If $N = p^n q^m$, then (T2) is simply

$$A(\zeta_{p^k}) = A(\zeta_{q^\ell}) = 0 \Rightarrow A(\zeta_{p^k q^\ell}) = 0$$

Example

Let $A \subseteq \mathbb{Z}_N$, $N = p^4 q^4 r^3$, such that

$$A(\zeta_p) = A(\zeta_{p^3}) = A(\zeta_{q^2}) = A(\zeta_{r^3}) = 0,$$

and $A(X)$ has no other root of order a power of p, q, or r. Then,

- (T1) is $|A| = p^2 q r$.

Example

Let $A \subseteq \mathbb{Z}_N$, $N = p^4 q^4 r^3$, such that

$$A(\zeta_p) = A(\zeta_{p^3}) = A(\zeta_{q^2}) = A(\zeta_{r^3}) = 0,$$

and $A(X)$ has no other root of order a power of p, q, or r. Then,

- (T1) is $|A| = p^2 qr$.
- (T2): $A(\zeta_p) = A(\zeta_{q^2}) = 0 \Rightarrow A(\zeta_{pq^2}) = 0$.

Example

Let $A \subseteq \mathbb{Z}_N$, $N = p^4 q^4 r^3$, such that

$$A(\zeta_p) = A(\zeta_{p^3}) = A(\zeta_{q^2}) = A(\zeta_{r^3}) = 0,$$

and $A(X)$ has no other root of order a power of p, q, or r.Then,

- (T1) is $|A| = p^2 qr$.
- (T2): $A(\zeta_p) = A(\zeta_{q^2}) = 0 \Rightarrow A(\zeta_{pq^2}) = 0$.
- (T2): $A(\zeta_{p^3}) = A(\zeta_{r^3}) = 0 \Rightarrow A(\zeta_{p^3 r^3}) = 0$.

Example

Let $A \subseteq \mathbb{Z}_N$, $N = p^4 q^4 r^3$, such that

$$A(\zeta_p) = A(\zeta_{p^3}) = A(\zeta_{q^2}) = A(\zeta_{r^3}) = 0,$$

and $A(X)$ has no other root of order a power of p, q, or r.Then,

- (T1) is $|A| = p^2 qr$.
- (T2): $A(\zeta_p) = A(\zeta_{q^2}) = 0 \Rightarrow A(\zeta_{pq^2}) = 0$.
- (T2): $A(\zeta_{p^3}) = A(\zeta_{r^3}) = 0 \Rightarrow A(\zeta_{p^3 r^3}) = 0$.
- (T2): $A(\zeta_p) = A(\zeta_{q^2}) = A(\zeta_{r^3}) = 0 \Rightarrow A(\zeta_{pq^2 r^3}) = 0$.

Example

Let $A \subseteq \mathbb{Z}_N$, $N = p^4 q^4 r^3$, such that

$$A(\zeta_p) = A(\zeta_{p^3}) = A(\zeta_{q^2}) = A(\zeta_{r^3}) = 0,$$

and $A(X)$ has no other root of order a power of p, q, or r.Then,

- (T1) is $|A| = p^2 qr$.
- (T2): $A(\zeta_p) = A(\zeta_{q^2}) = 0 \Rightarrow A(\zeta_{pq^2}) = 0$.
- (T2): $A(\zeta_{p^3}) = A(\zeta_{r^3}) = 0 \Rightarrow A(\zeta_{p^3 r^3}) = 0$.
- (T2): $A(\zeta_p) = A(\zeta_{q^2}) = A(\zeta_{r^3}) = 0 \Rightarrow A(\zeta_{pq^2 r^3}) = 0$.
- We also have

$$A(\zeta_{p^3 q^2}) = A(\zeta_{pr^3}) = A(\zeta_{q^2 r^3}) = A(\zeta_{p^3 q^2 r^3}) = 0.$$

Example

Let $A \subseteq \mathbb{Z}_N$, $N = p^4q^4r^3$, such that

$$A(\zeta_p) = A(\zeta_{p^3}) = A(\zeta_{q^2}) = A(\zeta_{r^3}) = 0,$$

and $A(X)$ has no other root of order a power of p, q, or r.Then,

- (T1) is $|A| = p^2qr$.
- (T2): $A(\zeta_p) = A(\zeta_{q^2}) = 0 \Rightarrow A(\zeta_{pq^2}) = 0$.
- (T2): $A(\zeta_{p^3}) = A(\zeta_{r^3}) = 0 \Rightarrow A(\zeta_{p^3r^3}) = 0$.
- (T2): $A(\zeta_p) = A(\zeta_{q^2}) = A(\zeta_{r^3}) = 0 \Rightarrow A(\zeta_{pq^2r^3}) = 0$.
- We also have

$$A(\zeta_{p^3q^2}) = A(\zeta_{pr^3}) = A(\zeta_{q^2r^3}) = A(\zeta_{p^3q^2r^3}) = 0.$$

Tiling, spectrality, and (T1), (T2)

Theorem (Coven-Meyerowitz, '98)

If $A \subseteq \mathbb{Z}_N$ satisfies (T1) and (T2), then it tiles $\mathbb{Z}_N$. If A tiles $\mathbb{Z}_N$, then it satisfies (T1); if in addition $N = p^n q^m$, then A satisfies (T2) as well.

Theorem (Łaba, '02)

If $A \subseteq \mathbb{Z}_N$ satisfies (T1) and (T2), then it is spectral. If $N = p^n$ and A is spectral, then it satisfies (T1).

Tiling, spectrality, and (T1), (T2)

Theorem (Coven-Meyerowitz, '98)

If $A \subseteq \mathbb{Z}_N$ satisfies (T1) and (T2), then it tiles $\mathbb{Z}_N$. If A tiles $\mathbb{Z}_N$, then it satisfies (T1); if in addition $N = p^n q^m$, then A satisfies (T2) as well.

Theorem (Łaba, '02)

If $A \subseteq \mathbb{Z}_N$ satisfies (T1) and (T2), then it is spectral. If $N = p^n$ and A is spectral, then it satisfies (T1).

(S-T($\mathbb{Z}_N$)), $N = p^n$

Let $A \subseteq \mathbb{Z}_N$ with spectrum Λ. The Nth roots of unity on which $A(X)$ vanishes are precisely

$$\zeta_{p^{\nu_1}}, \dots, \zeta_{p^{\nu_k}}.$$

Put $R = \{p^{\nu_1}, \dots, p^{\nu_k}\}$. Therefore

$$E(X) = \prod_{d \in R} \Phi_d(X) \mid A(X),$$

Let $A \subseteq \mathbb{Z}_N$ with spectrum Λ. The Nth roots of unity on which $A(X)$ vanishes are precisely

$$\zeta_{p^{\nu_1}}, \ldots, \zeta_{p^{\nu_k}}.$$

Put $R = \{p^{\nu_1}, \ldots, p^{\nu_k}\}$. Therefore

$$E(X) = \prod_{d \in R} \Phi_d(X) \mid A(X),$$

whence $p^k \mid |A|$. $E(X)$ is then the mask polynomial of a subset E with p^k elements, whose spectrum is Λ. Hence, $|A| = p^k$, so A satisfies (T1).

(S-T($\mathbb{Z}_N$)), $N = p^n$

Let $A \subseteq \mathbb{Z}_N$ with spectrum Λ. The Nth roots of unity on which $A(X)$ vanishes are precisely

$$\zeta_{p^{\nu_1}}, \ldots, \zeta_{p^{\nu_k}}.$$

Put $R = \{p^{\nu_1}, \ldots, p^{\nu_k}\}$. Therefore

$$E(X) = \prod_{d \in R} \Phi_d(X) \mid A(X),$$

whence $p^k \mid |A|$. $E(X)$ is then the mask polynomial of a subset E with p^k elements, whose spectrum is Λ. Hence, $|A| = p^k$, so A satisfies (T1).

(T-S($\mathbb{Z}_N$)), $N = p^n$

Let $A \oplus T = \mathbb{Z}_N$, or equivalently

$$A(X)T(X) \equiv 1 + X + X^2 + \cdots + X^{N-1} \bmod (X^N - 1).$$

As before, $\zeta_{p^{\nu_1}}, \ldots, \zeta_{p^{\nu_k}}$ are precisely the roots of $A(X)$, whence

$$E(X) = \prod_{d \in R} \Phi_d(X) \mid A(X),$$

(T-S($\mathbb{Z}_N$)), $N = p^n$

Let $A \oplus T = \mathbb{Z}_N$, or equivalently

$$A(X)T(X) \equiv 1 + X + X^2 + \cdots + X^{N-1} \bmod (X^N - 1).$$

As before, $\zeta_{p^{\nu_1}}, \ldots, \zeta_{p^{\nu_k}}$ are precisely the roots of $A(X)$, whence

$$E(X) = \prod_{d \in R} \Phi_d(X) \mid A(X),$$

and

$$\prod_{d \mid N, d \notin R} \Phi_d(X) \mid T(X),$$

yielding $p^k = |A|$, $p^{n-k} = |T|$, thus A satisfies (T1).

(T-S($\mathbb{Z}_N$)), $N = p^n$

Let $A \oplus T = \mathbb{Z}_N$, or equivalently

$$A(X)T(X) \equiv 1 + X + X^2 + \cdots + X^{N-1} \bmod (X^N - 1).$$

As before, $\zeta_{p^{\nu_1}}, \dots, \zeta_{p^{\nu_k}}$ are precisely the roots of $A(X)$, whence

$$E(X) = \prod_{d \in R} \Phi_d(X) \mid A(X),$$

and

$$\prod_{d \mid N, d \notin R} \Phi_d(X) \mid T(X),$$

yielding $p^k = |A|$, $p^{n-k} = |T|$, thus A satisfies (T1).

(T-S($\mathbb{Z}_N$)), $N = p_1^m p_2 \cdots p_n$

Lemma (Coven-Meyerowitz, '98)

Suppose $A \oplus T = \mathbb{Z}_N$ and p a prime such that $p \nmid |T|$. Then $A \oplus (pT) = \mathbb{Z}_N$.

Corollary

Suppose $A \oplus T = \mathbb{Z}_N$ and $M \in \mathbb{N}$ such that $\gcd(|T|, M) = 1$. Then $A \oplus (MT) = \mathbb{Z}_N$.

$(\mathbf{T\text{-}S}(\mathbb{Z}_N))$, $N = p_1^m p_2 \cdots p_n$

Lemma (Coven-Meyerowitz, '98)

Suppose $A \oplus T = \mathbb{Z}_N$ and p a prime such that $p \nmid |T|$. Then $A \oplus (pT) = \mathbb{Z}_N$.

Corollary

Suppose $A \oplus T = \mathbb{Z}_N$ and $M \in \mathbb{N}$ such that $\gcd(|T|, M) = 1$. Then $A \oplus (MT) = \mathbb{Z}_N$.

Corollary

Suppose $A \oplus T = \mathbb{Z}_N$ with N square-free and $M = |A|$. Then $A \oplus (MT) = \mathbb{Z}_N$.

This was used by Łaba and Meyerowitz to prove $(\mathbf{T\text{-}S}(\mathbb{Z}_N))$, for N square-free (Tao's blog, '11).

$(\mathbf{T}\text{-}\mathbf{S}(\mathbb{Z}_N))$, $N = p_1^m p_2 \cdots p_n$

Lemma (Coven-Meyerowitz, '98)

Suppose $A \oplus T = \mathbb{Z}_N$ and p a prime such that $p \nmid |T|$. Then $A \oplus (pT) = \mathbb{Z}_N$.

Corollary

Suppose $A \oplus T = \mathbb{Z}_N$ and $M \in \mathbb{N}$ such that $\gcd(|T|, M) = 1$. Then $A \oplus (MT) = \mathbb{Z}_N$.

Corollary

Suppose $A \oplus T = \mathbb{Z}_N$ with N square-free and $M = |A|$. Then $A \oplus (MT) = \mathbb{Z}_N$.

This was used by Łaba and Meyerowitz to prove $(\mathbf{T}\text{-}\mathbf{S}(\mathbb{Z}_N))$, for N square-free (Tao's blog, '11).

Let $A \oplus T = \mathbb{Z}_N$, with $|A| = M$. Suppose first $\gcd(M, |T|) = 1$. Then $|MT| = |T| = N/M$ and $MT \subseteq M\mathbb{Z}_N$, hence $MT = M\mathbb{Z}_N$. This shows that A tiles by the subgroup $M\mathbb{Z}_N$, whence

$$A(X) \equiv 1 + X + \cdots + X^{M-1} \bmod (X^M - 1),$$

and A clearly satisfies (T2).

Let $A \oplus T = \mathbb{Z}_N$, with $|A| = M$. Suppose first $\gcd(M, |T|) = 1$. Then $|MT| = |T| = N/M$ and $MT \subseteq M\mathbb{Z}_N$, hence $MT = M\mathbb{Z}_N$. This shows that A tiles by the subgroup $M\mathbb{Z}_N$, whence

$$A(X) \equiv 1 + X + \cdots + X^{M-1} \bmod (X^M - 1),$$

and A clearly satisfies (T2).

(T-S($\mathbb{Z}_N$)), $N = p_1^m p_2 \cdots p_n$

Let $A \oplus T = \mathbb{Z}_N$, with $\gcd(|A|, |T|) > 1$. Then

$$\Phi_{p_1^{\ell_1}}(X) \cdots \Phi_{p_1^{\ell_r}}(X) \Phi_{p_2}(X) \cdots \Phi_{p_k}(X) \mid A(X)$$

Let $A \oplus T = \mathbb{Z}_N$, with $\gcd(|A|, |T|) > 1$. Then

$$\Phi_{p_1^{\ell_1}}(X) \cdots \Phi_{p_1^{\ell_r}}(X) \Phi_{p_2}(X) \cdots \Phi_{p_k}(X) \mid A(X)$$

and

$$\Phi_{p_1^{m_1}}(X) \cdots \Phi_{p_1^{m_s}}(X) \Phi_{p_{k+1}}(X) \cdots \Phi_{p_n}(X) \mid T(X),$$

(T-S($\mathbb{Z}_N$)), $N = p_1^m p_2 \cdots p_n$

Let $A \oplus T = \mathbb{Z}_N$, with $\gcd(|A|, |T|) > 1$. Then

$$\Phi_{p_1^{\ell_1}}(X) \cdots \Phi_{p_1^{\ell_r}}(X) \Phi_{p_2}(X) \cdots \Phi_{p_k}(X) \mid A(X)$$

and

$$\Phi_{p_1^{m_1}}(X) \cdots \Phi_{p_1^{m_s}}(X) \Phi_{p_{k+1}}(X) \cdots \Phi_{p_n}(X) \mid T(X),$$

where $\{\ell_1, \ldots, \ell_r\}$ and $\{m_1, \ldots, m_s\}$ form a partition of $\{1, 2, \ldots, m\}$.

(T-S($\mathbb{Z}_N$)), $N = p_1^m p_2 \cdots p_n$

Let $A \oplus T = \mathbb{Z}_N$, with $\gcd(|A|, |T|) > 1$. Then

$$\Phi_{p_1^{\ell_1}}(X) \cdots \Phi_{p_1^{\ell_r}}(X) \Phi_{p_2}(X) \cdots \Phi_{p_k}(X) \mid A(X)$$

and

$$\Phi_{p_1^{m_1}}(X) \cdots \Phi_{p_1^{m_s}}(X) \Phi_{p_{k+1}}(X) \cdots \Phi_{p_n}(X) \mid T(X),$$

where $\{\ell_1, \ldots, \ell_r\}$ and $\{m_1, \ldots, m_s\}$ form a partition of $\{1, 2, \ldots, m\}$. Let $M = p_2 \cdots p_k$, so that $A \oplus (MT) = \mathbb{Z}_N$ and

$$\Phi_{p_1^{m_1}}(X) \cdots \Phi_{p_1^{m_s}}(X) \Phi_{p_{k+1}}(X) \cdots \Phi_{p_n}(X) \mid T(X^M).$$

Let $A \oplus T = \mathbb{Z}_N$, with $\gcd(|A|, |T|) > 1$. Then

$$\Phi_{p_1^{\ell_1}}(X) \cdots \Phi_{p_1^{\ell_r}}(X) \Phi_{p_2}(X) \cdots \Phi_{p_k}(X) \mid A(X)$$

and

$$\Phi_{p_1^{m_1}}(X) \cdots \Phi_{p_1^{m_s}}(X) \Phi_{p_{k+1}}(X) \cdots \Phi_{p_n}(X) \mid T(X),$$

where $\{\ell_1, \ldots, \ell_r\}$ and $\{m_1, \ldots, m_s\}$ form a partition of $\{1, 2, \ldots, m\}$. Let $M = p_2 \cdots p_k$, so that $A \oplus (MT) = \mathbb{Z}_N$ and

$$\Phi_{p_1^{m_1}}(X) \cdots \Phi_{p_1^{m_s}}(X) \Phi_{p_{k+1}}(X) \cdots \Phi_{p_n}(X) \mid T(X^M).$$

Let $d \mid M$ be composite. Then $A(\zeta_d)T(\zeta_d^M) = 0$ and $T(\zeta_d^M) = T(1) \neq 0$, hence $A(\zeta_d) = 0$, confirming (T2) for any set of primes dividing M.

Next, consider $p_1^{\ell_j} d$, where $d \mid M$, $d > 1$.

Let $d \mid M$ be composite. Then $A(\zeta_d)T(\zeta_d^M) = 0$ and $T(\zeta_d^M) = T(1) \neq 0$, hence $A(\zeta_d) = 0$, confirming (T2) for any set of primes dividing M.

Next, consider $p_1^{\ell_j} d$, where $d \mid M$, $d > 1$. We have

$$T(\zeta_{p_1^{\ell_j} d}^M) = T(\zeta_{p_1^{\ell_j}}^{M/d}) = \sigma(T(\zeta_{p_1^{\ell_j}})) \neq 0,$$

for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{\ell_j}})/\mathbb{Q})$, hence $A(\zeta_{p_1^{\ell_j}}) = 0$, confirming (T2) for A completely.

Let $d \mid M$ be composite. Then $A(\zeta_d)T(\zeta_d^M) = 0$ and $T(\zeta_d^M) = T(1) \neq 0$, hence $A(\zeta_d) = 0$, confirming (T2) for any set of primes dividing M.

Next, consider $p_1^{\ell_j} d$, where $d \mid M$, $d > 1$. We have

$$T(\zeta_{p_1^{\ell_j} d}^M) = T(\zeta_{p_1^{\ell_j}}^{M/d}) = \sigma(T(\zeta_{p_1^{\ell_j}})) \neq 0,$$

for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{\ell_j}})/\mathbb{Q})$, hence $A(\zeta_{p_1^{\ell_j}}) = 0$, confirming (T2) for A completely.

Vanishing sums of roots of unity

Lemma

Let $\mathrm{rad}(N) = pq$ *and* $A(X) \in \mathbb{Z}[X]$ *with nonnegative coefficients, such that* $A(\zeta_N^d) = 0$*, for some* $d \mid N$*. Then,*

$$A(X^d) \equiv P(X^d)\Phi_p(X^{N/p}) + Q(X^d)\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

where $P(X), Q(X) \in \mathbb{Z}[X]$ *can be taken with nonnegative coefficients.*

- The polynomial $A(X^d)$ is the mask polynomial of the multiset $d \cdot A$.

Vanishing sums of roots of unity

Lemma

Let $\mathrm{rad}(N) = pq$ *and* $A(X) \in \mathbb{Z}[X]$ *with nonnegative coefficients, such that* $A(\zeta_N^d) = 0$*, for some* $d \mid N$*. Then,*

$$A(X^d) \equiv P(X^d)\Phi_p(X^{N/p}) + Q(X^d)\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

where $P(X), Q(X) \in \mathbb{Z}[X]$ *can be taken with nonnegative coefficients.*

- The polynomial $A(X^d)$ is the mask polynomial of the multiset $d \cdot A$.
- $\Phi_p(X^{N/p})$ is the mask polynomial of the subgroup $\frac{N}{p}\mathbb{Z}_N$. Its cosets are called p-cycles.

Vanishing sums of roots of unity

Lemma

Let $\mathrm{rad}(N) = pq$ *and* $A(X) \in \mathbb{Z}[X]$ *with nonnegative coefficients, such that* $A(\zeta_N^d) = 0$*, for some* $d \mid N$*. Then,*

$$A(X^d) \equiv P(X^d)\Phi_p(X^{N/p}) + Q(X^d)\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

where $P(X), Q(X) \in \mathbb{Z}[X]$ *can be taken with nonnegative coefficients.*

- The polynomial $A(X^d)$ is the mask polynomial of the multiset $d \cdot A$.
- $\Phi_p(X^{N/p})$ is the mask polynomial of the subgroup $\frac{N}{p}\mathbb{Z}_N$. Its cosets are called p-cycles.
- The above Lemma shows that if $A(\zeta_N) = 0$, then A is the disjoint union of p- and q-cycles.

Vanishing sums of roots of unity

Lemma

Let $\mathrm{rad}(N) = pq$ *and* $A(X) \in \mathbb{Z}[X]$ *with nonnegative coefficients, such that* $A(\zeta_N^d) = 0$*, for some* $d \mid N$*. Then,*

$$A(X^d) \equiv P(X^d)\Phi_p(X^{N/p}) + Q(X^d)\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

where $P(X), Q(X) \in \mathbb{Z}[X]$ *can be taken with nonnegative coefficients.*

- The polynomial $A(X^d)$ is the mask polynomial of the multiset $d \cdot A$.
- $\Phi_p(X^{N/p})$ is the mask polynomial of the subgroup $\frac{N}{p}\mathbb{Z}_N$. Its cosets are called p-cycles.
- The above Lemma shows that if $A(\zeta_N) = 0$, then A is the disjoint union of p- and q-cycles.

(S-T($\mathbb{Z}_N$)), $N = pq$

Let (A, B) be a spectral pair in $\mathbb{Z}_N$. Wlog, $0 \in A \cap B$ and each of A, B generates $\mathbb{Z}_N$.

Lemma

Let $0 \in A \subseteq \mathbb{Z}_N$, such that A generates $\mathbb{Z}_N$, $N = p^m q^n$. Then,

$$(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing.$$

(S-T($\mathbb{Z}_N$)), $N = pq$

Let (A, B) be a spectral pair in $\mathbb{Z}_N$. Wlog, $0 \in A \cap B$ and each of A, B generates $\mathbb{Z}_N$.

Lemma

Let $0 \in A \subseteq \mathbb{Z}_N$, such that A generates $\mathbb{Z}_N$, $N = p^m q^n$. Then,

$$(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing.$$

Proof.

There are $a \notin p\mathbb{Z}_N$ and $a' \notin q\mathbb{Z}_N$.

(S-T($\mathbb{Z}_N$)), $N = pq$

Let (A, B) be a spectral pair in $\mathbb{Z}_N$. Wlog, $0 \in A \cap B$ and each of A, B generates $\mathbb{Z}_N$.

Lemma

Let $0 \in A \subseteq \mathbb{Z}_N$, such that A generates $\mathbb{Z}_N$, $N = p^m q^n$. Then,

$$(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing.$$

Proof.

There are $a \notin p\mathbb{Z}_N$ and $a' \notin q\mathbb{Z}_N$. If $a \notin q\mathbb{Z}_N$, then $a \in \mathbb{Z}_N^\star$,

(S-T($\mathbb{Z}_N$)), $N = pq$

Let (A, B) be a spectral pair in $\mathbb{Z}_N$. Wlog, $0 \in A \cap B$ and each of A, B generates $\mathbb{Z}_N$.

Lemma

Let $0 \in A \subseteq \mathbb{Z}_N$, such that A generates $\mathbb{Z}_N$, $N = p^m q^n$. Then,

$$(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing.$$

Proof.

There are $a \notin p\mathbb{Z}_N$ and $a' \notin q\mathbb{Z}_N$. If $a \notin q\mathbb{Z}_N$, then $a \in \mathbb{Z}_N^\star$, and similarly, if $a' \notin p\mathbb{Z}_N$, then $a' \in \mathbb{Z}_N^\star$.

(S-T($\mathbb{Z}_N$)), $N = pq$

Let (A, B) be a spectral pair in $\mathbb{Z}_N$. Wlog, $0 \in A \cap B$ and each of A, B generates $\mathbb{Z}_N$.

Lemma

Let $0 \in A \subseteq \mathbb{Z}_N$, such that A generates $\mathbb{Z}_N$, $N = p^m q^n$. Then,

$$(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing.$$

Proof.

There are $a \notin p\mathbb{Z}_N$ and $a' \notin q\mathbb{Z}_N$. If $a \notin q\mathbb{Z}_N$, then $a \in \mathbb{Z}_N^\star$, and similarly, if $a' \notin p\mathbb{Z}_N$, then $a' \in \mathbb{Z}_N^\star$. If $a \in q\mathbb{Z}_N$ and $a' \in p\mathbb{Z}_N$, then $a - a' \in \mathbb{Z}_N^\star$. □

(S-T($\mathbb{Z}_N$)), $N = pq$

Let (A, B) be a spectral pair in $\mathbb{Z}_N$. Wlog, $0 \in A \cap B$ and each of A, B generates $\mathbb{Z}_N$.

Lemma

Let $0 \in A \subseteq \mathbb{Z}_N$, such that A generates $\mathbb{Z}_N$, $N = p^m q^n$. Then,

$$(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing.$$

Proof.

There are $a \notin p\mathbb{Z}_N$ and $a' \notin q\mathbb{Z}_N$. If $a \notin q\mathbb{Z}_N$, then $a \in \mathbb{Z}_N^\star$, and similarly, if $a' \notin p\mathbb{Z}_N$, then $a' \in \mathbb{Z}_N^\star$. If $a \in q\mathbb{Z}_N$ and $a' \in p\mathbb{Z}_N$, then $a - a' \in \mathbb{Z}_N^\star$. □

Therefore,

$$(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing \neq (B - B) \cap \mathbb{Z}_N^\star,$$

which implies

$$A(\zeta_N) = B(\zeta_N) = 0.$$

(S-T($\mathbb{Z}_N$)), $N = pq$

Therefore,

$$(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing \neq (B - B) \cap \mathbb{Z}_N^\star,$$

which implies

$$A(\zeta_N) = B(\zeta_N) = 0.$$

Theorem (Lam & Leung)

If $A \subseteq \mathbb{Z}_N$ with $A(\zeta_N) = \sum_{a \in A} \zeta_N^a = 0$, $N = p^m q^n$, then A is a disjoint union of cosets of the subgroups $\frac{N}{p}\mathbb{Z}_N$ and $\frac{N}{q}\mathbb{Z}_N$.

(S-T($\mathbb{Z}_N$)), $N = pq$

Therefore,

$$(A-A)\cap\mathbb{Z}_N^\star \neq \varnothing \neq (B-B)\cap\mathbb{Z}_N^\star,$$

which implies

$$A(\zeta_N) = B(\zeta_N) = 0.$$

Theorem (Lam & Leung)

If $A\subseteq\mathbb{Z}_N$ with $A(\zeta_N)=\sum_{a\in A}\zeta_N^a=0$, $N=p^mq^n$, then A is a disjoint union of cosets of the subgroups $\frac{N}{p}\mathbb{Z}_N$ and $\frac{N}{q}\mathbb{Z}_N$.

Any two cosets of $p\mathbb{Z}_{pq}$ and $q\mathbb{Z}_{pq}$ intersect, so A (and B) is a disjoint union of cosets of $p\mathbb{Z}_{pq}$ (say).

Therefore,

$$(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing \neq (B - B) \cap \mathbb{Z}_N^\star,$$

which implies

$$A(\zeta_N) = B(\zeta_N) = 0.$$

Theorem (Lam & Leung)

If $A \subseteq \mathbb{Z}_N$ with $A(\zeta_N) = \sum_{a \in A} \zeta_N^a = 0$, $N = p^m q^n$, then A is a disjoint union of cosets of the subgroups $\frac{N}{p}\mathbb{Z}_N$ and $\frac{N}{q}\mathbb{Z}_N$.

Any two cosets of $p\mathbb{Z}_{pq}$ and $q\mathbb{Z}_{pq}$ intersect, so A (and B) is a disjoint union of cosets of $p\mathbb{Z}_{pq}$ (say).

(S-T($\mathbb{Z}_N$)), $N = pq$

Since B is also a union of cosets of $p\mathbb{Z}_{pq}$, we have $p\mathbb{Z}_{pq} \subseteq B - B$, hence

$$A(\zeta_q) = 0.$$

If $A(\zeta_p) = 0$, then $p \mid |A|$ and $A = \mathbb{Z}_N$.

(S-T($\mathbb{Z}_N$)), $N = pq$

Since B is also a union of cosets of $p\mathbb{Z}_{pq}$, we have $p\mathbb{Z}_{pq} \subseteq B - B$, hence

$$A(\zeta_q) = 0.$$

If $A(\zeta_p) = 0$, then $p \mid |A|$ and $A = \mathbb{Z}_N$. Otherwise, $(B - B) \cap q\mathbb{Z}_{pq} = \{0\}$, hence each element of B is unique $\bmod q$, giving $|A| \leq q$.

(S-T($\mathbb{Z}_N$)), $N = pq$

Since B is also a union of cosets of $p\mathbb{Z}_{pq}$, we have $p\mathbb{Z}_{pq} \subseteq B - B$, hence

$$A(\zeta_q) = 0.$$

If $A(\zeta_p) = 0$, then $p \mid |A|$ and $A = \mathbb{Z}_N$. Otherwise, $(B - B) \cap q\mathbb{Z}_{pq} = \{0\}$, hence each element of B is unique $\bmod q$, giving $|A| \leq q$. Thus, A is a single coset of $p\mathbb{Z}_{pq}$, which tiles $\mathbb{Z}_{pq}$.

(S-T($\mathbb{Z}_N$)), $N = pq$

Since B is also a union of cosets of $p\mathbb{Z}_{pq}$, we have $p\mathbb{Z}_{pq} \subseteq B - B$, hence

$$A(\zeta_q) = 0.$$

If $A(\zeta_p) = 0$, then $p \mid |A|$ and $A = \mathbb{Z}_N$. Otherwise, $(B - B) \cap q\mathbb{Z}_{pq} = \{0\}$, hence each element of B is unique $\bmod q$, giving $|A| \leq q$. Thus, A is a single coset of $p\mathbb{Z}_{pq}$, which tiles $\mathbb{Z}_{pq}$.

$(\mathbf{S}\text{-}\mathbf{T}(\mathbb{Z}_N))$, $N = p^m q^n$ (sketch)

1. Suppose $(\mathbf{S}\text{-}\mathbf{T}(\mathbb{Z}_N))$ fails, but holds for any proper subgroup of $\mathbb{Z}_N$.
2. Let $A \subseteq \mathbb{Z}_N$ be a maximal spectral non-tile, with spectrum B.

(S-T($\mathbb{Z}_N$)), $N = p^m q^n$ (sketch)

1. Suppose **(S-T($\mathbb{Z}_N$))** fails, but holds for any proper subgroup of $\mathbb{Z}_N$.
2. Let $A \subseteq \mathbb{Z}_N$ be a maximal spectral non-tile, with spectrum B.
3. Both A and B must be *primitive*, which implies $A(\zeta_N) = B(\zeta_N) = 0$.
4. This in turn implies $A(\zeta_p) = A(\zeta_q) = B(\zeta_p) = B(\zeta_q) = 0$.

(S-T($\mathbb{Z}_N$)), $N = p^m q^n$ (sketch)

1. Suppose **(S-T($\mathbb{Z}_N$))** fails, but holds for any proper subgroup of $\mathbb{Z}_N$.
2. Let $A \subseteq \mathbb{Z}_N$ be a maximal spectral non-tile, with spectrum B.
3. Both A and B must be *primitive*, which implies $A(\zeta_N) = B(\zeta_N) = 0$.
4. This in turn implies $A(\zeta_p) = A(\zeta_q) = B(\zeta_p) = B(\zeta_q) = 0$.
5. Actually, both $A(X)$ and $B(X)$ vanish at $\zeta_{pq}, \zeta_{p^m}, \zeta_{q^n}, \zeta_{p^m q}, \zeta_{pq^n}$. If $p < q$, they both vanish at ζ_{p^2}.

$(\mathbf{S\text{-}T}(\mathbb{Z}_N))$, $N = p^m q^n$ (sketch)

1. Suppose $(\mathbf{S\text{-}T}(\mathbb{Z}_N))$ fails, but holds for any proper subgroup of $\mathbb{Z}_N$.
2. Let $A \subseteq \mathbb{Z}_N$ be a maximal spectral non-tile, with spectrum B.
3. Both A and B must be *primitive*, which implies $A(\zeta_N) = B(\zeta_N) = 0$.
4. This in turn implies $A(\zeta_p) = A(\zeta_q) = B(\zeta_p) = B(\zeta_q) = 0$.
5. Actually, both $A(X)$ and $B(X)$ vanish at $\zeta_{pq}, \zeta_{p^m}, \zeta_{q^n}, \zeta_{p^m q}, \zeta_{pq^n}$. If $p < q$, they both vanish at ζ_{p^2}.
6. If $A(X)$ vanishes at $\zeta_{p^{m_1}}, \dots, \zeta_{p^{m_r}}, \zeta_{q^{n_1}}, \dots, \zeta_{q^{n_s}}$, then
$$p^{r+1} q^{s+1} \mid |A|.$$
This establishes a contradiction if either m or n is small, or $p^{m-2} < q^4$.

(S-T($\mathbb{Z}_N$)), $N = p^m q^n$ (sketch)

1. Suppose **(S-T($\mathbb{Z}_N$))** fails, but holds for any proper subgroup of $\mathbb{Z}_N$.
2. Let $A \subseteq \mathbb{Z}_N$ be a maximal spectral non-tile, with spectrum B.
3. Both A and B must be *primitive*, which implies $A(\zeta_N) = B(\zeta_N) = 0$.
4. This in turn implies $A(\zeta_p) = A(\zeta_q) = B(\zeta_p) = B(\zeta_q) = 0$.
5. Actually, both $A(X)$ and $B(X)$ vanish at $\zeta_{pq}, \zeta_{p^m}, \zeta_{q^n}, \zeta_{p^m q}, \zeta_{pq^n}$. If $p < q$, they both vanish at ζ_{p^2}.
6. If $A(X)$ vanishes at $\zeta_{p^{m_1}}, \dots, \zeta_{p^{m_r}}, \zeta_{q^{n_1}}, \dots, \zeta_{q^{n_s}}$, then

$$p^{r+1} q^{s+1} \mid |A|.$$

This establishes a contradiction if either m or n is small, or $p^{m-2} < q^4$.

Cyclic groups

The following hold for cyclic groups $G = \mathbb{Z}_N$:

- If $N = p_1^n p_2 \cdots p_m$, then **(T-S($\mathbb{Z}_N$))** (M, '20).

Cyclic groups

The following hold for cyclic groups $G = \mathbb{Z}_N$:

- If $N = p_1^n p_2 \cdots p_m$, then **(T-S**$(\mathbb{Z}_N)$**)** (M, '20).
- If $N = p^m q^n$, then **(T-S**$(\mathbb{Z}_N)$**)** (Łaba, '02).

Cyclic groups

The following hold for cyclic groups $G = \mathbb{Z}_N$:

- If $N = p_1^n p_2 \cdots p_m$, then **(T-S**$(\mathbb{Z}_N)$**)** (M, '20).
- If $N = p^m q^n$, then **(T-S**$(\mathbb{Z}_N)$**)** (Łaba, '02).
- Fuglede's conjecture holds if $N = p^2 qr$ (Somlai, '19).

Cyclic groups

The following hold for cyclic groups $G = \mathbb{Z}_N$:

- If $N = p_1^n p_2 \cdots p_m$, then **(T-S($\mathbb{Z}_N$))** (M, '20).
- If $N = p^m q^n$, then **(T-S($\mathbb{Z}_N$))** (Łaba, '02).
- Fuglede's conjecture holds if $N = p^2 qr$ (Somlai, '19).
- Let $p < q$; Fuglede's conjecture holds if $N = p^m q^n$ with $m \leq 9$ or $n \leq 6$ (M, '20).

Cyclic groups

The following hold for cyclic groups $G = \mathbb{Z}_N$:

- If $N = p_1^n p_2 \cdots p_m$, then **(T-S**($\mathbb{Z}_N$)**)** (M, '20).
- If $N = p^m q^n$, then **(T-S**($\mathbb{Z}_N$)**)** (Łaba, '02).
- Fuglede's conjecture holds if $N = p^2 qr$ (Somlai, '19).
- Let $p < q$; Fuglede's conjecture holds if $N = p^m q^n$ with $m \leq 9$ or $n \leq 6$ (M, '20).
- Let $p < q$; Fuglede's conjecture holds if $N = p^m q^n$ with $p^{m-2} < q^4$ (M, '20).

Cyclic groups

The following hold for cyclic groups $G = \mathbb{Z}_N$:

- If $N = p_1^n p_2 \cdots p_m$, then **(T-S**$(\mathbb{Z}_N)$**)** (M, '20).
- If $N = p^m q^n$, then **(T-S**$(\mathbb{Z}_N)$**)** (Łaba, '02).
- Fuglede's conjecture holds if $N = p^2 qr$ (Somlai, '19).
- Let $p < q$; Fuglede's conjecture holds if $N = p^m q^n$ with $m \leq 9$ or $n \leq 6$ (M, '20).
- Let $p < q$; Fuglede's conjecture holds if $N = p^m q^n$ with $p^{m-2} < q^4$ (M, '20).
- Fuglede's conjecture holds if $N = pqrs$ (Kiss, M, Somlai, Vizer, '20).

Cyclic groups

The following hold for cyclic groups $G = \mathbb{Z}_N$:

- If $N = p_1^n p_2 \cdots p_m$, then **(T-S**$(\mathbb{Z}_N)$**)** (M, '20).
- If $N = p^m q^n$, then **(T-S**$(\mathbb{Z}_N)$**)** (Łaba, '02).
- Fuglede's conjecture holds if $N = p^2 qr$ (Somlai, '19).
- Let $p < q$; Fuglede's conjecture holds if $N = p^m q^n$ with $m \leq 9$ or $n \leq 6$ (M, '20).
- Let $p < q$; Fuglede's conjecture holds if $N = p^m q^n$ with $p^{m-2} < q^4$ (M, '20).
- Fuglede's conjecture holds if $N = pqrs$ (Kiss, M, Somlai, Vizer, '20).
- If $N = (pqr)^2$, then **(T-S**$(\mathbb{Z}_N)$**)** (Łaba, Londner, '21).

Cyclic groups

The following hold for cyclic groups $G = \mathbb{Z}_N$:

- If $N = p_1^n p_2 \cdots p_m$, then **(T-S**$(\mathbb{Z}_N)$**)** (M, '20).
- If $N = p^m q^n$, then **(T-S**$(\mathbb{Z}_N)$**)** (Łaba, '02).
- Fuglede's conjecture holds if $N = p^2 qr$ (Somlai, '19).
- Let $p < q$; Fuglede's conjecture holds if $N = p^m q^n$ with $m \leq 9$ or $n \leq 6$ (M, '20).
- Let $p < q$; Fuglede's conjecture holds if $N = p^m q^n$ with $p^{m-2} < q^4$ (M, '20).
- Fuglede's conjecture holds if $N = pqrs$ (Kiss, M, Somlai, Vizer, '20).
- If $N = (pqr)^2$, then **(T-S**$(\mathbb{Z}_N)$**)** (Łaba, Londner, '21).

Thank you