Vanishing Sums of Roots of Unity: from Integer Tilings to Projections of Fractal Sets

University of Lethbridge–Iniskim
Number Theory and Combinatorics Seminar

Caleb Marshall (they/them or he/him)

October 2025

Land Acknowledgement

- Most of my research and study was conducted at the UBC (Vancouver) campus, which sits on the traditional, ancestral, and unceded territory of the Musqueam First Nation.
- This talk takes place in traditional Blackfoot Confederacy territory. As a visitor, I wish to honour the Blackfoot people and their traditional ways of knowing and caring for this land.

Overview

1. What are VSRU's?
2. Elementary Size Bounds for VSRU's & Extensions
3. Multiscale VSRU's and Size Bounds
4. Applications (or, better: *Here There Be Dragons*)

What are VSRU's?

The Definition

Definition (Vanishing Sums of Roots of Unity (VSRU's))

Suppose that $z_1, ..., z_K \in \mathbb{C}$ are **roots of unity**, so that

$$z_j := e^{2\pi i(a_j/N_j)}, \text{ for some } a_j \in \mathbb{Z}, N_j \in \mathbb{N}$$

and that

$$z_1 + \cdots + z_K = 0.$$

We call such a sum a **vanishing sum of roots of unity** (VSRU).

A Motivating Example: Regular Polygons

Example

Let $K \geq 2$ and suppose that $z_j := e^{2\pi i((j-1)/K)}$ for each $j = 1, ..., K$. The $z_1, ..., z_K$ then form a geometric series

$$z_1 + \cdots + z_K = \sum_{j=0}^{K-1} \left(e^{2\pi i/K}\right)^j = \frac{\left(e^{2\pi i/K}\right)^K - 1}{e^{2\pi i/K} - 1} = 0.$$

When $K = 2$, this becomes the famous *Euler's equation*

$$1 + e^{\pi i} = e^{2\pi i(0/2)} + e^{2\pi i(1/2)} = 0,$$

which many might have seen in their first complex analysis course (more on analysis later...)

The Geometry of VSRU's

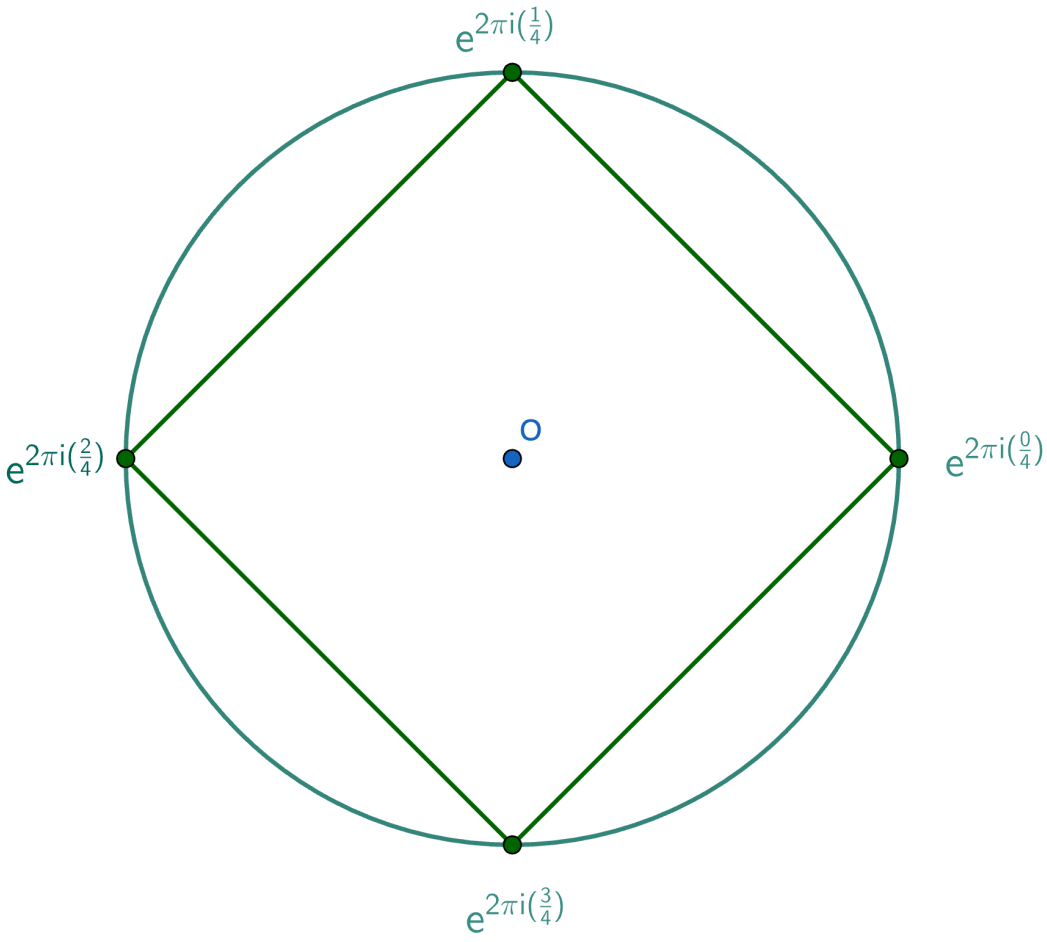

Figure: The previous example has a geometric interpretation as *regular polygons* on the complex unit circle.

Classifying VSRU's

We can now ask the following very general question.

Question

What fundamental structures characterize vanishing sums of roots of unity? Put another way: can we classify all possible VSRU's in a mathematically-rigorous manner?

This question has multiple mathematically well-posed answers, while still leaving many mysteries in its wake. Let's dive in!

Building VSRU's

Starting with what we know from the previous slides, let's start building more complicated VSRU's (by using simple, sneaky tricks).

Example (Rotations)

If $z_1, ..., z_K$ form a VSRU, and $\zeta \in \mathbb{C}$, then (of course!)

$$\zeta(z_1 + \cdots + z_K) = 0, \tag{1}$$

and so if we further require that ζ is a root of unity, then (1) is, itself, a VSRU.

Example (Sums)

If $z_1, ..., z_K$ and $w_1, ..., w_L$ both form VSRU's, then

$$(z_1 + \cdots + z_K) + (w_1 + \cdots + w_L) = 0 + 0 = 0,$$

and so $z_1, ..., z_K, w_1, ..., w_L$ again form a VSRU.

Building VSRU's: Rotations

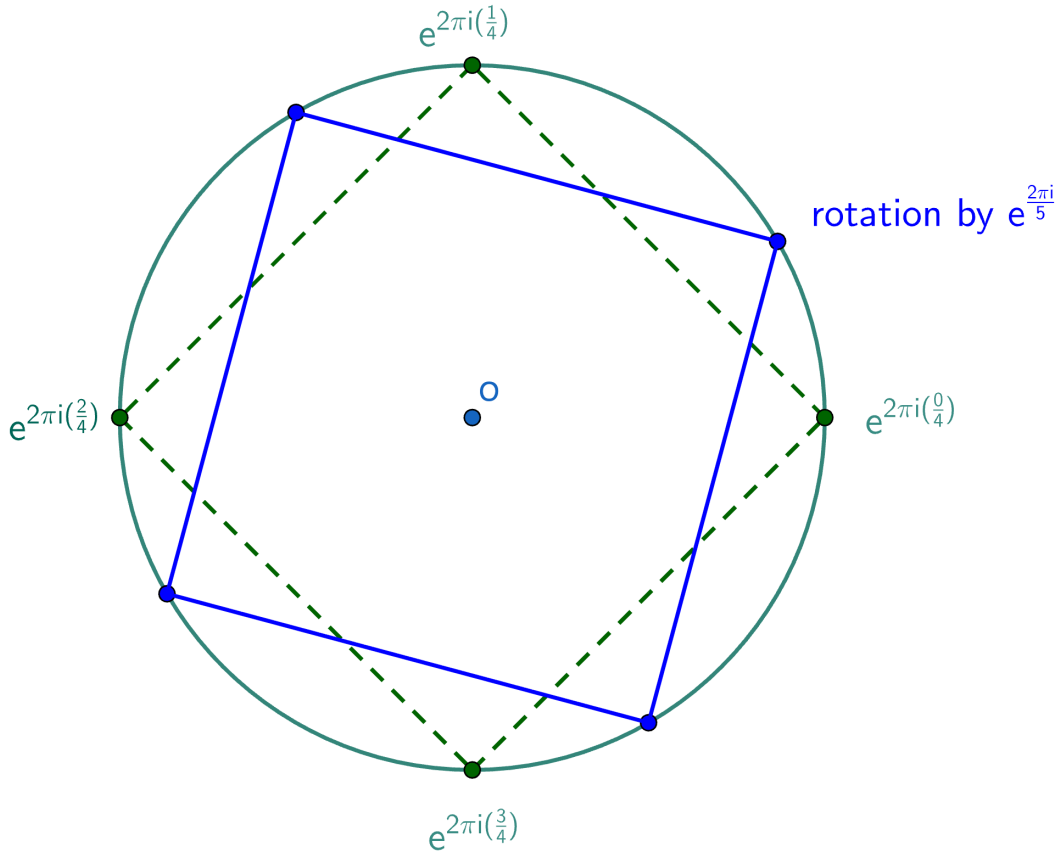

Figure: A rotation of a VSRU produces another VSRU.

Building VSRU's: Sums

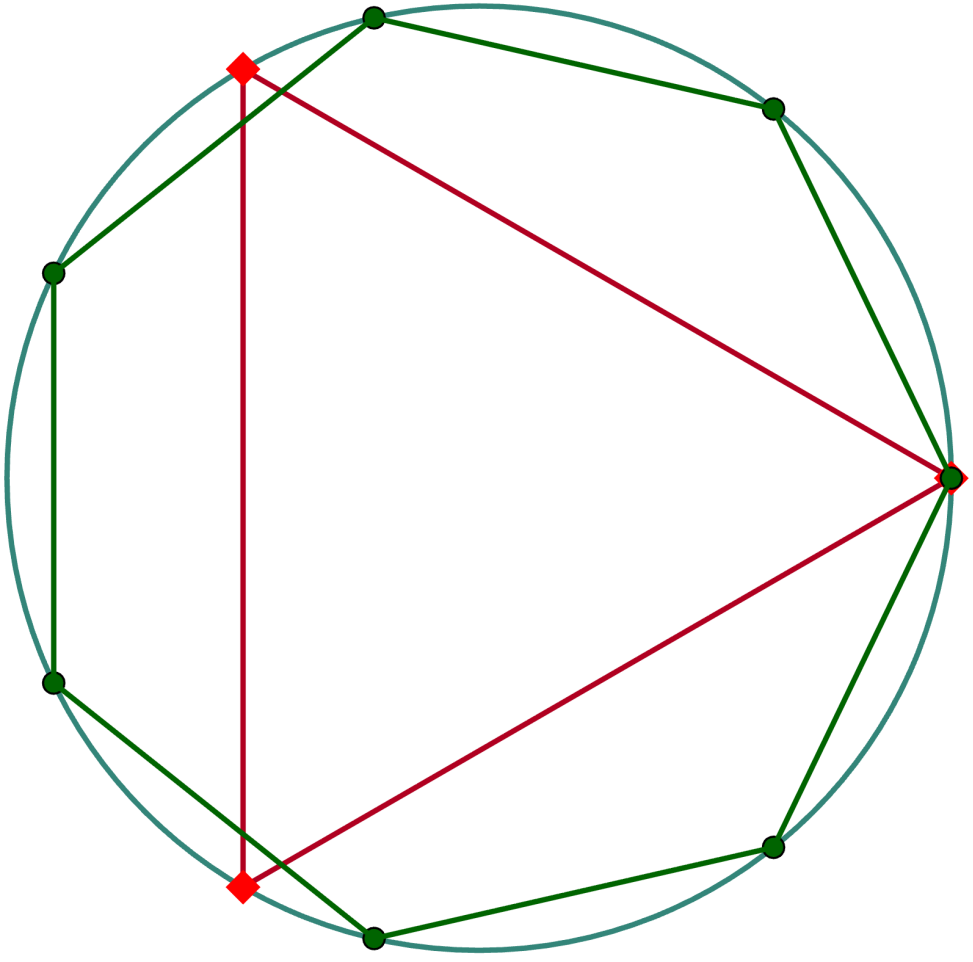

Figure: Adding together two VSRU's produces another VSRU.

Minimal VSRU's

The previous picture leads us to the following critical definition.

Definition (Minimality)

A VSRU is called **minimal** if no proper, non-empty sub-sum vanishes. That is, if

$$z_1 + \cdots + z_K = 0$$

and $\emptyset \neq \{z_{i_1}, ..., z_{i_L}\} \subsetneq \{z_1, ..., z_K\}$, then

$$z_{i_1} + \cdots + z_{i_L} \neq 0.$$

Proposition (Reality Check—Rotations and Sums)

Any rotation of a minimal VSRU is minimal. However, the positive sum of two (non-empty) minimal VSRU's is never minimal.

Why prime? Consider 4*th*-roots again!

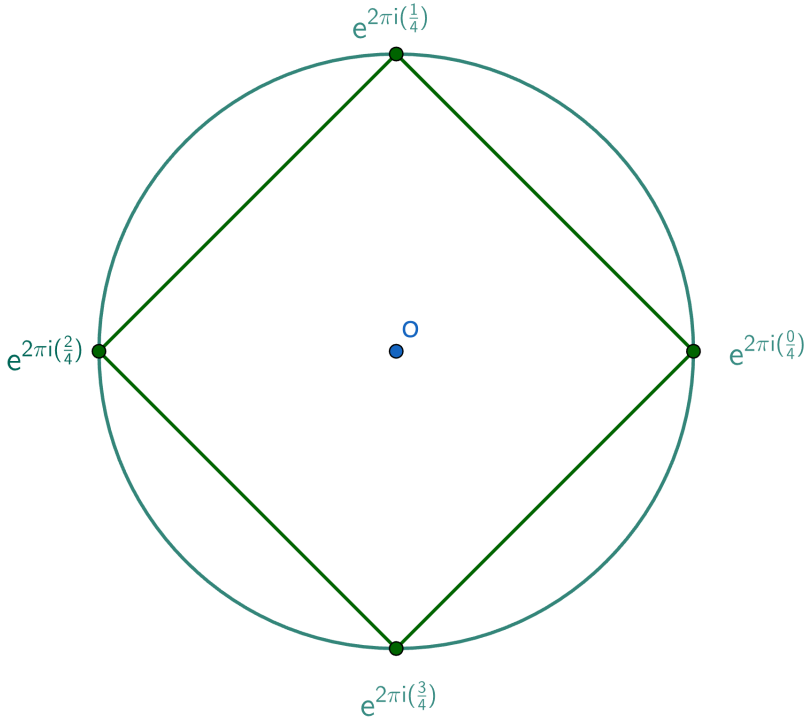

Figure: The previous example has a geometric interpretation as *regular polygons* on the complex unit circle.

Temptation to declare that all minimal VSRU's are just rotations of **prime** polygons...

We Almost Got Away With It...

Example

VSRU's can become quite complicated rather quickly:

$$\begin{aligned} & e^{2\pi i(\frac{1}{7})} + e^{2\pi i(\frac{1}{6})} + e^{2\pi i(\frac{2}{7})} \\ + \quad & e^{2\pi i(\frac{3}{7})} + e^{2\pi i(\frac{4}{7})} + e^{2\pi i(\frac{5}{7})} + e^{2\pi i(\frac{5}{6})} + e^{2\pi i(\frac{6}{7})} = 0. \end{aligned}$$

Two questions:

- Can we quickly verify that the above equality is, in fact, correct?
- How on *earth* do we come up with these more complicated VSRU's?

We Almost Got Away With It...

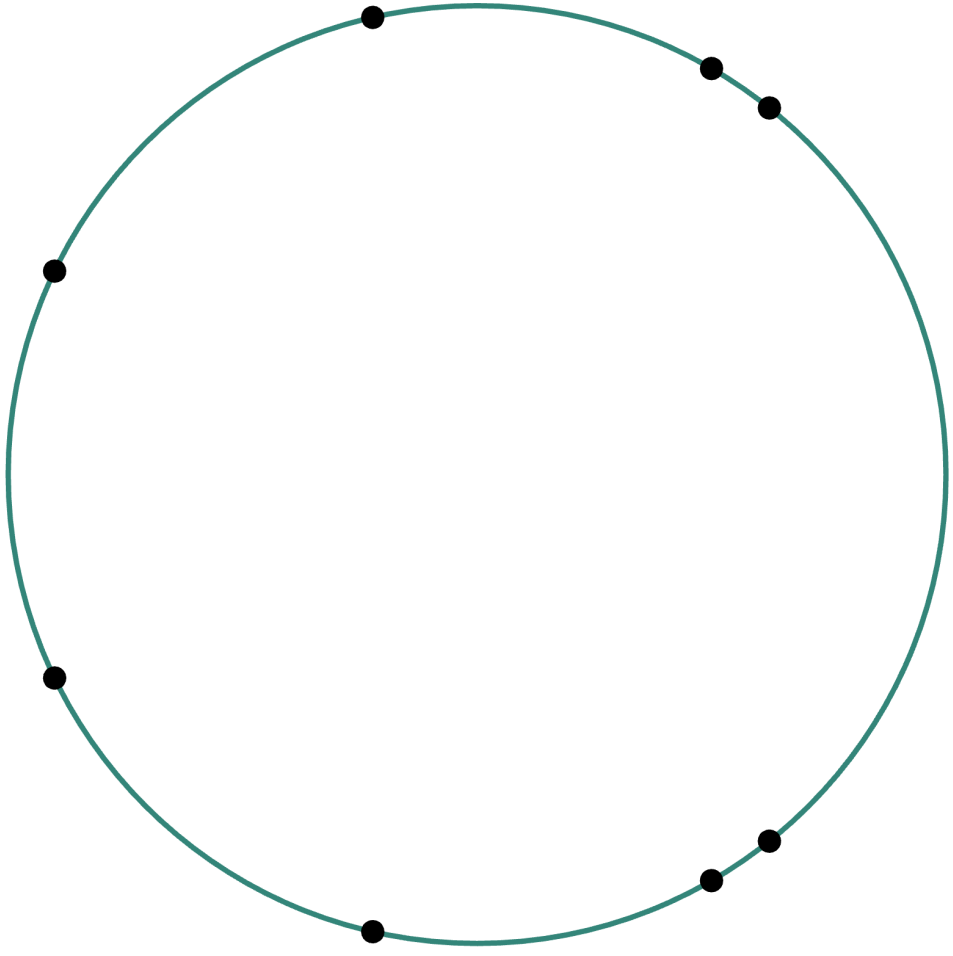

Figure: Another VSRU, but one which is decidedly **not** a regular polygon!

We Almost Got Away With It...

Example

In fact, the previous VSRU can be re-written as:

$$\underbrace{\left(1 + e^{2\pi i(\frac{1}{7})} + e^{2\pi i(\frac{2}{7})} + e^{2\pi i(\frac{3}{7})} + e^{2\pi i(\frac{4}{7})} + e^{2\pi i(\frac{5}{7})} + e^{2\pi i(\frac{6}{7})}\right)}_{\text{heptagon}}$$

$$+ \quad e^{2\pi i(\frac{1}{3})} \underbrace{\left(1 + e^{2\pi i(\frac{1}{2})}\right)}_{\text{segment}} + e^{2\pi i(\frac{2}{3})} \underbrace{\left(1 + e^{2\pi i(\frac{1}{2})}\right)}_{\text{segment}}$$

$$- \quad \underbrace{\left(1 + e^{2\pi i(\frac{1}{3})} + e^{2\pi i(\frac{2}{3})}\right)}_{\text{triangle}}$$

(In fact, this is the way I wrote it when first preparing the talk. Presentation order is (intentionally!) backwards.)

We Almost Got Away With It....

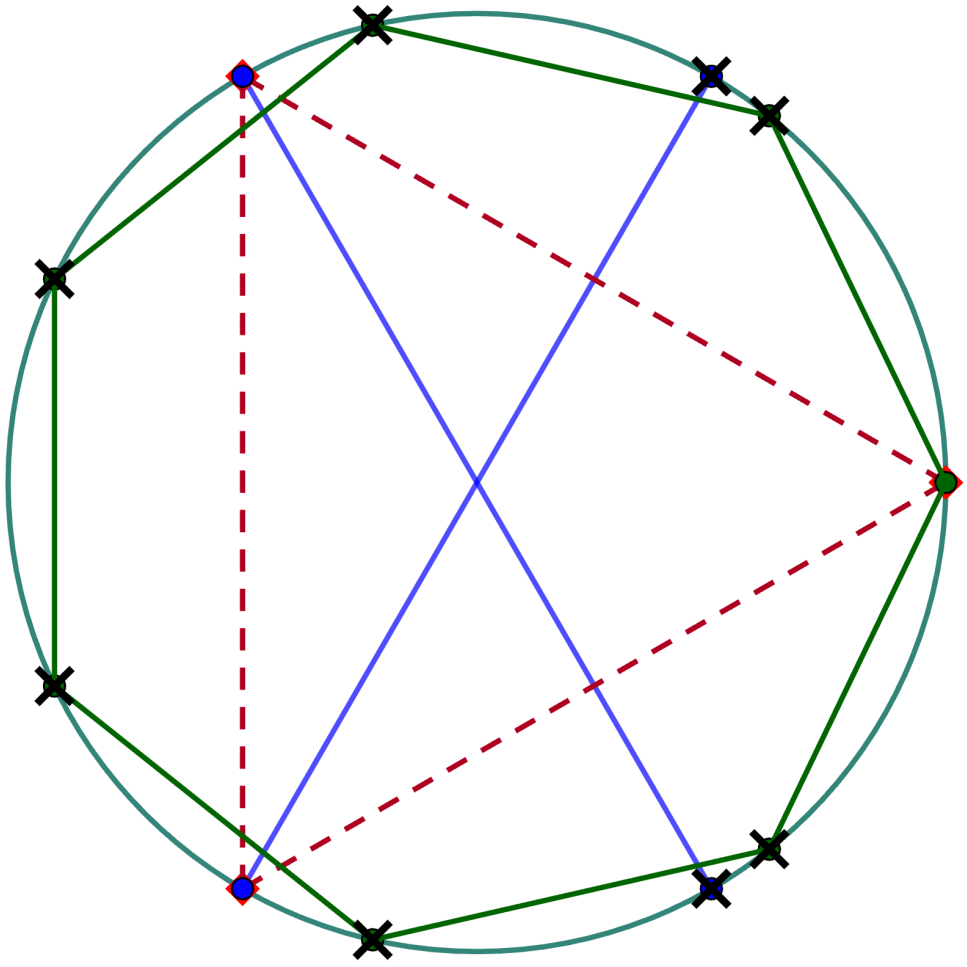

Figure: With the previous calculation made plain, we can now overlay our polygons to better understand our VSRU.

Linear Combinations of Regular Polygons

This leads us to the following (geometric) characterizations of VSRU's, which is due to (multiple separate results) from Rédei, de Bruijn and Schoenberg.

Theorem (Rédei-de Bruijn-Schoenberg Structure Result, 1965–1998)

Any vanishing sum of roots of unity is the linear combination of (rationally) rotated copies of prime order polygons with integer (but **not** *necessarily non-negative) coefficients.*

More flexible version of this coming later on!

Elementary Size Bounds for VSRU's & Extensions

Complexity and Size

This motivates the following notation for VSRU's.

Definition (Writing in a "Common Base")

If $z_1, ..., z_K$ form a VSRU, we will always assume that each z_j is written as a (not necessarily primitive) N-th root of unity, for some *fixed* $N \geq 2$.

Can think of parameter N as the level of **complexity** of the VSRU.

Question

Given a list $z_1, ..., z_K$ of roots of unity all written in some common base $N \geq 2$, can we determine, purely from the relationship of K to N, whether the $z_1,...,z_K$ form a VSRU?

The Lam-Leung Theorem

The main *combinatorial* tool for studying VSRU's are *size bounds*. These relate the complexity (i.e. the parameter $N \geq 2$) to the total number of terms $K \geq 2$. The most general result is the following.

Theorem (Lam-Leung Size Bound, 1990)

Suppose that $z_1, ..., z_K$ are N-th roots of unity, with

$$z_1 + \cdots + z_K = 0$$

and let $N := \prod_j p_j^{n_j}$ denote the prime factorization of N. Then, there exist non-negative integers ω_j such that

$$K := \sum_j \omega_j p_j.$$

In particular,

$$K \geq \min\{p \in \mathbb{N} : p \mid N \ \textit{and}\ p\ \textit{is prime}\}.$$

From VSRU's to (Cyclotomic) Polynomial Division

We recall the following definition.

Definition

The N-**th cyclotomic polynomial** $\Phi_N(X) \in \mathbb{Z}[X]$ is the unique, monic and irreducible polynomial whose roots are the *primitive* N-th roots of unity. In other words:

$$\Phi_N(\zeta) = 0 \Leftrightarrow \zeta = e^{\frac{2\pi i d}{N}} \text{ and } \gcd(d, N) = 1.$$

For $M \geq 2$, a *recursive* definition of the cyclotomic polynomials:

$$X^M - 1 = \prod_{N|M} \Phi_N(X).$$

We will now connect VSRU's to cyclotomic divisibility of polynomials $A(X) \in \mathbb{Z}[X]$ with non-negative coefficients.

From VSRU's to (Cyclotomic) Polynomial Division

Let $N \geq 2$ and suppose that $z_1, ..., z_K$ are N-th roots of unity. Define a polynomial $A(X) \in \mathbb{Z}[X]$ by writing

$$A(X) := \sum_{a=0}^{N-1} w(a) X^a,$$

where

$$w(a) := \#\{\ell \in \{1, ..., K\} : z_\ell := e^{2\pi i a_\ell / N} \text{ and } a \equiv a_\ell \bmod N\}$$

Proposition

The following conditions are equivalent.

1. $z_1 + \cdots + z_K = 0$
2. $\Phi_N(X) \mid A(X)$

The Lam-Leung Bound: Polynomial Version

Let us revisit our original bound for VSRU's in this new language.

Theorem (Lam-Leung, 1990)

Suppose that $A(X) \in \mathbb{Z}[X]$ *has non-negative coefficients and that* $\Phi_N(X) \mid A(X)$. *Then, we have the bound*

$$A(1) \geq \min\{p \in \mathbb{N} : p \mid N \text{ and } p \text{ is prime}\}. \tag{2}$$

While the above is *equivalent* to the original bound of Lam-Leung (as stated for VSRU's); however, it is a more flexible framework.

Question

Let $N_1, ..., N_J \in \mathbb{N}$ *be some list of integers, and suppose that* $0 \neq A(X) \in \mathbb{Z}[X]$ *has non-negative coefficients and satisfies*

$$\Phi_{N_j}(X) \mid A(X), \quad \forall 1 \leq j \leq N.$$

Then, does $A(1)$ *necessarily exceed the bound* (2)*?*

A Multiscale Lam-Leung Estimate

Theorem (I. Łaba, C.M., 2022)

Let $A(X)$ be a polynomial with non-negative coefficients and distinct cyclotomic factors $\Phi_{N_1}(X), ..., \Phi_{N_k}(X)$. Assume that there exist distinct prime numbers p, q, and exponents $\alpha_j, \beta_j \in \mathbb{N} \cup \{0\}$ such that $N_j = p^{\alpha_j} q^{\beta_j}$ for each $1 \leq j \leq k$. Assume further that $q \nmid A(1)$. Then we have the lower bound

$$A(1) \geq p^{E_p}, \text{ where } E_p = |\{\alpha_1, ..., \alpha_k\}|. \tag{3}$$

In words, E_p denotes the number of **distinct** *exponents α_i appearing among the $m_j = p^{\alpha_j} q^{\beta_j}$.*

The Exponential Bound

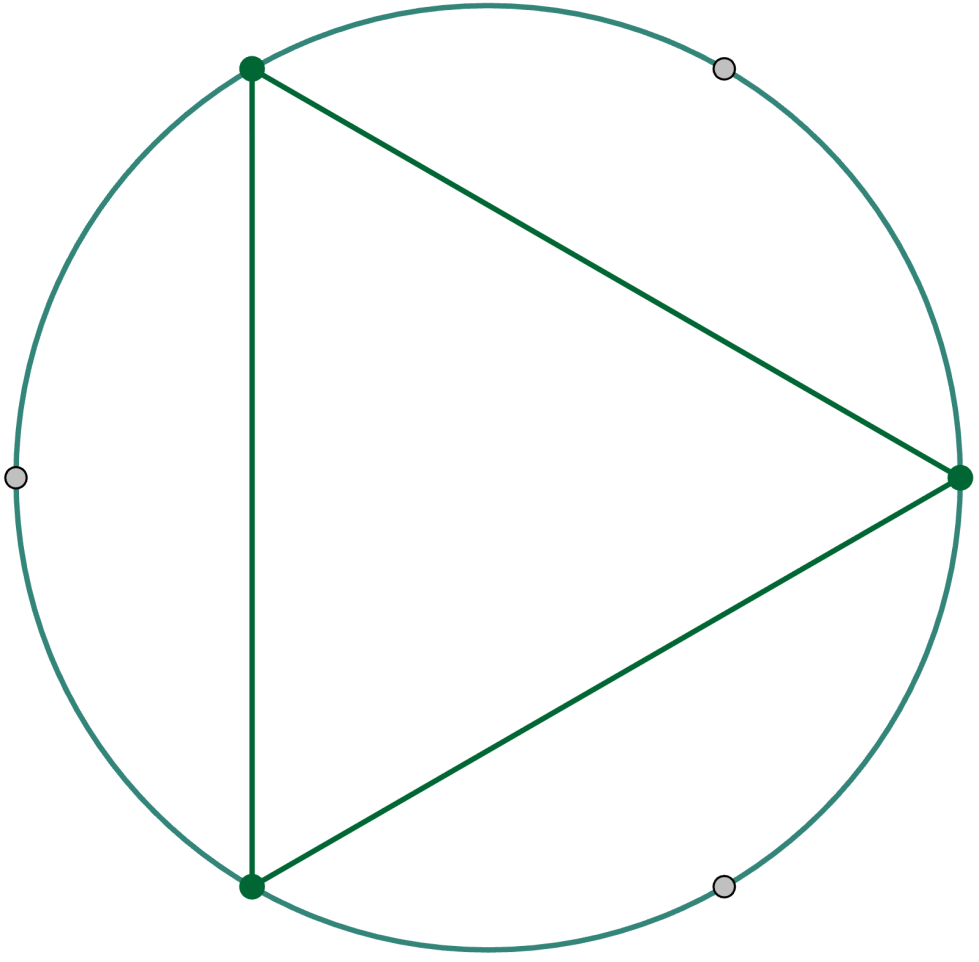

Figure: Starting in $\mathbb{Z}_6$.

The Exponential Bound

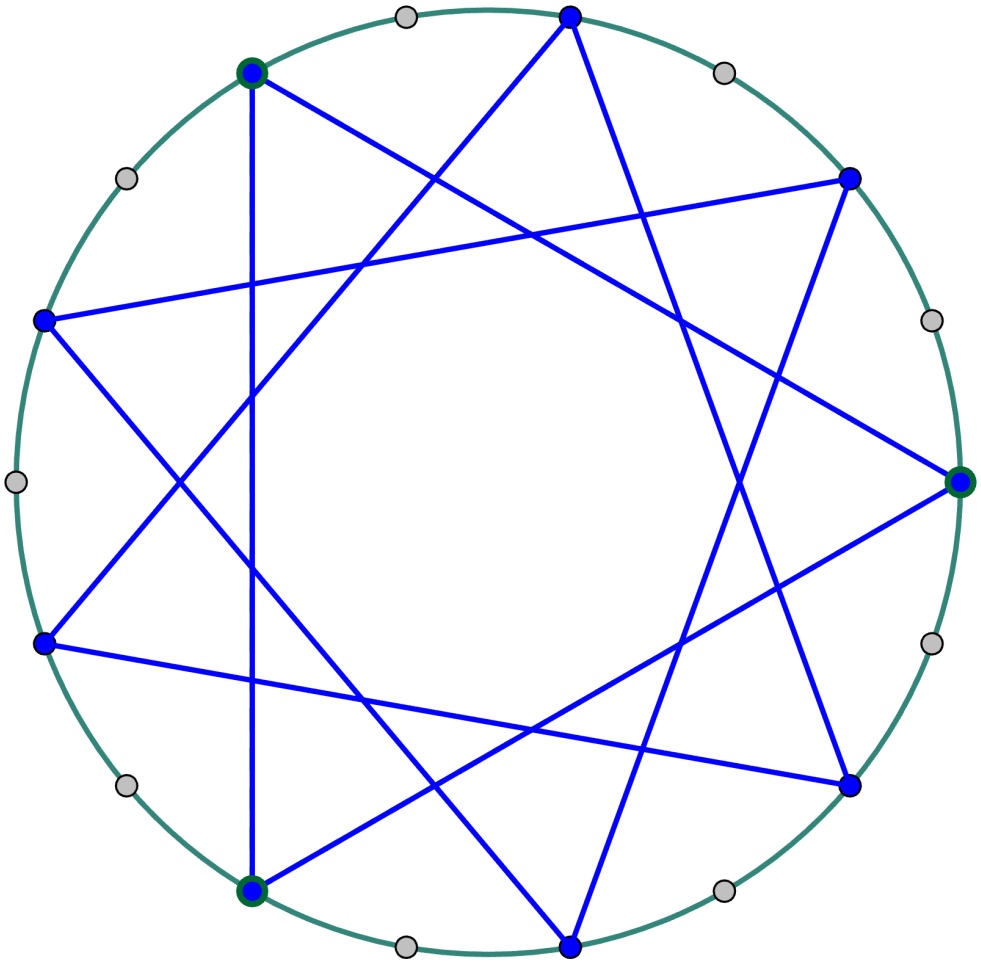

Figure: Lifting to $\mathbb{Z}_{18}$ gives *multiplicity* to the original polygon.

Multiscale VSRU's and Size Bounds

A "Coordinatization" of Cyclic Groups

We will use the following version of *Sunzi's Theorem* (i.e. the *Chinese Remainder Theorem*).

Note: we let $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ denote the cyclic group of order $N \geq 2$.

Theorem (The Remainder Theorem)

Let $N := \prod_{i=1}^{J} p_i^{n_i}$ for some prime numbers p_i and exponents $n_i \geq 1$ and set $N_i := N/p_i^{n_i}$ for each $i = 1, ..., J$. Then, to each $x \in \mathbb{Z}_N$ there exists a list $(x_1, ..., x_J) \in \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_J^{n_J}}$ such that

$$x \equiv x_1 N_1 + \cdots + x_J N_J \mod N.$$

Moreover, the choice of $x_1, ..., x_J$ is unique.

Of course, this is just another way of saying that $\mathbb{Z}_N$ is isomorphic to the direct product $\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_J^{n_J}}$.

Array Coordinates

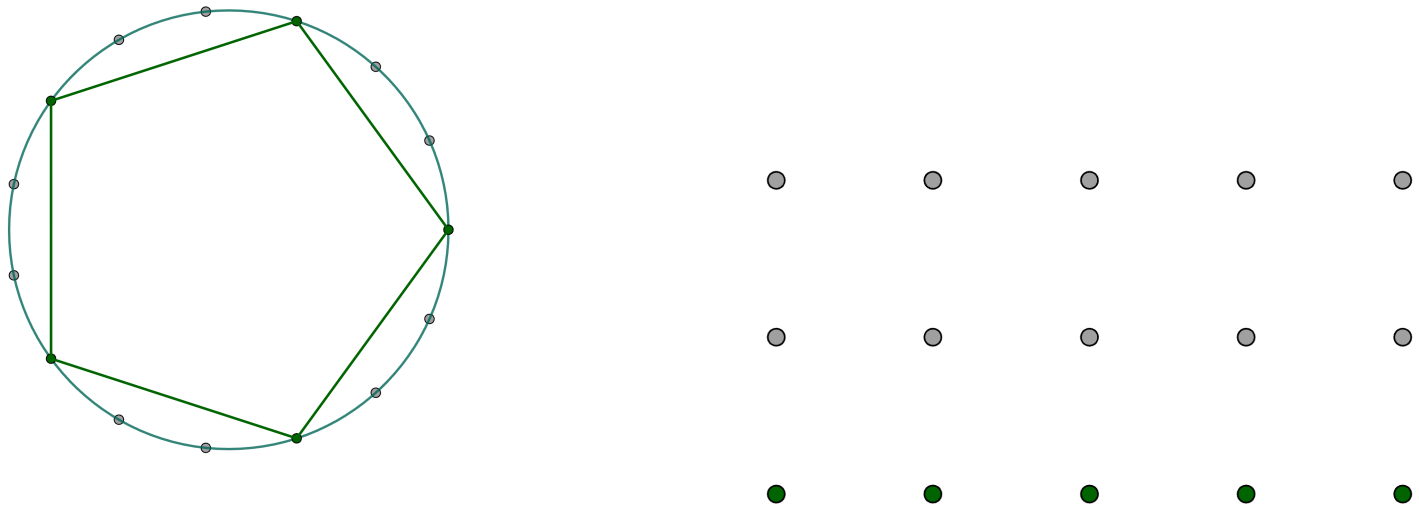

Figure: In $\mathbb{Z}_{15}$, there is one-and-only one subgroup of order 5.

Array Coordinates

Figure: The coset of the unique subgroup of order 5 which contains the element $1 \in \mathbb{Z}_{15}$.

Array Coordinates

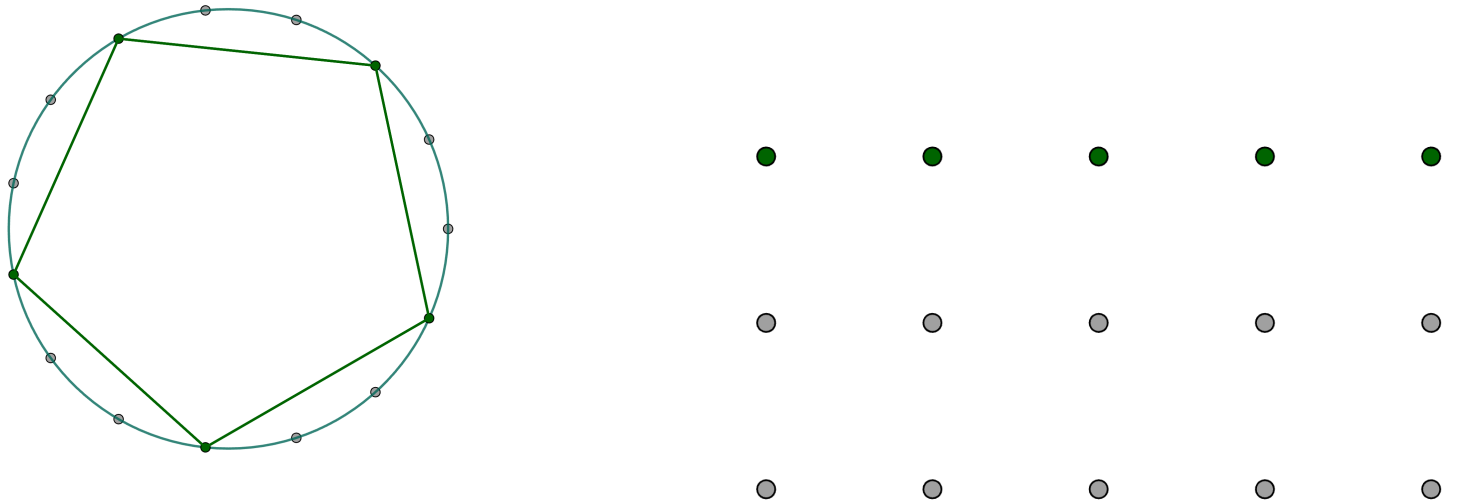

Figure: The coset of the unique subgroup of order 5 which contains the element $2 \in \mathbb{Z}_{15}$.

Linear Combinations of Regular Polygons

This leads us to the following (geometric) characterizations of VSRU's, which is due to (multiple separate results) from Rédei, de Bruijn and Schoenberg.

Theorem (Rédei-de Bruijn-Schoenberg Structure Result, 1965–1998)

Any vanishing sum of roots of unity is the linear combination of (rationally) rotated copies of prime order polygons with integer (but **not** *necessarily non-negative) coefficients.*

More flexible version of this coming.....now!

The Polynomial Rédei-de Bruijn-Schoenberg Theorem

Theorem (Rédei-de Bruijn-Schoenberg)

Let $A(X) \in \mathbb{Z}[X]$ have non-negative coefficients and suppose that $N \geq 2$ is an integer with prime divisors $p_1, ..., p_J$. The following are equivalent:

1. $\Phi_N(X) \mid A(X)$
2. *There exist polynomials $P_1(X), ..., P_J(X) \in \mathbb{Z}[X]$ such that*

$$A(X) := P_1(X)F_1^N(X) + \cdots + P_J(X)F_J^N(X) \mod X^N - 1,$$

where the F_j^N are called fibers and so satisfy:

$$F_j^N(X) := 1 + X^{N/p_j} + X^{2N/p_j} + \cdots + X^{(p_j-1)N/p_j}..$$

Sketch of the Lower Bound

Example

Let's assume that $A(X) \in \mathbb{Z}[X]$ satisfies $\Phi_{pq}(X), \Phi_{p^2q}(X) \mid A(X)$ and that $q \nmid A(1)$. Let's give a sketch as to why we must have (at least) that $A(1) \geq p \cdot \min(p, q)$. Observations:

- $A(X) \bmod X^{p^2q} - 1$ has to be the linear combination of cosets of prime power order (that's R-dB-S).
- A *cannot* be linear combination of q-subgroups alone (why?)
- Subgroups of order p inside of $\mathbb{Z}_{p^2q}$ "collapse" to a point (with multiplicity!) in $\mathbb{Z}_{pq}$!
- Apply R-dB-S again, now with multiplicity $\Rightarrow$ square-order bound (not quite good enough...)

From Polynomials to Multisets

Definition (Multisets in $\mathbb{Z}_M$)

If $A(X) \in \mathbb{Z}[X]$, then there exists a (coefficient) function $w_A^N : \mathbb{Z}_N \to \mathbb{Z}$ satisfying

$$A(X) := \sum_{x \in \mathbb{Z}_N} w_A^N(x) X^x \mod X^N - 1.$$

Hence, the **multiset** $A \bmod N$ associated to $A(X)$ is simply the collection of ordered pairs

$$A \bmod N := \{(x, w_A^N(x)) : x \in \mathbb{Z}_N\}.$$

Key idea: points can have multiplicity!

Multisets: an Example

Example

Let $A(X) := 1 + X^2 + X^4$ (can think of this the set of integers $\{0, 2, 4\}$).

$$A \bmod 6 := \{(0,1),(1,0),(2,1),(3,0),(4,1),(5,0)\}$$

$$A \bmod 3 := \{(0,1),(1,1),(2,1)\}$$

$$A \bmod 2 := \{(0,3),(1,0)\}$$

Quick maths: what is $A(X) \bmod X^N - 1$ for the following:

- $N = 6$?
- $N = 3$?
- $N = 2$?

Simplest Possible Sets: σ-Fibered Sets

From now on, we shall use the notation:

$$S_A := \{N \in \mathbb{N} : \Phi_N(X) \mid A(X)\}$$

Definition (Fibered Sets)

Given an $A(X) \in \mathbb{Z}[X]$ with non-negative coefficients, we say that A is **fibered** if, for each $N \in S_A$, exists a choice of prime $p_{\sigma(N)} \mid N$ such that

$$A(X) := P_N(X) F^N_{\sigma(N)}(X) \mod X^N - 1.$$

In words: $A(X)$ is a fibered set if there it is a linear combination of one-and-only-one type of prime order subgroups at each scale N such that $\Phi_N(X) \mid A(X)$.

Fibered Sets: a Picture

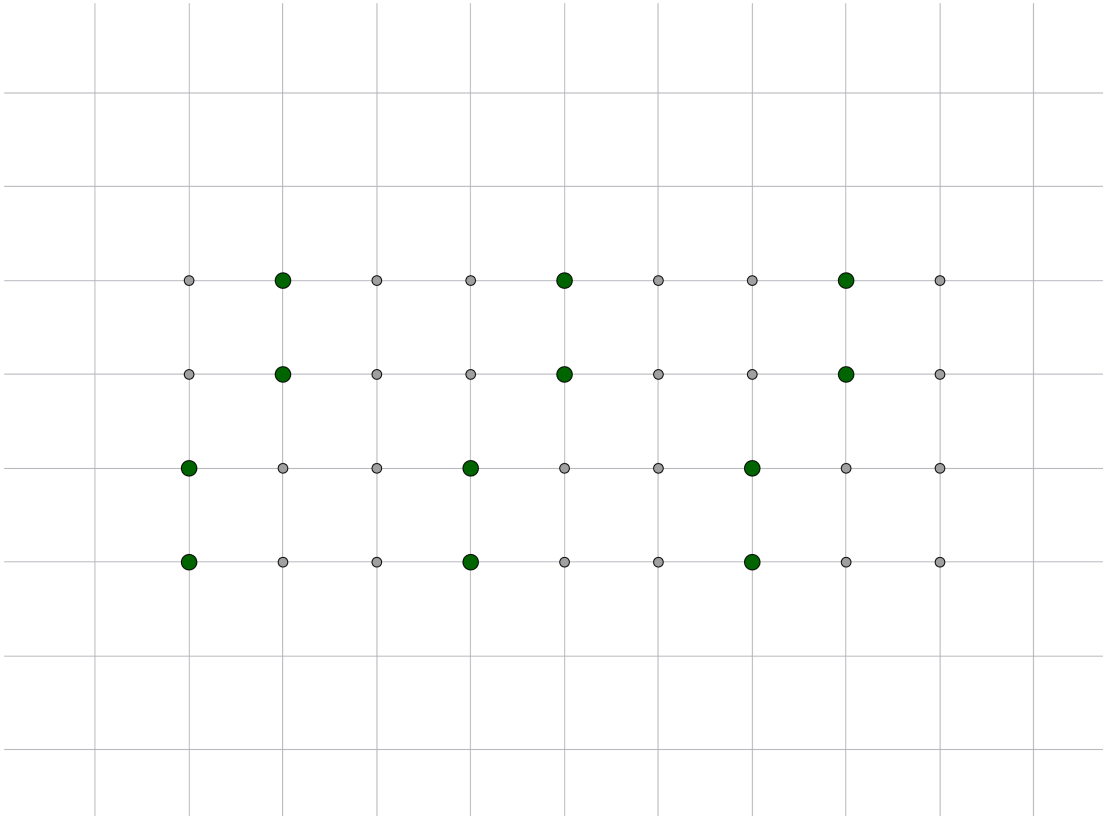

Figure: One representation of a fibered polynomial in $\mathbb{Z}_{36}$. Here, all of the fibers are cosets of the subgroup of order 3.

Fibered Sets: a Picture

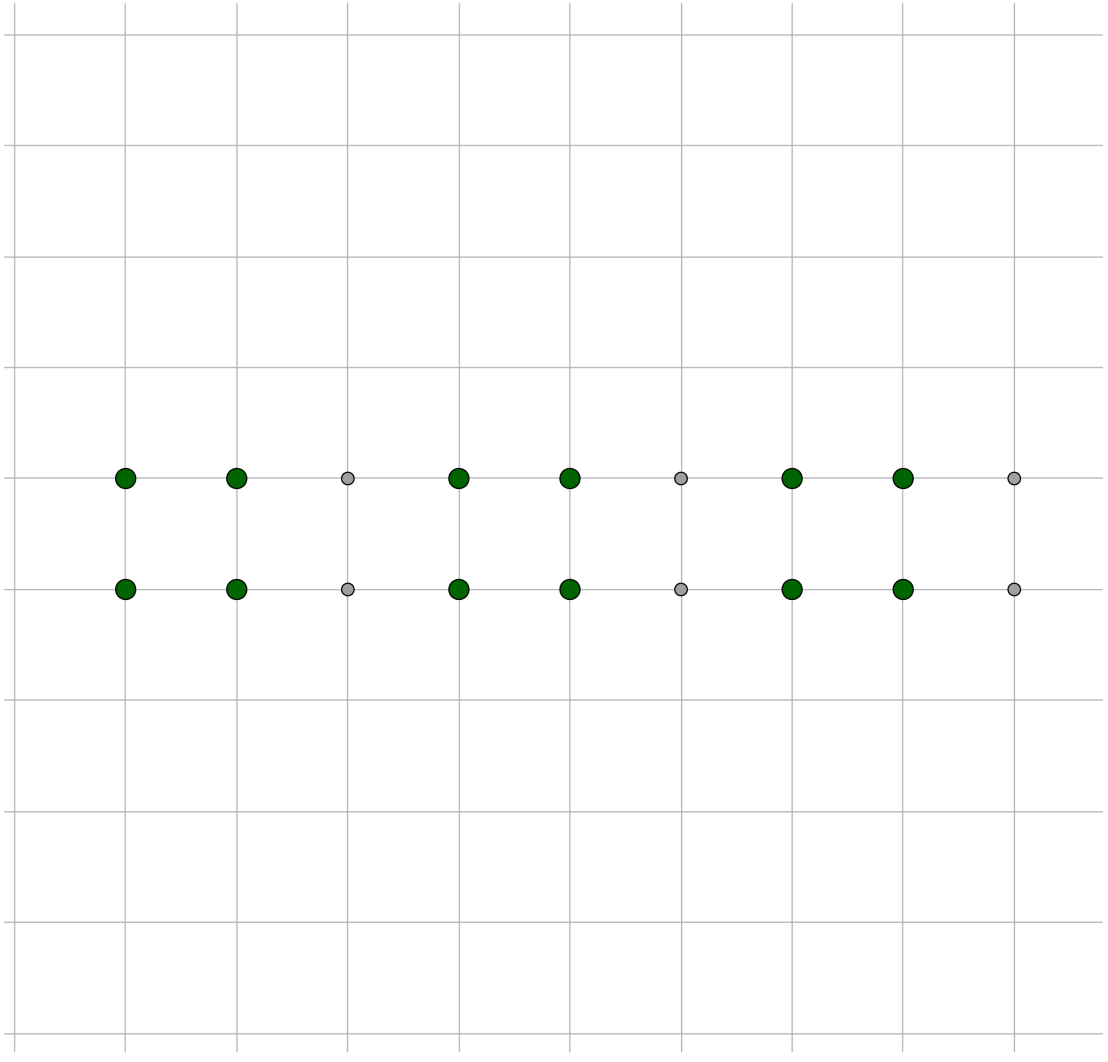

Figure: This same polynomial is also fibered in $\mathbb{Z}_{18}$. Here, all of the fibers are cosets of the subgroup of order 2.

The σ-Fibering Bound

We then have the following extension of our first lower bound.

Theorem (G. Kiss, I. Łaba, C.M., G. Somlai, 2025+)

Let $S \subset \mathbb{N}$, and let $\sigma : S \to \{1, ..., J\}$ be an assignment function. Suppose that $M := lcm(S) = \prod_i p_i^{n_i}$ and, for each i, let

$$EXP_i(S, \sigma) := \{\alpha \in \mathbb{N} : \exists\, N \in S \ with\ (N, p_i^{n_i}) = p_i^{\alpha}, \sigma(N) = i\}.$$

Let $E_i(S, \sigma) := \#EXP_i(S, \sigma)$. Then, if $A(X)$ is any (S, σ)-fibered polynomial, then

$$A(1) \geq \min_{\sigma_0} p_1^{E_1(S,\sigma_0)} \cdots p_J^{E_J(S,\sigma_0)},$$

where the minimum is taken over all assignment functions σ_0 on S.

We Got Away with Something...!

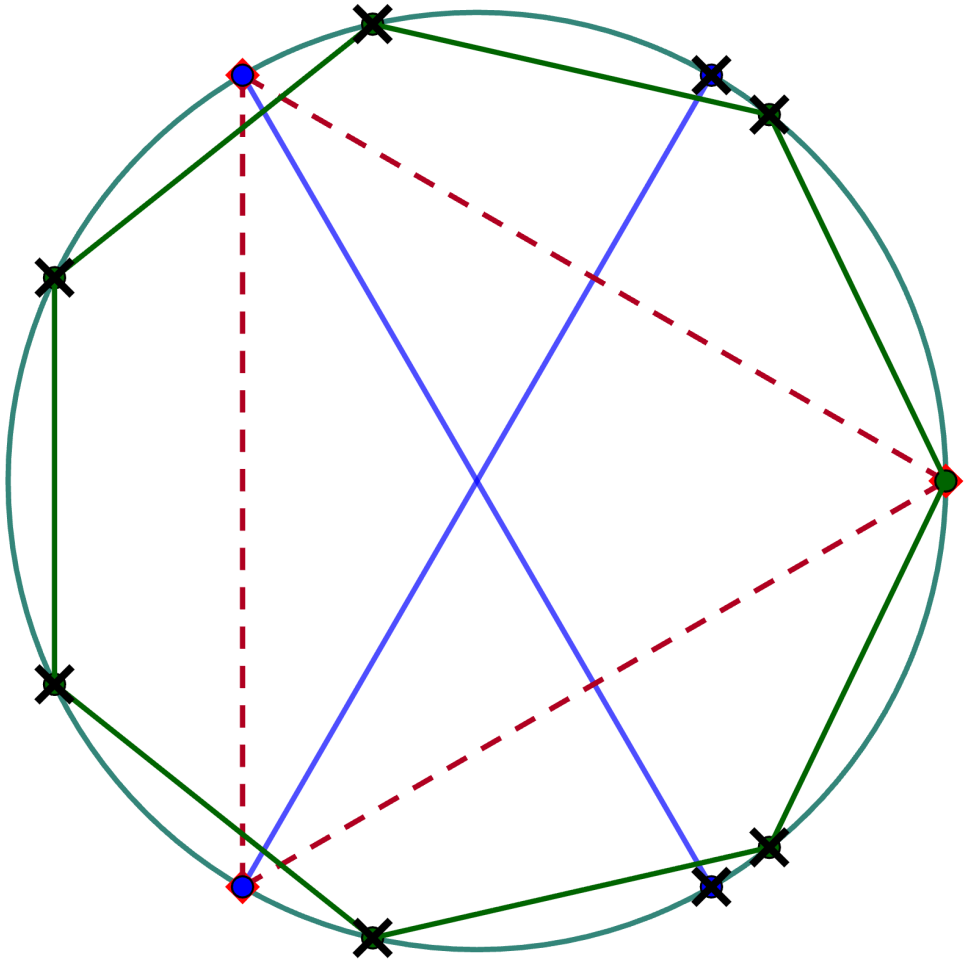

Figure: Still dreaming about polygons.

Applications (or, better: *Here There Be Dragons*)

Integer Tilings and Cyclotomic Polynomials

Definition (Tilings of $\mathbb{Z}_M$)

A **tiling** of $\mathbb{Z}_M$ ($M \geq 2$) is a pair of sets $A, B \subset \mathbb{Z}_M$ such that, for any $n \in \mathbb{Z}_M$, there exist *unique* choices $a \in A$ and $b \in B$ such that $n \equiv a + b \bmod M$. We denote this $A \oplus B = \mathbb{Z}_M$ and say that A (resp. B) **tiles** $\mathbb{Z}_M$.

When M is small, can compute tilings by hand, as the following example shows.

Example

If $A := \{0, 1, 5\}$ and $B := \{0, 3\}$, then

$$A + B := \{0, 1, 3, 4, 5, 8\} \equiv \mathbb{Z}_6 \bmod 6.$$

What if M is more complex? (Computationally complex problem, w/o additional necessary conditions for tiles)

From Sets of Integers to Polynomials

This leads us to the single most important conjecture in the theory of tilings of finite Abelian groups. First, some background.

Definition

If $A \subset \mathbb{Z}_M$, then we define the **mask polynomial** of A as

$$A(X) := \sum_{a \in A} X^a \mod X^M - 1.$$

Where we use $X^M - 1$ since $1 - 1$ correspondence between mask polynomials $A(X) \in \mathbb{Z}[X]/(X^M - 1)$ and subsets $A \subset \mathbb{Z}_M$.

Proposition

Let $A, B \subset \mathbb{Z}_M$. Then, the following are equivalent.

1. $A \oplus B = \mathbb{Z}_M$.
2. $A(X)B(X) = 1 + X + \cdots + X^{M-1} \mod X^M - 1$.

Necessary Conditions for Tiling: Cyclotomic Polynomials

Corollary

Let $A, B \subset \mathbb{Z}_M$. Then, the following conditions are equivalent.

1. $A \oplus B = \mathbb{Z}_M$
2. $\Phi_N(X) \mid A(X)B(X)$ *for each* $1 \neq N \mid M$.

This follows since

$$1 + X + \cdots + X^{M-1} = \frac{X^M - 1}{X - 1} = \prod_{1 \neq N \mid M} \Phi_N(X).$$

The Dragon and Its Golden Hoard

The single most important conjecture in the theory of tilings of finite Abelian groups is the following.

Conjecture (Coven and Meyerowitz, 1999)

Let $A, B \subset \mathbb{Z}_M$. Then, the following are equivalent.

1. $A \oplus B = \mathbb{Z}_M$
2. *A and B each satisfy the conditions $(T1)$ and $(T2)$, which are defined below.*

Definition (The $(T1)$ and $(T2)$ tiling conditions)

Say that $A \subset \mathbb{Z}_M$ satisfies:

- $(T1)$ if $(\#A) := \prod_{s:\Phi_s(X)|A(X)} \Phi_s(1)$
- $(T2)$ if, whenever $n_1, ..., n_T$ are powers of distinct prime numbers, and $\Phi_{n_1}(X), ..., \Phi_{n_T}(X) \mid A(X)$, then $\Phi_N(X) \mid A(X)$, where $N := n_1 \cdots n_T$.

σ-Fibered Sets and the C-M Conjecture

The following gives context for the previous bounds we have seen.

Theorem (G. Kiss, I. Łaba, C.M., G. Somlai, 2025+)

Suppose that $A \subset \mathbb{Z}_M$ and let $S := S_A$ be the set of cyclotomic divisors of $A(X)$, the mask polynomial of A. Suppose that:

- *$A \oplus B = \mathbb{Z}_M$ for some $B \subset \mathbb{Z}_M$.*
- *$A(1) \geq \min_{\sigma_0} p_1^{E_1(S,\sigma_0)} \cdots p_J^{E_J(S,\sigma_0)}$, where the minimum is taken over assignment functions on S. Then, A satisfies both $(T1)$ and $(T2)$.*

Corollary (G. Kiss, I. Łaba, C.M., G. Somlai, 2025+)

Suppose that $A \subset \mathbb{Z}_M$ is an (S_A, σ) fibered set which tiles $\mathbb{Z}_M$. Then, A satisfies $(T1)$ and $(T2)$.

Other Applications: Projections of Fractal Sets

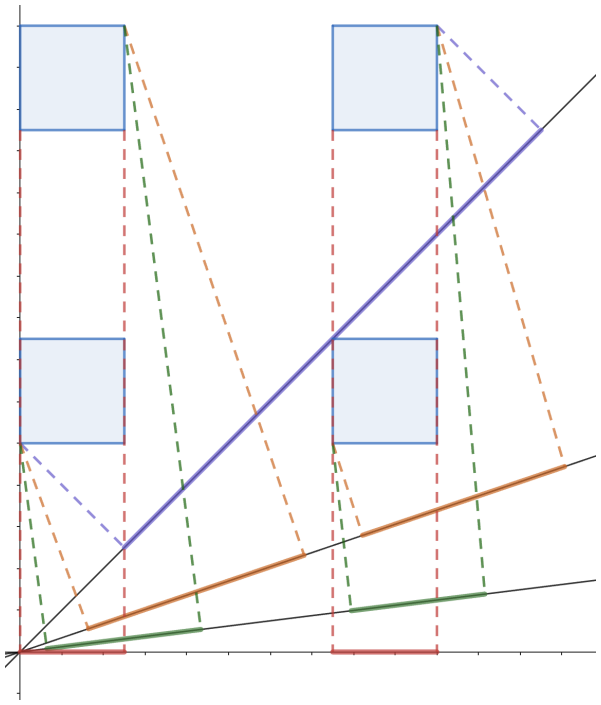

Figure: Determining the average lengths of projections of Cantor sets (i.e. the *Favard length problem*). Recent single-author work connecting this problem in geometric measure theory to σ-fibered bounds.

Other Applications: L^2 Estimates for Fourier series

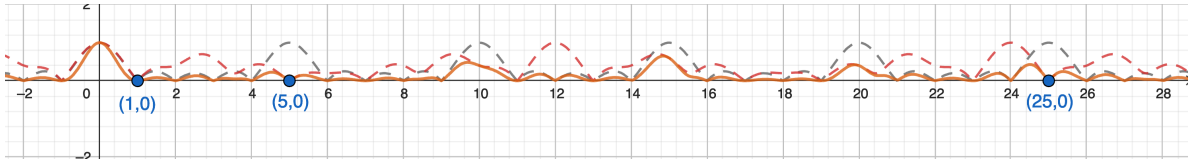

Figure: A complicated trigonometric polynomial

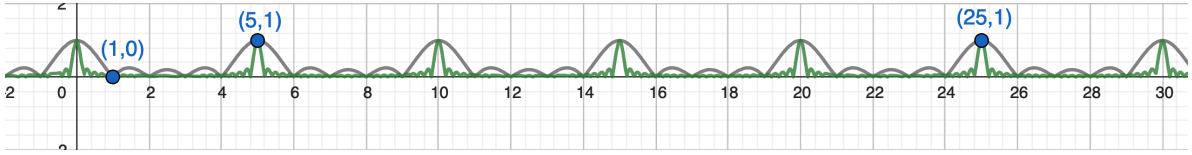

Figure: Factors into a term which "washes out" zeroes...

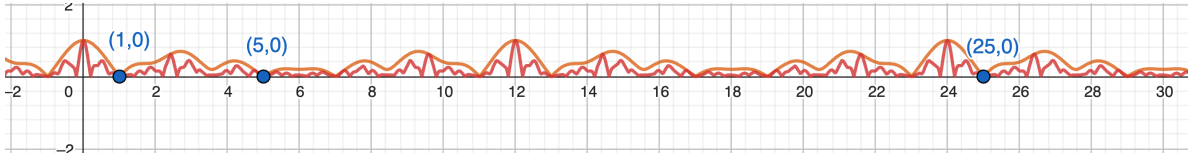

Figure: As well as a term with "persistent" zeroes.

Ongoing Fun Projects

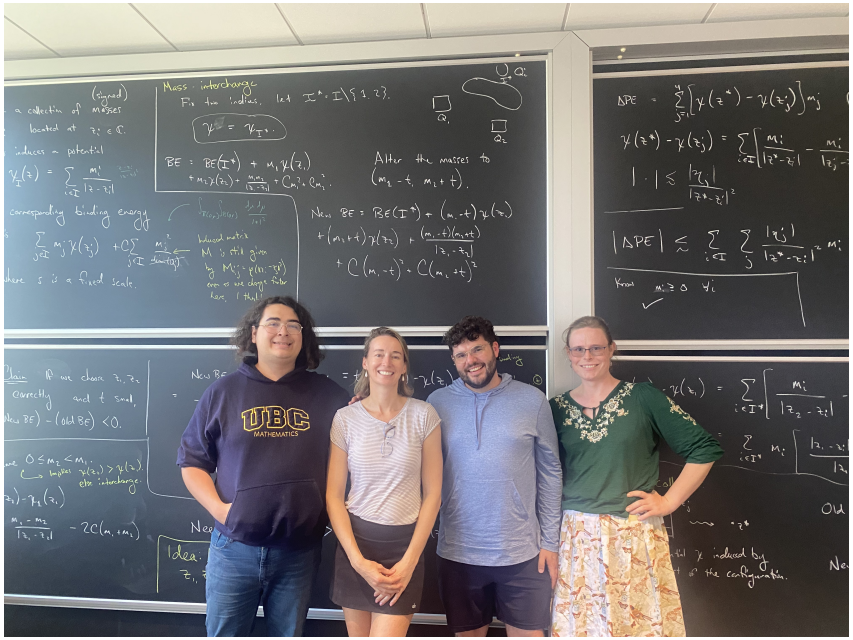

Figure: Friends doing math together—what more can one ask for in life??

- Tiling mentorship groups for Undergraduate/Masters students
- Ongoing working group at the *American Institute of Mathematics* (until 2028)
- Computational tilings and VSRU's at *Rényi Institute* in Budapest (April — August 2026)

Thank You!

Many thanks to:

- The *Number Theory and Combinatorics Seminar* organizers, Emily and Habiba.
- The *Number Theory and Combinatorics Seminar* for supporting my visit. It has been a lovely time!