

Some Combinatorial Aspects of Cyclotomic Polynomials

Richard P. Stanley

April 24, 2025

Partitions

partition of $n \geq 0$: an integer sequence $\lambda = (\lambda_1, \lambda_2, \dots)$ satisfying $\lambda_1 \geq \lambda_2 \geq \dots \geq 0$ and $\sum \lambda_i = n$

partitions of 5: 5, 41, 32, 311, 221, 2111, 11111

Terminology example. The partition $(6, 4, 4, 3, 2, 2, 2, 1)$ has two **parts** equal to 4. Equivalently, 4 has **multiplicity** two as a part.

Partitions

partition of $n \geq 0$: an integer sequence $\lambda = (\lambda_1, \lambda_2, \dots)$ satisfying $\lambda_1 \geq \lambda_2 \geq \dots \geq 0$ and $\sum \lambda_i = n$

partitions of 5: 5, 41, 32, 311, 221, 2111, 11111

Terminology example. The partition $(6, 4, 4, 3, 2, 2, 2, 1)$ has two **parts** equal to 4. Equivalently, 4 has **multiplicity** two as a part.

$f(n)$: number of partitions of n for which no part appears exactly once

Example. $f(8) = 6$: 44, 3311, 2222, 22211, 221111, 11111111

A theorem of MacMahon

Theorem (MacMahon, 1916) *The number $f(n)$ of partitions of n for which no part appears exactly once equals the number of partitions of n into parts $\not\equiv \pm 1 \pmod{6}$.*

A theorem of MacMahon

Theorem (MacMahon, 1916) *The number $f(n)$ of partitions of n for which no part appears exactly once equals the number of partitions of n into parts $\not\equiv \pm 1 \pmod{6}$.*

$$\begin{aligned} \text{Proof. } \sum_{n \geq 0} f(n)x^n &= \prod_{i \geq 1} (1 + x^{2i} + x^{3i} + x^{4i} + \cdots) \\ &= \prod_{i \geq 1} \left(\frac{1}{1 - x^i} - x^i \right) \\ &= \prod_{i \geq 1} \frac{1 - x^i + x^{2i}}{1 - x^i} \\ &= \prod_{i \geq 1} \frac{1 - x^{6i}}{(1 - x^{2i})(1 - x^{3i})} \\ &= \prod_{j \not\equiv \pm 1 \pmod{6}} (1 - x^j)^{-1}. \quad \square \end{aligned}$$

Why does this work?

$\Phi_n(x)$: the n th **cyclotomic polynomial**

$$\Phi_1(x) = 1 - x \quad (x - 1 \text{ is standard})$$

$$\Phi_n(x) = \prod_{\substack{1 \leq j \leq n \\ \gcd(j,n)=1}} (x - e^{2\pi ij/n}) = \prod_{d|n} (1 - x^d)^{\mu(n/d)}, \quad n \geq 2$$

Why does this work?

$\Phi_n(x)$: the n th **cyclotomic polynomial**

$$\Phi_1(x) = 1 - x \quad (x - 1 \text{ is standard})$$

$$\Phi_n(x) = \prod_{\substack{1 \leq j \leq n \\ \gcd(j,n)=1}} (x - e^{2\pi ij/n}) = \prod_{d|n} (1 - x^d)^{\mu(n/d)}, \quad n \geq 2$$

$$= \prod_{i=1}^k (1 - x^i)^{a_i}, \quad a_i \in \mathbb{Z}$$

Two points

1. (the main point)

$$F(x) := \frac{1}{1-x} - x = \frac{\Phi_6(x)}{1-x} = \frac{1-x^6}{(1-x^2)(1-x^3)}$$

Two points

1. (the main point)

$$F(x) := \frac{1}{1-x} - x = \frac{\Phi_6(x)}{1-x} = \frac{1-x^6}{(1-x^2)(1-x^3)}$$

- 2.

$$\begin{aligned} \sum_{n \geq 0} f(n)x^n &= F(x)F(x^2)F(x^3)\cdots \\ &= \frac{(1-x^6)(1-x^{12})(1-x^{18})\cdots}{(1-x^2)(1-x^4)(1-x^6)\cdots(1-x^3)(1-x^6)(1-x^9)\cdots} \\ &= \frac{1}{(1-x^2)(1-x^3)(1-x^4)(1-x^6)(1-x^8)(1-x^9)\cdots} \end{aligned}$$

Cyclotomic sets

Definition. A **cyclotomic set** is a subset S of $\mathbb{P} = \{1, 2, \dots\}$ such that

$$F_S(x) := \frac{1}{1-x} - \sum_{j \in S} x^j = \frac{N_S(x)}{D_S(x)},$$

where $N_S(x)$ and $D_S(x)$ are finite products of cyclotomic polynomials.

Cyclotomic sets

Definition. A **cyclotomic set** is a subset S of $\mathbb{P} = \{1, 2, \dots\}$ such that

$$F_S(x) := \frac{1}{1-x} - \sum_{j \in S} x^j = \frac{N_S(x)}{D_S(x)},$$

where $N_S(x)$ and $D_S(x)$ are finite products of cyclotomic polynomials.

Equivalently, $F_S(x) = \prod_{i=1}^k (1-x^i)^{a_i}$, $a_i \in \mathbb{Z}$.

Cyclotomic sets

Definition. A **cyclotomic set** is a subset S of $\mathbb{P} = \{1, 2, \dots\}$ such that

$$F_S(x) := \frac{1}{1-x} - \sum_{j \in S} x^j = \frac{N_S(x)}{D_S(x)},$$

where $N_S(x)$ and $D_S(x)$ are finite products of cyclotomic polynomials.

Equivalently, $F_S(x) = \prod_{i=1}^k (1 - x^i)^{a_i}$, $a_i \in \mathbb{Z}$.

Think of S as the set of “forbidden part multiplicities.”

An example: $S = \{1, 2, 3, 5, 7, 11\}$

$$\begin{aligned} F_S(x) &:= \frac{1}{1-x} - (x + x^2 + x^3 + x^5 + x^7 + x^{11}) \\ &= \frac{\Phi_6(x)\Phi_{12}(x)\Phi_{18}(x)}{1-x} \\ &= \frac{(1-x^{12})(1-x^{18})}{(1-x^4)(1-x^6)(1-x^9)} \end{aligned}$$

An example: $S = \{1, 2, 3, 5, 7, 11\}$

$$\begin{aligned}F_S(x) &:= \frac{1}{1-x} - (x + x^2 + x^3 + x^5 + x^7 + x^{11}) \\&= \frac{\Phi_6(x)\Phi_{12}(x)\Phi_{18}(x)}{1-x} \\&= \frac{(1-x^{12})(1-x^{18})}{(1-x^4)(1-x^6)(1-x^9)}\end{aligned}$$

$$F_S(x)F_S(x^2)F_S(x^3)\cdots = \prod_i (1-x^i)^{-1},$$

$$i \equiv 0, 4, 6, 8, 9, 12, 16, 18, 20, 24, 27, 28, 30, 32 \pmod{36}. \quad (*)$$

An example: $S = \{1, 2, 3, 5, 7, 11\}$

$$\begin{aligned}F_S(x) &:= \frac{1}{1-x} - (x + x^2 + x^3 + x^5 + x^7 + x^{11}) \\&= \frac{\Phi_6(x)\Phi_{12}(x)\Phi_{18}(x)}{1-x} \\&= \frac{(1-x^{12})(1-x^{18})}{(1-x^4)(1-x^6)(1-x^9)}\end{aligned}$$

$$F_S(x)F_S(x^2)F_S(x^3)\cdots = \prod_i (1-x^i)^{-1},$$

$i \equiv 0, 4, 6, 8, 9, 12, 16, 18, 20, 24, 27, 28, 30, 32 \pmod{36}$. (*)

Theorem. For all $n \geq 0$, the number of partitions of n such that no part occurs exactly 1, 2, 3, 5, 7 or 11 times equals the number of partitions of n into parts i satisfying (*).

A further example

$S = \{2, 3, 4, \dots\}$ is cyclotomic:

$$\frac{1}{1-x} - (x^2 + x^3 + \dots) = 1 + x = \frac{1-x^2}{1-x}$$

A further example

$S = \{2, 3, 4, \dots\}$ is cyclotomic:

$$\frac{1}{1-x} - (x^2 + x^3 + \dots) = 1 + x = \frac{1-x^2}{1-x}$$

$$\prod_{i \geq 1} \frac{1-x^{2i}}{1-x^i} = \prod_{i \geq 1} (1-x^{2i-1})^{-1}.$$

A further example

$S = \{2, 3, 4, \dots\}$ is cyclotomic:

$$\frac{1}{1-x} - (x^2 + x^3 + \dots) = 1 + x = \frac{1-x^2}{1-x}$$

$$\prod_{i \geq 1} \frac{1-x^{2i}}{1-x^i} = \prod_{i \geq 1} (1-x^{2i-1})^{-1}.$$

Theorem (Euler). *The number of partitions of n into distinct parts equals the number of partitions of n into odd parts.*

A property of finite cyclotomic sets

Classification: wide open.

A property of finite cyclotomic sets

Classification: wide open.

Theorem. Assume that S is finite. For $0 \leq j \leq d = \max(S)$, exactly one of j and $d - j$ belongs to S . Hence $\#S = (d + 1)/2$.

Proof sketch. Symmetry or antisymmetry of $\Phi_n(x)$ implies

$$P_S(x) + x^d P_S(1/x) = 1 + x + \cdots + x^d, \text{ where } P_S(x) = \sum_{i \in S} x^i. \quad \square$$

A property of finite cyclotomic sets

Classification: wide open.

Theorem. Assume that S is finite. For $0 \leq j \leq d = \max(S)$, exactly one of j and $d - j$ belongs to S . Hence $\#S = (d + 1)/2$.

Proof sketch. Symmetry or antisymmetry of $\Phi_n(x)$ implies

$$P_S(x) + x^d P_S(1/x) = 1 + x + \cdots + x^d, \text{ where } P_S(x) = \sum_{i \in S} x^i. \quad \square$$

Corollary. S finite $\Rightarrow \max(S)$ is odd.

Some data

Let d be odd. There are $2^{(d-1)/2}$ sets $S \subset \mathbb{P}$ with $\max(S) = d$ such that $N_S(x)$ is symmetric. Let $f(d)$ be the number of these that are cyclotomic. Then

d	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29
$f(d)$	1	2	3	5	5	9	10	12	18	22	22	37	39	41	54

Some data

Let d be odd. There are $2^{(d-1)/2}$ sets $S \subset \mathbb{P}$ with $\max(S) = d$ such that $N_S(x)$ is symmetric. Let $f(d)$ be the number of these that are cyclotomic. Then

d	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29
$f(d)$	1	2	3	5	5	9	10	12	18	22	22	37	39	41	54

Can show: $f(d) \leq a \exp b\sqrt{d}$ (number of polynomials of degree d that are a product of cyclotomic polynomials), and

$$f(2^{2k+1} - 1) \geq k + 2$$

Two infinite families

Write e.g. $125 = \{1, 2, 5\}$.

1, 23, 345, 4567, 56789, ...

1, 13, 135, 1357, ...

An aside (MathOverflow 461829)

The symmetric (palindromic) polynomials of the form

$$N_S(x) = 1 - (1 - x) \sum_{j \in S} x^j,$$

where S is a finite subset of \mathbb{P} , seem to have lots of zeros α on the unit circle ($|\alpha| = 1$).

An aside (MathOverflow 461829)

The symmetric (palindromic) polynomials of the form

$$N_S(x) = 1 - (1 - x) \sum_{j \in S} x^j,$$

where S is a finite subset of \mathbb{P} , seem to have lots of zeros α on the unit circle ($|\alpha| = 1$).

There are 2^m such polynomials when $\max(S) = 2m + 1$. For instance, when $n = 33$, the average number of zeros on the unit circle of the $2^{16} = 65536$ polynomials is

$$\frac{751153}{1081344} = 0.69464\dots$$

An aside (MathOverflow 461829)

The symmetric (palindromic) polynomials of the form

$$N_S(x) = 1 - (1 - x) \sum_{j \in S} x^j,$$

where S is a finite subset of \mathbb{P} , seem to have lots of zeros α on the unit circle ($|\alpha| = 1$).

There are 2^m such polynomials when $\max(S) = 2m + 1$. For instance, when $n = 33$, the average number of zeros on the unit circle of the $2^{16} = 65536$ polynomials is

$$\frac{751153}{1081344} = 0.69464\dots$$

No reason known.

Cleanness

Note. Any $f(x) \in \mathbb{Z}[[x]]$ with $f(0) = 1$ can be uniquely written (formally) as

$$f(x) = \prod_{n \geq 1} (1 - x^n)^{-a_n}, \quad a_n \in \mathbb{Z}.$$

Cleanness

Note. Any $f(x) \in \mathbb{Z}[[x]]$ with $f(0) = 1$ can be uniquely written (formally) as

$$f(x) = \prod_{n \geq 1} (1 - x^n)^{-a_n}, \quad a_n \in \mathbb{Z}.$$

Let S be a subset of \mathbb{P} and

$$F(x) = \frac{1}{1-x} - \sum_{j \in S} x^j.$$

S is **clean** if

$$F(x)F(x^2)F(x^3)\cdots = \prod_{n \geq 1} (1 - x^n)^{-a_n},$$

where each $a_n = 0, 1$. (Get a “clean” partition identity—no weighted or colored parts.)

An example

Not every cyclotomic set S is clean, e.g., $S = \{1, 5, 7, 8, 9, 11\}$, for which

$$\frac{F(x)F(x^2)F(x^3)\cdots}{(1-x^2)(1-x^3)(1-x^4)(1-x^6)(1-x^8)(1-x^9)(1-x^{10})(1-x^{12})\cdots} =$$
$$(1-x^5)(1-x^{25})(1-x^{35})(1-x^{55})\cdots$$

An example

Not every cyclotomic set S is clean, e.g., $S = \{1, 5, 7, 8, 9, 11\}$, for which

$$\frac{F(x)F(x^2)F(x^3)\cdots}{(1-x^2)(1-x^3)(1-x^4)(1-x^6)(1-x^8)(1-x^9)(1-x^{10})(1-x^{12})\cdots} = \frac{(1-x^5)(1-x^{25})(1-x^{35})(1-x^{55})\cdots}{(1-x^2)(1-x^3)(1-x^4)(1-x^6)(1-x^8)(1-x^9)(1-x^{10})(1-x^{12})\cdots}$$

No nice theory of clean sets.

Numerical semigroups

Definition. A **numerical semigroup** is a submonoid M of $\mathbb{N} = \{0, 1, 2, \dots\}$ (under addition) such that $\mathbb{N} - M$ is finite.

Numerical semigroups

Definition. A **numerical semigroup** is a submonoid M of $\mathbb{N} = \{0, 1, 2, \dots\}$ (under addition) such that $\mathbb{N} - M$ is finite.

Note. (a) Every submonoid of \mathbb{N} is either $\{0\}$ or of the form nM , where M is a numerical semigroup and $n \geq 1$.

(b) Every submonoid of \mathbb{N} is finitely-generated.

Numerical semigroups

Definition. A **numerical semigroup** is a submonoid M of $\mathbb{N} = \{0, 1, 2, \dots\}$ (under addition) such that $\mathbb{N} - M$ is finite.

Note. (a) Every submonoid of \mathbb{N} is either $\{0\}$ or of the form nM , where M is a numerical semigroup and $n \geq 1$.

(b) Every submonoid of \mathbb{N} is finitely-generated.

Define $A_M(\mathbf{x}) = \sum_{i \in M} x^i$.

Numerical semigroups

Definition. A **numerical semigroup** is a submonoid M of $\mathbb{N} = \{0, 1, 2, \dots\}$ (under addition) such that $\mathbb{N} - M$ is finite.

Note. (a) Every submonoid of \mathbb{N} is either $\{0\}$ or of the form nM , where M is a numerical semigroup and $n \geq 1$.

(b) Every submonoid of \mathbb{N} is finitely-generated.

Define $A_M(x) = \sum_{i \in M} x^i$.

Note $A_M(x) = \frac{1}{1-x} - \sum_{i \in \mathbb{N} - M} x^i$,

Cyclotomic numerical semigroups

Definition (E.-A. Ciolan, et al.) A numerical semigroup M is **cyclotomic** if $(1 - x)A_M(x)$ is a product of cyclotomic polynomials. Equivalently, $\mathbb{N} - M$ is a cyclotomic set.

Cyclotomic numerical semigroups

Definition (E.-A. Ciolan, et al.) A numerical semigroup M is **cyclotomic** if $(1-x)A_M(x)$ is a product of cyclotomic polynomials. Equivalently, $\mathbb{N} - M$ is a cyclotomic set.

Example. $M = \langle a, b \rangle$, where $a, b \geq 2$, $\gcd(a, b) = 1$. Then

$$A_M(x) = \frac{1 - x^{ab}}{(1 - x^a)(1 - x^b)},$$

so M is a cyclotomic semigroup (and clean).

Cyclotomic numerical semigroups

Definition (E.-A. Ciolan, et al.) A numerical semigroup M is **cyclotomic** if $(1-x)A_M(x)$ is a product of cyclotomic polynomials. Equivalently, $\mathbb{N} - M$ is a cyclotomic set.

Example. $M = \langle a, b \rangle$, where $a, b \geq 2$, $\gcd(a, b) = 1$. Then

$$A_M(x) = \frac{1 - x^{ab}}{(1 - x^a)(1 - x^b)},$$

so M is a cyclotomic semigroup (and clean).

Example. (a) $M = \langle 4, 6, 7 \rangle = \mathbb{N} - \{1, 2, 3, 5, 9\}$ is cyclotomic.

(b) $M = \langle 5, 6, 7 \rangle = \mathbb{N} - \{1, 2, 3, 4, 8, 9\}$ is not cyclotomic.

Consequence of $\langle a, b \rangle$ being cyclotomic and clean

Theorem. Let $a, b \geq 2$, $\gcd(a, b) = 1$. Let $M = \langle a, b \rangle$. Then for all $n \geq 0$, the following numbers are equal:

- ▶ the number of partitions of n all of whose part multiplicities belong to M
- ▶ the number of partitions of n into parts divisible by a or b (or both)

Consequence of $\langle a, b \rangle$ being cyclotomic and clean

Theorem. Let $a, b \geq 2$, $\gcd(a, b) = 1$. Let $M = \langle a, b \rangle$. Then for all $n \geq 0$, the following numbers are equal:

- ▶ the number of partitions of n all of whose part multiplicities belong to M
- ▶ the number of partitions of n into parts divisible by a or b (or both)

MacMahon identity: $a = 2, b = 3$

Semigroup algebra

The **semigroup algebra** $K[M]$ (over K) of a numerical semigroup M is

$$K[M] = K[z^i : i \in M].$$

Definition. Let $M = \langle a_1, \dots, a_r \rangle$. $K[M]$ is a **complete intersection** if all the relations among the generators z^{a_1}, \dots, z^{a_r} are consequences of $r - 1$ of them (the minimum possible).

Semigroup algebra

The **semigroup algebra** $K[M]$ (over K) of a numerical semigroup M is

$$K[M] = K[z^i : i \in M].$$

Definition. Let $M = \langle a_1, \dots, a_r \rangle$. $K[M]$ is a **complete intersection** if all the relations among the generators z^{a_1}, \dots, z^{a_r} are consequences of $r - 1$ of them (the minimum possible).

By elementary commutative algebra, if $K[M]$ is a complete intersection, then M is cyclotomic.

Semigroup algebra

The **semigroup algebra** $K[M]$ (over K) of a numerical semigroup M is

$$K[M] = K[z^i : i \in M].$$

Definition. Let $M = \langle a_1, \dots, a_r \rangle$. $K[M]$ is a **complete intersection** if all the relations among the generators z^{a_1}, \dots, z^{a_r} are consequences of $r - 1$ of them (the minimum possible).

By elementary commutative algebra, if $K[M]$ is a complete intersection, then M is cyclotomic.

Converse is **open** (main open problem on cyclotomic numerical semigroups).

An example

Example. $M = \langle 4, 6, 7 \rangle = \mathbb{N} - \{1, 2, 3, 5, 9\}$. Generators of $K[M]$ are $a = z^4, b = z^6, c = z^7$. Some relations:

$$a^3 = b^2, a^2b = c^2, a^7 = c^4, b^7 = c^6, \dots$$

An example

Example. $M = \langle 4, 6, 7 \rangle = \mathbb{N} - \{1, 2, 3, 5, 9\}$. Generators of $K[M]$ are $a = z^4, b = z^6, c = z^7$. Some relations:

$$a^3 = b^2, a^2b = c^2, a^7 = c^4, b^7 = c^6, \dots$$

All are consequences of the first two, so $K[M]$ is a complete intersection. E.g.,

$$c^4 = (a^2b)^2 = a^4b^2 = a^4a^3 = a^7.$$

An example

Example. $M = \langle 4, 6, 7 \rangle = \mathbb{N} - \{1, 2, 3, 5, 9\}$. Generators of $K[M]$ are $a = z^4, b = z^6, c = z^7$. Some relations:

$$a^3 = b^2, a^2b = c^2, a^7 = c^4, b^7 = c^6, \dots$$

All are consequences of the first two, so $K[M]$ is a complete intersection. E.g.,

$$c^4 = (a^2b)^2 = a^4b^2 = a^4a^3 = a^7.$$

The relation $a^3 = b^2$ has degree $3 \cdot 4 = 6 \cdot 2 = 12$.

The relation $a^2b = c^2$ has degree $2 \cdot 4 + 6 = 2 \cdot 7 = 14$

$$\Rightarrow A_M(x) = \frac{(1 - x^{12})(1 - x^{14})}{(1 - x^4)(1 - x^6)(1 - x^7)}.$$

A nonexample

$M = \langle 4, 13, 23 \rangle$. Generators of $K[M]$ are $a = z^4$, $b = z^{13}$, and $c = z^{23}$.

A nonexample

$M = \langle 4, 13, 23 \rangle$. Generators of $K[M]$ are $a = z^4$, $b = z^{13}$, and $c = z^{23}$.

Minimal relations: $a^9 = bc$, $b^3 = a^4c$, $c^2 = a^5b^2$, so **not** a complete intersection.

A nonexample

$M = \langle 4, 13, 23 \rangle$. Generators of $K[M]$ are $a = z^4$, $b = z^{13}$, and $c = z^{23}$.

Minimal relations: $a^9 = bc$, $b^3 = a^4c$, $c^2 = a^5b^2$, so **not** a complete intersection.

Note. Multiply $c^2 = a^5b^2$ by b : $c^2b = a^5b^3$. Substitute a^4c for b^3 : $c^2b = a^9c$. Divide by c : $bc = a^9$ (first relation). So why not just two relations?

A nonexample

$M = \langle 4, 13, 23 \rangle$. Generators of $K[M]$ are $a = z^4$, $b = z^{13}$, and $c = z^{23}$.

Minimal relations: $a^9 = bc$, $b^3 = a^4c$, $c^2 = a^5b^2$, so **not** a complete intersection.

Note. Multiply $c^2 = a^5b^2$ by b : $c^2b = a^5b^3$. Substitute a^4c for b^3 : $c^2b = a^9c$. Divide by c : $bc = a^9$ (first relation). So why not just two relations?

Answer: not allowed to divide (not a ring operation).

A theorem of Herzog

Theorem (H. Herzog, 1969) Let $M = \langle a, b, c \rangle$. The following conditions are equivalent.

- ▶ $K[M]$ is a complete intersection.

A theorem of Herzog

Theorem (H. Herzog, 1969) Let $M = \langle a, b, c \rangle$. The following conditions are equivalent.

- ▶ $K[M]$ is a complete intersection.
- ▶ M is a cyclotomic semigroup.

A theorem of Herzog

Theorem (H. Herzog, 1969) Let $M = \langle a, b, c \rangle$. The following conditions are equivalent.

- ▶ $K[M]$ is a complete intersection.
- ▶ M is a cyclotomic semigroup.
- ▶ If $M = \mathbb{N} - S$, then $1 - (1 - x) \sum_{j \in S} x^j$ is symmetric (palindromic).

A theorem of Herzog

Theorem (H. Herzog, 1969) Let $M = \langle a, b, c \rangle$. The following conditions are equivalent.

- ▶ $K[M]$ is a complete intersection.
- ▶ M is a cyclotomic semigroup.
- ▶ If $M = \mathbb{N} - S$, then $1 - (1 - x) \sum_{j \in S} x^j$ is symmetric (palindromic).

A theorem of Herzog

Theorem (H. Herzog, 1969) Let $M = \langle a, b, c \rangle$. The following conditions are equivalent.

- ▶ $K[M]$ is a complete intersection.
- ▶ M is a cyclotomic semigroup.
- ▶ If $M = \mathbb{N} - S$, then $1 - (1 - x) \sum_{j \in S} x^j$ is symmetric (palindromic).

Thus the main open problem on cyclotomic numerical semigroups is true for semigroups with at most three generators.

A more general framework

Key fact: a partition is determined by the multiplicity of each part, and these multiplicities are independent. Equivalently, define $\lambda \cup \mu$ by

$$m_i(\lambda \cup \mu) = m_i(\lambda) + m_i(\mu),$$

where m_i denotes the multiplicity of the part i . E.g.,

$$(6, 6, 4, 1, 1) \cup (6, 5, 4, 1) = (6, 6, 6, 5, 4, 4, 1, 1, 1).$$

Then \cup makes the set of all partitions of all $n \geq 0$ into a free commutative monoid with unique basis $\{(1), (2), (3), \dots\}$.

A more general framework

Key fact: a partition is determined by the multiplicity of each part, and these multiplicities are independent. Equivalently, define $\lambda \cup \mu$ by

$$m_i(\lambda \cup \mu) = m_i(\lambda) + m_i(\mu),$$

where m_i denotes the multiplicity of the part i . E.g.,

$$(6, 6, 4, 1, 1) \cup (6, 5, 4, 1) = (6, 6, 6, 5, 4, 4, 1, 1, 1).$$

Then \cup makes the set of all partitions of all $n \geq 0$ into a free commutative monoid with unique basis $\{(1), (2), (3), \dots\}$.

Further details omitted.

A more general framework

Key fact: a partition is determined by the multiplicity of each part, and these multiplicities are independent. Equivalently, define $\lambda \cup \mu$ by

$$m_i(\lambda \cup \mu) = m_i(\lambda) + m_i(\mu),$$

where m_i denotes the multiplicity of the part i . E.g.,

$$(6, 6, 4, 1, 1) \cup (6, 5, 4, 1) = (6, 6, 6, 5, 4, 4, 1, 1, 1).$$

Then \cup makes the set of all partitions of all $n \geq 0$ into a free commutative monoid with unique basis $\{(1), (2), (3), \dots\}$.

Further details omitted.

Where else can we find such monoids?

Polynomials over finite fields

Fix a prime power q .

$\beta(n)$: number of monic irreducible polynomials of degree n over \mathbb{F}_q .

Polynomials over finite fields

Fix a prime power q .

$\beta(n)$: number of monic irreducible polynomials of degree n over \mathbb{F}_q .

$$\beta(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} \quad (\text{irrelevant})$$

Polynomials over finite fields

Fix a prime power q .

$\beta(n)$: number of monic irreducible polynomials of degree n over \mathbb{F}_q .

$$\beta(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} \quad (\text{irrelevant})$$

There are q^n monic polynomials of degree n over \mathbb{F}_q . Every such polynomial is uniquely (up to order of factors) a product of monic irreducible polynomials. Hence

$$\sum_{n \geq 0} q^n x^n = \frac{1}{1 - qx} = \prod_{m \geq 1} (1 - x^m)^{-\beta(m)}.$$

Polynomials over finite fields

Fix a prime power q .

$\beta(n)$: number of monic irreducible polynomials of degree n over \mathbb{F}_q .

$$\beta(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} \quad (\text{irrelevant})$$

There are q^n monic polynomials of degree n over \mathbb{F}_q . Every such polynomial is uniquely (up to order of factors) a product of monic irreducible polynomials. Hence

$$\sum_{n \geq 0} q^n x^n = \frac{1}{1 - qx} = \prod_{m \geq 1} (1 - x^m)^{-\beta(m)}.$$

(cyclomatic identity)

Powerful polynomials

Example. Let $f(n)$ be the number of monic polynomials of degree n over \mathbb{F}_q such that every irreducible factor has multiplicity at least two (**powerful polynomials**). Thus

Powerful polynomials

Example. Let $f(n)$ be the number of monic polynomials of degree n over \mathbb{F}_q such that every irreducible factor has multiplicity at least two (**powerful polynomials**). Thus

$$\begin{aligned}\sum_{n \geq 0} f(n)x^n &= \prod_{m \geq 1} (1 + x^{2m} + x^{3m} + \dots)^{\beta(m)} \\ &= \prod_{m \geq 1} \left(\frac{1 - x^{6m}}{(1 - x^{2m})(1 - x^{3m})} \right)^{\beta(m)} \\ &= \frac{1 - qx^6}{(1 - qx^2)(1 - qx^3)} \\ &= \frac{1 + x + x^2 + x^3}{1 - qx^2} - \frac{x(1 + x + x^2)}{1 - qx^3} \\ \Rightarrow f(n) &= q^{\lfloor n/2 \rfloor} + q^{\lfloor n/2 \rfloor - 1} - q^{\lfloor (n-1)/3 \rfloor}.\end{aligned}$$

Generalization.

Theorem. Let S be a cyclotomic subset of \mathbb{P} , so

$$\frac{1}{1-x} - \sum_{i \in S} x^i = \frac{\prod (1-x^i)^{a_i}}{\prod (1-x^j)^{b_j}},$$

where the products are **finite**. Let $f(n)$ be the number of monic polynomials of degree n over \mathbb{F}_q such that no irreducible factor has multiplicity $m \in S$. Then

$$\sum f(n)x^n = \frac{\prod_i (1-qx^i)^{a_i}}{\prod_j (1-qx^j)^{b_j}}.$$

Generalization.

Theorem. Let S be a cyclotomic subset of \mathbb{P} , so

$$\frac{1}{1-x} - \sum_{i \in S} x^i = \frac{\prod (1-x^i)^{a_i}}{\prod (1-x^j)^{b_j}},$$

where the products are **finite**. Let $f(n)$ be the number of monic polynomials of degree n over \mathbb{F}_q such that no irreducible factor has multiplicity $m \in S$. Then

$$\sum f(n)x^n = \frac{\prod_i (1-qx^i)^{a_i}}{\prod_j (1-qx^j)^{b_j}}.$$

Can convert to a partial fraction in q and find an explicit (though in general very lengthy) formula for $f(n)$.

An example

$$S = \{1, 2, 3, 5, 7, 11\}$$

$$\sum_{n \geq 0} f(n)x^n = \frac{(1 - qx^{12})(1 - qx^{18})}{(1 - qx^4)(1 - qx^6)(1 - qx^9)}$$

An example

$$\begin{aligned} S &= \{1, 2, 3, 5, 7, 11\} \\ \sum_{n \geq 0} f(n)x^n &= \frac{(1 - qx^{12})(1 - qx^{18})}{(1 - qx^4)(1 - qx^6)(1 - qx^9)} \\ &= \frac{\Phi_2\Phi_4\Phi_8\Phi_7\Phi_{14}}{\Phi_5(1 - qx^4)} + \frac{\Phi_3\Phi_9 x^8}{\Phi_5(1 - qx^9)} \\ &\quad - \frac{\Phi_2\Phi_3\Phi_4\Phi_6^2\Phi_{12} x^2}{1 - qx^6}, \end{aligned}$$

where $\Phi_j = \Phi_j(x)$.

Yet another example

Let $S = \{2, 3, 4, \dots\}$. Recall

$$\frac{1}{1-x} - \sum_{i \in S} x^i = 1 + x = \frac{1-x^2}{1-x}.$$

$f(n)$: number of **squarefree** monic polynomials of degree n over \mathbb{F}_q . Then

$$\begin{aligned} \sum_{n \geq 0} f(n)x^n &= \frac{1-qx^2}{1-qx} \\ &= 1 + qx + \sum_{n \geq 2} (q-1)q^{n-1}x^n \\ \Rightarrow f(n) &= (q-1)q^{n-1}, \quad n \geq 2 \quad (\text{well-known}), \end{aligned}$$

Yet another example

Let $S = \{2, 3, 4, \dots\}$. Recall

$$\frac{1}{1-x} - \sum_{i \in S} x^i = 1 + x = \frac{1-x^2}{1-x}.$$

$f(n)$: number of **squarefree** monic polynomials of degree n over \mathbb{F}_q . Then

$$\begin{aligned} \sum_{n \geq 0} f(n)x^n &= \frac{1-qx^2}{1-qx} \\ &= 1 + qx + \sum_{n \geq 2} (q-1)q^{n-1}x^n \\ \Rightarrow f(n) &= (q-1)q^{n-1}, \quad n \geq 2 \quad (\text{well-known}), \end{aligned}$$

a kind of analogue (though not a q -analogue in the usual sense) of Euler's result on partitions of n into distinct parts and into odd parts.

Factorization of integers

Most familiar free commutative monoid: $\mathbb{P} = \{1, 2, 3, \dots\}$ under multiplication.

Factorization of integers

Most familiar free commutative monoid: $\mathbb{P} = \{1, 2, 3, \dots\}$ under multiplication.

For functions $f(n)$ involving factorization of integers into primes, often convenient to use **Dirichlet series** $\sum_{n \geq 1} f(n)n^{-s}$. In particular,

$$\begin{aligned}\zeta(s) &= \sum_{n \geq 1} n^{-s} \\ &= \prod_p (1 + p^{-s} + p^{-2s} + p^{-3s} + \dots) \\ &= \prod_p \frac{1}{1 - p^{-s}}.\end{aligned}$$

Powerful numbers

A positive integer is **powerful** if $p|n \Rightarrow p^2|n$ when p is prime.

$$\begin{aligned} F(s) &:= \sum_{\substack{n \geq 1 \\ n \text{ powerful}}} n^{-s} \\ &= \prod_p (1 + p^{-2s} + p^{-3s} + p^{-4s} + \dots) \\ &= \prod_p \left(\frac{1}{1 - p^{-s}} - p^{-s} \right) \\ &= \prod_p \frac{1 - p^{-6s}}{(1 - p^{-2s})(1 - p^{-3s})} \\ &= \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)} \quad (\text{Golomb, 1970}) \end{aligned}$$

Insignificant corollary

$$\zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \zeta(12) = \frac{691\pi^{12}}{638512875}$$

$$\begin{aligned} \Rightarrow \sum_{\substack{n \geq 1 \\ n \text{ powerful}}} \frac{1}{n^2} &= \frac{\zeta(4)\zeta(6)}{\zeta(12)} \\ &= \frac{15015}{1382\pi^2} \\ &\approx 1.100823\dots \end{aligned}$$

A general result

Theorem. Let S be a finite cyclotomic subset of \mathbb{P} , so

$$\frac{1}{1-x} - \sum_{i \in S} x^i = \frac{\prod (1-x)^{a_i}}{\prod (1-x)^{b_j}} \quad (\text{finite products}).$$

Then

$$\sum_n n^{-s} = \frac{\prod \zeta(b_i s)}{\prod \zeta(a_j s)},$$

where n ranges over all positive integers such that if $m \in S$, then no prime p divides n with multiplicity m .

The final slide

The final slide

