Some Combinatorial Aspects of Cyclotomic Polynomials

Richard P. Stanley
M.I.T. and U. Miami

February 2024

A theorem of Schur

Theorem (**Schur**, 1926) *The number $f(n)$ of partitions of n for which no part appears exactly once equals the number of partitions of n into parts $\not\equiv \pm 1 \pmod 6$.*

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

Why does this work?

$\Phi_n(x)$: the nth **cyclotomic polynomial**

$$\Phi_n(x) = \prod_{\substack{1 \le j \le n \\ \gcd(j,n)=1}} \left(x - e^{2\pi i j/n}\right) = \prod_{d|n} (1 - x^d)^{\mu(n/d)}$$

1. (the main point)

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

Why does this work?

$\Phi_n(x)$: the nth **cyclotomic polynomial**

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

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. $F(x)F(x^2)F(x^3)\cdots = \dfrac{1}{(1-x^{a_1})(1-x^{a_2})\cdots}$,
   where $1 \leq a_1 < a_2 < \cdots$

Cyclotomic sets

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

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

where $N_S(x)$ is a finite product of cyclotomic polynomials.

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

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

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

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

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

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

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

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

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

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

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

A further example

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

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

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

Properties of finite cyclotomic sets

Classification: wide open.

Properties of finite cyclotomic sets

Classification: wide open.

1. If S is a finite cyclotomic set, then $\max(S)$ is odd.

   Proof. We have $\deg \Phi_n(x)$ is even for $n > 2$. Since $N_S(x) = 1 - (1-x)\sum_{j \in S} x^j$ we have $\deg N_S(x) = 1 + \max(S)$. Thus it suffices to show that $N_S(x)$ isn't divisible by $\Phi_1(x) = x - 1$ or $\Phi_2(x) = x + 1$. But $N_S(\pm 1)$ is odd. $\square$

Properties of finite cyclotomic sets

Classification: wide open.

1. If S is a finite cyclotomic set, then $\max(S)$ is odd.

   Proof. We have $\deg \Phi_n(x)$ is even for $n > 2$. Since $N_S(x) = 1 - (1-x)\sum_{j\in S} x^j$ we have $\deg N_S(x) = 1 + \max(S)$. Thus it suffices to show that $N_S(x)$ isn't divisible by $\Phi_1(x) = x - 1$ or $\Phi_2(x) = x + 1$. But $N_S(\pm 1)$ is odd. $\square$

2. If $N_S(x)$ is divisible by $\Phi_n(x)$ then $n \neq 1$ (by above) and $n \neq p^r$, p prime.

   Proof. Suppose

   $$1 - (1-x)\sum_{j\in S} x^j = \Phi_{p^r}(x)A(x), \quad A(x) \in \mathbb{Z}[x].$$

   Set $x = 1$ to get $1 = pA(1)$, a contradiction. $\square$

Further properties

3. For $0 \le j \le d = \max(S)$, exactly one of j and $d - j$ belongs to S. Hence $\#S = (d+1)/2$ (yielding another proof that d is odd).

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

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

Further properties

3. For $0 \le j \le d = \max(S)$, exactly one of j and $d - j$ belongs to S. Hence $\#S = (d+1)/2$ (yielding another proof that d is odd).

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

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

4. 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

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

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

An example

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

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

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

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).

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

(b) $M = \langle 5, 6, 7 \rangle = \mathbb{N} - \{1, 2, 3, 4, 9\}$ is not 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 $M = \langle a_1, \ldots, a_r \rangle$. M is a **complete intersection** if all the relations among the generators $z^{a_1}, \ldots, z^{a_r}$ 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 $M = \langle a_1, \ldots, a_r \rangle$. M is a **complete intersection** if all the relations among the generators $z^{a_1}, \ldots, z^{a_r}$ 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 $M = \langle a_1, \ldots, a_r \rangle$. M is a **complete intersection** if all the relations among the generators $z^{a_1}, \ldots, z^{a_r}$ 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 semigrops).

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:

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

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:

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

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

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

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:

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

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

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

The relation $a^3 = b^2$ has degree $3 \cdot 4 = 6 \cdot 2 = 12$.
The relation $a^2 b = c^2$ has degree $2 \cdot 4 + 6 = 2 \cdot 7 = 14$

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

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

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

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

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

Generalization.

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

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

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*

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

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 $f(n)$.

Another example

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

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

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

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

Another example

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

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

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

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

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.

A generalization

- Argument did not involve $\beta(d)$.

A generalization

- Argument did not involve $\beta(d)$.
- Hence works for other situations with unique factorization.

A generalization

- Argument did not involve $\beta(d)$.
- Hence works for other situations with unique factorization.
- What about $\mathbb{Z}$?

A generalization

- Argument did not involve $\beta(d)$.
- Hence works for other situations with unique factorization.
- What about $\mathbb{Z}$?

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

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

Let ζ denote the Riemann zeta function. 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 $k \in S$, then no prime p divides n with multiplicity $m \in S$.

Happy 70th birthday, Bruce!