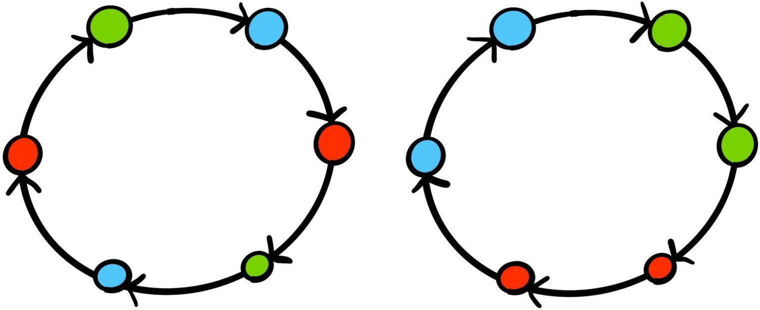
Cyclotomic Factors of Necklace Polynomials

Trevor Hyde
University of Michigan

Necklaces

Necklaces of length 6 in 3 colors:



Necklace is **primitive** if it has no rotational symmetry.

Counting Primitive Necklaces

Fact: For each length $d \geq 1$ there is a polynomial $M_d(x)$ such that $M_d(k)$ is the number of length d primitive necklaces in k colors.

$M_d(x)$ is called the d**th necklace polynomial**,

$$M_d(x) = \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e}.$$

Ex. $d = 10$,

$$M_{10}(x) = \tfrac{1}{10}(x^{10} - x^5 - x^2 + x).$$

Other Interpretations

- Necklace polys. arise naturally in a variety of contexts.
  - Algebraic dynamics
  - Representation theory
  - Lie algebras
  - Group theory
  - Number theory

- **Ex.** (Witt) The dimension of the degree d homogeneous part of the free Lie algebra on g generators is $M_d(g)$.

- **Ex.** (Gauss) If q is a prime power, then $M_d(q)$ is the number of degree d irreducible polynomials in $\mathbb{F}_q[x]$.

How Does $M_d(x)$ Factor?

$$M_{10}(x) = \tfrac{1}{10}(x^{10} - x^5 - x^2 + x)$$

$$= \tfrac{1}{10}(x^3 + x^2 - 1)(x^2 - x + 1)(x^2 + 1)(x + 1)(x - 1)x$$

How Does $M_d(x)$ Factor?

$$M_{10}(x) = \frac{1}{10}(x^{10} - x^5 - x^2 + x)$$

$$= \frac{1}{10}(x^3 + x^2 - 1)(x^2 - x + 1)(x^2 + 1)(x + 1)(x - 1)x$$

$$= \frac{1}{10}(x^3 + x^2 - 1) \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_2 \cdot \Phi_1 \cdot x$$

- $\Phi_m(x)$ is the *m*th **cyclotomic polynomial**, the minimal polynomial over $\mathbb{Q}$ of ζ_m a primitive *m*th root of unity.

More Examples

$$\begin{aligned} M_{105}(x) &= \tfrac{1}{105}(x^{105} - x^{35} - x^{21} - x^{15} + x^7 + x^5 + x^3 - x) \\ &= f_1 \cdot \Phi_8 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x \end{aligned}$$

$$\begin{aligned} M_{253}(x) &= \tfrac{1}{253}(x^{253} - x^{23} - x^{11} + x) \\ &= f_2 \cdot \Phi_{24} \cdot \Phi_{22} \cdot \Phi_{11} \cdot \Phi_{10} \cdot \Phi_8 \cdot \Phi_5 \cdot \Phi_2 \cdot \Phi_1 \cdot x \end{aligned}$$

$$\begin{aligned} M_{741}(x) &= \tfrac{1}{741}(x^{741} - x^{247} - x^{57} - x^{39} + x^{19} + x^{13} + x^3 - x) \\ &= f_3 \cdot \Phi_{20} \cdot \Phi_{18} \cdot \Phi_{12} \cdot \Phi_9 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x, \end{aligned}$$

where f_1, f_2, f_3 are non-cyclotomic irred. polynomials of degrees 92, 210, and 708 respectively.

Cyclotomic Factor Phenomenon (CFP)

CFP: The preponderance of cyclotomic factors of necklace polynomials.

- $\Phi_m(x)$ dividing $M_d(x)$ is equivalent to $M_d(\zeta_m) = 0$.

Question: When and why does $\Phi_m(x)$ divide $M_d(x)$?

Simplifying Conjecture

Observation: When $\Phi_m(x)$ divides $M_{105}(x)$, so does $\Phi_e(x)$ for all divisors $e \mid m$.

$$M_{105}(x) = f \cdot \Phi_8 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x$$

Recall that

$$x^m - 1 = \prod_{e \mid m} \Phi_e(x).$$

Thus all cyclotomic factors of $M_{105}(x)$ accounted for by

$$x^8 - 1,\ x^6 - 1 \mid M_{105}(x).$$

Simplifying Conjecture

Most cyclotomic factors of necklace polynomials are accounted for by factors of the form $x^m - 1$, but not all!

$$M_{10}(x) = g \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_2 \cdot \Phi_1 \cdot x$$

- Φ_6 divides $M_{10}(x)$ but Φ_3 does not.

Recall that

$$x^m + 1 = \prod_{\substack{e \mid 2m \\ e \nmid m}} \Phi_e(x).$$

- $x^3 + 1 = \Phi_6 \cdot \Phi_2$, thus all cyclotomic factors of $M_{10}(x)$ accounted for by

$$x^3 + 1,\ x^4 - 1 \mid M_{10}(x).$$

Simplifying Conjecture

Conjecture (H. 2018)

If $\Phi_m(x)$ divides $M_d(x)$, then either $x^m - 1$ divides $M_d(x)$ or m is even and $x^{m/2} + 1$ divides $M_d(x)$.

- Checked for $1 \leq m \leq 300$ and $1 \leq d \leq 5000$.
- Easier to analyze factors for the form $x^m \pm 1$!
- (Heuristic) There are good reasons for $M_d(x)$ to have factors of the form $x^m \pm 1$ and we do not expect any special factors without a good reason.

Structure of Cyclotomic Factors

This result highlights some of the structure underlying the CFP.

Theorem (H. 2018)

Let $m, d \geq 1$.

- *Ubiquity*
  - *If $p \mid d$ is a prime and $p \equiv 1 \bmod m$, then $x^m - 1 \mid M_d(x)$.*
    - *In particular, $x^{p-1} - 1 \mid M_d(x)$ for each $p \mid d$.*
- *Multiplicative Inheritance*
  - *If $x^m - 1 \mid M_d(x)$, then $x^m - 1 \mid M_{de}(x)$.*
  - *If $x^m + 1 \mid M_d(x)$ and e is odd, then $x^m + 1 \mid M_{de}(x)$.*
    - *$M_d(x)$ generally does not divide $M_{de}(x)$.*
- *Necessary Condition*
  - *If $x^m - 1 \mid M_d(x)$, then $m \mid \varphi(d)$.*
    - *$\varphi(d) := |(\mathbb{Z}/(d))^\times|$ is the **Euler totient function**.*

Non-Trivial Factors

Thm: If $p \mid d$, then $x^{p-1} - 1$ divides $M_d(x)$.

- $M_p(x) = \frac{1}{p}(x^p - x)$.

Ex. $d = 105 = 3 \cdot 5 \cdot 7$.

$$\begin{aligned} M_{105}(x) &= \tfrac{1}{105}(x^{105} - x^{35} - x^{21} - x^{15} + x^7 + x^5 + x^3 - x) \\ &= f_1 \cdot \Phi_8 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x \end{aligned}$$

- **Non-trivial** factors $x^m \pm 1$ are those not given by theorem.

- $x^8 - 1$ is a non-trivial factor of $M_{105}(x)$.

Goal: Characterize/classify the non-trivial cyclotomic factors of necklace polynomials.

CFP & Relations in Cyclotomic Units

Theorem (H. 2018)

Let $m, d \geq 1$ such that $m \nmid d$. If $x^m - 1 \mid M_d(x)$, then

$$\frac{x^m - 1}{x - 1} \mid \Phi_d(x) - 1.$$

Equivalently, if $M_d(\zeta_m) = 0$ for all mth roots of unity ζ_m, then for all non-trivial ζ_m,

$$\Phi_d(\zeta_m) = 1.$$

CFP & Relations in Cyclotomic Units

Theorem (H. 2018)

Let $m, d \geq 1$ such that $m \nmid d$. If $M_d(\zeta_m) = 0$ for all mth roots of unity ζ_m, thenfor all non-trivial ζ_m

$$\Phi_d(\zeta_m) = 1.$$

Ex. $x^8 - 1 \mid M_{105}(x)$, so

$$1 = \Phi_{105}(\zeta_8) = \prod_{j \in (\mathbb{Z}/(105))^\times} (\zeta_8 - \zeta_{105}^j).$$

- Factors on right are called **cyclotomic units**.
- CFP gives multiplicative relations in cyclotomic units.

CFP & Relations in Cyclotomic Units

- There are trivial relations satisfied by cyclotomic units coming from complex conjugation and taking norms.

- Milnor conj. only trivial relations,
  Bass (1966) published a proof.

- Ennola (1972) discovered new non-trivial relations, proved these give complete presentation.

Observation:

▷ Trivial cyclo. factors of necklace polys. give trivial cyclo. unit relations.

▷ Non-trivial cyclo. factors give non-trivial cyclo. unit relations.

CFP & Euler Characteristics

Let $\mathrm{Irr}_d(K)$ denote the space of deg. d irreducible monic polynomials in $K[x]$.

- $M_d(q) = |\mathrm{Irr}_d(\mathbb{F}_q)|$.

Theorem (H. 2018)

Let $d \geq 1$ and let χ_c denote the ***compactly supported Euler characteristic****.*

- $$M_d(1) = \chi_c(\mathrm{Irr}_d(\mathbb{C})) = \begin{cases} 1 & d = 1 \\ 0 & d > 1. \end{cases}$$
- $$M_d(-1) = \chi_c(\mathrm{Irr}_d(\mathbb{R})) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & d > 2. \end{cases}$$

CFP & Euler Characteristics

- Since $\mathbb{C}$ is alg. closed, only have irreducible polynomials in degree 1.

$$\mathrm{Irr}_{d,1}(\mathbb{C}) = \begin{cases} \mathbb{C} & d = 1 \\ \emptyset & d > 1. \end{cases} \implies M_d(1) = \begin{cases} 1 & d = 1 \\ 0 & d > 1. \end{cases}$$

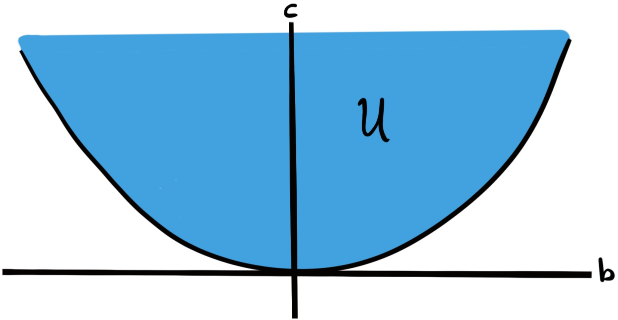
- Therefore $d > 1$ implies $\Phi_1 = x - 1$ divides $M_d(x)$.

CFP & Euler Characteristics

- All irreducible polynomials over $\mathbb{R}$ have degree at most 2.

$$\mathrm{Irr}_{d,1}(\mathbb{R}) = \begin{cases} \mathbb{R} & d = 1 \\ \mathcal{U} & d = 2 \\ \emptyset & d > 2, \end{cases} \implies M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & d > 2. \end{cases}$$

- $\mathcal{U} = \{x^2 + bx + c : b^2 - 4c < 0\}$



CFP & Euler Characteristics

- All irred. polys. over $\mathbb{R}$ have degree at most 2.

$$\mathrm{Irr}_{d,1}(\mathbb{R}) = \begin{cases} \mathbb{R} & d = 1 \\ U & d = 2 \\ \emptyset & d > 2, \end{cases} \implies M_d(-1) = \begin{cases} -1 & d = 1 \\ 1 & d = 2 \\ 0 & d > 2. \end{cases}$$

- Therefore, $d > 2$ implies $x^2 - 1$ divides $M_d(x)$.
- Geometric explanation of $M_d(\zeta_m) = 0$ for $m > 2$?

Generalizations

The CFP extends along at least two natural generalizations of necklace polynomials.

- If G is a finite group then one can define a G**-necklace polynomial** $M_G(x)$.
  - If $G = C_d$ is cyclic, then $M_{C_d}(x) = M_d(x)$.
  - CFP holds whenever G is solvable.
- If $d, n \geq 1$, let $\mathrm{Irr}_{d,n}(\mathbb{F}_q)$ be the space of deg. d irreducible polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$.
  - Define the **higher necklace polynomials** $M_{d,n}(x)$ by

$$M_{d,n}(q) := |\mathrm{Irr}_{d,n}(\mathbb{F}_q)|.$$

  - $M_{d,1}(x) = M_d(x)$.
  - For each n, CFP holds for all but finitely many d.

Thank you!