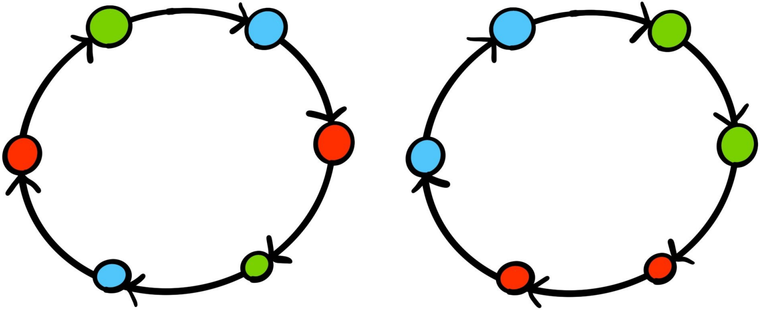
Cyclotomic Factors of Necklace Polynomials

Trevor Hyde
University of Michigan

Necklaces

Necklaces of length 6 in 3 colors:



Colored necklace is **aperiodic** if it has no rotational symmetry.

Counting Aperiodic 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 aperiodic necklaces in k colors.

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

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

Ex.

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

Other Interpretations

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

- **Ex.** 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?

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

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

How Does $M_d(x)$ Factor?

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

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

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

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

More Examples!

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

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

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

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 $M_d(\zeta_m) = 0$.

Questions:

- (Conceptual) Why do cyclotomic polynomials divide necklace polynomials?
- (Analytical) For which (m, d) 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

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

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**.*

Differences of Necklace Polynomials

Even when $M_d(\zeta_m) \neq 0$, there is structure to the values $M_d(\zeta_m)$!

Let $S_d(x) := dM_d(x) = \sum_{e|d} \mu(e)x^{d/e}$ (clear denominators).

$$\begin{aligned} S_{91}(x) - S_6(x) &= x^{91} - x^{13} - x^7 - x^6 + x^3 + x^2 \\ &= f \cdot \Phi_5 \cdot \Phi_2 \cdot \Phi_1 \cdot x^2 \end{aligned}$$

- Φ_1, Φ_2 divide both $S_6(x)$ and $S_{91}(x)$, but Φ_5 divides neither!
- Thus $S_{91}(\zeta_5) = S_6(\zeta_5)$ for all 5th roots of unity ζ_5.

Primewise Congruence

Definition

*Say d and e are **primewise congruent modulo** m and write $d \equiv_{pw} e \bmod m$ if d and e have prime factorizations*

$$d = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$
$$e = q_1^{a_1} q_2^{a_2} \cdots q_k^{a_k}$$

where $p_i \equiv q_i \bmod m$ for each i.

- Primewise congruence is strictly stronger than congruence:

  $$d \equiv_{pw} e \bmod m \implies d \equiv e \bmod m,$$

  but $11 \equiv 6 \bmod 5$ and $11 \not\equiv_{pw} 6 \bmod 5$.

Differences of Necklace Polynomials

Theorem (H. 2018)

Let $S_d(x) = dM_d(x)$. If $d \equiv_{pw} e \mod m$, then

$$S_d(x) \equiv S_e(x) \bmod x^m - 1.$$

Hence $S_d(\zeta_m) = S_e(\zeta_m)$ for all mth roots of unity ζ_m.

- As a function on mth roots of unity, $S_d(x)$ only depends on d up to primewise congruence modulo m.
- $91 \equiv_{pw} 6 \bmod 5$ since $91 = 7 \cdot 13$ and $6 = 2 \cdot 3$.
  - ▷ Theorem implies $x^5 - 1 \mid S_{91}(x) - S_6(x)$.

Necklace Operators

For $d \geq 1$ and $f(x) \in \mathbb{Q}[x]$ define the polynomial operator $[M_d]$ by

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

- We call $[M_d]$ the d**th necklace operator**.
- $M_d(x) = [M_d]x$

Claim: The CFP is a property of the operator $[M_d]$ more so than of the polynomial $M_d(x)$.

Necklace Operators

Theorem (H. 2018)

Let $f(x) \in \mathbb{Q}[x]$ and $d \geq 1$.

1. *If $x^m - 1 \mid M_d(x)$, then*
$$x^m - 1 \mid [M_d]f(x) := \frac{1}{d}\sum_{e|d} \mu(e) f(x^{d/e}).$$
2. *If $x^m + 1 \mid M_d(x)$ and $f(x)$ is an odd polynomial, then*
$$x^m + 1 \mid [M_d]f(x).$$

- Recall $f(x)$ **odd** means $f(-x) = -f(x)$.
- Second implication can fail if $f(x)$ is not odd.

Necklace Operators & Cyclotomic Relations

$$
\begin{aligned}
x^d - 1 = \prod_{e|d} \Phi_e(x) \implies \Phi_d(x) &= \prod_{e|d} (x^{d/e} - 1)^{\mu(e)} \\
\implies \log \Phi_d(x) &= \sum_{e|d} \mu(e) \log(x^{d/e} - 1) \\
\implies \log \Phi_d(x) &= d[M_d] \log(x - 1).
\end{aligned}
$$

Theorem (almost) shows that $M_d(\zeta_m) = 0$ implies

$$\log \Phi_d(\zeta_m) = 0 \quad (\iff \Phi_d(\zeta_m) = 1.)$$

Problem: $\log(x - 1)$ is not a polynomial!

Necklace Operators & Cyclotomic Relations

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

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

Necklace Operators & Cyclotomic Relations

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. $x^{15} - 1 \mid M_{6061}(x)$, so

$$1 = \Phi_{6061}(\zeta_{15}) = \prod_{j \in (\mathbb{Z}/(6061))^\times} (\zeta_{15} - \zeta_{6061}^j).$$

- Factors on right are called **cyclotomic units**.
- Cyclo. factors of necklace polys. correspond to multiplicative relations of cyclo. units!

Generalizations

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

1. 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.

2. 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.

Balanced Base Expansions

Let $b, n \geq 1$. Say n has a **balanced base b expansion** if all base b digits of n are 0 or $b-1$.

$$n = \sum_i (b-1)b^{k_i} = \sum_k a_k b^k,$$

where $a_k = -1, 0, 1$.

Ex.$n = 13$ and $b = 2$

$$\begin{aligned} 13 &= 2^3 + 2^2 + 1 \\ &= (2-1)2^3 + (2-1)2^2 + (2-1) \\ &= 2^4 - 2^3 + 2^3 - 2^2 + 2 - 1 \\ &= 2^4 - 2^2 + 2 - 1 \end{aligned}$$

Balanced Base Expansions

Let $b, n \geq 1$. Say n has a **balanced base b expansion** if all base b digits of n are 0 or $b-1$.

$$n = \sum_i (b-1)b^{k_i} = \sum_k a_k b^k,$$

where $a_k = -1, 0, 1$. Call this the **balanced expansion** of n.

Ex. $n = 13$ and $b = 2$

$$\begin{aligned} 13 &= 2^3 + 2^2 + 1 \\ &= (2-1)2^3 + (2-1)2^2 + (2-1) \\ &= 2^4 - 2^3 + 2^3 - 2^2 + 2 - 1 \\ &= 2^4 - 2^2 + 2 - 1 \end{aligned}$$

Higher CFP

Recall $M_{d,n}(x)$ is defined implicitly by

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

Theorem (H. 2018)

If p is a prime and n has a balanced base p expansion $n = \sum_k a_k p^k$, then for $\zeta_p \neq 1$ a pth root of unity,

$$M_{d,n}(\zeta_p) = \begin{cases} a_k & d = p^k \\ 0 & \textit{otherwise.} \end{cases}$$

Therefore, for each such n and for all but finitely many d we have

$$x^p - 1 \mid M_{d,n}(x).$$

Connection to Geometry

If K is a field, let $\mathrm{Irr}_{d,n}(K)$ denote the space of deg. d irreducible polynomials in $K[x_1, x_2, \ldots, x_n]$.

Theorem (H. 2018)

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

1. $$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{C})) = M_{d,n}(1) = \begin{cases} n & d = 1 \\ 0 & \text{otherwise.} \end{cases}$$

2. *Let $n = \sum_k a_k 2^k$ be the balanced base 2 expansion of n.*

$$\chi_c(\mathrm{Irr}_{d,n}(\mathbb{R})) = M_{d,n}(-1) = \begin{cases} a_k & d = 2^k \\ 0 & \text{otherwise.} \end{cases}$$

Why CFP?

We can compute $\chi_c(\mathrm{Irr}_{d,1}(\mathbb{C}))$ and $\chi_c(\mathrm{Irr}_{d,1}(\mathbb{R}))$ by hand.

- Note $M_{d,1}(x) = M_d(x)$.
- Since $\mathbb{C}$ is alg. closed, only have irred. polynomials in degree 1.

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

- For $d > 1$,

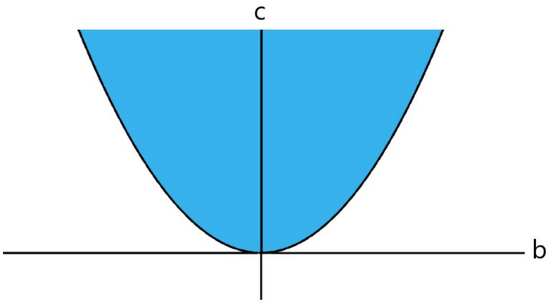
$$x - 1 \mid M_d(x).$$

Why CFP?

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

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

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



Why CFP?

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

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

- For $d > 2$,

$$x^2 - 1 \mid M_d(x).$$

- Geometric explanation of $M_d(\zeta_m) = 0$ for $m > 2$?

Thank you!

Reference: T. Hyde, Cyclotomic factors of necklace polynomials, ArXiv preprint, (2018).