The ternary cyclotomic polynomials Φ_{3pq}

Alexandre Benoist

Joint work with Prof. Antonella Perucca

November 19, 2025

Introduction

Definition

Let $n \in \mathbb{Z}_{>0}$. The n-th cyclotomic polynomial Φ_n is

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(X - \exp\left(\frac{2ik\pi}{n}\right)\right).$$

Introduction

Definition

Let $n \in \mathbb{Z}_{>0}$. The n-th cyclotomic polynomial Φ_n is

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(X - \exp\left(\frac{2ik\pi}{n}\right)\right).$$

First properties :

- $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Introduction

Definition

Let $n \in \mathbb{Z}_{>0}$. The n-th cyclotomic polynomial Φ_n is

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(X - \exp\left(\frac{2ik\pi}{n}\right)\right).$$

First properties :

- $X^n - 1 = \prod_{d|n} \Phi_d(X)$
- It has degree $\varphi(n)$ with integer coefficients

Introduction

Definition

Let $n \in \mathbb{Z}_{>0}$. The n-th cyclotomic polynomial Φ_n is

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(X - \exp\left(\frac{2ik\pi}{n}\right)\right).$$

First properties :

- $X^n - 1 = \prod_{d|n} \Phi_d(X)$
- It has degree $\varphi(n)$ with integer coefficients
- Φ_n is monic and irreducible

Introduction

Definition

Let $n \in \mathbb{Z}_{>0}$. The n-th cyclotomic polynomial Φ_n is

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(X - \exp\left(\frac{2ik\pi}{n} \right) \right).$$

First properties :

- $X^n - 1 = \prod_{d|n} \Phi_d(X)$
- It has degree $\varphi(n)$ with integer coefficients
- Φ_n is monic and irreducible

Coefficients

- $\Phi_1(X) = X - 1$

Coefficients

- $\Phi_1(X) = X - 1$
- $\Phi_2(X) = X + 1$

Coefficients

- $\Phi_1(X) = X - 1$
- $\Phi_2(X) = X + 1$
- $\Phi_3(X) = X^2 + X + 1$

Coefficients

- $\Phi_1(X) = X - 1$
- $\Phi_2(X) = X + 1$
- $\Phi_3(X) = X^2 + X + 1$
- $\Phi_4(X) = X^2 + 1$

Coefficients

- $\Phi_1(X) = X - 1$
- $\Phi_2(X) = X + 1$
- $\Phi_3(X) = X^2 + X + 1$
- $\Phi_4(X) = X^2 + 1$
- $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$

Coefficients

- $\Phi_1(X) = X - 1$
- $\Phi_2(X) = X + 1$
- $\Phi_3(X) = X^2 + X + 1$
- $\Phi_4(X) = X^2 + 1$
- $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$
- $\Phi_6(X) = X^2 - X + 1$

Coefficients

- $\Phi_1(X) = X - 1$
- $\Phi_2(X) = X + 1$
- $\Phi_3(X) = X^2 + X + 1$
- $\Phi_4(X) = X^2 + 1$
- $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$
- $\Phi_6(X) = X^2 - X + 1$
- The first cyclotomic polynomial to have a coefficient -2 is :

$$\begin{aligned}
\Phi_{105}(X) &= X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} + X^{36} + X^{35} \\
&+ X^{34} + X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} \\
&+ X^{16} + X^{15} + X^{14} + X^{13} + X^{12} - X^{9} - X^{8} - 2X^{7} - X^{6} - X^{5} \\
&+ X^{2} + X + 1.
\end{aligned}$$

Summary

1. Binary cyclotomic polynomials
2. Structure of ternary cyclotomic polynomials
3. The family $\Phi_{3p_2p_3}$

The binary case : explicit and general computation

Let p_1 and p_2 be two odd primes such that $p_1 < p_2$, and $\Phi_{p_1p_2}(X) = \sum_{k=0}^{\varphi(p_1p_2)} a_k X^k$.

Theorem (Lam and Leung, 1996)

Let u and v be the two unique non-negative integers such that $\varphi(p_1p_2) = up_1 + vp_2$. We have

$$a_k = \begin{cases} 1 & \text{if } k = ip_1 + jp_2 \text{ with } 0 \le i \le u \text{ and } 0 \le j \le v, \\ -1 & \text{if } k = ip_1 + jp_2 - p_1p_2 \text{ with } u+1 \le i \le p_2 - 1 \text{ and } v+1 \le j \le p_1 - 1, \\ 0 & \text{otherwise.} \end{cases}$$

The integer u is determined by $up_1 \equiv \varphi(p_1p_2) \bmod p_2$. We take $v = \frac{\varphi(p_1p_2) - up_1}{p_2}$.

Illustration : the LLL diagram (Lenstra, Lam and Leung)

We take $p_1 = 5$ and $p_2 = 7$. We have $\varphi(5 \cdot 7) = 24 = 5 \cdot 2 + 7 \cdot 2$, so $u = v = 2$.

$$v+1\left\{\vphantom{\begin{matrix}1\\1\\1\end{matrix}}\right. \overbrace{\begin{pmatrix} 28 & 33 & 3 & 8 & 13 & 18 & 23 \\ 21 & 26 & 31 & 1 & 6 & 11 & 16 \\ 14 & 19 & 24 & 29 & 34 & 4 & 9 \\ 7 & 12 & 17 & 22 & 27 & 32 & 2 \\ 0 & 5 & 10 & 15 & 20 & 25 & 30 \end{pmatrix}}^{p_2} \left.\vphantom{\begin{matrix}1\\1\\1\\1\\1\end{matrix}}\right\} p_1$$

$$\underbrace{\hphantom{0 \quad 5 \quad 10}}_{u+1}$$

Illustration : the LLL diagram (Lenstra, Lam and Leung)

We take $p_1 = 5$ and $p_2 = 7$. We have $\varphi(5 \cdot 7) = 24 = 5 \cdot 2 + 7 \cdot 2$, so $u = v = 2$.

$$
\begin{array}{ccc}
 & p_2 & \\
v+1 \left\{ \begin{array}{c} \\ \\ \\ \end{array} \right. & \begin{pmatrix} 28 & 33 & 3 & 8 & 13 & 18 & 23 \\ 21 & 26 & 31 & 1 & 6 & 11 & 16 \\ 14 & 19 & 24 & 29 & 34 & 4 & 9 \\ 7 & 12 & 17 & 22 & 27 & 32 & 2 \\ 0 & 5 & 10 & 15 & 20 & 25 & 30 \end{pmatrix} & \left. \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \right\} p_1 \\
 & u+1 &
\end{array}
$$

So,

$$
\begin{aligned}
\Phi_{5\cdot 7}(X) \quad = \quad & X^{24} - X^{23} + X^{19} - X^{18} + X^{17} - X^{16} + X^{14} - X^{13} + X^{12} - X^{11} + X^{10} \\
& - X^{8} + X^{7} - X^{6} + X^{5} - X + 1.
\end{aligned}
$$

Consequences

- For every k, $a_k \in \{0, 1, -1\}$.
- Formulas for the number of non-zero coefficients : for $c \in \mathbb{Z}$, let $N_c(\Phi_{p_1 p_2})$ be the number of coefficients equal to c in $\Phi_{p_1 p_2}$. We have

$$N_1(\Phi_{p_1 p_2}) = (u+1)(v+1) \quad \text{and} \quad N_{-1}(\Phi_{p_1 p_2}) = (p_1 - v - 1)(p_2 - u - 1).$$

- Structure : the exponents of positive (or negative) coefficients are given by arithmetic progressions.

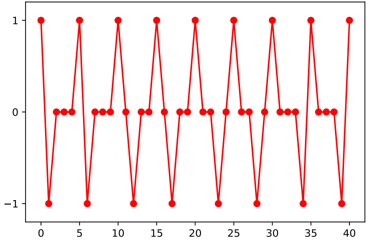


Figure – Coefficients of $\Phi_{5 \cdot 11}$.

The particular case $p_1 = 3$

- The case $p_2 \equiv 1 \bmod 3 : v = 0$. One arithmetic progression for the exponents of positive terms, two for negative terms. The coefficients are cyclic $1, -1, 0$ up to the middle, and $1, 0, -1$ after.

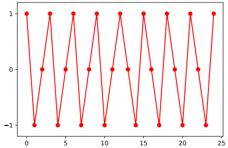


Figure – Coefficients of $\Phi_{3\cdot 13}$

- The case $p_2 \equiv 2 \bmod 3 : v = 1$. One arithmetic progression for negative terms, two for positive terms. The coefficients are cyclic $1, -1, 0$ up to the middle, and $-1, 1, 0$ after.

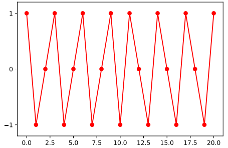
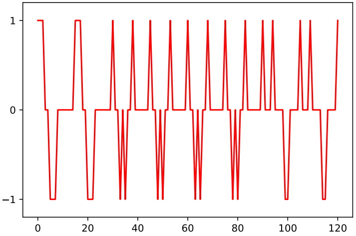


Figure – Coefficients of $\Phi_{3\cdot 11}$

Structure of ternary cyclotomic polynomials

The exponents of positive/negative terms are not described by arithmetic progressions. There are gaps (consecutive coefficients equal to 0).



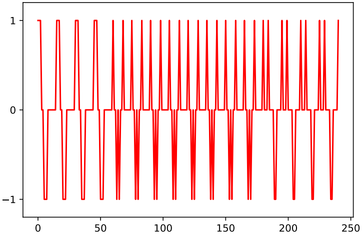


Figure – Coefficients of $\Phi_{3\cdot 5\cdot 31}$ and $\Phi_{3\cdot 5\cdot 61}$ (up to the middle)

Block structure

Let $p_1 < p_2 < p_3$ be three odd primes such that $p_3 > p_1 p_2$. Let q and r be the quotient and the remainder of the euclidean division of p_3 by $p_1 p_2$.

Definition (Blocks)

By grouping terms of degree contained between two multiples of p_3, we write

$$\Phi_{p_1 p_2 p_3} = \sum_{i=0}^{\varphi(p_1 p_2)-1} f_i(X) X^{i p_3} \quad \text{and} \quad f_i(X) = \sum_{j=0}^{q} f_{i,j}(X) X^{j p_1 p_2}.$$

The polynomials f_i are called p_3-blocks, the polynomials $f_{i,j}$ are called $p_1 p_2$-blocks for $0 \leq j < q$ and $f_{i,q}$ is an r-bloc.

Example

The polynomial $\Phi_{3.5.37}$ contains eight 37-blocks, each containing two 15-blocks and one 7-block.

Visualization of the blocks

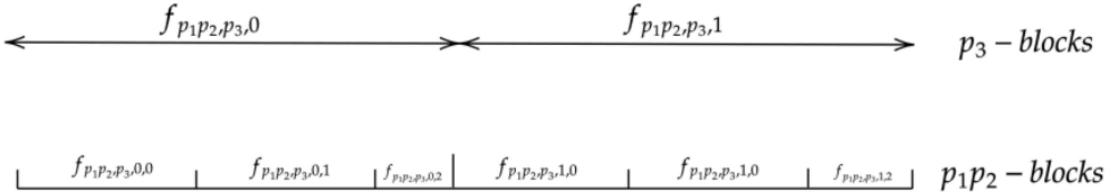


Figure – Blocks (from Jules Nies' Bachelor thesis). Example with $q = 2$.

Visualization of the blocks

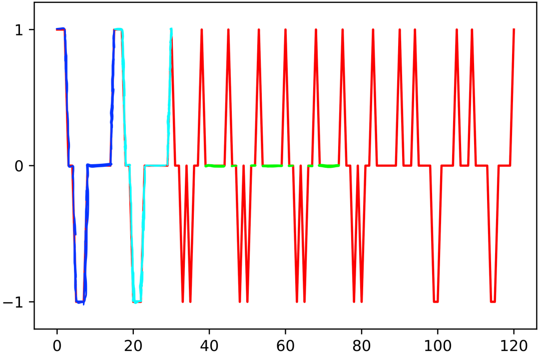


Figure – Coefficients of $\Phi_{3\cdot5\cdot31}$

Application : *maximum gap* problem

Definition (Maximum gap)

The *maximum gap* of $\Phi_{p_1 p_2 p_3}$ is the maximal number of consecutive coefficients equal to 0.

The following theorem was established by studying the gaps in each block f_i and between the blocks f_i and f_{i+1} :

Theorem (Ambrosino et al., 2021)

The maximum gap of $\Phi_{p_1 p_2 p_3}$ *is equal to* $(p_1 - 1)(p_2 - 1) - 1$.

Conjecture (Zhang, 2019)

The number of maximum gaps in $\Phi_{p_1 p_2 p_3}$ *is* $2\lfloor \frac{p_3}{p_1 p_2} \rfloor$.

Operations on blocks

Definition (Operations on the blocks)

For a p_1p_2-block $f_{i,j}$, the rotation operation $\mathcal{R}_r f_{i,j}$ consists in shifting circularly all the coefficients with a step equal to r. The truncation operation $\mathcal{T}_r f_{i,j}$ consists in keeping only the terms of degree smaller than r.

Example

For $p_1p_2 = 15$ *and* $f(X) = 1 + X + X^2 - X^5 - X^6 - X^7$, *we have*

$$\mathcal{R}_2 f(X) = X^{2-2} - X^{5-2} - X^{6-2} - X^{7-2} + X^{14-0} + X^{14-1}$$
$$\mathcal{T}_2 f(X) = 1 + X.$$

Interactions between the blocks

Write $\Psi_{p_1p_2}(X) = \frac{X^{p_1p_2}-1}{\Phi_{p_1p_2}} = -1 - X - \dots - X^{p_1-1} + X^{p_2} + \dots + X^{p_2+p_1-1}$.

Proposition (Relations between blocks)

Write $\Phi_{p_1p_2}(X) = \sum_{i=0}^{\varphi(p_1p_2)} b_i X^i$. *If* $p_3 > p_1p_2$, *we have :*

(i) $f_{0,0} = -\Psi_{p_1p_2}$

(ii) $f_{i,0} = f_{i,1} = \dots = f_{i,q-1}$,

(iii) $f_{i,q} = \mathcal{T}_r f_{i,0}$,

(iv) $f_{i+1,0} = \mathcal{R}_r f_{i,0} - b_{i+1}\Psi_{p_1p_2}$.

The family $\Phi_{3p_2p_3}$

Let $p_2 < p_3$ be two odd primes such that $p_3 > 3p_2$ and $p_3 \equiv \pm 1, \pm 2 \bmod 3p_2$. We write $\Phi_{3p_2}(X) = \sum_{i=0}^{\varphi(3p_2)} b_i X^i$. The goal is to compute all the blocks $f_{i,0}$ of $\Phi_{3p_2p_3}$ $(0 \leq i \leq \varphi(3p_2) - 1)$. To do so, we use the formula

$$f_{i,0} = -\Psi_{3p_2} \quad \text{and} \quad f_{i+1} = \mathcal{R}_r f_{i,0} - b_{i+1}\Psi_{3p_2}.$$

The family $\Phi_{3p_2p_3}$

Let $p_2 < p_3$ be two odd primes such that $p_3 > 3p_2$ and $p_3 \equiv \pm 1, \pm 2 \bmod 3p_2$. We write $\Phi_{3p_2}(X) = \sum_{i=0}^{\varphi(3p_2)} b_i X^i$. The goal is to compute all the blocks $f_{i,0}$ of $\Phi_{3p_2p_3}$ $(0 \leq i \leq \varphi(3p_2) - 1)$. To do so, we use the formula

$$f_{i,0} = -\Psi_{3p_2} \quad \text{and} \quad f_{i+1} = \mathcal{R}_r f_{i,0} - b_{i+1}\Psi_{3p_2}.$$

This is doable by hand because :

- since $r \equiv \pm 1, \pm 2 \bmod 3p_2$, we only do small rotations.
- the coefficients Φ_{3p_2} are periodic (before/after the middle coefficient).

Moreover, $\Psi_{3p_2}(X) = -1 - X - X^2 + X^{p_2} + X^{p_2+1} + X^{p_2+2}$. We partition the exponents in four "slices" :

$$S_1 = \{0, 1, 2\}, \quad S_2 = \{3, \dots, p_2 - 1\}, \quad S_3 = \{p_2, p_2 + 1, p_2 + 2\}, \quad S_4 = \{p_2 + 3, \dots, 3p_2 - 1\}.$$

Example of computation for $r = 1$ and $p_2 \equiv 1 \bmod 3$.

i	b_i	S_1			S_2	S_3			S_4
0	1	1	1	1	0 0	−1	−1	−1	0 0
1	−1	0	0	−1	0 . . . . 0−1	0	0	1	0 01
2	0	0	−1	0	0 . . 0−10	0	1	0	0 010
3	1	0	1	1	0 . 0−100	0	−1	−1	0 0100
4	−1	0	0	−1	0.0−1000	0	0	1	0 1000
...	...	...	...	...	. . . .	...	...	...	. . . .
$p_2 - 3$	−1	0	0	−1	−10 0	0	0	1	0 . . . . . . 10...0
$p_2 - 2$	0	0	−1	−1	0 0	0	1	0	0 . . . . . . 10...0
$p_2 - 1$	1	0	0	1	0 0	0	−1	−1	0 . . . . . . 10...0
p_2	0	0	1	0	0 0	−1	−1	0	0 . . . . . . 10...0
$p_2 + 1$	−1	0	−1	−1	0 . . . . 0−1	0	1	1	0 . . . . . . 10...0
...	...	...	...	...	. . . .	...	...	...	. . . .

The other cases

- Case $p_2 \equiv 2 \bmod 3$: the order of the operations from the middle is different (subtract Ψ_{3p_2}, add Ψ_{3p_2}, do nothing).
- Case $r \equiv -1$: rotations go the other way and there is a "perturbation" for S_3 at the step $p_2 - 2$, while there is no perturbation for S_1.
- Case $r \equiv \pm 2$: rotations by two indices, so more non-zero coefficients exit S_1 and S_3 to go in S_2 and S_4. So, there are more perturbations for S_1 and S_3, while S_2 and S_4 have more complex expressions. We can also reason by periodicity.

Properties for the family $\Phi_{3p_2p_3}$

Theorem

Let $p_2 < p_3$ be two odd primes such that $p_3 > 3p_2$ and $p_3 \equiv \pm 1, \pm 2 \mod 3p_2$. Then, the number of maximum gaps of $\Phi_{3p_2p_3}$ is $2\lfloor \frac{p_3}{3p_2} \rfloor$.

Properties for the family $\Phi_{3p_2p_3}$

Theorem

Let $p_2 < p_3$ be two odd primes such that $p_3 > 3p_2$ and $p_3 \equiv \pm 1, \pm 2 \bmod 3p_2$. Then, the number of maximum gaps of $\Phi_{3p_2p_3}$ is $2\lfloor \frac{p_3}{3p_2} \rfloor$.

Theorem

Let $p_2 < p_3$ be two odd primes such that $p_3 > 3p_2$ and $p_3 \equiv \pm 2 \bmod 3p_2$. Then, Φ_{3p_2} has at least one coefficient equal to 2 or -2.

Thank you !