

Cyclotomic polynomials

Experimental Mathematics Lab

Abstract

Cyclotomic polynomials are the minimal polynomials of primitive roots of unity. They are a fundamental topic in number theory and they have applications in other fields of mathematics. For instance, they appear in some geometrical problems such as straightedge and compass construction. Recently, they have been used in cryptography and some homomorphic encryption libraries.

Over $\mathbb{Q}$, the primitive n -th roots of unity are the elements $\exp\left(\frac{2ik\pi}{n}\right)$ for $\gcd(k, n) = 1$. The n -th cyclotomic polynomial is defined as

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

In fact, all cyclotomic polynomials have integer coefficients and these coefficients belong to the set $\{-1, 0, 1\}$ for every $n < 105$. For a prime number n , the n -th cyclotomic polynomial is very simple:

$$\Phi_n(X) = X^{n-1} + \dots + X + 1.$$

When n is the product of two odd primes (binary case), it is possible to compute Φ_n by hand through straightforward formulas. Much remains unknown about the ternary case, where n is the product of three odd primes. The main questions concern the height (maximum value of the coefficients), the gaps (sequences of consecutive coefficients equal to 0), or the density of non-zero coefficients: ternary cyclotomic polynomials are still an active field of research. The goal of the project is to investigate some open questions about ternary cyclotomic polynomials experimentally, using a programming language such as Python or a mathematical software system such as SageMath. Experiments might be assisted by AI.

Prerequisites

This project only relies on very basic notions of algebra. No programming experience is required.

Supervisors

- Alexandre Benoist, alexandre.benoist@uni.lu
- Prof. Antonella Perucca, antonella.perucca@uni.lu

References

- [1] K. Conrad. Cyclotomic extensions. <https://kconrad.math.uconn.edu/blurbs/galoistheory/cyclotomic.pdf>.
- [2] C. Sanna. A survey on coefficients of cyclotomic polynomials. <https://arxiv.org/abs/2111.04034>, 2021.