# polynomes cyclotomiques

Mano Etilé

January 2026

## 1 Définition

On définit le $n$-ième polynome cyclotomique comme $\Phi_n(X) = \prod(X - z_i)$ où les $z_i$ sont les racines primitives $n$-ième de l'unité.

On définit la fonction de Mobius par $\mu(n) = 1$ si $n = 1$, $\mu(n) = (-1)^k$ si $n$ est le produit de $k$ nombres premiers distincts, et $\mu(n) = 0$ sinon. Elle est multiplicative mais pas multiplicative.

## 2 Propriété

Citons un nombre de propriété en vrac :

- $X^n - 1 = \prod_{d|n} \Phi_n(X)$
- $\Phi_n$ est à coefficients entiers.
- $n = \sum_{d|n} \phi(d)$
- $X^n + 1 = \prod_{d|n} \Phi_{2d}(X)$
- $\Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}$
- Si $p$ est premier $\Phi_{pn}(X) = \Phi_n(X^p)$ Si $p|n$ et $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ Sinon.
- Si $n \geq 3$ est un entier impair, $\Phi_{2n}(X) = \Phi_n(-X)$
- Si $n$ et $a$ sont premiers entre eux alors $\Phi_n(X^a) = \prod_{d|a} \Phi_{nd}(X)$
- (lemme d'encadrement) pour tout $a$ complexe, on a $||a|-1|^{\phi(n)} \leq |\Phi_n(a)| \leq (|a| + 1)^{\phi(n)}$, de manière stricte pour $n \geq 3$
- $\Phi_n$ est irréductible modulo $Q$.

Citons celles en lien avec l'ordre multiplicatif :

- Soit $a, n$ des entiers positifs et $p$ un nombre premier. Si, modulo $p$, on a un polynome à coefficients entiers tel que $X^n - 1 = (X - a)^2 P(X)$ modulo $p$, alors $p$ divise $n$

• Si $p$ est premier tel que $p|\Phi_n(a)$ et $p|\Phi_d(a)$ où $d|n$ avec $d \neq n$ alors $p$ divise $n$

• Soient $m, n > 1$ des entiers, $a$ un entier relatif et $p$ un nombre premier. On suppose que $p$ divise $\Phi_m(a)$ et que $p$ divise $\Phi_n(a)$. Alors il existe $k$ entier relatif tel que $m/n = p^k$. De plus, $PGCD(\Phi_m(a), \Phi_n(a))$ est une puissance de $p$.

• Si $p$ est premier, $n \geq 1$ et $a$ un entier relatif, alors : Si $p|\Phi_n(a)$ alors $p \equiv 1 \pmod{n}$ ou $p|n$. Si $n = p^\alpha N$ avec $p$ premier avec $N$ et $p|\Phi_n(a)$ alors l'ordre de $a$ modulo $p$ vaut $N$. Si $p$ est premier avec $n$, alors $p|\Phi_n(a)$ ssi l'ordre de $a$ modulo $p$ vaut $n$.

Exercices

## 2.1 Exercice 1

Soit $p$ un nombre premier. Montrer que $p^p1$ admet un diviseur premier congru à 1 modulo $p$.

## 2.2 Exercice 2

Soient $n, b > 2$ des entiers. Montrer que si $(b^n1)/(b1)$ est une puissance d'un nombre premier, alors $n$ est une puissance d'un nombre premier.

## 2.3 Exercice 3

Soit $n > 1$ un entier. Prouver que $2^{2n} + 2^{2n1} + 1$ est divisible par au moins $n$ nombres premiers différents. Quel est le plus petit entier $n > 1$ tel que $2^{2n} + 2^{2n1} + 1$ est divisible par au moins $n + 1$ nombres premiers différents ?

## 2.4 Exercice 4

Soit $n > 1$ un entier et soient $p_1, ..., p_n$ des nombres premiers impairs distincts. Montrer que $2^{p_1p_2p_n} + 1$ a au moins $2^{2n1}$ diviseurs.

## 2.5 Exercice 5

Soit $p$ un nombre premier et $d$ un diviseur de $p1$. Trouver le produit de tous les éléments de modulo $p$ dont l'ordre vaut $d$.

## 2.6 Exercice 6

Trouver tous les entiers relatifs $x, y$ tels que $(x^7 1)/(x1) = y^5 1$.

## 2.7 Exercice 7

Prouver qu'il existe une infinité d'entiers positifs $n$ tels que les diviseurs premiers de $n^2 + n + 1$ sont tous inférieurs ou égaux à $\sqrt{n}$.

## 2.8 Exercice 8

Soit $n > 2$. Il existe une infinité de nombres premiers $p$ tels que $p \equiv 1 \pmod{n}$.

## 2.9 Exercice 9 [Super dur]

Soit $p$ un nombre premier. Si $m > 1$ est un entier, on pose $|m|_p = p^k$ si $p^k | m$ et $p^{k+1}$ ne divise pas $m$.

(i) (Théorème de Feit) Soit $N > 1$ fixé. Alors pour tous les couples d'entiers $(a, n)$ avec $a > 1$ et $n > 2$, sauf éventuellement pour un nombre fini d'entre eux, il existe un diviseur premier primitif $p$ de $a^n 1$ tel que $|a^n 1|p > n^{N+1}$.

(ii) Si $m > 1$ est un entier, on note maintenant $[m]p$ le plus grand diviseur de $m$ qui n'est pas divisible par $p$. Montrer que si $p$ est un nombre premier et que si $a > 2$ est un entier, alors $[an1]p/n$ tend vers l'infini quand $n$ tend vers l'infini.