Travail d'étude et de recherche - M1 de Mathématiques
Calcul des polynômes cyclotomiques

Jean-Philippe MERX

2025

Utilitaires

Théorèmes and Co.
Vidéo explicative du calcul des polynômes cyclotomiques à la main.
Intéressant pour la fonction de Möbius.
Propriétés des polynômes cyclotomiques.
Self-reciproqual or palindromic polynomials.

Résultats variés

Neighboring ternary cyclotomic coefficients differ by at most one
Problème de préparation à l'agrégation sur les polynômes cyclotomiques. Où l'on prouve entre autre que les coefficients des polynômes cyclotomiques binaires sont dans $\{-1, 0, 1\}$.
Une synthèse concernant les coefficients de polynômes cyclotomiquesThéorème sion On the size of the coefficients of

Introduction

Rappeler l'article qui est étudié et ce qui est attendu.

Mathématiques des polynômes cyclotomiques

Définitions

Pour un entier $n \geq 1$, on désigne le polynôme

$$P_n(X) = X^n - 1 \in \mathbb{Q}[X]$$

et par U_n les racines de P_n, c'est à dire les racines $n^{\text{ème}}$ de l'unité. U_n est un sous-groupe du groupe $\mathbb{U}$ des complexes de module un. C'est un groupe cyclique fini. On peut le montrer en se souvenant qu'un groupe abélien fini G est somme directe de ses sous-groupes p-maximaux $G(p)$, c'est à dire de ses éléments qui sont une puissance de p. Ici, on peut montrer que $G(p) = \{x \in U_n \mid x^{m_p} = 1\}$ où m_p est l'ordre de $G(p)$ et donc que $G(p)$ est cyclique. On conclut sachant qu'un groupe abélien fini somme directe de groupes d'ordres premiers est cyclique.

On désigne dans la suite par $U_n^* \subseteq U_n$ les générateurs de U_n, c'est à dire les éléments dont l'ordre est premier avec n. Le $n^{\text{ème}}$ polynôme cyclotomique $\Phi_n \in \mathbb{Q}[X]$ est alors défini par :

$$\Phi_n(x) = \prod_{\zeta \in U_n^*} (X - \zeta) = \prod_{\substack{j=1 \\ \gcd(j,n)=1}}^{n} (X - e^{\frac{2\pi i}{n} j})$$

et le $n^{\text{ème}}$ polynôme cyclotomique inverse $\Psi_n \in \mathbb{Q}[X]$ par :

$$\Psi_n(x) = \prod_{\zeta \in U_n \setminus U_n^*} (X - \zeta) = \prod_{\substack{j=1 \\ \gcd(j,n)>1}}^{n} (X - e^{\frac{2\pi i}{n} j}) = \frac{X^n - 1}{\Phi_n(X)}.$$

En particulier : $\Phi_1(X) = X - 1$ et $\Psi_1(X) = 1$.

Propriétés utiles au calcul des polynômes cyclotomiques

On s'attache maintenant à décrire et démontrer des propriétés des polynômes Φ_n, Ψ_n qui vont permettre de les calculer efficacement.

Propriété 1
Pour $n \geq 1$ on a $P_n(X) = X^n - 1 = \prod_{d|n} \Phi_d(X)$.

En effet, U_n est la réunion des U_d^* pour $d \mid n$ et les U_d^* sont deux à deux disjoints.

Propriété 2
Les polynômes Φ_n sont à coefficients entiers et unitaires.

Si P, Q sont des polynômes à coefficients entiers, et que Q est unitaire, alors la division euclidienne de $P = AQ + R$ par Q conduit à des polynômes A, R appartenant à $\mathbb{Z}[X]$. De plus, A est unitaire si P, Q le sont. L'utilisation de la propriete 1 et une récurrence forte permet de conclure que Φ_n est un polynôme à coefficients entiers unitaire pour $n \geq 1$.

Propriété 3 (Irréductibilité des polynômes cyclotomiques)
Les polynômes $\Phi_n \in \mathbb{Z}[X]$ sont irréductibles.

On démontre cette propriété bien qu'elle ne soit pas utile pour les algorithmes utilisés ici pour leur calcul.

Soit ζ une racine primitive n-ième de l'unité, p un nombre premier avec n et $f, g \in \mathbb{Q}[X]$ les polynômes minimaux unitaires de ζ et ζ^p. Montrons que f, g sont à coefficients entiers. $\mathbb{Z}$ étant factoriel, $\mathbb{Z}[X]$ l'est également et $\Phi_n = f_1^{\alpha_1} \cdots f_r^{\alpha_r}$ où $f_1, \ldots, f_r \in \mathbb{Z}[X]$. Φ_n étant unitaire, on peut supposer que les f_i le sont aussi. ζ est racine de l'un des f_i, qui est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$. Par conséquent, f est l'un des f_i, g aussi puisque ζ^p est racine de Φ_n et f, g divisent Φ_n dans $\mathbb{Z}[X]$.

Montrons que $f = g$. Dans le cas contraire, comme f, g sont irréductibles, le produit $f \cdot g$ divise Φ_n dans $\mathbb{Z}[X]$. ζ^p étant racine de g, ζ est racine de $g(X^p)$ et $f(X)$ divise $g(X^p)$ dans $\mathbb{Q}[X]$, donc aussi dans $\mathbb{Z}[X]$ puisque f est unitaire. On écrit $g(X^p) = f(X)h(X)$ avec $h(x) \in \mathbb{Z}[X]$.

Projetons cette égalité dans $\mathbb{F}_p$. $g(X) = a_r X^r + \cdots + a_0$ avec $a_i \in \mathbb{Z}$. Par Frobenius :

$$\overline{g}(X^p) = (\overline{a_r} X^r + \cdots + \overline{a_0})^p = \overline{g}(X)^p = \overline{f}(X)\overline{h}(X).$$

Si $\varphi \in \mathbb{F}_p[X]$ est un facteur irréductible de $\overline{f}$, φ divise $\overline{g}$ et donc φ^2 divise $\overline{\Phi}_n$ dans $\mathbb{F}_p[X]$. Ce qui est absurde, puisque p ne divisant pas n et que $\overline{\Phi}'_n(X) = nX^{n-1} \neq 0$, $\overline{\Phi}_n$ ne peut pas avoir de racine double dans un corps de décomposition.

Maintenant, si ζ' est une racine n-ième de l'unité, on a $\zeta' = \zeta^m$ avec $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ où $p_i \nmid n$. Une récurrence permet de montrer que ζ' et ζ ont le même polynôme minimal. De sorte que f admet toutes les racines primitives de l'unité comme zéro. Comme $f \mid_n^{\Phi}$, et que ces deux polynômes sont unitaires, on obtient que $f = \Phi_n$ et donc que Φ_n est irréductible.

Notons que les polynômes cyclotomiques, ne sont pas toujours irréductibles sur les corps finis. Ainsi, sur $\mathbb{F}_2$:

$$\Phi_7(X) = (X^2 + X^2 + 1)(X^3 + X + 1).$$

Nous définissons maintenant la fonction de Möbius $\mu : \mathbb{N}^* \to \{-1, 0, 1\}\}$:

$$\mu(n) =: \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ a un facteur premier carré} \\ (-1)^r & \text{où r est le nombre de facteurs premiers de n} \end{cases}$$

Propriété 4 (Deux propriétés de la fonction de Möbius)

1. *μ est multiplicative : si m, n sont premiers entre eux : $\mu(mn) = \mu(m)\mu(n)$.*
2. *Si $n > 1$, $\sum_{d|n} \mu(d) = 0$.*

Si m ou n est égal à 1, la première propriété est évidente. Si m, n sont premiers entre eux, ils n'ont pas de facteur premier commun. Alors $\mu(mn) = \mu(m)\mu(n) = 0$ si m ou n a un facteur premier carré. Dans le cas contraire, le nombre de facteurs premiers de mn est la somme des nombres de facteurs premiers de m et n.

Concernant la seconde propriété, supposons que $n = \prod_{n=1}^{r} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où $\{p_1, \ldots p_r\}$ sont des premiers distincts et $\alpha_1, \ldots, \alpha_r$ des entiers supérieurs ou égaux à 1. Dans la somme $\sum_{d|n} \mu(d)$, seuls les diviseurs d de n sans facteur premier carré ont une contribution non nulle, ce qui conduit à l'égalité :

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{r} \sum_{\substack{S \subseteq \{p_1, \ldots, p_r\} \\ |S| = i}} (-1)^i = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = (1-1)^r = 0.$$

Nous fournissons à présent une autre définition des polynômes cyclotomiques utilisant la fonction de Möbius.

Propriété 5 (Définition équivalente des polynômes cyclotomiques)

$$\Phi_n(X) = \prod_{d|n}(X^d-1)^{\mu(\frac{n}{d})} = \prod_{d|n}(1-X^d)^{\mu(\frac{n}{d})} = \prod_{d|n}(1-X^{\frac{n}{d}})^{\mu(d)} \tag{2.4}$$

$$\Psi_n(X) = \prod_{d|n,d<n}(X^d-1)^{-\mu(\frac{n}{d})} = -\prod_{d|n,d<n}(1-X^d)^{-\mu(\frac{n}{d})} \tag{2.5}$$

La seconde formule est une conséquence immédiate de la première et de l'égalité $\Phi_n(X)\Psi_n(X) = X^n - 1$. Pour montrer la première, notons

$$F_n(X) = \prod_{d|n}(X^d-1)^{\mu(\frac{n}{d})} = \prod_{d|n}(X^{\frac{n}{d}}-1)^{\mu(d)}.$$

Il suffit de prouver que $\prod_{d|n} F_d(X) = X^n - 1$, puisque l'on obtient alors par récurrence $F_n(X) = \Phi_n(X)$ partant du constat que $F_1(X) = \Phi_1(X) = 1$. Nous avons :

$$\prod_{d|n} F_d(X) = \prod_{d|n}\prod_{d'|d}(X^{d'}-1)^{\mu(\frac{d}{d'})}$$

et allons montrer que pour d' divisant n fixé

$$\sum_{d\in S'_d}\mu\left(\frac{d}{d'}\right) = \begin{cases}1 & \text{si } d = n\\ 0 & \text{autrement}\end{cases}$$

où $S_{d'} = \{d; d' \mid d \text{ et } d \mid n\}$. Dans la somme ci-dessus, on peut changer d'indice de sommation en prenant $e = d/d'$ et effectuer la somme sur l'ensemble $\overline{S}_{d'} = \{e; e \mid \frac{n}{d'}\}$, c'est à dire l'ensemble des diviseurs de $\frac{n}{d'}$. D'où

$$\sum_{d\in S'_d}\mu\left(\frac{d}{d'}\right) = \sum_{e|\frac{n}{d'}}\mu(e)$$

et le résultat compte tenu de la seconde propriété ci-dessus de la fonction de Möbius.
Cette définition permettra le calcul des polynômes cyclotomiques en effectuant des multiplications et des divisions par des polynômes du type $X^d - 1$.
Les propriétés suivantes des polynômes cyclotomiques sont importantes pour les algorithmes de calcul. Elles permettent en effet d'une part de limiter les calculs principaux au cas où n est un produit de nombres premiers distincts, et pour ce dernier cas d'élaborer un algorithme récursif pour leur calcul : l'algorithme `SPS4` de l'article étudié.

Propriété 6
Soient p, q des entiers premiers tels que $p \nmid n$ et $q \mid n$. Alors :

$$\Phi_{np}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)} \tag{2.8a}$$

$$\Phi_{nq}(X) = \Phi_n(X^q) \tag{2.8b}$$

$$\Psi_{np}(X) = \Psi_n(X^p)\Phi_n(X) \tag{2.8c}$$

$$\Psi_{nq}(X) = \Psi_n(X^q) \tag{2.8d}$$

Remarquons tout d'abord que si m est un entier quelconque

$$\Phi_{nm}(X)\Psi_{nm}(X) = X^{nm} - 1 = (X^p)^m - 1 = \Phi_n(X^m)\Psi_n(X^m).$$

Si 2.8*a* est vraie on obtient

$$\Psi_{np}(X) = \frac{X^{np}-1}{\Phi_{np}(X)} = \frac{X^{np}-1}{\Phi_n(X^p)}\Phi_n(X) = \Psi_n(X^p)\Phi_n(X)$$

montrant 2.8*c*. De manière similaire, on déduit 2.8*d* de 2.8*b*.

Pour n entier, nous noterons dorénavant D_n l'ensemble des diviseurs de n sans facteurs carré. On peut réécrire 2.4

$$\Phi_n(X) = \prod_{d\in S_n}(1 - X^{\frac{n}{d}})^{\mu(d)}.$$

Si d est un diviseur de np sans facteur premier, ou bien d divise n, ou bien d est de la forme $d'p$. D'où l'égalité

$$\Phi_{np}(X) = \prod_{d\in S_n}(1 - X^{\frac{np}{d}})^{\mu(d)} \prod_{dp\in S_{np}}(1 - X^{\frac{np}{dp}})^{\mu(dp)}.$$

Le premier facteur est $\Phi_n(X^p)$. Observons que dans le second, dp étant sans facteurs carré, d est premier avec p et donc $\mu(dp) = \mu(d)\mu(p) = -\mu(d)$. Ce second facteur est simplement l'inverse de Φ_n : nous avons prouvé 2.8*a*.

Il nous reste à prouver 2.8*b*. Puisque q divise n, les diviseurs sans facteurs carré de nq sont ceux de n et

$$\Phi_{nq}(X) = \prod_{d\in S_n}(1 - X^{\frac{nq}{d}})^{\mu(d)} = \Phi_n(X^q),$$

qui est le résultat souhaité.

Portant notre attention sur le cas où 2 divise n, nous allons obtenir la propriété suivante :

Propriété 7
Pour $n > 1$:

$$\Phi_{2n}(X) = \begin{cases} \Phi_n(X^2) & \textit{si } n \textit{ est pair} \\ \Phi_n(-X) & \textit{sinon} \end{cases}$$

Le cas n pair est une application immédiate de 2.8*b*. Si n est impair, les polynômes $\Phi_{2n}(X)$ et $\Phi_n(-X)$ sont égaux puisqu'ayant les mêmes racines qui sont simples. Ce résultat nous permet de nous concentrer sur le calcul des polynômes cyclotomiques Φ_n avec n impair.

On déduit d'autre part des formules précédentes 2.8*b* et 2.8*d* pour le cas où $q \mid n$ que

Propriété 8 (Réduction aux cas des entiers sans facteurs carré)
Si $n = q_1^{e_1}\cdots q_k^{e_k}$ où $q_1, \ldots, q_k$ sont des premiers distincts :

$$\Phi_n(X) = \Phi_{q_1\cdots q_k}(X^{q_1^{e_1-1}\cdots q_k^{e_k-1}})$$
$$\Psi_n(X) = \Psi_{q_1\cdots q_k}(X^{q_1^{e_1-1}\cdots q_k^{e_k-1}})$$

Cette propriété et la précédente permettent de limiter le calcul des polynômes cyclotomiques au cas où n est un produit de nombres premiers impairs distincts.

Pour ce faire, supposons que $n = p_1 \cdots p_k$ soit le produit de k nombres premiers **impairs** distincts. Pour $1 \leq i \leq k$, notons $m_i = p_1 \cdots p_{i-1}$ et $e_i = p_{i+1} \cdots p_k$. En particulier $m_1 = e_k = 1$ et on note $e_0 = n$. Pour $1 \leq i \leq k$, nous avons alors $n = e_i p_i n_i$, ainsi que $e_{i-1} = p_i e_i$ et $m_{i+1} = m_i p_i$. À partir de la formule 2.8*a* et de l'identité $\Phi_{m_k}(X)\Psi_{m_k}(X) = X^{m_k} - 1$ on obtient

$$\Phi_n(X) = -\frac{\Psi_{m_k}(X^{e_k})}{1 - X^{n/p_k}} \Phi_{m_k}(X^{e_{k-1}}).$$

Sachant que $\Phi_1(X^{e_0}) = \Phi_1(X^n) = X^n - 1$ on montre alors par récurrence :

$$\Phi_n(X) = \prod_{j=1}^{k} -\Psi_{m_j}(X^{e_j}) \prod_{j=1}^{k} (1 - X^{n/p_j})^{-1}(1 - X^n)$$

ou encore

$$\Phi_n(X) = \prod_{j=2}^{k} -\Psi_{m_j}(X^{e_j}) \prod_{j=1}^{k} (1 - X^{n/p_j})^{-1}(1 - X^n)$$

puisque $\Psi_{m_1}(X^{e_1}) = \Psi_1(X^{e_1}) = 1$. L'utilisation de la formule 2.8*c* et une récurrence similaire permet d'écrire $\Psi_n(X)$ comme produit de polynômes cyclotomiques d'ordres inférieurs ; ce que l'on résume dans la propriété suivante :

Propriété 9 (Formules récursives de calcul des polynômes cyclotomiques)

$$\Phi_n(X) = \prod_{j=2}^{k} -\Psi_{m_j}(X^{e_j}) \prod_{j=1}^{k} (1 - X^{n/p_j})^{-1}(1 - X^n) \tag{3.17}$$

$$\Psi_n(X) = \prod_{j=1}^{k} \Phi_{m_j}(X^{e_j}) \tag{3.25}$$

On note dans la suite du document $\varphi(n)$ l'indicatrice d'Euler de n.

Propriété 10 (Palindromie des polynômes cyclotomiques)
Pour $n > 1$ impair, le polynôme $\Phi_n(X) = \sum_{i=0}^{\varphi(n)} a_i X^i$ est palindromique tandis que $\Psi_n(X) = \sum_{j=0}^{n-\varphi(n)} b_j X^j$ est anti-palindromique, ce qui signifie que

$$a_i = a_{\varphi(n)-i} \text{ et } b_j = -b_{n-\varphi(n)-j}.$$

Si ω est une racine primitive n-ième de l'unité, ω^{-1} aussi. n étant supposé impair, $\omega \neq \omega^{-1}$ et le produit des racines de Φ_n est égal à $1 = a_0$ puisque $\varphi(n)$ est pair pour $n > 2$. $X^{\varphi(n)}\Phi_n(\frac{1}{X})$ est un polynôme unitaire, dont les racines sont exactement celles de $\Phi_n(X)$, ce qui prouve que $\Phi_n(X)$ est palindromique.

De l'égalité $\Phi_n(X)\Psi_n(X) = X^n - 1$ il résulte d'une part que $\Psi_n(X)$ est unitaire et d'autre part que $b_0 = -1$. On remarque aussi que si ζ n'est pas une racine primitive n-ième de l'unité, alors ζ^{-1} non plus. $-X^{n-\varphi(n)}\Psi_n(\frac{1}{X})$ est donc un polynôme unitaire, comme $\Psi_n(X)$ et qui possède précisément les racines de $\Psi_n(X)$. Ces deux polynômes sont donc égaux, et nous concluons que $\Psi_n(X)$ est anti-palindromique.

Propriété 11 (Produit de polynômes palindromiques / anti-palindromiques)
Le produit de deux polynômes palindromiques ou anti-palindromiques est palindromique.
Le produit d'un polynôme palindromique par un polynôme anti-palindromique est anti-palindromique.

Démonstration claire à partir des définitions.

Calcul des polynômes cyclotomiques

Éléments clefs

- Utilisation de la formule d'inversion de Mobiüs.
- Et des polynômes cyclotomiques inverses.
- Formules (LEMME 1) liant les polynômes cyclotomiques et polynômes cyclotomiques inverses pour les produits d'un entier par une entier premier. Ces formules font appel à la division de polynômes.
- Pour la division de polynômes, il est possible d'utiliser un algorithme FFT. L'article décrit des calculs dans des corps de cardinal premier et reconstruction par le théorème des restes chinois. Il mentionne *"For even though the numerator is sparse, the denominator and quotient are typically dense."*
- Analyser les problèmes provenant de la taille des entiers manipulés. En particulier, `Python` utilise pour les entiers une arithmétique sans limite de taille. *Quelle est l'implication pour les performances ?*
- La formule 3.14 est importante, car elle permet de transformer une division par un polynôme cyclotomique en un produit par un polynôme cyclotomique inverse et une division par un polynôme de la forme $1 - z^m$.
- Et en utilisant des résultats de séries formelles, cela revient à effectuer une multiplication par une série $1 + z^m + z^{2m} + \ldots\ldots$ où il est nécessaire de contrôler le nombre de termes à conserver de la série.
- Les propriétés palindromiques des polynômes cyclotomiques permettent quant à elle de diviser par deux le nombre de coefficients à calculer. Le LEMME 4 étend ces propriétés aux produits de polynômes cyclotomiques (et de polynômes cyclotomiques inverses).
- Ces propriétés peuvent-être utilisées dans tous les calculs intermédiaires.
- Les formules 3.17 et 3.19 indiquent comment calculer les polynômes cyclotomiques (et cyclotomiques inverses) à partir des précédents.
- Pour de "très grands" polynômes cyclotomiques, on peut être amené à calculer "trop de termes" $\Longrightarrow$ voir remarque 3.22.
- *Analyser le dernier algorithme récursif !!!*

Algorithmes de l'article

Implémentation SAGE

SAGE implémente la méthode `cyclotomic_coeffs` ici. Lorsque la hauteur du polynôme à calculer dépasse :

```
cdef long fits_long_limit = 169828113 if sizeof(long) >= 8 else 10163195
```

SAGE bascule sur un algorithme (plus lent) basé sur PARI/GP en précision infinie.

Implémentation SymPy

De son côté, SymPy implémente la méthode dup_zz_cyclotomic_poly, à analyser. Il y a visiblement une arithmétique en précision infinie, basée sur gmpy2, *comment s'effectue le basculement ?*

Considérations sur la hauteur des polynômes cyclotomiques