Brève étude sur les polynômes cyclotomiques

Chabab Ayman

6 juin 2025

Table des matières

1 Introduction

Le présent document reprend les différentes notions que j'ai étudiées au cours de la préparation de l'épreuve du TIPE pour les ENS.

La première introduction des polynômes cyclotomiques en mathématiques remonte à Gauss en 1799 dans sa thèse de doctorat, avant d'avoir trouvé une application intéressante dans les travaux d'Evariste Galois au début du XIXème siècle. Les polynômes cyclotomiques constituent un outil très puissant en algèbre et notamment en théorie des nombres ainsi qu'en théorie des corps.

Définition 1. n-ième polynôme cyclotomique

Le n-ième polynôme cyclotomique est défini comme ceci :

$$\Phi_n(X) = \prod_{\substack{0 \leq k < n \\ k \wedge n = 1}} X - \omega_n^k$$

Avec pour tout $n \in \mathbb{N}^*$, $\omega_n = \exp\left(\frac{2i\pi}{n}\right)$

2 Résultats préliminaires

2.1 Propriétés fondamentales utiles

Définition 2. Fonction de Möbius

La fonction de Möbius $\mu : \mathbb{N} \to \{-1, 0, 1\}$ est définie pour tout entier naturel $n \geq 1$ par :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ est un produit de } k \text{ nombres premiers distincts}, \\ 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier.} \end{cases}$$

Proposition 1

Soit $n \in \mathbb{N}^*$:
0. $X^n - 1 = \prod_{d|n} \Phi_d$
1. $\Phi_n \in \mathbb{Z}[X]$
2. $\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$
3. $\deg(\Phi_n) = \phi(n)$

Démonstration.

1. **Première égalité**
   Avec $\zeta_n = e^{2i\pi/n}$
   On a $X^n - 1 = \prod_{k=0}^{n-1}(X - \zeta_n^k) = \prod_{d|n}\prod_{k\wedge n=d}(X - \zeta_n^k) = \prod_{d|n}\prod_{k'\wedge n=1, 1\leq k'\leq \frac{n}{d}}(X - \zeta_n^k) = \prod_{d|n}\Phi_{n/d} = \prod_{d|n}\Phi_d$
2. **Intégralité des coefficients de Φ_n**
   On raisonne par récurrence. Le cas $n = 1$ est évident. Soit $n > 1$ on a $X^n - 1 = \prod_{d|n}\Phi_d$, ainsi $\prod_{d|n\wedge d<n}\Phi_d$ divise $X^n - 1$ et comme il est de coefficient dominant inversible dans $\mathbb{Z}$ (1), alors $\Phi_n \in \mathbb{Z}[X]$ en temps que quotient de la division euclidienne.
3. **Formule de Möbius pour Φ_n**
   On a tout simplement en enchainant les égalités :

$$\prod_{d|n}(X^d - 1)^{\mu(n/d)} = \prod_{d|n}\prod_{d'|d}\Phi_{d'}^{\mu(n/d)} = \prod_{ld'|n}\Phi_{d'}^{\mu(n/ld')} = \prod_{d'|n}\Phi_{d'}^{\sum_{l|n/d'}\mu(l)} = \prod_{d'|n}\Phi_{d'}^{\delta_{1,d'}} = \Phi_n$$

4. **Degré de Φ_n**
   En utilisant juste la Définition 1 et la définition de ϕ cela est direct.

□

2.2 Irréductibilité dans $\mathbb{Z}[X]$

Théorème 1. Irréductibilité des polynômes cyclotomiques

Pour tout entier $n \geq 1$, le polynôme cyclotomique $\Phi_n(X)$ est irréductible dans $\mathbb{Z}[X]$.

La démonstration est disponible dans l'annexe 1.

3 Dirichlet Faible

3.1 Dirichlet "fort"

Voici le théorème de Dirichlet qui est un cas général des cas que nous allons traiter dans la suite.

Théorème 2. Théorème de Dirichlet

Pour tout entier n non nul et tout entier m premier avec n, il existe une infinité de nombres premiers congrus à m modulo n.

3.2 Le cas 1 modulo n

Proposition 2

Soit $\mathbb{K}$ un corps tel que $n \cdot 1 \neq 0$ alors $X^n - 1$ n'a pas de racine double dans $\mathbb{K}$.

Démonstration. 0 n'est clairement pas une racine du polynôme. De plus le polynôme dérivée est nX^{n-1}, qui s'annule uniquement en 0 avec la supposition sur $n \cdot 1 \neq 0$. Ainsi, aucune racine double dans $\mathbb{K}$. □

Corolaire 1

Soit $x \in \mathbb{K}$ non nul,
x est d'ordre n si et seulement si $\Phi_n(x) = 0$

Démonstration. Le sens réciproque est évident car Φ_n divise $X^n - 1$.
Quant au sens direct, soit x d'ordre n, alors x est racine d'un unique Φ_d pour un certain d qui divise n d'après la formule de la Proposition 1.1 et l'unicité vient de la Proposition 2. Cependant on a donc $X^d - 1$ qui annule x, donc $d \geq n$, ainsi on a $d = n$ et $\Phi_n(x) = 0$. □

Proposition 3

Soit $P \in \mathbb{Z}[X]$ non constant, l'ensemble des nombres premiers divisant l'un des entiers $P(n)$ pour $n \in \mathbb{Z}$ est infini.

Démonstration. Supposons par l'absurde qu'il existe $p_1, ..., p_k$ un nombre fini de nombres premiers qui divisent à eux seuls les $P(n)$.
Quitte à considérer $-P$ on peut supposer que $cdom(P) > 0$ et donc $\lim_{x->\infty} P(x) = +\infty$.
On peut aussi considérer P strictement croissant, car $P(n+1) - P(n) \longrightarrow_{n->\infty} +\infty$ (P non constant) : quitte à considérer $P(X + a)$ avec a constant dans $\mathbb{N}$.
On peut aussi dernièrement considérer P positif de la même manière car il est positif à partir d'un certain rang.

Soit $M > 0$ on va associer à M le nombre $f(M)$ correspondant à $Card(\{(a_1, ..., a_k) \in \mathbb{N}^k$ tel que $p_1^{a_1} ... p_k^{a_k} \leq M\})$.

En posant $C = \max_{1 \leq i \leq k} \frac{1}{\ln p_i}$, on a une majoration grossière de f correspondant à

$$f(M) \leq C \cdot \ln(M)^k$$

.

Ainsi, on a par stricte croissance de P une inégalité de la forme

$$P(\lceil C \cdot \ln(M)^k \rceil) >= M$$

Or, on a $P(\lceil C \cdot \ln(M)^k \rceil) \underset{M->\infty}{\sim} C \cdot \ln(M)^{k \cdot deg(P)} = o(M)$ ce qui est absurde étant donné la comparaison qu'on en a fait. Ainsi par l'absurde, le résultat est démontré.

□

Théorème 3. Dirichlet faible : cas 1 modulo n

Soit $n \geq 1$ un entier. Il existe une infinité de nombres premiers $p \equiv 1 \pmod{n}$

Démonstration. On dispose d'une infinité de nombres premiers divisant les $\Phi_n(k)$ par la Proposition 3.
Soit p divisant $\Phi_n(x)$ pour $x \in \mathbb{N}$.
En se plaçant dans $\mathbb{F}_p$ on a donc $\Phi_n(\overline{x}) = \overline{0}$ donc par le Corolaire 1 on a que $\overline{x}$ est d'ordre n, car $\overline{x} \neq \overline{0}$ car $\Phi_n(0) = \pm 1$. Or par théorème de Fermat, on a que $\overline{x}^{p-1} = 1$ donc n divise $p - 1$ et $p \equiv 1 \pmod{n}$.
On a donc démontré le théorème.

□

3.3 Le cas -1 modulo n

Les démonstrations de cette parties sont fastidieuses, nous allons toutes les mettre en annexe 3.

Proposition 4

Soit $n \geq 3$, il existe $\Psi_n \in \mathbb{Z}[X]$ de degré $\frac{\phi(n)}{2}$ tel que

$$\Psi_n(X + \frac{1}{X}) = \frac{\Phi_n(X)}{X^{\frac{\phi(n)}{2}}}$$

Lemme 1

Soit $n \geq 3$. On note $\overline{\Psi_n}$ l'image dans $\mathbb{F}_p[X]$ de Ψ_n. On suppose que $n \wedge p = 1$. On note $\mathbb{K}$ une clotûre algébrique de $\mathbb{F}_p[X]$.
1. Soit $\omega \in \mathbb{K}^*$ et $\xi = \omega + \frac{1}{\omega}$. Alors $\xi^p = \xi$ si et seulement si $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$.
2. Soit $\xi \in Rac(\overline{\Psi}_n)$. On a $\xi \in \mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \pmod{n}$

Théorème 4. Dirichlet faible : cas -1 modulo n

Soit $n \geq 1$ un entier. Il existe une infinité de nombres premiers $p \equiv -1 \pmod{n}$

4 Borne sur les coefficients des polynômes cyclotomiques

Assez naturellement, on peut commencer à calculer les polynômes cyclotomiques un par un, afin de les admirer !
Ainsi pour faire des petites expériences, nous allons nous engager dans le code d'une fonction qui calcule Φ_n.

4.1 Fonction OCaml pour calculer Φ_n

Nous savons déjà que les polynômes cyclotomiques ont à coefficients dans $\mathbb{Z}$. Ainsi nous pouvons coder les polynômes sous forme de liste.

```
type poly = int list
```

FIGURE 1 – Définition du type

Nous allons aussi avoir besoin d'opérations de base sur les polynômes : Afin de pouvoir tronquer les coefficients dominants égaux à 0, additionner deux polynômes, soustraire, multiplier et avoir le degré. Le code pour ces fonctions est donné en annexe.

Il nous faudra aussi savoir diviser dans le cas où la fonction de Möbius renvoie -1, donc on code aussi cela en annexe.

Pour calculer le n-ième polynôme cyclotomique, nous allons utiliser la formule suivante :

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

Cette formule est naturelle à utiliser plutôt que celle de la définition. En effet, celle-ci nous demande un effort moindre informatiquement car nous n'avons pas besoin de coder de représentations de certains nombres complexes, et encore moins de réels ! (ce qui ne serait pas possible de toute manière.)
Cependant, en contrepartie, nous allons devoir coder de quoi calculer la fonction de Möbius, le code est aussi donné en annexe.
Puis enfin on a plus qu'à calculer le n-ième polynôme cyclotomique avec la formule.

```
let cyclotomic n =
  let pos_factors, neg_factors =
    List.fold_left (fun (pos, neg) d ->
      let mu = mobius (n / d) in
      let f = x_pow_d_minus_1 d in
      if mu = 1 then (f :: pos, neg)
      else if mu = -1 then (pos, f :: neg)
      else (pos, neg)
    ) ([], []) (divisors n)
  in
  let num = List.fold_left mul [1] pos_factors in
  let den = List.fold_left mul [1] neg_factors in
  div_exact num den
```

Ensuite, à l'aide d'une fonction d'affichage on peut commencer à calculer quelques polynômes cyclotomiques pour s'amuser...

```
Phi_2(x) = 1 + x
Phi_3(x) = 1 + x + x^2
Phi_4(x) = 1 + x^2
Phi_5(x) = 1 + x + x^2 + x^3 + x^4
Phi_6(x) = 1 - x + x^2
Phi_7(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6
Phi_8(x) = 1 + x^4
Phi_9(x) = 1 + x^3 + x^6
Phi_10(x) = 1 - x + x^2 - x^3 + x^4
```

FIGURE 2 – Les polynômes cyclotomiques du 2 au 20

En observant les coefficients, on serait tenté de conjecturer que les coefficients sont bornés par 1. Et si on continue comme cela, on pourrait avoir cette impression encore longtemps jusqu'à ce qu'il se passe une certaine singularité (Figure 7).

```
Phi_103(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 +
Phi_104(x) = 1 - x^4 + x^8 - x^12 + x^16 - x^20 + x
Phi_105(x) = 1 + x + x^2 - x^5 - x^6 - 2x^7 - x^8 -
```

FIGURE 3 – Surprise

Ainsi on pourrait se demander si il y a vraiment une borne pour les coefficients des polynômes cyclotomiques ? La réponse est en fait... non, prouvons-le !

4.2 Non-bornitude des coefficients des polynômes cyclotomiques

Définition 3. Fonction π

Soit $x \in \mathbb{R}^+$, on a $\pi(x) = |\{p \text{ premier tel que } p \leq x\}|$

Nous allons tout d'abord avoir besoin d'un encadrement utile :

Théorème 5. Théorème des nombres premiers

$$\pi(x) \underset{x->\infty}{\sim} \frac{x}{\ln(x)}$$

Nous montrons cette inégalité dans l'Annexe 2.
Soit $t \in \mathbb{N}$ et $t \geq 3$ impair.

Lemme 2

On dispose de $2 < p_1 < p_2 < ... < p_t$ premiers tels que $p_1 + p_2 > p_t$

Théorème 6. Coefficients non-bornés des Φ_n

Il existe des polynômes cyclotomiques avec des valeurs absolues de coefficients arbitrairement grandes.

Démonstration. Soit $n = p_1 p_2 ... p_t$ tels que fixés plus haut.
Montrons que le coefficient devant X^{p_t} de $\Phi_n(X)$ est $1-t$. Pour ce faire, nous allons regarder Φ_n modulo X^{p_t+1} :

$$\Phi_n(X) \equiv [\prod_{i=1}^{t}(1-x^{p_i})]/(1-x) \equiv (1+x+...+x^{p_t-1})(1-x^{p_1})(1-x^{p_2})...(1-x^{p_{t-1}})$$

$$\equiv (1+x+...+x^{p_t-1})(1-x^{p_1}-...-x^{p_{t-1}}) \pmod{x^{p_t+1}}$$

Ainsi le coefficient devant x^{p_t} est $1-t$. Etant donné qu'on aurait pu prendre t aussi grand qu'on veut, c'est gagné.

□

5 Annexe 1 : Irréductibilité de Φ_n dans $\mathbb{Z}[X]$

On cherche à démontrer que Φ_n est irréductible dans $\mathbb{Z}[X]$, et donc dans $\mathbb{Q}[X]$. Premièrement, on sait que pour tout $n \in \mathbb{N}$, Φ_n est unitaire et à valeurs dans $\mathbb{Z}[X]$. Soit maintenant p premier et premier avec n. Pour ζ une racine primitive n-ième de l'unité, et soit $\omega = \zeta^p$, qui est aussi une racine primitive n-ième de l'unité. On note respectivement $\prod_\zeta$ et $\prod_\omega$ leurs polynômes minimaux. On a que $\omega^n = (\zeta^p)^n = 1$, de sorte que, par définition, $\prod_\zeta$ et $\prod_\omega$ divisent $X^n - 1$. On décompose alors $X^n - 1$ en produit de facteurs premiers. On a $X^n - 1 = P_1 P_2 \dots P_k$, où chaque P_i est unitaire et irréductible dans $\mathbb{Z}[X]$, donc irréductible par Gauss dans $\mathbb{Q}[X]$.

Ainsi, on obtient que $\prod_\zeta$ et $\prod_\omega$ figurent parmi les P_i et sont dans $\mathbb{Z}[X]$. Supposons $\prod_\zeta \neq \prod_\omega$. Puisqu'ils sont premiers entre eux (irréductibles distincts), on obtient que le produit $\prod_\zeta \prod_\omega$ divise $X^n - 1$. Soit $H = \prod_\omega(X^p)$. On sait que $H(\zeta) = 0$, donc $\prod_\zeta$ divise H dans $\mathbb{Q}[X]$, mais aussi dans $\mathbb{Z}[X]$ car $\prod_\zeta$ est unitaire. En réduisant modulo p, on trouve $\overline{H} = (\overline{\prod_\omega(X)})^p$ d'après le morphisme de Frobenius, donc tout facteur irréductible φ de $\overline{\prod_\zeta}$ dans $\mathbb{F}_p[X]$ apparaît dans $\overline{H}$ donc dans $\overline{\prod_\omega}$, donc φ^2 divise $X^n - \overline{1}$. Or, $X^n - \overline{1}$ est premier avec $\overline{n}X^{n-1}$ puisque $\overline{n} \neq 0$ dans $\mathbb{F}_p[X]$, donc n'admet pas de facteurs carrés, absurde. On a ainsi montré que $\prod_\zeta = \prod_\omega$.
On obtient ainsi que pour tout p premier avec n, ζ^p est aussi racine de $\prod_\zeta$, et par récurrence immédiate il en est de même pour les $\zeta^{p_1^{a_1}...p_j^{a_j}}$ avec p_i ne divisant pas n. De là on en tire que $\prod_\zeta$ admet toutes les racines primitives n-ième comme racines, et donc que $deg(\prod \zeta) \geq deg(\Phi_n)$, donc on trouve que $\prod_\zeta = \Phi_n$. Comme Φ_n est donc le polynôme minimal des racines primitives n-ièmes de l'unité, il est irréductible.

6 Annexe 2 : Démonstrations du cas -1 de Dirichlet faible

6.1 Proposition 4

Démonstration. 4.1 - On montre premièrement que $\phi(n)$ est pair pour tout $n \geq 3$. En effet, pour un tel n donné, et pour $k \leq n$, on a que $k \wedge n = 1 \iff (n-k) \wedge n = 1$. De plus, $\frac{n}{2} \wedge n \neq 1$ puisque n'importe quel facteur premier divisant $\frac{n}{2}$ divise aussi n, de sorte que $k \wedge n = 1 \Rightarrow k \neq n-k$, de sorte qu'on peut former des paires $\{k, n-k\}$, et finalement $\phi(n)$ est pair.

4.2 - Soit $k \in \mathbb{N}$, et $(a_0, \ldots, a_k) \in \mathbb{Z}^{k+1}$. Il existe $Q \in \mathbb{Z}[X]$ tel que $a_0 + \sum_{i=1}^{k} a_l \left(X^l + \frac{1}{X^k}\right) = Q\left(X + \frac{1}{X}\right)$, et pour $a_k \neq 0, \deg(Q) = k$. En effet, on procède par récurrence sur k :

- Pour $k = 0$, $Q = a_0$ convient.
- Soit $k \in \mathbb{N}$. On suppose que la proposition est vérifiée au rang k, et soit alors $(a_0, \ldots, a_{k+1}) \in \mathbb{Z}^{k+2}$. Par la formule du binôme de Newton, on écrit $\left(X + \frac{1}{X}\right)^{k+1} = \sum_{l=0}^{k+1} b_l \left(X^l + \frac{1}{X^l}\right)$, où $b_{k+1} = 1$. On obtient alors par addition $a_0 + \sum_{i=1}^{k} a_l \left(X^l + \frac{1}{X^k}\right) - a_{k+1}\left(X + \frac{1}{X}\right)^{k+1} = a_0 - a_{k+1}b_0 + \sum_{l=1}^{k}(a_l - a_{k+1}b_l)\left(X^l + \frac{1}{X^l}\right)$, et donc par hypothèse de récurrence, il existe $Q_1 \in \mathbb{Z}[X]$ tel que $a_0 + \sum_{i=1}^{k} a_l \left(X^l + \frac{1}{X^k}\right) - a_{k+1}\left(X + \frac{1}{X}\right)^{k+1} = Q_1\left(X + \frac{1}{X}\right)$, de sorte que, pour $Q = Q_1 + a_{k+1}X^{k+1}$, il vient que $a_0 + \sum_{l=1}^{k+1} a_l \left(X^l + \frac{1}{X^l}\right) = Q\left(X + \frac{1}{X}\right)$, avec $\deg(Q) = k+1$ pour $a_{k+1} \neq 0$.
- Par principe de récurrence, la proposition est donc vraie pour tout $k \in \mathbb{N}$.

4.3 - Pour $P \in \mathbb{Z}[X]$ de degré $2k$ tel que $X^{2k}P\left(\frac{1}{X}\right) = P(X)$, il existe $Q \in \mathbb{Z}[X]$ de degré k tel que $X^k Q\left(X + \frac{1}{X}\right) = P(X)$. En effet, soit un tel P. L'hypothèse sur P nous permet d'écrire $P = \sum_{l=0}^{2k} a_l X^l = \sum_{l=0}^{2k} a_{2k-l} X^l$, de sorte que, par unicité de l'écriture polynomiale, on trouve que pour tout $l \in \{0, \ldots, 2k\}, a_{2k-l} = a_l$. On se ramène alors au point 4.2 en écrivant $\frac{1}{X^k}P(X) = a_k + \sum_{l=1}^{k} a_{k-l}\left(X^l + \frac{1}{X^l}\right)$. Il existe donc $Q \in \mathbb{Z}[X]$ tel que $\frac{1}{X^k}P(X) = Q\left(X + \frac{1}{X}\right)$, de degré k (car $a_{2k} \neq 0$).

4.4 - Soit Φ_n notre n-ième polynôme cyclotomique. On a $X^{\phi(n)}\Phi_n\left(\frac{1}{X}\right) = X^{\phi(n)} \prod_{k \in \mathbb{P}(n)} \left(\frac{1}{X} - \omega_{n,k}\right) = \prod_{k \in \mathbb{P}(n)} (1 - \omega_{n,k}X) = (-1)^{\phi(n)} \prod_{k \in \mathbb{P}(n)} \omega_{n,k} \prod_{k \in \mathbb{P}(n)} (X - \omega_{n,n-k})$. Or, $k \to n-k$ est une bijection de $\mathbb{P}(n)$ dans lui-même, donc les $\omega_{n,k}$ peuvent être associés deux à deux et leur produit vaut 1. De plus, $\phi(n)$ étant pair dans notre étude, $(-1)^{\phi(n)} = 1$, et finalement $X^{\phi(n)}\Phi_n\left(\frac{1}{X}\right) = \Phi_n(X)$. D'après 4-2, il existe alors $\Psi_n \in \mathbb{Z}[X]$ de degré $\frac{\phi(n)}{2}$ tel que $\Psi_n\left(X + \frac{1}{X}\right) = \frac{\Phi_n(X)}{X^{\frac{\phi(n)}{2}}}$

□

6.2 Lemme 1

Démonstration. 1.1 - Soit $\omega \in \mathbb{K}^*$. On pose $\xi = \omega + \frac{1}{\omega}$. Supposons $\xi^p = \xi$. On obtient alors $(\omega + \frac{1}{\omega})^p = \omega + \frac{1}{\omega}$. Or $(\omega + \frac{1}{\omega})^p = \omega + \frac{1}{\omega} \iff \omega^p + \frac{1}{\omega}^p = \omega + \frac{1}{\omega} \iff \omega^{2p} + 1 - \omega^{p+1} - \omega^{p-1} = 0 \iff \omega^{p+1}(\omega^{p-1} - 1) - \omega^{p-1} - 1 = 0 \iff (\omega^{p-1} - 1)(\omega^{p+1} - 1) = 0 \iff \omega^{p-1} = 1 \text{ou} \omega^{p+1} = 1 \iff \omega^p = \omega^{\pm 1}$

1.2 - Soit $\xi \in Rac(\overline{\Psi_n})$. Supposons $\xi \in \mathbb{F}_p$. On sait que $a \in \mathbb{F}_p$ si et seulement si $a^p - a = 0$. En effet, ce polynôme admet au maximum p racines. Or, par le petit théorème de Fermat, tout élément de

$\mathbb{F}_p$ est racine de ce polynôme, ce qui conclut notre argument. Or, $\xi \in Rac(\overline{\Psi_n}) \iff \overline{\Psi_n}(\xi) = 0 \iff \overline{\Psi_n}(\omega + \frac{1}{\omega}) = 0 \iff \frac{\overline{\Phi_n(\omega)}}{\omega^{\frac{\phi(n)}{2}}} = 0 \iff \omega \in Rac(\overline{\Phi_n})$. Or, puisque $k \wedge n = 1$, on obtient que $ord_{\mathbb{F}_p}(\omega) = n$. On a donc que $ord_{\mathbb{F}_p}(\omega)$ divise $p-1$ ou $p+1$, c'est-à-dire $p \equiv \pm 1 (\text{mod } n)$ □

6.3 Théorème de Dirichlet faible

Démonstration. Soit $n \geq 3, n \neq 4$. Supposons par l'absurde qu'il existe un nombre fini $p_1, \dots, p_k$ de nombres premiers congrus à -1 modulo n. Soit $\Theta_n(X) = \frac{1}{a}\Psi_n(aX)$, avec $a = \Psi_n(0)$, et soit $p_0 \equiv 1 (\text{mod } np_1 \dots p_k)$.

4.1 - Il s'agit premièrement de montrer que $a \neq 0$. En effet, $a = 0 \iff \Psi_n(0) = 0$. Or, $0 \in Rac(\Psi_n) \iff 0 = z + \frac{1}{z}$ avec z une racine de Φ_n. Mais $z + \frac{1}{z} = 0 \iff z^2 = -1 \iff z = \pm i$, cas qu'on a écarté au préalable en retirant $n = 4$ de l'étude. On en déduit alors que $\Theta_n = 1 + \sum_{k=1}^{d} a_k a^{k-1} X^k$ est bien à coefficients entiers.

4.2 - Montrons alors que les racines de Θ_n sont réelles et simples.
On sait que les racines de Φ_n sont les $\omega_{n,k}$, donc les racines de Ψ_n sont les $\omega_{n,k} + \frac{1}{\omega_{n,k}} = 2\cos(\frac{2k\pi}{n})$. Pour les $\phi(n)$ possibilités de $\omega_{n,k}$, chaque racine est représentée exactement deux fois en appariant les termes k et $n-k$, ce qui fournit $\frac{\phi(n)}{2}$ racines, donc d'après le degré de Ψ_n, on a trouvé toutes les racines. Les racines de Θ_n s'en déduisent alors immédiatement, et elles sont bien simples et réelles puis que $\deg(\Theta_n) = \deg(\Psi_n)$.

4.3 - On peut alors utiliser le théorème des valeurs intermédiaires pour montrer l'existence d'un intervalle $[a, b]$ sur lequel Θ_n est strictement négative, puisqu'elle change de signe entre ses racines. Comme $\frac{\phi(n)}{2} > 0$, cela est assuré d'arriver au moins une fois.

4.4 - On obtient alors l'existence d'un entier $m \in \mathbb{Z}$ et $l \in \mathbb{N}$ tels que $\Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k) < 0$. En effet, on a

$$\lim_{l \to \infty} \frac{m}{p_0^l} \times np_1 \dots p_k = 0$$

, donc il existe l tel que $0 < \frac{m}{p_0^l} \times np_1 \dots p_k < b - a$, alors d'après la propriété d'Archimède il existe m tel que $\frac{m}{p_0^l} \times np_1 \dots p_k \in [a, b]$, c'est-à-dire tel que $\Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k) < 0$.

4.5 - On explicite alors Θ_n : $\Theta_n = \sum_{j=0}^{\frac{\phi(n)}{2}} b_j X^j$. On a alors $p_0^{\frac{\phi(n)l}{2}} \Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k) = \sum_{j=0}^{\frac{\phi(n)}{2}} b_j (mnp_1 \dots p_k)^j p_0^{l(\frac{\phi(n)}{2} - j)} \in \mathbb{Z}$. De plus, pour tout $j > 0$ entier, $b_j (mnp_1 \dots p_k)^j p_0^{l(\frac{\phi(n)}{2} - j)} \equiv 0 (\text{mod } np_1 \dots p_k)$, de sorte que $p_0^{\frac{\phi(n)l}{2}} \Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k) \equiv p_0^{\frac{\phi(n)}{2} l} b_0 (\text{mod } np_1 \dots p_k)$. Or, par notre définition de Θ_n, il vient $b_0 = 1$ et clairement $p_0 \equiv 1 (\text{mod } np_1 \dots p_k)$, de sorte que, finalement, $p_0^{\frac{\phi(n)l}{2}} \Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k) \equiv 1 (\text{mod } np_1 \dots p_k)$.

4.6 - Soit p un diviseur premier de $p_0^{\frac{\phi(n)l}{2}} \Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k)$, distinct de p_0. Premièrement, la relation trouvée précédemment assure que $p_0^{\frac{\phi(n)l}{2}} \Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k) \wedge np_1 \dots p_k = 1$, de sorte que p est distinct de tous les p_i, et $n \wedge p = 1$. On observe alors qu'en passant dans $\mathbb{F}_p$, on arrive à $\sum_{j=0}^{\frac{\phi(n)}{2}} b_j (mnp_1 \dots p_k)^j p_0^{l(\frac{\phi(n)}{2} - j)} \equiv 0 (\text{mod } p)$. Or, notre terme en p_0 est inversible modulo p. On note q_0 son inverse, et on obtient alors $\sum_{j=0}^{\frac{\phi(n)}{2}} b_j (mnp_1 \dots p_k)^j q_0^{lj} \equiv 0 (\text{mod } p)$, soit $\overline{\Psi_n}(q_0^{lj} mnp_1 \dots p_k) = 0$. On a donc trouvé une racine non-triviale de $\overline{\Psi_n}$ dans $\mathbb{F}_p$, et puisque $n \wedge p = 1$, on en déduit $p \equiv \pm 1 (\text{mod } n)$. Or, p étant distinct des p_i, on élimine immédiatement $p \equiv -1 (\text{mod } n)$ et finalement $p \equiv 1 (\text{mod } n)$.
Tous les diviseurs premiers de $p_0^{\frac{\phi(n)l}{2}} \Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k)$ vérifient $p \equiv 1 (\text{mod } n)$, donc $|p_0^{\frac{\phi(n)l}{2}} \Theta_n(\frac{m}{p_0^l} \times$

$np_1 \dots p_k)| \equiv 1 (\text{mod } n)$. Mais comme on a démontré que $p_0^{\frac{\phi(n)l}{2}} \Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k) < 0$, on en déduit immédiatement $p_0^{\frac{\phi(n)l}{2}} \Theta_n(\frac{m}{p_0^l} \times np_1 \dots p_k) \equiv -1 (\text{mod } n)$, ce qui, comme on l'a vu précédemment, est absurde. Il y a donc une infinité de nombres premiers p tels que $p \equiv -1 (\text{mod } n)$ □

7 Annexe 3 : Code

Code OCaml

Voici le code des opérations de base sur les polynômes, telles que additionner, soustraire, multiplier, simplifier et avoir le degré.

```
let trim p =
  let rec aux = function
    | [] -> []
    | 0 :: xs -> aux xs
    | l -> l
  in
  match List.rev p with
    | [] -> [0]
    | r -> List.rev (aux r)

let add p q =
  let rec aux p q = match p, q with
    | [], r | r, [] -> r
    | x::xs, y::ys -> (x + y) :: aux xs ys
  in trim (aux p q)

let sub p q =
  let rec aux p q = match p, q with
    | [], [] -> []
    | x::xs, [] -> x :: aux xs []
    | [], y::ys -> (-y) :: aux [] ys
    | x::xs, y::ys -> (x - y) :: aux xs ys
  in trim (aux p q)

let mul p q =
  let res = Array.make (List.length p + List.length q - 1) 0 in
  List.iteri (fun i a ->
    List.iteri (fun j b ->
      res.(i + j) <- res.(i + j) + a * b
    ) q
  ) p;
  trim (Array.to_list res)

let degree p = List.length p - 1
```

Le code pour la division de polynôme, on en profite pour introduire une fonction auxiliaire qui permet d'avoir un objet représentant $X^d - 1$ pour tout $d \in \mathbb{N}$.

Division exacte et puissance de polynômes

```
let div_exact a b =
  let rec loop r q =
    if degree r < degree b then q
    else
      let lc_r = List.nth r (degree r) in
      let lc_b = List.nth b (degree b) in
      if lc_b = 0 then failwith "Division par polynme nul";
      if lc_r mod lc_b <> 0 then failwith "Division non exacte";
```

```
      let coeff = lc_r / lc_b in
      let shift = degree r - degree b in
      let monomial = List.init shift (fun _ -> 0) @ [coeff] in
      let prod = mul b monomial in
      let new_r = trim (sub r prod) in
      loop new_r (add q monomial)
  in
  let result = loop a [] in
  let remainder = trim (sub a (mul b result)) in
  if remainder <> [0] then failwith "Division inexacte"
  else trim result;;

let x_pow_d_minus_1 d =
  let x_d = List.init d (fun _ -> 0) @ [1] in
  sub x_d [1]
```

Voici évidemment la fonction Mobius dont on aura besoin pour le calcul :

```
let mobius n =
  (* teste si n est carr-libre *)
  let rec is_square_free n d =
    if d * d > n then true
    else if n mod (d * d) = 0 then false
    else is_square_free n (d + 1)
  in
  (* compte le nombre de facteurs premiers distincts de n *)
  let rec count_primes n d acc =
    if d * d > n then (* d dpasse n *)
      (if n > 1 then acc + 1 else acc)
    else if n mod d = 0 then (* d est un facteur premier *)
      let rec remove x =
        if x mod d = 0 then remove (x / d) else x
      in
      let n' = remove n in (* on enlve toutes les puissances de d *)
      count_primes n' (d + 1) (acc + 1)
    else
      count_primes n (d + 1) acc
  in
  (* dfinition de la fonction de Mbius *)
  if n = 1 then 1
  else if not (is_square_free n 2) then 0
  else
    let k = count_primes n 2 0 in
    if k mod 2 = 0 then 1 else -1
```

Et enfin une fonction diviseur qui nous servivra aussi :

```
let divisors n =
  let rec aux i acc =
    if i > n then List.rev acc
    else if n mod i = 0 then aux (i + 1) (i :: acc)
    else aux (i + 1) acc
  in aux 1 []
```

Le dernier code est directement dans le corps du rapport.
C'est ce même code qui a servi à calculer les résultats des Figures 2 et 3.

8 Bibliographie

Références

[1] E. Lehmer, *On the magnitude of the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **42** (1936), no. 6, 389–392.

[2] D. Perrein, *Cours d'Algèbre*, Ellipses, Paris, 2002.

[3] E. Caeiro, *An Introduction to Algebraic Number Theory through Olympiad Problems*, self-published manuscript, 2021.
https ://www.dropbox.com/sh/lribbpkfooq96gs/AABJsHF8MuGZCkP8J0FxslD7a ?dl=0

[4] G. Chenevier, *Algèbre : Cours de $1^{ère}$ année à l'École Normale Supérieure 2023/2024*, notes de cours, accessible sur le site personnel de l'auteur :
https ://gaetan.chenevier.perso.math.cnrs.fr