Problème – Polynômes cyclotomiques

Partie 1 : Calculs préliminaires

1) D'après le cours, $X^n-1=\prod_{1\leq k\leq n}(X-z_k)$. Puisque les polynômes de degré un sont irréductibles, il s'agit de la décomposition en produit d'irréductibles dans $\mathbb{C}[X]$.

2) C'est clair si $b=0$. Sinon,

$$\begin{aligned}\prod_{k=1}^{n}(a+bz_k) &= \prod_{k=1}^{n}b\left(\frac{a}{b}+z_k\right)=b^n\prod_{k=1}^{n}\left(\frac{a}{b}+z_k\right)\\ &= (-1)^n b^n\prod_{k=1}^{n}\left(\left(-\frac{a}{b}\right)-z_k\right)\end{aligned}$$

et on reconnait $(-b)^n(X^n-1)$ évalué en $-a/b$. Dans tous les cas,

$$\prod_{k=1}^{n}(a+bz_k)=a^n+(-1)^{n-1}b^n.$$

3)

$$\begin{aligned}\prod_{k=1}^{n}(z_k^2-2(\cos\theta)z_k+1) &= \prod_{k=1}^{n}\left[(z_k-e^{i\theta})(z_k-e^{-i\theta})\right]\\ &= \left(\prod_{k=1}^{n}(-(e^{i\theta}-z_k))\right)\left(\prod_{k=1}^{n}(-(e^{-i\theta}-z_k))\right)\\ &= (-1)^n(-1)^n((e^{i\theta})^n-1)((e^{-i\theta})^n-1)\\ &= (e^{in\theta}-1)(e^{-in\theta}-1)=1-e^{in\theta}-e^{-in\theta}+1\\ &= 2-2\cos n\theta=2(1-\cos n\theta)\end{aligned}$$

Partie 2 : L'indicatrice d'Euler

4) On applique l'agorithme d'Euclide étendu au couple (2018,1789). Les divisions euclidiennes successives sont :

$$\begin{aligned}2018 &= 1\times1789+229\\ 1789 &= 7\times229+186\\ 229 &= 1\times186+43\\ 186 &= 4\times43+14\\ 43 &= 3\times14+1\\ 14 &= 14\times1+0.\end{aligned}$$

Ceci permet d'écrire

$$\begin{pmatrix}0&1\\1&-3\end{pmatrix}\begin{pmatrix}0&1\\1&-4\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&-7\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}2018\\1789\end{pmatrix}=\begin{pmatrix}3\\1\end{pmatrix}.$$

En effectuant le produit des matrices 2×2, ceci se réécrit

$$\begin{pmatrix}*&*\\125&-141\end{pmatrix}\begin{pmatrix}2018\\1789\end{pmatrix}=\begin{pmatrix}3\\1\end{pmatrix}.$$

La dernière ligne donne la relation de Bézout $125\times2018-141\times1789=1$.
En particulier, $125\times2018\equiv1 \mod 1789$ et donc l'inverse de $\overline{2018}$ est $\overline{125}$ dans $\mathbb{F}_p$.

5) On a $p\binom{p-1}{k-1}=k\binom{p}{k}$. Comme p est premier avec k, p divise $\binom{p}{k}$ d'après le lemme de Gauss.

6) D'après le binôme de Newton, $(A+B)^p=\sum_{k=0}^{p}\binom{p}{k}A^kB^{p-k}$. Mais $\binom{p}{k}\equiv0 \mod p$ pour $1\leqslant k\leqslant p-1$. D'où $(A+B)^p=A^p+B^p$.

7) Par récurrence immédiate sur le nombre de termes dans la somme, $(A_1+A_2+\cdots+A_n)^p\equiv A_1^p+A_2^p+\cdots+A_n^p \mod p$ pour tous $A_1,..,A_n\in\mathbb{Z}[X]$. D'où

$$\left(\sum_k\overline{a_k}X^k\right)^p=\sum_k\overline{a_k}^pX^{kp}$$

et par le petit théorème de Fermat

$$\left(\sum_k\overline{a_k}X^k\right)^p=\sum_k\overline{a_k}X^{kp}.$$

Partie 3 : Racines primitives de l'unité

8) Montrons que $\exp i2k\pi/n$ est une racine primitive n^{e} si et seulement si $d=1$ où $d=pgcd(k,n)$.

— Si $d\geqslant2$. Alors $\exp i2k\pi/n=\exp i2k'\pi/n'$ où $k=dk'$ et $n=dn'$. Donc $n'<n$ et manifestement $\exp i2k\pi/n$ est une racine n'^{e} de l'unité, donc n'est pas une racine primitive de l'unité.

— Si $d=1$. Soit $u\in\mathbb{N}^*$ tel que $(\exp i2k\pi/n)^u=1$. Alors $ku/n\in\mathbb{Z}$. Donc n divise ku. Mais $pgcd(k,n)=1$, donc d'après le lemme de Gauss, n divise u. En particulier, $\exp i2k\pi/n$ n'est pas une racine u^{e} 1 pour $u<n$. Donc c'est une racine primitive n^{e} de l'unité.

9)

$n=1$	1
$n=2$	-1
$n=3$	j, j^2
$n=4$	$i, -i$
$n=5$	$e^{i2\pi/5}, e^{i4\pi/5}, e^{i6\pi/5}, e^{i8\pi/5}$
$n=6$	$e^{i\pi/3}, e^{-i\pi/3}$

10) On a

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

Le seul résultat qui ne s'obtient pas immédiatement est la forme de Φ_5. Plutôt que de développer la forme factorisée, on remarque que les racines de X^5-1 sont exactement les racines de Φ_5 auquelles on ajoute 1. Donc Φ_5 est le quotient de X^5-1 par $X-1$.

11) $\deg\Phi_n = \varphi(n)$ car $\mathrm{Card}\, Z_n = \varphi(n)$ par définition (cours).

12) Montrons que les les racines n^{e} sont exactement les racines primitive d^{e} de 1 pour un diviseur d de n. Déjà, si $d \geqslant 1$ divise n, alors toute racine primitive d^{e} de 1 est une racine d^{e} donc une racine n^{e} de 1. Réciproquement, si $z = \exp i2\pi k/n$ est une racine n^{e} de 1.

1re preuve Soit d le plus petit entier tel que $z^d = 1$. Montrons que $d = n/p$ où $p = pgcd(n,k)$. Or

$$z^d = \left(e^{i2\pi\frac{k}{n}}\right)^{\frac{n}{p}} = e^{i2\pi\frac{kn}{np}} = e^{i2\pi\frac{k}{p}} = 1$$

car p divise k donc k/p est un entier.

2e preuve L'idée sous-jacente est que le groupe des racines n^{e} de l'unité est isomorphe au groupe des entiers *modulo n*. Soit $\phi : \mathbb{Z} \to \mathbb{C}^*$ définie par $\phi(a) = e^{i2\pi ak/n}$. C'est un morphisme de groupe, donc son noyau est un sous-goupe de $\mathbb{Z}$, donc de la forme $d'\mathbb{Z}$ avec $d' \geqslant 0$. Comme manifestement n appartient au noyau, d' divise n donc d' est non-nul. Or d' est le plus petit entier strictement positif tel que $e^{i2\pi d'k/n} = 1$, donc $d' = d$.

13) En passant au degré dans l'égalité précédente,

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

14) On adapte la démonstration du cours. Montrons par récurrence sur $\deg A = n$ que pour tout $A, B \in \mathbb{Z}[X]$ avec B unitaire, le quotient Q et le reste R dans la division euclidienne de A par B sont à coefficients entiers.

Initialisation Si $n \leqslant 0$. Alors $A \in \mathbb{Z}$. Si B est constant, alors $B = 1$ car il est unitaire. Alors $R = 0 \in \mathbb{Z}[X]$ et $Q = A \in \mathbb{Z}[X]$. Si B est non constant, $Q = 0$ et $R = A$, gagné.

Hérédité Supposons la propriété vraie pour n et supposons $A \in \mathbb{Z}[X]$ de degré $n+1$. Si $\deg B > n+1$ alors $R = A$ et $Q = 0$, gagné. Si $\deg B \leqslant n+1$, on "pose la division". Si $B = \sum_{k=0}^{q} b_k X^k$, avec $\deg B = q$, alors $b_q = 1$. On a $A_0 := A - a_{n+1}X^{n+1-q}B \in \mathbb{Z}[X]$ où $a_{n+1} \in \mathbb{Z}$ est le coefficient dominant de A donc est non nul. On a donc $\deg A_0 \leqslant n$ car B est unitaire. Par hypothèse de récurrence, $A_0 = BQ_1 + R_1$ avec $Q_1, R_1 \in \mathbb{Z}[X]$ et $\deg R_1 < \deg B$. D'où

$$\begin{aligned} A = A_0 + a_{n+1}X^{n+1-q}B &= BQ_1 + R_1 + a_{n+1}X^{n+1-q}B \\ &= (a_{n+1}X^{n+1-q} + Q_1)B + R_1. \end{aligned}$$

Or $\deg R_1 < \deg B$ donc $R = R_1$ par unicité du reste. Donc $Q = a_{n+1}X^{n+1-q} + Q_1$. En particulier, R et Q appartiennent à $\mathbb{Z}[X]$.

15) Montrons par récurrence sur $n \geqslant 1$ que $\Phi_n \in \mathbb{Z}[X]$ est unitaire. C'est vrai pour $n \in [\![1,6]\!]$ d'après la question 10. Supposons la propriété vraie pour tout entier $\leqslant n-1$. Alors Φ_n est le quotient de X^n-1 par $\prod_{d|n, d<n}\Phi_d$ d'après la question 12. Or un produit de polynômes unitaires est unitaire. D'après la question précédente, Φ_n est donc un polynôme à coefficients entiers. Il est unitaire, car le coefficient dominant de X^n-1 est 1 et que le coefficient dominant de $\prod_{d|n}\Phi_d$ est celui de Φ_n.

Partie 4 : Irréductibilité sur $\mathbb{Q}$

16) Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ primitifs. Par l'absurde : si PQ n'est pas primitif. Soit p un diviseur premier de $c(PQ)$. Alors $PQ \equiv 0 \mod p$. Mais alors dans $\mathbb{F}_p[X]$, on a $\overline{P}\,\overline{Q} = \overline{0}$. Or $\mathbb{F}_p[X]$ est intègre. Donc $\overline{P}$ ou $\overline{Q} = 0$, *i.e.* p divise tous les coefficients de P ou Q, donc n'est pas primitif.

17) On écrit $PQ = c(P)c(Q)\frac{P}{c(P)}\frac{Q}{c(Q)}$. Or $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$ sont primitifs, donc $\frac{P}{c(P)}\frac{Q}{c(Q)}$ aussi d'après la question précédente. Donc le $pgcd$ des coefficients de PQ est $c(P)c(Q)$.

18) Soient $A_0, B_0 \in \mathbb{Q}[X]$ tels que $A_0B_0 = \frac{1}{c(P)}P$ et $\deg A_0, \deg B_0 \geqslant 1$. On peut trouver $a, b \in \mathbb{Z}$ non nuls tels que $aA_0 = A_1$ et $bB_0 = B_1$ avec $A_1, B_1 \in \mathbb{Z}[X]$ (prendre pour a

le produit ou le $ppcm$ des dénominateurs des coefficients de A_0). Soient $A_2 = \dfrac{A_1}{c(A_1)}$ et $B_2 = \dfrac{B_1}{c(B_1)}$. On a donc

$$\frac{1}{c(P)}P = \frac{c(A_1)c(B_1)}{ab}A_2B_2$$

avec $A_2, B_2 \in \mathbb{Z}[X]$ primitifs. En passant aux contenus, on obtient

$$ab\, c\left(\frac{1}{c(P)}P\right) = ab = c(A_1)c(B_1).$$

Donc $P = c(P)A_2B_2$, CQFD. *On a montré le résultat intéressant suivant : $P \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est irréductible dans $\mathbb{Q}[X]$.*

19) D'après la propriété (b), $\overline{P} = \overline{a_n}X^n \neq \overline{0}$ dans $\mathbb{F}_p[X]$. Par l'absurde. Soient $A, B \in \mathbb{Z}[X]$ de degrés $\geqslant 1$ tels que $AB = P$. On pose $r = \deg A$, $s = \deg B$. Donc $\overline{P} = \overline{a_n}X^n = \overline{A}\,\overline{B}$. Mais les seuls diviseurs de X^n sont les puissances de X et leurs associés. Donc $\overline{A}$ et $\overline{B}$ s'écrivent respectivement $\overline{\alpha_r}X^r$ et $\overline{B} = \overline{\beta_s}X^s$. Si $B = \sum_{k=0}^{r}\alpha_k X^k$ et $B = \sum_{k=0}^{s}X^k$, alors p divise α_0 et β_0, et donc p^2 divise $\alpha_0\beta_0 = a_0$. Contradiction.

20) Le nombre premier 2 divise 0, 2^2 ne divise pas le coefficient constant 2 et 2 ne divise pas le coefficient dominant 1. Donc $X^n - 2$ est irréductible sur $\mathbb{Q}[X]$ d'après le critère d'Eisenstein.

21) Toutes les racines p^e de l'unité sauf 1 étant primitive, on a $\Phi_p = \dfrac{X^p-1}{X-1} = X^p + \cdots + X + 1$. Donc

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X+1-1} = \frac{\sum_{k=0}^{p}\binom{p}{k}X^k - 1}{X} = \sum_{k=1}^{p}\binom{p}{k}X^{k-1}.$$

Or p ne divise pas le coefficient dominant $\binom{p}{p} = 1$, p divise $\binom{p}{k}$ pour tout $1 \leqslant k \leqslant p-1$ et p^2 ne divise pas le coefficient constant $\binom{p}{1} = p$. Par le critère d'Eisenstein, $\Phi_p(X+1)$ est irréductible sur $\mathbb{Q}[X]$.

Concluons par l'absurde : si Φ_p n'était pas irréductible sur $\mathbb{Q}$. Alors Φ_p s'écrirait $\Phi_p = AB$ avec $A, B \in \mathbb{Q}[X]$ de degrés $\geqslant 1$. Mais alors $\Phi_p(X+1) = A(X+1)B(X+1)$. Or $A(X+1)$ et $B(X+1)$ sont de même degré que respectivement A et B. Contradiction avec ce qu'on vient de prouver.

22) On a vu que Φ_p est irréductible sur $\mathbb{Q}$. Soit $P \in \mathbb{Q}[X]$ tel que $P(\zeta) = 0$, c'est-à-dire $X - \zeta$ divise P dans $\mathbb{C}[X]$. Mais alors $pgcd(P, \Phi_p) \neq 1$. Or Φ_p étant irréductible dans $\mathbb{Q}[X]$, il est premier avec tout polynôme qu'il ne divise pas. Donc il divise P. Réciproque évidente.

23) Multiplions P par $d \in \mathbb{N}^*$ et Q par $e \in \mathbb{N}^*$ pour avoir $dP, eQ \in \mathbb{Z}[X]$. Alors $\dfrac{dP}{c(dP)} \in \mathbb{Z}[X]$ est primitif et $c(dP)|d$ car d est le coefficient dominant de dP. De même, $\dfrac{eQ}{c(eQ)}$ est primitif et $c(eQ)|e$. D'autre part, en passant aux contenus dans l'égalité

$$c(dP)c(eQ)\frac{dP}{c(dP)}\frac{eQ}{c(eQ)} = de\,PQ$$

on trouve $c(dP)c(eQ) = de$ car $c(PQ) = 1$ (unitaire) et $\dfrac{dP}{c(dP)}\dfrac{eQ}{c(eQ)}$ est primitif comme produit de primitifs. Comme $c(dP) \leqslant d$ et $c(eQ) \leqslant e$, on a donc $c(dP) = d$ et $c(eQ) = e$. Donc $P = \dfrac{dP}{c(dP)} \in \mathbb{Z}[X]$ et de même pour Q.

Autre preuve. D'après la question 18 de la partie 4, PQ s'écrit comme produit de polynômes de $\mathbb{Z}[X]$ irréductibles sur $\mathbb{Q}$ (récurrence immédiate). Donc tout polynôme unitaire irréductible sur $\mathbb{Q}$ qui divise PQ est dans $\mathbb{Z}[X]$ (s'il existait un polynôme unitaire irréductible qui divisait P, et qui n'était pas dans $\mathbb{Z}[X]$, cela contredirait l'unicité de la décomposition en polynômes unitaires irréductibles). Donc tout polynôme unitaire irréductible sur $\mathbb{Q}$ qui divise P est dans $\mathbb{Z}[X]$. Maintenant, écrivons P comme produit de polynômes unitaires irréductibles sur $\mathbb{Q}$: tous ces polynômes sont dans $\mathbb{Z}[X]$, donc P est dans $\mathbb{Z}[X]$. De même pour Q.

Partie 5 : Irréductiblité de Φ_n

24) Soit désormais p un nombre premier ne divisant pas n. Par l'absurde. Si $B \in \mathbb{F}_p[X]$ est tel que $B^2|\overline{X^n-1}$, alors il existe $Q \in \mathbb{F}_p[X]$ tel que $B^2Q = \overline{X^n-1}$. Mais alors en dérivant cette égalité,

$$2BB'Q + B^2Q' = B(2B'Q + BQ') = \overline{n}X^{n-1}.$$

Donc B divise $\overline{n}X^{n-1}$ et donc divise $X(\overline{n}X^{n-1}) - \overline{n}(X^n - \overline{1}) = \overline{n}$. Donc B est constant, contradiction.

25) On a $pgcd(U, V) \neq 1$ car ils ont une racine complexe commune. Par irréductibilité de U, U divise V.

26) Soit $A, B \in \mathbb{Q}[X]$ unitaires tels que $\Phi_n = AB$ et $\deg A \geqslant 1$. D'après la question 23, A et B sont à coefficients entiers. Soit ζ une racine de A et p un nombre premier

ne divisant pas n. Montrons par l'absurde que $B(\zeta^p) \neq 0$. Comme ζ^p est aussi une racine primitive n^{e} de l'unité, on a $\Phi_n(\zeta^p) = 0$. On aura bien que $A(\zeta^p) = 0$.

Supposons que $B(\zeta^p) = 0$. On aura alors $B \circ X^p \in \mathbb{Z}[X]$ et admet ζ pour racine, donc est divisible par A car A est irréductible. Comme $A \in \mathbb{Z}[X]$ est unitaire, le quotient C de $B \circ X^p$ par A est encore à coefficients entiers et unitaire. Mais $B \circ X^p \equiv B^p$ mod p d'après la partie 2. Soit R un facteur irréductible de $\overline{A}$ dans $\mathbb{F}_p[X]$. Alors $R|\overline{A}$ et $R|\overline{AC} = \overline{B^p} = \overline{B}^p$. Par irréductibilité de R, R divise B. Donc R^2 divise A et B donc $\overline{\Phi_n}$. Ainsi R^2 divise $\overline{X^n - 1}$. Contradiction avec 24.

27) Soit A un facteur irréductible sur $\mathbb{Q}$ de Φ_n. Comme A est de degré $\geqslant 1$ et divise Φ_n, A admet pour racine une racine primitive n^{e} de l'unité. Soit ζ cette racine. Elle est donc de la forme $e^{ik2\pi/n}$ avec k premier avec n (question 8). Il suffit de montrer que tout autre racine primitive n^{e} de l'unité est encore racine de A. On aura alors que $\prod_{z \in Z_n} (X - z) = \Phi_n$ divisera A car les $X - z$ sont premiers entre eux deux à deux.

Soit $k' \in \mathbb{Z}$ premier avec n. Donc $\overline{k}$ et $\overline{k'}$ sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$ (cours). Soit donc $\overline{u} = \overline{k}^{-1}\overline{k'}$. Comme les inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ forment un groupe, $\overline{u}$ est inversible. Donc u est premier avec n. Écrivons la décomposition en facteurs premiers $u = p_1 p_2 \cdots p_s$. Comme u est premier avec n, les p_j sont premiers avec n. Si z est une racine primitive n^{e} de l'unité et p un nombre premier avec n, alors z^p est aussi une racine primitive n^{e} de l'unité. En effet $z = e^{i2\pi q/n}$ et donc $z^p = e^{i2\pi pq/n}$; or n étant premier à p et q, il est premier à pq.

Par récurrence immédiate, puisque ζ est une racine primitive n^{e}, alors $\zeta^{p_1}, \zeta^{p_1 p_2}, \ldots, \zeta^{p_1 p_2 \cdots p_s} = \zeta^u$ sont des racines de A d'après le lemme. Or $\zeta^u = e^{iku2\pi/n} = e^{ik'2\pi/n}$. QED.