Problème – Polynômes cyclotomiques

Le but du problème est de donner la décomposition en produit d'irréductibles sur $\mathbb{Q}$ de $X^n - 1$ lorsque n est un entier naturel non-nul. Le résultat et la preuve sont dus à Gauss.

On désigne par $\mathbb{Z}[X]$ l'ensemble des polynômes en l'indéterminée X à coefficients entiers relatifs. On prendra garde que $\mathbb{Z}$ n'est pas un corps, donc que certaines propriétés du cours ne s'appliquent pas à $\mathbb{Z}[X]$. Évidemment, $\mathbb{Z}[X]$ est un anneau pour la somme et le produit des polynômes. On désigne par $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ lorsque p est un entier premier.

Soient $n \in \mathbb{N}^*$ et $z_k = \exp\left(2i\pi\dfrac{k}{n}\right)$ avec $k \in \mathbb{Z}$.

Partie 1 : Calculs préliminaires

1) Donner la décomposition de $X^n - 1$ en produits d'irréductibles sur $\mathbb{C}$.
2) Soient $a, b \in \mathbb{C}$. Montrer que $\displaystyle\prod_{k=1}^{n}(a + bz_k) = a^n + (-1)^{n-1}b^n$.
3) Soit $\theta \in \mathbb{R}$. Montrer que $\displaystyle\prod_{k=1}^{n}(z_k^2 - 2(\cos\theta)z_k + 1) = 2(1 - \cos n\theta)$.

Partie 2 : Réduction *modulo* p

Soit p un entier naturel premier. Pour tout entier relatif k, on note $\overline{k}$ sa classe modulo p. On appelle *réduction modulo* p du polynôme $P = \displaystyle\sum_k a_k X^k$ le polynôme noté $\overline{P}$ de $\mathbb{F}_p[X]$ défini par $\displaystyle\sum_k \overline{a_k} X^k$. On a évidement $\overline{P+Q} = \overline{P} + \overline{Q}$ et $\overline{PQ} = \overline{P}\,\overline{Q}$.

4) On suppose dans cette question que p est le nombre premier 1789. (On ne justifiera pas la primalité de p.) Déterminer une relation de Bézout entre p et $k = 2018$. En déduire l'inverse de $\overline{2018}$ dans $\mathbb{F}_p$. (On fera apparaître la méthode et les calculs de la manières la plus concise mais complète possible.)
5) Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise le coefficient binomial $\dbinom{p}{k}$.
6) En déduire que pour $A, B \in \mathbb{F}_p[X]$, $(A+B)^p = A^p + B^p$.
7) Montrer que si $\displaystyle\sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X]$, alors $\left(\displaystyle\sum_{k=0}^{d} \overline{a_k} X^k\right)^p = \displaystyle\sum_{k=0}^{d} \overline{a_k} X^{kp}$.

Partie 3 : Racines primitives de l'unité

On rappelle que la *fonction indicatrice d'Euler* φ est définie par $\varphi(n) = \mathrm{Card}\{k \mid 1 \leqslant k \leqslant n$ et $\mathrm{pgcd}(n,k) = 1\}$. Autrement dit, $\varphi(n)$ est le nombre d'entiers $\leqslant n$ premiers à n.

On appelle *racine primitive n-ième de l'unité* toute racine n-ième de l'unité ζ telle que $\zeta^q \neq 1$ si $1 \leqslant q \leqslant n-1$. Autrement dit, une racine n-ième de l'unité est primitive si elle n'est pas racine q-ième de l'unité pour un q strictement plus petit. Soit Z_n l'ensemble des racines primitives n-ième de l'unité.

On définit le n-ième *polynôme cyclotomique* Φ_n par

$$\Phi_n = \prod_{\zeta \in Z_n}(X - \zeta).$$

8) A quelle condition sur k a-t-on z_k racine primitive n-ième ?
9) Déterminer les racines primitives n-ièmes de l'unité pour $n = 2, 3, 4, 5, 6$.
10) Déterminer $\Phi_2, \Phi_3, \Phi_4, \Phi_5, \Phi_6$. (On veut leurs coefficients.)
11) Déterminer $\deg \Phi_n$.
12) Montrer que $X^n - 1 = \displaystyle\prod_{d|n}\Phi_d$.
13) En déduire $\displaystyle\sum_{d|n}\varphi(d)$.
14) Soit $A, B \in \mathbb{Z}[X]$ avec B unitaire. Montrer que le quotient et le reste de la division euclidienne de A par B sont encore à coefficients entiers. (On pourra raisonner par récurrence sur $\deg A$.)
15) Montrer que Φ_n est à coefficients entiers.

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

On appelle *contenu* du polynôme $P \in \mathbb{Z}[X]$ le $pgcd$ des coefficients de P. On note $c(P)$ le contenu de P. Un polynôme est *primitif* si son contenu est 1.

16) Montrer que si $P, Q \in \mathbb{Z}[X]$ sont primitifs, PQ aussi. (Raisonner par l'absurde : sinon il existerait un diviseur premier p de $c(PQ)$; considérer alors le plus grand coefficient non divisible par p de P et Q - ou réduire modulo p, ce qui revient au même.)
17) Montrer que si $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)c(Q)$.
18) Soit $P \in \mathbb{Z}[X]$. On suppose que P n'est pas irréductible sur $\mathbb{Q}$. Montrer qu'il existe $A, B \in \mathbb{Z}[X]$ de degrés $\geqslant 1$ tels que $P = AB$.
19) On se propose de montrer le *critère d'Eisenstein* : soit $d \in \mathbb{N}^*$ et $P \in \mathbb{Z}[X]$, $P = a_d X^d + \cdots + a_1 X + a_0$ avec $a_d \neq 0$. On suppose qu'il existe un nombre premier p tel que :
    (a) p ne divise pas a_d ;

(b) p divise $a_0, a_1, \dots, a_{d-1}$;

(c) p^2 ne divise pas a_0.

Montrer que P est irréductible sur $\mathbb{Q}$. (Regarder modulo p et utiliser l'unicité de l'écriture comme produit d'irréductibles dans $\mathbb{F}_p[X]$.)

20) Application 1 : Montrer que $X^n - 2$ est irréductible sur $\mathbb{Q}$. *(Il existe donc des polynômes irréductibles de tout degré sur $\mathbb{Q}$.)*

21) Application 2 : Soit p premier. Déterminer $\Phi_p \circ (X+1)$. Montrer que ce polynôme est irréductible sur $\mathbb{Q}$ et en déduire que Φ_p est irréductible sur $\mathbb{Q}$.

22) Soit p un nombre premier et $\zeta = \exp \dfrac{2i\pi}{p}$. Montrer que pour tout $P \in \mathbb{Q}[X]$, $P(\zeta) = 0$ si et seulement si Φ_p divise P.

23) Soient $P, Q \in \mathbb{Q}[X]$ unitaires tels que $PQ \in \mathbb{Z}[X]$. Montrer que $P, Q \in \mathbb{Z}[X]$.

Partie 5 : Irréductiblité de Φ_n

On considère le lemme suivant :

Lemme 1 *Soit p un nombre premier ne divisant pas n, $A \in \mathbb{Q}[X]$ un facteur unitaire irréductible sur $\mathbb{Q}$ de Φ_n et ζ une racine primitive n-ième de l'unité telle que $A(\zeta) = 0$. Alors $A(\zeta^p) = 0$.*

24) On considère $\overline{\Phi_n} \in \mathbb{F}_p[X]$. Montrer qu'il n'existe pas de polynôme non-constant $B \in \mathbb{F}_p[X]$ tel que B^2 divise $\overline{X^n - 1}$. (Considérer $X(X^n-1)' - n(X^n-1)$.)

25) Soient $U, V \in \mathbb{Q}[X]$ et $z \in \mathbb{C}$ tels que $U(z) = V(z) = 0$. Montrer que si U est irréductible sur $\mathbb{Q}$, U divise V.

26) Sous les hypothèses du lemme : soit B unitaire tel que $\Phi_n = AB$. Montrer par l'absurde que $B(\zeta^p) \neq 0$. (Sinon $B \circ X^p = AC$; réduire modulo p et considérer un facteur irréductible sur $\mathbb{F}_p$ de $\overline{A}$.) En déduire le lemme.

27) Montrer que $A = \Phi_n$.

Donc Φ_n est irréductible sur $\mathbb{Q}$.