DM 53 : Polynômes cyclotomiques et théorème de Dirichlet

Le but de ce problème est de d'étudier les polynômes cyclotomiques pour démontrer deux cas particuliers du théorème de la progression arithmétique de Dirichlet. Ce théorème affirme que pour tout $a, n \in \mathbb{N}^*$ tel que $a \wedge n = 1$, il existe une infinité de nombres premiers p tels que $p \equiv a\ [n]$. Nous démontrons dans ce problème les deux cas $a = 1$ et $a = -1$, respectivement dans les parties II et III.

Notations, définitions et rappels

◇ Pour $n \in \mathbb{N}^*$, $\mathbb{P}(n)$ désigne l'ensemble des entiers de $\{1, \ldots, n\}$ premiers avec n : $\mathbb{P}(n) = \{k \in \{1, \ldots, n\} \ / \ k \wedge n = 1\}$.

◇ L'indicatrice d'Euler $\varphi(n)$ est le cardinal de $\mathbb{P}(n)$.

◇ Pour $(n, k) \in \mathbb{N}^* \times \mathbb{N}$, on note $\omega_{n,k} = e^{2i\pi\frac{k}{n}}$.

◇ Le polynôme cyclotomique $\Phi_n \in \mathbb{C}[X]$ est défini par : $\Phi_n = \prod_{k \in \mathbb{P}(n)} (X - \omega_{n,k})$.

◇ La notation $\sum_{d|n} a_d$ désigne la somme sur tous les diviseurs d de n tels que $d \in \mathbb{N}$.
De même, la notation $\prod_{d|n} a_d$ désigne le produit sur tous les diviseurs d de n tels que $d \in \mathbb{N}$.

◇ Soit $n \in \mathbb{N}^*$. Lorsque $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est la décomposition de n en produit de facteurs premiers, avec $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$, où $p_1, \ldots, p_k$ sont des nombres premiers deux à deux distincts, on définit $\mu(n)$ de la façon suivante :
si pour tout $i \in \{1, \ldots, k\}$, $\alpha_i = 1$, alors $\mu(n) = (-1)^k$
et s'il existe $i \in \{1, \ldots, k\}$ tel que $\alpha_i \geq 2$, alors $\mu(n) = 0$.
μ s'appelle la fonction de Möbius.

◇ Le symbole de Kronecker $\delta_{a,b}$ est égal à 1 si $a = b$ et est égal à 0 sinon.

◇ Pour tout nombre premier p, on rappelle que $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps, que l'on notera $\mathbb{F}_p$.

◇ Lorsque $\mathbb{K}$ est un corps et que $P \in \mathbb{K}[X]$, l'ensemble des racines dans $\mathbb{K}$ du polynôme P est noté $\mathrm{Rac}(P)$ ou bien $\mathrm{Rac}_{\mathbb{K}}(P)$ s'il y a ambiguïté sur le corps $\mathbb{K}$ dans lequel on se place.

Partie I : Propriétés élémentaires des polynômes cyclotomiques

Soit $n \in \mathbb{N}^*$.

1°) En fonction des définitions et des notations précédentes, donner le degré et le coefficient dominant de Φ_n.

2°) Déterminer Φ_n lorsque $n = 1$, 2, 3, 4 et pour $n = 6$.

3°) Déterminer Φ_n lorsque n est premier.

4°) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$.

5°) Soit $A, B \in \mathbb{Z}[X]$, deux polynômes à coefficients dans $\mathbb{Z}$.
On suppose de plus que B est non nul et unitaire.
Montrer qu'il existe un unique couple (Q, R) de polynômes dans $\mathbb{Z}[X]$
tels que $A = BQ + R$ avec $\deg(R) < \deg(B)$.

6°) Montrer que $\Phi_n \in \mathbb{Z}[X]$.

7°) Montrer que pour tout $n \geq 2$, $\Phi_n(0) = 1$.

8°) Montrer que $\sum_{d|n} \mu(d) = \delta_{1,n}$, où μ est la fonction de Möbius et $\delta_{1,n}$ le symbole de Kronecker.

9°) Montrer que, dans l'ensemble des fractions rationnelles $\mathbb{C}(X)$,
on a $\Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}$.
Indication : partir du produit et utiliser la question 4.

10°) Soit p un nombre premier. Montrer que $\Phi_{np}(X) = \begin{cases} \Phi_n(X^p) & \text{si } p \mid n, \\ \dfrac{\Phi_n(X^p)}{\Phi_n(X)} & \text{sinon.} \end{cases}$

Partie II : Une infinité de premiers congrus à 1 modulo n.

Dans cette partie, n désigne un entier supérieur ou égal à 1.
On fixe un nombre premier p. Lorsque $a \in \mathbb{Z}$, on note $\overline{a}$ la classe de congruence de a modulo p, de sorte que $\overline{a}$ est un élément de $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.
Lorsque $P = \sum_{k \in \mathbb{N}} p_k X^k \in \mathbb{Z}[X]$, on pose $\overline{P} = \sum_{k \in \mathbb{N}} \overline{p_k} X^k \in \mathbb{F}_p[X]$.

11°) Montrer que l'application $P \longmapsto \overline{P}$ est un morphisme d'anneaux de $\mathbb{Z}[X]$ dans $\mathbb{F}_p[X]$. Est-il surjectif ? Est-il injectif ?

Jusqu'à la question 16 incluse, on suppose que $\overline{\Phi_n}$ possède une racine dans $\mathbb{F}_p$, que l'on note a. On note ω l'ordre de a, c'est-à-dire le plus petit entier strictement positif tel que $a^\omega = \overline{1}$.

12°) Montrer que $a \neq \overline{0}$ et que ω divise $p - 1$.

13°) À l'aide de la question 4, montrer qu'il existe $d \in \mathbb{N}^*$ tel que d divise ω et tel que $\overline{\Phi_d}(a) = 0$, puis montrer que $d = \omega$.

14°) Soit $Q \in \mathbb{F}_p[X]$ et $x \in \mathbb{F}_p$ tel que $Q(x) = 0$ et $Q'(x) \neq 0$.
Montrer que x est une racine simple de Q.

15°) On suppose pour cette question que p et n sont premiers entre eux.
Montrer que a est une racine simple de $X^n - \overline{1}$
et en déduire que $\omega = n$ puis que $p \equiv 1\ [n]$.

16°) On suppose pour cette question que p divise n.
Montrer à l'aide de la question 10 que a est une racine de $\overline{\Phi_{\frac{n}{p}}}$.
En déduire qu'il existe $v \in \mathbb{N}^*$ tel que $n = p^v\omega$.
Montrer que p est le plus grand diviseur premier de n.

17°) Soit $\alpha \in \mathbb{Z}$. Si p divise $\Phi_n(\alpha)$, montrer que $p \equiv 1\ [n]$ ou que p est le plus grand diviseur premier de n.

18°) On suppose que $n \geq 2$.
Pour cette question, p n'est plus fixé. On suppose que l'ensemble des nombres premiers p tels que $p \equiv 1\ [n]$ est fini. On note k le cardinal de cet ensemble et $p_1, \ldots, p_k$ ses éléments.
On suppose que N est un multiple de n, et on pourra choisir N aussi grand que nécessaire. On pose $A = N \prod_{i=1}^{k} p_i$.
Montrer que $\Phi_n(A)$ et A sont premiers entre eux.
En considérant un diviseur premier de $\Phi_n(A)$, aboutir à une contradiction.

Partie III : Une infinité de premiers congrus à -1 modulo n.

p désigne à nouveau un nombre premier et $n \in \mathbb{N}^*$.
On admet l'existence d'un corps $\mathbb{K}$ tel que $\mathbb{F}_p$ est un sous-corps de $\mathbb{K}$ et tel que tout polynôme de $\mathbb{K}[X]$ est scindé dans $\mathbb{K}[X]$.

19°) Montrer que $\mathrm{Rac}_{\mathbb{K}}(X^p - X) = \mathbb{F}_p$.

20°) Lorsque a est un élément de $\mathbb{K} \setminus \{0\}$ d'ordre fini, on notera $\mathrm{ord}(a)$ son ordre.
On suppose que $p \wedge n = 1$.
Montrer que les racines de $\overline{\Phi_n}$ dans $\mathbb{K}$ sont simples.
Montrer que $\overline{\Phi_n}(X) = \prod_{\substack{a \in \mathbb{K}\setminus\{0\} \\ \text{tq } \mathrm{ord}(a)=n}} (X - a)$.

21°) Montrer que, pour tout $k \in \mathbb{N}^*$, il existe $(b_0, \ldots, b_k) \in \mathbb{Z}^{k+1}$
tel que $\left(X + \frac{1}{X}\right)^k = b_0 + \sum_{\ell=1}^{k} b_\ell \left(X^\ell + \frac{1}{X^\ell}\right)$, avec $b_k = 1$.

22°) Soit $k \in \mathbb{N}$ et $(a_0, \dots, a_k) \in \mathbb{Z}^{k+1}$. Montrer qu'il existe $Q \in \mathbb{Z}[X]$ avec $\deg(Q) \leq k$ tel que $a_0 + \sum_{\ell=1}^{k} a_\ell \Big(X^\ell + \frac{1}{X^\ell}\Big) = Q\Big(X + \frac{1}{X}\Big)$, et tel que $\deg(Q) = k$ si $a_k \neq 0$.

En déduire que, pour tout $P \in \mathbb{Z}[X]$ tel que $\deg(P) = 2k$ et $X^{2k} P\Big(\frac{1}{X}\Big) = P(X)$, il existe $Q \in \mathbb{Z}[X]$, avec $\deg(Q) = k$, tel que $P(X) = X^k Q\Big(X + \frac{1}{X}\Big)$.

Pour toute la suite de ce problème, on suppose que $n \geq 3$.

23°) Montrer que $\varphi(n)$ est pair et non nul.

24°) Montrer qu'il existe un polynôme $\Psi_n \in \mathbb{Z}[X]$, de degré $\frac{\varphi(n)}{2}$, tel que $\Psi_n\Big(X + \frac{1}{X}\Big) = \frac{\Phi_n(X)}{X^{\frac{\varphi(n)}{2}}}$.

25°) On suppose que $n \wedge p = 1$.
Soit $\omega \in \mathbb{K} \setminus \{0\}$. Posons $\beta = \omega + \frac{1}{\omega}$. Montrer que $\beta^p = \omega^p + \frac{1}{\omega^p}$.
Montrer que $\beta^p = \beta$ si et seulement si $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$.
En déduire que si γ est une racine dans $\mathbb{K}$ de $\overline{\Psi_n}$, alors $\gamma \in \mathbb{F}_p \Longleftrightarrow p \equiv \pm 1\ [n]$.

26°) On suppose que $n \geq 3$ avec $n \neq 4$ (les cas où $n = 1$ ou $n = 2$ sont évidents et le cas où $n = 4$ a été vu en TD). On suppose que l'ensemble des nombres premiers q tels que $q \equiv -1\ [n]$ est fini. On note k le cardinal de cet ensemble et $p_1, \dots, p_k$ ses éléments.
a) Montrer que $\Psi_n(0) \neq 0$.
On pose $a = \Psi_n(0)$ et $\Theta(X) = \frac{1}{a}\Psi_n(aX)$.
b) Montrer que $\Theta \in \mathbb{Z}[X]$.
c) Calculer les racines complexes de Ψ_n et en déduire que les racines complexes de Θ sont toutes réelles et simples.
d) En déduire qu'il existe $\alpha, \beta \in \mathbb{R}$ avec $\alpha < \beta$ tels que pour tout $t \in [\alpha, \beta]$, $\Theta(t) < 0$.
D'après la partie II, il existe un nombre premier p_0 tel que $p_0 \equiv 1\ [np_1 \cdots p_k]$.
e) Montrer l'existence d'un entier $m \in \mathbb{Z}$ et d'un entier $\ell \in \mathbb{N}$ tels que $\Theta\Big(\frac{m}{p_0^\ell} np_1 \cdots p_k\Big) < 0$.
f) Montrer que $p_0^{\frac{1}{2}\varphi(n)\ell} \Theta\Big(\frac{m}{p_0^\ell} np_1 \cdots p_k\Big)$ est un entier relatif, congru à 1 modulo $np_1 \cdots p_k$.
g) Aboutir à une contradiction en étudiant les diviseurs premiers de $p_0^{\frac{1}{2}\varphi(n)\ell} \Theta\Big(\frac{m}{p_0^\ell} np_1 \cdots p_k\Big)$ distincts de p_0.