

DS 8 : un corrigé

Barème

Le barème comporte un total de 80 points.

Partie I (sur 22 points) : 2 points pour les questions 1 et 2, puis 1, 4, 3, 1, 1, 3, 3, 4.

Partie 2 (sur 19 points) : 2, 2, 3, 1, 4, 3, 1, 3.

Partie 3 (sur 39 points) : 1, 4, 3, 3, 2, 3, pour la question 25 : 2, 2, 4, pour la question 26 : 2, 1, 2, 1, 2, 2, 5.

Partie I : Propriétés élémentaires des polynômes cyclotomiques

1°) Le degré de Φ_n est le cardinal de $P(n)$, donc $\deg(\Phi_n) = \varphi(n)$.

Le polynôme Φ_n est défini comme produit de polynômes unitaires, il est donc également unitaire.

2°) $\mathbb{P}(1) = \{1\}$, donc $\Phi_1 = X - \omega_{1,1} = \boxed{X - 1 = \Phi_1}$.

$\mathbb{P}(2) = \{1\}$, donc $\Phi_2 = X - \omega_{2,1} = \boxed{X + 1 = \Phi_2}$.

$\mathbb{P}(3) = \{1, 2\}$, donc $\Phi_3 = (X - \omega_{3,1})(X - \omega_{3,2}) = (X - j)(X - j^2) = \boxed{X^2 + X + 1 = \Phi_3}$.

$\mathbb{P}(4) = \{1, 3\}$, donc $\Phi_4 = (X - \omega_{4,1})(X - \omega_{4,3}) = (X - i)(X + i) = \boxed{X^2 + 1 = \Phi_4}$.

$\mathbb{P}(6) = \{1, 5\}$, donc $\Phi_6 = (X - e^{i\frac{\pi}{3}})(X - e^{i\frac{5\pi}{3}}) = X^2 - 2X \cos \frac{\pi}{3} + 1$, donc $\boxed{\Phi_6(X) = X^2 - X + 1}$.

3°) On suppose que n est premier. Alors $\mathbb{P}(n) = \{1, \dots, n-1\}$. Ainsi,

$$\Phi_n(X) = \prod_{k=1}^{n-1} (X - \omega_{n,k}) = \frac{X^n - 1}{X - 1} = \boxed{X^{n-1} + X^{n-2} + \dots + X + 1 = \Phi_n}.$$

4°) D'après le cours, $X^n - 1 = \prod_{k=1}^n (X - e^{2i\pi \frac{k}{n}})$.

Posons $A = \{\frac{k}{n} / k \in \mathbb{N}_n\}$. Ainsi, $X^n - 1 = \prod_{a \in A} (X - e^{2i\pi a})$.

Soit $a \in A$. Il existe $k \in \mathbb{N}_n$ tel que $a = \frac{k}{n}$. L'écriture irréductible de ce rationnel est de la forme $a = \frac{h}{d}$, où $h \wedge d = 1$, d étant un diviseur de n dans \mathbb{N} . De plus, $a \in]0, 1]$,

donc $h \in \mathbb{N}_d$. Ainsi, $a = \frac{h}{d}$, où $h \in \mathbb{P}(d)$. Ceci démontre que $A \subset \bigcup_{d \mid n} \left\{ \frac{h}{d} / h \in \mathbb{P}(d) \right\}$.

Réciproquement, si a est de la forme $a = \frac{h}{d}$, où $h \wedge d = 1$, d étant un diviseur de n , alors il existe $e \in \mathbb{N}$ tel que $n = de$, donc $a = \frac{he}{de} = \frac{he}{n} \in A$. De plus, cette réunion est disjointe par unicité de l'écriture d'un rationnel sous forme irréductible.

Ainsi $A = \bigsqcup_{d \mid n} \left\{ \frac{h}{d} / h \in \mathbb{P}(d) \right\}$. Alors, par produit par paquets,

$$X^n - 1 = \prod_{d \mid n} \prod_{h \in \mathbb{P}(d)} (X - e^{2i\pi \frac{h}{d}}), \text{ donc } \boxed{X^n - 1 = \prod_{d \mid n} \Phi_d}.$$

5°) \diamond Unicité : Supposons qu'il existe $(Q, R) \in \mathbb{Z}[X]^2$ tels que $A = BQ + R$ avec $\deg(R) < \deg(B)$. Alors $(Q, R) \in \mathbb{Q}[X]^2$, donc Q et R sont le reste et quotient de la division euclidienne de A par B dans $\mathbb{Q}[X]$ (\mathbb{Q} étant un corps). Ainsi, sous condition d'existence, il y a bien unicité.

\diamond **Existence :** On fixe $B \in \mathbb{Z}[X] \setminus \{0\}$ et on suppose que B est unitaire.

Soit $n \in \mathbb{N}$. On note $R(n)$ l'assertion suivante : pour tout $A \in \mathbb{Z}[X]$ avec $\deg(A) \leq n$, il existe un couple $(Q, R) \in \mathbb{Z}[X]^2$ tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$.

Pour $n = 0$, soit $A \in \mathbb{Z}[X]$ avec $\deg(A) \leq 0$.

Si $\deg(B) \geq 1$, le couple $(Q, R) = (0, A)$ convient.

Sinon, $\deg(B) = 0$, donc $B \in \mathbb{Z} \setminus \{0\}$. De plus, B est unitaire, donc $B = 1$. On peut alors écrire $A = BA + 0$ et $\deg(0) < \deg(B)$. Donc le couple $(A, 0)$ convient.

Pour $n \geq 1$, on suppose $R(n-1)$. Soit $A \in \mathbb{Z}[X]$ avec $\deg(A) \leq n$.

Si $\deg(A) < \deg(B)$, il suffit d'écrire $A = 0.B + A$.

Supposons maintenant que $\deg(A) \geq \deg(B)$. Posons $A = a_n X^n + C$

avec $\deg(C) \leq n-1$ et $B = X^p + D$ avec $\deg(D) < p \leq n$.

Alors $A - a_n X^{n-p} B = a_n X^n + C - a_n X^n - a_n X^{n-p} D = C - a_n X^{n-p} D$.

Or $\deg(C - a_n X^{n-p} D) \leq \max(\deg(C), n-p+\deg(D)) \leq n-1$, donc d'après $R(n-1)$, il existe $(Q', R) \in \mathbb{Z}[X]^2$ tels que $C - a_n X^{n-p} D = BQ' + R$ et $\deg(R) < \deg(B)$.

Alors $A = (a_n X^{n-p} + Q')B + R$, ce qui prouve $R(n)$, car $Q = a_n X^{n-p} + Q' \in \mathbb{Z}[X]$.

Ceci prouve l'existence d'après le principe de récurrence.

6°) Montrons par récurrence forte sur $n \in \mathbb{N}^*$ que $\Phi_n \in \mathbb{Z}[X]$.

— **Initialisation :** vérifiée pour $n \in \{1, 2, 3, 4\}$ d'après la question 2.

— **Hérédité :** soit $n \geq 2$ tel que pour tout $m \in \{1, \dots, n-1\}$, $\Phi_m \in \mathbb{Z}[X]$.

Alors, le polynôme $Q = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d$ est à coefficients entiers et unitaire. Or d'après

la question 4, Φ_n est le quotient de $X^n - 1$ par ce polynôme, donc d'après la question précédente, $\Phi_n \in \mathbb{Z}[X]$.

D'après le principe de récurrence, pour tout $n \geq 1$, $\Phi_n \in \mathbb{Z}[X]$.

7°) D'après la question 2, $\Phi_1(0) = -1$ et pour tout $n \in \{2, 3, 4\}$, $\Phi_n(0) = 1$.

Supposons que $n \geq 3$ et que, pour tout $k \in \{2, \dots, n-1\}$, $\Phi_k(0) = 1$. Alors pour tout $d \in \mathbb{N}^*$ tel que $d \mid n$ et $d < n$, $\Phi_d(0) = 1$. Or $X^n - 1 = \Phi_n \Phi_1 \prod_{\substack{d \mid n \\ d \notin \{1, n\}}} \Phi_d$, donc en évaluant

en 0, on obtient que $-1 = -\Phi_n(0)$, donc $\Phi_n(0) = 1$.

Le principe de récurrence forte permet de conclure.

8°) Notons $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la décomposition de n en produit de facteurs premiers, avec $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$, où p_1, \dots, p_k sont des nombres premiers deux à deux distincts. Si $n = 1$, le seul diviseur de n dans \mathbb{N} est 1, donc $\sum_{d|1} \mu(d) = \mu(1) = (-1)^0 = 1$.

On suppose maintenant que $n \geq 2$ et on doit montrer que $\sum_{d|n} \mu(d) = 0$.

Soit d un diviseur de n . Ainsi, il existe $\beta_1, \dots, \beta_k \in \mathbb{N}$ tels que $d = \prod_{i=1}^k p_i^{\beta_i}$ avec $\beta_i \leq \alpha_i$ pour tout $i \in \mathbb{N}_k$. S'il existe $i \in \mathbb{N}_k$ tel que $\beta_i \geq 2$, alors $\mu(d) = 0$, donc les seuls diviseurs d de n pour lesquels $\mu(d) \neq 0$ sont de la forme $d = \prod_{i \in I} p_i$, où $I \subset \mathbb{N}_k$, et dans

ce cas, $\mu(d) = (-1)^{|I|}$.

L'application $I \mapsto \prod_{i \in I} p_i$ est donc une bijection de $\mathcal{P}(\mathbb{N}_k)$ dans l'ensemble des diviseurs

d de n tels que $\mu(d) \neq 0$. Ainsi, par changement de variable,

$$\sum_{d|n} \mu(d) = \sum_{I \subset \mathbb{N}_k} (-1)^{|I|}, \text{ puis par sommation par paquets,}$$

$$\sum_{d|n} \mu(d) = \sum_{h=0}^k \sum_{\substack{I \subset \mathbb{N}_k \\ |I|=h}} (-1)^h = \sum_{h=0}^k \binom{k}{h} (-1)^h = (1-1)^k \text{ d'après la formule du binôme}$$

de Newton. Or $k \geq 1$, car $n \geq 2$, donc $\sum_{d|n} \mu(d) = 0$.

$$9^\circ) \text{ D'après la question 4, } \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|n} \prod_{d'|\frac{n}{d}} \Phi_d^{\mu(d')}.$$

Posons $A = \{(d, d') \in \mathbb{N}^{*2} / d|n \text{ et } d'|\frac{n}{d}\}$.

Soit $(d, d') \in A$. Alors $n = d \frac{n}{d}$ et $\frac{n}{d} \in \mathbb{N}$ et $\frac{n}{d} = d' \frac{n}{dd'}$ et $\frac{n}{dd'} \in \mathbb{N}$.

Dans ce cas, $\frac{n}{d'} = d \frac{n}{dd'} \in \mathbb{N}$, donc on peut écrire $n = d' \frac{n}{d'}$ et $\frac{n}{d'} = d \frac{n}{dd'}$. Ceci prouve que

$(d', d) \in A$. On peut donc poser $f : \begin{matrix} A & \longrightarrow & A \\ (d, d') & \longmapsto & (d', d) \end{matrix}$. On a clairement $f \circ f = Id_A$,

donc f est une bijection. Or

$$\prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{(d, d') \in A} \Phi_{d'}^{\mu(d)} = \prod_{(d, d') \in A} g(d, d'), \text{ en posant } g(d, d') = \Phi_{d'}^{\mu(d)}, \text{ donc par}$$

$$\text{changement de variables, } \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{(d, d') \in A} g(f(d, d')) = \prod_{(d, d') \in A} g(d', d). \text{ Ainsi,}$$

$$\prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|n} \prod_{d'|\frac{n}{d}} \Phi_d^{\mu(d')} = \prod_{d|n} \Phi_d^{\sum_{d'|\frac{n}{d}} \mu(d')} = \prod_{d|n} \Phi_d^{\delta_{1, \frac{n}{d}}} = \Phi_n.$$

10°) Supposons que p est premier. Notons à nouveau $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ la décomposition primaire de n .

Premier cas : on suppose que p ne divise pas n . Alors, la décomposition primaire de

np s'écrit $np = p \prod_{i=1}^k p_i^{\alpha_i}$, donc les diviseurs de np sont les entiers de la forme $p^{\beta_0} \prod_{i=1}^k p_i^{\beta_i}$

avec $\beta_0 \in \{0, 1\}$ et, pour tout $i \in \mathbb{N}_k$, $\beta_i \in \{0, \dots, \alpha_i\}$. Ainsi, si l'on note D l'ensemble des diviseurs de n , l'ensemble des diviseurs de np est $D \sqcup pD$. Alors, d'après la question

précédente, $\Phi_{np} = \prod_{d \in D \sqcup (pD)} (X^{\frac{np}{d}} - 1)^{\mu(d)} = \left(\prod_{d \in D} ((X^p)^{\frac{n}{d}} - 1)^{\mu(d)} \right) \left(\prod_{d \in D} (X^{\frac{np}{pd}} - 1)^{\mu(pd)} \right)$,

or par définition de μ , lorsque $d \in D$, $\mu(pd) = -\mu(d)$, donc

$$\Phi_{np} = \frac{\prod_{d \in D} ((X^p)^{\frac{n}{d}} - 1)^{\mu(d)}}{\prod_{d \in D} (X^{\frac{np}{pd}} - 1)^{\mu(d)}} = \frac{\Phi_n(X^p)}{\Phi_n(X)}.$$

Second cas : on suppose maintenant que p divise n . Sans perte de généralité, on peut

supposer que $p = p_1$. Alors, la décomposition primaire de np s'écrit $np = p_1^{\alpha_1+1} \prod_{i=2}^k p_i^{\alpha_i}$,

donc les diviseurs de np sont les entiers de la forme $\prod_{i=1}^k p_i^{\beta_i}$ avec $\beta_1 \in \{0, \alpha_1 + 1\}$ et,

pour tout $i \in \{2, \dots, k\}$, $\beta_i \in \{0, \dots, \alpha_i\}$. Ainsi l'ensemble des diviseurs de np est la

réunion disjointe de D et de $E = \left\{ p_1^{\alpha_1+1} \prod_{i=2}^k p_i^{\beta_i} \mid \forall i \in \{2, \dots, k\}, \beta_i \in \{0, \dots, \alpha_i\} \right\}$,

mais pour tout $d \in E$, $\mu(d) = 0$ car $\alpha_1 + 1 \geq 2$, donc d'après la question précédente,

$$\Phi_{np} = \prod_{d \in D} (X^{\frac{np}{d}} - 1)^{\mu(d)} = \Phi_n(X^p).$$

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

11°) \diamond Soit $P = \sum_{k \in \mathbb{N}} p_k X^k$ et $Q = \sum_{k \in \mathbb{N}} q_k X^k$ deux polynômes de $\mathbb{Z}[X]$. Alors

$$P + Q = \sum_{k \in \mathbb{N}} (p_k + q_k) X^k, \text{ donc } \overline{P + Q} = \sum_{k \in \mathbb{N}} \overline{p_k + q_k} X^k = \sum_{k \in \mathbb{N}} \overline{p_k} X^k + \sum_{k \in \mathbb{N}} \overline{q_k} X^k = \overline{P} + \overline{Q}.$$

$$\text{De même, } PQ = \sum_{k \in \mathbb{N}} \left(\sum_{h+\ell=k} p_h q_\ell \right) X^k,$$

$$\text{donc } \overline{PQ} = \sum_{k \in \mathbb{N}} \left(\sum_{h+\ell=k} \overline{p_h q_\ell} \right) X^k = \sum_{k \in \mathbb{N}} \left(\sum_{h+\ell=k} \overline{p_h} \overline{q_\ell} \right) X^k. \text{ D'autre part, en calculant}$$

$$\text{dans l'anneau } \mathbb{F}_p[X], \overline{P} \times \overline{Q} = \left(\sum_{k \in \mathbb{N}} \overline{p_k} X^k \right) \times \left(\sum_{k \in \mathbb{N}} \overline{q_k} X^k \right) = \sum_{k \in \mathbb{N}} \left(\sum_{h+\ell=k} \overline{p_h} \overline{q_\ell} \right) X^k, \text{ donc}$$

$\overline{PQ} = \overline{P} \times \overline{Q}$. De plus $\overline{1} = 1_{\mathbb{F}_p[X]}$, donc l'application $P \mapsto \overline{P}$ est un morphisme d'anneaux.

\diamond Soit $Q \in \mathbb{F}_p[X]$. Ses coefficients sont dans \mathbb{F}_p , donc Q est de la forme $Q = \sum_{k \in \mathbb{N}} \overline{p_k} X^k$,

où (p_k) est une famille presque nulle d'entiers. Ainsi, $Q = \overline{P}$ en posant $P = \sum_{k \in \mathbb{N}} p_k X^k$.

Ceci prouve que le morphisme est surjectif.

◇ p est un polynôme constant non nul de $\mathbb{Z}[X]$, mais $\overline{p} = 0$, donc p est un élément non nul du noyau du morphisme. Ceci prouve que le morphisme n'est pas injectif.

12°) ◇ Lorsque $P = \sum_{k \in \mathbb{N}} p_k X^k \in \mathbb{Z}[X]$ et $\alpha \in \mathbb{Z}$, $\overline{P(\alpha)} = \sum_{k \in \mathbb{N}} \overline{p_k} \overline{\alpha^k} = \overline{P(\overline{\alpha})}$.

Ainsi, si $a = \overline{0}$, alors $\overline{0} = \overline{\Phi_n(a)} = \overline{\Phi_n(\overline{0})} = \overline{\Phi_n(0)}$, donc d'après la question 7, lorsque $n \geq 1$, $\overline{0} = \overline{1}$ et lorsque $n = 1$, $\overline{0} = -\overline{1}$. Ceci est toujours faux. Ainsi $a \neq \overline{0}$.

◇ a est donc un élément du groupe multiplicatif (\mathbb{F}^*, \times) qui est de cardinal $p - 1$, donc d'après le théorème de Lagrange, l'ordre de a , qui correspond au cardinal du groupe multiplicatif engendré par a , est un diviseur de $p - 1$.

13°) ◇ Dans \mathbb{F}_p , $a^\omega = \overline{1}$, donc a est une racine du polynôme $X^\omega - \overline{1}$ de $\mathbb{F}_p[X]$. Mais d'après les questions 4 et 11, $X^\omega - \overline{1} = \prod_{d|\omega} \overline{\Phi_d}$. Ainsi, $\prod_{d|\omega} \overline{\Phi_d}(a) = 0$ or \mathbb{F}_p est un corps

donc il est intègre. Ainsi, il existe $d \in \mathbb{N}^*$ tel que d divise ω et tel que $\overline{\Phi_d}(a) = 0$.

◇ Toujours d'après la question 4, $X^d - 1 = \prod_{e|d} \Phi_e$, donc $a^d - \overline{1} = \overline{\Phi_d}(a) \prod_{\substack{e|d \\ e \neq d}} \overline{\Phi_e}(a) = 0$,

donc $a^d = \overline{1}$, donc d'après la définition de ω , $\omega \leq d$, mais d divise ω , donc $d = \omega$.

14°) Un résultat similaire a été établi en cours, mais seulement dans un corps de caractéristique nulle, ce qui n'est pas le cas ici.

x est une racine de Q , donc d'après le cours, il existe $H \in \mathbb{F}_p[X]$ tel que $Q = (X - x)H$. Alors $Q' = (X - x)H' + H$, donc $Q'(x) = H(x) \neq 0$. Ainsi, x n'est pas une racine de H , ce qui prouve que x est bien une racine simple de Q .

15°) ◇ À nouveau, on a $\overline{\Phi_n}(a) = 0$ et $X^n - 1 = \prod_{d|n} \Phi_d$, donc $a^n = \overline{1}$. Ainsi, a est bien

une racine de $X^n - \overline{1}$.

De plus, $(X^n - 1)'(a) = na^{n-1} = \overline{n} \times a^{n-1}$. Or $a \neq \overline{0}$, donc $a^{n-1} \neq 0$. De plus, $p \wedge n = 1$, donc $\overline{n} \neq 0$, or \mathbb{F}_p est intègre, donc $(X^n - 1)'(a) \neq 0$. Ceci prouve d'après la question précédente que a est une racine simple de $X^n - \overline{1}$.

◇ Supposons que $\omega \neq n$.

D'après le point précédent, $a^n = \overline{1}$, donc d'après le cours, ω est un diviseur strict de n . Alors, toujours d'après la question 4, $X^n - \overline{1} = \overline{\Phi_n} \times \overline{\Phi_\omega} \times \prod_{\substack{d|n \\ d \notin \{\omega, n\}}} \overline{\Phi_d}$, or a est une

racine de $\overline{\Phi_n}$ (par hypothèse) et de $\overline{\Phi_\omega}$ (d'après la question 13), donc a est une racine au moins double de $X^n - \overline{1}$, ce qui est faux. On a donc montré que $\omega = n$.

◇ D'après la question 12, $n = \omega$ divise $p - 1$, donc $p - 1 \equiv 0 [n]$ puis $p \equiv 1 [n]$.

16°) ◇ Supposons d'abord que $n = pq$ où p divise $q = \frac{n}{p}$. Alors, d'après la question 10, $\Phi_n(X) = \Phi_{p \frac{n}{p}}(X) = \Phi_{\frac{n}{p}}(X^p)$, donc $0 = \overline{\Phi_n}(a) = \overline{\Phi_{\frac{n}{p}}}(a^p)$, mais on a vu que $a^{p-1} = \overline{1}$, donc $a^p = a$. Ainsi, $\overline{\Phi_{\frac{n}{p}}}(a) = 0$.

Il reste à montrer cette propriété lorsque $n = pq$ avec $p \wedge q = 1$. Mais dans ce cas, selon la question 10, $\Phi_n(X) = \frac{\Phi_p(X^q)}{\Phi_p(X)}$, donc on a bien $\overline{\Phi_n}(a) = \overline{\Phi_p}(a^q) = \overline{\Phi_p}(a)\overline{\Phi_p}(a) = 0$.

◇ Par récurrence sur w , on montre que si p^w divise n , alors a est une racine de $\overline{\Phi_{\frac{n}{p^w}}}$. Notons v la valuation p -adique de n . Alors $n = p^v m$ où $m \wedge p = 1$. Alors a est une racine de $\overline{\Phi_m}$, donc d'après la question précédente en remplaçant n par $m \in \mathbb{N}^*$, $\omega = m$. On a bien montré que $n = p^v \omega$ où $v \in \mathbb{N}^*$.

◇ D'après la question 12, ω divise $p - 1$, donc $\omega \leq p - 1$, or les diviseurs premiers de n différents de p sont des diviseurs de ω , donc ils sont strictement inférieurs à p . Ainsi, p est le plus grand diviseur premier de n .

17°) Dans \mathbb{F}_p , on a $\overline{0} = \overline{\Phi_n(\alpha)} = \overline{\Phi_n(\bar{\alpha})}$, donc $\bar{\alpha}$ est une racine de Φ_n . On peut donc utiliser les questions précédentes. D'après les questions 16 et 17, si p est premier avec n , alors $p \equiv 1 [n]$ et sinon, alors p est le plus grand diviseur premier de n .

18°) ◇ Posons $\Phi_n(X) = \sum_{h \in \mathbb{N}} p_h X^h \in \mathbb{Z}[X]$. Alors, $\Phi_n(A) = \sum_{h \in \mathbb{N}} p_h A^h \equiv p_0 [A]$, or

$p_0 = \Phi_n(0) = 1$, car $n \geq 2$, donc $\Phi_n(A) \equiv 1 [A]$. Ainsi, dans $\mathbb{Z}/A\mathbb{Z}$, $\overline{\Phi_n(A)} = \bar{1}$ est inversible, donc d'après le cours, $\Phi_n(A)$ et A sont premiers entre eux.

◇ $\deg(\Phi_n) = \varphi_n \geq 1$, car $1 \wedge n = 1$ et Φ_n est unitaire, donc $\Phi_n(t) \xrightarrow[t \rightarrow +\infty]{} +\infty$. Ainsi, quitte à choisir N suffisamment grand, on peut supposer que $\Phi_n(A) \geq 2$. Alors il existe $p \in \mathbb{P}$ tel que p divise $\Phi_n(A)$.

D'après la question précédente, $p \equiv 1 [n]$ ou p est un diviseur de n . Dans le premier cas, il existe $i \in \mathbb{N}_k$ tel que $p = p_i$, donc p divise $A = N \prod_{j=1}^k p_j$, mais c'est encore vrai

dans le second cas car N est un multiple de n . Ainsi p est un diviseur commun de $\Phi_n(A)$ et de A , ce qui est impossible car ils sont premiers entre eux.

Il existe donc une infinité de nombres premiers congrus à 1 modulo n .

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

19°) Soit $x \in \mathbb{F}_p$. Lorsque $x \neq 0$, on a déjà vu que $x^{p-1} = 1$, donc $x^p = x$. Lorsque $x = 0$, on a aussi $x^p = 0 = x$, donc les éléments de \mathbb{F}_p sont tous des racines de $X^p - X$, or \mathbb{F}_p est de cardinal p et $X^p - X$ est de degré p , donc on a déjà toutes les racines de $X^p - X$, qui sont d'ailleurs simples. On a bien montré que $\boxed{\text{Rac}_{\mathbb{K}}(X^p - X) = \mathbb{F}_p}$.

20°) ◇ La question 14 est en fait valable dans n'importe quel corps, donc également dans $\mathbb{K}[X]$. Soit $a \in \text{Rac}_{\mathbb{K}}(X^n - 1)$. Alors $a^n = 1$, donc $a \neq 0$.

De plus, $(X^n - 1)'(a) = (n1_{\mathbb{K}})a^{n-1}$, mais $\mathbb{F} \subset \mathbb{K}$, donc $1_{\mathbb{K}} = 1_{\mathbb{F}_p} = \bar{1}$, or $n \wedge p = 1$, donc $n1_{\mathbb{K}} = \bar{n} \neq 0$. On en déduit que $(X^n - 1)'(a) \neq 0$, donc que a est une racine simple de $X^n - 1$. Ainsi, $X^n - 1$ est simplement scindé dans $\mathbb{K}[X]$, donc il en est de même de tout polynôme qui divise $X^n - 1$, ce qui est le cas de $\overline{\Phi_n}$, car on a toujours, dans

$$\mathbb{F}_p[X], X^n - 1 = \prod_{d|n} \overline{\Phi_d}.$$

◇ Pour montrer que $\overline{\Phi_n}(X) = \prod_{\substack{a \in \mathbb{K} \setminus \{0\} \\ \text{tq } \text{ord}(a) = n}} (X - a)$, il suffit donc

de montrer que $\text{Rac}_{\mathbb{K}}(\overline{\Phi_n}) = \{a \in \mathbb{K} \setminus \{0\} \mid \text{ord}(a) = n\}$.

Supposons que $a \in \mathbb{K} \setminus \{0\}$ avec $\text{ord}(a) = n$. Alors $a^n = 1_{\mathbb{K}}$, donc a est racine de $X^n - 1 = \prod_{d|n} \overline{\Phi_d}$. Ainsi, il existe $d \in \mathbb{N}^*$ tel que $d|n$ et tel que a est racine de $\overline{\Phi_d}$. Mais

$$X^d - 1 = \prod_{e|d} \overline{\Phi_e}, \text{ donc } a^d = 1_{\mathbb{K}}. \text{ Par définition de l'ordre de } a, d \geq n, \text{ or } d|n, \text{ donc}$$

$d = n$. Ainsi, a est bien une racine de $\overline{\Phi_n}$.

Réciproquement, supposons que a est une racine de $\overline{\Phi_n}$ dans \mathbb{K} . Alors $a^n = 1_{\mathbb{K}}$, donc $\text{ord}(a)$ divise n . Si $\text{ord}(a) \neq n$, on peut reprendre le même raisonnement qu'en question 15, en posant $\omega = \text{ord}(a)$, pour aboutir à une contradiction. Ainsi $\text{ord}(a) = n$.

21°) Cette propriété résulte de la formule du binôme de Newton et de la symétrie des coefficients binomiaux $\binom{k}{\ell} = \binom{k}{k-\ell}$ mais sa mise en oeuvre précise est laborieuse, on préfère une simple récurrence.

Soit $k \in \mathbb{N}^*$. Posons $R(k)$ l'assertion suivante : il existe $(b_0, \dots, b_k) \in \mathbb{Z}^{k+1}$ tel que

$$\left(X + \frac{1}{X}\right)^k = b_0 + \sum_{\ell=1}^k b_{\ell} \left(X^{\ell} + \frac{1}{X^{\ell}}\right), \text{ avec } b_k = 1.$$

$R(1)$ est évidente. Supposons que $R(k)$ est vraie et montrons $R(k+1)$.

$$\left(X + \frac{1}{X}\right)^{k+1} = \left(X + \frac{1}{X}\right)^k \left(X + \frac{1}{X}\right), \text{ donc d'après l'hypothèse de récurrence,}$$

$$\left(X + \frac{1}{X}\right)^{k+1} = b_0 \left(X + \frac{1}{X}\right) + \sum_{\ell=1}^k b_{\ell} \left(X^{\ell} + \frac{1}{X^{\ell}}\right) \left(X + \frac{1}{X}\right). \text{ Ainsi,}$$

$$\begin{aligned} \left(X + \frac{1}{X}\right)^{k+1} &= b_0 \left(X + \frac{1}{X}\right) + \sum_{\ell=1}^k b_{\ell} \left(X^{\ell+1} + \frac{1}{X^{\ell+1}} + X^{\ell-1} + \frac{1}{X^{\ell-1}}\right) \\ &= b_0 \left(X + \frac{1}{X}\right) + \sum_{\ell=2}^{k+1} b_{\ell-1} \left(X^{\ell} + \frac{1}{X^{\ell}}\right) + \sum_{\ell=0}^{k-1} b_{\ell+1} \left(X^{\ell} + \frac{1}{X^{\ell}}\right), \text{ puis} \end{aligned}$$

en convenant que $b_{\ell} = 0$ pour tout $\ell \in \mathbb{Z} \setminus \{0, \dots, k\}$, on peut écrire

$$\left(X + \frac{1}{X}\right)^{k+1} = \sum_{\ell=0}^{k+1} b_{\ell-1} \left(X^{\ell} + \frac{1}{X^{\ell}}\right) + \sum_{\ell=0}^{k+1} b_{\ell+1} \left(X^{\ell} + \frac{1}{X^{\ell}}\right) = \sum_{\ell=0}^{k+1} (b_{\ell-1} + b_{\ell+1}) \left(X^{\ell} + \frac{1}{X^{\ell}}\right).$$

$$\text{Ainsi, } \left(X + \frac{1}{X}\right)^{k+1} = c_0 + \sum_{\ell=1}^{k+1} c_{\ell} \left(X^{\ell} + \frac{1}{X^{\ell}}\right), \text{ en posant}$$

$c_0 = 2b_1 \in \mathbb{Z}$, et pour tout $\ell \in \{1, \dots, k+1\}$, $c_{\ell} = b_{\ell-1} + b_{\ell+1} \in \mathbb{Z}$. En particulier, $c_{k+1} = b_k = 1$, donc on a prouvé $R(k+1)$.

22°) ◇ On raisonne par récurrence sur k . Notons $R(k)$ l'assertion suivante :

Pour tout $(a_0, \dots, a_k) \in \mathbb{Z}^{k+1}$, il existe $Q \in \mathbb{Z}[X]$ avec $\deg(Q) \leq k$

tel que $a_0 + \sum_{\ell=1}^k a_\ell \left(X^\ell + \frac{1}{X^\ell} \right) = Q \left(X + \frac{1}{X} \right)$ et tel que $\deg(Q) = k$ si $a_k \neq 0$.

Pour $k = 0$: soit $a_0 \in \mathbb{Z}^*$. Notons Q le polynôme constant égal à a_0 .

Alors $a_0 = Q \left(X + \frac{1}{X} \right)$, ce qui prouve $R(0)$.

Supposons que $k \geq 1$ et que $R(k-1)$ est vrai. Soit $(a_0, \dots, a_k) \in \mathbb{Z}^{k+1}$.

Alors, avec les notations de la question précédente,

$a_0 + \sum_{\ell=1}^k a_\ell \left(X^\ell + \frac{1}{X^\ell} \right) - a_k \left(X + \frac{1}{X} \right)^k = a_0 - a_k b_0 + \sum_{\ell=1}^k (a_\ell - a_k b_\ell) \left(X^\ell + \frac{1}{X^\ell} \right)$, mais

$a_k - a_k b_k = a_k - a_k = 0$, donc d'après $R(k-1)$, il existe $H \in \mathbb{Z}[X]$ avec $\deg(H) \leq k-1$ tel

que $a_0 + \sum_{\ell=1}^k a_\ell \left(X^\ell + \frac{1}{X^\ell} \right) - a_k \left(X + \frac{1}{X} \right)^k = H \left(X + \frac{1}{X} \right)$. Ainsi, en posant $Q = H + a_k X^k$,

on a $a_0 + \sum_{\ell=1}^k a_\ell \left(X^\ell + \frac{1}{X^\ell} \right) = Q \left(X + \frac{1}{X} \right)$ et $\deg(Q) \leq k$. De plus, si $a_k \neq 0$, alors $\deg(Q) = k$. On a prouvé $R(k)$.

◇ Soit $P \in \mathbb{Z}[X]$ tel que $\deg(P) = 2k$ et $X^{2k} P \left(\frac{1}{X} \right) = P(X)$.

Notons $P(X) = \sum_{\ell=0}^{2k} p_\ell X^\ell$. Par hypothèse, $\sum_{\ell=0}^{2k} p_\ell X^\ell = \sum_{\ell=0}^{2k} p_\ell X^{2k-\ell}$, donc en posant

$h = 2k - \ell$, on obtient que $\sum_{\ell=0}^{2k} p_\ell X^\ell = \sum_{h=0}^{2k} p_{2k-h} X^h$.

Ainsi, pour tout $\ell \in \{0, \dots, 2k\}$, $p_\ell = p_{2k-\ell}$.

Alors $P(X) = p_k X^k + \sum_{\ell=k+1}^{2k} p_\ell X^\ell + \sum_{\ell=0}^{k-1} p_{2k-\ell} X^\ell = p_k X^k + \sum_{\ell=k+1}^{2k} p_\ell X^\ell + \sum_{h=k+1}^{2k} p_h X^{2k-h}$,

donc $\frac{1}{X^k} P(X) = p_k + \sum_{h=k+1}^{2k} p_h \left(X^{h-k} + \frac{1}{X^{h-k}} \right) = p_k + \sum_{\ell=0}^k p_{\ell+k} \left(X^\ell + \frac{1}{X^\ell} \right)$.

$\deg(P) = 2k$, donc $p_{2k} \neq 0$, donc d'après le point précédent, il existe $Q \in \mathbb{Z}[X]$ avec $\deg(Q) = k$ tel que $\frac{1}{X^k} P(X) = Q \left(X + \frac{1}{X} \right)$, ce qu'il fallait démontrer.

23°) 1 est premier avec n , donc $1 \in \mathbb{P}(n)$, ce qui prouve que $\varphi(n) \geq 1$.

Soit $k \in \mathbb{N}_n$. Si d est un diviseur commun de k et de n , $d|(n-k)$, donc d est un diviseur commun de k et $n-k$. La réciproque s'obtient par un raisonnement similaire, donc k est premier avec n si et seulement si $n-k$ est premier avec n .

Lorsque $(h, k) \in \mathbb{P}(n)$, convenons que $h R k \iff (h = k) \vee (h = n - k)$. On définit ainsi une relation d'équivalence sur $\mathbb{P}(n)$ dont les classes d'équivalence sont les $\{k, n - k\}$ avec $k \in \mathbb{P}(n)$.

$k = n - k \iff n = 2k$, mais si $n = 2k$, comme $n \geq 3$, alors $n \geq 4$ donc $k \geq 2$ et $k = k \wedge n \neq 1$, donc lorsque $n - k = k$, $k \notin \mathbb{P}(n)$. Ainsi, toutes les classes d'équivalence

sont de cardinal 2, or $\mathbb{P}(n)$ est la réunion disjointe de ses classes d'équivalence, donc son cardinal $\varphi(n)$ est pair.

24°) D'après la question 22, il suffit de montrer que $X^{\varphi(n)}\Phi_n\left(\frac{1}{X}\right) = \Phi_n$.

Or $\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} (X - e^{2i\pi \frac{k}{n}})$, donc

$$X^{\varphi(n)}\Phi_n\left(\frac{1}{X}\right) = X^{\varphi(n)} \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} \left(\frac{1}{X} - e^{2i\pi \frac{k}{n}}\right) = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} (1 - Xe^{2i\pi \frac{k}{n}}) = \alpha \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} (X - e^{-2i\pi \frac{k}{n}}),$$

où α désigne le coefficient dominant de ce polynôme. Or ce coefficient dominant vaut $\Phi_n(0) = 1$, donc $X^{\varphi(n)}\Phi_n\left(\frac{1}{X}\right) = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} (X - e^{2i\pi \frac{n-k}{n}}) = \Phi_n$, car on a vu lors de la question précédente que $\mathbb{P}(n) = \{n - k / k \in \mathbb{P}(n)\}$.

25°) \diamond D'après la formule du binôme de Newton, $\beta^p = \sum_{h=0}^p \binom{p}{h} \omega^{p-h} \omega^{-h}$.

Soit $h \in \{1, \dots, p-1\}$. Alors p divise le produit non vide (car $h \geq 1$)

$p(p-1) \cdots (p-h+1) = \binom{p}{h} h!$, or $p \wedge h! = 1$ (car $h \leq p-1$), donc d'après le lemme

de Gauss, p divise $\binom{p}{h}$. Ainsi, $\binom{p}{h} 1_{\mathbb{K}} = \binom{p}{h} \bar{1} = \bar{0}$ dans \mathbb{F}_p . On peut donc ne retenir dans la somme précédente que les termes d'indice $h \in \{0, p\}$, ce qui prouve que $\beta^p = \omega^p + \frac{1}{\omega^p}$.

\diamond Ainsi, $\beta^p = \beta \iff \omega^p + \frac{1}{\omega^p} = \omega + \frac{1}{\omega} \iff \omega^{2p} - \omega^{p+1} - \omega^{p-1} + 1 = 0$, puis

$\beta^p = 0 \iff \omega^{p+1}(\omega^{p-1} - 1) - (\omega^{p-1} - 1) = 0 \iff (\omega^{p-1} - 1)(\omega^{p+1} - 1) = 0$, or \mathbb{K} est intègre, donc $\beta^p = 0 \iff (\omega^{p-1} = 1) \vee (\omega^{p+1} = 1) \iff (\omega^p = \omega) \vee (\omega^p = \omega^{-1})$.

\diamond Soit $\gamma \in \text{Rac}_{\mathbb{K}}(\overline{\Psi_n})$. Par hypothèse sur le corps \mathbb{K} , le polynôme $X^2 - X\gamma + 1$ possède au moins une racine, notée ω , nécessairement non nulle. Alors $\omega^2 - \omega\gamma + 1 = 0$, donc $\gamma = \omega + \frac{1}{\omega}$. D'après la question 19,

$\gamma \in \mathbb{F}_p \iff \gamma^p = \gamma$, donc d'après le point précédent,

$\gamma \in \mathbb{F}_p \iff (\omega^{p-1} = 1) \vee (\omega^{p+1} = 1)$.

Par ailleurs, $0 = \overline{\Psi_n}(\gamma) = \overline{\Psi_n}(\omega + \frac{1}{\omega})$. Or $X^{\frac{\varphi(n)}{2}}\Psi_n\left(X + \frac{1}{X}\right) = \Phi_n(X)$.

On voudrait en déduire que $\overline{\Phi_n}(\omega) = 0$, mais le passage modulo p puis la substitution de X par ω n'est pas acquis car il s'agit de fractions rationnelles. On va le faire en se ramenant à des polynômes.

Posons $m = \frac{\varphi(n)}{2}$ et $\Psi_n(X) = \sum_{h=0}^m p_h X^h$.

On a $\Phi_n(X) = X^m \sum_{h=0}^m p_h \left(X + \frac{1}{X}\right)^h = \sum_{h=0}^m p_h X^{m-h} (X^2 + 1)^h$, donc d'après la question

11, $\overline{\Phi}_n(X) = \sum_{h=0}^m \overline{p_h} X^{m-h} (X^2 + 1)^h = \sum_{h=0}^m \overline{p_h} X^{m-h} (X^2 + \overline{1})^h$. C'est une égalité dans $\mathbb{K}[X]$, dans laquelle on peut donc remplacer X par ω .

On obtient que $\overline{\Phi}_n(\omega) = \sum_{h=0}^m \overline{p_h} \omega^{m-h} (\omega^2 + \overline{1})^h = \omega^m \sum_{h=0}^m \overline{p_h} \left(\omega + \frac{1}{\omega}\right)^h = \omega^m \overline{\Psi}_n\left(\omega + \frac{1}{\omega}\right)$.

Ainsi, ω est une racine de $\overline{\Phi}_n$.

D'après la question 20, ω est d'ordre n , donc d'après le cours,

$$\gamma \in \mathbb{F}_p \iff (n|(p-1)) \vee (n|(p+1)) \iff p \equiv \pm 1 [n].$$

26°) a) Supposons que $\Psi_n(0) = 0$. Posons $\omega = i$. Ainsi, $\omega^2 = -1$, donc $0 = \omega + \frac{1}{\omega}$.

Alors $0 = \Psi_n(0) = \Psi_n(\omega + \frac{1}{\omega}) = \frac{\Phi_n(\omega)}{\omega^{\frac{1}{2}\varphi(n)}}$, donc i est une racine de Φ_n , donc i est d'ordre n (on peut par exemple le démontrer en adaptant ce qui a été dit en seconde partie de question 20), or i est d'ordre 4, donc $n = 4$, ce qui est faux.

26.b) Posons $\Psi_n = \sum_{h \in \mathbb{N}} p_h X^h$, où (p_h) est une famille presque nulle d'entiers relatifs.

Alors $\Theta = \frac{1}{a} \sum_{h \in \mathbb{N}} p_h (aX)^h = \frac{p_0}{a} + \sum_{h \geq 1} p_h a^{h-1} X^h$, or $a = \Psi_n(0) = p_0 \in \mathbb{Z}$,

donc $\Theta = 1 + \sum_{h \geq 1} p_h a^{h-1} X^h \in \mathbb{Z}[X]$.

26.c) Soit $z \in \mathbb{C}^*$. Il existe $\omega \in \mathbb{C}^*$ tel que $z = \omega + \frac{1}{\omega}$.

Alors $\Psi_n(z) = 0 \iff \Phi_n(\omega) = 0 \iff \exists k \in \mathbb{P}(n), \omega = e^{2i\pi \frac{k}{n}},$ donc les racines de Ψ_n sont les $e^{2i\pi \frac{k}{n}} + e^{-2i\pi \frac{k}{n}} = 2 \cos(2\pi \frac{k}{n})$, où k décrit $\mathbb{P}(n)$.

Soit $h, k \in \mathbb{P}(n)$. Alors $2\pi \frac{k}{n}$ et $2\pi \frac{h}{n}$ sont dans $]0, 2\pi]$, donc $\cos(2\pi \frac{k}{n}) = \cos(2\pi \frac{h}{n}) \iff (2\pi \frac{k}{n} = 2\pi \frac{h}{n}) \vee (2\pi \frac{k}{n} = 2\pi - 2\pi \frac{h}{n}) \iff (k = h) \vee (k = n - h)$. Le nombre de racines de Ψ_n est donc égal au nombre de classes d'équivalence de la relation d'équivalence définie en question 23, c'est-à-dire à $\frac{1}{2}\varphi(n)$. C'est égal au degré de Ψ_n , donc Ψ_n est simplement scindé dans $\mathbb{R}[X]$.

$a \in \mathbb{Z}^*$, donc les racines de Θ sont les $\frac{1}{a} \cos(2\pi \frac{k}{n})$. Elles sont réelles et Θ est comme Ψ_n simplement scindé dans $\mathbb{R}[X]$.

26.d) On a vu que $\varphi(n)$ est pair et non nul, donc $\deg(\Theta) = \frac{1}{2}\varphi(n) \geq 1$. Ainsi, d'après la question précédente, Θ possède au moins une racine réelle, notée r et cette dernière est simple. Ainsi, au voisinage de r , $\Theta(t) \sim \lambda(t - r)$, où $\lambda \in \mathbb{R}^*$, donc il existe $\varepsilon > 0$ tel que $\Theta(t)$ est strictement négatif lorsque $t \in]r - \varepsilon, r[$ ou bien lorsque $t \in]r, r + \varepsilon[$. Il existe donc bien $\alpha, \beta \in \mathbb{R}$ avec $\alpha < \beta$ tels que pour tout $t \in [\alpha, \beta]$, $\Theta(t) < 0$.

26.e) Posons $s = np_1 \cdots p_k \in \mathbb{N}^*$.

$\frac{s}{p_0^\ell} \xrightarrow{\ell \rightarrow +\infty} 0$, donc il existe $\ell \in \mathbb{N}^*$ tel que $\frac{s}{p_0^\ell} < \beta - \alpha$.

Posons $m = \left\lfloor \frac{\beta p_0^\ell}{s} \right\rfloor \in \mathbb{Z}$. Alors $m \leq \frac{\beta p_0^\ell}{s} \leq m + 1$,

donc $\frac{ms}{p_0^\ell} \leq \beta \leq \frac{ms}{p_0^\ell} + \frac{s}{p_0^\ell} \leq \frac{ms}{p_0^\ell} + \beta - \alpha$. On en déduit que $\alpha \leq \frac{ms}{p_0^\ell} \leq \beta$, donc que

$$\Theta\left(\frac{m}{p_0^\ell} np_1 \cdots p_k\right) < 0.$$

f) On sait que Θ est de degré $d = \frac{1}{2}\varphi(n)$. Posons $\Theta = \sum_{h=0}^d t_h X^h \in \mathbb{Z}[X]$.

Posons à nouveau $s = np_1 \cdots p_k \in \mathbb{N}^*$.

$$\text{Alors } p_0^{\frac{1}{2}\varphi(n)\ell} \Theta\left(\frac{m}{p_0^\ell} np_1 \cdots p_k\right) = p_0^{d\ell} \sum_{h=0}^d t_h \left(\frac{m}{p_0^\ell} s\right)^h = \sum_{h=0}^d t_h p_0^{\ell(d-h)} (ms)^h \in \mathbb{Z}.$$

D'après cette expression, modulo s , $p_0^{\frac{1}{2}\varphi(n)\ell} \Theta\left(\frac{m}{p_0^\ell} np_1 \cdots p_k\right)$ est congru à $t_0 p_0^{\ell d}$,

or $t_0 = \Theta(0) = 1$ (cf la dernière égalité de la solution du b)) et $p_0 \equiv 1 [s]$ par hypothèse, donc $p_0^{\frac{1}{2}\varphi(n)\ell} \Theta\left(\frac{m}{p_0^\ell} np_1 \cdots p_k\right)$ est congru à 1 modulo $np_1 \cdots p_k$.

g) Soit p un diviseur premier de $p_0^{\frac{1}{2}\varphi(n)\ell} \Theta\left(\frac{m}{p_0^\ell} np_1 \cdots p_k\right)$ distinct de p_0 .

D'après le dernier résultat de f), $p_0^{\frac{1}{2}\varphi(n)\ell} \Theta\left(\frac{m}{p_0^\ell} np_1 \cdots p_k\right)$ est premier avec $np_1 \cdots p_k$, donc p est distinct de p_1, \dots, p_k et $p \wedge n = 1$.

Dans \mathbb{F}_p , en reprenant les notations de la question f), on a $0 = \sum_{h=0}^d \overline{t_h} \overline{p_0}^{\ell(d-h)} \overline{ms}^h$.

Mais $p \wedge p_0 = 1$, car p et p_0 sont deux nombres premiers distincts, donc il existe $q_0 \in \mathbb{Z}$ tel que $(\overline{p_0})^{-1} = \overline{q_0}$. Alors, en simplifiant par $\overline{p_0}^{\ell d}$, on obtient que $0 = \sum_{h=0}^d \overline{t_h} \overline{q_0}^{\ell h} \overline{ms}^h$, donc

$\overline{\Theta}(q_0^\ell \overline{ms}) = 0$. Or $a\Theta = \Psi_n(aX)$, donc $\overline{a}\overline{\Theta} = \overline{\Psi_n}(\overline{a}X)$. On en déduit que $\overline{\Psi_n}(\overline{a}\overline{ms}q_0^\ell) = 0$, donc $\overline{\Psi_n}$ possède une racine dans \mathbb{F}_p . D'après la question 25, sachant que $p \wedge n = 1$, $p \equiv \pm 1 [n]$, or p est distinct de p_1, \dots, p_k , donc $p \equiv 1 [n]$. On a aussi $p_0 \equiv 1 [n]$, donc tous les diviseurs premiers de $L = p_0^{\frac{1}{2}\varphi(n)\ell} \Theta\left(\frac{m}{p_0^\ell} np_1 \cdots p_k\right)$ sont congrus à 1 modulo n . On en déduit que $|L| \equiv 1 [n]$, mais d'après la question e), $L < 0$, donc $L = -|L| \equiv -1 [n]$, or d'après la question f), $L \equiv 1 [n]$. On aboutit à une contradiction, ce qui termine le problème.