Devoir surveillé n°7

Sujet donné le vendredi 11 février 2022, 4h.

L'usage de la calculatrice n'est pas autorisé.

La notation tiendra particulièrement compte de **la qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisées. Les réponses aux questions seront numérotées et séparées par un trait horizontal. Les résultats essentiels devront être encadrés ou soulignés.**

BON TRAVAIL

Problème - Autour des polynômes Cyclotomiques

Pour un entier naturel n donné, on note :

- $G_n = X^n - 1$ (en hommage au grand Gauss) ;
- $\mathbb{U}_n = \mathcal{Z}_{G_n}$, l'ensemble des zéros de G_n, c'est-à-dire l'ensemble des racines n-ième de l'unité ;
- $\mathbb{V}_n = \{z \in \mathbb{U}_n \mid \forall\, r \in [\![1, n-1]\!], z^r \neq 1\}$, ce sont les racines primitives n-ième de l'unité ;
- $\varphi(n) = \text{card}(\mathbb{V}_n)$ et $\Phi_n = \prod_{z \in \mathbb{V}_n} (X - z)$ ($\leftarrow$ *ce sont eux les polynômes cylcotomiques*).

I - Factorisation dans $\mathbb{Z}[X]$

On considère un nombre premier p et $P, Q \in \mathbb{Z}[X]$, deux polynômes à coefficients entiers.

I.1. Redonner, pour tout $n \in \mathbb{Z}$, l'expression de $[P \times Q]_n$, en fonction des nombres $([P]_i)_{0 \leqslant i \leqslant n}$ et $([Q]_j)_{0 \leqslant j \leqslant n}$.

I.2. On va montrer, par contraposée, l'implication : $(\forall\, n \in \mathbb{N},\ p | [PQ]_n) \Longrightarrow (\forall\, n \in \mathbb{N},\ p | [P]_n$ ou $\forall\, n \in \mathbb{N},\ p | [Q]_n)$.

(a) Supposons donc que $\{n$ tel que $p \nmid [P]_n\}$ et $\{n$ tel que $p \nmid [Q]_n\}$ sont non vides (et inclus dans $\mathbb{N}$).
Soient $m = \min\{n$ tel que $p \nmid [P]_n\}$ et $m' = \min\{n$ tel que $p \nmid [Q]_n\}$. Montrer que p ne divise pas $[PQ]_{m+m'}$

(b) Conclure.

I.3. On note, pour $R \in \mathbb{Z}[X]^*$, $c(R) = \bigwedge_{k=0}^{\deg R} [R]_k$ (PGCD des coefficients de R), appelé « contenu de R »(et $c(0) = 0$).

Par exemple, $c(2X^3 + 4X - 6) = 2 \wedge 0 \wedge 4 \wedge 6 = 2$ ou $c(6X^4 + 10X^2 - 15X) = 6 \wedge 0 \wedge 10 \wedge 0 \wedge 15 = 1$.

(a) Montrer que $P_1 := \dfrac{P}{c(P)}$ est un polynôme à coefficients entiers, puis que $c(P_1) = 1$.

(b) En exploitant la question 2., et les polynômes P_1 et Q_1, montrer que $c(P \times Q) = c(P) \times c(Q)$

I.4. Soit $R \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$. Montrer que R est irréductible dans $\mathbb{Z}[X]$ ssi R est irréductible dans $\mathbb{Q}[X]$.

I.5. Soit p un nombre premier et $R = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. On note $\overline{R} = \sum_{k=0}^{n} \overline{a_k} X^k$ (avec $\overline{a_k} = a_k \% p$).

Montrer que $\overline{R}(X^p) = (\overline{R}(X))^p$. *On pourra raisonner par récurrence forte sur $n = \deg R$.*

II - Décomposition des polynômes G_n

II.1. Effectuer, *en parallèle*, l'algorithme d'Euclide pour les nombres 14 et 3 et pour les polynômes G_{14} et G_3.
Donner un couple d'entiers (u, v) et un couple de polynômes (U, V) tels que $14u+3v = 1$ et $G_{14} \times U + G_3 \times V = G_1$.

II.2. Montrer que pour tous entiers $m > n \geqslant 1$, $G_m \wedge G_n = G_{m \wedge n}$

II.3. Factoriser G_3 et G_4 sur $\mathbb{C}[X]$, puis sur $\mathbb{R}[X]$.

II.4. Factoriser G_n sur $\mathbb{R}[X]$. On notera, pour $1 \leqslant k \leqslant n$, $c_{k,n} = \cos \dfrac{2k\pi}{n}$.

Soit $n \in \mathbb{N}$, fixé. On cherche à factoriser G_n en produit de polynômes de $\mathbb{Q}[X]$ (donc de $\mathbb{Z}[X]$) (questions 5 et 6).

II.5. On commence par trouver une factorisation

(a) On note, pour tout $k \in \mathbb{N}$, $z_k = e^{\frac{2ik\pi}{n}}$. On sait que $\mathbb{U}_n = \{z_k; k \in [\![1, n]\!]\}$.
Montrer que $z_k \in \mathbb{V}_n \iff \exists\ u \in \mathbb{Z}$ tel que $(z_k)^u = z_1 \iff k \wedge n = 1$.

(b) Montrer que $\mathbb{U}_n = \uplus_{d|n} \mathbb{V}_d$.
Donner la description des éléments de $\mathbb{U}_{12}$ regroupés selon les $\mathbb{V}_k$ auxquels ils appartiennent.

(c) Déduire de la réunion disjointe précédente, que $G_n = \prod_{d|n} \Phi_d$. Que vaut Φ_{12} ?

(d) Montrer, par récurrence forte sur $m \in \mathbb{N}^*$ que $\Phi_m \in \mathbb{Z}[X]$ et est unitaire.

(e) Quel est le de degré de Φ_m ? En déduire la valeur de $\sum_{d|n} \varphi(d)$, en fonction de n.

II.6. On démontre maintenant qu'il n'y a pas d'autres factorisations dans $\mathbb{Z}[X]$, ie que Φ_n est irréductible.

Supposons pour cela que $\Phi_n = \lambda \prod_{i=1}^{r} P_i$ où chaque P_r est un polynôme irréductible et unitaire de $\mathbb{Q}[X]$ et $\lambda \in \mathbb{Q}$.

(a) Montrer que $\lambda = 1$.

(b) Soit z une racine de P_1 et p premier tel que $p \nmid n$. Montrer qu'il existe i tel que $P_i(z^p) = 0$.

(c) Montrer que $\overline{\Phi_n}$ (défini en I.5) n'est divisible par le carré d'aucun polynôme non constant dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$.
Par l'absurde, on montrer qu'il existe Q tel que $\overline{Q}|\overline{G_n}$ et $\overline{Q}|\overline{G'_n}$ puis $\overline{Q}|X\overline{G'_n} - \overline{n}\overline{G_n}$...

(d) (**) Montrer que $i = 1$, i.e. $P_1(z^p) = 0$, puis que pour tout k entier, premier avec n, $P_1(z^k) = 0$.

(e) Conclure

III - Application pour la résolution d'un problème diophantien

Soit p et q deux nombres premiers vérifiant $3 \leqslant p < q$. On note $< p, q >= \{mp + nq, m, n \in \mathbb{N}\}$.
Soulignons, que les nombres m et n sont des entiers naturels et non des entiers relatifs.

III.1. Montrer que tout nombre entier $R \geqslant (p-1)(q-1)$ appartient à $< p, q >$.

III.2. Le nombre $(p-1)(q-1) - 1$ appartient-il à $< p, q >$?

III.3. On définit les polynômes $H = \sum_{s \in \mathbb{N} \setminus < p,q >} X^s$ et $K = 1 + (X-1)H(X)$, qui sont donc à coefficients entiers.

(a) Quels sont les degré de H et de K ?

(b) Calculer K pour le choix $(p, q) = (3, 5)$.

III.4. Considérons deux polynômes $S, T \in \mathbb{Z}[X]$ tel que pour tout $k \in \mathbb{N}$, $[S]_k \in \{0, 1\}$ et $T = (X-1)S$

(a) Exprimer pour tout $k \in \mathbb{N}$, $[T]_k$ en fonction des coefficients de S. En déduire que $[T]_k \in \{-1, 0, 1\}$.

(b) Soient $k_1 < k_2 \in \mathbb{N}$ tel que $[T]_{k_1} \neq 0$, $[T]_{k_2} \neq 0$ et pour tout $k \in [\![k_1 + 1, k_2 - 1]\!]$, $[T]_k = 0$.
Montrer que $[T]_{k_1} \times [T]_{k_2} = -1$.

(c) En déduire que K n'a que des coefficients égaux à -1, 0 ou 1 et que les 1 et -1 s'alternent dans la suite des coefficients (il ne peut y avoir que des zéros comme coefficient entre ces nombres).

On admet (raisonnement combinatoire) que

$$G_p \times G_q \times K = G_{pq} \times G_1$$

III.5. Quelles sont les racines de K, avec quelle multiplicité ?

III.6. D'après la question II.1., il existe $\alpha, \beta \in \mathbb{N}$ tel que $pq + 1 = \alpha p + \beta q$.

(a) Vérifier que $1 \leqslant \alpha \leqslant q - 1$ et $1 \leqslant \beta \leqslant p - 1$.

(b) Montrer la formule :

$$K = \left(\sum_{i=0}^{\alpha-1} X^{ip}\right) \times \left(\sum_{j=0}^{\beta-1} X^{jq}\right) - X^{-pq} \left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \times \left(\sum_{j=\beta}^{p-1} X^{jq}\right).$$

(c) Montrer que le nombre N de coefficients non nuls $[K]_j$ de K est égal à $2\alpha\beta - 1$.

(d) En déduire que $N \leqslant \frac{pq-1}{2}$.

On pourra commencer par montrer que N est inférieur à $\frac{p^2q^2+1}{2pq}$.

Correction

Problème - Autour des polynômes Cyclotomiques

I - Factorisation dans $\mathbb{Z}[X]$

On considère un nombre premier p et $P, Q \in \mathbb{Z}[X]$, deux polynômes à coefficients entiers.

I.1. Redonner, pour tout $n \in \mathbb{Z}$, l'expression de $[P \times Q]_n$, en fonction des nombres $([P]_i)_{0 \leqslant i \leqslant n}$ et $([Q]_j)_{0 \leqslant j \leqslant n}$.

Formule du cours. Elle marche même pour $n \geqslant \deg P + \deg Q \ldots$: /1

$$\boxed{\forall\, n \in \mathbb{N}, [P \times Q]_n = \sum_{i=0}^{n} [P]_i \times [Q]_{n-i} = \sum_{i+j=n}^{n} [P]_i \times [Q]_j}$$

I.2. On va montrer, par contraposée, l'implication : ($\forall\, n \in \mathbb{N}$, $p | [PQ]_n$) $\Longrightarrow$ ($\forall\, n \in \mathbb{N}$, $p | [P]_n$ ou $\forall\, n \in \mathbb{N}$, $p | [Q]_n$).

(a) Supposons donc que $\{n$ tel que $p \nmid [P]_n\}$ et $\{n$ tel que $p \nmid [Q]_n\}$ sont non vides (et inclus dans $\mathbb{N}$).
Soient $m = \min\{n$ tel que $p \nmid [P]_n\}$ et $m' = \min\{n$ tel que $p \nmid [Q]_n\}$. Montrer que p ne divise pas $[PQ]_{m+m'}$

D'après la formule précédente, en séparant la somme en trois parties :

$$[PQ]_{m+m'} = \sum_{i=0}^{m+m'} [P]_i [Q]_{m+m'-i} = \sum_{i=0}^{m-1} [P]_i [Q]_{m+m'-i} + [P]_m [Q]_{m'} + \sum_{i=m+1}^{m+m'} [P]_i [Q]_{m+m'-i}$$

Or, pour tout $i \leqslant m-1$, $p | [P]_i$. Donc , par combinaison linéaire entière : $p \Big| \sum_{i=0}^{m-1} [P]_i [Q]_{m+m'-i}$.

Et, pour tout $i \geqslant m+1$, $m + m' - i \leqslant m' - 1$, donc $p | [Q]_{m+m'-i}$, par définition de m'.

Donc , par combinaison linéaire entière : $p \Big| \sum_{i=m+1}^{m+m'} [P]_i [Q]_{m+m'-i}$.

Donc $p | [PQ]_{m+m'}$ si et seulement si $p | [P]_m [Q]_{m'}$.

Or p est un nombre premier, donc p divise $[P]_m \times [Q]_{m'}$ si et seulement si il divise l'un des deux termes.

Mais ceci est faux par définition de m et de m'. /2

Par conséquent p ne divise pas $[PQ]_{m+m'}$.

(b) Conclure.

En notant $\mathcal{P}_P$: « $\{n$ tel que $p \nmid [P]_n\}$ est non vide »; $\mathcal{P}_Q$: « $\{n$ tel que $p \nmid [Q]_n\}$ est non vide »et $\mathcal{P}_{PQ}$: « $\{n$ tel que $p \nmid [PQ]_n\}$ est non vide », on a démontré : $\mathcal{P}_P$ et $\mathcal{P}_Q \Longrightarrow \mathcal{P}_{PQ}$.
La contraposée de cette implication affirme donc : $NON(\mathcal{P}_{PQ}) \Longrightarrow NON(\mathcal{P}_P)$ ou $NON(\mathcal{P}_Q)$.
Or $NON(\mathcal{P}_P)$ signifie $\{n$ tel que $p \nmid [P]_n\}$ est vide, i.e. $\forall\, n \in \mathbb{N}$, $p | [P]_n$.
On a donc montré : /1,5

Si p divise tous les coefficients d'un produit de polynômes entiers $P \times Q$,
alors p divise tous les coefficients de P ou p divise tous les coefficients de Q.

I.3. On note, pour tout $R \in \mathbb{Z}[X]^*$, $c(R) = \bigwedge_{k=0}^{\deg R} [R]_k$, appelé « contenu de R ».

(a) Montrer que $P_1 := \dfrac{P}{c(P)}$ est un polynôme à coefficients entiers, puis que $c(P_1) = 1$.

Puisque $c(P)$ est le PGCD des nombres $[P]_k$, alors pour tout $k \in \mathbb{N}$, $c(P)$ divise $[P]_k$. /1

$$\boxed{\text{Donc pour tout entier } k \in \mathbb{N},\ [P_1]_k = \frac{[P]_k}{c(P)} \in \mathbb{Z} \text{ et donc } P_1 \in \mathbb{Z}[X].}$$

Notons $\delta = c(P_1)$, le PGCD des coefficients de P_1. Alors, pour tout $k \in \mathbb{N}$, $\delta | [P_1]_k = \dfrac{[P]_k}{c(P)}$, donc $c(P)\delta \mid [P]_k$.

Comme $c(P)\delta$ divise tous les nombres $[P]_k$, il divise alors leurs PGCD, donc $c(P)$.

Donc δ divise 1, il vaut donc 1. /2

$$\boxed{c(P_1) = 1}$$

(b) En exploitant la question 2., et les polynômes P_1 et Q_1, montrer que $c(P \times Q) = c(P) \times c(Q)$

Considérons donc $P_1 = \dfrac{P}{c(P)}$ et $Q_1 = \dfrac{Q}{c(Q)}$.

On a donc $c(P_1) = c(Q_1) = 1$ et $P \times Q = c(P)P_1 \times c(Q)Q_1 = c(P)c(Q)P_1 \times Q_1$.

Si $c(P_1Q_1) \neq 1$, considérons p un diviseur premier de $c(P_1 \times Q_1)$,

donc par transitivité p divise tous les coefficients $[P_1Q_1]_n$

D'après la question 2, alors p divise tous les coefficients de P_1 ou bien p divise tous les coefficients de Q_1.

Ainsi p divise $c_1(P) = 1$ ou bien p divise $c_1(Q) = 1$.

Cela est impossible car $p \geqslant 2$, donc $c(P_1Q_1) = 1\,(= c(P1)c(Q_1))$. /1,5

Enfin, montrons que $c(\lambda T) = |\lambda| c(T)$, pour tout $\lambda \in \mathbb{Z}$ et $P \in \mathbb{Z}[X]$

$$\begin{aligned} d | c(\lambda T) &\iff \forall\ n \in \mathbb{N}, d \mid [\lambda T]_n \iff \forall\ n \in \mathbb{N}, d \mid \lambda [T]_n \\ &\iff \forall\ n \in \mathbb{N}, \frac{d}{\lambda} \mid [T]_n \iff \frac{d}{\lambda} \mid c(T) \iff d \mid \lambda c(T) \end{aligned}$$

Les diviseurs de $c(\lambda T)$ et ceux de $\lambda c(T)$ sont les mêmes ; ces deux nombres sont associés.

Comme $c(T) > 0$ et $c(\lambda T) > 0$: $c(\lambda T) = |\lambda| c(T)$.

Bilan : $c(PQ) = c(c(P)P_1 c(Q)Q_1) = |c(P)c(Q)| c(P_1Q_1) = c(P)c(Q)$ /1,5

$$\boxed{c(PQ) = c(P)c(Q)}$$

I.4. Soit $R \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$. Montrer que R est irréductible dans $\mathbb{Z}[X]$ ssi R est irréductible dans $\mathbb{Q}[X]$.

Si R n'est pas irréductible dans $\mathbb{Z}[X]$,

il existe deux polynômes R_1 et $R_2 \in \mathbb{Z}[X]$ tels que $R = R_1 \times R_2$ et $\deg R_1 > 0$, $\deg R_2 > 0$.

Alors comme R_1 et R_2 sont aussi à coefficients dans $\mathbb{Z}$ donc dans $\mathbb{Q}$, R n'est pas irréductibles dans $\mathbb{Q}[X]$.

Par contraposée : R irréductible dans $\mathbb{Q}[X]$ implique R irréductible dans $\mathbb{Z}[X]$. /1

Réciproquement, supposons que $R(\in \mathbb{Z}[X])$ n'est pas irréductible dans $\mathbb{Q}[X]$,

il existe deux polynômes R_1 et $R_2 \in \mathbb{Q}[X]$ tels que $R = R_1 \times R_2$ et $\deg R_1 > 0$, $\deg R_2 > 0$.

Pour tout $n \in \mathbb{N}$, $[R_1]_n = \dfrac{a_n}{b_n} \in \mathbb{Q}$, fraction écrite sous forme irréductible ($a_n \wedge b_n = 1$).

Notons $m_1 = PPCM(b_i)$ et donc pour tout $n \in \mathbb{N}$, $b_n | m_1$, notons $c_n = \dfrac{m_1}{b_n} \in \mathbb{Z}$ et $S_1 = m_1 \times R_1$.

On a donc pour tout entier $n \in \mathbb{N}$, $[S_1]_n = m_1 \dfrac{a_n}{b_n} = c_n a_n \in \mathbb{Z}$. Donc $S_1 \in \mathbb{Z}[X]$.

Puis considérons $T_1 = \dfrac{S_1}{c(S_1)}$, on a donc $T_1 \in \mathbb{Z}[X]$ et $c(T_1) = 1$.

De même, il existe $m_2 \in \mathbb{N}$ tel que $S_2 = m_2 \times R_2 \in \mathbb{Z}[X]$. Soit $T_2 = \dfrac{S_2}{c(S_2)}$, on a $T_2 \in \mathbb{Z}[X]$ et $c(T_2) = 1$.

Ensuite : $m_1 m_2 R = m_1 R_1 \times m_2 R_2 = S_1 \times S_1 \in \mathbb{Z}[X]$

Donc $c(S_1)c(S_2) = c(S_1 S_2) = c(m_1 m_2 R) = |m_1 m_2| \times c(\underbrace{R}_{\in \mathbb{Z}[X]}) = m_1 \times m_2 \times c(R)$.

Enfin $T_1 \times T_2 = \dfrac{S_1}{c(S_1)} \times \dfrac{S_2}{c(S_2)} = \dfrac{S_1 S_2}{c(S_1)c(S_2)} = \dfrac{m_1 m_1 R}{m_1 m_2 c(R)} = \dfrac{R}{c(R)}$.
Ainsi $R = c(R)T_1 \times T_2$ n'est pas irréductible dans $\mathbb{Z}[X]$.
Par contraposée : R irréductible dans $\mathbb{Z}[X]$ implique R irréductible dans $\mathbb{Q}[X]$. /2

$\boxed{R \in \mathbb{Z}[X] \text{ est irréductible dans } \mathbb{Z}[X] \text{ ssi } R \text{ est irréductible dans } \mathbb{Q}[X].}$

I.5. Soit p un nombre premier et $R = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$.

On note $\overline{R} = \sum_{k=0}^{n} \overline{a_k} X^k$ (avec $\overline{a_k}$, reste de la division euclidienne de a_k par p.).
Montrer que $\overline{R}(X^p) = (\overline{R}(X))^p$. *On pourra raisonner par récurrence forte sur* $n = \deg R$.

Posons, pour tout $n \in \mathbb{N} \cup \{-\infty\}$, $\mathcal{H}_n$: « Si $R \in \mathbb{Z}[X]$ avec $\deg R = n$ alors $\overline{R}(X^p) = [\overline{R}(X)]^p$. »
— Si $R = 0$, alors $\overline{R}(X^p) = 0 = [\overline{R}(X)]^p$. Donc $\mathcal{H}_{-\infty}$ est vraie. /1
— Soit R un polynôme de degré 0, donc R est constant. On peut supposer $R = a_0$.
$\overline{R}(X^p) = \overline{a_0} = \overline{R}(X)]^p$. Donc $\mathcal{H}_0$ est vraie.
— Soit $n \in \mathbb{N}$. Supposons que $\mathcal{H}_k$ est vraie, pour tout $k \leqslant n$ et $k \in \mathbb{N} \cup \{-\infty\}$.
Soit R un polynôme de degré $n+1$, supposons $R \in \mathbb{Z}[X]$, $\deg R = n+1$ et $[R]_{n+1} = a$.
$R = aX^{n+1} + R_1$ avec $\deg R_1 \leqslant n$.
On applique la formule du binôme de Newton : $\dfrac{\mathbb{Z}}{p\mathbb{Z}}[X]$ est un anneau commutatif :

$$[\overline{R}(X)]^p = \left(\overline{a}X^n + \overline{R_1}(X)\right)^p = \sum_{i=0}^{p} \overline{\binom{p}{i}} (\overline{a}X^n)^i (\overline{R_1}(X))^{p-i}$$

Or $\binom{p}{i} = \dfrac{p(p-1)!}{i(i-1)!((p-1)-(i-1))!} = \dfrac{p}{i}\binom{p-1}{i-1}$, donc $p | i \times \binom{p}{i}$.

Et p est premier donc pour tout $i \in [\![1, p-1]\!]$, $p \wedge i = 1$; d'après le théorème de Gauss : $p | \binom{p}{i}$.

Finalement, il ne reste plus que :

$$[\overline{R}(X)]^p = \underbrace{(\overline{a}X^n)^0 (\overline{R_1}(X))^p}_{i=0} + 0 + \cdots + 0 + \underbrace{(\overline{a}X^n)^p (\overline{R_1}(X))^0}_{i=p} = (\overline{R_1}(X))^p + \overline{a}^p X^{pn}$$

Puis comme $\mathcal{H}_{\deg R_1}$ est vraie, on a $[\overline{R}(X)]^p = \overline{R_1}(X^p) + \overline{a}^p (X^p)^n = \overline{R_1}(X^p) + \overline{a}(X^p)^n$,
en exploitant le petit théorème de Fermat : $\overline{a}^p = \overline{a}[p]$ puisque p est premier.
Et donc $[\overline{R}(X)]^p = (\overline{R_1}(X) + \overline{a}X^n) \circ X^p = \overline{R}(X^p)$. /2
Par conséquent, $\mathcal{H}_n$ est vraie.

$\boxed{\text{Pour tout polynôme } R \in \mathbb{Z}[X],\ \overline{R}(X^p) = [\overline{R}(X)]^p.}$

II Décomposition des polynômes G_n

II.1. Effectuer, *en parallèle*, l'algorithme d'Euclide pour les nombres 14 et 3 et pour les polynômes G_{14} et G_3.
Donner un couple d'entiers (u, v) et un couple de polynômes (U, V) tels que $14u+3v = 1$ et $G_{14} \times U + G_3 \times V = G_1$.

On a donc, en appliquant l'algorithme d'Euclide :

$$14 = 3 \times 4 + 2$$
$$3 = 2 \times 1 + 1$$
$$2 = 1 \times 2 + 0$$

u_n	v_n	q_n	$au_n + bv_n$
1	0		14
0	1	4	3
1	−4	1	2
−1	5	2	1

/1

Donc $14 \wedge 3 = 1$ et $(-1) \times 14 + 5 \times 3 = 1$.

Et pour les polynômes :

$$\begin{aligned} X^{14} - 1 &= (X^3 - 1) \times (X^{11} + X^8 + X^5 + X^2) + (X^2 - 1) \\ X^3 - 1 &= (X^2 - 1) \times (X + 1) + (X - 1) \\ X^2 - 1 &= (X - 1) \times (X + 1) + 0 \end{aligned}$$

/1

U_n	V_n	Q_n	$AU_n + BV_n$
1	0		G_{14}
0	1	$X^{11} + X^8 + X^5 + X^2$	G_3
1	$-(X^{11} + X^8 + X^5 + X^2)$	$X + 1$	G_2
$-(X + 1)$	$X^{12} + X^{11} + X^9 + X^8 + X^6 + X^5 + X^3 + X^2 + 1$	$(X + 1)$	G_1

/1

Donc $G_{14} \wedge G_3 = G_1$ et $-(X + 1) \times G_{14} + (X^{12} + X^{11} + X^9 + X^8 + X^6 + X^5 + X^3 + X^2 + 1) \times G_3 = G_1$.

II.2. Montrer que pour tous entiers $m > n \geqslant 1$, $G_m \wedge G_n = G_{m \wedge n}$.

Soit $m > n \geqslant 1$, deux entiers.
On remarque que pour tout entier $q \in \mathbb{N}$ tel que $m - qn > 0$,

$$G_m = G_n \times (X^{m-n} + X^{m-2n} + \cdots + X^{m-qn}) + X^{m-qn} - 1 = G_n \times \sum_{k=1}^{q} X^{m-kn} + G_{m-qn}$$

En effet, par telescopage :

$$G_n \times \sum_{k=1}^{q} X^{m-kn} = \sum_{k=1}^{q} X^{m-kn+n} - \sum_{k=1}^{q} X^{m-kn} = \sum_{k=0}^{q-1} X^{m-kn} - \sum_{k=1}^{q} X^{m-kn} = X^m - X^{m-qn} = G_m - G_{m-qn}$$

Ainsi, si q est le quotient de la division euclidienne de m par n, et r son reste : $G_m = G_n \times \sum_{k=1}^{q} X^{m-qn} + G_r$ /1,5

Or $\deg G_r = r < n = \deg G_n$. On a donc écrit ici la division euclidienne de G_m par G_n.
On a donc $G_m \wedge G_n = G_n \wedge G_r$ où r, reste de la division euclidienne de m par n.
Notons (r_i) la suite des restes dans l'algorithme d'Euclide appliqué à m et n. Et r_{N-1}, le dernier reste non nul.
Alors, on a un invariant de boucle : pour tout $k \leqslant N - 1$: $G_{r_k} \wedge G_{r_{k+1}}$.
Cet invariant vaut $G_{r_0} \wedge G_{r_1} = G_m \wedge G_n$ au début de l'algorithme,
et il a pour valeur $G_{r_{N-1}} \wedge G_{r_N} = G_{m \wedge n} \wedge 0 = G_{m \wedge n}$ en fin d'algorithme. /1

Pour tous entiers $m > n \geqslant 1$, $G_m \wedge G_n = G_{m \wedge n}$.

II.3. Factoriser G_3 et G_4 sur $\mathbb{C}[X]$, puis sur $\mathbb{R}[X]$.

Ces calculs sont célèbres : /1

$$\begin{aligned} G_3 &= X^3 - 1 = (X - 1)(X - j)(X - j^2) = (X - 1)(X^2 + X + 1) \\ G_4 &= X^4 - 1 = (X - 1)(X - i)(X + 1)(X + i) = (X - 1)(X + 1)(X^2 + 1) \end{aligned}$$

II.4. Factoriser G_n sur $\mathbb{R}[X]$. On notera, pour $1 \leqslant k \leqslant n$, $c_{k,n} = \cos \dfrac{2k\pi}{n}$.

Selon la parité de n, -1 est une racine (n pair) ou non (n impair) de G_n.
On commence par factoriser G_n sur $\mathbb{C}[X]$: on connait exactement les racines de G_n, ce sont les éléments de $\mathbb{U}_n$.
On sait également décrire parfaitement $\mathbb{U}_n$: $\mathbb{U}_n = \{\exp \dfrac{2ik\pi}{n}, k \in [\![0, n-1]\!]\}$

$$G_n = \prod_{z \in \mathbb{U}_n} (X - z) = \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}}) = (X - 1) \prod_{k=1}^{n-1} (X - e^{\frac{2ik\pi}{n}})$$

Puis, notons que $\overline{e^{\frac{2ik\pi}{n}}} = e^{-\frac{2ik\pi}{n}} = e^{2i\pi - \frac{2ik\pi}{n}} = e^{\frac{2i(n-k)\pi}{n}}$.
Si n est impair, supposons $n = 2h+1$

$$\begin{aligned} G_n &= (X-1)\prod_{k=1}^{h}(X - e^{\frac{2ik\pi}{n}})\prod_{k=h+1}^{2h}(X - e^{\frac{2ik\pi}{n}}) = (X-1)\prod_{k=1}^{h}(X - e^{\frac{2ik\pi}{n}})\underbrace{\prod_{j=1}^{h}(X - e^{\frac{2i(n-j)\pi}{n}})}_{j=n-k=2h+1-k} \\ &= (X-1)\prod_{k=1}^{h}(X - e^{\frac{2ik\pi}{n}})\overline{(X - e^{\frac{2ik\pi}{n}})} = (X-1)\prod_{k=1}^{h}(X^2 - 2\mathrm{Re}(e^{\frac{2ik\pi}{n}})X + |e^{\frac{2ik\pi}{n}}|^2) \\ &= (X-1)\prod_{k=1}^{h}(X^2 - 2c_{k,n}X + 1) \end{aligned}$$

Si n est pair, supposons $n = 2h$ /1,5

$$\begin{aligned} G_n &= (X-1)\prod_{k=1}^{h-1}(X - e^{\frac{2ik\pi}{n}})(X+1)\prod_{k=h+1}^{2h-1}(X - e^{\frac{2ik\pi}{n}}) = (X-1)(X+1)\prod_{k=1}^{h-1}(X - e^{\frac{2ik\pi}{n}})\underbrace{\prod_{j=1}^{h-1}(X - e^{\frac{2i(n-j)\pi}{n}})}_{j=n-k=2h-k} \\ &= (X-1)(X+1)\prod_{k=1}^{h-1}(X - e^{\frac{2ik\pi}{n}})\overline{(X - e^{\frac{2ik\pi}{n}})} = (X-1)(X+1)\prod_{k=1}^{h-1}(X^2 - 2c_{k,n}X + 1) \end{aligned}$$

/1,5

$$\boxed{G_{2h} = (X-1)(X+1)\prod_{k=1}^{h-1}(X^2 - 2c_{k,n}X + 1) \text{ et } G_{2h+1} = (X-1)\prod_{k=1}^{h}(X^2 - 2c_{k,n}X + 1)}$$

Soit $n \in \mathbb{N}$, fixé. On cherche à factoriser G_n en produit de polynômes de $\mathbb{Q}[X]$ (donc de $\mathbb{Z}[X]$) (questions 5 et 6).

II.5. On commence par trouver une factorisation.

(a) On note, pour tout $k \in \mathbb{N}$, $z_k = e^{\frac{2ik\pi}{n}}$. On sait que $\mathbb{U}_n = \{z_k; k \in [\![1,n]\!]\}$.
Montrer que $z_k \in \mathbb{V}_n \iff \exists\, u \in \mathbb{Z}$ tel que $(z_k)^u = z_1 \iff k \wedge n = 1$.

Raisonnons par triple implications.
• Si $z_k \in \mathbb{V}_n$, alors pour tout $u \in [\![1, n-1]\!]$, $z_k^u \neq 1$.
Or $z_k^u \in \mathbb{U}_n$ et $\mathrm{card}(\mathbb{U}_n \setminus \{1\} = n-1$.
Donc :
— ou bien $[\![1, n-1]\!] \to \mathbb{U}_n \setminus \{1\}$, $u \mapsto z_k^u$ est surjective et donc injective,
Dans ce cas z_1 admet un antécédent et donc il existe $u \in [\![1, n-1]\!] \subset \mathbb{Z}$ tel que $z_k^u = z_1$.
— ou bien $[\![1, n-1]\!] \to \mathbb{U}_n \setminus \{1\}$, $u \mapsto z_k^u$ n'est pas surjective et donc n'est pas injective,
Il existe $u_1 < u_2 \in [\![1, n-1]\!]$ tel que $z_k^{u_1} = z_k^{u_2}$ et donc $z_k^{u_2-u_1} = \dfrac{z_k^{u_2}}{z_k^{u_1}} = 1$,
et donc $z_k \in \mathbb{V}_{u_2-u_1}$, ce qui est faux.
Finalement : il existe $u \in [\![1, n-1]\!] \subset \mathbb{Z}$ tel que $z_k^u = z_1$.
• S'il existe $u \in \mathbb{Z}$ tel que $z_k^u = z_1$ On a donc $\exp\dfrac{2iku\pi}{n} = \exp\dfrac{2i\pi}{n}$ donc $\dfrac{2uk\pi}{n} \equiv \dfrac{2\pi}{n}[2\pi]$
donc $\dfrac{uk}{n} \equiv \dfrac{1}{n}[1]$ puis $ku \equiv 1[n]$.
Donc, il existe $v) \in \mathbb{Z}$ tel que $uk + vn = 1$. Ainsi $k \wedge n = 1$ d'après Bézout.
• Enfin, supposons que $k \wedge n = 1$.
Soit $r \in \mathbb{N}^*$ tel que $z_k \in \mathbb{V}_r$, comme $z_k^n = 1$, nécessairement, $r \leqslant n$.
Puis on a $1 = z_k^r = \exp\dfrac{2ikr\pi}{n}$, donc $rk \equiv 0[n]$, donc $n|kr$.
Or $n \wedge k = 1$, donc $n|r$. Ainsi $r \in n\mathbb{Z} \cap [1, n]$, bilan $r = n$. /2

$$\boxed{z_k \in \mathbb{V}_n \iff \exists\, u \in \mathbb{Z} \text{ tel que } (z_k)^u = z_1 \iff k \wedge n = 1.}$$

(b) Montrer que $\mathbb{U}_n = \uplus_{d|n} \mathbb{V}_d$.
Donner la description des éléments de $\mathbb{U}_{12}$ regroupés selon les $\mathbb{V}_k$ auxquels ils appartiennent.

On rappelle que n et d (par la suite) sont des entiers naturels, donc positifs.
Soit d, un diviseur de n. Donc il existe $n_1 \in \mathbb{N}$ tel que $n = n_1 d$.
Soit $z \in \mathbb{V}_d$, alors $z^d = 1$ et donc $z^n = z^{n_1 d} = (z^d)^{n_1} = 1^{n_1} = 1$. Donc $z \in \mathbb{U}_n$.
Par conséquent $\mathbb{V}_d \subset \mathbb{U}_n$, on a donc $\bigcup_{d|n} \mathbb{V}_d = \mathbb{U}_n$
Réciproquement, soit $z \in \mathbb{U}_n$ (fixé !), i.e. $z^n = 1$.
L'ensemble $\{k \in [\![1, n]\!] \text{ tel que } z^k = 1\}$ est donc non vide (il contient n) , inclus dans $\mathbb{N}$,
il admet un plus petit élément k_0(qui dépend de z).
Alors $z \in \mathbb{V}_{k_0}$, par définition de k_0 et $\mathbb{V}_{k_0}$.
Puis, si on note $\delta = k_0 \wedge n$, il existe $u, v \in \mathbb{Z}$ tel que $\delta = uk_0 + vn$ et donc

$$z^\delta = (z^{k_0})^u \times (z^n)^v = 1^u \times 1^v = 1$$

Nécessairement, $\delta = k_0$ et donc $k_0 = \delta$ divise n.
On a la double inclusion, reste à montrer que la réunion est disjointe.
Si $z \in \mathbb{V}_d \cap \mathbb{V}_{d'}$, alors, SPDG, on peut supposer $d \leqslant d'$.
Donc $z^d = 1$ et pour tout $k < d'$, $z^k \neq 1$. Donc $d = d'$. La réunion est disjointe. /1,5

$$\boxed{\mathbb{U}_n = \uplus_{d|n} \mathbb{V}_d}$$

On a alors pour $\mathbb{U}_{12}$: /1

$$\mathbb{U}_{12} = \{\underbrace{1}_{\in\mathbb{V}_1}, \underbrace{-1}_{\in\mathbb{V}_2}, \underbrace{\overbrace{e^{\frac{i\pi}{3}}}^{=j}, \overbrace{e^{-\frac{i\pi}{3}}}^{=j^2}}_{\in\mathbb{V}_3}, \underbrace{\overbrace{e^{\frac{i\pi}{4}}}^{=i}, \overbrace{e^{-\frac{i\pi}{4}}}^{=-i}}_{\in\mathbb{V}_4}, \underbrace{e^{\frac{i\pi}{3}}, e^{-\frac{i\pi}{3}}}_{\in\mathbb{V}_6}, \underbrace{e^{\frac{i\pi}{6}}, e^{-\frac{i\pi}{6}}, e^{\frac{5i\pi}{6}}, e^{-\frac{5i\pi}{6}}}_{\in\mathbb{V}_{12}}\}$$

(c) Déduire de la réunion disjointe précédente, que $G_n = \prod_{d|n} \Phi_d$. Que vaut Φ_{12} ?

Il s'agit simplement d'une décomposition d'un produit (car la réunion est disjointe) : /1

$$\boxed{G_n = \prod_{z\in\mathbb{U}_n} (X - z) = \prod_{z\in\uplus_{d|n}\mathbb{V}_d} (X - z) = \prod_{d|n} \left(\prod_{z\in\mathbb{V}_d} (X - z) \right) = \prod_{d|n} \Phi_d}$$

On a alors, d'après la question précédente : $G_{12} = \Phi_1 \times \Phi_2 \times \Phi_3 \times \Phi_4 \times \Phi_6 \times \Phi_{12}$.
Et d'après la décomposition précédente,

$$\Phi_{12} = (X - e^{\frac{i\pi}{6}})(X - e^{-\frac{i\pi}{6}})(X - e^{\frac{5i\pi}{6}})(X - e^{-\frac{5i\pi}{6}}) = (X^2 - 2\cos\frac{\pi}{6} + 1)(X^2 - 2\cos\frac{5\pi}{6} + 1)$$

Or en notant $C = \cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$, on a $\cos\frac{5\pi}{6} = -\cos(\pi - \frac{5\pi}{6}) = -\cos\frac{\pi}{6} = -C$, donc /1,5

$$\boxed{\Phi_{12} = (X^2 - 2CX + 1)(X^2 + 2CX + 1) = X^4 + (2 - 4C^2)X^2 + 1 = X^4 + (2 - 3)X + 1 = X^4 - X^2 + 1}$$

(On peut aussi calculer par division euclidienne de polynômes entiers successivement $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$ et $\Phi_6 = X^2 - X + 1 \ldots$)

(d) Montrer, par récurrence forte sur $m \in \mathbb{N}^*$ que $\Phi_m \in \mathbb{Z}[X]$ et est unitaire.

$G_m = \Phi_m \times \prod_{d|m, d\neq m} \Phi_d$, donc Φ_m est le quotient de la division euclidienne de G_m par $\prod_{d|m, d<m} \Phi_d$.
Montrons d'abord que :

pour $A, B \in \mathbb{Z}[X]$ tels que $B|A$ dans $\mathbb{Q}[X]$, alors si B est unitaire, les coefficients de $\mathbb{Q}$ sont entiers.

Supposons donc $A = BQ$, avec $Q \in \mathbb{Q}[X]$. On trouve alors pour tout entier n, $[A]_n = \sum_{k=0}^{n} [B]_k [Q]_{n-k}$.

Supposons que $d_A = \deg A$ et $d_B = \deg B$, on a donc $d_Q := \deg Q = d_A - d_B$, puis

$$[A]_{d_A} = [B]_{d_B} \times [Q]_{d_Q} \Rightarrow [Q]_{d_Q} = \frac{[A]_{d_A}}{[B]_{d_B}} = [A]_{d_A} \in \mathbb{Z} \text{ (car } B \text{ unitaire, donc } [B]_{d_B} = 1).$$

Montrons alors par récurrence (forte), pour $k \in [\![0, d_Q]\!]$, $\mathcal{H}_k$: « $[Q]_{d_Q - k} \in \mathbb{Z}$ ».
— On vient de voir que $[Q]_{d_Q} \in \mathbb{Z}$, donc $\mathcal{H}_0$ est vraie.
— Soit $k \in [\![0, d_Q - 1]\!]$ tel que $\mathcal{H}_0$, $\mathcal{H}_1, \cdots, \mathcal{H}_k$ sont vraies.

$$[Q]_{d_Q-(k+1)}[B]_{d_B} = [Q]_{d_Q-k-1}[B]_{d_B} = \underbrace{[A]_{d_Q+d_B-k-1}}_{\in\mathbb{Z}} - \sum_{i=0}^{d_B-1} \underbrace{[B]_i}_{\in\mathbb{Z}} \underbrace{[Q]_{d_Q+d_B-k-1-i}}_{=[Q]_r \in \mathbb{Z}}$$

car $r = d_Q - k + \underbrace{d_B - 1 - i}_{\geqslant 0} \geqslant d_Q - k$ et en appliquant $\mathcal{H}_r$.

On termine en notant que $[B]_{d_B} = 1$. Donc $\mathcal{H}_{k+1}$ est vraie. /2

Ainsi, si $B|A$, avec $A, B \in \mathbb{Z}[X]$ et B unitaire, alors $Q = \dfrac{A}{B}$ est un polynôme à coefficients entiers.

Posons maintenant, pour $m \in \mathbb{N}^*$, $\mathcal{Q}_m$: « Φ_m est unitaire et à coefficients entiers. »
— $\Phi_1 = X - 1$, donc $\mathcal{Q}_1$ est vraie.
— Soit $m \in \mathbb{N}$, $m \geqslant 2$, supposons que $\mathcal{Q}_1, \ldots \mathcal{Q}_{m-1}$ sont vraies.
$G_m = \Phi_m \prod_{d|m, d<m} \Phi_d$, on a donc pour $d|m$ et $d < m$, Φ_d est unitaire à coefficients entiers.
Le produit de tels polynômes est unitaire, à coefficients entiers : $B = \prod_{d|m, d<m} \Phi_d \in \mathbb{Z}[X]$ et est unitaire.
G_m est également à coefficients entiers, donc $\Phi_m = \dfrac{G_m}{B}$ est à coefficients entiers.
Puis le coefficient dominant de Φ_m est égale à celui de G_m divisé par celui de B, i.e. $\dfrac{1}{1} = 1$.
Donc $\mathcal{Q}_m$ est vérifiée. /2

$\Phi_m \in \mathbb{Z}[X]$ et est unitaire.

Enfin, $\Phi_m = \prod_{z \in \mathbb{V}_m} (X - z)$, produit de $\text{card}(\mathbb{V}_m)$ polynôme de degré 1, donc son degré est $\text{card}(\mathbb{V}_m)\times = \varphi(m)$/1

$\deg \Phi_m = \varphi(m)$

(e) Quel est le de degré de Φ_m ? En déduire la valeur de $\sum_{d|n} \varphi(d)$, en fonction de n.

/1

On a donc, d'après la question précédente : $\deg G_n = \deg \left(\prod_{d|n} \Phi_d \right) = \sum_{d|n} \deg \Phi_d = \sum_{d|n} \varphi(d)$.

II.6. On démontrer maintenant qu'il n'y a pas d'autres factorisations dans $\mathbb{Z}[X]$.

Supposons pour cela que $\Phi_n = \prod_{i=1}^{r} P_i$ où chaque P_r est un polynôme irréductible et unitaire de $\mathbb{Q}[X]$.

(a) Soit z une racine de P_1 et p premier tel que $p \not| n$. Montrer qu'il existe i tel que $P_i(z^p) = 0$.

---

z est une racine de P_1, donc de Φ_n. Ainsi pour tout $k < n$, $z^k \neq 1$ et $z^n = 1$.
Comme p est un nombre premier et que $p \not| n$, alors $p \wedge n = 1$. Puis $(z^p)^r = z^{pr}$.

D'après la question précédente, on a : $(z^p)^s = 1 \iff n|ps \iff n|s \iff s \in n\mathbb{Z}$.
Ainsi, pour tout $s \in [\![1, n-1]\!]$, $(z^p)^s \neq 1$ et donc $z^p \in \mathbb{V}_n$.

Donc z^p est une racine de Φ_n, ainsi $\Phi_n(z^p) = 0 = \prod_{i=1}^{r} P_i(z^p)$ Or $\mathbb{C}$ est intègre, donc /1,5

$$\boxed{\text{il existe } i \in \mathbb{N}_r \text{ tel que } P_i(z^p) = 0.}$$

(b) Montrer que $\overline{\Phi_n}$ (défini en I.5) n'est divisible par le carré d'aucun polynôme non constant dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

Supposons que $\overline{\Phi_n}$ est divisible par le carré d'un polynôme Q (non constant),
Ainsi, supposons qu'il existe $Q, T \in \mathbb{Z}[X]$ tel que $\overline{\Phi_n} = \overline{Q}^2\overline{T}$ et $\deg \overline{Q} > 0$.
Alors comme Φ_n divise G_n, il existe $S \in \mathbb{Z}[X]$ tel que $\overline{G_n} = X^n - \overline{1} = \overline{Q}^2 \underbrace{\overline{TS}}_{\overline{R}}$.

On peut dériver cette égalité polynômiale : $\overline{n}X^{n-1} = \overline{Q}\left(2\overline{Q'R} + \overline{QR'}\right)$.
Donc $\overline{Q}$ divise $\overline{n}X^{n-1}$, et divise $X^n - \overline{1}$,
et $\overline{Q}$ divise aussi $X(\overline{n}X^{n-1}) - \overline{n}(X^n - \overline{1}) = \overline{n}$
Donc $\overline{Q}$ est une constante, non nulle, puisque $\overline{n} \neq 0$, puisque $p \wedge n = 1$. On a donc une contradiction : /2

$$\boxed{\overline{\Phi_n} \text{ n'est divisible par le carré d'aucun polynôme non constant.}}$$

(c) Montrer que $i = 1$, i.e. $P_1(z^p) = 0$, puis que pour tout k entier, premier avec n, $P_1(z^k) = 0$.

Reprenons les notations données plus haut, $P_1(z) = 0$ et $P_i(z^p) = 0$ avec $i \neq 1$.
La polynôme $R_1(X) = P_i(X^p)$ admet donc z comme racine, comme le polynôme P_1.
Ils ne sont pas premiers entre eux dans $\mathbb{Q}[X]$.
Mais si $\Delta = P_1 \wedge R_1$, alors $\Delta | P_1$, irréductible par hypothèse. Donc $\Delta = P_1$.
Et finalement, $P_1 = \lambda\Delta | R_1$ (dans $\mathbb{Q}[X]$).
La division euclidienne de R_1 par P_1 (dans $\mathbb{Q}[X]$) a un reste nul, mais elle s'effectue uniquement avec des nombres entiers car P_1 est unitaire (remarque vue en cours).
Donc il existe $S_1 \in \mathbb{Z}[X]$ tel que $R_1 = S_1 \times P_1$.
Prenons maintenant les classes modulo p (puisqu'on est dans $\mathbb{Z}[X]$) (avec I.5) :

$$\overline{P_1}|\overline{R_1} = \overline{P_i(X^p)} = [\overline{P_i}(X)]^p$$

Soit $\overline{Q}$, un facteur irréductible de $\overline{P_1}$ dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}[X]$, on a donc $\overline{Q}|\overline{P_1}|\overline{P_i}^p$.
Comme $\overline{Q}$ est irréductible, $\overline{Q}|\overline{P_i}$ et donc $\overline{Q}^2|\overline{\Phi_n} = \overline{P_1P_i} \times \prod_{j\neq 1,i} \overline{P_j}$.
D'après la question précédente, cela n'est possible que si $\overline{Q}$ est constant. Donc $\overline{P_1}$ est constant.
Impossible, donc $i = 1$

$$\boxed{P_1(z^p) = 0.}$$

Le résultat a été montré pour tout nombre premier p, premier avec n. Montrons par récurrence sur $s \in \mathbb{N}^*$,
$\mathcal{H}_s$: « Si $k = p_1 \cdots p_s$, produit de s nombres premiers (qui peuvent se répéter) tel que $k \wedge n = 1$, alors $P_1(z^k) = 0$ ».
— Si $k = p_1$, c'est toute la partie précédente.
— Soit $s \in \mathbb{N}^*$. Supposons que $\mathcal{H}_s$ est vraie.
Soit $k = p_1 \cdots p_s p_{s+1}$, produit de $s+1$ nombres premiers (qui peuvent se répéter) tel que $k \wedge n = 1$,
On note $k' = p_1 \cdots p_s$, on a alors $k' \wedge n = 1$, on peut appliquer $\mathcal{H}_s$.
Donc $P_1(z^{k'}) = 0$. Notons $z' = z^{k'}$, c'est une racine de P_1,
on a donc, puisque $p_{s+1} \wedge n = 1$, $P_1((z')^{p_{s+1}}) = 0$ (question précédente pour $(z, p) \leftarrow (z', p_{s+1})$).
Et donc finalement, $P_1(z^k) = 0$. Donc $\mathcal{H}_{s+1}$ est vraie. /4

$$\boxed{\text{Pour tout } k \text{ entier, premier avec } n,\ P_1(z^k) = 0.}$$

(d) Conclure

Soit $z \in \mathbb{V}_n$, alors on montre que $\mathbb{V}_n = \{z^k \ ; \ k \wedge n = 1\}$. *C'est vrai pour tous, mais on se contente de* $z = e^{\frac{2i\pi}{n}}$.
Et donc tous les éléments de $\mathbb{V}_n$ sont des racines de P_1, donc $\Phi_n = P_1$. /1

Ainsi Φ_n est irréductible dans $\mathbb{Z}[X]$.

III Application pour la résolution d'un problème diophantien

Soit p et q deux nombres premiers vérifiant $3 \leqslant p < q$. On note $< p, q >= \{mp + nq, m, n \in \mathbb{N}\}$.
Soulignons, que les nombres m et n sont des entiers naturels et non des entiers relatifs.

III.1. Montrer que tout nombre entier $R \geqslant (p-1)(q-1)$ appartient à $< p, q >$.

Soit $R \geqslant (p-1)(q-1)$.
p et q sont premiers entre eux, puisque ce sont deux nombres premiers.
Donc il existe $u, v \in \mathbb{Z}$ tel que $up + vq = 1$. En multipliant par R, on a $Ru \times p + Rv \times q = R$.
Le problème est que ces nombres sont des entiers relatifs, et non naturels, a priori.

Piste de recherche...
Considérons un autre couple $(a, b) \in \mathbb{Z}^2$ tel que $ap + bq = R = Rup + Rvq$.
On a donc $(a - Ru)p = (Rv - b)q$. Donc $p|(Rv - b)q$ et comme $p \wedge q = 1$, $p|Rv - b$.
Par conséquent : il existe $s \in \mathbb{Z}$ tel que $b = Rv - ps$
et ensuite $ap = Rup + Rvq - bq = Rup + pqs = p(Ru + qs)$ donc $a = Ru + q$.
On cherche donc deux nombres a et b tels que $a \equiv Ru[q]$ et $b \equiv Rv[p]$ et $a, b > 0$.

Faisons la division euclidienne de Ru par q. Il existe donc $a \in [\![0, q-1]\!]$ (reste de la D.E.) tel que $Ru \equiv a[q]$.
Et il existe $s \in \mathbb{Z}$ tel que $Ru = sq + a$, on a alors $R = Rup + Rvq = sqp + ap + Rvq = ap + (sp + Rv)q$.
Notons $b = sp + Rv \in \mathbb{Z}$. On a donc $R = ap + bq$.
Or $0 \leqslant a \leqslant q - 1$, donc $p > 0 : 0 \leqslant ap \leqslant p(q-1) = pq - p$
Et $R \geqslant (p-1)(q-1) = pq - p - q + 1$, donc $ap \leqslant R + q - 1$ et $bq = R - ap \geqslant 1 - q$.
Or si $b < 0$, $b \leqslant -1$ et donc $bq < -q$ ($q > 0$). Ceci n'est donc pas possible donc $b \geqslant 0$. /1,5

Ainsi, pour tout $R \geqslant (p-1)(q-1)$, il existe $a, b \in \mathbb{N}$ tel que $R = ap + bq \in < p, q >$

III.2. Le nombre $(p-1)(q-1) - 1$ appartient-il à $< p, q >$?

Supposons par l'absurde qu'il existe $a, b \in \mathbb{N}$, tel que $ap + bq = (p-1)(q-1) - 1 = pq - p - q$.
Donc $(a + 1 - q)p + (b + 1)q = 0$. Ainsi $q|(a + 1 - q)p$ et comme $p \wedge q = 1$, $q|a + 1 - q$ et donc $q|a + 1$.
Mais $a \in \mathbb{N}$, donc $a + 1 > 0$ et donc il existe $s \in \mathbb{N}^*$ tel que $a + 1 = sq$ et donc $a + 1 - q = (s-1)q$.
On a alors $0 = (s-1)qp + (b+1)q$, donc $(s-1)p + (b+1) = 0$, alors que $s - 1, p, b + 1 \in \mathbb{N}$.
Nécessairement : $s - 1 = 0$ et $b + 1 = 0$, donc $b = -1$. Contradiction. /1

$(p-1)(q-1) - 1$ n'appartient pas à $< p, q >$.

III.3. On définit les polynômes $H = \sum_{s \in \mathbb{N} \setminus < p,q >} X^s$ et $K = 1 + (X-1)H(X)$, qui sont donc à coefficients entiers.

(a) Quels sont les degré de H et de K ?

D'après les questions précédentes, pour tout $k \geqslant R(= (p-1)(q-1))$, $k \in < p, q >$, donc $[H]_k = 0$.
Ainsi $\deg H < R$.

Et $R-1 \notin < p, q >$, donc $[H]_{R-1} \neq 0$ et donc donc $\deg H \geqslant R-1$.

$$\boxed{\text{Par double inégalité : } \deg H = R-1 = (p-1)(q-1)-1 = pq-p-q.}$$

Puis $\deg((X-1)H) = \deg(X-1)+\deg H = 1+\deg H \geqslant 1$, donc $\deg K = \max(0, \deg((X-1)H) = 1+\deg H$ /1

$$\boxed{\deg K = R = (p-1)(q-1).}$$

(b) Calculer K pour le choix $(p,q) = (3,5)$.

Pour ce couple, $R = (p-1)(q-1) = 2 \times 4 = 8$.
Les termes suivants ($\geqslant 8$) ne sont pas intéressants à étudier.
On a, de plus, $0 = 0\times 3 + 0 \times 5$, $3 = 1\times 3 + 0\times 5$, $5 = 0\times 3 + 1 \times 5$, $6 = 2\times 3 + 0 \times 5$ dans $< 3, 5 >$.
Donc $H = X^1 + X^2 + X^4 + X^7$. Puis /1,5

$$\boxed{K = 1 + (X-1)H = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8}$$

III.4. Considérons deux polynômes $S, T \in \mathbb{Z}[X]$ tel que pour tout $k \in \mathbb{N}$, $[S]_k \in \{0,1\}$ et $T = (X-1)S$

(a) Exprimer pour tout $k \in \mathbb{N}$, $[T]_k$ en fonction des coefficients de S. En déduire que $[T]_k \in \{-1, 0, 1\}$.

Pour tout $k \in \mathbb{N}$, $[T]_k = \sum_{i=0}^{k} [(X-1)]_i [S]_{k-i} = [X-1]_0[S]_k + [X-1]_1[S]_{k-1} + 0 + \cdots = -[S]_k + [S]_{k-1}$.
Or $[S]_k, [S]_{k-1} \in \{0,1\}$, donc /1

$$\boxed{[T]_k = [S]_{k-1} - [S]_k \in \{-1, 0, 1\}}$$

(b) Soient $k_1 < k_2 \in \mathbb{N}$ tel que $[T]_{k_1} \neq 0$, $[T]_{k_2} \neq 0$ et pour tout $k \in [\![k_1+1, k_2-1]\!]$, $[T]_k = 0$.
Montrer que $[T]_{k_1} \times [T]_{k_2} = -1$.

Pour tout $k \in [\![k_1+1, k_2-1]\!]$, $[T]_k = 0 = [S]_{k-1} - [S]_k$, donc $[S]_k = [S]_{k-1}$.
La suite $([S]_k)_{k_1 \leqslant k \leqslant k_2-1}$ est donc une suite constante.
Alors que $[T]_{k_2} = [S]_{k_2-1} - [S]_{k_2} \neq 0$, donc $[S]_{k_2} \neq [S]_{k_2-1} = [S]_{k_1}$.
et de même $[T]_{k_1} = [S]_{k_1-1} - [S]_{k_1} \neq 0$, donc $[S]_{k_1-1} \neq [S]_{k_1}$.
Ainsi, ou bien $\forall\, k \in [\![k_1, k_2-1]\!]$, $[S]_{k-1} = 0$, $[S]_{k_1-1} = 1$ et $[S]_{k_2} = 1$,
ou bien $\forall\, k \in [\![k_1, k_2-1]\!]$, $[S]_{k-1} = 1$, $[S]_{k_1-1} = 0$ et $[S]_{k_2} = 0$,
Et donc, dans le premier cas : $[T]_{k_1} = [S]_{k_1-1} - [S]_{k_1} = 1 - 0 = 1$ et $[T]_{k_2} = [S]_{k_2-1} - [S]_{k_2} = 0 - 1 = -1$.
dans le second cas : $[T]_{k_1} = [S]_{k_1-1} - [S]_{k_1} = 0 - 1 = -1$ et $[T]_{k_2} = [S]_{k_2-1} - [S]_{k_2} = 1 - 0 = 1$.
Dans tous les cas : /2

$$\boxed{[T]_{k_1} \times [T]_{k_2} = -1.}$$

(c) En déduire que K n'a que des coefficients égaux à -1, 0 ou 1 et que les 1 et -1 s'alternent dans la suite des coefficients (il ne peut y avoir que des zéros comme coefficient entre ces nombres).

Le polynôme H vérifie les même conditions que le polynôme S des questions précédentes, donc $(X-1)S$.
Ainsi les coefficients de $K - 1 = (X-1)S$ sont tous égaux à -1, 0 et 1 et que les 1 et -1 s'alternent dans la suite des coefficients de $K-1$.
Par ailleurs, $[(X-1)H]_0 = -[S]_0 \in \{-1, 0\}$ et donc $[K]_0 = [1 + (X-1)H]_0 = 1 - [S]_0 \in \{0, 1\}$.
Si $[K]_0 = 0$, alors nous avons l'alternance de -1 et 1 dans les coefficients non nuls de $K-1$ donc de K.
Si $[K]_0 = 1$, alors $[S]_0 = 0$, et donc le premier coefficient non nul pour $(X-1)S$ est donné en r
avec $[(X-1)S]_r = [S]_{r-1} - [S]_r = 0 - 1 = -1$, donc $[K]_r = -1$, ce qui alterne bien avec $[K]_0 = 1$. /1

$$\boxed{\begin{array}{c}\text{Donc } K \text{ n'a que des coefficients égaux à } -1,\ 0 \text{ ou } 1 \\ \text{et les 1 et } -1 \text{ s'alternent dans la suite des coefficients (non nuls).}\end{array}}$$

On vérifie bien ce résultat sur notre exemple $(p,q)=(3,5)$.

On admet (raisonnement combinatoire) que

$$G_p \times G_q \times K = G_{pq} \times G_1$$

III.5. Quelles sont les racines de K, avec quelle multiplicité ?

---

1 est racine simple de G_{pq} et de G_1, donc racine double de $G_{pq}G_1$.
Et 1 est racine simple de G_p et de G_q, donc racine double de G_pG_q.
Donc 1 n'est pas racine de K.
Et, d'après la factorisation précédente : les racines de K, sont les racines de $G_{p,q}$ qui non racines de G_p et de G_q. /1

Donc les racines de K sont les éléments $\mathbb{U}_{pq} \setminus (\mathbb{U}_p \cup \mathbb{U}_q)$, chacune d'ordre 1.

III.6. D'après la question II.1., il existe $\alpha, \beta \in \mathbb{N}$ tel que $pq+1 = \alpha p + \beta q$.

(a) Vérifier que $1 \leqslant \alpha \leqslant q-1$ et $1 \leqslant \beta \leqslant p-1$.

Si $\alpha = 0$, alors $\alpha p + \beta q = \beta q = pq+1$, donc $(\beta - p)q = 1$. Donc q divise 1. Impossible.
Donc nécessairement, $\alpha \neq 0$ i.e. $\alpha \geqslant 1$. Pour les mêmes raisons : $\beta \geqslant 1$.
Puis $1 - \beta q = (\alpha - q)p$. Or $1 - \beta q < 0$, puisque $\beta \geqslant 1$ et $q > 2$. Donc $\alpha - p < 0$, i.e. $\alpha \leqslant p-1$.
Pour des raisons symétriques : $\beta \leqslant q-1$. /1,5

$1 \leqslant \alpha \leqslant q-1$ et $1 \leqslant \beta \leqslant p-1$.

(b) Montrer la formule :

$$K = \left(\sum_{i=0}^{\alpha-1} X^{ip}\right) \times \left(\sum_{j=0}^{\beta-1} X^{jq}\right) - X^{-pq} \left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \times \left(\sum_{j=\beta}^{p-1} X^{jq}\right).$$

Notons $T = \left(\sum_{i=0}^{\alpha-1} X^{ip}\right) \times \left(\sum_{j=0}^{\beta-1} X^{jq}\right) - X^{-pq} \left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \times \left(\sum_{j=\beta}^{p-1} X^{jq}\right)$. Alors (telescopage)

$$\begin{aligned}
G_p \times G_q \times T &= \left(G_p \sum_{i=0}^{\alpha-1} (X^p)^i\right) \times \left(G_q \sum_{j=0}^{\beta-1} (X^q)^j\right) - X^{-pq} \left(G_p \sum_{i=\alpha}^{q-1} (X^p)^i\right) \times \left(G_q \sum_{j=\beta}^{p-1} (X^q)^j\right) \\
&= \left(\sum_{i=0}^{\alpha-1} (X^p)^{i+1} - (X^p)^i\right) \left(\sum_{j=0}^{\beta-1} (X^q)^{j+1} - (X^q)^j\right) \\
&\quad - X^{-pq} \left(\sum_{i=\alpha}^{q-1} (X^p)^{i+1} - (X^p)^i\right) \left(\sum_{j=\beta}^{p-1} (X^q)^{j+1} - (X^q)^j\right) \\
&= (X^{p\alpha} - 1)\left(X^{q\beta} - 1\right) - X^{-pq} \left(X^{pq} - X^{p\alpha}\right)\left(X^{pq} - X^{q\beta}\right) \\
&= X^{p\alpha+q\beta} - X^{q\beta} - X^{p\alpha} + 1 - X^{pq} + X^{q\beta} + X^{p\alpha} - X^{p\alpha+q\beta-pq} \\
&= X^{pq+1} - X^{pq} - X + 1 = (X^{pq}-1)(X-1) = G_{pq} \times G_1 = G_p \times G_q \times K
\end{aligned}$$

car $p\alpha + q\beta = pq+1$.
Par régularité dans $\mathbb{K}[X]$, on a donc /2,5

$$K = T = \left(\sum_{i=0}^{\alpha-1} X^{ip}\right) \times \left(\sum_{j=0}^{\beta-1} X^{jq}\right) - X^{-pq} \left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \times \left(\sum_{j=\beta}^{p-1} X^{jq}\right)$$

(c) Montrer que le nombre N de coefficients non nuls $[K]_j$ de K est égal à $2\alpha\beta - 1$.

Le polynôme $\sum_{i=0}^{\alpha-1} X^{ip}$ possède exactement α coefficients non nuls ;

et le polynôme $\sum_{j=0}^{\beta-1} X^{jq}$ possède exactement β coefficients non nuls.

Par développement, $\left(\sum_{i=0}^{\alpha-1} X^{ip}\right) \times \left(\sum_{j=0}^{\beta-1} X^{jq}\right)$ possède $\alpha \times \beta$ coefficients non nuls,

ce sont les coefficients de X^0, $X^p \ldots X^{(\alpha-1)p}$; X^q, $X^{p+q} \ldots X^{(\alpha-1)p+q}$; $\cdots$ et $X^{(\beta-1)q} \ldots X^{(\alpha-1)p+(\beta-1)q}$.

De même, par développement, $\left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \times \left(\sum_{j=\beta}^{p-1} X^{jq}\right)$ possède $(q-\alpha)(p-\beta)$ coefficients non nuls,

ce sont les coefficients de $X^{\alpha p+\beta q}$, $X^{(\alpha+1)p+\beta q} \ldots X^{(q-1)p+(p-1)q}$.

Rappelons que $\alpha p + \beta q = pq + 1$, donc $X^{-pq}\left(\sum_{i=\alpha}^{q-1} X^{ip}\right)\left(\sum_{j=\beta}^{p-1} X^{jq}\right)$ possède comme coefficients non nuls,

les coefficients de X^1, $X^{p+1} \cdots X^{pq-p-q}$, en nombre égal à $(q-\alpha)(p-\beta)$.

Tous ces coefficients non nuls sont associés à des monômes distincts.

Donc K possède $\alpha\beta + (q-\alpha)(p-\beta) = 2\alpha\beta - p\alpha - q\beta + pq = 2\alpha\beta - 1$ coefficients non nuls. /2

Le nombre N de coefficients de K est égal à $2\alpha\beta - 1$.

(d) En déduire que $N \leqslant \dfrac{pq-1}{2}$.

On pourra commencer par montrer que N est inférieur à $\dfrac{p^2q^2+1}{2pq}$.

On sait que $\alpha p + \beta q = pq + 1$, donc $\beta = -\dfrac{p}{q}\alpha + p + \dfrac{1}{q}$.

Considérons $N : \alpha \mapsto 2\alpha(-\dfrac{p}{q}\alpha + p + \dfrac{1}{q}) - 1$, polynomiale de la variable réelle α.

$N'(\alpha) = -4\dfrac{p}{q}\alpha + 2p + \dfrac{2}{q}$. Et donc $N'(\alpha) = 0 \iff \alpha = \dfrac{pq+1}{2p}$

Comme $N''(\alpha) < 0$, c'est un maximum. Donc : $\forall\ \alpha \in \mathbb{R}$, $N(\alpha) \leqslant N\left(\dfrac{pq+1}{2p}\right) = \dfrac{(pq+1)^2}{2pq} - 1 = \dfrac{p^2q^2+1}{2pq}$./1,5

Ainsi, $N \leqslant \dfrac{pq}{2} + \dfrac{1}{2pq} \leqslant \dfrac{pq}{2} + \dfrac{1}{2}$ Or p, q sont premiers impairs, donc /1,5

$$\boxed{N = \lfloor N \rfloor \leqslant \frac{pq}{2} + \frac{1}{2} - 1 = \frac{pq-1}{2}.}$$

Remarques !

On peut appliquer la factorisation de la partie précédente, p étant premier $\mathbb{U}_p = \uplus_{d|p}\mathbb{V}_d = \mathbb{V}_1 \uplus \mathbb{V}_p = \{1\} \uplus \mathbb{V}_p$.

$$X^p - 1 = G_p = (X-1)\Phi_p$$

On peut faire la division euclidienne : $\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1 = \sum_{h=0}^{p-1} X^h$.

On a donc $G_pG_qK = (X-1)^2\Phi_p\Phi_qK = G_{pq}(X-1) = (X-1)\prod_{d|pq}\Phi_d = (X-1)^2\Phi_p\Phi_q \times \prod_{d|pq, d\notin\{1,p,q\}}\Phi_d$.

On peut simplifier par $(X-1)^2\Phi_p\Phi_q$ *:* $K = \prod_{d|pq, d\notin\{1,p,q\}}\Phi_d$.

Mais l'ensemble des diviseurs de pq est $\{1, p, q, pq\}$ car p et q sont des nombres premiers. Donc $K = \Phi_{pq}$.