Devoir à la maison n°3

Pour ce troisième devoir, vous devez faire les deux premières parties, puis choisir entre l'un des deux applications : partie III ou partie IV (et pas deux !). La solution sera en binôme.

Lorsqu'une question est jugée, a priori, plus difficile, elle est précédée du symbole $(*)$ voire $(**)$.
La notation tiendra particulièrement compte de **la qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisées**.

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*).

A. Factorisation dans $\mathbb{Z}[X]$

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

1. On va montrer, par contraposée, l'implication :
$$\Big(\forall\, n \in \mathbb{N},\, p \,|\, \big[PQ\big]_n\Big) \Longrightarrow \Big(\forall\, n \in \mathbb{N},\, p \,\Big|\, [P]_n \text{ ou } \forall\, n \in \mathbb{N},\, p \,\Big|\, [Q]_n\Big)$$
   (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.
2. On note, pour $R \in \mathbb{Z}[X] \setminus \{0\}$, $c(R) = \bigwedge_{k=0}^{\deg R} [R]_k$ le PGCD des coefficients de R et $c(0) = 0$.
   $c(R)$ est appelé « contenu de R ».
   Par exemple, $c(2X^3+4X-6) = 2\wedge 0\wedge 4\wedge(-6) = 2$ ou $c(6X^4+10X^2-15X) = 6\wedge 10\wedge(-15) = 1$.
   (a) Montrer, pour $P \neq 0$, que $P_1 := \frac{P}{c(P)}$ est un polynôme à coefficients entiers, puis que $c(P_1) = 1$.
   (b) En exploitant la question 1., et les polynômes P_1 et Q_1, montrer que $c(P \times Q) = c(P) \times c(Q)$
3. Soit $R \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$.
   Montrer que R est irréductible dans $\mathbb{Z}[X]$ ssi R est irréductible dans $\mathbb{Q}[X]$.
4. 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 $\overline{a_k} = a_k \% p$, reste de la division euclidienne de a_k par le nombre premier p).
   Montrer que $\overline{R}(X^p) = (\overline{R}(X))^p$.
   On pourra raisonner par récurrence forte sur $n = \deg R$.

B. Décomposition des polynômes G_n

5. 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 $G_{14} \times U + G_3 \times V = G_1$.
6. Montrer que pour tous entiers $m > n \geqslant 1$, $G_m \wedge G_n = G_{m\wedge n}$

7. Factoriser G_3 et G_4 sur $\mathbb{C}[X]$, puis sur $\mathbb{R}[X]$.
8. Factoriser G_n sur $\mathbb{R}[X]$. On notera, pour $1 \leqslant k \leqslant n$, $c_{k,n} = \cos\frac{2k\pi}{n}$.

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

9. 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 $\mathbb{U}_n = \biguplus_{d|n} V_d$.
   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.
10. 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

C. 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.

11. Montrer que tout nombre entier $R \geqslant (p-1)(q-1)$ appartient à $< p, q >$.
12. Le nombre $(p-1)(q-1) - 1$ appartient-il à $< p, q >$?
13. 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 $(p, q) = (3, 5)$.
14. 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

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

15. Quelles sont les racines de K, avec quelle multiplicité ?
16. 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 $N \leqslant \dfrac{pq-1}{2}$.

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

C′. Sommes des puissances des racines

Soit Q un polynôme de degré n de $\mathbb{C}[X]$: $Q(X) = \sum_{k=0}^{n} b_k X^k$.

On note $\alpha_1, \cdots, \alpha_n$ ses racines complexes, distinctes ou non et on a donc : $Q(X) = b_n \prod_{i=1}^{n}(X - \alpha_i)$.

On note, pour tout $k \in \mathbb{N}^*$: $T_k = \sum_{i=1}^{n} \alpha_i^k$ et $T_0 = n$.

L'objectif est de calculer les termes de la suite $(T_k)_{k\in\mathbb{N}}$ à partir des coefficients du polynôme Q.

11. Exploiter le polynôme Q.

(a) Soit $i \in [\![1, n]\!]$. On note Q_i le polynôme (justifié par la question suivante) défini par : $Q_i(X) = \dfrac{Q(X)}{X - \alpha_i}$.
Montrer que Q' est une combinaison linéaire des Q_i que l'on déterminera.

(b) En remarquant que $Q_i(X) = \dfrac{Q(X) - Q(\alpha_i)}{X - \alpha_i}$, montrer que l'on a :

$$Q_i(X) = \sum_{r=1}^{n} \left(\sum_{k=r}^{n} b_k \alpha_i^{k-r} \right) X^{r-1}$$

(c) Déduire des questions précédentes que l'on a :

$$\forall r \in [\![1, n]\!], \qquad r b_r = \sum_{j=0}^{n-r} b_{r+j} T_j$$

12. Relation de récurrence.

(a) Soit $k \in [\![1, n-1]\!]$. Exprimer T_k en fonction de $T_0, \cdots, T_{k-1}$ et des coefficients du polynôme Q.

(b) Soit $k \geqslant n$. Montrer que l'on a : $\sum_{j=0}^{n} b_j T_{k-n+j} = 0$.
Exprimer alors T_k à l'aide de $T_{k-n}, T_{k-n+1}, \cdots, T_{k-1}$ et des coefficients du polynôme Q.

(c) Conclure.

13. Soit $P \in \mathbb{Z}[X]$, un polynôme unitaire de degré $n \geqslant 1$, irréductible dans $\mathbb{Q}[X]$ et dont toutes les racines complexes sont de module 1.
L'objectif est de montrer que toutes les racines de P sont alors des racines de l'unité. Soient $z_1, \ldots z_n$ les racines complexes de P comptées avec leurs multiplicités, de sorte que

$$P = \prod_{i=1}^{n}(X - z_i)$$

Pour tout entier k, $S_k = z_1^k + z_2^k + \cdots + z_n^k$.

(a) Pourquoi est-ce que pour tout entier $k \in \mathbb{N}$, $S_k \in \mathbb{Z}$.

(b) Montrer qu'il existe deux entiers k et ℓ ($0 \leqslant k < \ell$) tels que $S_{k+i} = S_{\ell+i}$ pour tout $i \in \{0, 1, \ldots n\}$.

On fixe k et ℓ.

(c) Montrer que $\sum_{i=1}^{n} F(z_i)(z_i^\ell - z_i^k) = 0$, pour tout polynôme $F \in \mathbb{C}[X]$ de degré inférieur ou égal à n.

(d) Montrer que $z_1, z_2, \ldots z_n$ sont deux à deux distincts.
En déduire que $z_i^{\ell-k} = 1$, pour tout $i \in \{1, 2, \ldots n\}$ et conclure.