



L'usage des calculatrices est interdit.

Un grand soin devra être apporté à la présentation et à la rédaction.

Si vous constatez ce qui vous semble être une erreur d'énoncé, signalez-le et poursuivez votre composition en expliquant les raisons des initiatives que vous serez amenés à prendre.



Problème. Soit E un ensemble. On rappelle que E est de cardinal p s'il contient p éléments, i.e. s'il existe une bijection entre E et $\llbracket 1, p \rrbracket$. On note alors $|E| = p$. Par convention, $|\emptyset| = 0$. On rappelle également que si E et F sont deux ensembles finis, alors $|E \times F| = |E| \cdot |F|$. De plus, si A et B sont deux parties disjointes finies d'un ensemble E , alors $|A \cup B| = |A| + |B|$.

Dans tout le problème, n désigne un entier naturel non nul. L'ensemble des nombres entiers premiers sera noté $\mathcal{P}$.

La fonction d'Euler φ est définie pour tout entier naturel n non nul par

$$\varphi(n) = |\{k \in \llbracket 1, n \rrbracket ; n \wedge k = 1\}|.$$

On définit le sous-ensemble $\mathbb{U}_n^*$ des racines n -èmes de l'unité par

$$\mathbb{U}_n^* = \left\{ e^{\frac{2ik\pi}{n}}, k \in \llbracket 1, n-1 \rrbracket, k \wedge n = 1 \right\}.$$

On note Φ_n le n -ème polynôme cyclotomique, i.e.

$$\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^*} (X - \zeta).$$

Partie I : La fonction indicatrice d'Euler

1. Déterminer $\varphi(1)$, $\varphi(3)$, $\varphi(6)$, $\varphi(8)$.
2. Soit p un nombre premier positif.
 - a) Calculer $\varphi(p)$ et $\varphi(p^2)$.
 - b) Soit $k \in \mathbb{N}^*$. Calculer $\varphi(p^k)$.
3. Soit d un diviseur de n . On pose $E_d = \{k \in \llbracket 1, n \rrbracket ; n \wedge k = d\}$ et $F_d = \{k \in \llbracket 1, \frac{n}{d} \rrbracket ; \frac{n}{d} \wedge k = 1\}$.
 - a) Montrer que F_d et E_d sont en bijection
 - b) Montrer que $\llbracket 1, n \rrbracket = \bigcup_{d|n} E_d$.
 - c) En déduire que $\sum_{d|n} \varphi(d) = n$.
4. Soit m un entier naturel premier avec n .
 - a) Montrer que $z \in \mathbb{U}_n^*$ si et seulement si $z^n = 1$ et pour tout $k \in \llbracket 1, n-1 \rrbracket$, $z^k \neq 1$.
 - b) Montrer que pour tout $z \in \mathbb{U}_{mn}^*$, il existe un unique couple $(a, b) \in \mathbb{U}_m^* \times \mathbb{U}_n^*$ tel que $z = ab$.
 - c) Montrer que

$$\varphi(mn) = \varphi(m)\varphi(n).$$

5. En déduire que

$$\varphi(n) = n \prod_{p \in \mathcal{P} ; p|n} \left(1 - \frac{1}{p}\right).$$

Partie II : Polynômes cyclotomiques

On note $\mathbb{Q}[X]$ (resp. $\mathbb{Z}[X]$) l'ensemble des polynômes à coefficients rationnels (resp. entiers).

6. Déterminer, sous forme canonique, Φ_1 , Φ_2 , Φ_3 , Φ_4 et Φ_5 .

7. Déterminer le degré de Φ_n .

8. Soit p un nombre premier positif. Déterminer Φ_p .

9. Soit p un nombre premier positif ne divisant pas n . Montrer que

$$\Phi_{np}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}.$$

10. On suppose que n est impair. Montrer que $\Phi_{2n}(X) = \Phi_n(-X)$.

11. Montrer que

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

12. Soit $A \in \mathbb{Z}[X]$. Le contenu de A , noté $c(A)$, est le plus grand diviseur commun des coefficients de A . On dit que A est primitif si $c(A) = 1$. Dans cette question, $(A, B) \in \mathbb{Z}[X]^2$.

a) Montrer que si A et B sont primitifs, alors AB est primitif.

b) Montrer que pour tout entier naturel m , $c(mA) = m \cdot c(A)$, puis que $c(AB) = c(A)c(B)$.

c) Soient P et Q deux polynômes unitaires de $\mathbb{Q}[X]$ tels que $PQ \in \mathbb{Z}[X]$. Montrer que P et Q appartiennent à $\mathbb{Z}[X]$.

d) On suppose que $B \neq 0$ et unitaire. On note $A = BQ + R$ la division euclidienne de A par B (dans $\mathbb{C}[X]$). Montrer que $(Q, R) \in \mathbb{Z}[X]^2$.

13. En déduire que $\Phi_n \in \mathbb{Z}[X]$.

Partie III : Irréductibilité de certains polynômes cyclotomiques

Soit $P \in \mathbb{Q}[X]$. P est dit irréductible dans $\mathbb{Q}[X]$ si pour tout $(A, B) \in \mathbb{Q}[X]^2$,

$$(P = AB) \Rightarrow (A \text{ ou } B \text{ est associé à } P).$$

Soit $P = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$. On admet le critère d'Eisenstein, i.e. si

1. p ne divise pas a_n ,
2. $\forall i \in \llbracket 0, n-1 \rrbracket$, p divise a_i ,
3. p^2 ne divise pas a_0 ,

alors A est irréductible dans $\mathbb{Q}[X]$.

Dans cette partie, p désigne un nombre premier positif. On note

$$\omega = e^{\frac{2i\pi}{p}} \text{ et } \mathcal{Z} = \{P \in \mathbb{Q}[X] ; P(\omega) = 0\}.$$

14. On suppose que Φ_p est irréductible dans $\mathbb{Q}[X]$.

a) Montrer que $\mathcal{Z}$ est non vide.

b) Montrer qu'il existe $Q_0 \in \mathcal{Z}$ unitaire et de degré minimal.

c) En déduire que $\mathcal{Z} = \{\Phi_p \cdot Q, Q \in \mathbb{Q}[X]\}$.

15. Montrer que le polynôme $Q = \sum_{k=0}^{p-1} (X+1)^k$ est irréductible dans $\mathbb{Q}[X]$.

16. En déduire que Φ_p est irréductible dans $\mathbb{Q}[X]$.