Partie I

Dans toute cette partie, n désigne un entier naturel non nul. On rappelle que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif de cardinal n. Pour tout entier relatif a, on note $\overline{a}$ la classe de a modulo n.

1. Soit $a \in \mathbb{Z}$ vérifiant $a \wedge n = 1$.
   (a) Montrer qu'il existe deux entiers relatifs b et v tels que $ab + nv = 1$.
   (b) Montrer que $\overline{a} \times \overline{b} = \overline{1}$. Qu'en déduit-on pour l'élément $\overline{a}$ de l'anneau $\mathbb{Z}/n\mathbb{Z}$?
   (c) Dans cette question uniquement, on prend $n = 2025$. Quel est l'inverse dans $\mathbb{Z}/n\mathbb{Z}$ de l'élément $\overline{1492}$?
   (d) Soit maintenant $a \in \mathbb{Z}$ vérifiant $a \wedge n = \delta \neq 1$. Soit $b = \frac{n}{\delta} \in \mathbb{Z} \setminus \{0\}$. Que vaut $a \times b$? En déduire que $\overline{a}$ n'est pas inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

   On vient de démontrer qu'un élément $x = \overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $a \wedge n = 1$. On note dorénavant $\mathcal{U}_n$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. On pose également $\varphi(n) = \operatorname{card} \mathcal{U}_n$. La fonction φ est appelée la fonction indicatrice d'Euler. *À titre d'exemple, $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(5) = 4$ et $\varphi(6) = 2$.*

2. On suppose donnée une fonction `pgcd` renvoyant le pgcd de deux entiers. Écrire une fonction `phi_naive` prenant en paramètre un entier $n \geq 1$ et renvoyant $\varphi(n)$.
3. Donner dans un tableau la valeur de $\varphi(n)$ pour $n \in [\![1, 20]\!]$.

Partie II

Dans cette partie, on établit une formule donnant la valeur de $\varphi(n)$ pour tout entier $n \geq 2$.

1. Soit p un nombre premier.
   (a) Calculer $\varphi(p)$.
   (b) Plus généralement, calculer $\varphi(p^\alpha)$ pour tout entier naturel non nul α.
2. On se donne deux entiers naturels non nuls a et b *premiers entre-eux*. Pour tout entier relatif x, on note $\overline{x}$ la classe de x modulo ab, $\hat{x}$ la classe de x modulo a, et $\tilde{x}$ la classe de x modulo b. On considère l'application

   $$f : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

   définie pour tout $x \in \mathbb{Z}$ par

   $$f(\overline{x}) = (\hat{x}, \tilde{x})$$

   (a) Soient $x, x' \in \mathbb{Z}$ vérifiant simultanément $x \equiv x' \mod a$ et $x \equiv x' \mod b$.
      i. Montrer que $x \equiv x' \mod ab$.
      ii. Que vient-on de montrer à propos de la fonction f ?
   (b) Soient α et β deux entiers relatifs.
      i. Soient $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$ (l'existence de tels entiers u et v est assurée par le théorème de Bézout). Soit $x_0 = ua\beta + vb\alpha$. Montrer que $x_0 \equiv \alpha \mod a$ et $x_0 \equiv \beta \mod b$.

ii. En déduire le *théorème des restes chinois* : f est surjective.

iii. Écrire une fonction `chinois` prenant en paramètres 4 entiers a, b, α, β et telle que, si a et b sont premiers entre-eux, l'appel `chinois(a, b, alpha, beta)` renvoie l'unique entier $x \in [\![0, ab-1]\!]$ tel que $x \equiv \alpha \bmod a$ et $x \equiv \beta \bmod b$.

(c) Soit $x \in \mathbb{Z}/ab\mathbb{Z}$. Montrer que si $x \in \mathcal{U}_{ab}$ alors $f(x) \in \mathcal{U}_a \times \mathcal{U}_b$.

On peut donc considérer la fonction $g : \mathcal{U}_{ab} \to \mathcal{U}_a \times \mathcal{U}_b$ définie par $g(x) = f(x)$ pour tout $x \in \mathcal{U}_{ab}$.

(d) En utilisant l'injectivité de f, prouver que g est injective.

(e) Soit $(\alpha, \beta) \in \mathcal{U}_a \times \mathcal{U}_b$. Soit $x \in \mathbb{Z}/ab\mathbb{Z}$ l'unique antécédent de (α, β) par f. Montrer que $x \in \mathcal{U}_{ab}$ et en déduire que (α, β) a un antécédent par g.

(f) L'application g est donc bijective. En déduire que $\varphi(ab) = \varphi(a)\varphi(b)$.

3. Soit n un entier naturel supérieur ou égal à 2. On écrit n sous la forme $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ où les p_i sont des nombres premiers distincts et les α_i des entiers naturels non nuls. Montrer que
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_k}\right)$$

4. Que valent $\varphi(2024)$? $\varphi(2025)$?

5. On suppose donnée une fonction `facteurs_premiers` prenant en paramètre un entier $n \geq 1$ et telle qu'un appel à `facteurs_premiers(n)` renvoie, en reprenant les notations de la question 3, la liste $[(p_1, \alpha_1), \dots, (p_k, \alpha_k)]$. Écrire une fonction `euler_phi` prenant en paramètre un entier $n \geq 1$ et renvoyant $\varphi(n)$.

Partie III

Ce qui précède montre que si l'on sait décomposer n en produit de facteurs premiers, alors on sait calculer $\varphi(n)$. On se pose dans cette partie la question de la réciproque : *si l'on sait calculer $\varphi(n)$, sait-on décomposer n en produit de facteurs premiers ?*. On donne dans ce qui suit la réponse à cette question dans un cas particulier.

On se donne un entier $n \geq 2$. On suppose que $n = pq$ où p et q sont deux nombres premiers distincts.

1. Déterminer $\varphi(n)$ en fonction de p et q, et en déduire $p + q$ en fonction de n et de $\varphi(n)$.
2. Montrer que p et q sont les racines d'une équation du second degré dont les coefficients ne dépendent que de n et de $\varphi(n)$.
3. Écrire une fonction `decomposer` prenant en paramètres deux entiers n et v, et telle que si $n = pq$ est le produit de deux nombres premiers distincts p et q, et $v = \varphi(n)$, alors l'appel `decomposer(n,v)` renvoie le couple (p, q).
4. L'entier
$$n = 124702704813441811944131913231501396808839604840033$$
est le produit de 2 nombres premiers p et q. Sachant que
$$\varphi(n) = 124702704813441811944131890897145841253284150406660$$
que valent p et q ?