Recasages possibles : 102, 120, 121.
Référence : Théorie de Galois, Gozard (p. 67-68, 84).

Développement Soit $n \in \mathbb{N}_{\geqslant 2}$.

Lemme 1 On a $X^n - 1 = \prod_{d|n} \Phi_d(X)$. En particulier, $\Phi_n \in \mathbb{Z}[X]$.

Lemme 2 Soit $a \in \mathbb{Z}$, et p premier divisant $\Phi_n(a)$ mais ne divisant pas $\Phi_d(a)$ pour $d \mid n$, $d < n$. Alors, $p \equiv 1\ [n]$.

Théorème 3 (Dirichlet faible) Il existe une infinité de nombres premiers congrus à 1 modulo n.

- **Preuve du Lemme 1** : Par définition, pour tout $d \mid n$, $\Phi_d(X) = \prod_{\zeta \in \mu_d^*} (X - \zeta)$.

  Montrons que $\{\mu_d^* : d \mid n\}$ est une partition de μ_n. D'après le théorème de Lagrange, l'ordre des éléments de μ_n divise $\#\mu_n = n$. Or, dire que $\zeta \in \mu_n$ est d'ordre d revient exactement à dire que $\zeta \in \mu_d^*$. Ainsi, si $d \mid n$, μ_d^* est l'ensemble des éléments de μ_n d'ordre d, donc

  $$\mu_n = \bigsqcup_{d|n} \mu_d^*.$$

  Ainsi, puisque $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta)$, on obtient

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

  Notons qu'on retrouve en considérant les degrés la formule $n = \sum_{d|n} \varphi(d)$.

  On montre alors par récurrence forte sur $n \in \mathbb{N}_{\geqslant 1}$ la propriété $\Phi_n(X) \in \mathbb{Z}[X]$:
  · Pour $n = 1$, on a $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.
  · Soit $n \in \mathbb{N}_{\geqslant 2}$. Supposons que pour tout $k < n$, on ait $\Phi_k(X) \in \mathbb{Z}[X]$. Posons

  $$F(X) = \prod_{\substack{d|n \\ d<n}} \Phi_d(X).$$

  Par hypothèse de récurrence, $F(X) \in \mathbb{Z}[X]$. On effectue la division euclidienne de $X^n - 1$ par F dans $\mathbb{Z}[X]$ (possible même si $\mathbb{Z}[X]$ n'est pas euclidien car F est unitaire) : il existe $Q, R \in \mathbb{Z}[X]$ tels que

  $$X^n - 1 \overset{(*)}{=} F(X)Q(X) + R(X) \quad \text{avec } \deg(R) < \deg(F).$$

  Or, dans l'anneau euclidien $\mathbb{C}[X]$, d'après la formule précédente, $F(X)$ divise $X^n - 1$ donc la division euclidienne de $X^n - 1$ par $F(X)$ est

  $$X^n - 1 = F(X)\Phi_n(X).$$

  Ainsi, comme l'égalité $(*)$ est une division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{C}[X]$, par unicité d'une telle écriture, on a $R(X) = 0$ et $Q(X) = \Phi_n(X)$. En particulier, on a $\Phi_n(X) \in \mathbb{Z}[X]$, ce qui conclut la récurrence et la preuve du **Lemme 1**.

- *Preuve du Lemme 2* : Soit $a \in \mathbb{Z}$ et p premier divisant $\Phi_n(a)$. On note $\overline{k}$ la classe de $k \in \mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z}$. On a d'après le **Lemme 1**

  $$a^n - 1 = \Phi_n(a) \prod_{\substack{d|n \\ d<n}} \Phi_d(a) \text{ donc } \Phi_n(a) \mid a^n - 1.$$

  En particulier, $p \mid a^n - 1$, c'est-à-dire que $\overline{a}^n = \overline{1}$. Ainsi, $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ et si δ est l'ordre de $\overline{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$, on a $\delta \mid n$. Encore d'après le **Lemme 1**, on a

  $$a^\delta - 1 = \prod_{d|\delta} \Phi_d(a).$$

  Ainsi, $\prod_{d|\delta} \overline{\Phi_d(a)} = \overline{0}$. Or, par intégrité de $\mathbb{Z}/p\mathbb{Z}$, il existe d divisant δ (donc divisant n) tel que $\overline{\Phi_d(a)} = \overline{0}$, c'est-à-dire $p \mid \Phi_d(a)$. Or, par hypothèse, le seul diviseur d de n tel que $p \mid \Phi_d(a)$ est n, d'où $\delta = n$. Or, d'après le théorème de Lagrange, l'ordre de $\overline{a}$ divise $\#(\mathbb{Z}/p\mathbb{Z})^\times = p-1$, d'où $n \mid p-1$, ou encore $p \equiv 1\ [n]$.

- *Preuve du Théorème 3* : Il faut et il suffit de montrer que pour tout $N \in \mathbb{N}_{\geqslant n}$, il existe $p > N$ premier congru à 1 modulo n. Fixonx $N \in \mathbb{N}_{\geqslant n}$ et posons $a = 3N!$. D'après le **Lemme 1**, $\Phi_n(a) \in \mathbb{Z}$ et comme $a \geqslant 3 > 2$, $a - 1 > 1$ donc

  $$|\Phi_n(a)| = \prod_{\substack{k=1 \\ \text{pgcd}(k,n)=1}}^{n} |a - e^{2i\pi\frac{k}{n}}| \geqslant \prod_{\substack{k=1 \\ \text{pgcd}(k,n)=1}}^{n} (a-1) \geqslant a - 1 \geqslant 2.$$

On va montrer que tout diviseur p premier de $\Phi_n(a)$ vérifie $p > N$ et $p \equiv 1\ [n]$.

Soit p diviseur premier de $\Phi_n(a)$. Supposons $p \leqslant N$. Alors p apparaît dans la définition de $N!$ (c'est le produit des entiers inférieurs ou égaux à N), donc $p \mid a$. Ainsi, p divise tout polynôme en a à coefficient constant nul. En particulier, p divise $\big(\Phi_n(X) - \Phi_n(0)\big)(a) = \Phi_n(a) - \Phi_n(0)$. Or, comme $p \mid \Phi_n(a)$, on a $p \mid \Phi_n(0) = \pm 1$, ce qui est absurde. Ainsi on a bien $p > N$. On veut désormais que p vérifie les hypothèses du **Lemme 2**, auquel cas on aura bien le résultat souhaité. Supposons qu'il existe $\delta < n$ tel que $\delta \mid n$ et $p \mid \Phi_\delta(a)$. D'après le **Lemme 1**, on a

$$X^n - 1 = \Phi_n(X)\Phi_\delta(X) \prod_{\substack{d \mid n \\ d \neq n, \delta}} \Phi_d(X).$$

En projetant dans $\mathbb{Z}/p\mathbb{Z}$, on obtient

$$X^n - \overline{1} = \overline{\Phi_n(X)} \cdot \overline{\Phi_\delta(X)} \cdot \prod_{\substack{d \mid n \\ d \neq n, \delta}} \overline{\Phi_d(X)}.$$

Or, comme $p \mid \Phi_n(a)$ et $p \mid \Phi_\delta(a)$, on a $\overline{\Phi_n(a)} = \overline{\Phi_n}(\overline{a}) = \overline{0}$ et de même $\overline{\Phi_\delta(a)} = \overline{0}$. Ainsi, le polynôme $X^n - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$ admet $\overline{a}$ comme racine double. Or c'est absurde car son polynôme dérivé est $\overline{n}X^{n-1}$, qui est premier avec $X^n - \overline{1}$. En effet, comme $p > N \geqslant n$, en particulier $p \nmid n$ donc $\overline{n} \in (\mathbb{Z}/p\mathbb{Z})^\times$, et on a la relation de Bézout

$$\overline{n}^{-1}X \times \overline{n}X^{n-1} + (-1) \times (X^n - \overline{1}) = \overline{1}.$$

Donc d'après le théorème de Bézout, on a bien $\operatorname{pgcd}(X^n - \overline{1}, \overline{n}X^{n-1}) = \overline{1}$, et donc $X^n - \overline{1}$ ne peut pas avoir de racine multiple. Par conséquent, p ne divise pas les $\Phi_d(a)$ pour $d \mid n$ et $d < n$, et $p \mid \Phi_n(a)$ donc on peut appliquer le **Lemme 2**, et on obtient $p \equiv 1\ [n]$.

Finalement, on a bien montré que pour tout $N \geqslant$, il existe $p > N$ premier tel que $p \equiv 1\ [n]$, d'où l'existence d'une infinité de nombres premiers congrus à 1 modulo n.