Dirichlet Faible.

Gozard p84
FGN algèbre 1

Théorème : Il existe une infinité de nombre premier du type $\lambda n + 1$ $\lambda \in \mathbb{N}^*$

Lemme : Soit $a \in \mathbb{Z}$ et p premier tq $p \mid \Phi_n(a)$ et $p \nmid \Phi_d(a)$ $\forall d \mid n$ alors $p \equiv 1 [n]$ $d < n$

Preuve Lemme : Soit p premier vérifiant l'hypothèse.

Comme $p \mid \Phi_n(a)$, on a $\Phi_n(a) = kp$ et donc $a^n - 1 = \prod_{d \mid n} \Phi_n(a) = \Phi_n(a) \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(a)$

$= p \times k \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(a)$

Donc $p \mid a^n - 1$.

On a alors l'ordre de $\bar{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ qui divise n.

Montrons que son ordre est exactement n : On note w son ordre.

Si $w \mid n$ et $w < n$, on a dans $\mathbb{Z}/p\mathbb{Z}$: $\bar{a}^w - 1 = \prod_{d \mid w} \overline{\Phi_d(a)}$

Or si $d \mid w$, alors $d \mid n$, et par hypothèse, $\overline{\Phi_d(a)} \neq \bar{0}$. Or $\mathbb{Z}/p\mathbb{Z}$ est un corps (=> intègre)

On a alors $\prod_{d \mid w} \overline{\Phi_d(a)} \neq \bar{0} \Rightarrow \bar{a}^w \neq \bar{1}$ Impossible par définition de w. Donc $w = n$.

Donc l'ordre de a, qui est n, divise $p - 1$ donc $p \equiv 1 [n]$ (Lagrange)

Preuve Théorème : On raisonne par l'absurde et on suppose qu'il existe un nombre fini d'entiers premiers congrus à $1 \bmod(n)$ notés $p_1, \dots, p_q$. On pose $N = n p_1 p_2 \dots p_q$ et $B = \prod_{\substack{d \mid N \\ d < N}} \Phi_d$. Il faut donc trouver $a \in \mathbb{Z}$ et p premier tq $p \mid \Phi_N(a)$ et $p \nmid B(a)$ (On aura le Lemme)

Le polynôme B est premier avec Φ_N car ils sont scindés et n'ont aucunes racines en commun dans $\mathbb{C}[X]$, donc $B \wedge \Phi_N = 1$ dans $\mathbb{Q}[X]$ car les coeff de B et Φ_N sont entiers, ainsi, l'algo d'Euclide fonctionne pareil sur $\mathbb{Q}[X]$ que sur $\mathbb{C}[X]$.

D'après le Théorème de Bezout : $\exists (U,V) \in \mathbb{Q}[X]^2$ tq $1 = U\Phi_N + VB$.

Il existe $a \in \mathbb{Z}$, $U' = aU \in \mathbb{Z}[X]$ (On prend a = ppcm (dénominateur coeff de U et de V))
$V' = aV \in \mathbb{Z}[X]$

Comme $\Phi_N \neq 0$ et $\Phi_N \neq \pm 1$, on peut même choisir $a \in \mathbb{Z}$ tel que $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$ étant donné l'infinité de $a \in \mathbb{Z}$ vérifiant $aU \in \mathbb{Z}[X]$ et $aV \in \mathbb{Z}[X]$,

On a donc $a = U'\Phi_N + V'B$ et en particulier, $\circledast$ $a = U'(a)\Phi_N(a) + V'(a)B(a)$

Soit p premier divisant $\Phi_N(a)$. Alors $p \mid a^N - 1$ car $\Phi_N \mid X^N - 1$ dans $\mathbb{Z}[X]$

Dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^N = \overline{1}$ et donc $\overline{a}$ est inversible, ce qui signifie que a est premier avec p.

Si p divisait $B(a)$, il diviserait a, d'après $\circledast$, ce qui est exclu.

On est donc dans les hypothèses du Lemme :

Donc $p \equiv 1 [N]$

D'où $\begin{cases} p \equiv 1 [n] \\ p \neq p_i \quad \forall i \in [\![1, q]\!] \end{cases}$ qui est la contradiction voulue.