Théorème de Dirichlet (faible)

Lemme 1 : $\Phi_n(X) \in \mathbb{Z}[X] \quad \forall n \in \mathbb{N}$

Lemme 2 : Soit p premier, si $\exists a \in \mathbb{Z}$, $n \in \mathbb{N}$ tels que
$p \mid \Phi_n(a)$ et $p \nmid \Phi_d(a) \quad \forall d \in \mathbb{N}$ $d \mid n$
alors $p \equiv 1 \ [n]$

Théorème : $\forall n \in \mathbb{N}^*$, il existe une infinité de nombres premiers de la forme $kn+1$ ($p \equiv 1 [n]$)

preuve Lemme 1 : on a $X^n - 1 = \prod_{k=1}^{n} (X - e^{\frac{2ik\pi}{n}})$
Comme U_n := ensemble des racines n-ème de l'unité) est réunion disjointe des P_d (= ensemble des racines primitives de l'unité) pour $d \mid n$
On a alors

$$X^n - 1 = \prod_{\xi \in U_n} (X - \xi) = \prod_{d \mid n} \left(\prod_{\xi \in P_d} (X - \xi) \right) = \prod_{d \mid n} \Phi_d$$

On va faire une preuve par récurence en utilisant le lemme suivant

(Lemme : $A, B \in \mathbb{Z}[X]$, B non nul unitaire. Le quotient et le reste de la division euclidienne de A par B dans $\mathbb{C}[X]$ sont aussi dans $\mathbb{Z}[$

récurence forte :
vrai par déf pour $n = 1$
si $n \geq 2$ Φ_n est le quotient dans $\mathbb{C}[X]$ de $X^n - 1$ par B où B est le produit des Φ_d où d sont les diviseurs strict de n
D'après hypothèse de récurence B est à coef entier et unitaire.
Donc d'après le lemme Φ_n aussi.

preuve Lemme 2 : Soit p, a et n selon les hypothèses

$p \mid \Phi_n(a) \Rightarrow p \mid a^n - 1$ D'où ordre de $\bar{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ divise n

montrons que cet ordre est exactement n.

si $d \mid n$ et $d < n$ on a dans $\mathbb{Z}/p\mathbb{Z}$

$$\bar{a}^d - 1 = \prod_{d' \mid d} \overline{\Phi_{d'}(a)}$$

or si $d' \mid d$, $d' \mid n$ et par hypothèse $\overline{\Phi_{d'}(a)} \neq 0$

$\mathbb{Z}/p\mathbb{Z}$ étant un corps, ce produit est non nul (Intégrité)

D'où $\bar{a}^d \neq 1$. Ainsi l'ordre de a est n dans $(\mathbb{Z}/p\mathbb{Z})^\times$

D'après le théorème de Lagrange $n \mid |(\mathbb{Z}/p\mathbb{Z})^\times|$

Soit $n \mid p-1$ D'où $p \equiv 1 [n]$

preuve Th : Supposons par l'absurde, il existe un nombre fini $p_1, p_2 \dots, p_q$ de premiers congrues à 1 modulo n.

On pose $N = n p_1 p_2 \dots p_q$ on cherche alors p et a vérifiant les hypothèses précédentes pour N. Le Lemme assurerait $p \equiv 1 [N]$ donc $p \equiv 1 [n]$ et $p \neq p_1, \dots p_q$ ce qui aboutirait à une contradiction

On cherche alors $a \in \mathbb{Z}$ et p premier tels que $p \mid \Phi_N(a)$ mais $p \nmid \Phi_d(a)$, $d \mid N$, $d < N$. On note $B = \prod_{\substack{d \mid n \\ d < N}} \Phi_d$

On cherche alors a et p / $p \mid \Phi_N(a)$ et $p \nmid B(a)$

B est premier avec Φ_n dans $\mathbb{C}[X]$ (scindés sans racines communes) donc dans $\mathbb{Q}[X]$. Donc d'après la relation de Bezout, $\exists (U, V) \in \mathbb{Q}(X)$ tels que $1 = U\Phi_N + VB$ $\exists a \in \mathbb{Z}$ / aU et $aV \in \mathbb{Z}[X]$

et comme $\Phi_N \neq 0$ et $\Phi_N \neq \pm 1$ on peut choisir a / $\Phi_N(a) \neq 0$ et $\neq \pm 1$

on pose $U' = aU$ et $V' = aV \in \mathbb{Z}[X]$ et on a

$$a = U'\Phi_N + V'B \quad \text{soit} \quad a = U'(a)\Phi_N(a) + V'(a)B(a) \quad (*)$$

Soit p premier qui divise $\Phi_N(a)$, alors $p \mid a^N - 1$

Dans $\mathbb{Z}/p\mathbb{Z}$ $\bar{a}^N = 1$ donc $\bar{a}$ inversible donc a et p premier entre eux

si $p \mid B(a)$ il diviserait a d'après $(*)$ ce qui est impossible

On a bien $p \mid \Phi_N(a)$ et $p \nmid B(a)$

On aboutit alors à une contradiction d'après le Lemme 2.