Théorème de Dirichlet faible

Ce développement se trouve dans les recueils d'oraux X-ENS.
Le but de ce développement est de montrer une version faible du théorème de Dirichlet :

Théorème. *Soit $n \geqslant 1$ fixé. Il existe une infinité de nombres premiers congrus à 1 modulo n.*

Pour ce faire, on indroduit l'ensemble $\mathcal{P}_d$ des racines primitives d^{e} de l'unité (on note $\mathbb{U}_d$ les racines d^{e} de l'unité), et Φ_d le d^{e} polynôme cyclotomique :

$$\Phi_d = \prod_{\xi \in \mathcal{P}_d} (X - \xi).$$

On admet aussi le lemme suivant (dont la démonstration se justifie sans peine via l'algorithme d'Euclide) : si $A, B \in \mathbb{Z}[X]$ avec B unitaire, alors le quotient et le reste de la division euclidienne dans $\mathbb{C}[X]$ de A par B sont dans $\mathbb{Z}[X]$.

Démonstration. 1. Φ_d est à coefficients entiers. Soit $\xi \in \mathbb{U}_n$. Alors ξ est d'ordre $d \mid n$. Aussi,

$$\mathbb{U}_n = \bigcup_{d|n} \mathcal{P}_d \qquad \text{(union disjointe).}$$

De fait,

$$X^n - 1 = \prod_{\xi \in \mathbb{U}_n} (X - \xi) = \prod_{d|n} \Phi_d.$$

On va maintenant établir l'appartenance à $\mathbb{Z}[X]$ de Φ_n par récurrence sur n.
Pour $n = 1$, c'est clair.
Si c'est vrai pour tout $k < n$, puisque Φ_n est le quotient de $X^n - 1$ par $\prod_{d \neq n} \Phi_d$, qui est à coefficients entiers par hypothèse de récurrence, et unitaire. Il est dont à coefficients entiers.

2. Preuve du théorème On fixe donc $n \in \mathbb{N}^*$. Supposons qu'il existe un nombre fini de nombres premiers de la forme $\lambda n + 1$, notés $p_1 < \cdots < p_r$. On pose $N = n p_1 p_2 \cdots p_r$.
Soit $a \in \mathbb{Z}$ et p premier tels que p divise $\Phi_n(a)$ mais aucun des $\Phi_d(a)$ pour d diviseur strict de n. p divise $a^N - 1$ donc donc N divise l'ordre de a dans $(\mathbb{Z}/p\mathbb{Z})^*$. Montrons que cet ordre est N.
Dans $(\mathbb{Z}/p\mathbb{Z})^*$, on a

$$\overline{a}^d - 1 = \prod_{d'|d} \underbrace{\overline{\Phi_{d'}(a)}}_{\neq 0 \text{ car } d'|n} .$$

Par intégrité, $\overline{a}^d - 1 \neq 0$ et l'ordre de a est exactement N, et divise $p - 1$. ceci implique que $p \equiv 1 \mod N$, donc que $p \equiv 1 \mod n$, donc que p est l'un des p_i. Or c'est impossible, car $p \equiv 1 \mod N$. L'ensemble des premiers de la forme $\lambda n + 1$ est donc infini.
Reste à montrer l'existence de tels couples (a, p) tels que p divise $\Phi_n(a)$ et pas $\Phi_d(a)$ pour d diviseur strict de n. Soit $B \in \mathbb{Z}[X]$ tel que $X^n - 1 = \Phi_n(X)B(X)$. Puisque Φ_n et B n'ont aucune racine commune dans $\mathbb{C}$, ils sont premiers entre eux dans $\mathbb{C}[X]$, donc dans $\mathbb{Q}[X]$. Il existe donc $U, V \in \mathbb{Q}[X]$ tels que $UB + V\Phi_n = 1$.
Soit $a \in \mathbb{Z}$ tel que $U' = aU \in \mathbb{Z}[X]$ et $V' = aV \in \mathbb{Z}[X]$. Alors, $a = U'B + V'\Phi_n$, et, en particulier,

$$a = U'(a)B(a) + V'(a)\Phi_n(a).$$

Soit p premier divisant $\Phi_n(a)$: p divise alors $a^n - 1$. Dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^n = 1$ donc $\overline{a}$ est inversible, donc $a \wedge p = 1$. Si p divise l'un des $\Phi_d(a)$ $(d \neq n)$, p diviserait $B(a)$ donc diviserait a, ce qui est impossible. Le couple ainsi défini convient donc.

□