Titre : Théorème de Dirichlet faible
Recasages : 102,120,121,141
Thème : Polynômes, arithmétique
Références : Francinou, Gianella, Nicolas - Oraux X-Ens algèbre 1 (p. 158,159)

Théorème 1. *Pour tout $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers congrus à 1 modulo n, c'est à dire de la forme*

$$p = 1 + \lambda n, \lambda \in \mathbb{Z}$$

Lemme 2. *Soit $a \in \mathbb{Z}$, et p un nombre premier tel que*

- *p divise $\Phi_n(a)$*
- *p ne divise pas $\Phi_d(a)$ pour tout d diviseur propre de n.*

Alors p est congru à 1 modulo n.

Démonstration. Comme $p|\Phi_n(a)$, p divise $a^n - 1$ car $\Phi_n | X^n - 1$, donc $a^n \equiv 1[p]$, donc l'ordre de a dans $\mathbb{F}_p^*$ divise n. Montrons que cet ordre est exactement n, si $d < n$ est un diviseur de n, alors

$$a^d - 1 = \prod_{d'|d} \Phi_{d'}(a)$$

or p ne divise pas ce produit par hypothèse, donc a est bien d'ordre exactement n dans $\mathbb{F}_p^*$, par le théorème de Lagrange, n divise $p - 1 = |\mathbb{F}_q^*|$, d'où le résultat. □

Supposons par l'absurde qu'il n'existe qu'un nombre fini $p_1, \cdots, p_n$ de nombres premiers congrus à 1 modulo n, on souhaite appliquer notre lemme, mais pour parvenir à une franche contradiction, on change n en $N := np_1 \cdots p_n$ (si $p \equiv 1[N]$ et $p \neq \{p_1, \cdots, p_n\}$, on aura bien $p \equiv 1[n]$) on recherche donc a et p tels que $p|\Phi_N(a)$ et $p \nmid \Phi_d(a)$ pour d diviseur strict de N. Posons

$$B(X) := \prod_{\substack{d|N \\ d<N}} \Phi_d(X)$$

on recherche donc p divisant $\Phi_N(a)$ et $B(a)$. Les polynômes Φ_N et B sont premiers entre eux dans $\mathbb{C}[X]$ (ils sont scindés et n'ont aucune racines distinctes) ils sont dont aussi premiers entre eux dans $\mathbb{Q}[X]$ (l'algo d'Euclide tournera de la même manière), donc par le théorème de Bézout, il existe U et V dans $(\mathbb{Q}[X])^2$ tels que

$$\Phi_N U + BV = 1$$

On choisit alors $a \in \mathbb{N}$ tel que $U' = aU \in \mathbb{Z}[X]$ et $V' = aV \in \mathbb{Z}[X]$ (en prenant pour a comme $N!$ fois le ppcm des dénominateurs des coefficients de V et U). Comme $\Phi_N \notin \{-1, 0, 1\}$, on peut même choisir a tel que $\Phi_N(a) \notin \{-1, 0, 1\}$. On a en particulier

$$a = U'(a)\Phi_N(a) + V'(a)B(a)$$

Par hypothèse, $\Phi_N(a)$ admet des facteurs premiers $\geqslant 2$, montrons que si p premier divise $\Phi_N(a)$, alors $p > N$, en effet dans le cas contraire, p divise $N!$ et a, donc p divise $\Phi_N(a) - \Phi_N(0)$, comme p divise $\Phi_N(a)$, on en déduit que p divise $\Phi_N(0) = \pm 1$, ce qui est absurde.
On peut donc prendre p premier divisant a et différent de tous les p_i, on a $a^N \equiv 1[p]$, donc $a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$, donc $a \wedge p = 1$. Si $p|B(a)$, alors $a = \Phi_N(a)U'(a) + V'(a)B(a) = 0[p]$, ce qui est contradictoire, donc $p \nmid B(a)$ ce qui clos la démonstration.