Théorème de Dirichlet faible

Notations :

- Pour tout n entier naturel on définit le n-ème polynôme cyclotomique $\phi_n(X) = \prod_{d \wedge n = 1} (X - e^{\frac{2ik\pi}{n}})$

Théorème : Soit $n \in \mathbb{N}^*$. Il existe une infinité de nombres premiers p tels que $p = 1[n]$.

Lemme 0 : Pour tout $n \in \mathbb{N}$, $X^n - 1 = \prod_{d|n} \phi_d(X)$.

Lemme 1 : Soit $a, n \in \mathbb{N}$ et p un nombre premier tel que $\begin{cases} p | \phi_n(a) \\ p \wedge \phi_d(a) = 1 \text{ si d divise strictement n} \end{cases}$.
Alors $p = 1[n]$.

Preuve du lemme 0 : Admis.

Preuve du lemme 1 : Soit a, p et n comme dans l'énoncé. Comme $p|\phi_n(a)$ on sait en particulier que $p|a^n - 1$ avec le lemme 0. Il suit que $\overline{a}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$ et $\delta := \text{ordre}(\overline{a})|n$. Montrons que $\delta = n$.

Si $d|n$ et $d < n$ on a, dans $\mathbb{Z}/p\mathbb{Z}$,

$$\overline{a}^d - \overline{1} = \prod_{d'|d} \overline{\phi_{d'}(a)}.$$

Par hypothèse, comme $d'|d$ implique que $d'|n$, $\overline{\phi_{d'}(a)} \neq \overline{0}$. Ainsi $\overline{a}^d - \overline{1} \neq 0$ car $\mathbb{Z}/p\mathbb{Z}$ est intègre. Ainsi $\overline{a}$ n'est pas d'ordre d, donc $\overline{a}$ est d'ordre n.

Comme $\delta | p - 1$ par le théorème de Lagrange, il existe $\lambda \in \mathbb{N}$ tel que $p = \lambda n + 1$, d'où le lemme. □

Preuve du théorème : On raisonne par l'absurde en supposant qu'il n'existe qu'un nombre fini de nombres premiers $p_1, ..., p_k$ comme voulus. Posons alors $N = np_1...p_k$. Si on trouve un nombre premier $p = 1[N]$, il sera en particulier congru à $1[n]$ et sera différent des p_i, on aura alors notre contradiction. L'idée va être de trouver un nombre premier p qui vérifie les hypothèses du lemme 1 avec N et un certain entier a. Pour ça on pose

$$B(X) = \prod_{\substack{d|N \\ d \neq N}} \phi_d(X).$$

Comme B et ϕ_N n'ont pas de racines en communs (on peut le voir dans la preuve du lemme 0 par exemple, en montrons que $X^n - 1$ est à racines simples et qu'elles sont unions disjointes de celles des ϕ_d) ET qu'ils sont scindés sur $\mathbb{C}[X]$, ils sont premiers entre eux sur $\mathbb{C}[X]$. Ils sont cependant à coefficients rationnels donc,

l'algorithme d'Euclide fonctionnant de la même manière, ils sont en particuliers premiers entre eux sur $\mathbb{Q}[X]$. Par le théorème de Bézout il existe alors $U, V \in \mathbb{Q}[X]$ tels que

$$UB + V\phi_N = 1.$$

On peut se donner $a \in N$ tel que $aU, aV \in \mathbb{Z}[X]$ (en prenant le produit des tous les dénominateurs par exemple). De plus, ϕ_N n'est pas constant. Comme un polynôme non constant n'est pas borné sur $\mathbb{R}$ on peut prendre a tel que $|\phi_N(a)| \geq 2$. On a alors

$$a = a(U(a)B(a) + V(a)\phi_N(a)).$$

Comme $|\phi_N(a)| \geq 2$ on peut se donner un nombre premier $p|\phi_N(a)$. On a alors $\overline{a}^N = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$ et donc a est premier avec p. Maintenant, si $p|B(a)$, par la relation de Bézout on aurait p qui divise a donc $p \not| B(a)$. Ainsi, comme

$$p \not| B(a) \Rightarrow p \wedge \phi_d(a) = 1 \text{ si d divise strictement N,}$$

le lemme 1 nous dit que $p = 1[n]$ et p est différent des p_i, d'où la contradiction ! $\square$

Remarques importantes :

- Il faut en savoir un minimum sur les polynômes cyclotomiques, la preuve du lemme 0 est un minimum obligatoire je trouve.
- Il faut être au clair sur l'algorithme de Bézout pour l'argument de la primalité dans $\mathbb{Q}[X]$ (et sur l'argument précédent pour celle dans $\mathbb{C}[X]$ tant qu'à faire !).