Forme faible de la progression arithmétique de Dirichlet

Lemme 1. *Soit $a \in \mathbb{Z}$ et p premier tel que $p | \Phi_n(a)$ et $p \nmid \Phi_d(a)$ pour $d|n$ et $d < n$. Alors $p \equiv 1[n]$.*

Démonstration.

Soit p premier vérifiant l'hypothèse.
Comme p divise $\Phi_n(a)$, il divise aussi $a^n - 1$. Ainsi, l'ordre de $\overline{a}$ dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ divise n.
Montrons que cet ordre est exactement n. Si d divise n, $d < n$, on a dans $\mathbb{Z}/p\mathbb{Z}$:

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

Or, si d' divise d, d' divise aussi n, et par hypothèse $\overline{\Phi_{d'}(a)} \neq 0$.
Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, le produit de ces éléments non nuls est également non nul, si bien que $\overline{a}^d \neq 1$.
L'ordre de $\overline{a}$ est donc n. Comme cet ordre divise $p - 1$ d'après le théorème de Lagrange, $p \equiv 1[n]$.

□

Théorème 2 (Dirichlet faible)**.** *Pour $n \geqslant 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.*

Démonstration.

Supposons qu'il n'existe qu'un nombre fini de premiers $p_1, \ldots, p_q$ de la forme $\lambda n + 1$. On pose $N = np_1 \ldots p_q$.

On suppose qu'il existe $a \in \mathbb{Z}$ et p un nombre premier tel que $p|\Phi_N(a)$ mais $p \nmid \Phi_d(a)$ pour $d|N$ et $d < N$.
Par le lemme, $p \equiv 1[N]$. Alors $p \equiv 1[n]$, et $p \equiv 1[p_i]$. p est donc de la forme $\lambda n + 1$ et distinct des p_i.
On en conclut qu'il existe une infinité de nombres premiers de la forme $\lambda n + 1$.

Il faut maintenant montrer l'existence d'un tel couple (a, p).
En notant $B = \prod_{d|N, d<N} \Phi_d$, on cherche donc $a \in \mathbb{Z}$ et p premier tels que p divise $\Phi_N(a)$ et ne divise pas $B(a)$.
B et Φ_N sont premiers dans $\mathbb{C}[X]$, car ils n'ont pas de racine commune, donc dans $\mathbb{Q}[X]$, puisque leurs coefficients sont rationnels et que l'algorithme d'Euclide s'écrit de la même manière dans $\mathbb{C}[X]$ et dans $\mathbb{Q}[X]$.
Par le théorème de Bézout, il existe donc $(U, V) \in \mathbb{Q}[X]^2$ tel que $U\Phi_N + VB = 1$.
Il existe $a \in \mathbb{Z}$ tel que $U' = aU$ et $V' = aV$ appartiennent à $\mathbb{Z}[X]$. Comme $\Phi_N \neq 0$ et $\Phi_N \neq \pm 1$, on peut même choisir a tel que $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$, étant donnée l'infinité de $a \in \mathbb{Z}$ vérifiant $aU, aV \in \mathbb{Z}[X]$, alors :

$$a = U'\Phi_N + V'B \text{ et en particulier } a = U'(a)\Phi_N(a) + V'(a)B(a) \tag{1}$$

Soit p un nombre premier divisant $\Phi_N(a)$. Alors p divise $a^N - 1$, car Φ_N divise $X^N - 1$ dans $\mathbb{Z}[X]$. Dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^N = 1$, donc $\overline{a}$ est inversible, a est premier avec p. Si p divisait $B(a)$, il diviserait a, d'après (1), exclu.
On a donc trouver $a \in \mathbb{Z}$ et p premier comme on les cherchait.

□

Conclusion. Pour $n \geqslant 1$, il existe une infinité de nombres premiers congrus à 1 modulo n. ◁

Références

[FGN] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X-ENS Algèbre 1.* Cassini