Version faible du théorème de la progreesion arithmétique de Dirichlet

Geoffrey Deperle

Leçons associées :
— 102 : Groupes des nombres complexes de module 1. Racines de l'unité. Applications.
— 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
— 121 : Nombres premiers. Applications.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Soit $n \geq 1$, un entier fixé. Il existe une infinité de nombres premiers congrus à 1 modulo n.*

Commençons par présenter un lemme qui permet de reformuler le problème.

Lemme 1. *Soit $n \geq 1$, s'il existe $a \in \mathbb{Z}$, p premier tel que*
- $p|\phi_n(a)$
- $\forall d < n, d|n, p \not| \phi_d(a)$

avec ϕ_n le n-ième polynôme cyclotomique, alors $p \equiv 1[n]$.

Preuve du lemme : Soit $a \in \mathbb{Z}$, p premier vérifiant les hypothèses,
Comme $\phi_n|X^n - 1$, on a $\phi_n(a)|a^n - 1$ d'où $p|a^n - 1$ donc l'ordre de $\overline{a}$ divise n dans $(\mathbb{Z}/p\mathbb{Z})^*$.
Montrons que l'ordre de $\overline{a}$ est exactement n.
Soit d un diviseur strict de n, d'après la décomposition

$$X^d - 1 = \prod_{d'|d} \phi_{d'}$$

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

Pour $d' \in \mathbb{N}$ tel que $d'|d$, on a $d'|n$ donc par hypothèse, p ne divise aucun $\phi_{d'}(a)$ pour $d'|d$ donc $\overline{\phi_{d'}(a)} \neq 0$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, c'est un anneau intègre donc $\prod\limits_{d'|d} \overline{\phi_{d'}(a)} \neq 0$ d'où $\overline{a}^d - 1 \neq 0$.

Ainsi, l'ordre de $\overline{a}$ est n d'où $n|p-1$ d'après le théorème de Lagrange donc p est de la forme $p = \lambda n+1$ avec $\lambda \in \mathbb{Z}$. $\square$

Passons à la preuve du théorème.

Preuve du théorème : Supposons qu'il existe un nombre fini de nombres premiers congrus à 1 modulo n noté $\{p_1, \ldots, p_q\}$.
Il faut trouver un entier p premier différent de $p_1, \ldots, p_q$ congruent à 1 modulo n.
Nous allons utiliser le lemme avec $N = np_1 \ldots p_q$ car si $p \equiv 1[N]$ alors $p \notin \{p_1, \ldots, p_q\}$ et $p \equiv 1[n]$.

Soit $B = \prod_{d|N, d<N} \phi_d$, il suffit de trouver $a \in \mathbb{Z}$, p premier tel que $p|\phi_d(a)$ et $p \not| B(a)$.
B est premier avec ϕ_N dans $\mathbb{C}[X]$ car n'ont pas de racine complexe en commun donc ne sont pas premiers entre eux dans $\mathbb{Q}[X]$ par invariance du pgcd par extension de corps (l'algorithme d'Euclide est le même dans $\mathbb{C}[X]$ et $\mathbb{Q}[X]$).
D'après le théorème de Bézout,

$$\exists (U, V) \in \mathbb{Q}[X]^2 / U\phi_N + VB = 1$$

Soit a un multiple du ppcm des dénominateurs des coefficients de U, V que l'on peut supposer tel que $\phi_N(a) \neq 0$ et $\phi_N(a) \not= \pm 1$ (possible car il y a une infinité de choix pour a).
En posant $\begin{cases} \tilde{U} & = aU \in \mathbb{Z}[X] \\ \tilde{V} & = aV \end{cases}$
La relation de Bézout peut s'écrire $a = \tilde{U}\phi_N + \tilde{V}B$ d'où $a = \tilde{U}(a)\phi_N(a) + \tilde{V}(a)B(a)$.
Soit p un nombre premier divisant $\phi_N(a)$ alors $p|a^d - 1$ car ϕ_N divise $X^N - 1$ dans $\mathbb{Z}[X]$ donc dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^N = 1$ donc $\overline{a}$ est inversible et donc a est premier avec p.
Si p divisait $B(a)$, alors p diviserait a ce qui est exclu.
Ainsi, d'après le lemme $p \equiv 1[N]$ et on a donc construit un nombre premier p tel que $p \notin \{p_1, \ldots, p_q\}$ et $p \equiv 1[n]$ d'où la contradiction. $\square$

Références

[1] Serge Francinou, Hervé Gianella et Serge Nicolas. *Oraux X-ENS Algèbre 1*. Cassini, 2007.