# Développement: Théorème faible de la progression arithmétique de Dirichlet

Arthur Maritch-Roy

Ce développement a pour but de montrer le théorème de la progression arithmétique de Dirichlet dans une version faible. Le théorème général énonce que si $a$ et $b$ sont premiers entre eux, il existe une infinité de nombres premiers congrus à $a$ modulo $b$, et sa version faible correspond à $a = 1$.

**Théorème 1.** (de la progression arithmétique de Dirichlet, version faible)
Soit $n \in \mathbb{N}^*$. Il existe une infinité de nombres premiers congrus à 1 modulo $n$.

***Démonstration.*** Fixons $n \in \mathbb{N}^*$. Un nombre $p$ est congru à 1 modulo $n$ si et seulement si $n$ divise $(p-1)$. Ceci équivaut à l'existence d'un élément $a$ d'ordre $n$ dans $\mathbb{Z}/p\mathbb{Z}$. On cherche donc $a \in \mathbb{N}^*$ tel que $\overline{a}^n - 1 = 0$ (la barre désigne la classe modulo $p$). Ceci se réécrit :

$$\prod_{d|n} \overline{\Phi_d(a)} = 0.$$

Chercher une racine de $\Phi_n$ dans $\mathbb{Z}/p\mathbb{Z}$ qui n'est pas racine des autres $\Phi_d$ semble alors être une bonne idée, puisqu'alors l'ordre de cet élément $a$ ne pourra être que $n$. De plus, on sait que le polynôme $X^n - 1$ n'a que des racines simples dans $\mathbb{Z}/p\mathbb{Z}$, et donc que si on est racine de $\Phi_n$, on n'est pas racine des autres.

Si on récapitule, il nous faut donc trouver des nombres premiers $p$ qui divisent $\Phi_n(a)$ arbitrairement grands. On va prendre $N$ un entier plus grand que 3 et $a = N!$. Puisque $a \geq 3$ :

$$|\Phi_n(a)| = \prod_{\zeta \in \mu_n^*(\mathbb{C})} |a - \zeta| \geq 2,$$

on s'en convainc par un dessin. On peut donc considérer $p$ un facteur premier de $\Phi_n(a)$. Si $p \leq N$ alors $p$ divise $a = N!$ donc $p$ divise tout polynôme de $X\mathbb{Z}[X]$ en $a$ donc $\Phi_n(a) - \Phi(0)$ donc $\Phi(0)$ qui vaut 1 ou $-1$. Nécessairement, $p > N$, ce qu'il fallait démontrer. $\square$