Théorème de la progression arithmétique de Dirichlet
Version faible

Riffaut Antonin

2013-2014

Théorème 1. *Pour tout entier $n \geq 2$, il existe une infinité de nombres premiers congrus à 1 modulo n.*

Commençons par démontrer le lemme suivant :

Lemme 2. *Soient $n \geq 2$ un entier naturel et p un nombre premier. Alors $p \equiv 1(n)$ si et seulement si $\mathbb{F}_p$ possède une racine primitive n-ième de l'unité.*

Démonstration.

($\Leftarrow$) Supposons que $\mathbb{F}_p$ possède une racine primitive n-ième de l'unité ζ. Par le théorème de Lagrange, l'ordre de ζ dans $\mathbb{F}_p^\times$, c'est-à-dire n, divise l'ordre du groupe $\mathbb{F}_p^\times$, c'est-à-dire $p-1$. On a bien $p \equiv 1(n)$.

($\Rightarrow$) Réciproquement, si $p \equiv 1(n)$, il suffit de remarquer que $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, et comme n divise $p-1$, alors $\mathbb{Z}/(p-1)\mathbb{Z}$ possède un élément d'ordre n, d'où l'existence d'une racine primitive n-ième de l'unité dans $\mathbb{F}_p$. ■

Démonstration du théorème. Soient $k \geq n$ un entier naturel et p un facteur premier de $\Phi_n(k!)$. On veut montrer que $p \equiv 1(n)$ et que $p > k$. Comme Φ_n divise $X^n - 1$, alors $\Phi_n(k!)$ divise $(k!)^n - 1$, et a fortiori p divise également $(k!)^n - 1$, soit $(k!)^n \equiv 1(p)$. D'une part, p ne divise pas $k!$, car sinon p ne diviserait pas $(k!)^n - 1$; donc nécessairement $p > k$ (puisque que les facteurs premiers de $k!$ sont tous inférieurs ou égaux à k). D'autre part, il s'agit de vérifier que $k!$ est une racine primitive n-ième de l'unité dans $\mathbb{F}_p$, ce qui impliquera que $p \equiv 1(n)$ par le lemme précédent. Supposons que $k!$ soit d'ordre d avec d un diviseur strict de n. Alors $k!$ est racine de Φ_d, mais également de Φ_n. Cependant, $X^n - 1 = \prod_{l|n} \Phi_l(X)$, si bien que $k!$ est une racine au moins double de $X^n - 1$. Or $X^n - 1$ est premier avec sa dérivée nX^{n-1} (qui n'est pas nulle, puisque p ne divise pas n, sachant que $p > k \geq n$), donc toutes ses racines sont simples, ce qui aboutit à une contradiction. On en déduit que $k!$ est une racine primitive n-ième de l'unité dans $\mathbb{F}_p$, puis que $p \equiv 1(n)$.

En conclusion, on peut ainsi construire une suite strictement croissante $(p_j)_{j\in\mathbb{N}}$ de nombres premiers congrus à 1 modulo n : on choisit pour p_0 un facteur premier de $\Phi_n(n!)$, et pour tout $j \in \mathbb{N}$, on choisit pour p_{j+1} un facteur premier de $\Phi_n(p_j!)$, qui est nécessairement strictement supérieur à p_j. Pour tout $j \in \mathbb{N}$, on a bien $p_j \equiv 1(n)$. Le théorème est ainsi démontré. ■

Complément : un autre cas particulier du théorème de la progression arithmétique de Dirichlet

Proposition 3. *Tout entier $a \in \mathbb{Z}^*$ est un carré modulo une infinité de nombres premiers.*

Démonstration. Pour $n > |a|$, posons $b_n = \frac{(n!)^2}{a} - 1$. Soit p un facteur premier de b_n. Nécessairement $p > n$, car sinon p diviserait $\frac{(n!)^2}{a}$, donc p diviserait 1, ce qui est absurde. D'autre part, a est un carré

modulo p, car $a \equiv (n!)^2 \mod p$. Comme précédemment, on peut donc construire par récurrence une suite strictement croissante $(p_j)_{j\in\mathbb{N}}$ de nombres premiers telle que pour tout $j \in \mathbb{N}$, a soit un carré modulo p_j. ■

Corollaire 4. *Il existe une infinité de nombres premiers congrus à* 1 *modulo* 4.

Démonstration. Par la proposition 3, -1 est un carré modulo une infinité de nombres premiers ; or, étant donné un nombre premier p, -1 est un carré modulo p si et seulement si p est congru à 1 modulo 4, ce qui conclut. ■

Références

[Per] Daniel Perrin, *Cours d'algèbre*, page 93 exercice 14.

[Gou] Xavier Gourdon, *Les maths en tête : Algèbre.*