Version faible du théorème de progression arithmétique de Dirichlet

1 Version faible du théorème de progression arithmétique de Dirichlet

Le théorème de progression arithmétique est l'une des pièces maîtresses de l'arithmétique et en particulier de l'étude des nombres premiers, tant par son énoncé que par la place de sa démonstration dans l'histoire mathématique. Démontré pour la première fois en 1838 par Gustave Lejeune Dirichlet, il énonce que pour tout couple d'entiers (m, n) premiers entre eux, il existe une infinité de nombres premiers congrus à m modulo n (autrement dit, la suite arithmétique de premier terme m et de raison n possède une infinité de termes premiers).

On propose ici de démontrer une version "faible" de ce théorème, à savoir uniquement le cas "$m = 1$".

Théorème 1.1. *Soit n un entier plus grand que 2. Il existe une infinité de nombres premiers congrus à 1 modulo n.*

Remarque. Tout d'abord, une petite **heuristique** (historique !). "Tout le monde" connaît la preuve d'Euclide de l'infinité des nombres premiers: Par l'absurde s'il y a un nombre fini de premiers, on peut considérer $\phi_2(2\prod_{p\in\mathcal{P}_{1,2}} p)$ où $\mathcal{P}_{1,2}$ désigne l'ensemble des nombres premiers impairs, qui est alors un nouveau nombre premier impair, et patatatra !...

Bon là normalement vous faîtes les gros yeux parce que sortir des polynômes cyclotomiques pour traiter un problème résolu il y a environ 23 siècles, c'est un peu comme dégainer un marteau-pilon pour dézinguer une mouche. Alors oui, certes, mais il n'empêche que c'est le point de vue "naturel" de la preuve qui va suivre. Si on est sérieux deux minutes, l'énoncé classique de la démonstration d'Euclide est "prendre le produit de tous les nombres premiers, y ajouter 1 et obtenir ainsi un nouveau nombre premier". Comme le deuxième polynôme cyclotomique s'écrit $\phi_2(X) = X + 1$, on voit bien qu'à défaut d'être éclairant, le lien entre la formulation historique et la tarabiscotée est clair.

Par ailleurs, comme tous les nombres premiers sauf 2 sont impairs, il est équivalent de montrer qu'il existe une infinité de premiers ou de premiers impairs. Autrement dit, Euclide avait démontré le cas (très) particulier du théorème de Dirichlet pour $(m, n) = (1, 2)$!

Proof. **Plan de la preuve:** Calquer la preuve d'Euclide. On suppose par l'absurde qu'il y a un nombre fini de premiers qui conviennent, on considère n fois leur produit le tout augmenté de 1 et on aboutit à une contradiction en évaluant le n-ième polynôme cyclotomique en ce nombre.

Par l'absurde, supposons que l'ensemble $\mathcal{P}_{1,n}$ des nombres premiers congrus à 1 modulo n est fini et considérons l'entier $a := (n\prod_{p\in\mathcal{P}_{1,n}} p) + 1$. On va établir une contradiction sur la valeur de $\phi_n(a)$.

Montrons d'abord que $|\phi_n(a)| \geq 2$. Si $n = 2$, alors on a

$$|\phi_2(a)| = |a + 1| \geq 3.$$

Maintenant si $n \geq 3$, en considérant $\omega \in \mathbb{C}$ une racine primitive n-ième de l'unité, on a

$$|\phi_n(a)| = \prod_{k\wedge n=1} |a - \omega^k|.$$

On utilise la deuxième inégalité triangulaire pour en déduire le résultat escompté:

$$|\phi_n(a)| \geq \prod_{k\wedge n=1} ||a| - |\omega^k|| \geq \prod_{k\wedge n=1} |3 - 1| \geq 2.$$

Montrons maintenant que $|\phi_n(a)| = 1$. Pour cela, raisonnons par l'absurde et supposons que $\phi_n(a)$ est multiple d'un certain nombre premier q. On va utiliser le lemme suivant:

Lemme: Soit p un nombre premier qui ne divise pas n. S'il existe $x \in \mathbb{F}_p$ tel que $\phi_n(x) = 0$ (dans $\mathbb{F}_p$), alors n divise $p-1$.

Preuve du lemme: Il suffit de montrer que les racines de ϕ_n dans $\mathbb{F}_p[X]$ sont des racines primitives n-ièmes de l'unité. Tout d'abord, l'égalité

$$X^n - 1 = \prod_{d|n} \phi_d(X)$$

est une égalité dans l'anneau $\mathbb{Z}[X]$ (on montre facilement que les polynômes cyclotomiques sont à coefficients entiers par récurrence) et la réduction modulo p est un morphisme d'anneaux, donc cette égalité est encore vérifiée dans $\mathbb{F}_p[X]$.

De plus, X^n-1 est à racines simples dans $\mathbb{F}_p[X]$: Soient $Q, R \in \mathbb{F}_p[X]$ tels que $X^n-1 = Q^2(X)R(X)$. On dérive cette égalité pour obtenir :

$$nX^{n-1} = Q(X)(2Q'(X)R(X) + Q(X)R'(X)).$$

Comme on a d'autre part $n = X(nX^{n-1}) - n(X^n-1)$, on en déduit :

$$n = Q(X)[2XQ'(X)R(X) + XQ(X)R'(X) - nQ(X)R(X)].$$

Les entiers n et p étant premiers entre eux, n est une constante non nulle de $\mathbb{F}_p[X]$, et Q est nécessairement constant comme diviseur d'un polynôme constant non nul.

En particulier, les racines de ϕ_n sont donc les racines de X^n-1 qui ne sont racines d'aucun ϕ_d pour $d < n$ divisant n, et donc d'aucun $X^d - 1$. Ce sont bien les racines primitives n-ièmes de l'unité.

Ainsi, si ϕ_n admet une racine x dans $\mathbb{F}_q$, alors x est d'ordre n dans $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Par le théorème de Lagrange, on a donc bien finalement $n|p-1$. □

Comme $\phi_n(X)$ divise X^n-1, en particulier on a $q|a^n-1$. Les entiers q et a^n sont donc premiers entre eux, et q et a sont donc premiers entre eux (par le lemme d'Euclide). Comme n divise a par construction, q ne divise donc pas n et on peut appliquer le lemme. Par hypothèse, $\phi_n(a) = 0$ dans $\mathbb{F}_q$, donc n divise $q-1$. Ainsi, q est un élément de $\mathcal{P}_{1,n}$ et donc q divise a, ce qui est absurde puisque l'on vient de montrer qu'ils étaient premiers entre eux !

L'entier $\phi_n(a)$ n'est donc multiple d'aucun nombre premier, et comme $|\phi_n(a)| \geq 2$ on aboutit à une nouvelle contradiction.

Bilan des courses: $\mathcal{P}_{1,n}$ est nécessairement infini ! □