Théorème de Dirichlet (version faible)

Mohamed NASSIRI

Recasage :

●●●●● 102 : Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
●●●●● 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
●●●●● 121 : Nombres premiers. Applications.
●●●●○ 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Résumé :

S'il y a quelque chose qu'il faut savoir sur les nombres premiers, c'est que l'on a aucune formule explicite (de type polynomiale) pour tous les atteindre. D'ailleurs, on peut démontrer que c'est impossible. En revanche, ce développement assure qu'il en existe une infinité sous une forme polynomiale de degré 1.

Prérequis :

Polynômes cyclotomiques - Irréductibilité des polynômes - Corps finis

---

Théorème : (i) $\Phi_n(X)$ désigne le n-ième polynôme cyclotomique.
Si un nombre premier $p|\Phi_n(a)$ où a est un entier, mais aucun $\Phi_d(a)$ où d décrit l'ensemble des diviseurs de n, alors $p \equiv 1\ [n]$
(ii) Il existe une infinité de nombres premiers de la forme $\lambda n + 1$, $\lambda \in \mathbb{N}^*$

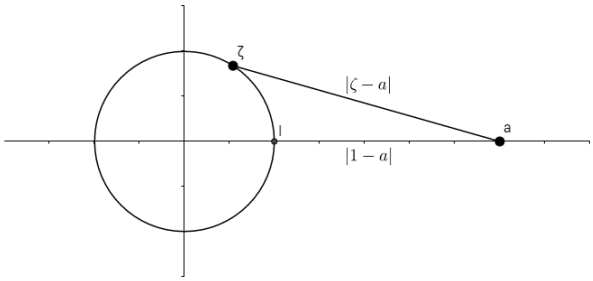
Démonstration. On va utiliser les corps finis $\mathbb{F}_p$ ainsi que son groupe multiplicatif $\mathbb{F}_p^*$. Ce qui est naturel, car la congruence avec les nombres premiers se traduit par de « vraies » égalités dans ces ensembles.

(i) Si $p|\Phi_n(a)$, alors $p|a^n - 1$ (car on a l'égalité $X^n - 1 = \prod_{d|n} \Phi_d(X)$), et donc $\bar{a}^n = \bar{1}$ dans $\mathbb{F}_p$.
On va montrer maintenant que l'ordre de $\bar{a}$ dans $\mathbb{F}_p$ est exactement n.
Soit ω l'ordre de $\bar{a}$ dans $\mathbb{F}_{p^*}$ (donc $\omega|n$). Comme $a^\omega - 1 = \prod_{d|n} \Phi_d(a)$, si $\omega < n$, il existe d diviseur strict de n tel que $p|\Phi_d(a)$, ce que l'on a exclu ! Donc $\omega = n$, et ainsi l'ordre de $\bar{a}$ est n dans $\mathbb{F}_{p^*}$ qui lui-même est d'ordre $p-1$. Par conséquent, $n|p-1 \Leftrightarrow p \equiv 1[n]$.

(ii) Soit $N \in \mathbb{N}^*$, $N \geq n$. Posons $a = 3N!$. Ce nombre peut paraître "sorti de nulle part" mais il nous faut seulement un "grand" nombre qui contient tous les facteurs premiers jusqu'à N (et le "3" permet d'assurer la propriété suivante). $\Phi_n(a) \in \mathbb{Z}$ et :

$$|\Phi_n(a)| = \prod_{i=1}^{n} |a - exp(2ik\pi/n)| \geq \prod_{i=1}^{n} |a-1| \geq a - 1 \geq 2$$

La seule inégalité qui semble la moins directe est la première. Le dessin ci-dessous permet néanmoins de s'en convaincre :



Soit p un diviseur premier de $\Phi_n(a)$ (on sait qu'il en existe puisque $|\Phi_n(a)| \geq 2$)

- Si $p \leq N$ alors $p|a$, donc divise tout entier de la forme $\sum_{i=1}^{n} z_i a^i$ ($z_i \in \mathbb{Z}$) et donc $\Phi_n(a) - \Phi_n(0)$ (qui est de la forme $\sum_{i=1}^{n} z_i a^i$). Donc $p|\Phi_n(0) = \pm 1$. Ce qui est absurde ... Donc $p > N$.

- Supposons qu'il existe d diviseur strict de n tel que $p|\Phi_d(a)$.
  Comme $X^n - 1 = \prod_{d|n} \Phi_d(X)$, $\bar{(a)}$ est une racine de multiplicité ≥ 2 du polynôme $X^n - \bar{1}$ de $\mathbb{F}_p[X]$.
  Par conséquent, $X^n - \bar{1} \in \mathbb{F}_p[X]$ possède une racine multiple : ce qui est absurde car $X^n - \bar{1}$ est premier avec sa dérivée $\bar{n}X^{n-1}$. En effet, par le théorème de Bézout et l'égalité $(1/\bar{n})X\bar{n}X^{n-1} - (X^n - 1) = 1$.
  Ainsi $p|\Phi_n(a)$ mais aucun $\Phi_d(a)$ où $d|n$ ($d < n$). Donc $p \equiv 1$ $[n]$.
  Conclusion : $\forall N \in \mathbb{N}^*$, il existe p premier tel que $p > N$ et $p \equiv 1$ $[n]$.

□

Remarques :

- Qui dit "version faible", dit "version forte". En effet, il existe une version plus générale de ce théorème (mais beaucoup plus longue à démontrer ...) :
  Théorème : Pour tout entier n non nul et tout entier m premier avec n, il existe une infinité de nombres premiers congrus à m modulo n (*i.e.* de la forme $m + an$ avec a entier).