Théorème de la progression arithmétique de Dirichlet : version faible

Benjamin Hellouin

Théorème 1. *Soit $n \leq 2$. Alors il y a une infinité de nombres premiers dans $(1 + n\mathbb{N})$.*

Pré-requis : on admet que $\Phi_n(X) = \prod_{\substack{k \leq n \\ k \wedge n = 1}} (1 - \exp(2ik\pi/n)) \in \mathbb{Z}(X)$ et la formule $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Lemme 1. *Soit $\Phi_n(X)$ le n-ème polynôme cyclotomique. S'il existe $a \in \mathbb{R}$ tel que*
- *$p \mid \Phi_n(a)$, et*
- *$\forall d \mid n, p \not| \Phi_d(a)$,*

alors $p = 1 \mod n$.

Preuve. $p \mid \Phi_n(a) \mid a^n - 1$, donc $\overline{a}^n = 1$ dans dans $\mathbb{F}_p$ et ω l'ordre de $\overline{a}$ dans $\mathbb{F}_p^*$ divise n. Comme $a^\omega - 1 = \prod_{d|\omega} \Phi_d(a)$, p divise un des $\Phi_d(a)$: ce n'est possible que si $d = \omega = n$.

Donc $\overline{a}$ est d'ordre n dans $\mathbb{F}_p^*$ et, par le théorème de Lagrange, on a $n \mid p-1$, soit $p = 1 \mod n$.

Preuve du théorème. Soit $N > n$ et $a = 3N!$: on veut montrer qu'il existe un nombre premier $> N$ satisfaisant. On a alors :

$$|\Phi_n(a)| = \prod |a - \exp(2ik\pi/n)| \geq \prod (a - 1) \geq 2$$

et $\Phi_n(a)$ admet donc des facteurs premiers : soit p un de ces facteurs.

Supposons $p \leq N$, alors $p \mid a$ et en particulier, $p \mid (\Phi_n(a) - \Phi_n(0))$ (polynôme sans facteur constant). Donc p divise $\Phi_n(0) = \pm 1$: absurde. Donc $p > N$.

Soit d un diviseur strict de n et supposons que $p \mid \Phi_d(a)$. Comme $X^n - 1 = \prod_{d \mid n} \Phi_n(X)$, $\overline{a}$ est une racine au moins double de $X^n - 1$ dans $\mathbb{F}_p$. C'est absurde car $X^n - 1$ est premier avec sa dérivée nX^{n-1} dans $\mathbb{F}_p$. En effet, on a

$$X^n - 1 + n^{-1}X \cdot nX^{n-1} = 1$$

et on conclut par le théorème de Bezout.

Conclusion : $\forall N, \exists p \in P$ tel que $p > N$ et $p = 1 \mod n$. Ceci permet de conclure.