Théorème de Dirichlet faible

Recasage : 102 / 120 / 121 / 141

Référence : Oraux X-ENS Algèbre 1 / Gozard "Théorie de Galois"

Lemme 1

Soit $a \in \mathbb{N}$ et p un nombre premier tel $p|\Phi_n(a)$ et $p \nmid \Phi_d(a)$ pour tout les $d|n$ et $d \neq n$ alors $p \equiv 1\ [n]$

Preuve.

On commence par la relation sur les polynômes cyclotomiques c'est à dire $X^n - 1 = \prod_{d|n} \Phi_d(X)$ on peut alors évaluer en a c'est à dire $a^n - 1 = \prod_{d|n} \Phi_d(a)$ on obtient alors que $\Phi_n(a)|(a^n - 1)$ et comme $p|\Phi_n(a)$, par transitivité on obtient que $p|(a^n - 1)$. Ce qui veut également dire que $\overline{a}^n = \overline{1}$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$. On va à présent montrer que n est exactement l'ordre de a dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$. Soit ω l'ordre de a dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ donc $\omega|n$. Toujours par la formule sur les polynôme cyclotomiques on a alors :

$$a^\omega - 1 = \prod_{d|\omega} \Phi_d(a) \Longrightarrow \overline{0} = \prod_{d|\omega} \overline{\Phi_d(a)}$$

Or si $d|\omega$ alors $d|n$ et par hypothèse $\overline{\Phi_d(a)} \neq 0$ de plus $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps donc il est en particulier intègre et donc $\prod_{d|\omega} \overline{\Phi_d(a)} \neq 0$ et donc $\overline{a} \neq \overline{1}$ de ce fait $\omega = n$. Comme a est non nul et que son ordre est n par le théorème de Lagrange $n|(p-1)$ ce qui signifie que $p \equiv 1\ [n]$.

■

Théorème 1 (Dirichlet faible)

Il existe une infinité de nombre premier de la forme $\lambda n + 1$ avec $\lambda \in \mathbb{N}^*$

Preuve.

Soit $N \in \mathbb{N}^*$ tel que $N \geq n$ on pose $a = 3N!$. On sait que $\Phi_n(a) \in \mathbb{Z}$ ainsi :

$$|\Phi_n(a)| = \Big| \prod_{\xi \in \mathbb{U}_n^*} (a - \xi) \Big| = \prod_{\xi \in \mathbb{U}_n^*} |a - \xi| \geq \prod_{\xi \in \mathbb{U}_n^*} (a - 1) \geq 2$$

On peut alors considérer p un facteur premier de $\Phi_n(a)$ montrons que $p > N$ et que $p \equiv 1\ [n]$.

► Montrons dans un premier temps que $p > N$ par l'absurde supposons que $p \leq N$ donc $p|a$ puisque p apparaitrait alors dans l'écriture de $N!$. De ce fait $p|(\Phi_n(a) - \Phi_n(0))$ donc comme $p|\Phi_n(a)$ par hypothèse il divise également $\Phi_n(0) = \pm 1$ et ainsi $p| \pm 1$ ce qui est absurde donc $p > N$.

► Montrons à présent que $p \equiv 1[n]$ pour cela on va revenir au lemme, soit d un diviseur de $\Phi_n(a)$ tel que $d < n$ donc comme $X^n - 1 = \prod_{d|n} \Phi_d(X)$ on peut affirmer que a est une racine de multiplicité supérieur ou égale à 2 du polynôme $X^n - 1$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ ceci est absurde car le polynôme $X^n - 1$ et nX^{n-1} sont premier entre eux dans $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ en effet on peut alors trouver une relation de Bézout entre ces deux polynômes :

$$\frac{1}{\overline{n}} X \overline{n} X^{n-1} - (X^n - \overline{1}) = \overline{1}$$

Ainsi $p|\Phi_n(a)$ mais aucun des diviseurs de n ne divise $\Phi_n(a)$ donc d'après le lemme $p \equiv 1[n]$. De ce fait $\forall N \in \mathbb{N}^*\ \exists p$ premier tel que $p > N$ et $p \equiv 1[n]$ ce qui revient à dire $p = \lambda n + 1$ pour $\lambda \in \mathbb{N}^*$

■