Théorème faible de la progression arithmétique de Dirichlet

Notions utilisées : Racines de l'unité, polynômes cyclotomiques, division euclidienne.

Motivations : Trouver une infinité de nombres premiers d'une forme donnée. (raffinement du théorème des nombres premiers)

Lemme 1. *Soient A un anneau commutatif intègre et $P, B \in A[X]$. On suppose que le coefficient dominant b_m de B est inversible dans A. Alors il existe un unique couple $(Q, R) \in A[X]$ tels que $P = BQ + R$ et $deg(R) < deg(B)$.*

Preuve. On procède par récurrence sur $n = \deg(P)$. Supposons le résultat vérifié pour un certain $n \in \mathbb{N}$. Alors le polynôme $P - p_{n+1}^{-1} b_m X^{n+1-m} B$ vérifie l'hypothèse de récurrence dans le cas où $n+1 = \deg(P)$ est plus grand ou égal à $m = \deg(B)$. Si $m > n+1$, alors $R = P$ est bien à coefficients dans A et la propriété de récurrence est aussi vérifiée. □

Corollaire 2. *En particulier, la division d'un $P \in \mathbb{Z}[X]$ par un $B \in \mathbb{Z}[X]$ unitaire se fait entièrement dans $\mathbb{Z}[X]$.*

Lemme 3. *Soit $n \in \mathbb{N}^*$ et Φ_n le n-ième polynôme cyclotomique associé. Alors*

1. $X^n - 1 = \prod_{d|n} \Phi_d$.
2. $\Phi_n \in \mathbb{Z}[X]$.

Preuve. Le premier point provient du fait que $\mu_n = \bigsqcup_{p|n} \mu_p^*$. Le second se fait par récurrence sur n et en utilisant le lemme 1. □

Théorème 4. *Soit $n \in \mathbb{N}^*$. Alors il existe une infinité de nombres premiers dans $n\mathbb{Z} + 1$.*

Preuve. On fixe $n \in \mathbb{N}^*$ dans toute la preuve. On procède en deux étapes.

Etape 1 : Montrer que si $a \in \mathbb{Z}$ et p premier vérifient $p \mid \Phi_n(a)$ et $\forall d \mid n, d \neq n$, $p \nmid \Phi_d(a)$, alors $p \in n\mathbb{Z} + 1$.

On a $a^n = 1$ dans $\mathbb{Z}/p\mathbb{Z}$, et en fait n est l'ordre a dans $\mathbb{Z}/p\mathbb{Z}^\times$. En effet si $d \mid n$ avec $d \neq n$ alors $a^d - 1 = \prod_{e|d, e\neq d} \Phi_e(a)$ qui n'est pas nul car par hypothèse, p ne divise aucun des e (car ici $d < n$). Ainsi a est d'ordre n dans $\mathbb{Z}/p\mathbb{Z}^\times$ qui est de cardinal $p-1$ et donc n divise $p-1$. Donc il existe $k \in \mathbb{Z}$ tel que

$p = 1 + kn$.

Etape 2 : Montrer qu'il y a une **infinité de premiers dans** $n\mathbb{Z} + 1$**.**

Supposons qu'il n'y ait qu'un nombre fini $p_1 \dots p_n$ de premiers dans $n\mathbb{Z} + 1$.

Etape 2.a : trouver a **et** p vérifiant les hypothèses de l'étape 1 avec $N := n \times p_1 \dots p_n$.

On pose $B := \prod_{d|N, d \neq N} \Phi_d$. On remarque que B est premier avec Φ_N dans $\mathbb{C}[X]$ car ces deux polynômes sont scindés et n'ont pas de racine commune. Puisqu'ils sont à coefficients rationnels, ils sont aussi premiers dans $\mathbb{Q}[X]$. Soient alors $U, V \in \mathbb{Q}[X]$ tels que $U\Phi_N + VB = 1$. Soit aussi $a \in \mathbb{Z}$ tels que aU et aV soient à coefficients entiers. Comme $\Phi_N \neq 0$ et $\Phi_N \neq \pm 1$, et que le nombre de $x \in \mathbb{C}$ vérifiant $\Phi_N(x) \in \{-1, 0, 1\}$ est fini (car $\mathbb{C}$ est intègre), on peut supposer quitte à multiplier a par un entier que $\Phi_N(a) \in \mathbb{Z} \setminus \{-1, 0, 1\}$. On se retrouve alors dans le cadre de l'étape 1. En effet en multipliant par a puis en évaluant en a, il vient

$$a = aU(a)\Phi_N(a) + aV(a)B(a).$$

En particulier si p désigne un diviseur premier de $\Phi_N(a)$ alors p divise $a^N - 1$ à plus forte raison, et donc a est inversible dans $\mathbb{Z}/p\mathbb{Z}^\times$, c'est à dire premier avec p. De plus p ne divise pas $B(a)$ car sinon d'après la relation précédente on aurait $p \mid aU(a)\Phi_N(a) + aV(a)B(a)$ i.e $p \mid a$.

Etape 2.b : Conclure.

On a trouvé p premier tel que $p \mid \Phi_n(a)$ et $\forall d \mid n, d \neq n$, $p \nmid \Phi_d(a)$ donc d'après l'étape 1, $p \in n\mathbb{Z} + 1$. Cela contredit l'hypothèse de départ et donc il y a bien une infinité de premiers dans $n\mathbb{Z} + 1$. □

Références

[1]