Théorème de Dirichlet faible

Pour tout $n \in \mathbb{N}^*$, on pose $\mu_n^* = \{z \in \mathbb{C},\ z^n = 1,\ \forall k < n,\ z^k \neq 1\}$ l'ensemble des racines n-ièmes primitives de l'unité et $\Phi_n(X) = \prod_{z \in \mu_n^*} (X - z)$.

Lemme : $\forall n \in \mathbb{N}^*,\ X^n - 1 = \prod_{d|n} \Phi_d(X)$ et $\Phi_n(X) \in \mathbb{Z}[X]$.

Démonstration.
- Comme $\mu_n = \bigsqcup_{d|n} \mu_d^*$ alors $X^n - 1 = \prod_{z \in \mu_n} (X - z) = \prod_{d|n} \prod_{z \in \mu_d^*} (X - z) = \prod_{d|n} \Phi_d(X)$.
- Pour tout $n \in \mathbb{N}^*$, on pose $H_n : \Phi_n \in \mathbb{Z}[X]$ et est unitaire.

Pour $n = 1$, $\Phi_1(X) = X - 1$ donc H_1 est vraie.
Soit $n \in \mathbb{N}\backslash\{0, 1\}$. Supposons H_d vraie pour tout $d < n$. Posons $F(X) = \prod_{\substack{d<n \\ d|n}} \Phi_d(X)$.
D'après l'hypothèse, $F \in \mathbb{Z}[X]$ est unitaire.
On peut effectuer la division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Z}[X]$ (effectuable sur $A[X]$ euclidien, ce n'est pas le cas de $\mathbb{Z}[X]$ mais on peut le faire car F est unitaire).

$$X^n - 1 = F(X)P(X) + R(X) \text{ avec } P, R \in \mathbb{Z}[X] \text{ et } \deg R < \deg F$$

De plus, $X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X)F(X)$ dans $\mathbb{Q}[X]$. On a donc que Φ_n est unitaire.
Et $F(X)(\Phi_n(X) - P(X)) = R(X)$.
Comme $\deg R < \deg F$, $\Phi_n = P \in \mathbb{Z}[X]$. Donc H_n est vraie.
Le principe de récurrence assure que la propriété est vraie pour tout $n \in \mathbb{N}^*$. □

Théorème de Dirichlet faible :
Soit $n \geqslant 2$. Il existe une infinité de nombres premiers congrus à 1 modulo n (i.e. de la forme $1 + an$ avec $a \in \mathbb{Z}$).

Démonstration. La stratégie est de trouver des nombres premiers congrus à 1 modulo n arbitrairement grands, fixons donc $N \in \mathbb{N}^*$ et cherchons $p > N$ premier et congru à 1 modulo n. Posons $a = 3N!$ (ce nombre a l'avantage d'être grand et de contenir tous les facteurs premiers jusque N).

$$|\Phi_n(a)| = \prod \left| a - e^{\frac{2ik\pi}{n}} \right| \geqslant \prod (a - 1) \geqslant 2$$

Donc $\Phi_n(a)$ contient un facteur premier $p \geqslant 2$. On va montrer qu'il est plus grand que N et congru à 1 modulo n.

- Supposons $p \leqslant N$ alors $p \mid N!$ donc $p \mid a$ ainsi $p \mid \Phi_n(a) - \Phi_n(0)$ (un polynôme en a sans facteur constant). Comme $p \mid \Phi_n(a)$ alors p divise aussi $\Phi_n(0) = \pm 1$. Ce qui est absurde car $p \geqslant 2$. Donc $p > N$.
- Le polynôme $X^n - 1$ est à racines simples dans $\mathbb{Z}/p\mathbb{Z}$ car il est premier avec son polynôme dérivé nX^{n-1} ($n \not\equiv 0\ [p]$ car $p > N \geqslant n$ et p est premier). Comme $X^n - 1 = \prod_{d|n} \Phi_d(X)$ est à racines simples dans $\mathbb{Z}/p\mathbb{Z}$ et $p \mid \Phi_n(a)$ alors p ne divise pas $\Phi_d(a)$ pour $d \mid n$ et $d \neq n$. De plus, $\Phi_n(a) \mid a^n - 1$. Donc, par transitivité $p \mid a^n - 1$. Donc $\overline{a}^n = 1$ dans $\mathbb{Z}/p\mathbb{Z}$.

On va maintenant montrer que l'ordre de $\overline{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ est exactement n.
Notons m l'ordre de $\overline{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Donc $m \mid n$ et supposons $m \neq n$. On peut également

écrire $a^m - 1 = \prod_{d|m} \Phi_d(a)$. Or $\overline{a}^m - 1 = 0$ et $\forall d \mid n$ (avec $d \neq n$), $\overline{\Phi_d(a)} \neq 0$ par hypothèse.
Donc $\prod_{d|m} \overline{\Phi_d(a)} \neq 0$. Ainsi, $n = m$. Donc, $\overline{a}$ est d'ordre n.
Par le théorème de Lagrange pour $(\mathbb{Z}/p\mathbb{Z})^\times$, $n \mid p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$ i.e. $p \equiv 1\ [n]$.
Finalement, $\forall N \in \mathbb{N}^*,\ \exists p > N$ premier et $p \equiv 1\ [n]$. □

Remarque.

- Le théorème de Dirichlet faible est un résultat de localisation des nombres premiers. Le théorème de Dirichlet fort (théorème de la progression arithmétique) dit que si $a \wedge b = 1$, alors la classe de congruence $a\mathbb{Z} + b$ contient une infinité de nombres premiers. Le théorème faible c'est si $b = 1$.
  C'est une preuve complètement différente. Elle ressemble un peu (en plus dur) à la preuve analytique de l'infinité de nombres premiers.
- Le polynôme $X^n - 1$ a des racines simples dans $\mathbb{C}$. Est-ce toujours le cas dans $\mathbb{F}_p$? Oui c'est possible, par exemple sur $\mathbb{F}_2$, avec $n = 2 = X^2 - 1 = (X - 1)^2$. Ou $X^p - 1$ sur $\mathbb{F}_p$. Si la caractéristique est première à n les racines sont simples (cf. démo).
- On a la division euclidienne dans $\mathbb{Z}[X]$? C'est un anneau euclidien ?
  Il n'est pas euclidien (non principal car $(2, X)$ n'est pas principal et donc non euclidien), mais on peut faire de la division euclidienne dans $A[X]$ si on se limite à diviser par un polynôme unitaire (ou à coefficient dominant inversible).
- Le coefficient constant d'un polynôme cyclotomique vaut ± 1 car il divise -1, à cause de la formule $X^n - 1 = \prod \Phi_d$. En fait, à part pour $n = 1$, le coefficient constant de Φ_n vaut toujours 1 (récurrence).
- Les autres coefficients de Φ_n ont l'air de toujours valoir ± 1 ou 0. Savez-vous si c'est le cas ? Φ_{105} possède deux coefficients qui sont égaux à -2.
- **Théorème d'Euclide :** Il existe une infinité de nombres premiers.
  Supposons par l'absurde qu'il existe qu'un nombre fini de nombres premiers $p_1, \ldots, p_r$.
  Posons $p = p_1 \cdots p_r + 1$. Comme $p \geqslant 2$ alors p admet un diviseur premier p_k.
  Or $p_k \mid p - p_1 \cdots p_r = 1$. Ce qui est absurde.
- Il existe une infinité de nombres premiers de type $3n + 2$ (ou $4n + 3$ ou $6n + 5$).
  On adapte la preuve d'Euclide : si $p_1, \ldots, p_r$ sont de tels nombres, on considère les facteurs premiers de $3 \prod p_k + 1$. Tous ces facteurs sont différents de 3 et ne peuvent être tous congrus à 1 modulo 3 sinon leur produit le serait aussi.
- Y a-t-il une infinité de nombres premiers de type $3n + 1$ (ou $4n + 1$ ou $5n + 1$) ?
  Si on considère $3 \prod p_k + 1$ et ses facteurs premiers. On prend un nombre premier de cette forme par exemple 7, or on $3 \times 7 + 1 = 22$ donc aucun facteur premier n'est de la bonne forme.
  Le principe de ces exos, un nombre premier ne peut avoir que deux classes de congruence modulo n : 1 et autre chose (ici $n - 1$).