2.3 Théorème de la progression arithmétique de Dirichlet (version faible) (102, 120, 121, 141)

Le théorème de la progression arithmétique de Dirichlet s'énonce ainsi : pour tout $n \in \mathbb{N}^*$ et pour tout $m \in \mathbb{N}^*$ tel que $m \wedge n = 1$, alors il existe une infinité de nombres premiers congrus à m modulo n. La preuve classique de ce théorème utilise la théorie des séries de Dirichlet, ce qui est compliqué à appréhender (pour moi en tout cas). On va donc prouver le résultat plus faible suivant, en utilisant les polynômes cyclotomiques :

Théorème 2.8 (Dirichlet, version faible)**.** Soit $n \in \mathbb{N}^*$. Alors il existe une infinité de nombres premiers congrus à 1 modulo n.

Démonstration. On va commencer par montrer un lemme intermédiaire qui va nous aider à trouver la bonne marche à suivre pour prouver le théorème

Lemme 2.9. Soit $a \in \mathbb{Z}$ et p un facteur premier de $\Phi_n(a)$ tel que $p \wedge n = 1$. Alors $p \equiv 1[n]$.

Démonstration. On va se placer dans le corps $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$. L'énoncé nous dit donc que $\overline{a}$ annule le polynôme cyclotomique $\Phi_{n,\mathbb{F}_p}$. Or, $n \wedge p = 1$, ainsi le polynôme $X^n - 1$ est premier avec son polynôme dérivé. Il est donc scindé à racines simples dans son corps de décomposition. Ainsi, étant donné la relation :

$$X^n - 1 = \prod_{d|n} \Phi_d,$$

les racines de $\Phi_{n,\mathbb{F}_p}$ sont distinctes des racines de $\Phi_{d,\mathbb{F}_p}$ pour tout $d|n$. Ainsi, les racines de $\Phi_{n,\mathbb{F}_p}$ sont exactement d'ordre n dans $\mathbb{F}_p^\times$. Ainsi, $\overline{a}$ est d'ordre n, et, par le théorème de Lagrange, on a que $n|p-1$. Ainsi :

$$p \equiv 1\ [n].$$

□

Prouvons la version faible du théorème de Dirichlet par l'absurde. Supposons qu'il existe un nombre fini de nombres premiers $p_1, \dots, p_k$ congrus à 1 modulo n. Le cas $n = 1$ peut être écarté d'emblée car on sait qu'il existe une infinité de nombres premiers. Si $n \geq 2$, montrons que le coefficient constant de Φ_n est égal à 1 :

On a : $\Phi_1 = X - 1$ et $\Phi_2 = X + 1$. Supposons que pour tout $d < n$, $\Phi_d(0) = 1$. Par la relation :

$$X^n - 1 = \prod_{d|n} \Phi_d$$

on a :

$$-1 = \Phi_n(0) \times \underbrace{\Phi_1(0)}_{=-1} \times \underbrace{\prod_{\substack{d|n \\ d \notin \{1,n\}}} \Phi_d(0)}_{=1}$$

et donc :

$$\Phi_n(0) = 1.$$

En prenant $a = np_1 \dots p_k$, on a donc :

$$\begin{cases} \Phi_n(a) & \equiv & 1\ [p_1 \dots p_r] \\ \Phi_n(a) & \equiv & 1\ [n]. \end{cases}$$

Ainsi, un facteur premier p de $\Phi_n(a)$ vérifie :

— $p \notin \{p_1, \dots, p_k\}$,
— $p \nmid n$ et donc $n \wedge p = 1$.
Ainsi, d'après le lemme, on a $p \equiv 1\ [n]$! **ABSURDE !** Cela conclut donc la preuve. □

Détaillons tout de même pourquoi, lorsqu'un polynôme $P \in K[X]$ est premier avec son polynôme dérivé, il devient scindé à racines simples dans un corps de décomposition L.
Dans ce corps de décomposition, P s'écrit :

$$P = \lambda \prod_{i=1}^{r} (X - \alpha_i)^{m_i}$$

avec $\alpha_1, \dots, \alpha_r \in L$ les racines de P distinctes deux à deux et $m_1, \dots, m_r \in \mathbb{N}^*$. On a également :

$$P' = \lambda \sum_{i=1}^{r} \left(m_i (X - \alpha_i)^{m_i - 1} \prod_{j \neq i} (X - \alpha_j)^{m_j} \right).$$

Ainsi, s'il existe i_0 tel que $m_{i_0} \geq 2$, on a :

$$P' = \lambda (X - \alpha_{i_0}) \left(m_{i_0} (X - \alpha_{i_0})^{m_{i_0} - 2} \prod_{j \neq i_0} (X - \alpha_k)^{m_j} + (X - \alpha_{i_0})^{m_{i_0} - 1} \sum_{i \neq i_0} m_i (X - \alpha_i)^{m_i - 1} \prod_{j \notin \{i, i_0\}} (X - \alpha_j)^{m_j} \right).$$

Ainsi (et peu importe la caractéristique du corps ! !) s'il existe i_0 tel que $m_{i_0} \leq 2$ (i.e. P n'est pas à racines simples), alors :

$$(X - \alpha_{i_0}) \mid P \wedge P'$$

et donc P et P' ne sont pas premiers entre eux dans L. Étant donné que le pgcd est invariant par extension de corps, P et P' ne sont pas premiers entre eux dans K.