1.8 Moyen & semi-classique : Version faible du théorème de Dirichlet par les polynômes cyclo/corps finis

(haut) Référence : Hindry (ne le fait pas tout à fait pareil, il regarde les racines). Recasages : 120, 121, 123, 125, 141

Énoncé : Soit Φ_n le n-ème polynôme cyclotomique, q la puissance d'un nombre premier premier à n. Alors, dans $\mathbf{F}_q$, Φ_n est le produit de d polynômes irréductibles (différents par séparabilité) de mêmes degrés $m = \frac{\varphi(n)}{d}$, et m vaut l'ordre de $q \in (\mathbf{Z}/n\mathbf{Z})^\times$.
Applications :

- Φ_n est irréductible sur $\mathbf{F}_q$ ssi q engendre $(\mathbf{Z}/n\mathbf{Z})^\times$.
- $\Phi_8 = X^4 + 1$ est irréductible dans $\mathbf{Q}[X]$, mais jamais dans $\mathbf{F}_q[X]$.
- Φ_n a une racine dans $\mathbf{F}_q$ ssi $q = 1 \pmod n$ ssi Φ_n est scindé dans $\mathbf{F}_q$.
- Si n est un entier naturel non nul, il y a une infinité de nombres premiers congrus à $1 \pmod n$.

Preuve : On écrit : $\Phi_n = \prod_{i=1}^d P_i$ la décomposition en irréductibles. Soit $i \in \{1, \dots, d\}$, soit ζ une racine d'un P_i dans un corps de rupture $L = \mathbf{F}_q(\zeta)$. Alors $\deg(P_i) = [L : K] =: m$ (dépendant de i a priori). Alors on a $\Phi_n(\zeta) = 0$, donc ζ est d'ordre divisant n. De plus, $X^n - 1$ est à racines simples, (car premier à sa dérivée) donc les $(\Phi_d)_{d|n}$ sont premiers entre eux : en particulier, ζ n'annule aucun des autres Φ_d, ce qui prouve que ζ est d'ordre n.
Par le théorème de Lagrange, on a $n \mid |L^*| = q^m - 1$, ie : $q^m = 1 \pmod n$. Montrons que m est minimal en ce sens. Si m' est l'ordre de q, alors $L' = \{x \in L, x^{q^{m'}} = x\} = L^{\mathrm{Frob}^{m'}}$ est une sous-extension de $L/\mathbf{F}_q$ contenant ζ : c'est égal à L. Donc $m' = m$. Ainsi, m est bien l'ordre de q modulo n.

Pour la version faible de Dirichlet : on a $\Phi_n(0) = 1$ pour tout n, donc pour tout entier N, N est premier avec $\Phi_n(N)$ (car N divise $\Phi_n(N) - \Phi_n(0)$). De plus, comme Φ_n est un polynôme, il n'y a qu'un nombre fini de a tels que $\Phi_n(a) = \pm 1$. Il existe des nombres premiers $= 1 \pmod n$: en effet, on prend N tel que $\Phi_n(N) \neq \pm 1$, puis n'importe quel diviseur premier de $\Phi_n(N)$ convient. S'il n'y avait qu'un nombre fini de premiers congrus à $1 \pmod n$, notés $p_1 \dots, p_k$ alors on prend $N = \ell p_1 \dots p_k$, pour un ℓ tel que $\Phi_n(N) \neq \pm 1$; si p est un diviseur premier à $\Phi_n(N)$, alors par ce qui précède, $p = 1 \pmod n$, et p est premier à N : c'est impossible.

Remarque : Si $n \geq 3$, il existe une infinité de nombres premiers non congrus à $1 \pmod n$: en effet, il y en a (2 par exemple) et s'il y en avait un nombre fini, disons $p_1, \dots, p_k$, alors $2np_1 \dots p_k - 1$ aurait un diviseur premier non congru à $1 \pmod n$.

Remarque 2 : Factoriser Φ_n dans $\mathbf{F}_p$ revient à trouver la décomposition de $p\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$, où $K = \mathbf{Q}(\zeta_n)$ est la n-ème extension cyclotomique. En particulier, p est totalement décomposé ssi $p \equiv 1 \pmod n$, et p reste premier dans $\mathcal{O}_K$ ssi p engendre $(\mathbf{Z}/n\mathbf{Z})^\times$.