39 Théorème de Dirichlet version faible

ref : ?

THÉORÈME 39.1 *Soit $n \geq 2$, il existe une infinité de nombres premiers de la forme $1 + an$ avec $a \in \mathbb{N}$ (c'est-à-dire dans la classe de 1 modulo n).*

PREUVE. Commençons par un lemme qui nous fournit un critère pour trouver des nombres premiers congrus à 1 modulo n parmi les facteurs premiers de $\Phi_n(a)$.

LEMME 39.2 *Soit $a \in \mathbb{N}$ et p premier tel que : p divise $\Phi_n(a)$ et p ne divise pas $\Phi_d(a)$ pour d divisant n et $d \neq n$. Alors :*

$$p = 1 \pmod{n}$$

PREUVE. On écrit la relation liant les polynômes cyclotomiques :

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

On a p divise $\Phi_n(a)$, donc p divise $a^n - 1$, autrement dit $a^n = 1$ dans $\mathbb{Z}/p\mathbb{Z}$. L'ordre ω de a dans $\mathbb{Z}/p\mathbb{Z}^\times$ est alors un diviseur de n. On réexploite une deuxième fois la relation entre polynômes cyclotomiques :

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

Le premier membre vaut 0 modulo p alors que le deuxième est non nul sauf si $\omega = n$ par hypothèse. Ensuite, le théorème de Lagrange dans $\mathbb{Z}/p\mathbb{Z}^*$ donne n divise $p-1$, c'est-à-dire $p = 1 \pmod{n}$. □

La stratégie est de trouver des nombres premiers congrus à 1 modulo n arbitrairement grand, fixons donc $N \geq 1$ et cherchons $p > N$. On pose $a = 3 \times N!$, ce nombre a l'avantage d'être grand et de contenir tous les facteurs premiers jusque N, c'est tout ce qu'on lui demande.

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

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

Pour le premier point, on remarque que si $p \leq N$, p divise a, donc p divise $\Phi_n(a) - \Phi_n(0)$ qui est un polynôme en a sans facteur constant. Comme p divise $\Phi_n(a)$, il divise aussi $\Phi_n(0) = \pm 1$. C'est absurde, donc $p > N$.

Pour le deuxième point, on utilise le lemme : 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} ($n \neq 0 \pmod{p}$ car $p > N \geq n$ ne peut diviser n). Or p ne peut pas diviser un autre $\Phi_d(a)$ pour $d|n$, $d \neq n$, sans que a soit racine double de $X^n - 1$, donc d'après le lemme $p = 1 \pmod{n}$. □

Remarque : 1) La version forte établit la même chose dans la classe de m modulo n dès que $m \wedge n = 1$.

2) On utilise un peu de connaissance des polynômes cyclotomiques, à mettre dans le plan ou à démontrer si le temps le permet.

Leçons concernées : anneaux $\mathbb{Z}/n\mathbb{Z}$, nombres premiers, nombres complexes de module 1.