Dirichlet faible

Développement pour les leçons 102 [1], 120 [2], 121 [3], 141 [4].

1 Introduction

Le théorème de Dirichlet faible stipule que pour tout entier $n \geq 2$, il existe une infinité de nombres premiers congru à 1 modulo n. Pour ce faire, nous aurons besoin des polynômes cyclotomiques [5] défini par $\phi_1 = X - 1$ et $\phi_n = \prod_{\xi \in \mu_n^*}(X - \xi)$ pour $n \geq 2$, où μ_n^* est l'ensemble des racines primitives n-èmes de l'unité. On fera quelques rappels préliminaires sur les polynômes cyclotomiques et on fera par la suite la preuve du théorème de Dirichlet faible.

2 Rappels sur les polynômes cyclotomiques

Nous aurons besoin de deux résultats sur ces (fabuleux) polynômes dans ce développement. Le premier est que pour tout $n \in \mathbb{N}^*$, on a

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

En effet, pour $n \in \mathbb{N}^*$, on a

$$\begin{aligned} X^n - 1 &= \prod_{k=1}^{n} (X - e^{\frac{2ik\pi}{n}}) \\ &= \prod_{\xi \in \mu_n} (X - \xi) \\ &= \prod_{d|n} \left(\prod_{o(\xi)=d} (X - \xi) \right) \\ &= \prod_{d|n} \phi_d \end{aligned}$$

Le deuxième point dont nous aurons besoin est unitaire et que $\phi_n \in \mathbb{Z}[X]$. Pour ce faire, on procède par récurrence sur n. On a bien que $\phi_1 \in \mathbb{Z}[X]$. On suppose donc la propriété vraie pour tout $m \leq n-1$ et on va montrer que $\phi_n \in \mathbb{Z}[X]$. Or, on sait que

$$\phi_n = \frac{X^n - 1}{\prod_{d|n,\, d \neq n} \phi_d} := \frac{X^n - 1}{B}$$

et donc ϕ_n est le quotient de la division euclidienne de $X^n - 1$ par B qui est, par hypothèse, unitaire et à coefficient dans $\mathbb{Z}$. Ainsi, on a bien que $\phi_n \in \mathbb{Z}[X]$ ce qui nous permet de conclure.

3 Preuve du théorème

Tout d'abord, soit $n \in \mathbb{N}^*$ et soit p un nombre premier et $a \in \mathbb{Z}$ tel que $p | \phi_n(a)$ et p ne divise pas $\phi_d(a)$ pour tout diviseur strict d de n. Montrons alors que $p = 1[n]$.

On a $p|\phi_n(a)$ et $\phi_n | X^n - 1$ donc $p|a^n - 1$ et donc l'ordre multiplicatif de a dans $\mathbb{Z}/p\mathbb{Z}$ divise n. Montrons qu'en fait on a $o(a) = n$. Si d divise n, on a que $a^d - 1 = \prod_{d'|d} \phi_{d'}(a)$. Mais alors on a, dans $\mathbb{Z}/p\mathbb{Z}$, la relation $a^d - 1 = \prod_{d'|d} \phi_{d'}(a)[p]$. mais p ne divise aucun des $\phi_{d'}(a)$ par hypothèse, donc par intégrité de $\mathbb{Z}/p\mathbb{Z}$ on a que $a^d \neq 1[p]$ et donc $o(a) \neq d$. D'où $o(a) = n$ et donc $n|p-1$ et on en déduit par le théorème de Lagrange que $p = 1[n]$.

On va appliquer ce résultat afin de démontrer le théorème de Dirichlet faible. Soit $n \in \mathbb{N}^*$ et supposons par l'absurde qu'il existe un nombre fini de nombres premiers $p_1, \ldots, p_r$ tels que $p_i = 1[n]$. Soit $N = np_1 \ldots p_r$ et B le polynôme défini par

$$B = \prod_{d|N,\, d \neq N} \phi_d$$

1. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
2. Anneaux Z/nZ. Applications.
3. Nombres premiers. Applications.
4. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
5. Ou cyclotoniques, ou cyclotodjintonic, à choisir selon votre aisance avec le jury.

On a $B \wedge \phi_N = 1$ dans $\mathbb{C}[X]$. En effet, si ξ est une racine de B dans $\mathbb{C}$, alors l'ordre de ξ dans μ_N divise strictement N (car ξ va être racine de l'un des ϕ_d mais pas de ϕ_N), donc $o(\xi) < N$ et ξ n'est pas racine de ϕ_N. Étant des polynômes scindés sur $\mathbb{C}[X]$ ayant leurs racines qui sont différentes, on a bien que $B \wedge \phi_N = 1$ dans $\mathbb{C}[X]$. De plus, le PGCD est invariant par extension de corps et comme $B \in \mathbb{Q}[X]$ et $\phi_N \in \mathbb{Q}[X]$, on a que $B \wedge \phi_N = 1$ dans $\mathbb{Q}[X]$.

Ainsi, par Bézout, il existe $U, V \in \mathbb{Q}[X]$ tels que $U\phi_N + VB = 1$. Or, il existe $a \in \mathbb{Z}$ tel que $U' = aU$, $V' = aV$ et $U', V' \in \mathbb{Z}[X]$. De plus, on a que $\deg \phi_N \geq 1$, donc ϕ_N à un nombre fini de racine et on peut donc supposer que $\phi_N(a) \neq 0$ et $\phi_N(a) \neq \pm 1$. Ainsi, on a que

$$U'\phi_N + V'B = a$$

Et en évaluant en a, on obtient que

$$U'(a)\phi_N(a) + V'(a)B(a) = a$$

Soit p un nombre premier divisant $\phi_N(a)$. On a alors que p divise $a^N - 1$, donc $a^N = 1[p]$ et donc $a \wedge p = 1$. On a de plus que p ne divise pas $B(a)$, sinon on aurait que p divise a ce qui contredirait que fait que a et p soient premiers entre eux. On a donc que p ne divise aucun des $\phi_d(a)$ avec $d|N$ et $d \neq N$. On se retrouve dans les hypothèses de la propriété montrée précédemment et donc $p = 1[N]$ et donc, par le théorème chinois, on a que $p = 1[n]$. Mais alors on a que $p = p_i$ pour un certain $i \in \{1, \ldots, r\}$. Mais le théorème chinois nous donne aussi que $p = 1[p_i]$ et donc que $p \neq p_i$ pour tout $i \in \{1, \ldots, r\}$ d'où une contradiction. Ainsi, on obtient bien le fait qu'il existe une infinité de nombres premiers congrus à 1 modulo n.

4 Bibliographie

Encore et toujours le Francinou tome 1, page 137.