DÉVELOPPEMENT 10

FORME FAIBLE DU THÉORÈME DE DIRICHLET

Lemme. — *Si $f, g \in \mathbb{Q}[X]$ sont unitaires et vérifient $fg \in \mathbb{Z}[X]$ alors $f, g \in \mathbb{Z}[X]$*

Démonstration. — Soit $a > 0$ le plus petit entier tel que $af \in \mathbb{Z}[X]$, on pose $af = f_1$; soit $b > 0$ le plus petit entier tel que $bg \in \mathbb{Z}[X]$, on pose $bg = g_1$. Supposons que $ab > 1$ et soit p un diviseur premier de ab, on considère alors le morphisme $\pi_P : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$. On a $f_1 g_1 = abfg \in \mathbb{Z}[X]$ d'où

$$\pi_P(f_1)\pi_P(g_1) = \pi_P(f_1 g_1) = \pi_P(ab)\pi_P(fg) = 0$$

et il en résulte (puisque $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre) que $\pi_P(f_1) = 0$ ou $\pi_P(g_1) = 0$, par exemple $\pi_P(f_1) = 0$. On peut alors écrire $f_1 = pf_2$ où $f_2 \in \mathbb{Z}[X]$. Comme f est unitaire et puisque $f_1 = af$, a est le coefficient dominant de f_1, donc p divise a et on écrit $a = pa'$. Il vient donc $pa'f = f_1 = pf_2$ *i.e.* $a'f = f_2 \in \mathbb{Z}[X]$, ce qui est impossible puisque $a' < a$. Donc $ab = 1$ *i.e.* $a = b = 1$. □

Théorème. — *Pour tout entier $n \geq 1$, il existe une infinité de premiers congrus à 1 modulo n.*

Démonstration. — On considère le $k^{\text{è}}$ polynôme cyclotomique

$$\Phi_k = \prod_{\zeta \in U_k^\circ} (X - \zeta) = \prod_{\substack{1 \leq \ell \leq k \\ k \wedge \ell = 1}} \left(X - e^{\frac{2i\ell\pi}{n}} \right),$$

puisque la réunion $U_n = \bigcup_{d|n} U_d^\circ$ est disjointe, il vient

$$X^n - 1 = \prod_{\zeta \in U_n} (X - \zeta) = \prod_{\zeta \in \bigcup_{d|n} U_d^\circ} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in U_d^\circ} (X - \zeta) = \prod_{d|n} \Phi_d = \Phi_n \prod_{\substack{d|n \\ d \leq n-1}} \Phi_d.$$

On a $\Phi_1 = X - 1 \in \mathbb{Q}[X]$, supposons que $\Phi_{n'} \in \mathbb{Q}[X]$ pour tout $n' < n$. Puisque $X^n - 1 \in \mathbb{Q}[X]$ et $\prod_{\substack{d|n \\ d \leq n-1}} \Phi_d \in \mathbb{Q}[X]$, on peut écrire $X^n - 1 = Q \prod_{\substack{d|n \\ d \leq n-1}} \Phi_d + R$ avec $Q, R \in \mathbb{Q}[X]$ et $\deg R < \deg \prod_{\substack{d|n \\ d \leq n-1}} \Phi_d$. Il vient donc

$$(\Phi_n - Q) \prod_{\substack{d|n \\ d \leq n-1}} \Phi_d = R.$$

Puisque $\deg R < \deg \prod_{\substack{d|n \\ d \leq n-1}} \Phi_d$, il s'ensuit que $\Phi_n - Q = 0$ d'où $\Phi_n \in \mathbb{Q}[X]$. Enfin, on a $\Phi_n \in \mathbb{Z}[X]$ d'après le lemme, puisque $\Phi_n \prod_{\substack{d|n \\ d \leq n-1}} \Phi_d = X_n - 1 \in \mathbb{Z}[X]$.

Soit p un nombre premier et $a \in \mathbb{Z}$ tels que p divise $\Phi_n(a)$ mais ne divise aucun $\Phi_d(a)$ pour tout diviseur d de n. Comme p divise $\Phi_n(a)$, p divise aussi $a^n - 1$ donc l'ordre de la classe $\overline{a}$ de a dans $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ divise n. Si d divise n strictement alors

$$\overline{a}^d - 1 = \prod_{d'|d} \overline{\Phi_{d'}(a)}$$

dans $\mathbb{Z}/p\mathbb{Z}$. Mais si d' divise d où d est un diviseur de n alors d' divise n et par hypothèse, on a donc $\overline{\Phi_{d'}(a)} \neq 0$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, il s'ensuit que le produit des $\overline{\Phi_{d'}(a)}$ est non nul *i.e.* $\overline{a}^d \neq 1$. Ainsi, on a $\overline{a}^n = 1$ et $\overline{a}^d \neq 1$ pour tout diviseur d de n donc l'ordre de $\overline{a}$ dans $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ est exactement n. D'autre part, cet ordre divise l'ordre du groupe *i.e.* n divise $p-1$ et le nombre premier p est donc de la forme $kn+1$ avec k entier.

Supposons maintenant qu'il n'existe qu'un nombre fini de premiers congrus à 1 modulo n, on les note $p_1, \ldots, p_q$. On pose $N = np_1 \cdots, p_q$, d'après ce qui précède, il suffit de trouver un nombre premier p et un entier a tel que p divise $\Phi_N(a)$ mais ne divise aucun $\Phi_d(a)$ pour tout diviseur d de N. On pose

$$B = \prod_{\substack{d|N \\ d<N}} \Phi(d),$$

i.e. il s'agit de trouver p premier et $a \in \mathbb{Z}$ tels que p divise $\Phi_N(a)$ mais ne divise pas $B(a)$. Les polynômes B et Φ_N sont tous deux à coefficients dans $\mathbb{Q}$ et n'ont aucune racine commune dans $\mathbb{C}$ (où ils sont scindés) donc B et Φ_N sont premiers entre eux dans $\mathbb{Q}$ et, d'après le théorème de Bézout, on a $UB + V\Phi_N = 1$ avec $U, V \in \mathbb{Q}[X]$. Il existe alors un entier $a \in \mathbb{Z}$ tel que $U' = aU$ et $V' = aV$ soient à coefficients entiers ; puisque Φ_N n'est pas constant, on peut choisir $a \in \mathbb{Z}$ tel que $|\Phi_N(a)| \geq 2$. Soit p un diviseur premier de $\Phi_N(a)$ alors p divise $a^N - 1$ (puisque Φ_N divise $X^N - 1$) *i.e.* $\overline{a}^N = 1$ dans $\mathbb{Z}/p\mathbb{Z}$; en particulier $\overline{a}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$ ce qui signifie que a et p sont premiers entre eux. Ainsi, p ne divise pas $a = U'(a)B(a) + V'(a)\Phi_N(a)$ et comme p divise $\Phi_N(a)$, p ne divise pas $B(a)$ et p est donc congru à 1 modulo N. Donc p est congru à 1 modulo n et est distinct de $p_1, \ldots, p_q$. □

Leçons concernées

09 Congruences dans $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications

10 Nombres premiers.Applications

15 Groupe des nombres complexes de module 1. Applications

Références

S. Francinou et H. Gianella, *Exercices d'algèbre 1*, Masson, 1993.

S. Francinou, H. Gianella et S. Nicolas, *Oraux X-ENS, algèbre 1*, Cassini, 2001.

Sébastien Pellerin