Enoncé : Soit $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers congrus à 1 modulo n

Soit $n \in \mathbb{N}^*$. On va montrer que :

i) Si un nombre premier p divise $\Phi_n(a)$, où a est un entier, mais aucun $\Phi_d(a)$ où d décrit l'ensemble des diviseurs stricts de n, alors $p \equiv 1 \pmod n$

ii) Il existe une infinité de nombres premiers de la forme $\lambda n + 1$, $\lambda \in \mathbb{N}^*$.

Rappels

* on note $P_n = \{\xi \in \mathbb{C} / \xi^n = 1 \text{ et } \forall d \in [\![1; n-1]\!] \ \xi^d \neq 1\}$

$\Phi_n(X) = \prod_{\xi \in P_n} (X - \xi)$ est le n-ième polynôme cyclotomique de l'unité

* $X^n - 1 = \prod_{d \in \mathrm{Div}(n)} \Phi_d(X)$

* $\Phi_n(X) \in \mathbb{Z}[X]$.

---

i) Soit p un nombre premier et a un entier tels que p divise $\Phi_n(a)$ et aucun $\Phi_d(a)$ avec d diviseurs stricts de n.

p divise $a^n - 1$ car :

$$a^n - 1 = \prod_{d \in \mathrm{Div}(n)} \Phi_d(a) = \Phi_n(a) \prod_{\substack{d \in \mathrm{Div}(n) \\ d \neq n}} \Phi_d(a)$$

Donc $a^n \equiv 1 \pmod p$ et donc $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Soit ω l'ordre de $\bar{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$, ω divise n

L'ensemble des diviseurs de ω est donc inclus dans l'ensemble des diviseurs de n.

$$a^\omega - 1 = \prod_{d \in \mathrm{Div}\,\omega} \Phi_d(a) \equiv 0 \pmod p$$

Donc $\exists d \in \mathrm{Div}\,\omega \subset \mathrm{Div}\,n$ tq $p \mid \Phi_d(a)$

Par hypothèse $d = n$ et donc $\omega = n$. $\Rightarrow$ $\bar{a}$ est d'ordre n dans $(\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre $p-1$.

Th de Lagrange $\Rightarrow$ $n \mid p-1$ d'où $\underline{p \equiv 1 \pmod n}$

ii) Soit $N > n$. Posons $a = 3N!$

$\Phi_n(a)$ est un entier.

$$|\Phi_n(a)| = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} \left| a - \exp\left(\frac{2ik\pi}{n}\right) \right| \geq \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} (a-1) = (a-1)^{\varphi(n)} \geqslant 2.$$

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