Théorème de Dirichlet faible

En raisonnant par l'absurde et en utilisant certaines propriétés des polynômes cyclotomiques, on démontre que l'ensemble des premiers congrus à 1 *modulo un certain entier* n *est infini.*

Lemme 1. Soient $a \in \mathbb{N}$ et p premier tels que $p \mid \Phi_n(a)$ mais $p \nmid \Phi_d(a)$ pour tout diviseur strict d de n. Alors $p \equiv 1 \mod n$ ou $p \mid n$. [GOU21] p. 99

Démonstration. On a,

$$X^n - 1 = \prod_{d \mid n} \Phi_d = \Phi_n \underbrace{\prod_{d \mid\mid n} \Phi_d}_{=F}$$

Comme $F \in \mathbb{Z}[X]$, en évaluant en a :

$$a^n - 1 = \Phi_n(a)F(a) \implies p \mid a^n - 1 \text{ car } F(a) \in \mathbb{Z}$$

Autrement dit, $a^n \equiv 1 \mod p$. En notant m l'ordre de $\overline{a}$ dans $(\mathbb{Z}/p\mathbb{Z})^*$, on a $a^m \equiv 1 \mod p$. D'où $m \mid n$. Ainsi :

- Si $m = n$, alors $\overline{a}$ est d'ordre n. Donc par le théorème de Lagrange, $n \mid |(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$ ie. $p \equiv 1 \mod n$.
- Sinon, $m < n$. Comme $m \mid n$,

$$X^n - 1 = \prod_{d \mid n} \Phi_d = \Phi_n \left(\prod_{d \mid m} \Phi_d \right) \left(\prod_{\substack{d \mid\mid n \\ d \nmid m}} \Phi_d \right) = \Phi_n (X^m - 1) \left(\prod_{\substack{d \mid\mid n \\ d \nmid m}} \Phi_d \right)$$

  Mais, $\overline{a}$ est racine de $\overline{\Phi_n}$ et $X^m - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$. En particulier, $\overline{a}$ est (au moins) racine double de $X^n - \overline{1}$. On peut donc écrire,

$$X^n - 1 \equiv (X - a)^2 G(X) \mod p$$

  Avec $X = Y + a$, cela donne :

$$(Y + a)^n - 1 \equiv Y^2 G(Y + a) \mod p$$

  Le polynôme de droite est de degré ≥ 2, donc p divise les coefficients des termes de degré 0 et 1 de $(Y + a)^n - 1$, ie.

$$p \mid a^n - 1 \text{ et } p \mid \binom{n}{1} a^{n-1} = n a^{n-1}$$

  De la première égalité, on en tire $p \nmid a$. Ainsi, a est premier avec p (c'est donc également vrai pour a^{n-1}). Finalement, on tire de la deuxième égalité que $p \mid n$.

□

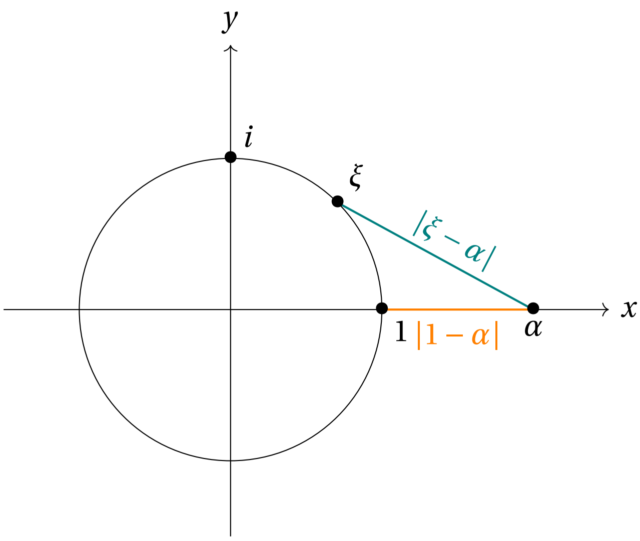
Théorème 2 (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n.

Démonstration. On suppose par l'absurde qu'il n'existe qu'un nombre fini de premiers de la forme $1 + kn$, que l'on note $p_1, \dots, p_m$. On considère $N = \Phi_n(\alpha)$ où $\alpha = np_1 \dots p_m$. On remarque en particulier que $N \equiv a_0 \mod \alpha$, où a_0 est le coefficient constant de Φ_n (cela se voit en écrivant $\Phi_n = \sum_{k=0}^{\varphi(n)} a_k X^k$, ce qui donne $N = a_0 + \alpha \sum_{k=1}^{\varphi(n)} a_k \alpha^{k-1}$ une fois évalué en α).

Or, $X^n - 1 = \prod_{d \mid n} \Phi_d$. En évaluant en 0, on en tire :

$$-1 = \prod_{d \mid n} \Phi_d(0) \implies \pm 1 = a_0, \text{ car } \forall d \mid n, \Phi_d \in \mathbb{Z}[X]$$

Ainsi, $N \equiv \pm 1 \mod \alpha$. Or $|N| = |\Phi_n(\alpha)| = \prod_{\xi \in \pi_n^*} |\alpha - \xi| > 1$. On peut en effet interpréter $|\alpha - \xi|$ comme la distance du complexe α au complexe ξ ; le premier est sur l'axe réel et est supérieur ou égal à 2, le second est sur le cercle unité :



En particulier, il existe p premier tel que $p \mid N$. Par le Lemme 1 :

— Ou bien $p \mid n$, dans ce cas $p \mid \alpha = np_1 \dots p_m$.

— Ou bien $p \equiv 1 \mod n$, dans ce cas $p = p_k$ pour un certain $k \in [\![1, m]\!]$. Et on a encore $p \mid \alpha$.

Pour conclure, on écrit $N = \alpha q \pm 1$ (par division euclidienne), et on a $p \mid N - \alpha q = \pm 1$: absurde. □

Si vous choisissez de présenter ce développement, il faut au moins connaître l'énoncé de la version forte du théorème.

Théorème 3 (Progression arithmétique de Dirichlet)**.** Pour tout entier n et pour tout m premier avec n, il existe une infinité de nombres premiers congrus à m modulo n.

Bibliographie

Les maths en tête **[GOU21]**

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3e éd. Ellipses, 13 juill. 2021. `https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html`.