Le théorème de Wilson

Christian V. Nguembou Tagne

2 octobre 2022

Le théorème de Wilson est un résultat d'arithmétique qui donne une condition nécessaire et suivante pour qu'un entier positif distinct de 1 soit premier. Dans cette note, nous proposons deux démonstrations de ce théorème : l'une utilisant exclusivement des arguments de l'arithmétique élémentaire et l'autre faisant usage de la symbolique et de résultats basiques de la théorie des groupes.

1. Énoncé du théorème de Wilson

Pour qu'un nombre entier p supérieur ou égal à 2 soit premier, il faut et il suffit que $(p-1)!+1$ soit divisible par p, c'est-à-dire $(p-1)!+1 \equiv 0\,[\mathrm{mod}\,p]$.

2. Une première démonstration du théorème de Wilson

Soit p un entier supérieur ou égal à 2.

Soit p non premier. Alors, il existe un diviseur q de p vérifiant $1 < q < p$. Ces dernières inégalités induisent que q est l'un des facteurs de $(p-1)!$. De ce fait, $(p-1)!$ est divisible par q. Mais, $(p-1)!+1$ n'est pas divisible par q : le contraire induirait en effet que q divise 1, et donc $q \leq 1$. N'étant pas divisible par un diviseur de p, le nombre $(p-1)!+1$ n'est pas a fortiori divisible par p. Par contraposition, nous avons ainsi établi que, si $(p-1)!+1$ est divisible par p, alors p est un nombre premier.

De toute évidence,

$$(2-1)!+1 = 2 \equiv 0\,[\mathrm{mod}\,2] \qquad \text{et} \qquad (3-1)!+1 = 3 \equiv 0\,[\mathrm{mod}\,3].$$

Supposons maintenant que p est un nombre premier supérieur ou égal à 5, et considérons les ensembles

$$E = [2, p-2] \cap \mathbb{N} = \Big\{2, 3, \ldots, p-2\Big\}$$

et

$$F = [1, p-1] \cap \mathbb{N} = \Big\{1, 2, \ldots, p-1\Big\}.$$

Soit a un élément de E. Alors, pour chaque $k \in F$, il existe un unique couple (q_k, r_k) d'entiers naturels tels que $1 \leq r_k \leq p-1$ et $ak = pq_k + r_k$. Ainsi, pour tout couple (k, ℓ) d'éléments distincts de F, nous avons $1 \leq |k-\ell| \leq p-2$, et donc $\mathrm{PGCD}(k-\ell, p) = 1$, puis

$$a(k-\ell) = p(q_k - q_\ell) + (r_k - r_\ell).$$

À ce compte-là, l'égalité $r_k = r_\ell$ entraînerait que p divise a, puis $p \leq a$: une contradiction. De ce fait, les restes r_k sont deux à deux distincts, et

$$\Big\{r_1, r_2, \ldots, r_{p-1}\Big\} = \Big\{1, 2, \ldots, p-1\Big\}.$$

Notons que $r_1 \neq 1$ et $r_{p-1} \neq 1$; le contraire induirait en effet $a-1 = pq_1$ ou $ap-a-1 = pq_{p-1}$, et donc que p divise $a-1$ ou $a+1$, et par suite $p \leq a-1$ ou $p \leq a+1$: une contradiction. Pour chaque $a \in E$, il existe donc un unique élément b de E tel que $ab \equiv 1\,[\mathrm{mod}\, p]$. Cet élément b est distinct de a, car la relation $a^2 \equiv 1\,[\mathrm{mod}\, p]$ impliquerait $(a-1)(a+1) \equiv 0\,[\mathrm{mod}\, p]$, puis $p|(a-1)$ ou $p|(a+1)$. Tout compte fait, l'ensemble

$$E = \Big\{2, 3, \ldots, p-2\Big\},$$

de cardinal pair $p-3$, peut être partitionné en paires $\{a, b\}$ d'éléments distincts vérifiant $ab \equiv 1\,[\mathrm{mod}\, p]$. De ce fait, $2 \cdot 3 \cdots (p-2) \equiv 1\,[\mathrm{mod}\, p]$. Il en résulte que

$$(p-1)! = 1 \cdot \Big[2 \cdot 3 \cdots (p-2)\Big] \cdot (p-1) \equiv p-1\,[\mathrm{mod}\, p].$$

Par conséquent, $(p-1)! + 1 \equiv 0\,[\mathrm{mod}\, p]$. Nous avons ainsi prouvé que, si p est un nombre premier, alors p divise $(p-1)! + 1$.

3. Une deuxième démonstration du théorème de Wilson

La démonstration à suivre est fondée sur l'exercice 55 du chapitre 3 de l'ouvrage [1] référencé au pied de cette note.

Soit n un entier naturel non nul et distinct de 1.

Supposons que n est non premier et différent de 4. Alors, il existe des entiers naturels a et b tels que $2 \leq a \leq b$ et $n = ab$. Précisément, $2 < a \leq b$ ou $2 \leq a < b$, car $ab \neq 4$. Si $2 < a \leq b$, alors $n = ab > 2b = b + b \geq a + b$. Si en revanche $2 \leq a < b$, alors

$$n = ab \geq 2b = b + b > a + b.$$

En tout état de cause, $n > a+b$, c'est-à-dire $n-1 \geq a+b$. De ce fait, $(a+b)!$ divise $(n-1)!$. Cependant,

$$(a+b)! = \binom{a+b}{a} \times (a!b!).$$

De ce fait, $a!b!$ est un diviseur $(a+b)!$. Par conséquent, ab divise $(a+b)!$, et $(n-1)!$, a fortiori. Donc, si n est non premier et différent de 4, alors n divise $(n-1)!$.

✍

Notons au passage que, pour $n = 4$, le reste de la division de $(n-1)!$ par n est 2.

Maintenant, supposons que n est premier et considérons le groupe $\left((\mathbb{Z}/n\mathbb{Z})^*, \overline{\times}\right)$. Chaque élément de ce groupe a la forme $\overline{a}$, où a est un nombre entier vérifiant $1 \leq a \leq n-1$. Pour qu'un tel élément soit égal à son inverse, il faut et il suffit que $a^2 \equiv 1\,[\operatorname{mod} n]$, c'est-à-dire

$$a - 1 \equiv 0\,[\operatorname{mod} n] \qquad \text{ou} \qquad a + 1 \equiv 0\,[\operatorname{mod} n].$$

Si $2 \leq a \leq n-2$, alors $1 \leq a-1 \leq n-3$ et $2 \leq a+1 \leq n-1$, puis

$$a - 1 \not\equiv 0\,[\operatorname{mod} n] \qquad \text{et} \qquad a + 1 \not\equiv 0\,[\operatorname{mod} n].$$

Cependant, $1 - 1 \equiv 0\,[\operatorname{mod} n]$ et $(n-1) + 1 \equiv 0\,[\operatorname{mod} n]$. De ce fait, $\overline{1}$ et $\overline{n-1}$ sont les seuls éléments du groupe $\left((\mathbb{Z}/n\mathbb{Z})^*, \overline{\times}\right)$ qui sont égaux à leur inverse.

Le produit des éléments du groupe $\left((\mathbb{Z}/n\mathbb{Z})^*, \overline{\times}\right)$ se réduit au produit des éléments égaux à leur inverse, car les autres, si elles existent, peuvent être regroupés en paires d'inverses mutuels. Donc,

$$\overline{(n-1)!} = \overline{1 \cdot 2 \cdots (n-2)(n-1)} = \overline{1 \cdot (n-1)} = \overline{n-1}.$$

Par conséquent, $(n-1)!$ est congru à $n-1$ modulo n.

✍

La technique du paragraphe précédent, qui consiste à regrouper les éléments du groupe $\left((\mathbb{Z}/n\mathbb{Z})^*, \overline{\times}\right)$ en paires d'inverses mutuels, est fondamentalement la même que celle utilisée dans la deuxième partie de la première démonstration. La différence d'approche en l'espèce est symbolique, de pure forme.

Références

[1] Monge, M. ; Lemaire-Body, F. ; Audouin-Egoroff, M.-C. ; **Mathématiques**, **Terminales C et E**, Tome 2 : Arithmétique, analyse et probabilités, Belin, Paris, 1974.