Une généralisation du théorème d'Euler

Alexandre Bailleul

Théorème (Fermat)**.** *Soit p un nombre premier et soit $a \in \mathbb{Z}$. Alors p divise $a^p - a$.*

Cet énoncé peut se traduire par le fait que tout élément x de l'anneau $\mathbb{Z}/p\mathbb{Z}$ vérifie $x^p = x$. En effet, p divise $a^p - a$ revient à dire que $a^p = a \pmod{p}$. Il existe une démonstration très simple de ce théorème utilisant le théorème de Lagrange en théorie des groupes. Tout d'abord si a est divisible par p alors le résultat évident. Sinon, la classe de a modulo p est un élément du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ pour la multiplication, qui est de cardinal $p-1$. Le théorème de Lagrange donne alors que $a^{p-1} = 1 \pmod{p}$, soit finalement $a^p = a \pmod{p}$.

Si on souhaite généraliser ce théorème au cas d'un entier n non premier, on est amené à introduire l'indicatrice d'Euler φ, telle que

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{k \in \{1, \dots, n-1\} \mid (n,k) = 1\}|,$$

où (n,k) désigne le PGCD de n et k, la dernière égalité étant vraie car l'inversibilité modulo n est équivalente à l'existence d'une relation de Bezout avec n. La même démonstration fournit alors le

Théorème (Euler)**.** *Soit $n \in \mathbb{N}^*$ et soit a un entier divisible par n ou premier avec n. Alors*

$$a^{\varphi(n)+1} = a \pmod{n}.$$

Cependant, cette égalité n'est pas forcément vérifiée pour tous les éléments de $\mathbb{Z}/n\mathbb{Z}$. Par exemple 12 ne divise jamais $2^k - 2$ pour $k \geq 2$, qui vaut toujours 2 ou 6 modulo 12. Mais 10 divise $2^5 - 2 = 30$ alors que 2 n'est ni divisible par 10, ni premier avec 10. Ces deux situations sont différentes car dans le second cas, 2 et $10/2 = 5$ sont premiers entre eux, tandis que dans le premier cas, 2 et $12/2 = 6$ ne le sont pas.

Définition. Soit $n \in \mathbb{N}^*$ et a un diviseur de n. On dit que a est un **diviseur unitaire** de n si $(a, n/a) = 1$.

Lemme 1. *Soit $n \in \mathbb{N}^*$ et a un diviseur unitaire de n. Alors*

$$a^{\varphi(n)+1} = a \pmod{n}.$$

Démonstration. En effet, par hypothèse, a et n/a sont premiers entre eux, donc d'après le théorème d'Euler (et après avoir simplifié par a, ce qui est possible car a est inversible modulo n/a),

$$a^{\varphi(n/a)} = 1 \pmod{n/a}.$$

De plus, comme φ est une fonction multiplicative (ce qui résulte du lemme chinois), on a $\varphi(n) = \varphi(a \times n/a) = \varphi(a)\varphi(n/a)$ et donc

$$a^{\varphi(n)} = a^{\varphi(n/a)\varphi(a)} = 1^{\varphi(a)} = 1 \pmod{n/a},$$

et donc en multipliant par a,

$$a^{\varphi(n)+1} = a \pmod{n}.$$

□

Remarque. On a en fait

$$a^{\varphi(n/a)+1} = a \pmod{n}.$$

Lemme 2. *Soit $n \in \mathbb{N}^*$ sans facteur carré (c'est-à-dire qui n'est divisible par aucun carré de nombres premiers). Alors tout entier $a \in \{1, \ldots, n-1\}$ est produit d'un diviseur unitaire de n et d'un entier premier avec n.*

Démonstration. En effet, si a n'est pas premier avec n, c'est qu'il admet certains facteurs premiers en commun avec n. Notons d le produit de ces facteurs. Comme n est sans facteurs carrés, chacun de ces nombres premiers n'apparaît qu'une seule fois dans d, et donc d divise n. De plus d est un diviseur unitaire de n car les facteurs premiers de n/d ne divisent pas d, encore une fois car n est sans facteur carré. Enfin les facteurs premiers de a/d sont ceux de a qui ne divisent pas n, et donc a/d est premier avec n. Finalement on a bien

$$a = d \times a/d,$$

avec d diviseur unitaire de n et a/d premiers avec n. □

Corollaire. *Soit $n \in \mathbb{N}^*$ sans facteur carré. Alors pour tout $a \in \mathbb{Z}$,*

$$a^{\varphi(n)+1} = a \pmod{n}.$$

Démonstration. Si $a = 0 \pmod{n}$, le résultat est évident. Sinon on écrit $a = cd \pmod{n}$ par le lemme 2, avec c premier avec n et d diviseur unitaire de n. D'après le théorème d'Euler,

$$c^{\varphi(n)+1} = c \pmod{n}$$

et d'après le lemme 1,

$$d^{\varphi(n)+1} = d \pmod{n}.$$

Ainsi

$$a^{\varphi(n)+1} = c^{\varphi(n)+1} d^{\varphi(n)+1} = cd = a \pmod{n}.$$

□

Référence

[1] R. Hansen, L. Swanson, *Unitary divisors*, Mathematics Magazine, 1979