Réflexions sur le petit théorème de Fermat

Christian V. Nguembou Tagne

2 octobre 2022

Pour tout entier relatif a et tout nombre premier p, le nombre $a^p - a$ est divisible par p.

Cette proposition est appelée **petit théorème de Fermat**. Dans cette note, nous proposons deux démonstrations de ce théorème, non sans avoir au préalable examiné des cas particuliers et un contre-exemple pour en montrer la pertinence et la profondeur.

1. Des cas particuliers du petit théorème de Fermat

(a) Par définition, le reste de la division euclidienne d'un entier par 3 est 0, 1 ou 2. Cette observation permet d'établir aisément qu'un triplet constitué d'entiers consécutifs contient exactement un multiple de 3. Par conséquent, pour tout entier relatif n, le nombre

$$n^3 - n = n(n^2 - 1) = (n-1)n(n+1)$$

est divisible par 3.

(b) Soit n un entier relatif. Alors,

$$n^5 - n = n(n^2 - 1)(n^2 + 1) = (n-1)n(n+1)(n^2 + 1).$$

Si le chiffre des unités de n est 0, 1, 4, 5, 6 ou 9, alors un des facteurs du produit $(n-1)n(n+1)$ est divisible par 5. Si en revanche le chiffre des unités de n est 2, 3, 7 ou 8, alors

$$n^2 \equiv r^2 \,[\mathrm{mod}\, 10]$$

avec $r^2 \in \{4, 9, 49, 64\}$; ceci signifie que le chiffre des unités de n^2 est 4 ou 9, et que $n^2 + 1$ est divisible par 5. Par conséquent, 5 est un diviseur de $n^5 - n$ pour tout entier n.

(c) Soit n un entier relatif. Alors, $n^7 - n = n\Big(\left(n^3\right)^2 - 1\Big) = n(n^3 - 1)(n^3 + 1)$. D'où

$$n^7 - n = n(n-1)(n+1)(n^2 + n + 1)(n^2 - n + 1).$$

Par ailleurs, soit r le reste de la division euclidienne de n par 7. Si r est égal à 0, 1 ou 6, alors le produit $n(n-1)(n+1)$ est divisible par 7. Cependant, il existe un entier k tel que $n = 7k + r$ et $n^2 = 49k^2 + 14k + r^2$. De ce fait,

$$n^2 + n + 1 \equiv (r^2 + r + 1) \,[\mathrm{mod}\, 7] \qquad \text{et} \qquad n^2 - n + 1 \equiv (r^2 - r + 1) \,[\mathrm{mod}\, 7].$$

Donc, si $r = 2$ ou $r = 4$, alors $r^2 + r + 1$ vaut 7 ou 21, puis $n^2 + n + 1$ est divisible par 7. Dans le même esprit, si $r = 3$ ou $r = 5$, alors $r^2 - r + 1$ vaut 7 ou 21, puis $n^2 - n + 1$ est divisible par 7. Par conséquent, $n^7 - n$ est divisible par 7 pour tout entier relatif n.

(d) Soit n un entier relatif. Alors,

$$n^{11} - n = n\Big((n^2)^5 - 1\Big) = n(n^2 - 1)\Big((n^2)^4 + (n^2)^3 + (n^2)^2 + (n^2)^1 + 1\Big).$$

Donc,

$$n^{11} - n = n(n-1)(n+1)(n^8 + n^6 + n^4 + n^2 + 1).$$

Si le reste r de la division euclidienne de n par 11 est égal à 0, 1 ou 10, alors le produit $n(n-1)(n+1)$ et le nombre $n^{11} - n$ sont divisibles par 11. Si $r = 2$ ou $r = 9$, alors il existe un entier k tel que $n = 11k \pm 2$. Il en résulte que n^2, n^4, n^6 et n^8 sont congrus respectivement à 4, 5, 9 et 3 modulo 11, puis

$$n^8 + n^6 + n^4 + n^2 + 1 \equiv 22 \,[\mathrm{mod}\, 11] \equiv 0 \,[\mathrm{mod}\, 11].$$

Un raisonnement analogue permet d'établir que $n^8 + n^6 + n^4 + n^2 + 1$ est divisible par 11 si $r = 3$ ou $r = 8$ (c'est-à-dire $n = 11k \pm 3$), si $r = 4$ ou $r = 7$ (c'est-à-dire $n = 11k \pm 4$), ainsi que lorsque $r = 5$ ou $r = 6$ (c'est-à-dire $n = 11k \pm 5$). Ceci signifie que 11 est un diviseur de $n^{11} - n$, en tout état de cause.

(e) Soit n un entier relatif. Alors,

$$\begin{aligned} n^{13} - n &= n\Big((n^6)^2 - 1\Big) = n\Big(n^6 - 1\Big)\Big(n^6 + 1\Big) = n\Big((n^2)^3 - 1\Big)\Big((n^2)^3 + 1\Big) \\ &= n(n^2 - 1)\Big((n^2)^2 - n^2 + 1\Big)\Big((n^2)^2 + n^2 + 1\Big). \end{aligned}$$

Ainsi,

$$n^{11} - n = n(n-1)(n+1)(n^2+1)(n^4 - n^2 + 1)(n^4 + n^2 + 1).$$

Au demeurant, il existe des entiers k et ℓ, avec $0 \leq \ell \leq 6$, tels que $n = 13k \pm \ell$. Si $\ell = 0$ ou $\ell = 1$, alors le produit $n(n-1)(n+1)$ est divisible par 13. Si $\ell = 5$, alors $n^2 \equiv 12 \,[\mathrm{mod}\, 13]$ et $n^2 + 1$ est divisible par 13. Si $\ell = 2$ ou $\ell = 6$, alors $n^4 - n^2 \equiv -1 \,[\mathrm{mod}\, 13]$ et $n^4 - n^2 + 1$ est divisible par 13. Si $\ell = 3$ ou $\ell = 4$, alors $n^4 + n^2 \equiv 12 \,[\mathrm{mod}\, 13]$ et $n^4 + n^2 + 1$ est divisible par 13. Ceci montre que le nombre $n^{13} - n$ est un multiple de 13 pour tout entier relatif n.

2. Un contre-exemple

Le nombre $n^9 - n$ n'est pas divisible par 9 pour tout entier relatif n. En effet,

$$2^9 - 2 = 512 - 2 = 510 = 56 \times 9 + 6.$$

3. Une première démonstration du petit théorème de Fermat

Soit a un entier relatif et p un nombre premier.

Si a est divisible par p, alors il en est de même pour le nombre $a^p - a$, égal à $a(a^{p-1} - 1)$.

Dans la suite de l'argumentation, supposons que a n'est pas divisible par p. Par ailleurs, soit E l'ensemble des $p-1$ premiers entiers naturels non nuls. Autrement dit,

$$E = \Big\{m \in \mathbb{N} \mid \ 1 \leq m \leq p-1\Big\} = \Big\{1, \ldots, p-1\Big\}.$$

Alors, pour chaque $k \in E$, le nombre ka n'est pas divisible par p. Il existe donc un couple unique (q_k, r_k) d'entiers tel que $r_k \in E$ et $ka = q_k p + r_k$. Par conséquent,

$$[1 \cdot 2 \cdots (p-1)]a^{p-1} = \prod_{k=1}^{p-1}(ka) = \prod_{k=1}^{p-1}(q_k p + r_k) = bp + (r_1 r_2 \cdots r_{p-1}), \qquad (*)$$

où $b \in \mathbb{Z}$. Maintenant, soient k et ℓ des éléments distincts de E. Alors, $0 < |k - \ell| \leq p-2$ et

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

De ce fait, $r_k \neq r_\ell$, car le contraire induirait $(k-\ell)a = (q_k - q_\ell)p$, et que p divise a. Ainsi,

$$\Big\{r_k \mid \ k \in \mathbb{N} \ \wedge \ 1 \leq m \leq p-1\Big\} = \Big\{r_1, \ldots, r_{p-1}\Big\} = E.$$

D'où $1 \cdot 2 \cdots (p-1) = r_1 r_2 \cdots r_{p-1}$. D'après $(*)$, ceci entraîne

$$[1 \cdot 2 \cdots (p-1)](a^{p-1} - 1) = bp.$$

Par conséquent, p divise $a^{p-1} - 1$, car le produit $1 \cdot 2 \cdots (p-1)$ et p sont premiers entre eux. Donc, $a^p - a$ est divisible par p.

4. Une seconde démonstration du petit théorème de Fermat

Soit p un nombre premier et k un entier vérifiant $0 < k < p$. Alors,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p}{k} \times \frac{(p-1)!}{(k-1)![(p-1)-(k-1)]!} = \frac{p}{k} \times \binom{p-1}{k-1}.$$

D'où $k\binom{p}{k} = p\binom{p-1}{k-1}$. Donc, p divise $k\binom{p}{k}$. Puisque k et p sont premiers entre eux, et compte tenu du théorème de Gauss, il s'ensuit que p divise $\binom{p}{k}$. La formule binôme livre alors

$$(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1}\binom{p}{k}x^p y^{p-k},$$

puis

$$(x+y)^p \equiv x^p + y^p \,[\mathrm{mod}\, p]$$

pour tout couple (x, y) d'entiers relatifs. Cette relation permet d'établir par récurrence que

$$\left(\sum_{k=1}^{n} x_k\right)^p \equiv \left(\sum_{k=1}^{n} x_k^p\right) \,[\mathrm{mod}\, p]$$

pour tout entier naturel non nul n et chaque n-uplet $(x_1, \ldots, x_n)$.

En posant, $n = a$ et $x_k = 1$ pour tout $k \in \{1, \ldots, n\}$, nous obtenons alors $a^p \equiv a \,[\mathrm{mod}\, p]$ pour chaque entier naturel non nul a.

Au demeurant, si $p > 2$, alors p est impair et $(-a)^p = -a^p \equiv -a \,[\mathrm{mod}\, p]$. Du reste,

$$(-a)^2 - (-a) = a^2 + a = a(a+1) \equiv 0 \,[\mathrm{mod}\, 2].$$

En conséquence, $a^p \equiv a \,[\mathrm{mod}\, p]$ pour tout entier relatif a.