GENOCCHI

Démonstration d'un théorème de Fermat

Nouvelles annales de mathématiques 3e série, tome 2 (1883), p. 306-310

<http://www.numdam.org/item?id=NAM_1883_3_2__306_1>

DÉMONSTRATION D'UN THÉORÈME DE FERMAT;

PAR M. GENOCCHI,
Professeur à l'Université de Turin.

Ce théorème est énoncé dans les *Recherches* de M. Ch. Henry sur les manuscrits de Fermat, et revient à dire que le système des deux équations

$$2y^2 - 1 = x, \quad 2z^2 - 1 = x^2$$

n'admet de solution en nombres entiers que pour $x = 7$. On écarte, bien entendu, les solutions évidentes $x = 1$, $y = \pm 1$, $z = \pm 1$, et $x = -1$, $y = 0$, $z = \pm 1$.

Le P. Pepin vient de s'occuper de la question ainsi posée, mais ses calculs assez prolongés et difficiles ne conduisent pas à un résultat simple et précis qui devrait être la vérité ou la fausseté de l'assertion de Fermat, car il conclut seulement que, si un nombre peut la démentir, il doit dépasser l'unité suivie de 3848 chiffres. J'ai donc pensé qu'il n'était pas sans intérêt de montrer que quelques principes connus depuis longtemps permettaient non seulement d'abréger beaucoup la discussion, mais de parvenir à une conclusion précise, et cela en suivant la voie tracée par le P. Pepin.

En éliminant x, on trouve

$$z^2 - 1 = 2y^2(y^2 - 1),$$

ou, sous une autre forme,

$$z^2 = y^4 + (y^2 - 1)^2;$$

et ici y peut être un nombre impair ou bien un nombre pair.

Soit y impair. Les formules connues pour les *triangles rectangles en nombres* donneront

$$\pm z = \frac{f^2 + g^2}{2}, \quad y^2 = fg, \quad y^2 - 1 = \frac{f^2 - g^2}{2},$$

f et g étant deux nombres entiers impairs et premiers entre eux. Il s'ensuit, d'après l'équation $y^2 = fg$, qu'on aura

$$f = m^2, \quad g = n^2,$$

avec m et n entiers, et, par conséquent,

$$y^2 = m^2 n^2, \quad m^2 n^2 - 1 = \frac{f^2 - g^2}{2} = \frac{m^4 - n^4}{2},$$

d'où

$$2(m^4 + 1^4) = (m^2 + n^2)^2,$$

résultat absurde, puisque le double de la somme de deux bicarrés ne peut être un carré. Il y aurait exception pour $m = \pm 1$, $n = \pm 1$, mais cela donnerait $y^2 = 1$, et, par suite, $x = 1$, $z^2 = 1$, solution écartée.

Soit maintenant y pair. On fera

$$\pm z = f^2 + g^2, \quad y^2 = 2fg, \quad y^2 - 1 = f^2 - g^2,$$

en supposant que f et g sont deux nombres entiers, premiers entre eux, le premier pair et le deuxième impair. L'équation $y^2 = 2fg$ donnera

$$f = 2\alpha^2, \quad g = \beta^2,$$

avec α et β nombres entiers, et il en résultera

$$y^2 = 4\alpha^2\beta^2, \quad 4\alpha^2\beta^2 - 1 = f^2 - g^2 = 4\alpha^4 - \beta^4.$$

Cette dernière équation se met sous la forme

$$(2\alpha^2 + \beta^2)^2 = 1 + 8\alpha^4,$$

et, en faisant, pour abréger, $2\alpha^2 + \beta^2 = p$, on a

$$8\alpha^4 = (p+1)(p-1).$$

p est un nombre impair, et $p+1$, $p-1$ sont deux nombres pairs n'ayant d'autre facteur commun que 2. Soit donc $\alpha = mn$, m et n étant premiers entre eux, il s'ensuit

$$p \pm 1 = 2m^4, \quad p \mp 1 = 4n^4;$$

d'où

$$\pm 1 = m^4 - 2n^4,$$

partant

$$m^4 \mp 1 = 2n^4.$$

Ainsi la différence ou la somme $m^4 \mp 1$ de deux bicarrés serait double d'un carré, ce qui est encore impossible. Il y a exception pour $m = \pm 1$, $n = 0$ ou $n = \pm 1$; mais, dans le premier cas, on aurait

$$\alpha = 0, \quad y = 0, \quad x = -1, \quad z^2 = 1,$$

solution écartée; dans le dernier, on aura

$$\alpha = \pm 1, \quad p = 3,$$

d'où

$$2\alpha^2 + \beta^2 = 3, \quad \beta^2 = 1,$$

et, par conséquent,

$$y^2 = 4, \quad x = 8 - 1 = 7,$$

solution de Fermat. Celle-ci est donc la seule admissible, et le théorème de Fermat est démontré complètement.

Les principes dont j'ai fait usage, sur la somme et la différence de deux bicarrés, remontent au *Traité sur les triangles rectangles* de Frenicle, et on peut les trouver dans un ancien Mémoire d'Euler (*Comment. Acad. Petrop.*, t. X pour 1738, publié en 1747, p. 125 et suiv.). En 1855, j'ai obtenu ces théorèmes en étudiant la théorie des nombres appelés *congrus* par Fibonacci, lesquels peuvent être regardés comme exprimant l'*aire d'un triangle rectangle*, de manière que cette théorie des congrus est intimement liée avec celle des triangles rectangles en nombres, tant cultivée par Diophante, Frenicle, Fermat. J'ai prouvé que les formules

$$r^4 + 4s^4, \quad 2r^4 + 2s^4, \quad r^4 - s^4,$$

où r et s sont supposés entiers, représentent toujours des congrus, et que la même chose a lieu pour les formules

$$r^4 + 6r^2s^2 + s^4, \quad \pm(r^4 - 6r^2s^2 + s^4),$$

si r et s sont deux nombres entiers, l'un pair et l'autre impair. J'ai prouvé de plus qu'aucun congru n'est carré, ni double d'un carré, ni égal à un carré multiplié par un nombre premier de la forme $8m+3$, ou par le double d'un nombre premier de la forme $8m+5$, ni par le produit de deux nombres premiers de la forme $8m'+3$, ni enfin par le double produit de deux nombres premiers de la forme $8m+5$. Je crois que ces derniers théorèmes étaient nouveaux.