BULLETIN DE LA S. M. F.

S. WACHS

Démonstration d'un théorème de Fermat

Bulletin de la S. M. F., tome 66 (1938), p. 164-170

<http://www.numdam.org/item?id=BSMF_1938__66__164_0>

DÉMONSTRATION D'UN THÉORÈME DE FERMAT;

Par M. S. WACHS
(Paris)

Dans les *Recherches sur les manuscrits de Fermat* par Henry, on lit à la fin d'un extrait de lettre de Fermat à Carcavi :

« M. Fermat a envoyé à M. Frénicle la démonstration par laquelle il prouve qu'il n'y a aucun nombre que le seul 7 qui étant le double d'un carré — 1, soit la racine carrée d'un carré de la même nature; 7 est le double du carré 4 — 1, c'est-à-dire égal à 8 — 1, et son carré 49 est le double du carré 25, c'est-à-dire 50 — 1. »

Le R. P. Th. Pépin montra dans un Mémoire paru en 1882 aux *Atti dell'Academia pontifica de Nuovi Lincei,* que si un autre nombre que 7 existe et jouit de la propriété énoncée, ce nombre est formé d'un 1 suivi de 3848 chiffres; dans un second Mémoire paru immédiatement après aux mêmes *Atti*, Pépin revient sur la question mais d'une façon très sommaire. C'est pourquoi il nous a paru intéressant de publier ici nos recherches personnelles sur cette question.

Le théorème de Fermat se traduit en langage algébrique par la proposition suivante :

L'équation diophantique

$$(2x^2-1)^2 = 2y^2-1 \tag{1}$$

n'a pas d'autres solutions positives que

$$x=0, \quad y=1; \quad x=1, \quad y=1; \quad x=2, \quad y=5.$$

Pour le démontrer nous écrirons l'équation (1) sous la forme équivalente

$$x^4+(x^2-1)^2 = y^2,$$

ou encore

$$(x^2)^2 + (x^2 - 1)^2 = y^2, \tag{2}$$

x^2 et $x^2 - 1$ étant premiers entre eux, y est aussi premier avec ces deux nombres et l'équation de Pythagore (2) aura pour solutions l'un des deux systèmes

$$x^2 = a^2 - b^2; \quad x^2 - 1 = 2ab; \quad y = a^2 + b^2, \tag{I}$$

$$x^2 = 2ab; \quad x^2 - 1 = a^2 - b^2; \quad y = a^2 + b^2, \tag{II}$$

où a et b sont premiers entre eux. Nous allons montrer que chacun de ces cas est impossible sauf pour des valeurs particulières de a et b qui fournissent précisément pour x et y les valeurs de l'énoncé du théorème de Fermat.

A cet effet, nous allons établir les propositions suivantes qui sont plus ou moins connues.

Lemme I. — *Le système diophantique*

$$\text{(F)} \qquad \begin{cases} X^2 + Y^2 = 2Z^2, \\ X^2 - Y^2 = 2U^2 \end{cases}$$

est impossible en nombres entiers tous différents de zéro.

Ce lemme constitue une proposition tout à fait classique dont la démonstration se trouve dans tous les traités d'Analyse diophantique, en particulier dans le livre de M. Carmichael *L'Analyse indéterminée*, page 13 et suivantes.

Corollaire I. — *L'équation diophantique*

$$x^4 + y^4 = 2z^2$$

n'a pas d'autres solutions que $z = \pm x^2 = \pm y^2$.

En effet, on a

$$x^4 + y^4 = (x^2 + y^2)^2 - 2x^2y^2,$$
$$x^4 + y^4 = (x^2 - y^2)^2 + 2x^2y^2,$$

de sorte que l'on peut écrire simultanément

$$2(x^2 + y^2)^2 = (2z)^2 + (2xy)^2,$$
$$2(x^2 - y^2)^2 = (2z)^2 - (2xy)^2,$$

mais, d'après le lemme précédent, une des inconnues $X = 2z$, $Y = 2xy$, $Z = x^2 + y^2$, $U = x^2 - y^2$ doit être nulle; or

$X = 0$ entraîne $Y = Z = U = 0$, d'où $x = y = z = 0$;
$Y = 0$ » $X = Z = U = 0$, » $x = y = z = 0$;
$Z = 0$ » $X = Y = U = 0$, » $x = y = z = 0$;
$U = 0$ » $X = Y = \pm Z$, » $z = \pm x = \pm y^2$,

notre proposition est donc établie.

Corollaire II_1. — *L'équation diophantique*

$$2z^2 = y^4 + 1$$

n'a pas d'autres solutions positives que $z = y = 1$.

En effet, l'équation proposée n'est autre que l'équation du corollaire précédent où l'on a remplacé x par 1; cette dernière équation n'ayant d'autres solutions positives que $z = x^2 = y^2$, l'équation considérée n'a pas d'autres solutions que $z = y = 1$.

Corollaire III_1. — *L'équation diophantique*

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

n'a pas d'autres solutions positives que $z = 2$, $y = 1$.

En effet, d'après l'équation même z est pair, si l'on pose $z = 2z'$ on est ramené à l'équation

$$2z'^2 = 1 + y^4$$

qui, d'après le corollaire précédent n'a pas d'autres solutions que $z' = y = 1$, donc l'équation proposée n'a pas d'autres solutions que $z = 2$, $y = 1$.

Lemme II. — *Les deux équations diophantiques*

(E) $2x^4 + 1 = y^2$,
(E') $8X^4 + 1 = Y^2$,

n'ont pas d'autres solutions positives que $x = 0$, $y = 1$ *pour l'équation* (E), *et* $X = 0$, $Y = 1$, *ou* $X = 1$, $Y = 3$ *pour l'équation* (E').

Remarquons d'abord que si n est un nombre quelconque, les

deux nombres $n-1$ et $n+1$ sont simultanément pairs ou impairs et que leur plus grand commun diviseur ne peut être que 1 ou 2. Cela étant, écrivons les équations données (E) et (E′) sous la forme équivalente

$$2x^4 = (y-1)(y+1), \tag{2}$$

$$8X^4 = (Y-1)(Y+1); \tag{3}$$

ces équations montrent que $y-1$ et $y+1$ sont pairs ainsi que $Y-1$ et $Y+1$. Posons donc

$$y+1 = 2m, \qquad y-1 = 2n; \tag{4}$$

$$Y+1 = 2M, \qquad Y-1 = 2N, \tag{5}$$

on a

$$m-n = M-N = 1.$$

Donc m et n sont premiers entre eux ainsi que M et N. Les équations (2) et (3) deviennent alors

$$x^4 = 2mn; \tag{6}$$

$$2X^4 = MN. \tag{7}$$

la première donne l'un des deux cas

$$m = 8m'^4, \qquad n = n'^4; \tag{A}$$

$$m = m'^4, \qquad n = 8n'^4. \tag{B}$$

L'hypothèse A est impossible car l'on aurait

$$8m'^4 - n'^4 \equiv 2(m'^2)^2 - n'^4 = 1,$$

cette équation n'admet pas d'autres solutions que $n' = 1$, $2m'^2 = 1$; cette dernière n'étant satisfaite par aucune valeur entière de m', l'équation précédente, donc l'hypothèse (A) est impossible.

L'hypothèse (B) donne

$$m'^4 - 8n'^4 = 1,$$

ce qui peut s'écrire

$$8n'^4 = (m'^2)^2 - 1. \tag{8}$$

Or, les équations (4) entraînent

$$n < m < y \qquad \text{pour} \quad y > 1,$$

et l'équation (E) donne

$$y < 2x^2 \qquad \text{pour} \quad x \geq 1,$$

enfin (B) prouve que

$$x^2 < m^4 < y$$

et que

$$2n^2 < y < 2x^2,$$

ou

$$y^n < x^n,$$

d'où, en définitive,

$$n < 2n^2 < x.$$

Donc si l'équation (E) admet une solution $x = x_0$, $y = y_0$, l'équation (E′) admet aussi une solution $X = X_0$, $Y = Y_0$ et l'on a $X_0 < x_0$ et $Y_0 < Y_0$.

Nous allons montrer maintenant que, si l'équation (E′) admet des solutions X'_0 et Y'_0, l'équation (E) admet aussi des solutions x'_0 et y'_0 telles que $x'_0 < X'_0$ et $y'_0 < Y'_0$. Nous aurons ainsi prouvé notre proposition par une double descente de l'infini.

En effet, d'après (7), on a l'un des deux cas

(A′) $\qquad M = 2M'^4, \qquad N = N'^4;$

(B′) $\qquad M = M'^4, \qquad N = 2N'^4.$

L'hypothèse (A′) donne

$$2M'^4 - N'^4 = 1,$$

équation qui, d'après le corollaire II, n'a pas d'autres solutions que $M' = N' = 1$ d'où $M = 2$ et $N = 1$ d'où enfin pour l'équation (E′) $X = 1$ et $Y = 3$.

L'hypothèse (B′) donne à son tour

$$M'^4 - 2N'^4 = 1,$$

ou

$$M'^4 = 2N'^4 + 1.$$

équation qui est de la forme (E) si l'on fait $y = M'^2$ et $x = N'$.

Or, les équations (5) donnent

$$N < M < Y \qquad \text{pour} \quad Y > 1,$$

et l'équation (E′) fournit

$$Y < 4X^2 \qquad \text{pour} \quad X \geq 1.$$

on en conclut

$$M'^2 < M'^4 < Y,$$

et

$$2N'^4 < 4X^2,$$

d'où

$$N'^2 < 2X.$$

et comme $2N' < N'^2$ dès que $N' > 2$, on a donc, dans ce cas,

$$N' < X.$$

Or il est clair que l'hypothèse $N' > 2$ est toujours satisfaite, car pour $N' = 1$ on a $M' = (3)^{\frac{1}{4}}$ et pour $N' = 2$ on a $M' = (33)^{\frac{1}{4}}$, et ces valeurs de M' ne sont pas acceptables puisqu'elles ne sont pas entières.

Pour achever notre démonstration, il nous reste à examiner le cas $y = 1$ pour l'équation (E) et le cas $Y = 1$ pour l'équation (E'). Pour $y = 1$, on a évidemment, d'après (E), $x = 0$; pour $Y = 1$, (E') donne de même $X = 0$. Donc, en dehors de la solution banale $x = 0, y = 1$ pour l'équation (E), et des solutions $X = 0$, $Y = 1$ et $X = 1, Y = 3$ pour l'équation (E'), ces équations n'admettent pas d'autres solutions (1). Notre lemme est donc établi.

Nous sommes maintenant en mesure de démontrer le théorème de Fermat. Examinons les hypothèses I et II.

D'après I on a

$$x^2 = a^2 - b^2 = (a + b)(a - b),$$

a et b étant premiers entre eux, ou bien il en est de même de $a + b$ et $a - b$ ou bien ces deux nombres ont 2 pour plus grand commun diviseur; or cette dernière éventualité n'est pas possible, car dans ce cas, l'équation précédente montre que x^2 est pair, mais puisque nous sommes dans l'hypothèse I, $x^2 - 1$ est aussi pair, ce qui est absurde. Donc $a + b$ et $a - b$ sont premiers entre eux, on doit donc avoir

$$a + b = u^2 \qquad \text{et} \qquad a - b = v^2,$$

d'où

$$x^2 = u^2 v^2; \qquad a = \frac{1}{2}(u^2 + v^2); \qquad b = \frac{1}{2}(u^2 - v^2),$$

et en portant ces valeurs dans l'équation $x^2 - 1 = 2ab$, on a

$$u^2 v^2 - 1 = \frac{1}{2}(u^2 - v^2)(u^2 + v^2),$$

ou encore

$$(u^2 + v^2)^2 = 2(u^4 + 1),$$

(1) En toute rigueur, il faut montrer que la solution $X = 1$, $Y = 3$ appliquée à l'équation (8) ne fournit pas de solutions pour l'équation (6), ce qui est immédiat puisqu'on aurait pour ces valeurs $n' = 1$ et $m'^2 = 3$, et cette dernière relation ne donne pas pour m' une valeur entière.

équation qui, d'après le corollaire III, n'a pas d'autres solutions positives que

$$u^2 + v^2 = 2, \qquad u = 1.$$

ce qui donne $u = 1$ et $v = 1$, d'où $a = 1$ et $b = 0$ et finalement $x = 1$ et $y = 1$.

Passons à l'hypothèse II. Puisque a et b sont toujours premiers entre eux, la relation $x^2 = 2ab$ entraînera l'un des deux cas

II′ $\qquad a = 2u^2 \qquad$ et $\qquad a = v^2.$

II″ $\qquad a = u^2 \qquad$ et $\qquad b = 2v^2.$

Examinons le cas II′; en portant ces valeurs dans la relation

$$x^2 - 1 = a^2 - b^2,$$

on aura

$$4u^2v^2 - 1 = 4u^4 - v^4,$$

ce qui peut s'écrire encore

$$(v^2 + 2u^2)^2 = 8u^4 + 1.$$

équation qui, d'après le lemme II, n'a pas d'autres solutions que $v^2 + 2u^2 = 1$, $u = 0$ et $v^2 + 2u^2 = 3$, $u = 1$; la première donne immédiatement $u = 0$, $v = 1$, d'où $a = 0$, $b = 1$, et enfin, $x = 0$, $y = 1$; de même, la seconde solution fournit $u = 1$, $v = 1$, d'où $a = 2$, $b = 1$, et finalement, $x = 2$, $y = 5$.

Passons maintenant au cas II″. En portant les valeurs de x, a et b dans la relation $x^2 - 1 = a^2 - b^2$, on obtient

$$4u^2v^2 - 1 = u^4 - 4v^4,$$

ou

$$(2v^2 + u^2)^2 = 2u^4 + 1.$$

équation qui, d'après le lemme II, n'a d'autres solutions que

$$u = 0, \qquad 2v^2 + u^2 = 1, \qquad \text{d'où} \qquad u = 0, \qquad 2v^2 = 1,$$

ce qui ne fournit pas de valeur entière pour v.

Notre théorème est donc établi, puisque nous avons épuisé toutes les hypothèses en présence.