Le théorème des deux carrés de Fermat

D. R. Heath-Brown

Pierre de Fermat (1601-1665) était un magistrat français. On l'a décrit comme le plus grand mathématicien amateur de tous les temps, pour ses contributions à l'optique, aux probabilités, et, plus notablement, à la théorie des nombres. Peut-être est-il davantage connu pour le "dernier théorème de Fermat", l'assertion (toujours non démontrée[1]) que $x^n + y^n = z^n$ n'a pas de solutions x, y, z dans les entiers positifs pour tout $n \geq 3$. Les étudiants de première année d'université rencontrent un autre théorème de Fermat (authentique !) énonçant que $x^p \equiv x \pmod{p}$ pour tout entier x et tout nombre premier p, comme conséquence du théorème de Lagrange pour les groupes finis.

Le théorème de Fermat des deux carrés est le suivant :

Si $p \equiv 1 \pmod 4$ est un nombre premier,
alors p est la somme de deux carrés.

Ce résultat est remarquable en cela qu'il relie les nombres premiers - des objets dont la définition ne fait intervenir que la multiplication et la division - à la structure *additive* des entiers. Comme exemples d'illustrations de ce théorème, on a $5 = 1 + 4, 13 = 4 + 9, 17 = 1 + 16$, etc. *Exercice :* Montrer que si $p \equiv 3 \pmod 4$ alors p ne peut pas être la somme de deux carrés (considérer le reste de la division lorsqu'on divise un carré par 4).

Plus de 50 démonstrations différentes du théorème ont été publiées. Les étudiants non diplômés peuvent rencontrer eux-mêmes deux preuves : l'une utilisant la propriété de factorisation unique de $\mathbb{Z}[\sqrt{-1}]$ et l'autre, dans le livre de cours *Elementary Number Theory*, utilisant le théorème d'approximation de Dirichlet. La grande majorité des preuves publiées, et en effet, les deux preuves qui viennent d'être mentionnées, ont de nombreux points communs. En particulier, elles dépendent du fait suivant :

Si $p \equiv 1 \pmod 4$ est un nombre premier, il existe un entier x pour lequel $x^2 + 1 \equiv 0 \pmod p$ - par exemple $x = \left(\frac{(p-1)}{2}\right)!$.

Je décrirai une preuve nouvelle et complètement différente, utilisant les actions de groupes sur les ensembles. Soit

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix}$$

et

$$M = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Référence du fichier original :
https://ora.ox.ac.uk/objects/uuid:c91a3bdd-7d8a-4bea-9734-28caf66f0914.
Traduction : Denise Vella-Chemla, février 2023.

[1] i.e. à l'époque de l'écriture de l'article d'Heath-Brown. Le dernier théorème de Fermat a été démontré, ultérieurement à l'écriture du présent article, en 1994 par Andrew Wiles.

On vérifie aisément que $A^2 = B^2 = C^2 = I$, et que $A^T MA = B^T MB = C^T MC = M$. En particulier A^{-1}, B^{-1}, et C^{-1} existe, par conséquent, les applications linéaires produites par A, B, C sont bijectives.

Définissons

$$S = \{\mathbf{v} = (x, y, z) \in \mathbb{Z}^3 : \mathbf{v}^T M\mathbf{v} = p \text{ et } x, y > 0\}$$

(on pense à $\mathbf{v}$ comme à un vecteur colonne) et soit

$$T = \{(x, y, z) \in S : z > 0\}, \quad U = \{(x, y, z) \in S : x + z > y\}.$$

Notons que $\mathbf{v}^T M\mathbf{v} = p$ signifie simplement que $4xy + z^2 = p$. Il en découle que S est un ensemble fini, puisque $x, y > 0$. On aura besoin de savoir que A envoie S dans lui-même, B envoie T dans lui-même, et C envoie U dans lui-même. On ne regardera que le dernier cas, les autres étant plus faciles. Si $\mathbf{v} = (x, y, z) \in S$ avec $x + z > y$, alors $C\mathbf{v} = (x - y + z, y, 2y - z) = (x', y', z')$, disons. Donc $x' > 0$, parce que $x + z > y$; $y' > 0$, parce que $y > 0$; et $x' + z' > y'$, parce que $x > 0$. De plus

$$(C\mathbf{v})^T M(C\mathbf{v}) = \mathbf{v}^T (C^T MC)\mathbf{v} = \mathbf{v}^T M\mathbf{v} = p,$$

donc C envoie U dans lui-même.

Ensuite on montre que S est l'union disjointe de T et AT, et aussi de U et AU. À nouveau, on vérifiera juste la dernière assertion. Si $(x, y, z) \in S$ alors soit $x + z > y$ (donc $(x, y, z) \in U$) ou $x + z = y$, ou $x + z < y$. Le cas $x + z = y$ ne peut advenir, puisque $\mathbf{v}^T M\mathbf{v} = p$ implique $p = 4xy + z^2 = 4x(x + z) + z^2 = (2x + z)^2$, contredisant la primalité de p. On montrera que si

$$U' = \{(x, y, z) \in S : x + z < y\}$$

alors $U' = AU$; cela donne le résultat requis.

Si $\mathbf{v} = (x, y, z) \in U$ alors $\mathbf{v} \in S$, donc $A\mathbf{v} \in AS = S$. De plus $A\mathbf{v} = (y, x, -z) = (x', y', z')$, disons, avec $x' + z' = y - z < x = y'$ donc $A\mathbf{v} \in U'$. Alors $AU \subseteq U'$. De façon similaire $AU' \subseteq U$, donc $U' = A^2 U \subseteq AU$. Ainsi $U' = AU$.

On atteint maintenant le cœur de la preuve. Puisque A est 1-1, on a $\#T = \#AT, \#U = \#AU$. De plus, comme S est l'union disjointe de T et AT on a $\#S = \#T + \#AT = 2\#T$. De façon similaire $\#S = 2\#U$, donc $\#T = \#U$.

Puisque $C^2 = I$, l'action de C sur U produit des orbites de longueur 1 ou 2. Si (x, y, z) est un point fixe de C alors $x - y + z = x, y = y, 2y - z = z$, donc $y = z$, et puisque $4xy + z^2 = p$ on a $p = 4xy + y^2 = y(4x + y)$. En utilisant le fait que p est un nombre premier et le fait que $p \equiv 1 \pmod 4$, on voit que cela arrive si et seulement si $y = 1$ et $x = (p - 1)/4$. Par conséquent, C a exactement un point fixe dans son action sur U. Puisque toutes les autres orbites ont pour longueur 2, on en déduit que $\#U$ est impair.

On argumente maintenant de façon similaire avec l'action de B sur T. Puisque $\#T(= \#U)$ est impair, il en découle que B doit avoir un nombre impair de points fixes sur U. Il y a donc au moins

un point fixe. Pourtant, un point fixe de B doit avoir $x = y$, et donc $p = 4xy + z^2$ aura une solution pour laquelle $x = y$. Il en découle que $p = (2x)^2 + z^2$ comme requis.

Appendice - Janvier 2008

Invariant était une publication occasionnelle de la société Invariant (la société mathématique des élèves non encore diplômés de l'université d'Oxford). Comme l'article original n'était pas disponible électroniquement, je l'ai réécrit en LaTeX, en corrigeant quelques coquilles.

L'histoire de l'argument utilisé ici a peut-être de l'intérêt. J'ai été amené à cet argument à partir de l'étude d'une présentation des articles de Liouville au sujet des identités pour les fonctions de parité, présentée dans le livre de Uspensky et Heaslet [1]. Mes notes originales datent de 1971. J'ai donné un exposé dans un groupe dissident[2] au colloque mathématique britannique en 1980 (ou 1979 ?), après quoi les notes semblent s'être propagées à travers le monde par le bouche à oreille. Cela devint un exercice pour entraîner les professeurs en France (Varouchas [2]). Plus tard, l'intérêt pour ces éléments a été engendré par la version de la preuve de Zagier en une seule phrase [3].

Références

[1] J.V. Uspensky and M.A. Heaslet, *Elementary Number Theory*, (McGraw-Hill Book Company, Inc., New York, 1939).

[2] I. Varouchas, Une démonstration élementaire du théorème des deux carrés, *I.R.E.M., Bull.*, n° 6 (1984), 31-39.

[3] D. Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, *Amer. Math. Monthly*, 97 (1990), 144.

Mathematical Institute,
24-29, St. Giles',
Oxford
OX1 3LB
UK

rhb@maths.ox.ac.uk

[2] ?