**L'enseignement des mathématiques**
Édité par Melvin Henriksen et Stan Wagon

# Une preuve en une seule phrase que tout nombre premier $p \equiv 1 \pmod 4$ est somme de deux carrés

D. Zagier
*Département de Mathématiques, Université du Maryland, College Park, MD 20742*

L'involution sur l'ensemble fini $S = \{(x, y, z) \in \mathbb{N}^3 \ : \ x^2 + 4yz = p\}$ définie par

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{si } x < y - z \\ (2y - x, y, x - y + z) & \text{si } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{si } x > 2y \end{cases}$$

a exactement un point fixe, donc $|S|$ est impair et l'involution définie par $(x, y, z) \mapsto (x, z, y)$ a également un point fixe. □

Cette preuve est une simplification de celle due à Heath-Brown [1] (inspirée, à son tour, par une preuve donnée par Liouville). Les vérifications des assertions implicitement supposées - que $S$ est fini et que l'application est bien définie et involutive (i.e., égale à sa propre inverse) et a exactement un point fixe - sont immédiates et ont été laissées au lecteur. Seule la dernière nécessite que $p$ soit un nombre premier de la forme $4k + 1$, le point fixe étant alors $(1, 1, k)$.

Notons que la preuve n'est pas constructive : elle ne donne pas une méthode pour effectivement trouver la représentation de $p$ comme somme de deux carrés. Un phénomène similaire advient avec des résultats en topologie et analyse qui sont démontrés en utilisant des théorèmes de points fixes. En effet, le principe de base que nous utilisons : "Les cardinalités d'un ensemble fini et de son ensemble de points fixes par n'importe quelle involution ont la même parité", est un analogue combinatoire et un cas particulier du résultat topologique correspondant : "La caractéristique d'Euler d'un espace topologique et de son ensemble de points fixes sous n'importe quelle involution continue ont la même parité.".

Pour une discussion des preuves constructives du théorème des deux carrés, voir le Coin de l'Éditeur ailleurs dans ce numéro.

## Référence

1. D. R. Heath-Brown, Fermat's two-squares theorem, Invariant(1984) 3-5.

Source : https://people.mpim-bonn.mpg.de/zagier/files/doi/10.2307/2323918/fulltext.pdf
Traduction : Denise Vella-Chemla, février 2023.