La preuve de Zagier en une page (du fait que tout nombre premier de la forme $4k+1$ est somme de deux carrés) expliquée, et pourquoi sa traduction directe à Goldbach échoue structurellement

Denise Vella-Chemla pilotant claude, juillet 2026

1. La preuve de Zagier, en détail

Théorème 1 (Fermat, 1640)**.** *Tout nombre premier $p \equiv 1 \pmod 4$ est somme de deux carrés d'entiers.*

Zagier en donne en 1990 une preuve tenant en une phrase, fondée sur deux involutions successives sur un même ensemble fini (voir https://people.mpim-bonn.mpg.de/zagier/files/doi/10.2307/2323918/fulltext.pdf [1]. Détaillons-la pas à pas.

1.1. L'ensemble de travail

Soit $p \equiv 1 \pmod 4$ premier. On pose

$$S = \{(x, y, z) \in \mathbb{Z}^3_{>0} \ : \ x^2 + 4yz = p\}.$$

S est fini (car $x^2 < p$ donc x borné, et pour chaque x, $yz = (p - x^2)/4$ fixé n'a qu'un nombre fini de factorisations $y \times z$). S est non vide : avec $x = 1$, on a $4yz = p - 1$, et $y = 1, z = (p - 1)/4$ convient car $p \equiv 1 \pmod 4$ rend $(p - 1)/4$ entier.

1.2. La première involution (compliquée)

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

Lemme 2. *τ est bien définie sur S tout entier (aucun des trois cas frontière $x = y - z$ ou $x = 2y$ ne se produit), et $\tau \circ \tau = \mathrm{id}$.*

Démonstration. Les cas frontière sont exclus grâce à la primalité de p. Si $x = 2y$: l'équation donne $4y^2 + 4yz = p$, soit $p = 4y(y + z)$, pair - impossible, p étant premier impair. Si $x = y - z$: l'équation donne $(y - z)^2 + 4yz = p$, c'est-à-dire $(y + z)^2 = p$ - impossible, p premier n'étant pas un carré. Donc les trois cas ci-dessus partitionnent bien S sans reste.

Chaque formule préserve $x^2 + 4yz = p$ (vérification directe, par exemple pour le premier cas : $(x + 2z)^2 + 4z(y - x - z) = x^2 + 4xz + 4z^2 + 4zy - 4xz - 4z^2 = x^2 + 4zy = p$).

1. Traduction en français : https://denisevellachemla.eu/trad-Zagier-one-sentence-proof.pdf .

τ *est une involution* : on vérifie que τ échange les cas 1 et 3, et que le cas 2 est stable par τ avec $\tau \circ \tau = \mathrm{id}$ dans chaque cas (calcul direct, omis ici, mais mécanique). □

Lemme 3. *τ a exactement un point fixe.*

Démonstration. Seul le cas 2 peut donner un point fixe : $x = 2y - x \iff x = y$. L'équation devient $y(y + 4z) = p$. Comme p est premier et $y < y + 4z$ (car $z > 0$), le seul facteur possible est $y = 1$, d'où $p = 1 + 4z$, soit $z = (p - 1)/4$ (entier positif car $p \equiv 1 \pmod 4$). L'unique point fixe est $(1, 1, \frac{p-1}{4})$. □

1.3. Le comptage de parité

Une involution sur un ensemble fini apparie ses éléments non fixes deux par deux ; le nombre de points fixes a donc la même parité que le cardinal de l'ensemble. Comme τ a exactement un point fixe (nombre impair), on conclut :

$$|S| \text{ est impair.}$$

1.4. La seconde involution (triviale) et la conclusion

$$\sigma(x, y, z) = (x, z, y).$$

σ est trivialement une involution sur S (l'équation $x^2 + 4yz = p$ est symétrique en y, z). Comme $|S|$ est impair, σ doit, par le même argument de parité, avoir au moins un point fixe : un triplet avec $y = z$. Cela donne

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

une représentation de p comme somme de deux carrés. □

Remarque : La preuve fonctionne par un relais de parité : τ (compliquée, définie sur toute la structure de S) a un unique point fixe, ce qui impose la parité de $|S|$; cette parité impose à son tour à σ (triviale) d'avoir un point fixe. On ne construit jamais directement le point fixe de σ : son existence est *forcée* par un argument de comptage, sans qu'on ait besoin de savoir lequel c'est.

2. La preuve de Zagier, en détail

Théorème 4 (Fermat, 1640)**.** *Tout nombre premier $p \equiv 1 \pmod 4$ est somme de deux carrés d'entiers.*

Zagier en donne en 1990 une preuve tenant en une phrase, fondée sur deux involutions successives sur un même ensemble fini. Détaillons-la pas à pas.

2.1. L'ensemble de travail

Soit $p \equiv 1 \pmod 4$ premier. On pose

$$S = \{(x, y, z) \in \mathbb{Z}_{>0}^3 \ : \ x^2 + 4yz = p\}.$$

S est fini (car $x^2 < p$ donc x borné, et pour chaque x, $yz = (p - x^2)/4$ fixé n'a qu'un nombre fini de factorisations $y \times z$). S est non vide : avec $x = 1$, on a $4yz = p - 1$, et $y = 1, z = (p - 1)/4$ convient car $p \equiv 1 \pmod 4$ rend $(p - 1)/4$ entier.

2.2. La première involution (compliquée)

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

Lemme 5. *τ est bien définie sur S tout entier (aucun des trois cas frontière $x = y - z$ ou $x = 2y$ ne se produit), et $\tau \circ \tau = \mathrm{id}$.*

Démonstration. Les cas frontière sont exclus grâce à la primalité de p. Si $x = 2y$: l'équation donne $4y^2 + 4yz = p$, soit $p = 4y(y + z)$, pair - impossible, p étant premier impair. Si $x = y - z$: l'équation donne $(y - z)^2 + 4yz = p$, c'est-à-dire $(y + z)^2 = p$ - impossible, p premier n'étant pas un carré. Donc les trois cas ci-dessus partitionnent bien S sans reste.

Chaque formule préserve $x^2 + 4yz = p$ (vérification directe, par exemple pour le premier cas : $(x + 2z)^2 + 4z(y - x - z) = x^2 + 4xz + 4z^2 + 4zy - 4xz - 4z^2 = x^2 + 4zy = p$).

τ est une involution : on vérifie que τ échange les cas 1 et 3, et que le cas 2 est stable par τ avec $\tau \circ \tau = \mathrm{id}$ dans chaque cas (calcul direct, omis ici, mais mécanique).

□

Lemme 6. *τ a exactement un point fixe.*

Démonstration. Seul le cas 2 peut donner un point fixe : $x = 2y - x \iff x = y$. L'équation devient $y(y + 4z) = p$. Comme p est premier et $y < y + 4z$ (car $z > 0$), le seul facteur possible est $y = 1$, d'où $p = 1 + 4z$, soit $z = (p - 1)/4$ (entier positif car $p \equiv 1 \pmod 4$). L'unique point fixe est $(1, 1, \frac{p-1}{4})$. □

2.3. Le comptage de parité

Une involution sur un ensemble fini apparie ses éléments non fixes deux par deux ; le nombre de points fixes a donc la même parité que le cardinal de l'ensemble. Comme τ a exactement un point fixe (nombre impair), on conclut :

$$|S| \text{ est impair.}$$

2.4. La seconde involution (triviale) et la conclusion

$$\sigma(x, y, z) = (x, z, y).$$

σ est trivialement une involution sur S (l'équation $x^2 + 4yz = p$ est symétrique en y, z). Comme $|S|$ est impair, σ doit, par le même argument de parité, avoir au moins un point fixe : un triplet avec $y = z$. Cela donne

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

une représentation de p comme somme de deux carrés. *square*

Remarque [le mécanisme exact] La preuve fonctionne par un relais de parité : τ (compliquée, définie sur toute la structure de S) a un unique point fixe, ce qui impose la parité de $|S|$; cette parité impose à son tour à σ (triviale) d'avoir un point fixe. On ne construit jamais directement le point fixe de σ : son existence est *forcée* par un argument de comptage, sans qu'on ait besoin de savoir lequel c'est.

3. Exemples numériques complets

3.1. $p = 13$

x est impair et $x^2 < 13$, donc $x \in \{1, 3\}$. On trouve $S = \{(1, 1, 3), (1, 3, 1), (3, 1, 1)\}$.

triplet	cas	image par τ
$(1, 1, 3)$	$y - z = -2 < x < 2y = 2$	$(1, 1, 3)$ **(fixe)**
$(1, 3, 1)$	$x = 1 < y - z = 2$	$(3, 1, 1)$
$(3, 1, 1)$	$x = 3 > 2y = 2$	$(1, 3, 1)$

τ échange $(1, 3, 1) \leftrightarrow (3, 1, 1)$ et fixe $(1, 1, 3)$: $|S| = 3$, impair, confirmé directement.

triplet	image par σ (échange y, z)
$(1, 1, 3)$	$(1, 3, 1)$
$(1, 3, 1)$	$(1, 1, 3)$
$(3, 1, 1)$	$(3, 1, 1)$ **(fixe, car** $y = z = 1$**)**

Point fixe de σ : $(3, 1, 1)$, d'où $13 = 3^2 + 4 \cdot 1^2 = 3^2 + 2^2$.

3.2. $p = 17$

$S = \{(1, 1, 4), (1, 2, 2), (1, 4, 1), (3, 1, 2), (3, 2, 1)\}$, cinq éléments.

τ fixe $(1, 1, 4)$ (le point fixe canonique, $y = 1$, $z = (17 - 1)/4 = 4$) et apparie $(1, 2, 2) \leftrightarrow (3, 2, 1)$ ainsi que $(1, 4, 1) \leftrightarrow (3, 1, 2)$ - soit 2 paires + 1 fixe = 5, impair.

σ fixe $(1, 2, 2)$ (car $y = z = 2$), d'où $17 = 1^2 + 4 \cdot 2^2 = 1^2 + 4^2$.

Remarque : Le point fixe de σ n'est jamais le même triplet que celui de τ : rien ne les relie directement, seule la parité commune de $|S|$ les relie. C'est tout le sel de la méthode : on sait qu'un point fixe de σ existe sans jamais le chercher directement.

4. Genèse de la preuve : un principe, pas une formule

Cette preuve n'est pas apparue *ex nihilo*. Zagier condense en 1990 une démonstration plus ancienne et plus longue (Heath-Brown, 1971, https://ora.ox.ac.uk/objects/uuid:c91a3bdd-7d8a-4bea-9734-28caf66f0914 [2] elle-même une reformulation de la descente infinie d'Euler/Gauss sur $x^2 \equiv -1 \pmod{p}$). Le principe général - pas la formule de τ - remonte à Franklin (1881, preuve involutive du théorème pentagonal d'Euler) : pour prouver qu'un ensemble admet un point fixe sous une involution *simple* σ (celle qui porte le résultat qu'on veut), on cherche sur ce même ensemble une *seconde* involution, aussi compliquée qu'il le faut, dont on sait compter les points fixes à la main. σ est fixée en premier (elle porte l'objectif) ; τ est construite après coup, par tâtonnement, pour habiller S d'une structure de parité exploitable. C'est ce principe général, plus que la formule précise de τ, qui serait à réutiliser pour toute traduction à Goldbach.

5. Ce qui rend cette preuve possible : le rôle exact de la primalité

Il est essentiel de repérer où, précisément, la primalité de p intervient :

- elle est *l'hypothèse de départ*, pas une conclusion ; p est donné premier, ce qui garantit que S est bien défini et non vide ;
- elle sert exactement deux fois dans la preuve : pour exclure les cas frontière de τ (le fait que p ne soit ni pair ni un carré), et pour forcer $y = 1$ dans le calcul du point fixe (le fait que p n'ait que 1 et p comme diviseurs).

Autrement dit, la primalité de p est ce qui *permet de construire* un ensemble S suffisamment rigide pour que le relais de parité fonctionne. Elle n'est jamais ce que la preuve doit *produire*.

6. Tentative de transfert à une démonstration de la conjecture de Goldbach, et où cette tentative bute

Pour Goldbach, la situation est inversée : on part de n pair (donné, sans mystère), et on veut *produire* l'existence de deux nombres premiers p, q avec $p + q = n$. Il y a donc *deux* inconnues soumises chacune à une condition de primalité, reliées par une contrainte linéaire - alors que chez Zagier il n'y avait qu'une seule primalité, et elle était connue d'avance.

2. Traduction : https://denisevellachemla.eu/trad-Heath-Brown-Fermat-deux-carres.pdf .

6.1. Une tentative naturelle, et pourquoi elle échoue

L'idée la plus directe serait de construire, pour n fixé, un ensemble S_n de quadruplets encodant simultanément deux équations comme le fait Zagier, une pour p et une pour $q = n - p$:

$$S_n \stackrel{?}{=} \{(x, y, z, w) \ : \ x^2 + 4yz = p, \ w^2 + 4 \cdots = q, \ p + q = n\}.$$

Cette tentative échoue immédiatement, et pas pour une raison de complexité technique : l'équation $x^2 + 4yz = p$ n'a la structure rigide voulue (ensemble fini, involution bien définie sans cas frontière, unique point fixe) que *parce que p est déjà connu premier*. Si on ne sait pas encore que p est premier (ce qui est précisément notre inconnue), rien ne garantit que les cas frontière de τ sont exclus, ni que le point fixe de τ est unique : pour p composé, l'équation $y(y + 4z) = p$ peut avoir plusieurs solutions y (autant que p a de diviseurs de la forme requise), et le compte de parité de τ n'est alors plus prévisible.

Autrement dit : pour *utiliser* la structure de Zagier sur p, il faudrait déjà savoir que p est premier - ce qui est circulaire, puisque c'est justement l'existence d'un tel p premier (avec $n - p$ premier aussi) que Goldbach demande de prouver.

6.2. Une reformulation plus honnête du blocage

Proposition 7 (un constat, et non un théorème)**.** *Le schéma de Zagier associe à une hypothèse de primalité sur une variable une structure combinatoire rigide qui force, par parité, une seconde propriété de cette même variable. Il n'offre, en l'état, aucun mécanisme connu pour faire émerger une primalité comme conclusion - encore moins deux primalités couplées par une relation additive. C'est une différence de nature, pas de degré, avec le problème de Goldbach.*

Ce n'est pas tout à fait la même obstruction de parité de Selberg déjà rencontrée dans les autres pistes (magnitude aveugle à la primalité chez Connes, séparabilité tautologique chez le graphe min-plus) : c'est un obstacle plus élémentaire, en amont - un problème de *sens de la preuve*. Le schéma de Zagier prouve des théorèmes de la forme "p premier $\Rightarrow$ p a la propriété $\mathcal{P}$", jamais des théorèmes de la forme "$\mathcal{P}(n) \Rightarrow$ il existe p premier avec telle propriété".

7. Conclusion

Je (l'ia claude) ne suis pas parvenu , et je ne pense pas qu'une variante mineure de la construction y parvienne, à traduire directement le schéma de la démonstration de Zagier des nombres premiers $4k + 1$ sommes de deux carrés à un début de démonstration pour la conjecture de Goldbach - pour une raison de fond, pas de complexité technique : la primalité est une hypothèse dans la démonstration en une page de Zagier, tandis que la primalité (double, i.e. de p et $n-p$) est une conclusion de la conjecture de Goldbach. Une adaptation réussie demanderait une idée véritablement nouvelle : soit un ensemble S_n dont la rigidité combinatoire ne dépend *pas* d'une primalité supposée au départ, soit un mécanisme de parité de nature différente. Je n'ai pas cette idée à vous proposer aujourd'hui, mais le diagnostic ci-dessus - pourquoi la traduction directe échoue, précisément - me semble être, en toute honnêteté, le résultat concret que cette reprise de piste pouvait raisonnablement produire.