Österreichische Mathematische Gesellschaft

MATHE-BRIEF

November 2026 — Nr. 142

Herausgegeben von der Österreichischen Mathematischen Gesellschaft
http://www.oemg.ac.at/Mathe–Brief ——— mathe–brief@oemg.ac.at

In der Kürze liegt die Würze

Der Zwei-Quadrate-Satz von Fermat besagt, dass eine Primzahl $p \neq 2$ genau dann als Summe von zwei Quadraten ganzer Zahlen geschrieben werden kann, wenn sie kongruent zu 1 (mod 4) ist. Abgesehen von 2 sind alle Primzahlen entweder kongruent zu 1 (mod 4) oder kongruent zu 3 (mod 4) und da Quadrate stets zu 0 oder 1 (mod 4) kongruent sind, kann eine Summe zweier Quadrate niemals zu 3 kongruent sein. Damit reduziert sich die Aussage des Zwei-Quadrate-Satzes auf:

> *Jede Primzahl p, die kongruent 1 mod 4 ist, kann in der Form*
>
> $$p = x^2 + y^2$$
>
> *mit $x, y \in \mathbb{N}$ geschrieben werden.*

Der erste Beweis dieser Aussage stammt von Euler, weitere Beweise wurden von Lagrange, Gauß, Dedekind und Minkowski gegeben. Viele davon verwenden, dass die Kongruenz $x^2 \equiv -1 \pmod{p}$ für besagte Primzahlen stets lösbar ist, was man auch als „-1 ist quadratischer Rest mod p“ formulieren kann. Es wäre sehr lohnenswert, die verschiedenen Beweismethoden zu vergleichen – wir wollen uns allerdings einem Beweis neueren Datums zuwenden, der auf eine einzigen Satz (im Sinne der Grammatik) komprimiert werden kann. Die Idee dazu stammt von R. Heath-Brown, die Ein-Satz-Version von Don Zagier. Hier ist der Ein-Satz-Beweis:

> *Die durch*
>
> $$(x,y,z) \overset{f}{\longmapsto} \begin{cases} (x+2z,\ z,\ y-z-x) & \textit{falls} \quad x < y-z, \\ (2y-x,\ y,\ x-y+z) & \textit{falls} \quad y-z < x < 2y, \\ (x-2y,\ x-y+z,\ y) & \textit{falls} \quad 2y < x \end{cases}$$
>
> *bestimmte Involution f auf der endlichen Menge*
>
> $$S := \{(x,y,z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$$
>
> *hat genau einen Fixpunkt, sodass $|S|$ ungerade ist und die Involution $(x,y,z) \mapsto (x,z,y)$ ebenfalls einen Fixpunkt besitzen muss.*

Alles klar? Wohl kaum, denn wenngleich der Beweis sehr kurz aufgeschrieben ist, muss man dennoch etwas länger darüber nachdenken, um ihn zu durchblicken.

Dazu muss man zunächst den Begriff *Involution* gut verstehen: eine Abbildung f einer Menge M in sich heißt Involution, falls für alle $x \in M$ gilt: $f(f(x)) = x$. Daraus folgt unmittelbar, dass die Elemente $x \in M$ in zwei Klassen zerfallen:

(1) es gilt entweder $f(x) = x$, das heißt x ist Fixpunkt von f,
(2) oder es gilt $f(x) = y$ mit $x \neq y$, wobei dann $f(y) = x$ gilt.

Bei endlichem M entsteht hieraus eine Partition von M in die Menge der Fixpunkte von f und endlich viele zweielementige Mengen. Daraus folgt: Ist die Anzahl der Fixpunkt ungerade, so ist auch die Anzahl der Elemente in M ungerade; ist die Anzahl der Fixpunkte gerade, so ist auch $|M|$ gerade. Insbesondere kann bei $|M|$ ungerade die Menge der Fixpunkte nicht leer sein.

Nun zu den im Beweis impliziten Behauptungen:

- Die angegebene Menge S ist wirklich endlich, weil wegen $x, y, z \geq 1$ alle drei Parameter x, y, z nicht größer als p sein können.

Als nächstes gilt es, zu überprüfen, ob die im Beweis definierte Abbildung f tatsächlich eine Involution ist.

- Bezeichnen wir dazu die drei angegebenen Teilmengen von S mit A, B, C. Sie sind offenbar disjunkt, weil $y - z < 2y$. Wir behaupten, dass für $p \equiv 1 \pmod 4$ auch $S = A \cup B \cup C$ gilt. Das ist deshalb so, weil die Fälle $x = y - z$ und $x = 2y$ für Punkte in S nicht möglich sind. Ersteres würde $p = (y - z)^2 + 4yz = (y + z)^2$ implizieren, d.h. p ist eine Quadratzahl, keine Primzahl. Aus zweiterem folgt $p = 4y^2 + 4yz$, d.h. p ist durch 4 teilbar und damit auch keine Primzahl.
- Man überzeugt sich schnell durch direktes Nachrechnen, dass
$$f(A) \subseteq C, \quad f(C) \subseteq A, \quad f(B) \subseteq B.$$
Damit bildet f die Menge S in sich ab, und Fixpunkte können nur in B liegen.
- Der Nachweis, dass f eine Involution ist, erfolgt analog. Ist etwa $(x, y, z) \in A$, so ist $f(x, y, z) = (x + 2z, z, y - x - z) \in C$ und $f(f(x, y, z)) = f(x + 2z, z, y - x - z) = (x + 2z - 2z, x + 2z - z + y - x - z, z) = (x, y, z)$. Die Fälle $(x, y, z) \in B, C$ folgen analog.

Wir überlegen nun, dass f genau einen Fixpunkt besitzt:

- Da jeder Fixpunkt in B liegen muss, muss für seine Komponenten $2y - x = x$, also $x = y$ gelten, sodass $p = x^2 + 4yz = x^2 + 4xz = x(x + 4z)$ folgt. Laut Voraussetzung gilt $p = 4k + 1$, also ist wegen der Primalität von p nur $x = 1$ und $z = k$ möglich. Umgekehrt liegt der Punkt $(1, 1, k)$ in B, sodass f genau einen Fixpunkt hat.

Jetzt folgt der Beweis unmittelbar aus unseren anfänglichen Überlegungen zu Involutionen:

- Da die Involution f auf S genau einen Fixpunkt besitzt, ist $|S|$ ungerade. Die Abbildung
$$\varphi : S \to S, \ (x, y, z) \mapsto (x, z, y)$$
ist offensichtlich eine Involution auf derselben Menge, muss daher aus Paritätsgründen mindestens einen Fixpunkt besitzen. Für jeden solchen ist $y = z$ und daher $p = x^2 + 4y^2 = x^2 + (2y)^2$, d.h. p is als eine Summe zweier Quadrate dargestellt.

LITERATUR

[1] D.R. Heath-Brown, Fermat's two-squares theorem. *Invariant* **11** (1984), 3–5.
[2] 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.

Leonhard Summerer