Österreichische Mathematische Gesellschaft

MATHE-BRIEF

November 2025 — Nr. 136

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

Der Vierquadratesatz von Lagrange

Jede positive ganze Zahl lässt sich als Summe von 4 Quadraten nichtnegativer ganzer Zahlen schreiben, zum Beispiel $7 = 1^2 + 1^2 + 1^2 + 2^2$, $17 = 0^2 + 0^2 + 1^2 + 4^2 = 0^2 + 2^2 + 2^2 + 3^2$, $46 = 0^2 + 1^2 + 3^2 + 6^2 = 1^2 + 2^2 + 4^2 + 5^2$; die Darstellung ist also offensichtlich nicht immer eindeutig.

Der erste Beweis des Vierquadratesatzes wird Lagrange zugeschrieben: er zeigt zunächst, dass für jede Primzahl p ein Vielfaches mp mit $m \leq p$ existiert, das als Summe von vier Quadraten darstellbar ist. Konkret zeigt er die Existenz zweier Zahlen $a, b \in \{0, 1, \ldots, (p-1)/2\}$, sodass $mp = a^2 + b^2 + 1^2 + 0^2$ mit Hilfe des Studiums der Quadrate in $\mathbb{Z}/p\mathbb{Z}$. Danach zeigt er mit einem indirekten Beweis, dass das minimale m für das mp Summe von vier Quadraten ist, gleich 1 sein muss (siehe auch [1]).

Dass es genügt, die Aussage für Primzahlen herzuleiten, wird anhand folgender bemerkenswerter Identität klar:

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) &= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 \\ &+ (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\ &+ (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 \\ &+ (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2.\end{aligned}$$

In Worten gesagt: das Produkt zweier Zahlen, die Summe von vier Quadraten sind, ist wieder Summe von vier Quadraten.

Diverse andere Beweise und Verallgemeinerungen wurden seither entdeckt, insbesondere hat Jacobi für beliebes $n \in \mathbb{N}$ die Anzahl der Darstellungen von n als Summe von vier Quadraten in Abhängigkeit der Teilersumme von n bestimmt.

Das Thema dieses Briefs ist ein anderer, sehr eleganter Beweis des Vierquadratesatzes, der auf Methoden der Geometrie der Zahlen beruht, konkret auf einer Anwendung des Gitterpunktsatzes von Minkowski. Um diesen Zugang zu erläutern, wollen wir zunächst einige grundlegende Begriffe aus der Geometrie der Zahlen einführen.

Zunächst benötigen wir im $\mathbb{R}^n$ den Begriff eines Gitters, das als Verallgemeinerung von $\mathbb{Z}^n$, also der Punkte mit ganzzahligen Koordinaten angesehen werden kann. Seien dazu $v_1, \ldots, v_m$ m linear unabhängige Vektoren im $\mathbb{R}^n$, also insbesondere $1 \leq m \leq n$. Dann bildet die Menge aller ganzzahligen Linearkombinationen von $v_1, \ldots, v_m$ ein Gitter vom Rang m in $\mathbb{R}^n$, im Fall $m = n$ sprechen wir von einem vollständigen Gitter. $\mathbb{Z}^n$ entspricht dem Gitter, das durch die Auswahl $v_i = e_i$, wobei

e_i den i-ten Vektor der Standardbasis bezeichnet, entsteht. Als Gitterdeterminante eines vollständigen Gitters bezeichnet man das Volumen des Quaders, der von $v_1, \ldots, v_n$ aufgespannt wird. Dieses Volumen kann ganz einfach als $|\det(v_1, \ldots, v_n)|$ berechnet werden und liefert ein Maß für die Dichte des Gitters.

Als nächstes betrachten wir im $\mathbb{R}^n$ beschränkte Mengen M, die den Ursprung O als inneren Punkt enthalten, bezüglich des Ursprungs symmetrisch liegen und konvex sind. Letzteres bedeutet, dass für je zwei Punkte in M das gesamte Geradensegment zwischen diesen Punkten auch in M liegt. Solche Mengen bezeichnet man als zentralsymmetrische, konvexe Mengen. Man kann zeigen dass diese stets Jordan messbar sind (also ein n-dim. Volumen besitzen). Für die Vorstellung genügt es, sich unter zentralsymmetrischen, konvexen Mengen etwa Quader, Kugeln oder Ellipsoide vorzustellen.

Jetzt ist es an der Zeit, zentralsymmetrische, konvexe Mengen und Gitter gleichzeitig zu betrachten. Ist M eine solche Menge und Λ ein Gitter, so folgt aus beider Definition, dass der Ursprung O sowohl in M als auch in Λ liegt, dass also Λ einen Gitterpunkt enthält. Es stellt sich unmittelbar die Frage, ob noch weitere Gitterpunkte in M liegen, bzw. nach notwendigen Bedingungen an M, die dies garantieren. Eine einfache solche Bedingung gibt der Gitterpunktsatz von Minkowski an, der das Volumen von M und die Gitterdeterminante von Λ in Beziehung setzt:

Sei M eine zentralsymmetrische, konvexe Menge im $\mathbb{R}^n$ und Λ ein vollständiges Gitter im $\mathbb{R}^n$. Falls $V(M) > 2^n \det(\Lambda)$, so enthält M mindestens einen von O verschiedenen Gitterpunkt.

Für einen Beweis siehe etwa [2, S. 259ff].

Mit dieser Aussage können wir nun den Beweis des Satzes von Lagrange in Angriff nehmen. Wie bereits anfänglich erläutert, genügt es, die Darstellbarkeit aller Primzahlen p als Summe von vier Quadraten herzuleiten. Als erstes überlegen wir uns, dass die Kongruenz $r^2 + s^2 + 1 \equiv 0 \pmod{p}$ stets in ganzen r, s lösbar ist. Dies ist für $p = 2$ klar, sodass wir uns auf ungerade p beschränken können. Die Menge S der Restklassen $\{0^2, 1^2, \ldots, ((p-1)/2)^2\} \bmod p$ erfüllt $|S| = (p+1)/2$ denn all diese Quadrate sind inkongruent $\bmod p$. Analog gilt für die Menge S' der Restklassen $\{-1-0^2, -1-1^2, \ldots, -1-((p-1)/2)^2\} \bmod p$, dass $|S'| = (p+1)/2$. S und S' sind Teilmengen von $\mathbb{Z}/p\mathbb{Z}$ und müssen sich daher in mindestens einem Element schneiden, was eine Lösung von $r^2 \equiv -1 - s^2 \pmod{p}$ liefert.

Ausgehend von r, s betrachten wir nun im $\mathbb{R}^4$ die Vektoren $(p, 0, 0, 0)$, $(0, p, 0, 0)$, $(r, s, 1, 0)$ und $(s, -r, 0, 1)$ und das von ihnen aufgespannte Gitter Λ. Berechnung der Determinante der Vektoren liefert $\det(\Lambda) = p^2$. Ist (x_1, x_2, x_3, x_4) ein Gitterpunkt, so ist

$$(x_1, x_2, x_3, x_4) = \begin{pmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$$

für ein $(\alpha, \beta, \gamma, \delta) \in \mathbb{Z}^4$ und daher

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= (\alpha p + \gamma r + \delta s)^2 + (\beta p - \gamma s - \delta r)^2 + \gamma^2 + \delta^2 \\ &\equiv (1 + r^2 + s^2)(\gamma^2 + \delta^2) \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Fehlt noch die passende zentralsymmetrische, konvexe Menge: wir wählen dafür die Kugel bestehend aus den Punkten $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ mit $x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p$. Das Volumen einer 4-dimensionalen Kugel mit Radius r ist gegeben durch $\pi^2 r^4/2$, was mit $r = \sqrt{2p}$ auf $2\pi^2 p^2$ führt und sicher grösser als $2^4 p^2$ ist. Minkowskis Gitterpunktsatz besagt daher, dass sich in der Kugel ein Gitterpunkt (x_1, x_2, x_3, x_4) ungleich $(0, 0, 0, 0)$ liegt, für den also

$$0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p$$

gilt, nebst $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{p}$. Es bleibt also nur die Möglichkeit $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$, wie gewünscht.

Damit ist der Beweis des Vierquadratesatzes vollendet, eine Zusatzüberlegung scheint aber noch angebracht: zumal in Lagranges Formulierung die Quadrate aus nichtnegativen Zahlen zu bilden sind, ist 0^2 als Summand zulässig und bei manchen Zahlen auch notwendig, wie etwa das Beispiel $6 = 0^2 + 1^2 + 1^2 + 2^2$ zeigt.

Wieviele Quadrate würde man brauchen, würde man auf Quadrate positiver ganzer Zahlen einschränken? Diesbezüglich gilt folgender Satz:

Jede ganze Zahl > 169 *ist Summe von fünf Quadraten positiver ganzer Zahlen.*

Zum Beweis bemerken wir zunächst, dass 169 sich als Summe von einem, von zwei, von drei und von vier positiven Quadraten schreiben lässt, nämlich

$$169 = 13^2 = 12^2 + 5^2 = 12^2 + 4^2 + 3^2 = 8^2 + 8^2 + 5^2 + 4^2.$$

Zudem wissen wir aus dem Vierquadratesatz, dass jede ganze Zahl n als Summe von einem, von zwei, von drei oder von vier positiven Quadraten darstellbar ist. Für $n > 169$ schreiben wir nun $n = m + 13^2$ mit positivem m und je nachdem, wieviele positive Quadrate zur Darstellung von m gebraucht werden, belassen wir den Summanden 13^2 oder ersetzen ihn durch $12^2 + 5^2$ oder $12^2 + 4^2 + 3^2$ oder $8^2 + 8^2 + 5^2 + 4^2$ um genau fünf Summanden zu erhalten, wie behauptet.

Durch explizite Untersuchung der Zahlen < 169 kann überdies gezeigt werden, dass 33 die größte Zahl ist, die nicht Summe von fünf Quadraten positiver ganzer Zahlen ist.

LITERATUR

[1] Wacław Sierpiński: Elementary Theory of Numbers. Chapter XI: Representations of Natural Numbers as Sums of Non-Negative kth Powers (= North-Holland Mathematical Library. Band 31). 2. überarbeitete und erweiterte Auflage. North-Holland 1988, S. 378-430.

[2] Armin Leutbecher: Zahlentheorie: Eine Einführung in die Algebra. Springer-Verlag, 1996.

Leonhard Summerer