Zerlegung in Quadratzahlen

Die Zerlegung von natürlichen Zahlen in die Summe von Quadratzahlen ist eine alte, abgeschlossene Theorie, die schon von FERMAT im 17. Jahrhundert und später von EULER, LAGRANGE und JACOBI bearbeitet wurde; die wichtigsten Resultate gehen auf die oben genannten zurück.

Unmöglichkeitssätze zu Zerlegungen

Wir werden später sehen, dass jede natürliche Zahl als Summe von höchstens vier Quadratzahlen darstellbar ist. Dies wurde schon von FERMAT vermutet und später von LAGRANGE bewiesen. Die Anzahl dieser Darstellungen bestimmte JACOBI, siehe Satz 10.

Satz 1 (a) *Eine Primzahl der Form* $4k + 3$ *lässt sich nicht als Summe von zwei Quadratzahlen schreiben*
(b) *Eine Zahl der Form* $4^n(8k+7)$ *lässt sich nicht als Summe von drei Quadratzahlen schreiben.*

Beweis . (a) Die quadratischen Reste modulo 4 sind 0 und 1. Somit läßt sich 3 nicht als Summe zweier solcher Reste schreiben.
(b) Mit vollständiger Induktion über n. Im Falle $n = 0$ betrachten wir die quadratischen Reste modulo 8; das sind 0, 1 und 4. Die Summe dreier solcher Reste kann aber niemals den Rest 7 ergeben. Nehmen wir jetzt an, die Zahl $4^a(8k + 7)$ ist nicht als Summe von drei Quadraten darstellbar. Wir haben zu zeigen, dass dann auch $4^{a+1}(8k + 7)$ nicht als Summe von drei Quadratzahlen darstellbar ist. Angenommen, es gibt doch eine derartige Darstellung

$$4^{a+1}(8k + 7) = u^2 + v^2 + w^2.$$

Dann folgt aus $u^2 + v^2 + w^2 \equiv 0 \pmod 4$ sofort $u \equiv v \equiv w \equiv 0 \pmod 2$, denn der Rest 0 lässt sich nur als $0 = 0 + 0 + 0 \pmod 4$ mit drei quadratischen Resten modulo 4 darstellen. Dann kann man aber die obige Gleichung durch 4 dividieren und man erhält einen Widerspruch zur Induktionsannahme, [4, Abschnitt 6.2]. □

Bemerkung . Es ist erwähnenswert, dass alle Zahlen, die nicht von der Form $4^n(8k+7)$ sind, als Summe von 3 Quadratzahlen darstellbar sind. Dies ist schwierig zu zeigen. Den Beweis findet man etwa in [5, Band I, Teil III, Kap. 4] ■

Die Darstellung natürlicher Zahlen als Summe von Quadraten

Im folgenden Abschnitt werden wir die Frage beleuchten, wann eine natürliche Zahl als Summe von zwei bzw. vier Quadratzahlen darstellbar ist. Zum Schluss werden wir — allerdings ohne Beweis — auch Formeln für die Anzahl solcher Zerlegungen angeben. Haben wir im vorigen Abschnitt einfache Negativ-Resultate bewiesen, so wollen wir uns nun den etwas schwierigeren Existenz- und Eindeutigkeitssätzen für Zerlegungen zuwenden.

Satz 2 (a) *Es seien* $m = a^2 + b^2$ *und* $n = x^2 + y^2$*. Dann ist*

$$mn = (ax + by)^2 + (ay - bx)^2 = (ax - by)^2 + (ay + bx)^2.$$

(b) *Es seien* $m = a^2 + b^2 + c^2 + d^2$ *und* $n = x^2 + y^2 + z^2 + u^2$*. Dann gilt*

$$\begin{aligned} & mn = A^2 + B^2 + C^2 + D^2, \text{ wobei} \\ & A = ax + by + cz + du, \qquad && B = ay - bx - cu + dz, \\ & C = az + bu - cx - dy, && D = au - bz + cy - dx. \end{aligned}$$

Bemerkung: Die Formeln aus (a) werden mitunter LEONARDO VON PISA (1180 –1250), genannt FIBONACCI, zugeschrieben. Die Formeln (b) gehen wahrscheinlich auf EULER zurück.

Beweis . Man erhält die Identitäten unmittelbar durch Ausmultiplizieren (binomische Formel). Natürlich gibt es auch bei (b) mehrere Möglichkeiten, der Darstellung des Produkts. □

Somit kann man sich in beiden Fällen auf die Zerlegung von Primzahlen zurückziehen. Oben haben wir gesehen, dass sich die Primzahlen der Form $4k + 3$ nicht als Summe von zwei Quadraten schreiben lassen.

Satz 3 *Jede Primzahl der Form* $4n + 1$ *lässt sich eindeutig als Summe von zwei Quadratzahlen schreiben.*

Der erste Schritt zum Beweis dises Satzes ist die Feststellung, dass -1 quadratischer Rest modulo p ist, wenn $p = 4n + 1$. Das heißt, es gibt einen Rest x mit $x^2 \equiv -1 \pmod p$. Hierfür geben wir drei verschiedene Beweise an. Der erste benutzt ausschließlich Kongruenzrechnung und ist daher am längsten. Der zweite benutzt Polynome über dem Körper $\mathbb{F}_p$. Der dritte Beweis benutzt, dass die Gruppe der Einheiten $\mathbb{F}_p^*$ zyklisch ist.

1. Beweis.
Satz 4 (Wilson) *Für jede Primzahl* p *ist*

$$(p - 1)! \equiv -1 \pmod p.$$

Wenn umgekehrt diese Kongruenz besteht, dann ist p *eine Primzahl.*

Beweis . Für $p = 2$ und $p = 3$ ist der Satz sofort einzusehen. Es sei also $p > 3$. Keine der Zahlen

$$2, 3, \ldots, p - 2$$

genügt der Kongruenz $x^2 \equiv 1 \pmod p$. Denn diese Kongruenz ist gleichwertig mit $p|(x-1)(x+1)$ und, da p Primzahl ist, sind $x \equiv \pm 1 \pmod p$ die einzigen beiden Lösungen. In der oben genannten Folge von Resten gibt es also zu jedem x ein x' mit $xx' \equiv 1 \pmod p$, wobei $x' \not\equiv x \pmod p$. Die obigen $p-3$ Reste lassen sich also zu Paaren anordnen, deren Produkt immer kongruent 1 modulo p ist. Somit gilt

$$(p-2)! \equiv 1 \pmod p, \quad \text{bzw.} \quad (p-1)! \equiv -1 \pmod p.$$

Für jede zusammengesetzte Zahl $n = ab$ ist $(n-1)! \equiv 0 \pmod n$, da die Faktoren a und b beide in den Zahlen $1, \ldots, n-1$ als Faktoren aufgehen. □

Satz 5 *Ist p eine Primzahl der Form $4n+1$, so ist*

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p.$$

Beweis . Nach dem WILSONschen Satz gilt

$$\begin{aligned} -1 &\equiv (p-1)! \equiv 1{\cdot}2 \cdots 2n{\cdot}(2n+1) \cdots 4n \equiv 1 \cdots 2n(-2n)(-2n+1) \cdots (-1) \\ &\equiv (2n)!(-1)^{2n} \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p. \end{aligned}$$

Insbesondere erhält man für $x \equiv \left(\frac{p-1}{2}\right)! \pmod p$, dass $x^2 \equiv -1 \pmod p$. □

Zweiter Beweis.

Satz 6 (Eulersches Kriterium) *Es sei p eine Primzahl und $a \in \mathbb{Z}$, $p \nmid a$. Dann gilt*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p \tag{1}$$

Beweis . Wegen $\mathrm{ggT}\,(a,p) = 1$ gilt nach dem Kleinen Satz von FERMAT

$$0 \equiv a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \pmod p.$$

Somit gilt entweder $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$ oder $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$, da p eine ungerade Primzahl ist. Ist a einer der $(p-1)/2$ quadratischen Reste $1^2, 2^2, \ldots, ((p-1)/2)^2$ (mehr quadratische Reste kann es nicht geben, da nicht mehr Quadratzahlen in $\mathbb{F}_p$ existieren) also etwa $a \equiv x^2 \pmod p$, dann gilt $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$. Umgekehrt hat die Gleichung $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$ höchstens $(p-1)/2$ Lösungen. Somit gilt genau für die $(p-1)/2$ quadratischen Nicht-Reste $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. □

Setzt man insbesondere $a = -1$ ein, so hat man

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{2n} \equiv 1 \pmod p.$$

Somit ist -1 quadratischer Rest.

Dritter Beweis: Da die multiplikative Gruppe der primen Reste $\mathbb{F}_p^*$ zyklisch mit der Ordnung $p-1 = 4n$ ist, existieren auch Elemente der Ordnung 4, etwa $x^4 \equiv 1 \pmod p$. Also gilt $(x^2-1)(x^2+1) \equiv 0 \pmod p$. Da aber x nicht die Ordnung 1 oder 2 hat, gilt $x^2 - 1 \not\equiv 0 \pmod p$ und somit $x^2 \equiv -1 \pmod p$.

Satz 7 (Thue) *Es sei p eine Primzahl, e und f zwei natürliche Zahlen mit $e, f \leq p-1$ und $p < ef$. Dann lassen sich alle Reste r modulo p auf die folgende Gestalt bringen: $r \equiv 0 \pmod p$ oder*

$$r \equiv \pm\frac{x}{y} \pmod p, \quad \textit{wobei} \quad 1 \leq x \leq e-1 \quad \textit{und} \quad 1 \leq y \leq f-1.$$

Beweis . Es sei $r \not\equiv 0 \pmod p$. Wir betrachten die ef Reste $v + rw$, wobei $0 \leq v < e$ und $0 \leq w < f$ gelte. Weil $ef > p$, müssen mindestens zwei dieser Reste übereinstimmen, etwa

$$v_1 + rw_1 \equiv v_2 + rw_2 \pmod p.$$

Der Fall $w_1 = w_2$ ist aber unmöglich, da sonst auch $v_1 = v_2$ gelten würde, und die Paare sind gleich. Es gilt also

$$r \equiv \frac{v_2 - v_1}{w_1 - w_2} \equiv \pm\frac{v_1 - v_2}{w_1 - w_2} \pmod p$$

und $|v_1 - v_2| < e$ und $|w_1 - w_2| < f$. □

Beweis (von Satz 3). Wir richten uns nach [6, Kapitel VII, Abschnitt 3]. Nach der obigen Satz 5 gibt es eine Lösung der Kongruenz $z^2 \equiv -1 \pmod p$. Wir wenden den Satz von THUE mit $e = f$ an, so dass $e^2 > p$ gilt. Dabei sei e die kleinste derartige Zahl. Es gibt also zwei natürliche Zahlen x und y mit $0 < x, y < e$, so dass $z \equiv \pm x/y \pmod p$ gilt. Dann ist aber

$$\left(\frac{x}{y}\right)^2 \equiv z^2 \equiv -1 \pmod p$$

und somit $x^2 + y^2 = pr$ für eine gewisse natürlichen Zahl r. Wegen $x, y < e$ ist $x^2 < p$ und auch $y^2 < p$, denn sonst wäre e nicht die kleinste Zahl mit $e^2 > p$. Somit ist $x^2 + y^2 = pr < 2p$. Also gilt $r = 1$ und somit $x^2 + y^2 = p$.

Zur Eindeutigkeit. Angenommen, $p = x^2 + y^2 = u^2 + v^2$ sind zwei Darstellungen für p. Dann gilt $-1 \equiv x^2/y^2 \equiv u^2/v^2 \pmod p$. Hieraus folgt

$$\frac{x}{y} \equiv \pm\frac{u}{v} \equiv \mp\frac{v}{u} \pmod p.$$

Durch Vertauschung von u und v kann man jedenfalls erreichen, dass $x/y \equiv u/v \pmod p$ bzw. $xv - yu \equiv 0 \pmod p$ gilt. Nun ist aber

$$p^2 = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2.$$

Da der letzte Summand durch p^2 teilbar sein muss, muss er sogar gleich 0 sein, also $xv = yu$. Wegen $\mathrm{ggT}\,(x, y) = 1$ und $\mathrm{ggT}\,(u, v) = 1$ folgt hieraus $x = u$ und $y = v$. $\square$

In schönster Allgemeinheit lautet der 2-Quadrate Satz dann

Satz 8 *Eine natürliche Zahl n ist genau dann als Summe zweier Quadratzahlen darstellbar, wenn jeder Primfaktor der Form $4k + 3$ in gerader Anzahl in n auftritt.*

Potenzreihen

In diesem Abschnitt soll ganz knapp angedeutet werden, wie man Potenzreihen zum Abzählen von Lösungen nutzen kann.

Satz 9 (Jacobi, 1828) *Die Anzahl der Darstellungen einer natürlichen Zahl n als Summe von 2 Quadraten ist gleich*

$$4(\mathrm{d}_{1,4}(n) - \mathrm{d}_{3,4}(n)).$$

Dabei ist $\mathrm{d}_{r,4}(n)$ die Anzahl der Teiler von n (einschließlich 1 und n), die bei der Division durch 4 den Rest r lassen.

Satz 10 (Jacobi, 1829) *Die Anzahl der Darstellungen einer natürlichen Zahl n als Summe von 4 Quadraten ist gleich*

$$8 \sum_{d|n,\, 4\nmid d} d.$$

Bemerkung . In beiden Sätzen zählen die Darstellungen $5 = 1^2 + 2^2 = (-1)^2 + 2^2 = 1^2 + (-2)^2 = (-1)^2 + (-2)^2 = 2^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + 1^2 = (-2)^2 + (-1)^2$ alle als verschiedene Darstellungen. Tatsächlich ist $\mathrm{d}_{1,4}(5) = 2$, da 1 und 5 beides Teiler von 5 sind, die den Rest 1 lassen. Ferner ist $\mathrm{d}_{3,4}(5) = 0$ und somit kommt man auf 8 Darstellungen. Darstellungen mit 0 als Summand werden ebenfalls mitgezählt: $4 = (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2$ (16 Möglichkeiten) und $4 = (\pm 2)^2 + 0^2 + 0^2 + 0^2 = 0^2 + (\pm 2)^2 + 0^2 + 0^2 = 0^2 + 0^2 + (\pm 2)^2 + 0^2 = 0^2 + 0^2 + 0^2 + (\pm 2)^2$ (8 Möglichkeiten). Tatsächlich ist $\sum_{d|4,\, 4\nmid d} d = 1 + 2 = 3$ und es gibt 24 Zerlegungen von 4 in 4 Quadrate. ■

Bemerkung . Der Satz 10 hat den Satz von LAGRANGE zur Folge: Jede natürliche Zahl lässt sich als Summe von 4 Quadratzahlen schreiben. Denn die im Satz angegebene Anzahl von Zerlegungen ist für alle n eine *positive* natürliche Zahl, da $d = 1$ als Teiler stets mitgezählt wird. ■

Der Ausgangspunkt für unseren Beweis ist dabei der folgende Satz. Einen elementaren Beweis dieses Satzes — durch reines Abzählen von Partitionen — findet man in [1, Chapter 2.2].

Satz 11 Jacobi-Tripelprodukt-Identität *Für $|q| < 1$ und alle x gilt:*

$$\prod_{i=1}^{\infty}(1 + q^i x)(1 + q^{i-1}x^{-1})(1 - q^i) = \sum_{n\in\mathbb{Z}} q^{n(n+1)/2} x^n. \tag{2}$$

Durch trickreiche Umformungen [3] leitet man hieraus die folgenden beiden Identitäten ab

$$\left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^2 = 1 + 4 \sum_{k\geq 1, l\geq 0} (q^{k(4l+1)} - q^{k(4l+3)}) = 1 + 4 \sum_{n\geq 1} (\mathrm{d}_{1,4}(n) - \mathrm{d}_{3,4}(n)) q^n, \tag{3}$$

$$\left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^4 = 1 + 8 \sum_{n\geq 1} \left(\sum_{d|n,\, 4\nmid d} d\right) q^n. \tag{4}$$

Schauen wir uns die linke Seite von (3) einmal genauer an. Nach formalem Ausmultiplizieren der beiden unendlichen Reihen lautet der allgemeine Summand $a_r q^r$, wobei für ein festes r alle Summanden $q^r = q^{n_1^2} q^{n_2^2}$ mit $n_1, n_2 \in \mathbb{Z}$ zu berücksichtigen sind. Jede Lösung (n_1, n_2) der Gleichung $r = n_1^2 + n_2^2$ liefert also einen Summanden q^r. Also ist a_r die gesuchte Anzahl.

Literatur

[1] Bressoud, D. M.: *Proofs and confirmations. The story of the alternating sign matrix conjecture*, MAA Spectrum, Cambridge University Press, Cambridge, 1999

[2] Engel, A.: *Problem-solving strategies*, Springer, New York, 1998

[3] Hirschhorn, M. D.: Partial fractions and four classical theorems of number theory, *Amer. Math. Monthl.* **107** (2000), 260–264

[4] Krätzel, E.: *Zahlentheorie*, Nummer 19 in Studienbücherei. Mathematik für Lehrer, VEB Deutscher Verlag der Wissenschaften, Berlin, 1981

[5] Landau, E.: *Vorlesungen über Zahlentheorie*, Chelsea Publishing Co., New York, 1969

[6] Neiß, F.: *Einführung in die Zahlentheorie*, S. Hirzel Verlag, Leipzig, 1952

[7] Pieper, H.: *Die komplexen Zahlen. Theorie – Praxis – Geschichte*, Nummer 110 in Mathematische Schülerbücherei, Deutscher Verlag der Wissenschaften, Berlin, 1991

[8] Postnikov, M. M.: *Vvedenie v teoriyu algebraicheskikh chisel (Russian) [Introduction to algebraic number theory]*, Nauka, Moscow, 1982