Zerlegung von natürlichen Zahlen in die Summe von Quadratzahlen

Axel Schüler, Mathematisches Institut, Univ. Leipzig

mailto:schueler@mathematik.uni-leipzig.de

Februar 2001

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.

Die pythagoräischen Tripel

Wir suchen Lösungen der Gleichung

$$x^2 + y^2 = z^2, \quad \text{mit} \quad x, y, z \in \mathbb{N}. \tag{1}$$

Diese Tripel (x, y, z) natürlicher Zahlen heißen *pythagoräische Zahlentripel*. Sicherlich kennt jeder das Tripel $(3, 4, 5)$, es gilt die Gleichung $3^2 + 4^2 = 9 + 16 = 25 = 5^2$. Vielleicht kennen ja auch einige das Tripel $(5, 12, 13)$ — es ist $5^2 + 12^2 = 25 + 144 = 169 = 13^2$. Es stellt sich nun die Frage nach *allen* Lösungen der obigen Gleichung. Als erstes beobachtet man, dass mit (x, y, z) auch (tx, ty, tz), $t \in \mathbb{N}$ eine Lösung von (1) ist. Haben umgekehrt zwei der Zahlen x, y, z einen gemeinsamen Teiler t, so ist auch die dritte Zahl durch t teilbar und man kann (1) duch t^2 dividieren und erhält eine kleinere Lösung. Das kann man so lange machen, bis $\mathrm{ggT}\,(x, y, z) = 1$. Solche Lösungen heißen *primitiv*. Als zweites stellt man fest, dass in einer primitiven Lösung (x, y, z) immer genau eine der Zahlen x, y gerade ist, die andere und z sind stets ungerade. Wären nämlich x und y gerade, dann hat man keine primitive Lösung mehr, da man das Tripel durch 2 teilen kann, wären beide ungerade, etwa $x = 2a + 1$, $y = 2b + 1$, dann wäre $z^2 = 4(a(a + 1) + b(b + 1)) + 2$. Eine Quadratzahl kann aber nicht den Rest 2 bei der Division durch 4 lassen.

Gibt es endlich oder unendlich viele primitive pythagoräische Tripel? Eine einfache Beobachtung der Folge der Quadratzahlen und ihrer Differenzenfolge beantwortet die Frage sofort.

n	1	2	3	4	5	6	7	8
n^2	1	4	9	16	25	36	49	64
Differenz		3	5	7	9	11	13	15

Die Differenzenfolge der aufeinanderfolgenden Quadratzahlen durchläuft also alle ungeraden natürlichen Zahlen. Jede ungerade Quadratzahl $(2n+1)^2$ in der Differenzenfolge liefert also ein pythagoräisches Tripel $(2n(n+1), 2n+1, 2n(n+1)+1)$. Dies ist primitiv, da x und z aufeinanderfolgend und damit teilerfremd sind. Unsere obigen beiden Beispiel sind genau von dieser Gestalt. Gibt es aber noch andere primitive Tripel? Mit etwas Geschick oder mit dem Computer findet man das primitive Tripel $(8, 15, 17)$, das offenbar keine aufeinanderfolgenden Quadratzahlen enthält. Nun ist es an der Zeit eine vollständige Lösung anzugeben.

Satz 1 *Für beliebige paarweise teilerfremde natürliche Zahlen m und n mit $m > n$, wobei eine von beiden gerade und die andere ungerade ist, liefern die Formeln*

$$\begin{aligned} x &= 2mn, \\ y &= m^2 - n^2, \\ z &= m^2 + n^2 \end{aligned} \tag{2}$$

eine primitive Lösung von (1)*. Umgekehrt ist jede primitive Lösung von* (1) *mit geradem x von dieser Gestalt.*

Beweis: (nach [8, §2]) Die leicht nachzurechnende Identität

$$(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$$

beweist, dass (2) ein pythagoräisches Tripel von positiven ganzen Zahlen (x, y, z) liefert. Hätten die drei Zahlen einen gemeinsamen Teiler $t \geq 2$, so hätten auch

$$2m^2 = y + z = (m^2 - n^2) + (m^2 + n^2) \quad \text{und} \quad 2n^2 = z - y = (m^2 + n^2) - (m^2 - n^2)$$

diesen gemeinsamen Teiler. Da aber m und n teilerfremd sind, muss $t = 2$ gelten. Dann ist aber $y = m^2 - n^2$ gerade. Also sind m und n beide gerade oder beide ungerade, was unserer Voraussetzung widerspricht. Es gibt daher keinen echten gemeinsamen Teiler; die angegebene Lösung ist primitiv.
Sei umgekehrt (x, y, z) eine primitive Lösung von (1) mit positiven ganzen Zahlen. O. B. d. A. sei $x = 2a$ die gerade Zahl und y und z ungerade. Dann sind $z + y = 2b$ und $z - y = 2c$ gerade Zahlen mit $a, b, c \in \mathbb{N}$. Jeder gemeinsame Teiler d von b und c ist auch gemeinsamer Teiler von y und z, also sind b und c teilerfremd. Andererseits ist nach (1)

$$4a^2 = x^2 = z^2 - y^2 = (z + y)(z - y) = 4bc \quad \text{also} \quad a^2 = bc.$$

Wegen der eindeutigen Primfaktorzerlegung der natürlichen Zahlen und wegen der Teilerfremdheit von b und c, müssen b und c bereits für sich Quadratzahl sein, also $b = m^2$ und $c = n^2$. Dann ergibt sich $a^2 = m^2n^2$ und somit $a = mn$. Wir erhalten insgesamt $x = 2mn$, $z = b + c = m^2 + n^2$ und $y = b - c = m^2 - n^2$. Wegen $b > c$ gilt auch $m > n$. $\square$

Aufgabe 1 Man zeige, dass jedes primitive pythagoräische Tripel (m, n) mit $m > n$ genau 3 primitive Tripel als Nachfolger hat und, falls es von $(1, 0, 0)$ veschieden ist, genau einen Vorgänger. Keine zwei Nachfolger fallen dabei zusammen.

Lösung: Es sei $M = \{(m, n) \in \mathbb{N} \times \mathbb{N} \,|\, m > n, \operatorname{ggT}(m, n) = 1, m \not\equiv n \pmod 2\}$ die Menge der Paare, die die primitiven pythagoräischen Tripel parametrisiert. Man überzeugt sich

leicht davon, dass die drei Funktionen $f(m,n) := (2n+m,n)$, $g(m,n) := (2m+n,m)$ und $h(m,n) := (2m-n,m)$ die Menge M in sich selbst abbilden, denn der ggT bleibt erhalten, die verschiedene Parität und die erste Komponente ist noch immer größer als die zweite. Zur Eindeutigkeit des Nachfolgers. Es sei (m',n') der Nachfolger von (m,n) unter f, g bzw. h. Für die Abbildung f gilt $m' > 3n'$, für g gilt $3n' > m' > 2n'$ und für h gilt schließlich $2n' > m'$. Die Größenverhältnisse von m' und n' bestimmen also den Vorgänger eindeutig. Man überzeugt sich auch davon, dass diese Rückabbildung stets möglich ist.
Im Falle $a > 3b$ wähle man $\tilde{a} := a - 2b$ und $\tilde{b} := b$; im Falle $3b > a > 2b$ wähle man $\tilde{a} := b$ und $\tilde{b} := a - 2b$; im Falle $2b > a$ wähle man $\tilde{a} := b$ und $\tilde{b} := 2b - a$.

Die Methode des unendlichen Abstiegs und die Lösungen der Gleichung $x^4 + y^4 = z^4$

Schon Fermat war 1637 in der Lage zu zeigen, dass diese Gleichung keine Lösung besitzt. Er benutzte dabei die *Methode des unendlichen Abstiegs*, die *Descendenzmethode*, die in der Olympiademathematik auch einfach unter dem Namen *Extremalprinzip* bekannt ist. Ein weiterer Name ist — *die Suche nach dem kleinsten Verbrecher*. Diese Prinzip beruht ganz einfach auf der Tatsache, dass jede Teilmenge natürlicher Zahlen ein kleinstes Element besitzt. In folgender Gestalt wird es meist verwendet:

> Wir wollen zeigen, dass eine Aufgabe keine Lösung besitzt. Dazu nehmen wir an, sie hätte eine. Wir wählen uns unter allen hypothetischen Lösungen eine minimale (bezüglich einer geeigneten Ordnung). Wenn es uns dann gelingt, eine kleinere Lösung zu konstruieren, dann sind wir offensichtlich an einem Widerspruch angelangt. Die Aufgabe hat keine Lösung.

Als Beispiel geben wir einen recht ungewöhnlichen Beweis für die Tatsache, dass $\sqrt{2}$ irrational ist, siehe [2, Kapitel 3]. Dazu sei $M = \{n\sqrt{2} \mid n \in \mathbb{N}\} \cap \mathbb{N}$ die Menge der Vielfachen von $\sqrt{2}$, die natürliche Zahlen liefern. Wir müssen zeigen, dass M leer ist. Ist M nichtleer, so gibt es eine *kleinste* natürliche Zahl $k \in M$. Wir betrachten die Zahl $n = (\sqrt{2}-1)k$. Dann gilt

$$n\sqrt{2} = (\sqrt{2}-1)k\sqrt{2} = 2k - k\sqrt{2}.$$

Nach Definition der Menge M und wegen $k \in M$ sind sowohl $(\sqrt{2}-1)k$ als auch $2k - k\sqrt{2}$ natürliche Zahlen. Folglich, wieder nach Definition von M, ist auch $(\sqrt{2}-1)k \in M$. Nun ist aber $(\sqrt{2}-1)k < k$, was der Minimalität von k widerspricht. Also ist M leer und $\sqrt{2}$ irrational.

Satz 2 *Die Gleichung*

$$x^4 + y^4 = z^2 \tag{3}$$

hat keine von Null verschiedene ganzzahlige Lösung.

Beweis:[(nach [8])] Angenommen, es gibt Lösungen der obigen Gleichung. Dann können wir wieder unsere Betrachtungen auf teilerfremde (primitive) Tripel von natürlichen Zahlen beschränken. Unter allen primitiven Tripeln wählen wir dasjenige (x,y,z), wo z am kleinsten (aber von Null verschieden) ist. Wie schon bei der Lösung von (1) schließt man, dass genau eine der Zahlen x und y gerade, die andere ungerade sein muss. O. B. d. A. sei x gerade. Wegen $(x^2)^2 + (y^2)^2 = z^2$ bilden (x^2, y^2, z) ein primitives pythagoräisches Tripel. Also gibt es teilerfremde natürliche Zahlen m, n, $n > m$, verschiedener Parität (gerade/ungerade) mit

$$x^2 = 2mn, \quad y^2 = m^2 - n^2, \quad z = m^2 + n^2.$$

Falls m gerade und n ungerade, dann ist $y^2 \equiv -1 \pmod 4$, was nicht möglich ist. Also ist m ungerade und $n = 2q$ gerade. Also gilt $x^2 = 4qm$ bzw. $(x/2)^2 = qm$. Wegen der Teilerfremdheit von m und n sind auch q und m teilerfremd, also müssen sie bereits beide einzeln Quadratzahlen sein, etwa

$$m = s^2, \quad q = t^2,$$

wobei s und t gewisse teilerfremde positive ganze Zahlen sind. Wir sehen, dass

$$y^2 = (s^2)^2 - (2t^2)^2 \quad \text{bzw.} \quad (2t^2)^2 + y^2 = (s^2)^2$$

gilt. Da t und s teilerfremd sind, können wir erneut Satz 1 anwenden und folglich gibt es teilerfremde natürliche Zahlen a und b verschiedener Parität mit $a > b$ und

$$2t^2 = 2ab, \quad y = a^2 - b^2, \quad s^2 = a^2 + b^2.$$

Da a und b teilerfremd sind, folgt aus der ersten Gleichung wieder $a = u^2$ und $b = v^2$ und somit aus der letzten Gleichung

$$s^2 = u^4 + v^4,$$

wobei u, v und s paarweise teilerfremde natürliche Zahlen sind. Dabei ist

$$z = m^2 + n^2 > m = s^2 > s.$$

Dies widerspricht aber der minimalen Wahl von z. Somit hat Gleichung (3) keine Lösung. □

Mit Hilfe des Extremalprinzips löse man die folgende Aufgaben

Aufgabe 2 Es gibt kein Quadrupel (x, y, z, u) von natürlichen Zahlen mit

$$x^2 + y^2 = 3(z^2 + u^2).$$

Aufgabe 3 Finde alle Paare (x, y) von natürlichen Zahlen mit $2x^2 - 3y^2 = 0$!

Aufgabe 4 Zeige, dass die Gleichung $x^2 + y^2 + z^2 = 2xyz$ keine ganzzahlige Lösung bis auf $x = y = z = 0$ besitzt.

Aufgabe 5 Die Menge $\mathbb{Z} \times \mathbb{Z}$ heißt *ebenes Gitter*. Man zeige, dass es für $n \neq 4$ kein reguläres n-Eck gibt, dessen Ecken auf dem ebenen Gitter liegen!

Lösung: Die Drehung um 90° um einen Punkt aus $\mathbb{Z}/2 \times \mathbb{Z}/2$ überführt das Gitter $\Gamma = \mathbb{Z} \times \mathbb{Z}$ in sich. Es sei $P_0 \cdots P_{n-1}$ ein reguläres n-Eck minimaler Kantenlänge mit $P_i \in \Gamma$. Wir betrachten die n Drehungen um die Mittelpunkte $(P_i + P_{i+1})/2$, $i = 0, \ldots, n-1$ um $+90°$. Das Bild von P_{i+1} bei der zugehörigen Drehung sei P'_{i+1} und liegt echt im Innern von $P_0 \cdots P_{n-1}$. Dann ist das n-Eck $P'_0 \cdots P'_{n-1}$ wieder regulär und liegt auf dem Gitter Γ. Dies ist aber ein Widerspruch zur Minimalität der Seitenlänge. Nur für $n = 4$ fallen die 4 Bildpunkte zusammen und es ergibt sich kein Widerspruch.

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 11.

Satz 3 (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]. $\square$

Bemerkung 1 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]

Aufgabe 6 Die Gleichung $x_1^4 + x_2^4 + \cdots + x_{14}^4 = 1599$ hat keine ganzzahlige Lösung.

Aufgabe 7 Zahlen der Form $8k+6$ sind nicht als Summe von zwei Quadratzahlen darstellbar.

Lösung: Die quadratischen Reste modulo 8 sind 0,1,4. Die Summe zweier solcher Reste ist niemals gleich 6.

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

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

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

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

Ferner gilt $2m = (a-b)^2 + (a+b)^2 + (c-d)^2 + (c+d)^2$.

Beweis: Man erhält die Identitäten unmittelbar durch Ausmultiplizieren (binomische Formel). Natürlich gibt es auch bei (b) mehrere Möglichkeiten, der Darstellung des Produkts. Wie viele eigentlich? $\square$

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

Bevor wir diesen Satz beweisen, müssen wir noch einige Hilfsmittel zur Verfügung stellen.

Satz 6 ((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 der Aussage $p|(x-1)(x+1)$ 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. $\square$

Satz 7 *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

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

□

Dieser Satz zeigt insbesondere, dass für die Primzahlen der Form $4n + 1$ die Kongruenz $x^2 \equiv -1 \pmod p$ stets eine Lösung hat.

Satz 8 ((Thue)) *Es sei p eine Primzahl, e und f zwei ganze Zahlen mit $1 < e, f < p$ und $p < ef$. Dann lassen sich alle Reste r modulo p auf die folgende Gestalt bringen: $r \equiv 0 \pmod p$ oder*

$$r \equiv \pm\frac{x}{y} \pmod p, \quad \textit{wobei} \quad 0 < x < e \quad \textit{und} \quad 0 < y < f.$$

Beweis: Es sei $r \not\equiv 0 \pmod p$. Wir betrachten die ef Reste $v + rw$, wobei $0 \le v < e$ und $0 \le w < f$ 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 5)] Wir richten uns nach [6, Kapitel VII, Abschnitt 3]. Nach Satz 7 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 $\operatorname{ggT}(x, y) = 1$ und $\operatorname{ggT}(u, v) = 1$ folgt hieraus $x = u$ und $y = v$. □

In schönster Allgemeinheit lautet der 2-Quadrate Satz dann

Satz 9 *Ist* $n = 2^e p_1^{f_1} \cdots p_k^{f_k} q_1^{h_1} \cdots q_s^{h_s}$ *mit Primzahlen* $p_1, \ldots, p_k$ *der Form* $4m+1$ *und Primzahlen* $q_1, \ldots, q_s$ *der Form* $4m+3$ *und gilt*

$$2|h_1, \ldots, 2|h_s,$$

so kann man n *als Summe zweier Quadrate — Null ist auch ein Quadrat — darstellen. Gilt für ein* j *unter gleichen Voraussetzungen* $2 \nmid h_j$, *so lässt sich* n *nicht als Summe zweier Quadrate darstellen.*

Potenzreihen

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

Satz 10 ((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 11 ((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 2 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: $4 = (\pm1)^2 + (\pm1)^2 + (\pm1)^2 + (\pm1)^2$ (16 Möglichkeiten) und $4 = (\pm2)^2 + 0^2 + 0^2 + 0^2 = 0^2 + (\pm2)^2 + 0^2 + 0^2 = 0^2 + 0^2 + (\pm2)^2 + 0^2 = 0^2 + 0^2 + 0^2 + (\pm2)^2$ (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 3 Der Satz 11 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 12 (Jacobi-Tripelprodukt-Identität) *Für* $|q| < 1$ *und alle* x *gilt:*

$$\prod_{i=1}^{\infty} (1 + q^i x)(1 + q^{i-1} x^{-1})(1 - q^i) = \sum_{n \in \mathbb{Z}} q^{n(n+1)/2} x^n. \tag{4}$$

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

$$\left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^2 = 1 + 4\sum_{k\geq 1, l\geq 0}(q^{k(4l+1)} - q^{k(4l+3)}) = 1 + 4\sum_{n\geq 1}(\mathrm{d}_{1,4}(n) - \mathrm{d}_{3,4}(n))q^n, \tag{5}$$

$$\left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^4 = 1 + 8\sum_{n\geq 1}\left(\sum_{d|n,\, 4\nmid d} d\right) q^n. \tag{6}$$

Schauen wir uns die linke Seite von (5) 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

Attribution Section

schueler (2004-09-09): Contributed to KoSemNet
graebe (2004-09-09): Prepared along the KoSemNet rules