Elem. Math. 71 (2016) 100 – 108
0013-6018/16/030100-9
DOI 10.4171/EM/305

Elemente der Mathematik

Spezielle, orthogonale Gitterbasen im $\mathbb{R}^3$

Peter Thurnheer

Peter Thurnheer (1946) doktorierte 1979 an der ETH Zürich bei Professor K. Chandrasekharan auf dem Gebiet der Zahlentheorie und seither hat ihn die Faszination für die "Königin der Mathematik" nicht mehr losgelassen. Er arbeitete in verschiedenen Funktionen an Gymnasien, Fachhochschulen und Universitäten und an ganz unterschiedlichen Orten, von Zürich, Bülach, über Trogen, Paris bis Port-au-Prince. Vor allem aber hielt er an der ETH Zürich während vieler Jahre Vorlesungen, hauptsächlich über Calculus, aber auch über Darstellende Geometrie, Kombinatorik und Klassische Zahlentheorie.

1 Einleitung

In dieser Arbeit geht es um ein Problem, das wir im folgenden das Gitterbasenproblem nennen.

Gitterbasenproblem. *Gegeben sei die natürliche Zahl $L > 1$. Gesucht werden 3 paarweise orthogonale Vektoren $\underline{A}, \underline{B}, \underline{C}$ aus $\mathbb{Z}^3$ mit der Eigenschaft $|\underline{A}| = |\underline{B}| = |\underline{C}| = L$, und höchstens einer der Vektoren ist parallel zu einer Koordinatenachse.*

Ein geometrisches Problem, das – doch etwas überraschend – mit rein zahlentheoretischen Überlegungen gelöst werden kann: Finde im $\mathbb{R}^3$ zu einer gegebenen natürlichen Zahl L drei paarweise senkrechte Gittervektoren der Länge L, von denen mindestens einer nicht parallel zu einer Koordinatenachse ist. Es wird gezeigt unter welchen Bedingungen und wie solche Gitterbasen gefunden werden können. Eine wichtige Rolle in diesem Zusammenhang spielen natürlich die Darstellungen von L^2 als Summe von 2 oder 3 Quadraten. Es stellt sich heraus, dass es, um *alle* diese Darstellungen zu finden, genügt, die *viel kleineren* ungeraden Teiler von L zu studieren. Die dabei zur Anwendung kommenden Aussagen erinnern, wenig überraschend, an den bekannten Dreiquadratesatz. Schon erstaunlicher ist, dass sie mit elementaren Argumenten hergeleitet werden können, ganz im Gegensatz zum erwähnten, sehr tiefen Theorem von Gauss–Legendre.

Wir unterscheiden zwei Arten von Lösungen:

1. *Art: Genau ein Lösungsvektor ist parallel zu einer Koordinatenachse.*
2. *Art: Kein Lösungsvektor ist parallel zu einer Koordinatenachse.*

Bemerkungen

(i) In den Arbeiten [3], [4] wird eine ähnliche Frage studiert. In [4, Satz 1] wird zwar zu Beginn auch eine elegante Bedingung angegeben, welche die Konstruktion von orthogonalen Gitterbasen im $\mathbb{R}^3$, bestehend aus Vektoren gleicher, ganzzahliger Länge erlaubt. Bei weitem nicht alle solchen Basen erfüllen aber die Bedingung und beide Arbeiten [3], [4] verfolgen schliesslich ein ganz anderes Ziel als der vorliegende Text, nämlich die Bestimmung *aller* orthogonalen Gitterbasen des $\mathbb{R}^n$ (in [3]) respektive des $\mathbb{R}^3$ (in [4]), deren Vektoren ganzzahlige, aber überhaupt nicht notwendigerweise gleiche, vorgegebene Länge haben. Das an sich geometrische Gitterbasenproblem kann mit rein zahlentheoretischen Überlegungen gelöst werden. Dies ermöglicht es zum Beispiel, anders als in [3], [4], auch Existenzfragen zu beantworten.

(ii) *Wichtig*: Immer wenn wir im folgenden von Quadraten sprechen meinen wir, *anders als in der Zahlentheorie üblich*, Quadrate natürlicher Zahlen, die also nicht 0 sind.

(iii) Vielmals danken möchte ich dem Gutachter für seine ausführlichen und hilfreichen Hinweise zur Verbesserung dieses Textes, sowie Andreas Umbach, Mathematiklehrer an der Kantonsschule Pfäffikon, für die Anregung zur Beschäftigung mit diesen Fragen.

2 Hauptergebnisse

Satz 1.

(a) *Sei $K \in \mathbb{N}$. Falls gilt*

$$K = a^2 + b^2 + u^2 + v^2, \qquad a, b, u, v \text{ aus } \mathbb{Z}, \tag{1}$$

so ist

$$K^2 = \big(a^2 + u^2 - b^2 - v^2\big)^2 + \big(2(ab + uv)\big)^2 + \big(2(av - bu)\big)^2, \tag{2}$$

und die folgenden Vektoren $\underline{A}, \underline{B}, \underline{C}$ haben Länge K und sind paarweise orthogonal.

$$\begin{aligned}
\underline{A} &= \big\langle a^2 + u^2 - b^2 - v^2 \;/\; 2(ab + uv) \;/\; 2(av - bu) \big\rangle, \\
\underline{B} &= \big\langle 2(ab - uv) \;/\; -a^2 - v^2 + b^2 + u^2 \;/\; 2(au + bv) \big\rangle, \\
\underline{C} &= \big\langle 2(av + bu) \;/\; -2(au - bv) \;/\; -a^2 - b^2 + u^2 + v^2 \big\rangle.
\end{aligned}$$

(b) *Ist K ungerade, so liefern die obigen Vektoren $\underline{A}, \underline{B}, \underline{C}$ eine Lösung des Gitterbasenproblems zur Länge $L = K$*

1. *Art, falls genau zwei der Parameter* a, b, u, v *gleich* 0 *sind, das heisst, falls* K *in* (1) *Summe von* 2 *Quadraten ist.*
2. *Art, falls höchstens einer der Parameter* a, b, u, v *gleich* 0 *ist, das heisst, falls* K *in* (1) *Summe von* 3 *oder* 4 *Quadraten ist.*

Satz 2. *Sei* $K \in \mathbb{N}$*,* K *ungerade. Zu jeder Darstellung von* K^2 *als Summe von* 2 *respektive* 3 *Quadraten*

$$K^2 = r^2 + s^2 + t^2, \qquad r, s \text{ aus } \mathbb{N},\ t \in \mathbb{N}_0, \quad \text{mit } \mathrm{ggT}(K, r, s, t) = 1, \tag{3}$$

existiert eine Darstellung von K *als Summe von* 2 *respektive* 3 *oder* 4 *Quadraten der Form* (1) *so, dass die entsprechende Formel* (2) *in Satz* 1 *die Darstellung* (3) *und Satz* 1 *damit eine Lösung* $\underline{A}, \underline{B}, \underline{C}$ *des Gitterbasenproblems zur Länge* $L = K$ *liefert, wobei für eine bestimmte Wahl der Vorzeichen gilt* $\underline{A} = \langle \pm r / \pm s / \pm t \rangle$.

Satz 3. *Sei* $L \in \mathbb{N}$*,* $L > 1$*. Das Gitterbasenproblem hat zur Länge* L dann und nur dann

- *Lösungen, wenn gilt* $L \neq 2^k$ *,* $k \in \mathbb{N}$*,*
- *Lösungen 1. Art, wenn* L *einen Primfaktor* p *der Form* $p = 4m + 1$*,* $m \in \mathbb{N}$*, enthält,*
- *Lösungen 2. Art, wenn gilt* $L \neq 2^k$ *und* $L \neq 5 \cdot 2^k$*,* $k \in \mathbb{N}_0$*.*

Bemerkungen

(iv) Im Folgenden nennen wir eine Lösung des Gitterbasenproblems zur Länge $L = K$ kurz eine *K-Lösung* und eine Darstellung der Form (3), welche die Bedingung an den ggT erfüllt, eine *primitive Darstellung*.

(v) Für ungerades K ist nach dem Satz von Jacobi ([5, Prop. 1, S. 621], [2, S. 166]) die Anzahl der Darstellungen von K als Summe von höchstens 4 Quadraten ganzer Zahlen, das heisst der Form (1), gleich $8\sigma(K)$, wobei $\sigma(K)$ die Summe aller positiven Teiler von K bezeichnet. Genauer gesagt gilt:

Für ungerades K *gibt es* $8\sigma(K)$ *verschiedene, geordnete Quadrupel* a, b, u, v *ganzer Zahlen, welche* (1) *erfüllen.*

Offensichtlich ergeben alle diese, eingesetzt in Satz 1, Quadratsummen-Darstellungen von K^2 respektive K-Lösungen, die allerdings natürlich nicht alle verschieden sind. Die Anzahl der verschiedenen Darstellungen und K-Lösungen, die man erhält, hängt unter anderem davon ab, wieviele der Parameter a, b, u, v voneinander und von 0 verschieden sind in den Fällen wo alle 4 nicht negativ sind.

(vi) Mit folgender Überlegung lassen sich aus einer K-Lösung weitere solche konstruieren: Man denkt sich die Lösungsvektoren als Spaltenvektoren einer 3×3-Matrix. Multipliziert man eine Zeile oder Spalte dieser Matrix mit -1 oder vertauscht 2 ihrer Zeilen, so ändern diese Operationen die Länge der Spaltenvektoren und den Betrag der Determinante nicht, so dass auch die Spaltenvektoren der neuen Matrix eine K-Lösung bilden.

Die hier beschriebenen Operationen auf einer Lösung nennen wir unten kurz *Zeilenumformungen*.

Korollar 1. *Sei $L \in \mathbb{N}$, $L \neq 2^k$, $k \in \mathbb{N}_0$. Mit Satz* 1 *lassen sich* alle *Darstellungen von L^2 als Summe von* 2 *respektive* 3 *Quadraten aus den Darstellungen der* – viel kleineren – *Zahl L, respektive ihrer ungeraden Teiler, als Summe von* 2 *respektive* 3 *oder* 4 *Quadraten gewinnen. Man findet damit natürlich auch alle Gittervektoren der Länge L.*

Korollar 2. *Sei $L \in \mathbb{N}$, $L \neq 2^k$, $k \in \mathbb{N}_0$. Zu jedem Gittervektor $\underline{A}$ der Länge L und nicht parallel zu einer Koordinatenachse, existieren Vektoren $\underline{B}, \underline{C}$ so, dass $\underline{A}, \underline{B}, \underline{C}$ eine L-Lösung bilden.*

Brauchen werden wir das folgende Lemma, welches zeigt, dass es genügt, das Gitterbasenproblem für ungerade Längen L zu studieren.

Lemma 1. *Seien K und k aus $\mathbb{N}$. Sind $\underline{A}_j, \underline{B}_j, \underline{C}_j$, $j = 1, 2, \ldots, m$, alle K-Lösungen, so sind $2^k\underline{A}_j, 2^k\underline{B}_j, 2^k\underline{C}_j$, $j = 1, 2, \ldots, m$, die einzigen 2^k K-Lösungen.*

3 Sätze aus der Zahlentheorie, Lemmas

Satz A (Euler, [1, S. 29 und 30])**.** *Eine ungerade Primzahl p ist genau dann Summe von* 2 *Quadraten, wenn p von der Form $p = 4m + 1$, $m \in \mathbb{N}$, ist.*

Satz B (Vierquadratesatz; Lagrange, 1770, [1, S. 31])**.** *Jede natürliche Zahl ist Summe von höchstens* 4 *Quadraten.*

Satz C (Dreiquadratesatz; Legendre, Gauss, [5, Prop. 41, S. 372], [2, S. 161])**.** *Eine natürliche Zahl n ist Summe von höchstens drei Quadraten dann und nur dann, wenn gilt $n = 4^k m$ mit $k \in \mathbb{N}_0$, $4 \nmid m$ und $m \not\equiv 7 \pmod 8$.*

Satz D (siehe Bemerkung (viii))**.** *Eine natürliche Zahl grösser* 1*, welche eine Summe von Quadraten von* 2 *natürlichen, teilerfremden Zahlen teilt, ist selbst Summe zweier Quadrate von teilerfremden natürlichen Zahlen.*

Satz E ([2, S. 168 und 169])**.** *Zu einem pythagoreischen Tripel $K^2 = r^2 + s^2$, mit $\mathrm{ggT}(K, r, s) = 1$, r gerade, existieren eindeutig definierte Zahlen a, b aus $\mathbb{N}$ mit $K = a^2 + b^2$, $r = 2ab$, $s = a^2 - b^2$.*

Bemerkungen

(vii) Den Dreiquadratesatz haben wir an dieser Stelle nur der Vollständigkeit halber angeführt, werden ihn aber für die Beweise nicht brauchen. Das mag erstaunen, scheint er doch auf den ersten Blick für unsere Zwecke speziell geeignet. Dass dem nicht so ist liegt daran, dass er Aussagen macht über Darstellungen *beliebiger natürlicher Zahlen* durch *höchstens* 3 Quadrate, während es beim Gitterbasenproblem um Darstellungen von *Quadratzahlen* durch *genau* 2 respektive *genau* 3 Quadrate geht. Der Dreiquadratesatz ist wesentlich tiefer als der Vierquadratesatz und sein Beweis ([5, S. 372 und 373]) beruht auf äusserst starken Hilfsmitteln aus der Theorie der quadratischen Formen, im Gegensatz zu den entsprechenden Aussagen in diesem Text, die mit elementaren Überlegungen hergeleitet werden können.

(viii) Die Aussage in Satz D folgt zum Beispiel aus der Argumentation in [1, S. 20 und 21]: Beim Beweis des Korollars ([1, S. 21]) wird gezeigt, dass es, falls eine natürliche Zahl n Teiler von $A^2 + B^2$, A, B aus $\mathbb{N}$, $\mathrm{ggT}(A, B) = 1$ ist, ein $Z \in \mathbb{N}$ so gibt, dass n auch $Z^2 + 1$ teilt. Nach Satz 5 ([1, S. 20]) und der dazugehörigen Bemerkung ([1, S. 21 oben]) ist somit n darstellbar in der Form $n = s^2+t^2$, s, t aus $\mathbb{N}$, $\mathrm{ggT}(s, t) = 1$. Ist also $n > 1$, so sind s und t nicht 0.

Zum Beweis von Satz 3 brauchen wir die folgenden beiden Lemmas.

Lemma 2. *Die einzigen Primzahlen, die sich nicht als Summe von* 3 *oder* 4 *Quadraten schreiben lassen, sind* 2 *und* 5.

Lemma 3. *Ein Produkt $p_1 \cdot p_2 \cdots p_k$ von Primzahlen p_j, die alle von der Form $p_j = 4m_j + 3$, $m_j \in \mathbb{N}_0$, $j = 1, 2, \ldots, k$ sind, kann nicht als Summe von* 2 (*nicht verschwindenden!*) *Quadraten geschrieben werden.*

4 Beweise

Beweis Satz 1 (a). Sei $K \in \mathbb{N}$ und

$$K = a^2 + b^2 + u^2 + v^2, \qquad a, b, u, v \text{ aus } \mathbb{Z}. \tag{1}$$

Mit $w = b^2 + v^2$ ist $K - w = a^2 + u^2$ und

$$K^2 - (K - 2w)^2 = 4(K - w)w = 4\big(a^2+u^2\big)\big(b^2+v^2\big) = \big(2(ab+uv)\big)^2 + \big(2(av-bu)\big)^2.$$

Mit $K - 2w = a^2 + u^2 - b^2 - v^2$ erhält man

$$K^2 = \big(a^2 + u^2 - b^2 - v^2\big)^2 + \big(2(ab + uv)\big)^2 + \big(2(av - bu)\big)^2.$$

Folgerung:
Ist K wie in (1), so hat der Vektor

$$\underline{A} = \underline{A}(a, b, u, v) = \big\langle \pm(a^2 + u^2 - b^2 - v^2) \;/\; \pm 2(ab + uv) \;/\; \pm 2(av - bu) \big\rangle$$

die Länge K für irgendeine Wahl der Vorzeichen. Da die rechte Seite in (1) unabhängig ist von der Reihenfolge der Summanden, erhält man, wenn man in $\underline{A}$ die Argumente a, b, u, v permutiert, wieder einen Vektor der Länge K. Solche Vektoren sind

$$\underline{B}^\star = \big\langle \pm(a^2 + v^2 - b^2 - u^2) \;/\; \pm 2(au + bv) \;/\; \pm 2(ab - uv) \big\rangle \qquad (abuv \longrightarrow auvb),$$
$$\underline{C}^\star = \big\langle \pm(a^2 + b^2 - u^2 - v^2) \;/\; \pm 2(av + bu) \;/\; \pm 2(au - bv) \big\rangle \qquad (abuv \longrightarrow avbu).$$

Durch Vertauschen der Komponenten dieser Vektoren erhält man die Vektoren $\underline{A}, \underline{B}, \underline{C}$ des Satzes. Diese sind paarweise orthogonal, da gilt $\underline{A} \cdot \underline{B} = \underline{A} \cdot \underline{C} = \underline{B} \cdot \underline{C} = 0$. □

Beweis Satz 1 (b). Die Behauptungen folgen aus der Voraussetzung, dass K ungerade ist. Sind *genau* 2 der Parameter a, b, u, v nicht 0, so sind diese damit verschieden und in 2 der Vektoren $\underline{A}, \underline{B}, \underline{C}$ sind 2 Komponenten nicht 0, während im dritten 2 Komponenten verschwinden.

Sind 3 der Parameter a, b, u, v nicht 0, so gilt, wieder weil K ungerade vorausgesetzt ist, $a^2 + b^2 \neq u^2 + v^2$, $a^2 + u^2 \neq b^2 + v^2$, $a^2 + v^2 \neq b^2 + u^2$, sodass in allen Vektoren $\underline{A}, \underline{B}, \underline{C}$ mindestens 2 Komponenten nicht 0 sind. □

Beweis Satz 2. Ist $t = 0$, so folgt die Behauptung aus Satz E.

Sei also $t \in \mathbb{N}$. Wären alle 3 Zahlen r, s, t ungerade, so wäre K^2 kongruent 3 modulo 4, was der Tatsache widerspricht, dass ein Quadrat nur die Werte 0, 1 annimmt modulo 4. Also sind o.B.d.A. die Zahlen s, t gerade und r ist ungerade. Damit enthält der $\mathrm{ggT}(s, t)$ einen Faktor 2 und r kann in folgender Form geschrieben werden

$$r = K - 2w, \quad \mathrm{ggT}(s, t) = 2z, \qquad z, w \text{ aus } \mathbb{N}.$$

Ist $d = \mathrm{ggT}(K - 2w, w) = \mathrm{ggT}(r, w)$, so ist wegen $\mathrm{ggT}(K, r, s, t) = 1$ auch $\mathrm{ggT}(z, d) = 1$ und mit teilerfremden natürlichen Zahlen m, n respektive x, y gilt

$$w = dm, \quad K - w = dn \tag{4}$$

und

$$K^2 - r^2 = K^2 - (K - 2w)^2 = 4(K - w)w = 4d^2mn = s^2 + t^2 = 4z^2(x^2 + y^2) \tag{5}$$

oder

$$d^2mn = z^2(x^2 + y^2), \quad \mathrm{ggT}(m, n) = \mathrm{ggT}(x, y) = \mathrm{ggT}(d, z) = 1.$$

Wegen $\mathrm{ggT}(m, n) = 1$ und $\mathrm{ggT}(d, z) = 1$ gibt es teilerfremde natürliche Zahlen μ, ν und m_1, n_1 mit

$$\mu^2\nu^2 = z^2, \quad m = \mu^2 m_1, \quad n = \nu^2 n_1, \tag{6}$$

und damit ist

$$dm_1 \cdot dn_1 = x^2 + y^2, \quad \mathrm{ggT}(x, y) = 1.$$

Die Zahlen dm_1 und dn_1 können nicht beide gleich 1 sein. Nach Satz D ist somit mindestens eine von ihnen Summe von 2 Quadraten. Also gibt es ganze Zahlen a, b, u, v, von denen mindestens 3 nicht 0 sind, so, dass mit (4) und (6) gilt

$$w = \mu^2 dm_1 = b^2 + v^2, \quad K - w = \nu^2 dn_1 = a^2 + u^2.$$

Damit erhält man

$$K = a^2 + b^2 + u^2 + v^2,$$

also eine Darstellung von K der Form (1), und wenn man noch (5) beachtet

$$r = K - 2w = a^2 + u^2 - b^2 - v^2; \quad s^2 + t^2 = 4(K - w)w = 4\big(a^2 + u^2\big)\big(b^2 + v^2\big),$$

sodass die entsprechende Formel (2)

$$\begin{aligned} K^2 &= \big(a^2 + u^2 - b^2 - v^2\big)^2 + \big(2(ab + uv)\big)^2 + \big(2(av - bu)\big)^2 \\ &= r^2 + 4\big(a^2 + u^2\big)\big(b^2 + v^2\big) = r^2 + s^2 + t^2 \end{aligned}$$

wie behauptet die Darstellung (3) liefert. □

Beweis Lemma 1. Es genügt, die Aussage für $k = 1$ zu beweisen. Sie folgt dann daraus, dass es keine anderen Darstellungen von $(2L)^2$ als Summe von 2 oder 3 Quadraten gibt als „die Doppelten" der Darstellungen von L^2, das heisst zu jeder Darstellung

$$(2L)^2 = 4L^2 = r^2 + s^2 + t^2, \qquad r, s \text{ aus } \mathbb{N}, t \in \mathbb{N}_0, \tag{7}$$

existiert eine Darstellung

$$L^2 = x^2 + y^2 + z^2, \qquad x, y \text{ aus } \mathbb{N}, z \in \mathbb{N}_0, \quad \text{wobei } r = 2x, s = 2y, t = 2z.$$

Dies folgt unmittelbar aus der Tatsache, dass die rechte Seite der letzten Gleichung in (7) nur genau dann kongruent 0 modulo 4 ist, wie die linke, wenn alle 3 Zahlen r, s, t gerade sind. □

Beweis Korollar 1. Um alle gesuchten Darstellungen von L^2 zu finden genügt es nach Lemma 1 offensichtlich, für alle ungeraden Teiler K von L die entsprechenden primitiven Darstellungen von K^2 zu bestimmen. Nach Satz 2 erhält man diese, indem man alle Darstellungen der Form (1) von K in Satz 1 einsetzt. (In der Praxis braucht man dabei gemäss Bem. (v) bei weitem nicht alle $8\sigma(K)$ derselben zu berücksichtigen.) □

Beweis Korollar 2. Sei $\underline{A} = M\,\langle x/y/z\rangle$, $M \in \mathbb{N}$, ein Vektor der Länge L und mindestens 2 der 3 ganzen Zahlen x, y, z nicht 0, sowie

$$x^2 + y^2 + z^2 = K^2 \quad \text{und} \quad \mathrm{ggT}\big(K, |x|, |y|, |z|\big) = 1.$$

Also ist nach Lemma 1 K ungerade und $L = KM$. Nach Satz 2 existiert eine Darstellung der Form (1) von K, welche, eingesetzt in Satz 1, eine K-Lösung $\underline{A}_1 = \langle \pm x/ \pm y/ \pm z\rangle$, $\underline{B}_1$, $\underline{C}_1$ liefert. Durch Zeilenumformungen (s. Bem. (vi)) erhält man aus dieser eine K-Lösung $\underline{A}^\star = \langle x/y/z\rangle$, $\underline{B}^\star$, $\underline{C}^\star$, so dass $\underline{B} = M\underline{B}^\star$, $\underline{C} = M\underline{C}^\star$ die gesuchten Vektoren sind. □

Beweis Lemma 2. Dass 2 und 5 die fragliche Eigenschaft haben ist klar.

Es bleibt zu zeigen, dass alle übrigen Primzahlen p, $p \neq 2$, $p \neq 5$, als Summe von 3 oder 4 Quadraten geschrieben werden können.

1. $p = 4m + 3, m \in \mathbb{N}_0$.
   Nach Satz A und Satz B kann p in diesem Fall in der gewünschten Form dargestellt werden.
2. $p = 4m + 1, m \in \mathbb{N}$.
   Nach Satz A kann p geschrieben werden in der Form $p = r^2 + s^2$, r, s aus $\mathbb{N}$.
   2.1. Einer der Summanden enthält einen Primfaktor $q \geq 3$. Dieser ist keine Quadratzahl, lässt sich somit nach Satz B als Summe von 2, 3 oder 4 Quadraten schreiben. Aus Satz 1 folgt, dass damit q^2 Summe von 2 oder 3 Quadraten ist, was eine Darstellung der gewünschten Art ergibt.

Zu untersuchen bleiben Primzahlen p der Form

2.2. $p = 2^{2k} + 1, k \in \mathbb{N}$.

2.2.1. $p = 2^{2k} + 1, k = 2n$ gerade, $n \in \mathbb{N}$.
Dann erhält man mit $p = 2^{4n} + 1 = \left(2^{2n} - 1\right)^2 + 2 \cdot 2^{2n} = \left(2^{2n} - 1\right)^2 + \left(2^n\right)^2 + \left(2^n\right)^2$ das Gewünschte.

2.2.2. $p = 2^{2k} + 1, k = 2n + 1$ ungerade, $n \in \mathbb{N}_0$.
Nun ist $p = 2^{4n+2}+1$. Eine einfache Induktion zeigt, dass 5 die Einerziffer aller natürlichen Zahlen dieser Form ist. Die einzige Primzahl dieser Form ist somit 5. □

Beweis Lemma 3. Wir machen die indirekte *Annahme*

$$p_1 \cdot p_2 \cdots p_k = a^2 + b^2, \ a, b \text{ aus } \mathbb{N}.$$

Dann gibt es eine natürliche Zahl z und teilerfremde natürliche Zahlen x, y so, dass gilt $p_1 \cdot p_2 \cdots p_k = z^2\left(x^2 + y^2\right)$. Da $x^2 + y^2 > 1$ ist, kann z^2 nicht alle auf der linken Seite auftretenden Primfaktoren enthalten. Somit gibt es mindestens eine Primzahl $p_j = 4m_j + 3$, $m_j \in \mathbb{N}_0$, welche die Summe $x^2 + y^2$ mit ggT$(x, y) = 1$ teilt. Nach Satz D ist p_j Summe von 2 Quadraten, was nach Satz A einen Widerspruch darstellt, der Lemma 3 beweist. □

Beweis Satz 3.

a) Notwendige Bedingungen.

a1) *Es gibt keine 2^k-Lösungen, $k \in \mathbb{N}$.*

a2) *Es gibt keine $5 \cdot 2^k$-Lösungen 2. Art, $k \in \mathbb{N}_0$.*
Aufgrund von Lemma 1 gäbe es andernfalls insbesondere eine 2-Lösung, respektive eine 5-Lösung 2. Art, das heisst insbesondere, eine Darstellung von 4 als Summe von 2 oder 3, respektive von 25 als Summe von 3 Quadraten. Solche Darstellungen existieren aber nicht.

a3) *Ist $L = p_1 \cdot p_2 \cdots p_k$ ein Produkt von lauter Primzahlen p_j der Form $p_j = 4m_j + 3$, $m_j \in \mathbb{N}_0$, $j = 1, 2, \ldots, k$, so gibt es keine L-Lösungen 1. Art.*
Eine notwendige Bedingung für die Existenz einer L-Lösung 1. Art ist die Darstellbarkeit von L^2 als Summe von 2 Quadraten. Enthält L nur Primfaktoren p der Form $p = 4m + 3$, $m \in \mathbb{N}_0$, so auch L^2 und nach Lemma 3 kann die Bedingung nicht erfüllt werden.

b) Hinreichende Bedingungen. Natürlich bilden mit einer M-Lösung $\underline{A}$, $\underline{B}$, $\underline{C}$ die Vektoren $K\underline{A}$, $K\underline{B}$, $K\underline{C}$, $K \in \mathbb{N}$, eine MK-Lösung und umgekehrt. Um die Existenz einer L-Lösung zu garantieren, genügt es somit, für irgendeinen Faktor K von L die Existenz einer entsprechenden K-Lösung nachzuweisen.

b1) *Enthält L einen Primfaktor p der Form $p = 4m + 1$, $m \in \mathbb{N}$, so gibt es L-Lösungen 1. Art.*
Nach Satz A ist die Primzahl $p = 4m + 1, m \in \mathbb{N}$, als Summe von 2 Quadraten darstellbar. Aus Satz 1 folgt die Behauptung.

b2) *Enthält L einen Faktor* 25*, so gibt es L-Lösungen 2. Art.*
Da gilt $25 = 4^2 + 2^2 + 2^2 + 1^2$ erhält man aus Satz 1 mit $a = 4$, $b = 2$, $u = 2$, $v = 1$ die 25-Lösung 2. Art $\underline{A} = \langle 15/20/0\rangle$, $\underline{B} = \langle 12/-9/20\rangle$, $\underline{C} = \langle 16/-12/-15\rangle$.

b3) *Enthält L irgendeinen Primfaktor p verschieden von* 2 *und* 5*, so gibt es L-Lösungen 2. Art.*
Die Behauptung folgt unmittelbar aus Lemma 2 und Satz 1.

Die obigen 6 Aussagen zusammengefasst ergeben Satz 3. □

Literatur

[1] Komaravolu Chandrasekharan. *Introduction to analytic number theory*. Die Grundlehren der mathematischen Wissenschaften, Band 148. Springer-Verlag New York Inc., New York, 1968.

[2] Peter Bundschuh. *Einführung in die Zahlentheorie*. Springer-Lehrbuch. Springer-Verlag, Berlin, second edition, 1992.

[3] Hans Liebeck and Anthony Osborne. The generation of all rational orthogonal matrices. *Amer. Math. Monthly*, 98(2):131–133, 1991.

[4] Anthony Osborne and Hans Liebeck. Orthogonal bases of $\mathbf{R}^3$ with integer coordinates and integer lengths. *Amer. Math. Monthly*, 96(1):49–53, 1989.

[5] William A. Coppel. *Number theory: an introduction to mathematics. Part B*. Phalanger Press, Griffith, 2002.

Peter Thurnheer
ETHZ HG J54
Rämistrasse 101
CH-8092 Zürich
e-mail: tpeter@math.ethz.ch