Werk

Titel: Variationen über ein diophantisches Thema.

Autor: Becker, E.; Robson, R.; Schrage, G.

Jahr: 1995

PURL: https://resolver.sub.uni-goettingen.de/purl?378850199_0050|log11

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

El. Math. *50* (1995)

0013-6018/95/020045-20$1.50 + 0.20/0
© 1995 Birkhäuser Verlag, Basel

Variationen über ein diophantisches Thema

Eberhard Becker, Robert Robson[1], Georg Schrage

Eberhard Becker, geboren 1943, studierte Mathematik und Physik an der Universität Hamburg. Nach der Assistentenzeit in Köln wurde er 1979 auf den Lehrstuhl für Algebra an der Universität Dortmund berufen. Seine mathematischen Arbeitsgebiete sind Algebra, Computeralgebra, Zahlentheorie und reelle algebraische Geometrie.

Robert Robson, geboren 1954, studierte am Hampshire College und an der Stanford University, wo er 1981 mit einer Arbeit aus dem Bereich der algebraischen Geometrie promovierte. Von 1982 bis 1984 arbeitete er als Assistent an der Universität Regensburg, seither als Associate Professor an der Oregon State University. Forschungsprojekte führten ihn an die Universitäten in Dortmund, Rennes und Berkeley. Er ist Mitglied der Gruppe "Factoregon", die sich mit der Faktorisierung großer Zahlen beschäftigt, spielt in seiner Freizeit Guitarre, jongliert und nimmt erfolgreich an Bridge-Turnieren teil.

Georg Schrage, geboren 1940, studierte Mathematik, Physik und Wirtschaftswissenschaften an den Universitäten in Köln, Saarbrücken, Madrid und Bonn. Nach Assistentenzeit und Promotion an der Universität Bonn arbeitete er an den Hochschulen in Siegen, Dortmund und Frankfurt. Hinzu kamen zwei Forschungsaufenthalte in den USA. Seit 1980 ist er am Institut für Didaktik der Mathematik der Universität Dortmund tätig. Sei besonderes Interesse gilt der Arbeit mit mathematisch interessierten Schülern und der Rolle neuer Technologien im Mathematikunterricht.

Man bestimme alle rechtwinkligen Dreiecke mit ganzzahligen Seitenlängen, so dass die Katheten sich in ihrer Länge um 1 *unterscheiden.* Diese Aufgabe, die zu Beginn des vorliegenden Beitrages gestellt wird, führt offensichtlich auf die Frage nach den ganzzahligen Lösungen einer einfachen Gleichung zweiten Grades. In dieser Form handelt es sich um eine klassische Fragestellung der Zahlentheorie. Ausgehend von der genannten und einigen weiteren ähnlichen Aufgaben behandeln die Autoren die Zahlentheorie der zugehörigen Klasse diophantischer Gleichungen. Beginnend mit ganz einfachen Problemen führt der Beitrag schliesslich zu Fragen, die bis heute noch nicht gelöst sind. Die Darstellung macht Gebrauch von einigen wohlbekannten Methoden und Sätzen der Zahlentheorie. An mehreren Stellen übernimmt der Computer die Rolle eines Forschungswerkzeuges: Er erlaubt es, bestehende Vermutungen zu testen und neue Vermutungen aus dem Zahlenmaterial abzuleiten. *ust*

1) Der zweite Autor dankt der Alexander von Humboldt-Stiftung für die großzügige Unterstützung eines Forschungsaufenthaltes an der Universität Dortmund.

1 Einleitung

Die folgende Aufgabe kann man in verschiedenen Büchern zur Wahrscheinlichkeitsrechnung finden, z.B. [1], S. 26 oder [3], Problem 1.

Aufgabe 1: *Eine Urne enthält s Kugeln, darunter r rote. Die Wahrscheinlichkeit dafür, daß zwei Kugeln, die ohne Zurücklegen gezogen werden, beide rot sind, ist* $1/2$. *Wie viele Kugeln enthält die Urne, und wie viele davon sind rot?*

Da es $\binom{s}{2}$ Stichproben der Ordnung zwei gibt, von denen $\binom{r}{2}$ aus zwei roten Kugeln bestehen, stellt sich die Aufgabe, natürliche Zahlen r und s zu finden, so daß gilt $s(s-1) = 2r(r-1)$.

Mit $n = s - 1$ und $k = r - 1$ wird hieraus

$$n(n+1) = 2k(k+1). \tag{1}$$

Diese Gleichung kann wie folgt interpretiert werden:

Aufgabe 2: *Bestimme natürliche Zahlen n und k, so daß die Summe der Zahlen* 1 *bis n doppelt so groß ist wie die Summe der Zahlen* 1 *bis k.* (Problem 502 in: The College Mathematics Journal No. 3, 1993.)

Durch Multiplikation mit 2 und Addition von 1 wird aus (1) die äquivalente Gleichung

$$n^2 + (n+1)^2 = (2k+1)^2.$$

Diese Darstellung gibt Anlaß zu dem pythagoräischen Problem

Aufgabe 3: *Bestimme alle rechtwinkligen Dreiecke mit ganzzahligen Seitenlängen, so daß die Katheten sich in ihrer Länge um* 1 *unterscheiden.*

Wir haben somit drei sehr unterschiedliche Fragestellungen, die aber alle auf die Lösung der diophantischen Gleichung (1) im Bereich der natürlichen Zahlen hinauslaufen.

Durch Probieren findet man schnell die Lösung $n = 3$ und $k = 2$. Gibt es weitere Lösungen, und wie findet man diese?

Es ist naheliegend, das Problem zu verallgemeinern, indem man nach natürlichen Zahlen n und k fragt, welche bei gegebenem $d \in \mathbb{N}$ die Gleichung

$$n(n+1) = d \cdot k(k+1) \tag{2}$$

lösen.

Diese Problemstellung steht in Beziehung zu einer Vielzahl anderer reizvoller und wichtiger Fragen. So führt sie unter anderem zur Beschäftigung mit quadratischen Zahlkörpern, genauer: zur Beschäftigung mit der Pellschen Gleichung, mit Kettenbrüchen und Rekursionen, ohne daß die dazu benötigten Hilfsmittel den Rahmen einer elementaren Einführung in die Zahlentheorie übersteigen würden.

Ist d keine Quadratzahl, so hat die Gleichung (2) unendlich viele Lösungen, und wir werden angeben, wie man alle Lösungen erhalten kann.

Für Quadratzahlen d ergibt sich ein völlig anderes Bild. Im Falle der Lösbarkeit hat (2) nur endlich viele Lösungen, aber nicht jede Quadratzahl d führt zu einer lösbaren Gleichung. Wir werden ein Verfahren angeben, diejenigen Quadratzahlen d zu bestimmen,

für die (2) mindestens eine Lösung hat. Überraschend stellt sich ein enger Zusammenhang mit den aus der Numerik und Approximationstheorie bekannten Tschebyscheff-Polynomen heraus. Weiter werden auch unendlich viele Quadratzahlen ermittelt, für welche die Gleichung zwei Lösungen besitzt. Offen bleibt dagegen, ob es Quadratzahlen gibt, für welche die Gleichung mehr als zwei Lösungen hat.

Bei Fragestellungen dieser Art ist das mathematische Experiment ein wichtiges heuristisches Hilfsmittel. Die vorliegende Untersuchung läßt Möglichkeiten, aber auch Grenzen des Computereinsatzes bei der Lösung mathematischer Probleme erkennen.

2 Erste Ergebnisse

d	Lösungspaare (oben: n, unten: k)				
2	3	20	119	696	4059
	2	14	84	492	2870
3	2	9	35	132	494
	1	5	20	76	285
4	keine Lösung				
5	5	14	99	260	1785
	2	6	44	116	798
6	3	8	35	84	351
	1	3	14	34	143
7	6	14	104	231	1665
	2	5	39	87	629
8	15	32	527	1104	17919
	5	11	186	390	6335
9	keine Lösung				
10	4	20	39	175	779
	1	6	12	55	246

Tabelle 1 Lösungen von Gleichung (2)

Tabelle 1 zeigt zunächst die ersten fünf Lösungen der Gleichung (2) für $2 \leq d \leq 10$, d keine Quadratzahl. Ein Blick auf diese Tabelle macht deutlich, daß man wohl allenfalls die ersten zwei oder drei Lösungen durch Probieren "von Hand" finden kann. Ein einfaches Suchprogramm liefert dagegen genügend Daten, um interessante Muster und Zusammenhänge zu erkennen. Schon eine kurze Liste von Lösungen der Gleichung (1), d.h. $d = 2$, läßt Beziehungen zur Kettenbruchentwicklung von $\sqrt{2}$ und deren Näherungsbrüchen vermuten (vgl. Satz 8).

Systematisches Suchen nach Lösungen für den Fall, daß d eine Quadratzahl ist, scheint den Verdacht nahezulegen, daß lediglich für Werte der Form $d = 4v^2$ mit ungeradem $v \geq 3$ eine Lösung für (2) existiert, nämlich $n = v^2 - 1$ und $k = (v-1)/2$, was sich allerdings nicht bestätigt (vgl. Kapitel 8). Auch mit Computerhilfe wird man schwerlich die erste Quadratzahl $d = 48024900 = 6930^2$ finden, für die (2) mehr als eine Lösung

besitzt: $k_1 = 1732$, $k_2 = 1$. Ausgestattet mit dem theoretischen Rüstzeug, das in Kapitel 8 entwickelt wird, ist es jedoch ein Leichtes, diese Lösung (und weitere) sogar von Hand zu ermitteln.

3 Eine nützliche Transformation und Neu-Interpretation

Für die weitere Untersuchung der Gleichung (2) formen wir diese durch quadratische Ergänzung beider Seiten um:

$$\left(n+\frac{1}{2}\right)^2 - \frac{1}{4} = d\left(\left(k+\frac{1}{2}\right)^2 - \frac{1}{4}\right).$$

Multiplikation mit 4 ergibt $(2n+1)^2 - 1 = d((2k-1)^2 - 1)$. Mit $u = 2n+1$ und $v = 2k+1$ wird daraus $u^2 - 1 = d(v^2 - 1)$ beziehungsweise

$$u^2 - dv^2 = 1 - d. \tag{3}$$

Jede Lösung von (2) mit $k > 0$ entspricht umkehrbar eindeutig einer Lösung von (3) in ungeraden Zahlen ≥ 3.

Mit $d = e^2$ läßt sich diese Gleichung auch in der Form $e^2 - 1 = (ev - u)(ev + u)$ oder $e^2 - 1 = r \cdot s$ mit $r = ev - u$ und $s = ev + u$ schreiben. Das heißt, für $d = e^2$ ist das Problem genau dann lösbar, wenn für $e^2 - 1$ eine Faktorisierung $r \cdot s$ existiert, so daß $u = (s-r)/2$ und $v = (r+s)/(2e)$ ungerade ganze Zahlen ≥ 3 sind. Da weder für $e^2 = 4$ noch für $e^2 = 9$ solche Faktorisierungen existieren, ist die Frage nach eventuellen Lösungen für diese Fälle in Tabelle 1 entschieden. Ebenso läßt sich sofort zeigen, daß z.B. für $e^2 = 16, 25, 49, 64, 81, 121$ keine Lösung existiert. Die triviale Faktorisierung mit $r = 1$ und $s = e^2 - 1$ führt wegen $u = (e^2-2)/2$ und $v = e/2$ genau dann zu einer Lösung, wenn e vom Typ $4x+2$ mit $x \in \mathbb{N}$ ist. So erhalten wir für die kleinste Quadratzahl, die eine Lösung unseres Problems zuläßt, nämlich $e^2 = 36$, die Paare $(u,v) = (17,3)$ bzw. $(n,k) = (8,1)$. Der nächste Fall, $e^2 = 100$, liefert $(u,v) = (49,5)$ bzw. $(n,k) = (24,2)$. Die allgemeine Untersuchung erfolgt in Abschnitt 8.

Auch im Fall, daß d keine Quadratzahl ist, läßt sich die Gleichung (3) aus dem Blickwinkel der Faktorisierung umdeuten:

$$\left(u + v\sqrt{d}\right)\left(u - v\sqrt{d}\right) = 1 - d.$$

Als Faktoren erhalten wir jetzt reelle Zahlen aus dem in $\mathbb{R}$ enthaltenen Ring

$$\mathbb{Z}\left[\sqrt{d}\right] := \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}.$$

Bei jeder Faktorisierung in einem kommutativen Ring R spielen die *Einheiten* eine große Rolle, das sind diejenigen Elemente $\epsilon \in R$, für die es ein multiplikatives Inverses ϵ^{-1} in R gibt: $\epsilon \cdot \epsilon^{-1} = 1$. Ist nämlich $x = A \cdot B$ eine Faktorisierung in R, so liefert jede Einheit ϵ eine weitere $x = (\epsilon A) \cdot (\epsilon^{-1} B)$.

In unserer Situation werden wir daher dazu geführt, die Einheiten des Ringes $R = \mathbb{Z}[\sqrt{d}] \subseteq \mathbb{R}$ zu untersuchen, was im folgenden Abschnitt erfolgt.

4 Die Pellsche Gleichung[2]

Sei $d \in \mathbb{N}$, $d > 1$ und keine Quadratzahl. Als Pellsche Gleichung bezeichnet man die diophantische Gleichung

$$x^2 - dy^2 = \pm 1. \tag{4}$$

($x^2 - dy^2 = \pm 1$ steht als Abkürzung für $x^2 - dy^2 = 1$ oder $x^2 - dy^2 = -1$.)

Die Lösungstheorie der Pellschen Gleichung ist wohlbekannt, ebenfalls der Zusammenhang dieser Gleichung mit den Einheiten von $\mathbb{Z}[\sqrt{d}]$. Auf der Basis der Überlegungen in [6], II.5 stellen wir die in dieser Arbeit benötigten Ergebnisse zusammen.

Der Ring $\mathbb{Z}$ ist ein echter Teilring von $\mathbb{Z}[\sqrt{d}]$, da $\sqrt{d}$ irrational ist. Aus der Irrationalität von $\sqrt{d}$ erkennt man, daß ein Element $z \in \mathbb{Z}[\sqrt{d}]$ eine eindeutige Darstellung der Form $z = x + y\sqrt{d}$ mit $x, y \in \mathbb{Z}$ besitzt. Ist $z = x + y\sqrt{d}$ so heißt $\overline{z} := x - y\sqrt{d}$ die zu z konjugierte Zahl. Es gilt offenbar für beliebige $z, w \in \mathbb{Z}[\sqrt{d}]$:

$$\begin{aligned} \overline{z + w} &= \overline{z} + \overline{w}, \\ \overline{zw} &= \overline{z} \cdot \overline{w}, \\ z = \overline{z} &\Leftrightarrow z \in \mathbb{Z}. \end{aligned} \tag{5}$$

Die ganze Zahl $N(z) := z\overline{z} = x^2 - y^2 d$ nennt man die Norm von z. Aus (5) folgt sofort

$$N(zw) = N(z)N(w). \tag{6}$$

Die Pellsche Gleichung zu lösen, ist also gleichbedeutend damit, $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ zu finden mit $N(z) = \pm 1$. Die Elemente z mit $N(z) = \pm 1$ sind aber auch gleichzeitig die Einheiten von $\mathbb{Z}[\sqrt{d}]$, d.h. gemäß der Definition diejenigen Elemente z, für die es ein Element $w \in \mathbb{Z}[\sqrt{d}]$ mit $zw = 1$ gibt.

Satz 1: *$z \in \mathbb{Z}[\sqrt{d}]$ ist genau dann Einheit von $\mathbb{Z}[\sqrt{d}]$, wenn $N(z) = \pm 1$ gilt.*

Beweis: Gilt $zw = 1$, so folgt aus (6): $N(z)N(w) = N(1) = 1$. Die Normen $N(z)$ und $N(w)$ sind ganze Zahlen, somit $N(z) = \pm 1$. Sei umgekehrt $N(z) = \pm 1$, dann ist $w := \frac{1}{N(z)}\overline{z} \in \mathbb{Z}[\sqrt{d}]$, und es folgt $zw = \frac{1}{N(z)}N(z) = 1$. □

Die Zahlen ± 1 sind sicherlich Einheiten von $\mathbb{Z}[\sqrt{d}]$. Angenommen, $z \neq \pm 1$ sei eine Einheit. Da auch $-z$ und $\pm z^{-1}$ Einheiten sind, findet man in diesem Fall eine Einheit $z > 1$. Derartige Einheiten sind für uns von großem Interesse.

---

2) Die Bezeichnung Pellsche Gleichung beruht auf einem Irrtum Eulers. Tatsächlich hat der englische Mathematiker John Pell (1610–1680), dessen Namen die Gleichung trägt, keinerlei Beitrag zu deren Erforschung geleistet. Zur Geschichte der Pellschen Gleichung sei auf [6], [9] verwiesen.

Satz 2: *Sei $z = x + y\sqrt{d}$ eine Einheit. Dann sind äquivalent:*

$$\text{(i)} \quad z > 1, \qquad \text{(ii)} \quad x, y \geq 1.$$

Beweis: Sind $x, y \geq 1$, so folgt offenbar $z > 1$. Für die noch fehlende Implikation verwenden wir die Formeln $2x = z + \bar{z}$, $z\bar{z} = \pm 1$, woraus $2x = z + 1/z$ und $|\bar{z}| < 1$ folgt. Man erkennt $x > 0$ und damit $x \geq 1$, da x eine ganze Zahl ist. Weiterhin schließt man $z = x \pm \sqrt{x^2 \pm 1}$. Wegen $z > 1$ kommt nur $z = x + \sqrt{x^2 \pm 1}$ in Betracht, was zu $y = \sqrt{x^2 + 1}/\sqrt{d} > 0$ und, wie eben, zu $y \geq 1$ führt. □

Satz 2 besagt, daß die Lösungen der Pellschen Gleichung im Bereich der natürlichen Zahlen umkehrbar eindeutig den Einheiten $z > 1$ entsprechen, und zwar durch die Zuordnung $(x, y) \mapsto z = x + y\sqrt{d}$.

Eine weitere Konsequenz ist ebenfalls von Wichtigkeit.

Satz 3: *Seien $z = x + y\sqrt{d}$, $z' = x' + y'\sqrt{d}$ zwei Einheiten mit $z, z' > 1$. Dann sind äquivalent:*

$$\text{(i)} \quad z < z', \qquad \text{(ii)} \quad x < x', \qquad \text{(iii)} \quad y < y'.$$

Beweis: Die Äquivalenz von (ii) und (iii) ergibt sich aus den Bedingungen $N(z) = \pm 1$, $N(z') = \pm 1$ und $d \geq 1$. Daher wird (i) von (ii) impliziert. Sei jetzt (i) vorausgesetzt. Dann ist auch $w := z'z^{-1}$ eine Einheit > 1 und hat somit eine Darstellung $w = a + b\sqrt{d}$ mit $a, b \geq 1$. Aus $z' = w \cdot z$ folgt sofort $x' > x$. □

Bisher ist noch nicht gezeigt worden, daß es überhaupt eine Einheit $z > 1$ gibt. Der Existenznachweis ist in der Tat nichttrivial und kann etwa über die Kettenbruchentwicklung von $\sqrt{d}$ erfolgen, siehe [6], Satz 9, S. 120. In dieser Arbeit werden wir diese Tatsache ohne weiteren Beweis verwenden. Aus der Kombination der Sätze 2 und 3 ergibt sich unmittelbar die Existenz einer *kleinsten Einheit* $z_0 > 1$. Sie heißt die *Grundeinheit* von $\mathbb{Z}[\sqrt{d}]$. Aus der Darstellung $z_0 = x_0 + y_0\sqrt{d}$, $x_0, y_0 \geq 1$ gewinnt man die (bzgl. x oder y) kleinste Lösung der Pellschen Gleichung $x^2 - dy^2 = \pm 1$ in natürlichen Zahlen; wir nennen (x_0, y_0) die Grundlösung dieser Gleichung. Weitere Einheiten > 1 erhält man offenbar durch die Potenzen z_0^k, $k \in \mathbb{N}$. Andere Einheiten $z > 1$ gibt es nicht, wie man wie folgt einsieht: Ist $z > 1$ eine Einheit, so gibt es wegen $z_0 > 1$ einen Exponenten k mit $z_0^k \leq z \leq z_0^{k+1}$. Für die Einheit $w = zz_0^{-k}$ gilt dann $1 \leq w < z_0$. Die Minimalität von z_0 erzwingt $w = 1$, d.h. $z = z_0^k$. Wir fassen zusammen:

Satz 4:

(i) *Für jedes $k \in \mathbb{N}$ ist $z = x + y\sqrt{d} := z_0^k$ eine Einheit > 1 von $\mathbb{Z}[\sqrt{d}]$ und $(x, y) \in \mathbb{N}^2$ eine Lösung der Pellschen Gleichung,*

(ii) *jede Einheit $z > 1$ bzw. jede Lösung der Pellschen Gleichung in natürlichen Zahlen wird so erhalten.*

Die Norm $N(z_0)$ der Grundeinheit entscheidet, ob nur die Pellsche Plus-Gleichung $x^2 - dy^2 = 1$ oder auch die Pellsche Minus-Gleichung $x^2 - dy^2 = -1$ lösbar ist. In der Tat,

aus $N(z_0^k) = N(z_0)^k$ ergibt sich, daß bei $N(z_0) = 1$ nur die Plus-Gleichung lösbar ist, während bei $N(z_0) = -1$ die Potenzen z_0^{2k}, $k \geq 1$, zu den Lösungen der Plus-Gleichung und die Potenzen z_0^{2k+1}, $k \geq 0$, zu den Lösungen der Minus-Gleichung führen.

Die Grundlösung von $x^2 - dy^2 = \pm 1$ findet man für kleine d's bereits durch systematisches Probieren (evtl. mit einem einfachen Computerprogramm), im allgemeinen mit Hilfe der Kettenbruchentwicklung von $\sqrt{d}$, [6], loc. cit.

Die folgende Tabelle betrifft die ersten zehn Grundlösungen sowie die Fälle $d = 61, 94$.

d	2	3	5	6	7	8	10	11	12	13	61	94
x_0	1	2	2	5	8	3	3	10	7	18	29718	2143295
y_0	1	1	1	2	3	1	1	3	2	5	3805	221064
$N(z_0)$	-1	1	-1	1	1	1	-1	1	1	-1	-1	1

Tabelle 2: Grundlösungen der Pellschen Gleichung

Die Beispiele $d = 61, 94$ weisen auf die bemerkenswerte Tatsache hin, daß die Grundlösungen bzw. Grundeinheiten, relativ zu d, oft recht groß sind. Als weiterführende Lektüre seien dazu die Abschnitte 58 und 72 in [7] empfohlen.

Ohne Beweis sei noch angefügt, daß die Gleichung $x^2 - dy^2 = -1$ genau dann lösbar ist, wenn die Kettenbruchentwicklung von $\sqrt{d}$ eine Periode von ungerader Länge hat, siehe [6], Beweis von Satz 10, S. 120.

5 Die Gleichung $n(n+1) = 2k(k+1)$

Die Ergebnisse des vorigen Kapitels können wir direkt auf die Gleichung (3) mit $d = 2$ und somit zur Lösung von (1) anwenden. Mit $d = 2$ wird aus (3) die Pellsche Gleichung

$$u^2 - 2v^2 = -1. \tag{7}$$

Dabei interessieren uns nur Lösungen (u, v) mit ungeraden $u, v \geq 3$.

Offenbar gilt für jede positive Lösung von (7), daß u ungerade und größer als v ist. Aber auch v muß ungerade sein, da sonst $u^2 \equiv -1 \bmod 4$ gelten würde. Also erfüllt jede Lösung von (7) mit $v \geq 3$ und $u > 0$ die obigen Bedingungen und liefert damit eine Lösung von (1).

Das Paar $(u, v) = (1, 1)$ löst Gleichung (7) und ist offenbar die Grundlösung der Pellschen Gleichung. Anders formuliert: $z_0 = 1 + \sqrt{2}$ ist die Grundeinheit von $\mathbb{Z}[\sqrt{2}]$. Nach dem vorigen Abschnitt wird die Pellsche Gleichung durch die Potenzen z_0^{m+1}, die Minus-Gleichung durch die Potenzen z_0^{2m+1}, $m \in \mathbb{N}_0$ gelöst. Wir interessieren uns, wie oben gesagt, nur für Einheiten $u + v\sqrt{2}$ mit $v \geq 3$, $u > 0$. Da bereits $z_0^3 = 7 + 5\sqrt{2}$ diese Bedingung erfüllt, erhalten wir als Lösung von (7) mit ungeraden $u, v \geq 3$ genau die Paare (u, v) mit $u + v\sqrt{2} = z_0^{2m+1}$, $m \in \mathbb{N}$. Indem wir die Transformation von Abschnitt 3 rückgängig machen, erhalten wir aus den Lösungen von (7) die uns interessierenden Lösungen der Ausgangsgleichung

$$n(n+1) = 2k(k+1). \tag{1}$$

Eine unmittelbare Rechnung liefert nun unter Beachtung von $(1+\sqrt{2})^2 = 3+2\sqrt{2}$

Satz 5: *Die Gleichung* (1) *hat unendlich viele Lösungen in natürlichen Zahlen* n, k. *Sie sind gegeben durch*

$$n_m + k_m\sqrt{2} = \frac{1}{2}\left(1+\sqrt{2}\right)\left(\left(3+2\sqrt{2}\right)^m - 1\right),\ m \in \mathbb{N}.$$

Für $m = 1$ erhält man das Paar $(3,2)$, für $m = 2$ das Paar $(20,14)$ etc. Aus der Darstellung in Satz 5 lassen sich mittels der Konjugation in $\mathbb{Z}[\sqrt{d}]$ Formeln für n_m und k_m gewinnen. Unter Berücksichtigung von $(3+2\sqrt{2})^m = (1+\sqrt{2})^{2m}$ und den Rechenregeln (5) erhält man

$$n_m \pm k_m\sqrt{2} = \frac{1}{2}\left(\left(1\pm\sqrt{2}\right)^{2m+1} - \left(1\pm\sqrt{2}\right)\right)$$

und daraus für $m \in \mathbb{N}$:

$$\begin{aligned} n_m &= \frac{1}{4}\left(\left(1+\sqrt{2}\right)^{2m+1} + \left(1-\sqrt{2}\right)^{2m+1}\right) - \frac{1}{2}, \\ k_m &= \frac{\sqrt{2}}{8}\left(\left(1+\sqrt{2}\right)^{2m+1} - \left(1-\sqrt{2}\right)^{2m+1}\right) - \frac{1}{2}. \end{aligned} \tag{8}$$

Das so beschriebene Verfahren ist noch recht unhandlich und auch für den Computereinsatz zunächst wenig geeignet, da beim Rechnen mit reellen Zahlen Rundungsfehler unvermeidlich sind. Es sollen deshalb Verfahren zur rekursiven Berechnung der Lösungen von (1) und (2) entwickelt werden.

Wir werden zwei Verfahren darstellen, die beide auf der Berechnung der Potenzen z^n, $n \in \mathbb{N}$, eines Elementes $z \in \mathbb{Z}[\sqrt{d}]$ beruhen. Sie unterscheiden sich durch die Methoden, diese Potenzen zu bestimmen. Während der Beschreibung der Verfahren ist d eine beliebige natürliche Zahl, die kein Quadrat ist.

Sei die Zahl $z = x + y\sqrt{d}$ in $\mathbb{Z}[\sqrt{d}]$ gegeben. Wir wollen die Potenzen $z^n = x_n + y_n\sqrt{d}$, $n \in \mathbb{N}_0$, rekursiv berechnen. z erfüllt die quadratische Gleichung

$$z^2 = 2x \cdot z - N(z),$$

Multiplikation mit z^{n-2}, $n \geq 2$ liefert $z^n = 2xz^{n-1} - N(z)z^{n-2}$. Daraus erhalten wir die folgenden linearen Rekursionsformeln, zusammen mit den Anfangsbedingungen:

$$\begin{aligned} (x_0, y_0) &= (1,0),\ (x_1, y_1) = (x, y), \\ x_n &= 2x \cdot x_{n-1} - N(z)x_{n-2}, \\ y_n &= 2x \cdot y_{n-1} - N(z)y_{n-2}. \end{aligned} \tag{9}$$

Für die Anwendung auf Satz 5 haben wir ein Produkt $z^n(a+b\sqrt{d}) = x'_n + y'_n\sqrt{d}$ bei vorgegebenen Zahlen a und b rekursiv zu berechnen. Als Linearkombination von x_n und y_n erfüllen x'_n und y'_n dieselbe Rekursionsformel wie x_n und y_n; der Unterschied liegt allein in den Anfangsbedingungen. Daher erhält man aus Satz 5 Rekursionsformeln für $n_m + 1/2$ und $k_m + 1/2$, wenn man noch beachtet, daß $z = 3 + 2\sqrt{2}$ die quadratische Gleichung

$$z^2 = 6z - 1$$

erfüllt. Weitere Umformung liefert mit $(n_0, k_0) := (0,0)$ den folgenden

Satz 6: *Für die Lösungen* (n_m, k_m), $m \geq 0$ *der Gleichung* $n(n+1) = 2k(k+1)$ *gilt:*

$$(n_m, k_m) = \begin{cases} (0,0) & \text{falls } m = 0, \\ (3,2) & \text{falls } m = 1, \\ 6(n_{m-1}, k_{m-1}) - (n_{m-2}, k_{m-2}) + (2,2) & \text{falls } m \geq 2. \end{cases}$$

Diese Rekursionsformeln erlauben eine schnelle Berechnung für nicht zu große Indizes m. Bei weiter wachsenden Indizes wird sich jedoch bald die Überlegenheit des nun folgenden Verfahrens erweisen. Für gegebenes $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ betrachten wir die Multiplikation mit z in $\mathbb{Z}[\sqrt{d}]$. Sei $w = a + b\sqrt{d}$ und $zw = u + v\sqrt{d}$, dann erhalten wir in Matrixform

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} x & yd \\ y & x \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Durch die wiederholte Anwendung ergibt sich für $z^n(a+b\sqrt{d}) = x'_n + y'_n\sqrt{d}$ die Beziehung

$$\begin{pmatrix} x'_n \\ y'_n \end{pmatrix} = \begin{pmatrix} x & yd \\ y & x \end{pmatrix}^n \begin{pmatrix} a \\ b \end{pmatrix}. \tag{10}$$

Speziell in der Situation von Satz 5 gilt $a = b = 1/2$, $x = 3$, $y = d = 2$. Daher folgt

Satz 7: *Für die Lösungen* $(n_m, k_m)_{m \geq 0}$ *der Gleichung* $n(n+1) = 2k(k+1)$ *gilt:*

$$\begin{pmatrix} n_m \\ k_m \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^m \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} - \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}.$$

Zurück in der Situation eines allgemeinen d hat man in (10) die Potenzen der Matrix

$$M := \begin{pmatrix} x & yd \\ y & x \end{pmatrix}$$

zu berechnen. Hierzu schlagen wir einen Spezialfall der schnellen Berechnung von Potenzen durch Additionsketten vor, vgl. [2], section 4.6.3. Es gelingt damit, die Potenzen M^n in höchstens $2 \cdot \log_2 n$ Matrix-Multiplikationen zu berechnen. Das Berechnungsverfahren beruht auf der dyadischen Entwicklung von n. Sei

$$n = 2^{t_1} + 2^{t_2} + \ldots + 2^{t_r}, \; 0 \leq t_1 < t_2 < \ldots < t_r.$$

Durch fortgesetztes Quadrieren nach der Formel $M^{2^{t+1}} = (M^{2^t})^2$ berechnet man in t_r Matrix-Multiplikationen die Potenzen $M, M^2, M^{2^2}, \ldots, M^{2^t}, \ldots, M^{2^{t_r}}$. Durch weitere $(r-1)$ Multiplikationen gewinnt man dann $M^n = M^{2^{t_1}} \cdot M^{2^{t_2}} \cdot \ldots \cdot M^{2^{t_r}}$. Insgesamt wird M^n mit $t_r + (r-1)$ Matrix-Multiplikationen bestimmt.

Unser Problem mit $d = 2$ läßt sich auch ohne Rückgriff auf die Pellsche Gleichung lösen, indem man aufgrund von Zahlenmustern die Rekursionsformel errät und dann durch vollständige Induktion beweist. Dieses Vorgehen findet man in [5]. Mit Blick auf das Ziel, Gleichung (2) für beliebiges d zu lösen, führen die hier benutzten Methoden jedoch weiter.

6 Beziehungen zu Kettenbruchentwicklungen

Der Kettenbruch

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ldots}}}$$

hat die Näherungsbrüche 1, 3/2, 7/5, 17/12, 41/29, 99/70, ... Vergleichen wir nun diese mit der Folge

$$(n_m/k_m):\ 3/2,\ 20/14 = (3+17)/(2+12),\ 119/84 = (3+17+99)/(2+12+70),\ \ldots$$

Eine enge Beziehung zwischen den Lösungen von (2) und der Kettenbruchentwicklung von $\sqrt{d}$ kann nicht überraschen, da Gleichung (2) äquivalent ist zu

$$d = (n/k)(n+1)/(k+1).$$

Das bedeutet, daß für die Lösungen (n_m, k_m) die Folge der Quotienten (n_m/k_m) gegen $\sqrt{d}$ konvergiert.

Für $d = 2$ sind die Zusammenhänge besonders einfach, da (x, y) genau dann eine positive Lösung der Pellschen Gleichung $x^2 - 2y^2 = \pm 1$ ist, wenn x/y ein Näherungsbruch von $\sqrt{2}$ ist, siehe [6], loc. cit. Ist p_i/q_i der i-te Näherungsbruch von $\sqrt{2}$, so gilt (vgl. z.B. [6]):

$$(p_i, q_i) = (2p_{i-1} + p_{i-2}, 2q_{i-1} + q_{i-2})$$

mit den Anfangsbedingungen $(p_1, q_1) = (1, 1)$ und $(p_2, q_2) = (3, 2)$. Für die i-te Lösung (x_i, y_i) der Pellschen Gleichung gilt mit den gleichen Anfangsbedingungen ebenfalls $x_i = 2x_{i-1} + x_{i-2}$, $y_i = 2y_{i-1} + y_{i-2}$, wie aus (9) folgt.

Satz 8: *Ist p_i/q_i der i-te Näherungsbruch der Kettenbruchentwicklung von $\sqrt{2}$ und (n_m, k_m) die m-te Lösung von (1), so gilt*

$$(n_m, k_m) = \frac{1}{2}(p_{2m+1} - 1, q_{2m+1} - 1) = \left(\sum_{i=1}^{m} p_{2i}, \sum_{i=1}^{m} q_{2i}\right).$$

Beweis: Die Gültigkeit der ersten Gleichung wurde bereits gezeigt. Zähler und Nenner der Näherungsbrüche mit geradzahligem Index ergeben die Lösungen von $x^2 - 2y^2 = 1$. Für die Folge dieser Lösungen gelten die rekursiven Beziehungen, wie wir sie im vorigen Kapitel für die Lösungen von $x^2 - 2y^2 = -1$, d.h. für die Elemente

$$\left(1+\sqrt{2}\right)^{2m+1} = \left(3+2\sqrt{2}\right)^m \left(1+\sqrt{2}\right)$$

hergeleitet haben, nämlich $p_{2m} = 6p_{2m-2} - p_{2m-4}$ und $q_{2m} = 6q_{2m-2} - q_{2m-4}$.
Mit der Abkürzung $\sum_m = p_2 + p_4 + \ldots + p_{2m}$ gilt für $m \geq 3$:

$$\begin{aligned} 6\sum_{m-1} - \sum_{m-2} &= 6p_2 + (6p_4 - p_2) + (6p_6 - p_4) + \ldots + (6p_{2m-2} - p_{2m-4}) \\ &= 6p_2 + p_6 + \ldots + p_{2m} \\ &= \sum_m +5p_2 - p_4. \end{aligned}$$

Wegen $p_2 = 3$ und $p_4 = 17$ ergibt dies $\sum_m = 6\sum_{m-1} - \sum_{m-2} - 2$, die gleiche rekursive Beziehung, die wir für die Folge (n_m) hergeleitet haben. Da die Anfangsbedingungen $\sum_1 = 3 = n_1$ und $\sum_2 = 20 = n_2$ übereinstimmen, gilt $\sum_m = n_m$ für alle $m \geq 1$.
Die gleiche Argumentation gilt für die Folge (k_m) und die Summe der Nenner der Näherungsbrüche mit geradzahligem Index. □

7 Die Gleichung $n(n+1) = dk(k+1)$

Wir kommen nun zu der aus (2) abgeleiteten Gleichung

$$u^2 - dv^2 = 1 - d, \tag{11}$$

wobei $d \geq 2$, aber keine Quadratzahl ist. Wir erinnern daran, daß die Lösungen der Gleichung (2) in $\mathbb{N}$ den ungeraden Lösungen $u, v \geq 3$ von (11) entsprechen. Zunächst lassen wir jedoch diese Einschränkung unberücksichtigt und studieren die Lösungen von (11) im Bereich aller natürlichen Zahlen, d.h. $u, v \geq 1$.

Mit $z = u + v\sqrt{d}$ ist (11) gleichbedeutend mit $N(z) = 1 - d$, anders formuliert: mit der Faktorisierung $1 - d = z \cdot \bar{z}$. Ist ϵ eine Einheit mit $N(\epsilon) = 1$, so gilt ebenfalls $N(z\epsilon) = 1 - d$. Sind $u, v \geq 1$ und ist $\epsilon \geq 1$, so erhält man in $z\epsilon = u' + v'\sqrt{d}$ positive Koeffizienten u', v'. Die Gleichung $N(z) = 1 - d$ hat jedenfalls die Lösung $z = 1 + \sqrt{d}$, woraus sich nach Multiplikation mit den Einheiten $\epsilon > 1$, $N(\epsilon) = 1$ weitere, insgesamt unendlich viele Lösungen ergeben.

Sei z_0 die Grundlösung von $N(z) = \pm 1$, d.h. die Grundeinheit von $\mathbb{Z}[\sqrt{d}]$. Den Wert $s = p + q\sqrt{d}$ definieren wir durch $s = z_0$ falls $N(z_0) = 1$ und $s = z_0^2$ falls $N(z_0) = -1$. Da die Norm multiplikativ ist und $z_0 > 1$, gilt $N(s) = 1$ und $s > 1$. s ist die kleinste Zahl, die diese beiden Bedingungen erfüllt.

Wie gesagt, liefert jede Zahl der Form $(1 + \sqrt{d})s^m$ eine Lösung von (11). Genauer gilt

Satz 9: *Falls d keine Quadratzahl ist, so hat* (11) *unendlich viele Lösungen. Eine Schar von Lösungen ist gegeben durch* (u_m, v_m) *mit* $u_m + v_m\sqrt{d} = (1 + \sqrt{d})s^m$. *Dabei ist* $s = p + q\sqrt{d}$ *die kleinste Lösung von* $N(z) = 1$, $z > 1$.

Die Paare (u_m, v_m) *genügen den Bedingungen*

$$(u_m, v_m) = \begin{cases} (1,1) & \text{falls } m = 0, \\ (p + dq, p + q) & \text{falls } m = 1, \\ 2p(u_{m-1}, v_{m-1}) - (u_{m-2}, v_{m-2}) & \text{falls } m \geq 2. \end{cases}$$

Beweis: Wegen $N((1+\sqrt{d})s^m) = N(1+\sqrt{d})N(s^m) = 1-d$ sind die Zahlen $(1+\sqrt{d})s^m$ Lösungen von $N(z) = 1-d$, die uns Lösungen (u, v) von (11) liefern. Die Anfangswerte $(u_0, v_0) = (1,1)$ und $(u_1, v_1) = (p + dq, p + q)$ sind offensichtlich. Aus (9) ergibt sich $(u_m, v_m) = 2p(u_{m-1}, v_{m-2}) - (u_{m-2}, v_{m-2})$. □

Die in Satz 9 beschriebene Lösungsschar basiert auf der Anfangslösung $1 + \sqrt{d}$. Im allgemeinen enthält diese Schar nicht alle Lösungen von (11). Ist beispielsweise $d = 5$, so ist die zugehörige Grundeinheit $z_0 = 2 + \sqrt{5}$ mit $N(2 + \sqrt{5}) = -1$. Mit $(1 + \sqrt{5})z_0^2$ und $(1 + \sqrt{5})z_0^4$ erhalten wir die Lösungen $(29, 13)$ und $(521, 233)$. Dem entsprechen die in Tabelle 1 angegebenen Lösungen $(14, 6)$ und $(260, 116)$ der Gleichung (2). Die übrigen in Tabelle 1 angegebenen Lösungen gehören zu einer anderen, nämlich auf der Anfangslösung $11 + 5\sqrt{5}$ basierenden Lösungsschar. Gibt es weitere Lösungsscharen, vielleicht sogar unendlich viele, und wie findet man sie? Diesen Fragen wollen wir nun nachgehen.

Wie oben bereits festgelegt, gelte

$$s = p + q\sqrt{d} = \begin{cases} z_0 & \text{falls } N(z_0) = 1, \\ z_0^2 & \text{falls } N(z_0) = -1. \end{cases}$$

Es ist $s > 1$ und $N(s) = 1$, und nach Satz 4 stimmen die Einheiten ϵ mit $\epsilon > 1$, $N(\epsilon) = 1$ mit den Potenzen s^m, $m > 1$ überein. Gesucht werden Lösungen von $u^2 - dv^2 = -c$ mit $c = d - 1 > 0$ und $u, v > 0$.

Definition: Zwei positive Lösungen (u_1, v_1) und (u_2, v_2) von (11) gehören genau dann zur gleichen Schar, wenn es ein $m \in \mathbb{Z}$ gibt, so daß $u_2 + v_2\sqrt{d} = (u_1 + v_1\sqrt{d})s^m$. Die kleinste positive Lösung einer Schar bezeichnen wir als Anfangslösung dieser Schar.

Offenbar liefern die Scharen eine Klasseneinteilung der Menge aller positiven Lösungen von Gleichung (11). Jede Schar enthält unendlich viele Lösungen. Ist (u, v) eine Lösung von (11), aber keine Anfangslösung, so ist die in der Schar vorhergehende Lösung gegeben durch

$$(u + v\sqrt{d})s^{-1} = (u + v\sqrt{d})(p - q\sqrt{d}) = (up - vqd) + (vp - uq)\sqrt{d}.$$

Es sind also folgende Bedingungen erfüllt:

(i) $up - vqd > 0$ bzw. $u/v > dq/p$,

(ii) $vp - uq > 0$ bzw. $u/v < p/q$.

Sind für eine Lösung (u, v) diese Bedingungen nicht erfüllt, so muß es sich um eine Anfangslösung handeln und umgekehrt.

Bedingung (ii) ist für alle positiven Lösungen erfüllt, da aus $u^2 - dv^2 = -c$ folgt $(u/v)^2 = d - c/v^2 < d$ und andererseits, wegen $p^2 - dq^2 = 1$, gilt: $(p/q)^2 = d + 1/q^2 > d$. Aus $p^2 - dq^2 = 1$ folgt $(dq/p)^2 = d - d/p^2$. Wegen $(u/v)^2 = d - c/v^2$ ist somit die erste Bedingung genau dann erfüllt, wenn $c/v^2 < d/p^2$ bzw. $v^2 > p^2 c/d$. Eine positive Lösung ist somit genau dann Anfangslösung einer Schar, wenn $v^2 = (u^2 + c)/d \leq p^2 c/d$ oder gleichwertig, wenn $u^2 \leq c(p^2 - 1) = (d - 1)(p^2 - 1)$.

Die Existenz dieser Schranke bedeutet, daß es zu gegebenem d nur endlich viele Anfangslösungen und somit nur endlich viele Scharen von Lösungen gibt. Mit einem einfachen Suchprogramm lassen sich diese ermitteln. Aus dem Blickwinkel der Faktorisierbarkeit besagt dieses Ergebnis, daß $1 - d$ nur endlich viele wesentlich verschiedene Faktorisierungen der Art $1 - d = z \cdot \bar{z}$, $z = u + v\sqrt{d}$, $u, v > 0$ gestattet. Dabei sehen wir zwei Faktorisierungen als im wesentlichen gleich an, wenn sich die eine Zerlegung aus der anderen durch Multiplikation der Faktoren mit Einheiten ergibt.

Teil (i) des folgenden Satzes haben wir bereits bewiesen.

Satz 10:

(i) *Die Gleichung* (11) *hat nur endlich viele Lösungsscharen, die jeweils aus den Elementen* zs^m, $m \geq 0$, z *eine Anfangslösung, bestehen.*

(ii) *Für ein Element* $z = u + v\sqrt{d} \in \mathbb{Z}[d]$ *mit* $N(z) = 1 - d$ *sind äquivalent:*

(1) z *ist Anfangslösung,*

(2) $u, v > 0$, $u^2 < (d - 1)(p^2 - 1) = d(d - 1)q^2$,

(3) $u, v > 0$, $dv^2 < p^2(d - 1)$,

(4) $\sqrt{d - 1} < z < s\sqrt{d - 1}$.

Beweis: Es bleibt, die zusätzlichen Aussagen in (ii) zu zeigen. Ist $z = u + v\sqrt{d}$, $u, v > 0$ gegeben, so hatten wir bereits die Äquivalenz von (1) mit den gleichwertigen Bedingungen

$$u^2 \leq (d - 1)(p^2 - 1) \quad \text{und} \quad v^2 \leq p^2 \frac{d - 1}{d}$$

erkannt. Aus $p^2 - dq^2 = 1$ erhält man $u^2 \leq (d - 1)dq^2$ für die erste Ungleichung. Wäre $u^2 = (d - 1)dq^2$, so müßte $d(d - 1)$ ein Quadrat in $\mathbb{N}$ sein, also auch d wegen der Teilerfremdheit von d und $d - 1$. Somit gilt $u^2 < (d - 1)dq^2$. Analog führte die Annahme

$$v^2 = p^2 \frac{d - 1}{d}$$

über $(dv)^2 = p^2 d(d - 1)$ zum Widerspruch. Wir kommen jetzt zur Äquivalenz von (1) und (4). Sei z Anfangslösung. Dann $\sqrt{d - 1} < 1 + \sqrt{d} \leq z$ und $z = u + v\sqrt{d} < q\sqrt{d(d - 1)} + p\sqrt{d - 1} = s\sqrt{d - 1}$. Sei umgekehrt $N(z) = (u + v\sqrt{d})(u - v\sqrt{d}) = 1 - d$

und die Ungleichungen in (4) erfüllt. Aus $N(z) = 1 - d$ folgert man $|u| < |v| \cdot \sqrt{d}$. Aus $v \leq 0$ folgte $z < 0$. Somit $v > 0$, und aus $-\bar{z} = d - 1/z < \sqrt{d-1}$ schließt man auch $u > 0$. Die andere Ungleichung liefert $zs^{-1} < \sqrt{d-1}$, d.h. z ist eine Anfangslösung. □

Als Beispiel betrachten wir $d = 5$. Es ist $z_0 = 2 + \sqrt{5}$ die Grundeinheit von $\mathbb{Z}[\sqrt{5}]$ mit $N(z_0) = -1$. Somit erhalten wir $s = z_0^2 = 9 + 4\sqrt{5}$ und daraus die Abschätzungen $v \leq 8$ für die Anfangslösungen $z = u + v\sqrt{5}$. Man ermittelt leicht alle Anfangslösungen $1 + \sqrt{5}$, $4 + 2\sqrt{5}$, $11 + 5\sqrt{5}$.

Die Abschätzung

$$v^2 < p^2 \frac{d-1}{d},$$

aus der $v \leq p - 1$ folgt, besagt, daß es höchstens $(p-1)$ verschiedene Anfangslösungen, damit auch Lösungsscharen für die Gleichung (11) gibt. Wie man diese grobe Anzahlabschätzung verbessern, eventuell sogar zu einer genauen Anzahlbestimmung ausbauen kann, scheint ein schwieriges Problem zu sein, und wir gehen, abgesehen von den folgenden Bemerkungen, nicht weiter darauf ein.

Satz 11:

(i) *Ist z eine Anfangslösung von (11), so auch $w = -\bar{z}s$.*

(ii) *Ist $d - 1$ eine Primzahl oder $d = 2$, so gibt es höchstens zwei Lösungsscharen, die zu den Anfangslösungen $z = 1 + \sqrt{d}$ und $-\bar{z}s = (\sqrt{d} - 1)s$ gehören. Diese Anfangslösungen stimmen genau für $d = 2, 3$ überein.*

Beweis: (i) folgt sofort aus Satz 10, (ii). Die beiden in (ii) angegebenen Anfangslösungen stimmen genau dann überein, wenn $(1+\sqrt{d})^2 = (d-1)s$ gilt. Das ist der Fall für $d = 2, 3$, aber auch nur hierfür, da notwendigerweise $d - 1$ ein Teiler von 2 sein muß. Es bleibt zu zeigen, daß es keine weiteren Anfangslösungen gibt. Für $d = 2$ wurde diese Aussage in Abschnitt 4 gezeigt. Sei jetzt $l = d - 1$ eine Primzahl ≥ 2 und $z = u + v\sqrt{d}$ eine Anfangslösung. Aus $N(z) = -l$ folgt $u^2 \equiv v^2 \bmod l$ und, da l Primzahl ist, $u \equiv \epsilon v \bmod l$ für $\epsilon = \pm 1$. Wir setzen $u = \epsilon v + xl$. Wegen $u > v$ haben wir $x \geq 0$. Einsetzen in $N(z) = -l$ und Kürzen durch $-l$ führt zu der Gleichung $v^2 - 2\epsilon vx - x^2 l = 1$, aus der wir $(v - \epsilon x)^2 - x^2(l+1) = 1$ erhalten. Ist $x = 0$, so ergibt sich $v = u = 1$, $z = 1 + \sqrt{d}$. Sei dann $x > 0$ und zunächst $\epsilon = 1$. Aus $u < v(l+1)$ schließt man $x < v$ und dann, daß $\eta := (v - x) + v\sqrt{d}$ eine Einheit mit $\eta > 1$, $N(\eta) = 1$ ist. Somit $p \leq v - x$ und angesichts von Satz 10, (ii) führt dies zum Widerspruch $v < p \leq v - x$. Somit muß $\epsilon = -1$ sein. Jetzt ist $\eta = v + x + x\sqrt{d}$ eine derartige Einheit, was $\eta = s^i$ nach sich zieht. Weiterhin erkennt man: $(\sqrt{d} - 1)\eta = z$, d.h. $z = [-\overline{(1 + \sqrt{d})s}] \cdot s^{i-1}$ und folglich $z = (\sqrt{d} - 1)s$, da z eine Anfangslösung sein sollte. □

Die Überlegungen im Beweis zeigen, daß ganz generell die Zuordnung $z \mapsto -\bar{z}s$ eine involutorische Selbstabbildung in der Menge der Lösungsscharen induziert (man beachte, daß $w = -\bar{z}s$ seinerseits $z = -\bar{w}s$ liefert). Diese Involution kann auch in anderen Fällen Fixpunkte aufweisen: für $d = 5$ sieht man, daß die Anfangslösungen $1+\sqrt{5}$ und $11+5\sqrt{5}$ durch diese Involution zugeordnet werden, während $4 + 2\sqrt{5}$ ein Fixpunkt ist.

Bisher haben wir die Lösungen der Gleichung (11) in beliebigen natürlichen Zahlen u, v untersucht. Im Hinblick auf die Ausgangsgleichung $n(n+1) = dk(k+1)$ dieser Arbeit müssen wir aber speziell nach ungeraden Lösungen $u = 2n+1$, $v = 2k+1 \geq 3$ von (11) suchen. Das erfordert, für die Elemente in einer Lösungsschar die Parität der Koeffizienten u, v festzustellen. Hierbei stellt sich eine Abhängigkeit der Parität allein von der Kongruenzklasse von d mod 8 und von q mod 2 heraus mit $s = p + q\sqrt{d}$ wie bisher. Wir haben einige Fälle zu unterscheiden.

Fall 1: $d \equiv 2, 3 \bmod 4$

(i) Für jede Lösung von $u^2 - dv^2 = 1 - d$ sind u und v ungerade.

Beweis: Wir verwenden die Tatsache, daß $x^2 \equiv 0, 1 \bmod 4$ ist je nachdem, ob x gerade oder ungerade ist. Aus $u^2 \equiv dv^2 + (1-d) \bmod 4$ ergibt sich in den beiden Fällen, daß u, v ungerade sein müssen.

(ii) Die Lösungsschar zu $1+\sqrt{d}$ enthält $(1+\sqrt{d})(p+q\sqrt{d}) = z_1 = (qd+p)+(p+q)\sqrt{d}$ als kleinstes Element mit ungeraden Koeffizienten ≥ 3. Jede andere Lösungsschar enthält nur Elemente mit derartigen Koeffizienten. Insbesondere liegt noch die Lösungsschar zu $w_1 = (\sqrt{d}-1)(p+q\sqrt{d}) = (qd-p)+(p-q)\sqrt{d}$ vor. Es ist $w_1 \neq z_1$ für $d \neq 2, 3$.

Fall 2: $d \equiv 1 \bmod 4$

(i) In einer Lösungsschar sind entweder alle Koeffizienten gerade oder alle ungerade. Beide Fälle treten auf. Ist $d \equiv 9 \bmod 16$, so gibt es keine Lösungsschar mit geraden Koeffizienten.

(ii) Die Lösungsscharen zu $1+\sqrt{d}$ und $(\sqrt{d}-1)s$ enthalten nur Elemente mit ungeraden Koeffizienten.

Beweis: Aus $N(u+v\sqrt{d}) = 1-d$, $d \equiv 1 \bmod 4$ folgt $u^2 \equiv v^2 \bmod 4$ und daraus $u \equiv v \bmod 2$. Entsprechend schließt man für $s = p + q\sqrt{d}$ aus $p^2 \equiv q^2 + 1 \bmod 4$, daß p ungerade und q gerade ist. Hat eine Anfangslösung z gerade Koeffizienten, so gilt dies auch für alle anderen Elemente zs^m, $m \geq 0$. Hat eine Lösung $z = u + v\sqrt{d}$ ungerade Koeffizienten, so folgt für $zs = u' + v'\sqrt{d}$, $u' = up + dqv \equiv up \equiv 1 \bmod 2$, d.h. in der Lösungsschar zu einer derartigen Anfangslösung treten nur ungerade Koeffizienten auf. Speziell gilt dies für die Scharen zu $1+\sqrt{d}$, $(\sqrt{d}-1)(p+q\sqrt{d})$. Für $d = 5, 13, 17, 21, 29, 33, 37$ treten beide Fälle auf. Sei dann $d \equiv 9 \bmod 16$ und $N(u+v\sqrt{d}) = 1-d$ mit u, v gerade. Wir setzen $u = 2\overline{u}$, $v = 2\overline{v}$ und erhalten

$$\overline{u}^2 - d\overline{v}^2 = -\frac{d-1}{4}.$$

Betrachtung mod 4 liefert die Gleichung $\overline{u}^2 - \overline{v}^2 \equiv 2 \bmod 4$, die aber keine Lösung besitzt.

Fall 3: $d \equiv 0 \bmod 4$

3.1: $d \equiv 4 \bmod 8$

Die Aussagen im Fall $d \equiv 2, 3 \bmod 4$ gelten auch hier.

Beweis: An Quadraten mod 8 gibt es nur $0, 1, 4$. Aus $N(z) = 1 - d$ erhält man im vorliegenden Fall $u^2 \equiv 4v^2 - 3 \bmod 8$. Einsetzen der möglichen Quadrate zeigt, daß $u^2 \equiv v^2 \equiv 1 \bmod 8$ sein muß, d.h. u und v sind ungerade. Die Aussage (ii) des Falls 1 ist von allgemeiner Natur.

3.2: $d \equiv 0 \bmod 8$

Für jede Lösung ist u ungerade, weiterhin ist p ungerade.

Der Beweis erfolgt aus der Betrachtung von $N(z) = 1 - d$ und $N(s) = 1$ modulo 8.

3.2.1: q gerade

In einer Lösungsschar haben alle Koeffizienten v diesselbe Parität. Beide Fälle treten auf. Ist $d - 1$ eine Primzahl, so sind für alle Lösungen die Koeffizienten ungerade. In den Lösungsscharen von $1 + \sqrt{d}$ und $(\sqrt{d} - 1)s$ sind alle Koeffizienten ungerade.

Beweis: Für $zs = u' + v'\sqrt{d}$ ergibt sich $v' = pv + qu \equiv v \bmod 2$. Die Koeffizienten von $(\sqrt{d} - 1)s$ sind ungerade. Nach Satz 11 gibt es keine weiteren Scharen, falls $d - 1$ eine Primzahl ist. Für $d = 56$ berechnet man $s = 15 + 2\sqrt{56}$ und u. a. eine Anfangslösung $z = 13 + 2\sqrt{56}$.

3.2.2: q ungerade

In jeder Lösungsschar gibt es eine kleinste Lösung z_1 mit ungeraden Koeffizienten. Alle anderen erhält man in der Form $z_1 \cdot s^{2m}$, $m \geq 0$.

Beweis: Wir wissen bereits, daß stets der Koeffizient u ungerade ist, ebenso p. Für $zs = u' + v'\sqrt{d}$ gilt $v' \equiv v + 1 \bmod 2$. Hat die Anfangslösung z ungerades v, so ist $z_1 = z$; im anderen Fall haben wir $z_1 = zs$. Für $d = 8$ ist $s = 3 + \sqrt{8}$, $z = 1 + \sqrt{8}$ und $w = -\bar{z}s = 5 + 2\sqrt{8}$ sind die einzigen Anfangslösungen. Im zweiten Fall folgt $z_1 = 31 + 11\sqrt{8}$.

Abschließend fassen wir die obigen Ergebnisse für die Lösbarkeit der Gleichung

$$n(n+1) = dk(k+1) \tag{2}$$

zusammen.

Satz 12: *Ist $d > 1$, d keine Quadratzahl, so hat (2) unendlich viele Lösungen. Die Lösungen zerfallen in endlich viele Lösungsscharen. In jeder Lösungsschar gibt es eine kleinste Lösung (n_0, k_0), aus der sich die anderen Lösungen wie folgt ableiten:*

$$2n + 1 + (2k+1)\sqrt{d} = \left(2n_0 + 1 + (2k_0 + 1)\sqrt{d}\right) t^m, \quad m \geq 0$$

wobei $t = s$ ist, außer im Fall $d \equiv 0 \bmod 8$, q ungerade, in dem $t = s^2$ gilt.

Für die aktuelle Berechnung kann man die Verfahren aus Abschnitt 4 verwenden.

8 Der Fall $d = e^2$

Zu untersuchen bleibt noch der Fall, daß $d = e^2$ eine Quadratzahl > 1 ist. Gleichung (3) erhält dann die Form

$$u^2 - e^2v^2 = 1 - e^2. \tag{12}$$

Es sei daran erinnert, daß wir ungerade Lösungen $u, v \geq 3$ suchen. (12) läßt sich umformen zu

$$u^2 - e^2(v^2 - 1) = 1, \tag{12a}$$

sowie zu

$$e^2 - 1 = (ev + u)(ev - u). \tag{12b}$$

Satz 13:

(i) *Die Gleichung* (12) *hat keine Lösung mit* $u > e^2 - 2$ *oder* $v \geq e$. *Daher hat* (2) *höchstens endlich viele Lösungen, wenn d eine Quadratzahl ist.*

(ii) *Für* $e = p^r$, *p eine Primzahl, besitzt* (2) *keine Lösung, für* $e = 2v$, *v ungerade* ≥ 3, *hat* (2) *die Lösung* $n = v^2 - 1$, $k = (v - 1)/2$.

Beweis: Aus (12b) folgt im Falle der Lösbarkeit $u \leq e^2 - 2$ und $v < e$. Damit ist (i) bewiesen. Zum Beweis von (ii), $e = p^r$ folgern wir (siehe [8], S. 74) zunächst aus $n(n + 1) = p^{2r}k(k + 1)$ und Teilerfremdheit von n und $n + 1$, daß $p^{2r} | n$ oder $p^{2r} | n + 1$ gelten muß. In jedem Fall ergibt sich $p^{2r} \leq n + 1$. Nach (i) mit $u = 2n + 1$ erhalten wir in $2n + 1 \leq p^{2r} - 2$ einen Widerspruch dazu. Die Aussage für $e = 2v$ ergibt sich durch Einsetzen und wurde bereits im Abschnitt 3 erwähnt. □

Um weitere Aussagen über Lösbarkeit und Lösungen zu erhalten, betrachten wir die Gleichung (12a) als Pellsche Plus-Gleichung für die Unbekannten u, e und $d = v^2 - 1$. Für $v \geq 2$ ist bekanntlich d kein Quadrat. Aus $N(v + \sqrt{v^2 - 1}) = 1$ erhält man $z_0 = v + \sqrt{v^2 - 1}$ als Grundeinheit, und $u + e\sqrt{v^2 - 1}$ erweist sich als Potenz von z_0. Wir setzen

$$u_m(v) + e_m(v)\sqrt{v^2 - 1} = \left(v + \sqrt{v^2 - 1}\right)^m, \quad m \geq 0. \tag{13}$$

Nach den Überlegungen im Abschnitt 4 haben wir mehrere Möglichkeiten, $u_m(v)$ und $e_m(v)$ auszurechnen. Zunächst erhalten wir aus der Anwendung der Konjugation in $\mathbb{Z}[\sqrt{v^2 - 1}]$ die Formeln ($m \geq 0$)

$$\begin{aligned} u_m(v) &= \frac{\left(v + \sqrt{v^2 - 1}\right)^m + \left(v - \sqrt{v^2 - 1}\right)^m}{2}, \\ e_m(v) &= \frac{\left(v + \sqrt{v^2 - 1}\right)^m - \left(v - \sqrt{v^2 - 1}\right)^m}{2\sqrt{v^2 - 1}}. \end{aligned} \tag{14}$$

Als Funktion von v lassen sich u_m und e_m durch Polynome beschreiben, und zwar durch die wohlbekannten Tschebyscheff-Polynome 1. und 2. Art, die von großer Bedeutung für

die Numerik und Approximationstheorie sind, vgl. [4], S. 84 ff, 277 ff. Die folgenden Aussagen ergeben sich unmittelbar aus (14), vgl. auch [4], loc. cit.

$$\begin{aligned} &\text{(i)} \quad e_n(u_m(v))e_m(v) = e_{nm}(v), \quad n, m \geq 0, \\ &\text{(ii)} \quad e_m(v)v - u_m(v) = e_{m-1}(0), \quad m \geq 1, \\ &\qquad e_m(v)v + u_m(v) = e_{m+1}(v), \quad m \geq 0. \end{aligned} \tag{15}$$

Die Grundeinheit $v + \sqrt{v^2 - 1}$ liefert nach den Überlegungen in Abschnitt 4, daß $u_m(v)$ und $e_m(v)$ die Rekursionsformel

$$a_m = 2va_{m-1} - a_{m-2}, \quad m \geq 2. \tag{16}$$

mit den Anfangsbedingungen $u_0 = 1$, $u_1 = v$, $e_0 = 0$, $e_1 = 1$ erfüllt. Alternativ lassen sich $u_m(v)$ und $e_m(v)$ wie folgt beschreiben:

$$\begin{pmatrix} u_m(v) \\ e_m(v) \end{pmatrix} = \begin{pmatrix} v & v^2 - 1 \\ 1 & v \end{pmatrix}^m \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad m \geq 0 \tag{17}$$

Ist v ungerade, so ist wegen (12a) auch u ungerade. Für $m \geq 2$, $v \geq 3$ sieht man $u_m(v) \geq 3$, $e_m(v) > 1$.

Der Beweis des folgenden Satzes ergibt sich direkt aus den obigen Überlegungen und (15), (ii).

Satz 14: *Sei* $d = e^2 > 1$.

(i) *Die Gleichung* $n(n+1) = dk(k+1)$ *hat genau dann eine Lösung, wenn* $e = e_m(v)$ *für ein ungerades* $v \geq 3$ *und* $m \geq 2$ *ist.*

(ii) *Ist* $e = e_m(v)$, v *ungerade,* $v \geq 3$, $m \geq 2$, *dann ist* $(u_m(v), v)$ *eine Lösung von* (12), *und die Faktorisierung in* (12*b*) *ist von der Form* $e^2 - 1 = e_{m+1}(v) \cdot e_{m-1}(v)$.

Für $m = 2$ erhält man $u_2(v) = 2v^2 - 1$, $e_2(v) = 2v$. Daraus ergibt sich noch einmal die Existenz von Lösungen für $e = 2v$, v ungerade, $v \geq 3$.

In der Tabelle 3 sind die Werte $e_m(v)$ für $2 \leq m \leq 7$ und $3 \leq v \leq 15$ mit zugehörigen $u = u_m(v)$ (unter $e_m(v)$) angegeben.

Die Kettenbruchentwicklung von $\sqrt{2}$ liefert die Näherungsbrüche 1, 3/2, 7/5, 17/12, 41/29, 99/70 ... Bezeichnen wir den Zähler des i-ten Näherungsbruches mit p_i, so fällt auf, daß $u_m(3) = p_{2m}$. Der Beweis für diese Beziehung folgt aus dem Vergleich der Rekursionsformel für $u_m(v)$ und p_i. Es lassen sich weitere Zusammenhänge zu Kettenbruchentwicklungen entdecken, denen wir aber hier nicht nachgehen wollen.

Zu $d = e^2$ existieren offenbar genau dann weitere Lösungen von Gleichung (12) und somit von Gleichung (2), wenn der Wert e mehrfach in der Tabelle der $e_m(v)$ enthalten ist. Um solche Werte zu finden, betrachten wir zunächst die $e_m(v)$ modulo 4. Aus der Rekursionsformel ergibt sich unabhängig von v:

$$e_{m+4} = 2ve_{m+3} - e_{m+2} = 2v(2ve_{m+2} - e_{m+1}) - 2ve_{m+1} + e_m \equiv e_m \bmod 4.$$

$v\backslash m$	2	3	4	5	6	7
3	6	35	204	1189	6930	40391
	17	99	577	3363	19601	114243
5	10	99	980	9701	96030	950599
	49	485	4801	47525	470449	4656965
7	14	195	2716	37829	526980	7338631
	97	1351	18817	262087	3650401	50843527
9	18	323	5796	104005	1866294	33489287
	161	2889	51841	930249	16692641	299537289
11	22	483	10604	232805	5111106	112211527
	241	5291	116161	2550251	55989361	1229215691
13	26	675	17524	454949	11811150	306634951
	337	8749	227137	5896813	153090001	3974443213
15	30	899	26940	807301	24192090	724955399
	449	13455	403201	12082575	362074049	10850138895

Tabelle 3: Die Werte $e_m(v)$ und $u_m(v)$

Weiter gilt

$$e_0 \equiv 0 \bmod 4,$$

$$e_1 \equiv 1 \bmod 4,$$

$$e_2 = 2ve_1 - e_0 \equiv 2v \equiv 2 \bmod 4$$

$$e_3 = 2ve_2 - e_1 \equiv -e_1 \equiv 3 \bmod 4.$$

Somit ist $e_m(v) \equiv m \bmod 4$ für alle ungeraden v und alle m. Nun enthält die Spalte $m = 2$ der Tabelle 3 genau alle natürlichen Zahlen größer oder gleich 6, die kongruent zu 2 modulo 4 sind. Somit muß jeder Wert $e_m(v)$ mit $m \equiv 2 \bmod 4$ auch in der Spalte $m = 2$ auftauchen. Genauer gilt nach diesen Überlegungen

Satz 15: *Ist* $m \equiv 2 \bmod 4$, *so gilt* $e_m(v) = e_2(v')$ *mit* $v' = e_m(v)/2$.

Zu jedem Wert e, der in Tabelle 3 in einer der Spalten mit $m = 6, 10, 14, \ldots$ zu finden ist, hat also Gleichung (12) und folglich Gleichung (2) mindestens 2 Lösungen. Der kleinste derartige Wert ist $e_6(3) = 6930 = e_2(3465)$.

$d = 6930^2 = 48024900$ ist demnach die kleinste Quadratzahl, für welche die Gleichung $u^2 - dv^2 = 1 - d$ zwei verschiedene Lösungen hat, nämlich $(u_1, v_1) = (19601, 3)$ und $(u_2, v_2) = (24012449, 3465)$. Unsere Ausgangsgleichung $n(n+1) = d \cdot k(k+1)$ hat entsprechend die Lösungen $(n_1, k_1) = (9800, 1)$ und $(n_2, k_2) = (12006224, 1732)$. Weitere Lösungen existieren für diesen Wert von d nicht.

Wir haben somit unendlich viele Quadrate ermittelt, für die Gleichung (2) zwei Lösungen hat. Ob es weitere Quadratzahlen mit dieser Eigenschaft oder sogar Quadratzahlen mit drei oder mehr Lösungen gibt, sind offene Fragen. Systematische Suche mit dem Computer hat ergeben, daß in jedem Fall $d \geq 36 \cdot 10^{26}$ sein müßte. Bei dieser Suche

haben sich (15), (i) und die folgenden, direkt zu verifizierenden Aussagen als nützlich erwiesen:

$$\text{(i)} \quad e_m(v) \equiv \begin{cases} m \bmod 32 & \text{falls } m \text{ ungerade,} \\ m \cdot v \bmod 32 & \text{sonst.} \end{cases} \tag{18}$$

$$\text{(ii)} \quad \frac{(v-1)^m - 1}{2v} < e_m(v) < \frac{(2v)^m}{2(v-1)}, \quad m \geq 0.$$

Literatur

[1] Armstrong, R. und Pederson, P. (editors), Comprehensive School Mathematics Programm, Probability and Statistics, CEMREL Inc, 1982.

[2] Knuth, D.E., The Art of Computer Programming, 2d ed., Addison-Wesley 1981.

[3] Mosteller, F., Fifty Challenging Problems in Probability with Solutions, Addison-Wesley, 1965.

[4] Müller, M. W., Approximationstheorie, Akad. Verlagsgesellschaft 1978.

[5] Ryden, R., Nearly Isosceles Pythagorean Triples, Mathematics Teacher 76, January 1983, 52–56.

[6] Scheid, H., Zahlentheorie, BI Wissenschaftsverlag, 1991.

[7] Shanks, D., Solved and Unsolved Problems in Number Theory, 2d ed., Chelsea Publ. Company 1978.

[8] Sierpinski, W., 250 Problems in Elementary Number Theory, Elsevier Publ. Company 1970.

[9] Weil, A., Zahlentheorie – Ein Gang durch die Geschichte, Birkhäuser, 1992.

Eberhard Becker, Robert Robson, Georg Schrage
Fachbereich Mathematik
Universität Dortmund
D-44221 Dortmund