Reguläre Kettenbrüche und quadratische diophantische Probleme

Autor(en): **Läuchli, Peter**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **35 (1980)**

Heft 4

PDF erstellt am: **30.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-34683

inequality (2), this case reduces to the problem of establishing the following inequality:

$$\prod(a_i-\omega)\leqslant\prod(a_i/2). \tag{**}$$

However, we have not been able to establish either of (*) or (**).
There exist in the plane of (T) points P such that $\prod\beta_i=\prod(a_i-\beta_i)$. For such points, inequality (*) is easily verified. Examples of such points are the orthocenter and the circumcenter, when (T) is acute, and the incenter. This suggests the following problem which appears to be of interest.

Problem: Find all points interior to (T) such that $\prod\beta_i=\prod(a_i-\beta_i)$, and discuss any special properties of the set of all such points.
Finally we note that, if in (*) the values of the angles are replaced by the sines of these angles, then the resulting inequalities are much easier. Indeed, the same method used above gives,

$$\prod\sin\beta_i\leqslant\prod\sin(a_i/2). \tag{4}$$

In particular if, in (4), P is taken to be the orthocenter, we get

$$\prod\cos(a_i)\leqslant\prod\sin(a_i/2). \tag{5}$$

Faruk F. Abi-Khuzam, American University of Beirut

Elementarmathematik und Didaktik

Reguläre Kettenbrüche und quadratische diophantische Probleme

Einleitung

Die Theorie der regulären Kettenbrüche, zeitweise etwas in Vergessenheit geraten, hat doch immer wieder das Interesse der Mathematiker gefesselt und auch Anregung zum Experimentieren geboten. Verschiedene recht einfach zu formulierende Resultate eignen sich vorzüglich zu einer Behandlung im Rahmen der Elementarmathematik. Wir besprechen hier zwei Anwendungen auf quadratische diophantische Probleme, nämlich 1. die Pellsche Gleichung, welche in der Theorie der quadratischen diophantischen Gleichungen mit zwei Unbekannten eine zentrale Rolle spielt, sowie 2. einen etwas ungewohnten Aspekt der pythagoreischen Zahlen, d.h. der ganzen Zahlen, welche Seitenlängen von rechtwinkligen Dreiecken darstellen.
Bei diesem Aufsatz handelt es sich um eine völlig umgeschriebene und stark

gekürzte Version einer früheren Arbeit des Verfassers [3], wobei auch einige neue Gesichtspunkte hinzugekommen sind. Für Details und Beweise muss auf diese Quelle sowie auf Perron [4] verwiesen werden, der insbesondere viele elegante Herleitungen unter Benützung von konjugierten Zahlen bringt. Dort findet man auch viel Material über die Pellsche Gleichung, weiteres elementar und sehr ansprechend dargeboten bei Gelfond [1], von einem computerorientierten Standpunkt aus betrachtet bei Kirch [2]. Die Ursprünge in der griechischen Mathematik verfolgt ausführlich van der Waerden [5].

1. Problemstellung

Problem: Wir suchen ein gleichschenklig-rechtwinkliges Dreieck mit rationalen Seitenverhältnissen oder, in zahlentheoretischer Formulierung, positive ganzzahlige Lösungen des Gleichungssystems

$$x^2+y^2=z^2, \qquad (*)$$

$$x=y. \qquad (**)$$

Offensichtlich besitzt dieses Problem keine Lösungen. Wir betrachten deshalb Modifikationen in zwei Richtungen:

1.
(*) «beinahe erfüllt», d.h.

$$x^2+y^2\pm 1=z^2.$$

(**) bleibt, also:

$$z^2-2x^2=\pm 1.$$

2.
(**) «beinahe erfüllt», d.h.

$$x\pm 1=y.$$

(*) bleibt, also:

$$x^2+(x\pm 1)^2=z^2.$$

Für beide Fälle existieren nun Lösungen, sogar unendlich viele:

z	1	3	7	...
x	1	2	5	...

x	3	21	119	...
y	4	20	120	...
z	5	29	169	...

Um etwas interessantere Fragestellungen zu erhalten, wollen wir sofort verallgemeinern:

1. Mit geläufigeren Variablenbezeichnungen lautet die Gleichung: $x^2-2y^2=\pm 1$ oder nun allgemeiner:

$$x^2-Dy^2=\pm 1, \qquad D>0, \qquad \text{ganz, kein Quadrat.}$$

(Falls D Quadratzahl ist, existieren nur triviale Lösungen.) Diese Gleichung wird seit Euler *Pellsche Gleichung* genannt. Der Spezialfall $D=2$ war schon den Pythagoreern wohlbekannt (siehe [5]): Wenn x, y die Länge der Diagonale bzw. Seite eines Quadrates darstellen, dann auch $x'=x+2y$, $y'=x+y$. Diese Tatsache lässt vermuten, dass dieselbe Rekursion auch für die Lösungen der Pellschen Gleichung (mit $D=2$) gilt, was sehr leicht zu verifizieren ist. Und im allgemeinen Fall kommt man, wegen $x^2/y^2=D\pm 1/y^2$, bald einmal auf die Idee, es mit rationalen Approximationen x/y für $\sqrt{D}$ zu versuchen. In 3.2 werden wir darauf zurückkommen.

2. Hier lautet unsere Verallgemeinerung: Gesucht sind positive ganzzahlige Lösungen der Gleichung $x^2+y^2=z^2$ derart, dass das Verhältnis y/x möglichst nahe bei einem gegebenen rationalen Verhältnis u/v liegt, d.h. pythagoreische Zahlen, welche die Seiten eines rechtwinkligen Dreiecks mit gegebenen Winkeln (mit rationalem Tangens) approximieren. (u^2+v^2 soll kein Quadrat sein, da sonst $x=v$, $y=u$ das Approximationsproblem exakt lösen.) Es zeigt sich, dass sich jedes gegebene Seitenverhältnis durch genügend grosse pythagoreische Zahlen (p.Z.) beliebig genau annähern lässt. (Was heisst dies, wenn man einen beliebigen Strahl durch den Nullpunkt und das ganzzahlige Punktegitter betrachtet?)
Durch einen bekannten einfachen Kunstgriff lässt sich nun die Bedingung, wonach unsere Lösungen p.Z. sein sollen, eliminieren: Aus den Zahlenpaaren p, q mit $p>q>0$; p, q teilerfremd; $p-q$ ungerade erhält man mit

$$x=p^2-q^2; \qquad y=2pq; \qquad z=p^2+q^2$$

genau die Menge der irreduziblen p.Z. mit geradem y. (Bei irreduziblen p.Z., d.h. solchen ohne gemeinsamen Teiler, ist z immer ungerade.) Sei ferner φ ein Winkel im gegebenen Dreieck, also etwa $u/v=\tan\varphi$. Der entsprechende Winkel im approximierenden Dreieck sei a: $y/x=\tan a$. Mit $t=q/p$ gilt dann

$$\tan a=y/x=2pq/(p^2-q^2)=2t/(1-t^2),$$

also $t=\tan(a/2)$. Entsprechend mit $s=\tan(\varphi/2)$: $u/v=2s/(1-s^2)$ oder durch Auflösen der quadratischen Gleichung:

$$s=\left(-v+\sqrt{u^2+v^2}\right)/u=u/\left(v+\sqrt{u^2+v^2}\right).$$

(Die andere Lösung ist negativ.)

Damit drängt sich folgendes Vorgehen auf:
— Berechne s aus den gegebenen u, v.
— Approximiere das irrationale s durch ein q/p (ohne Nebenbedingung).

Es hat sich gezeigt, dass für die Lösung der beiden gestellten Aufgaben die regulären Kettenbrüche ein äusserst elegantes Instrument liefern. Daher sollen zunächst einige Grundlagen zusammengestellt werden.

2. Aus der Kettenbruch-Theorie

2.1 *Der reguläre Kettenbruch*

Man nennt einen Ausdruck der folgenden Art einen endlichen *regulären Kettenbruch* (r.Kb.) und benützt mit Vorteil gerade eine abgekürzte Schreibweise:

$$[b_0, b_1, \ldots, b_n] := b_0 + 1/(b_1 + 1/(b_2 + \cdots + 1/b_n)) \ldots),$$

wobei die b_i ganzzahlig sind, und $b_0 \geqslant 0$, $b_i > 0$ $(i = 1, 2, \ldots)$.
Durch «Aufrollen» von rechts her, d.h. sukzessives Erweitern mit dem jeweils letzten Nenner, kann der Ausdruck auf einen einzigen Bruch A_n/B_n reduziert werden. Man nennt den Zähler A_k bzw. den Nenner B_k eines Anfangsstückes $[b_0, \ldots, b_k]$ des r.Kb. den k-ten Näherungszähler bzw. -nenner und A_k/B_k den k-ten Näherungsbruch. Die A_k, B_k können sehr bequem rekursiv berechnet werden, wobei man die Verankerung zweckmässigerweise schon beim Index -2 beginnen lässt:

$$\left.\begin{array}{l} A_{-2} := 0; \qquad A_{-1} := 1; \qquad B_{-2} := 1; \qquad B_{-1} := 0. \\ \text{Für} \quad k = 0, 1, \ldots: \\ A_k := b_k A_{k-1} + A_{k-2}; \\ B_k := b_k B_{k-1} + B_{k-2}. \end{array}\right\} \tag{2.1.1}$$

Die Folgen der A_k, B_k wachsen monoton. Ferner gilt:

$$A_{k-1} B_k - A_k B_{k-1} = (-1)^k;$$

woraus folgt, dass die A_k, B_k teilerfremd sind und dass

$$A_{k-1}/B_{k-1} - A_k/B_k = (-1)^k/(B_{k-1} B_k).$$

Daraus ist wiederum ersichtlich, dass für jeden unendlichen r.Kb. $[b_0, b_1, \ldots]$ die Folge der Werte seiner Näherungsbrüche konvergiert; den Grenzwert bezeichnet man als Wert des unendlichen r.Kb.
Bildet man, ausgehend von einem reellen $\xi_0 > 0$ für $k = 0, 1, \ldots$ die Grössen

$$b_k := \lfloor \xi_k \rfloor; \qquad \xi_{k+1} := 1/(\xi_k - b_k)^{1)},$$

dann brechen diese Folgen genau dann nicht ab, wenn ξ_0 irrational ist, und es gilt dann $\xi_0 = [b_0, b_1, \ldots]$. Diese Entwicklung einer irrationalen Zahl in einen r.Kb. ist eindeutig. Wir bemerken noch, dass für alle k gilt:

1) Wir verwenden, um Verwechslungen mit der Kb.-Notation auszuschliessen, die Bezeichnung $\lfloor x \rfloor$ für die grösste ganze Zahl, welche x nicht übertrifft.

$$\xi_0=[b_0,\ldots,b_{k-1},\xi_k]; \qquad \xi_k=[b_k,b_{k+1},\ldots].$$

Für rationale ξ_0 erhält man einen endlichen r.Kb. Die Entwicklung wird dann besser als euklidischer Divisionsalgorithmus angesetzt; sie ist auch eindeutig bis auf die triviale Umformung am Schluss: $[b_0,\ldots,b_n,1]=[b_0,\ldots,b_n+1]$.

2.2 *Periodische reguläre Kettenbrüche*

Für periodische r.Kb. verwenden wir, in Analogie zu den Dezimalbrüchen, eine Notation mit offensichtlicher Bedeutung:

$$\xi_0=[b_0,b_1,\ldots]=[b_0,\ldots,b_{h-1},\overline{b_h,\ldots,b_{h-1+r}}],$$

wobei h, r immer die kleinsten Zahlen sein sollen, so dass für alle $k\geqslant h$: $b_{k+r}=b_k$. Euler hat festgestellt, dass ξ_0 in diesem Falle eine irrationale Lösung einer quadratischen Gleichung mit ganzzahligen Koeffizienten, eine sogenannte *quadratische Irrationalität*, ist, sich also in der Form

$$\xi_0=(P+\sqrt{D})/Q; \qquad P,Q,D \text{ ganz } Q\neq 0; \qquad D>0, \qquad \text{kein Quadrat},$$

darstellen lässt. Die andere Lösung der Gleichung, $\eta_0=(P-\sqrt{D})/Q$, nennt man die zu ξ_0 konjugierte Zahl.

Um umgekehrt eine quadratische Irrationalität in einen r.Kb. zu entwickeln, soll vorausgesetzt werden, dass $Q\,|\,D-P^2$. (Dies kann nötigenfalls durch Erweitern des ξ_0 darstellenden Bruches mit $|Q|$ erzwungen werden.) Dann gibt es für $k=0,1,\ldots$ ganzzahlige P_k, Q_k; $Q_k\neq 0$, so dass

$$\xi_k=[b_k,\ldots]=(P_k+\sqrt{D})/Q_k,$$

und

$$P_k+P_{k+1}=b_kQ_k; \qquad Q_kQ_{k+1}=D-P_{k+1}^2.$$

(Beachte, dass $\xi_k=b_k+1/\xi_{k+1}$.) Aus der Tatsache, dass von einem gewissen Index an immer $0<P_k<\sqrt{D}$; $0<Q_k<2\sqrt{D}$, folgt dann die Periodizität des r.Kb. (Satz von Lagrange).

Weiter kann auch noch eine Verbindung zu den A_k, B_k gezogen werden: Mit der Definition

$$F_k(x)=(xA_{k-1}+A_{k-2})/(xB_{k-1}+B_{k-2})$$

gilt $F_k(b_k)=[b_0,\ldots,b_k]$; und für beliebiges reelles x:

$$F_k(x)=[b_0,\ldots,b_{k-1},x], \qquad \text{also} \qquad \xi_0=F_k(\xi_k).$$

Wenn man nun in

$$\xi_k = F_k^{-1}(\xi_0) = (\xi_0 B_{k-2} - A_{k-2})/(-\xi_0 B_{k-1} + A_{k-1})$$

für ξ_k und ξ_0 die entsprechenden Brüche $(P_k + \sqrt{D})/Q_k$ und $(P + \sqrt{D})/Q$ einsetzt, dann ergibt der Koeffizientenvergleich, dass sich die P_k, Q_k folgendermassen als quadratische bzw. bilineare Formen in den A_k, B_k darstellen lassen ($k = 0, 1, \ldots$):

$$Q_k = (-1)^k (A_{k-1}^2 Q - 2A_{k-1}B_{k-1}P - B_{k-1}^2 R), \tag{2.2.1}$$

$$P_k = (-1)^k \left(-A_{k-1}A_{k-2}Q + (A_{k-1}B_{k-2} + B_{k-1}A_{k-2})P + B_{k-1}B_{k-2}R\right), \tag{2.2.2}$$

mit $R = (D - P^2)/Q$.
Dazu beachte man noch, dass die Werte von A_k/B_k um ξ_0 herumpendeln und dass die quadratische Form (Gl. 2.2.1), wenn man statt A_{k-1} und B_{k-1} reelle Werte A, B mit $A/B = \xi_0$ einsetzt, verschwindet. Damit versteht man eher, dass die P_k, Q_k beschränkt bleiben, obwohl die A_k, B_k exponentiell anwachsen.

Schliesslich betrachten wir zum periodischen r.Kb.

$$\xi_0 = [b_0, \ldots, b_{h-1}, \overline{b_h, \ldots, b_{h-1+r}}]$$

den rein periodischen Teil

$$\xi_h = [\overline{b_h, \ldots, b_{h-1+r}}] = \xi_0' = [\overline{b_0', \ldots, b_{r-1}'}].$$

Wenn man die Rekursionsformeln für die A_k', B_k' (entsprechend Gl. 2.1.1) als lineare Differenzengleichungen mit variablen Koeffizienten interpretiert, dann sind die Folgen der A_k', B_k' deren Grundlösungen mit den Anfangsbedingungen $A_{-2}' = 0$, $A_{-1}' = 1$ bzw. $B_{-2}' = 1$, $B_{-1}' = 0$. Wegen der Periodizität der b_k' lassen sich nun die um r verschobenen Folgen als Lösungen derselben Differenzgleichungen, aber jetzt mit den Anfangswerten A_{r-2}', A_{r-1}' bzw. B_{r-2}', B_{r-1}' aus den obigen Grundlösungen linear kombinieren ($k \geqslant -2$):

$$\left.\begin{aligned} A_{k+r}' &= A_{r-1}'A_k' + A_{r-2}'B_k', \\ B_{k+r}' &= B_{r-1}'A_k' + B_{r-2}'B_k'. \end{aligned}\right\} \tag{2.2.3}$$

Mit derselben Überlegung lassen sich die Näherungszähler und -nenner A_k, B_k des ursprünglichen r.Kb. ξ_0 auf diejenigen von ξ_0' zurückführen ($k \geqslant h-2$):

$$\left.\begin{aligned} A_k &= A_{h-1}A_{k-h}' + A_{h-2}B_{k-h}', \\ B_k &= B_{h-1}A_{k-h}' + B_{h-2}B_{k-h}'. \end{aligned}\right\} \tag{2.2.4}$$

Unter Verwendung der beiden Gleichungspaare lässt sich das Vorwärtsspringen um eine Periode auch im r.Kb. ξ_0 bewerkstelligen. Alle diese Zusammenhänge stellen sich in der vektoriellen Schreibweise etwas eleganter dar.

2.3 *Rein periodische Kettenbrüche, Symmetrien*

Nach einem Satz von Galois ist der r.Kb. für die quadratische Irrationalität ξ_0 genau dann *rein periodisch* ($h=0$), wenn $\xi_0>1$ und $-1<\eta_0<0$ (wo η_0 wieder der konjugierte Wert ist).
Man erkennt leicht, dass diese «Galois-Bedingung» äquivalent ist mit:

$$0<\sqrt{D}-P<Q<\sqrt{D}+P.$$

Ferner vererbt sich die Gültigkeit der Bedingung mit zunehmendem k, wenn sie bei einem beliebigen r.Kb. einmal für ein Paar P_k, Q_k erfüllt war.
Wir betrachten weiter den Spezialfall eines rein periodischen r.Kb. mit *symmetrischer Periode*, d.h. $b_{r-1-k}=b_k$ $(k=0,1,\dots,r-1)$. Zunächst gilt: Das Anfangsstück $b_0,\dots,b_n$ der Koeffizientenfolge eines r.Kb. ist genau dann symmetrisch, wenn $A_{n-1}=B_n$. Angewendet auf die quadratische Gleichung für ξ_0, η_0 (bei rein periodischem r.Kb.) ergibt sich: Die Periode ist genau dann symmetrisch, wenn $\xi_0\eta_0=-1$; dies ist gleichbedeutend mit: $D-P^2=Q^2$.
Diese Symmetrie hat aber weiter die interessante Konsequenz, dass auch die Folgen der P_k, Q_k symmetrisch sind, nämlich:

$$P_{r-k}=P_k \quad (k=0,\dots,r); \qquad Q_{r-1-k}=Q_k \quad (k=0,\dots,r-1).$$

Für die Untersuchung der Periodenmitte spielt offenbar die Parität von r eine Rolle: Je nachdem, ob r ungerade oder gerade ist, sind (für $r>1$) entweder zwei aufeinanderfolgende P_k oder zwei Q_k gleich. Von praktischer Bedeutung ist nun, dass diese Erscheinung auch nicht früher auftritt:
Wenn zum erstenmal

$$P_k=P_{k+1}(k\geqslant 0), \quad \text{dann ist} \quad r=2k+1, \quad \text{wenn}$$

$$Q_k=Q_{k+1}(k\geqslant 1), \quad \text{dann ist} \quad r=2k+2$$

($r=2$ kommt nicht vor).
Damit ist es möglich, schon die Mitte der Periode zu erkennen.

3. Anwendung der Kettenbruch-Theorie

3.1 *Entwicklung einer quadratischen Irrationalität in einen regulären Kettenbruch*

Es sei deutlich festgehalten, dass für die Aufgabe, aus einer quadratischen Irrationalität (definiert durch 3 ganze Zahlen) deren Entwicklung in einen r.Kb. (definiert durch $(h+r)$ ganze Zahlen) zu ermitteln, der Umweg über die Irrationalzahl ξ_0 selber nicht nötig ist, dass vielmehr die ganze Rechnung ganzzahlig durchgeführt werden kann. (Auch für die Berechnung von $\lfloor\sqrt{D}\rfloor$ muss natürlich der Bereich der ganzen Zahlen nicht verlassen werden.) Wenn man noch beachtet, dass für a,b ganz, $b\neq 0$, $0<\eta<1$ gilt:

$$\lfloor (a+\eta)/b \rfloor = \begin{cases} \lfloor a/b \rfloor, & \text{falls} \quad b>0 \\ \lfloor (a+1)/b \rfloor, & \text{falls} \quad b<0, \end{cases}$$

dann kommt man mit den in 2.2 angegebenen Beziehungen, und nachdem nötigenfalls $Q \mid D-P^2$ erzwungen wurde, auf die folgende Rekursion:

$$\left.\begin{aligned} & P_0 := P; \qquad Q_0 := Q; \qquad w := \lfloor \sqrt{D} \rfloor. \\ & \text{Für} \quad k=0,1,\ldots: \\ & \qquad b_k := \begin{cases} \lfloor (P_k+w)/Q_k \rfloor, & \text{falls} \quad Q_k>0 \\ \lfloor (P_k+w+1)/Q_k \rfloor, & \text{falls} \quad Q_k<0; \end{cases} \\ & \qquad P_{k+1} := b_k Q_k - P_k; \qquad Q_{k+1} := (D-P_{k+1}^2)/Q_k. \end{aligned}\right\} \tag{3.1.1}$$

Dabei beachte man, dass es zur Erkennung der Länge von Vorperiode (h) und Periode (r) nicht etwa nötig ist, die b_k, P_k, Q_k alle aufzubewahren, sondern man benütze, dass für den Index h zum erstenmal die «Galois-Bedingung» erfüllt ist:

$$0 < \sqrt{D} - P_h < Q_h < \sqrt{D} + P_h$$

und dass das Periodenende erreicht ist, sobald $P_{h+r} = P_h$ und $Q_{h+r} = Q_h$.
Ein Zahlenbeispiel zur Illustration:

$$P=1, \qquad Q=12, \qquad D=37 \qquad (w=6, h=2, r=3).$$

Die Bedingung $Q \mid D-P^2$ ist erfüllt.

k	-2	-1	0	1	2	3	4	5
b_k			0	1	1	2	3	1
P_k			1	-1	4	3	5	4
Q_k			12	3	7	4	3	7
A_k	0	1	0	1	1	3	10	13
B_k	1	0	1	1	2	5	17	22

Also: $\xi_0 = (1+\sqrt{37})/12 = 0.59023\ldots = [0, 1, \overline{1, 2, 3}]$.
Approximationsfehler bei $k=5$:

$$A_5/B_5 - \xi_0 = 13/22 - 0.59023\ldots = 0.00067\ldots$$

3.2 *Die Pellsche Gleichung*

Gefragt wird nach positiven ganzzahligen Lösungen der Gleichung

$$x^2 - Dy^2 = \pm 1, \qquad D>0, \qquad \text{kein Quadrat.} \tag{3.2.1}$$

Nach den Andeutungen von Abschnitt 1 wird man sich Resultate von einer r.Kb.-Entwicklung von $\sqrt{D}$ erhoffen. In der Tat gilt für diese mit $P=0$, $Q=1$:

$$A_{k-1}^2-DB_{k-1}^2=(-1)^k Q_k$$

(aus Gl. 2.2.1). Da nun aber der r.Kb. von $\sqrt{D}$ in den b_k, P_k, Q_k - bis auf b_0 und P_0 - mit dem rein periodischen r.Kb. von $w+\sqrt{D}$ übereinstimmt, erhält man wegen der Periodizität der Q_k Lösungen für $k=v\cdot r$ ($v=1,2,\ldots$). Dies sind aber auch die einzigen; somit existieren Lösungen von Gleichung 3.2.1 mit rechter Seite $+1$ für alle nichtquadratischen D, mit -1 dagegen nur, falls der r.Kb. eine Periode ungerader Länge besitzt (Beispiel: $D=2$: $r=1$; $D=3$: $r=2$). Die Gleichungen 2.2.3 lassen uns ferner plausibel erscheinen, dass eine Rekursion, wie sie in Abschnitt 1 für $D=2$ angegeben wurde, auch im allgemeinen Fall existiert. Tatsächlich gelten, wenn $x_0^2-Dy_0^2=\pm 1$, die Rekursionsformeln

$$x'=x_0x+Dy_0y; \qquad y'=y_0x+x_0y.$$

Die Symmetriebetrachtungen von Abschnitt 2.3 finden, in leicht modifizierter Form, auch hier ihre Anwendung: Unter den rein periodischen r.Kb. besitzen genau diejenigen, wo $Q\,|\,2P$, die Eigenschaft, dass die Sequenz $b_0,\ldots,b_r$ symmetrisch ist. Dies trifft offenbar für $\xi_0=w+\sqrt{D}$ zu. Es ist auch hier möglich, mit entsprechenden Überlegungen wie vorher, ein Kriterium für die Periodenmitte anzugeben. Die für die Lösung der Pellschen Gleichung benötigten A_k, B_k sind natürlich der Kb.-Entwicklung von $\sqrt{D}$ zu entnehmen.
Übungsaufgabe: Man diskutiere die beiden Spezialfälle $D=a^2+1$ und $D=a^2-1$ (für beliebiges ganzes a).
Zwei Beispiele zum Nachrechnen:
1. $D=14$:

$$\sqrt{14}=[3,\overline{1,2,1,6}], \qquad w=3, \qquad r=4,$$

$$\sqrt{14}+3=[\overline{6,1,2,1}].$$

Erste nichttriviale Lösung: $x_0=A_3=15, y_0=B_3=4$.
Rekursion: $x'=15x+56y, y'=4x+15y$.

x	15	449	13455	...
y	4	120	3596	...
x^2-Dy^2	1	1	1	...

2. $D=13$:

$$\sqrt{13}=[3,\overline{1,1,1,1,6}], \qquad w=3, \qquad r=5,$$

$$\sqrt{13}+3=[\overline{6,1,1,1,1}].$$

Erste nichttriviale Lösung: $x_0 = A_4 = 18, y_0 = B_4 = 5$.
Rekursion: $x' = 18x + 65y, y' = 5x + 18y$.

x	18	649	23382	...
y	5	180	6485	...
$x^2 - Dy^2$	-1	1	-1	...

3.3 *Pythagoreische Zahlen*

Die Problemstellung lautet hier:
Gegeben: $u, v > 0$, ganz, teilerfremd, $u^2 + v^2$ kein Quadrat.
Gesucht: positive ganzzahlige Lösungen von $x^2 + y^2 = z^2$, so dass y/x möglichst nahe bei u/v liegt.
Wie in Abschnitt 1 ausgeführt, approximieren wir $s = (-v + \sqrt{u^2 + v^2})/u$ durch rationale q/p und bilden dann

$$x = p^2 - q^2; \qquad y = 2pq; \qquad z = p^2 + q^2.$$

Jetzt liegt es nahe, die quadratische Irrationalität s in einen periodischen r.Kb. zu entwickeln und die A_k, B_k als q und p zu nehmen. Etwas schöner wird die Entwicklung bei $1/s = (v + \sqrt{u^2 + v^2})/u$, da dann offensichtlich die «Galois-Bedingung» (Abschnitt 2.3) erfüllt und damit der r.Kb. rein periodisch ist. Ferner gilt die Symmetriebedingung, da $P = v$, $Q = u$, $D = u^2 + v^2$. (Auch $Q \mid D - P^2$ ist hier immer erfüllt.)
Der Übergang von s auf $1/s$ fällt nicht ins Gewicht; er bedeutet im wesentlichen eine Vertauschung der Näherungszähler und -nenner. Man wird dann also als Lösungen

$$x_k = A_k^2 - B_k^2; \qquad y_k = 2A_k B_k; \qquad z_k = A_k^2 + B_k^2 \tag{3.3.1}$$

bilden, sofern $A_k - B_k$ ungerade ist, da ja sicher nur irreduzible p.Z. interessieren. (Man überlege sich, dass nie zwei aufeinanderfolgende Paare A_k, B_k eine gerade Differenz besitzen!) Die Frage, in welchem Sinne man mit diesem Verfahren alle «besten» Approximationen für das Verhältnis u/v erhält, erfordert etwas subtilere Überlegungen (siehe [3]). Hier sei nur soviel bemerkt, dass man bei Vertauschung von u und v im allgemeinen durchaus andere p.Z. erhält.
Für die Durchführung der Rechnung benötigt man $w = \lfloor \sqrt{D} \rfloor$. Vielleicht ist es nicht ganz selbstverständlich, dass auch im ganzzahligen Falle die quadratisch konvergente Newton-Methode funktioniert. Es gilt nämlich (siehe [3]) für beliebige ganze $a > 0$: Sei

$$X_0 := a; \qquad Y_0 := 1;$$

$$X_{i+1} := \lfloor (X_i + Y_i)/2 \rfloor; \qquad Y_{i+1} := \lfloor a/X_{i+1} \rfloor \qquad (i = 0, 1, \ldots).$$

Dann ist $X_n = \lfloor \sqrt{a} \rfloor$, wo $n =$ kleinster Index i, für welchen $X_i \leqslant Y_i$.
So kommen wir auf folgenden Algorithmus zur Bestimmung der r.Kb.-Entwicklung

von $1/s$ bis zur Periodenmitte, wobei die P_k, Q_k selbstverständlich nicht aufbewahrt werden müssen, sondern es genügt, das aktuelle Paar P, Q und die neuen Werte P', Q' mitzuführen. (Für die ganzzahlige Division wurde die Bezeichnung $a\,\mathbf{div}\,b := \lfloor a/b \rfloor$ verwendet):

Eingabe (u, v); $D := u*u+v*v$;
Quadratwurzel nach Newton:
$x := D$; $y := 1$;
Wiederhole $x := (x+y)\,\mathbf{div}\,2$; $y := D\,\mathbf{div}\,x$ solange bis $x \leqslant y$;
$w := x$;
Initialisieren:
$k := -1$; $P' := v$; $Q' := u$;
Rekursion:
Wiederhole
$k := k+1$; $P := P'$; $Q := Q'$;
$b := (P+w)\,\mathbf{div}\,Q$;
$P' := b*Q-p$; $Q' := (D-P'*P')\,\mathbf{div}\,Q$;
Ausgabe (k, b)
solange bis $(P=P')$ oder $(Q=Q')$;
Berechnung der Periodenlänge:
Falls $(P=P')$, dann $r := 2*k+1$, sonst $r := 2*k+2$; Ausgabe (r)

Wie schon früher bemerkt, bleiben die P_k, Q_k (und damit natürlich auch b_k), im Gegensatz zu den A_k, B_k, beschränkt:

$$0 < P_k \leqslant w; \qquad 0 < Q_k,\ b_k \leqslant 2w.$$

Die Berechnung der x_k, y_k, z_k hätte nach Gleichungen 2.1.1 und 3.3.1 zu geschehen. Ein Beispiel möge das bisherige illustrieren:

$$u=10, \qquad v=3 \qquad (D=109, w=10, r=7).$$

k	-2	-1	0	1	2	3	4	5	6
b_k			1	2	1	9	1	2	1
P_k			3	7	5	9	9	5	7
Q_k			10	6	14	2	14	6	10
A_k	0	1	1	3	4	39	43	125	168
B_k	1	0	1	2	3	29	32	93	125
x_k			*	5	7	*	825	*	12599
y_k			*	12	24	*	2752	*	42000
z_k			*	13	25	*	2873	*	43849
$\frac{y_k}{x_k} - \frac{u}{v}$			*	$-9.3E$-1	$9.5E$-2	*	$2.4E$-3	*	$2.6E$-4

Zum Schluss noch ein Hinweis auf den Spezialfall konstanter b_k (d.h. $r=1$): $1/s=[\bar{b}]=[b,b,\ldots]$. Einsetzen im Kb. führt auf $1/s=b+1/(1/s)$ und damit schliesslich auf die beiden Möglichkeiten (da $(u,v)=1$ vorausgesetzt):

$$u=1, \quad v \text{ beliebig}, \quad b=2v,$$

$$u=2, \quad v \text{ ungerade}, \quad b=v.$$

In diesem Falle gilt:

$$y_k/(x_k+(-1)^k)=u/v.$$

(Folgt aus Gl. 2.2.1; vgl. auch Einführungsbeispiel in Abschnitt 1.)
Beispiele:

$$u=2, \quad v=1: \quad b=1, \quad 1/s=(1+\sqrt{5})/2.$$

(Die A_k, B_k bilden, um eine Position gegeneinander verschoben, je die Folge der Fibonaccizahlen.)

$$u=v=1: \quad b=2, \quad 1/s=1+\sqrt{2}.$$

(Beispiel aus Abschnitt 1.)

Peter Läuchli, ETH Zürich

LITERATURVERZEICHNIS

1 Gelfond, A.O.: Die Auflösung von Gleichungen in ganzen Zahlen. Deutscher Verlag der Wissenschaften, Berlin 1973.
2 Kirch, A.M.: Elementary Number Theory, A Computer Approach. Intext Educational Publishers, New York 1974.
3 Läuchli, P.: Ein Problem der ganzzahligen Approximation. Berichte des Instituts für Informatik, Nr. 22. ETH Zürich 1977.
4 Perron, O.: Die Lehre von den Kettenbrüchen, Bd. 1. Teubner, Stuttgart 1954.
5 Van der Waerden, B.L.: Erwachende Wissenschaft, 2. Aufl. Birkhäuser, Basel 1966.

Aufgaben

Aufgabe 825. Es sei N eine natürliche Zahl. Für $n=1,2,\ldots,2N$ sei $f(n)$ definiert durch

$$f(n)=\binom{2N}{n}^{-1}\sum_{k=0}^{n}\left|\frac{n-2k}{n}\right|\binom{N}{k}\binom{N}{n-k}.$$