A.O. Gelfond

Die Auflösung von Gleichungen in ganzen Zahlen

Übersetzung: Gerhard Ränike
1960 Deutscher Verlag der Wissenschaften
MSB: Nr. 22
Abschrift und LaTex-Satz: 2021

Vorwort

Grundlage dieses Buches ist ein Vortrag über Diophantische Gleichungen, den ich im Jahre 1951 auf der mathematischen Olympiade in der Moskauer Staatlichen Universität gehalten habe.

Ich möchte an dieser Stelle meinem Schüler, Doz. N. M. Kopobow, danken, der den ersten, den zweiten und einen Teil des dritten Paragraphen nach dem Konzept meiner Lektion geschrieben hat.

Das Büchlein ist für Schüler der höheren Klassen von Oberschulen gedacht.

A. Gelfond

Inhaltsverzeichnis

Einleitung

Die Zahlentheorie untersucht im wesentlichen die arithmetischen Eigenschaften der natürlichen Zahlen, also der ganzen positiven Zahlen, und gehört zu den ältesten Teilgebieten der Mathematik.
Eines der zentralen Probleme der (im 19. Jahrhundert entstandenen; d. Red.) sog. analytischen Zahlentheorie ist die Verteilung der Primzahlen in der Folge der natürlichen Zahlen.

Primzahl nennt man jede ganze positive Zahl, die größer als Eins ist, wenn sie ohne Rest lediglich durch sich selbst und durch Eins teilbar ist. Das Problem der Verteilung der Primzahlen in der Folge der natürlichen Zahlen besteht darin, zu untersuchen, nach welchen Gesetzmäßigkeiten die Anzahl der Primzahlen unterhalb einer gewissen Zahl N anwächst, falls diese Zahl N immer größer wird. (Die von Gauß [1777-1855] vermutete Beziehung wurde Ende des 19. Jahrhunderts von Hadamard und de la Vallée-Poussin bewiesen; d. Red.)

Das erste Ergebnis in dieser Richtung finden wir schon bei Euklid (IV. Jahrhundert v. u. Zeitr.). Es handelt sich um den Beweis der Tatsache, dass es unendlich Viele Primzahlen gibt.
Das zweite Resultat nach Euklid lieferte in der zweiten Hälfte des XIX. Jahrhunderts der große russische Mathematiker P. L. Tschebyscheff. Eine andere wesentliche Aufgabe der Zahlentheorie ist die Darstellung ganzer Zahlen als Summe ganzer Zahlen eines bestimmten Typus, z.B. die Darstellung der ungeraden Zahlen als Summen dreier Primzahlen.

Dieses letzte Problem, die Goldbachsche Vermutung wurde erst 1937 von dem bedeutendsten derzeitigen Vertreter der Zahlentheorie, dem sowjetischen Mathematiker I. M. Winogradow, gelöst.

Das vorliegende Büchlein behandelt eines der interessantesten Gebiete der Zahlentheorie, nämlich die Auflösung von sog. diophantischen Gleichungen.
Die Ermittlung der ganzzahligen Lösungen algebraischer Gleichungen mit ganzen Koeffizienten und mehr als einer Unbekannten ist eines der schwierigsten Probleme der Zahlentheorie. Mit diesen Problemen beschäftigten sich viele hervorragende Mathematiker des Altertum, z.B. der griechische Mathematiker Pythagoras (VI. Jahrhundert v.u.Zeitr.), der alexandrinische Mathematiker Diophant (II.-III. Jahrhundert [nach ihm werden diese Gleichungen benannt; d. Red.]) und die besten Mathematiker der Neuzeit, Pierre Fermat (XVII. Jahrhundert), Leonhard Euler (XVIII. Jahrhundert), Lagrange und andere.

Ungeachtet der Bemühungen vieler Generationen hervorragender Mathematiker fehlen auf diesem Gebiet irgendwelche allgemeine Methoden, etwa von der Art der Winogradowschen Methode der trigonometrischen Summen, welche die Lösung der verschiedensten Probleme der analytischen Zahlentheorie erlaubt.

Das Problem, die ganzzahligen Lösungen von Gleichungen zu finden, ist nur bis zu Gleichungen zweiten Grades mit zwei Unbekannten vollständig gelöst. Für Gleichungen beliebigen Grades mit einer Unbekannten ist das Problem nicht sehr interessant, da es hier in endlich vielen Schritten entschieden werden kann. (Man probiert, ob die Teiler des absoluten Gliedes Lösungen sind; d. Red).

Für Gleichungen höheren als zweiten Grades mit zwei oder mehr Unbekannten ist nicht nur das Problem, alle ganzzahligen Lösungen zu ermitteln, sehr schwierig, sondern sogar schon die wesentlich leichtere Aufgabe, festzustellen, ob endlich oder unendlich viele solcher Lösungen existieren.

Die Auflösung von Gleichungen in ganzen Zahlen hat nicht nur theoretisches Interesse; solche Gleichungen kommen bisweilen auch in der Physik vor.
Das theoretische Interesse an diesen Gleichungen ist sehr groß, da sie eng mit vielen Problemen der Zahlentheorie zusammenhängen. Außerdem können die in diesem Büchlein behandelten elementaren Teile der Theorie solcher Gleichungen gut zur Erweiterung des mathematischen Gesichtskreises von Schülern der Oberschule und von Studierenden an Lehrerbildungsinstituten und Pädagogischen Instituten verwendet werden.

In diesem Buch werden die grundlegenden Resultate der Theorie der diophantischen Gleichungen behandelt. Die Beweise der vorkommenden Sätze sind angegeben, soweit sie nicht zu schwierig sind.

1 Gleichungen mit einer Unbekannten

Wir betrachten eine Gleichung ersten Grades mit einer Unbekannten

$$a_1 x + a0 = 0 \tag{1}$$

Sind die Koeffizienten a_1 und a_0 der Gleichung ganze Zahlen, so ist klar, dass die Lösung dieser Gleichung,

$$x = -\frac{a_0}{a_1}$$

nur dann eine ganze Zahl ist, wenn a_1 in a_0 aufgeht. Somit ist die Gleichung (1) nicht immer in ganzen Zahlen lösbar; so hat zum Beispiel von den beiden Gleichungen $3x^-27 = 0$ und $5x + 21 = 0$ die erste die ganzzahlige Lösung $x = 9$, die zweite ist jedoch nicht in ganzen Zahlen lösbar.

Denselben Sachverhalt finden wir auch bei Gleichungen höheren als ersten Grades: die quadratische Gleichung $x^2 + x - 2 = 0$ hat die ganzzahligen Lösungen $x_1 = 1$ und $x_2 = -2$; die Gleichung $x^2 - 4x + 2 = 0$ hat keine ganzzahligen Lösungen, da ihre Wurzeln $x_{1,2} = 2 \pm \sqrt{2}$ irrational sind.

Das Problem, die ganzzahligen Lösungen einer Gleichung n-ten Grades mit ganzzahligen Koeffizienten

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0 \qquad (n \geq 1) \tag{2}$$

zu finden, ist leicht zu lösen. Angenommen, $x = a$ sei eine ganzzahlige Wurzel dieser Gleichung. Dann gilt

$$a_n a^n + a_{n-1} a^{n-1} + ... + a_1 a + a_0 = 0 \quad , \quad a_0 = -a(a_n a^{n-1} + a_{n-1} a^{n-2} + ... + a_1)$$

Aus dieser Identität ist ersichtlich, dass a_0 ohne Rest durch a teilbar ist; folglich ist jede ganzzahlige Wurzel der Gleichung (2) ein Teiler ihres absoluten Gliedes.
Um die ganzzahligen Lösungen einer Gleichung zu finden, muss man diejenigen Teiler von a_0 suchen, die beim Einsetzen in die Gleichung eine Identität liefern.

So ist zum Beispiel von den Zahlen 1, -1, 2 und -2, die sämtliche Teiler des absoluten Gliedes der Gleichung

$$x^{10} + x^7 + 2x^3 + 2 = 0$$

ausmachen, nur -1 eine Wurzel. Folglich ist unter den Wurzeln dieser Gleichung $x = -1$ die einzige ganzzahlige. Nach der gleichen Methode kann man leicht zeigen, dass die Gleichung

$$x^6 - x^5 + 3x^4 + x^2 - x + 3 = 0$$

keine ganzzahligen Wurzeln hat.

Von wesentlich größerem Interesse ist die Ermittlung der ganzzahligen Lösungen bei Gleichungen mit mehreren Unbekannten.

2 Gleichungen ersten Grades mit zwei Unbekannten

Wir betrachten eine Gleichung ersten Grades mit zwei Unbekannten

$$ax + by + c = 0 \tag{3}$$

wobei a und b ganze, von Null verschiedene Zahlen sind, während c eine beliebige ganze Zahl ist. Wir dürfen annehmen, dass die Koeffizienten a und b keine gemeinsamen Teiler außer 1 haben[1]:
Ist nämlich der größte gemeinsame Teiler $d = (a, b)$ dieser Koeffizienten von 1 verschieden, so gelten die Beziehungen $a = a_1 \cdot d$ und $b = b_1 \cdot d$; die Gleichung (3) nimmt die Form

$$(a_1 x + b_1 y)d + c = 0$$

an und kann nur dann ganzzahlige Lösungen haben, wenn c durch d teilbar ist. Somit müssen für den Fall $(a, b) = d \neq 1$ sämtliche Koeffizienten der Gleichung (3) ganze Vielfache von d sein. Wenn wir (3) durch d kürzen, kommen wir zur Gleichung

$$a_1 x + b_1 y + c_1 = 0 \qquad \left(c_1 = \frac{c}{d}\right)$$

deren Koeffizienten a_1 und b_1 teilerfremd sind.

Wir betrachten zuerst den Fall $c = 0$. Aus Gleichung (3) wird dann:

$$ax + by = 0 \tag{3'}$$

Lösen wir die Gleichung nach x auf, so erhalten wir:

$$x = -\frac{b}{a}y$$

Es ist klar, dass x dann und nur dann ganzzahlige Werte annehmen kann, wenn y ohne Rest durch a teilbar ist. Nun können alle ganzen Zahlen y, die Vielfache von a sind, in der Form

$$y = at$$

dargestellt werden, wobei t alle ganzzahligen Werte $(t = 0, \pm 1, \pm 2, ...)$ annimmt. Setzen wir diesen Wert für y in die obige Gleichung ein, so erhalten wir

$$x = -\frac{b}{a}at = -bt$$

und besitzen damit folgende Formeln, die alle ganzzahligen Lösungen der Gleichung (3') liefern:

$$x = -bt, \qquad y = at \qquad (t = 0, \pm 1, \pm 2, ...)$$

Wir gehen jetzt zum Fall $c \neq 0$ über.
Wir zeigen zunächst, dass es für das Auffinden aller ganzzahligen Lösungen der Gleichung (3) genügt, irgendeine ihrer Lösungen zu finden, d.h. solche ganzen Zahlen x_0, y_0 zu finden, für die

$$ax_0 + by_0 + c = 0$$

[1] Solche Zahlen a und b nennt man teilerfremd; bezeichnet man mit (a, b) den größten gemeinsamen Teiler der Zahlen a und b, so ist also für teilerfremde Zahlen $(a, b) = 1$.

gilt.

Satz I. Sind a und b teilerfremd und ist $[x_0, y_0]$ irgendeine Lösung[2] der Gleichung

$$ax + by + c = 0 \tag{3}$$

so liefern die Formeln

$$x = x_0 - bt \qquad , \qquad y = y_0 + at \tag{4}$$

mit $t = 0, \pm 1, \pm 2, ...$ alle Lösungen der Gleichung (3).

Beweis: Sei $[x, y]$ eine beliebige Lösung der Gleichung (3). Wir erhalten dann aus den Gleichungen

$$ax + by + c = 0 \qquad \text{und} \qquad ax_0 + by_0 + c = 0$$

die Beziehungen

$$ax - ax_0 + by - by_0 = 0 \qquad ; \qquad y - y_0 = \frac{a(x_0 - x)}{b}$$

Da $y - y_0$ eine ganze Zahl ist und die Zahlen a und b teilerfremd sind, muss $x_0 - x$ ein ganzes Vielfaches von b sein, d.h., $x_0 - x$ hat die Form

$$x_0 - x = bt$$

wobei t eine ganze Zahl ist. Dann ist aber

$$y - y_0 = \frac{abt}{b} = at$$

und wir erhalten:

$$x = x_0 - bt \qquad , \qquad y = y_0 + at$$

Damit ist bewiesen, dass jede Lösung $[x, y]$ die Form (4) hat.
Es bleibt noch zu verifizieren, dass jedes Zahlenpaar $[x_1, y_1]$, das man durch die Formeln (4) bei ganzzahligem $t = t_1$ erhält, eine Lösung der Gleichung (3) ist. Zu diesem Zwecke setzen wir die Größen $x_1 = x_0 - bt_1$ und $y_1 = y_0 + at_1$ in die linke Seite von (3) ein:

$$ax_1 + by_1 + c = ax_0 - abt_1 + by_0 + abt_1 + c = ax_0 + by_0 + c$$

da aber $[x_0, y_0]$ eine Lösung ist, ist $ax_0 + by_0 + c = 0$, und folglich

$$ax_1 + by_1 + c = 0$$

d.h., $[x_1, y_1]$ ist eine Lösung der Gleichung (3), womit der Satz vollständig bewiesen ist.

Wenn also eine Lösung der Gleichung $ax + by + c = 0$ bekannt ist, findet man alle übrigen Lösungen aus den arithmetischen Progressionen, deren allgemeine Glieder die Form

$$x = x_0 - bt \qquad , \qquad y = y_0 + at \qquad (t = 0, \pm 1, \pm 2, ...)$$

haben.

[2] Ein Paar ganzer Zahlen x und y, welche die Gleichung befriedigen, wollen wir eine Lösung nennen und mit $[x, y]$ bezeichnen.

Wir bemerken, dass man für $c = 0$ die früher gefundenen Lösungsformeln

$$x = -bt \qquad , \qquad y = at$$

aus den eben abgeleiteten Formeln

$$x = x_0 - bt \qquad , \qquad y = y_0 + at$$

erhält, wenn man $x_0 = y_0 = 0$ wählt. Das ist möglich, da das Paar $x = 0$, $y = 0$ offenbar eine Lösung der Gleichung $ax + by = 0$ ist.

Wie kann man aber irgendeine Lösung $[x_0, y_0]$ der Gleichung (3) im allgemeinen Fall, also mit $c \neq 0$ finden? Gehen wir von einem Beispiel aus!

Es sei die Gleichung

$$127x - 52y + 1 = 0$$

vorgelegt. Wir bilden den Quotienten der Koeffizienten der Unbekannten.
Zunächst verwandeln wir den unechten Bruch $\frac{127}{52}$ in die Summe einer ganzen Zahl und eines echten Bruches:

$$\frac{127}{52} = 2 + \frac{23}{52}$$

Der echte Bruch $\frac{23}{52}$ ist gleich $\frac{1}{\frac{52}{23}}$. Somit erhalten wir

$$\frac{127}{52} = 2 + \frac{1}{\frac{52}{23}}$$

Wir formen den im Nenner stehenden unechten Bruch $\frac{52}{23}$ in gleicher Weise um:

$$\frac{52}{23} = 2 + \frac{6}{23} = 2 + \frac{1}{\frac{23}{6}}$$

Jetzt hat der ursprüngliche Bruch die Form

$$\frac{127}{52} = 2 + \frac{1}{2 + \frac{1}{\frac{23}{6}}}$$

Wiederholen wir dieselben Überlegungen für den Bruch $\frac{23}{6}$

$$\frac{23}{26} = 3 + \frac{5}{6} = 3 + \frac{1}{\frac{6}{5}}$$

so erhalten wir

$$\frac{127}{52} = 2 + \frac{1}{2 + \frac{1}{3 + \frac{1}{\frac{6}{5}}}}$$

Nun stellen wir den unechten Bruch $\frac{6}{5}$ als Summe einer ganzen Zahl und eines echten Bruches

$$\frac{6}{5} = 1 + \frac{1}{5}$$

dar. Dann kommen wir zum Endresultat:

$$\frac{127}{52} = 2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5}}}}$$

Wir haben einen sogenannten endlichen Kettenbruch erhalten. Vernachlässigen wir $\frac{1}{5}$, das letzte Glied dieses Kettenbruches, und verwandeln wir den dadurch entstehenden neuen Kettenbruch in einen einfachen Bruch und subtrahieren wir diesen von dem ursprünglichen Bruch $\frac{127}{52}$, so erhalten wir

$$2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1}}} = 2 + \frac{1}{2 + \frac{1}{4}} = 2 + \frac{4}{9} = \frac{22}{9}$$

$$\frac{127}{52} - \frac{22}{9} = \frac{1143 - 1144}{52 \cdot 9} = -\frac{1}{52 \cdot 9}$$

Jetzt multiplizieren wir den so erhaltenen Ausdruck mit dem Hauptnenner:

$$127 \cdot 9 - 52 \cdot 22 + 1 = 0$$

Aus dem Vergleich dieses Ausdruckes mit der Gleichung

$$127x - 52y + 1 = 0$$

folgt, dass $x = 9$ und $y = 22$ eine Lösung dieser Gleichung bilden.
Nach Satz I werden alle ihre Lösungen durch die Folgen

$$x = 9 + 52t \qquad , \qquad y = 22 + 127t \qquad (t = 0, \pm 1, \pm 2, ...)$$

geliefert.
Dieses Resultat bringt uns auf den Gedanken, dass man auch im allgemeinen Fall zur Auflösung der Gleichung $ax + by + c = 0$ so vorgehen kann:

Der Quotient der Koeffizienten der Unbekannten wird in einen Kettenbruch entwickelt, dessen letztes Glied man wegfallen lässt; danach führt man Berechnungen durch, die den obigen analog sind.
Für den Beweis dieser Vermutung benötigen wir einige Eigenschaften der Kettenbrüche.

Wir betrachten einen gekürzten Bruch $\frac{a}{b}$ [d.h. $(a, b) = 1$]. Mit q_1 bezeichnen wir den Quotienten und mit r_2 den Rest der Division von a durch b. Dann erhalten wir

$$a = q_1 b + r_2, \qquad r_2 < b$$

Wir nehmen ferner an, q_2 sei der Quotient und r_3 der Rest der Division von b durch r_2 Dann ist

$$b = q_2 r_2 + r_3, \qquad r_3 < r_2$$

und ebenso

$$\begin{aligned} r_2 &= q_3 r_3 + r_4, \qquad & r_4 < r_3 \\ r_3 &= q_4 r_4 + r_5, \qquad & r_5 < r_4 \\ &... \end{aligned}$$

Die Größen$q_1, q_2, ...$ werden unvollständige Quotienten genannt. Dieses Verfahren nennt man Euklidischen Algorithmus. Die Reste $r_2, r_3, ...$ der Division erfüllen die Ungleichungen

$$b > r_2 > r_3 > r_4 > ... \geq 0 \tag{5}$$

d.h., sie bilden eine Folge abnehmender nichtnegativer Zahlen. Nun kann die Anzahl der nichtnegativen ganzen Zahlen, welche die Zahl b nicht übertreffen, nicht unendlich sein; also muss bei einem gewissen Schritt das Verfahren abbrechen, da ein Rest r Null wird. Ist r_n der letzte von Null verschiedene Rest in der Folge (5), so ist $r_{n+1} = 0$, und der Euklidische Algorithmus für die Zahlen a und b hat die Form

$$\left.\begin{aligned} a &= q_1 b + r_2, \\ b &= q_2 r_2 + r_3, \\ r_2 &= q_3 r_3 + r_4, \\ &... \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, \\ r_{n-1} &= q_n r_n \end{aligned}\right\} \tag{6}$$

Wir schreiben die erhaltenen Gleichungen in der Form

$$\begin{aligned} \frac{a}{b} &= q_1 + \frac{1}{\frac{b}{r_2}}, \\ \frac{b}{r_2} &= q_2 + \frac{1}{\frac{r_2}{r_3}}, \\ &... \\ \frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}}, \\ \frac{r_{n-1}}{r_n} &= q_n \end{aligned}$$

Ersetzen wir den Wert r_1 in der ersten Zeile dieser Gleichungen durch den entsprechenden Wert aus der zweiten Zeile, den Wert $\frac{r_2}{r_3}$ durch den Ausdruck aus der dritten Zeile usw., so erhalten wir die Entwicklung von $\frac{a}{b}$ in einen Kettenbruch

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + ... + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

Die Ausdrücke, die sich aus einem Kettenbruch beim Vernachlässigen aller seiner Glieder von einem gewissen Glied ab ergeben, nennen wir Teilbrüche. (Ihr Zahlenwert wird als Näherungsbruch oder Näherungswert bezeichnet.) Der erste Teilbruch δ_1 ergibt sich, wenn man alle Glieder von $\frac{1}{q_2}$ ab vernachlässigt:

$$\delta_1 = q_1 < \frac{a}{b}$$

Der zweite Teilbruch δ_2 ergibt sich, wenn man alle Glieder von $\frac{1}{q_3}$ ab vernachlässigt:

$$\delta_2 = q_1 + \frac{1}{q_2} > \frac{a}{b}$$

Ebenso

$$\delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}} < \frac{a}{b} \qquad , \qquad \delta_4 = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q^4}}} > \frac{a}{b}$$

usw.
Aus der Art und Weise, wie wir die Teilbrüche erhalten haben folgen offenbar die Ungleichungen

$$\delta_1 < \delta_3 < ... < \delta_{2k-1} < \frac{a}{b}; \qquad \delta_2 > \delta_4 > ... > \delta_{2k} > \frac{a}{b}$$

Wir schreiben nun den k-ten Teilbruch δ_k in der Form

$$\delta_k = \frac{P_k}{Q_k} \qquad (1 \leq k \leq n)$$

und suchen das Bildungsgesetz für die Zähler und Nenner der Teilbrüche. Wir bilden die ersten Teilbrüche δ_1, δ_2 und δ_3:

$$\delta_1 = q_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}; \qquad P_1 = q_1; \qquad Q_1 = 1$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_1 q_2 + 1}{q_2} = \frac{P_2}{Q_2}; \qquad P_2 = q_1 q_2 + 1; \qquad Q_2 = 2$$

$$\delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}} = \frac{q_1 q_2 q_3 + q_1 + q_3}{q_2 q_3 + 1} = \frac{P_3}{Q_3}; \qquad P_3 = q_1 q_2 q_3 + q_1 + q_3; \qquad Q_3 = q_2 q_3 + 1$$

Daraus erhalten wir:

$$P_3 = P_2 q_3 + P_1 \qquad ; \qquad Q_3 = Q_2 q_3 + Q_1$$

Wenden wir vollständige Induktion an[3], so zeigt sich, dass die Beziehungen

$$P_k = P_{k-1} q_k + P_{k-2} \qquad ; \qquad Q_k = Q_{k-1} q_k + Q_{k-2} \tag{7}$$

für alle $k \leq 3$ gelten.

Wir nehmen an, die Gleichungen (7) seien für ein gewisses $k \leq 3$ erfüllt. Aus der Definition der Teilbrüche folgt unmittelbar, dass beim Ersetzen von q_k durch $q_k + \frac{1}{q_{k+1}}$ der Ausdruck für δ_k in δ_{k+1} übergeht. Nach Induktionsannahme ist

$$\delta_k = \frac{P_k}{Q_k} = \frac{P_{k-1} q_k + P_{k-2}}{Q_{k-1} q_k + Q_{k-2}}$$

Ersetzen wir hier q_k durch $q_k + \frac{1}{q_{k+1}}$, so erhalten wir

$$\delta_{k+1} = \frac{P_{k-1}\left(q_k + \frac{1}{q_{k+1}}\right) + P_{k-2}}{Q_{k-1}\left(q_k + \frac{1}{q_{k+1}}\right) + Q_{k-2}} = \frac{P_k + \frac{1}{q_{k+1}} P_{k-1}}{Q_k + \frac{1}{q_{k+1}} Q_{k-1}} = \frac{P_k q_{k+1} + P_{k-1}}{Q_k q_{k+1} + Q_{k-1}}$$

[3] Siehe in dieser Reihe das Büchlein von I.S. Sominski: "Die Methode der vollständigen Induktion", 2. Auflage, VEB Deutscher Verlag der Wissenschaften, Berlin 1960.

Hieraus folgt wegen $\delta_{k+1} = \frac{P_{k+1}}{Q_{k+1}}$ die Beziehung

$$P_{k+1} = P_k q_{k+1} + P_{k-1} \qquad , \qquad Q_{k+1} = Q_k q_{k+1} + Q_{k-1}$$

Somit ergibt sich aus der Annahme der Gültigkeit der Gleichungen (7) für ein gewisses $k \geq 3$ ihre Gültigkeit für $k+1$. Da aber für $k = 3$ die Gleichungen (7) erfüllt sind, ist damit ihre Gültigkeit für alle $k \geq 3$ erwiesen.

Wir zeigen jetzt, dass die Differenz aufeinanderfolgender Teilbrüche $\delta_k - \delta_{k-1}$ die Beziehung

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \qquad (k > 1) \tag{8}$$

erfüllt. Es ist

$$\delta_k - \delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_k Q_{k-1}}$$

Unter Benutzung der Formeln (7) formen wir den Zähler des erhaltenen Bruches um:

$$\begin{aligned} P_k Q_{k-1} - Q_k P_{k-1} = (P_{k-1} q_k + P_{k-2}) Q_{k-1} - (Q_{k-1} q_k + Q_{k-2}) P_{k-1} = \\ - (P_{k-1} Q_{k-2} - Q_{k-1} P_{k-2}) \end{aligned}$$

Den in Klammern stehenden Ausdruck erhält man aus dem ursprünglichen, indem man k durch $k-1$ ersetzt. Wir wiederholen dieselben Umformungen für die abgeleiteten Ausdrücke und erhalten offensichtlich eine Kette von Gleichungen:

$$\begin{aligned} P_k Q_{k-1} - Q_k P_{k-1} &= (-1)(P_{k-1} Q_{k-2} - Q_{k-1} P_{k-2}) = (-1)^2 (P_{k-2} Q_{k-3} - Q_{k-2} P_{k-3}) \\ &= \ldots = (-1)^{k-2} (P_2 Q_1 - Q_2 P_1) = (-1)^{k-2} (q_1 q_2 + 1 - q_1 q_2) = (-1)^{k-2} \end{aligned}$$

Hieraus folgt

$$\delta_k - \delta_{k-1} = \frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_k Q_{k-1}} = \frac{(-1)^{k-2}}{Q_k Q_{k-1}} = \frac{(-1)^k}{Q_k Q_{k-1}}$$

Hat die Entwicklung von $\frac{a}{b}$ in einen Kettenbruch n Glieder, so ist der n-te Teilbruch δ_n gleich $\frac{a}{b}$. Aus Gleichung (8) erhalten wir für $k = n$

$$\delta_n - \delta_{n-1} = \frac{(-1)^n}{Q_n Q_{n-1}} \qquad , \qquad \frac{a}{n} - \delta_n = \frac{(-1)^n}{b Q_{n-1}} \tag{9}$$

Wenden wir uns jetzt wieder der Auflösung der Gleichung

$$ax + by + c = 0, \qquad (a, b) = 1 \tag{10}$$

zu. Wir schreiben die Beziehung (9) in der Form

$$\frac{a}{b} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^k}{Q_k Q_{k-1}}$$

Bringen wir die Gleichung auf den Hauptnenner, so erhalten wir

$$\begin{aligned} a Q_{n-1} - b P_{n-1} &= (-1)^n \\ a Q_{n-1} + b(-P_{n-1}) + (-1)^{n-1} &= 0 \end{aligned}$$

Multiplizieren wir diese Beziehung mit $(-1)^{n-1} \cdot c$, so erhalten wir

$$a[(-1)^{n-1}cQ_{n-1}] + b[(-1)^n cP_{n-1}] + c = 0$$

Daraus folgt, dass das Zahlenpaar $[x_0, y_0]$,

$$x_0 = (-1)^{n-1}cQ_{n-1} \qquad , \qquad y_0 = (-1)^n cP_{n-1} \tag{11}$$

eine Lösung der Gleichung (10) ist. Nach Satz I haben alle Lösungen dieser Gleichung die Form

$$x = (-1)^{n-1}cQ_{n-1} - bt \qquad , \qquad y = (-1)^n cP_{n-1} + at \qquad (t = 0, \pm 1, \pm 2, ...)$$

Diese Resultat löst das Problem, alle ganzzahligen Lösungen einer diophantischen Gleichung ersten Grades mit zwei Unbekannten zu finden. Wir gehen nun zur Untersuchung von Gleichungen zweiten Grades über.

3 Beispiele für Gleichungen zweiten Grades mit drei Unbekannten

Beispiel 1. Wir betrachten folgende Gleichung zweiten Grades mit drei Unbekannten

$$x^2 + y^2 = z^2 \tag{12}$$

Die Aufgabe, die ganzzahligen Lösungen dieser Gleichung zu bestimmen, bedeutet geometrisch, alle pythagoreischen Dreiecke zu finden, d.h. die rechtwinkligen Dreiecke, bei denen die Katheten x, y und die Hypotenuse z ganzzahlige Werte haben.

Bezeichnen wir mit d den größten gemeinsamen Teiler der Zahlen x und y, so ist

$$x = x_1 d \qquad , \qquad y = y_1 d$$

und Gleichung (12) erhält die Form

$$x_1^2 d^2 + y_1^2 d^2 = z^2$$

Hieraus folgt, dass z^2 durch d^2 teilbar ist; das bedeutet, dass z ein Vielfaches von d ist: $z = z_1 \cdot d$.

Nun kann man Gleichung (12) in der Form

$$x_1^2 d^2 + y_1^2 d^2 = z_1^2 d^2$$

schreiben; teilen wir durch d^2, so erhalten wir:

$$x_1^2 + y_1^2 = z_1^2$$

Wir kommen so zu einer Gleichung, welche dieselbe Gestalt hat wie die Ausgangsgleichung, wobei jetzt die Größen x_1 und y_1 außer 1 keine gemeinsamen Teiler haben. Somit können wir uns bei der Auflösung der Gleichung (12) auf den Fall beschränken, dass x und y teilerfremd sind.

Sei also $(x, y) = 1$. Dann ist mindestens eine der Größen x und y (etwa x) ungerade. Indem wir y^2 auf die rechte Seite der Gleichung (12) bringen, erhalten wir

$$x^2 = z^2 - y^2 \qquad , \qquad x^2 = (z + y)(z - y) \tag{13}$$

Wir bezeichnen den größten gemeinsamen Teiler von $z + y$ und $z - y$ mit d_1. Dann ist

$$z + y = a d_1 \qquad , \qquad z - y = b d_1 \tag{14}$$

wobei a und b teilerfremd sind.
Wir setzen die Ausdrücke für $z + y$ und $z - y$ in (13) ein und erhalten:

$$x^2 = a b d_1^2$$

Da die Zahlen a und b keine gemeinsamen Teiler haben, ist die erhaltene Gleichung nur dann möglich, wenn a und b Quadratzahlen sind[4]

$$a = u^2 \qquad b = v^2$$

[4] Bekanntlich kann das Produkt zweier teilerfremder Zahlen nur dann eine Quadratzahl sein, wenn jeder Faktor eine Quadratzahl ist.

Dann ist aber

$$x^2 = u^2 v^2 d_1^2 \qquad \text{und} \qquad x = uvd_1 \tag{15}$$

Wir bestimmen jetzt y und z aus den Gleichungen (14). Die Addition dieser Gleichungen ergibt

$$2z = ad_1 + bd_1 = u^2 d_1 + v^2 d_1 \qquad ; \qquad z = \frac{u^2 + v^2}{2} d_1 \tag{16}$$

Subtrahieren wir die zweite der Gleichungen (14) von der ersten, so erhalten wir

$$2y = ad_1 - bd_1 = u^2 d_1 - v^2 d_1 \qquad ; \qquad y = \frac{u^2 - v^2}{2} d_1 \tag{17}$$

Da x ungerade ist, folgt aus (15), dass u, v und d_1 ebenfalls ungerade sind; überdies ist $d_1 = 1$, da sonst aus den Identitäten

$$x = uvd_1 \qquad \text{und} \qquad y = \frac{u^2 - v^2}{2} d_1$$

folgen würde, dass x und y einen gemeinsamen Teiler $d_1 \neq 1$ haben, was der vorausgesetzten Teilerfremdheit widersprüche.
Die Zahlen u und v sind mit den teilerfremden Zahlen a und b durch die Beziehungen

$$a = u^2 \qquad , \qquad b = v^2$$

verknüpft und infolgedessen selbst teilerfremd; es ist $v < u$, da aus den Gleichungen (14) ersichtlich ist, dass $b < a$ ist.
Setzen wir in den Gleichungen (15), (17) und (16) $d_1 = 1$, so erhalten wir die Formeln

$$x = uv, \qquad y = \frac{u^2 - v^2}{2}, \qquad z = \frac{u^2 + v^2}{2} \tag{18}$$

welche bei ungeraden teilerfremden u und v ($v < u$) alle von gemeinsamen Teilern freien Tripel ganzer positiver Zahlen x, y und z liefern, die der Gleichung (12) genügen. Durch einfaches Einsetzen von x, y und z in die Gleichung (12) ist leicht zu zeigen, dass bei beliebigen u und v die Zahlen (18) dieser Gleichung genügen.

Für die ersten Werte von u und v führen die Formeln (18) auf die folgenden oft anzutreffenden Gleichungen

$$\begin{aligned} 3^2 + 4^2 &= 5^2 \qquad (v = 1, u = 3) \\ 5^2 + 12^2 &= 13^2 \qquad (v = 1, u = 5) \\ 15^2 + 8^2 &= 17^2 \qquad (v = 3, u = 5) \end{aligned}$$

Wie schon erwähnt, liefern die Formeln (18) nur jene Lösungen der Gleichung

$$x^2 + y^2 = z^2$$

für welche die Zahlen x, y und z keine gemeinsamen Teiler haben.
Alle übrigen ganzzahligen positiven Lösungen dieser Gleichung erhält man durch Multiplikation der Lösungen, die sich aus den Formeln (18) ergeben, mit einem beliebigen gemeinsamen Faktor d.
In gleicher Weise, wie wir alle Lösungen der Gleichung (12) erhielten, können wir zu allen Lösungen anderer Gleichungen desselben Typus gelangen.

Beispiel 2. Wir wollen alle Lösungen der Gleichung

$$x^2 + 2y^2 = z^2 \tag{19}$$

in ganzen positiven paarweise teilerfremden x, y, z finden.

Wir bemerken folgendes: Bilden x, y, z eine Lösung der Gleichung (19) und haben diese Zahlen außer 1 keinen gemeinsamen Teiler, so sind sie paarweise teilerfremd; wären nämlich x und y Vielfache einer Primzahl $p > 2$, so folgte aus der Gleichung

$$\left(\frac{x}{p}\right)^2 + 2\left(\frac{y}{p}\right)^2 = \left(\frac{z}{p}\right)^2$$

dass 2 ein Vielfaches von p wäre, da die linke Seite der Gleichung eine ganze Zahl ist. Das gleiche ist der Fall, wenn x und z oder y und z durch p teilbar sind.

Wir bemerken, dass x ungerade sein muss, damit der größte gemeinsame Teiler von x, y und z gleich 1 ist. Wäre nämlich x gerade, so wäre die linke Seite der Gleichung (19) eine gerade Zahl, d.h., z^2 und damit z wäre ebenfalls gerade.
Die Zahlen x^2 und z^2 wären dann Vielfache von 4; daraus folgte, dass $2y^2$ durch 4 teilbar sein müsste, mit anderen Worten, dass auch y eine gerade Zahl sein müsste. Das bedeutet, dass bei geradem xa alle Zahlen x, y, z gerade sein müssen. Somit muss, wenn 1 der größte gemeinsame Teiler der Lösung sein soll, x ungerade sein. Daraus folgt schon, dass z ebenfalls ungerade sein muss.

Bringen wir x^2 auf die rechte Seite, so erhalten wir

$$2y^2 = z^2 - x^2 = (z + x)(z - x)$$

Die Zahlen $z + x$ und $z - x$ haben als größten gemeinsamen Teiler die Zahl 2.

Beweis: Ihr größter gemeinsamer Teiler sei d. Dann ist

$$z + x = kd \qquad , \qquad z - x = ld$$

wobei k und l ganze Zahlen sind. Durch Addition und Subtraktion dieser Gleichungen erhalten wir

$$2z = d(k - l) \qquad , \qquad 2x = d(k - l)$$

Nun sind aber z und x ungerade und zueinander teilerfremd. Daher ist der größte gemeinsame Teiler von $2x$ und $2z$ gleich 2. Daraus folgt, dass $d = 2$ ist.

Somit ist entweder $\frac{z+x}{2}$ oder $\frac{z-x}{2}$ ungerade. Daher ist für alle, den Bedingungen genügenden x und z eines der beiden Zahlenpaare

$$z + x \quad \text{und} \quad z - x \quad , \quad \frac{z + x}{2} \quad \text{und} \quad \frac{z - x}{2}$$

teilerfremd. Im ersten Fall folgt aus der Gleichung

$$(z + x)\frac{z - x}{2} = y^2 \quad \text{dass} \quad z + x = n^2 \quad , \quad z - x = 2m^2$$

im zweiten Fall aus der Gleichung

$$\frac{z + x}{2}(z - x) = y^2 \quad \text{dass} \quad z + x = 2m^2 \quad , \quad z - x = n^2$$

gilt. Dabei sind n und m ganze Zahlen, m ist ungerade, m und n sind positiv. Lösen wir die zwei Gleichungssysteme nach x und z auf und bestimmen wir y, so erhalten wir

$$z = \frac{1}{2}(n^2 + 2m^2) \quad , \quad x = \frac{1}{2}(n^2 - 2m^2) \quad , \quad y = mn$$

oder

$$z = \frac{1}{2}(n^2 + 2m^2) \quad , \quad x = \frac{1}{2}(2m^2 - n^2) \quad , \quad y = mn$$

wobei m ungerade ist. Fassen wir die zwei Lösungsformeln für x, y und z zusammen, so erhalten wir die allgemeine Formel

$$x = \pm\frac{1}{2}(n^2 - 2m^2) \quad , \quad y = mn \quad , \quad z = \frac{1}{2}(n^2 + 2m^2)$$

wobei m ungerade ist. Damit z und x ganze Zahlen sind, muss n notwendig eine gerade Zahl sein. Setzen wir $n = 2b$ und $m = a$, so erhalten wir schließlich die allgemeinen Formeln, welche alle Lösungen der Gleichung (19) in ganzen positiven teilerfremden Zahlen liefern:

$$x = \pm(a^2 - 2b^2) \quad , \quad y = 2ab \quad , \quad z = s^2 + 2b^2 \tag{19'}$$

Dabei sind a und b positiv und teilerfremd, a ist ungerade. Unter diesen Bedingungen können die Größen a und b beliebig gewählt werden, aber so, dass x positiv ist.

Die Formeln (19') liefern tatsächlich alle Lösungen in ganzen positiven teilerfremden Zahlen x, y, z; wir haben nämlich einerseits gezeigt, dass x, y, z in diesem Falle durch die Formeln (19') dargestellt werden müssen; andererseits sind bei vorgegebenen a und b, die unseren Bedingungen genügen, die sich ergebenden x, y, z tatsächlich teilerfremd und bilden eine Lösung der Gleichung (19).

4 Gleichungen der Form $x^2 - Ay^2 = 1$

Die Ermittlung aller Lösungen dieser Gleichungen

Wir kommen jetzt zur Untersuchung der Lösungen in ganzen Zahlen von Gleichungen zweiten Grades mit zwei Unbekannten der Form

$$x^2 - Ay^2 = 1 \tag{20}$$

wobei A ganz und positiv, aber keine Quadratzahl ist.
Um einen Lösungsansatz für solche Gleichungen zu finden, lernen wir die Entwicklung von Irrationalzahlen der Form $\sqrt{A}$ in Kettenbrüche kennen.

Aus dem Euklidischen Algorithmus folgt, dass jede rationale Zahl in einen Kettenbruch mit endlich vielen Gliedern entwickelt werden kann. Anders ist es mit den Irrationalzahlen.
Ihnen entsprechen unendliche Kettenbrüche. Entwickeln wir z.B. die Irrationalzahl $\sqrt{2}$ in einen Kettenbruch. Wir gehen von der Identität

$$(\sqrt{2}-1)(\sqrt{2}+1) = 1$$

aus und finden

$$\sqrt{2} = \frac{1}{\sqrt{2}+1} \quad , \quad \sqrt{2}-1 = \frac{1}{2+(\sqrt{2}-1)}$$

Ersetzen wir die Differenz $\sqrt{2}-1$, die wir im Nenner erhalten haben, durch den ihr gleichen Ausdruck

$$\frac{1}{2+(\sqrt{2}+1)}$$

so erhalten wir

$$\sqrt{2}-1 = \frac{1}{2+\dfrac{1}{2+(\sqrt{2}+1)}} \quad , \quad \sqrt{2} = 1+\frac{1}{2+\dfrac{1}{2+(\sqrt{2}+1)}}$$

Ersetzen wir erneut die im Nenner der letzten Gleichung stehende Klammer durch $\frac{1}{2+(\sqrt{2}+1)}$, so erhalten wir

$$\sqrt{2} = 1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+(\sqrt{2}+1)}}}$$

Setzen wir das Verfahren fort, so kommen wir auf folgende Entwicklung von $\sqrt{2}$ in einen unendlichen Kettenbruch:

$$\sqrt{2} = 1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\ldots}}}} \tag{21}$$

Man bemerkt, dass die oben verwendete Methode zur Entwicklung in einen Kettenbruch, die auf der Verwendung der Identität

$$(\sqrt{m^2+1}-m)(\sqrt{m^2+1}+m) = 1$$

beruhte, nicht für jede Irrationalzahl $\sqrt{A}$ anwendbar ist.
Diese Methode kann offensichtlich nur dann verwendet werden, wenn die ganze Zahl A in der Form $A = m^2 + 1$ dargestellt werden kann, wobei m irgendeine ganze von Null verschiedene Zahl ist (speziell für $m = 1$ erhalten wir die Entwicklung für $\sqrt{2}$; $m = 2$ führt auf die Entwicklung von $\sqrt{5}$ usw.).
Auch für den allgemeinen Fall sind jedoch verhältnismäßig einfache Methoden zur Entwicklung von $\sqrt{A}$ in einen unendlichen Kettenbruch bekannt.[5]

Genau wie früher bei den endlichen Kettenbrüchen bilden wir für einen unendlichen Kettenbruch (21) die Folge der Teilbrüche δ_1, δ_2, δ_3, ...

$$\begin{aligned} \delta_1 &= 1 && \delta_1 < \sqrt{2} \\ \delta_2 &= 1 + \frac{1}{2} = \frac{3}{2} && \delta_2 > \sqrt{2} \\ \delta_3 &= 1 + \frac{1}{1 + \frac{1}{2}} = \frac{7}{5} && \delta_3 < \sqrt{2} \\ \delta_4 &= ... = \frac{17}{12} && \delta_4 > \sqrt{2} \end{aligned}$$

usw.
Aus der Bildungsweise der Kettenbrüche folgt, dass

$$\delta_1 < \delta_3 < ... < \sqrt{2} \qquad , \qquad \delta_2 > \delta_3 > ... > \sqrt{2}$$

ist. Allgemein: Ist die Entwicklung irgendeiner Irrationalzahl α in einen unendlichen Kettenbruch gegeben,

$$\alpha = q_1 + \cfrac{1}{q2 + \cfrac{1}{q_3 + ...}}$$

so erfüllen die Näherungsbrüche die Ungleichungen

$$\delta_1 < \delta_3 < ... < \delta_{k+1} < ... < \sqrt{\alpha} < ... < \delta_{2k} < ... < \delta_4 < \delta_2 \tag{23}$$

Wir stellen den Näherungsbruch δ_k in der Form

$$\delta_k = \frac{P_k}{Q_k}$$

dar. Die Beziehungen (7)

$$P_k = P_{k-1}q_k + P_{k-2} \qquad , \qquad Q_k = Q_{k-1}q_k + Q_{k-2}$$

die wir früher für endliche Kettenbrüche erhielten, bleiben auch für unendliche Kettenbrüche erhalten, da wir bei der Herleitung dieser Beziehungen nirgends davon Gebrauch gemacht haben, dass der Kettenbruch endlich ist. Daher bleibt auch die Beziehung (8) zwischen aufeinander folgenden Näherungsbrüchen gültig:

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \tag{24}$$

[5]Siehe z.B. I.W. Arnold, "Zahlentheorie", Kapitel VI, Staatsverlag für pädagogische Literatur 1939, oder A.J. Chintschin "Kettenbrüche", Staatsverlag für technisch-theoretische Literatur, 1949; Deutsche Literatur: O. Perron, Irrationalzahlen, Berlin 1939 ; O. Perron, Kettenbrüche, Leipzig 1929; ferner: C. Knochendöppel, Von den Kettenbrüchen und den Diophantischen Gleichungen, Volk und Wissen, Berlin-Leipzig 1948 (d. Red.).

Beispielsweise erhalten wir für die Näherungsbrüche der Entwicklung von $\sqrt{2}$ in einen Kettenbruch für $k = 3$ und $k = 4$ aus (22)

$$\delta_3 - \delta_2 = \frac{7}{5} - \frac{3}{2} = -\frac{1}{10} \quad , \quad \delta_4 - \delta_3 = \frac{17}{12} - \frac{7}{5} = \frac{1}{60}$$

Dies stimmt natürlich mit dem Resultat von (24) überein.
Aus (24) folgt insbesondere

$$\delta_{2k} - \delta_{2k+1} = -(\delta_{2k+1} - \delta_{2k}) = -\frac{(-1)^{2k+1}}{Q_{2k+1}Q_{2k}} = \frac{1}{Q_{2k+1}Q_{2k}}$$

Wir zeigen jetzt, dass die Ungleichung

$$0 < P_{2k} - \alpha Q_{2k} = \frac{1}{Q_{2k+1}} \tag{25}$$

gilt. Die linke Hälfte dieser Ungleichung ergibt sich sofort, da nach (23)

$$\alpha < \delta_{2k} = \frac{P_{2k}}{Q_{2k}}$$

ist. Der Beweis der rechten Hälfte der Ungleichung (25) lässt sich ebenfalls unschwer erbringen. Nach (23) gilt

$$\delta_{2k+1} < \alpha < \delta_{2k}$$

und folglich

$$\delta_{2k} - \alpha < \delta_{2k} - \delta_{2k+1} = \frac{1}{Q_{2k}Q_{2k+1}}$$

Daraus erhalten wir, wenn wir δ_{2k} durch $\frac{P_{2k}}{Q_{2k}}$ ersetzen,

$$\frac{P_{2k}}{Q_{2k}} - \alpha < \frac{1}{Q_{2k}Q_{2k+1}}$$

Wenn wir diese Ungleichung mit Q_{2k} multiplizieren, kommen wir zu dem gewünschten Resultat

$$P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k+1}}$$

Verwenden wir nunmehr die gewonnenen Ergebnisse zur Lösung der Gleichung

$$x^2 - 2y^2 = 1 \tag{26}$$

Wir formen die linke Seite dieser Gleichung um:

$$x^2 - 2y^2 = (x - 2\sqrt{y})(x + \sqrt{2}y)$$

Setzen wir $x = P_{2k}$ und $y = Q_{2k}$ wobei P_{2k} und Q_{2k} Zähler und Nenner der entsprechenden Näherungsbrüche aus der Entwicklung von $\sqrt{2}$ in einen Kettenbruch sind, so ist

$$P_{2k}^2 - 2Q_{2k}^2 = (P_{2k} - \sqrt{2}Q_{2k})(P_{2k} + \sqrt{2}Q_{2k}) \tag{27}$$

Die linke, also auch die rechte Seite der erhaltenen Gleichung ist eine ganze Zahl. Wir werden zeigen, dass diese ganze Zahl größer als Null und kleiner als Zwei, also folglich gleich Eins ist.

Dazu benutzen wir die Ungleichung (25) für $\alpha = \sqrt{2}$:

$$0 < P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{Q_{2k+1}} \tag{28}$$

Daraus ist ersichtlich, dass beide Faktoren auf der rechten Seite von Gleichung (27) positiv sind. Das bedeutet

$$P_{2k}^2 - 2Q_{2k}^2 > 0$$

Andererseits ist

$$P_{2k} - \sqrt{Q}_{2k} < \frac{1}{Q_{2k+1}} = \frac{1}{Q_{2k}q_{2k+1} + Q_{2k-1}} = \frac{1}{2Q_{2k} + Q_{2k-1}} < \frac{1}{2Q_{2k}}$$

Wegen (28) gilt aber

$$\delta_{2k} = \frac{P_{2k}}{Q_{2k}} > \sqrt{2}$$

Hieraus folgt

$$\sqrt{2}Q_{2k} < P_{2k} \qquad , \qquad P_{2k} + \sqrt{2}Q_{2k} < 2P_{2k}$$

und wir erhalten zwei Ungleichungen für die Faktoren auf der rechten Seite der Gleichung (27):

$$P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{2Q_{2k}} \qquad , \qquad P_{2k} + \sqrt{2}Q_{2k} < 2P_{2k}$$

Die Multiplikation dieser Ungleichungen liefert

$$P_{2k}^2 - 2Q_{2k}^2 < \frac{P_{2k}}{Q_{2k}}$$

Wenden wir Ungleichung (28) an, so erhalten wir hieraus:

$$P_{2k}^2 - 2Q_{2k}^2 < \frac{\sqrt{2}Q_{2k} + \frac{1}{Q_{2k+1}}}{Q_{2k}} = \sqrt{2} + \frac{1}{Q_{2k}Q_{2k+1}}$$

Da für alle $k \geq 1$ die Ungleichung

$$\frac{1}{Q_{2k}Q_{2k+1}} \leq \frac{1}{Q_2Q_3} = \frac{1}{10}$$

gilt, folgt

$$P_{2k}^2 - 2Q_{2k}^2 < \sqrt{2} + \frac{1}{10} < 2$$

Damit haben wir gezeigt, dass die ganze Zahl $P_{2k}^2 - 2Q_{2k}^2$ bei beliebigem $k \geq 1$ der Ungleichung

$$0 < P_{2k}^2 - 2Q_{2k}^2 < 2$$

genügt. Folglich ist

$$P_{2k}^2 - 2Q_{2k}^2 = 1$$

d.h., die Zahlen $x = P_{2k}$ und $y = Q_{2k}$ stellen bei beliebigem $k \geq 1$ eine Lösung der Gleichung

$$x^2 - 2y^2 = 1$$

dar.

Wir wissen vorläufig nicht, ob die von uns gefundenen Lösungen der Gleichung (26) alle Lösungen dieser Gleichung ausmachen.
Es entsteht nun natürlich die Frage, wie man alle Lösungen der Gleichung 7

$$x^2 - Ay^2 = 1 \tag{29}$$

bei ganzem positivem nichtquadratischem A in ganzen x und y erhält. Wie wir zeigen werden, kann man diese Lösungen leicht konstruieren, wenn man eine Lösung der Gleichung (29) kennt. Am Beispiel der Gleichung (26) sahen wir schon, dass solche Gleichungen auch wirklich Lösungen haben.

Wir beschäftigen uns jetzt mit der Frage, wie man alle Lösungen der Gleichung (29) aus einer bestimmten Lösung erhalten kann, die wir Minimal-Lösung nennen; dabei lassen wir die Frage, ob die Gleichung (29) auch immer mindestens eine von der trivialen Lösung $x = 1$, $y = 0$ verschiedene Lösung in ganzen Zahlen hat, zunächst offen.
Wir nehmen an, (29) habe eine nichttriviale Lösung $[x_0, y_0]$ mit $x_0 > 0$ und $y_0 > 0$, d.h. es sei

$$x_0^2 - Ay_0^2 = 1 \tag{30}$$

(Wir nannten ein Paar ganzer Zahlen $[x_0, y_0]$, welche die Gleichung befriedigen, eine Lösung der Gleichung.) Wir nennen $[x_0, y_0]$ Minimal-Lösung, wenn für $x = x_0$ und $y = y_0$ das Binom $x + \sqrt{A} \cdot y$, $\sqrt{A} > 0$, den kleinstmöglichen Wert unter denjenigen Werten hat, die es beim Einsetzen aller möglichen ganzen positiven (von Null verschiedenen) Zahlen der Lösungen der Gleichung (29) annehmen kann.

Für Gleichung (26) ist zum Beispiel das Paar $x = 3, y = 2$ die Minimal-Lösung, da $x + \sqrt{A}y$ bei diesen Werten von x und y den Wert $3 + 2\sqrt{2}$ annimmt und keine andere Lösung der Gleichung (26) existiert, die das Binom $x + \sqrt{2}y$ nicht größer als $3 + 2\sqrt{2}$ machen würde.
Dies erkennt man sofort, wenn man die kleinen ganzen positiven Zahlen, die Lösungen sein könnten, durchprobiert. Die der Größe nach folgende Lösung der Gleichung (26) ist das Paar $x = 17, y = 12$; und offenbar ist $17 + 12\sqrt{2}$ größer als $3 + 2\sqrt{2}$.

Wir stellen auch fest, dass nicht zwei Minimal-Lösungen der Gleichung (29) existieren. Denn würde es zwei Lösungen $[x_1, y_1]$ und $[x_2, y_2]$ geben, für welche das Binom $x + \sqrt{2}y$ denselben Wert liefert, so wäre

$$x_1 + \sqrt{A}y_1 = x_2 + \sqrt{A}y_2 \tag{31}$$

Nun ist aber $\sqrt{A}$ irrational, während x_1, y_1, x_2, y_2 ganze Zahlen sind. Aus Gleichung (31) folgt unmittelbar:

$$x_1 - x_2 = (y_2 - y_1)\sqrt{A}$$

Dies ist nicht möglich, da $x_1 - x_2$ eine ganze Zahl ist, während $(y_2 - y_1)\sqrt{A}$ als Produkt einer ganzen mit einer irrationalen Zahl irrational ist. Eine ganze Zahl kann aber nicht irrational sein.

Dieser Widerspruch verschwindet, wenn $x_1 = x_2$ und $y_1 = y_2$ ist, mit anderen Worten, wenn nicht zwei verschiedene Lösungen angenommen werden, sondern nur eine.
Wenn also eine Minimal-Lösung existiert, so auch nur eine.

Wir erwähnen jetzt noch eine sehr wichtige Eigenschaft der Lösungen von Gleichung (29). Es sei $[x_1, y_1]$ eine Lösung der Gleichung (29). Dann gilt

$$x_1^2 - Ay_1^2 = 1 \qquad \text{oder} \qquad (x_1 + \sqrt{A}y_1)(x_1 - \sqrt{A}y_1) = 1 \tag{32}$$

Wir erheben jetzt beide Seiten von (32) in die n-te Potenz (n positiv und ganzzahlig; d. Red.) und erhalten

$$(x_1 + \sqrt{A}y_1)^n(x_1 - \sqrt{A}y_1)^n = 1 \tag{33}$$

Entwickeln wir nach dem binomischen Satz, so kommt

$$(x_1 + \sqrt{A}y_1)^n = x_1^n + nx_1^{n-1}\sqrt{A}y + \frac{n(n-1)}{2}x_1^{n-2}Ay_1^2 + ... + (\sqrt{A})^n y^n = x_n + \sqrt{A}y_n \tag{34}$$

dabei sind x_n und y_n ganze Zahlen, da das erste, dritte und allgemein alle Glieder ungerader Nummer der Binomialentwicklung ganze Zahlen sind, während die Glieder gerader Nummer ganze, mit dem Faktor $\sqrt{A}$ multiplizierte Zahlen sind. Wenn wir die ganzzahligen Summanden und die Zahlen, die ein Vielfaches von $\sqrt{A}$ sind, einzeln zusammenfassen, so erhalten wir die Gleichung (34).

Die Zahlen x_n und y_n bilden, wie wir jetzt zeigen werden, ebenfalls eine Lösung von Gleichung (29). Aus Gleichung (34) erhalten wir die Gleichung

$$(x_1 - \sqrt{A}y_1)^n = x_n - \sqrt{A}y_n \tag{35}$$

wenn wir das Vorzeichen von $y\sqrt{A}$ wechseln. Multiplizieren wir die Gleichungen (34) und (35) und benutzen wir (33), so erhalten wir schließlich

$$(x_1 + \sqrt{A}y_1)^n(x_1 - \sqrt{A}y_1)^n = (x_n + \sqrt{A}y_n)(x_n - \sqrt{A}y_n) = x_n^2 - Ay_n^2 = 1 \tag{36}$$

d.h., $[x_n, y_n]$ ist ebenfalls eine Lösung der Gleichung (29).
Wir können jetzt den grundlegenden Satz über die Auflösung der Gleichung (29) beweisen. ‘

Satz II. Jede Lösung der Gleichung (29)

$$x^2 - Ay^2 = 1$$

hat bei positivem nichtquadratischem A die Form $[\pm x_n, \pm y_n]$, wobei

$$x_n = \frac{1}{2}[(x_0+y_0\sqrt{A})^n+(x_0-y_0\sqrt{A})^n] \quad , \quad y_n = \frac{1}{2\sqrt{A}}[(x_0+y_0\sqrt{A})^n-(x_0-y_0\sqrt{A})^n] \tag{37}$$

und $[x_0, y_0]$ die Minimal-Lösung ist.

Beweis. Wir nehmen im Gegensatz dazu an, es existiere eine Lösung $[x', y']$ der Gleichung (29) in ganzen positiven Zahlen, derart, dass die Gleichung

$$x' + \sqrt{A}y' = (x_0 + \sqrt{A}y_0)^n \tag{38}$$

bei keinem ganzzahligen positiven n gilt. Wir betrachten die Zahlen

$$x_0 + \sqrt{A}y_0, \quad (x_0 + \sqrt{A}y_0)^2, \quad (x_0 + \sqrt{A}y_0)^3, \quad ...$$

Sie bilden eine Folge positiver unbegrenzt wachsender Zahlen, da $x_0 \geq 1$, $y_0 \geq 1$ und $x_0 + \sqrt{A}y_0 > 1$ ist. Da $[x_0, y_0]$ Minimal-Lösung ist, gilt nach Definition

$$x' + \sqrt{A}y' > x_0 + \sqrt{A}y_0$$

Daher kann man immer ein solches $n \geq 1$ finden, dass

$$(x_0 + \sqrt{A}y_0)^n < x' + \sqrt{A}y' < (x_0 + \sqrt{A}y_0)^{n+1} \tag{39}$$

gilt. Nun ist aber $x_0 - \sqrt{A}y_0$ positiv, wegen

$$(x_0 + \sqrt{A}y_0)(x_0 - \sqrt{A}y_0) = x_0^2 - Ay_0^2 = 1 > 0$$

Darum bleiben bei der Multiplikation aller Glieder der Ungleichungen (39) mit ein und derselben positiven Zahl $(x_0 - \sqrt{A}y_0)^n$ die Vorzeichen der einzelnen Terme erhalten. Wir bekommen

$$(x_0 + \sqrt{A}y_0)^n(x_0 - \sqrt{A}y_0)^n < (x' + \sqrt{A}y')(x_0 - \sqrt{A}y_0)^n < (x_0 + \sqrt{A}y_0)^{n+1}(x_0 + \sqrt{A}y_0)^n \tag{40}$$

Wegen

$$(x_0 + \sqrt{A}y_0)^n(x_0 - \sqrt{A}y_0)^n = (x_0^2 - Ay_o^2) = 1 \tag{41}$$

ist

$$(x_0 + \sqrt{A}y_0)^{n+1}(x_0 - \sqrt{A}y_0)^n = x_0 + \sqrt{A}y_0 \tag{42}$$

Außerdem ist

$$\begin{aligned}(x' + \sqrt{A}y')(x_0 - \sqrt{A}y_0)^n = (x' + \sqrt{A}y')(x_n - \sqrt{A}y_n) = \\ x'x_n + Ay'y_n + \sqrt{A}(y'x_n - x'y_n) = \overline{x} + \sqrt{A}\overline{y}\end{aligned} \tag{43}$$

wobei $\overline{x}$ und $\overline{y}$ ganze Zahlen sind und

$$x_n - \sqrt{A}y_n = (x_0 - \sqrt{A}y_0)^n$$

gilt. Benutzen wir die Beziehungen (41), (42), (43) und die Ungleichungen (40), so erhalten wir die Ungleichungen

$$1 < \overline{x} + \sqrt{A}\overline{y} < x_0 + \sqrt{y}_0 \tag{44}$$

Wir zeigen, dass das Paar $\overline{x}, \overline{y}$ eine Lösung der Gleichung (29) ist.
Multiplizieren wir nämlich die linken und die rechten Seiten der Gleichung (43), d.h. der Gleichung

$$\overline{x} + \sqrt{A}\overline{y} = (x' + \sqrt{A}y')(x_0 - \sqrt{A}y_0)^n \tag{45}$$

und der Gleichung

$$\overline{x} - \sqrt{A}\overline{y} = (x' - \sqrt{A}y')(x_0 + \sqrt{A}y_0)^n \tag{46}$$

die sich unmittelbar aus (43) ergibt, wenn man das Vorzeichen von $y\sqrt{A}$ ändert, miteinander, so erhalten wir

$$\begin{aligned}(\overline{x} + \sqrt{A}\overline{y})(\overline{x} - \sqrt{A}\overline{y}) &= \overline{x}^2 - \overline{y}^2 \\ &= (x' + \sqrt{A}y')(x' - \sqrt{A}y')(x_0 - \sqrt{A}y_0)^n(x_0 + \sqrt{A}y_0)^n \\ &= (x'^2 - Ay'^2)(x_0^2 - Ay_0^2) = 1\end{aligned} \tag{47}$$

da $[x', y']$ und $[x_0, y_0]$ Lösungen der Gleichung (29) sind. Wir beweisen schließlich, dass $\overline{x}$ und $\overline{y}$ beide positiv sind. Zunächst ist klar, dass $\overline{x}$ nicht gleich Null sein kann. Wäre $\overline{x}$ gleich Null, so folgte aus Gleichung (47)

$$-A\overline{y}^2 = 1$$

Dies ist aber nicht möglich, da A positiv ist.

Ferner folgte, falls $\overline{y} = 0$ wäre, $\overline{x}^2 = 1$, aus Ungleichung (44) jedoch $\overline{x} > 1$, was nicht möglich ist.
Außerdem stellen wir fest, dass die Vorzeichen von $\overline{x}$ und $\overline{y}$ gleich sein müssen. Wären nämlich die Vorzeichen von $\overline{x}$ und $\overline{y}$ verschieden, so hätten $\overline{x}$ und $-\overline{y}$ gleiche Vorzeichen.

Vergleichen wir dann die absoluten Beträge der Zahlen $\overline{x} + \sqrt{2}\overline{y}$ und $\overline{x} - \sqrt{A}\overline{y}$, so müsste der erstere kleiner als der zweite sein, da wir im ersten Fall die Differenz zweier Zahlen gleichen Vorzeichens zu bilden haben, im zweiten aber die Summe. Nun wissen wir schon, dass

$$\overline{x}\sqrt{A}\overline{y} > 1$$

ist; also ist $\overline{x} - \sqrt{2}\overline{y}$ auch dem absoluten Betrage nach größer als Eins. Nun gilt

$$(\overline{x} + \sqrt{A}\overline{y})(\overline{x} + \sqrt{A}\overline{y}) = \overline{x}^2 - A\overline{y}^2 = 1$$

und wir kommen auf einen Widerspruch, da das Produkt zweier Zahlen, deren absoluter Betrag größer als Eins ist, ebenfalls dem Betrage nach größer als Eins sein muss. Somit haben $\overline{x}$ und $\overline{y}$ gleiche Vorzeichen, und es gilt $\overline{x} \neq 0$ und $\overline{y} \neq 0$. Dann folgt aber aus Ungleichung (44) unmittelbar, dass $\overline{x} > 0$ und $\overline{y} > 0$ ist.

Aus der Annahme, dass eine solche Lösung $[x', y']$ der Gleichung

$$x^2 - Ay^2 = 1, \qquad A > 0$$

existiert, für welche Gleichung (38) bei keinem ganzzahligen positiven n gilt, konnten wir eine Lösung $[\overline{x}, \overline{y}]$ ($\overline{x} > 0$, $\overline{y} > 0$, $\overline{x}$ und $\overline{y}$ ganzzahlig) konstruieren, die den Ungleichungen (44) genügt, welche im Widerspruch zur Definition der Minimal-Lösung $[x_0, y_0]$ stehen.
Somit haben wir bewiesen, dass die Annahme der Existenz einer Lösung, die nicht durch die Formel (38) dargestellt wird, auf einen Widerspruch führt.
Mit anderen Worten: wir haben bewiesen, dass man alle Lösungen unserer Gleichung aus Formel (38) erhält.

Somit ergibt sich jede Lösung $[x, y]$ der Gleichung (29) aus

$$x + \sqrt{A}y = (x_0 + \sqrt{A}y_0)^n, \qquad n > 0 \tag{48}$$

wobei $[x_0, y_0]$ die Minimal-Lösung ist. Ändern wir in dieser letzten Gleichung das Vorzeichen von $y\sqrt{A}$, so erhalten wir die Gleichung

$$x - \sqrt{A}y = (x_0 - \sqrt{A}y_0)^n \tag{49}$$

Durch Addition und Subtraktion dieser Gleichungen und Division beider Seiten durch 2 bzw. durch 2 $\sqrt{A}$ erhalten wir

$$\left.\begin{array}{l} x = x_n = \frac{1}{2}[(x_0 + \sqrt{A}y_0)^n + (x_0 - \sqrt{A}y_0)^n] \\ y = y_n = \frac{1}{2\sqrt{A}}[(x_0 + \sqrt{A}y_0)^n - (x_0 - \sqrt{A}y_0)^n] \end{array}\right\} \tag{50}$$

m.a.W., explizite Ausdrücke für alle Lösungen $[x, y]$ mit positivem x und y. Hieraus erhält man alle Lösungen, wenn man die Vorzeichen bei x_n und y_n variiert.

Da wir weiter oben schon gesehen hatten, dass die Minimal-Lösung für die Gleichung $x^2 - 2y^2 = 1$ das Paar $x = 3, y = 2$ ist, werden z.B. alle Lösungen dieser Gleichung somit durch die Formeln

$$x_n = \frac{1}{2}[(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n]$$
$$y_n = \frac{1}{2\sqrt{2}}[(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n]$$

geliefert.
Für $n = 1, 2, 3$ erhalten wir die Lösungen $[3, 2]$, $[17, 12]$ und $[99, 70]$.

Wir bemerken noch, dass die Zahlen x_n und y_n bei wachsendem n in der Größenordnung einer geometrischen Reihe mit dem Quotienten $x_0 + \sqrt{A}y_0$ wachsen, da wir infolge der Gleichung

$$(x_0 + \sqrt{A}y_0)(x_0 - \sqrt{A}y_0) = 1$$

die Ungleichung

$$0 < x_0 - \sqrt{A}y_0 < 1$$

aufstellen können. Hieraus folgt, dass $(x_0 - \sqrt{A}y_0)^n$ mit wachsendem n gegen Null strebt.

Wenn also die Gleichung (29) mindestens eine nichttriviale Lösung hat, d.h. wenn eine Lösung mit $y \neq 0$ existiert, so existiert die Minimal-Lösung dieser Gleichung, und alle Lösungen ergeben sich durch die Formeln (50).
Die Frage nach der Existenz einer nichttrivialen Lösung dieser Gleichung bei beliebigem ganzzahligem positivem nichtquadratischem A haben wir bisher offengelassen; ihr wenden wir uns nun zu.

5 Die allgemeine Gleichung zweiten Grades mit zwei Unbekannten

Wir werden in diesem Paragraphen beweisen, dass bei beliebigem ganzzahligem positivem nichtquadratischem A ($\sqrt{A}$ also irrational) die Gleichung[6]

$$x^2 - Ay^2 = 1 \tag{51}$$

immer eine nichttriviale Lösung hat. Es existiert also immer ein Paar ganzer Zahlen x_0, y_0 mit $x_0, y_0 \neq 0$, das dieser Gleichung genügt.

Zuerst zeigen wir, wie man eine beliebige positive Zahl in einen Kettenbruch entwickelt. Weiter oben hatten wir zur Entwicklung der Zahl $\sqrt{2}$ in einen Kettenbruch besondere Eigenschaften von $\sqrt{2}$ benutzt.

Es sei α eine beliebige positive Zahl. Dann existiert stets eine ganze Zahl, die kleiner oder gleich α und größer als $\alpha - 1$ ist. Eine solche Zahl heißt der ganzzahlige Anteil von α und wird mit $[\alpha]$ bezeichnet.
Die Differenz zwischen α und seinem ganzzahligen Anteil wird der gebrochene Anteil der Zahl α genannt und mit $\{\alpha\}$ bezeichnet. Aus der Definition des ganzzahligen und des gebrochenen Anteils der Zahl α folgen unmittelbar die Beziehungen

$$\alpha - [\alpha] = \{\alpha\} \qquad , \qquad \alpha = [\alpha] + \{\alpha\} \tag{52}$$

Da der gebrochene Anteil einer Zahl gleich der Differenz zwischen einer positiven Zahl und einer ganzen Zahl ist, die nicht größer ist als diese positive Zahl, ist der gebrochene Anteil immer kleiner als Eins und nichtnegativ. Beispielsweise ist von $\frac{27}{5}$ der ganzzahlige Anteil 5 und der gebrochene Anteil $\frac{2}{5}$; der ganzzahlige Anteil von $\sqrt{2}$ ist 1, der gebrochene $\sqrt{2} - 1$; von $\sqrt[3]{52}$ ist der ganzzahlige Anteil 3, der gebrochene $\sqrt[3]{52} - 3$, usw.

Diese Begriffe können wir bei der Entwicklung einer Zahl in einen Kettenbruch verwenden. Setzen wir

$$[\alpha] = q_1 \qquad ; \qquad \{\alpha\} = \frac{1}{\alpha_1}$$

so gilt

$$\alpha = q_1 + \frac{1}{\alpha_1} \tag{53}$$

Da $\{\alpha\}$ immer kleiner als Eins ist, ist α_1 stets größer als Eins. Wäre α selbst eine ganze Zahl, so wäre der gebrochene Anteil Null und wir würden die Gleichung $\alpha = q_1$ erhalten. Dieser spezielle Fall kommt hier nicht vor, da wir ja. eine irrationale Zahl in einen Kettenbruch entwickeln.
Wir können also sagen, dass α_1 eine positive Zahl größer als Eins ist. Mit dieser Zahl α_1 verfahren wir genauso wie mit α und schreiben

$$\alpha_1 = q_2 + \frac{1}{\alpha_2}, \qquad q_2 = [\alpha_1], \qquad \frac{1}{\alpha_2} = \{\alpha_1\}$$

[6] In der zahlentheoretischen Literatur ist der Name "Pellsche Gleichung" gebräuchlich (d. Red.).

Setzen wir dieses Verfahren fort, so erhalten wir die Gleichungen

$$\left.\begin{array}{ll} \alpha = q_1 + \frac{1}{\alpha_1}, & q_1 = [\alpha], \\ \alpha_1 = q_2 + \frac{1}{\alpha_2}, & q_2 = [\alpha_1], \\ \alpha_2 = q_3 + \frac{1}{\alpha_3}, & q_3 = [\alpha_3], \\ \ldots & \\ \alpha_{n-1} = q_n + \frac{1}{\alpha_n}, & q_n = [\alpha_{n-1}], \\ \ldots & \end{array}\right\} \tag{54}$$

Dieses Verfahren der schrittweisen Ermittlung der ganzen Zahlen $q_1, q_2, a_3, ..., q_n, ...$ unterscheidet sich, wie man leicht feststellt, in dem Fall, dass α eine rationale Zahl, $\alpha = \frac{a}{b}$ (a, b ganz und positiv) ist, in nichts von der Bestimmung der unvollständigen Quotienten durch den Euklidischen Algorithmus (s. Formeln (6)).

Das Verfahren muss also bei rationalem α nach endlich vielen Schritten abbrechen. Bei irrationalem α bricht der Prozess nicht ab. Wäre nämlich für irgendein n die Größe α_n eine ganze Zahl, so folgte daraus, dass α_{n-1} rational wäre, was zur Folge hätte, dass α_{n-2} rational wäre usw.
Schließlich wäre α_1 rational. Durch sukzessives Einsetzen von α_1, α_2, ..., α_{n-1} erhalten wir aus den Formeln (54) den Kettenbruch

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + ... + \cfrac{1}{q_n + \cfrac{1}{\alpha_n}}}} \tag{55}$$

Da n beliebig groß genommen werden kann, können wir (55) auch als unendlichen Kettenbruch schreiben:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + ... + \cfrac{1}{q_n + ...}}}$$

Wie wir bereits in § 4 erwähnten, bleibt die Beziehung (8) zwischen den Näherungsbrüchen auch für unendliche Kettenbrüche gültig. Wir sahen bereits oben, dass aus der Beziehung (8) für Näherungsbrüche gerader Nummer die Ungleichung (25) folgt.

Die Ungleichung (25) bildet ihrerseits wieder die Grundlage für den Beweis der Existenz von Lösungen der Gleichung (51), jedoch wird dieser Beweis schwieriger als im Spezialfall $A = 2$.

Für ein eingehenderes Studium der Theorie der Kettenbrüche verweisen wir den Leser auf das Buch von Prof. A. J. Chintschin, "Kettenbrüche".[7]

Satz III. Bei beliebigem ganzem positivem nichtquadratischem A hat die Gleichung (51)

$$x^2 - Ay^2 = 1$$

eine nichttriviale Lösung $[x_0, y_0]$ mit $x_0 > 0$ und $y_0 > 0$.

[7] Den deutschen Leser verweisen wir auf O. Perron, "Kettenbrüche".

Beweis: Da der Beweis für die Existenz einer Lösung der Gleichung (51) etwas kompliziert ist, führen wir ihn in mehreren Schritten durch.
Der erste Schritt wird damit abschließen, dass wir die Existenz einer ganzen positiven Zahl k bewiesen haben, welche die Eigenschaft besitzt, dass

$$x^2 - Ay^2 = k \tag{56}$$

unendlich viele Lösungen $[x, y]$ in ganzen positiven Zahlen x, y hat. Betrachten wir nämlich das Polynom $x^2 - Ay^2$ und setzen wir an Stelle von x und y die Zähler und Nenner aufeinanderfolgender Näherungsbrüche gerader Nummer der irrationalen Zahl $\alpha = \sqrt{A}$ ein, so erhalten wir

$$z_{2n} = P_{2n}^2 - AQ_{2n}^2 = (P_{2n} - \alpha Q_{2n})(P_{2n} + \alpha Q_{2n}) \tag{57}$$

Nun folgt aus

$$0 < P_{2n} + \alpha Q_{2n} < \frac{1}{Q_{2n+1}}$$

unmittelbar

$$0 < P_{2n} + \alpha Q_{2n} = 2\alpha Q_{2n} + P_{2n} - \alpha Q_{2n} = 2\alpha Q_{2n} + \frac{1}{Q_{2n+1}}$$

Wir verwenden die letzten beiden Ungleichungen zur Abschätzung von z_{2n}. Ersetzen wir die beiden Faktoren auf der rechten Seite von (57) mit Hilfe dieser Ungleichungen durch die größeren Werte, so erhalten wir für z_{2n} die Ungleichung

$$0 < z_{2n} < \frac{1}{Q_{2n+1}}(2\alpha Q_{2n} + \frac{1}{Q_{2n+1}} < 2\alpha + 1 \tag{58}$$

da Q_{2n} kleiner als Q_{2n+1} ist. Setzen wir in das Binom

$$z = x^2 - Ay^2$$

für x und y die Größen P_{2n} bzw. Q_{2n} ein, so nimmt z einen positiven ganzzahligen Wert an. Somit sind alle Zahlen $z_2, z_4, ..., z_{2n}, ...$ positiv, ganz und nicht größer als die Zahl $2\alpha + 1$.
Da aber $\alpha = \sqrt{A}$ irrational ist, ist der Kettenbruch unendlich. Das bedeutet, dass es unendlich viele solcher Zahlenpaare P_{2n}, Q_{2n} gibt.

Von den ganzen positiven Zahlen $z_2, z_4, ..., z_{2n}, ...$ sind nur endlich viele verschieden, da zwischen 1 und der wohlbestimmten Zahl $2\alpha+1$, die von n nicht abhängt, nicht mehr als $[2\alpha+1]$ ganze Zahlen liegen können.
Die unendliche Folge der Zahlen $z_2, z_4, ..., z_{2n}, ...$ besteht also nur aus sich irgendwie wiederholenden Zahlen der Folge $1, 2, 3, ..., [2\alpha + 1]$, wobei nicht einmal alle diese Zahlen in der Folge $z_2, z_4, ...,$ vorkommen müssen.
Da $z_2, z_4, ..., z_{2n}, ...$ eine unendliche Folge ist, jedoch nur endlich viele verschiedene Glieder hat, kommt eine Zahl k $(1 \leq k \leq [2\alpha + 1])$ in dieser Folge unendlich oft vor[8].

Unter den Zahlenpaaren $[P_2, Q_2], [P_4, Q_4]$, ..., $[P_{2n}, Q_{2n}], ...$ befinden sich also unendlich viele Paare, die beim Einsetzen in die Gleichung $z = x^2 - Ay^2$ ein und denselben Wert k liefern. Somit haben wir die Existenz einer ganzen positiven Zahl k bewiesen, für welche Gleichung (56) unendlich viele ganzzahlige Lösungen hat.

[8] Diese Schlussweise wird nach dem deutschen Mathematiker Dirichlet (1805-1859) das Drichletsche Schubfachverfahren genannt.

Wir nummerieren die Zahlenpaare, die eine Lösung von Gleichung (56) bei vorgegebenem k sind, neu und bezeichnen sie mit $[u_1, v_1]$, $[u_2, v_2]$, ..., $[u_n, v_n]$, ... So erhalten wir

$$u_n^2 - Av_n^2 = k \tag{59}$$

Wir bemerken, dass die Folge der Zahlenpaare $[u_1, v_1]$, $[u_2, v : 2]$, ..., $[u_n, v_n]$, ... eine Teilfolge der Paare ist, die jeweils aus Zähler und Nenner eines Näherungsbruches der Zahl an mit gerader Nummer bestehen.
Könnten wir $k = 1$ beweisen, so wäre schon gezeigt, dass Gleichung (51) unendlich viele ganzzahlige Lösungen hat. Da wir das so ohne weiteres nicht können, nehmen wir $k > 1$ an (im Fall $k = 1$ sei schon alles bewiesen) und kommen zum zweiten Schritt unseres Beweises.

Wir zeigen jetzt, dass von den Zahlenpaaren $[u_1 v_1]$, ..., $[u_n, v_n]$, ... unendlich viele Paare bei Division durch k ein und denselben Rest ergeben, m.a.W., dass zwei ganze nichtnegative Zahlen p und q, die kleiner als k sind, existieren, derart, dass für unendlich viele Paare $[u_1, v_1]$, ..., $[u_n, v_n]$, ... die Gleichungen

$$u_n = a_n k + p \qquad , \qquad v_n = b_n k + q \tag{60}$$

gelten; a_n und b_n sind die bei der Division von u_n und v_n durch k entstehenden Quotienten, p und q die Reste. Teilen wir u_n und v_n durch die ganze Zahl k ($k > 1$), so erhalten wir Beziehungen der Form (60), wobei die Reste wie stets zwischen 0 und $k - 1$ liegen.
Da diese Reste der Division sowohl von u_n als auch von v_n durch k jeweils nur Zahlen aus der endlichen Folge $0, 1, 2, ..., k - 1$ sein können, ist die Anzahl der möglichen Paare dieser Reste $k \cdot k = k^2$.

Dies ergibt sich auch daraus, dass jedem Paar $[u_n, v_n]$ ein Restepaar $[p_n, q_n]$ entspricht, wobei p_n und q_n einzeln nicht mehr als k verschiedene Werte annehmen können und somit die Anzahl der Paare nicht größer als k^2 ist.
Somit entspricht bei Division durch k jedem Paar ganzer Zahlen $[u_n, v_n]$ ein Reste- paar $[p_n, q_n]$. Nun ist aber die Zahl der verschiedenen Restepaare endlich (sie ist nicht größer als k^2), während die Anzahl der Paare $[u_n, v_n]$ unendlich ist.
Da in der Folge $[p_1, q_1]$, $[p_2, q_2]$, ..., $[p_n, q_n]$, ... nur endlich viele verschiedene Paare vorkommen, bedeutet das, dass mindestens ein Paar unendlich oft vorkommt.

Bezeichnen wir dieses Restepaar mit $[p, q]$, so ergibt sich gerade, dass unendlich viele Paare $[u_n, v_n]$ existieren, für die (60) gilt. Da nicht alle Paare $[u_n, v_n]$ bei vorgegebenen p und q, deren Existenz wir eben bewiesen haben, den Gleichungen (GO) genügen, nummerieren wir alle diejenigen Paare $[u_n, v_n]$, die den Gleichungen (GO) genügen, neu und bezeichnen sie mit $[R_n, S_n]$.
Somit ist die unendliche Folge $[R_1, S_1]$, $[R_2, S_2]$, ..., $[R_n, S_n]$, ... eine Teilfolge der Folge der Paare $[u_n, v_n]$, die ihrerseits eine Teilfolge der aus den Zählern und Nennern der Näherungsbrüche von α gerader Nummer gebildeten Paare ist. Die Zahlenpaare dieser Folge erfüllen die Gleichung (59) und liefern bei Division durch k jeweils ein und dieselben Reste p und q.

Nachdem wir die Existenz unendlich vieler Paare ganzer positiver Zahlen R_n und S_n nachgewiesen haben, kommen wir zum dritten und letzten Schritt unseres Beweises.
Zunächst stellen wir fest, dass die Zahlen der Paare $[R_n, S_n]$ als Zähler und Nenner von Näherungsbrüchen teilerfremd sind. Ersetzen wir nämlich in der Beziehung (24) k durch $2k$ und setzen wir $\delta_{2k} = \frac{P_{2k}}{Q_{2k}}$ und $\delta_{2k-1} = \frac{P_{2k-1}}{Q_{2k-1}}$, so erhalten wir aus Gleichung

$$\frac{P_{2k}}{Q_{2k}} - \frac{P_{2k-1}}{Q_{2k-1}} = \frac{1}{Q_{2k} Q_{2k-1}}$$

wenn wir beide Seiten mit $Q_{2k} \cdot Q_{2k-1}$ multiplizieren,

$$P_{2k}Q_{2k-1} - Q_{2k}P_{2k-1} = 1 \tag{61}$$

Diese Beziehung zwischen den ganzen Zahlen P_{2k}, Q_{2k}, $_{2k-1}$ und Q_{2k-1} zeigt folgendes: wenn P_{2k} und Q_{2k} einen gemeinsamen Teiler hätten, der größer als 1 wäre, so müsste die linke Seite dieser Gleichung ohne Rest durch diesen gemeinsamen Teiler teilbar sein.
Die rechte Seite der Gleichung ist aber gleich Eins und somit durch keine Zahl, die größer als 1 ist, teilbar.

Hiermit ist gezeigt, dass die Zahlen R_n und S_n, die nur Zähler und Nenner von Näherungsbrüchen sein können, teilerfremd sind. Aus den Beziehungen (7) folgt ferner unmittelbar

$$Q_2 < Q_4 < ... < Q_{2n} < ...$$

Da die Zahlen R_n und S_n teilerfremd sind und die Zahlen s_1, S_2, ..., S_n, ..., die der Folge der voneinander verschiedenen Zahlen Q_{2n} entnommen wurden, ebenfalls voneinander verschieden sind, folgt unmittelbar, dass in der unendlichen Folge der Brüche

$$\frac{R_1}{S_1}, \frac{R_2}{S_2}, ..., \frac{R_n}{S_n}, ...$$

keine gleichen Zahlen vorkommen. Wir schreiben zwei Gleichungen, die aus der Definition von R_n und S_n folgen, auf:

$$R_1^2 - AS_1^2 = (R_1 - \alpha S_1)(R_1 + \alpha S_1) = k \qquad \text{und} \tag{62}$$

$$R_2^2 - AS_2^2 = (R_2 - \alpha S_2)(R_2 + \alpha S_2) = k \tag{63}$$

dabei ist wie vorher $\alpha = \sqrt{A}$. Weiterhin ist

$$(R_1 - \alpha S_1)(R_2 + \alpha S_2) = R_1R_2 - AS_1S_2 + \alpha(R_1S_2 - S_1R_2) \tag{64}$$

da $\alpha^2 = A$ ist, und ebenso

$$(R_1 + \alpha S_1)(R_2 - \alpha S_2) = R_1R_2 - AS_1S_2 - \alpha(R_1S_2 - S_1R_2) \tag{65}$$

Nun liefern R_n und S_n bei Division durch k jeweils ein und dieselben, nicht von n abhängigen Reste. Folglich gilt infolge der Beziehungen (60)

$$R_n = c_nk + p \qquad , \qquad S_n = d_nk + q \tag{66}$$

Wir erhalten dann durch einfache Umformungen und Substitutionen die Gleichungen

$$\begin{aligned} R_1R_2 - AS_1S_2 &= R_1(c_2k + p) - AS_1(d_2k + p) \\ &= R_1[(c_2 - c_1)k + c_1k + p] - AS_1[(d_2 - d_1)k + d_1k + q] \\ &= R_1[(c_2 - c_1)k + R_1] - AS_1[(d_2 - d_1)k + S_1] \\ &= k[R_1(c_2 - c_1)AS_1(d - 2 - d_1)] + R_1^2 - AS_1^2 \\ &= k[R_1(c_2 - c_1) - AS_1(d_2 - d_1) + 1] = kx_1 \end{aligned} \tag{67}$$

in denen x_1 eine, ganze Zahl ist, da $R_1^2 - AS_1^2 = k$ gilt. Ebenso gilt

$$\begin{aligned} R_1S_2 - S_1R_2 &= R_1[(d_2 - d_1)k + d_1k + q] - S_1[(c_2 - c_1)k + c_1k + p] \\ &= R_1[(d_2 - d_1)k + S_1] - S_1[(c_2 - c_1)k + R_1] \\ &= k[R_1(d_2 - d_1) - S_1(c_2 - c_1)] = ky_1 \end{aligned} \tag{68}$$

wobei y_1 ebenfalls eine ganze Zahl ist. Wir wollen nun zeigen, dass y_1 nicht gleich Null ist. Wäre y_1 gleich Null, so würde

$$ky_1 = R_1S_2 - R_2S_1 = 0$$

gelten; daraus folgte

$$\frac{R_1}{S_1} = \frac{R_2}{S_2}$$

Die letzte Gleichung ist nicht möglich, da wir festgestellt haben, dass alle Brüche $\frac{R_n}{S_n}$ voneinander verschieden sind. Die Gleichungen (67) und (68) zeigen, dass

$$(R_1 - \alpha S_1)(R_2 + \alpha S_2) = kx_1 + \alpha k y_1 = k(x_1 + \alpha y_1) \tag{69}$$

und

$$(R_1 + \alpha S_1)(R_2 + \alpha S_2) = kx_1 - \alpha k y_1 = k(x_1 - \alpha y_1) \tag{70}$$

gelten. Multiplizieren wir die Gleichungen (62) und (63) miteinander und verwenden wir (69) und (70), so erhalten wir

$$\begin{aligned} k^2 &= (R_1^2 - AS_1^2)(R_2^2 - AS_2^2) = (R_1 - \alpha S_1)(R_2 + \alpha S_2)(R_1 + \alpha S_1)(R_2 - \alpha S_2) \\ &= k^2(x_1 + \alpha y_1)(x_1 - \alpha y_1) = k^2(x_1^2 - Ay_1^2) \end{aligned} \tag{71}$$

Wenn wir durch k^2 teilen, erhalten wir schließlich

$$x_1^2 - Ay_1^2 = 1 \tag{72}$$

Nun ist y_1 nicht gleich Null; das bedeutet, dass auch x_1 nicht gleich Null sein kann, denn sonst würde links eine negative Zahl, rechts jedoch Eins stehen. Somit fanden wir sogar unter der Voraussetzung, dass k ungleich Eins ist, zwei ganze von Null verschiedene Zahlen x_1 und y_1 die der Gleichung (51) genügen.

Damit ist die Theorie von Gleichungen des Typs (51) abgeschlossen, da wir wissen, dass solche Gleichungen bei ganzzahligem positivem nichtquadratischem A immer eine Lösung haben.
Mit Hilfe der Minimal-Lösung, deren Existenz damit bewiesen ist, können wir alle übrigen Lösungen konstruieren.

In der Praxis kann man die kleinste Lösung finden, indem man x_0 und y_0 passend auswählt.
Wir haben somit die Untersuchung des Falles $A > 0$ ($\alpha = \sqrt{A}$ irrational) für die Gleichung

$$x^2 - Ay^2 = 1$$

zu Ende geführt.

Ist $A > 0$ und $\alpha = \sqrt{A}$ eine ganze Zahl, so kann man die Gleichung in der Form

$$x^2 - \alpha^2 y^2 = (x + \alpha y)(x - \alpha y) = 1$$

schreiben; da α eine ganze Zahl ist, müssen, wenn x_0 und y_0 ganze Zahlen sind, welche die Gleichung erfüllen, die Gleichungen

$$x_0 + \alpha y_0 = 1 \qquad , \qquad x_0 - \alpha y_0 = 1$$

oder die Gleichungen

$$x_0 + \alpha y_0 = -1 \qquad , \qquad x_0 - \alpha y_0 = -1$$

einzeln gelten, da das Produkt zweier ganzer Zahlen dann und nur dann gleich Eins sein kann, wenn jede dieser Zahlen gleich $+1$ oder gleich -1 ist.

Diese beiden Systeme von zwei Gleichungen mit zwei Unbekannten x_0 und y_0 haben nur triviale Lösungen, nämlich $x_0 = 1$, $y_0 = 0$ und $x_0 = -1, y_0 = 0$.

Somit hat die Gleichung (51), wenn A gleich dem Quadrat einer ganzen Zahl ist, als Lösung in ganzen Zahlen nur die trivialen Lösungen $x_0 = \pm 1$ und $y_0 = 0$. Bei ganzzahligem negativen A hat die Gleichung (51) als Lösungen in ganzen Zahlen dieselben trivialen Lösungen. (Bei $A = -1$ hat die Gleichung die symmetrischen trivialen Lösungen $x_0 = 0$ und $y_0 = \pm 1$.)

Wir betrachten jetzt die Gleichung der allgemeineren Form

$$x^2 - Ay^2 = C \tag{73}$$

dabei sei $A > 0$ ganzzahlig, C ganzzahlig, $\alpha = \sqrt{A}$ irrational.
Wir sahen schon, dass für $C = 1$ diese Gleichung immer unendlich viele ganzzahlige Lösungen x und y hat. Bei beliebigen C und A hat diese Gleichung im allgemeinen keine Lösung.

Beispiel: Wir zeigen, dass die Gleichung

$$x^2 - 3y^2 = -1 \tag{74}$$

überhaupt keine Lösung in ganzen x und y hat.
Zunächst bemerken wir, dass das Quadrat einer ungeraden Zahl bei Division durch 8 immer den Rest 1 liefert. Da nämlich jede ungerade Zahl a in der Form $a = 2N + 1$ geschrieben werden kann, wobei N eine ganze Zahl ist, gilt

$$a^2 = (2N + 1)^2 = 4N^2 + 4N + 1 = 4N(N + 1) + 1 = 8M + 1 \tag{75}$$

Hierbei ist M eine ganze Zahl, da entweder N oder $N + 1$ eine gerade Zahl sein muss. Nun können, falls $[x_0, y_0]$ eine Lösung von (74) darstellt, die Zahlen x_0 und y_0 nicht gleichzeitig beide gerade oder ungerade sein. Wären nämlich x_0 und y_0 beide gleichzeitig gerade oder ungerade, so wäre $x_0^2 - 3y_0^2$ eine gerade Zahl und könnte nicht gleich -1 sein.
Wäre aber x_0 ungerade und y_0 gerade, so würde x_0^2 bei Division durch 4 den Rest 1 ergeben, die Zahl $3y_0^2$ wäre durch 4 teilbar, und $x_0^2 - 3y_0^2$ würde bei Division durch 4 den Rest 1 ergeben. Dies ist aber nicht möglich, da bei Division durch 4 die rechte Seite trivialerweise den Rest -1 oder 3 = 4 -1 liefert. Wäre schließlich x_0 gerade und y_0 ungerade, so wäre x_0^2 durch 4 teilbar, die Zahl $-3y_0^2$ könnte wegen (75) in der Form

$$-3y_0^2 = -3(8M + 1) = -24M - 3 = 4(-6M - 1) + 1$$

geschrieben werden; das würde bedeuten, dass die Zahl $-3y_0^2$ bei Division durch 4 den Rest 1 ergibt. Daher müsste $x_0^2 - 3y_0^2$ bei Division durch 4 als Rest wieder 1 liefern. Das ist, wie wir schon gesehen haben, nicht möglich.

Es kann daher keine zwei ganzen Zahlen x_0 und y_0 geben, welche die Gleichung (74) befriedigen.

Wir beschäftigen uns nicht mit der Frage, unter welchen Bedingungen für C und A die Gleichung (73) eine Lösung hat. Die Frage ist schwierig und wird mit Hilfe der allgemeinen Theorie der quadratischen Irrationalitäten in der algebraischen Zahlentheorie beantwortet.

Wir befassen uns mit dem Fall, dass (73) nichttriviale Lösungen hat. Wie früher werden wir eine Lösung $[x', y']$ als nichttrivial bezeichnen, wenn $x', y' \neq 0$ gilt. Wir nehmen an, Gleichung (73) habe eine nichttriviale Lösung $[x', y']$; m.a.W., es soll

$$x'^2 - Ay'^2 = C \tag{76}$$

gelten. Bei gleichem Wert für A betrachten wir die Gleichung

$$x^2 - Ay^2 = 1 \tag{77}$$

Sie hat unendlich viele ganzzahlige Lösungen bei positivem nichtquadratischem A. Jede Lösung $[\overline{x}, \overline{y}]$ hat die Form

$$\overline{x} = \pm x_n \qquad , \qquad \overline{y} = \pm y_n$$

wobei x_n und y_n durch die Formeln (50) gegeben werden. Da $[\overline{x}, \overline{y}]$ eine Lösung von (77) ist, gilt

$$\overline{x}^2 - A\overline{y}^2 = (\overline{x} + \alpha\overline{y})(\overline{x} - \alpha\overline{y}) = 1$$

Gleichung (76) ihrerseits kann in der Form

$$(x' + \alpha y')(x' - \alpha y') = C$$

geschrieben werden. Multiplizieren wir die letzten beiden Gleichungen miteinander, so erhalten wir

$$(x' + \alpha y')(\overline{x} + \alpha\overline{y})(x' - \alpha y')(\overline{x} - \alpha\overline{y}) = C \tag{78}$$

Nun gilt aber

$$(x' + \alpha y')(\overline{x} + \alpha\overline{y}) = x'\overline{x} + Ay'\overline{y} + \alpha(x'\overline{y} + y'\overline{x})$$

und ebenso

$$(x' - \alpha y')(\overline{x} - \alpha\overline{y}) = x'\overline{x} + Ay'\overline{y} - \alpha(x'\overline{y} + y'\overline{x})$$

Verwenden wir diese beiden Gleichungen, so können wir (78) in der Form

$$[x'\overline{x} + Ay'\overline{y} + \alpha(x'\overline{y} + y'\overline{x})][x'\overline{x} + Ay'\overline{y} - \alpha(x'\overline{y} + y'\overline{x})] = c$$

oder

$$(x'\overline{x} + Ay'\overline{y})^2 - A(x'\overline{y} - y'\overline{x})^2 = C$$

schreiben. Damit haben wir bewiesen, dass das Zahlenpaar $[x, y]$,

$$x = x'\overline{x} + Ay'\overline{y} \qquad , \qquad y = x'\overline{y} + y'\overline{x} \tag{79}$$

ebenfalls diese Gleichung befriedigt, sofern $[x', y']$ eine Lösung der Gleichung (73) ist; das Paar $[\overline{x}, \overline{y}]$ ist dabei eine beliebige Lösung der Gleichung (77).
Hiermit ist bewiesen, dass aus der Existenz einer einzigen Lösung der Gleichung (73) das Vorhandensein unendlich vieler Lösungen folgt.

Man kann natürlich nicht behaupten, dass die Formeln (79) alle Lösungen der Gleichung (73) liefern. In der Theorie der algebraischen Zahlen wird gezeigt, dass man alle ganzzahligen Lösungen der Gleichung (73) erhalten kann, indem man eine endliche wohlbestimmte, von A und C abhängige Anzahl von Lösungen dieser Gleichung nimmt und diese Lösungen mit Hilfe der Formeln (79) vermehrt.

Ist A negativ oder das Quadrat einer ganzen Zahl, so kann (73) nur endlich viele Lösungen haben.

Den Beweis dieser einfach zu beweisenden Aussage überlassen wir dem Leser. Die Auflösung der allgemeinsten diophantischen Gleichung zweiten Grades mit zwei Unbekannten, einer Gleichung der Form

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0 \tag{80}$$

wobei A, B, C, D, E, F ganze Zahlen sind, lässt sich durch Variablentransformation wieder auf eine Gleichung der Form (73) mit positivem oder negativem A zurückführen.
Daher verläuft sie, falls Lösungen existieren, analog wie bei den Gleichungen vom Typ (73).

Ziehen wir das Fazit des oben Behandelten, so können wir folgendes aussagen:
Eine Gleichung zweiten Grades mit zwei Unbekannten vom Typ (80) kann keine ganzzahligen Lösungen, endlich viele ganzzahlige Lösungen oder unendlich viele ganzzahlige Lösungen haben; dabei ergeben sich diese Lösungen aus einer endlichen Anzahl verallgemeinerter geometrischer Progressionen, die durch die Formeln (79) geliefert werden.

Vergleichen wir das Aufsuchen und die Art der ganzzahligen Lösungen der Gleichungen zweiten Grades mit zwei Unbekannten mit dem Aufsuchen der ganzzahligen Lösungen der Gleichungen ersten Grades, so stellen wir einen wesentlichen Unterschied fest.
Die Lösungen der Gleichungen ersten Grades bilden nämlich, wenn sie existieren, arithmetische Progressionen, während die Lösungen der Gleichungen zweiten Grades, wenn es unendlich viele gibt, aus endlich vielen verallgemeinerten geometrischen Progressionen entstehen. Für Gleichungen zweiten Grades sind also die Paare ganzer Zahlen, die Lösungen einer Gleichung sind, wesentlich seltener anzutreffen, als die Paare ganzer Zahlen, die Lösungen einer Gleichung ersten Grades sind. Dies ist nicht zufällig.

Es wird sich zeigen, dass Gleichungen von höherem als zweitem Grade mit zwei Unbekannten im allgemeinen nur endlich viele Lösungen haben können. Ausnahmen von dieser Regel sind äußerst selten.

6 Gleichungen höheren als zweiten Grades mit zwei Unbekannten

Gleichungen höheren als zweiten Grades mit zwei Unbekannten haben bis auf seltene Ausnahmen nur endlich viele Lösungen $[x, y]$ in ganzen Zahlen. Wir betrachten zunächst die Gleichung

$$a_0x^n + a_1x^{n-1}y + a_2x^{n-2}y^2 + ... + a_ny^n = c \tag{81}$$

dabei sei n eine ganze Zahl, die größer als Zwei ist; alle Zahlen $a_1, a_2, a_3, ..., a_n, c$ seien ganze Zahlen.

Wie zu Beginn dieses Jahrhunderts von A. Thue bewiesen wurde, hat eine solche Gleichung nur endlich viele Lösungen $[x, y]$ in ganzen Zahlen.
Eine Ausnahme ist in den Fällen möglich, in denen die linke homogene Seite dieser Gleichung eine Potenz eines homogenen Binoms ersten Grades oder eines homogenen Trinoms zweiten Grades ist.

Dann hat nämlich unsere Gleichung die Form

$$(ax + by)^n = c_0 \qquad \text{oder} \qquad (ax^2 + bxy + cy^2)^n = c_0$$

und lässt sich daher auf eine Gleichung ersten oder zweiten Grades zurückführen, da für die Existenz von Lösungen die Zahl c_0 die n-te Potenz einer ganzen Zahl sein muss.

Da die Methode von Thue schwierig ist, können wir sie hier nicht behandeln. Wir beschränken uns auf einige erläuternde Bemerkungen, die uns Hinweise auf das Prinzip des Beweises für die Endlichkeit der Anzahl der Lösungen der Gleichung (81) geben.[9]

Wir dividieren beide Seiten der Gleichung (81) durch y^n:

$$a_0\left(\frac{x}{y}\right)^n + a_1\left(\frac{x}{y}\right)^{n-1} + ... + a_{n-1}\frac{x}{y} + a_n = \frac{c}{y^n} \tag{82}$$

Zur Vereinfachung der Überlegungen setzen wir nicht nur voraus, alle Wurzeln der Gleichung

$$a_0z^n + a_1z^{n-1} + ... + a_{n-1}z + a_n = 0 \tag{83}$$

seien verschieden und es sei $a_0 \cdot a_n \neq 0$, sondern auch, dass die Wurzeln dieser Gleichung nicht Wurzeln einer Gleichung niedrigeren Grades mit ganzzahligen Koeffizienten sein können; dies erweist sich für uns als besonders wichtig.

In der höheren Algebra wird bewiesen, dass jede algebraische Gleichung mindestens eine Wurzel hat. Hieraus folgt dann schon ganz einfach auf Grund der Tatsache, da jedes Polynom ohne Rest durch $z-\alpha$ teilbar ist, sofern α eine Wurzel ist, dass ein Polynom in Form eines Produktes

$$a_0z^n + a_1z^{n-1} + ... + a_{n-1}z + a_n = a_0(z - \alpha_1)(z - \alpha_2)...(z - \alpha_n) \tag{84}$$

dargestellt werden kann, wobei $\alpha_1, \alpha_2, ..., \alpha_n$ die n Wurzeln des betreffenden Polynome sind. Benutzen wir diese Produktdarstellung eines Polynome, so können wir (82) in der Form

$$a_0\left(\frac{x}{y} - \alpha_1\right)\left(\frac{x}{y} - \alpha_2\right)...\left(\frac{x}{y} - \alpha_n\right) = \frac{c}{y^n} \tag{85}$$

[9] Literaturangaben zu dieser Frage findet man zum Beispiel im Artikel des Verfassers "Die Approximation algebraischer Zahlen durch algebraische Zahlen und die Theorie der transzendenten Zahlen", Fortschritte der Mathematik, Band 4, 4 (32), 1949, S. 19; Deutsche Literatur: E. Landau, Vorlesungen über Zahlentheorie, Bd. III, Hirzel, Leipzig 1927 (d. Red.).

schreiben.

Nehmen wir an, es existieren unendlich viele Lösungen $[x_k, y_k]$ von Gleichung (85) in ganzen Zahlen. Das würde bedeuten, dass auch Lösungen mit beliebig großen Absolutbeträgen von y_k existieren.
Würden unendliche viele Paare mit beschränktem y_k (d.h. mit absoluten Beträgen aller y_k kleiner als eine wohlbestimmte Zahl) und beliebig großen x_k existieren, so würde für diese x_k die linke Seite beliebig groß werden, während die rechte beschränkt ist; dies ist natürlich nicht möglich.

Wir könnten nun y_k sehr groß annehmen. Die rechte Seite von Gleichung (85) würde dann klein, (d.h. auch die linke Seite müsste klein sein. Nun ist die linke Seite ein Produkt von n Faktoren, die $\frac{x_k}{y_k}$ und die ganze Zahl a_0, welche nicht kleiner als 1 sein kann, enthalten.
Das bedeutet, dass die linke Seite nur dadurch klein werden kann, dass irgendeine der Differenzen

$$\frac{x_k}{y_k} - \alpha_m$$

einen kleinen Absolutbetrag hat. Offenbar kann diese Differenz nur dann klein werden, wenn α_m reell ist, d.h. wenn nicht $\alpha_m = a + bi$ mit $b \neq 0$ gilt. Andernfalls kann nämlich der absolute Betrag dieser Differenz nicht beliebig klein gemacht werden, da

$$\left|\frac{x_k}{y_k} - a - bi\right| = \sqrt{\left(\frac{x_k}{y_k} - a\right)^2 + b^2} > |b|$$

ist. Zwei dieser Differenzen, d h. zwei Faktoren der linken Seite von Gleichung (85) können nicht gleichzeitig einen kleinen Absolutbetrag haben, da alle Wurzeln verschieden sind und daher

$$\left|\left(\frac{x_k}{y_k} - \alpha_m\right) - \left(\frac{x_k}{y_k} - \alpha_s\right)\right| = |\alpha_m - \alpha_s| \neq 0 \tag{86}$$

ist. Hat eine der Differenzen einen absoluten Betrag kleiner als $\frac{1}{2}|\alpha_m - \alpha_s|$, so muss infolge (86) jede andere größer als $\frac{1}{2}|\alpha_m - \alpha_s|$ sein. Dies folgt daraus, dass der Absolutbetrag einer Summe niemals größer als die Summe der Absolutbeträge ist.
Da alle Zahlen α_m voneinander verschieden sind, ist die kleinste Differenz ihrem Absolutbetrag $|\alpha_m - \alpha_s|$ nach größer als Null ($m \neq s$.
Bezeichnen wir diesen Wert mit $2d$, so erhalten wir bei einem genügend großen y_k, das vorkommen muss, weil y_k unbeschränkt wächst,

$$\left|\frac{x_k}{y_k} - \alpha_m\right| < d \qquad \text{und} \qquad \left|\frac{x_k}{y_k} - \alpha_s\right| > d \tag{87}$$

$s = 1, 2, ..., n$, $s \neq m$.
Da der absolute Betrag eines Produktes gleich dem Produkt der absoluten Beträge ist, folgt aus Gleichung (85), dass

$$|a_0| \left|\frac{x_k}{y_k} - \alpha_1\right| ... \left|\frac{x_k}{y_k} - \alpha_{m-1}\right| \left|\frac{x_k}{y_k} - \alpha_m\right| \left|\frac{x_k}{y_k} - \alpha_{m+1}\right| ... \left|\frac{x_k}{y_k} - \alpha_n\right| = \frac{|c|}{|y_k|^n} \tag{88}$$

gilt. Ersetzen wir in dieser Gleichung jede der Differenzen $\left|\frac{x_k}{y_k} - \alpha_s\right|$, $s \neq m$ durch den kleineren Wert d und die Zahl $|a_0|$ durch 1 (kleiner kann die ganze Zahl $[a_0]$ nicht sein), so wird die linke Seite von (88) kleiner als die rechte, und wir erhalten die Ungleichung

$$d^{n-1}\left|\frac{x_k}{y_k} - \alpha_m\right| < \frac{|c|}{|y_k|^n} \qquad \text{oder} \qquad \left|\frac{x_k}{y_k} - \alpha_m\right| < \frac{c_1}{|y_k|^n}, \quad c_1 = \frac{|c|}{d^{n-1}} \tag{89}$$

wobei c_1 nicht von x_n und y_n abhängt. Zahlen α_m gibt es nicht mehr als n, aber Paare $[x_k, y_k]$, für welche bei irgendeinem Ungleichung (89) richtig sein muss, gibt es unendlich viele. Daher existiert ein m derart, dass für das entsprechende α_m die Ungleichung (89) durch unendlich viele $[x_k, y_k]$ erfüllt wird.

Mit anderen Worten: Wenn Gleichung (81) unendlich viele ganzzahlige Lösungen hat, so besitzt die algebraische Gleichung mit ganzzahligen Koeffizienten (83) eine solche Wurzel α, für die bei beliebig großem q die Ungleichung

$$\left|\alpha - \frac{p}{q}\right| < \frac{A}{q^n} \tag{90}$$

gilt; dabei ist A eine von p und q unabhängige konstante Zahl, p und q ganze Zahlen, n ist der Grad der Gleichung, welcher α genügt.
Wäre α eine beliebige reelle Zahl, so könnte man sie so wählen, dass unendlich viele Lösungen $[p, q]$ der Ungleichung (90) in ganzen p und q existieren würden.

Nun ist in unserem Fall α Wurzel einer algebraischen Gleichung mit ganzzahligen Koeffizienten. Solche Zahlen nennt man algebraisch; sie haben besondere Eigenschaften. Als Grad einer algebraischen Zahl bezeichnet man den Grad derjenigen algebraischen Gleichung niedrigsten Grades mit ganzzahligen Koeffizienten, der diese Zahl genügt.

Der norwegische Mathematiker A. Thue (1863-1922) bewies, dass für eine algebraische Zahl α vom Grade n die Ungleichung

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\frac{n}{2}+1}} \tag{91}$$

nur endlich viele Lösungen in ganzen p und q haben kann. Ist aber $n \geq 3$, so wird die rechte Seite der Ungleichung (90) bei hinreichend großem q kleiner als die rechte Seite der Ungleichung (91), da dann $n > \frac{n}{2} + 1$ ist.
Daher hat, wenn Ungleichung (91) nur endlich viele Lösungen in ganzen p und q haben kann, die Ungleichung (90) erst recht nur endlich viele Lösungen. Das bedeutet, dass die Gleichung (81) nur endlich viele Lösungen in ganzen Zahlen haben kann, wenn alle Wurzeln der Gleichung (83) nicht Wurzeln einer Gleichung niedrigeren als n-ten Grades mit ganzzahligen Koeffizienten sein können.

Bei $n = 2$ kann, wie man leicht feststellen kann, die Ungleichung (90) unendlich viele Lösungen in ganzen p und q bei einem gewissen A haben.

Der Satz von A. Thue wurde später noch wesentlich verschärft. Es sei nur noch erwähnt, dass die Methode für den Beweis dieses Satzes es prinzipiell nicht ermöglicht, eine obere Schranke für die Beträge der Lösungen anzugeben, d.h. eine obere Schranke für die möglichen Werte $|x|$ und $|y|$ in Abhängigkeit von den Koeffizienten $a_0, a_1, ..., a_n$ und c.

Dieses Problem ist auch heute noch offen. Die Methode von A. Thue ermöglicht es zwar nicht, eine Schranke für die Beträge der Lösungen zu finden, dafür ermöglicht sie es aber, eine wenn auch recht grobe Schranke für die Anzahl der Lösungen von Gleichung (83) anzugeben. Für einzelne Klassen von Gleichungen des Type (83) kann die Schranke wesentlich genauer angegeben werden. Der sowjetische Mathematiker B.N. Delaunay[10] bewies zum Beispiel, dass die Gleichung

$$ax^3 + y^3 = 1$$

[10]Weitere Literaturangaben zu dieser Frage sind in dem Artikel "Zahlentheorie" des Verfassers in "Mathematik in der UdSSR in 30 Jahren" (1917-1947), Staatsverlag für technisch-theoretische Literatur, 1948, zu finden.

bei ganzzahligem a außer der trivialen Lösung $x = 0, y = 1$ nicht mehr als eine Lösung in ganzen x und y haben kann. Weiterhin bewies er, dass die Gleichung

$$ax^3 + bx^2y + cxy^2 + dy^3 = 1$$

nicht mehr als fünf Lösungen in ganzen x und y bei ganzzahligen a, b, c, d haben kann.

Es sei $P(x, y)$ ein beliebiges Polynom mit ganzzahligen Koeffizienten, es gelte also

$$P(x, y) = \sum A_{ks} x^k y^s$$

wobei die A_{ks} ganze Zahlen sind. Wir nennen ein solches Polynom irreduzibel, wenn man es nicht als Produkt zweier anderer Polynome mit ganzzahligen Koeffizienten darstellen kann (natürlich sollen diese Faktoren keine bloßen Zahlen sein).

Mit Hilfe einer speziellen, sehr komplizierten Methode bewies der deutsche Mathematiker C.L. Siegel (geb. 1896), dass die Gleichung

$$P(x, y) = 0$$

wenn $P(x, y)$ ein irreduzibles Polynom höheren als zweiten Grades in x und y ist (d.h. wenn darin Glieder der Form $A_{ks}x^k y^s$, $k + s > 2$, vorkommen), nur dann unendlich viele Lösungen in ganzen x und y haben kann, wenn Zahlen $a_n, a_{n-1}, ..., a_0, a_{-1}, ..., a_{-n}$ und $b_n, b_{n-1}, ..., b_0, b_{-1}, ..., b_{-n}$ existieren, derart, dass wir bei Ersetzung von x und y in unserer Gleichung durch

$$x = a_n t^n + a_{n-1} t^{n-1} + ... + a_0 + \frac{a_{-1}}{t} + ... + \frac{a_{-n}}{t^n}$$
$$y = b_n t^n + b_{n-1} t^{n-1} + ... + b_0 + \frac{b_{-1}}{t} + ... + \frac{b_{-n}}{t^n}$$

die Identität

$$Px, y) \equiv 0$$

in t erhalten. Hierbei ist n eine ganze Zahl.

7 Algebraische Gleichungen höheren als zweiten Grades mit drei Unbekannten und einige Exponentialgleichungen

Für Gleichungen mit zwei Unbekannten konnten wir die Frage nach der Existenz endlich oder unendlich vieler ganzzahliger Lösungen beantworten.
Bei Gleichungen höheren als zweiten Grades mit mehr als zwei Unbekannten können wir das nur für sehr spezielle Klassen von Gleichungen. Um so weniger lässt sich in diesem letzten Fall die noch schwierigen Frage nach der Bestimmung aller ganzzahligen Lösungen solcher Gleichungen lösen.

Als Beispiel behandeln wir die sogenannte Fermatsche Vermutung.
Der hervorragende französische Mathematiker Pierre Fermat (1601-1665) stellte die Behauptung auf, dass die Gleichung

$$x^n + y^n = z^n \tag{92}$$

bei ganzem $n \geq 3$ keine Lösung in ganzen positiven x, y, z habe (der Fall $x = y = z = 0$ wird dadurch ausgeschlossen, dass x, y und z positiv sein sollen).

Obwohl Pierre Fermat behauptete, einen Beweis zu besitzen (wahrscheinlich nach der Deszendenz-Methode, von der weiter unten noch die Rede sein wird), konnte man bisher keinen Beweis finden.

Als der deutsche Mathematiker E. Kummer (1810-1893) ihn zu finden versuchte und eines Tages dachte, ihn gefunden zu haben, entdeckte er, dass eine Voraussetzung, die bei den gewöhnlichen ganzen Zahlen erfüllt ist, für komplizierte Zahlengebilde, auf die man bei den Untersuchungen des Fermatschen Problems ganz naturgemäß stößt, falsch ist.

Die sogenannten ganzen algebraischen Zahlen, d.h. die Wurzeln algebraischer Gleichungen mit ganzrationalen Koeffizienten, deren höchste Potenz den Koeffizienten 1 hat, können nämlich nicht eindeutig in Primfaktoren der gleichen algebraischen Art zerlegt werden.
Die gewöhnlichen ganzen Zahlen lassen sich (bis auf die Reihenfolge; d. Red.) eindeutig in Primfaktoren zerlegen. Zum Beispiel ist $6 = 2 \cdot 3$; es gibt keine andere Zerlegung in Primfaktoren innerhalb der natürlichen Zahlen.

Betrachten wir aber einmal die Menge aller ganzen algebraischen Zahlen $m + n\sqrt{-5}$, wobei m und n gewöhnliche ganze Zahlen sind. Man sieht leicht, dass sowohl die Summe als auch das Produkt zweier solcher Zahlen wieder eine solche Zahl ist.
Eine Menge von Zahlen, welche die Eigenschaft besitzt, dass Summe und Produkt zweier Elemente wieder zu dieser Menge gehören, nennt man einen Ring. In dem oben angeführten Ring sind u.a. die Zahlen 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ enthalten.

Jede dieser Zahlen ist in diesem Ring, wie man leicht feststellen kann, eine Primzahl, d.h., man kann sie nicht als Produkt zweier zum Ring gehöriger ganzer Zahlen, von denen keine gleich Eins ist, darstellen. Nun ist aber

$$6 = 2\dot{3} = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

die Zahl 6 kann also in unserem Ring nicht eindeutig in Primfaktoren zerlegt werden. Diese nicht eindeutige Zerlegbarkeit in Primfaktoren kann auch in anderen komplizierten Ringen ganzer algebraischer Zahlen auftreten.

Als Kummer diese Tatsache entdeckt hatte, fand er, dass sein Beweis der Fermatschen Vermutung falsch war. Zur Überwindung der Schwierigkeiten, die mit der Nichteindeutigkeit der Primfaktorenzerlegung zusammenhingen, wurde von KUMMER die Idealtheorie entwickelt. Diese Theorie spielt heute in Algebra und Zahlentheorie eine große Rolle.

Aber auch mit dieser neuen Theorie konnte Kummer die Fermatsche Vermutung nicht vollständig beweisen. Er bewies sie nur für solche n, die durch mindestens eine der sogenannten regulären Primzahlen teilbar sind. Wir wollen uns hier nicht mit dem Begriff der regulären Primzahl beschäftigen; es sei lediglich darauf hingewiesen, dass bis heute nicht bekannt ist, ob endlich oder unendlich viele dieser Zahlen existieren.

Die Fermatsche Vermutung ist heute für viele n bewiesen, insbesondere für beliebige n, die durch eine Primzahl, welche kleiner als 100 ist, teilbar sind.
Die Fermatsche Vermutung spielte eine große Rolle in der Entwicklung der Mathematik, da im Zusammenhang mit den Versuchen, sie zu beweisen, die Idealtheorie entwickelt wurde. Dazu sei aber noch bemerkt, dass diese Theorie auf ganz anderem Wege und aus anderem Anlass von dem berühmten russischen Mathematiker E.I. Solotarjow, der in der Blüte seines wissenschaftlichen Schaffens starb[11] entwickelt wurde.

Heute kann ein Beweis der Fermatschen Vermutung, insbesondere ein Beweis, der auf Überlegungen der Theorie der Teilbarkeit von Zahlen beruht, nur noch von "sportlichem" Interesse sein.
Freilich, sollte ein solcher Beweis mit einer neuen und fruchtbaren Methode gelingen, so kann seine Bedeutung im Zusammenhang mit der Bedeutung dieser Methode sehr groß sein.

Die Versuche von Amateurmathematikern, die Fermatsche Vermutung mit ganz elementaren Mitteln zu beweisen, haben heute keine Aussicht auf Erfolg. Elementare Überlegungen, die sich auf die Theorie der Teilbarkeit von Zahlen stützen, wurden schon von Kummer angewendet, und die Fortführung dieser Überlegungen durch hervorragendste Mathematiker hat bis jetzt nichts Wesentliches ergeben.

Wir führen hier den Beweis des Fermatschen Satzes für $n = 4$ durch, da die Deszendenz-Methode, auf der dieser Beweis beruht, auch an sich sehr interessant ist.

Satz IV. Die Fermatsche Gleichung

$$x^4 + y^4 = z^4 \tag{93}$$

hat keine Lösung in ganzen x, y und z ($xyz \neq= 0$).

Beweis. Wir beweisen sogar den schärferen Satz, dass die Gleichung

$$x^4 + y^4 = z^2 \tag{94}$$

keine Lösung in ganzen x, y und z hat ($xyz \neq 0$).
Aus diesem Satz folgt dann unmittelbar, dass Gleichung (93) keine Lösungen hat. Hat Gleichung (94) eine Lösung $[x, y, z]$ in ganzen nichtverschwindenden x, y, z, so kann man annehmen, diese Zahlen seien paarweise teilerfremd. Existierte nämlich eine Lösung, in der x und y einen größten gemeinsamen Teiler $d > 1$ haben, so gälte

$$x = dx_1 \qquad , \qquad y = dy_1$$

[11] und von dem deutschen Mathematiker R. Dedekind (1831-1916) (d. Red).

mit $(x_1, y_1) = 1$. Teilten wir beide Seiten von (94) durch d, so erhielten wir

$$x_1^4 + y_1^4 = \left(\frac{z}{d^2}\right)^2 = z_1^2 \tag{95}$$

Nun sind x_1 und y_1 ganze Zahlen, d.h., $z_1 = \frac{z}{d^2}$ ist ebenfalls eine ganze Zahl. Hätten z_1 und y_1 einen gemeinsamen Teiler $k > 1$, so müsste x_1^2 infolge (95) durch k teilbar sein; x_1 und k können also nicht teilerfremd sein. Somit haben wir folgendes bewiesen:

falls eine Lösung $[x, y, z]$ von (94) in ganzen von Null verschiedenen x, y, z existiert, so existiert eine Lösung in ganzen von Null verschiedenen teilerfremden x, y, z. Daher genügt es zu beweisen, dass Gleichung (94) keine Lösungen in ganzen von Null verschiedenen paarweise teilerfremden Zahlen hat.

Im Verlaufe unseres Beweises werden wir immer dann, wenn wir davon sprechen, dass Gleichung (94) eine Lösung hat, meinen, dass sie eine Lösung in ganzen positiven und paarweise teilerfremden Zahlen besitzt.

In § 3 haben wir gezeigt, dass alle Lösungen von Gleichung (12)

$$x^2 + y^2 = z^2 \tag{96}$$

in ganzen positiven paarweise teilerfremden Zahlen durch die Formeln (18) geliefert werden:

$$x = uv, \qquad y = \frac{u^2 - v^2}{2}, \qquad z = \frac{u^2 + v^2}{2} \tag{97}$$

dabei sind u und v zwei beliebige ungerade positive teilerfremde Zahlen.
Wir formen die Formeln (97), die alle Lösungen von (96) bestimmen, etwas um. Da u und v ungerade sind, erhalten wir, wenn wir

$$\frac{u+v}{2} = a \qquad , \qquad \frac{u-v}{2} = b \tag{98}$$

setzen, die Zahlen u und v durch die Gleichungen

$$u = a + b \qquad , \qquad v = a - b \tag{99}$$

wobei a und b ganze Zahlen sind, von denen wegen (98) eine gerade, die andere ungerade sein muss. Die Gleichungen (98) und (99) zeigen, dass jedem Paar ungerader teilerfremder Zahlen u und v ein Paar teilerfremder Zahlen a und b entspricht, die nicht beide gleichzeitig gerade oder ungerade sind; und dass jedem Paar teilerfremder Zahlen a und b, die nicht beide gleichzeitig gerade oder ungerade sind, ein Paar teilerfremder ungerader Zahlen u und v entspricht.

Ersetzen wir in den Formeln (97) u und v durch a und b, so stellen wir fest, dass alle Tripel ganzer positiver paarweise teilerfremder Zahlen x, y und z (x ist ungerade), welche eine Lösung von Gleichung (96) bilden, durch die Formeln

$$x = a^2 - b^2, \qquad y = 2ab, \qquad z = a^2 + b^2 \tag{100}$$

geliefert werden, wobei a und b zwei beliebige teilerfremde Zahlen sind, die nicht gleichzeitig gerade oder ungerade sind, wobei $x > 0$ sein muss.
Diese Formeln zeigen, dass x und y nicht gleichzeitig gerade oder ungerade sein können. Hat Gleichung (94) eine Lösung $[x_0, y_0, z_0]$, so ist

$$[x_0^2]^2 + [y_0^2]^2 = z_0^2$$

d.h., das Tripel (x_0^2, y_0^2, z_0) ist Lösung der Gleichung (96). Dann existieren aber zwei Zahlen a und b ($a > b$), die teilerfremd und nicht gleichzeitig gerade oder ungerade sind, derart, dass

$$x_0^2 = a^2 - b^2, \qquad y_0^2 = 2ab, \qquad z_0 = a^2 + b^2 \tag{101}$$

gilt.
Wir nehmen etwa an, x_0 sei ungerade und y_0 gerade. Die entgegengesetzte Annahme würde nichts ändern, da es dann genügen würde, x_0 durch y_0 zu ersetzen und y_0 durch x_0.

Nun wissen wir schon (siehe Gleichung (75)), dass das Quadrat einer ungeraden Zahl bei Division durch 4 den Rest 1 ergibt. Daher folgt aus Gleichung

$$x_0^2 = a^2 - b^2 \tag{102}$$

dass a ungerade und b gerade ist. Andernfalls würde die linke Seite dieser Gleichung bei Division durch 4 den Rest 1 ergeben, die rechte aber, da wir annehmen, a sei gerade und b ungerade, den Rest -1. Da a ungerade ist und $(a, b) = 1$ gilt, ist auch $(a, 2b) = 1$.
Dann folgt aber aus Gleichung

$$y_0^2 = 2ba \qquad \text{dass} \qquad a = t^2, \quad 2b = s^2 \tag{103}$$

gilt, wobei t und s irgendwelche ganze Zahlen sind. Aus der Beziehung (102) folgt aber, dass $[x_0, b, a]$ eine Lösung von (96) ist, d.h.

$$x_0 = m^2 - n^2, \qquad b = 2mn, \qquad a = m^2 + n^2$$

dabei sind m und n teilerfremde Zahlen, die nicht beide gleichzeitig gerade oder ungerade sind. Aus (103) erhalten wir

$$mn = \frac{b}{2} = \left(\frac{s}{2}\right)^2$$

hieraus folgt, da m und n teilerfremd sind, dass

$$m = p^2 \qquad , \qquad n = q^2 \tag{104}$$

ist; dabei sind p und q von Null verschiedene ganze Zahlen. Da $a = t^2$ und $a = m^2 + n^2$ gilt, ist

$$q^4 + p^4 = t^2 \tag{105}$$

Wegen

$$z_0 = a^2 + b^2 > a^2 \qquad \text{gilt} \qquad 0 < t = \sqrt{a} < \sqrt[4]{z_0} < z_0 \quad (z_0 > 1) \tag{106}$$

Setzen wir $q = x_1$, $p = y_1$ und $t = z_1$, so sehen wir, dass eine Lösung $[x_1, y_1, z_1]$ existieren muss, sofern eine Lösung $[x_0 \text{fl} y_0, z_0]$ existiert; dabei ist $0 < z_1 < z_0$.

Diesen Prozess der Bildung von Lösungen der Gleichung (94) kann man beliebig lange fortsetzen. Wir erhalten eine Folge von Lösungen

$$[x_0, y_0, z_0], \quad [x_1, y_1, z_1], \quad ..., [x_n, y_n, z_n], \quad ...$$

Die ganzen positiven Zahlen $z_0, z_1, z_2, ..., z_n, ...$ bilden eine monoton fallende Folge, d.h. für sie gilt die Ungleichung

$$z_0 > z_1 > z_2 > ... > z_n > ...$$

Nun können aber ganze positive Zahlen keine unendliche monoton fallende Folge bilden, da in einer solchen Folge nicht mehr als z_0 Glieder vorkommen können.

Unter der Annahme, dass Gleichung (94) eine Lösung $[x, y, z]$ in ganzen von Null verschiedenen x, y, z besitzt, kommen wir somit zu einem Widerspruch.

Es ist also bewiesen, dass Gleichung (94) keine solchen Lösungen hat.
Folglich hat auch Gleichung (93) keine Lösungen $[x, y, z]$ in positiven ganzen x, y, z, da $[x, y, z]$ eine Lösung von (94) ist, falls $[x, y, z]$ Lösung von (98) ist.

Die Beweismethode, die wir verwendeten, bestand in der Konstruktion einer unendlichen Folge von Lösungen mit unbeschränkt fallendem z aus einer einzigen Lösung. Man nennt sie die Deszendenz-Methode.

Wie wir schon weiter oben sagten, verhindert die Nichteindeutigkeit der Zerlegung ganzer Zahlen algebraischer Ringe in Primfaktoren des jeweiligen Ringes die Anwendung dieser Methode auf die Fermatsche Vermutung im allgemeinen Falle.[12]

Wir haben bewiesen, dass Gleichung (94) und damit die Gleichung

$$x^{4n} + y^{4n} = z^{2n}$$

keine Lösung in ganzen Zahlen hat. Es ist interessant, dass die Gleichung

$$x^4 + y^2 = z^2$$

unendlich viele Lösungen in ganzen Zahlen hat, zum Beispiel $x = 2$, $y = 3$, $z = 5$. Die Ermittlung der Form aller Lösungen dieser Gleichung in ganzen positiven x, y, z überlassen wir dem Leser.

Wir bringen noch ein weiteres Beispiel für die Deszendenz-Methode, verändern jedoch den Gedankengang ein wenig.

Beispiel. Wir beweisen, dass die Gleichung

$$x^4 + 2y^4 = z^2 \tag{107}$$

keine Lösungen in ganzen von Null verschiedenen x, y, z hat.
Nehmen wir an, Gleichung (107) habe eine Lösung $[x_0, y_0, z_0]$ in ganzen positiven Zahlen. Diese Zahlen können wir sogleich als teilerfremd annehmen, da, falls sie einen größten gemeinsamen Teiler $d > 1$ haben sollten, auch die Zahlen $\frac{x_0}{d}$, $\frac{y_0}{d}$, $\frac{z_0}{d}$ Lösungen von (107) sind.
Das Vorhandensein eines gemeinsamen Teilers zweier dieser Zahlen würde die Existenz eines gemeinsamen Teilers aller drei Zahlen zur Folge haben.

Wir nehmen außerdem an, z_0 habe den kleinsten Wert unter allen z in Lösungen von (107) in ganzen positiven x, y, z. Da $[x_0, y_0, z_0]$ eine Lösung von Gleichung (107) ist, ist $[x_0^2, y_0^2, z_0]$ eine Lösung der Gleichung

$$x^2 + 2y^2 = z^2 \tag{108}$$

[12] Zum weiteren Studium der Fermatschen Vermutung verweisen wir den Leser auf das Buch von A.J. Chintschin "Der große Fermatsche Satz"(russisch). Deutsche Literatur: W. Lietzmann, Der Pythagoreische Lehrsatz ... Leipzig 1951, E. Landau, Vorlesungen über Zahlentheorie III, Leipzig 1927. P. Bachmann, Das Fermatproblem ..., Berlin 1919 (d. Red.)

Verwenden wir die Formeln (19') aus § 3, die alle Lösungen von (108) in ganzen positiven Zahlen liefern, so sehen wir, dass zwei ganze positive teilerfremde Zahlen a und b existieren, die den Gleichungen

$$x_0^2 = \pm(a^2 - 2b^2), \qquad y_0^2 = 2ab, \qquad z_0 = a^2 + 2b^2 \tag{109}$$

genügen; dabei ist a ungerade.
Aus der Gleichung $y_0^2 = 2ab$ folgt, dass b gerade ist; denn y_0 ist gerade, y_0^2 also durch 4 teilbar, a jedoch ungerade. Da $\frac{b}{2}$ und a teilerfremd sind, folgt aus Gleichung

$$\left(\frac{y_0}{2}\right)^2 = a\frac{b}{2}$$

unmittelbar, dass

$$a = m^2 \qquad , \qquad \frac{b}{2} = n^2$$

gilt; dabei sind m und n ganze positive Zahlen, und es gilt $(m, 2n) = 1$. Nun folgt aber aus (109), dass

$$x_0^2 = \pm(a^2 - 2b^2) = \pm\left[a^2 - 8\left(\frac{b}{2}\right)^2\right] \tag{110}$$

ist, wobei x_0 und a ungerade sind.
Wir sahen schon, dass das Quadrat einer ungeraden Zahl bei Division durch 4 den Rest 1 ergibt. Daher liefert die linke Seite von (110) bei Division durch 4 den Rest 1; die Zahl $a^2 - 8\left(\frac{b}{2}\right)^2$ liefert bei Division durch 4 ebenfalls den Rest 1.
Das bedeutet, dass die Klammer auf der rechten Seite von Gleichung (110) nur mit dem Pluszeichen stehen kann. Jetzt kann man Gleichung (110) schon in der Form

$$x_0^2 = m^4 - 8n^4 \qquad , \qquad x_0^2 + 2(2n^2)^2 = (m^2)^2 \tag{111}$$

schreiben, wobei x_0, n und m ganze positive teilerfremde Zahlen sind. Die Zahlen x_0, $2n^2$ und m^2 bilden also eine Lösung von Gleichung (108), wobei x_0, $2n^2$ und m^2 teilerfremd sind.
Daher lassen sich infolge der Formeln (19') aus § 3 wieder solche ganzen Zahlen p und q (p ungerade, $(p, q) = 1$) finden, dass

$$2n^2 = 2pq, \qquad m^2 = p^2 + 2q^2, \qquad x_0 = \pm(p^2 - 2q^2) \tag{112}$$

gilt. Nun ist

$$p = s^2 \qquad , \qquad q = r^2$$

da $(p, q) = 1$ und $n^2 = pq$ gilt; s und r sind ganze teilerfremde Zahlen. Hieraus folgt schließlich die Beziehung

$$s^4 + 2r^2 = m^2 \tag{113}$$

Sie besagt, dass die Zahlen s, r, m eine Lösung der Gleichung (107) bilden. Nun folgt aber aus der oben abgeleiteten Gleichung

$$z_0 = a^2 + 2b^2 \qquad , \qquad a = m^2$$

dass $z_0 > m$ ist. Unter der Voraussetzung, dass $[x_0, y_0, z_0]$ eine Lösung ist, fanden wir eine andere Lösung $[s, r, m]$, wobei $0 < m < z_0$ gilt.

Dies widerspricht unserer Annahme, dass in der Lösung $[x_0, y_0, z_0]$ die Zahl z_0 den kleinsten

aller möglichen Werte haben soll. Somit führte die Annahme, dass Gleichung (107) eine Lösung hat, zu einem Widerspruch.
Damit ist der Beweis erbracht, dass diese Gleichung in ganzen von Null verschiedenen Zahlen nicht lösbar ist.

Wir überlassen es jetzt dem Leser zu beweisen, dass die Gleichungen

$$x^4 + 4y^4 = z^2, \qquad x^4 - y^4 = 2z^2, \qquad x^4 - y^4 = z^2, \qquad x^4 - 4y^4 = z^2$$

keine Lösungen in ganzen positiven Zahlen haben.

Zum Abschluss noch einige Bemerkungen über Exponentialgleichungen.
Die Gleichung

$$a^x + b^y = c^z \tag{114}$$

mit ganzen a, b, c, die weder Null noch Potenzen von 2 sind, kann nur endlich viele Lösungen in ganzzahligen x, y, z haben.
Diese Behauptung bleibt mit wenigen zusätzlichen Voraussetzungen in Kraft, wenn a, b und c beliebige algebraische Zahlen sind. Überdies kann die Gleichung

$$A\alpha_1^{x_1}...\alpha_n^{x_n} + B\beta_1^{y_1}...\beta_m^{y_m} + C\gamma_1^{z_1}...\gamma_p^{z_p} = 0 \tag{115}$$

wo A, B, C ganz $(ABC \neq 0)$, $\alpha_1, ..., \alpha_n$, $\beta_1, ..., \beta_m$, $\gamma_1, ...\gamma_p$ ganz und die Zahlen α, β, γ:

$$\alpha = \alpha_1...\alpha_n, \qquad \beta = \beta_1...\beta_m, \qquad \gamma = \gamma_1...\gamma_p$$

teilerfremd sind, nur endlich viele Lösungen in ganzen Zahlen $x_1, ..., x_n$, $y_1, ..., y_m$, $z_1, ..., z_p$ haben.
Diese Aussage lässt sich auch auf den Fall, dass A, B, C und $\alpha_i, \beta_k, \gamma_s$ algebraisch sind, verallgemeinern.

Gleichungen vom Typ (115) und ihre Verallgemeinerungen sind von großem Interesse, da in der Theorie der algebraischen Zahlen bewiesen wird, dass jeder algebraischen Gleichung vom Typ (81) eine gewisse Exponentialgleichung vom Typ (115) entspricht; dabei entspricht jeder Lösung von (81) eine Lösung von (115) in ganzen Zahlen.
Diese Zuordnung lässt sich auch auf Gleichungen allgemeineren Typs als (81) und (115) ausdehnen.