AℓZAGK-Seminar: Pellsche Gleichung: Kettenbruchverfahren und das Archimedische problema bovinum

Claas Grenzebach

25. Juni 2002

1 Die Pellsche Gleichung

> „Wenn Harolds Streitkräfte, die in 13 Quadrate aufgeteilt waren, mit ihm zusammen auch ein einziges großes Quadrat hätten bilden können, wie viele Männer müssen es dann gewesen sein?“

Mit anderen Worten ist $x^2 = 13y^2 + 1$ für x, $y \in \mathbb{N}$ zu lösen – dies ist ein spezieller Fall einer Pellschen Gleichung:

$$\boxed{a^2 - d \cdot b^2 = 1};$$

dabei ist d eine natürliche Zahl, die kein Quadrat ist. Man kann sich auf $a, b \in \mathbb{N}$ beschränken, da mit (a, b) auch $(-a, b)$, $(a, -b)$ und $(-a, -b)$ Lösungen darstellen. Offensichtlich gibt es immer die triviale Lösung $(1, 0)$, während $a = 0$ nie eintreten kann. Für nichttriviale Lösungen genügt es also, sogar $a, b \in \mathbb{N}^\times := \mathbb{N} \setminus \{0\}$ zu fordern. Im weiteren soll dies stets vorausgesetzt sein, soweit nichts anderes notiert ist.

Pellsche Gleichungen treten zum Beispiel bei der Bestimmung von Einheiten in reellquadratischen Zahlringen auf, es gilt:

$$\begin{aligned}\alpha = a + b\sqrt{d} \in \mathbb{Z}\big[\sqrt{d}\big] \text{ Einheit} &\Leftrightarrow N(\alpha) := \alpha\bar{\alpha} := (a + b\sqrt{d})(a - b\sqrt{d}) = \pm 1 \\ &\Leftrightarrow a^2 - d \cdot b^2 = \pm 1 \text{ lösbar.}\end{aligned}$$

Falls es überhaupt eine nichttriviale Lösung (a_1, b_1) der Pellschen Gleichung $a^2 - d \cdot b^2 = 1$ gibt, kann man unendlich viele weitere konstruieren: Für alle $n \in \mathbb{N}^\times$ ist nämlich $(a_1 + b_1\sqrt{d})^n (a_1 - b_1\sqrt{d})^n = 1$; definiert man $a_n + b_n\sqrt{d} := (a_1 + b_1\sqrt{d})^n$ durch Zerlegung[1] in einen rationalen und einen irrationalen Teil, so stellt auch (a_n, b_n) eine Lösung dar.

[1] Beispiel $n = 2$: $(a + b\sqrt{d})^2 = (a^2 + d \cdot b^2) + 2ab \cdot \sqrt{d}$

Ist (a_1, b_1) die kleinste Lösung der Pellschen Gleichung in $\mathbb{N}^\times$, erhält man auf diese Weise alle Lösungen und bezeichnet daher (a_1, b_1) als Fundamentallösung. Eine Möglichkeit, die Fundamentallösung zu bestimmen, ist das sogenannte Kettenbruchverfahren (siehe nächsten Abschnitt). Dieses liefert sogar die Existenz einer Fundamentallösung für alle $d \in \mathbb{N}^\times$, die kein Quadrat sind.

Läßt man auch Potenzen $n \in \mathbb{Z}$ zu, so reproduziert man für $n = 0$ die triviale Lösung, und für $n < 0$ ist einfach $a_n = a_{-n}$, $b_n = -b_{-n}$ wegen $(a_1 + b_1\sqrt{d})^{-n} = (a_1 - b_1\sqrt{d})^n$. Es gilt der

Satz 1: *Seien $(a_n,\, b_n)$ die Lösungen der Pellschen Gleichung $a^2 - d \cdot b^2 = 1$ mit $a_n + b_n\sqrt{d} := \big(a_1 + b_1\sqrt{d}\big)^n$, $n \in \mathbb{Z}$ und (a_1, b_1) als Fundamentallösung, so gilt für $n, m \in \mathbb{Z}$:*

$$a_{n\pm m} = a_n a_m \pm b_n b_m \cdot d; \qquad\qquad b_{n\pm m} = a_m b_n \pm a_n b_m.$$

Beweis. Man kann direkt berechnen:

$$\begin{aligned} a_{n\pm m} + b_{n\pm m}\sqrt{d} &= \big(a_1 + b_1\sqrt{d}\big)^{n\pm m} = \big(a_1 + b_1\sqrt{d}\big)^n \cdot \big(a_1 + b_1\sqrt{d}\big)^{\pm m} \\ &= \big(a_1 + b_1\sqrt{d}\big)^n \cdot \big(a_1 \pm b_1\sqrt{d}\big)^m = \big(a_n + b_n\sqrt{d}\big) \cdot \big(a_m \pm b_m\sqrt{d}\big) \\ &= a_n a_m \pm b_n b_m \cdot d + (a_m b_n \pm a_n b_m)\sqrt{d}. \end{aligned}$$

Durch Trennen in rationalen und irrationalen Anteil folgt die Behauptung. $

2 Kettenbrüche

Unter einer Kettenbruchentwicklung einer reellen Zahl r verstehen wir die Folge ganzer Zahlen (Koeffizienten) $(a_n)_{\mathbb{N}}$, die durch die Vorschrift:

$$\xi_0 := r; \qquad a_n := [\xi_n] \ (\geq 1 \text{ für } n \geq 1); \qquad \xi_{n+1} := \frac{1}{\xi_n - a_n} > 1$$

gebildet wird – falls eine der Restzahlen ξ_k ganz ist, ist die Entwicklung bei a_k abzubrechen, in dem Fall liegt ein endlicher Kettenbruch vor. Dieser weist eine Zweideutigkeit auf:

$$(a_0, \ldots, a_n, 1) = (a_0, \ldots, a_n + 1).$$

Beispiele für Kettenbruchentwicklungen sind:

$$\frac{11}{3} = 3 + \frac{2}{3} = 3 + \frac{1}{1 + \frac{1}{2}} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{1}}}; \qquad \sqrt{13} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \sqrt{13}}}}};$$

die Entwicklung der rationalen Zahl $\frac{11}{3}$ bricht offensichtlich ab, und die Entwicklung von $\sqrt{13}$ ist periodisch, wobei man die einzelnen Koeffizienten gemäß der Vorschrift in folgenden Schritten gewinnt:

$$\begin{aligned}
\frac{1}{\sqrt{13}-3} &= \frac{\sqrt{13}+3}{4} = 1 + \frac{\sqrt{13}-1}{4} \\
\frac{4}{\sqrt{13}-1} &= \frac{\sqrt{13}+1}{3} = 1 + \frac{\sqrt{13}-2}{3} \\
\frac{3}{\sqrt{13}-2} &= \frac{\sqrt{13}+2}{3} = 1 + \frac{\sqrt{13}-1}{3} \\
\frac{3}{\sqrt{13}-1} &= \frac{\sqrt{13}+1}{4} = 1 + \frac{\sqrt{13}-3}{4} \\
\frac{4}{\sqrt{13}-3} & \qquad\qquad = 3 + \sqrt{13}
\end{aligned}$$

Platzsparender als den Kettenbruch vollständig auszuschreiben ist es, nur die Koeffizienten der Kettenbruchentwicklung anzugeben (im weiteren sollen Kettenbrüche stets durch diese Kurzschreibweise charakterisiert werden):

$$\frac{11}{3} = (3,1,2) = (3,1,1,1); \quad \sqrt{13} = (3,1,1,1,1,3+\sqrt{13}) = (3,\overline{1,1,1,1,6});$$

der Balken gibt die periodische Wiederholung der Koeffizienten an.

In dem gewählten Beispiel stellt $\frac{11}{3}$ die nach dem vierten Koeffizienten abgebrochene Entwicklung von $\sqrt{13}$ dar. Hat allgemein $x \in \mathbb{R}$ die unendliche Kettenbruchentwicklung $(a_n)_{\mathbb{N}}$, so heißt die rationale Zahl $(a_0, \ldots, a_k) =: \frac{u_k}{v_k} \in \mathbb{Q}$ (gekürzt) der k-te Näherungsbruch von x. Diese Bezeichnung wird durch den folgenden Satz verständlich, in dem einige Eigenschaften von Kettenbrüchen zusammengefaßt sind:

Satz 2: *Genau die rationalen Zahlen* $\mathbb{Q}$ *werden durch* endliche *Kettenbrüche dargestellt, und zwar (im wesentlichen) eindeutig. Jeder* unendliche *(nichtabbrechende) Kettenbruch, genauer die Folge seiner Näherungsbrüche, konvergiert gegen eine irrationale Zahl mit der gegebenen Kettenbruchentwicklung, das heißt:*

$$\lim_{k\to\infty}(a_0, a_1, \ldots, a_k) = \lim_{k\to\infty}\frac{u_k}{v_k} = x = (a_0, a_1, a_2, \ldots) \in \mathbb{R}\setminus\mathbb{Q}.$$

Die Kettenbruchentwicklung von $x \in \mathbb{R}\setminus\mathbb{Q}$ *ist genau dann* periodisch, *wenn* x *quadratisch irrational ist, das heißt, Nullstelle eines quadratischen Polynoms.*[2]

Beweis. Wie man leicht sieht, ist jeder endliche Kettenbruch rational und jeder periodische eine quadratische irrationale Zahl. Die eigentliche Aussage des Satzes steckt in der Umkehrung.

[2]Man kann dann schreiben: $x = \frac{m+\sqrt{d}}{q}$ mit geeigneten ganzen Zahlen $d > 0$, m, $q | d - m^2$.

Für rationale Zahlen wird die Behauptung durch den euklidischen Algorithmus geliefert. Sei nämlich $\frac{u_0}{u_1} \in \mathbb{Q}$, u_0, $u_1 \in \mathbb{Z}$, dann hat man:

$$\begin{aligned}
u_0 &= a_0 u_1 + u_2 && \text{mit } 0 < u_2 < |u_1|, \\
u_1 &= a_1 u_2 + u_3 && \text{mit } 0 < u_3 < u_2, \\
&\vdots \\
u_{n-1} &= a_{n-1} u_n + u_{n+1} && \text{mit } 0 < u_{n+1} < u_n, \\
u_n &= a_n u_{n+1} && \text{mit } u_{n+1} = \text{ggT}(u_0, u_1),
\end{aligned}$$

und es gilt: $\frac{u_0}{u_1} = (a_0, \ldots, a_n)$, zur Eindeutigkeit vgl. oben.

Der Beweis zur Konvergenz einer beliebigen Folge von Näherungsbrüchen gegen eine irrationale Zahl soll hier ausgelassen werden, siehe dazu z. B. Forster, Algorithmische Zahlentheorie (1996). Jedenfalls erhält man dabei:

- $(a_0, \ldots, a_n, \frac{b}{c}) = \frac{r}{s} \Leftrightarrow \left(\begin{smallmatrix} r \\ s \end{smallmatrix}\right) = A_0 \cdot \ldots \cdot A_n \cdot \left(\begin{smallmatrix} b \\ c \end{smallmatrix}\right)$ mit $A_j = \left(\begin{smallmatrix} a_j & 1 \\ 1 & 0 \end{smallmatrix}\right)$
- Speziell gilt für Näherungsbrüche: $\left(\begin{smallmatrix} u_k \\ v_k \end{smallmatrix}\right) = A_0 \cdot \ldots \cdot A_{k-1} \cdot \left(\begin{smallmatrix} a_k \\ 1 \end{smallmatrix}\right) = A_0 \cdot \ldots \cdot A_k \cdot \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \Rightarrow \left(\begin{smallmatrix} u_k & u_{k-1} \\ v_k & v_{k-1} \end{smallmatrix}\right) = A_0 \cdot \ldots \cdot A_k$
- Außerdem: $x = (a_0, \ldots, a_k, \xi_{k+1}) = \left(\begin{smallmatrix} u_k & u_{k-1} \\ v_k & v_{k-1} \end{smallmatrix}\right)\left(\begin{smallmatrix} \xi_{k+1} \\ 1 \end{smallmatrix}\right)$
- Also:

$$\forall k \in \mathbb{N}^\times : \quad x = \frac{u_k \xi_{k+1} + u_{k-1}}{v_k \xi_{k+1} + v_{k-1}} \quad \wedge \quad u_k v_{k-1} - v_k u_{k-1} = (-1)^{k+1}. \qquad (*)$$

Es bleibt zu zeigen, daß quadratische irrationale Zahlen eine periodische Kettenbruchentwicklung haben. Sei also $x = \frac{m_0 + \sqrt{d}}{q_0}$ gegeben mit ganzen Zahlen $d > 0$ (kein Quadrat), m_0, $q_0 | d - m_0^2$. Dann können alle Restzahlen ξ_k ebenfalls in dieser Form geschrieben werden:

$$\xi_k = \frac{m_k + \sqrt{d}}{q_k} \quad \text{mit ganzen Zahlen } m_k, q_k \text{ und } q_k q_{k-1} = d - m_k^2,$$

wie man per Induktion zeigt:

Für $k = 0$ ist $x = \xi_0$ und daher $q_{-1} := (d - m_0^2)/q_0 \in \mathbb{Z}$ zu setzen. Nun gelte die Behauptung für k, dann hat man:

$$\xi_{k+1} \overset{\text{Def.}}{=} \frac{1}{\xi_k - a_k} \overset{\text{Ind.vor.}}{=} \frac{q_k}{m_k + \sqrt{d} - q_k a_k} = \frac{m_{k+1} + \sqrt{d}}{q_{k+1}}$$

mit

$$m_{k+1} := q_k a_k - m_k, \qquad q_{k+1} := \frac{d - (m_k - q_k a_k)^2}{q_k} = \frac{d - m_{k+1}^2}{q_k}.$$

Man kann nun schreiben (in Umkehrung von $(*)$ mittels inverser Matrix):

$$\bar{\xi}_{k+1} \overset{(*)}{=} \frac{v_{k-1}\bar{x} - u_{k-1}}{-v_k\bar{x} + u_k} = -\frac{v_{k-1}}{v_k} \cdot \underbrace{\frac{\bar{x} - u_{k-1}/v_{k-1}}{\bar{x} + u_k/v_k}}_{\longrightarrow 1}$$

Es gibt also ein $k_0 \in \mathbb{N}$, so daß $\bar{\xi}_k < 0$ für $k \geq k_0$. Wegen $\xi_k > 1$ ist $q_k = \frac{2\sqrt{d}}{\xi_k - \bar{\xi}_k} > 0$, und daraus folgt für $k > k_0$: $m_k^2 = d - q_k q_{k-1} < d$ und $q_k < m_k + \sqrt{d} < 2\sqrt{d}$.

Das bedeutet, daß es nur endlich viele verschiedene Restzahlen ξ_k mit $k > k_0$ gibt, insbesondere gibt es $k_1 \neq k_2$ mit $\xi_{k_1} = \xi_{k_2}$, und daher ist die Kettenbruchentwicklung von x periodisch! **\$**

Spezielle quadratisch irrationale Zahlen sind die Quadratwurzeln nichtquadratischer natürlicher Zahlen. Hier tritt eine besondere Symmetrie in der Kettenbruchentwicklung auf:

Satz 3: ① *Sei $d \in \mathbb{N}$ kein Quadrat. Dann gilt für die Kettenbruchentwicklung:*

$$\sqrt{d} = (a_0, \overline{a_1, \ldots, a_{n-1}, 2a_0})$$

mit der Periodenlänge n, $a_0 = \left[\sqrt{d}\right]$ und $a_{n-i} = a_i$ für alle $i \in \{1, \ldots, n-1\}$.

② *Ist $\frac{u_k}{v_k}$ der k-te Näherungsbruch, $\xi_k = \frac{m_k + \sqrt{d}}{q_k}$ die k-te Restzahl, so gilt:*

$$u_k^2 - d \cdot v_k^2 = (-1)^{k+1} q_{k+1}.$$

Beweis. ad ①: Beweisskizze (Details siehe z. B. Forster, Algorithmische Zahlentheorie (1996)):

- $x := a_0 + \sqrt{d}$ ist reduziert ($x > 1$ und $-1 < \bar{x} < 0$ mit $\bar{x} = a_0 - \sqrt{d}$)
- $\Rightarrow x$ ist rein periodischer Kettenbruch: $x = (\overline{2a_0, a_1, \ldots, a_{n-1}})$
- $(\overline{a_{n-1}, \ldots, a_1, 2a_0}) = -1/\bar{x} \Rightarrow (\overline{2a_0, a_{n-1}, \ldots, a_1}) = 2a_0 - \bar{x} = x$

ad ②: Es gilt für alle $k \in \mathbb{N}$:

$$\sqrt{d} \overset{(*)}{=} \frac{u_k\xi_{k+1} + u_{k-1}}{v_k\xi_{k+1} + v_{k-1}} = \frac{u_k(m_{k+1} + \sqrt{d}) + u_{k-1}q_{k+1}}{v_k(m_{k+1} + \sqrt{d}) + v_{k-1}q_{k+1}}$$

$$\Leftrightarrow \sqrt{d} \cdot \left(v_k(m_{k+1} + \sqrt{d}) + v_{k-1}q_{k+1}\right) = u_k(m_{k+1} + \sqrt{d}) + u_{k-1}q_{k+1}$$

$$\Leftrightarrow \sqrt{d} \cdot \left(v_k m_{k+1} + v_{k-1}q_{k+1} - u_k\right) = u_k m_{k+1} + u_{k-1}q_{k+1} - dv_k$$

Da $\sqrt{d}$ irrational ist, müssen beide Seiten der letzten Gleichung verschwinden. Durch Elimination von m_{k+1} aus dem sich ergebenden Gleichungssystem folgt:

$$u_k^2 - u_k v_{k-1} q_{k+1} = dv_k^2 - v_k u_{k-1} q_{k+1},$$

und mit $u_k v_{k-1} - v_k u_{k-1} = (-1)^{k+1}$ (vgl. $(*)$) erhält man die Behauptung. **\$**

Folgerung: Wählt man im Satz 3 speziell $k = n-1$, so ist wegen der Periodizität $q_{k+1} = q_n = q_0 = 1$, es gilt

$$u_{n-1}^2 - d \cdot v_{n-1}^2 = (-1)^n;$$

bei gerader Periodenlänge n ist somit durch den Näherungsbruch $\frac{u_{n-1}}{v_{n-1}}$ eine Lösung der Pellschen Gleichung $a^2 - d \cdot b^2 = 1$ gegeben, bei ungerader Periodenlänge ist $2n$ statt n zu verwenden.

Beispiel: Wir sind nun in der Lage, die eingangs gestellte Aufgabe zu lösen; die Pellsche Gleichung hat hier den Parameter $d = 13$. Nach dem Kettenbruchverfahren ist $\sqrt{13}$ in einen Kettenbruch zu entwickeln und dessen Periode festzustellen. Wie bereits oben bestimmt, gilt:

$$\sqrt{13} = (3, \overline{1, 1, 1, 1, 6}).$$

Die Periode hat eine ungerade Länge, also muß man berechnen:

$$(3, 1, 1, 1, 1, 6, 1, 1, 1, 1) = \frac{649}{180},$$

und in der Tat gilt: $180^2 \cdot 13 + 1 = 649^2$, Harolds Armee bestand somit aus $180^2 \cdot 13 = 421200$ Mannen.

3 Das problema bovinum des Archimedes

In dem Archimedischen Problem ist die Aufgabe gestellt, die Größe der Rinderherde des Gottes Helios auszurechnen. Der Sonnengott hat Rinder in vier Sorten, weiße, schwarze, gescheckte („Schwarzbunte“) und braune. Bezeichnet man die Zahlen der weißen, schwarzen, gescheckten bzw. braunen Stiere mit α, β, γ bzw. δ und die Zahlen der jeweiligen Kühe mit einem zusätzlichen Strich, so entnimmt man dem griechischen Text bzw. seiner Übersetzung die folgenden Bedingungen:

$$\begin{aligned}
\alpha &= \left(\tfrac{1}{2} + \tfrac{1}{3}\right) \beta + \delta & \qquad \alpha' &= \left(\tfrac{1}{3} + \tfrac{1}{4}\right) (\beta + \beta') \\
\beta &= \left(\tfrac{1}{4} + \tfrac{1}{5}\right) \gamma + \delta & \beta' &= \left(\tfrac{1}{4} + \tfrac{1}{5}\right) (\gamma + \gamma') \\
\gamma &= \left(\tfrac{1}{6} + \tfrac{1}{7}\right) \alpha + \delta & \gamma' &= \left(\tfrac{1}{5} + \tfrac{1}{6}\right) (\delta + \delta') \\
& & \delta' &= \left(\tfrac{1}{6} + \tfrac{1}{7}\right) (\alpha + \alpha')
\end{aligned}$$

Diese Gleichungssysteme führen auf ganzzahlige Lösungen:

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} 2226 \\ 1602 \\ 1580 \\ 891 \end{pmatrix} \cdot t, \qquad \begin{pmatrix} \alpha' \\ \beta' \\ \gamma' \\ \delta' \end{pmatrix} = \begin{pmatrix} 7206360 \\ 4893246 \\ 3515820 \\ 5439213 \end{pmatrix} \cdot s \text{ mit } s, t \in \mathbb{N}; t = 4657 \cdot s.$$

Die kleinste Lösung erhält man für $s = 1$ zu:

weiß	schwarz	gescheckt	braun	
10366482	7460514	7358060	4149387	Stiere
7206360	4893246	3515820	5439213	Kühe

mit einer Gesamtzahl von 50389082.

Hier sind wir noch nicht fertig, im zweiten Teil des Archimedischen Problems soll die Anzahl der weißen und schwarzen Stiere zusammen eine Quadratzahl ($\alpha + \beta = n^2$, $n \in \mathbb{N}$), die Zahl der gescheckten und der braunen Stiere zusammen eine Dreieckszahl ($\gamma + \delta = \frac{m(m+1)}{2}$, $m \in \mathbb{N}$) bilden. Setzt man die Lösung des ersten Teiles an, so lautet die Quadratbedingung:

$$\alpha + \beta = 3828 \cdot t = 4 \cdot 3 \cdot 11 \cdot 29 \cdot 4657 \cdot s \stackrel{!}{=} n^2$$

und dies ist nur erfüllbar, falls s die Primfaktoren zu einer Quadratzahl ergänzt:

$$s = 3 \cdot 11 \cdot 29 \cdot 4657 \cdot r^2; r \in \mathbb{N}.$$

Die mit dieser Bedingung kleinstmögliche Lösung ($r = 1$) ist mit um $3 \cdot 11 \cdot 29 \cdot 4657 = 4456749$-fach größeren Werten als in obiger Tabelle bereits recht groß, jedoch verschwindend im Vergleich zum Ergebnis, das man bei Hinzunahme der Dreiecksbedingung erhält. Diese führt auf:

$$\begin{aligned} \gamma + \delta &= 2471 \cdot t = (7 \cdot 353) \cdot 4657 \cdot s \\ &= 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot 4657^2 \cdot r^2 \stackrel{!}{=} \frac{m(m+1)}{2} = \frac{(2m+1)^2 - 1}{8} \\ \Leftrightarrow 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot (2 \cdot 4657 \cdot r)^2 &= (2m+1)^2 - 1 \end{aligned}$$

Wir haben also eine Pellsche Gleichung $a^2 - d \cdot b^2 = 1$ mit ungeradem a und $d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 = 4729494$ zu lösen. Unter ihren Lösungen ist anschließend die kleinste zu finden, bei der $2 \cdot 4657$ ein Teiler von b ist.[3] Das gesuchte kleinstmögliche r für obige Dreiecksbedingung ist dann $r = \frac{1}{2 \cdot 4657} b$.

Mit Hilfe des Kettenbruchverfahrens findet man, daß $\sqrt{d} = \sqrt{4729494}$ eine Periodenlänge von 92 besitzt, die kleinste Lösung der Pellschen Gleichung ergibt sich aus dem zur ersten Periode gehörigen Näherungsbruch zu:

$$\begin{aligned} a_1 &= 109931986732829734979866232821433543901088049 \\ b_1 &= 50549485234315033074477819735540408986340 \end{aligned}$$

[3]Ein direkter Lösungsversuch der Gleichung $a^2 - (4 \cdot 4657^2 \cdot d) \cdot r^2 = 1$ über das Kettenbruchverfahren führt nicht sehr weit, so gab 1867 der Mathematiker C. F. Meyer nach 240 Schritten auf – ohne Computer kein Wunder, da die Periodenlänge hier 203254 beträgt!

Wie bereits erwähnt, erhält man alle weiteren Lösungen durch Potenzieren von $a_1 + b_1 \cdot \sqrt{d}$ und Trennen in einen rationalen und einen irrationalen Teil:

$$a_n + b_n\sqrt{d} := \left(a_1 + b_1\sqrt{d}\right)^n.$$

Gesucht ist nun das kleinste $\varrho \in \mathbb{N}^\times$ mit $b_\varrho \equiv 0 \ (2 \cdot 4657)$. Allgemein kann man folgende Sätze zeigen (Amthor, 1880):

Satz 4: *Sei p eine Primzahl. Ist (a_ϱ, b_ϱ) die Lösung der Pellschen Gleichung $a^2 - d \cdot b^2 = 1$ mit kleinstem $\varrho \in \mathbb{N}^\times$, so daß $b_\varrho \equiv 0 \ (p)$ gilt, so erhält man alle Lösungen der Pellschen Gleichung mit dieser Eigenschaft durch Vielfache von ρ:*

$$(a_{\nu\varrho}, b_{\nu\varrho}) \ \textit{mit} \ \nu \in \mathbb{N}^\times.$$

Beweis. ① Für alle $\nu \in \mathbb{N}^\times$ sind $(a_{\nu\varrho}, b_{\nu\varrho})$ Lösungen der Pellschen Gleichung mit $b_{\nu\varrho} \equiv 0 \ (p)$, wie man per Induktion unter Verwendung von Satz 1 zeigt:

$$b_{(\nu+1)\varrho} = b_{\nu\varrho+\varrho} = a_\varrho b_{\nu\varrho} + a_{\nu\varrho} b_\varrho \equiv 0 \quad (p).$$

② Umgekehrt sei (a_μ, b_μ) eine weitere Lösung der Pellschen Gleichung mit $b_\mu \equiv 0 \ (p)$, $\mu \notin \varrho\mathbb{N}^\times$, $\mu > \varrho$. Sei $\nu_0 := [\mu/\varrho]$, das heißt, $\nu_0 \in \mathbb{N}^\times$ mit $0 < \mu - \nu_0\varrho < \varrho$. Dann ist gemäß Satz 1 auch $(a_{\mu-\nu_0\varrho}, b_{\mu-\nu_0\varrho})$ eine Lösung, wobei gilt:

$$b_{\mu-\nu_0\varrho} = a_\mu b_{\nu_0\varrho} + a_{\nu_0\varrho} b_\mu \equiv 0 \quad (p).$$

Das ist ein Widerspruch zur vorausgesetzten Minimalität von (a_ϱ, b_ϱ)! **\$**

Satz 5: *Sei p eine Primzahl, teilerfremd zu d. Sind $a_1, b_1 \not\equiv 0 \ (p)$, so gilt:*

$$\left(\tfrac{d}{p}\right) = \pm 1 \quad \Rightarrow \quad a_{p\mp 1} \equiv 1 \quad (p) \quad \wedge \quad b_{p\mp 1} \equiv 0 \quad (p).$$

Das Legendresymbol $\left(\frac{d}{p}\right)$ ist 1 oder -1, je nachdem, ob d quadratischer Rest oder quadratischer Nichtrest von p ist.

Beweis. Binomialkoeffizienten erfüllen: $\binom{p}{0} = \binom{p}{p} = 1$ und $\binom{p}{j} \equiv 0 \ (p)$ für $j \in \{1, \ldots, p-1\}$. Daher gilt hier:

$$a_p + b_p\sqrt{d} = \left(a_1 + b_1\sqrt{d}\right)^p \equiv a_1^p + b_1^p d^{\frac{p-1}{2}} \cdot \sqrt{d} \quad (p).$$

Zusammen mit dem Fermatschen Satz ($a_1^{p-1} \equiv b_1^{p-1} \equiv 1 \ (p)$, gültig, da $p \nmid a_1, b_1$) folgt:

$$a_p \equiv a_1 \quad (p); \quad b_p \equiv b_1 d^{\frac{p-1}{2}} \quad (p).$$

Nun gilt: $d^{\frac{p-1}{2}} \equiv \left(\frac{d}{p}\right) = \pm 1 \ (p)$, dann liefert Satz 1:

$$\begin{aligned} a_{p\mp 1} &= a_p a_1 \mp b_p b_1 \cdot d \equiv a_1^2 - b_1^2 \cdot d = 1 \quad (p), \\ b_{p\mp 1} &= a_1 b_p \mp a_p b_1 \equiv \pm a_1 b_1 \mp a_1 b_1 = 0 \quad (p). \end{aligned}$$

Das war zu zeigen. **\$**

Folgerung: Mit $M := \frac{p\mp 1}{2}$ gilt sogar: $b_M \equiv 0 \ (p)$, denn sonst wäre $a_M \equiv 0$, weil $0 \equiv b_{2M} = 2a_M b_M$ (Satz 1) und $\mathbb{Z}/p\mathbb{Z}$ nullteilerfrei ist. Es folgt:

$$1 \equiv a_{2M} = a_M^2 + d \cdot b_M^2 = a_M^2 + (a_M^2 - 1) \equiv -1 \quad (p),$$

d. h., $p|2$ im Widerspruch zur Annahme, daß p eine ungerade Primzahl ist.

Folgerung: Die kleinste Lösung a_ϱ, b_ϱ der Pellschen Gleichung $a^2 - d \cdot b^2 = 1$ mit $b_\varrho \equiv 0 \ (p)$ für eine zu d teilerfremde ungerade Primzahl p findet man, indem man $p - \left(\frac{d}{p}\right)$ in seine Primfaktoren zerlegt: $\frac{p\pm 1}{2} = \prod p_i^{n_i}$; dann muß ϱ sich aus gefundenen Primfaktoren zusammensetzen.

Mit den Sätzen 4 und 5 kann nun die vollständige Lösung des Archimedischen Problems angegeben werden. Dazu stellt man zunächst fest, daß $d = 4729494$ ein quadratischer Nichtrest von $p = 4657$ ist:

Es gilt: $\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{3}{p}\right) \cdot \left(\frac{7}{p}\right) \cdot \left(\frac{11}{p}\right) \cdot \left(\frac{29}{p}\right) \cdot \left(\frac{353}{p}\right)$. Mit $\frac{p-1}{2} = 2328$ hat man nach dem Quadratischen Reziprozitätsgesetz:

$$\left(\tfrac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{2710956} = 1; \qquad \left(\tfrac{3}{p}\right) = \left(\tfrac{p}{3}\right) \equiv p \equiv 1 \quad (3);$$
$$\left(\tfrac{7}{p}\right) = \left(\tfrac{p}{7}\right) \equiv p^3 \equiv 1 \quad (7); \qquad \left(\tfrac{11}{p}\right) = \left(\tfrac{p}{11}\right) \equiv p^5 \equiv 1 \quad (11);$$
$$\left(\tfrac{29}{p}\right) = \left(\tfrac{p}{29}\right) \equiv p^{14} \equiv 17^{14} \equiv (-1)^7 = -1 \quad (29); \quad \left(\tfrac{353}{p}\right) = \left(\tfrac{p}{353}\right) \equiv \ldots \equiv 1 \quad (353).$$

Es sind also die Teiler von $\frac{p+1}{2} = 2329 = 17 \cdot 137$ zu untersuchen, es muß gelten: $\varrho \in \{17, 137, 2329\}$. Mit Satz 1 ($a_{n+m} = a_n a_m + b_n b_m \cdot d; b_{n+m} = a_m b_n + a_n b_m$) rechnet man aus:

$$a_1 \equiv -251; \quad b_1 \equiv -1606; \quad a_{17} \equiv -1411; \quad b_{17} \equiv 1933;$$
$$a_{137} \equiv 1686; \quad b_{137} \equiv -2323; \quad a_{2329} \equiv -1; \quad b_{2329} \equiv 0.$$

Da $b_1 \equiv 0 \ (2)$, folgt $b_n \equiv 0 \ (2)$ für alle $n \in \mathbb{N}^\times$, also gilt sogar: $b_{2329} \equiv 0 \ (2 \cdot 4657)$. Das kleinste r, für das die Dreiecksbedingung des Problems erfüllt ist, erhält man folglich zu:

$$r = \frac{b_{2329}}{2 \cdot 4657},$$

alle anderen zu $r_\nu = \frac{1}{2 \cdot 4657} \cdot b_{2329 \cdot \nu}$ mit $\nu \in \mathbb{N}$. Damit ergibt sich die Gesamtanzahl der Rinder zu etwa:

$$50389082 \cdot 4456749 \cdot r^2 = 224571490814418 \cdot r^2 \approx 7{,}76 \cdot 10^{206541}.$$

Abschließend kann man alle Lösungen wie folgt notieren:

weiß	schwarz	gescheckt	braun	
$10366482 \cdot s_\nu$	$7460514 \cdot s_\nu$	$7358060 \cdot s_\nu$	$4149387 \cdot s_\nu$	Stiere
$7206360 \cdot s_\nu$	$4893246 \cdot s_\nu$	$3515820 \cdot s_\nu$	$5439213 \cdot s_\nu$	Kühe

$$s_\nu = 4456749 \cdot r_\nu^2 = \frac{4456749}{2^2 \cdot 4657^2} \cdot b_{2329 \cdot \nu}^2$$

$

Literatur

Forster, Otto. *Algorithmische Zahlentheorie.* Braunschweig; Wiesbaden: Vieweg, 1996.

Krumbiegel, B. und A. Amthor. „Das Problema bovinum des Archimedes“. *Historisch-literarische Abtheilung der Zeitschrift für Mathematik und Physik* 25 (1880): 121 – 136, 153 – 171.

Lenstra, H. W. Jr. „Solving the Pell Equation“. *Notices of the AMS* 49 (2002): 182 – 192.