(b) Man schreibe eine MuPAD-Funktion, die zu einer natürlichen Zahl d, die keine Quadratzahl ist, nach dem in (16.18) beschriebenen Verfahren QWplus den Kettenbruch

$$\sqrt{d} \;=\; [a_0, \overline{a_1, a_2, \ldots, a_{l-1}, a_l}]$$

berechnet.

(c) Man vergleiche die Funktionen aus (a) und (b).

Aufgabe 4: Man schreibe eine MuPAD-Funktion, die zu einer natürlichen Zahl d, die keine Quadratzahl ist, nach dem in (16.18) beschriebenen Verfahren QWplus die Länge einer primitiven Periode des Kettenbruchs

$$\sqrt{d} \;=\; [a_0, \overline{a_1, a_2, \ldots, a_{l-1}, a_l}]$$

berechnet, ohne die Periode wirklich auszurechnen.

17 Die Pellschen Gleichungen

(17.1) In diesem Paragraphen wird eine spezielle Klasse von Diophantischen Gleichungen behandelt. Eine Diophantische Gleichung ist – im einfachsten Fall – eine Gleichung der Form

$$f(X_1, X_2, \ldots, X_n) \;=\; 0,$$

wobei f ein Polynom in $n \geq 2$ Unbestimmten X_1, $X_2, \ldots,$ X_n über dem Ring $\mathbb{Z}$ ist und wobei nach den Lösungen $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ gefragt wird. Der griechische Mathematiker Diophantos (um 250 n. Chr. Geb.) hat sich mit der Untersuchung solcher "unbestimmter Gleichungen" beschäftigt, er interessierte sich aber mehr für ihre Lösungen $(x_1, x_2, \ldots, x_n) \in \mathbb{Q}^n$. Trotzdem sind Gleichungen der angegebenen Form, bei denen man sich für die ganzzahligen Lösungen interessiert, nach ihm benannt.

Im Jahr 1621 veröffentlichte C. G. Bachet de Méziriac (1581 – 1638) den griechischen Text der Schriften von Diophantos, zusammen mit einer Übersetzung ins Lateinische und einem ausführlichen Kommentar, und zwischen diesem Jahr und 1636 beschaffte sich P. de Fermat ein Exemplar, wohl das, in das er seine berühmte Vermutung notierte. Mit Fermats Beschäftigung mit diesem Buch beginnt nach der Meinung von A. Weil (vgl. [112]) die moderne Zahlentheorie. Fermat befaßte sich dabei auch mit Diophantischen Gleichungen der Gestalt

$$(*) \qquad X^2 - dY^2 \;=\; 1,$$

in denen d eine natürliche Zahl ist, die keine Quadratzahl ist, und fand wohl ein Verfahren, Lösungen solcher Gleichungen zu berechnen. Auch die englischen

Mathematiker J. Wallis (1616 – 1703) und W. Brouncker (1620 – 1684), die von Fermat zur Beschäftigung mit solchen Gleichungen angeregt worden waren, fanden eine Lösungsmethode. Später hat L. Euler die Gleichungen vom Typ (∗) nach dem englischen Mathematiker J. Pell (1611 – 1685) benannt, der sich wohl nie damit beschäftigt hat, und so heißen sie noch heute Pellsche Gleichungen, auch wenn sie immer wieder ein Autor nach einem anderen Mathematiker, etwa nach Fermat oder nach Archimedes (vgl. (17.15)), benennen wollte.

Die von Fermat begonnene Untersuchung der Diophantischen Gleichungen vom Typ (∗) hat J. L. Lagrange in mehreren Arbeiten zwischen 1766 und 1770 zu Ende geführt.

(17.2) Satz: *Es sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, es sei $(r_n/s_n)_{n\geq 0}$ die Folge der Näherungsbrüche des Kettenbruchs für α, und es seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$.*
(1) *Wenn es ein $n \in \mathbb{N}_0$ mit*

$$|\, b\alpha - a\,| \;<\; |\, s_n\alpha - r_n\,|$$

gibt, so ist $b \geq s_{n+1}$.
(2) *Wenn es ein $n \in \mathbb{N}$ mit*

$$\left|\, \alpha - \frac{a}{b}\,\right| \;<\; \left|\, \alpha - \frac{r_n}{s_n}\,\right|$$

gibt, so ist $b > s_n$.

Beweis: Es sei $n \in \mathbb{N}_0$, und es gelte $b < s_{n+1}$. Gezeigt wird: Dann ist

$$|\, b\alpha - a\,| \;\geq\; |\, s_n\alpha - r_n\,|.$$

Für die Matrix

$$A \;:=\; \begin{pmatrix} r_{n+1} & r_n \\ s_{n+1} & s_n \end{pmatrix} \;\in\; M(2;\mathbb{Z})$$

gilt $\det(A) = r_{n+1}s_n - r_n s_{n+1} = (-1)^n \in \{-1, 1\}$, also ist sie invertierbar, und die dazu inverse Matrix

$$A^{-1} \;=\; \frac{1}{\det(A)} \begin{pmatrix} s_n & -r_n \\ -s_{n+1} & r_{n+1} \end{pmatrix}$$

liegt ebenfalls in $M(2;\mathbb{Z})$. Also gibt es ganze Zahlen x und y mit

$$r_{n+1}x + r_n y \;=\; a \quad \text{und} \quad s_{n+1}x + s_n y \;=\; b.$$

(a) Es ist $y \neq 0$, denn sonst ist $b = s_{n+1}x$, und wegen $b \in \mathbb{N}$ und $s_{n+1} \in \mathbb{N}$ folgt $x \in \mathbb{N}$ und daher $b = s_{n+1}x \geq s_{n+1}$, im Widerspruch zur Voraussetzung

$b < s_{n+1}$. Wegen $0 < b = s_{n+1}x + s_n y < s_{n+1}$ können x und y nicht beide positiv und nicht beide negativ sein.
(b) Nach (a) gilt entweder $x = 0$ oder $xy < 0$. Ist $x = 0$, so gilt $a = r_n y$ und $b = s_n y$ und daher wegen $|y| \geq 1$

$$|b\alpha - a| = |s_n\alpha - r_n| \cdot |y| \geq |s_n\alpha - r_n|.$$

Ist $xy < 0$, so gilt

$$\begin{aligned} |b\alpha - a| &= \left|(s_{n+1}x + s_n y)\,\alpha - (r_{n+1}x + r_n y)\right| = \\ &= \left|(s_{n+1}\alpha - r_{n+1})\,x + (s_n\alpha - r_n)\,y\right| = \\ &\overset{(*)}{=} |s_{n+1}\alpha - r_{n+1}| \cdot |x| + |s_n\alpha - r_n| \cdot |y| \geq \\ &\geq |s_n\alpha - r_n| \cdot |y| \geq |s_n\alpha - r_n|; \end{aligned}$$

daß darin das Gleichheitszeichen bei $(*)$ richtig ist, sieht man so: Ist n gerade, so gilt $r_n/s_n < \alpha < r_{n+1}/s_{n+1}$ (vgl. (15.3)(2)) und daher $s_{n+1}\alpha - r_{n+1} < 0$ und $s_n\alpha - r_n > 0$; ist n ungerade, so gilt $r_n/s_n < \alpha < r_{n+1}/s_{n+1}$ und daher $s_{n+1}\alpha - r_{n+1} > 0$ und $s_n\alpha - r_n < 0$, und daher gilt wegen $xy < 0$ in jedem Fall: Die Zahlen $(s_{n+1}\alpha - r_{n+1})\,x$ und $(s_n\alpha - r_n)\,y$ sind entweder beide positiv oder beide negativ.
(2) Es sei $n \in \mathbb{N}$, und es gelte

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{r_n}{s_n}\right|.$$

Angenommen, es ist $b \leq s_n$. Dann gilt

$$|b\alpha - a| = b \cdot \left|\alpha - \frac{a}{b}\right| \leq s_n \cdot \left|\alpha - \frac{a}{b}\right| < s_n \cdot \left|\alpha - \frac{r_n}{s_n}\right| = |s_n\alpha - r_n|.$$

Nach (1) ist daher $b \geq s_{n+1}$, im Widerspruch dazu, daß $b \leq s_n$ und $s_n < s_{n+1}$ gilt.

(17.3) Bemerkung: Von Archimedes wurde 22/7 als Näherung für π angegeben. 22/7 ist der erste Näherungsbruch des Kettenbruchs für π. Nach (17.2)(2) gibt es keine rationale Zahl mit einem Nenner $b \in \{1, 2, 3, 4, 5, 6, 7\}$, die eine bessere Approximation an π als 22/7 ist. In diesem Sinn liefern Kettenbrüche optimale rationale Approximationen an irrationale reelle Zahlen.

(17.4) Satz: *Es sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, es sei $(r_n/s_n)_{n\geq 0}$ die Folge der Näherungsbrüche des Kettenbruchs für α, es seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$, und es gelte*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}.$$

Dann gibt es ein $n \in \mathbb{N}_0$ mit

$$\frac{a}{b} = \frac{r_n}{s_n}.$$

Beweis: Angenommen, a/b ist kein Näherungsbruch des Kettenbruchs für α. Für jedes $n \in \mathbb{N}_0$ gilt $1 = s_0 \leq s_n < s_{n+1}$, und daher gibt es ein $n \in \mathbb{N}_0$ mit $s_n \leq b < s_{n+1}$. Nach (17.2)(1) gilt $|b\alpha - a| \geq |s_n\alpha - r_n|$, also

$$\left|\alpha - \frac{r_n}{s_n}\right| = \frac{|s_n\alpha - r_n|}{s_n} \leq \frac{|b\alpha - a|}{s_n} = \frac{b}{s_n} \cdot \left|\alpha - \frac{a}{b}\right| < \frac{b}{s_n} \cdot \frac{1}{2b^2} = \frac{1}{2bs_n}.$$

Wegen $a/b \neq r_n/s_n$ ist $as_n - br_n \in \mathbb{Z} \setminus \{0\}$, und daher gilt

$$\frac{1}{bs_n} \leq \frac{|as_n - br_n|}{bs_n} = \left|\frac{a}{b} - \frac{r_n}{s_n}\right| \leq \left|\frac{a}{b} - \alpha\right| + \left|\alpha - \frac{r_n}{s_n}\right| < \frac{1}{2b^2} + \frac{1}{2bs_n}.$$

Also gilt

$$\frac{1}{2bs_n} < \frac{1}{2b^2}$$

und daher $s_n > b$. Aber n war so gewählt, daß $s_n \leq b$ gilt.
Damit ist gezeigt, daß a/b ein Näherungsbruch des Kettenbruchs für α ist.

(17.5) Es sei d eine natürliche Zahl, die keine Quadratzahl ist.
(1) $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{R}$ und ein Oberkörper von $\mathbb{Q}$, $\{1, \sqrt{d}\}$ ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{d})$, und die Abbildung

$$\sigma_d : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}) \quad \text{mit} \quad \sigma_d(x + y\sqrt{d}) = x - y\sqrt{d} \quad \text{für alle } x, y \in \mathbb{Q}$$

ist ein $\mathbb{Q}$-Automorphismus des Körpers $\mathbb{Q}(\sqrt{d})$. Für jedes $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ heißt die rationale Zahl

$$N_d(\alpha) := \alpha\sigma_d(\alpha) = x^2 - dy^2$$

die Norm von α. Für jedes $x \in \mathbb{Q}$ ist $N_d(x) = x^2$, und für alle $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ gilt

$$N_d(\alpha\beta) = \alpha\beta\,\sigma_d(\alpha)\sigma_d(\beta) = \alpha\sigma_d(\alpha)\,\beta\sigma_d(\beta) = N_d(\alpha)N_d(\beta).$$

Für jedes $\alpha \in \mathbb{Q}(\sqrt{d})$ mit $\alpha \neq 0$ gilt $\sigma_d(\alpha) \neq 0$ und $N_d(\alpha) = \alpha\sigma_d(\alpha) \neq 0$, und wegen $N_d(\alpha)N_d(\alpha^{-1}) = N_d(\alpha\alpha^{-1}) = N_d(1) = 1$ folgt $N_d(\alpha^{-1}) = N_d(\alpha)^{-1}$.
(2) $\mathbb{Z}[\sqrt{d}] := \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\}$ ist ein Unterring von $\mathbb{Q}(\sqrt{d})$ und ein Oberring von $\mathbb{Z}$. Es gilt

$$\mathbb{Q}(\sqrt{d}) = \left\{\frac{\alpha}{y} \,\middle|\, \alpha \in \mathbb{Z}[\sqrt{d}], y \in \mathbb{N}\right\} = \left\{\frac{\alpha}{\beta} \,\middle|\, \alpha, \beta \in \mathbb{Z}[\sqrt{d}], \beta \neq 0\right\}.$$

Also ist $\mathbb{Q}(\sqrt{d})$ der kleinste Unterkörper von $\mathbb{R}$, der $\mathbb{Z}[\sqrt{d}]$ enthält, d.h. $\mathbb{Q}(\sqrt{d})$ ist Quotientenkörper von $\mathbb{Z}[\sqrt{d}]$. Für jedes $\alpha \in \mathbb{Z}[\sqrt{d}]$ ist $\sigma_d(\alpha) \in \mathbb{Z}[\sqrt{d}]$ und $N_d(\alpha) \in \mathbb{Z}$.
(3) Die Einheitengruppe des Rings $\mathbb{Z}[\sqrt{d}]$ ist

$$E(\mathbb{Z}[\sqrt{d}]) = \{\varepsilon \in \mathbb{Z}[\sqrt{d}] \mid N_d(\varepsilon) = 1 \text{ oder } N_d(\varepsilon) = -1\} = \\ = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z};\ x^2 - dy^2 \in \{1, -1\}\}.$$

Beweis: (a) Ist ε eine Einheit in $\mathbb{Z}[\sqrt{d}]$, so gilt auch $1/\varepsilon \in \mathbb{Z}[\sqrt{d}]$, also sind $N_d(\varepsilon)$ und $N_d(\varepsilon)^{-1} = N_d(\varepsilon^{-1})$ ganze Zahlen, und daher gilt $N_d(\varepsilon) = 1$ oder $N_d(\varepsilon) = -1$.
(b) Es seien x, $y \in \mathbb{Z}$, und es gelte $x^2 - dy^2 = 1$ oder $x^2 - dy^2 = -1$. Für $\varepsilon := x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ gilt dann

$$\frac{1}{\varepsilon} = \frac{\sigma_d(\varepsilon)}{\varepsilon\sigma_d(\varepsilon)} = \frac{x - y\sqrt{d}}{x^2 - dy^2} \in \mathbb{Z}[\sqrt{d}],$$

und somit ist ε eine Einheit in $\mathbb{Z}[\sqrt{d}]$.

(17.6) Bezeichnung: Es sei d eine natürliche Zahl, die keine Quadratzahl ist. Die Gleichungen

$$X^2 - dY^2 = 1 \quad \text{und} \quad X^2 - dY^2 = -1$$

heißen die Pellschen Gleichungen zu d.

(17.7) Bemerkung: Es sei d eine natürliche Zahl, die keine Quadratzahl ist.
(a) Die Pellsche Gleichung

$$(*) \qquad X^2 - dY^2 = 1$$

besitzt die trivialen Lösungen $(1, 0)$ und $(-1, 0)$. Für jede andere Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ gilt $x \neq 0$ und $y \neq 0$. Man kennt jede nichttriviale Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ von $(*)$, wenn man jede Lösung $(x, y) \in \mathbb{N} \times \mathbb{N}$ kennt, und zu jedem $x \in \mathbb{N}$ gibt es höchstens ein $y \in \mathbb{N}$, für das (x, y) eine Lösung von $(*)$ ist. Wenn es in $\mathbb{Z} \times \mathbb{Z}$ überhaupt eine nichttriviale Lösung von $(*)$ gibt, so gibt es eine eindeutig bestimmte Lösung $(x_1, y_1) \in \mathbb{N} \times \mathbb{N}$, für die gilt: Für jede andere Lösung $(x, y) \in \mathbb{N} \times \mathbb{N}$ gilt $x > x_1$ und $y > y_1$. Diese Lösung (x_1, y_1) heißt die Fundamentallösung von $(*)$.
(b) Für jede Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ von

$$(**) \qquad X^2 - dY^2 = -1$$

gilt $x \neq 0$ und $y \neq 0$. Wieder gilt: Man kennt jede Lösung $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ von $(**)$, wenn man jede Lösung $(x,y) \in \mathbb{N} \times \mathbb{N}$ kennt, und zu jedem $x \in \mathbb{N}$ gibt es höchstens ein $y \in \mathbb{N}$, für das (x,y) eine Lösung von $(**)$ ist. Auch hier gilt: Wenn es in $\mathbb{Z} \times \mathbb{Z}$ überhaupt Lösungen von $(**)$ gibt, so gibt es eine eindeutig bestimmte Lösung $(x_1,y_1) \in \mathbb{N} \times \mathbb{N}$, für die gilt: Für jede andere Lösung $(x,y) \in \mathbb{N} \times \mathbb{N}$ gilt $x > x_1$ und $y > y_1$. Diese Lösung (x_1,y_1) heißt die Fundamentallösung von $(**)$.

(17.8) Beispiele: Man kann nach der Fundamentallösung (x_1,y_1) der Pellschen Gleichung

$$(*) \qquad X^2 - 54\,Y^2 \;=\; 1$$

folgendermaßen suchen: Man sucht nach der kleinsten natürlichen Zahl y, für die $1 + 54y^2$ eine Quadratzahl ist. Man findet so $(x_1,y_1) = (485,66)$. Nach (17.5)(3) ist $\varepsilon_1 := 485 + 66\sqrt{54}$ eine Einheit im Ring $\mathbb{Z}[\sqrt{54}]$ mit $N_{54}(\varepsilon_1) = 1$. Auch $\varepsilon_1^2 = 470\,449 + 64\,020\sqrt{54}$ ist eine Einheit in diesem Ring mit $N_{54}(\varepsilon_1^2) = N_{54}(\varepsilon_1)^2 = 1$, und daher ist auch $(470\,449, 64\,020)$ eine Lösung von $(*)$. Man sieht, daß auf diese Weise jede Potenz von ε_1 eine Lösung von $(*)$ liefert (vgl. dazu (17.13)).
Die Gleichung

$$X^2 - 54\,Y^2 \;=\; -1$$

besitzt in $\mathbb{Z} \times \mathbb{Z}$ keine Lösung, denn für jedes $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ gilt

$$x^2 - 54y^2 \;\equiv\; x^2 \;\not\equiv\; -1 \pmod 3.$$

(2) Die Gleichung

$$X^2 - 73\,Y^2 \;=\; -1$$

besitzt Lösungen in $\mathbb{Z} \times \mathbb{Z}$: Durch direkte Suche wie in (1) findet man ihre Fundamentallösung $(1068,125)$. Nach (17.5) ist $\varepsilon_1 := 1068 + 125\sqrt{73}$ eine Einheit im Ring $\mathbb{Z}[\sqrt{73}]$ mit $N_{73}(\varepsilon_1) = -1$, und $\varepsilon_1^2 = 2\,281\,249 + 26\,700\sqrt{73}$ ist eine Einheit in diesem Ring mit $N_{73}(\varepsilon_1^2) = N_{73}(\varepsilon_1)^2 = 1$. Also ist $(2\,281\,249, 26\,700)$ eine Lösung von $X^2 - 73Y^2 = 1$. Dies ist übrigens die Fundamentallösung dieser Gleichung, wie man mit Hilfe der später in diesem Paragraphen behandelten Algorithmen sehen kann.

(17.9) Satz: *Es sei d eine natürliche Zahl, die keine Quadratzahl ist, es sei $(r_n/s_n)_{n\geq 0}$ die Folge der Näherungsbrüche des Kettenbruchs für $\sqrt{d}$, und es seien x und y natürliche Zahlen, für die $x^2 - dy^2 = 1$ oder $x^2 - dy^2 = -1$ gilt. Dann gibt es ein $n \in \mathbb{N}_0$ mit $x = r_n$ und $y = s_n$.*

Beweis: (a) Es gelte $x^2 - dy^2 = 1$. Dann gilt

$$1 \;=\; x^2 - dy^2 \;=\; (x + y\sqrt{d})(x - y\sqrt{d}),$$

also $x - y\sqrt{d} > 0$ und daher $x + y\sqrt{d} > 2y\sqrt{d} > 2y$ und

$$0 < \frac{x}{y} - \sqrt{d} = \frac{x - y\sqrt{d}}{y} = \frac{x^2 - dy^2}{(x + y\sqrt{d})y} = \frac{1}{(x + y\sqrt{d})y} < \frac{1}{2y^2}.$$

Nach (17.4) gibt es daher ein $n \in \mathbb{N}_0$ mit $x/y = r_n/s_n$. Wegen $x^2 - dy^2 = 1$ sind x und y teilerfremd, und weil auch r_n und s_n teilerfremd sind (vgl. dazu (15.3)(1)), gilt daher $x = r_n$ und $y = s_n$.
(b) Es gelte $x^2 - dy^2 = -1$. Dann gilt

$$x^2 = dy^2 - 1 \geq 2y^2 - 1 = y^2 + (y^2 - 1) \geq y^2,$$

also $x \geq y$, und es gilt

$$1 = dy^2 - x^2 = (y\sqrt{d} - x)(y\sqrt{d} + x),$$

also $y\sqrt{d} - x > 0$ und

$$0 < \sqrt{d} - \frac{x}{y} = \frac{y\sqrt{d} - x}{y} = \frac{dy^2 - x^2}{(y\sqrt{d} + x)y} = \\ = \frac{1}{(y\sqrt{d} + x)y} \leq \frac{1}{(y\sqrt{d} + y)y} = \frac{1}{(\sqrt{d} + 1)y^2} < \frac{1}{2y^2}.$$

Nach (17.4) gibt es daher ein $n \in \mathbb{N}_0$ mit $x/y = r_n/s_n$, und wie in (a) folgt, daß $x = r_n$ und $y = s_n$ gilt.

(17.10) Es sei d eine natürliche Zahl, die keine Quadratzahl ist, es sei

$$\sqrt{d} = [a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots]$$

der Kettenbruch für $\sqrt{d}$, und es sei $(r_n/s_n)_{n\geq 0}$ die Folge der Näherungsbrüche dieses Kettenbruchs. Für jedes $n \in \mathbb{N}$ gilt $1 \leq r_0 = a_0 < r_n < r_{n+1}$ und $1 = s_0 \leq s_n < s_{n+1}$. Es seien $(v_n)_{n\geq 0}$ und $(w_n)_{n\geq 0}$ die Folgen in $\mathbb{Z}$ mit $v_0 := 0$ und $w_0 := 1$ und mit

$$v_{n+1} := a_n w_n - v_n \quad \text{und} \quad w_{n+1} := \frac{d - v_{n+1}^2}{w_n} \quad \text{für jedes } n \in \mathbb{N}_0.$$

Für jedes $n \in \mathbb{N}_0$ gilt

$$\alpha_n := [a_n, a_{n+1}, a_{n+2}, \ldots] = \frac{v_n + \sqrt{d}}{w_n},$$

und für jedes $n \in \mathbb{N}$ gilt $v_n \in \mathbb{N}$ und $w_n \in \mathbb{N}$ (vgl. (16.15)(2)).

(1) Es sei $n \in \mathbb{N}_0$. Nach (16.15)(6) gilt

$$r_n^2 - ds_n^2 \;=\; (-1)^{n+1} w_{n+1},$$

und daher gilt:
(a) (r_n, s_n) ist eine Lösung der Gleichung $X^2 - dY^2 = 1$, genau wenn n ungerade und $w_{n+1} = 1$ ist.
(b) (r_n, s_n) ist eine Lösung der Gleichung $X^2 - dY^2 = -1$, genau wenn n gerade und $w_{n+1} = 1$ ist.
(2) Nach (16.14) ist der Kettenbruch für $\sqrt{d}$ periodisch mit einer Vorperiode der Länge 1. Es sei l die Länge einer primitiven Periode dieses Kettenbruchs. Dann gilt

$$\sqrt{d} \;=\; [a_0, \overline{a_1, a_2, \ldots, a_l}],$$

und nach (16.14) ist $a_l = 2a_0$. Es gilt: Für $n \in \mathbb{N}$ ist $w_n = 1$, genau wenn n durch l teilbar ist.
Beweis: (a) Für jedes $k \in \mathbb{N}$ gilt

$$\begin{aligned}\frac{v_{kl} + \sqrt{d}}{w_{kl}} \;&=\; \alpha_{kl} \;=\; [a_{kl}, a_{kl+1}, a_{kl+2}, \ldots] \;= \\ &=\; [a_{kl}, \overline{a_{kl+1}, a_{kl+2}, \ldots, a_{kl+l}}] \;=\; [a_l, \overline{a_1, a_2, \ldots, a_l}] \;= \\ &=\; [2a_0, \overline{a_1, a_2, \ldots, a_l}] \;=\; a_0 + [a_0, \overline{a_1, a_2, \ldots, a_l}] \;=\; a_0 + \sqrt{d},\end{aligned}$$

und weil $\{1, \sqrt{d}\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{d})$ ist, folgt daraus: Es ist $w_{kl} = 1$.
(b) Es sei $m \in \mathbb{N}$, und es gelte $w_m = 1$. Dann gilt

$$\alpha_m \;=\; [a_m, a_{m+1}, a_{m+2}, \ldots] \;=\; [\overline{a_m, a_{m+1}, \ldots, a_{m+l-1}}],$$

also ist der Kettenbruch für $\alpha_m = (v_m + \sqrt{d})/w_m = v_m + \sqrt{d}$ rein-periodisch. Nach (16.11) gilt daher

$$-1 \;<\; \sigma_d(\alpha_m) \;=\; v_m - \sqrt{d} \;<\; 0,$$

und somit ist $v_m < \sqrt{d} < v_m + 1$. Also ist $v_m = \lfloor \sqrt{d} \rfloor = a_0$ und

$$\begin{aligned}\alpha_m \;&=\; v_m + \sqrt{d} \;=\; a_0 + \sqrt{d} \;=\; a_0 + [a_0, a_1, a_2, \ldots] \;= \\ &=\; [2a_0, a_1, a_2, \ldots] \;=\; [a_l, a_{l+1}, a_{l+2}, \ldots] \;=\; \alpha_l.\end{aligned}$$

Es ist $0 \le k := m \bmod l < l$. Wäre $k \ge 1$, so wäre $\alpha_k = \alpha_{k+\lfloor m/l \rfloor l} = \alpha_m = \alpha_l$, also $a_k = \lfloor \alpha_k \rfloor = \lfloor \alpha_l \rfloor = a_l$ und

$$\begin{aligned}\alpha_{k+1} \;&=\; \frac{1}{\alpha_k - a_k} \;=\; \frac{1}{\alpha_l - a_l} \;=\; \alpha_{l+1} \;= \\ &=\; [a_{l+1}, a_{l+2}, a_{l+3}, \ldots] \;=\; [a_1, a_2, a_3, \ldots] \;=\; \alpha_1,\end{aligned}$$

und daher wäre

$$\sqrt{d} \;=\; [\,a_0, a_1, \ldots, a_k, \alpha_{k+1}\,] \;=\; [\,a_0, a_1, \ldots, a_k, \alpha_1\,] \;=\; [\,a_0, \overline{a_1, \ldots, a_k}\,].$$

Aber dies ist nicht möglich, denn es ist $k < l$, und $(a_1, a_2, \ldots, a_l)$ ist eine Periode minimaler Länge des Kettenbruchs für $\sqrt{d}$. Damit ist gezeigt, daß m durch l teilbar ist.

(17.11) Satz: *Es sei d eine natürliche Zahl, die keine Quadratzahl ist, es sei l die Länge einer primitiven Periode des Kettenbruchs*

$$\sqrt{d} \;=\; [\,a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots\,],$$

und es sei $(r_n/s_n)_{n\geq 0}$ die Folge der Näherungsbrüche dieses Kettenbruchs.
(1) *Ist l gerade, so gilt: Die Gleichung*

$$(*) \qquad X^2 - dY^2 \;=\; 1$$

besitzt nichttriviale Lösungen in $\mathbb{Z} \times \mathbb{Z}$, und zwar ist (r_{l-1}, s_{l-1}) die Fundamentallösung von $(*)$, die Menge aller Lösungen $(x, y) \in \mathbb{N} \times \mathbb{N}$ von $(*)$ ist

$$\big\{(r_{kl-1}, s_{kl-1}) \mid k \in \mathbb{N}\big\},$$

und die Gleichung

$$(**) \qquad X^2 - dY^2 \;=\; -1$$

besitzt keine Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.
(2) *Ist l ungerade, so gilt: Die Gleichungen $(*)$ und $(**)$ besitzen beide Lösungen in $\mathbb{Z} \times \mathbb{Z}$, (r_{l-1}, s_{l-1}) ist die Fundamentallösung von $(**)$, (r_{2l-1}, s_{2l-1}) ist die Fundamentallösung von $(*)$, und es gilt*

$$\big\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x^2 - dy^2 = -1\big\} \;=\; \big\{(r_{kl-1}, s_{kl-1}) \mid k \in \mathbb{N} \text{ ungerade}\big\}$$

und

$$\big\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x^2 - dy^2 = 1\big\} \;=\; \big\{(r_{kl-1}, s_{kl-1}) \mid k \in \mathbb{N} \text{ gerade}\big\}.$$

Beweis: (a) Nach (17.9) gibt es zu jeder Lösung $(x, y) \in \mathbb{N} \times \mathbb{N}$ von $(*)$ oder von $(**)$ ein $n \in \mathbb{N}_0$ mit $(x, y) = (r_n, s_n)$.
(b) Nach (17.9) gilt: Für jedes $n \in \mathbb{N}$, das nicht durch l teilbar ist, ist $r_n^2 - ds_n^2$ weder gleich 1 noch gleich -1, d.h. (r_n, s_n) ist weder Lösung von $(*)$ noch von $(**)$; für jedes $k \in \mathbb{N}$ gilt andererseits

$$r_{kl-1}^2 - ds_{kl-1}^2 \;=\; (-1)^{kl} w_{kl} \;=\; (-1)^{kl},$$

und daher ist (r_{kl-1}, s_{kl-1}) eine Lösung von $(*)$, falls kl gerade ist, und eine Lösung von $(**)$, falls kl ungerade ist.
(c) Ist l gerade, so folgt aus (a) und (b): $(**)$ besitzt keine Lösungen in $\mathbb{N} \times \mathbb{N}$ und daher auch keine Lösung in $\mathbb{Z} \times \mathbb{Z}$, und $\{(r_{kl-1}, s_{kl-1}) \mid k \in \mathbb{N}\}$ ist die Menge aller Lösungen in $\mathbb{N} \times \mathbb{N}$ von $(*)$; wegen $s_{l-1} < s_{2l-1} < s_{3l-1} < \dots$ ist (r_{l-1}, s_{l-1}) die Fundamentallösung von $(*)$.
(d) Ist l ungerade, so folgt aus (a) und (b): Die Menge aller Lösungen in $\mathbb{N} \times \mathbb{N}$ von $(*)$ ist $\{(r_{kl-1}, s_{kl-1}) \mid k \in \mathbb{N}$ gerade$\}$, und die Menge aller Lösungen in $\mathbb{N} \times \mathbb{N}$ von $(**)$ ist $\{(r_{kl-1}, s_{kl-1}) \mid k \in \mathbb{N}$ ungerade$\}$; wegen $s_{2l-1} < s_{4l-1} < s_{6l-1} < \dots$ ist (r_{2l-1}, s_{2l-1}) die Fundamentallösung von $(*)$, wegen $s_{l-1} < s_{3l-1} < s_{5l-1} < \dots$ ist (r_{l-1}, s_{l-1}) die Fundamentallösung von $(**)$.

(17.12) Satz: *Es sei d eine natürliche Zahl, die keine Quadratzahl ist, es sei $(r_n/s_n)_{n\geq 0}$ die Folge der Näherungsbrüche des Kettenbruchs*

$$\sqrt{d} \;=\; [a_0, a_1, a_2, \dots, a_n, a_{n+1}, \dots],$$

und es sei l die Länge einer primitiven Periode dieses Kettenbruchs. Für jedes $k \in \mathbb{N}$ gilt

$$r_{kl-1} + s_{kl-1}\sqrt{d} \;=\; (r_{l-1} + s_{l-1}\sqrt{d})^k.$$

Beweis: Es seien $r_{-1} := 1$ und $s_{-1} := 0$.
(a) Es seien $(v_n)_{n\geq 0}$ und $(w_n)_{n\geq 0}$ die Folgen in $\mathbb{Z}$ mit $v_0 := 0$, $w_0 := 1$ und

$$v_{n+1} \;:=\; a_n w_n - v_n \quad \text{und} \quad w_{n+1} \;:=\; \frac{d - v_{n+1}^2}{w_n} \quad \text{für jedes } n \in \mathbb{N}_0.$$

Es gilt $v_l \in \mathbb{N}$, $w_l \in \mathbb{N}$ und

$$\begin{aligned}\frac{v_l + \sqrt{d}}{w_l} \;&=\; [a_l, a_{l+1}, a_{l+2}, \dots] \;=\; [2a_0, a_1, a_2, \dots] \;= \\ &=\; a_0 + [a_0, a_1, a_2, \dots] \;=\; a_0 + \sqrt{d},\end{aligned}$$

und daher gilt $v_l = a_0$ und $w_l = 1$. Es folgt (vgl. (16.15)(6))

$$\begin{aligned}a_0 r_{l-1} + r_{l-2} \;&=\; v_l r_{l-1} + w_l r_{l-2} \;=\; d s_{l-1} \quad \text{und} \\ a_0 s_{l-1} + s_{l-2} \;&=\; v_l s_{l-1} + w_l s_{l-2} \;=\; r_{l-1}.\end{aligned}$$

(b) Es sei jetzt $(\widetilde{r}_n/\widetilde{s}_n)_{n\geq 0}$ die Folge der Näherungsbrüche des Kettenbruchs $[a_l, a_{l+1}, a_{l+2}, \dots]$, und es sei $m \in \mathbb{N}$. Es gilt

$$\begin{aligned}\begin{pmatrix} r_{m+l} & r_{m+l-1} \\ s_{m+l} & s_{m+l-1} \end{pmatrix} \;&= \\ \overset{(13.2)(5)}{=}\; \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{l-1} & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_l & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{m+l} & 1 \\ 1 & 0 \end{pmatrix} \;&= \\ =\; \begin{pmatrix} r_{l-1} & r_{l-2} \\ s_{l-1} & s_{l-2} \end{pmatrix} \cdot \begin{pmatrix} \widetilde{r}_m & \widetilde{r}_{m-1} \\ \widetilde{s}_m & \widetilde{s}_{m-1} \end{pmatrix}\end{aligned}$$

und daher

$$r_{m+l} = r_{l-1}\widetilde{r}_m + r_{l-2}\widetilde{s}_m \quad \text{und} \quad s_{m+l} = s_{l-1}\widetilde{r}_m + s_{l-2}\widetilde{s}_m.$$

Es gilt

$$\frac{\widetilde{r}_m}{\widetilde{s}_m} = [a_l, a_{l+1}, \ldots, a_{m+l}] \overset{(16.14)}{=} [2a_0, a_1, \ldots, a_m] =$$
$$= a_0 + [a_0, a_1, a_2, \ldots, a_m] = a_0 + \frac{r_m}{s_m} = \frac{a_0 s_m + r_m}{s_m},$$

und wegen $\mathrm{ggT}(\widetilde{r}_m, \widetilde{s}_m) = 1$ und $\mathrm{ggT}(a_0 s_m + r_m, s_m) = \mathrm{ggT}(r_m, s_m) = 1$ folgt

$$\widetilde{r}_m = a_0 s_m + r_m \quad \text{und} \quad \widetilde{s}_m = s_m.$$

Also gilt

$$r_{m+l} = r_{l-1}(a_0 s_m + r_m) + r_{l-2}s_m = (a_0 r_{l-1} + r_{l-2})s_m + r_{l-1}r_m =$$
$$\overset{(a)}{=} d s_{l-1} s_m + r_{l-1} r_m$$

und

$$s_{m+l} = s_{l-1}(a_0 s_m + r_m) + s_{l-2}s_m = (a_0 s_{l-1} + s_{l-2})s_m + s_{l-1}r_m =$$
$$\overset{(a)}{=} r_{l-1}s_m + s_{l-1}r_m.$$

Es folgt

$$(r_{l-1} + s_{l-1}\sqrt{d}) \cdot (r_m + s_m\sqrt{d}) =$$
$$= (r_{l-1}r_m + d s_{l-1}s_m) + (r_{l-1}s_m + s_{l-1}r_m)\sqrt{d} = r_{m+l} + s_{m+l}\sqrt{d}.$$

(c) Durch Induktion folgt mit Hilfe des letzten Ergebnisses in (b): Für jedes $k \in \mathbb{N}$ ist

$$r_{kl-1} + s_{kl-1}\sqrt{d} = (r_{l-1} + s_{l-1}\sqrt{d})^k.$$

(17.13) Bemerkung: Es sei d eine natürliche Zahl, die keine Quadratzahl ist, es sei $(r_n/s_n)_{n\geq 0}$ die Folge der Näherungsbrüche des Kettenbruchs

$$\sqrt{d} = [a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots],$$

und es sei l die Länge einer primitiven Periode dieses Kettenbruchs.

(1) Es gelte: l ist gerade.
(a) $(x_1, y_1) := (r_{l-1}, s_{l-1})$ ist die Fundamentallösung der Gleichung

$$(*) \qquad X^2 - dY^2 = 1,$$

und nach (17.11) und (17.12) gilt: $(x, y) \in \mathbb{N} \times \mathbb{N}$ ist genau dann eine Lösung von $(*)$, wenn es eine natürliche Zahl k mit

$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^k$$

gibt. Die Gleichung

$$(**) \qquad X^2 - dY^2 = -1$$

hat keine Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.
(b) $\varepsilon_1 := x_1 + y_1\sqrt{d}$ ist eine Einheit im Ring $\mathbb{Z}[\sqrt{d}]$. Aus (17.11) und (17.12) folgt: Die Abbildung

$$\big([j]_2, k\big) \mapsto (-1)^j \varepsilon_1^k : (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z} \to E\big(\mathbb{Z}[\sqrt{d}]\big)$$

ist ein Isomorphismus des cartesischen Produkts der Gruppen $(\mathbb{Z}/2\mathbb{Z}, +)$ und $(\mathbb{Z}, +)$ auf die Einheitengruppe $E(\mathbb{Z}[\sqrt{d}])$ des Rings $\mathbb{Z}[\sqrt{d}]$.
(2) Es gelte: l ist ungerade.
(a) $(x_1, y_1) := (r_{l-1}, s_{l-1})$ ist die Fundamentallösung von $(**)$, und nach (17.11) und (17.12) gilt: $(x, y) \in \mathbb{N} \times \mathbb{N}$ ist genau dann eine Lösung von $(**)$, wenn es eine ungerade natürliche Zahl k mit

$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^k$$

gibt, und $(x, y) \in \mathbb{N} \times \mathbb{N}$ ist genau dann eine Lösung von $(*)$, wenn es eine gerade natürliche Zahl k mit

$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^k$$

gibt. Es gilt

$$(r_{2l-1}, s_{2l-1}) = (x_1 + \sqrt{d}y_1)^2 = (x_1^2 + dy_1^2) + 2x_1y_1\sqrt{d},$$

und daher ist $(x_1^2 + dy_1^2, 2x_1y_1)$ die Fundamentallösung von $(*)$.
(b) Wie in (1) ergibt sich: Die Abbildung

$$\big([j]_2, k\big) \mapsto (-1)^j \varepsilon_1^k : (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z} \to E\big(\mathbb{Z}[\sqrt{d}]\big)$$

ist ein Isomorphismus des cartesischen Produkts der Gruppen $(\mathbb{Z}/2\mathbb{Z}, +)$ und $(\mathbb{Z}, +)$ auf die Einheitengruppe $E(\mathbb{Z}[\sqrt{d}])$ des Rings $\mathbb{Z}[\sqrt{d}]$.

(17.14) Beispiel: Der Algorithmus QWplus aus (16.18) liefert für die Zahl $d = 47\,29494$ den Kettenbruch

$$\begin{aligned}\sqrt{47\,29494} &= \\ &= [2174, \overline{1,2,1,5,2,25,3,1,1,1,1,1,1,15,1,2,16,1,2,1,1,8,6,} \\ &\qquad \overline{1,21,1,1,3,1,1,1,2,2,6,1,1,5,1,17,1,1,47,3,1,1,\mathbf{6},} \\ &\qquad \overline{1,1,3,47,1,1,17,1,5,1,1,6,2,2,1,1,1,3,1,1,21,1,} \\ &\qquad \overline{6,8,1,1,2,1,16,2,1,15,1,1,1,1,1,1,3,25,2,5,1,2,1,4348}\,].\end{aligned}$$

(Die fettgedruckte 6 markiert die Mitte der Periode). Die Periode dieses Kettenbruchs hat die Länge 92. Für die Fundamentallösung (x_1, y_1) der Pellschen Gleichung

$$X^2 - 47\,29494\,Y^2 = 1$$

gilt daher nach (17.13): x_1 ist der Näherungszähler r_{91} des Kettenbruchs für $\sqrt{47\,29494}$, und y_1 ist der Näherungsnenner s_{91} dieses Kettenbruchs. Damit ergibt sich: Es gilt

$$\begin{aligned}x_1 &= 10993\,19867\,32829\,73497\,98662\,32821\,43354\,39010\,88049 \quad \text{und} \\ y_1 &= \quad 5\,05494\,85234\,31503\,30744\,77819\,73554\,04089\,86340.\end{aligned}$$

Die Gleichung

$$X^2 - 47\,29494\,Y^2 = -1$$

besitzt nach (17.13) keine Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

(17.15) Bemerkung: Das Beispiel in (17.14) hat eine historische Bedeutung. Aus der Antike ist eine Aufgabe überliefert, die Archimedes einst den Mathematikern in Alexandria gestellt haben soll und die mit einiger Wahrscheinlichkeit auch wirklich von ihm stammt, nämlich das sogenannte Rinderproblem (vgl. [3], Band III). Diese Aufgabe führt auf die Pellsche Gleichung

$$(*) \qquad V^2 - 8 \cdot 5128\,58029\,09803 \cdot W^2 = 1,$$

deren Fundamentallösung (v, w) zu berechnen ist. Dies ist mittels MuPAD auf dem direkten Weg wohl nicht möglich, da eine primitive Periode des Kettenbruch für $\sqrt{8 \cdot 5128\,58029\,09803}$ die Länge 2 03254 besitzt, wie sich mit Hilfe des Algorithmus QWplus in (16.18) ergibt (vgl. Aufgabe 4 in (16.20)). Statt $(*)$ direkt zu lösen, berechnet man die Fundamentallösung (x, y) der in (17.14) betrachteten Pellschen Gleichung

$$X^2 - 47\,29494\,Y^2 = 1$$

und berechnet daraus die natürlichen Zahlen v und w mit

$$v + w\sqrt{47\,29494} \;=\; (x + y\sqrt{47\,29494}\,)^{2329}.$$

Hier kann nicht darauf eingegangen werden, warum man auf diese Weise gerade die Fundamentallösung (v, w) von $(*)$ erhält. Die Formulierung der Aufgabe, eine genauere Beschreibung des Lösungswegs und der Berechnung der Lösung mit Hilfe von MuPAD, sowie ausführliche Literaturhinweise zu ihrer Geschichte findet man in [100].

Jedenfalls erfordert die Berechnung einer Lösung des Rinderproblems von Archimedes die Berechnung der Fundamentallösung einer Pellschen Gleichung. Da die Aufgabe ohne Zweifel aus der Antike stammt, kamen Mathematikhistoriker zu der Meinung, daß der Autor des Rinderproblems, also mit einiger Sicherheit Archimedes, ein Lösungsverfahren für Pellsche Gleichungen kannte. Leider sagen die überlieferten Schriften von Archimedes darüber nichts. Immerhin gab es schon vor Fermat Mathematiker, die sich mit Pellschen Gleichungen beschäftigten, allerdings außerhalb der abendländischen Mathematikgeschichte: Bereits um das Jahr 1000 lösten die indischen Mathematiker Jayadeva und Bhāskara der Jüngere Pellsche Gleichungen, und manches spricht dafür, daß die von ihnen verwendeten Methoden schon 500 Jahre früher bekannt waren. Warum sollte also nicht auch Archimedes oder ein anderer griechischer Mathematiker ein Lösungsverfahren gekannt haben? Wie C.-O. Selenius in [101] zeigt, läßt sich übrigens auch das Lösungsverfahren der alten indischen Mathematiker mit Hilfe von Kettenbruchentwicklungen beschreiben; die dabei auftretenden Kettenbrüche sind allerdings, anders als in diesem Buch, sogenannte halbregelmäßige Kettenbrüche. So darf man sich vielleicht wirklich vorstellen, daß Archimedes Kettenbrüche kannte und daß er dann auch mit ihrer Hilfe die rationalen Approximationen für Quadratwurzeln fand, die er zur Berechnung von π verwendete (vgl. (15.8)).

(17.16) Aufgabe: (1) Man schreibe eine MuPAD-Funktion, die zu einer natürlichen Zahl d, die keine Quadratzahl ist, die Fundamentallösung der Gleichung $X^2 - dY^2 = 1$ berechnet.

(2) Man schreibe eine MuPAD-Funktion, die zu einer natürlichen Zahl d, die keine Quadratzahl ist, die Fundamentallösung der Gleichung $X^2 - dY^2 = -1$ berechnet, falls diese Gleichung überhaupt eine Lösung in $\mathbb{Z} \times \mathbb{Z}$ besitzt.