Kapitel 5
Kettenbrüche

§1: Der Kettenbruchalgorithmus

Der EUKLIDische Algorithmus läßt sich auch verwenden, um eine reelle Zahl durch Brüche zu approximieren. Beginnen wir der Einfachheit halber mit einer rationalen Zahl $\alpha = \frac{n}{m}$ mit $n, m \in \mathbb{N}$. Der erste Schritt des EUKLIDischen Algorithmus dividiert n durch m:

$$n : m = q_0 \text{ Rest } r_1 \Longrightarrow \alpha = \frac{n}{m} = q_0 + \frac{r_1}{m} .$$

Falls $r_1 \neq 0$ ist, wird im zweiten Schritt m durch r_1 dividiert:

$$m : r_1 = q_1 \text{ Rest } r_2 \Longrightarrow \frac{m}{r_1} = q_1 + \frac{r_2}{r_1} \Longrightarrow \alpha = q_0 + \frac{1}{q_1 + \frac{r_2}{r_1}} .$$

Ist auch noch r_2 von Null verschieden, wird sodann r_1 durch r_2 dividiert:

$$r_1 : r_2 = q_2 \text{ Rest } r_3 \Longrightarrow \frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2} \Longrightarrow \alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}}} ,$$

und so weiter. Die Konstruktion muß nach endlich vielen Schritten abbrechen, denn die Folge der Reste r_i beim EUKLIDischen Algorithmus ist monoton fallend und muß daher schließlich Null erreichen. Damit ist α dargestellt als ein sogenannter **Kettenbruch**.

Wir können die Konstruktion auch so formulieren, daß sie nur von der Zahl $\alpha = \frac{n}{m}$ abhängt: Der Quotient bei der Division mit Rest von n

durch m ist $q_0 = [\alpha]$, und der durch m dividierte Rest ist $\alpha - q_0$. Dies führt zu folgender Formulierung des Algorithmus:

Setze zur Initialisierung $c_0 = [\alpha]$ und schreibe

$$\alpha = c_0 + \alpha_1 \quad \text{mit} \quad 0 \leq \alpha_1 < 1 \,.$$

Im i-ten Schritt, $i \geq 1$, bricht der Algorithmus ab, falls α_i verschwindet; andernfalls wird c_i definiert als größte ganze Zahl kleiner oder gleich $1/\alpha_i$ und α_{i+1} so, daß gilt

$$\frac{1}{\alpha_i} = c_i + \alpha_{i+1} \,.$$

Offensichtlich ist dann

$$\alpha = c_0 + \alpha_0 = c_0 + \frac{1}{c_1 + \alpha_1} = c_0 + \frac{1}{c_1 + \dfrac{1}{c_2 + \alpha_2}}$$

$$= \cdots = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots \; + \cfrac{1}{c_{r-1} + \cfrac{1}{c_r + \alpha_r}}}}} \,.$$

Da diese Darstellung sehr viel Platz verbraucht, verwendet man dafür oft auch die kompaktere Schreibweise

$$\alpha = [c_0, c_1, \ldots, c_r; \alpha_r] \,.$$

Falls der Algorithmus mit $\alpha_r = 0$ abbricht, steht im untersten Bruch natürlich nur c_r im Nenner, und wir schreiben den Kettenbruch kurz als $[c_0, c_1, \ldots, c_r]$.

So, wie der Algorithmus jetzt formuliert ist, können wir ihn auch auf irrationale Zahlen α anwenden. Dann kann kein α_r verschwinden, denn sonst hätten wir ja eine Darstellung von α als rationale Zahl. Wir können aber nach dem r-ten Schritt abbrechen und den Bruch betrachten, der entsteht, wenn wir $\alpha_r = 0$ setzen. Diesen Bruch bezeichnen wir als die r-te **Konvergente** der Kettenbruchentwicklung von α.

Als Beispiel betrachten wir $\alpha = \sqrt{2}$. Hier ist $c_0 = \lfloor\sqrt{2}\rfloor = 1$ und $\alpha_1 = \sqrt{2} - 1$. Also ist

$$\frac{1}{\alpha_1} = \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)} = \sqrt{2}+1\,,$$

d.h. $c_1 = \lfloor 1+\sqrt{2}\rfloor = 2$ und $\alpha_2 = 1+\sqrt{2}-2 = \sqrt{2}-1 = \alpha_1$. Damit wiederholt sich ab jetzt alles, d.h.

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2+\dots}}}}}\,.$$

In Analogie zu periodischen Dezimalbrüchen schreibt man dies auch kurz in der Form

$$\sqrt{2} = [1,2,2,2,\dots] = [1,\overline{2}]\,.$$

Die ersten Partialbrüche sind

$$P_0 = 1, \quad P_1 = 1+\frac{1}{2} = 1{,}5, \quad P_2 = 1 + \cfrac{1}{2+\frac{1}{2}} = \frac{7}{5} = 1{,}4\,,$$

$$P_3 = 1 + \cfrac{1}{2 + \cfrac{1}{2+\frac{1}{2}}} = \frac{17}{12} = 1{,}41\overline{6} \quad \text{und} \quad P_4 = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2+\frac{1}{2}}}} = \frac{41}{29}\,,$$

was ungefähr gleich 1,4137931 ist. Die Fehler $\sqrt{2} - P_n$ sind, gerundet auf sechs Nachkommastellen, die Zahlen

$$0{,}414214,\ -0{,}085786,\ 0{,}014214,\ -0{,}002453 \quad \text{und} \quad 0{,}000420\,;$$

verglichen mit den kleinen Nennern $1, 2, 5, 12$ und 29 haben wir also erstaunlich gute Übereinstimmungen, und im übrigen ist auch die Kettenbruchentwicklung erheblich regelmäßiger als die Dezimalbruchdarstellung von $\sqrt{2}$.

Als zweites Beispiel betrachten wir $\alpha = \pi$; hier erhalten wir zunächst $c_0 = 3$ und $\alpha_1 = \pi - 3 \approx 0{,}14159$, sodann

$$c_1 = \left[\frac{1}{\pi - 3}\right] = 7 \quad \text{und} \quad \alpha_2 \approx 0{,}062513285\,.$$

Im nächsten Schritt ist $c_2 = \left[\frac{1}{\alpha_2}\right] = 15$ und $\alpha_3 \approx 0{,}99659976$. Weiter geht es mit $c_3 = 1$, $c_4 = 292$, $c_5 = c_6 = c_7 = 1$, $c_8 = 2$ und $c_9 = 1$. Ein Muster ist weder erkennbar, noch ist eines bekannt.

Die Kettenbruchentwicklung von π ist somit

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, \ldots]\,.$$

Die ersten Partialbrüche und ihre Differenzen von π sind

3	$3\,\frac{1}{7}$	$3\,\frac{15}{106}$	$3\,\frac{16}{113}$	$3\,\frac{4687}{33102}$
$0{,}14$	$-0{,}0013$	$8{,}3 \cdot 10^{-5}$	$-2{,}7 \cdot 10^{-7}$	$5{,}8 \cdot 10^{-10}$

Auch hier haben wir wieder, verglichen mit der Größe des Nenners, exzellente Approximationseigenschaften.

§2: Geometrische Formulierung

Wir wollen uns zunächst überlegen, daß die Konvergenten der Kettenbruchentwicklung einer irrationalen Zahl stets die bei vorgegebener Größenordnung des Nenners bestmögliche rationale Approximation dieser Zahl liefern.

Dazu betrachten wir (im wesentlichen nach dem Ansatz von HAROLD STARK in seinem Buch *An Introduction to Number Theory*, MIT Press, 1978) das Problem der rationalen Approximation von der geometrischen Seite: Zur reellen Zahl $\alpha > 0$ haben wir die Gerade $y = \alpha x$ durch den Nullpunkt, und offensichtlich ist α genau dann rational, wenn auf dieser Geraden außer dem Nullpunkt noch ein weiterer Punkt (q, p) mit ganzzahligen Koordinaten liegt. Rationale Approximationen erhalten wir durch Punkte $(q, p) \in \mathbb{Z} \times \mathbb{Z}$, die in der Nähe der Geraden liegen.

(Die Reihenfolge der Koordinaten mag auf den ersten Blick verwundern; sie kommt daher, daß wir die Steigung α der Geraden durch die Steigung des Ortsvektors zum Punkt (q, p) annähern wollen, und die ist p/q.)

Die folgende Konstruktion liefert Punkte P_n nahe der Geraden, die für gerade n stets unterhalb $y = \alpha x$ liegen und für ungerade n darüber:

Wir starten mit $P_{-2} = (1, 0)$ und $P_{-1} = (0, 1)$.

Zu zwei Punkten $P = (q, p)$ und $P' = (q', p')$, die auf verschiedenen Seiten der Geraden liegen, gibt es stets eine nichtnegative ganze Zahl $c \in \mathbb{N}_0$, so daß $P + cP'$ entweder auf der Geraden liegt oder aber auf derselben Seite wie P, während $P + (c+1)P'$ auf der anderen Seite liegt.

Liegt nämlich beispielsweise P unterhalb der Geraden, so ist $p/q < \alpha$, also $p - \alpha q < 0$. Für den oberhalb der Geraden liegenden Punkt P' ist entsprechend $p' - \alpha q' > 0$. Damit ist klar, daß

$$c = \left\lceil \left| \frac{p - \alpha q}{p' - \alpha q'} \right| \right\rceil$$

das Verlangte leistet. Man überlegt sich leicht, daß diese Formel auch gilt, wenn P oberhalb und P' unterhalb der Geraden liegt.

Zähler und Nenner des obigen Bruchs lassen sich einfach geometrisch interpretieren: $(q, \alpha q)$ hat dieselbe x-Koordinate wie $P = (q, p)$ und liegt auf der Geraden $y = \alpha x$; daher ist $p - \alpha q$ der (gerichtete) vertikale Abstand von P zur Geraden und $p' - \alpha q'$ entsprechend der von P'.

Ausgehend von $P = P_{-2} = (1, 0)$ und $P' = P_{-1} = (0, 1)$ definieren wir nun die Punkte P_n für $n \geq 0$ mit dem wie oben definierten $c = c_n$ aus ihren beiden Vorgängern rekursiv als

$$P_n = P_{n-2} + c_n P_{n-1} .$$

Dann liegt P_n auf derselben Seite der Geraden wie P_{n-2}, für gerades n also unterhalb und für ungerades oberhalb – es sei denn, irgendwann einmal liegt ein P_n *auf* der Geraden. In diesem Fall ist α rational und wir brechen die Konstruktion ab. Für irrationales α erhalten wir eine unendliche Folge von Punkten P_n.

Bezeichnen wir mit $d_n = p_n - \alpha q_n$ den gerichteten vertikalen Abstand des Punktes $P_n = (q_n, p_n)$ von der Geraden $y = \alpha x$, so ist nach obiger Formel

$$c_n = \left[\left|\frac{d_{n-2}}{d_{n-1}}\right|\right] .$$

Daher verschwindet c_n genau dann, wenn $\left|d_{n-2}\right| < \left|d_{n-1}\right|$ ist.

Ist dagegen $\left|d_{n-1}\right| < \left|d_{n-2}\right|$, so ist $c_n \geq 1$, und da $P_n = P_{n-2} + c_n P_{n-1}$ auf derselben Seite der Geraden liegt wie P_{n-2}, ist auch

$$\begin{aligned} d_n &= d_{n-2} + c_n d_{n-1} = d_{n-2} + \left[\left|\frac{d_{n-2}}{d_{n-1}}\right|\right] d_{n-1} \\ &= d_{n-1}\left(\left[\left|\frac{d_{n-2}}{d_{n-1}}\right|\right] + \frac{d_{n-2}}{d_{n-1}}\right) \end{aligned}$$

betragsmäßig kleiner als d_{n-1}. (Man beachte, daß d_{n-1} und d_{n-2} verschiedene Vorzeichen haben!) Falls daher für einen Index n der Abstand von P_{n-1} zur Geraden $y = \alpha x$ kleiner ist als der von P_{n-2}, gilt dasselbe auch für alle folgenden Indizes, und ab dem Index n sind alle $c_i \geq 1$.

Die ersten beiden Abstände sind $d_{-2} = -\alpha$ und $d_{-1} = 1$; es hängt von α ab, welche der beiden Zahlen den größeren Betrag hat.

Der nächste Punkt ist $P_0 = (1, c_0)$ mit $c_0 = [\alpha]$, also ist $d_0 = [\alpha] - \alpha$, und der Betrag davon ist kleiner als $d_{-1} = 1$. Somit ist für alle $n \geq 1$ der Koeffizient c_n von Null verschieden und $|d_n| < \left|d_{n-1}\right|$.

Aus den Beziehungen $p_n = p_{n-2} + c_n p_{n-1}$ und $q_n = q_{n-2} + c_n q_{n-1}$ sehen wir daher, daß die Folge der q_n wie auch der p_n für $n \geq 1$ strikt monoton ansteigt, während die Folge der Differenzen

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{|d_n|}{q_n}$$

strikt monoton fällt. Die Brüche p_n/q_n geben also immer bessere Annäherungen an α.

Wir können die obigen Rekursionsformeln zusammenfassen zur Matrixgleichung

$$\begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} = \begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p_{n-1} & q_{n-1} \\ p_{n-2} & q_{n-2} \end{pmatrix} ;$$

wenden wir darauf den Multiplikationssatz für Determinanten an, erhalten wir die Formel

$$p_n q_{n-1} - q_n p_{n-1} = -(p_{n-1} q_{n-2} - q_{n-1} p_{n-2}) .$$

Für $n = 0$ ist $p_{-1} q_{-2} - q_{-1} p_{-2} = 0 \cdot 0 - 1 \cdot 1 = -1$; daraus folgt induktiv die Formel $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$. Insbesondere sind die Zahlen p_n und q_n stets teilerfremd, p_n/q_n ist also ein gekürzter Bruch.

Als nächstes wollen wir uns überlegen, daß die Folge dieser Brüche gegen α konvergiert. Da P_n und P_{n+1} auf verschiedenen Seiten der Geraden $y = \alpha x$ liegen, ist für $n \geq 0$

$$\left| \alpha - \frac{p_n}{q_n} \right| \leq \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \left| \frac{p_{n+1} q_n - q_{n+1} p_n}{q_n q_{n+1}} \right|$$
$$= \frac{1}{q_n q_{n+1}} = \frac{1}{q_n (q_{n-1} + c_{n+1} q_n)} \leq \frac{1}{q_n^2} .$$

Da die Folge der q_n strikt monoton ansteigt, konvergiert die Folge der p_n/q_n somit gegen α, und dies sogar extrem gut: Ist p/q eine rationale Approximation einer irrationalen Zahl α, so kann der Fehler im allgemeinen bis zu $1/2q$ betragen; hier ist er höchstens $1/q^2$ und tatsächlich wohl, da wir recht grob abgeschätzt haben, meist noch kleiner. Wie wir gleich sehen werden, muß umgekehrt p/q eine Konvergente der Kettenbruchentwicklung von α sein, wenn $|\alpha - p/q| < 1/2q^2$ ist.

Zuvor müssen wir uns aber noch überlegen, daß die hier betrachteten Brüche p_n/q_n tatsächlich die Konvergenten der in §1 definierten Kettenbruchentwicklung sind und daß die hier betrachteten Zahlen c_i mit denen übereinstimmen, die der Kettenbruchalgorithmus liefert.

Dazu setzen wir

$$\alpha_n = \left| \frac{d_{n-1}}{d_{n-2}} \right| = -\frac{d_{n-1}}{d_{n-2}} ;$$

zumindest für $n \geq 1$ ist dann $\alpha_n < 1$. Wegen $c_n = \left[\left| d_{n-2}/d_{n-1} \right| \right]$ ist dann $c_n = [1/\alpha_n]$. Division der Beziehung $d_n = d_{n-2} + c_n d_{d-1}$ durch d_{n-1} führt auf

$$\frac{d_n}{d_{n-1}} = \frac{d_{n-2}}{d_{n-1}} + c_n \quad \text{oder} \quad -\alpha_{n+1} = -\frac{1}{\alpha_n} + c_n ,$$

was wir wiederum umformen können zu

$$\frac{1}{\alpha_n} = c_n + \alpha_{n+1} .$$

Da $c_n = [1/\alpha_n]$ ist $\alpha = c_0 + \alpha_1$, führt dies genau auf die in §1 konstruierten Folgen der c_n und α_n.

Insbesondere liefern unsere Rekursionsformeln für die Koordinaten p_n und q_n Zähler und Nenner der Konvergenten der Kettenbruchentwicklung von α, was wir als Satz festhalten wollen:

Satz: Ist $\alpha = [c_0, c_1, c_2, \dots]$ die Kettenbruchentwicklung einer reellen Zahl, so lassen sich die Konvergenten p_n/q_n folgendermaßen rekursiv berechnen:

$$p_0 = c_0, q_0 = 1, p_1 = c_0c_1 + 1, q_1 = c_1,$$
$$p_n = p_{n-2} + c_n p_{n-1} \quad \text{und} \quad q_n = q_{n-2} + c_n q_{n-1} \quad \text{für } n \geq 2 .$$

Die so berechneten Zahlen p_n und q_n sind stets teilerfremd; genauer ist $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$ für alle n.

Zu *beweisen* gibt es hier nichts, denn wir haben alle diese Formeln bereits bewiesen für die Koordinaten q_n und p_n von P_n, und wie wir gerade gesehen haben, sind das der Nenner und der Zähler der n-ten Konvergenten.

∎

Für spätere Anwendungen wollen wir noch eine Formel herleiten, wie sich α aus α_n sowie den Konvergenten p_{n-1}/q_{n-1} und p_{n-2}/q_{n-2} berechnet läßt: Nach Definition ist

$$\alpha_n = -\frac{d_{n-1}}{d_{n-2}} = -\frac{p_{n-1} - \alpha q_{n-1}}{p_{n-2} - \alpha q_{n-2}} .$$

Damit ist $\alpha_n(\alpha q_{n-2} - p_{n-2}) = p_{n-1} - \alpha q_{n-1}$, was durch Umordnung der Terme auf $\alpha(\alpha_n q_{n-2} + \alpha q_{n-1}) = \alpha_n p_{n-2} + p_{n-1}$ führt. Also ist

$$\alpha = \frac{\alpha_n p_{n-2} + p_{n-1}}{\alpha_n q_{n-2} + q_{n-1}} .$$

§3: Optimale Approximation

Nach den Vorbereitungen im letzten Paragraphen können wir nun beweisen, daß Kettenbrüche in der Tat bestmögliche Approximationen sind im folgenden Sinne: Ist r/s irgendein Bruch, dessen Nenner s zwischen den Nennern q_{n-1} und q_n zweier Konvergenten der Kettenbruchentwicklung liegt, so ist p_{n-1}/q_{n-1} eine bessere Approximation als r/s:

Lemma: p_n/q_n seien die Konvergenten der Kettenbruchentwicklung einer reellen Zahl α. Falls α irrational ist oder rational mit einem Nenner echt größer q_n, $n \geq 2$, so ist für jede rationale Zahl r/s mit $s \leq q_n$ und $r/s \notin \{p_{n-1}/q_{n-1}, p_n/q_n\}$

$$\left|\alpha - \frac{r}{s}\right| > \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| .$$

Beweis: Wir betrachten die Punkte $P_{n-1} = (q_{n-1}, p_{n-1})$, $P_n = (q_n, p_n)$ und $R = (s, r)$. Es genügt zu zeigen, daß der vertikale Abstand von P_{n-1} zur Geraden $y = \alpha x$ einen kleineren Betrag hat als der von R.

Wir schreiben R als ganzzahlige Linearkombination $R = kP_{n-1} + \ell P_n$ der Punkte P_{n-1} und P_n. Das ist möglich, denn die Determinante des linearen Gleichungssystems

$$\begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix} \begin{pmatrix} k \\ \ell \end{pmatrix} = \begin{pmatrix} r \\ s \end{pmatrix}$$

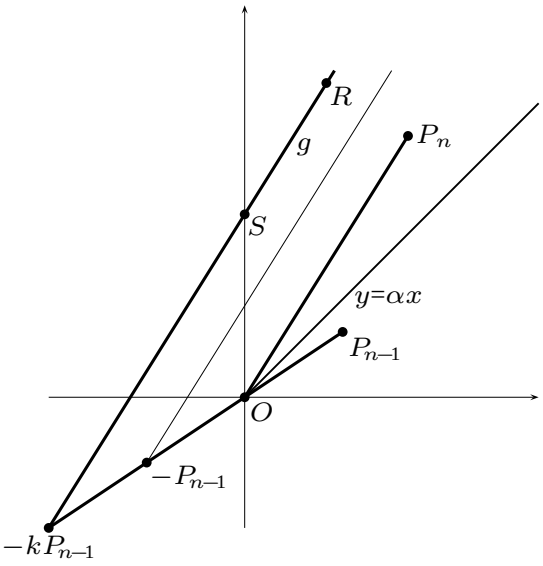
ist nach dem Satz am Ende des vorigen Paragraphen gleich

$$p_{n-1}q_n - p_n q_{n-1} = (-1)^{n-1} .$$

Die somit eindeutig bestimmte Lösung (k, ℓ) des Gleichungssystems ist ganzzahlig, denn wenn wir sie nach der CRAMERschen Regel ausdrücken, sind k und ℓ Brüche mit dieser Determinante im Nenner und einer ganzzahligen Determinante im Zähler.

Für das Folgende wollen wir uns auf den Fall $p_{n-1}/q_{n-1} < \alpha < p_n/q_n$ beschränken; der Fall $p_{n-1}/q_{n-1} > \alpha > p_n/q_n$ geht völlig analog.

Wir betrachten die Gerade g durch kP_{n-1} mit Steigungsvektor $\overrightarrow{OP_n}$; nach unserer Annahme ist ihre Steigung größer als α.



Im Fall $k < 0$ liegt der Punkt kP_{n-1} und damit die ganze Gerade g zumindest ab dem Punkt kP_{n-1} oberhalb der Geraden $y = \alpha x$, und wegen der größeren Steigung von g steigt der Abstand zwischen den beiden Geraden mit wachsendem x. Wir können den Abstand von R zur Geraden $y = \alpha x$ daher nach unten abschätzen durch den Abstand des Schnittpunkts S von g mit der y-Achse. Dessen Abstand wiederum können wir nach unten abschätzen, indem wir $k = -1$ setzen, denn in diesem Fall ist der Abstand von g zur Geraden $y = \alpha x$ am kleinsten. Der Punkt $-P_{n-1}$ hat (betragsmäßig) denselben Abstand von $y = \alpha x$ wie P_{n-1}, und da die Abszisse $x = 0$ von S größer ist als die von $-P_n$, hat somit S einen größeren Abstand von $y = \alpha x$ als P_{n-1}. Im Fall $k < 0$ ist damit die Behauptung bewiesen.

Als nächstes betrachten wir den Fall $k > 0$. Dann muß $\ell \leq 0$ sein, denn sonst wäre die x-Koordinate $s = kq_{n-1} + \ell q_n$ von R größer als q_n. Der Punkt kP_{n-1} liegt unterhalb der Geraden $y = \alpha x$ und die Gerade g nähert sich dieser mit steigender Abszisse immer mehr an. Da der Punkt R entweder dieselbe Abszisse wie kP_{n-1} hat oder eine kleinere, ist sein Abstand somit höchstens gleich dem von kP_{n-1}, der wiederum das k-fache des Abstands von P_{n-1} ist. Für $k \geq 2$ erhalten wir damit die gewünschte strikte Ungleichung. Für $k = 1$ erhalten wir auch eine, denn wegen der Voraussetzung $R \neq P_{n-1}$ muß dann $\ell \geq 1$ sein.

Bleibt noch der Fall $k = 0$. Dann ist $R = \ell P_n$, wobei $\ell \neq 1$, da $R \neq P_n$. Anderseits kann ℓ auch nicht größer als eins sein, denn $s \leq q_n$. Somit kommt dieser Fall gar nicht vor.

■

Als nächstes wollen wir uns überlegen, wann gute Approximationen Konvergenten der Kettenbruchentwicklung sein müssen. Wir wissen

bereits, daß für die Konvergenten gilt

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}\,.$$

Dies charakterisiert die Konvergenten allerdings noch nicht: Betrachten wir etwa die Kettenbruchentwicklung von $\alpha = \sqrt{3}$. Der Algorithmus liefert zunächst $c_0 = \lfloor\sqrt{3}\rfloor = 1$ und $\alpha_1 = \sqrt{3} - 1$. Der Kehrwert davon ist

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} \Longrightarrow c_1 = 1 \quad \text{und} \quad \alpha_2 = \frac{\sqrt{3}-1}{2}\,.$$

Der Kehrwert davon ist

$$\frac{2}{\sqrt{3}-1} = \sqrt{3}+1 \Longrightarrow c_2 = 2 \quad \text{und} \quad \alpha_3 = \sqrt{3}-1 = \alpha_1\,.$$

Ab hier wiederholt sich also alles periodisch, d.h.

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cdots}}}} = [1, \overline{1,2}]\,.$$

Die ersten Konvergenten der Kettenbruchentwicklung sind

$$1, \quad 2, \quad 1\frac{2}{3}, \quad 1\frac{3}{4}, \quad 1\frac{8}{11} \quad \text{und} \quad 1\frac{11}{15}\,;$$

da die Folge der Nenner monoton steigt, gibt es also keine Konvergente mit Nenner sieben. Trotzdem ist

$$\left|\sqrt{3} - 1\frac{5}{7}\right| \approx 0{,}017765 < 0{,}2 = \frac{1}{50} < \frac{1}{49} = \frac{1}{7^2}\,.$$

Dafür gilt aber der folgende Satz, dessen zweite Hälfte bereits 1808 von ADRIEN-MARIE LEGENDRE (1752–1833) bewiesen wurde:

Satz: *a)* Eine irrationale Zahl α erfüllt für jedes $n \geq 2$ mindestens eine der beiden Ungleichungen

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2} \quad \text{oder} \quad \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2}\,.$$

b) Erfüllen zwei ganze Zahlen p, q die Ungleichung $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, so ist $\frac{p}{q}$ eine Konvergente der Kettenbruchentwicklung von α.

Beweis: a) Angenommen, beide Ungleichungen sind falsch. Nach Multiplikation mit q_{n-1} *bzw.* q_n haben wir dann die beiden Relationen

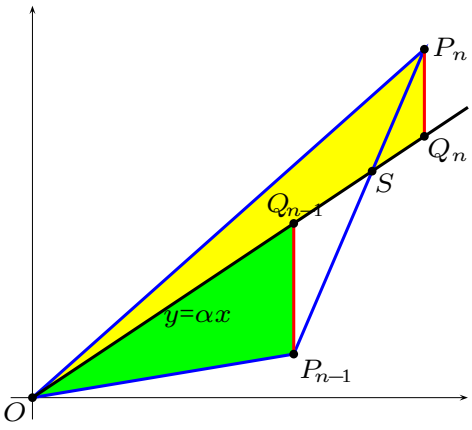
$$\left|q_{n-1}\alpha - p_{n-1}\right| \geq \frac{1}{2q_{n-1}} \quad \text{und} \quad \left|q_n\alpha - p_n\right| \geq \frac{1}{2q_n}\,.$$

Wir nehmen für den Beweis wieder an, daß $p_{n-1}/q_{n-1} < \alpha < p_n/q_n$ ist; der umgekehrte Fall geht völlig analog.

Nach unserer Annahme liegt der Punkt $P_{n-1} = (q_{n-1}, p_{n-1})$ unterhalb der Geraden $y = \alpha x$, und $P_n = (q_n, p_n)$ liegt darüber.

Das Kreuzprodukt (siehe Anhang) der Vektoren $\overrightarrow{OP_{n-1}}$ und $\overrightarrow{OP_n}$ hat als Betrag die Fläche des davon aufgespannten Parallelogramms; das Dreieck mit Ecken O, P_{n-1} und P_n ist halb so groß. Wegen der Beziehung $p_nq_{n-1} - q_np_{n-1} = (-1)^{n-1}$ ist die Fläche dieses Dreiecks daher gleich $1/2$.

Als nächstes betrachten wir zu den Punkten $P_i = (q_i, p_i)$ ihre Projektionen $Q_i = (q_i, \alpha q_i)$ in y-Richtung auf die Gerade $y = \alpha x$ und die Dreiecke $\triangle OP_iQ_i$. Nach Voraussetzung ist die Länge der Seite P_iQ_i für $i = n-1$ und $i = n$ mindestens $1/2q_i$. Die darauf senkrecht stehende Höhe ist q_i, also ist die Fläche jedes der beiden Dreiecks mindestens $1/4$.



Ist S der Schnittpunkt der Geraden $y = \alpha x$ mit der Verbindungsstrecke von P_{n-1} und P_n, so ist das Dreieck $\triangle OP_{n-1}P_n$ die Vereinigung der Dreiecke $\triangle OP_{n-1}Q_{n-1}$, $\triangle OP_nQ_n$ und $\triangle P_{n-1}Q_{n-1}S$, minus dem Dreieck $\triangle SP_nQ_n$. Die Dreiecke beiden $\triangle P_{n-1}Q_{n-1}S$ und $\triangle SP_nQ_n$ sind ähnlich, und da jede Konvergente eine bessere Approximation liefert als ihre Vorgänger,

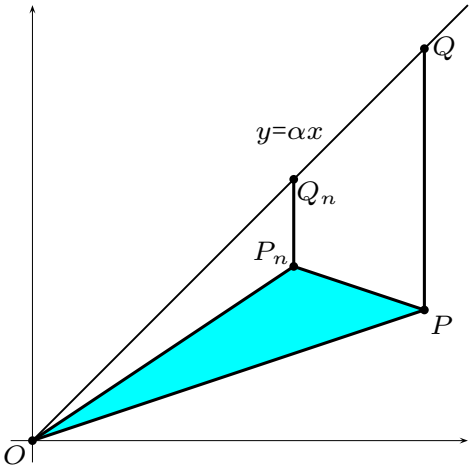
ist das zweite dieser Dreiecke das kleinere. Daher ist die Fläche des Dreiecks $\triangle OP_{n-1}P_n$ größer als die Summe der Flächen der Dreiecke $\triangle OP_{n-1}Q_{n-1}$ und $\triangle OP_nQ_n$, also größer als $1/4 + 1/4 = 1/2$. Dies ist ein Widerspruch zur obigen direkten Berechnung dieser Fläche.

b) Wir können natürlich voraussetzen, daß der Bruch p/q gekürzt ist, denn für jede nichtgekürzte Darstellung ist die Bedingung echt schärfer.

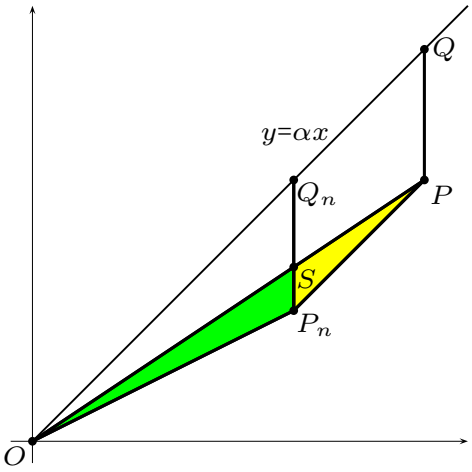
Da die Folge der Nenner q_n strikt monoton ansteigt, gibt es genau ein n, so daß $q_n \leq q < q_{n+1}$ ist; wir müssen zeigen, daß $p/q = p_n/q_n$ ist. Andernfalls ist $pq_n - qp_n \neq 0$, also – da dies eine ganze Zahl ist – $|pq_n - qp_n| \geq 1$. Setzen wir $P = (q, p)$, so ist also die Fläche des Dreiecks $\triangle OPP_n$ mindestens gleich $1/2$.

Seien wieder $Q = (q, \alpha q)$ und $Q_n = (q_n, \alpha q_n)$ die Projektionen der betrachteten Punkte auf die Gerade $y = \alpha x$. Die Länge der Strecke $\overline{PQ}$ ist $|\alpha q - p|$, was nach Voraussetzung kleiner als $1/2q$ ist. Nach dem Lemma zu Beginn dieses Paragraphen ist die Strecke $\overline{P_nQ_n}$ kürzer als $\overline{PQ}$, also ebenfalls kleiner als $1/2q$ und damit erst recht kleiner als $1/2q_n$. Somit haben beide Dreiecke $\triangle OPQ$ und $\triangle OP_nQ_n$ Flächen, die kleiner sind als $1/4$.

Wir wollen uns überlegen, daß dann auch die Fläche des Dreiecks $\triangle OPP_n$ kleiner als $1/2$ sein muß, im Widerspruch zur obigen Rechnung. Die Geometrie hängt dabei stark davon ab, wie die Punkte P und P_n sowohl zueinander wie auch in Bezug auf die Gerade $y = \alpha x$ liegen.



Betrachten wir als erstes den Fall, daß p_n/q_n zwischen α und p/q liegt. Dann liegt der Punkt P_n im Innern des Dreiecks $\triangle OPQ$, also ist das gesamte Dreieck $\triangle OPP_n$ im Dreieck $\triangle OPQ$ enthalten. Da ersteres mindestens die Fläche $1/2$ hat, letzteres aber weniger als $1/4$, kann dieser Fall offensichtlich nicht vorkommen.

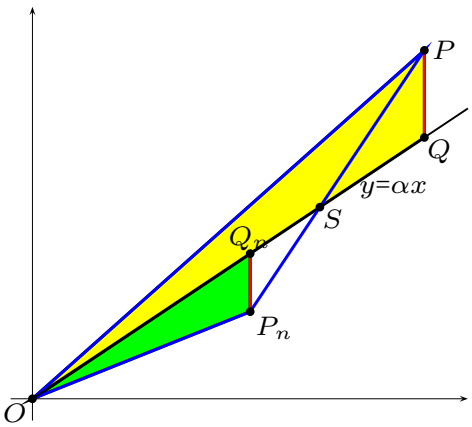


Als nächstes nehmen wir an, p/q liege zwischen α und p_n/q_n. Dann schneiden sich die Strecken $\overline{P_nQ_n}$ und $\overline{OP}$ in einem Punkt S, und das Dreieck $\triangle OPP_n$ ist die Vereinigung der beiden Dreiecke $\triangle OSP_n$ und $\triangle SPP_n$. Zur Flächenberechnung gehen wir aus von der gemeinsamen Kante $\overline{SP_n}$; die darauf senkrecht stehenden Höhen haben die Längen q_n und $q - q_n$. Somit ist die verdoppelte Fläche des gesamten Dreiecks $\triangle OPP_n$ gleich

$$\left|\overline{SP_n}\right| \cdot q_n + \left|\overline{SP_n}\right| \cdot (q - q_n) = \left|\overline{SP_n}\right| \cdot q \le \left|\overline{P_nQ_n}\right| \cdot q \le \left|\overline{PQ}\right| \cdot q\,,$$

denn da q zwischen q_n und q_{n+1} liegt, kann P_n nach obigem Lemma keinen größeren Abstand von der Geraden $y = \alpha x$ haben als P. Rechts steht aber die verdoppelte Fläche des Dreiecks $\triangle OPQ$, von der wir wissen, daß sie höchstens gleich $1/2$ ist, so daß auch dieser Fall nicht auftreten kann.

Bleibt noch der Fall, daß α zwischen p/q und p_n/q_n liegt, P und P_n also auf verschiedenen Seiten der Geraden $y = \alpha x$ liegen. Dann schneidet ihre Verbinungsstrecke $\overline{PP_n}$ diese Gerade in einem Punkt S. Damit sind wir in einer ähnlichen Situation wie beim Beweis von *a):* Das Dreieck $\triangle OPP_n$ ist gleich dem Dreieck $\triangle OP_nQ_n$ plus dem Dreieck $\triangle OPQ$ plus $\triangle SP_nQ_n$ minus $\triangle SPQ$. Die beiden letzteren



Dreiecke sind ähnlich, und da $\overline{PQ}$ nicht kürzer sein kann als $\overline{P_nQ_n}$ ist das subtrahierte Dreieck mindestens genauso groß wie $\triangle SP_nQ_n$. Somit ist die Fläche von $\triangle OPP_n$ höchstens gleich der Summe der Flächen von $\triangle OPQ$ und $\triangle OP_nQ_n$, also kleiner als $1/4 + 1/4 = 1/2$. Damit haben wir auch hier einen Widerspruch, d.h. $p/q = p_n/q_n$. ∎

Anhang: Das Kreuzprodukt zweier Vektoren

Im $\mathbb{R}^3$ (und nur dort) gibt es eine bilineare Verknüpfung, die zwei Vektoren einen dritten zuordnet, das (vielleicht aus der Schule bekannte) Vektorprodukt oder Kreuzprodukt. Wie schon der Name sagt, ordnet es je zwei Vektoren v und w aus $\mathbb{R}^3$ einen *Vektor* zu, und dieser wird mit $v \times w \in \mathbb{R}^3$ bezeichnet. Er ist festgelegt durch folgende Eigenschaften:

- $v \times w$ hat die Länge $|v \times w| = |v|\,|w|\,|\sin \measuredangle(v,w)|$.
  Insbesondere ist also $v \times w = \vec{0}$, wenn v und w auf einer Geraden liegen, denn dann bilden sie einen Winkel von null oder 180 Grad, so daß der Sinus verschwindet.
- $v \times w$ steht senkrecht sowohl auf v als auch auf w.
  Falls $v \times w \neq \vec{0}$ ist, spannen v und w eine Ebene auf, auf der (da wir im $\mathbb{R}^3$ sind) genau ein eindimensionaler Unterraum senkrecht steht. Darin gibt es allerdings für jede vorgegebene positive Länge zwei Vektoren, die sich durch ihr Vorzeichen unterscheiden. Um $v \times w$ eindeutig festzulegen, brauchen wir daher noch eine weitere Bedingung:
- Die drei Vektoren v, w und $v \times w$ bilden ein Rechtssystem, d.h. wenn sich die Finger der *rechten* Hand so ausrichten lassen, daß der Daumen in Richtung von v zeigt, der Zeigefinger in Richtung von w und der Mittelfinger in Richtung von $v \times w$.

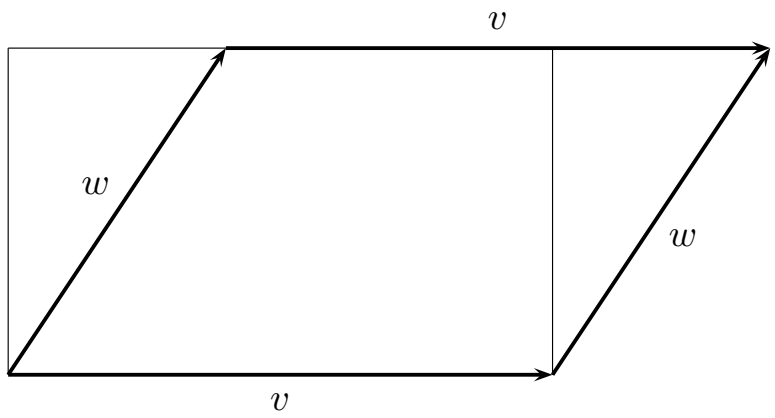
Alternativ kann man ein Rechtssystem auch so definieren, daß sich, ein von v nach w gedrehter Korkenzieher in Richtung $v \times w$ in den Kork bohrt. Ähnlich geht es auch mit Schrauben; da es allerdings neben den (üblichen) Rechtsschrauben auch die (seltenen) Linksschrauben gibt, ist diese Definition eventuell zirkulär: Alles hängt davon ab, wie man Rechtsschrauben definiert.

Aus jeder dieser Regeln folgt sofort die *Antikommutativität* des Vektorprodukts:

$$v \times w = -w \times v\,.$$

Weitere Rechenregeln lassen sich leicht geometrisch ableiten: Da der Sinus eines Winkels gleich Gegenkathete durch Hypothenuse ist, ist in der von v und w aufgespannten Ebenen $|w|\,|\sin \measuredangle(v,w)|$ gleich der Länge

des auf die senkrecht auf v stehenden Geraden projizierten Vektors w, das heißt also gleich der Höhe des in der Abbildung eingezeichneten Rechtecks. Die Länge des Vektors $v \times w$ ist daher gleich dem Flächeninhalt dieses Rechtecks und damit – wie eine Scherung zeigt – gleich der Fläche des von v und w aufgespannten Parallelogramms.



Daraus folgt nun sofort das Distributivgesetz

$$v \times (w + u) = v \times w + v \times u$$

für den zweiten Faktor, und wegen der Antikommutativität folgt daraus wiederum das für den ersten:

$$(u + v) \times w = u \times w + v \times w\,.$$

Um das Vektorprodukt in Koordinaten ausrechnen zu können, müssen wir zunächst die Produkte der Koordinateneinheitsvektoren e_i kennen. Da sie allesamt die Länge eins haben und paarweise aufeinander senkrecht stehen, ist klar, daß das Produkt zweier verschiedener dieser Vektoren bis aufs Vorzeichen gleich dem dritten ist; das Vorzeichen hängt ab von der Orientierung des Koordinatensystems. Das Produkt eines Vektors e_i mit sich selbst ist natürlich, wie jedes Produkt eines Vektors mit sich selbst, gleich dem Nullvektor, denn der eingeschlossene Winkel ist null Grad.

Für die folgende Rechnung wollen wir annehmen, daß e_1, e_2 und e_3 in dieser Reihenfolge ein Rechtssystem bilden; das ist beispielsweise dann der Fall, wenn e_1 nach rechts, e_2 nach vorne und e_3 nach oben zeigt.

Dann folgt sofort, daß

$$e_1 \times e_2 = e_3$$

ist, und nach einigen Fingerübungen auch findet man auch die Formeln

$$e_2 \times e_3 = e_1 \quad \text{und} \quad e_1 \times e_3 = -e_2\,.$$

Die Produkte mit vertauschten Faktoren sind natürlich gerade das negative davon, und $e_i \times e_i = 0$. Für

$$v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \quad \text{und} \quad w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}$$

ist also

$$v \times w = (v_1 e_1 + v_2 e_2 + v_3 e_3) \times (w_1 e_1 + w_2 e_2 + w_3 e_3)\,,$$

nach den obigen Rechenregeln gleich

$$\sum_{i=1}^{3} \sum_{j=1}^{3} v_i w_j \, e_i \times e_j$$

$$= (v_2 w_3 - v_3 w_2) e_1 + (v_3 w_1 - v_1 w_3) e_2 + (v_1 w_2 - v_2 w_1) e_3\,,$$

d.h.

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \times \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \begin{pmatrix} v_2 w_3 - v_3 w_2 \\ v_3 w_1 - v_1 w_3 \\ v_1 w_2 - v_2 w_1 \end{pmatrix}\,.$$

Dies läßt sich dadurch merken, daß man im Schema

$$\begin{array}{ccccccccc} e_1 & & e_2 & & e_3 & & e_1 & & e_2 \\ & \searrow & & \swarrow\!\!\searrow & & \swarrow\!\!\searrow & & \swarrow & \\ v_1 & & v_2 & & v_3 & & v_1 & & v_2 \\ & \swarrow & & \swarrow\!\!\searrow & & \swarrow\!\!\searrow & & \searrow & \\ w_1 & & w_2 & & w_3 & & w_1 & & w_2 \end{array}$$

von e_i ausgeht und als dessen Koeffizient das Zweierprodukt entlang der schrägen Linie nach rechts unten *positiv* und das entlang der schrägen Linie nach links unten *negativ* nimmt; man wendet also die SARRUSsche Regel an auf die „Determinante“

$$\begin{vmatrix} e_1 & e_2 & e_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{vmatrix}\,.$$

§4: Kettenbrüche und Kalender

Schon in den ältesten bekannten Kulturen richtete sich die Zeitrechnung nach astronomischen Gesetzmäßigkeiten: dem Umlauf der Erde um die Sonne, dem Umlauf des Mondes um die Erde sowie der Drehung der Erde um sich selbst.

Der Tag als Zeiteinheit ist ein so selbstverständlicher Teil unseres Lebensrhythmus, daß er als Zeiteinheit nie zur Debatte stand. Ebenso selbstverständlich war, daß als Tag nicht die Dauer einer vollen Drehung der Erde um ihre Achse genommen wurde, sondern der etwa vier Minuten längere Zeitraum, bis sie der Sonne wieder dieselbe Stelle zuwendet.

Als nächstgrößere Einheit führten wahrscheinlich die Babylonier die Woche ein; ob sie sich dabei vom ungefähren Abstand zwischen zwei Mondphasen leiten ließen, ist unbekannt; vielleicht wurde die Dauer von sieben Tagen auch einfach deshalb gewählt, weil die Sieben als heilige Zahl galt.

Definitiv vom Mond abgeleitet ist der Monat. Der Mond dreht sich bekanntlich um die Erde; die Zeit für einen vollständigen Umlauf beträgt ungefähr 27,3 Tage. Dieser sogenannte *siderische* Monat spielt allerdings für die Kalenderrechnung keine Rolle; für die Zeitbestimmung wurden seit Alters her die gut und einfach zu beobachtenden Mondphasen verwendet. Da der Mond nicht selbst leuchtet, sondern das Sonnenlicht reflektiert, hängen diese ab vom Winkelabstand zwischen Sonne und Mond; für den Kalender relevant ist daher der sogenannte *synodische* Monat von 29,53 Tagen, nach dem sich dieser Winkelabstand wiederholt. (Der tatsächliche Abstand zwischen zwei Neumonden ist wegen der komplizierten Mondbewegung keine Konstante; erst im Mittel kommt man auf den synodischen Monat.)

Da 29,53 keine ganze Zahl ist, lassen sich Monate nicht einfach als eine feste Anzahl von Tagen definieren sondern müssen in einem lunaren Kalender mal 29, mal 30 Tage haben.

Einer der einfachsten und zugleich einer der jüngsten dieser Kalender ist der islamische: Sobald mindestens zwei vertrauenswürdige Männer den

neuen Mond gesehen haben, beginnt ein neuer Monat, bei bewölktem Himmel unabhängig davon dreißig Tage nach dem letzten Monatsanfang. Alle zwölf Monate beginnt ein neues Jahr.

Es ist klar, daß bei einer solchen Festlegung die Länge der Monate sowohl innerhalb eines Jahres als auch von Jahr zu Jahr schwankt, außerdem sind die Jahre nicht synchron zum Umlauf der Erde um die Sonne. Da der Kalender auf der arabischen Halbinsel entstand, wo Jahreszeiten keine Rolle spielen und auch die Landwirtschaft das ganze Jahr über konstante Bedingungen vorfindet, ist letzteres dort kein Nachteil.

Für Regionen mit ausgeprägten Jahreszeiten oder jährlich wiederkehrenden Ereignissen ist die Synchronisation des Kalenders mit der Sonne wichtiger als die mit dem Mond. Das wohl älteste Beispiel eines reinen Sonnenjahrs bietet der ägyptische Kalender. Da die für die Landwirtschaft fundamentalen jährlichen Nilüberschwemmungen ungefähr mit der ersten Sichtung des Sterns Sirius übereinstimmten, wurde dieses Ereignis als Beginn des neuen Jahrs genommen. Dies ist das sogenannte *siderische* Jahr mit einer Länge von 365,256 Tagen. Obwohl die Ägypter wußten, daß diese Länge ungefähr $365\frac{1}{4}$ Tage beträgt, legten Sie doch fest, daß jedes Jahr genau 365 Tage haben sollte, verteilt auf zwölf Monate zu jeweils dreißig Tagen sowie fünf Zusatztage.

Ein Jahr, das wirklich synchron zu den Jahreszeiten ist, sollte allerdings nicht anhand des Fixsternhimmels definiert werden, sondern anhand jahreszeitlicher Phänomene wie beispielsweise der Tag- und Nachtgleiche oder dem Durchgang der Sonne durch den Frühlingspunkt. Das ist (im Mittel) das sogenannte *tropische* Jahr mit einer Länge von 356,2422 Tagen. Der Unterschied zum siderischen Jahr ist zwar gering, aber – wie wir gleich sehen werden – trotzdem relevant.

Viel bedeutender als dieser Unterschied war aber zunächst einmal die Tatsache, daß ein Jahr mit exakt 365 Tagen natürlich im Laufe der Jahrhunderte zu einem Verlust der Synchronisation des Kalenders mit den Jahreszeiten führt. Aus diesem Grund beauftragte GAIUS JULIUS CAESAR (100–44) den alexandrinischen Astronomen SOSIGENES mit einer Kalenderreform, die die damit verbundene Verschiebung des Jahresanfang (die sich in nur 120 Jahren auf einen Monat summiert) kompensieren sollte.

Das Ergebnis, der *Julianischer Kalender,* wurde offiziell eingeführt zum 1. Januar des Jahres 709 *ab urbe condita,* d.h. nach Gründung der Stadt Rom. In unserer heutigen Zeitrechnung handelt es sich dabei um das Jahr 45 v.Chr. Die Monatsnamen und -längen des Julianischen Kalenders sind die heute noch gebräuchlichen. Er unterscheidet sich vom klassischen ägyptischen Kalender durch die zusätzliche Regel, daß in jedem vierten Jahr ein Schalttag eingeführt wird, der 29. Februar.

Dabei blieb es bis ins sechzehnte Jahrhundert. Bis dahin hatte das astronomisch etwas zu lange Julianische Jahr zu einer Verschiebung beispielsweise der Frühjahrssonnenwende um rund elf Tage geführt. Um dies zu korrigieren, setzte Papst GREGOR XIII (UGO BONCOMPAGNI, 1502–1585, Papst ab 1572) eine Kommission ein, auf Grund von deren Empfehlungen in den Jahren, die durch hundert aber nicht durch vierhundert teilbar sind, auf den Schalttag verzichtet wird. Dieser *Gregorianische Kalender* trat in den katholischen Ländern am Freitag, dem 15. Oktober 1582 in Kraft; um die bis dahin akkumulierten Fehler des Julianischen Kalenders zu kompensieren, folgte dieser Tag auf den noch Julianischen Donnerstag, den 4. Oktober 1582. In nichtkatholischen Ländern galt der Julianische Kalender noch länger, wurde aber schließlich (mit den verschiedensten Übergangsregeln) überall durch den Gregorianischen ersetzt – zuletzt 1927 in der Türkei.

Um die Neuerung des Gregorianischen Kalenders zu verstehen, betrachten wir die Kettenbruchentwicklung von 365,2422; sie ist

$$[365, 4, 7, 1, 3, 4, 1, 1, 1, 2]$$

und hat die Konvergenten

$$365, \quad 365\frac{1}{4}, \quad 365\frac{7}{29}, \quad 365\frac{8}{33}, \quad 365\frac{31}{128}, \quad 365\frac{132}{545}, \quad \ldots .$$

Der Julianische Kalender verwendet die einfach zu realisierende Konvergente $365\frac{1}{4}$. Unter den folgenden Konvergenten finden wir keine mit einem Nenner, der sich gut für eine einfache Kalenderregel eignen würde. Am ehesten kommt vielleicht noch der Nenner 33 in Frage, da er ungefähr ein Drittel von hundert ist. Arbeitet man mit der Approximation $365\frac{8}{33}$, so sollten unter 33 Jahren acht Schaltjahre sein, also

24 pro 99 Jahre. Nimmt man stattdessen 24 Schaltjahre pro Jahrhundert, was der Regel entspricht, daß durch hundert teilbaren Jahre *keine* Schaltjahre sind, so sorgt der Unterschied zwischen 99 und 100 dafür, daß nach jeweils 400 Jahren eine Vierjahresperiode fehlt. Auch diese hat Anspruch auf ein Schaltjahr, daher die Gregorianische Regel, daß durch hundert teilbare Jahre *keine* Schaltjahre sind, es sei denn, die Jahreszahl sei sogar durch vierhundert teilbar. Innerhalb einer jeden Periode von 400 Jahren gibt es also $100 - 3 = 97$ Schaltjahre; das Gregorianische Jahr hat somit eine Länge von $365\frac{97}{400}$ Tagen, eine praktikable Zahl in der Nähe der Konvergente $365\frac{8}{33}$.

Zum Einstieg in die Kalenderrechnung beginnen wir mit dem einfachsten Problem, den Wochentagen, und überlegen wir uns, auf welchen Wochentag der T-te Tag des M-ten Monats im Jahr J fällt.

Alle Wochen haben exakt sieben Tage und die Jahre haben nach einer recht klaren Regel 365 oder 366 Tage; es ist daher relativ einfach, den Wochentag für den i-ten Tag des Jahres zu berechnen, sofern man ihn für irgendeinen anderen Tag dieses Jahres kennt: Er hängt innerhalb eines Jahres schließlich nur ab von $i \bmod 7$.

Um auch die Abhängigkeit vom Jahr noch zu berücksichtigen, ist es am einfachsten, die Tage nicht vom 1. Januar des jeweils betrachteten Jahres aus zu zählen, sondern ab irgendeinem festen Datum. Historisch sinnvoll wäre hier beispielsweise das Datum der Einführung des Gregorianischen Kalenders; da hier aber Jahr, Monat und Tag „krumme“ Zahlen sind, würde dies zu unnötig komplizierten mathematischen Formeln mit zu vielen willkürlich erscheinenden Konstanten führen.

Für die Mathematik ist es unerheblich, ob zum fiktiven Anfangspunkt bereits der Gregorianische Kalender in Gebrauch war oder nicht; wir können daher beispielsweise ausgehen von einem 1. Januar eines fiktiven Jahres Null. (Die Zählung der Jahre ab Christi Geburt wurde im sechsten Jahrhundert initiiert von DIONYSIUS EXIGUUS, der allerdings ein falsches Geburtsjahr 1 berechnete, auf das wir uns heute noch beziehen. Jahre davor interessierten ihn nicht; der erste der auch Jahre zuvor in Bezug auf Christi Geburt datierte, war wohl der angelsächsische Theologe und Historiker BEDA VENERABILIS (673–735), der – da er keine Null

kannte – das Jahr vor dem Jahr eins *nach* Christus als eins *vor* Christus bezeichnete.)

Wenn wir dem fiktiven 1. Januar 0 die Nummer eins geben und der Einfachheit halber davon ausgehen, daß das Jahr Null *kein* Schaltjahr war, können wir die Nummer des 31. Dezembers des Jahres $J-1$ folgendermaßen berechnen: Bis dahin sind $J-1$ Jahre verflossen, von denen jedes mindestens 365 Tage hatte; damit kommen schon einmal $365(J-1)$ Tage zusammen. Was noch fehlt sind die Schalttage: Im Julianischen Kalender hätte es davon $[(J-1)/4]$ gegeben, im Gregorianischen sind aber die durch 100, nicht aber durch 400 teilbaren Jahre keine Schaltjahre, also müssen wir $[(J-1)/100]-[(J-1)/400]$ subtrahieren. Der i-te Tag des Jahres J hat somit die Nummer

$$365(J-1)+[(J-1)/4]-[(J-1)/100]+[(J-1)/400]+i\,.$$

Um den zugehörigen Wochentag zu finden, müssen wir nun nur noch den Wochentag des Tags Nummer eins bestimmen. Dazu können wir von irgendeinem bekannten Datum ausgehen: Donnerstag, der 10. April 2014 ist der $(31+28+31+10)=100$-te Tag des Jahres 2014, hat also die Nummer

$$365\cdot 2013+503-20+5+100=735\,333\,.$$

Diese Zahl ist kongruent vier modulo sieben; somit war Tag eins ein Montag. Geben wir den Wochentagen, wie es die DIN- und ISO-Normen vorsehen, von Montag ausgehend die Nummern eins bis sieben, so fällt der Tag mit Nummer i also auf den Wochentag mit Nummer $i \bmod 7$, wobei die Null dem normgemäß mit 7 bezeichneten Sonntag entspricht.

Tatsächlich hätten wir die obige Rechnung etwas vereinfachen können: Da $365\equiv 1 \bmod 7$ ist, reicht es, wenn wir

$$(J-1)+[(J-1)/4]-[(J-1)/100]+[(J-1)/400]+i \bmod 7$$

berechnen, im Beispiel also

$$2013+503-20+5+100=2601\equiv 4 \bmod 7\,.$$

Um den Wochentag zu einem vorgegebene Datum bestimmen zu können, müssen wir immer noch berechnen, der wievielte Tag des Jahres

der T-te Tag des M-ten Monats ist. Eine sehr einfache Methode besteht darin, daß wir zählen, wie viele Tage vor dem Ersten des jeweiligen Monats bereits vergangen sind. Dabei müssen wir natürlich zwischen Schaltjahren und gewöhnlichen Jahren unterscheiden: Für letztere seien dies t_M Tage, für erste s_M. Dann haben wir folgende Tabelle:

M =	1	2	3	4	5	6	7	8	9	10	11	12
t_M =	0	31	59	90	120	151	181	212	243	273	304	334
s_M =	0	31	60	91	121	152	182	213	244	274	305	335

Dann fällt der T-te Tag des M-ten Monats des Jahrs J auf den Wochentag mit der Nummer

$$(J-1) + [(J-1)/4] - [(J-1)/100] + [(J-1)/400] + t_M + T$$

modulo sieben, falls J kein Schaltjahr ist; andernfalls muß t_M durch s_M ersetzt werden. Es genügt natürlich, die Zahlen t_M oder s_M modulo 7 einzusetzen, also

M =	1	2	3	4	5	6	7	8	9	10	11	12
t_M mod 7 =	0	3	3	6	1	4	6	2	5	0	3	5
s_M mod 7 =	1	4	4	0	2	5	0	3	6	1	4	6

Da wohl niemand eine dieser beiden Tabellen auswendig lernen möchte, stellt sich die Frage, ob es vielleicht auch eine geschlossene Formel gibt. Dazu ignorieren wir zunächst einmal die historisch überkommenen Monatslängen und tun so, als könnte ein Mathematiker am grünen Tisch festlegen, wie er 365 Tage auf zwölf Monate verteilt.

Für ihn wäre die am wenigsten irreguläre Verteilung der Monatslängen wohl die, bei der Tag i eines Jahres mit N Tagen genau dann im k-ten Monat liegt, wenn gilt

$$\frac{(k-1)N}{12} < i \le \frac{kN}{12} \quad \text{oder} \quad k - 1 < \frac{12i}{N} \le k\,,$$

d.h. k ist die kleinste ganze Zahl größer oder gleich $12i/N$. Für ein Jahr mit N = 365 Tagen würde dies auf die Monatslängen

$$30, 30, 31, 30, 31, 30, 30, 31, 30, 31, 30, 31$$

führen, in einem Schaltjahr mit $N = 366$ hätten alle ungeraden Monate dreißig und alle geraden Monate 31 Tage. Ein Februar mit 28 oder 29 Tagen kann bei einer derartigen Strategie natürlich nie vorkommen.

Trotzdem läßt sich auch unser chaotisches Monatssystem fast auf eine solche Formel bringen: Nehmen wir an, wir hätten ein Jahr mit 367 Tagen und zwölf Monaten. Dann liefert uns die obige Vorgehensweise Monate der Längen

$$30, 31, 30, 31, 30, 31, 31, 30, 31, 30, 31, 31\,,$$

wir haben also wie im wirklichen Kalender an zwei Stellen aufeinanderfolgende Monate mit 31 Tagen. Im Kalender sind dies Juli/August und Dezember/Januar, hier sind es die Monate 6 und 7 sowie 11 und 12. Wenn wir zyklisch um eine Position verschieben, so daß die hintere 31 an der ersten Stelle steht, stimmen die beiden Positionen überein, und abgesehen vom Februar, der hier dreißig Tage hat, haben wir genau die Folge der Monatslängen.

(Kurioserweise gab es 1712 in Schweden sogar ein Jahr mit 367 Tagen und einem 30. Februar: 1699 wurde beschlossen, langsam zum Gregorianischen Kalender überzugehen und dazu als erstes den Schalttag 1700 zu streichen. Danach wurde der Beschluß aufgegeben, und um wieder synchron zum Julianischen Kalender zu werden, gab es 1712 einen 30. Februar als zweiten Schalttag. 1753 wurde der Gregorianische Kalender dann endgültig und abrupt eingeführt.)

Die Anzahl der Tage vor dem Ersten des M-ten Monats wäre in unserem hypothetischen Kalender einfach gleich $[367M/12]$; durch die zyklische Verschiebung wird diese Formel freilich zerstört. Sie kann aber gerettet werden durch eine Verschiebung im Zähler: Wie explizites Nachrechnen zeigt, sind in einem Jahr mit 367 Tagen, in dem der Februar dreißig Tage hat, vor dem Ersten des M-ten Monats gleich $[(367M - 362)/12]$ Tage vergangen. Somit ist für unseren realen Kalender

$$t_M = \begin{cases} \left[\frac{367M-362}{12}\right] & \text{für } M \le 2 \\ \left[\frac{367M-362}{12}\right] - 2 & \text{für } M \ge 3 \end{cases} \quad \text{und}$$

$$s_M = \begin{cases} \left[\frac{367M-362}{12}\right] & \text{für } M \le 2 \\ \left[\frac{367M-362}{12}\right] - 1 & \text{für } M \ge 3 \end{cases} .$$

Der Wochentag des T-ten Tags im M-ten Monat des Jahrs J ist somit

$$(J-1)+\left[\frac{J-1}{4}\right]-\left[\frac{J-1}{100}\right]+\left[\frac{J-1}{400}\right]+\left[\frac{367M-362}{12}\right]+\delta_M+T$$

modulo sieben mit

$$\delta_M=\begin{cases}0 & \text{falls } M\le 2\\ -1 & \text{falls } M\ge 3 \text{ und } J \text{ Schaltjahr}\\ -2 & \text{falls } M\ge 3 \text{ und } J \text{ kein Schaltjahr}\end{cases}.$$

Diese Formel gilt selbstverständlich nur für Daten nach dem Gregorianischen Kalender; bei älteren Daten muß man zunächst wissen, auf welchem Kalender und welchem Jahresanfang sie beruhen.

Als beispielsweise der amerikanische Naturwissenschaftler, Philosoph und Politiker BENJAMIN FRANKLIN geboren wurde, zeigten die Kalender in seiner Heimatstadt Boston den 6. Januar 1705. Massachusetts war zu der Zeit noch britische Kolonie, und da Großbritannien den Gregorianischen Kalender erst 1752 einführte, ist das ein Julianisches Datum. Gregorianisch ist sein Geburtstag elf Tage später, d.h. am 17. Januar. Allerdings handelt es sich dabei nicht um den 17. Januar 1705, sondern um den des Jahres 1706: In Großbritannien begann das neue Jahr damals nämlich nicht am ersten Januar, sondern am 25. März. Auf den 31. Dezember 1705 folgte also der 1. Januar 1705 und auf den 24. März 1705 der 25. März 1706. Solche Besonderheiten bei der Interpretation alter Datumsangaben gibt es viele; hier ist also Vorsicht geboten.

Mindestens genauso wichtig wie eine verbesserte Schaltjahrregel war für Papst Gregor das Datum des Osterfests; auch darum sollte sich seine Kommission kümmern. Damit kam nun plötzlich auch der Mond in den Kalender, denn 325 beschloß das Konzil von Nicäa (bei Konstantinopel), daß Ostern stets am ersten Sonntag nach dem ersten Vollmond am oder nach der Frühlings-Tag-und-Nacht-Gleiche zu feiern sei. (Man beachte, daß das erste *nach* im Sinne eines $>$, das zweite im Sinne eines $\ge$ definiert ist. Der Grund für das $>$ lag darin, daß so Ostern nur sehr selten gleichzeitig mit dem jüdischen Pascha-Fest begangen wird.)

Der erste Vollmond am oder nach der Frühlings-Tag-und-Nacht-Gleiche kann nicht einfach nach einer ähnlichen Regel wie der Monatsanfang im islamischen Kalender bestimmt werden, also etwa dann, wenn ihn

mindestens zwei vertrauenswürdige Kardinäle gesehen haben, denn der österliche Festkreis beginnt bereits siebzig Tage vor Ostern. Das Datum mußte daher im Voraus berechnet werden. Der Mathematiker und Informatiker DONALD E. KNUTH sagt in Abschnitt 1.3.2, Aufgabe 14 seiner *Art of Computer Programming: There are many indications that the sole important application of arithmetic in Europe during the Middle Ages was the calculation of the Easter date, and so such algorithms are historically significant.* So ordnete etwa KARL DER GROSSE (747/8–814) bei seiner Neuordnung des Bildungssystems mehrfach an, daß in jeder Diözese mindestens ein Geistlicher in der Lage sein müsse, das Osterdatum zuverlässig zu berechnen. Schauen wir uns also an, wie Papst Gregor das Osterdatum berechnen ließ.

Wir brauchen Informationen über die Wochentage, über die Mondphasen und über die Tag-Nacht-Gleiche im Frühling. Letztere ist, da der Gregorianische Kalender das tropische Jahr recht genau approximiert, noch recht lange konstant am 21. März jedes Jahres; bei der bei der Berechnung des Osterdatums geht man daher stets von diesem Tag aus. Wie man Wochentage bestimmt, haben wir uns gerade überlegt; bleibt also noch das Problem mit den Mondphasen.

Die mittlere Zeitspanne zwischen zwei Neumonden, die synodische Umlaufzeit des Mondes, beträgt etwa 29,5306 Tage; ein tropisches Jahr mit seinen 365,2422 Tagen besteht also aus

$$365{,}2422 : 29{,}5306 \approx 12{,}3679$$

solchen Zykeln. Die Kettenbruchentwicklung dieses Quotienten ist

$$[12, 2, 1, 2, 1, 1, 4, 1, 81]$$

mit Konvergenten

$$12, \quad 12\frac{1}{3}, \quad 12\frac{3}{8}, \quad 12\frac{4}{11}, \quad 12\frac{7}{19}, \quad 12\frac{32}{87}, \quad 12\frac{39}{106}, \quad \ldots .$$

Für einen Kalender, der sowohl mit der Sonne als auch mit dem Mond synchronisiert ist, könnte man also Jahre mit 12 und 13 Monaten kombinieren, wobei in erster Näherung jedes dritte Jahr 13 Monate hätte. Tatsächlich war man im fünften vorchristlichen Jahrhundert bereits erheblich weiter: Der um 440 v.Chr. lebende Athener Mathematiker und

Astronomen METON verwendete die Konvergente mit Nenner 19. Ein Metonischer Zyklus besteht besteht demnach aus 19 Jahren, darunter zwölf *Gemeinjahren* aus zwölf Monaten und sieben *Schaltjahren* aus 13 Monaten. Die Monate hatten teils 29, teils 30 Tage. Der darauf basierende Kalender wurde in Griechenland bis 46 v.Chr. verwendet. Die Synchronisation zwischen Sonnen- und Mondzykeln ist fast perfekt:

$$19 \cdot 365{,}2422 = 6939{,}6018 \quad \text{und} \quad 235 \cdot 29{,}5306 = 6939{,}691\,,$$

der Fehler pro Zyklus liegt also bei nur etwa zwei Stunden. Seit Einführung des Gregorianischen Kalenders sind etwas über 22 Metonische Zykeln vergangen; der akkumulierte Fehler liegt also noch unter zwei Tagen.

Der Gregorianische Kalender geht deshalb bei der Bestimmung des Osterdatums nicht von astronomischen Beobachtungen aus, sondern von Metonischen Zykeln, allerdings mit einer Korrektur für den akkumulierten Fehler. Ebenfalls unberücksichtigt bleiben die Irregularitäten der realen Mondbewegung; gerechnet wird mit einer Approximation der *mittleren* Mondbewegung. Auf den ersten Blick seltsam erscheinen mag auch die Tatsache, daß bei der Fehlerkorrektur mit der *Julianischen* Jahreslänge von $365\frac{1}{4}$ Tagen gerechnet wird; der Grund lag wohl vor allem darin, daß Papst Gregor bisherige Praktiken nicht mehr als unbedingt notwendig ändern wollte.

Die wesentliche Größe, mit der die Mondphasen in unseren an der Sonne orientierten Kalender gebracht werden, ist der sogenannte *Epakt*. Mit diesem Wort bezeichneten die Griechen die Anzahl der Tage, die an Neujahr seit dem letzten Neumond des alten Jahres vergangen waren. Gemäß dem Metonischen Zyklus sollte diese Zahl sich alle 19 Jahre wiederholen; in der Kalenderrechnung wird daher die um eins vermehrte Restklasse modulo 19 der Jahreszahl als die „Goldene Zahl“ bezeichnet. (Die Addition der Eins kommt natürlich daher, daß zur Zeit ihrer Einführung die Null in der europäischen Mathematik noch nicht vorkam.)

Wenn jedes Jahr genau 365 Tage hätte, könnten wir einfach mit den $12 \times 29{,}5 = 354$ Tagen eines Mondjahrs vergleichen und wüßten dann,

daß sich die Mondphase an einem festen Datum jedes Jahr um elf Tage verschiebt. Als *Mondphase* bezeichnen wir dabei die Anzahl von Tagen, die seit dem letzten Neumond vergangen sind.

Eine der vielen Vereinfachungen in der Berechnung des Osterdatums liegt darin, daß man innerhalb des aktuellen Metonischen Zyklus im wesentlichen von dieser Formel ausgeht, die Schalttage also ignoriert.

Da die Schalttage Ende Februar eingeführt werden, wir uns aber für den Vollmond am oder nach dem 21. März interessieren, sollten wir nicht mit dem klassischen Epakt, der Mondphase des 1. Januar, rechnen: Sonst gäbe es schließlich algorithmisch unangenehme Fallunterscheidungen für die Schaltjahre. Aus Effizienzgründen bietet sich an, stattdessen mit einem *verschobenen* Epakt zu rechnen, d.h. mit der Mondphase eines geeigneten Datums, das näher bei Ostern liegt.

Die Länge eines lunaren Zyklus liegt bei ungefähr 29,5 Tagen; zum einfacheren Rechnen sollten wir das zumindest für den einen Zyklus, in den Ostern fällt, auf den ganzzahligen Wert 30 runden. Der erste Vollmond nach dem 21. März ist dann der letzte Vollmond vor dem 19. April, und sein Abstand zum 19. April ist, wenn wir den Vollmond als Tag mit Mondphase 14 betrachten, gleich dem Abstand des letzten Neumonds vor dem 5. April zum 5. April, also die Mondphase des 5. Aprils. Somit bietet sich an, als verschobenen Epakt die Mondphase des 5. Aprils zu nehmen. Gemäß unserer vereinfachenden Annahmen sollte auch sie sich alle 19 Jahre wiederholen und sollte sich zumindest innerhalb eines Metonischen Zyklus von Jahr zu Jahr modulo 30 um elf verschieben.

Damit brauchen wir nur noch für ein Jahr des Metonischen Zyklus den tatsächlichen Wert der Mondphase des fünften Aprils kennen, um den verschobenen Epakt allgemein berechnen zu können. Die vor der Gregorianischen Reform gebräuchliche Formel berechnet ihn für das Jahr J als

$$E = \big(14 + 11 \cdot (J \bmod 19)\big) \bmod 30\,.$$

Der erste Vollmond am oder nach dem 21. März lag somit E Tage vor dem 19. April, und Ostern war der (echt) darauf folgende Sonntag. So

wird Ostern noch heute in fast allen orthodoxen Kirchen berechnet; die einzige Ausnahme ist die finnische.

Der Gregorianische Kalender modifiziert diese Formel durch drei zusätzliche Terme: Zunächst berücksichtigt er, daß der Metonische Zyklus nicht wirklich exakt ist, insbesondere dann nicht, wenn man mit dem Julianischen Jahr arbeitet:

$$19 \cdot 365{,}25 = 6939{,}750 \quad \text{und} \quad 235 \cdot 29{,}5306 = 6939{,}691\,;$$

hier beträgt die Differenz also 0,059 Tage pro Zyklus und

$$0{,}059 \times \frac{100}{19} \approx 0{,}31$$

Tage pro Jahrhundert. Die Gregorianische Osterformel approximiert dies durch $8/25 = 0{,}32$, addiert allerdings im h-ten Jahrhundert nicht $[8h/25]$, sondern $\left[(5+8h)/25\right]$. Diese Modifikation soll in erster Linie dafür sorgen, daß Ostern möglichst selten mit dem jüdischen Paschafest zusammenfällt. Für das Jahrhundert wird dabei die gleiche Konvention benutzt wie für die Feier des Jahrtausendanfangs am 1. Januar 2000: Das h-te Jahrhundert beginnt mit dem Jahr $100(h-1)$, d.h. $h = [J/100] + 1$.

Da der Gregorianische Kalender bei der Korrektur der Metonischen Zyklen mit Julianischen Jahren arbeitet, am Ende aber ein Gregorianisches Datum braucht, müssen als nächstes die unterschiedlichen Anzahlen von Schalttagen berücksichtigt werden, d.h. die „ausfallenden“ Schalttage des Gregorianischen Kalenders müssen subtrahiert werden. Das sind drei Stück pro 400 Jahre, also wird $[3h/4]$ subtrahiert. Dies ergäbe die neue Formel

$$E = \left(14 + 11 \cdot (J \bmod 19) + \left[\frac{5+8h}{25}\right] - \left[\frac{3h}{4}\right]\right) \bmod 30\,.$$

Tatsächlich gibt es noch eine weitere Modifikation, die dafür sorgen soll, daß die 19 Epakte eines Metonischen Zyklus alle verschieden sind und $E = 0$ nicht auftritt: Falls $E = 0$ ist oder falls $E = 1$ ist und $J \bmod 19 > 10$, wird E um eins erhöht. Der (berechnete) Vollmond ist dann E Tage vor dem 19. April, und Ostern wird weiterhin am darauf folgenden Sonntag gefeiert.

Das Jahr $J = 2014$ liegt im $h = 21$. Jahrhundert und $2014 \equiv 0 \bmod 19$. Somit ist

$$E = \left(14 + 11 \cdot 0 + \left[\frac{173}{25}\right] - \left[\frac{63}{4}\right]\right) \bmod 30 = 5$$

Der rechnerische Vollmond ist daher am 14. April. (Der tatsächliche ist erst am 15. April um 9 Uhr 42.) Der darauf folgende Sonntag ist der 20. April 2014, also wird dann Ostern gefeiert.

§5: Eine kryptographische Anwendung

Beim RSA-Verfahren wählt man den öffentlichen Exponenten e oft ziemlich klein, z.B. $e = 3$ oder $e = 2^{16} + 1$. Dies hat den Vorteil, daß zumindest die Verschlüsselung ziemlich schnell geht und man nur zur Entschlüsselung mit einem Exponenten in der Größenordnung des Moduls arbeiten muß.

Für jemanden, der RSA hauptsächlich für elektronische Unterschriften verwendet, würde sich anbieten, stattdessen den privaten Exponenten d relativ klein zu wählen. Dann könnte er schnell viele Dokumente unterschreiben, und falls jeder Empfänger nur eines davon bekommt, fällt dessen höherer Aufwand bei der Überprüfung nicht so sehr ins Gewicht.

Natürlich kann man nicht $d = 3$ oder $d = 2^{16} + 1$ wählen: Der private Exponent muß schließlich geheim sein und es darf nicht möglich sein, ihn durch Probieren zu erraten.

Andererseits geht man heute bei symmetrischen Kryptoverfahren davon aus, daß ein Verfahren sicher ist, falls ein Gegner mindestens 2^{128} Möglichkeiten durchprobieren muß, so daß gängige Verfahren wie AES mit einer Schlüssellänge von 128 Bit auskommen. Verglichen damit erscheinen 2048 Bit für einen privaten Entschlüsselungsexponenten recht hoch.

Trotzdem läßt sich hier nicht wesentlich sparen, denn ein Gegner kann kurze private Exponenten nicht nur durch Ausprobieren bestimmen, sondern auch wesentlich schneller nach dem Kettenbruchalgorithmus.

Wir gehen aus von einem öffentlichen RSA-Schlüssel (N, e) sowie dem zugehörigen privaten Exponenten d. Dann gibt es bekanntlich eine natürliche Zahl k, so daß $ed - k\varphi(N) = 1$ ist. Dies können wir umschreiben als

$$\frac{e}{\varphi(N)} - \frac{k}{d} = \frac{1}{d\varphi(N)} .$$

Falls d sehr viel kleiner ist als $\varphi(N)$ haben wir hier einen Bruch mit dem großen Nenner $\varphi(N)$ sehr gut angenähert durch einen Bruch mit dem sehr viel kleineren Nenner d. Für hinreichend kleines d ist das nur möglich, wenn k/d eine Konvergente der Kettenbruchentwicklung von $e/\varphi(N)$ ist.

Das mag zunächst harmlos erscheinen, denn die Sicherheit von RSA beruht ja gerade darauf, daß niemand außer dem Inhaber des privaten Schlüssels d die Faktorisierung $N = pq$ und damit den Wert von

$$\varphi(N) = (p-1)(q-1) = N - (p+q) + 1$$

kennt. Dafür kennt aber jeder den Wert von N, und wie die obige Gleichung zeigt, liegt der recht nahe bei $\varphi(N)$: Die Primzahlen p und q sind schließlich nur von der Größenordnung $\sqrt{N}$. Damit sollte k/d auch eine gute Approximation für e/N liefern.

In der Tat zeigte Kryptologe MICHAEL JAMES WIENER 1990 ein Resultat, wonach insbesondere der folgende Satz gilt:

Satz: Ist $N = pq$ Produkt zweier Primzahlen p und q mit $p < q < 2q$, und ist $d < \frac{1}{3}\sqrt[4]{N}$ der private Exponent zum öffentlichen Exponenten $e < \varphi(N)$, so ist d Nenner einer Konvergenten der Kettenbruchentwicklung von e/N.

Beweis: Wegen $ed \equiv 1 \bmod \varphi(N)$ gibt es ein $k \in \mathbb{N}$; so daß $ed - k\varphi(N) = 1$ ist; wegen $e < \varphi(N)$ ist dabei $k < d$. Nach dem Satz von LEGENDRE aus §3 reicht es, wenn wir zeigen können, daß

$$\left| \frac{e}{N} - \frac{k}{d} \right| < \frac{1}{2d^2}$$

ist, denn dann ist k/d eine Konvergente der Kettenbruchentwicklung von e/N.

$$\begin{aligned}\left|\frac{e}{N}-\frac{k}{d}\right| &= \left|\frac{ed-kN}{dN}\right| \\ &= \left|\frac{\big(ed-k\varphi(N)\big)+k\varphi(N)-kN}{dN}\right| \\ &= \left|\frac{1+k\big(\varphi(N)-N\big)}{dN}\right| \\ &= \left|\frac{1+k(1-p-q)}{dN}\right| = \frac{k(p+q)-(k+1)}{dN} \\ &< \frac{k(p+q)}{dN}\,.\end{aligned}$$

Natürlich ist $p < \sqrt{N}$, und wegen der Voraussetzung $q < 2p$ folgt $p+q < 3\sqrt{N}$. Außerdem ist $k < d < \frac{1}{3}\sqrt[4]{N}$, also

$$\left|\frac{e}{N}-\frac{k}{d}\right| < \frac{3k\sqrt{N}}{dN} = \frac{3k}{d\sqrt{N}} < \frac{\sqrt[4]{N}}{\sqrt{N}} = \frac{1}{\sqrt[4]{N}}\,.$$

Dies ist genau dann kleiner als $1/2d^2$, wenn $d < \frac{1}{2}\sqrt[4]{N}$ ist. Nach Voraussetzung ist aber d sogar kleiner als $\frac{1}{3}\sqrt[4]{N}$, womit der Satz bewiesen wäre. ∎

Um d zu berechnen, müssen wir daher nur so lange Konvergenten p_n/q_n bestimmen, bis für einen der Nenner q_n die Exponentiation mit q_n modulo N invers ist zu der mit e. Falsche Kandidaten sollten dabei praktisch immer bereits beim ersten Versuch erkannt werden.

Tatsächlich gibt es Algorithmen, mit denen man sogar private Exponenten $d < N^{0{,}289}$ rekonstruieren kann, und manche Fachleute meinen, daß man vielleicht sogar in vielen Fällen mit $d < \sqrt{N}$ mit geeigneten Algorithmen eine realistische Erfolgschance haben könnte; bei diesen Attacken arbeitet man allerdings nicht mit Kettenbrüchen, sondern mit anderen Verfahren zur diophantischen Approximation.

Private Exponenten müssen somit immer groß sein. Falls man von einem vorgegebenen öffentlichen Exponenten ausgeht, ist das für realistische N mit an Sicherheit grenzender Wahrscheinlichkeit erfüllt; Vorsicht ist nur geboten, wenn man mit dem privaten Exponenten startet. Daher verlangen auch die Vorschriften der Bundesnetzagentur, daß man immer vom öffentlichen Exponenten e ausgehen muß, und erst daraus einen privaten Exponenten berechnet.

§6: Die Kettenbruchentwicklung der Eulerschen Zahl

Aufgabe 1*b)* des neunten Übungsblatts läßt eine erstaunliche Regelmäßigkeit in der Kettenbruchentwicklung von e vermuten:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1 \cdots] .$$

Diese Entwicklung ist bereits im 18. Kapitel der 1748 erschienenen *Introductio in analysin infinitorium* von EULER enthalten; HERMITE bewies sie 1873 im Rahmen seiner Arbeit über die Transzendenz von e mit anderen Methoden die zusammenhängen mit der Approximation der Exponentialfunktion durch rationale Funktionen. Sein Schüler PADÉ entwickelte später eine systematische Theorie solcher Approximationen, die PADÉ-Approximanten, die in der Numerik eine große Rolle spielen für die näherungsweise Berechnung von Standardfunktionen. Durch Kombination solcher Ideen kamen verschiedene Mathematiker zu immer einfacheren Beweisen; der hier wiedergegebene Beweis von HENRY COHN erschien 2006 im *American Mathematical Monthly;* direkt dahinter folgt eine Arbeit von THOMAS J. OSLER, der den Beweis so verallgemeinert, daß er auch die Kettenbruchentwicklungen der Wurzeln aus e liefert.

Wir können die obige Kettenbruchentwicklung noch etwas regelmäßiger schreiben, indem wir beachten, daß für alle $x \in \mathbb{R}$ gilt

$$1 + \cfrac{1}{0 + \cfrac{1}{1 + x}} = 1 + (1 + x) = 2 + x \, ;$$

der obige Kettenbruch kann also auch geschrieben werden als

$$[1, 0, 1, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \ldots] .$$

Hier läßt sich der n-te Koeffizient c_i völlig regelmäßig durch n ausdrücken: Für $n = 3k + 1$ mit $k \in \mathbb{N}_0$ ist er $2k$, ansonsten eins.

Für die Kettenbruchentwicklung der M-ten Wurzel aus e müssen wir daran nur wenig ändern: Hier wollen wir sehen, daß

$$c_{3k} = c_{3k+2} = 1 \quad \text{und} \quad c_{3k+1} = (2k+1)M - 1$$

ist für alle $k \in \mathbb{N}_0$, d.h.

$$\sqrt[M]{e} = [1, M-1, 1, 1, 3M-1, 1, 1, 5M-1, 1, 1, 7M-1, 1, \ldots] .$$

Wir gehen aus von diesem Kettenbruch und wollen zeigen, daß er gegen $\sqrt[M]{e}$ konvergiert. Nach dem Satz am Ende von §2 lassen sich der Zähler p_n und der Nenner q_n der n-ten Konvergente eines Kettenbruchs $[c_0, c_1, c_2, \ldots]$ rekursiv berechnen nach den Formeln

$$p_0 = c_0, q_0 = 1, p_1 = c_0c_1 + 1, q_1 = c_1,$$
$$p_n = p_{n-2} + c_n p_{n-1} \quad \text{und} \quad q_n = q_{n-2} + c_n q_{n-1} \quad \text{für } n \geq 2 .$$

Speziell für die hier betrachtete Kettenbruchentwicklung haben wir also die Anfangsterme $p_0 = q_0 = p_1 = 1$ und $q_1 = M - 1$, was insbesondere bedeutet, daß die erste Konvergente im Falle $M = 1$, bei der Kettenbruchentwicklung von e also, nicht definiert ist. Weiter geht es nach obiger Rekursionsformel; da die c_n von n mod 3 abhängen, bekommen wir je nach Restklasse von n drei verschiedene Formeln:

$$\begin{aligned} p_{3k} &= p_{3k-2} + p_{3k-1} & q_{3k} &= q_{3k-2} + q_{3k-1} \\ p_{3k+1} &= p_{3k-1} + \big((2k+1) - 1\big)Mp_{3k} & q_{3k+1} &= q_{3k-1} + \big((2k+1)M - 1\big)q_{3k} \\ p_{3k+2} &= p_{3k} + p_{3k+1} & q_{3k+2} &= q_{3k} + q_{3k+1} \end{aligned}$$

Wir müssen zeigen, daß die Folge der Quotienten p_n/q_n gegen $\sqrt[N]{e}$ konvergiert.

Der Trick dazu hängt mit PADÉ-Approximanten zusammen; ich möchte darauf nicht eingehen, sondern ohne Begründung einfach die drei Integrale

$$A_k = \int_0^1 \frac{x^k(x-1)^k}{k!M^{k+1}} e^{x/M}\, dx, \quad B_k = \int_0^1 \frac{x^{k+1}(x-1)^k}{k!M^{k+1}} e^{x/M}\, dx$$

$$\text{und} \qquad C_k = \int_0^1 \frac{x^k (x-1)^{k+1}}{k! M^{k+1}} e^{x/M}\, dx$$

betrachten.

Satz: Für alle $k \in \mathbb{N}_0$ gilt:

$$p_{3k} - q_{3k} \sqrt[M]{e} = -A_k$$
$$p_{3k+1} - q_{3k+1} \sqrt[M]{e} = B_k$$
$$p_{3k+2} - q_{3k+2} \sqrt[M]{e} = C_k$$

Da in allen drei Integranden der Zähler kleiner als eins und die Exponentialfunktion höchstens $\sqrt[M]{e}$ ist, während der Nenner für $k \to \infty$ gegen ∞ geht, ist

$$\lim_{k\to\infty} A_k = \lim_{k\to\infty} B_k = \lim_{k\to\infty} C_k = 0\,;$$

daher folgt aus diesem Satz sofort

Korollar: $\lim\limits_{n\to\infty} \dfrac{p_n}{q_n} = \sqrt[M]{e}$, d.h.

$$\sqrt[M]{e} = [1, M-1, 1, 1, 3M-1, 1, 1, 5M-1, 1, 1, 7M-1, 1, \dots]\,.$$

Insbesondere ist $e = [1, 0, 1, 1, 2, 1, 1, 4, 1, \dots] = [2, 1, 2, 1, 1, 4, 1, \dots]$.

■

Der obige Satz wird durch Induktion bewiesen. Für $k = 0$ ist

$$A_0 = \int_0^1 \frac{1}{M} e^{x/M}\, dx = e^{x/M}\Big|_0^1 = \sqrt[M]{e} - 1$$

$$B_0 = \int_0^1 \frac{x}{M} e^{x/M}\, dx = (x-M)e^{x/M}\Big|_0^1 = (1-M)\sqrt[M]{e} + M$$

$$C_0 = \int_0^1 \frac{x-1}{M} e^{x/M}\, dx = (x-1-M)e^{x/M}\Big|_0^1 = -M\sqrt[M]{e} + M + 1$$

Nach den eingangs angegebenen Rekursionsformeln für die p_n und q_n ist

$$p_0 = q_0 = 1, \quad p_1 = M, \quad q_1 = M - 1, \quad p_2 = 1 + M \quad \text{und} \quad q_2 = M\,.$$

Die drei Formeln aus dem Satz werden also für $k = 0$ zu den Gleichungen

$$1 - \sqrt[M]{e} = 1 - \sqrt[M]{e}$$
$$M - (M-1)\sqrt[M]{e} = (1-M)\sqrt[M]{e} + M$$
$$1 + M - M\sqrt[M]{e} = -M\sqrt[M]{e} + M + 1\,,$$

die offensichtlich alle drei richtig sind.

Für den Induktionsschritt brauchen wir Beziehungen zwischen den Integralen A_k, B_k und C_k. Hier gilt für alle $k \in \mathbb{N}$

a) $A_k = -B_{k-1} - C_{k-1}$
b) $B_k = -\big((2k+1)M - 1\big)A_k + C_{k-1}$
c) $C_k = B_k - A_k$

Zum *Beweis* von *a)* wenden wir die LEIBNIZ-Regel zur Ableitung eines Produkts an auf das Produkt der drei Faktoren x^k, $(x-1)^k$ und $e^{x/M}$. Für ein solches Dreierprodukt ist $(uvw)' = u'vw + uv'w + uvw'$, also ist

$$\frac{d}{dx}x^k(x-1)^k e^{x/M}$$
$$= kx^{k-1}(x-1)^k e^{x/M} + kx^k(x-1)^{k-1}e^{x/M} + \frac{x^k(x-1)^k}{M}e^{x/M}\,.$$

Division durch $k!M^k$ macht daraus

$$\frac{d}{dx}\,\frac{x^k(x-1)^k}{k!M^k}e^{x/M}$$
$$= \frac{x^{k-1}(x-1)^k e^{x/M}}{(k-1)!M^k} + \frac{x^k(x-1)^{k-1}}{(k-1)!M^k}e^{x/M} + \frac{x^k(x-1)^k}{k!M^{k+1}}e^{x/M}\,.$$

Integrieren wir beide Seiten von 0 bis 1, so erhalten wir auf der linken Seite den Wert null, da die Stammfunktion des Integranden an beiden Intervallenden verschwindet. Rechts erhalten wir die Summe der Integrale C_{k-1}, B_{k-1} und A_k; somit ist $A_k + B_{k-1} + C_{k-1} = 0$, was *a)* beweist.

Der Beweis von *b)* geht ähnlich: Wir berechnen zunächst die Ableitung von $x^k(x-1)^{k+1}e^{x/M}$ und dividieren wieder durch $k!M^k$; wir erhalten

$$\frac{d}{dx}\frac{x^k(x-1)^{k+1}}{k!M^k}e^{x/M}$$

$$= \frac{x^{k-1}(x-1)^{k+1}}{(k-1)!M^k}e^{x/M} + \frac{(k+1)x^k(x-1)^k}{k!M^k}e^{x/M} + \frac{x^k(x-1)^{k+1}}{k!M^{k+1}}e^{x/M}$$

$$= \frac{kMx^{k-1}(x-1)^{k+1} + M(k+1)x^k(x-1)^k + x^k(x-1)^{k+1}}{k!M^{k+1}}e^{x/M}$$

$$= \frac{x^{k-1}(x-1)^k\big(kM(x-1) + (k+1)Mx + x(x-1)\big)}{k!M^{k+1}}e^{x/M}$$

$$= \frac{x^{k-1}(x-1)^k\Big(\big((2k+1)M-1\big)x - kM + x^2\Big)}{k!M^{k+1}}e^{x/M}$$

$$= \big((2k+1)M-1\big)\frac{x^k(x-1)^k}{k!M^{k+1}}e^{x/M} - \frac{x^{k-1}(x-1)^k}{(k-1)!M^k}e^{x/M}$$

$$+ \frac{x^{k+1}(x-1)^k}{k!M^{k+1}}e^{x/M}\,.$$

Wenn wir die linke Seite dieser Gleichung von 0 bis 1 integrieren, erhalten wir wieder den Wert null, bei der rechten erhalten wir

$$\big((2k+1)M-1\big)A_{k-1} - B_k + C_{k-1}\,.$$

Auflösen nach B_k zeigt die Behauptung *b)*

Zum Beweis von *c)* schließlich gehen wir aus von der Gleichung $(x-1)^2 = x(x-1) - (x-1)$ und multiplizieren diese mit

$$\frac{x^k(x-1)^{k-1}}{k!M^{k+1}}e^{x/M}\,.$$

Integration von 0 bis 1 führt auf die Gleichung $C_k = B_k - A_k$.

Damit sind alle drei Relationen bewiesen, und wir können mit dem Induktionsschritt zum Beweis unseres zentralen Satzes beginnen. Sei also $k \geq 1$; wir nehmen an, daß die drei Gleichungen für $k-1$ gelten.

Als erstes wollen wir zeigen, daß

$$p_{3k} - q_{3k}\sqrt[M]{e} = -A_k$$

ist. Nach den Rekursionsformeln für Zähler und Nenner der Konvergenten ist

$$p_{3k} = p_{3k-2} + p_{3k-1} \quad \text{und} \quad q_{3k} = q_{3k-2} + q_{3k-1}\,;$$

also ist

$$\begin{aligned} p_{3k} - q_{3k}\sqrt[M]{e} &= \left(p_{3k-2} - q_{3k-2}\sqrt[M]{e}\right) + \left(p_{3k-1} - q_{3k-1}\sqrt[M]{e}\right) \\ &= B_{k-1} + C_{k-1} = -A_k \end{aligned}$$

nach Induktionsannahme und der Beziehung $A_k = -B_{k-1} - C_{k-1}$.

Genauso können wir auch bei den anderen beiden Gleichungen vorgehen:

$$\begin{aligned} p_{3k+1} - q_{3k+1}\sqrt[M]{e} &= \left(p_{3k-1} - q_{3k-1}\sqrt[M]{e}\right) \\ &\qquad + \left((2k+1)M - 1\right)\left(p_{3k} - q_{3k}\sqrt[M]{e}\right) \\ &= C_{k-1} - \left((2k+1)M - 1\right)A_k = B_k \end{aligned}$$

und

$$\begin{aligned} p_{3k+2} - q_{3k+2}\sqrt[M]{e} &= \left(p_{3k} - q_{3k}\sqrt[M]{e}\right) + \left(p_{3k+1} - q_{3k+1}\sqrt[M]{e}\right) \\ &= -A_k + B_k = C_k \end{aligned}$$

Somit gelten alle drei Beziehungen auch für k, also für alle $k \in \mathbb{N}_0$. Dies beweist den Satz sowie die Kettenbruchentwicklungen für e und seine Wurzeln. ∎

Wer sich genauer dafür interessiert, wie man auf die hier einfach hingeschriebenen Integrale A_k, B_k und C_k kommt, sollte die verwendeten Originalarbeiten (und eventuell auch die dort zitierte Literatur) konsultieren:

HENRY COHN: A Short Proof of the Simple Continued Fraction Expansion of e, *American Mathematical Monthly* **113** (2006), 56–62

und

THOMAS J. OSLER: A Proof of the Continued Fraction Expansion of $e^{1/M}$, *American Mathematical Monthly* **113** (2006), 62–66

Das *American Mathematical Monthly,* eine Mitgliederzeitschrift der *Mathematical Association of America,* ist im Internet frei verfügbar.