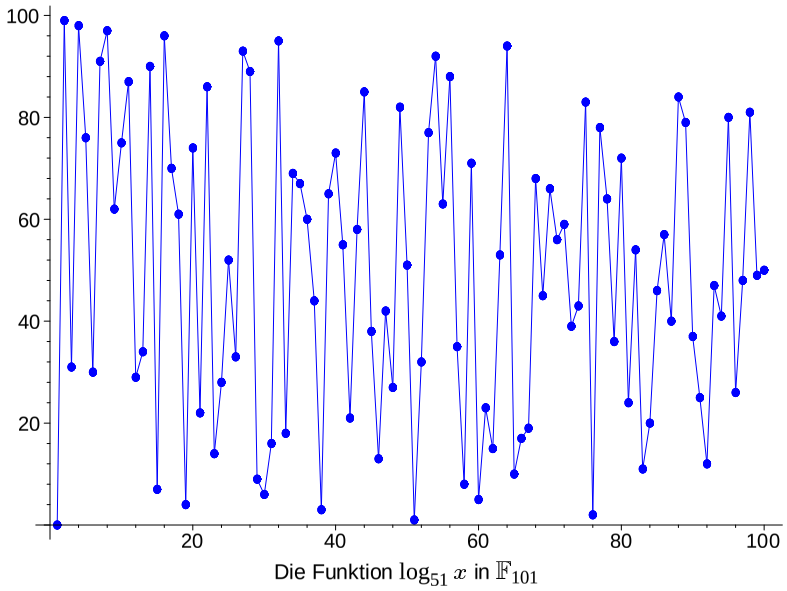


Die Funktion $\log_{51} x$ in $\mathbb{F}_{101}$

tenzen, und jeder Fall erfordert einen neue Hardwareentwurf. Falls man die Primzahlen hinreichend häufig wechselt, dürfte sich dieser Aufwand für kaum einen Gegner lohnen.

Da Körper von Primzahlordnung auch einfacher sind als solche von Primzahlpotenzordnung, wollen wir uns zunächst auf diese beschränken; die spätere Übertragung des Algorithmus auf Körper von Zweipotenzordnung sollte dem Leser keine Schwierigkeiten machen.

Beim DIFFIE-HELLMAN-Verfahren, dem ältesten auf der Grundlage diskreter Logarithmen, geht es wie gesagt darum, daß zwei Teilnehmer, die weder über gemeinsame Schlüsselinformation noch über eine sichere Leitung verfügen, einen Schlüssel vereinbaren wollen.

Dazu einigen sie sich zunächst (über die unsichere Leitung) auf eine Primzahl p und eine natürliche Zahl a derart, daß die Potenzfunktion $x \mapsto a^x$ möglichst viele Werte annimmt.

Als nächstes wählt Teilnehmer A eine Zufallszahl $x < p$ und B entsprechend $y < p$; A schickt $u = a^x \bmod p$ an B und erhält dafür $v = a^y \bmod p$.

Sodann berechnet A die Zahl

$$v^x \bmod p = \left(a^y\right)^x \bmod p = a^{xy} \bmod p$$

und B entsprechend

$$u^y \bmod p = \left(a^x\right)^y \bmod p = a^{xy} \bmod p\,;$$

beide haben also auf verschiedene Weise dieselbe Zahl berechnet, die sie nun als Schlüssel in einem klassischen Kryptosystem verwenden können, wobei sie sich wohl meist auf einen Teil der Bits beschränken müssen, da solche Schlüssel typischerweise eine Länge von 128 bis 256 Bit haben, während die Primzahl p erheblich größer sein muß.

Ein Gegner, der den Datenaustausch abgehört hat, kennt die Zahlen p, a, u und v; um $a^{xy} \bmod p$ zu finden, muß er den diskreten Logarithmus von u oder v berechnen.

Mit den besten heute bekannten Algorithmen ist die möglich, wenn p eine Primzahl von bis zu etwa 200 Dezimalstellen ist; dies entspricht etwa 665 Bit. Auch in diesem Fall dauert die Berechnung allerdings selbst bei massiver Parallelisierung über das Internet mehrere Monate, gefolgt von einer Schlußrechnung auf einem Supercomputer.

Natürlich gibt es keine Garantie, daß kein Gegner mit einem besseren als den bislang bekannten Verfahren diskrete Logarithmen oder Faktorisierungen auch in weitaus größeren Körpern berechnen kann. Dazu bräuchte er allerdings einen Durchbruch entweder auf der mathematischen oder auf der technischen Seite, für den weit und breit keine Grundlage zu sehen ist.

Falls sich allerdings die sogenannten *Quantencomputer* realisieren lassen, werden alle heute bekannten Verfahren der Kryptographie mit öffentlichen Schlüsseln, egal ob mit diskreten Logarithmen, RSA oder elliptischen Kurven, unsicher sein. Bislang können Quantencomputer kaum mit acht Bit rechnen, und nicht alle Experten sind davon überzeugt, daß es je welche geben wird, die mit mehreren Tausend Bit rechnen können.

§6: DSA

DSA steht für *Digital Signature Algorithm*, ein Algorithmus der im *Digital Signature Standard* DSS der USA festgelegt ist und neben RSA auch zu den von der Bundesnetzagentur empfohlenen „Geeigneten Algorithmen“ zählt.

Aus Sicht der amerikanischen Behörden hat DSA gegenüber RSA und Verfahren wie DIFFIE-HELLMAN vor allem einen großen Vorteil: Es läßt sich *nur* für elektronische Unterschriften benutzen, nicht zur Verschlüsselung.

Seine Sicherheit beruht auf diskreten Logarithmen, allerdings wird das klassische Verfahren dadurch modifiziert, daß die Sicherheit zwar auf dem diskreten Logarithmenproblem in einem großen Körper beruht, die Rechenoperationen bei der Anwendung des Algorithmus aber nur eine deutlich kleinere Untergruppe verwenden.

Für diese kleine Untergruppe wählt man eine Primzahl q, die im ursprünglichen Standard eine Länge von mindestens 160 Bit haben sollte. Laut Bundesnetzagentur sollte diese Länge auch noch bis Ende 2009 ausreichen, bis Ende 2012 sind allerdings nach dem Entwurf für 2007 mindestens 224 Bit vorgeschrieben, was wahrscheinlich mehr mit den verwendeten Hashfunktionen als mit der Sicherheit der Unterschrift zu tun hat.

Zu dieser Primzahl q sucht man eine Primzahl $p \equiv 1 \bmod q$, für deren Länge die Bundesnetzagentur bis Ende 2007 mindestens 1024 Bit vorschreibt, bis Ende 2008 mindestens 1280, bis Ende 2009 mindestens 1536 und bis Ende 2012 mindestens 2048. „Empfohlen“ sind auch hier 2048 Bit.

Daß diese Zahlen (bis auf die unwesentliche Differenz zwischen 2048 und 1976) mit den RSA-Modullängen für die entsprechenden Jahre übereinstimmen, ist kein Zufall: Auch wenn kein direkter Zusammenhang zwischen faktorisierung und der Berechnung diskreter Logarithmen bekannt ist, hat bislang doch jede neue Idee für einen Faktorisierungsalgorithmus auch zu einem Algorithmus zur Berechnung diskreter

Logarithmen geführt, und die auch Laufzeiten dieser Algorithmen sind bei gleicher Zahlenlänge ungefähr gleich.

Als nächstes muß ein Element g gefunden werden, dessen Potenzen im Körper $\mathbb{F}_p$ eine Gruppe der Ordnung q bilden. Das ist einfach: Man starte mit irgendeinem Element $g_0 \in \mathbb{F}_p \setminus \{0\}$ und berechne seine $(p-1)/q$-te Potenz. Falls diese ungleich eins ist, muß sie wegen $g_0^{p-1} = 1$ die Ordnung q haben; andernfalls muß ein neues g_0 betrachtet werden.

Die so bestimmten Zahlen q, p und g werden veröffentlicht und können auch in einem ganzen Netzwerk global eingesetzt werden. Geheimer Schlüssel jedes Teilnehmers ist eine Zahl x zwischen eins und $q-1$; der zugehörige öffentliche Schlüssel ist $y = g^x \bmod p$.

Unterschreiben lassen sich mit diesem Verfahren Nachrichtenblöcke m mit $0 \le m < q$, insbesondere also 160 *bzw.* 224 Bit lange Hashwerte. Dazu wählt man für jede Nachricht eine Zufallszahl k mit $0 < k < q$ und berechnet

$$r = (g^k \bmod p) \bmod q\,.$$

Da q eine Primzahl ist, hat k ein multiplikatives Inverses modulo q; man kann also durch k dividieren und erhält eine Zahl s, für die

$$sk \equiv m + xr \bmod q$$

ist; die Unterschrift unter die Nachricht m besteht dann aus den beiden 160 Bit lagen Zahlen r und s. Sie kann nur berechnet werden von jemanden, der den geheimen Schlüssel x kennt.

Überprüfen kann die Unterschrift allerdings jeder: Ist t das multiplikative Inverse zu s modulo q, so ist

$$k \equiv tsk \equiv tm + xtr \bmod q\,,$$

also, da g die Ordnung q hat,

$$r \equiv g^k \equiv g^{tm} g^{xtr} \equiv g^{tm} y^{tr} \bmod p\,.$$

in dieser Gleichung sind die linke wie auch die rechte Seite *modulo* q öffentlich bekannt, die Gleichung kann also modulo q überprüft werden. Die Unterschrift wird anerkannt, wenn beide Seiten modulo q gleich sind.

Ein Angreifer müßte sich x aus y verschaffen, müßte also ein diskretes Logarithmenproblem modulo der großen Primzahl p lösen.

§ 7: Anwendungen bei SSL/TLS

SSL steht für *secure socket layer,* TLS für *transport layer security;* Zweck ist jeweils der Aufbau einer sicheren Internetverbindung.

Wie im Internet üblich, können dazu die verschiedensten Verfahren benutzt werden; die auf Grundlage von RSA zählen derzeit zu den populärsten.

Natürlich ist RSA zu aufwendig, um damit eine längere Kommunikation wie beispielsweise eine *secure shell* Sitzung zu verschlüsseln; tatsächlich dient RSA daher nur zur Übetragung eines Schlüssels für ein konventionelles Kryptoverfahren wie AES, IDEA oder Triple-DES, auf das sich die Beteiligten unter SSL/TLS ebenfalls einigen müssen.

Am einfachsten wäre es, wenn der Client einen Schlüssel für ein solches Verfahren wählt und dann diesen mit dem RSA-Schlüssel des Servers verschlüsselt an diesen schickt – vorausgesetzt, er kennt diesen RSA-Schlüssel. Letzteres ist im allgemeinen nicht der Fall; daher muß zunächst der Server dem Client seinen Schlüssel mitteilen.

Da der Client nicht sicher sein kann, mit dem richtigen Server verbunden zu sein, schickt er diesen Schlüssel meist zusammen mit einem Zertifikat, das sowohl seine Identität als auch seinen RSA-Schlüssel enthält und von einer Zertifizierungsstelle unterschrieben ist.

Die öffentlichen Schlüssel der gängigen Zertifizierungsstellen sind in die Browserrprogramme eingebaut; bei weniger bekannten Zertifizierungsstellen wie etwa dem Rechenzentrum der Universität Mannheim fragt der Browser den Benutzer, ob er das Zertifikat anerkennen will oder nicht. Bei *secure shell* schließlich, wo die Gegenseite typischerweise keinerlei Zertifikat vorweisen kann, frägt das Programm beim ersten Verbindungsaufbau zu einem server, ob dessen Schlüssel anerkannt werden soll und speichert dann einen sogenannten *fingerprint* davon; dieser wird bei späteren Verbindungen zur Identitätsfeststellung benutzt.

§ 8: Ausblick

Dieses kurze Kapitel konnte selbstverständlich keine umfassende Übersicht über die Kryptographie oder auch nur die asymmetrische Kryptographie geben: Auch das RSA-Verfahren kann mit anderen Methoden angegriffen werden als der direkten Faktorisierung des Moduls; gelegentlich werden wir auch im Laufe dieser Vorlesung darauf zurückkommen.

Mit Ausnahme von Verfahren wie dem *one time pad* gibt es für keines der heute benutzten Kryptoverfahren einen Sicherheitsbeweis, nicht einmal in dem Sinn, daß man den Aufwand eines Gegners zum Knacken des Verfahrens in irgendeiner realistischen Weise nach unten abschätzen könnte. Seriöse Kryptographie außerhalb des Höchstsicherheitsbereichs muß sich daher damit begnügen, daß die Verantwortlichen für den Einsatz eines Verfahrens und der Wahl seiner Parameter (wie den Primzahlen bei RSA) darauf achten, auf dem neuesten Stand der Forschung zu bleiben und ihre Wahl so treffen, daß nicht nur die bekannten Angriffsmethoden versagen, sondern daß auch noch ein recht beträchtlicher Sicherheitszuschlag für künftige Entwicklungen und für nicht publizierte Entwicklungen bleibt.

Auf ewige Sicherheit kann man mit Verfahren wie RSA ohnehin nicht hoffen: Als RSA 1977 von MARTIN GARDNER im *Scientific American* vorgestellt wurde, bekam er von RIVEST, SHAMIR und ADLEMAN die 129-stellige Zahl

$$114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541$$

(seither bekannt als RSA-129) und eine damit verschlüsselte Nachricht, für deren Entschlüsselung die drei einen Preis von hundert Dollar ausgesetzt hatten. Sie schätzten, daß eine solche Entschlüsselung etwa vierzig Quadrillionen ($4 \cdot 10^{25}$) Jahre dauern würde. (Heute sagt RIVEST, daß dies auf einem Rechenfehler beruhte.) Tatsächlich wurde der Modul 1994 faktorisiert in einer gemeinsamen Anstrengung von 600 Freiwilligen, deren Computer immer dann, wenn sie nichts besseres zu tun hatten, daran arbeiteten. Nach acht Monaten war die Faktorisierung gefunden:

Die obige Zahl ist gleich

$$4905295108476509491478496199038981334177646384933878439908205 77 \times 32769132993266709549961988190834461413177642967992942539798288533 .$$

Mit dem Schema $A = 01$ bis $Z = 26$ und Zwischenraum gleich 00 war die Nachricht *The Magic Words are Squeamish Ossifrage* dann schnell entschlüsselt.

Auch bei heute den heute als sicher geltenden symmetrischen Kryptoverfahren rechnet niemand ernsthaft damit, daß sie noch in hundert Jahren sicher sind: Diese Verfahren werden üblicherweise so gewählt, daß man auf eine Sicherheit für etwa dreißig Jahren hoffen kann – sicher kann aber auch das niemand vorhersagen.

Wer mehr über Kryptographie wissen will, findet einen ersten Überblick beispielsweise bei

BUCHMANN: Einführung in die Kryptographie, *Springer,* ^{3}2004

oder natürlich auch in der Kryptologie-Vorlesung des nächsten Semesters.

Mehr über die Geschichte der Kryptographie mit öffentlichen Schlüsseln ist (mathematikfrei) zu finden in

STEVEN LEVY: **crypto:** how the rebels beat the government – saving privacy in the digital age, *Penguin Books,* 2002

Kapitel 3
Kettenbrüche

§ 1: Der Kettenbruchalgorithmus

Der EUKLIDische Algorithmus läßt sich auch verwenden, um eine 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:

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

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

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

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

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

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

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

Im i-ten Schritt, $i \ge 1$, 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

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

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

Falls der Algorithmus mit $\alpha_r = 0$ abbricht, steht im untersten Bruch natürlich nur c_r im Nenner.

So, wie der Algorithmus formuliert ist, können wir ihn aber 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.

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

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 Nenner $1, 2, 5, 12$ 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

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

Im nächsten Schritt ist $c_2 = \left\lfloor \frac{1}{\alpha_2} \right\rfloor = 15$ 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 beginnt ist somit

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cdots}}}}}}}}}$$

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

Tatsächlich werden wir sehen, daß die Konvergenten der Kettenbruchentwicklung einer irrationalen Zahl stets die bei vorgegebener Größenordnung des Nenners bestmögliche rationale Approximation der 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 (p, q) mit ganzzahligen Koordinaten liegt. Rationale Approximationen erhalten wir durch Punkte $(p, q) \in \mathbb{Z} \times \mathbb{Z}$, die in der Nähe der Geraden liegen.

Die folgende Konstruktion liefert solche Punkte P_n. Sie liegen für gerade n stets unterhalb der Geraden $y = \alpha x$ und für ungerades 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

$$c = \left[\left| \frac{p - \alpha q}{p' - \alpha q'} \right|\right]$$

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

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 gerade konstruierten $c = c_n$ 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.

Der gerichtete vertikale Abstand des Punktes $P_n = (q_n, p_n)$ von der Geraden $y = \alpha x$ ist $d_n = p_n - \alpha q_n$; damit ausgedrückt ist

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

Somit verschwindet a_n genau dann, wenn $|d_{n-2}| < |d_{n-1}|$ ist.

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

$$d_n = d_{n-2} + a_n d_{n-1} = d_{n-2} + \left[\left| \frac{d_{n-2}}{d_{n-1}} \right|\right] d_{n-1}$$

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 $a_i \geq 1$.

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 $P_0 = (1, a_0)$ mit $a_0 = [\alpha]$, 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 a_n von Null verschieden und $|d_n| < |d_{n-1}|$.

Aus den Beziehungen

$$p_n = p_{n-2} + a_n p_{n-1} \quad \text{und} \quad q_n = q_{n-2} + a_n q_{n-1}$$

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

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

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

$$p_{n-1} q_{n-2} - q_{n-1} p_{n-2} = p_{-1} q_{-2} - q_{-1} p_{-2} = 0 \cdot 0 - 1 \cdot 1 = -1;$$

daraus folgt induktiv, daß

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

ist. 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 $n \geq 0$

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

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 deutlich 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 sollten 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 a_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 $a_n = \left[\left|d_{n-2}/d_{n-1}\right|\right]$ ist dann $a_n = [1/\alpha_n]$. Division der Beziehung $d_n = d_{n-2} + a_n d_{d-1}$ durch d_{n-1} führt auf

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

was zusammen mit $a_n = [1/\alpha_n]$ und dem Induktionsanfang $\alpha = a_0 + \alpha_1$ genau auf die zu Beginn des Abschnitts konstruierten Folgen der a_n und α_n führt.

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

Als nächstes wollen wir uns überlegen, daß Kettenbrüche in der Tat bestmögliche Approximationen geben: Ist $\frac{r}{s}$ 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 zur Geraden $y = \alpha x$ einen kleineren Betrag hat als der von R.

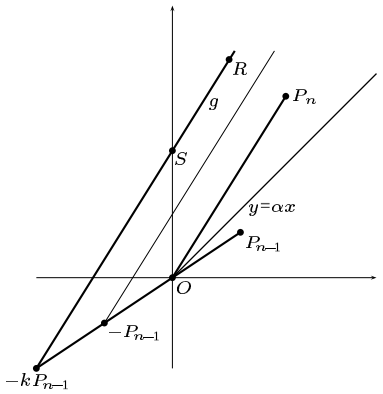
Wir schreiben R als ganzzahlige Linearkombination $R = kP_{n-1} + \ell P_n$ der Punkte P_{n-1} und P_n. Das ist möglich, denn die Determinante des linearen Gleichungssystems

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

ist, wie wir oben gesehen haben, gleich $(-1)^{n-1}$; wenn wir es nach der CRAMERschen Regel lösen, erhalten wir also eine ganzzahlige Lösung (k, l).

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 Geraden g durch kP_{n-1} mit Steigungsvektor $\overrightarrow{OP_n}$; nach unserer Annahme ist ihre Steigung somit 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 Vorraussetzung $R \neq P_{n-1}$ 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 $a_0 = \lfloor\sqrt{3}\rfloor = 1$ und $\alpha_1 = \sqrt{3} - 1$. Der Kehrwert davon ist

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} \Longrightarrow a_1 = 1 \quad \text{und} \quad \alpha_2 = \frac{\sqrt{3}-1}{2}\,.$$

Der Kehrwert davon ist

$$\frac{2}{\sqrt{3}-1} = \sqrt{3}+1 \Longrightarrow a_2 = 2 \quad \text{und} \quad \alpha_3 = \sqrt{3}-1 = \alpha_1\,.$$

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

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \dots}}}}\,.$$

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

Satz: *a)* Für eine irrationale Zahl α und jedes $n \geq 2$ ist mindestens eine der beiden Relationen

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

erfüllt.
b) Ist für eine rationale Zahl $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, so ist 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

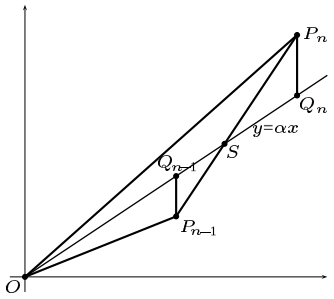
$$|q_{n-1}\alpha - p_{n-1}| \geq \frac{1}{2q_{n-1}} \quad \text{und} \quad |q_n\alpha - p_n| \geq \frac{1}{2q_n}\,.$$

Wir nehmen für den Beweis wieder an, daß $p_{n-1}/q_{n-1} < \alpha < p_n/q_n$ ist; der andere 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 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 $y = \alpha x$. Nach unserer Annahme 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 des Dreiecks mindestens gleich $1/4$.



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,

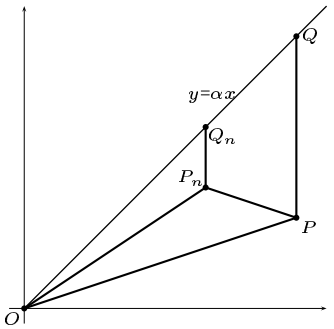
ist das zweite dieser Dreiecke das kleinere. Daher ist die Fläche des Dreiecks $\triangle OP_{n-1}P_n$ größer als die Summe der Flächen der Dreiecke $\triangle OP_{n-1}Q_{n-1}$ und $\triangle OP_nQ_n$, also größer als $1/4 + 1/4 = 1/2$. Dies ist ein Widerspruch zur obigen direkten Berechnung dieser Fläche.

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

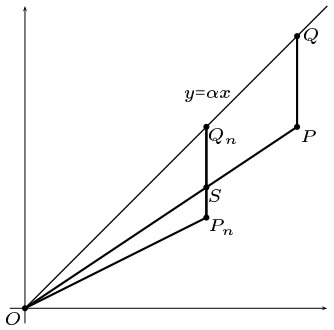
Da die Folge der Nenner q_n strikt monoton ansteigt, gibt es genau ein n, so daß $q_n \le q < q_{n+1}$ ist; wir müssen zeigen, daß $p/q = p_n/q_n$ ist. Andernfalls ist $pq_n - qp_n \neq 0$, also – da dies eine ganze Zahl ist – $|pq_n - qp_n| \ge 1$. Setzen wir $P = (q, p)$, so ist also die Fläche des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



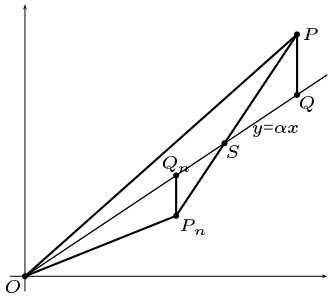
Betrachten wir als erstes den Fall, daß p_n/q_n zwischen α und p/q liegt. Dann liegt der Punkt P_n im Innern des Dreiecks $\triangle OPQ$, also ist das gesamte Dreieck $\triangle OPP_n$ imd Dreieck $\triangle OPQ$ enthalten. Da ersteres mindestens die Fläche $1/2$ hat, letzteres aber weniger als $1/4$, 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 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 Fläche des Dreiecks $\triangle OPQ$, von der wir wissen, daß sie höchstens gleich $1/4$ 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 muß gleich p_n/q_n sein. ∎

§4: 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 möglicherweise 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.

Ausgangspunkt ist die Gleichung $ed - k\varphi(N) = 1$, die wir umschreiben können 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, und in der Tat ist

$$\begin{aligned}\left|\frac{e}{N} - \frac{k}{d}\right| &= \left|\frac{e}{N} - \frac{e}{(p-1)(q-1)} + \frac{e}{(p-1)(q-1)} - \frac{k}{d}\right| \\ &\le \left|\frac{e(p-1)(q-1) - epq}{N(p-1)(q-1)}\right| + \frac{1}{d(p-1)(q-1)} \\ &= \frac{e(p+q-1)}{N(p-1)(q-1)} + \frac{1}{d(p-1)(q-1)} .\end{aligned}$$

Falls dies kleiner ist als $1/2d^2$, muß k/d eine Konvergente der Kettenbruchentwicklung von e/N sein; um d zu berechnen, müssen wir also 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.

Eine einfache Abschätzung zeigt, daß dies für p und q von etwa gleicher Größe funktioniert, sofern d höchstens die Größenordnung von etwa $\sqrt[4]{N}$ hat; neuere, etwas aufwendigere Untersuchungen zeigen, daß auch man d auch noch für $d < N^{0,289}$ rekonstruieren kann. Fachleute erwarten, daß möglicherweise sogar alle $d < \sqrt{N}$ unsicher sind.

Private Exponenten müssen also 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.