Exkurs: Die Fermatsche Faktorisierungsmethode für RSA-Zahlen

Sei N eine ungerade natürliche Zahl. Bei der Fermatschen Faktorisierungsmethode versucht man, N als Differenz von Quadratzahlen zu schreiben:

$$N = u^2 - w^2 \quad \text{mit} \quad u \in \mathbb{N}, w \in \mathbb{N}_0,$$

denn dann erhält man die Zerlegung

$$N = (u - w)(u + w).$$

Die Gleichung $N = u^2 - w^2$ kann man auch in der Form

$$u^2 - N = w^2$$

schreiben. Ist sie erfüllt, so gilt $u^2 \geq N$, also $u \geq \lceil\sqrt{N}\rceil$. Man probiert daher nacheinander für $u = \lceil\sqrt{N}\rceil, \lceil\sqrt{N}\rceil + 1, \lceil\sqrt{N}\rceil + 2, \lceil\sqrt{N}\rceil + 3, \ldots$, ob $u^2 - N$ eine Quadratzahl ist, d.h. ob ein $w \in \mathbb{N}_0$ existiert mit $u^2 - N = w^2$, denn dann erhält man sofort $N = u^2 - w^2 = (u - w)(u + w)$.

Wir beginnen mit Beispielen, die man auch mit einem Taschenrechner behandeln kann.

Beispiele:

(1) Wir wollen $N = 2263$ faktorisieren. Es ist $\sqrt{2263} = 47.57\ldots$, weswegen wir mit $u = 48$ beginnen.

u	$u^2 - N$	$\sqrt{u^2 - N}$
48	41	≈ 6.40
49	138	≈ 11.75
50	237	≈ 15.39
51	338	≈ 18.38
52	441	21 (exakt)

Daher ist

$$2263 = 52^2 - 21^2 = (52 - 21) \cdot (52 + 21) = 31 \cdot 73.$$

(2) Wir wollen $N = 5353$ faktorisieren. Es ist $\sqrt{5353} = 73.16\ldots$, also beginnen wir mit $u = 74$:

u	$u^2 - N$	$\sqrt{u^2 - N}$
74	123	≈ 11.09
75	272	≈ 16.49
76	423	≈ 20.57
77	576	24 (exakt)

Daher gilt

$$5353 = 77^2 - 24^2 = (77 - 24) \cdot (77 + 24) = 53 \cdot 101.$$

(3) Sei $N = 20696041$. Es ist $\sqrt{20696041} = 4549.29\ldots$, also beginnen wir mit $u = 4550$.

u	$u^2 - N$	$\sqrt{u^2 - N}$
4550	6459	≈ 80.37
4551	15560	≈ 124.74
4552	24663	≈ 157.04
4553	33768	≈ 183.76
4554	42875	≈ 207.06
4555	51984	228 (exakt)

Daher gilt

$$20696041 = 4555^2 - 228^2 = (4555 - 228) \cdot (4555 + 228) = 4327 \cdot 4783.$$

Datei: ki_fermatfaktorisierung.tex. Version vom 29.5.2018

Bemerkung: Ist $n \in \mathbb{N}$ eine Quadratzahl, so gibt es für die letzten beiden Ziffern nur folgende 22 Möglichkeiten:

$$00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96.$$

Hat man diese Liste, kann man oft schnell sehen, dass es sich bei einer Zahl nicht um eine Quadratzahl handelt.

Bemerkungen:

(1) Sind $N, u, w \in \mathbb{Z}$ mit $N = u^2 - w^2$, so gibt es zwei Möglichkeiten:
- Ist $u \equiv w \bmod 2$, so ist $u - w \equiv u + w \equiv 0 \bmod 2$, also ist $N = (u - w)(u + w)$ durch 4 teilbar, $4 \mid N$.
- Ist $u \not\equiv w \bmod 2$, so ist $u - w \equiv u + w \equiv 1 \bmod 2$, also ist $N = (u - w)(u + w)$ ungerade, $2 \nmid N$.

Zahlen der Form $N = 2m$ mit $m \equiv 1 \bmod 2$ lassen sich also nicht in der Form $u^2 - w^2$ schreiben. Daher beschränkt man sich bei der Fermatschen Faktorisierungsmethode auf ungerade Zahlen.

(2) Ist N eine ungerade natürliche Zahl mit $N = u^2 - w^2$ (und $u, w \in \mathbb{Z}$), so erhält man sofort folgende Implikationen:

$$\begin{aligned} N \equiv 1 \bmod 4 \quad &\Longrightarrow \quad u \equiv 1 \bmod 2, \quad w \equiv 0 \bmod 2, \\ N \equiv 3 \bmod 4 \quad &\Longrightarrow \quad u \equiv 0 \bmod 2, \quad w \equiv 1 \bmod 2. \end{aligned}$$

Bei der Fermatschen Faktorisierungsmethoden kann man sich im Fall $N \equiv 1 \bmod 4$ also auf Zahlen $u \equiv 1 \bmod 2$, im Fall $N \equiv 3 \bmod 4$ auf Zahlen $u \equiv 0 \bmod 2$ beschränken. (Im Folgenden wurde dies aber nicht berücksichtigt.)

Das folgende Lemma zeigt, dass sich jede Faktorisierung $N = x \cdot y$ einer ungeraden natürlichen Zahl mit $x \leq y$ in der Form $N = (u - w)(u + w)$ schreiben lässt.

LEMMA. *Sei N eine ungerade natürliche Zahl und dazu*

$$U_N = \{(u, w) \in \mathbb{N} \times \mathbb{N}_0 : u^2 - w^2 = N\}, \quad V_N = \{(x, y) \in \mathbb{N} \times \mathbb{N} : xy = N, x \leq y\}.$$

(1) *Durch*

$$f : U_N \to V_N, \quad (u, w) \mapsto (u - w, u + w)$$

wird eine bijektive Abbildung definiert mit Umkehrabbildung

$$g : V_N \to U_N, \quad (x, y) \mapsto (\frac{x + y}{2}, \frac{y - x}{2}).$$

(2) *Ist $N = pq$ eine RSA-Zahl mit zwei verschiedenen ungeraden Primzahlen $p < q$, so gilt*

$$U_N = \{(\frac{p + q}{2}, \frac{q - p}{2}), (\frac{N + 1}{2}, \frac{N - 1}{2})\} \quad \textit{und} \quad V_N = \{(p, q), (1, N)\}.$$

Außerdem gilt $\frac{p+q}{2} < \frac{N+1}{2}$.

Beweis:

(1) (a) Ist $(u, w) \in U_N$, so gilt $u \in \mathbb{N}$, $w \in \mathbb{N}_0$ und $u^2 - w^2 = N$, was sofort $(u - w)(u + w) = N$ und natürlich $u - w, u + w \in \mathbb{N}$, $u - w \leq u + w$, also $(u - w, u + w) \in V_N$ liefert. Daher ist die Abbildung f wohldefiniert.

(b) Ist $(x, y) \in V_N$, so gilt $x, y \in \mathbb{N}$, $xy = N$ und $x \leq y$. Da N ungerade ist, sind auch x und y ungerade, was sofort $\frac{x+y}{2} \in \mathbb{N}$, $\frac{y-x}{2} \in \mathbb{N}_0$ liefert. Mit

$$(\frac{x + y}{2})^2 - (\frac{y - x}{2})^2 = \frac{(x^2 + 2xy + y^2) - (y^2 - 2yx + x^2)}{4} = xy = N$$

folgt $(\frac{x+y}{2}, \frac{y-x}{2}) \in U_N$, weswegen die Abbildung g wohldefiniert ist.

(c) Für $(u,w) \in U_N$ gilt

$$(g \circ f)((u,w)) = g(f((u,w)) = g((u-w, u+w)) = (u,w),$$

für $(x,y) \in V_N$ gilt

$$(f \circ g)((x,y)) = f(g((x,y)) = f((\frac{x+y}{2}, \frac{y-x}{2}) = (x,y).$$

Daher sind f und g invers zueinander, wie behauptet.

(2) Wegen der eindeutigen Primfaktorzerlegung folgt aus $N = 1 \cdot N = p \cdot q$ sofort

$$V_N = \{(1,N), (p,q)\}.$$

U_N erhält man nach (1), wenn man die Abbildung g auf V_N anwendet. Wegen

$$\frac{N+1}{2} - \frac{p+q}{2} = \frac{N+1-p-q}{2} = \frac{pq-p-q+1}{2} = \frac{(p-1)(q-1)}{2} > 0$$

folgt $\frac{p+q}{2} < \frac{N+1}{2}$. ■

In der folgenden Variante des Fermatschen Faktorisierungsverfahrens wird benutzt, dass man zu $n \in \mathbb{N}$ (schnell) $\lfloor \sqrt{n} \rfloor$ berechnen kann. (Wir haben zur Berechnung von $\lfloor \sqrt{n} \rfloor$ bereits ein Intervallschachtelungsverfahren kennengelernt.) Wir beschränken uns auf RSA-Zahlen $N = pq$.

Fermatsche Faktorisierungsmethode: Sei N eine RSA-Zahl, d.h. das Produkt zweier verschiedener ungerader Primzahlen $p < q$. Bestimmt werden p und q.

(1) Berechne $u = \left\lfloor \sqrt{N} \right\rfloor$. (Ist nicht ausgeschlossen, dass N ein Quadrat ist, kann man testen, ob $u^2 = N$ gilt.)
(2) $u := u+1$, $v = u^2 - N$, $w = \lfloor \sqrt{v} \rfloor$
(3) Gilt $v = w^2$? (Hier wird getestet, ob v ein Quadrat ist.)
  (a) Wenn nein, gehe zu (2).
  (b) Wenn ja, gib $u-w$ und $u+w$ als Teiler von N aus.

(Als Schrittzahl der Faktorisierungsmethode bezeichnen wir die Anzahl, wie oft Schritt (2) durchlaufen wurde.)

Etwas algorithmischer aufgeschrieben ergibt sich:

Fermat-Faktorisierung einer RSA-Zahl:
Eingabe: Eine RSA-Zahl N (mit $N = pq$).
Ausgabe: Die Primteiler p, q von N.

```
1: u ← ⌊√N⌋.
2: loop
3:     u ← u + 1, v ← u² − N, w ← ⌊√v⌋.
4:     if v = w² then return Gib u − w und u + w als Primteiler p und q von N aus.
5:     end if
6: end loop
```

Bemerkung: Sei $N = pq$ eine RSA-Zahl (mit $p < q$). Nach dem vorangegangenen Lemma hat die Gleichung $N = u^2 - w^2$ für $u \in \mathbb{N}$, $w \in \mathbb{N}_0$ nur die Lösungen

$$N = (\frac{p+q}{2})^2 - (\frac{q-p}{2})^2 = (\frac{N+1}{2})^2 - (\frac{N-1}{2})^2,$$

d.h. nur für

$$u = \frac{p+q}{2} \quad \text{und} \quad u = \frac{N+1}{2}$$

ist $u^2 - N$ eine Quadratzahl. Wegen $\frac{p+q}{2} < \frac{N+1}{2}$ hat die Fermatsche Faktorisierungsmethode Erfolg, wenn

$$u = \frac{p+q}{2}$$

erreicht ist. Schreiben wir $u_i = \left\lfloor \sqrt{N} \right\rfloor + i$, so wird im i-ten Schritt getestet, ob $u_i^2 - N$ ein Quadrat ist. Hat die Faktorisierungsmethode im n-ten Schritt Erfolg, so gilt also

$$u_n = \frac{p+q}{2}, \quad \text{d.h.} \quad \left\lfloor \sqrt{N} \right\rfloor + n = \frac{p+q}{2}.$$

Die Schrittzahl n zur Faktorisierung von N ist also

$$n = \frac{p+q}{2} - \left\lfloor \sqrt{N} \right\rfloor.$$

Wir formulieren dies noch etwas schöner:

SATZ. *Sei $N = pq$ eine RSA-Zahl und n die Anzahl der Schritte, die die Fermatsche Faktorisierungsmethode zum Faktorisieren von N braucht. Dann gilt*

$$n = \left\lfloor \frac{1}{2}(\sqrt{q} - \sqrt{p})^2 + 1 \right\rfloor.$$

Beweis:

(1) Wir zeigen zunächst, dass für $x \in \mathbb{R} \setminus \mathbb{Z}$ die Gleichheit

$$-\lfloor x \rfloor = \lfloor -x + 1 \rfloor$$

gilt. Dies sieht man sofort, wenn man schreibt $x = m + \varepsilon$ mit $m \in \mathbb{Z}$ und $0 < \varepsilon < 1$, denn dann ist (wegen $0 < 1 - \varepsilon < 1$)

$$-\lfloor x \rfloor = -m \quad \text{und} \quad \lfloor -x + 1 \rfloor = \lfloor -m - \varepsilon + 1 \rfloor = \lfloor -m + (1 - \varepsilon) \rfloor = -m.$$

(2) Mit der in der vorangegangenen Bemerkung gezeigten Formel $n = \frac{p+q}{2} - \left\lfloor \sqrt{N} \right\rfloor$ und (1) erhalten wir

$$\begin{aligned} n &= \frac{p+q}{2} - \left\lfloor \sqrt{N} \right\rfloor = \frac{p+q}{2} + \left\lfloor -\sqrt{N} + 1 \right\rfloor = \left\lfloor \frac{p+q}{2} - \sqrt{N} + 1 \right\rfloor = \\ &= \left\lfloor \frac{p+q-2\sqrt{pq}}{2} + 1 \right\rfloor = \left\lfloor \frac{(\sqrt{q} - \sqrt{p})^2}{2} + 1 \right\rfloor = \left\lfloor \frac{1}{2}(\sqrt{q} - \sqrt{p})^2 + 1 \right\rfloor, \end{aligned}$$

was wir zeigen wollten. ■

FOLGERUNG. *Sei $N = pq$ eine RSA-Zahl mit $p < q$. Die Fermatsche Faktorisierungsmethode faktorisiert N genau dann in n Schritten, wenn gilt*

$$p + \sqrt{8(n-1)} \cdot \sqrt{p} + 2(n-1) \leq q < p + \sqrt{8n} \cdot \sqrt{p} + 2n.$$

Insbesondere hat die Faktorisierungsmethode schon im 1. Schritt Erfolg, wenn gilt

$$p < q < p + \sqrt{8} \cdot \sqrt{p} + 2.$$

Beweis: Wir formen die Formel aus dem vorangegangenen Satz einfach um:

$$\begin{aligned} n = \left\lfloor \frac{1}{2}(\sqrt{q} - \sqrt{p})^2 + 1 \right\rfloor \quad &\iff \quad n \leq \frac{1}{2}(\sqrt{q} - \sqrt{p})^2 + 1 < n + 1 \quad \iff \\ &\iff \quad n - 1 \leq \frac{1}{2}(\sqrt{q} - \sqrt{p})^2 < n \quad \iff \\ &\iff \quad \sqrt{2(n-1)} \leq \sqrt{q} - \sqrt{p} < \sqrt{2n} \quad \iff \\ &\iff \quad \sqrt{p} + \sqrt{2(n-1)} \leq \sqrt{q} < \sqrt{p} + \sqrt{2n} \quad \iff \\ &\iff \quad p + 2\sqrt{2(n-1)}\sqrt{p} + 2(n-1) \leq q < p + 2\sqrt{2n}\sqrt{p} + 2n \quad \iff \\ &\iff \quad p + \sqrt{8(n-1)} \cdot \sqrt{p} + 2(n-1) \leq q < p + \sqrt{8n} \cdot \sqrt{p} + 2n. \end{aligned}$$

Dies beweist die Behauptung. ■

Beispiel: Die Fermatsche Faktorisierungsmethode führt bei der RSA-Zahl

$$N = 152415787532388367517222749904475445377900724289038357752343009989967173845865 1$$

im 1. Schritt zum Erfolg. N hat die Primteiler

$$\begin{aligned} p &= 12345678901234567891117264774540116247 37, \\ q &= 12345678901234567890123456789012345681 23. \end{aligned}$$

Wir wollen nun noch der Frage nachgehen, wann die Fermatsche Faktorisierungsmethode praktisch Aussicht bzw. keine Aussicht auf Erfolg hat.
Zunächst schauen wir uns eine Situation an, bei der die Fermatsche Faktorisierungsmethode schnell zum Ziel führt.

SATZ. *Sei $N = pq$ eine RSA-Zahl, $\Delta = |p - q|$ und n die Schrittzahl bei der Fermatschen Faktorisierungsmethode zur Faktorisierung von N.*

(1) *Es gilt*
$$n < \frac{\Delta^2}{8\sqrt{N}} + 1.$$

(2) *Ist $m \in \mathbb{N}$ und*
$$\Delta \leq \sqrt{8m} \cdot N^{1/4}, \quad \textit{so gilt} \quad n \leq m,$$
d.h. die Fermatsche Faktorisierungsmethode faktorisiert N in höchstens m Schritten.

Beweis:

(0) Wir zeigen zunächst, dass für $x, y \in \mathbb{R}_{>0}$ folgende Abschätzung gilt:
$$\frac{1}{2}(x-y)^2 \leq \frac{(x^2-y^2)^2}{8xy}.$$
Wir können uns auf den Fall $x \neq y$ beschränken und erhalten dann die Äquivalenzen:
$$\begin{aligned} \frac{1}{2}(x-y)^2 \leq \frac{(x^2-y^2)^2}{8xy} \quad &\iff \quad \frac{1}{2}(x-y)^2 \leq \frac{(x-y)^2(x+y)^2}{8xy} \quad \iff \\ &\iff \quad 4xy \leq (x+y)^2 \quad \iff \quad 4xy \leq x^2+2xy+y^2 \quad \iff \\ &\iff \quad 0 \leq x^2-2xy+y^2 \quad \iff \quad 0 \leq (x-y)^2. \end{aligned}$$
Da $0 \leq (x-y)^2$ immer gilt, gilt auch die behauptete Abschätzung.

(1) Mit der Formel $n = \left\lfloor \frac{1}{2}(\sqrt{q}-\sqrt{p})^2 + 1 \right\rfloor$ und (0) erhalten wir
$$\begin{aligned} n &= \left\lfloor \frac{1}{2}(\sqrt{q}-\sqrt{p})^2 + 1 \right\rfloor \leq \frac{1}{2}(\sqrt{q}-\sqrt{p})^2 + 1 \overset{x=\sqrt{q}, y=\sqrt{p}}{\leq} \\ &\leq \frac{(\sqrt{q}^2-\sqrt{p}^2)^2}{8\sqrt{q}\cdot\sqrt{p}} + 1 = \frac{(q-p)^2}{8\sqrt{qp}} + 1 = \frac{\Delta^2}{8\sqrt{N}} + 1. \end{aligned}$$
Da $\sqrt{N}$ und damit auch $\frac{\Delta^2}{8\sqrt{N}}$ keine rationale Zahl ist, folgt auch
$$n < \frac{\Delta^2}{8\sqrt{N}} + 1.$$

(2) Setzen wir jetzt $\Delta \leq \sqrt{8m} \cdot N^{1/4}$ in die letzte Abschätzung ein, so folgt
$$n < \frac{\Delta^2}{8\sqrt{N}} + 1 \leq \frac{8m\sqrt{N}}{8\sqrt{N}} + 1 = m + 1, \quad \text{also} \quad n \leq m,$$
was auch die zweite Behauptung beweist. ■

Bemerkung: Die Fermatsche Faktorisierungsmethode funktioniert also, wenn $\Delta = |p-q|$ in der Größenordnung von $N^{1/4}$ bleibt. Zahlen solcher Bauart muss man für RSA-Anwendungen meiden.

Der folgende Satz liefert ein Kriterium, wann die Fermatsche Faktorisierungsmethode praktisch für große Zahlen nicht funktionieren wird.

SATZ. *Ist $N = pq$ eine RSA-Zahl und $q \geq \lambda p$ mit $\lambda > 1$, so braucht die Fermatsche Faktorisierungsmethode mindestens*

$$\frac{1}{2}(\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}} - 2)\sqrt{N}$$

Schritte um N zu faktorisieren. Ist $q \geq 1.1\,p$, so braucht die Faktorisierungsmethode mindestens $\frac{1}{1000}\sqrt{N}$ Schritte.

Beweis:

(1) Wir schreiben $p = \frac{1}{u}\sqrt{N}$, $q = u\sqrt{N}$ mit $u > 1$. Es gilt die Äquivalenz:

$$q \geq \lambda p \quad \Longleftrightarrow \quad u \geq \lambda \frac{1}{u} \quad \Longleftrightarrow \quad u^2 \geq \lambda \quad \Longleftrightarrow \quad u \geq \sqrt{\lambda}.$$

Für die Schrittzahl n gilt

$$n > \frac{1}{2}(\sqrt{q} - \sqrt{p})^2 = \frac{1}{2}(\sqrt{u\sqrt{N}} - \sqrt{\frac{1}{u}\sqrt{N}})^2 = \frac{1}{2}(u + \frac{1}{u} - 2)\sqrt{N}.$$

Nun ist die Funktion $x \mapsto x + \frac{1}{x} - 2$ für $x \geq 1$ streng monoton steigend, da die Ableitung $\frac{d}{dx}(x + \frac{1}{x}) = 1 - \frac{1}{x^2}$ in diesem Intervall > 0 ist. Damit erhalten wir

$$n > \frac{1}{2}(u + \frac{1}{u} - 2)\sqrt{N} \geq \frac{1}{2}(\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}} - 2)\sqrt{N},$$

wie behauptet wurde.

(2) Aus der allgemeinen Abschätzung folgt durch Einsetzen von $\lambda = 1.1$

$$n > \frac{1}{2}(\sqrt{1.1} + \frac{1}{\sqrt{1.1}} - 2)\sqrt{N} > 0.0011\sqrt{N} > \frac{1}{1000}\sqrt{N},$$

was auch die letzte Abschätzung beweist. ■

Bemerkung: Will man große RSA-Zahlen $N = pq$, die sich mit der Fermatschen Faktorisierungsmethode praktisch nicht faktorisieren lassen, so genügt eine Bedingung der Art $q \geq 1.1\,p$.

Hier ist nochmals ein Algorithmus für den Allgemeinfall:

Fermat-Faktorisierung einer ungeraden natürlichen Zahl:
Eingabe: Eine ungerade natürliche Zahl N
Ausgabe: Eine Zerlegung $N = xy$ mit $x, y \in \mathbb{N}$ und $x \leq y$.

$u \leftarrow \left\lfloor \sqrt{N} \right\rfloor$.
if $u^2 = N$ **then return** Zerlegung $N = u^2$.
end if
loop
    $u \leftarrow u + 1$, $v \leftarrow u^2 - N$, $w \leftarrow \lfloor \sqrt{v} \rfloor$.
    if $v = w^2$ **then**
        $x \leftarrow u - w$, $y \leftarrow u + w$.
        if $x = 1$ **then**
            return N ist eine Primzahl.
        end if
        return Die nichttriviale Zerlegung $N = xy$.
    end if
end loop