KAPITEL 2

Lucas-Folgen

1. Einführung

Zu vorgebenen ganzen Zahlen P und Q werden die **Lucas-Folgen** $(U_i(P,Q))_{i\geq 0}$ und $(V_i(P,Q))_{i\geq 0}$ rekursiv durch die Formeln

$$U_0(P,Q)=0,\quad U_1(P,Q)=1,\quad U_i(P,Q)=P\,U_{i-1}(P,Q)-Q\,U_{i-2}(P,Q) \text{ für } i\geq 2$$

und

$$V_0(P,Q)=2,\quad V_1(P,Q)=P,\quad V_i(P,Q)=P\,V_{i-1}(P,Q)-Q\,V_{i-2}(P,Q) \text{ für } i\geq 2$$

definiert. Sind die Parameter P und Q fest, schreibt man oft auch nur U_i für $U_i(P,Q)$ und V_i für $V_i(P,Q)$. Nach Konstruktion ist klar, dass es sich um Folgen ganzer Zahlen handelt.

Beispiel: $P=1$, $Q=-1$. Die Rekursionsformeln lauten hier für $U_n(1,-1)$

$$U_0=0,\quad U_1=1,\quad U_i=U_{i-1}+U_{i-2} \text{ für } i\geq 2,$$

sodass man die Folge

$$0,\quad 1,\quad 1,\quad 2,\quad 3,\quad 5,\quad 8,\quad 13,\quad 21,\quad 34,\quad 55,\quad 89,\quad 144,\quad 233,\quad 377,\quad \ldots$$

erhält, also die Folge der **Fibonacci-Zahlen**. Für $V_i(1,-1)$ lauten die Rekursionsformeln

$$V_0=2,\quad V_1=1,\quad V_i=V_{i-1}+V_{i-2} \text{ für } i\geq 2,$$

sodass man die Folge

$$2,\quad 1,\quad 3,\quad 4,\quad 7,\quad 11,\quad 18,\quad 29,\quad 47,\quad 76,\quad 123,\quad 199,\quad 322,\quad 521,\quad 843,\quad \ldots$$

erhält.

Bemerkung: Wie kann man die ersten Folgenglieder einer Lucas-Folge einfach mit Python berechnen? Wir illustrieren dies am Beispiel der Fibonacci-Folge, d.h. für $P=1$, $Q=-1$:

```
P,Q=1,-1
U=[0,1]
while len(U)<1000:
  U.append(P*U[-1]-Q*U[-2])
```

Mit `U[10]` erhält man U_{10}, mit `U[:20]` werden die ersten 20 Folgenglieder ausgegeben.

Beispiele: In den folgenden Tabellen haben wir die Lucas-Folgen $(U_i(P,Q))_{i\geq 0}$ und $(V_i(P,Q))_{i\geq 0}$ für $\{|P|,|Q|\}=\{2,3\}$ und $i\leq 12$ aufgelistet:

P	Q	U_0	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8	U_9	U_{10}	U_{11}	U_{12}
2	3	0	1	2	1	-4	-11	-10	13	56	73	-22	-263	-460
2	-3	0	1	2	7	20	61	182	547	1640	4921	14762	44287	132860
-2	3	0	1	-2	1	4	-11	10	13	-56	73	22	-263	460
-2	-3	0	1	-2	7	-20	61	-182	547	-1640	4921	-14762	44287	-132860
3	2	0	1	3	7	15	31	63	127	255	511	1023	2047	4095
3	-2	0	1	3	11	39	139	495	1763	6279	22363	79647	283667	1010295
-3	2	0	1	-3	7	-15	31	-63	127	-255	511	-1023	2047	-4095
-3	-2	0	1	-3	11	-39	139	-495	1763	-6279	22363	-79647	283667	-1010295

Datei: kii_lucas_einfuehrung.tex. Version vom 26.5.2022

P	Q	V_0	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8	V_9	V_{10}	V_{11}	V_{12}
2	3	2	2	-2	-10	-14	2	46	86	34	-190	-482	-394	658
2	-3	2	2	10	26	82	242	730	2186	6562	19682	59050	177146	531442
-2	3	2	-2	-2	10	-14	-2	46	-86	34	190	-482	394	658
-2	-3	2	-2	10	-26	82	-242	730	-2186	6562	-19682	59050	-177146	531442
3	2	2	3	5	9	17	33	65	129	257	513	1025	2049	4097
3	-2	2	3	13	45	161	573	2041	7269	25889	92205	328393	1169589	4165553
-3	2	2	-3	5	-9	17	-33	65	-129	257	-513	1025	-2049	4097
-3	-2	2	-3	13	-45	161	-573	2041	-7269	25889	-92205	328393	-1169589	4165553

Es fällt auf, dass die Parameterpaare (P, Q) und $(-P, Q)$ zu bis aufs Vorzeichen gleichen Folgen führen:

LEMMA. *Es gilt*

$$U_i(-P,Q) = (-1)^{i-1}U_i(P,Q) \quad \textit{und} \quad V_i(-P,Q) = (-1)^i V_i(P,Q) \quad \textit{für alle } i \geq 0.$$

Beweis: Wir beweisen dies durch Induktion. Wegen

$$U_0(-P,Q) = 0 = U_0(P,Q), \quad U_1(-P,Q) = 1 = U_1(P,Q)$$

und

$$V_0(-P,Q) = 2 = V_0(P,Q), \quad V_1(-P,Q) = -P = -V_1(P,Q)$$

stimmt die Aussage für $i = 0$ und $i = 1$. Sie nun $i \geq 2$ und die Aussagen bereits für $i-1$ und $i-2$ gezeigt. Dann folgt:

$$\begin{aligned}
U_i(-P,Q) &= (-P)U_{i-1}(-P,Q) - QU_{i-2}(-P,Q) = \\
&= (-P)(-1)^{i-2}U_{i-1}(P,Q) - Q(-1)^{i-3}U_{i-2}(P,Q) = \\
&= (-1)^{i-1} \cdot (PU_{i-1}(P,Q) - QU_{i-2}(P,Q)) = (-1)^{i-1}U_i(P,Q), \\
V_i(-P,Q) &= (-P)V_{i-1}(-P,Q) - QV_{i-2}(-P,Q) = \\
&= (-P)(-1)^{i-1}V_{i-1}(P,Q) - Q(-1)^{i-2}V_{i-2}(P,Q) = \\
&= (-1)^i \cdot (PV_{i-1}(P,Q) - QV_{i-2}(P,Q)) = (-1)^i V_i(P,Q),
\end{aligned}$$

was die Behauptungen durch Induktion beweist. ■

Wegen des Lemmas kann man sich oft auf den Fall $P \geq 0$ beschränken. Wir behandeln zunächst ein paar Spezialfälle:

LEMMA. *Im Fall $P = 0$ gilt*

$$U_i(0,Q) = \begin{cases} 0 & \textit{für } i \equiv 0 \bmod 2, \\ (-Q)^{\frac{i-1}{2}} & \textit{für } i \equiv 1 \bmod 2 \end{cases} \quad \textit{und} \quad V_i(0,Q) = \begin{cases} 2 \cdot (-Q)^{\frac{i}{2}} & \textit{für } i \equiv 0 \bmod 2, \\ 0 & \textit{für } i \equiv 1 \bmod 2. \end{cases}$$

(Dabei sei $(-Q)^0 = 1$, damit die Formeln in der angegebenen Form gültig sind.)

Beweis: Die Rekursionsformeln lauten im Fall $P = 0$

$$U_n = -QU_{n-2} \quad \text{und} \quad V_n = -QV_{n-2} \text{ für } n \geq 2.$$

Der Rest folgt mit $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = 0$ durch Induktion. ■

Nun betrachten wir den Fall $Q = 0$:

LEMMA. *Im Fall $Q = 0$ gilt*

$$U_i(P,0) = P^{i-1} \textit{ für } i \geq 2 \quad \textit{und} \quad V_i(P,0) = P^i \textit{ für } i \geq 1.$$

(Interpretiert man $P^0 = 1$, so gilt die $U_i(P,0)$-Formel auch für $i = 1$. Allerdings lassen sich $U_0(P,0) = 0$ und $V_0(P,0) = 2$ so nicht in der Formel deuten.)

Beweis: Die Rekursionsformeln lauten im Fall $Q = 0$ einfach

$$U_i = PU_{i-1} \quad \text{und} \quad V_i = PV_{i-1} \quad \text{für } i \geq 2,$$

woraus die Aussagen sofort durch Induktion folgen. ■

Wir werden später sehen, dass das Polynom $x^2 - Px + Q$ eine wichtige Rolle spielt. Es hat Diskriminante $P^2 - 4Q$. Der Fall $P^2 - 4Q = 0$ ist auch ein Sonderfall und wird in folgendem Lemma beschrieben:

LEMMA. *Im Fall $P^2 - 4Q = 0$ gilt $Q = (\frac{P}{2})^2$ und*

$$U_i(P,Q) = i \cdot (\frac{P}{2})^{i-1} \text{ für } i \geq 2 \quad \text{und} \quad V_i(P,Q) = 2 \cdot (\frac{P}{2})^i \text{ für } i \geq 1.$$

(Die Formeln gelten für alle $i \geq 0$, wenn man $0 \cdot (\frac{P}{2})^{0-1}$ als 0 und $(\frac{P}{2})^0$ als 1 interpretiert.)

Beweis: Aus $P^2 - 4Q = 0$ folgt $Q = \frac{1}{4}P^2 = (\frac{P}{2})^2$, sodass die Rekursionsformeln hier

$$U_i = 2 \cdot (\frac{P}{2}) \cdot U_{i-1} - (\frac{P}{2})^2 \cdot U_{i-2} \quad \text{und} \quad V_i = 2 \cdot (\frac{P}{2}) \cdot V_{i-1} - (\frac{P}{2})^2 \cdot V_{i-2}$$

geschrieben werden können.

(1) Es gilt $U_0 = 0$ und $U_1 = 1$, und damit

$$U_2 = 2 \cdot (\frac{P}{2}) \cdot U_1 - (\frac{P}{2})^2 \cdot U_0 = 2 \cdot (\frac{P}{2})$$

und

$$U_3 = 2 \cdot (\frac{P}{2}) \cdot U_2 - (\frac{P}{2})^2 \cdot U_1 = 2 \cdot (\frac{P}{2}) \cdot 2 \cdot (\frac{P}{2}) - (\frac{P}{2})^2 = 3 \cdot (\frac{P}{2})^2.$$

Ist nun $i \geq 4$ und gilt die Aussage bereits für $i-1$ und $i-2$, so folgt

$$\begin{aligned} U_i &= 2 \cdot (\frac{P}{2}) \cdot U_{i-1} - (\frac{P}{2})^2 \cdot U_{i-2} = \\ &= 2 \cdot (\frac{P}{2}) \cdot (i-1) \cdot (\frac{P}{2})^{i-2} - (\frac{P}{2})^2 \cdot (i-2) \cdot (\frac{P}{2})^{i-3} = i \cdot (\frac{P}{2})^{i-1}, \end{aligned}$$

was zu zeigen war.

(2) Es ist $V_0 = 2$ und $V_1 = P = 2 \cdot (\frac{P}{2})$ und

$$V_2 = 2 \cdot (\frac{P}{2}) \cdot V_1 - (\frac{P}{2})^2 \cdot V_0 = 2 \cdot (\frac{P}{2}) \cdot 2 \cdot (\frac{P}{2}) - (\frac{P}{2})^2 \cdot 2 = 2 \cdot (\frac{P}{2})^2.$$

Ist nun $i \geq 3$ und die Aussage bereits für $i-1$ und $i-2$ gezeigt, so folgt

$$\begin{aligned} V_i &= 2 \cdot (\frac{P}{2}) \cdot V_{i-1} - (\frac{P}{2})^2 \cdot V_{i-2} = \\ &= 2 \cdot (\frac{P}{2}) \cdot 2 \cdot (\frac{P}{2})^{i-1} - (\frac{P}{2})^2 \cdot 2 \cdot (\frac{P}{2})^{i-2} = 2 \cdot (\frac{P}{2})^i, \end{aligned}$$

woraus die Behauptung durch Induktion folgt. ■

Der folgende Satz zeigt für die ersten Indizes die Folgenglieder $U_i(P,Q)$ und $V_i(P,Q)$ als Polynome in P und Q:

SATZ. *Für $i = 0, \ldots, 10$ haben $U_i(P,Q)$ und $V_i(P,Q)$ folgende Gestalt:*

i	$U_i(P,Q)$	$V_i(P,Q)$
0	0	2
1	1	P
2	P	P^2-2Q
3	P^2-Q	P^3-3PQ
4	P^3-2PQ	$P^4-4P^2Q+2Q^2$
5	$P^4-3P^2Q+Q^2$	$P^5-5P^3Q+5PQ^2$
6	$P^5-4P^3Q+3PQ^2$	$P^6-6P^4Q+9P^2Q^2-2Q^3$
7	$P^6-5P^4Q+6P^2Q^2-Q^3$	$P^7-7P^5Q+14P^3Q^2-7PQ^3$
8	$P^7-6P^5Q+10P^3Q^2-4PQ^3$	$P^8-8P^6Q+20P^4Q^2-16P^2Q^3+2Q^4$
9	$P^8-7P^6Q+15P^4Q^2-10P^2Q^3+Q^4$	$P^9-9P^7Q+27P^5Q^2-30P^3Q^3+9PQ^4$
10	$P^9-8P^7Q+21P^5Q^2-20P^3Q^3+5PQ^4$	$P^{10}-10P^8Q+35P^6Q^2-50P^4Q^3+25P^2Q^4-2Q^5$

Beweis: Man wendet einfach die Rekursionsformeln an. ■

Bemerkungen:

(1) An den Formeln des vorangegangenen Satzes lassen sich eine Reihe von Gesetzmäßigkeiten ablesen bzw. vermuten.

(2) Die Formeln des Satzes kann man leicht mit SAGE (oder der Python-Bibliothek SymPy) herleiten:

```
var("P,Q")
U=[0,1]
while len(U)<11:
  U.append(expand(P*U[-1]-Q*U[-2]))
U
```

(Ohne `expand` wird nur eingesetzt, aber nicht ausmultipliziert und vereinfacht.)

(3) SAGE berechnet $U_n(P,Q)$ mit `lucas_number1(n,P,Q)` und $V_n(P,Q)$ mit `lucas_number2(n,P,Q)`.

Der folgende Satz liefert eine wichtige Darstellung der Lucas-Folgen mit Hilfe der Nullstellung des Polynoms $x^2 - Px + Q$:

SATZ. *Seien $P, Q \in \mathbb{Z}$ und $D = P^2 - 4Q$, $\alpha = \frac{P+\sqrt{D}}{2}$, $\beta = \frac{P-\sqrt{D}}{2}$ (mit $\alpha, \beta \in \mathbb{C}$). α und β sind die Nullstellen des Polynoms $x^2 - Px + Q$. Dann gilt*

$$\alpha + \beta = P, \quad \alpha\beta = Q, \quad \alpha - \beta = \sqrt{D}$$

und für alle $i \geq 0$

$$U_i(P,Q) = \begin{cases} i\alpha^{i-1} & \text{für } \alpha = \beta, \\ \frac{\alpha^i - \beta^i}{\alpha - \beta} & \text{für } \alpha \neq \beta \end{cases} \qquad \text{und} \qquad V_i(P,Q) = \alpha^i + \beta^i,$$

wenn man $0 \cdot \alpha^{0-1} = 0$ und $\alpha^0 = \beta^0 = 1$ liest. (Die Darstellung $V_i(P,Q) = \alpha^i + \beta^i$ erklärt auch gut die Konvention $V_0(P,Q) = 2$.)

Beweis: Wir müssen nur die Formeln für $U_i(P,Q)$ und $V_i(P,Q)$ zeigen, der Rest ist klar. Im Fall $D = 0$, also $\alpha = \beta$ folgen die Aussagen aus bereits bewiesenen Formeln wegen $\alpha = \frac{P}{2}$. Sei nun $\alpha \neq \beta$. Wir beweisen dies durch Induktion. U_i und V_i sind für $i = 0$ und $i = 1$ so definiert, dass die Formeln gelten. Sei nun $i \geq 2$ und die Formeln bereits gezeigt für $i-1$ und $i-2$. Dann folgt:

$$\begin{aligned}
(\alpha-\beta)U_i &= (\alpha-\beta)(PU_{i-1} - QU_{i-2}) = P(\alpha-\beta)U_{i-1} - Q(\alpha-\beta)U_{i-2} = \\
&= P(\alpha^{i-1} - \beta^{i-1}) - Q(\alpha^{i-2} - \beta^{i-2}) = (\alpha+\beta)(\alpha^{i-1} - \beta^{i-1}) - \alpha\beta(\alpha^{i-2} - \beta^{i-2}) = \\
&= \alpha^i - \beta^i, \\
V_i &= PV_{i-1} - QV_{i-2} = P(\alpha^{i-1} + \beta^{i-1}) - Q(\alpha^{i-2} + \beta^{i-2}) = \\
&= (\alpha+\beta)(\alpha^{i-1} + \beta^{i-1}) - \alpha\beta(\alpha^{i-2} + \beta^{i-2}) = \alpha^i + \beta^i,
\end{aligned}$$

was die Behauptung durch Induktion beweist. ■

Beispiel: $(U_i(1,-1))_{i\geq 0}$ ist die Fibonacci-Folge 0, 1, 1, 2, 3, 5, 8, ... Hier ist $D = 5$, das Polynom $x^2 - x - 1$ hat die Nullstellen

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{und} \quad \beta = \frac{1-\sqrt{5}}{2},$$

sodass gilt

$$U_i(1,-1) = \frac{1}{\sqrt{5}}\left((\frac{1+\sqrt{5}}{2})^i - (\frac{1-\sqrt{5}}{2})^i\right).$$

Wegen $\alpha \approx 1.6180$ und $\beta \approx -0.6180$ ist

$$\left|U_i(1,-1) - \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^i\right| = \frac{1}{\sqrt{5}}\left|\frac{1-\sqrt{5}}{2}\right|^i \leq 0.45 \cdot 0.62^i \leq 0.45 \text{ für alle } i \geq 0,$$

sodass man $U_i(1,-1)$ auch durch Runden auf die nächste ganze Zahl erhalten kann:

$$U_i(1,-1) = \left\lfloor \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^i \right\rceil.$$

i	$\frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^i$	$U_i(1,-1)$	i	$\frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^i$	$U_i(1,-1)$
0	0.4472	0	16	987.0002	987
1	0.7236	1	17	1596.9999	1597
2	1.1708	1	18	2584.0001	2584
3	1.8944	2	19	4181.0000	4181
4	3.0652	3	20	6765.0000	6765
5	4.9597	5	21	10946.0000	10946
6	8.0249	8	22	17711.0000	17711
7	12.9846	13	23	28657.0000	28657
8	21.0095	21	24	46368.0000	46368
9	33.9941	34	25	75025.0000	75025
10	55.0036	55	26	121393.0000	121393
11	88.9978	89	27	196418.0000	196418
12	144.0014	144	28	317811.0000	317811
13	232.9991	233	29	514229.0000	514229
14	377.0005	377	30	832040.0000	832040
15	609.9997	610	31	1346269.0000	1346269

2. Verschiedene Berechnungsmethoden von $U_i(P,Q)$ und $V_i(P,Q)$

In nachfolgenden Anwendungen brauchen wir $U_i(P,Q)$ mod n und $V_i(P,Q)$ mod n oft für große Indizes i. Es ist klar, dass dann eine rekursive Berechnung über die Definition nicht mehr funktioniert. Wir stellen ein paar Berechnungsmöglichkeiten vor. Da wir nur einfache Rechenoperationen benutzen, formulieren wir alles allgemein für einen kommutativen Ring R.

Satz. *Sei R ein kommutativer Ring mit 1, seien $P, Q \in R$ und die Folgen U_i und V_i rekursiv definiert durch*

$$U_0 = 0, \quad U_1 = 1, \quad U_i = PU_{i-1} - QU_{i-2} \text{ für } i \geq 2$$

und

$$V_0 = 2, \quad V_1 = P, \quad V_i = PV_{i-1} - QV_{i-2} \text{ für } i \geq 2.$$

Dann gilt für $i \geq 1$

$$\begin{pmatrix} U_{i-1} \\ U_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix}^{i-1} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} V_{i-1} \\ V_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix}^{i-1} \begin{pmatrix} 2 \\ P \end{pmatrix},$$

und zusammengefasst

$$\begin{pmatrix} U_{i-1} & V_{i-1} \\ U_i & V_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix}^{i-1} \begin{pmatrix} 0 & 2 \\ 1 & P \end{pmatrix} \text{ für } i \geq 1.$$

Beweis: Die Rekursionsformeln liefern für $i \geq 1$

$$\begin{pmatrix} U_i \\ U_{i+1} \end{pmatrix} = \begin{pmatrix} U_i \\ PU_i - QU_{i-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix} \begin{pmatrix} U_{i-1} \\ U_i \end{pmatrix}$$

und

$$\begin{pmatrix} V_i \\ V_{i+1} \end{pmatrix} = \begin{pmatrix} V_i \\ PV_i - QV_{i-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix} \begin{pmatrix} V_{i-1} \\ V_i \end{pmatrix},$$

woraus dann die Behauptungen unter Beachtung der Startwerte durch Induktion folgen. ■

Bemerkung: Da man mit der square-and-multiply-Methode Potenzen von $\begin{pmatrix} 0 & 1 \\ -Q & P \end{pmatrix}$ im Matrizenring $\mathrm{M}_2(R)$ schnell berechnen kann, liefert der Satz eine schnelle Berechnungsmöglichkeit für $U_i(P,Q)$ und $V_i(P,Q)$ auch für große Indizes i.

Beispiel: Die größte 30-stellige Primzahl ist $p = 10^{30} - 11$. Wir wollen modulo p rechnen, d.h. wir nehmen als Grundring den Körper $\mathbb{F}_p$. Für $P = 2$, $Q = 3$ erhalten wir (mit SAGE)

$$\begin{pmatrix} 0 & 1 \\ -3 & 2 \end{pmatrix}^{10^{20}-1} \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 889597345267587290427270199194 & 160980762156610429185477053357 \\ 470087726345892505020008725878 & 602591381086261267476396256537 \end{pmatrix},$$

also

$$U_{10^{20}} = 470087726345892505020008725878 \quad \text{und} \quad V_{10^{20}} = 602591381086261267476396256537$$

(in $\mathbb{F}_p$, d.h. modulo p). Hier sind die SAGE-Befehle:

```
p=10^30-11
U,V=(Matrix(GF(p),[[0,1],[-3,2]])^(10^20-1)*Matrix([[0,2],[1,2]]))[1]
```

Wir haben zu diesem Berechnungsverfahren auch eine Python-Funktion geschrieben:

```
def UV_modn_1(i,P,Q,n):
  if i==0:
    return 0,2
  def mult(a,b):
    a11,a12,a21,a22=a
    b11,b12,b21,b22=b
    return [(a11*b11+a12*b21)%n,(a11*b12+a12*b22)%n,(a21*b11+a22*b21)%n,
            (a21*b12+a22*b22)%n]
  b=[1,0,0,1]
  c=[0,1,(-Q)%n,P%n]
  i=i-1
  while i>0:
    while i%2==0:
      c=mult(c,c)
      i=i//2
    b=mult(b,c)
    i=i-1
  _,_,U_i,V_i=mult(b,[0,2,1,P])
  return U_i,V_i
```

Der letzte Satz beruht darauf, dass man die Rekursionsformeln für die Lucas-Folgen in Matrizenform darstellen kann. Der folgende Ansatz kommt mit noch weniger Operationen aus, ist aber zunächst etwas algebraischer.

SATZ. *Sei R ein kommutativer Ring mit 1, $P, Q \in R$ und die Folgen U_i und V_i rekursiv definiert durch*

$$U_0 = 0, \quad U_1 = 1, \quad U_i = PU_{i-1} - QU_{i-2} \text{ für } i \geq 2$$

und

$$V_0 = 2, \quad V_1 = P, \quad V_i = PV_{i-1} - QV_{i-2} \text{ für } i \geq 2.$$

Sei X eine Unbestimmte über R, $S = R[X]/(X^2 - PX + Q)$ und ξ das Bild von X in S. Es gilt $\xi^2 = -Q + P\xi$. Dann hat man die direkte Summenzerlegung $S = R + R\xi$, insbesondere gibt es für $i \geq 1$ eindeutig bestimmte $a_i, b_i \in R$ mit

$$\xi^i = a_i + b_i\xi,$$

wobei wir auch noch $a_0 = 1$, $b_0 = 0$ definieren. Dann gilt für alle $i \geq 0$

$$U_i = b_i \quad \text{und} \quad V_i = 2a_i + Pb_i.$$

Beweis:

(1) Wir zeigen zunächst, dass

$$\xi^i = -QU_{i-1} + U_i\xi \text{ für } i \geq 1$$

gilt.

- Für $i = 1$ ist
$$\xi^1 = \xi = -Q \cdot 0 + 1 \cdot \xi = -QU_0 + U_1\xi.$$
- Für $i = 2$ ist (mit $U_2 = P$)
$$\xi^2 = -Q + P\xi = -Q \cdot 1 + P\xi = -QU_1 + U_2\xi.$$
- Sei nun $i \geq 3$ und die Behauptung bereits für $i-1$ und $i-2$ gezeigt. Es folgt
$$\begin{aligned} \xi^i &= \xi^{i-1} \cdot \xi = (-QU_{i-2} + U_{i-1}\xi)\xi = -QU_{i-2}\xi + U_{i-1}(-Q + P\xi) = \\ &= -QU_{i-1} + (PU_{i-1} - QU_{i-2})\xi = -QU_{i-1} + U_i\xi, \end{aligned}$$
sodass die Behauptung durch Induktion bewiesen ist.

Daher gilt

$$a_i = -QU_{i-1} \text{ für } i \geq 1 \quad \text{und} \quad b_i = U_i \text{ für } i \geq 1.$$

(2) Wir zeigen, dass

$$-2QU_{i-1} + PU_i = V_i \text{ für } i \geq 1$$

gilt.

- Für $i = 1$ ist die linke und rechte Seite jeweils P, die Aussage also richtig.
- Für $i = 2$ ist
$$-2QU_1 + PU_2 = -2Q + P^2 = P \cdot P - Q \cdot 2 = P \cdot V_1 - Q \cdot V_0 = V_2,$$
die Aussage also auch richtig.
- Sei nun $i \geq 3$ und die Aussage bereits für $i-1$ und $i-2$ gezeigt. Es folgt
$$\begin{aligned} -2QU_{i-1} + PU_i &= -2Q(PU_{i-2} - QU_{i-3}) + P(PU_{i-1} - QU_{i-2}) = \\ &= P \cdot (-2QU_{i-2} + PU_{i-1}) - Q \cdot (-2QU_{i-3} + PU_{i-2}) = \\ &= P \cdot V_{i-1} - Q \cdot V_{i-2} = V_i, \end{aligned}$$
sodass die Behauptung durch Induktion folgt.

(3) Nun gilt für $i \geq 1$ mit (1) und (2)

$$2a_i + Pb_i = -2QU_{i-1} + PU_i = V_i \quad \text{und} \quad b_i = U_i.$$

Für $i = 0$ ist

$$2a_0 + Pb_0 = 2 = V_0 \quad \text{und} \quad b_0 = 0 = U_0.$$

Damit ist alles bewiesen. ■

Bemerkungen:

(1) Wir verwenden die Bezeichnungen des Satzes. Da

$$S \to R \times R, \quad u + v\xi \mapsto (u, v)$$

eine Bijektion ist, können wir die Ringstruktur von S auf $R \times R$ übertragen: Das Produkt

$$\begin{aligned}(u_1 + v_1\xi)(u_2 + v_2\xi) &= u_1u_2 + (u_1v_2 + u_2v_1)\xi + v_1v_2\xi^2 = \\ &= u_1u_2 + (u_1v_2 + u_2v_1)\xi + v_1v_2(-Q + P\xi) = \\ &= (u_1u_2 - v_1v_2Q) + (u_1v_2 + u_2v_1 + v_1v_2P)\xi\end{aligned}$$

wird dann zu in $R \times R$ zu

$$(u_1, v_1) \cdot (u_2, v_2) = (u_1u_2 - v_1v_2Q, u_1v_2 + u_2v_1 + v_1v_2P).$$

Außerdem entspricht 1 dem Paar $(1, 0)$ und ξ entspricht $(0, 1)$. Mit den Bezeichnungen des Lemmas ist wegen $\xi^i = a_i + b_i\xi$ dann

$$(0, 1)^i = (a_i, b_i), \quad U_i = b_i, \quad V_i = 2a_i + Pb_i.$$

Mit der/einer square-and-multiply-Methode berechnen wir $(0, 1)^i$ und erhalten damit U_i und V_i:

Algorithmus zur Berechnung von $U_i(P, Q)$ und $V_i(P, Q)$:
Eingabe: Ring R, $P, Q \in R$ und $i \geq 0$
Ausgabe: $U_i(P, Q)$ und $V_i(P, Q)$

```
1: b ← (1,0), c ← (0,1)
2: while i > 0 do
3:     while i mod 2 = 0 do
4:         c ← c · c, i ← ⌊i/2⌋          ▷ Mit der oben definierten Multiplikation
5:     end while
6:     b ← b · c, i ← i − 1              ▷ Mit der oben definierten Multiplikation
7: end while
8: (a_i, b_i) ← b, U_i ← b_i, V_i ← 2a_i + Pb_i
9: return U_i, V_i
```

Das folgende Python-Programm benutzt obigen Algorithmus um $U_i(P, Q)$ mod n und $V_i(P, Q)$ mod n zu berechnen:

```
def UV_modn_2(i,P,Q,n):
  def mult(uv1,uv2):
    u1,v1=uv1
    u2,v2=uv2
    return [(u1*u2-v1*v2*Q)%n,(u1*v2+u2*v1+v1*v2*P)%n]
  b=[1,0]
  c=[0,1]
  while i>0:
    while i%2==0:
      c=mult(c,c)
      i=i//2
    b=mult(b,c)
    i=i-1
  a_i,b_i=b
  U_i,V_i=b_i,(2*a_i+P*b_i)%n
  return U_i,V_i
```

Wir werden nun noch eine weitere Berechnungsmöglichkeit entwickeln. Dazu stellen wir erst ein paar Formeln bereit:

LEMMA. *Es gilt für $U_i = U_i(P,Q)$, $V_i = V_i(P,Q)$ und $i \geq j \geq 0$*

$$\begin{aligned} U_{i+j} &= U_iV_j - Q^jU_{i-j}, \\ V_{i+j} &= V_iV_j - Q^jV_{i-j}. \end{aligned}$$

Beweis: Sind α, β die Nullstellen von $x^2 - Px + Q$ und $D = P^2 - 4Q$, so ist

$$U_i = \frac{\alpha^i - \beta^i}{\alpha - \beta} \text{ (im Fall } D \neq 0) \quad \text{und} \quad V_i = \alpha^i + \beta^i,$$

und wir erhalten für $i \geq j \geq 0$ mit $\alpha\beta = Q$

$$\begin{aligned} U_{i+j} &= \frac{\alpha^{i+j} - \beta^{i+j}}{\alpha - \beta} = \frac{\alpha^i\alpha^j - \beta^i\beta^j}{\alpha - \beta} = \frac{(\alpha^i - \beta^i)(\alpha^j + \beta^j) - (\alpha^i\beta^j - \alpha^j\beta^i)}{\alpha - \beta} = \\ &= \frac{(\alpha^i - \beta^i)(\alpha^j + \beta^j) - (\alpha\beta)^j(\alpha^{i-j} - \beta^{i-j})}{\alpha - \beta} = \frac{\alpha^i - \beta^i}{\alpha - \beta} \cdot (\alpha^j + \beta^j) - (\alpha\beta)^j \cdot \frac{\alpha^{i-j} - \beta^{i-j}}{\alpha - \beta} = \\ &= U_iV_j - Q^jU_{i-j}, \\ V_{i+j} &= \alpha^{i+j} + \beta^{i+j} = (\alpha^i + \beta^i)(\alpha^j + \beta^j) - (\alpha^i\beta^j + \alpha^j\beta^i) = \\ &= (\alpha^i + \beta^i)(\alpha^j + \beta^j) - (\alpha\beta)^j(\alpha^{i-j} + \beta^{i-j}) = V_iV_j - Q^jV_{i-j}. \end{aligned}$$

Wir müssen die Formel für U_{i+j} noch im Fall $D = 0$ zeigen. Mit $D = P^2 - 4Q$ gilt $Q = (\frac{P}{2})^2$ und

$$U_i = i \cdot \alpha^{i-1} \quad \text{und} \quad V_i = 2\alpha^i.$$

(Dabei ist $U_0 = 0$.) Es folgt

$$\begin{aligned} U_iV_j - Q^jU_{i-j} &= i \cdot \alpha^{i-1} \cdot 2 \cdot \alpha^j - (\alpha^2)^j \cdot (i-j) \cdot \alpha^{i-j-1} = 2i \cdot \alpha^{i+j-1} - (i-j) \cdot \alpha^{i+j-1} = \\ &= (i+j) \cdot \alpha^{i+j-1} = U_{i+j}, \end{aligned}$$

was noch zu zeigen war. ■

Für nachfolgende Anwendung brauchen wir nur einen Spezialfall:

LEMMA. *Es gilt für $U_k = U_k(P,Q)$ und $V_k = V_k(P,Q)$*

$$\begin{aligned} U_{2k} &= U_kV_k, & U_{2k-1} &= U_kV_{k-1} - Q^{k-1}, \\ V_{2k} &= V_k^2 - 2Q^k, & V_{2k-1} &= V_kV_{k-1} - PQ^{k-1}. \end{aligned}$$

Beweis: Wir wenden einfach das vorangegangene Lemma an:

$$\begin{aligned} U_{2k} &= U_{k+k} = U_kV_k - Q^kU_{k-k} = U_kV_k, \\ U_{2k-1} &= U_{k+(k-1)} = U_kV_{k-1} - Q^{k-1}U_{k-(k-1)} = U_kV_{k-1} - Q^{k-1}, \\ V_{2k} &= V_{k+k} = V_kV_k - Q^kV_{k-k} = V_k^2 - Q^k \cdot 2, \\ V_{2k-1} &= V_{k+(k-1)} = V_kV_{k-1} - Q^{k-1}V_{k-(k-1)} = V_kV_{k-1} - Q^{k-1} \cdot P. \end{aligned}$$

Dies war zu zeigen. ■

Beispiele: Wir wollen die Formeln des Lemmas benutzen um U_i und V_i auch für größere Indizes zu berechnen.

(1) Wir wollen U_{100} und V_{100} berechnen. Wir ordnen das Vorgehen zunächst tabellenartig an:

Anwendung der Formeln	Wir brauchen
$U_{100} = U_{50}V_{50}$, $V_{100} = V_{50}^2 - 2Q^{50}$	U_{50}, V_{50}, Q^{50}
$U_{50} = U_{25}V_{25}$, $V_{50} = V_{25}^2 - 2Q^{25}$	U_{25}, V_{25}, Q^{25}
$U_{25} = U_{13}V_{12} - Q^{12}$, $V_{25} = V_{13}V_{12} - PQ^{12}$	U_{13}, V_{13}, V_{12}, Q^{12}
$U_{13} = U_7V_6 - Q^6$, $V_{13} = V_7V_6 - PQ^6$, $V_{12} = V_6^2 - 2Q^6$	U_7, V_7, V_6, Q^6
$U_7 = U_4V_3 - Q^3$, $V_7 = V_4V_3 - PQ^3$, $V_6 = V_3^2 - 2Q^3$	U_4, V_4, V_3, Q^3
$U_4 = U_2V_2$, $V_4 = V_2^2 - 2Q^2$, $V_3 = V_2V_1 - PQ$	U_2, V_2, V_1, Q
$U_2 = U_1V_1$, $V_2 = V_1^2 - 2Q$	U_1, V_1, Q

Wegen $U_1 = 1$, $V_1 = P$ kann man nun die Formeln von unten nach oben lesen und damit U_{100} und V_{100} berechnen.

(2) Nun wollen wir U_{231} und V_{231} berechnen:

Anwendung der Formeln	Wir brauchen
$U_{231} = U_{116}V_{115} - Q^{115}$, $V_{231} = V_{116}V_{115} - PQ^{115}$	U_{116}, V_{116}, V_{115}, Q^{115}
$U_{116} = U_{58}V_{58}$, $V_{116} = V_{58}^2 - 2Q^{58}$, $V_{115} = V_{58}V_{57} - PQ^{57}$	U_{58}, V_{58}, V_{57}, Q^{57}
$U_{58} = U_{29}V_{29}$, $V_{58} = V_{29}^2 - 2Q^{29}$, $V_{57} = V_{29}V_{28} - PQ^{28}$	U_{29}, V_{29}, V_{28}, Q^{28}
$U_{29} = U_{15}V_{14} - Q^{14}$, $V_{29} = V_{15}V_{14} - PQ^{14}$, $V_{28} = V_{14}^2 - 2Q^{14}$	U_{15}, V_{15}, V_{14}, Q^{14}
$U_{15} = U_8V_7 - Q^7$, $V_{15} = V_8V_7 - PQ^7$, $V_{14} = V_7^2 - 2Q^7$	U_8, V_8, V_7, Q^7
$U_8 = U_4V_4$, $V_8 = V_4^2 - 2Q^4$, $V_7 = V_4V_3 - PQ^3$	U_4, V_4, V_3, Q^3
$U_4 = U_2V_2$, $V_4 = V_2^2 - 2Q^2$, $V_3 = V_2V_1 - PQ$	U_2, V_2, V_1, Q
$U_2 = U_1V_1$, $V_2 = V_1^2 - 2Q$	U_1, V_1, Q

Wieder erhält man U_{231}, V_{231}, indem man die Formeln von unten nach oben liest und $U_1 = 1$, $V_1 = P$ einsetzt.

Überlegungen:

(1) Die Beispiele deuten an, dass es in den vorangegangenen Tabellen sinnvoll ist, sich neben U_j, V_j auch V_{j-1} und Q^{j-1} zu merken. Wir betrachten also 4-Tupel

$$(U_j, V_j, V_{j-1}, Q^{j-1}).$$

Wir führen dafür die Bezeichung (u_j, v_j, w_j, q_j) ein, d.h.

$$(u_j, v_j, w_j, q_j) = (U_j, V_j, V_{j-1}, Q^{j-1}).$$

Nun unterscheiden wir zwei Fälle:

- **Fall $j \equiv 0 \bmod 2$:** Wir schreiben $j = 2k$. Dann ist also $k = \frac{j}{2} = \left\lfloor \frac{j+1}{2} \right\rfloor$. Wir brauchen die Formeln

$$U_{2k} = U_kV_k, \quad V_{2k} = V_k^2 - 2Q^k, \quad V_{2k-1} = V_kV_{k-1} - PQ^{k-1}$$

des vorangegangenen Lemmas. Dann gilt also

$$U_j = U_kV_k, \quad V_j = V_k^2 - 2Q \cdot Q^{k-1}, \quad V_{j-1} = V_kV_{k-1} - P \cdot Q^{k-1}, \quad Q^{j-1} = Q \cdot (Q^{k-1})^2$$

bzw. mit $(u_k, v_k, w_k, q_k) = (U_k, V_k, V_{k-1}, Q^{k-1})$

$$(u_j, v_j, w_j, q_j) = (u_kv_k, v_k^2 - 2Qq_k, v_kw_k - Pq_k, Qq_k^2).$$

- **Fall $j \equiv 1 \bmod 2$:** Wir schreiben $j = 2k - 1$. Dann ist $k = \frac{j+1}{2} = \left\lfloor \frac{j+1}{2} \right\rfloor$. Wir brauchen die Formeln

$$U_{2k-1} = U_kV_{k-1} - Q^{k-1}, \quad V_{2k-1} = V_kV_{k-1} - PQ^{k-1}, \quad V_{2k-2} = V_{k-1}^2 - 2Q^{k-1}.$$

Also

$$U_j = U_kV_{k-1} - Q^{k-1}, \quad V_j = V_kV_{k-1} - P \cdot Q^{k-1}, \quad V_{j-1} = V_{k-1}^2 - 2Q^{k-1}, \quad Q^{j-1} = (Q^{k-1})^2$$

bzw.

$$(u_j, v_j, w_j, q_j) = (u_kw_k - q_k, v_kw_k - Pq_k, w_k^2 - 2q_k, q_k^2).$$

Es ist

$$(u_1, v_1, w_1, q_1) = (U_1, V_1, V_0, Q^0) = (1, P, 2, 1).$$

(2) Wir wollen U_i, V_i für einen Index $i \geq 2$ berechnen. Wir definieren zugehörig rekursiv eine Folge $j_1, j_2, \ldots, j_\ell$ wie folgt:

$$j_1 = i \quad \text{und} \quad j_{\alpha+1} = \left\lfloor \frac{j_\alpha + 1}{2} \right\rfloor \quad \text{bis } j_\ell = 1 \text{ erreicht ist.}$$

Wir nehmen an, wir kennen bereits

$$(u_{j_{\alpha+1}}, v_{j_{\alpha+1}}, w_{j_{\alpha+1}}, q_{j_{\alpha+1}}),$$

was für $\alpha = \ell - 1$ der Fall ist. Wir unterscheiden zwei Fälle:

- Ist $j_\alpha \equiv 0 \bmod 2$, dann können wir obige Formeln für $j = j_\alpha$, $k = j_{\alpha+1}$ anwenden:
$$(u_j, v_j, w_j, q_j) = (u_k v_k, v_k^2 - 2Qq_k, v_k w_k - Pq_k, Qq_k^2),$$
also
$$(u_{j_\alpha}, v_{j_\alpha}, w_{j_\alpha}, q_{j_\alpha}) = (u_{j_{\alpha+1}} v_{j_{\alpha+1}}, v_{j_{\alpha+1}}^2 - 2Qq_{j_{\alpha+1}}, v_{j_{\alpha+1}} w_{j_{\alpha+1}} - Pq_{j_{\alpha+1}}, Qq_{j_{\alpha+1}}^2).$$
- Ist $j_\alpha \equiv 1 \bmod 2$, dann können wir obige Formeln für $j = j_\alpha$, $k = j_{\alpha+1}$ anwenden:
$$(u_j, v_j, w_j, q_j) = (u_k v_k - q_k, v_k w_k - Pq_k, w_k^2 - 2q_k, q_k^2),$$
also
$$(u_{j_\alpha}, v_{j_\alpha}, w_{j_\alpha}, q_{j_\alpha}) = (u_{j_{\alpha+1}} v_{j_{\alpha+1}} - q_{j_{\alpha+1}}, v_{j_{\alpha+1}} w_{j_{\alpha+1}} - Pq_{j_{\alpha+1}}, w_{j_{\alpha+1}}^2 - 2q_{j_{\alpha+1}}, q_{j_{\alpha+1}}^2).$$

Wir sind fertig, wenn wir bei $j_1 = i$ angelangt sind.

Beispiel: Wir wollen $U_{79}(2,5)$ und $V_{79}(2,5)$ berechnen. Die j-Folge ist

$$j_1 = 79, \quad j_2 = 40, \quad j_3 = 20, \quad j_4 = 10, \quad j_5 = 5, \quad j_6 = 3, \quad j_7 = 2, \quad j_8 = 1.$$

Wir legen eine Tabelle und schreiben $j_8, j_7, \ldots, j_1$ in die erste Spalte. In die erste Zeile kommt $(u_1, v_1, w_1, q_1) = (1, 2, 2, 1)$. Dann verwenden wir die oben angegebenen Formeln um von einer Zeile zur nächsten zu kommen.

j	(u_j, v_j, w_j, q_m)
1	(1, 2, 2, 1)
2	(2, -6, 2, 5)
3	(-1, -22, -6, 25)
5	(-19, 82, -14, 625)
10	(-1558, 474, -2398, 1953125)
20	(-738492, -19306574, -5042902, 19073486328125)
40	(14257750446408, 182008936336226, 59214187981498, 1818989403545856475830078125)
79	(-974728288418966137885518941, 713953256343407528273499029 8, -131…, 330…)

Es gilt also

$$U_{79}(2,5) = -974728288418966137885518941, \quad V_{79}(2,5) = 713953256343407528273499029 8.$$

Wir erhalten folgenden Algorithmus:

Algorithmus zur Berechnung von $U_i(P,Q)$ und $V_i(P,Q)$:
Eingabe: P, Q und $i \geq 0$
Ausgabe: $U_i(P,Q)$ und $V_i(P,Q)$

```
if i = 0 then
    return 0, 2
end if
j ← i, J ← []
while j > 1 do
    Hänge j an J an
    j ← ⌊(j+1)/2⌋
end while
u, v, w, q ← 1, P, 2, 1
while J ≠ [] do
    Sei j das letzte Element von J, streiche es anschließend aus J
    if j ≡ 0 mod 2 then
        u, v, w, q ← uv, v^2 − 2Qq, vw − Pq, Qq^2
    else
        u, v, w, q ← uw − q, vw − Pq, w^2 − 2q, q^2
    end if
end while
return u, v
```

Hier ist eine zugehörige Python-Funktion:

```
def UV_modn_3(i,P,Q,n):
  if i==0:
    return 0,2
  j=i
  J=[]
  while j>1:
    J.append(j%2)
    j=(j+1)//2
  u,v,w,q=1,P%n,2%n,1
  while J!=[]:
    j=J.pop()
    if j==0:
      u,v,w,q=u*v%n,(v*v-2*Q*q)%n,(v*w-P*q)%n,Q*q*q%n
    else:
      u,v,w,q=(u*w-q)%n,(v*w-P*q)%n,(w*w-2*q)%n,q*q%n
  return u,v
```

Bemerkung: Wir haben drei Methoden beschrieben, wie man effektiv $U_i(P,Q)$ mod n und $V_i(P,Q)$ mod n berechnen kann. Wie schnell sind die Methoden im Vergleich?
Wir haben jeweils 100 Zahlen i, P, Q, n mit 4096 Bit gewählt und dann $U_i(P,Q)$ mod n und $V_i(P,Q)$ mod n berechnet.

Funktion	`UV_modn_1(i,P,Q,n)`	`UV_modn_2(i,P,Q,n)`	`UV_modn_3(i,P,Q,n)`
1. Durchlauf	93.80 sec	99.76 sec	60.76 sec
2. Durchlauf	94.02 sec	99.99 sec	60.72 sec
3. Durchlauf	93.15 sec	99.23 sec	60.64 sec

Man sieht, dass die 3. Methode am schnellsten ist.

3. Die „Nullstellenmengen“ der Lucas-Folgen $(U_i(P,Q))_{i\geq 1}$

Wir interessieren uns hier für die „Nullstellenmengen“ einer Lucas-Folge $(U_i(P,Q))_{i\geq 0}$, also bei gegebenem Parameterpaar (P,Q) für

$$\{i \in \mathbb{N}_0 : U_i(P,Q) = 0\}.$$

(Wegen $U_0(P,Q) = 0$ und $U_1(P,Q) = 1$ ist 0 immer Element dieser Menge, 1 nie.) Kann man $U_i(P,Q)$ in der Form $\frac{\alpha^i-\beta^i}{\alpha-\beta}$ schreiben, so ist die Diskussion recht einfach. Darum unterscheiden wir zwei Fälle.

LEMMA. *Sei $P, Q \in \mathbb{Z}$ mit $D = P^2 - 4Q \neq 0$ und $Q \neq 0$. Dann gilt für*

$$\alpha = \frac{P+\sqrt{D}}{2} \quad \text{und} \quad \beta = \frac{P-\sqrt{D}}{2}$$

$\alpha \neq 0$, $\beta \neq 0$, $\alpha \neq \beta$ und

$$U_i(P,Q) = \frac{\alpha^i - \beta^i}{\alpha - \beta} \text{ für alle } i \geq 0.$$

(1) *Es gilt:*

$$\{i \in \mathbb{N}_0 : U_i(P,Q) = 0\} = \{i \in \mathbb{N}_0 : (\frac{\alpha}{\beta})^i = 1\}.$$

(2) *Existiert ein $k \in \mathbb{N}$ mit $(\frac{\alpha}{\beta})^k = 1$ und ist k minimal mit dieser Eigenschaft, so ist*

$$\{i \in \mathbb{N}_0 : U_i(P,Q) = 0\} = \mathbb{N}_0 \cdot k$$

und

$$k \in \{2, 3, 4, 6\}.$$

Außerdem gilt:

$$\begin{aligned} k=2 &\iff P=0,\\ k=3 &\iff P^2=Q,\\ k=4 &\iff P^2=2Q,\\ k=6 &\iff P^2=3Q. \end{aligned}$$

Beweis:

(1) Die Darstellung $U_i(P,Q)=\frac{\alpha^i-\beta^i}{\alpha-\beta}$ und $\alpha\neq 0$, $\beta\neq 0$, $\alpha\neq\beta$ haben wir bereits früher gesehen. Damit folgt:

$$U_i(P,Q)=0 \quad\iff\quad \alpha^i=\beta^i \quad\iff\quad (\frac{\alpha}{\beta})^i=1.$$

(2) Sei also $k\in\mathbb{N}$ mit $(\frac{\alpha}{\beta})^k=1$ und k minimal mit dieser Eigenschaft.

(a) Mit (1) ist

$$\mathbb{N}_0\cdot k\subseteq\{i\in\mathbb{N}_0 : U_i(P,Q)=0\}$$

klar. Sei umgekehrt $i\in\mathbb{N}_0$ mit $U_i(P,Q)=0$, also $(\frac{\alpha}{\beta})^i=1$. Wir dividieren i durch k und erhalten eine Darstellung $i=qk+r$ mit $q,r\in\mathbb{N}_0$ und $0\leq r\leq k-1$. Es folgt

$$1=(\frac{\alpha}{\beta})^i=((\frac{\alpha}{\beta})^k)^q(\frac{\alpha}{\beta})^r=(\frac{\alpha}{\beta})^r.$$

Wegen $0\leq r\leq k-1$ und der Minimalität von k folgt $r=0$ und damit $i=qk\in\mathbb{N}_0\cdot k$, was noch zu zeigen war.

(b) Ist $k\in\mathbb{N}$ minimal mit $(\frac{\alpha}{\beta})^k=1$, so ist $\frac{\alpha}{\beta}$ eine primitive k-te Einheitswurzeln. Da $\frac{\alpha}{\beta}\in\mathbb{Q}(\sqrt{D})$ gilt, ist $\frac{\alpha}{\beta}$ höchstens quadratisch über $\mathbb{Q}$. Nun weiß man, dass dann $k\in\{1,2,3,4,6\}$ gilt, die zugehörigen Einheitswurzeln sind

$$1,\quad -1,\quad \frac{-1\pm\sqrt{-3}}{2},\quad \pm\sqrt{-1},\quad \frac{1\pm\sqrt{-3}}{2}$$

mit den Minimalpolynomen

$$x-1,\quad x+1,\quad x^2+x+1,\quad x^2+1,\quad x^2-x+1.$$

Wir gehen nun die einzelnen Möglichkeiten durch:

(i) $k=1$: Der Fall $\frac{\alpha}{\beta}=1$ ist wegen der Voraussetzung $\alpha\neq\beta$ hier nicht möglich.

(ii) $k=2$: Die Bedingung $\frac{\alpha}{\beta}=-1$ ist äquivalent zu $P=\alpha+\beta=0$.

(iii) $k=3$: $\frac{\alpha}{\beta}$ ist genau dann eine primitive 3-te Einheitswurzel, wenn gilt $(\frac{\alpha}{\beta})^2+\frac{\alpha}{\beta}+1=0$, was sich auch in der Form $\alpha^2+\alpha\beta+\beta^2=0$ formulieren lässt. Nun gilt aber

$$\alpha^2+\alpha\beta+\beta^2=(\alpha+\beta)^2-\alpha\beta=P^2-Q,$$

sodass sich die Bedingung auch als $P^2=Q$ schreiben lässt.

(iv) $k=4$: $\frac{\alpha}{\beta}$ ist genau dann eine primitive 4-te Einheitswurzel, wenn gilt $(\frac{\alpha}{\beta})^2+1=0$ bzw. $\alpha^2+\beta^2=0$. Wegen

$$\alpha^2+\beta^2=(\alpha+\beta)^2-2\alpha\beta=P^2-2Q$$

lässt sich die Bedingung auch in der Form $P^2=2Q$ formulieren.

(v) $k=6$: $\frac{\alpha}{\beta}$ ist genau dann eine primitive 6-te Einheitswurzel, wenn gilt $(\frac{\alpha}{\beta})^2-\frac{\alpha}{\beta}+1=0$, was sich auch in der Form $\alpha^2-\alpha\beta+\beta^2=0$ formulieren lässt. Nun gilt aber

$$\alpha^2-\alpha\beta+\beta^2=(\alpha+\beta)^2-3\alpha\beta=P^2-3Q,$$

sodass sich die Bedingung auch als $P^2=3Q$ schreiben lässt. ■

LEMMA. *Für $P,Q\in\mathbb{Z}$ mit $D=P^2-4Q=0$ oder $Q=0$ gilt:*

$$\{i\in\mathbb{N}_0 : U_i(P,Q)\}\neq\{0\} \quad\iff\quad (P,Q)=(0,0).$$

Im Fall $(P,Q)=(0,0)$ gilt

$$\{i\in\mathbb{N}_0 : U_i(0,0)=0\}=\{0\}\cup\mathbb{N}_{\geq 2}.$$

Beweis:

(1) **Fall** $P^2 - 4Q = 0$**:** Hier ist $U_1(P,Q) = 1$ und

$$U_i(P,Q) = i \cdot (\frac{P}{2})^{i-1} \text{ für } i \geq 2.$$

Ist also $U_i = 0$ für ein $i \geq 1$, so folgt bereits $P = Q = 0$ und

$$U_i(0,0) = \begin{cases} 0 & \text{für } i \neq 1, \\ 1 & \text{für } i = 1. \end{cases}$$

(2) **Fall** $Q = 0$**:** Hier ist

$$U_i(P,0) = \begin{cases} 0 & \text{für } i = 0, \\ 1 & \text{für } i = 1, \\ P^{i-1} & \text{für } i \geq 2. \end{cases}$$

Ist also $U_i =$ für ein $i \geq 1$, so folgt $P = Q = 0$. Dieser Fall wurde bereits oben erwähnt. ■

Wir fassen nochmals zusammen:

SATZ. *Für $P, Q \in \mathbb{Z}$ gilt:*

$$\{i \in \mathbb{N}_0 : U_i(P,Q) = 0\} = \begin{cases} \{0\} \cup \mathbb{N}_{\geq 2} & \textit{für } (P,Q) = (0,0), \\ \mathbb{N}_0 \cdot 2 & \textit{für } P = 0, Q \neq 0, \\ \mathbb{N}_0 \cdot 3 & \textit{für } P^2 - Q = 0, Q \neq 0, \\ \mathbb{N}_0 \cdot 4 & \textit{für } P^2 - 2Q = 0, Q \neq 0, \\ \mathbb{N}_0 \cdot 6 & \textit{für } P^2 - 3Q = 0, Q \neq 0, \\ \{0\} & \textit{sonst .} \end{cases}$$

Beispiele:

(P,Q)	$U_i(P,Q)$ für $0 \leq i \leq 20$
$(0,0)$	0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
$(0,1)$	0, 1, 0, -1, 0, 1, 0, -1, 0, 1, 0, -1, 0, 1, 0, -1, 0, 1, 0, -1, 0
$(1,1)$	0, 1, 1, 0, -1, -1, 0, 1, 1, 0, -1, -1, 0, 1, 1, 0, -1, -1, 0, 1, 1
$(2,2)$	0, 1, 2, 2, 0, -4, -8, -8, 0, 16, 32, 32, 0, -64, -128, -128, 0, 256, 512, 512, 0
$(3,3)$	0, 1, 3, 6, 9, 9, 0, -27, -81, -162, -243, -243, 0, 729, 2187, 4374, 6561, 6561, 0, -19683, -59049

4. Lucas-Folgen modulo p

Wir untersuchen hier Eigenschaften der von $U_i(P,Q) \bmod p$ und $V_i(P,Q) \bmod p$ für Primzahlen p.

LEMMA. *Sei p eine ungerade Primzahl, $\mathbb{F}_p$ der endliche Körper mit p Elementen und $\overline{\mathbb{F}}_p$ sein algebraischer Abschluss. Seien weiter $P, Q \in \mathbb{F}_p$ mit $D = P^2 - 4Q \neq 0$ und $Q \neq 0$. Rekursiv seien in $\mathbb{F}_p$ Folgen $(U_i)_{i \geq 0}$ und $(V_i)_{i \geq 0}$ durch folgende Vorschriften definiert:*

$$U_0 = 0, \quad U_1 = 1, \quad U_i = PU_{i-1} - QU_{i-2} \textit{ für } i \geq 2,$$

$$V_0 = 2, \quad V_1 = P, \quad V_n = PV_{i-1} - QV_{i-2} \textit{ für } i \geq 2.$$

Seien α, β die Nullstellen des Polynoms $x^2 - Px + Q$ im algebraischen Abschluss $\overline{\mathbb{F}}_p$, d.h. $x^2 - Px + Q = (x - \alpha)(x - \beta)$. Dann gilt:

(1) *Für $a, b \in \overline{\mathbb{F}}_p$ ist*

$$(a + b)^p = a^p + b^p.$$

Für $c \in \overline{\mathbb{F}}_p$ gilt folgende Charakterisierung:

$$c \in \mathbb{F}_p \quad \Longleftrightarrow \quad c^p = c.$$

(2) *Es gilt* $P = \alpha + \beta$, $Q = \alpha\beta$ *und* $D = (\alpha - \beta)^2$. *O.E. kann man* $\sqrt{D} = \alpha - \beta$ *wählen. (Da* $D \neq 0$ *vorausgesetzt war, ist* $\alpha \neq \beta$. *Da* $Q \neq 0$ *vorausgesetzt war, ist* $\alpha \neq 0$, $\beta \neq 0$.*) Dann gilt*

$$\alpha = \frac{P + \sqrt{D}}{2} \quad \textit{und} \quad \beta = \frac{P - \sqrt{D}}{2}.$$

(3) *Für* $i \geq 0$ *gilt*

$$U_i = \frac{\alpha^i - \beta^n}{\alpha - \beta} \quad \textit{und} \quad V_i = \alpha^i + \beta^i.$$

(4) *Ist* $\left(\frac{D}{p}\right) = 1$ *(Legendre-Symbol), so ist* $\sqrt{D}^p = \sqrt{D}$, $\alpha^p = \alpha$, $\beta^p = \beta$, $\alpha^{p-1} = 1$, $\beta^{p-1} = 1$ *und*

$$U_{k(p-1)} = 0, \quad V_{k(p-1)} = 2 \textit{ für alle } k \in \mathbb{N}_0.$$

(5) *Ist* $\left(\frac{D}{p}\right) = -1$ *(Legendre-Symbol), so ist* $\sqrt{D}^p = -\sqrt{D}$, $\alpha^p = \beta$, $\beta^p = \alpha$, $\alpha^{p+1} = Q$, $\beta^{p+1} = Q$ *und*

$$U_{k(p+1)} = 0, \quad V_{k(p+1)} = 2Q^k \textit{ für alle } k \in \mathbb{N}_0.$$

(6) *Zerlegt man* $p - \left(\frac{D}{p}\right) = 2^\ell u$ *mit* $u \equiv 1 \bmod 2$, *so gilt*

$$U_u = 0 \quad \textit{oder} \quad V_{2^i u} = 0 \textit{ für ein } i \in \{0, \ldots, \ell - 1\}.$$

(7) *Bezeichnet* $\operatorname{ord}(\frac{\alpha}{\beta})$ *die (multiplikative) Ordnung von* $\frac{\alpha}{\beta}$ *in* $\overline{\mathbb{F}}_p$, *d.h.*

$$\operatorname{ord}(\frac{\alpha}{\beta}) = \min\{m \in \mathbb{N} : (\frac{\alpha}{\beta})^m = 1\},$$

so gilt

$$\operatorname{ord}(\frac{\alpha}{\beta}) \mid p - \left(\frac{D}{p}\right) \quad \textit{und} \quad \{i \in \mathbb{N}_0 : U_i = 0\} = \mathbb{N}_0 \cdot \operatorname{ord}(\frac{\alpha}{\beta}).$$

Beweis:

(1) (Dies sind grundlegende Aussagen in der Theorie der endlichen Körper.)

(2) Nach Definition von α und β gilt

$$x^2 - Px + Q = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta,$$

sodass Koeffizientenvergleich sofort $P = \alpha + \beta$ und $Q = \alpha\beta$ liefert. (Da $Q \neq 0$ vorausgesetzt war, folgt $\alpha \neq 0$, $\beta \neq 0$.) Damit gilt

$$D = P^2 - 4Q = (\alpha + \beta)^2 - 4\alpha\beta = (\alpha - \beta)^2.$$

Die Voraussetzung $D \neq 0$ zeigt, dass $\alpha \neq \beta$ ist. Wegen $D = (\alpha - \beta)^2$ gilt $\sqrt{D} = \pm(\alpha - \beta)$ (für die Wurzel von D). Die die Wurzel nur bis aufs Vorzeichen bestimmt ist, können wir o.E. $\sqrt{D} = \alpha - \beta$ annehmen. Addiert bzw. subtrahiert man die Gleichungen $\alpha + \beta = P$, $\alpha - \beta = \sqrt{D}$ und dividiert dann durch 2, so erhält man

$$\alpha = \frac{P + \sqrt{D}}{2} \text{ und } \beta = \frac{P - \sqrt{D}}{2}.$$

(3) Dies beweist man durch Induktion genauso wie bei den „gewöhnlichen“ Lucas-Folgen in $\mathbb{Z}$.

(4) *Fall* $\left(\frac{D}{p}\right) = 1$*:* Mit Euler gilt

$$1 = \left(\frac{D}{p}\right) = D^{\frac{p-1}{2}} = ((\sqrt{D})^2)^{\frac{p-1}{2}} = \sqrt{D}^{p-1}, \quad \text{also} \quad \sqrt{D}^p = \sqrt{D}.$$

Mit (1) und $P^p = P$, $2^p = 2$ folgt

$$\alpha^p = \left(\frac{P + \sqrt{D}}{2}\right)^p = \frac{P^p + \sqrt{D}^p}{2^p} = \frac{P + \sqrt{D}}{2} = \alpha$$

und

$$\beta^p = \left(\frac{P - \sqrt{D}}{2}\right)^p = \frac{P^p - \sqrt{D}^p}{2^p} = \frac{P - \sqrt{D}}{2} = \beta.$$

Wegen $\alpha, \beta \neq 0$ folgt aus $\alpha^p = \alpha$ und $\beta^p = \beta$ sofort $\alpha^{p-1} = 1$ und $\beta^{p-1} = 1$. Für $k \in \mathbb{N}_0$ erhält man durch Potenzieren

$$\alpha^{k(p-1)} = 1 \text{ und } \beta^{k(p-1)} = 1.$$

Damit wird

$$U_{k(p-1)} = \frac{\alpha^{k(p-1)} - \beta^{k(p-1)}}{\alpha - \beta} = \frac{1-1}{\alpha - \beta} = 0 \text{ und } V_{k(p-1)} = \alpha^{k(p-1)} + \beta^{k(p-1)} = 1 + 1 = 2.$$

Wir bemerken auch noch die Beziehung

$$(\frac{\alpha}{\beta})^{p-1} = 1.$$

(5) *Fall* $\left(\frac{D}{p}\right) = -1$*:* Mit Euler gilt

$$-1 = \left(\frac{D}{p}\right) = D^{\frac{p-1}{2}} = ((\sqrt{D})^2)^{\frac{p-1}{2}} = \sqrt{D}^{p-1}, \quad \text{also} \quad \sqrt{D}^p = -\sqrt{D}.$$

Wir zuvor berechnen wir

$$\alpha^p = \left(\frac{P + \sqrt{D}}{2}\right)^p = \frac{P^p + \sqrt{D}^p}{2^p} = \frac{P - \sqrt{D}}{2} = \beta$$

und

$$\beta^p = \left(\frac{P - \sqrt{D}}{2}\right)^p = \frac{P^p - \sqrt{D}^p}{2^p} = \frac{P + \sqrt{D}}{2} = \alpha.$$

Es folgt

$$\alpha^{p+1} = \alpha\alpha^p = \alpha\beta = Q \text{ und } \beta^{p+1} = \beta^p\beta = \alpha\beta = Q.$$

Potenzieren mit $k \in \mathbb{N}_0$ ergibt dann

$$\alpha^{k(p+1)} = Q^k \text{ und } \beta^{k(p+1)} = Q^k.$$

Eingesetzt in die Formeln aus (3) liefert

$$U_{k(p+1)} = \frac{\alpha^{k(p+1)} - \beta^{k(p+1)}}{\alpha - \beta} = \frac{Q^k - Q^k}{\alpha - \beta} = 0 \text{ und } V_{k(p+1)} = \alpha^{k(p+1)} + \beta^{k(p+1)} = Q^k + Q^k = 2Q^k.$$

Dies war zu zeigen. Wir bemerken auch noch die Beziehung

$$(\frac{\alpha}{\beta})^{p+1} = 1.$$

(6) Die letzten Formeln in (4) und (5) können wir zusammengefasst auch in der Form

$$(\frac{\alpha}{\beta})^{p-\left(\frac{D}{p}\right)} = 1$$

schreiben. Ist nun $p - \left(\frac{D}{p}\right) = 2^\ell u$ mit $u \equiv 1 \bmod 2$, so folgt

$$(\frac{\alpha}{\beta})^{2^\ell u} = 1.$$

Genau wie bei der Herleitung des Miller-Rabin-Tests folgt

$$(\frac{\alpha}{\beta})^u = 1 \quad \text{oder} \quad (\frac{\alpha}{\beta})^{2^i u} = -1 \text{ für ein } i \in \{0, \ldots, \ell - 1\},$$

was sich auch in der Form

$$\alpha^u - \beta^u = 0 \quad \text{oder} \quad \alpha^{2^i u} + \beta^{2^i u} = 0 \text{ für ein } i \in \{0, \ldots, \ell - 1\}$$

schreiben lässt. Dies bedeutet aber

$$U_u = 0 \quad \text{oder} \quad V_{2^i u} = 0 \text{ für ein } i \in \{0, \ldots, \ell - 1\}.$$

Dies wollten wir zeigen.

(7) Wie üblich folgt aus der gezeigten Beziehung $(\frac{\alpha}{\beta})^{p-\left(\frac{D}{p}\right)} = 1$ sofort

$$\operatorname{ord}(\frac{\alpha}{\beta}) \mid p - \left(\frac{D}{p}\right).$$

Die zweite Aussage ergibt sich (mit den üblichen Rechenregeln für Ordnungen) so:

$$\begin{aligned} U_i = 0 \quad &\iff \quad \frac{\alpha^i - \beta^i}{\alpha - \beta} = 0 \quad \iff \quad \alpha^i = \beta^i \quad \iff \quad (\frac{\alpha}{\beta})^i = 1 \quad \iff \\ &\iff \quad \operatorname{ord}(\frac{\alpha}{\beta}) \mid i \quad \iff \quad i \in \mathbb{N}_0 \cdot \operatorname{ord}(\frac{\alpha}{\beta}). \end{aligned}$$

Dies war zu zeigen. ■

Ist p eine Primzahl, sind $a, b \in \mathbb{Z}$ und $\overline{a}, \overline{b}$ die Bilder in $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$, so gilt

$$a \equiv b \bmod p \quad \iff \quad \overline{a} = \overline{b} \quad (\text{in } \mathbb{F}_p).$$

Damit können wir das vorangegangene Lemma sofort in Kongruenzen modulo p übersetzen:

Satz. *Sei p eine ungerade Primzahl, seien $P, Q \in \mathbb{Z}$, $D = P^2 - 4Q$ mit $D \not\equiv 0 \bmod p$, $Q \not\equiv 0 \bmod p$. (Die Bedingungen können auch zu $\operatorname{ggT}(p, 2QD) = 1$ zusammengefasst werden.)*

(1) *Es gilt für alle $k \in \mathbb{N}_0$*

$$U_{k(p-\left(\frac{D}{p}\right))}(P,Q) \equiv 0 \bmod p \quad \textit{und} \quad V_{k(p-\left(\frac{D}{p}\right))}(P,Q) \equiv \begin{cases} 2 \bmod p & \textit{im Fall } \left(\frac{D}{p}\right) = 1, \\ 2Q^k \bmod p & \textit{im Fall } \left(\frac{D}{p}\right) = -1. \end{cases}$$

(2) *Zerlegt man $p - \left(\frac{D}{p}\right) = 2^\ell u$ mit $u \equiv 1 \bmod 2$, so gilt*

$$U_u(P,Q) \equiv 0 \bmod p \quad \textit{oder} \quad V_{2^i u}(P,Q) \equiv 0 \bmod p \textit{ für ein } i \in \{0, \ldots, \ell - 1\}.$$

Beispiele: Da die Eigenschaften (1) des Satzes immer gilt, schauen wir uns nur Eigenschaft (2) an. Der Satz sagt, dass in der letzten Spalte eine 0 vorkommen muss.

p	P	Q	D	$\left(\frac{D}{p}\right)$	ℓ	u	$U_u \bmod p$, $V_{2^i u} \bmod p$ für $i = 0, \ldots, \ell - 1$
929	326	785	103136	-1	1	465	0, 585
223	213	201	44565	1	1	111	0, 221
557	384	505	145436	1	2	139	321, 119, 0
223	40	22	1512	-1	5	7	192, 9, 134, 161, 44, 0
239	78	115	5624	1	1	119	75, 0
887	10	470	-1780	-1	3	111	495, 767, 352, 0
977	613	491	373805	1	4	61	196, 322, 226, 726, 0
929	41	364	225	1	5	29	925, 836, 86, 0, 281, 927
787	43	415	189	-1	2	197	311, 0, 310
641	466	243	216184	-1	1	321	629, 0
127	98	18	9532	-1	7	1	1, 98, 43, 58, 41, 0, 58, 31
283	195	56	37801	-1	2	71	232, 278, 0
751	618	114	381468	-1	4	47	217, 635, 694, 608, 0
701	309	526	93377	1	2	175	0, 431, 699
367	250	13	62448	-1	4	23	324, 225, 212, 0, 230
607	82	146	6140	-1	5	19	293, 147, 247, 445, 0, 398
211	204	204	40800	-1	2	53	0, 141, 129
967	681	298	462569	-1	3	121	116, 0, 442, 15
389	307	289	93093	1	2	97	122, 0, 387
839	645	270	414945	-1	3	105	524, 728, 0, 390
281	220	266	47336	1	3	35	153, 168, 227, 0
257	219	135	47421	1	8	1	1, 219, 146, 29, 130, 194, 242, 0, 2
409	136	246	17512	1	3	51	291, 267, 0, 2
911	531	800	278761	-1	4	57	766, 444, 0, 792, 248
593	516	38	266104	1	4	37	494, 417, 142, 0, 591
127	2	51	-200	-1	7	1	1, 2, 29, 84, 122, 58, 89, 0
673	639	570	406041	1	5	21	0, 308, 322, 21, 557, 671
839	420	336	175056	-1	3	105	0, 451, 601, 635
521	92	287	7316	1	3	65	274, 0, 51, 519
223	117	112	13241	-1	5	7	180, 28, 0, 189, 132, 15

Man kann nun schauen, ob die im Satz dargestellten Eigenschaften auch für zusammengesetzte Zahlen gelten.

5. Der Lucas-Primzahltest und Lucas-Pseudoprimzahlen

Ist p eine Primzahl, sind $P, Q \in \mathbb{Z}$ und $D = P^2 - 4Q$ mit $\mathrm{ggT}(p, 2QD) = 1$, so gilt

$$U_{p-\left(\frac{D}{p}\right)} \equiv 0 \bmod p.$$

Was passiert, wenn wir für natürliche Zahlen n mit $\mathrm{ggT}(n, 2QD) = 1$

$$U_{n-\left(\frac{D}{n}\right)} \bmod n$$

betrachten? Hier sind ein paar zufällig gewählte Beispiele:

n	P	Q	D	$\left(\frac{D}{n}\right)$	$U_{n-\left(\frac{D}{n}\right)} \bmod n$	Faktorisierung von n
903	642	368	410692	-1	267	$3 \cdot 7 \cdot 43$
833	4	12	-32	1	714	$7^2 \cdot 17$
157	32	150	424	1	0	157
273	181	137	32213	1	0	$3 \cdot 7 \cdot 13$
789	755	161	569381	-1	574	$3 \cdot 263$
179	105	91	10661	1	0	179
569	177	53	31117	-1	0	569
941	409	196	166497	-1	0	941
943	143	278	19337	1	161	$23 \cdot 41$
673	275	454	73809	-1	0	673
461	154	206	22892	1	0	461
281	171	189	28485	-1	0	281
757	85	467	5357	1	0	757
939	42	289	608	-1	45	$3 \cdot 313$
307	161	47	25733	1	0	307
155	30	38	748	-1	35	$5 \cdot 31$
949	461	201	211717	-1	487	$13 \cdot 73$
953	318	772	98036	-1	0	953
983	896	846	799432	-1	0	983
539	394	290	154076	-1	44	$7^2 \cdot 11$

Man sieht, dass (bis auf eine Ausnahme) $U_{n-\left(\frac{D}{p}\right)}(P,Q) \bmod n$ nur für Primzahlen 0 ist. Die Ausnahmen haben einen Namen:

Definition. *Seien $P, Q \in \mathbb{Z}$ mit $D = P^2 - 4Q \neq 0$. Eine zusammengesetzte natürliche Zahl n heißt eine* **Lucas-Pseudoprimzahl** *zum Parameterpaar (P,Q), wenn* $\mathrm{ggT}(n, 2QD) = 1$ *und*

$$U_{n-\left(\frac{D}{n}\right)}(P,Q) \equiv 0 \bmod n$$

gilt.

Wir formulieren auch einen zugehörigen Primzahltest:

Lucas-Primzahltest zum Parameterpaar (P,Q): Sind $P, Q \in \mathbb{Z}$ mit $Q \neq 0$ und $D = P^2 - 4Q \neq 0$ und $n \in \mathbb{N}_{\geq 3}$ mit $\mathrm{ggT}(n, 2QD) = 1$, so berechnet man

$$U_{n-\left(\frac{D}{n}\right)}(P,Q) \bmod n.$$

- Gilt $U_{n-\left(\frac{D}{n}\right)}(P,Q) \mod n = 0$, so *besteht n den Lucas-Test zum Parameterpaar (P,Q)*. Die Zahl n ist dann eine Primzahl oder eine Lucas-Pseudoprimzahl zum Parameterpaar (P,Q).
- Gilt $U_{n-\left(\frac{D}{n}\right)}(P,Q) \mod n \neq 0$, so ist n zusammengesetzt.

Beispiel: Wir haben zufällig P und Q gewählt und dazu (im Fall $D = P^2 - 4Q \neq 0$, $Q \neq 0$ die erste Lucas-Pseudoprimzahl zum Parameterpaar (P, Q) bestimmt:

P	Q	D	n	n	$\left(\frac{D}{n}\right)$
98	10	9564	49	7^2	1
33	59	853	33	$3 \cdot 11$	-1
40	-8	1632	35	$5 \cdot 7$	-1
3	-65	269	209	$11 \cdot 19$	-1
73	-85	5669	9	3^2	1
60	-98	3992	15	$3 \cdot 5$	1
99	25	9701	9	3^2	1
85	-23	7317	35	$5 \cdot 7$	-1
73	77	5021	9	3^2	1
21	7	413	143	$11 \cdot 13$	-1
40	-78	1912	35	$5 \cdot 7$	-1
47	-21	2293	209	$11 \cdot 19$	-1
42	-79	2080	21	$3 \cdot 7$	1
30	-38	1052	15	$3 \cdot 5$	1
38	21	1360	703	$19 \cdot 37$	1
65	-8	4257	35	$5 \cdot 7$	-1
31	56	737	65	$5 \cdot 13$	-1
66	-28	4468	33	$3 \cdot 11$	-1
31	85	621	169	13^2	1
64	-21	4180	527	$17 \cdot 31$	-1

P	Q	D	n	n	$\left(\frac{D}{n}\right)$
8	70	-216	1111	$11 \cdot 101$	1
6	17	-32	95	$5 \cdot 19$	-1
4	77	-292	69	$3 \cdot 23$	1
6	83	-296	65	$5 \cdot 13$	1
10	31	-24	95	$5 \cdot 19$	-1
13	86	-175	377	$13 \cdot 29$	-1
7	93	-323	55	$5 \cdot 11$	1
15	81	-99	35	$5 \cdot 7$	-1
9	80	-239	9	3^2	1
8	19	-12	35	$5 \cdot 7$	-1
11	66	-143	35	$5 \cdot 7$	-1
10	26	-4	15	$3 \cdot 5$	-1
8	23	-28	9	3^2	1
5	24	-71	115	$5 \cdot 23$	-1
12	38	-8	119	$7 \cdot 17$	-1
16	89	-100	39	$3 \cdot 13$	-1
7	20	-31	9	3^2	1
15	68	-47	15	$3 \cdot 5$	-1
6	83	-296	65	$5 \cdot 13$	1
10	40	-60	899	$29 \cdot 31$	-1

Wir hatten zuvor die Parameterpaare (P, Q) bestimmt, für die die „Nullstellenmenge“ $\{i \in \mathbb{N}_0 : U_i(P, Q) = 0\}$ nicht nur aus 0 besteht. Der folgende Satz zeigt, dass man sie bei Anwendungen ausschließen sollte:

SATZ. *Sind $P, Q \in \mathbb{Z}$ mit $D = P^2 - 4Q \neq 0$ und $Q \neq 0$, aber*

$$P = 0 \quad \text{oder} \quad P^2 - Q = 0 \quad \text{oder} \quad P^2 - 2Q = 0 \quad \text{oder} \quad P^2 - 3Q = 0,$$

so gilt für jede natürliche Zahl n mit $\mathrm{ggT}(n, 2QD) = 1$

$$U_{n-\left(\frac{D}{n}\right)}(P, Q) = 0.$$

(Jede natürliche Zahl n mit $\mathrm{ggT}(n, 2QD) = 1$ *besteht also den Lucas-Test zum Parameterpaar (P, Q). Insbesondere ist jedes zusammengesetzte n mit* $\mathrm{ggT}(n, 2QD) = 1$ *eine Lucas-Pseudoprimzahl zum Parameterpaar (P, Q).)*

Beweis:

(1) Wir stellen nochmals die früheren Ergebnisse zusammen:

(P, Q)	$D = P^2 - 4Q$	$\{i \in \mathbb{N}_0 : U_i(P, Q) = 0\}$
$P = 0$, $Q \neq 0$	$-4Q$	$\mathbb{N}_0 \cdot 2$
$P^2 - Q = 0$, $Q \neq 0$	$-3P^2$	$\mathbb{N}_0 \cdot 3$
$P^2 - 2Q = 0$, $Q \neq 0$	$-P^2$	$\mathbb{N}_0 \cdot 4$
$P^2 - 3Q = 0$, $Q \neq 0$	$-\frac{1}{3}P^2$	$\mathbb{N}_0 \cdot 6$

(2) Ist $n \in \mathbb{N}$ ungerade mit $\mathrm{ggT}(n, QD) = 1$, so unterscheiden wir:
   (a) **Fall $P = 0$:** Es ist $\left(\frac{D}{n}\right) = \pm 1$, also $n - \left(\frac{D}{n}\right) \equiv 0 \bmod 2$ und damit $U_{n-\left(\frac{D}{n}\right)}(0, Q) = 0$.
   (b) **Fall $P^2 - Q = 0$ oder $P^2 - 3Q = 0$:**
   - **Fall $n \equiv 1 \bmod 6$:** Dann gilt $\left(\frac{-3}{n}\right) = 1$ und damit auch $\left(\frac{D}{n}\right) = 1$. Es folgt $n - \left(\frac{D}{n}\right) \equiv 0 \bmod 6$.
   - **Fall $n \equiv 5 \bmod 6$:** Dann ist $\left(\frac{-3}{n}\right) = -1$ und damit $\left(\frac{D}{n}\right) = -1$. Es folgt $n - \left(\frac{D}{n}\right) \equiv 0 \bmod 6$.

   Wegen $n - \left(\frac{D}{n}\right) \equiv 0 \bmod 6$ folgt $U_{n-\left(\frac{D}{n}\right)}(P, Q) = 0$.

(c) **Fall** $P^2 - 2Q = 0$**:**
- **Fall** $n \equiv 1 \bmod 4$**:** Dann ist $\left(\frac{-1}{n}\right) = 1$, also $\left(\frac{D}{n}\right) = 1$ und damit $n - \left(\frac{D}{n}\right) \equiv 0 \bmod 4$.
- **Fall** $n \equiv 3 \bmod 4$**:** Dann ist $\left(\frac{-1}{n}\right) = -1$, also $\left(\frac{D}{n}\right) = -1$ und damit $n - \left(\frac{D}{n}\right) \equiv 0 \bmod 4$.

Aus $n - \left(\frac{D}{n}\right) \equiv 0 \bmod 4$ folgt auch hier $U_{n-\left(\frac{D}{n}\right)}(P,Q) = 0$. ■

Bemerkung: Mit Lucas-Folgen kann man auch weitere Primzahltests formulieren. Der folgende Satz zeigt, wie sich der Miller-Rabin-Test mit Lucas-Folgen formulieren lässt.

SATZ. *Sei* $a \in \mathbb{Z}$ *und* $n \in \mathbb{N}_{\geq 3}$ *eine ungerade natürliche Zahl mit* $\mathrm{ggT}(n, a(a-1)) = 1$. *Sei* $n - 1 = 2^\ell u$ *mit* $u \equiv 1 \bmod 2$. *Dann sind folgende Aussagen äquivalent:*

(1) *n besteht den Miller-Rabin-Test zur Basis a, d.h.*

$$a^u \equiv 1 \bmod n \quad \textit{oder} \quad (a^u)^{2^i} \equiv -1 \bmod n \textit{ für ein } i \in \{0, \ldots, \ell - 1\}.$$

(2) *Es gilt:*

$$U_u(a+1, a) \equiv 0 \bmod n \quad \textit{oder} \quad V_{2^i u}(a+1, a) \equiv 0 \bmod n \textit{ für ein } i \in \{0, \ldots, \ell - 1\}.$$

Beweis: Wir betrachten die Lucas-Folgen $U_i(P,Q)$ und $V_i(P,Q)$ für $P = a+1$ und $Q = a$. Die Nullstellen des Polynoms $x^2 - Px + Q = x^2 - (a+1)x + a = (x-a)(x-1)$ sind a und 1. Die Voraussetzung $\mathrm{ggT}(n, a(a-1)) = 1$ impliziert $a \neq 1$, sodass wir erhalten

$$U_i(a+1, a) = \frac{a^i - 1}{a - 1} \quad \text{und} \quad V_i(a+1, a) = a^i + 1.$$

Wegen $\mathrm{ggT}(n, a(a-1)) = 1$ ist $a - 1$ invertierbar modulo n, woraus folgt:

$$U_u(a+1, a) \equiv 0 \bmod n \iff \frac{a^u - 1}{a - 1} \equiv 0 \bmod n \iff a^u \equiv 1 \bmod n.$$

Weiter gelten die Äquivalenzen:

$$V_{2^i u}(a+1, a) \equiv 0 \bmod n \iff a^{2^i u} + 1 \equiv 0 \bmod n \iff a^{2^i u} \equiv -1 \bmod n.$$

Daraus ergibt sich sofort die Äquivalenz von (1) und (2). ■

Bemerkung: Mit Lucas-Folgen kann man auch weitere Primzahltests formulieren, beispielsweise nach Art des letzten Satzes. Wir werden uns aber mit dem oben dargestellten Lucas-Primzahltest zufriedengeben. Im Folgenden werden wir uns Kombinationen des Lucas-Tests mit früher behandelten Tests anschauen.

6. Kombination: Fermat-Test und Lucas-Test

Wir probieren folgende Variante: Seien $P, Q \in \mathbb{Z}$ mit $Q \neq 0$ und $D = P^2 - 4Q \neq 0$ und $n \in \mathbb{N}_{\geq 3}$ mit $\mathrm{ggT}(n, 2QD) = 1$.

- Gilt $2^{n-1} \not\equiv 1 \bmod n$, so besteht n den Fermat-Test zur Basis 2 nicht, ist also zusammengesetzt.
- Gilt $2^{n-1} \equiv 1 \bmod n$, so besteht n den Fermat-Test zur Basis 2. Wir berechnen nun

$$U_{n-\left(\frac{D}{n}\right)}(P,Q) \bmod n.$$

  - Gilt $U_{n-\left(\frac{D}{n}\right)}(P,Q) \bmod n \neq 0$, so besteht n den Lucas-Test zum Parameterpaar (P,Q) nicht, ist also zusammengesetzt.
  - Gilt $U_{n-\left(\frac{D}{n}\right)}(P,Q) \bmod n = 0$, so besteht n den Lucas-Test zum Parameterpaar (P,Q) (und auch den Fermat-Test zur Basis 2).

Kann eine zusammengesetzte Zahl diesen kombinierten Test bestehen?

Wir suchen nach Zahlen, die gleichzeitig Fermat-Pseudoprimzahlen zur Basis 2 und Lucas-Pseudoprimzahlen sind. Wir haben dabei (P, Q) zufällig gewählt mit $P^2 - 4Q \neq 0$ und $Q \neq 0$ und nach der ersten solchen Zahl gesucht:

P	Q	D	n	n	$\left(\frac{D}{n}\right)$
9	-17	149	8911	$7 \cdot 19 \cdot 67$	1
30	67	632	2701	$37 \cdot 73$	1
9	-47	269	15841	$7 \cdot 31 \cdot 73$	1
5	-84	361	341	$11 \cdot 31$	1
33	6	1065	1729	$7 \cdot 13 \cdot 19$	1
36	-9	1332	2465	$5 \cdot 17 \cdot 29$	-1
36	61	1052	1729	$7 \cdot 13 \cdot 19$	1
100	-63	10252	10585	$5 \cdot 29 \cdot 73$	1
32	-37	1172	13747	$59 \cdot 233$	1
93	-6	8673	188057	$89 \cdot 2113$	1
16	-82	584	5461	$43 \cdot 127$	1
72	65	4924	83333	$167 \cdot 499$	1
76	96	5392	30889	$17 \cdot 23 \cdot 79$	1
89	59	7685	30889	$17 \cdot 23 \cdot 79$	1
50	-4	2516	18721	$97 \cdot 193$	1
27	39	573	6601	$7 \cdot 23 \cdot 41$	1
86	65	7136	1387	$19 \cdot 73$	1
70	-5	4920	4033	$37 \cdot 109$	1
5	62	-223	561	$3 \cdot 11 \cdot 17$	1
11	-22	209	49141	$157 \cdot 313$	1

P	Q	D	n	n	$\left(\frac{D}{n}\right)$
14	-72	484	1105	$5 \cdot 13 \cdot 17$	1
65	11	4181	2047	$23 \cdot 89$	1
53	16	2745	6601	$7 \cdot 23 \cdot 41$	1
36	-43	1468	6601	$7 \cdot 23 \cdot 41$	1
70	-77	5208	2701	$37 \cdot 73$	1
47	28	2097	1105	$5 \cdot 13 \cdot 17$	1
54	-99	3312	1105	$5 \cdot 13 \cdot 17$	1
53	-43	2981	10585	$5 \cdot 29 \cdot 73$	1
67	59	4253	4371	$3 \cdot 31 \cdot 47$	-1
16	57	28	31621	$103 \cdot 307$	1
5	-14	81	1105	$5 \cdot 13 \cdot 17$	1
79	-33	6373	8321	$53 \cdot 157$	1
32	-74	1320	6601	$7 \cdot 23 \cdot 41$	1
58	44	3188	5461	$43 \cdot 127$	1
39	67	1253	1387	$19 \cdot 73$	-1
80	94	6024	15841	$7 \cdot 31 \cdot 73$	1
98	-49	9800	561	$3 \cdot 11 \cdot 17$	1
57	-34	3385	6601	$7 \cdot 23 \cdot 41$	1
29	80	521	341	$11 \cdot 31$	1
23	-89	885	2701	$37 \cdot 73$	1

Es fällt bereits auf, dass deutlich mehr Fälle mit $\left(\frac{D}{n}\right) = 1$ auftreten als mit $\left(\frac{D}{n}\right) = -1$. Im Folgenden haben wir nur die Fälle mit $\left(\frac{D}{n}\right) = -1$ aufgeschrieben:

P	Q	D	n	n	$\left(\frac{D}{n}\right)$
89	78	7609	341	$11 \cdot 31$	-1
53	27	2701	341	$11 \cdot 31$	-1
46	-59	2352	2465	$5 \cdot 17 \cdot 29$	-1
62	-52	4052	4371	$3 \cdot 31 \cdot 47$	-1
7	49	-147	341	$11 \cdot 31$	-1
22	89	128	341	$11 \cdot 31$	-1
55	-13	3077	341	$11 \cdot 31$	-1
74	20	5396	341	$11 \cdot 31$	-1
58	-66	3628	2465	$5 \cdot 17 \cdot 29$	-1
97	-26	9513	2047	$23 \cdot 89$	-1

P	Q	D	n	n	$\left(\frac{D}{n}\right)$
23	-29	645	341	$11 \cdot 31$	-1
37	-57	1597	341	$11 \cdot 31$	-1
16	37	108	2465	$5 \cdot 17 \cdot 29$	-1
6	-19	112	341	$11 \cdot 31$	-1
67	-31	4613	2465	$5 \cdot 17 \cdot 29$	-1
27	78	417	341	$11 \cdot 31$	-1
18	-16	388	2047	$23 \cdot 89$	-1
14	70	-84	228241	$13 \cdot 97 \cdot 181$	-1
4	16	-48	341	$11 \cdot 31$	-1
36	25	1196	341	$11 \cdot 31$	-1

Nun betrachten wir Fermat-Pseudoprimzahlen zur Basis a mit zufällig gewähltem a und wieder zufällig gewählten P und Q:

a	P	Q	D	n	n	$\left(\frac{D}{n}\right)$
15	82	-78	7036	8911	$7 \cdot 19 \cdot 67$	1
29	96	15	9156	49051	$181 \cdot 271$	1
13	13	-9	205	1891	$31 \cdot 61$	1
28	27	58	497	9	3^2	1
7	58	54	3148	38081	$113 \cdot 337$	1
23	13	39	13	28939	$43 \cdot 673$	1
22	43	65	1589	1247	$29 \cdot 43$	1
9	50	-39	2656	6601	$7 \cdot 23 \cdot 41$	1
18	49	62	2153	49	7^2	1
11	27	-50	929	2047	$23 \cdot 89$	1
21	45	-51	2229	5473	$13 \cdot 421$	-1
25	48	17	2236	5963	$67 \cdot 89$	1
11	83	-33	7021	114211	$181 \cdot 631$	1
4	21	70	161	27511	$11 \cdot 41 \cdot 61$	1
19	64	-55	4316	15841	$7 \cdot 31 \cdot 73$	1
24	89	98	7529	25	5^2	1
20	6	33	-96	15841	$7 \cdot 31 \cdot 73$	1
14	4	15	-44	211951	$181 \cdot 1171$	1
13	53	-56	3033	30889	$17 \cdot 23 \cdot 79$	1
3	82	-14	6780	15457	$13 \cdot 29 \cdot 41$	1

a	P	Q	D	n	n	$\left(\frac{D}{n}\right)$
9	82	-7	6752	205	$5 \cdot 41$	1
22	96	76	8912	38503	$139 \cdot 277$	1
17	8	-10	104	4033	$37 \cdot 109$	1
19	64	-49	4292	9	3^2	1
28	85	-18	7297	145	$5 \cdot 29$	1
3	54	-25	3016	1891	$31 \cdot 61$	1
5	33	-50	1289	6601	$7 \cdot 23 \cdot 41$	1
12	77	11	5885	8911	$7 \cdot 19 \cdot 67$	1
6	94	60	8596	6533	$47 \cdot 139$	1
14	62	39	3688	128627	$293 \cdot 439$	1
17	93	-82	8977	158401	$23 \cdot 71 \cdot 97$	1
6	67	-12	4537	35	$5 \cdot 7$	-1
11	99	43	9629	15	$3 \cdot 5$	-1
27	40	23	1508	121	11^2	1
30	17	56	65	11041	$61 \cdot 181$	1
3	18	-81	648	6601	$7 \cdot 23 \cdot 41$	1
8	12	-7	172	1661	$11 \cdot 151$	-1
8	76	40	5616	133	$7 \cdot 19$	1
23	63	60	3729	5149	$19 \cdot 271$	1
12	65	96	3841	65	$5 \cdot 13$	-1

Es gibt also viele Zahlen, die sowohl den Fermat-Test zur Basis 2 als auch eine Lucas-Test zu einem Parameterpaar (P, Q) bestehen.

7. Kombination: Miller-Rabin-Test zur Basis 2 und Lucas-Test

Nun gehen wir so vor: Seien $P, Q \in \mathbb{Z}$ mit $Q \neq 0$ und $D = P^2 - 4Q \neq 0$. Sei $n \in \mathbb{N}_{\geq 3}$ mit $\mathrm{ggT}(n, 2QD) = 1$.

(1) Wir beginnen mit einem Miller-Rabin-Test zur Basis 2, d.h. wir zerlegen $n - 1 = 2^\ell u$ mit $u \equiv 1 \bmod 2$ und testen, ob

$$2^u \equiv 1 \bmod n \quad \text{oder} \quad 2^{2^i u} \equiv -1 \bmod n \text{ für ein } i \in \{0, \ldots, \ell - 1\}$$

gilt. Wenn nein, ist n zusammengesetzt, und wir hören auf. Wenn ja, besteht n den Test, ist also eine Primzahl oder eine starke Pseudoprimzahl zu Basis 2.

(2) Hat n den Miller-Rabin-Test bestanden, machen wir einen Lucas-Test zum Parameterpaar (P, Q), d.h. wir überprüfen, ob gilt

$$U_{n-\left(\frac{D}{n}\right)}(P, Q) \equiv 0 \bmod n.$$

Gilt die Gleichung nicht, ist n zusammengesetzt, andernfalls besteht n den Lucas-Test, ist also eine Primzahl oder eine Lucas-Pseudoprimzahl zum Parameterpaar (P, Q) (und eine starke Pseudoprimzahl zur Basis 2).

Gibt es zusammengesetzte Zahlen, die diesen kombinierten Test bestehen?

Wieder wählen wir zufällig P und Q und suchen die kleinste natürliche Zahl n, die den Miller-Rabin-Test zur Basis 2 und den Lucas-Test zum Parameterpaar (P, Q) besteht. Dabei haben wir uns zunächst auf

$n \leq 10^6$ beschränkt.

P	Q	D	n	n	$\left(\frac{D}{n}\right)$
53	33	2677	15841	$7 \cdot 31 \cdot 73$	1
25	-22	713	252601	$41 \cdot 61 \cdot 101$	1
48	-95	2684	741751	$431 \cdot 1721$	1
26	-81	1000	90751	$151 \cdot 601$	1
86	-4	7412	2047	$23 \cdot 89$	1
67	45	4309	?		
96	11	9172	?		
59	-66	3745	357761	$131 \cdot 2731$	1
27	61	485	741751	$431 \cdot 1721$	1
21	-12	489	?		
42	24	1668	486737	$233 \cdot 2089$	1
36	-7	1324	916327	$479 \cdot 1913$	1
6	-77	344	?		
74	79	5160	15841	$7 \cdot 31 \cdot 73$	1
29	73	549	?		
19	25	261	458989	$277 \cdot 1657$	1
70	83	4568	486737	$233 \cdot 2089$	1
68	61	4380	130561	$137 \cdot 953$	1
7	20	-31	196093	$157 \cdot 1249$	1
7	-95	429	52633	$7 \cdot 73 \cdot 103$	1

P	Q	D	n	n	$\left(\frac{D}{n}\right)$
9	10	41	741751	$431 \cdot 1721$	1
5	72	-263	2047	$23 \cdot 89$	1
95	37	8877	88357	$149 \cdot 593$	1
46	81	1792	3277	$29 \cdot 113$	1
64	-81	4420	390937	$313 \cdot 1249$	1
19	76	57	8321	$53 \cdot 157$	1
42	37	1616	196093	$157 \cdot 1249$	1
29	33	709	49141	$157 \cdot 313$	1
80	93	6028	?		
66	8	4324	74665	$5 \cdot 109 \cdot 137$	1
39	-53	1733	2047	$23 \cdot 89$	1
61	26	3617	390937	$313 \cdot 1249$	1
60	-39	3756	?		
45	96	1641	15841	$7 \cdot 31 \cdot 73$	1
98	17	9536	15841	$7 \cdot 31 \cdot 73$	1
7	-86	393	280601	$277 \cdot 1013$	1
62	-34	3980	2047	$23 \cdot 89$	1
81	51	6357	15841	$7 \cdot 31 \cdot 73$	1
19	-62	609	?		
88	-96	8128	29341	$13 \cdot 37 \cdot 61$	1

Nun haben wir die oben offenen Fälle weiter untersucht:

P	Q	D	n	n	$\left(\frac{D}{n}\right)$
67	45	4309	2205967	$743 \cdot 2969$	1
96	11	9172	1302451	$571 \cdot 2281$	1
21	-12	489	1207361	$449 \cdot 2689$	1
6	-77	344	1373653	$829 \cdot 1657$	1
29	73	549	1207361	$449 \cdot 2689$	1
80	93	6028	1373653	$829 \cdot 1657$	1
60	-39	3756	1909001	$41 \cdot 101 \cdot 461$	1
19	-62	609	1357441	$673 \cdot 2017$	1

Dies deutet darauf hin, dass man zu (P, Q) vermutlich starke Pseudoprimzahlen zur Basis 2 finden kann, die auch Lucas-Pseudoprimzahlen zum Parameterpaar (P, Q) sind. Es fällt auf, dass hier keine Fälle mit $\left(\frac{D}{n}\right) = -1$ vorkommen. Wir haben deshalb weiter probiert. Wir wählen zufällig P und Q, sodass $D = P^2 - 4Q$ kein Quadrat ist und bestimmen die ersten 5 Zahlen, die starke Pseudoprimzahlen zur

Basis 2 und Lucas-Pseudoprimzahlen sind:

(P,Q)	D	n mit Faktorisierung, in der Klammer steht $\left(\frac{D}{n}\right)$
$(85,96)$	6841	$8321 = 53 \cdot 157$ (1), $29341 = 13 \cdot 37 \cdot 61$ (1), $314821 = 13 \cdot 61 \cdot 397$ (1), $2284453 = 1069 \cdot 2137$ (1) $5310721 = 13 \cdot 37 \cdot 61 \cdot 181$ (1)
$(77,85)$	5589	$1907851 = 11 \cdot 251 \cdot 691$ (1), $5049001 = 31 \cdot 271 \cdot 601$ (1), $9056501 = 1229 \cdot 7369$ (1), $9863461 = 2221 \cdot 4441$ (1), $13694761 = 2617 \cdot 5233$ (1)
$(45,24)$	1929	$458989 = 277 \cdot 1657$ (1), $1373653 = 829 \cdot 1657$ (1), $6140161 = 937 \cdot 6553$ (1), $10974881 = 1913 \cdot 5737$ (1), $15101893 = 829 \cdot 18217$ (1)
$(62,-67)$	4112	$314821 = 13 \cdot 61 \cdot 397$ (1), $916327 = 479 \cdot 1913$ (1), $2510569 = 709 \cdot 3541$ (1), $9863461 = 2221 \cdot 4441$ (1), $16879501 = 1453 \cdot 11617$ (1)
$(41,69)$	1405	$3277 = 29 \cdot 113$ (1), $5044033 = 1297 \cdot 3889$ (1), $5049001 = 31 \cdot 271 \cdot 601$ (1), $5444489 = 29 \cdot 197 \cdot 953$ (1), $10974881 = 1913 \cdot 5737$ (1)
$(95,85)$	8685	$4681 = 31 \cdot 151$ (1), $271951 = 151 \cdot 1801$ (1), $3125281 = 1021 \cdot 3061$ (1), $4181921 = 1181 \cdot 3541$ (1), $9863461 = 2221 \cdot 4441$ (1)
$(92,5)$	8444	$2047 = 3 \cdot 89$ (1), $983401 = 331 \cdot 2971$ (1), $1730977 = 439 \cdot 3943$ (1), $3125281 = 1021 \cdot 3061$ (1), $3375041 = 1061 \cdot 3181$ (1)
$(68,-85)$	4964	$3277 = 29 \cdot 113$ (1), $256999 = 233 \cdot 1103$ (1), $5444489 = 29 \cdot 197 \cdot 953$ (1), $7759937 = 929 \cdot 8353$ (1), $9006401 = 1733 \cdot 5197$ (1)
$(19,8)$	329	$104653 = 229 \cdot 457$ (1), $741751 = 431 \cdot 1721$ (1), $983401 = 331 \cdot 2971$ (1), $1987021 = 997 \cdot 1993$ (1), $3116107 = 883 \cdot 3529$ (1)
$(80,4)$	6384	$873181 = 661 \cdot 1321$ (1), $1441091 = 347 \cdot 4153$ (1), $2746477 = 829 \cdot 3313$ (1), $4863127 = 1103 \cdot 4409$ (1), $9863461 = 2221 \cdot 4441$ (1)

Immer ist das Jacobi-Symbol 1.

Es scheint also schwierig zu sein, zusammengesetzte Zahlen zu finden, die den Miller-Rabin-Test zur Basis 2 bestehen und gleichzeitig $U_{n-\left(\frac{D}{n}\right)}(P,Q) = 0$ mit $\left(\frac{D}{n}\right) = -1$. (Dabei sollte man sicherheitshalber die Lucas-Folgen mit nichttrivialer Nullstellenmenge ausschließen.) Daraus hat sich der nachfolgende Primzahltest entwickelt:

8. Der BPSW-Primzahltest (Baillie-PSW-Primzahltest) nach Baillie-Pomerance-Selfridge-Wagstaff

Überlegungen:

(1) Gegeben ist eine ungerade natürliche Zahl. Es soll untersucht werden, ob sie zusammengesetzt oder (wahrscheinlich) prim ist.

(2) Zunächst wird man untersuchen, ob die Zahl einen kleinen Primteiler hat. In vielen Fällen ist man dann schon fertig.

(3) Nun macht man einen Miller-Rabin-Test zur Basis 2, d.h. man zerlegt $n - 1 = 2^\ell u$ mit $u \equiv 1 \bmod 2$ und testet, ob

$$2^u \equiv 1 \bmod n \quad \text{oder} \quad 2^{2^i u} \equiv -1 \bmod n \text{ für ein } i \in \{0, \dots, \ell - 1\}$$

gilt. Besteht n den Test nicht, ist n zusammengesetzt und man ist fertig.

(4) Nun braucht man ein D mit $\left(\frac{D}{n}\right) = -1$. Ist n eine Quadratzahl, existiert natürlich kein solches D, weshalb man diesen Fall irgendwie ausschließen muss. (Bisher sind nur zwei Quadratzahlen bekannt, die den Miller-Rabin-Test zur Basis 2 bestehen, nämlich 1093^2 und 3511^2. Die Zahlen 1093 und 3511 sind Primzahlen.)

(5) Selfridge hat vorgeschlagen, der Reihe nach

$$D \in \{5, -7, 9, -11, 13, -15, 17, \dots\}$$

zu probieren, bis man ein D mit $\left(\frac{D}{n}\right) < 1$ erhält. Ist $\left(\frac{D}{n}\right) = 0$, so ist $\mathrm{ggT}(n, D) > 1$ und man ist fertig. Andernfalls ist $\left(\frac{D}{n}\right) = -1$ und man setzt

$$P = 1, \quad Q = \frac{1 - D}{4}.$$

Jetzt überprüft man, ob $U_{n+1}(P,Q) \equiv 0 \bmod n$ gilt. Wenn nein, ist n zusammengesetzt, andernfalls wahrscheinlich prim.

Wir fassen unsere Überlegungen in einem Algorithmus zusammen:

BPSW-Primzahltest:
Eingabe: $n \in \mathbb{N}_{\geq 2}$
Ausgabe: n ist zusammengesetzt oder (wahrscheinlich) prim

$P \leftarrow \{p : 2 \leq p \leq 997\} \cup \{1093, 3511\}$ ▷ P sollte man schon als Liste gespeichert haben
if $n \in P$ **then**
  return n ist prim
end if
for $p \in P$ **do**
  if $n \bmod p = 0$ **then**
    return n ist zusammengesetzt
  end if
end for
if $n < 1000000$ **then**
  return n ist prim
end if
if n besteht den Miller-Rabin-Test zur Basis 2 nicht **then**
  return n ist zusammengesetzt
end if ▷ Nach den Vorbereitungen sollte jetzt n kein Quadrat sein, sonst braucht man einen Test
$D \leftarrow 5$, $e \leftarrow 2$
while $\left(\frac{D}{n}\right) = 1$ **do**
  $D \leftarrow -D - e$, $e \leftarrow -e$
end while ▷ Praktisch ist nun der Fall $\left(\frac{D}{n}\right) = 0$ unwahrscheinlich, weshalb er hier nicht beachtet wird
$P \leftarrow 1$, $Q \leftarrow \frac{1-D}{4}$
if $U_{n+1}(P,Q) \bmod n \neq 0$ **then**
  return n ist zusammengesetzt
end if
return n ist (wahrscheinlich) prim

Hier ist eine zugehörige Python-Funktion:

```
def prim(n):
  if n<2:
    return False
  PZ=[2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,
      101,103,107,109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,
      193,197,199,211,223,227,229,233,239,241,251,257,263,269,271,277,281,283,
      293,307,311,313,317,331,337,347,349,353,359,367,373,379,383,389,397,401,
      409,419,421,431,433,439,443,449,457,461,463,467,479,487,491,499,503,509,
      521,523,541,547,557,563,569,571,577,587,593,599,601,607,613,617,619,631,
      641,643,647,653,659,661,673,677,683,691,701,709,719,727,733,739,743,751,
      757,761,769,773,787,797,809,811,821,823,827,829,839,853,857,859,863,877,
      881,883,887,907,911,919,929,937,941,947,953,967,971,977,983,991,997,
      1093,3511]
  if n in PZ:
    return True
  for p in PZ:
    if n%p==0:
      return False
  if n<1000000:
    return True
```

```
# Miller-Rabin-Test zur Basis 2 - n sollte ungerade sein.
def miller_rabin_2(n):
  u,l=n-1,0
  while u%2==0:
    u,l=u//2,l+1
  b=pow(2,u,n)
  if b==1 or b==n-1:
    return True
  for i in range(1,l):
    b=(b**2)%n
    if b==n-1:
      return True
  return False
if miller_rabin_2(n)==False:
  return False
# Berechnung des Jacobi-Symbols (a/b)
def jac(a,b):
  j=1
  a=a%b
  while a>0:
    e=0
    while a%2==0:
      e+=1; a=a//2
    if e%2==1 and (b%8 in {3,5}):
      j=-j
    if a%4==3 and b%4==3:
      j=-j
    a,b=b%a,a
  if b>1: j=0
  return j
# Berechnung von U_i(P,Q) mod n
def U_modn_3(i,P,Q,n):
  j=i
  J=[]
  while j>1:
    J.append(j%2)
    j=(j+1)//2
  u,v,w,q=1,P%n,2%n,1
  while J!=[]:
    j=J.pop()
    if j==0:
      u,v,w,q=u*v%n,(v*v-2*Q*q)%n,(v*w-P*q)%n,Q*q*q%n
    else:
      u,v,w,q=(u*w-q)%n,(v*w-P*q)%n,(w*w-2*q)%n,q*q%n
  return u
# Suche nach D mit (D/n)!=1. (Wir testen nicht, ob n eine Quadratzahl ist.)
D,e=5,2
while jac(D,n)==1:
  D,e=-D-e,-e
# Lucas-Primzahltest
P,Q=1,(1-D)//4
if U_modn_3(n+1,P,Q,n)!=0:
  return False
return True
```

Bemerkung: Trotz intensiver Bemühungen ist bis heute keine zusammengesetzte natürliche Zahl bekannt, die den BPSW-Primzahltest besteht. Daher wird dieser Test (oder Varianten) davon gerne eingesetzt.

Beispiele: Wir haben die ersten 200 starken Pseudoprimzahlen (zur Basis 2) untersucht: In der Tabelle ist das erste D aus obiger Liste mit $\left(\frac{D}{n}\right) \neq 1$ angegeben.

i	n	n	D	$\left(\frac{D}{n}\right)$
1	2047	$23 \cdot 89$	5	-1
2	3277	$29 \cdot 113$	5	-1
3	4033	$37 \cdot 109$	5	-1
4	4681	$31 \cdot 151$	-7	-1
5	8321	$53 \cdot 157$	-7	-1
6	15841	$7 \cdot 31 \cdot 73$	-7	0
7	29341	$13 \cdot 37 \cdot 61$	13	0
8	42799	$127 \cdot 337$	17	-1
9	49141	$157 \cdot 313$	17	-1
10	52633	$7 \cdot 73 \cdot 103$	5	-1
11	65281	$97 \cdot 673$	-7	-1
12	74665	$5 \cdot 109 \cdot 137$	5	0
13	80581	$61 \cdot 1321$	-11	-1
14	85489	$53 \cdot 1613$	-7	-1
15	88357	$149 \cdot 593$	5	-1
16	90751	$151 \cdot 601$	-7	-1
17	104653	$229 \cdot 457$	5	-1
18	130561	$137 \cdot 953$	-11	-1
19	196093	$157 \cdot 1249$	5	-1
20	220729	$103 \cdot 2143$	-7	-1
21	233017	$43 \cdot 5419$	5	-1
22	252601	$41 \cdot 61 \cdot 101$	-7	-1
23	253241	$157 \cdot 1613$	-11	-1
24	256999	$233 \cdot 1103$	-11	-1
25	271951	$151 \cdot 1801$	-23	-1
26	280601	$277 \cdot 1013$	-7	-1
27	314821	$13 \cdot 61 \cdot 397$	-7	-1
28	357761	$131 \cdot 2731$	-7	-1
29	390937	$313 \cdot 1249$	5	-1
30	458989	$277 \cdot 1657$	-7	-1
31	476971	$11 \cdot 131 \cdot 331$	-7	-1
32	486737	$233 \cdot 2089$	5	-1
33	489997	$157 \cdot 3121$	5	-1
34	514447	$359 \cdot 1433$	5	-1
35	580337	$499 \cdot 1163$	5	-1
36	635401	$13 \cdot 37 \cdot 1321$	-11	-1
37	647089	$79 \cdot 8191$	-23	-1
38	741751	$431 \cdot 1721$	-7	-1
39	800605	$5 \cdot 13 \cdot 109 \cdot 113$	5	0
40	818201	$101 \cdot 8101$	-7	-1
41	838861	$397 \cdot 2113$	-23	-1
42	873181	$661 \cdot 1321$	17	-1
43	877099	$307 \cdot 2857$	-7	-1
44	916327	$479 \cdot 1913$	5	-1
45	976873	$313 \cdot 3121$	5	-1
46	983401	$331 \cdot 2971$	-7	-1
47	1004653	$13 \cdot 109 \cdot 709$	5	-1
48	1016801	$251 \cdot 4051$	13	-1
49	1023121	$11 \cdot 281 \cdot 331$	-11	0
50	1082401	$601 \cdot 1801$	-7	-1
51	1145257	$103 \cdot 11119$	5	-1
52	1194649	1093^2	n ist Quadrat	
53	1207361	$449 \cdot 2689$	-15	-1
54	1251949	$409 \cdot 3061$	-7	-1
55	1252697	$733 \cdot 1709$	5	-1
56	1302451	$571 \cdot 2281$	-7	-1
57	1325843	$499 \cdot 2657$	5	-1
58	1357441	$673 \cdot 2017$	-11	-1
59	1373653	$829 \cdot 1657$	5	-1
60	1397419	$67 \cdot 20857$	-43	-1
61	1441091	$347 \cdot 4153$	13	-1
62	1493857	$547 \cdot 2731$	5	-1
63	1507963	$971 \cdot 1553$	5	-1
64	1509709	$389 \cdot 3881$	-7	-1
65	1530787	$619 \cdot 2473$	5	-1
66	1678541	$1013 \cdot 1657$	-11	-1
67	1730977	$439 \cdot 3943$	5	-1
68	1811573	$389 \cdot 4657$	5	-1
69	1876393	$613 \cdot 3061$	5	-1
70	1907851	$11 \cdot 251 \cdot 691$	-11	0
71	1909001	$41 \cdot 101 \cdot 461$	-7	-1
72	1969417	$919 \cdot 2143$	5	-1
73	1987021	$997 \cdot 1993$	17	-1
74	2004403	$307 \cdot 6529$	5	-1
75	2081713	$373 \cdot 5581$	5	-1
76	2181961	$661 \cdot 3301$	-7	-1
77	2205967	$743 \cdot 2969$	5	-1
78	2264369	$389 \cdot 5821$	-11	-1
79	2269093	$953 \cdot 2381$	5	-1
80	2284453	$1069 \cdot 2137$	5	-1
81	2304167	$1103 \cdot 2089$	5	-1
82	2387797	$773 \cdot 3089$	5	-1
83	2419385	$5 \cdot 229 \cdot 2113$	5	0
84	2510569	$709 \cdot 3541$	-7	-1
85	2746477	$829 \cdot 3313$	5	-1
86	2748023	$479 \cdot 5737$	5	-1
87	2757241	$461 \cdot 5981$	13	-1
88	2811271	$881 \cdot 3191$	13	-1
89	2909197	$293 \cdot 9929$	5	-1
90	2953711	$31 \cdot 151 \cdot 631$	-7	-1
91	2976487	$863 \cdot 3449$	5	-1
92	3090091	$1163 \cdot 2657$	-31	-1
93	3116107	$883 \cdot 3529$	5	-1
94	3125281	$1021 \cdot 3061$	-7	-1
95	3375041	$1061 \cdot 3181$	-7	-1
96	3400013	$1597 \cdot 2129$	5	-1
97	3429037	$157 \cdot 21841$	5	-1
98	3539101	$941 \cdot 3761$	-7	-1
99	3567481	$311 \cdot 11471$	13	-1
100	3581761	$29 \cdot 113 \cdot 1093$	-11	-1

i	n	n	D	$\left(\frac{D}{n}\right)$
101	3605429	$137 \cdot 26317$	-15	-1
102	3898129	$1249 \cdot 3121$	17	-1
103	4181921	$1181 \cdot 3541$	-11	-1
104	4188889	$431 \cdot 9719$	-7	-1
105	4335241	$53 \cdot 157 \cdot 521$	17	-1
106	4360621	$1321 \cdot 3301$	-7	-1
107	4469471	$1831 \cdot 2441$	-7	-1
108	4502485	$5 \cdot 13 \cdot 113 \cdot 613$	5	0
109	4513841	$1021 \cdot 4421$	-7	-1
110	4682833	$29 \cdot 113 \cdot 1429$	5	-1
111	4835209	$239 \cdot 20231$	13	-1
112	4863127	$1103 \cdot 4409$	5	-1
113	5016191	$647 \cdot 7753$	-7	-1
114	5044033	$1297 \cdot 3889$	5	-1
115	5049001	$31 \cdot 271 \cdot 601$	-7	-1
116	5173169	$1093 \cdot 4733$	-15	-1
117	5173601	$929 \cdot 5569$	-7	-1
118	5256091	$811 \cdot 6481$	17	-1
119	5310721	$13 \cdot 37 \cdot 61 \cdot 181$	-7	-1
120	5444489	$29 \cdot 197 \cdot 953$	-11	-1
121	5489641	$1657 \cdot 3313$	-7	-1
122	5590621	$409 \cdot 13669$	-23	-1
123	5599765	$5 \cdot 37 \cdot 30269$	5	0
124	5672041	$661 \cdot 8581$	13	-1
125	5681809	$7 \cdot 73 \cdot 11119$	-7	0
126	5919187	$1777 \cdot 3331$	5	-1
127	6140161	$937 \cdot 6553$	-7	-1
128	6226193	$1933 \cdot 3221$	5	-1
129	6233977	$1117 \cdot 5581$	5	-1
130	6334351	$727 \cdot 8713$	29	-1
131	6368689	$1129 \cdot 5641$	-7	-1
132	6386993	$653 \cdot 9781$	5	-1
133	6787327	$1303 \cdot 5209$	5	-1
134	6836233	$313 \cdot 21841$	5	-1
135	6952037	$2153 \cdot 3229$	5	-1
136	7177105	$5 \cdot 13 \cdot 109 \cdot 1013$	5	0
137	7306261	$2341 \cdot 3121$	-11	-1
138	7306561	$1153 \cdot 6337$	-7	-1
139	7462001	$911 \cdot 8191$	-11	-1
140	7674967	$937 \cdot 8191$	5	-1
141	7759937	$929 \cdot 8353$	5	-1
142	7820201	$1831 \cdot 4271$	-15	-1
143	7883731	$811 \cdot 9721$	13	-1
144	8036033	$1637 \cdot 4909$	5	-1
145	8095447	$1423 \cdot 5689$	5	-1
146	8384513	$277 \cdot 30269$	5	-1
147	8388607	$47 \cdot 178481$	5	-1
148	8534233	$709 \cdot 12037$	5	-1
149	8725753	$2089 \cdot 4177$	5	-1
150	8727391	$71 \cdot 122921$	-11	-1
151	9006401	$1733 \cdot 5197$	-7	-1
152	9056501	$1229 \cdot 7369$	-7	-1
153	9069229	$13 \cdot 293 \cdot 2381$	13	0
154	9073513	$953 \cdot 9521$	5	-1
155	9371251	$1531 \cdot 6121$	-11	-1
156	9564169	$619 \cdot 15451$	-7	-1
157	9567673	$509 \cdot 18797$	5	-1
158	9588151	$79 \cdot 121369$	-7	-1
159	9729301	$1201 \cdot 8101$	-11	-1
160	9774181	$181 \cdot 54001$	-11	-1
161	9863461	$2221 \cdot 4441$	-7	-1
162	9995671	$7 \cdot 31 \cdot 73 \cdot 631$	-7	0
163	10323769	$349 \cdot 29581$	37	-1
164	10386241	$1861 \cdot 5581$	-7	-1
165	10425511	$2441 \cdot 4271$	-7	-1
166	10610063	$2351 \cdot 4513$	5	-1
167	10655905	$5 \cdot 13 \cdot 29 \cdot 5653$	5	0
168	10712857	$2143 \cdot 4999$	5	-1
169	10763653	$409 \cdot 26317$	5	-1
170	10974881	$1913 \cdot 5737$	13	-1
171	11081459	$227 \cdot 48817$	-15	-1
172	11335501	$1321 \cdot 8581$	13	-1
173	11473885	$5 \cdot 37 \cdot 109 \cdot 569$	5	0
174	11541307	$1699 \cdot 6793$	5	-1
175	11585293	$2153 \cdot 5381$	5	-1
176	11777599	$127 \cdot 92737$	13	-1
177	12263131	$811 \cdot 15121$	-7	-1
178	12327121	3511^2	n ist Quadrat	
179	13057787	$467 \cdot 27961$	5	-1
180	13216141	$29 \cdot 37 \cdot 109 \cdot 113$	-23	-1
181	13338371	$3163 \cdot 4217$	-11	-1
182	13421773	$53 \cdot 157 \cdot 1613$	5	-1
183	13446253	$509 \cdot 26417$	5	-1
184	13500313	$103 \cdot 131071$	5	-1
185	13635289	$739 \cdot 18451$	-7	-1
186	13694761	$2617 \cdot 5233$	-7	-1
187	13747361	$2141 \cdot 6421$	-7	-1
188	14179537	$2917 \cdot 4861$	5	-1
189	14324473	$1693 \cdot 8461$	5	-1
190	14709241	$631 \cdot 23311$	-11	-1
191	14794081	$2221 \cdot 6661$	-23	-1
192	14865121	$241 \cdot 61681$	-7	-1
193	15101893	$829 \cdot 18217$	5	-1
194	15139199	$2383 \cdot 6353$	-7	-1
195	15188557	$1949 \cdot 7793$	5	-1
196	15220951	$151 \cdot 100801$	13	-1
197	15247621	$61 \cdot 181 \cdot 1381$	-31	-1
198	15479777	$587 \cdot 26371$	5	-1
199	15510041	$29 \cdot 113 \cdot 4733$	-11	-1
200	15603391	$89 \cdot 199 \cdot 881$	-7	-1

Das betragsmäßig größte D hier war $D = -43$ (für die 60. Zahl).

9. Gibt es Gegenbeispiele zum BPSW-Test?

Die nachfolgenden Ideen gehen auf Pomerance zurück:
Carl Pomerance. Are there counter-examples to the Baillie-PSW primality test? (dopo.pdf)

Bemerkung: Eine ungerade natürliche Zahl $n \geq 3$ besteht den Miller-Rabin-Test zur Basis 2, wenn mit $n-1 = 2^\ell u$ und $u \equiv 1 \bmod 2$ gilt

$$2^u \equiv 1 \bmod n \quad \text{oder} \quad 2^{2^i u} \equiv -1 \bmod n \text{ für ein } i \in \{0, \ldots, \ell-1\}.$$

Nun ist $2^{\ell-1}u = \frac{n-1}{2}$. Gilt also

$$2^{\frac{n-1}{2}} \equiv -1 \bmod n,$$

so besteht n den Miller-Rabin-Test zur Basis 2. Dies wird in folgendem Lemma benutzt:

LEMMA. *Sei $r \geq 3$ ungerade, seien $p_1, \ldots, p_r$ verschiedene Primzahlen $p_i \equiv 3 \bmod 8$, sodass für $n = p_1 \ldots p_r$ gilt*

$$p_i - 1 \mid n-1 \text{ für alle } i = 1, \ldots, r.$$

Dann gilt

$$2^{\frac{n-1}{2}} \equiv -1 \bmod n,$$

insbesondere besteht n den Miller-Rabin-Test zur Basis 2. (Außerdem ist n eine Carmichael-Zahl.)

Beweis:

(1) Wegen $p_i \equiv 3 \bmod 8$ ist $\left(\frac{2}{p_i}\right) = -1$ und damit

$$2^{\frac{p_i-1}{2}} \equiv \left(\frac{2}{p_i}\right) \equiv -1 \bmod p_i.$$

(2) Da r ungerade ist, folgt mit $p_i \equiv 3 \bmod 4$

$$n \equiv p_1 \ldots p_r \equiv 3^r \equiv (-1)^r \equiv -1 \equiv 3 \bmod 4,$$

also

$$\frac{n-1}{2} \equiv 1 \bmod 2.$$

Da mit $p_i - 1 \mid n-1$ auch $\frac{p_i-1}{2} \mid \frac{n-1}{2}$ gilt, ergibt sich (als Teiler einer ungeraden Zahl)

$$\frac{\frac{n-1}{2}}{\frac{p_i-1}{2}} \equiv 1 \bmod 2$$

und damit durch Potenzieren

$$2^{\frac{n-1}{2}} \equiv \left(2^{\frac{p_i-1}{2}}\right)^{\frac{\frac{n-1}{2}}{\frac{p_i-1}{2}}} \equiv (-1)^{\frac{\frac{n-1}{2}}{\frac{p_i-1}{2}}} \equiv -1 \bmod p_i.$$

Dies ergibt nun die Behauptung

$$2^{\frac{n-1}{2}} \equiv -1 \bmod n.$$

(3) Nach Voraussetzung ist n zusammengesetzt, quadratfrei, außerdem gilt für alle Primteiler p von n die Beziehung $p-1 \mid n-1$. Nach dem Korselt-Kriterium ist n daher eine Carmichael-Zahl. ■

Beispiele: Wir haben alle Primzahlen $p \leq 10^5$ mit $p \equiv 3 \bmod 8$ bestimmt:

$3, 11, 19, 43, 59, 67, 83, 107, 131, 139, 163, 179, 211, 227, 251, 283, 307, 331, 347, 379, 419, 443, 467, 491, 499, \ldots$

(Es gibt 2409 Primzahlen $\leq 10^5$, die $\equiv 3 \bmod 8$ sind.) Dann haben wir getestet, für welche drei Primzahlen $p_1 < p_2 < p_3$ (aus dieser Liste) und $n = p_1p_2p_3$ die Beziehung $p_i - 1 \mid n - 1$ für $i = 1, 2, 3$ gilt. Folgende Beispiele haben wir gefunden:

$n = p_1p_2p_3$ mit $p_i - 1 \mid n - 1$	p_1	p_2	p_3
48354810571	331	2971	49171
46493311411	547	2731	31123
37870128451	619	2267	26987
245291853691	1171	10531	19891
4963134761131	4243	21211	55147
4525783922251	4651	23251	41851
2152302898747	6763	10627	29947
4443982738651	7411	19267	31123
5811733744867	8219	22307	31699
22139875582819	11443	26699	72467

Beim Baillie-PSW-Test wird zuerst getestet, ob n den Miller-Rabin-Test zur Basis 2 besteht. Wenn ja, wird in der Folge $5, -7, 9, -11, 13, -15, \ldots$ die erste Zahl D bestimmt mit $\left(\frac{D}{n}\right) = -1$. Dann setzt man $P = 1$, $Q = \frac{1-D}{4}$ und testet, ob $U_{n+1}(P, Q) \equiv 0 \bmod n$ gilt. Ist $\left(\frac{5}{n}\right) = -1$, so ist $P = 1$, $Q = -1$, $(U_i(1, -1))_{i\geq 0}$ die Fibonacci-Folge. Wir formulieren Bedingungen an n, dass n diesen Test erfüllt.

LEMMA. *Sei $r \geq 3$ ungerade, seien $p_1, \ldots, p_r$ verschiedene ungerade Primzahlen mit $p_i \equiv 2$ oder $3 \bmod 5$ und $n = p_1 \ldots p_r$, sodass gilt*

$$p_i + 1 \mid n + 1 \text{ für alle } i = 1, \ldots, r.$$

Dann gilt

$$\left(\frac{5}{n}\right) = -1 \quad \text{und} \quad U_{n+1}(1, -1) \equiv 0 \bmod n.$$

(n besteht also den Lucas-Test zum Parameterpaar $(P, Q) = (1, -1)$.)

Beweis:

(1) Wegen $p_i \equiv 2, 3 \bmod 5$ ist

$$\left(\frac{5}{p_i}\right) = \left(\frac{p_i}{5}\right) = -1 \text{ für } i = 1, \ldots, r,$$

und daher wegen $r \equiv 1 \bmod 2$

$$\left(\frac{5}{n}\right) = \left(\frac{5}{p_1 \ldots p_r}\right) = \left(\frac{5}{p_1}\right) \ldots \left(\frac{5}{p_r}\right) = (-1)^r = -1.$$

(2) Für $(P, Q) = (1, -1)$ ist $D = P^2 - 4Q = 5$. Wegen $\left(\frac{D}{p_i}\right) = -1$ gilt daher

$$U_{k(p_i+1)}(1, -1) \equiv 0 \bmod p_i \text{ für alle } k \in \mathbb{N}_0 \text{ und } i = 1, \ldots, r.$$

Die Voraussetzung $p_i + 1 \mid n + 1$ impliziert sofort

$$U_{n+1}(1, -1) \equiv 0 \bmod p_i \text{ für } i = 1, \ldots, r,$$

und damit natürlich auch

$$U_{n+1}(1, -1) \equiv 0 \bmod n,$$

wie behauptet. ■

Beispiele: Wir haben alle Primzahlen $\leq 10^4$ bestimmt, die $\equiv 2, 3 \bmod 5$ sind:

$$3, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 103, 107, 113, 127, 137, 157, 163, 167, 173, 193, 197, \ldots$$

(Es gibt 618 dieser Primzahlen.) Dann haben wir getestet, für welche drei Primzahlen $p_1 < p_2 < p_3$ (aus dieser Liste) und $n = p_1p_2p_3$ die Beziehung $p_i + 1 \mid n + 1$ für $i = 1, 2, 3$ gilt. Folgende Beispiele haben wir gefunden:

$n = p_1p_2p_3$ mit $p_i + 1 \mid n + 1$	p_1	p_2	p_3
104663	13	83	97
90287	17	47	113
1811687	23	227	347
4681247	47	103	967
190137023	53	863	4157
161516543	97	293	5683
2953352063	103	5303	5407
800484227	107	1907	3923
1877893247	127	2687	5503
1296364607	197	1583	4157
282639743	227	683	1823
789206183	233	467	7253
563601257	257	773	2837
13647432707	257	5417	9803
1915827647	283	1987	3407
4388676767	293	2477	6047
3331739423	317	2543	4133
843018643	337	883	2833
8046928343	353	2477	9203
4829213843	467	1637	6317
11194977863	643	3863	4507
4469435207	683	1367	4787
20415870143	947	2843	7583
18809998367	1103	2207	7727

Kombinieren wir die beiden vorangegangenen Lemmas, so erhalten wir folgendes Ergebnis:

LEMMA. *Sei $r \geq 3$ ungerade, seien $p_1, \ldots, p_r$ verschiedene Primzahlen mit $p_i \equiv 3 \bmod 8$ und $p_i \equiv 2, 3 \bmod 5$, sodass mit $n = p_1 \ldots p_r$ gilt*

$$p_i - 1 \mid n - 1, \quad p_i + 1 \mid n + 1 \quad \text{für } i = 1, \ldots, r.$$

Dann folgt

$$2^{\frac{n-1}{2}} \equiv -1 \bmod n, \quad \left(\frac{5}{n}\right) = -1, \quad U_{n+1}(1, -1) \equiv 0 \bmod n.$$

Insbesondere erfüllt n den Baillie-PSW-Test.

Beispiele: Wir haben alle Primzahlen $\leq 10^6$ bestimmt, die $\equiv 3 \bmod 8$ und $\equiv 2, 3 \bmod 5$ sind:

$$3, 43, 67, 83, 107, 163, 227, 283, 307, 347, 443, 467, 523, 547, 563, 587, \ldots$$

(Es gibt 9807 Stück), dann zu Tripeln $p_1 < p_2 < p_3$ die Zahl $n = p_1p_2p_3$ gebildet und den Vektor

$$\begin{aligned} v \quad = \quad & ((n-1) \bmod (p_1 - 1), (n-1) \bmod (p_2 - 1), (n-1) \bmod (p_3 - 1), \\ & (n+1) \bmod (p_1 + 1), (n+1) \bmod (p_2 + 1), (n+1) \bmod (p_3 + 1)) \end{aligned}$$

dazu bestimmt. Wir haben nach Fällen gesucht, bei denen v mindestens 4 Nullen enthält. Gefunden haben wir:

$n = p_1p_2p_3$	p_1	p_2	p_3	v
46520126267	83	587	954827	$(0, 0, 48720, 0, 0, 906108)$

Es kann aber sein, dass es noch mehr Fälle gibt, da wir nach einiger Zeit das Programm abgebrochen haben.

Das folgende Lemma zeigt, dass man mit nur 3 Primfaktoren keinen Erfolg haben kann.

LEMMA. *Gegeben seien drei Primzahlen $p_1 < p_2 < p_3$ mit $p_i \equiv 3 \bmod 8$ und $n = p_1p_2p_3$. Dann gilt*

$$p_3 - 1 \nmid n - 1 \quad \textit{oder} \quad p_3 + 1 \nmid n + 1.$$

Beweis: Wir nehmen an, es gilt $p_3 - 1 \mid n - 1$ und $p_3 + 1 \mid n + 1$. Es ist

$$n - 1 = p_1p_2p_3 - 1 = p_1p_2(p_3 - 1) + (p_1p_2 - 1)$$

und

$$n + 1 = p_1p_2p_3 + 1 = p_1p_2(p_3 + 1) - (p_1p_2 - 1).$$

Aus $p_3 - 1 \mid n - 1$ und $p_3 + 1 \mid n + 1$ folgt dann

$$p_3 - 1 \mid p_1p_2 - 1 \quad \text{und} \quad p_3 + 1 \mid p_1p_1 - 1.$$

Es ist $\mathrm{ggT}(p_3 - 1, p_3 + 1) = 2$. Da $\frac{p_3-1}{2}$ und $\frac{p_3+1}{4}$ ungerade natürliche Zahlen sind, folgt

$$\mathrm{ggT}(\frac{p_3 - 1}{2}, \frac{p_3 + 1}{4}) = 1,$$

und damit

$$\frac{p_3 - 1}{2} \cdot \frac{p_3 + 1}{4} \mid p_1p_2 - 1.$$

Da $p_1p_2 - 1$ durch 8 teilbar ist, folgt

$$8 \cdot \frac{p_3 - 1}{2} \cdot \frac{p_3 + 1}{4} \mid p_1p_2 - 1$$

und damit schließlich

$$p_3^2 - 1 \mid p_1p_2 - 1.$$

Daraus ergibt sich $p_3^2 - 1 \leq p_1p_2 - 1$ und daraus der Widerspruch $p_3^2 \leq p_1p_2 < p_3^2$. Die Annahme ist also falsch, was dann die Behauptung beweist. ■

Der Pomerance-Ansatz beruht auf folgendem Lemma:

LEMMA. *Sei $T \in \mathbb{N}$ und $k \in \mathbb{N}_{\geq 2}$. Dazu wird definiert*

$$Q_1 = \prod_{\substack{q\,prim \\ q<T \\ q\equiv 1 \bmod 4}} q \quad \textit{und} \quad Q_3 = \prod_{\substack{q\,prim \\ q<T \\ q\equiv 3 \bmod 4}} q.$$

Sei $P_k(T)$ die Menge der Primzahlen p, die folgende Eigenschaften haben:

1. $T \leq p \leq T^k$.
2. $p \equiv 3 \bmod 8$.
3. $p \equiv 2$ *oder* $3 \bmod 5$.
4. $\frac{p-1}{2} \mid Q_1$. *(Anders ausgedrückt: $\frac{p-1}{2}$ ist quadratfrei und setzt sich nur aus Primzahlen $q < T$ mit $q \equiv 1 \bmod 4$ zusammen.)*
5. $\frac{p+1}{4} \mid Q_3$. *(Anders ausgedrückt: $\frac{p+1}{4}$ ist quadratfrei und setzt sich nur aus Primzahlen $q < T$ mit $q \equiv 3 \bmod 4$ zusammen.)*

Ist nun $r \geq 3$, sind $p_1, \ldots, p_r$ paarweise verschiedene Elemente von $P_k(T)$, sodass für $n = p_1 \ldots p_r$ gilt

$$n \equiv 1 \bmod Q_1 \quad \textit{und} \quad n \equiv -1 \bmod Q_3,$$

so erfüllt n den Baillie-PSW-Test.

Beweis: Wir müssen nur noch nachweisen, dass die Vorausetzungen des vorletzten Lemmas erfüllt sind, also

$$p_i - 1 \mid n - 1 \text{ und } p_i + 1 \mid n + 1 \text{ für } i = 1, \ldots, r.$$

(1) Nach Konstruktion gilt $\frac{p_i-1}{2} \mid Q_1$. Aus $n \equiv 1 \bmod Q_1$ folgt $Q_1 \mid n-1$, also

$$\frac{p_i-1}{2} \mid n-1.$$

Da $\frac{p_i-1}{2}$ ungerade, $n-1$ aber gerade ist, folgt

$$2 \cdot \frac{p_i-1}{2} \mid n-1, \quad \text{also} \quad p_i - 1 \mid n-1.$$

(2) Nach Konstruktion gilt $\frac{p_i+1}{4} \mid Q_3$. Aus $n \equiv -1 \bmod Q_3$ folgt $Q_3 \mid n+1$. Damit ergibt sich

$$\frac{p_i+1}{4} \mid n+1.$$

Da aber $\frac{p_i+1}{4}$ ungerade und $n+1$ durch 4 teilbar ist, folgt

$$4 \cdot \frac{p_i+1}{4} \mid n+1, \quad \text{also} \quad p_i + 1 \mid n+1.$$

Daher sind die Voraussetzungen des vorletzten Lemmas erfüllt. Also erfüllt n den Baillie-PSW-Test. ■

Pomerance hat heuristisch argumentiert, dass sich bei geeigneter Parameterwahl für T und k Zahlen n finden lassen sollten, die zusammengesetzt sind, aber den BPSW-Test bestehen. Bisher wurde aber weder ein explizites Beispiel gefunden noch bewiesen, dass eines existieren muss. Das folgende Beispiel soll einen Eindruck von der Problemstellung geben:

Beispiel: $T = 500$, $k = 3$. Dann ist

$$\begin{aligned} Q_1 &= \prod_{\substack{q \text{ prim} \\ q<T \\ q \equiv 1 \bmod 4}} q = \\ &= 639658903780233725308369667090104458894117477589862107443046377277023188806310245487183621512950 5, \\ Q_3 &= \prod_{\substack{q \text{ prim} \\ q<T \\ q \equiv 3 \bmod 4}} q = \\ &= 975883587200560042454143201872069648416438691125144595280987328948455790006468299415743755218669908233104898 9. \end{aligned}$$

Die Menge $P_3(500)$ enthält 24 Primzahlen:

$$\begin{aligned} P_3(500) = \{&563, 5987, 10427, 11867, 29867, 40763, 67307, 73883, 123323, 129083, 203627, 281867, \\ &479027, 893147, 1558307, 4999187, 5696123, 6208067, 9693947, 14472803, 17182283, \\ &19821107, 19852067, 32604563\}, \end{aligned}$$

die wir uns durchnummeriert denken:

$$P_3(500) = \{p_1, \ldots, p_{24}\}.$$

Es gibt 2^{24} Teilmengen von $P_3(500)$. Jeder Teilmenge $M \subseteq P_3(500)$ ordnet man die Zahl

$$n_M = \prod_{p \in M} p$$

zu. Praktisch lassen sich die Teilmengen durch die ganzen Zahlen $z \in \{0, \ldots, 2^{24}-1\}$ wie folgt parametrisieren: Man schreibt

$$z = \sum_{i=0}^{23} z_i \cdot 2^i \text{ mit } z_i \in \{0,1\}$$

und hat dann

$$M_z = \{p_i \in P_3(500) : z_i = 1\}.$$

Dazu bildet man

$$n_z = \prod_{p \in M_z} p = \prod_{\substack{0 \le i \le 23 \\ z_i = 1}} p_i.$$

Für alle diese 2^{24} Zahlen n_z muss man testen, ob

$$n_z \equiv 1 \bmod Q_1 \quad \text{und} \quad n_z \equiv -1 \bmod Q_3$$

gilt.
Ergebnisse:

- Es gibt 26255 Zahlen n_z mit $n_z + 1 \ge Q_3$. (Nur für solche Zahlen n gilt möglicherweise $n \equiv -1 \bmod Q_3$.)
- Nur eine Zahl n_z erfüllt $n_z \equiv 1 \bmod Q_1$, nämlich $n_0 = 1$.
- Keine Zahl n_z genügt der Bedingung $n_z \equiv -1 \bmod Q_3$.

10. Primzahlbeweise mit Lucas-Folgen

Wir haben verschiedene Primzahltests kennengelernt, deren Ergebnis für eine Zahl n die Aussage „n ist zusammengesetzt“ oder “n ist wahrscheinlich prim“ ist. Im Folgenden stellen wir zwei Verfahren vor, mit denen man zeigen kann, dass eine Zahl n tatsächlich eine Primzahl und nicht nur wahrscheinlich prim ist. Sie beruhen allerdings darauf, dass man die Faktorisierung von $n-1$ bzw. $n+1$ kennt, was natürlich bei großen Zahlen im Allgemeinen nicht der Fall sein wird.

Satz. *Sei $n \in \mathbb{N}$, $n \ge 3$. Von der Zahl $n-1$ sei die Primfaktorzerlegung bekannt:*

$$n - 1 = q_1^{e_1} \dots q_r^{e_r}.$$

Findet man nun ein $a \in \mathbb{Z}$ mit

$$a^{n-1} \equiv 1 \bmod n \quad \textit{und} \quad a^{\frac{n-1}{q_i}} \not\equiv 1 \bmod n \textit{ für alle } i = 1, \dots, r,$$

so ist n eine Primzahl. (Außerdem ist dann a eine Primitivwurzel modulo n.)

Beweis: Für a gilt $\operatorname{ord}_n(a) = n - 1$, weswegen n eine Primzahl und a eine Primitivwurzel von n ist. ■

Beispiel: Für

$$n = 165593888434429117491978522389872339436583406091281126055799731632036481250000001$$

gilt

$$n - 1 = 2^6 \cdot 3^9 \cdot 5^{10} \cdot 7^{14} \cdot 11^{14} \cdot 13^{13} \cdot 17^7 \cdot 19^{13}.$$

Durch Ausprobieren findet man, dass für $a = 83$ die Voraussetzungen des Satzes erfüllt sind, also ist n eine Primzahl.

Mit Lucas-Folgen kann man nun auch Primzahlbeweise für Zahlen n geben, wenn man die Faktorisierung von $n+1$ kennt:

Satz. *Sei $n \in \mathbb{N}$ ungerade und $n \ge 3$. Von $n+1$ sei die Primfaktorzerlegung bekannt:*

$$n + 1 = q_1^{e_1} \dots q_r^{e_r}.$$

Findet man $P, Q \in \mathbb{Z}$, $D = P^2 - 4Q$ mit $\operatorname{ggT}(n, QD) = 1$ und

$$U_{n+1}(P,Q) \equiv 0 \bmod n \quad \textit{und} \quad \operatorname{ggT}(n, U_{\frac{n+1}{q_i}}(P,Q)) = 1 \textit{ für alle } i = 1, \dots, r,$$

so ist n eine Primzahl. (Außerdem gilt dann $\left(\frac{D}{n}\right) = -1$.)

Beweis: Sei p ein Primteiler von n. Dann gilt

$$U_{n+1}(P,Q) \equiv 0 \bmod p \quad \text{und} \quad U_{\frac{n+1}{q_i}}(P,Q) \not\equiv 0 \bmod p \text{ für alle } i = 1,\dots,r.$$

Wir betrachten die Situation in $\mathbb{F}_p$ bzw. $\overline{\mathbb{F}}_p$. Sind α und β die Nullstellen von $x^2 - Px + Q$ in $\overline{F}_p$, so gilt $\alpha \neq 0$, $\beta \neq 0$, $\alpha \neq \beta$ (wegen $\mathrm{ggT}(n, QD) = 1$) und wir können schreiben

$$U_i = \frac{\alpha^i - \beta^i}{\alpha - \beta}.$$

Die angegebenen Kongruenzen modulo p werden nun zu

$$\alpha^{n+1} = \beta^{n+1} \quad \text{und} \quad \alpha^{\frac{n+1}{q_i}} \neq \beta^{\frac{n+1}{q_i}} \text{ für alle } i = 1,\dots,r,$$

also

$$(\frac{\alpha}{\beta})^{n+1} = 1 \quad \text{und} \quad (\frac{\alpha}{\beta})^{\frac{n+1}{q_i}} \neq 1 \text{ für alle } i = 1,\dots,r.$$

Es folgt für die (multiplikative) Ordnung von $\frac{\alpha}{\beta}$ in $\overline{\mathbb{F}}_p^*$

$$\mathrm{ord}\,(\frac{\alpha}{\beta}) = n + 1.$$

Nun gibt es zwei Fälle, die wir zuvor bereits untersucht hatten:

- **Fall $\left(\frac{D}{p}\right) = 1$:** Hier gilt $(\frac{\alpha}{\beta})^{p-1} = 1$, also $\mathrm{ord}\,(\frac{\alpha}{\beta}) \mid p-1$ was zu $n+1 \mid p-1$, einem offensichtlichen Widerspruch führt. Dieser Fall kann also nicht eintreten.
- **Fall $\left(\frac{D}{p}\right) = -1$:** Hier haben wir gesehen, dass gilt $(\frac{\alpha}{\beta})^{p+1} = 1$. Es folgt $\mathrm{ord}\,(\frac{\alpha}{\beta}) \mid p+1$, und damit
$$n + 1 \mid p + 1,$$
was wegen $p \mid n$ sofort $n = p$ liefert. Daher ist n eine Primzahl. Außerdem gilt $\left(\frac{D}{n}\right) = \left(\frac{D}{p}\right) = -1$. Damit ist die Behauptung bewiesen. ■

Beispiele:

(1) Für
$$n = 984532715207418452877375371682884999999$$
gilt
$$n + 1 = 2^7 \cdot 3^2 \cdot 5^8 \cdot 7^{11} \cdot 11^5 \cdot 13^5 \cdot 17^5 \cdot 19^4.$$
Einen Primzahlbeweis erhält man für $(P, Q) = (24, 145)$ zu $D = -4$.

(2) Für
$$n = 42208862717429306425545096913093781450420634140325393055620881249999999$$
gilt
$$n + 1 = 2^6 \cdot 3^4 \cdot 5^{10} \cdot 7^{11} \cdot 11^9 \cdot 13^8 \cdot 17^{13} \cdot 19^{12}$$
Einen Primzahlbeweise erhält man für $(P, Q) = (18, 82)$ mit $D = -4$.

(3) Für
$$n = 346233894398346499741706582703226214950276020875031713480999999999999999$$
gilt
$$n + 1 = 2^{13} \cdot 3^{10} \cdot 5^{13} \cdot 7^{12} \cdot 11^{10} \cdot 13^{10} \cdot 17^8 \cdot 19^8$$
Einen Primzahlbeweise erhält man für $(P, Q) = (24, 145)$ mit $D = -4$.

(4) Für
$$n = 233636357073018178850877016249890477602235210297479543793754871999999 9$$
gilt
$$n + 1 = 2^{10} \cdot 3^8 \cdot 5^7 \cdot 7^{14} \cdot 11^9 \cdot 13^9 \cdot 17^9 \cdot 19^{12}$$
Einen Primzahlbeweise erhält man für $(P, Q) = (40, 401)$ mit $D = -4$.

(5) Für

$$n = 145399920326069781176815391091013236709426444839945910480469999999999$$

gilt

$$n+1 = 2^{11} \cdot 3^{16} \cdot 5^{11} \cdot 7^{10} \cdot 11^{7} \cdot 13^{11} \cdot 17^{10} \cdot 19^{8}$$

Einen Primzahlbeweise erhält man für $(P,Q) = (18, 82)$ mit $D = -4$.

(6) Für

$$n = 247057118869575691260137741568902083601185845117717073774997999999999$$

gilt

$$n+1 = 2^{11} \cdot 3^{8} \cdot 5^{10} \cdot 7^{12} \cdot 11^{10} \cdot 13^{12} \cdot 17^{8} \cdot 19^{9}$$

Einen Primzahlbeweise erhält man für $(P,Q) = (24, 145)$ mit $D = -4$.

Bemerkung: Die Zahl $n = 399 = 3{\cdot}7{\cdot}19$ erfüllt für alle P, Q mit $0 \le P, Q \le n-1$ und $D = P^2 - 4Q = -4$ die Beziehung $U_{n+1}(P,Q) \equiv 0 \bmod n$.

Bemerkung: Zahlen n, bei denen $n+1$ eine besonders einfache Primfaktorzerlegung hat, sind die Mersenne-Zahlen

$$n = 2^k - 1.$$

Da wir uns für Primzahlen interessieren, erwähnen wir folgendes Lemma:

LEMMA. *Ist für $k \in \mathbb{N}$ die Zahl $n = 2^k - 1$ eine Primzahl, so ist auch k eine Primzahl.*

Beweis: Wir können uns auf $k \ge 2$ beschränken. Sei k zusammengesetzt. Wir müssen zeigen, dass n auch zusammengesetzt ist. Sei $k = lm$ mit $1 < l < k$ und $d = 2^l - 1$. Dann ist $d > 1$ und modulo d gilt

$$2^l \equiv 1 \bmod d, \quad \text{also} \quad 2^k \equiv (2^l)^m \equiv 1 \bmod d,$$

woraus $d \mid n$ folgt. Da $d < n$ ist, ist d ein nichttrivialer Teiler von n, n also zusammengesetzt. ■

Überlegung: Wir betrachten also Primzahlen ℓ und dazu $n = 2^\ell - 1$. Wegen $\ell \ge 2$ ist $n \equiv 3 \bmod 4$ und damit gilt

$$\left(\frac{-4}{n}\right) = -1.$$

Wir wählen also P gerade und setzen $Q = (\frac{P}{2})^2 + 1$. Dann ist nämlich $D = P^2 - 4Q = P^2 - 4{\cdot}(\frac{P^2}{4} + 1) = -4$. Nun testen wir, ob

$$U_{n+1}(P,Q) \equiv 0 \bmod n$$

gilt. Wenn nein, besteht n den Lucas-Test zum Parameterpaar (P,Q) nicht, ist also zusammengesetzt. Wenn ja, betrachten wir

$$U_{\frac{n+1}{2}}(P,Q) \not\equiv 0 \bmod n \quad \text{bzw.} \quad \mathrm{ggT}(n, U_{\frac{n+1}{2}}(P,Q)).$$

Es gibt drei Fälle:

- **Fall** $\mathrm{ggT}(n, U_{\frac{n+1}{2}}(P,Q)) = 1$**:** Dann ist n eine Primzahl.
- **Fall** $\mathrm{ggT}(n, U_{\frac{n+1}{2}}(P,Q)) \in \{2, \ldots, n-1\}$**:** Dann ist n zusammengesetzt (und der berechnete ggT liefert eine erste Zerlegung von n).
- **Fall** $\mathrm{ggT}(n, U_{\frac{n+1}{2}}(P,Q)) = n$**:** Dann gilt $U_{\frac{n+1}{2}}(P,Q) \equiv 0 \bmod n$. Hier können wir nichts sagen, wir nehmen ein neues P.

Im Folgenden haben wir mit $P = 2$ begonnen und dann - bei Misserfolg - P jeweils um 2 erhöht. Zunächst haben wir die Primzahlen $2 \leq \ell \leq 97$ untersucht:

ℓ	$2^\ell - 1$	prim oder nicht prim	D	P	Q
2	3	prim	-4	2	2
3	7	prim	-4	4	5
5	31	prim	-4	8	17
7	127	prim	-4	4	5
11	2047	nicht prim	-4	4	5
13	8191	prim	-4	8	17
17	131071	prim	-4	10	26
19	524287	prim	-4	4	5
23	8388607	nicht prim	-4	4	5
29	536870911	nicht prim	-4	4	5
31	2147483647	prim	-4	4	5
37	137438953471	nicht prim	-4	4	5
41	2199023255551	nicht prim	-4	4	5
43	8796093022207	nicht prim	-4	4	5
47	140737488355327	nicht prim	-4	4	5
53	9007199254740991	nicht prim	-4	4	5
59	576460752303423487	nicht prim	-4	4	5
61	2305843009213693951	prim	-4	8	17
67	147573952589676412927	nicht prim	-4	4	5
71	2361183241434822606847	nicht prim	-4	4	5
73	9444732965739290427391	nicht prim	-4	4	5
79	604462909807314587353087	nicht prim	-4	4	5
83	967140655691703339764940 7	nicht prim	-4	4	5
89	618970019642690137449562111	prim	-4	10	26
97	158456325028528675187087900671	nicht prim	-4	4	5

Im nächsten Fall haben wir die Primzahlen mit $2 \leq \ell \leq 10000$ angeschaut. Es konnte immer entschieden werden, ob $2^\ell - 1$ prim oder zusammengesetzt ist:

- Ist $2^\ell - 1$ nicht prim (und $2 \leq \ell \leq 10000$), so besteht $2^\ell - 1$ den Lucas-Test zum Parameterpaar $(P, Q) = (4, 5)$ nicht, d.h.

$$U_{n+1}(4, 5) \not\equiv 0 \bmod n.$$

- Ist $2^\ell - 1$ prim, so mussten wir etwas mehr suchen. Diese Fälle sind in folgender Tabelle aufgeführt:

ℓ	prim oder nicht prim	D	P	Q
2	prim	-4	2	2
3	prim	-4	4	5
5	prim	-4	8	17
7	prim	-4	4	5
13	prim	-4	8	17
17	prim	-4	10	26
19	prim	-4	4	5
31	prim	-4	4	5
61	prim	-4	8	17
89	prim	-4	10	26
107	prim	-4	4	5
127	prim	-4	4	5
521	prim	-4	10	26
607	prim	-4	4	5
1279	prim	-4	4	5
2203	prim	-4	4	5
2281	prim	-4	12	37
3217	prim	-4	12	37
4253	prim	-4	8	17
4423	prim	-4	4	5
9689	prim	-4	10	26
9941	prim	-4	8	17

(Hier stellt sich die Frage: Ist $2^\ell - 1$ genau dann prim, wenn $U_{n+1}(4,5) \equiv 0 \bmod n$ gilt? Keine Ahnung!)

11. Der Lucas-Lehmer-Test für Mersenne-Zahlen

LEMMA. *Sei $\ell \geq 2$ und $n = 2^\ell - 1$ und*

$$V_{2^{\ell-2}}(4,1) \equiv 0 \bmod n.$$

Dann ist n eine Primzahl.

Bemerkung: Für $\ell = 2$ ist $n = 2^2 - 1 = 3$, aber $V_1(4,1) = 4 \equiv 1 \bmod 3$. Die Voraussetzung des Lemmas ist in diesem Fall also nicht erfüllt.

Beweis des Lemmas:

(1) Sei p ein Primteiler von n. Dann gilt $V_{2^{\ell-2}}(4,1) \equiv 0 \bmod p$. Wir rechnen nun in $\mathbb{F}_p$ bzw. $\overline{\mathbb{F}}_p$. Dann schreibt sich die Beziehung als $V_{2^{\ell-2}}(4,1) = 0$ (in $\mathbb{F}_p$).

(2) Sei $\sqrt{3} \in \overline{\mathbb{F}}_p$ mit $(\sqrt{3})^2 = 3$ gewählt. Definieren wir dann

$$\alpha = 2 + \sqrt{3} \quad \text{und} \quad \beta = 2 - \sqrt{3},$$

so gilt

$$\alpha + \beta = 4, \quad \alpha\beta = 1,$$

d.h. α und β sind die Nullstellen von $x^2 - 4x + 1$ in $\overline{\mathbb{F}}_p$. Es folgt

$$V_i(4,1) = \alpha^i + \beta^i \text{ für alle } i \geq 0 \text{ in } \overline{\mathbb{F}}_p.$$

(3) Die Voraussetzung $V_{2^{\ell-2}}(4,1) = 0$ impliziert

$$0 = \alpha^{2^{\ell-2}} V_{2^{\ell-2}}(4,1) = \alpha^{2^{\ell-2}} \left(\alpha^{2^{\ell-2}} + \beta^{2^{\ell-2}} \right) = \alpha^{2^{\ell-1}} + 1,$$

also

$$\alpha^{2^{\ell-1}} = -1.$$

Mit der üblichen Argumentation folgt für die Ordnung von α in $\overline{\mathbb{F}}_p^*$

$$\operatorname{ord}(\alpha) = 2^\ell, \quad \text{also} \quad \operatorname{ord}(\alpha) = n+1.$$

(4) Wir unterscheiden nun drei Fälle:

(a) **Fall $p = 3$:** In $\mathbb{F}_3$ ist $\alpha = \beta = 2 = -1$, also

$$V_i(4,1) = 2^i + 2^i = 2^{i+1} = (-1)^{i+1} \neq 0 \text{ für alle } i \geq 0.$$

Dieser Fall kann also nicht eintreten, da die Voraussetzung nicht erfüllt ist.

(b) **Fall $\left(\frac{3}{p}\right) = 1$:** 3 ist Quadrat in $\mathbb{F}_p$, d.h. $\sqrt{3} \in \mathbb{F}_p$ und damit auch $\alpha \in \mathbb{F}_p$. Wegen $\alpha\beta = 1$ ist $\alpha \neq 0$, sodass der kleine Satz von Fermat $\alpha^{p-1} = 1$ liefert, also $\operatorname{ord}(\alpha) \mid p-1$, und damit $n+1 \mid p-1$, was wegen $p \mid n$ natürlich nicht geht. Also ist dieser Fall nicht möglich.

(c) **Fall $\left(\frac{3}{p}\right) = -1$:** Mit dem Satz von Euler gilt

$$\sqrt{3}^p = \sqrt{3}^{p-1} \cdot \sqrt{3} = (\sqrt{3}^2)^{\frac{p-1}{2}} \cdot \sqrt{3} = 3^{\frac{p-1}{2}} \cdot \sqrt{3} = \left(\frac{3}{p}\right) \cdot \sqrt{3} = -\sqrt{3},$$

was mit $2^p = 2$ sofort zu

$$\alpha^p = (2+\sqrt{3})^p = 2^p + \sqrt{3}^p = 2 - \sqrt{3},$$

und damit zu

$$\alpha^{p+1} = \alpha^p \alpha = (2-\sqrt{3})(2+\sqrt{3}) = 1$$

führt. Daher gilt $\operatorname{ord}(\alpha) \mid p+1$, also

$$n+1 \mid p+1,$$

was wegen $p \mid n$ natürlich

$$n = p$$

liefert. n ist also eine Primzahl, was wir zeigen wollten. ■

Beispiele: Wir haben für $2 \leq \ell \leq 100$ das hinreichende Kriterium des Lemmas angewandt und folgende Primzahlen erhalten:

ℓ	Primzahl $2^\ell - 1$
3	7
5	31
7	127
13	8191
17	131071
19	524287
31	2147483647
61	2305843009213693951
89	618970019642690137449562111

Bemerkung: Ist die angegebene Bedingung des vorangegangenen Lemmas auch notwendig? Das folgende Lemma bejaht diese Frage. Wir formulieren es gleich etwas allgemeiner und benutzen dafür, dass im Fall $\ell \geq 2$ und $\ell \equiv 1 \bmod 2$ für $n = 2^\ell - 1$

$$2^{\ell-2} = \frac{n+1}{4}, \quad n \equiv 2^\ell - 1 \equiv -1 \equiv 7 \bmod 8 \quad \text{und} \quad n \equiv 2^\ell - 1 \equiv (-1)^\ell - 1 \equiv -1 - 1 \equiv 1 \bmod 3$$

gilt.

LEMMA. *Ist p eine Primzahl mit $p \equiv 7 \bmod 8$ und $p \equiv 1 \bmod 3$, so gilt*

$$V_{\frac{p+1}{4}}(4,1) \equiv 0 \bmod p.$$

(Mit dem chinesischen Restsatz kann man $p \equiv 7 \bmod 8$, $p \equiv 1 \bmod 3$ auch zu $p \equiv 7 \bmod 24$ zusammenfassen.)

Beweis:

(1) Die Bedingungen $p \equiv 7 \bmod 8$ und $p \equiv 1 \bmod 3$ sind genau so gemacht, dass
$$p \equiv 3 \bmod 4, \quad \left(\frac{2}{p}\right) = 1 \quad \text{und} \quad \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{1}{3}\right) = -1$$
gilt.

(2) Im Folgenden rechnen wir in $\mathbb{F}_p$ bzw. $\overline{\mathbb{F}}_p$. Wir müssen dann zeigen $V_{\frac{p+1}{4}}(4,1) = 0$ (in $\mathbb{F}_p$).

(3) Sei $\sqrt{3} \in \overline{\mathbb{F}}_p$ mit $(\sqrt{p})^2 = 3$. Mit dem Satz von Euler gilt
$$\sqrt{3}^p = \sqrt{3}^{p-1} \cdot \sqrt{3} = (\sqrt{3}^2)^{\frac{p-1}{2}} \cdot \sqrt{3} = 3^{\frac{p-1}{2}} \cdot \sqrt{3} = \left(\frac{3}{p}\right) \cdot \sqrt{3} = -\sqrt{3}.$$

(4) Setzen wir $\alpha = 2 + \sqrt{3}$ und $\beta = 2 - \sqrt{3}$, so gilt
$$\alpha + \beta = 4 \quad \text{und} \quad \alpha\beta = 1,$$
d.h. α und β sind die Nullstellen von $x^2 - 4x + 1$ in $\overline{\mathbb{F}}_p$, was insbesondere
$$V_i(4,1) = \alpha^i + \beta^i$$
impliziert. Daher gilt
$$V_{\frac{p+1}{4}}(4,1) = \alpha^{\frac{p+1}{4}} + \beta^{\frac{p+1}{4}} = \alpha^{\frac{p+1}{4}}(\alpha\beta)^{\frac{p+1}{4}} + \beta^{\frac{p+1}{4}} = \beta^{\frac{p+1}{4}}\left(\alpha^{\frac{p+1}{2}} + 1\right).$$

(5) Mit der (hier entscheidenden) Relation
$$(1+\sqrt{3})^2 = 4 + 2\sqrt{3} = 2\alpha$$
folgt (mit dem Ergebnis aus (4))
$$\begin{aligned} 2^{\frac{p+1}{2}}\alpha^{\frac{p+1}{4}}V_{\frac{p+1}{4}}(4,1) &= 2^{\frac{p+1}{2}}\left(\alpha^{\frac{p+1}{2}} + 1\right) = (2\alpha)^{\frac{p+1}{2}} + 2^{\frac{p+1}{2}} = \\ &= ((1+\sqrt{3})^2)^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} \cdot 2 = (1+\sqrt{3})^{p+1} + \left(\frac{2}{p}\right) \cdot 2 = \\ &= (1+\sqrt{3})^p(1+\sqrt{3}) + 2 = (1-\sqrt{3})(1+\sqrt{3}) + 2 = 0. \end{aligned}$$
Dies beweist die Behauptung. ■

Bemerkung: Dass auch zusammengesetzte Zahlen die Bedingungen
$$n \equiv 7 \bmod 8, \quad n \equiv 1 \bmod 3, \quad V_{\frac{n+1}{4}}(4,1) \equiv 0 \bmod n$$
erfüllen können, zeigen die Zahlen
$$1037623 = 337 \cdot 3079, \quad 2211631 = 271 \cdot 8161, \quad 4196191 = 31 \cdot 223 \cdot 607,$$
$$7076623 = 271 \cdot 26113, \quad 9100783 = 1231 \cdot 7393.$$
(Dies sind alle zusammengesetzten Zahlen $\leq 10^7$, die die angegebenen Bedingungen erfüllen.)

Wir fassen nun die beiden vorangegangenen Lemmas zusammen:

SATZ. *Sei $\ell \geq 3$ und $n = 2^\ell - 1$. Dann gilt:*
$$n \text{ ist Primzahl} \quad \Longleftrightarrow \quad V_{2^{\ell-2}}(4,1) \equiv 0 \bmod n.$$

Beweis:

$\Longrightarrow$ Sei $n = 2^\ell - 1$ eine Primzahl (und $\ell \geq 3$). Dann ist ℓ ungerade, da man sonst die nichttriviale Faktorisierung $2^\ell - 1 = (2^{\frac{\ell}{2}} - 1)(2^{\frac{\ell}{2}} + 1)$ hätte. Die Bemerkung vor dem letzten Lemma zeigt dann $n \equiv 7 \bmod 8$ und $n \equiv 1 \bmod 3$, sodass mit $\frac{n+1}{4} = 2^{\ell-2}$ das vorangegangene Lemma
$$V_{2^{\ell-2}}(4,1) \equiv V_{\frac{n+1}{4}}(4,1) \equiv 0 \bmod n$$
liefert.

$\Longleftarrow$ Dies ist der Inhalt des ersten Lemmas. ■

Bemerkung: Für $\ell \geq 3$ und $n = 2^\ell - 1$ wollen wir

$$V_{2^{\ell-2}}(4,1) \bmod n$$

berechnen. Nun gilt allgemein die Formel

$$V_{2k}(P,Q) = V_k(P,Q)^2 - 2Q^k,$$

woraus hier

$$V_{2k}(4,1) = V_k(4,1)^2 - 2$$

wird. Für $k = 2^i$ ergibt sich

$$V_{2^{i+1}}(4,1) = V_{2^i}(4,1)^2 - 2.$$

Wir definieren nun

$$v_i = V_{2^i}(4,1) \bmod n.$$

Dann ist $v_0 \equiv V_1(4,1) \equiv 4 \bmod n$ und

$$v_{i+1} \equiv V_{2^{i+1}}(4,1) \equiv V_{2^i}(4,1)^2 - 2 \equiv v_i^2 - 2 \bmod n$$

und

$$v_{\ell-2} = V_{2^{\ell-2}}(4,1) \bmod n.$$

Insbesondere lässt sich v_i rekursiv berechnen. Wir erhalten damit:

Satz (Lucas-Lehmer-Test). *Sei $\ell \geq 3$ und $n = 2^\ell - 1$. Rekursiv wird eine Folge v_i durch*

$$v_0 = 4 \quad \textit{und} \quad v_{i+1} = (v_i^2 - 2) \bmod n \textit{ für } i \geq 0$$

definiert. Dann gilt

$$n \textit{ ist Primzahl} \quad \Longleftrightarrow \quad v_{\ell-2} = 0.$$

(Es ist $v_i = V_{2^i}(4,1) \bmod n$.)

Bemerkung: Für $3 = 2^2 - 1$ funktioniert der Test nicht, da wir die Voraussetzung $\ell \geq 3$ brauchen.

Beispiele:

ℓ	$n = 2^\ell - 1$	$v_0, \ldots, v_{\ell-2}$
2	3	4,2 (Hier funktioniert der Test nicht.)
3	7	4,0
4	15	4,14,14
5	31	4,14,8,0
7	127	4,14,67,42,111,0
11	2047	4,14,194,788,701,119,1877,240,282,1736
13	8191	4,14,194,4870,3953,5970,1857,36,1294,3470,128,0

Lucas-Lehmer-Test:
Eingabe: $\ell \geq 3$
Ausgabe: $2^\ell - 1$ ist Primzahl oder zusammengesetzt

1: $n \leftarrow 2^\ell - 1$
2: $v \leftarrow 4$
3: **for** $i = 1, \ldots, \ell - 2$ **do**
4: $\quad v \leftarrow (v^2 - 2) \bmod n$
5: **end for**
6: **if** $v = 0$ **then**
7: $\quad$ **return** $2^\ell - 1$ ist Primzahl
8: **else**
9: $\quad$ **return** $2^\ell - 1$ ist zusammengesetzt
10: **end if**

Hier ist eine zugehörige Python-Funktion:

```
def lucas_lehmer_test(l):
  n=2**l-1
  v=4
  for i in range(l-2):
    v=(v**2-2)%n
  if v==0:
    return '2^'+str(l)+'-1 ist prim'
  else:
    return '2^'+str(l)+'-1 ist nicht prim'
```

Beispiele: Hier sind alle Mersenne-Primzahlen $2^\ell - 1$ mit $\ell \leq 10^4$, die wir (bis auf $2^2 - 1$) mit dem Lucas-Lehmer-Test bestimmt haben:

ℓ	$2^\ell - 1$	Dezimalstellen
3	$2^3 - 1 = 7$	1
5	$2^5 - 1 = 31$	2
7	$2^7 - 1 = 127$	3
13	$2^{13} - 1 = 8191$	4
17	$2^{17} - 1 = 131071$	6
19	$2^{19} - 1 = 524287$	6
31	$2^{31} - 1 = 2147483647$	10
61	$2^{61} - 1 = 2305843009213693951$	19
89	$2^{89} - 1 = 618970019642690137449562111$	27
107	$2^{107} - 1 = 162259276829213363391578010288127$	33
127	$2^{127} - 1 = 170141183460469231731687303715884105727$	39
521	$2^{521} - 1$	157
607	$2^{607} - 1$	183
1279	$2^{1279} - 1$	386
2203	$2^{2203} - 1$	664
2281	$2^{2281} - 1$	687
3217	$2^{3217} - 1$	969
4253	$2^{4253} - 1$	1281
4423	$2^{4423} - 1$	1332
9689	$2^{9689} - 1$	2917
9941	$2^{9941} - 1$	2993

Zur Zeit sind 51 Mersenne-Primzahlen bekannt. Die 51. wurde 2018 gefunden und ist

$$2^{82589933} - 1$$

mit

$$\left\lfloor \frac{\log(2^{82589933} - 1)}{\log(10} + 1 \right\rfloor = \left\lfloor 82589933 \cdot \frac{\log(2)}{\log(3)} + 1 \right\rfloor = 24862048$$

Dezimalstellen.

Anmerkung: Python kann zwar noch mit obiger Zahl umgehen, unser Lucas-Lehmer-Test bleibt aber bei schon bei der Berechnung von v_{26} hängen.

12. Variation von Lucas-Folgen - Lucas-Folgen mit anderen Anfangsbedingungen

SATZ. *Seien $P, Q \in \mathbb{Z}$. Dann sind die Lucas-Folgen $U_i = U_i(P, Q)$ und $V_i = V_i(P, Q)$ rekursiv durch*

$$U_0 = 0, \quad U_1 = 1, \quad U_i = PU_{i-1} - QU_{i-2} \text{ für } i \geq 2$$

und

$$V_0 = 2, \quad V_1 = P, \quad V_i = PV_{i-1} - QV_{i-2} \text{ für } i \geq 2$$

definiert. Eine Folge $T_i = T_i(P,Q)$ *werde rekursiv durch*

$$T_0 = 1, \quad T_1 = 0, \quad T_i = PT_{i-1} - QT_{i-2} \text{ für } i \geq 2$$

definiert. Sei $D = P^2 - 4Q$ *und* $\alpha = \frac{P+\sqrt{D}}{2}$, $\beta = \frac{P-\sqrt{D}}{2}$. *Dann gilt:*

(1) *Für alle* $i \geq 0$ *ist*

$$T_i = -\frac{1}{2}PU_i + \frac{1}{2}V_i.$$

(2) *Im Fall* $D = P^2 - 4Q \neq 0$ *gilt*

$$T_i = \frac{\alpha\beta^i - \alpha^i\beta}{\alpha - \beta}, \quad U_i = \frac{\alpha^i - \beta^i}{\alpha - \beta}, \quad V_i = \alpha^i + \beta^i.$$

(Dabei sei $\alpha^0 = \beta^0 = 1$.*)*

(3) *Im Fall* $D = 0$ *gilt*

$$T_i = (1-i)\cdot\alpha^i, \quad U_i = i\cdot\alpha^{i-1}, \quad V_i = 2\cdot\alpha^i.$$

(Dabei sei $\alpha^0 = 1$ *und* $0\cdot\alpha^{-1} = 0$.*)*

(4) *Sind* $X_0, X_1 \in \mathbb{Z}$ *und* X_i *rekursiv definiert durch*

$$X_i = PX_{i-1} - QX_{i-2} \text{ für } i \geq 2,$$

so gilt

$$X_i = X_0T_i + X_1U_i \text{ für alle } i \geq 0$$

und

$$X_i = (X_1 - \frac{1}{2}PX_0)U_i + \frac{1}{2}X_0V_i.$$

Beweis:

(1) Wir zeigen die Behauptung durch Induktion. Für $i = 0$ und $i = 1$ gilt

$$-\frac{1}{2}PU_0 + \frac{1}{2}V_0 = 1 = T_0 \quad \text{und} \quad -\frac{1}{2}PU_1 + \frac{1}{2}V_1 = -\frac{1}{2}P + \frac{1}{2}P = 0 = T_1,$$

sodass die Aussage für $i = 0$ und $i = 1$ stimmt. Sei nun $i \geq 2$ und die Aussage bereits für $i-1$ und $i-2$ Dann folgt

$$\begin{aligned} -\frac{1}{2}PU_i + \frac{1}{2}V_i &= -\frac{1}{2}P(PU_{i-1} - QU_{i-2}) + \frac{1}{2}(PV_{i-1} - QV_{i-2}) = \\ &= P\left(-\frac{1}{2}PU_{i-1} + \frac{1}{2}V_{i-1}\right) - Q\left(-\frac{1}{2}PU_{i-2} + \frac{1}{2}V_{i-2}\right) = \\ &= PT_{i-1} - QT_{i-2} = T_i, \end{aligned}$$

sodass die Behauptung durch Induktion folgt.

(2) Die Formeln für U_i und V_i sind bekannt. Dann folgt mit (1) und $P = \alpha + \beta$

$$\begin{aligned} T_i &= -\frac{1}{2}PU_i + \frac{1}{2}V_i = -\frac{1}{2}\cdot(\alpha+\beta)\cdot\frac{\alpha^i - \beta^i}{\alpha - \beta} + \frac{1}{2}(\alpha^i + \beta^i) = \\ &= \frac{(\alpha+\beta)(\beta^i - \alpha^i) + (\alpha-\beta)(\alpha^i + \beta^i)}{2(\alpha-\beta)} = \\ &= \frac{(\alpha\beta^i - \alpha^{i+1} + \beta^{i+1} - \alpha^i\beta) + (\alpha^{i+1} + \alpha\beta^i - \alpha^i\beta - \beta^{i+1})}{2(\alpha-\beta)} = \\ &= \frac{2\alpha\beta^i - 2\alpha^i\beta}{2(\alpha-\beta)} = \frac{\alpha\beta^i - \alpha^i\beta}{\alpha - \beta}, \end{aligned}$$

was zu zeigen war.

(3) Die Formeln für U_i und V_i sind bekannt. Wir zeigen die Aussage für T_i mit der Rekursionsformel, die sich hier wegen $P = \alpha + \beta = 2\alpha$ und $Q = \alpha\beta = \alpha^2$ in der Form

$$T_i = 2\alpha T_{i-1} - \alpha^2 T_{i-2}$$

schreiben lässt. Für $i = 0$ und $i = 1$ stimmt die Aussage. Sei nun $i \geq 2$ und die Aussage bereits für $i-1$ und $i-2$ gezeigt. Es folgt

$$\begin{aligned} T_i &= 2\alpha T_{i-1} - \alpha^2 T_{i-2} = 2\alpha(1-(i-1))\alpha^{i-1} - \alpha^2(1-(i-2))\alpha^{i-2} = \\ &= (2 - 2i + 2 - 1 + i - 2)\,\alpha^i = (1-i)\alpha^i. \end{aligned}$$

Es folgt die Behauptung.

(4) Die Richtigkeit der ersten Darstellung für X_i überprüft man zunächst für $i = 0$ und $i = 1$:

$$X_0T_0 + X_1U_0 = X_0 \quad \text{und} \quad X_0T_1 + X_1U_1 = X_1.$$

Sei nun $i \geq 2$ und die Aussage für $i-1$ und $i-2$ bereits gezeigt. Dann folgt:

$$\begin{aligned} X_0T_i + X_1U_i &= X_0(PT_{i-1} - QT_{i-2}) + X_1(PU_{i-1} - QU_{i-2}) = \\ &= P(X_0T_{i-1} + X_1U_{i-1}) - Q(X_0T_{i-2} + X_1U_{i-2}) = \\ &= PX_{i-1} - QX_{i-2} = X_i. \end{aligned}$$

Damit folgt die Behauptung durch Induktion. Mit (1) ergibt sich daraus

$$X_i = X_0T_i + X_1U_i = X_0\left(-\frac{1}{2}PU_i + \frac{1}{2}V_i\right) + X_1U_i = \left(X_1 - \frac{1}{2}PX_0\right)U_i + \frac{1}{2}X_0V_i.$$

Damit ist auch die zweite Darstellung für X_i bewiesen. ■

13. LUCAS-RSA-Verschlüsselung (LUC)

Bemerkungen:

(1) Wir erinnern zunächst an die RSA-Verschlüsselung:

(a) Der öffentliche Schlüssel einer Person A besteht aus einem Zahlenpaar (N, e), wobei $N = pq$ eine RSA-Zahl ist. Der zugehörige private Schlüssel von A ist durch die Beziehung

$$ed \equiv 1 \bmod (p-1)(q-1) \quad \text{bzw.} \quad ed \equiv 1 \bmod \varphi(N)$$

mit dem öffentlichen Schlüssel verknüpft.

(b) Will man eine Nachricht verschlüsselt an A schicken, wandelt man sie zunächst nach einem vereinbarten Schema in eine Zahlenfolge a_i mit $0 \leq a_i \leq N-1$ um, dann berechnet man

$$b_i = a_i^e \bmod N$$

und schickt die Zahlenfolge b_i an A.

(c) A erhält mit seinem privaten Schlüssel (N, d) die Zahlenfolge a_i und damit den Klartext, indem er

$$a_i = b_i^d \bmod N$$

berechnet.

Zum Verschlüsseln wird also die Funktion

$$x \mapsto x^e \bmod N,$$

zum Entschlüsseln die Funktion

$$x \mapsto x^d \bmod N$$

benutzt, wobei das Funktionieren darauf beruht, dass

$$x^{de} \equiv x \bmod N \text{ für alle } x \in \mathbb{Z}$$

gilt. Für die Sicherheit ist entscheidend, dass man aus (N, e) nicht einfach (N, d) berechnen kann.

(2) Wie kann man das verallgemeinern? Wir nehmen an, wir haben für Funktionen $f_a : \mathbb{Z} \to \mathbb{Z}$ für alle $a \in \mathbb{N}$ mit folgenden Eigenschaften:

(i) Für $x, y \in \mathbb{Z}$ gilt die Implikation

$$x \equiv y \bmod N \quad \Longrightarrow \quad f_a(x) \equiv f_a(y) \bmod N \text{ für alle } a \in \mathbb{N}.$$

(ii) Für alle $a, b \in \mathbb{N}$ gilt

$$f_a \circ f_b = f_{ab} \quad \text{und} \quad f_1 = \mathrm{id}.$$

(iii) Zu jeder Zahl $N \in \mathbb{N}$ gibt es eine Zahl $\psi(N) \in \mathbb{N}$ mit folgender Eigenschaft:

$$a \equiv 1 \bmod \psi(N) \quad \Longrightarrow \quad f_a(x) \equiv f_1(x) \bmod N \text{ für alle } x \in \mathbb{Z}.$$

Damit kann man nun Folgendes versuchen:

(a) Öffentlicher Schlüssel einer Person A ist (N, e), privater (N, d), wobei die Beziehung

$$ed \equiv 1 \bmod \psi(N)$$

gilt.

(b) Zum Verschlüsseln wird die Nachricht in eine Zahlenfolge a_i mit $0 \le a_i \le N-1$ umgewandelt, dann wird

$$b_i = f_e(a_i) \bmod N$$

berechnet und an A geschickt.

(c) A berechnet mit seinem privaten Schlüssel d

$$f_d(b_i) \bmod N$$

und erhält damit a_i wegen

$$f_d(b_i) \overset{\text{(i)}}{\equiv} f_d(f_e(a_i)) \overset{\text{(ii)}}{\equiv} f_{de}(a_i) \overset{\text{(iii)}}{\equiv} f_1(a_i) \overset{\text{(ii)}}{\equiv} a_i \bmod N.$$

Bei der klassischen RSA-Verschlüsselung werden die Potenz-Funktionen

$$f_a(x) = x^a$$

verwendet. Wir werden im Folgenden sehen, dass man auch die Funktionen

$$f_a(x) = V_a(x, 1)$$

verwenden kann.

Um das dargestellte Programm auszuführen, brauchen wir ein paar vorbereitende Lemmas:

LEMMA. *Für $P, Q, \widetilde{P}, \widetilde{Q} \in \mathbb{Z}$, $i \in \mathbb{N}_0$ und $n \in \mathbb{N}$ gilt die Implikation*

$$P \equiv \widetilde{P} \bmod n \text{ und } Q \equiv \widetilde{Q} \bmod n \quad \Longrightarrow \quad V_i(P, Q) \equiv V_i(\widetilde{P}, \widetilde{Q}) \bmod n.$$

Beweis: Dies beweist man einfach durch Induktion. ■

LEMMA. *Für $i, j \in \mathbb{N}_0$ und $P, Q \in \mathbb{Z}$ gilt*

$$V_j(V_i(P, Q), Q^i) = V_{ij}(P, Q).$$

Beweis: Sind α, β die Nullstellen von $x^2 - Px + Q$, so gilt

$$V_i(P, Q) = \alpha^i + \beta^i \quad \text{und} \quad V_{ij}(P, Q) = \alpha^{ij} + \beta^{ij}.$$

Zur Berechnung von $V_j(V_i(P, Q), Q^i)$ brauchen wir die Nullstellen von $x^2 - V_i(P, Q)x + Q^i$, die sich mit $Q = \alpha\beta$ so ergeben:

$$x^2 - V_i(P, Q)x + Q^i = x^2 - (\alpha^i + \beta^i)x + \alpha^i\beta^i = (x - \alpha^i)(x - \beta^i).$$

Daher folgt

$$V_j(V_i(P, Q), Q^i) = (\alpha^i)^j + (\beta^i)^j = \alpha^{ij} + \beta^{ij} = V_{ij}(P, Q),$$

was wir zeigen wollten. ■

Für $Q = 1$ folgt sofort:

FOLGERUNG. *Für $P \in \mathbb{Z}$, $i, j \in \mathbb{N}_0$ gilt*

$$V_j(V_i(P, 1), 1) = V_{ij}(P, 1).$$

LEMMA. *Sei p eine ungerade Primzahl. Dann gilt für $a \in \mathbb{Z}$ und $i, j \in \mathbb{N}_0$ die Implikation*

$$i \equiv j \bmod (p^2-1) \quad \Longrightarrow \quad V_i(a,1) \equiv V_j(a,1) \bmod p,$$

und insbesondere

$$i \equiv 1 \bmod (p^2-1) \quad \Longrightarrow \quad V_i(a,1) \equiv a \bmod p.$$

Beweis: Wir zeigen die entsprechenden Aussagen in $\mathbb{F}_p$ bzw. $\overline{\mathbb{F}}_p$. Seien α, β die Nullstellen des Polynoms $x^2 - ax + 1$ in $\overline{\mathbb{F}}_p$. Dann gilt

$$\alpha + \beta = a, \quad \alpha\beta = 1 \quad \text{und} \quad V_i(a,1) = \alpha^i + \beta^i.$$

Insbesondere folgt

$$\alpha \neq 0 \quad \text{und} \quad \beta = \frac{1}{\alpha}, \quad \text{also} \quad V_i(a,1) = \alpha^i + \frac{1}{\alpha^i}.$$

Der kleine Satz von Fermat liefert $a^p = a$ und damit

$$\begin{aligned} 0 &= a^p - a = (\alpha + \frac{1}{\alpha})^p - (\alpha + \frac{1}{\alpha}) = \alpha^p + \frac{1}{\alpha^p} - \alpha - \frac{1}{\alpha} = \frac{\alpha^{2p} + 1 - \alpha^{p+1} - \alpha^{p-1}}{\alpha^p} = \\ &= \frac{(\alpha^{p+1}-1)(\alpha^{p-1}-1)}{\alpha^p}, \end{aligned}$$

sodass

$$\alpha^{p+1} = 1 \quad \text{oder} \quad \alpha^{p-1} = 1$$

gilt, und damit natürlich insbesondere

$$\alpha^{p^2-1} = \alpha^{(p-1)(p+1)} = 1.$$

Seien nun $i, j \in \mathbb{N}_0$ mit $i \equiv j \bmod (p^2-1)$. O.E. können wir $i \geq j$ annehmen. Dann gibt es ein $k \in \mathbb{N}_0$ mit $i = j + k(p^2-1)$. Es folgt

$$V_i(a,1) = \alpha^i + \frac{1}{\alpha^i} = \alpha^{j+k(p^2-1)} + \frac{1}{\alpha^{j+k(p^2-1)}} = \alpha^j(\alpha^{p^2-1})^k + \frac{1}{\alpha^j(\alpha^{p^2-1})^k} = \alpha^j + \frac{1}{\alpha^j} = V_j(a,1).$$

Mit $V_1(a,1) = a$ folgt die Behauptung, wenn man die Gleichheiten in $\mathbb{F}_p$ nun als Kongruenzen in $\mathbb{Z}$ interpretiert. ■

LEMMA. *Sei $N = pq$ eine RSA-Zahl, seien $e, d \in \mathbb{N}$ mit $ed \equiv 1 \bmod (p^2-1)(q^2-1)$. Dann gilt für $a, b \in \mathbb{Z}$ die Implikation*

$$b \equiv V_e(a,1) \bmod N \quad \Longrightarrow \quad a \equiv V_d(b,1) \bmod N.$$

Beweis: Modulo N gilt

$$V_d(b,1) \equiv V_d(V_e(a,1),1) \equiv V_{ed}(a,1) \bmod N.$$

Aus $ed \equiv 1 \bmod (p^2-1)$ folgt $V_{ed}(a,1) \equiv a \bmod p$, aus $ed \equiv 1 \bmod (q^2-1)$ folgt $V_{ed}(a,1) \equiv a \bmod q$, sodass sich insgesamt $V_{ed}(a,1) \equiv a \bmod N$ und damit

$$V_d(b,1) \equiv a \bmod N$$

ergibt, was zu zeigen war. ■

Nun können wir die Theorie anwenden:

LUC-Verschlüsselung:

(1) **Schlüsselerzeugung:**
   (a) Jeder Teilnehmer A sucht sich verschiedene ungerade Primzahlen p_A, q_A, berechnet $N_A = p_A q_A$. (N_A sollte sich praktisch von einem Außenstehenden nicht faktorisieren lassen.)
   (b) A konstruiert sich mit dem erweiterten euklidischen Algorithmus Zahlen $e_A, d_A \in \mathbb{N}$ mit $e_A d_A \equiv 1 \bmod (p_A^2-1)(q_A^2-1)$. ($d_A$ sollte nicht zu klein sein.)
   (c) Öffentlicher Schlüssel von A ist (N_A, e_A), privater Schlüssel ist (N_A, d_A).

(2) **Verschlüsselung:** Will jemand eine Nachricht verschlüsselt an A schicken, geht er so vor:
   (a) Er wandelt die Nachricht nach einem vereinbarten Schema in eine Zahlenfolge a_i mit $0 \leq a_i \leq N_A - 1$ um.

(b) Mit dem öffentlichen Schlüssel (N_A, e_A) von A berechnet er

$$b_i = V_{e_A}(a_i, 1) \bmod N_A.$$

(c) Die Zahlenfolge b_i wird als Chiffretext an A geschickt.

(3) **Entschlüsselung:** A erhält also die Zahlenfolge b_i.

(a) Mit seinem privaten Schlüssel (N_A, d_A) berechnet A

$$a_i = V_{d_A}(b_i, 1) \bmod N_A.$$

(b) A wandelt die Zahlenfolge a_i nach dem vereinbarten Schema in Text um.

Bemerkungen:

(1) Natürlich sind e_A und d_A wie bei RSA immer ungerade Zahlen.
(2) 3 kommt als öffentlicher Schlüssel e_A nicht in Frage, da für jede Primzahl $p \neq 3$ gilt $p^2 \equiv 1 \bmod 3$, also $\mathrm{ggT}(3, p^2 - 1) = 3$.
(3) Die zu $e_A = 5$ und $e_A = 7$ gehörigen Verschlüsselungsabbildungen sind

$$V_5(a, 1) = a^5 - 5a^3 + 5a \quad \text{und} \quad V_7(a, 1) = a^7 - 7a^5 + 14a^3 - 7a.$$

Beispiel: Wir wählen (zufällig) Primzahlen p und q und berechnen $N = pq$:

$$\begin{aligned} p &= 44618650311848916653827678189760501422 93, \\ q &= 80411519482208715622378181410807444081 63, \\ N &= 35878534688210971463193705793594418837499541084574688962430970226723860220737759. \end{aligned}$$

Nun suchen wir die kleinste Zahle $e > 1$ mit $\mathrm{ggT}(e, (p^2 - 1)(q^2 - 1)) = 1$ und erhalten $e = 5$. Dazu berechnen wir das Inverse von e modulo $(p^2 - 1)(q^2 - 1)$ als privaten Schlüssel d:

$$\begin{aligned} e &= 5, \\ d &= 25745385027463159025295829722315398841744514861000487156272011062731681218423670 \\ &\quad 78529118207754343428104218444300811409308160810027773147969596044301719120019 33. \end{aligned}$$

(Auffällig ist die Größe von d.) Wir wollen „HEUTE IST DER LETZTE DIENSTAG IM JUNI“ verschlüsseln und wandeln dies nach unserem üblichen Verfahren (A$\leftrightarrow$ 01, …, Z$\leftrightarrow$ 26) in eine Zahl a um und berechnen dazu $b = V_5(a, 1) \bmod N$:

$$\begin{aligned} a &= 80521200500091920000405180012052026200500040905141920010700091300102 11409, \\ b &= 34570087008838797788474197077336892130998127099024323149050325777640738217992553. \end{aligned}$$

Wir werden jetzt einen Angriff auf RSA auf LUC übertragen. Wir beginnen mit einem Lemma:

LEMMA. *Seien N_1, N_2, N_3, N_4, N_5 paarweise teilerfremde natürliche Zahlen, $a \in \mathbb{Z}$ mit $0 \leq a \leq \min(N_1, N_2, N_3, N_4, N_5) - 1$ und*

$$b_i = a^5 - 5a^3 + 5a \bmod N_i \text{ für } i = 1, \ldots, 5.$$

Bestimmt man mit dem chinesischen Rest ein $c \in \mathbb{Z}$ mit

$$c \equiv \begin{cases} b_1 \bmod N_1, \\ b_2 \bmod N_2, \\ b_3 \bmod N_3, \\ b_4 \bmod N_4, \\ b_5 \bmod N_5 \end{cases} \qquad \text{und} \quad 0 \leq c \leq N_1 N_2 N_3 N_4 N_5 - 1,$$

so gilt (in $\mathbb{R}$)

$$a^5 - 5a^3 + 5a = c.$$

(a ist also eine ganzzahlige Nullstelle des Polynoms $f(x) = x^5 - 5x^3 + 5x - c$.)

Beweis: Nach Konstruktion gilt

$$c \equiv b_i \equiv a^5 - 5a^3 + 5a \bmod N_i \text{ für } i = 1, \ldots, 5,$$

und damit

$$c \equiv a^5 - 5a^3 + 5a \bmod N_1N_2N_3N_4N_5.$$

Mit etwas Kurvendiskussion sieht man, dass für $a \in \mathbb{N}_0$

$$0 \leq a^5 - 5a^3 + 5a \leq a^5$$

gilt, woraus

$$0 \leq a^5 - 5a^3 + 5a \leq a^5 < N_1N_2N_3N_4N_5$$

und damit schließlich $c = a^5 - 5a^3 + 5a$ folgt. ■

Bemerkung: Es gibt verschiedene Methoden, die ganzzahligen Nullstellen eines Polynoms $f(x) \in \mathbb{Z}[x]$ schnell zu bestimmen. SAGE macht dies mit dem Befehl `f.roots(ring=ZZ)`. Wir wollen hier noch eine einfache Intervallschachtelungsmethode vorstellen, mit der man im vorliegenden Fall eine Lösung der Gleichung

$$x^5 - 5x^3 + 5x = c$$

findet.

- Sei $f(x) = x^5 - 5x^3 + 5x$. Die Ableitung ist

  $$f'(x) = 5x^4 - 15x^2 + 5 = 5(x^4 - 3x^2) + 5 = 5x^2(x^2 - 3) + 5.$$

  Man sieht, dass f für $x \geq 2$ streng monoton steigend ist.
- Wir starten mit zwei Zahlen $a_L < a_R$, sodass f im Intervall $[a_L, a_R]$ streng monoton ist, beispielsweise $a_L = 2$ und $a_R = N_1$ (mit N_1 wie oben). Dabei sollte gelten

  $$f(a_L) < c < f(a_R).$$

- Wir berechnen $a = \left\lfloor \frac{a_L + a_R}{2} \right\rfloor$ und $f(a)$.
  - Gilt $f(a) = c$, so sind wir fertig, wir haben das gesuchte a gefunden.
  - Gilt $f(a) < c$, so setzen wir $a_L \leftarrow a$, sodass weiterhin $f(a_L) < c < f(a_R)$ gilt.
  - Gilt $f(a) > c$, so setzen wir $a_R \leftarrow a$. Dann gilt weiterhin $f(a_L) < c < f(a_R)$.

  Diesen Schritt wiederholen wir, bis wir eine Lösung haben.
- Da in jedem Schritt das Intervall $[a_L, a_R]$ ungefähr halbiert wird, findet man schnell eine Lösung.

Ein Angriff auf LUC mit dem chinesischen Restsatz:

(1) Eine Nachricht a, die in Form einer Zahl gegeben ist, geht an 5 Personen, die jeweils öffentlichen Schlüssel $(N_i, 5)$ haben:

$$b_i = V_5(a, 1) \bmod N_i.$$

(2) Wir kennen $b_1, \ldots, b_5$. Mit dem chinesischen Restsatz berechnen wir

$$c \equiv \begin{cases} b_1 \bmod N_1, \\ b_2 \bmod N_2, \\ b_3 \bmod N_3, \\ b_4 \bmod N_4, \\ b_5 \bmod N_5 \end{cases} \qquad \text{mit} \quad 0 \leq c \leq N_1N_2N_3N_4N_5 - 1.$$

(3) Dann ist a eine Nullstelle aus $\mathbb{N}_0$ des Polynoms

$$f(x) = x^5 - 5x^3 + 5x - c.$$

Beispiel: Wir haben fünf öffentliche Schlüssel $(N_i, 5)$ mit

$$\begin{aligned}
N_1 &= 605309931210697067030363872936642248814079404476762419984650437138036224633307 49,\\
N_2 &= 142467499981742172569847498025637305018560981283321377082387253460340562470469 99,\\
N_3 &= 793332086480037390311341122444407886566365266042422812367852647785784030172312 69,\\
N_4 &= 384715680862037868738891120236883959350904394256984669883367685672185172424499 1,\\
N_5 &= 142598751136068062337718737755122467388935905492303853831377251325534598540383 99.
\end{aligned}$$

Eine in eine Zahl a umgewandelte Nachricht wurde an die fünf Personen verschickt mit folgendem Chiffretext $b_i = V_5(a,1) \bmod N_i$:

$$\begin{aligned}
b_1 &= 532378081390679062449243443382119544073367626405314401321992267007336839637550 66,\\
b_2 &= 436908371084419526112590103882413973072627135931207758849602164342343727114075 7,\\
b_3 &= 166897088297172636262806697431424829469592847318266153297648225745797657795760 23,\\
b_4 &= 319748779514172005076806052215996280182106779302916646121640670869900877864574 04,\\
b_5 &= 361140683277609631852840944677773683323262398294528312284940177921672693165269 2.
\end{aligned}$$

Mit dem chinesischen Restsatz berechnen wir c mit $c \equiv b_i \bmod N_i$ für $i = 1, \ldots, 5$ und $0 \le c \le N_1N_2N_3N_4N_5 - 1$ und erhalten

$$\begin{aligned}
c = {} & 271413662829723238091862663143931450769256833540633342142918650648509893389496 12\\
& 248283597887730619666044334470914339164989117748855748461700858218579369582334 61\\
& 221523067476042741099581050445668863932309520258444282786797445582626767029799 70\\
& 530913540992956609454616781639149839367857945965924956469971396563495262981354 42\\
& 140214299377214817882905526041200845151598404122981725915370507284183430467 4
\end{aligned}$$

Sage liefert als einzige ganzzahlige Wurzel des Polynoms $f(x) = x^5 - 5x^3 + 5x - c$ die Zahl

$$122103001903080509142000140903082000020519190518000112190018190100262100190509 14.$$

Umgesetzt in Text ergibt sich „LUC SCHEINT NICHT BESSER ALS RSA ZU SEIN“.

Wir wollen jetzt noch eine andere Entschlüsselungsmethode vorstellen, die einen allzu langen privaten Schlüssel vermeidet. Wir beginnen mit einem Lemma:

LEMMA. *Sei p eine ungerade Primzahl und $e \in \mathbb{N}$ mit $\mathrm{ggT}(e, p^2-1) = 1$. Seien $d_{p,1}, d_{p,-1} \in \mathbb{N}$ mit*

$$ed_{p,1} \equiv 1 \bmod (p-1) \quad \text{und} \quad ed_{p,-1} \equiv 1 \bmod (p+1).$$

Sind $a, b \in \mathbb{Z}$ mit

$$b \equiv V_e(a,1) \bmod p,$$

so gilt

$$a \equiv \begin{cases} V_{d_{p,1}}(b,1) \bmod p & \text{im Fall } \left(\frac{b^2-4}{p}\right) = 1,\\ V_{d_{p,-1}}(b,1) \bmod p & \text{im Fall } \left(\frac{b^2-4}{p}\right) = -1,\\ V_{d_{p,1}}(b,1) \equiv V_{d_{p,-1}}(b,1) \bmod p & \text{im Fall } \left(\frac{b^2-4}{p}\right) = 0. \end{cases}$$

Beweis: Wir zuvor rechnen wir in $\mathbb{F}_p$ bzw. $\overline{\mathbb{F}}_p$ und interpretieren die Ergebnisse dann modulo p.

(1) Sei nun $a \in \mathbb{F}_p$ und $b = V_e(a,1)$. Sei $\alpha \in \overline{\mathbb{F}}_p$ eine Nullstelle von $x^2 - ax + 1$. Dann gilt

$$x^2 - ax + 1 = (x - \alpha)(x - \frac{1}{\alpha}).$$

Insbesondere gilt $a = \alpha + \frac{1}{\alpha}$. Die Zahl α ist bis auf Inversenbildung durch diese Bedingung eindeutig bestimmt. Es ist

$$V_i(a,1) = \alpha^i + \frac{1}{\alpha^i},$$

insbesondere

$$b = \alpha^e + \frac{1}{\alpha^e}.$$

(2) Wegen $a \in \mathbb{F}_p$ gilt $a^p = a$ und damit

$$\begin{aligned} 0 &= a^p - a = (\alpha + \frac{1}{\alpha})^p - (\alpha + \frac{1}{\alpha}) = \alpha^p + \frac{1}{\alpha^p} - \alpha - \frac{1}{\alpha} = \\ &= \frac{\alpha^{2p} + 1 - \alpha^{p+1} - \alpha^{p-1}}{\alpha^p} = \frac{(\alpha^{p-1} - 1)(\alpha^{p+1} - 1)}{\alpha^p}. \end{aligned}$$

Daher gilt

$$\alpha^{p-1} = 1 \quad \text{oder} \quad \alpha^{p+1} = 1,$$

und als Folge

$$\alpha^p = \alpha \quad \text{oder} \quad \alpha^p = \frac{1}{\alpha}.$$

(Immer gilt $\alpha^{p^2-1} = 1$.)

(3) Um $V_i(b, 1)$ zu berechnen, brauchen wir die Nullstellen des Polynoms $x^2 - bx + 1$. Es gilt

$$x^2 - bx + 1 = x^2 - (\alpha^e + \frac{1}{\alpha^e})x + 1 = (x - \alpha^e)(x - \frac{1}{\alpha^e}).$$

Daher gilt

$$V_i(b, 1) = (\alpha^e)^i + (\frac{1}{\alpha^e})^i = \alpha^{ei} + \frac{1}{\alpha^{ei}}.$$

Wir unterscheiden zwei Fälle:

(a) **Fall $\alpha^{p-1} = 1$:** Wegen $ed_{p,1} = 1 + k(p-1)$ (für ein $k \in \mathbb{N}_0$ folgt sofort

$$V_{d_{p,1}}(b, 1) = \alpha^{ed_{p,1}} + \frac{1}{\alpha^{ed_{p,1}}} = \alpha + \frac{1}{\alpha} = a.$$

(b) **Fall $\alpha^{p+1} = 1$:** Wegen $ed_{p,-1} = 1 + k(p+1)$ (für ein $k \in \mathbb{N}_0$) folgt analog

$$V_{d_{p,-1}}(b, 1) = \alpha^{ed_{p,-1}} + \frac{1}{\alpha^{ed_{p,-1}}} = \alpha^{1+k(p+1)} + \frac{1}{\alpha^{1+k(p+1)}} = \alpha + \frac{1}{\alpha} = a.$$

(4) Wie können wir die Fälle (a) und (b) unterscheiden? Es gilt

$$b^2 - 4 = (\alpha^e + \frac{1}{\alpha^e})^2 - 4 = (\alpha^e - \frac{1}{\alpha^e})^2,$$

und damit

$$\left(\frac{b^2 - 4}{p}\right) = (b^2 - 4)^{\frac{p-1}{2}} = ((\alpha^e - \frac{1}{\alpha^e})^2)^{\frac{p-1}{2}} = (\alpha^e - \frac{1}{\alpha^e})^{p-1}.$$

- **Fall $b^2 \neq 4$:** Es ist (unter Beachtung von $\alpha^p = \alpha$ bzw. $\alpha^p = \frac{1}{\alpha}$)

$$\begin{aligned} \left(\frac{b^2 - 4}{p}\right) &= (b^2 - 4)^{\frac{p-1}{2}} = (\alpha^e - \frac{1}{\alpha^e})^{p-1} = \frac{(\alpha^e - \frac{1}{\alpha^e})^p}{\alpha^e - \frac{1}{\alpha^e}} = \\ &= \frac{\alpha^{pe} - \frac{1}{\alpha^{pe}}}{\alpha^e - \frac{1}{\alpha^e}} = \begin{cases} 1, & \text{falls } \alpha^{p-1} = 1, \\ -1, & \text{falls } \alpha^{p+1} = 1. \end{cases} \end{aligned}$$

- **Fall $b = 2$:** Wegen

$$x^2 - bx + 1 = (x - 1)^2 = (x - \alpha^e)(x - \frac{1}{\alpha^e})$$

folgt

$$\alpha^e = 1.$$

Da in jedem $\alpha^{p^2-1} = 1$ gilt, folgt aus $\mathrm{ggT}(e, p^2 - 1) = 1$ sofort

$$\alpha = 1,$$

und damit

$$a = 2.$$

$V_i(2, 1)$ ist die konstante Folge, die nur aus der 2 besteht. Insbesondere stimmt in diesem Fall die behauptete Aussage.

- **Fall $b = -2$:** Wegen

$$x^2 - bx + 1 = (x+1)^2 = (x - \alpha^e)(x - \frac{1}{\alpha^e})$$

folgt

$$\alpha^e = -1.$$

Wegen $\mathrm{ggT}(e, p^2-1) = 1$ gibt es $k, l \in \mathbb{Z}$ mit $1 = ke + l(p^2-1)$. (k und e sind dann ungerade.) Es folgt

$$\alpha = \alpha^{ke+l(p^2-1)} = (\alpha^e)^k = (-1)^k = -1.$$

Dann ist

$$a = -2.$$

Es ist $V_{2i}(-2,1) = 2$ und $V_{2i+1}(-2,1) = -2$. Da $d_{p,1}$ und $d_{p,-1}$ ungerade sind, stimmt auch in diesem Fall die behauptete Aussage. ■

Alternativer privater Schlüssel: Teilnehmer A hat $N_A = p_A q_A$ und e_A mit $\mathrm{ggT}(e_A, (p_A^2-1)(q_A^2-1)) = 1$. Der Einfachkeit halber schreiben wir nun $p = p_A$ und $q = q_A$. Er berechnet sich nun

$$d_{p,1}, \quad d_{p,-1}, \quad d_{q,1}, \quad d_{q,-1}$$

mit

$$e_A d_{p,1} \equiv 1 \bmod (p-1), \quad e_A d_{p,-1} \equiv 1 \bmod (p+1)$$

und

$$e_A d_{q,1} \equiv 1 \bmod (q-1), \quad e_A d_{q,-1} \equiv 1 \bmod (q+1).$$

Die Zahlen $d_{p,1}$, $d_{p,-1}$, $d_{q,1}$. $d_{q,-1}$ sind nun der alternative private Schlüssel von A.

Entschlüsselung mit dem alternativen privaten Schlüssel: A erhält also die Zahlenfolge b_i und berechnet

$$a_{i,p} = \begin{cases} V_{d_{p,1}}(b_i, 1) \bmod p, & \text{falls } \left(\frac{b_i^2-4}{p}\right) = 1, \\ V_{d_{p,-1}}(b_i, 1) \bmod p & \text{sonst,} \end{cases}$$

$$a_{i,q} = \begin{cases} V_{d_{q,1}}(b_i, 1) \bmod q, & \text{falls } \left(\frac{b_i^2-4}{q}\right) = 1, \\ V_{d_{q,-1}}(b_i, 1) \bmod q & \text{sonst,} \end{cases}$$

und mit dem chinesischen Restsatz

$$a_i \equiv \begin{cases} a_{i,p} \bmod p, \\ a_{i,q} \bmod q \end{cases} \quad \text{mit} \quad 0 \le a_i \le N-1.$$

Die Zahlenfolge a_i liefert den Klartext.

Beispiel: Wir nehmen wieder das Beispiel von zuvor:

$$\begin{aligned} p &= 44618650311848916653827678189760501422 93 \\ q &= 80411519482208715622378181410807444081 63 \\ N &= 35878534688210971463193705793594418837499541084574688962430970226723860220737759 \end{aligned}$$

Zum öffentlichen Schlüssel $e = 5$ bestimmen wir nun die privaten Schlüssel $d_{p,1}$, $d_{p,-1}$, $d_{q,1}$, $d_{q,-1}$ mit

$$5d_{p,1} \equiv 1 \bmod (p-1), \quad 5d_{p,-1} \equiv 1 \bmod (p+1), \quad 5d_{q,1} \equiv 1 \bmod (q-1), \quad 5d_{q,-1} \equiv 1 \bmod (q+1):$$

$$\begin{aligned} d_{p,1} &= 17847460124739566661531071275904200569 17 \\ d_{p,-1} &= 89237300623697833307655356379521002845 9 \\ d_{q,1} &= 32164607792883486248951272564322977632 65 \\ d_{q,-1} &= 16082303896441743124475636282161488816 33 \end{aligned}$$

Wir wollen damit die zuvor verschlüsselte Nachricht

$$b = 345700870088387977884741970773368921309981270990243231490503257776407382179925 53$$

entschlüsseln: Zunächst gilt

$$\left(\frac{b^2-4}{p}\right) = 1 \quad \text{und} \quad \left(\frac{b^2-4}{q}\right) = 1,$$

weshalb wir berechen

$$a_p = V_{d_{p,1}}(b,1) \bmod p \quad \text{und} \quad a_q = V_{d_{q,1}}(b,1) \bmod q$$

und erhalten

$$\begin{aligned} a_p &= 109650764874865886117467041353240244 4735 \\ a_q &= 207254979111528806726052820697583557 4492 \end{aligned}$$

Der chinesische Restsatz liefert dann

$$a = 805212005000919200004051800120520262005000409051419200107000913001021 1409,$$

das gleiche Ergebnis wie früher: „HEUTE IST DER LETZTE DIENSTAG IM JUNI“.

Bemerkung: Es gibt noch eine **alternative Schlüsseldarstellung**, bei der man dann auf den chinesischen Restsatz verzichten kann. Man berechnet:

$$\begin{aligned} ed_{+1,+1} &\equiv 1 \bmod (p-1)(q-1), \\ ed_{+1,-1} &\equiv 1 \bmod (p-1)(q+1), \\ ed_{-1,+1} &\equiv 1 \bmod (p+1)(q-1), \\ ed_{-1,-1} &\equiv 1 \bmod (p+1)(q+1). \end{aligned}$$

Dann gilt:

$$a_i = \begin{cases} V_{d_{+1,+1}}(b_i,1) \bmod N, & \text{falls } \left(\frac{b_i^2-4}{p}\right) = 1, \left(\frac{b_i^2-4}{q}\right) = 1, \\ V_{d_{+1,-1}}(b_i,1) \bmod N, & \text{falls } \left(\frac{b_i^2-4}{p}\right) = 1, \left(\frac{b_i^2-4}{q}\right) = -1, \\ V_{d_{-1,+1}}(b_i,1) \bmod N, & \text{falls } \left(\frac{b_i^2-4}{p}\right) = -1, \left(\frac{b_i^2-4}{q}\right) = 1, \\ V_{d_{-1,-1}}(b_i,1) \bmod N, & \text{falls } \left(\frac{b_i^2-4}{p}\right) = -1, \left(\frac{b_i^2-4}{q}\right) = -1 \end{cases}$$

Beispiel: Für das letzte Beispiel erhält man nun

$$\begin{aligned} d_{+1,+1} &= 71757069376421942926387411587188837674974076135190566398406699281527606852374 61 \\ d_{+1,-1} &= 21527120812926582877916223476156651302497577078594591789520469105841053315883133 \\ d_{-1,+1} &= 21527120812926582877916223476156651302501872222895034965396695166227578949002177 \\ d_{-1,-1} &= 28702827750568777170554964634875535070009635281243275780526872650147133612230573 \end{aligned}$$

(Man überprüft, dass die Entschlüsselung mit $d_{+1,+1}$ funktioniert.) Warum sind $d_{+1,-}$ und $d_{-1,+1}$ am Anfang gleich? In unserem Beispiel ist $e = 5$ und $p \equiv q \equiv 3 \bmod 5$. Modulo 5 gilt

$$(p-1)(q+1) \equiv 2 \cdot 4 \equiv 3 \bmod 5 \quad \text{und ebenso} \quad (p+1)(q-1) \equiv 3 \bmod 5.$$

Daher ist

$$1 + 3(p-1)(q+1) \equiv 0 \bmod 5 \quad \text{und} \quad 1 + 3(p+1)(q-1) \equiv 0 \bmod 5,$$

was sofort

$$d_{+1,-1} = \frac{1+3(p-1)(q+1)}{5} = \frac{1+3(N-1-(q-p))}{5}$$

und

$$d_{-1,+1} = \frac{1+3(p+1)(q-1)}{5} = \frac{1+3(N-1+(q-p))}{5}$$

liefert. Es folgt

$$d_{-1,+1} - d_{+1,-1} = \frac{6(q-p)}{5},$$

was die Beobachtung erklärt.

14. Diffie-Hellman-Schlüsselaustausch mit Lucas-Folgen

Diskrete Logarithmen: Sei p eine ungerade Primzahl.

(1) Ist $g \in \mathbb{Z}$ und $k \in \mathbb{N}$, so lässt sich
$$g^k \bmod p$$
mit der square-and-multiply-Methode schnell berechnen.

(2) Sind $g, a \in \mathbb{Z}$ mit $\mathrm{ggT}(p, g) = \mathrm{ggT}(p, a) = 1$, so nennt man $x \in \mathbb{N}_0$ einen **diskreten Logarithmus** von a zur Basis g modulo p, wenn gilt
$$a \equiv g^x \bmod p.$$
Ein diskreter Logarithmus muss nicht existieren. Wenn ja, ist x nur modulo $\mathrm{ord}_p(g)$ eindeutig bestimmt. Diskrete Logarithmen lassen sich im Allgemeinen schlecht berechnen.

(3) Bei geeigneter Parameterwahl lassen sich diskrete Logarithmen praktisch nicht berechnen. (Zur Zeit fordert BSI $p \geq 2^{1999} \approx 0.57 \cdot 10^{602}$.)

Diffie-Hellman-Schlüsselaustausch: Sei p eine ungerade Primzahl und $g \in \mathbb{Z}$ mit $\mathrm{ggT}(p, g) = 1$. (BSI empfiehlt $p \geq 2^{1999}$, $\mathrm{ord}_p(g)$ prim und $\mathrm{ord}_p(g) \geq 2^{250}$.) Zwei Personen A und B wollen sich auf einen gemeinsamen Schlüssel einigen.

- A wählt zufällig und geheim $e_A \in \{1, \ldots, p-1\}$, berechnet $f_A = g^{e_A} \bmod p$ und gibt f_A als seinen öffentlichen Schlüssel bekannt. (e_A ist der private Schlüssel von A.)
- B wählt zufällig und geheim $e_B \in \{1, \ldots, p-1\}$, berechnet $f_B = g^{e_B} \bmod p$ und gibt f_B als seinen öffentlichen Schlüssel bekannt. (e_B ist der private Schlüssel von B.)

Der gemeinsame Schlüssel von A und B ist dann
$$k_{AB} = g^{e_A e_B} \bmod p,$$
den sich A aus der Gleichung
$$k_{AB} = f_B^{e_A} \bmod p$$
und B aus der Gleichung
$$k_{AB} = f_A^{e_B} \bmod p$$
berechnen kann.

Beispiel: Die Zahl

$$p = 761012558000454483803911743306401464092009245985317882180807618189189893928870 03$$

ist wahrscheinlich prim, und auch q mit $p-1 = 2q$ ist wahrscheinlich prim. Man testet schnell, dass $g = 2$ eine Primitivwurzel modulo p ist. Wir haben e_A und e_B gewählt und dann die andern Größen berechnet:

$$\begin{aligned}
e_A &= 11111111111111111111111111111111111111111111111111111111111111111111111111111111\\
f_A &= 45895238420095846549846158560699244998274010999554978546095510828029339896405345\\
e_B &= 22222222222222222222222222222222222222222222222222222222222222222222222222222222\\
f_B &= 15726049412719778574324816611127346380843786452610583503769168494059163668117851\\
k_{AB} &= 18903790410282053649664231955109720099675031951034271654056551563783740928985036
\end{aligned}$$

Bemerkung: Als „Diffie-Hellman-Problem“ bezeichnet man die Frage, wie man mit der Kenntnis von p, g, $g^{e_A} \bmod p$, $g^{e_B} \bmod p$ die Zahl $g^{e_A e_B} \bmod p$ berechnen kann. Kann man diskrete Logarithmen berechnen, beispielsweise den diskreten Logarithmus von f_A zur Basis g modulo p, so erhält man e_A und damit auch k_{AB}. Es ist eine offene Frage, ob es auch andere Möglichkeiten gibt.

Den Diffie-Hellman-Schlüsselaustausch kann man leicht auch auf andere Situationen übertragen. Wir geben eine Variante mit Lucas-Folgen an.

Bemerkung: Wir hatten früher gesehen, dass für $P, Q \in \mathbb{Z}$ und $i, j \geq 0$
$$V_{ij}(P, Q) = V_i(V_j(P, Q), Q^i)$$

gilt. Insbesondere gilt:

$$V_{ij}(P,1) = V_i(V_j(P,1),1).$$

Außerdem haben wir für $P, Q, \widetilde{P}, \widetilde{Q} \in \mathbb{Z}$, $n \in \mathbb{N}$ und $i \geq 0$ die Implikation

$$\widetilde{P} \equiv P \bmod n, \quad \widetilde{Q} \equiv Q \bmod n \quad \Longrightarrow \quad V_i(\widetilde{P}, \widetilde{Q}) \equiv V_i(P,Q) \bmod n$$

gezeigt. Dies verwenden wir nun:

LEMMA. *Ist p eine Primzahl, ist $g \in \mathbb{Z}$, sind $e_1, e_2 \in \mathbb{N}$, definiert man*

$$f_1 = V_{e_1}(g,1) \bmod p \quad \textit{und} \quad f_2 = V_{e_2}(g,1) \bmod p,$$

so gilt

$$V_{e_1}(f_2,1) \equiv V_{e_2}(f_1,1) \equiv V_{e_1e_2}(g,1) \bmod p.$$

Beweis:

$$V_{e_1}(f_2,1) \equiv V_{e_1}(V_{e_2}(g,1),1) \equiv V_{e_1e_2}(g,1) \bmod p,$$

und analog

$$V_{e_2}(f_1,1) \equiv V_{e_2}(V_{e_1}(g,1),1) \equiv V_{e_1e_2}(g,1) \bmod p,$$

was die Behauptung beweist. ■

Damit erhalten wir nun:

Diffie-Hellman-Schlüsselaustausch mit Lucas-Folgen: Gegeben sei eine ungerade Primzahl p und $g \in \mathbb{Z}$. Zwei Personen A und B wollen sich auf einen gemeinsamen Schlüssel einigen:

- A wählt als seinen privaten Schlüssel e_A, berechnet $f_A = V_{e_A}(g,1) \bmod p$ und gibt f_A als seinen öffentlichen Schlüssel bekannt.
- B wählt als seinen privaten Schlüssel e_B, berechnet $f_B = V_{e_B}(g,1) \bmod p$ und gibt f_B als seinen öffentlichen Schlüssel bekannt.

Der gemeinsame Schlüssel von A und B ist dann

$$k_{AB} = V_{e_Ae_B}(g,1) \bmod p,$$

den sich A aus der Gleichung

$$k_{AB} = V_{e_A}(f_B,1) \bmod p,$$

B aus der Gleichung

$$k_{AB} = V_{e_B}(f_A,1) \bmod p$$

berechnen kann.

Beispiel: Wir wählen ähnliche Parameter wie beim letzten Beispiel, also

$$\begin{aligned}
p &= 76101255800045448380391174330640146409200924598531788218080761818918989392887003\\
e_A &= 11111111111111111111111111111111111111111111111111111111111111111111111111111111\\
e_B &= 22222222222222222222222222222222222222222222222222222222222222222222222222222222
\end{aligned}$$

Zunächst haben wir $g = 2$ gewählt, aber damit nur $f_A = f_B = k_{AB} = 2$ erhalten. Dies scheint keine gute Wahl zu sein. Deshalb haben wir $g = 3$ gewählt und erhalten:

$$\begin{aligned}
g &= 3\\
f_A &= 643690630322301669598332120109671755888902585712185470051132657722501543502058 72\\
f_B &= 638406752575748140769046383603315881618732777722398064727124207137800445178742 33\\
k_{AB} &= 252742904022982458756781922877798227303677932075265009568281473473786082614870 81
\end{aligned}$$

Um Sicherheitsprobleme wie im Beispiel zu vermeiden, werden wir die Situation weiter analysieren. Können wir bei Kenntnis von p, g und f_A (mit $f_A = V_{e_A}(g,1) \bmod p$) die Zahl e_A berechnen, so ist der Schlüsselaustausch unsicher. Wie kompliziert ist die Gleichung

$$V_x(g,1) \equiv f \bmod p?$$

15. LUCAS-ELGAMAL-Verschlüsselung

(1) **Schlüsselerzeugung:**
   (a) Man wählt eine Primzahl p und ein $g \in \mathbb{Z}$. Um gewisse Angriffe unmöglich zu machen, kann man noch folgende Bedingungen stellen:
      (i) Die Faktorisierung von $p+1$ ist bekannt: $p+1 = q_1^{e_1} \dots q_r^{e_r}$.
      (ii) $p+1$ sollte mindestens einen großen Primteiler haben.
      (iii) $\left(\frac{g^2-4}{p}\right) = -1$.
      (iv) $V_{\frac{p+1}{q_i}}(g,1) \not\equiv 2 \bmod p$ für $i = 1, \dots, r$.
   (b) Jeder Teilnehmer A wählt sich geheim eine Zahl e_A, berechnet
   $$f_A = V_{e_A}(g,1) \bmod p$$
   und gibt f_A als seinen öffentlichen Schlüssel bekannt.

(2) **Verschlüsselung:**
   (a) Nach einem vereinbarten Verfahren wird der Text in eine Zahlenfolge a_i mit $0 \le a_i \le p-1$ umgewandelt.
   (b) Für jedes a_i wird eine Zufallszahl z_i gewählt und anschließend
   $$b_i = V_{z_i}(g,1) \bmod p \quad \text{und} \quad c_i = a_i \cdot V_{z_i}(f,1) \bmod p$$
   berechnet. Der Chiffretext ist die Zahlenpaarfolge (b_i, c_i).

(3) **Entschlüsselung:** Man berechnet
$$a_i = \frac{c_i}{V_e(b_i,1)} \bmod p$$
und wandelt a_i wieder in Text um.

Begründung für die Richtigkeit der Entschlüsselung: Es gilt
$$V_e(b_i,1) \equiv V_e(V_{z_i}(g,1),1) \equiv V_{ez_i}(g,1) \equiv V_{z_i}(V_e(g,1),1) \equiv V_{z_i}(f,1) \bmod p,$$
woraus dann sofort die Richtigkeit der Entschlüsselung folgt.

Beispiel: Wir starten mit
$$p = 64598364958726948562984659836485365132 81.$$
Die Primfaktorzerlegung von $p+1$ ist
$$p+1 = 2 \cdot q \text{ mit } 32299182479363474281492329918242682566 41.$$
Die kleinste Zahl g mit
$$\left(\frac{g^2-4}{p}\right) = -1, \quad V_2(g,1) \not\equiv 2 \bmod p, \quad V_q(g,1) \not\equiv 2 \bmod p$$
ist $g = 5$, weshalb wir als weiteren Parameter $g = 5$ wählen. Nach Wahl des privaten Schlüssels
$$e = 11111111111111111111111111111111111111111$$
wird mit $f = V_e(g,1) \bmod p$ der öffentliche Schlüssel zu
$$f = 38454665033699540155147861328529792505 54.$$
Wir wollen `HEUTE IST FREITAG` verschlüsseln. Nach unserem üblichen Verfahren liefert die Umwandlung in eine Zahl
$$a = 80521200500091920000618050920010 7.$$
Nun wählen wir eine Zufallszahl
$$z = 589581861444458703364419182932630629 7564$$
und berechnen
$$b = V_z(g,1) \bmod p, \quad c = a \cdot V_z(f,1) \bmod p$$

mit dem Ergebnis

$$b = 44630841003364603998341248645144768272 44, \quad c = 55191434397174217998435857832614699936 71.$$

Der Chiffretext ist (b, c). (Man überprüft, dass $a = \frac{c}{V_e(b,1)} \bmod p$ gilt.)

16. Zur Gleichung $V_x(g,1) \equiv a \bmod p$

Wir beginnen mit einem Lemma, das im Folgenden wiederholt Verwendung findet:

LEMMA. *Ist K ein Körper, sind $x, y \in K^*$, so gilt*

$$x + \frac{1}{x} = y + \frac{1}{y} \quad \Longleftrightarrow \quad x = y \text{ oder } x = \frac{1}{y}.$$

Beweis: Wir geben zwei Beweise an:

(1) Es gilt

$$x + \frac{1}{x} = y + \frac{1}{y} \quad \Longleftrightarrow \quad x - (y + \frac{1}{y}) + \frac{1}{x} = 0 \quad \Longleftrightarrow \quad x^2 - (y + \frac{1}{y})x + 1 = 0 \quad \Longleftrightarrow$$
$$\Longleftrightarrow \quad (x - y)(x - \frac{1}{y}) = 0,$$

was die Behauptung beweist.

(2) Die Richtung $\Longleftarrow$ ist klar. Wir betrachten $\Longrightarrow$. Sei t eine Unbestimmte über K. Wir betrachten die Polynome

$$t^2 - (x + \frac{1}{x})t + 1 = (t - x)(t - \frac{1}{x}) \quad \text{und} \quad t^2 - (y + \frac{1}{y})t + 1 = (t - y)(t - \frac{1}{y}).$$

Aus $x + \frac{1}{x} = y + \frac{1}{y}$ folgt dann sofort $\{x, \frac{1}{x}\} = \{y, \frac{1}{y}\}$, und damit die Behauptung. ■

Der Einfachkeit halber argumentieren wir in $\mathbb{F}_p$.

LEMMA. *Sei p eine ungerade Primzahl, seien $g, a \in \mathbb{F}_p$ und $\gamma \in \overline{\mathbb{F}}_p$ eine Nullstelle des Polynoms $x^2 - gx + 1$, $\alpha \in \overline{\mathbb{F}}_p$ eine Nullstelle des Polynoms $x^2 - ax + 1$. Dann gilt*

$$g = \gamma + \frac{1}{\gamma}, \quad a = \alpha + \frac{1}{\alpha}, \quad V_i(g,1) = \gamma^i + \frac{1}{\gamma^i}.$$

Außerdem gilt für $x \in \mathbb{N}_0$

$$V_x(g,1) = a \quad \Longleftrightarrow \quad \gamma^x = \alpha \text{ oder } \gamma^x = \frac{1}{\alpha}.$$

Beweis: Nur die letzte Zeile ist zu zeigen, die anderen Aussagen sind bekannt:

$$V_x(g,1) = a \quad \Longleftrightarrow \quad \gamma^x + \frac{1}{\gamma^x} = \alpha + \frac{1}{\alpha}.$$

Die Behauptung ergibt sich nun aus dem vorangegangenen Lemma. ■

Das vorangegangene Lemma stellt also einen Zusammenhang zwischen der Gleichung $V_x(g,1) = a$ in $\mathbb{F}_p$ und der Gleichung $\gamma^x = \alpha$ bzw. $\gamma^x = \frac{1}{\alpha}$ her. Als Anwendung zeigen wir: Könnte man die Gleichung $V_x(g,1) = a$ schnell lösen, so könnte man auch diskrete Logarithmen in $\mathbb{F}_p$ schnell berechnen:

FOLGERUNG. *Seien $g, a \in \mathbb{F}_p^*$ (mit einer ungeraden Primzahl p). Sei $\widetilde{g} = g + \frac{1}{g}$ und $\widetilde{a} = a + \frac{1}{a}$. Ist $x \in \mathbb{N}_0$ mit*

$$V_x(\widetilde{g}, 1) = \widetilde{a},$$

so gilt

$$g^x = a \text{ oder } g^{-x} = a.$$

Beweis: Die Nullstellen des Polynoms $x^2 - \widetilde{g}x + 1$ sind g und $\frac{1}{g}$, woraus

$$V_i(\widetilde{g}, 1) = g^i + \frac{1}{g^i}$$

folgt. Damit erhalten wir

$$V_x(\widetilde{g}, 1) = \widetilde{a} \quad \Longrightarrow \quad g^x + \frac{1}{g^x} = a + \frac{1}{a} \quad \Longrightarrow \quad g^x = a \text{ oder } \frac{1}{g^x} = a,$$

was die Behauptung beweist. ■

Bei kryptographischen Anwendungen darf $\operatorname{ord}(\gamma)$ nicht zu klein sein, da man sonst die Gleichung $\gamma^x \in \{\alpha, \frac{1}{\alpha}\}$ durch Probieren lösen kann. Das folgende Lemma beschreibt die Ordnung von γ mit Hilfe der Lucas-Folge $V_i(g, 1)$.

LEMMA. *Sei p eine ungerade Primzahl, $g \in \mathbb{F}_p$ und $\gamma \in \overline{\mathbb{F}}_p$ eine Nullstelle von $x^2 - gx + 1$, sodass gilt $g = \gamma + \frac{1}{\gamma}$. Dann gilt für $i \geq 0$*

$$V_i(g, 1) = 2 \quad \Longleftrightarrow \quad \operatorname{ord}(\gamma) \mid i,$$

insbesondere

$$\operatorname{ord}(\gamma) = \min\{i \in \mathbb{N} : V_i(g, 1) = 2\}.$$

Beweis: Es ist $V_i(g, 1) = \gamma^i + \frac{1}{\gamma^i}$. Mit Hilfe eines vorangegangenen Lemmas folgt für $i \geq 0$

$$V_i(g, 1) = 2 \quad \Longleftrightarrow \quad \gamma^i + \frac{1}{\gamma^i} = 1 + \frac{1}{1} \quad \Longleftrightarrow \quad \gamma^i = 1 \quad \Longleftrightarrow \quad \operatorname{ord}(\gamma) \mid i.$$

Dies beweist die Behauptung. ■

LEMMA. *Sei p eine ungerade Primzahl, $g \in \mathbb{F}_p$ und $\gamma \in \overline{\mathbb{F}_p}$ eine Nullstelle des Polynoms $x^2 - gx + 1$. Dann gilt: Die Folge $(V_i(g, 1))_{i \geq 0}$ ist periodisch und hat die (minimale) Periodenlänge* $\operatorname{ord}(\gamma)$.

Beweis:

- Gilt $i \equiv j \bmod \operatorname{ord}(\gamma)$, so folgt $\gamma^i = \gamma^j$ und damit

  $$V_i(g, 1) = \gamma^i + \frac{1}{\gamma^i} = \gamma^j + \frac{1}{\gamma^j} = V_j(g, 1),$$

  also ist $\operatorname{ord}(\gamma)$ eine Periodenlänge, insbesondere ist die Folge $(V_i(g, 1))_{i \geq 0}$ periodisch.
- Sei umgekehrt ℓ irgendeine Periodenlänge, d.h.

  $$V_{i+\ell}(g, 1) = V_i(g, 1) \text{ für alle } i \geq 0.$$

  Dann folgt für $i = 0$

  $$V_\ell(g, 1) = V_0(g, 1) = 2,$$

  und dann nach nach dem letzten Lemma

  $$\operatorname{ord}(\gamma) \mid \ell.$$

Damit folgt, dass $\operatorname{ord}(\gamma)$ minimale Periodenlänge ist. ■

LEMMA. *Sei p eine ungerade Primzahl, $g \in \mathbb{F}_p$ und $\gamma \in \overline{\mathbb{F}}_p$ eine Nullstelle des Polynoms $x^2 - gx + 1$. Dann gilt*

$$V_i(g, 1) = -2 \quad \Longleftrightarrow \quad 2 \mid \operatorname{ord}(\gamma) \text{ und } i \equiv \frac{\operatorname{ord}(\gamma)}{2} \bmod \operatorname{ord}(\gamma).$$

Beweis:

- $\Longrightarrow$: Es gilt

$$V_i(g,1) = -2 \quad \Longleftrightarrow \quad \gamma^i + \frac{1}{\gamma^i} = -1 + \frac{1}{-1} \quad \Longleftrightarrow \quad \gamma^i = -1.$$

Wegen

$$(-1)^{\operatorname{ord}(\gamma)} = \gamma^{i\operatorname{ord}(\gamma)} = 1$$

folgt $\operatorname{ord}(\gamma) \equiv 0 \bmod 2$. Nun gilt

$$\left(\gamma^{\frac{\operatorname{ord}(\gamma)}{2}}\right)^2 = 1, \text{ aber } \gamma^{\frac{\operatorname{ord}(\gamma)}{2}} \neq 1.$$

Daher gilt

$$\gamma^{\frac{\operatorname{ord}(\gamma)}{2}} = -1.$$

Wir können nun weitermachen:

$$\begin{aligned} V_i(g,1) = -2 \quad &\Longleftrightarrow \quad \gamma^i = -1 = \gamma^{\frac{\operatorname{ord}(\gamma)}{2}} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad i \equiv \frac{\operatorname{ord}(\gamma)}{2} \bmod \operatorname{ord}(\gamma). \end{aligned}$$

- $\Longleftarrow$: Hier muss man die letzten Ausführungen nur rückwärts lesen. ■

LEMMA. *Sei p eine ungerade Primzahl, $g \in \mathbb{F}_p$ und γ eine Nullstelle des Polynoms $x^2 - gx + 1$ in $\overline{\mathbb{F}}_p$.*

(1) *Dann gilt für $x, y \in \mathbb{N}_0$:*

$$V_y(g,1) = V_x(g,1) \quad \Longleftrightarrow \quad y \equiv x \bmod \operatorname{ord}(\gamma) \text{ oder } y \equiv -x \bmod \operatorname{ord}(\gamma).$$

(2) *Für $0 < i < \frac{\operatorname{ord}(\gamma)}{2}$ gilt $\frac{\operatorname{ord}(\gamma)}{2} < \operatorname{ord}(\gamma) - i < \operatorname{ord}(\gamma)$ und*

$$V_i(g,1) = V_{\operatorname{ord}(\gamma)-i}(g,1).$$

(3) *Gilt $0 < i < j < \operatorname{ord}(\gamma)$ und $V_i(g,1) = V_j(g,1)$, so gilt $0 < i < \frac{\operatorname{ord}(\gamma)}{2}$ und $j = \operatorname{ord}(\gamma) - i$.*

Beweis:

(1) Wegen $V_i(g,1) = \gamma^i + \frac{1}{\gamma^i}$ gilt:

$$\begin{aligned} V_x(g,1) = V_y(g,1) \quad &\Longleftrightarrow \quad g^x + \frac{1}{g^x} = g^y + \frac{1}{g^y} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad g^x = g^y \text{ oder } g^x = \frac{1}{g^y} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad g^{x-y} = 1 \text{ oder } g^{x+y} = 1 \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \operatorname{ord}(\gamma) \mid x - y \text{ oder } \operatorname{ord}(\gamma) \mid x + y, \end{aligned}$$

woraus die Behauptung folgt.

(2) Sei $0 < i < \frac{\operatorname{ord}(\gamma)}{2}$. Natürlich gilt dann $\frac{\operatorname{ord}(\gamma)}{2} < \operatorname{ord}(\gamma) - i < \operatorname{ord}(\gamma)$. Der Rest folgt aus (1) oder nochmals direkt:

$$V_{\operatorname{ord}(\gamma)-i}(g,1) = \gamma^{\operatorname{ord}(\gamma)-i} + \frac{1}{\gamma^{\operatorname{ord}(\gamma)-i}} = \frac{1}{\gamma^i} + \gamma^i = V_i(g,1).$$

(3) Sei $0 < i < j < \operatorname{ord}(\gamma)$ mit $V_i(g,1) = V_j(g,1)$. Nach (1) gilt dann

$$j \equiv i \bmod \operatorname{ord}(\gamma) \quad \text{oder} \quad j \equiv -i \bmod \operatorname{ord}(\gamma).$$

Wegen $0 < i < j < \operatorname{ord}(\gamma)$ ist $i \not\equiv j \bmod \operatorname{ord}(\gamma)$, sodass $j \equiv -i \bmod \operatorname{ord}(\gamma)$ folgt. Dann gilt

$$\operatorname{ord}(\gamma) \mid i + j.$$

Wegen

$$i + j < 2j < 2\operatorname{ord}(\gamma)$$

folgt dann aber

$$i + j = \operatorname{ord}(\gamma),$$

wie behauptet. ■

Beispiele: Wir haben hier für ein paar kleine Primzahlen p alle Folgen $(V_i(g,1))_{0\le i\le p+1}$ zusammen mit $\operatorname{ord}(\gamma)$ und $\left(\frac{g^2-4}{p}\right)$ aufgelistet:

$p=3$

i	0	1	2	3	4	$\operatorname{ord}(\gamma)$	$\left(\frac{g^2-4}{p}\right)$
$V_i(0,1)$	2	0	1	0	2	4	-1
$V_i(1,1)$	2	1	2	1	2	2	0
$V_i(2,1)$	2	2	2	2	2	1	0

$p=5$

i	0	1	2	3	4	5	6	$\operatorname{ord}(\gamma)$	$\left(\frac{g^2-4}{p}\right)$
$V_i(0,1)$	2	0	3	0	2	0	3	4	1
$V_i(1,1)$	2	1	4	3	4	1	2	6	-1
$V_i(2,1)$	2	2	2	2	2	2	2	1	0
$V_i(3,1)$	2	3	2	3	2	3	2	2	0
$V_i(4,1)$	2	4	4	2	4	4	2	3	-1

$p=7$

i	0	1	2	3	4	5	6	7	8	$\operatorname{ord}(\gamma)$	$\left(\frac{g^2-4}{p}\right)$
$V_i(0,1)$	2	0	5	0	2	0	5	0	2	4	-1
$V_i(1,1)$	2	1	6	5	6	1	2	1	6	6	1
$V_i(2,1)$	2	2	2	2	2	2	2	2	2	1	0
$V_i(3,1)$	2	3	0	4	5	4	0	3	2	8	-1
$V_i(4,1)$	2	4	0	3	5	3	0	4	2	8	-1
$V_i(5,1)$	2	5	2	5	2	5	2	5	2	2	0
$V_i(6,1)$	2	6	6	2	6	6	2	6	6	3	1

$p=11$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	$\operatorname{ord}(\gamma)$	$\left(\frac{g^2-4}{p}\right)$
$V_i(0,1)$	2	0	9	0	2	0	9	0	2	0	9	0	2	4	-1
$V_i(1,1)$	2	1	10	9	10	1	2	1	10	9	10	1	2	6	-1
$V_i(2,1)$	2	2	2	2	2	2	2	2	2	2	2	2	2	1	0
$V_i(3,1)$	2	3	7	7	3	2	3	7	7	3	2	3	7	5	1
$V_i(4,1)$	2	4	3	8	7	9	7	8	3	4	2	4	3	10	1
$V_i(5,1)$	2	5	1	0	10	6	9	6	10	0	1	5	2	12	-1
$V_i(6,1)$	2	6	1	0	10	5	9	5	10	0	1	6	2	12	-1
$V_i(7,1)$	2	7	3	3	7	2	7	3	3	7	2	7	3	5	1
$V_i(8,1)$	2	8	7	4	3	9	3	4	7	8	2	8	7	10	1
$V_i(9,1)$	2	9	2	9	2	9	2	9	2	9	2	9	2	2	0
$V_i(10,1)$	2	10	10	2	10	10	2	10	10	2	10	10	2	3	-1

Die Nullstellen des Polynoms $x^2-gx+1\in\mathbb{F}_p[x]$ haben wir im algebraischen Abschluss $\overline{\mathbb{F}}_p$ gewählt. In Anwendungen reicht aber der Körper $\mathbb{F}_{p^2}$, an den das folgende Lemma nochmals erinnert.

LEMMA. *Sei p eine ungerade Primzahl und $\overline{\mathbb{F}}_p$ ein/der algebraische Abschluss von $\mathbb{F}_p$. Dann gilt:*

(1) *Es ist*
$$\mathbb{F}_p=\{\alpha\in\overline{\mathbb{F}}_p:\alpha^p=\alpha\}.$$

(2) *Die Menge*
$$\{\alpha\in\overline{\mathbb{F}}_p:\alpha^{p^2}=\alpha\}$$
ist ein Teilkörper von $\overline{\mathbb{F}}_p$, der p^2 Elemente enthält und mit $\mathbb{F}_{p^2}$ bezeichnet wird und $\mathbb{F}_p$ enthält.

(3) *$\mathbb{F}_{p^2}$ ist ein 2-dimensionaler Vektorraum über $\mathbb{F}_p$. Ist $\omega\in\mathbb{F}_{p^2}\setminus\mathbb{F}_p$, so gilt*
$$\mathbb{F}_{p^2}=\mathbb{F}_p+\mathbb{F}_p\,\omega=\{a+b\omega:a,b\in\mathbb{F}_p\}.$$

(4) *Sei $a \in \mathbb{F}_p^*$ und $\omega \in \overline{\mathbb{F}}_p$ mit $\omega^2 = a$. Dann gilt:*
- *Im Fall $\left(\frac{a}{p}\right) = 1$ ist $\omega \in \mathbb{F}_p$ und $\omega^p = \omega$.*
- *Im Fall $\left(\frac{a}{p}\right) = -1$ ist $\omega \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ und $\omega^p = -\omega$.*

Beweis:

(1) Es ist $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\} \simeq \mathbb{Z}/p\mathbb{Z}$. Nach dem kleinen Satz von Fermat gilt für $\alpha \in \mathbb{F}_p$ die Gleichung $\alpha^p = \alpha$, woraus
$$\mathbb{F}_p \subseteq \{\alpha \in \overline{\mathbb{F}}_p : \alpha^p = \alpha\}$$
folgt. Das Polynom $f(x) = x^p - x \in \overline{\mathbb{F}}_p[x]$ hat Grad p, hat also höchstens p Nullstellen. Wegen
$$\{\alpha \in \overline{\mathbb{F}}_p : \alpha^p = \alpha\} = \{\alpha \in \overline{\mathbb{F}}_p : f(\alpha) = 0\}$$
hat die Menge höchstens p Elemente, woraus dann sofort die Gleichheit
$$\mathbb{F}_p = \{\alpha \in \overline{\mathbb{F}}_p : \alpha^p = \alpha\}$$
folgt.

(2) Sei
$$K = \{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^2} = \alpha\}.$$
Da p-Potenzierung in Charakteristik p ein additiv ist, gilt für alle $\alpha, \beta \in \overline{\mathbb{F}}_p$
$$(\alpha+\beta)^{p^2} = \alpha^{p^2} + \beta^{p^2} \quad \text{und} \quad (\alpha\beta)^{p^2} = \alpha^{p^2}\beta^{p^2}.$$
Damit sieht man, dass K ein Teilring von $\overline{\mathbb{F}}_p$ ist. Natürlich gilt auch
$$\mathbb{F}_p \subseteq K.$$
Ist $\alpha \in K \setminus \{0\}$, so folgt aus $\alpha^{p^2} = \alpha$ sofort
$$\alpha^{p^2-1} = 1,$$
und insbesondere
$$\frac{1}{\alpha} = \alpha^{p^2-2}.$$
Daher ist K auch ein Teilkörper von $\overline{\mathbb{F}}_p$. Wir betrachten nun das Polynom $g(x) = x^{p^2} - x \in \overline{\mathbb{F}}_p[x]$. Die Nullstellen von g sind genau die Elemente von K. Nun ist $g'(x) = -1$. Daher ist $g(x)$ separabel, hat also genau p^2 Nullstellen in $\overline{\mathbb{F}}_p$. Daher hat K genau p^2 Elemente, wie behauptet.

(3) Natürlich ist $\mathbb{F}_{p^2}$ ein $\mathbb{F}_p$-Vektorraum. Aus der Dimensionsformel
$$|\mathbb{F}_{p^2}| = |\mathbb{F}_p|^{\dim_{\mathbb{F}_p}(\mathbb{F}_{p^2})}$$
folgt sofort, dass $\mathbb{F}_{p^2}$ Dimension 2 über $\mathbb{F}_p$ hat, und damit auch der Rest der Behauptung.

(4) Mit dem Satz von Euler erhalten wir
$$\omega^p = \omega^{p-1}\omega = (\omega^2)^{\frac{p-1}{2}}\omega = a^{\frac{p-1}{2}}\omega = \left(\frac{a}{p}\right)\omega.$$
- Im Fall $\left(\frac{a}{p}\right) = 1$ folgt $\omega^p = \omega$, was nach (1) sofort $\omega \in \mathbb{F}_p$ liefert. (Natürlich folgt dies auch aus der Definition des Legendre-Symbols.)
- Im Fall $\left(\frac{a}{p}\right) = -1$ erhalten wir $\omega^p = -\omega$. Natürlich gilt dann $\omega \notin \mathbb{F}_p$. Wegen
$$\omega^{p^2} = (\omega^p)^p = (-\omega)^p = (-1)^p\omega^p = -(-\omega) = \omega$$
folgt aus (2) dann $\omega \in \mathbb{F}_{p^2}$. ■

Nach dieser Erinnerung betrachten wir wieder die Nullstellen eines Polynoms $x^2 - gx + 1 \in \mathbb{F}_p[x]$:

LEMMA. *Sei p eine ungerade Primzahl, $g \in \mathbb{F}_p$ und $\gamma \in \overline{\mathbb{F}}_p$ eine Nullstelle des Polynoms $x^2 - gx + 1$. Dann gilt:*

(1) *Ist $\left(\frac{g^2-4}{p}\right) = 1$, so gilt $\gamma \in \mathbb{F}_p$, $\gamma^{p-1} = 1$ und $\operatorname{ord}(\gamma) \mid p-1$.*

(2) *Ist* $\left(\frac{g^2-4}{p}\right) = -1$, *so gilt* $\gamma \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, $\gamma^{p+1} = 1$ *und* $\operatorname{ord}(\gamma) \mid p+1$.

Beweis: Sei $\omega \in \overline{\mathbb{F}}_p$ mit $\omega^2 = g^2 - 4$. Die Nullstellen von $x^2 - gx + 1$ sind dann (o.E.)

$$\gamma = \frac{g+\omega}{2} \quad \text{und} \quad \gamma' = \frac{g-\omega}{2}.$$

Es folgt

$$\gamma + \gamma' = g \quad \text{und} \quad \gamma\gamma' = 1.$$

Wegen $g, 2 \in \mathbb{F}_p$ folgt

$$\gamma^p = \frac{g^p + \omega^p}{2^p} = \frac{g+\omega^p}{2}.$$

(1) Fall $\left(\frac{g^2-4}{p}\right) = 1$: Dann gilt $\omega \in \mathbb{F}_p$ und $\omega^p = \omega$, und damit

$$\gamma^p = \gamma, \quad \text{also} \quad \gamma^{p-1} = 1.$$

(2) Fall $\left(\frac{g^2-4}{p}\right) = -1$: Dann gilt $\omega^p = -\omega$, $\omega \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ und damit

$$\omega^p = \frac{g-\omega}{2} = \gamma' = \frac{1}{\gamma},$$

insbesondere

$$\gamma^{p+1} = 1,$$

woraus auch der Rest folgt. ■

Bemerkung: Direkt mit der Definition sieht man:

$$\begin{aligned} V_i(2,1) &= 2 \text{ für alle } i \geq 0, \\ V_i(-2,1) &= \begin{cases} 2 & \text{für } i \equiv 0 \bmod 2, \\ -2 & \text{für } i \equiv 1 \bmod 2. \end{cases} \end{aligned}$$

Lemma. *Sei p eine ungerade Primzahl, $g \in \mathbb{F}_p$ und $\gamma \in \overline{\mathbb{F}}_p$ eine Nullstelle des Polynoms $x^2 - gx + 1$. Ist $g \neq \pm 2$ und $a \in \mathbb{F}_p$ mit $a = V_i(g,1)$ für ein i, so gilt $a = \pm 2$ oder $\left(\frac{a^2-4}{p}\right) = \left(\frac{g^2-4}{p}\right)$.*

Beweis: Es ist

$$a = V_i(g,1) = \gamma^i + \frac{1}{\gamma^i},$$

und damit

$$a^2 - 4 = (\gamma^i + \frac{1}{\gamma^i})^2 - 4 = (\gamma^i)^2 + 2 + (\frac{1}{\gamma^i})^2 - 4 = (\gamma^i)^2 - 2 + (\frac{1}{\gamma^i})^2 = (\gamma^i - \frac{1}{\gamma^i})^2.$$

Damit folgt, wenn wir $a \neq \pm 2$ und damit $\gamma^i \neq \frac{1}{\gamma^i}$ annehmen,

$$\begin{aligned} \left(\frac{a^2-4}{p}\right) &= (a^2-4)^{\frac{p-1}{2}} = (\gamma^i - \frac{1}{\gamma^i})^{p-1} = \frac{(\gamma^i - \frac{1}{\gamma^i})^p}{\gamma^i - \frac{1}{\gamma^i}} = \\ &= \frac{(\gamma^p)^i - \frac{1}{(\gamma^p)^i}}{\gamma^i - \frac{1}{\gamma^i}} \end{aligned}$$

Ist $\left(\frac{g^2-4}{p}\right) = 1$, so ist $\gamma^p = \gamma$ und damit auch $\left(\frac{a^2-4}{p}\right) = 1$. Ist $\left(\frac{g^2-4}{p}\right) = -1$, so gilt $\gamma^p = \frac{1}{\gamma}$. Damit folgt dann $\left(\frac{a^2-4}{p}\right) = -1$. ■

LEMMA. *Sei p eine ungerade Primzahl, seien $g, a \in \mathbb{F}_p \setminus \{\pm 2\}$ und*

$$\left(\frac{g^2-4}{p}\right) = \left(\frac{a^2-4}{p}\right) = 1.$$

Seien $\sqrt{g^2-4}, \sqrt{a^2-4} \in \mathbb{F}_p$ Quadratwurzeln von g^2-4 bzw. a^2-4 und

$$\gamma = \frac{g+\sqrt{g^2-4}}{2} \quad \text{und} \quad \alpha = \frac{a+\sqrt{a^2-4}}{2}.$$

Dann gilt für $x \in \mathbb{N}_0$:

$$V_x(g,1) = a \quad \Longleftrightarrow \quad \gamma^x = \alpha \text{ oder } \gamma^x = \frac{1}{\alpha}.$$

Der Beweis folgt sofort aus den vorangegangenen Betrachtungen.

Bemerkung: Im Fall $\left(\frac{g^2-4}{p}\right) = 1$ führt das vorangegangene Lemma die Gleichung $V_x(g,1) = a$ auf eine Logarithmenberechnung von $\mathbb{F}_p$ zuürck. Kryptographisch haben hier Lucas-Folgen keine Vorteile.

LEMMA. *Sei p eine ungerade Primzahl, seien $g, a \in \mathbb{F}_p \setminus \{\pm 2\}$ und*

$$\left(\frac{g^2-4}{p}\right) = \left(\frac{a^2-4}{p}\right) = -1.$$

Sei $c \in \mathbb{F}_p^*$ mit

$$c^2 = \frac{a^2-4}{g^2-4}.$$

Sei $\omega \in \overline{\mathbb{F}}_p$ mit $\omega^2 = g^2-4$ und

$$\gamma = \frac{g+\omega}{2} \quad \text{und} \quad \alpha = \frac{a+c\omega}{2}.$$

Dann ist γ Nullstelle des Polynoms $x^2 - gx + 1$, α ist Nullstelle des Polynoms $x^2 - ax + 1$ und es gilt:

$$V_x(g,1) = a \quad \Longleftrightarrow \quad \gamma^x = \alpha \text{ oder } \gamma^x = \frac{1}{\alpha}.$$

Beweis: Es ist

$$\frac{g+\omega}{2} \cdot \frac{g-\omega}{2} = \frac{g^2-\omega^2}{4} = \frac{g^2-(g^2-4)}{4} = 1$$

und

$$\frac{a+c\omega}{2} \cdot \frac{a-c\omega}{2} = \frac{a^2-c^2\omega^2}{4} = \frac{a^2-c^2(g^2-4)}{4} = \frac{a^2-(a^2-4)}{4} = 1,$$

also

$$\frac{1}{\gamma} = \frac{g-\omega}{2}, \quad \frac{1}{\alpha} = \frac{a-c\omega}{2}.$$

Also gilt

$$\gamma + \frac{1}{\gamma} = g, \quad \alpha + \frac{1}{\alpha} = a.$$

Daraus sieht man sofort, dass γ eine Nullstelle des Polynoms $x^2 - gx + 1$ und α eine Nullstelle des Polynoms $x^2 - ax + 1$ ist. Der Rest folgt mit früheren Aussagen. ■

Im Fall $\left(\frac{g^2-4}{4}\right) = -1$ kann man also die Gleichung $V_x(g,1) = a$ auf die Berechnung von Logarithmen in $\mathbb{F}_p[\sqrt{g^2-4}]$ zurückführen.

Bemerkung: Sei p eine ungerade Primzahl und $d \in \mathbb{F}_p$ mit $\left(\frac{d}{p}\right) = -1$. Sei $\sqrt{d} \in \overline{\mathbb{F}}_p$ ein Element mit $(\sqrt{d})^2 = d$. Dann ist

$$\mathbb{F}_p[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{F}_p\}$$

ein 2-dimensionaler $\mathbb{F}_p$-Vektorraum:

$$\mathbb{F}_p[\sqrt{d}] \to \mathbb{F}_p \times \mathbb{F}_p, \quad a + b\sqrt{d} \mapsto (a,b)$$

ist also eine Bijektion. Die Multiplikation

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}$$

wird dann zu

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 + b_1b_2d, a_2b_2 + a_1b_2).$$

Wie man das und das Potenzieren in Python3 realisieren kann, zeigen die folgenden Python3-Funktionen:

```
def Fp_sqrtd_mult(ab1,ab2,pd):
   a1,b1=ab1
   a2,b2=ab2
   p,d=pd
   return [(a1*a2+b1*b2*d)%p,(a1*b2+a2*b1)%p]

def Fp_sqrtd_pot(ab,e,pd):
   i,a,b=e,[1,0],ab[:]
   while i>0:
     while i%2==0:
      i,b=i//2,Fp_sqrtd_mult(b,b,pd)
     i,a=i-1,Fp_sqrtd_mult(a,b,pd)
   return a
```

Beispiel: $p = 13$, $g = 3$ und in $\mathbb{F}_p$

$$V_5(g, 1) = 6.$$

Es ist $\left(\frac{g^2-4}{p}\right) = \left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$. Wir betrachten

$$\gamma = \frac{g + \sqrt{g^2 - 4}}{2} = \frac{3 + \sqrt{5}}{2} = 8 + 7\sqrt{5}.$$

Wir brauchen c mit $a = 6$ und

$$c^2 = \frac{a^2 - 4}{g^2 - 4} = \frac{13}{5} = 9 = 3^2,$$

wir wählen $c = 3$ und setzen

$$\alpha = \frac{a + c\sqrt{5}}{2} = \frac{6 + 3\sqrt{5}}{2} = 3 + 8\sqrt{5}.$$

Dann ist

$$\frac{1}{\alpha} = 3 - 8\sqrt{5} = 3 + 5\sqrt{5}.$$

Wir berechnen

$$\begin{aligned}
\gamma &= 8 + 7\sqrt{5}, \\
\gamma^2 &= 10 + 8\sqrt{5}, \\
\gamma^3 &= 9 + 4\sqrt{5}, \\
\gamma^4 &= 4 + 4\sqrt{5}, \\
\gamma^5 &= 3 + 8\sqrt{5}, \\
\gamma^6 &= 5 + 7\sqrt{5}, \\
\gamma^7 &= 12, \\
\gamma^8 &= 5 + 6\sqrt{5}, \\
\gamma^9 &= 3 + 5\sqrt{5}, \\
\gamma^{10} &= 4 + 9\sqrt{5}, \\
\gamma^{11} &= 9 + 9\sqrt{5}, \\
\gamma^{12} &= 10 + 5\sqrt{5}, \\
\gamma^{13} &= 8 + 6\sqrt{5}, \\
\gamma^{14} &= 1.
\end{aligned}$$

Wir sehen also: $\gamma^5 = \alpha$, was zu $V_5(g,1) = 6$ passt. (Außerdem gilt $\gamma^9 = \frac{1}{\alpha}$.)

Im Fall $\left(\frac{g^2-4}{p}\right) = -1$ ist $p+1$ die größtmögliche Ordnung von γ. Das folgende Lemma zeigt, wie man diese Situation erreichen kann, wenn man die Faktorisierung von $p+1$ kennt:

LEMMA. *Sei p eine ungerade Primzahl, $g \in \mathbb{F}_p$ mit $\left(\frac{g^2-4}{p}\right) = -1$, γ eine Nullstelle von $x^2 - gx + 1$ in $\mathbb{F}_{p^2}$. Sind $q_1, \ldots, q_r$ die verschiedenen Primteiler von $p+1$ und gilt*

$$V_{\frac{p+1}{q_i}}(g,1) \neq 2 \text{ für alle } i = 1, \ldots, r,$$

so folgt

$$\operatorname{ord}(\gamma) = p+1.$$

(Da immer $\operatorname{ord}(\gamma) \mid p+1$ gilt, hat γ also maximale Ordnung.)

Beweis: Wir wissen bereits, dass $\operatorname{ord}(\gamma) \mid p+1$ gilt. Wäre $\operatorname{ord}(\gamma) < p+1$, so gäbe es einen Primteiler q_i von $p+1$ mit

$$\operatorname{ord}(\gamma) \mid \frac{p+1}{q_i}.$$

Nach einem zuvor gezeigten Lemma würde dies aber

$$V_{\frac{p+1}{q_i}}(g,1) = 2$$

implizieren im Widerspruch zur Voraussetzung. Also folgt die Behauptung. ■

Bemerkung: Sei p eine ungerade Primzahl. Dann sind

$$Z_{p-1} = \{\alpha \in \overline{\mathbb{F}}_p^* : \alpha^{p-1} = 1\} = \mathbb{F}_p^*$$

und

$$Z_{p+1} = \{\alpha \in \overline{\mathbb{F}}_p^* : \alpha^{p+1} = 1\} \subseteq \mathbb{F}_{p^2}$$

zyklische Gruppen der Ordnung $p-1$ bzw. $p+1$. Im Fall $\left(\frac{g^2-4}{p}\right) = -1$ spielt das Logarithmenproblem in der Gruppe $Z_{p+1} \subseteq \mathbb{F}_{p^2}^*$. Welches Sicherheitsniveau liefert dies?

Bisher haben wir nur einen spezialisierten Algorithmus zur Berechnung diskreter Logarithmen betrachtet - beim Wurzelziehen modulo p. Wir zeigen an einem Beispiel, dass man diesen auch hier anwenden kann. Wir wiederholen den Satz:

SATZ. *Sei G eine (multiplikativ geschriebene) zyklische Gruppe der Ordnung 2^ℓ mit erzeugendem Element $g \in G$, d.h. $\operatorname{ord}(g) = 2^\ell$ und $G = \{g^i : 0 \leq i \leq 2^\ell - 1\}$, und $a \in G$.*

(1) *Es gibt $y_0, y_1, \ldots, y_{\ell-1} \in \{0,1\}$ mit*

$$a \cdot g^{\sum_{i=0}^{\ell-1} y_i \cdot 2^i} = 1.$$

(2) *Definiert man $g_j = g^{2^j}$, so gelten die Rekursionsformeln*

$$g_0 = g \quad \text{und} \quad g_{j+1} = g_j^2.$$

(3) *Definiert man für $0 \leq j \leq \ell - 1$*

$$h_j = a \cdot \prod_{0 \leq i \leq j-1} (g^{2^i})^{y_i},$$

so gelten die Rekursionsformeln

$$h_0 = a \quad \text{und} \quad h_{j+1} = h_j \cdot (g_j)^{y_j} = \begin{cases} h_j, & \text{falls } y_j = 0, \\ h_j g_j, & \text{falls } y_j = 1. \end{cases}$$

(4) *Es gilt für $0 \leq j \leq \ell - 1$*

$$y_j = \begin{cases} 0, & \text{falls } h_j^{2^{\ell-1-j}} = 1, \\ 1, & \text{sonst.} \end{cases}$$

(5) *Es ist*

$$a = g^{2^\ell - \sum_{i=0}^{\ell-1} y_i \cdot 2^i},$$

d.h. $2^\ell - \sum_{i=0}^{\ell-1} y_i \cdot 2^i$ *ist ein diskreter Logarithmus von* a *zur Basis* g*.*

Der vorangegangene Satz führt sofort zu folgendem Algorithmus:

Berechnung diskreter Logarithmen in einer zyklischen Gruppe der Ordnung 2^ℓ:
Eingabe: Zyklische Gruppe G der Ordnung 2^ℓ, $g \in G$ mit $\operatorname{ord}(g) = 2^\ell$, $a \in G$
Ausgabe: $x \in \mathbb{N}_0$ mit $g^x = a$ (x ist diskreter Logarithmus von a zur Basis g in G)

1: $g_j \leftarrow g$, $h \leftarrow a$, $x \leftarrow 2^\ell$
2: **for** $0 \le j \le \ell - 1$ **do**
3: **if** $h^{2^{\ell-1-j}} \neq 1$ **then**
4: $x \leftarrow x - 2^j$
5: $h \leftarrow h g_j$
6: **end if**
7: $g_j \leftarrow g_j^2$
8: **end for**
9: **return** x (oder $x \bmod 2^\ell$)

Für unsere Anwendung ist $\gamma \in \mathbb{F}_p[\sqrt{d}] = \mathbb{F}_{p^2}$ mit $\operatorname{ord}(\gamma) = 2^\ell$. Es muss gelten $\alpha^{2^\ell} = 1$. Dann liefert die folgende Python3-Funktion ein x mit

$$\gamma^x = \alpha,$$

sodass insbesondere $V_x(g, 1) = a$ (in $\mathbb{F}_p$) gilt:

```
# Diskrete Logarithmus bei 2-Potenz-Ordnung
# g habe Ordnung 2^l modulo p, ausserdem sei a^(2^l)=1 mod p.
# Bestimmt wird der diskrete Logarithmus von a zur Basis g modulo p.
def Fp_sqrtd_dlog2(a,g,pd,l):
  g_j=g
  h=a
  x=2**l
  for j in range(l):
    if Fp_sqrtd_pot(h,2**(l-1-j),pd)!=[1,0]:
      x=x-2**j
      h=Fp_sqrtd_mult(h,g_j,pd)
    g_j=Fp_sqrtd_mult(g_j,g_j,pd)
  return x%(2**l)
```

Beispiel: Wir verwenden

$$p = 2^{127} - 1 = 170141183460469231731687303715884105727.$$

Für $g = 3$ gilt

$$\left(\frac{g^2 - 4}{p}\right) = -1, \quad V_{p+1}(g, 1) \equiv 2 \bmod p, \quad V_{\frac{p+1}{2}}(g, 1) \not\equiv 2 \bmod p,$$

weswegen wir im Folgenden $g = 3$ wählen. Nun gilt für

$$a = 48496884446176924557492608885515476347$$

ebenso $\left(\frac{a^2-4}{p}\right) = -1$.
Wir wählen $\sqrt{5} \in \overline{\mathbb{F}}_p$ mit $(\sqrt{5})^2 = 5$ und erhalten dann als (eine) Nullstelle von $x^2 - 3x + 1$ in $\overline{\mathbb{F}}_p$

$$\gamma = \frac{3 + \sqrt{5}}{2}.$$

Man rechnet nach, dass gilt

$$\operatorname{ord}(\gamma) = 2^{127}.$$

Mit

$$c = 97558773622640599281512762427975712262$$

gilt in $\mathbb{F}_p$

$$a^2 - 4 = c^2 \cdot (g^2 - 4) = c^2 \cdot 5.$$

(c haben wir durch Wurzelziehen modulo p bestimmt.) Daher ist

$$\alpha = \frac{a + c\sqrt{5}}{2}$$

eine Nullstelle von $x^2 - ax + 1$. Man stellt fest, dass gilt

$$\alpha^{2^{127}} = 1.$$

Nun berechnen wir den diskreten Logarithmus von α zur Basis γ in $\mathbb{F}_p[\sqrt{5}]$ mit obiger Python3-Funktion. Wir erhalten

$$x = 703017704005960307793406293646966859 72 \quad \text{mit} \quad \gamma^x = \alpha.$$

Nun überprüft man, dass mit diesem x tatsächlich gilt

$$a \equiv V_y(g, 1) \bmod p.$$

Wir haben also die Gleichung $V_x(g, 1) \equiv a \bmod p$ schnell gelöst.

17. Die Zeckendorf-Zerlegung

Die Fibonacci-Folge $(f_i)_{i\geq 0}$ ist die Lucas-Folge $(U_i(1, -1))_{i\geq 1}$, sodass folgende Rekursionsbedingungen gelten:

$$f_0 = 0, \quad f_1 = 1, \quad f_i = f_{i-1} + f_{i-2} \text{ für } i \geq 2.$$

Die Fibonacci-Zahlen erhält man so: Man beginnt mit 0, 1. Hat man schon Folgenglieder berechnet, so erhält man ein neues Folgenglied, indem man die beiden zuletzt berechneten Folgenglieder addiert:

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad 55, \quad 89, \quad 144, \quad 233, \quad \ldots$$

Hier sind nochmals die ersten Folgenglieder mit Indizes:

$$f_0 = 0, \quad f_1 = 1, \quad f_2 = 1, \quad f_3 = 2, \quad f_4 = 3, \quad f_5 = 5, \quad f_6 = 8, \quad f_7 = 13, \quad f_8 = 21, \quad f_9 = 34,$$
$$f_{10} = 55, \quad f_{11} = 89, \quad f_{12} = 144, \quad f_{13} = 233, \quad f_{14} = 377, \quad f_{15} = 610, \quad f_{16} = 987, \quad f_{17} = 1597,$$
$$f_{18} = 2584, \quad f_{19} = 4181, \quad f_{20} = 6765, \quad f_{21} = 10946, \quad f_{22} = 17711, \quad f_{23} = 28657, \quad f_{24} = 46368.$$

E. Zeckendorf (1901-1983) hat beobachtet, dass sich jede natürliche Zahl als Summe verschiedener Fibonacci-Zahlen schreiben lässt:

$$\begin{aligned}
1 &= f_1 = f_2 \\
2 &= f_1 + f_2 = f_3 \\
3 &= f_1 + f_3 = f_2 + f_3 = f_4 \\
4 &= f_1 + f_2 + f_3 = f_1 + f_4 = f_2 + f_4 \\
5 &= f_1 + f_2 + f_4 = f_3 + f_4 = f_5 \\
6 &= f_1 + f_3 + f_4 = f_1 + f_5 = f_2 + f_3 + f_4 = f_2 + f_5 \\
7 &= f_1 + f_2 + f_3 + f_4 = f_1 + f_2 + f_5 = f_3 + f_5 \\
8 &= f_1 + f_3 + f_5 = f_2 + f_3 + f_5 = f_4 + f_5 = f_6 \\
9 &= f_1 + f_2 + f_3 + f_5 = f_1 + f_4 + f_5 = f_1 + f_6 = f_2 + f_4 + f_5 = f_2 + f_6 \\
10 &= f_1 + f_2 + f_4 + f_5 = f_1 + f_2 + f_6 = f_3 + f_4 + f_5 = f_3 + f_6 \\
11 &= f_1 + f_3 + f_4 + f_5 = f_1 + f_3 + f_6 = f_2 + f_3 + f_4 + f_5 = f_2 + f_3 + f_6 = f_4 + f_6 \\
12 &= f_1 + f_2 + f_3 + f_4 + f_5 = f_1 + f_2 + f_3 + f_6 = f_1 + f_4 + f_6 = f_2 + f_4 + f_6 \\
13 &= f_1 + f_2 + f_4 + f_6 = f_3 + f_4 + f_6 = f_5 + f_6 = f_7 \\
14 &= f_1 + f_3 + f_4 + f_6 = f_1 + f_5 + f_6 = f_1 + f_7 = f_2 + f_3 + f_4 + f_6 = f_2 + f_5 + f_6 = f_2 + f_7 \\
15 &= f_1 + f_2 + f_3 + f_4 + f_6 = f_1 + f_2 + f_5 + f_6 = f_1 + f_2 + f_7 = f_3 + f_5 + f_6 = f_3 + f_7
\end{aligned}$$

Wenn man fordert, dass keine zwei aufeinanderfolgenden Fibonacci-Zahlen in der Summenzerlegung benutzt werden, und dass nur Fibonacci-Zahlen f_i für $i \geq 2$ verwendet werden, erhält man sogar eine eindeutige Zerlegung:

$$
\begin{aligned}
1 &= f_2 = 1 \\
2 &= f_3 = 2 \\
3 &= f_4 = 3 \\
4 &= f_4 + f_2 = 3 + 1 \\
5 &= f_5 = 5 \\
6 &= f_5 + f_2 = 5 + 1 \\
7 &= f_5 + f_3 = 5 + 2 \\
8 &= f_6 = 8 \\
9 &= f_6 + f_2 = 8 + 1 \\
10 &= f_6 + f_3 = 8 + 2 \\
11 &= f_6 + f_4 = 8 + 3 \\
12 &= f_6 + f_4 + f_2 = 8 + 3 + 1 \\
13 &= f_7 = 13 \\
14 &= f_7 + f_2 = 13 + 1 \\
15 &= f_7 + f_3 = 13 + 2 \\
16 &= f_7 + f_4 = 13 + 3 \\
17 &= f_7 + f_4 + f_2 = 13 + 3 + 1 \\
18 &= f_7 + f_5 = 13 + 5 \\
19 &= f_7 + f_5 + f_2 = 13 + 5 + 1 \\
20 &= f_7 + f_5 + f_3 = 13 + 5 + 2 \\
21 &= f_8 = 21 \\
22 &= f_8 + f_2 = 21 + 1 \\
23 &= f_8 + f_3 = 21 + 2 \\
24 &= f_8 + f_4 = 21 + 3 \\
25 &= f_8 + f_4 + f_2 = 21 + 3 + 1 \\
26 &= f_8 + f_5 = 21 + 5 \\
27 &= f_8 + f_5 + f_2 = 21 + 5 + 1 \\
28 &= f_8 + f_5 + f_3 = 21 + 5 + 2 \\
29 &= f_8 + f_6 = 21 + 8 \\
30 &= f_8 + f_6 + f_2 = 21 + 8 + 1 \\
31 &= f_8 + f_6 + f_3 = 21 + 8 + 2 \\
32 &= f_8 + f_6 + f_4 = 21 + 8 + 3 \\
33 &= f_8 + f_6 + f_4 + f_2 = 21 + 8 + 3 + 1 \\
34 &= f_9 = 34 \\
35 &= f_9 + f_2 = 34 + 1 \\
36 &= f_9 + f_3 = 34 + 2 \\
37 &= f_9 + f_4 = 34 + 3 \\
38 &= f_9 + f_4 + f_2 = 34 + 3 + 1 \\
39 &= f_9 + f_5 = 34 + 5 \\
40 &= f_9 + f_5 + f_2 = 34 + 5 + 1 \\
41 &= f_9 + f_5 + f_3 = 34 + 5 + 2 \\
42 &= f_9 + f_6 = 34 + 8 \\
43 &= f_9 + f_6 + f_2 = 34 + 8 + 1 \\
44 &= f_9 + f_6 + f_3 = 34 + 8 + 2 \\
45 &= f_9 + f_6 + f_4 = 34 + 8 + 3 \\
46 &= f_9 + f_6 + f_4 + f_2 = 34 + 8 + 3 + 1 \\
47 &= f_9 + f_7 = 34 + 13 \\
48 &= f_9 + f_7 + f_2 = 34 + 13 + 1 \\
49 &= f_9 + f_7 + f_3 = 34 + 13 + 2 \\
50 &= f_9 + f_7 + f_4 = 34 + 13 + 3 \\
51 &= f_9 + f_7 + f_4 + f_2 = 34 + 13 + 3 + 1 \\
52 &= f_9 + f_7 + f_5 = 34 + 13 + 5 \\
53 &= f_9 + f_7 + f_5 + f_2 = 34 + 13 + 5 + 1 \\
54 &= f_9 + f_7 + f_5 + f_3 = 34 + 13 + 5 + 2 \\
55 &= f_{10} = 55 \\
56 &= f_{10} + f_2 = 55 + 1 \\
57 &= f_{10} + f_3 = 55 + 2 \\
58 &= f_{10} + f_4 = 55 + 3 \\
59 &= f_{10} + f_4 + f_2 = 55 + 3 + 1 \\
60 &= f_{10} + f_5 = 55 + 5 \\
61 &= f_{10} + f_5 + f_2 = 55 + 5 + 1 \\
62 &= f_{10} + f_5 + f_3 = 55 + 5 + 2 \\
63 &= f_{10} + f_6 = 55 + 8 \\
64 &= f_{10} + f_6 + f_2 = 55 + 8 + 1 \\
65 &= f_{10} + f_6 + f_3 = 55 + 8 + 2 \\
66 &= f_{10} + f_6 + f_4 = 55 + 8 + 3 \\
67 &= f_{10} + f_6 + f_4 + f_2 = 55 + 8 + 3 + 1 \\
68 &= f_{10} + f_7 = 55 + 13 \\
69 &= f_{10} + f_7 + f_2 = 55 + 13 + 1 \\
70 &= f_{10} + f_7 + f_3 = 55 + 13 + 2 \\
71 &= f_{10} + f_7 + f_4 = 55 + 13 + 3 \\
72 &= f_{10} + f_7 + f_4 + f_2 = 55 + 13 + 3 + 1 \\
73 &= f_{10} + f_7 + f_5 = 55 + 13 + 5 \\
74 &= f_{10} + f_7 + f_5 + f_2 = 55 + 13 + 5 + 1 \\
75 &= f_{10} + f_7 + f_5 + f_3 = 55 + 13 + 5 + 2 \\
76 &= f_{10} + f_8 = 55 + 21 \\
77 &= f_{10} + f_8 + f_2 = 55 + 21 + 1 \\
78 &= f_{10} + f_8 + f_3 = 55 + 21 + 2 \\
79 &= f_{10} + f_8 + f_4 = 55 + 21 + 3 \\
80 &= f_{10} + f_8 + f_4 + f_2 = 55 + 21 + 3 + 1 \\
81 &= f_{10} + f_8 + f_5 = 55 + 21 + 5 \\
82 &= f_{10} + f_8 + f_5 + f_2 = 55 + 21 + 5 + 1 \\
83 &= f_{10} + f_8 + f_5 + f_3 = 55 + 21 + 5 + 2 \\
84 &= f_{10} + f_8 + f_6 = 55 + 21 + 8 \\
85 &= f_{10} + f_8 + f_6 + f_2 = 55 + 21 + 8 + 1 \\
86 &= f_{10} + f_8 + f_6 + f_3 = 55 + 21 + 8 + 2 \\
87 &= f_{10} + f_8 + f_6 + f_4 = 55 + 21 + 8 + 3 \\
88 &= f_{10} + f_8 + f_6 + f_4 + f_2 = 55 + 21 + 8 + 3 + 1 \\
89 &= f_{11} = 89 \\
90 &= f_{11} + f_2 = 89 + 1 \\
91 &= f_{11} + f_3 = 89 + 2 \\
92 &= f_{11} + f_4 = 89 + 3 \\
93 &= f_{11} + f_4 + f_2 = 89 + 3 + 1 \\
94 &= f_{11} + f_5 = 89 + 5 \\
95 &= f_{11} + f_5 + f_2 = 89 + 5 + 1 \\
96 &= f_{11} + f_5 + f_3 = 89 + 5 + 2 \\
97 &= f_{11} + f_6 = 89 + 8 \\
98 &= f_{11} + f_6 + f_2 = 89 + 8 + 1 \\
99 &= f_{11} + f_6 + f_3 = 89 + 8 + 2 \\
100 &= f_{11} + f_6 + f_4 = 89 + 8 + 3
\end{aligned}
$$

SATZ (Zeckendorf-Zerlegung). *Für jedes $n \in \mathbb{N}$ gibt es eine eindeutige Summenzerlegung*

$$n = f_{i_1} + f_{i_2} + \cdots + f_{i_k}$$

mit

$$i_1 > i_2 > \cdots > i_k \geq 2 \quad \textit{und} \quad i_1 - i_2 \geq 2,\, i_2 - i_3 \geq 2,\, \ldots, i_{k-1} - i_k \geq 2.$$

Außerdem gilt

$$f_{i_1} \leq n < f_{i_1+1},$$

wodurch i_1 (mit $i_1 \geq 2$) eindeutig bestimmt ist.

Bemerkung: Im nachfolgenden Beweis werden wir die Formeln

$$\sum_{i=1}^{n} f_{2i} = f_{2n+1} - 1 \quad \text{und} \quad \sum_{i=1}^{n} f_{2i-1} = f_{2n}$$

benutzen, die sich leicht durch Induktion beweisen lassen.

Beweis des Satzes:

(1) Zur Existenz der Darstellung: Es ist

$$1 = f_2, \quad 2 = f_3, \quad 3 = f_4, \quad 4 = f_4 + f_1, \quad 5 = f_5, \quad 6 = f_5 + f_2, \quad \ldots$$

sodass der Induktionsanfang kein Problem ist. Sei jetzt $n > 1$ gegeben, die Behauptung gelte für alle kleineren natürlichen Zahlen. Wir bestimmen den (größten) Index i_1 mit $f_{i_1} \leq n < f_{i_1+1}$. Dann ist $i_1 \geq 2$. Es folgt $0 \leq n - f_{i_1} < f_{i_1+1} - f_{i_1} = f_{i_1-1} < n$. Wir wenden die Induktionsvoraussetzung auf $n - f_{i_1}$ an und erhalten eine Darstellung

$$n - f_{i_1} = f_{i_2} + \cdots + f_{i_k}$$

mit

$$i_2 > i_3 > \cdots > i_k \geq 2 \quad \text{und} \quad i_2 - i_3 \geq 2, \ldots, i_{k-1} - i_k \geq 2.$$

Wegen $n - f_{i_1} < f_{i_1-1}$ ist $f_{i_2} < f_{i_1-1}$, also $i_2 < i_1 - 1$, d.h. $i_1 > i_2$ und $i_1 - i_2 \geq 2$. Daraus folgt die Behauptung.

(2) Wir nehmen jetzt an, dass wir eine Darstellung

$$n = f_{i_1} + \cdots + f_{i_k} \text{ mit } i_1 > \cdots > i_k \geq 2 \text{ und } i_1 - i_2 \geq 2, \ldots, i_{k-1} - i_k \geq 2$$

haben. Wir benützen die Formeln der vorangehenden Bemerkung:

(a) Falls i_1 gerade ist, so gilt

$$f_{i_2} + f_{i_3} + \cdots + f_{i_k} \leq f_{i_1-2} + f_{i_2-4} + \cdots + f_4 + f_2 = f_{i_1-1} - 1.$$

(b) Falls i_1 ungerade ist, so gilt

$$f_{i_2} + f_{i_3} + \cdots + f_{i_k} \leq f_{i_1-2} + f_{i_1-4} + \cdots + f_5 + f_3 = f_{i_1-1} - 1.$$

In jedem Fall gilt also

$$f_{i_2} + \cdots + f_{i_k} \leq f_{i_1-1} - 1.$$

Da offensichtlich $f_{i_1} \leq n$ ist, folgt weiter

$$f_{i_1} \leq n = f_{i_1} + (f_{i_2} + \cdots + f_{i_k}) \leq f_{i_1} + f_{i_1-1} - 1 = f_{i_1+1} - 1 < f_{i_1+1},$$

wie behauptet. Wegen $i_1 \geq 2$, der strengen Monotonie $f_2 < f_3 < f_4 < \ldots$ und $\lim_{i\to\infty} f_i = \infty$ ist dann i_1 eindeutig bestimmt.

(3) Zur Eindeutigkeit der Darstellung: Auch dies kann man durch Induktion sehen. Der Anfang ist klar. Ist n gegeben, so ist f_{i_1} durch $f_{i_1} \leq n < f_{i_1+1}$ nach (2) eindeutig bestimmt. Nun hat man für $n - f_{i_1}$ die Darstellung

$$n - f_{i_1} = f_{i_2} + \cdots + f_{i_k}$$

und kann darauf die Induktionsvoraussetzung anwenden. ■

Der Satz liefert ein Verfahren zur Herleitung der Zeckendorf-Zerlegung:

Algorithmus zur Bestimmung der Zeckendorf-Zerlegung: Gegeben sei $n \in \mathbb{N}$. Bestimmt wird eine Darstellung

$$n = f_{i_1} + \cdots + f_{i_k} \text{ mit } i_1 > \cdots > i_k \geq 2 \text{ und } i_1 - i_2 \geq 2, \ldots, i_{k-1} - i_k \geq 2.$$

(1) Setze $n_1 := n$ und $k := 1$.
(2) Bestimme den größten Index i_k mit

$$f_{i_k} \leq n_k < f_{i_k+1}$$

und setze

$$n_{k+1} := n_k - f_{i_k}.$$

(3) Ist $n_{k+1} > 0$, setze $k := k + 1$ und gehe zu (2).
(4) Hier ist $n_{k+1} = 0$. Gib die Darstellung

$$n = f_{i_1} + \cdots + f_{i_k} \quad \text{bzw. die Indexfolge } (i_1, i_2, \ldots, i_k)$$

aus.

Man kann die Zeckendorf-Zerlegung auch rekursiv bestimmen, wie folgendes Python-Funktion zeigt:

```
# Es wird der Index i mit f_i<=n<f_(i+1) bestimmt und (i,n-f_i)
# zurueckgegeben.
def zeckendorf0(n):
  f,g=0,1; i=0 # f=f_i, g=f_(i+1)
  while g<=n:
    f,g=g,f+g
    i+=1
  # Jetzt gilt f=f_i<=n<f_(i+1)
  return (i,n-f)

# Zu n>0 wird I=[i1,i2,...] bestimmt, sodass n=f_(i1)+f_(i2)+... gilt.
def zeckendorf(n):
  I=[]
  while n>0:
    (i,n)=zeckendorf0(n)
    I.append(i)
  return I
```

Hier ist eine weitere Python-Funktion, die die Zeckendorf-Zerlegung einer natürlichen Zahl n bestimmt, und die zugehörige Umkehrfunktion.

```
def zeckendorf(n):
  f=[0,1,1]
  while f[-1]<n:
    f.append(f[-1]+f[-2])
  I=[]
  while n>0:
    while f[-1]>n:
      f.pop()
    I.append(len(f)-1)
    n=n-f[-1]
  return I

def zeckendorf_inv(I):
  f=[0,1]
```

```
while len(f)<=I[0]:
    f.append(f[-1]+f[-2])
n=0
for i in I:
    n+=f[i]
return n
```