KAPITEL 1

Quadrate und Quadratwurzeln modulo n

Wir werden zunächst die Lösbarkeit der Gleichung $x^2 \equiv a \bmod p$ für eine Primzahl p untersuchen und gegebenenfalls eine Lösung konstruieren. Die Schwierigkeit, die Gleichung $x^2 \equiv a \bmod n$ für zusammengesetztes n zu lösen, wird zur Konstruktion von Kryptosystemen benutzt.

1. Einführung

Wir betrachten für einige „Zahlbereiche“ die Frage, wann eine Zahl ein Quadrat in diesem „Zahlbereich“ ist.

Quadrate in $\mathbb{R}$: Wann ist eine reelle Zahl r ein Quadrat (einer reellen Zahl)? Anders ausgedrückt: Für welche $r \in \mathbb{R}$ ist die Gleichung

$$x^2 = r$$

in $\mathbb{R}$ lösbar? Die Antwort ist hier einfach:

$$r \text{ ist Quadrat in } \mathbb{R} \quad \Longleftrightarrow \quad r \geq 0.$$

Quadrate in $\mathbb{N}$: Wann ist eine natürliche Zahl n eine Quadratzahl? Anders ausgedrückt: Für welche $n \in \mathbb{N}$ ist die Gleichung

$$x^2 = n$$

in $\mathbb{N}$ lösbar? Es sind hier durchaus unterschiedliche Antworten möglich:

- **Theoretische Antwort:** Hat n die Primfaktorzerlegung

  $$n = p_1^{e_1} \dots p_r^{e_r},$$

  so gilt

  $$n \text{ ist Quadratzahl} \quad \Longleftrightarrow \quad \text{alle } e_i \text{ sind gerade.}$$

- **Praktische Antwort:**

  $$n \text{ ist Quadratzahl} \quad \Longleftrightarrow \quad \left(\lfloor \sqrt{n} \rfloor\right)^2 = n.$$

  Dabei ist $\lfloor \sqrt{n} \rfloor$ die abgerundete Wurzel aus n, die man schnell berechnen kann ($\longrightarrow$ Kryptographie I), beispielsweise mit folgender Python-Funktion:

```
def sqrt(n):
  if n==0:
    return 0
  x=n
  while True:
    y=(x+n//x)//2
    if y>=x:
      return x
    x=y
```

  Damit kann man dann schnell testen, ob eine natürliche Zahl n eine Quadratzahl ist.

Datei: kii_quad_einfuehrung.tex. Version vom 21.4.2025

2. Das Legendre-Symbol $\left(\frac{a}{p}\right)$

Die Lösbarkeit der Gleichung $x^2 \equiv a \bmod p$ wird durch das sogenannte Legendre-Symbol beschrieben:

DEFINITION. *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann definiert man das* **Legendre-Symbol** $\left(\frac{a}{p}\right)$ *durch*

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{falls } \mathrm{ggT}(a,p) = 1 \text{ und ein } x \in \mathbb{Z} \text{ existiert mit } x^2 \equiv a \bmod p, \\ -1, & \text{falls } \mathrm{ggT}(a,p) = 1 \text{ und kein } x \in \mathbb{Z} \text{ existiert mit } x^2 \equiv a \bmod p, . \\ 0, & \text{falls } a \equiv 0 \bmod p. \end{cases}$$

Ist $\left(\frac{a}{p}\right) = 1$, so nennt man a einen **quadratischen Rest modulo** *p, d.h. a ist Quadrat modulo p; ist $\left(\frac{a}{p}\right) = -1$, so nennt man a einen* **quadratischen Nichtrest modulo** *p, d.h. a ist kein Quadrat modulo p.*

Achtung: Die Schreibweise $\left(\frac{a}{p}\right)$ meint hier die eben definierte Funktion und nicht den Bruch $\frac{a}{p}$, der in Klammern gesetzt wurde. Die Notation geht wohl auf Legendre zurück (A. M. Legendre. Essai sur la théorie des nombres. Paris, 1798. Seite 186). Heutzutage könnte man sich besser eine Schreibweise wie $\mathrm{LS}(a,p)$ (oder ähnlich) vorstellen.

Aus der Definition ergibt sich sofort folgende Eigenschaft, die wir der Wichtigkeit halber als Satz formulieren:

SATZ. *Ist p eine ungerade Primzahl, so gilt für $a, b \in \mathbb{Z}$ die Implikation*

$$a \equiv b \bmod p \quad \Longrightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Bemerkung: Für eine ungerade Primzahl p ist das Legendre-Symbol also eine Funktion

$$\mathbb{Z} \xrightarrow{a \mapsto \left(\frac{a}{p}\right)} \{0, 1, -1\}.$$

Da aber $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ für $a \equiv b \bmod p$ gilt, kann man das Legendre-Symbol auch als Funktion

$$\mathbb{F}_p \xrightarrow{a \mapsto \left(\frac{a}{p}\right)} \{0, 1, -1\}$$

auffassen, wenn wir jetzt $\mathbb{F}_p$ mit $\mathbb{Z}/p\mathbb{Z}$ identifizieren. Man erhält dann folgende Beschreibung:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } a \in \mathbb{F}_p^{*2}, \\ -1, & \text{falls } a \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{*2}, \\ 0, & \text{falls } a = 0. \end{cases}$$

Dabei ist

$$\mathbb{F}_p^{*2} = \{b^2 : b \in \mathbb{F}_p^*\}$$

die Menge der Quadrate ($\neq 0$) in $\mathbb{F}_p$.

Wenn man für (kleine) p also $\mathbb{F}_p^{*2}$ explizit ausrechnet, kann man eine Tabelle für $\left(\frac{a}{p}\right)$ erstellen.

Beispiele:

- $p = 3$:

$b \in \mathbb{F}_3$	0	1	2
$b^2 \in \mathbb{F}_3$	0	1	1

$\mathbb{F}_3^{*2} = \{1\}$

a	0	1	2
$\left(\frac{a}{3}\right)$	0	1	-1

- $p = 5$:

$b \in \mathbb{F}_5$	0	1	2	3	4
$b^2 \in \mathbb{F}_5$	0	1	4	4	1

$\mathbb{F}_5^{*2} = \{1, 4\}$

a	0	1	2	3	4
$\left(\frac{a}{5}\right)$	0	1	-1	-1	1

- $p = 7$:

$b \in \mathbb{F}_7$	0	1	2	3	4	5	6
$b^2 \in \mathbb{F}_7$	0	1	4	2	2	4	1

$\mathbb{F}_7^{*2} = \{1, 2, 4\}$

a	0	1	2	3	4	5	6
$\left(\frac{a}{7}\right)$	0	1	1	-1	1	-1	-1

- $p = 11$:

$b \in \mathbb{F}_{11}$	0	1	2	3	4	5	6	7	8	9	10
$b^2 \in \mathbb{F}_{11}$	0	1	4	9	5	3	3	5	9	4	1

(Beachte: $(p-x)^2 = (-x)^2 = x^2$ in $\mathbb{F}_p$)

$\mathbb{F}_{11}^{*\ 2} = \{1, 3, 4, 5, 9\}$

a	0	1	2	3	4	5	6	7	8	9	10
$\left(\frac{a}{11}\right)$	0	1	-1	1	1	1	-1	-1	-1	1	-1

Bemerkung: Wird die Gleichung $x^2 \equiv a \bmod p$ von $x = b$ und $x = c$ gelöst, so folgt $c \equiv \pm b \bmod p$, da $\mathbb{F}_p$ ein Körper ist. Damit erhält man sofort folgende Formel:

$$\#\{x \in \mathbb{F}_p : x^2 \equiv a \bmod p\} = \left(\frac{a}{p}\right) + 1 = \begin{cases} 2, & \text{falls } \left(\frac{a}{p}\right) = 1, \\ 1, & \text{falls } a \equiv 0 \bmod p, \\ 0, & \text{falls } \left(\frac{a}{p}\right) = -1. \end{cases}$$

Erinnerung: Aus der Algebra ist bekannt, dass die multiplikative Gruppe $\mathbb{F}_p^*$ des Körpers $\mathbb{F}_p$ zyklisch von der Ordnung $p-1$ ist. Ein Erzeuger g der multiplikativen Gruppe wird eine **Primitivwurzel modulo** p genannt. (Mit der Ordnungsfunktion drückt sich dies als $\operatorname{ord}_p(g) = p-1$ aus.)

- Es ist dann
$$\mathbb{F}_p = \{0, g, g^2, g^3, g^4, \ldots, g^{p-2}, g^{p-1} = 1\}.$$
- Für $m, n \in \mathbb{Z}$ gilt
$$g^m = g^n \quad \Longleftrightarrow \quad m \equiv n \bmod p-1.$$
- Aus $(g^{\frac{p-1}{2}})^2 = g^{p-1} = 1$ und $g^{\frac{p-1}{2}} \neq 1$ folgt sofort
$$g^{\frac{p-1}{2}} = -1.$$

Beispiel: Wir rechnen in $\mathbb{F}_7$:

i	0	1	2	3	4	5
$2^i \in \mathbb{F}_7$	1	2	4	1	2	4

i	0	1	2	3	4	5
$3^i \in \mathbb{F}_7$	1	3	2	6	4	5

Daraus ersieht man, dass 3 eine Primitivwurzel modulo 7 ist, 2 jedoch nicht. ($\operatorname{ord}_7(2) = 3$, $\operatorname{ord}_7(3) = 6$.)

Man kann ganz einfach charakterisieren, wann die Potenz g^m einer Primitivwurzel ein Quadrat in $\mathbb{F}_p$ ist:

LEMMA. *Sei p eine ungerade Primzahl und g eine Primitivwurzel modulo p. Dann gilt für $m \in \mathbb{Z}$:*

$$g^m \text{ ist Quadrat modulo } p, \text{ d.h. } \left(\frac{g^m}{p}\right) = 1 \quad \Longleftrightarrow \quad m \equiv 0 \bmod 2.$$

Anders ausgedrückt:

$$\left(\frac{g^m}{p}\right) = (-1)^m.$$

Beweis: Ist g^m ein Quadrat, so gibt es ein Element g^n mit $g^m = (g^n)^2$, also nach der Vorbemerkung $m \equiv 2n \bmod p-1$, was sofort $m \equiv 0 \bmod 2$ liefert. Ist umgekehrt $m \equiv 0 \bmod 2$, d.h. $m = 2n$, so ist $g^m = (g^n)^2$ natürlich ein Quadrat, also $\left(\frac{g^m}{p}\right) = 1$. ■

Bemerkungen:

(1) Aus der Formel ergibt sich unmittelbar, dass es jeweils genau $\frac{p-1}{2}$ Quadrate und Nichtquadrate modulo p gibt, wenn man die 0 herausnimmt:

$$\begin{aligned} \text{Quadrate mod } p: &\quad g^0, g^2, g^4, g^6, \ldots, g^{p-3} \quad \text{bzw.} \quad g^{2i} \text{ für } i = 0, \ldots, \tfrac{p-3}{2}, \\ \text{Nichtquadrate mod } p: &\quad g^1, g^3, g^5, g^7, \ldots, g^{p-2} \quad \text{bzw.} \quad g^{1+2i} \text{ für } i = 0, \ldots, \tfrac{p-3}{2}. \end{aligned}$$

(Beachte: $g^{p-1} = g^0 = 1$.)

(2) Zwar existieren für jede Primzahl p Primitivwurzeln - es gibt genau $\varphi(p-1)$ verschiedene Primitivwurzeln modulo p -, aber die Bestimmung einer Primitivwurzel ist für große p nur möglich, wenn man $p-1$ faktorisieren kann ($\longrightarrow$ Kryptographie I).

(3) Kennt man eine Primitivwurzel g modulo p und ist $a \in \mathbb{F}_p^*$, so gibt es ein $m \in \mathbb{N}_0$ mit $a = g^m$. Die Zahl m ist ein **diskreter Logarithmus** von a zur Basis g modulo p. Logarithmenberechnung ist für große p im Allgemeinen schwierig ($\longrightarrow$ Kryptographie I).

(4) Das vorangegangene Lemma ist zur Berechnung von $\left(\frac{a}{p}\right)$ praktisch also nicht/wenig geeignet.

Eine wichtige Rolle für das Legendre-Symbol spielt der folgende Satz von Euler:

Satz (Euler). *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann gilt:*

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

Beweis: Ist $a \equiv 0 \bmod p$, so stimmt die Gleichung offensichtlich. Sei jetzt $a \not\equiv 0 \bmod p$ und g eine Primitivwurzel modulo p. Dann gibt es $m \in \mathbb{N}$ mit $a \equiv g^m \bmod p$ und damit liefern unsere Vorbetrachtungen

$$\left(\frac{a}{p}\right) = \left(\frac{g^m}{p}\right) = (-1)^m \equiv (g^{\frac{p-1}{2}})^m = (g^m)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p,$$

was wir zeigen wollten. ■

Da man mit der **square-and-multiply-Methode** ($\longrightarrow$ Kryptographie I) schnell potenzieren kann, kann man mit dem Satz das Legendre-Symbol auch für große Primzahlen schnell berechnen.
Eine zugehörige Python-Funktion für das Legendre-Symbol könnte so aussehen:

```
def LS(a,p):
  L=pow(a,(p-1)//2,p)
  if L==p-1:
    L=-1
  return L
```

Beispiel: Für $p = 10^{100} + 267$ findet man

$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = -1, \quad \left(\frac{6}{p}\right) = 1.$$

Das Legendre-Symbol sagt, dass die Gleichung $x^2 \equiv 6 \bmod p$ lösbar ist, wir wissen aber noch nicht, wie man die Gleichung wirklich lösen kann. (Wir werden später verschiedene Lösungsmethoden kennenlernen.)

Wir stellen im Folgenden noch einige wichtige Eigenschaften des Legendre-Symbol zusammen:

Satz. *Für eine ungerade Primzahl p und $a, b \in \mathbb{Z}$ gilt*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Beweis: Mit dem Satz von Euler erhalten wir

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p.$$

Damit gilt

$$p \mid \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Da das Legendre-Symbol nur die Werte $0, 1, -1$ annehmen kann, folgt

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \in \{0, \pm 1, \pm 2\}.$$

Wegen $p \geq 3$ folgt dann aber $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0$, und damit die Behauptung. ■

Bemerkung: Die Formel $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ kann man für $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = \mathrm{ggT}(b,p) = 1$ auch so interpretieren:

a Quadrat modulo p und	b Quadrat modulo p	$\Longrightarrow$	ab Quadrat modulo p,
a kein Quadrat modulo p und	b Quadrat modulo p	$\Longrightarrow$	ab kein Quadrat modulo p,
a Quadrat modulo p und	b kein Quadrat modulo p	$\Longrightarrow$	ab kein Quadrat modulo p,
a kein Quadrat modulo p und	b kein Quadrat modulo p	$\Longrightarrow$	ab Quadrat modulo p.

Die ersten drei Aussagen gelten in jedem Körper, die letzte nicht.

Bemerkung: Ist a eine Quadratzahl in $\mathbb{N}$ mit $p \nmid a$, so ist a natürlich auch ein Quadrat modulo p, also $\left(\frac{a}{p}\right) = 1$. So gilt

$$\left(\frac{1}{p}\right) = 1, \quad \left(\frac{4}{p}\right) = 1, \quad \left(\frac{9}{p}\right) = 1 \text{ für } p \neq 3, \quad \left(\frac{16}{p}\right) = 1, \quad \left(\frac{25}{p}\right) = 1 \text{ für } p \neq 5, \quad \ldots$$

Der folgende Satz liefert eine Formel für $\left(\frac{-1}{p}\right)$:

Satz. *Für eine ungerade Primzahl p gilt:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{falls } p \equiv 1 \bmod 4, \\ -1, & \text{falls } p \equiv 3 \bmod 4. \end{cases}$$

(Statt $p \equiv 3 \bmod 4$ kann man auch $p \equiv -1 \bmod 4$ schreiben.)

Beweis: Aus dem Satz von Euler folgt für $a = -1$

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

Daher gilt

$$p \mid \left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}.$$

Wegen

$$\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}} \in \{0, \pm 1, \pm 2\}$$

und $p \geq 3$ folgt $\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}} = 0$, und damit die erste Gleichung. Für die zweite Gleichung machen wir eine Fallunterscheidung:

- **Fall $p \equiv 1 \bmod 4$:** Dann ist $p = 1 + 4k$ mit $k \in \mathbb{N}$ und
$$(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1.$$
- **Fall $p \equiv 3 \bmod 4$:** Dann ist $p = 3 + 4k$ mit $k \in \mathbb{N}_0$ und
$$(-1)^{\frac{p-1}{2}} = (-1)^{1+2k} = -1.$$

Damit ist die Behauptung bewiesen. ■

Bemerkung: Ist p eine Primzahl $\equiv 1 \bmod 4$, so ist $4 \mid p-1$ und $\frac{p-1}{4} \in \mathbb{N}$. Für eine Primitivwurzel $g \in \mathbb{F}_p$ gilt

$$\left(g^{\frac{p-1}{4}}\right)^2 = g^{\frac{p-1}{2}} = -1,$$

$g^{\frac{p-1}{4}}$ ist also eine Quadratwurzel von -1 in $\mathbb{F}_p$. Dies wird in folgendem Lemma verallgemeinert:

LEMMA. *Sei p eine Primzahl mit $p \equiv 1 \bmod 4$. Definiert man für $a \in \{1, \ldots, p-1\}$*

$$w = a^{\frac{p-1}{4}} \bmod p, \qquad \textit{so gilt} \qquad w^2 \equiv \begin{cases} 1 \bmod p, & \textit{falls } \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv 1 \bmod p, \\ -1 \bmod p, & \textit{falls } \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv -1 \bmod p. \end{cases}$$

Beweis: Für $a \in \{1, \ldots, p-1\}$ ist $\left(\frac{a}{p}\right) \in \{\pm 1\}$. Mit dem Satz von Euler erhalten wir daher

$$w^2 \equiv \left(a^{\frac{p-1}{4}}\right)^2 \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p,$$

was die Behauptung beweist. ■

Bemerkung: Für die Hälfte der Zahlen $a \in \{1, \ldots, p-1\}$ gilt $\left(\frac{a}{p}\right) = -1$. Durch zufällige Wahl von a sollte man daher schnell ein a mit $\left(\frac{a}{p}\right) = -1$ finden, und dann mit Hilfe des Lemmas eine Quadratwurzel von -1 modulo p. Der folgende Algorithmus führt dies aus.

Algorithmus zur Bestimmung einer Quadratwurzel aus -1 modulo p für eine Primzahl $p \equiv 1 \bmod 4$

Eingabe: Primzahl $p \equiv 1 \bmod 4$
Ausgabe: $w \in \{1, \ldots, p-1\}$ mit $w^2 \equiv -1 \bmod p$

1: $a \leftarrow 2$
2: **while** $a^{\frac{p-1}{2}} \bmod p = 1$ **do**
3: $\quad a \leftarrow a + 1$
4: **end while**
5: $w \leftarrow a^{\frac{p-1}{4}}$
6: Return w

Eine zugehörige Python-Funktion könnte so aussehen:

```
def wurzel_minus1_modp(p):
  a=2
  while pow(a,(p-1)//2,p)==1:
    a=a+2
  return pow(a,(p-1)//4,p)
```

Eine Anwendung des letzten Satzes gibt folgender Satz:

SATZ (Zwei-Quadrate-Satz von Fermat). *Für Primzahlen p gilt folgende Äquivalenz:*

$$\textit{Es gibt } x, y \in \mathbb{Z} \textit{ mit } p = x^2 + y^2 \quad \Longleftrightarrow \quad p = 2 \textit{ oder } p \equiv 1 \bmod 4.$$

(Eine Primzahl p ist genau dann Summe zweier Quadrate, wenn $p = 2$ oder $p \equiv 1 \bmod 4$ gilt.)

Beispiele: Hier sind Darstellungen $p = x^2 + y^2$ für alle Primzahlen $p \equiv 1 \bmod 4$ mit $p < 100$:

$$\begin{aligned} 5 &= 1^2 + 2^2 \\ 13 &= 2^2 + 3^2 \\ 17 &= 1^2 + 4^2 \\ 29 &= 2^2 + 5^2 \\ 37 &= 1^2 + 6^2 \\ 41 &= 4^2 + 5^2 \\ 53 &= 2^2 + 7^2 \\ 61 &= 5^2 + 6^2 \\ 73 &= 3^2 + 8^2 \\ 89 &= 5^2 + 8^2 \\ 97 &= 4^2 + 9^2 \end{aligned}$$

Beweis des Satzes: Da der Fall $p = 2$ klar ist ($2 = 1^2 + 1^2$), können wir $p \geq 3$ voraussetzen.

- $\Longrightarrow$ Sei $p = x^2 + y^2$. Wäre $\mathrm{ggT}(y, p) > 1$, so würde $p \mid y$ und dann auch $p \mid x$, also $p^2 \mid x^2 + y^2 = p$ folgen, was natürlich nicht sein kann. Also ist $\mathrm{ggT}(p, y) = 1$, und damit ist y invertierbar modulo p. Wir können dann modulo p so rechnen:

  $$(\frac{x}{y})^2 \equiv \frac{x^2}{y^2} \equiv \frac{p - y^2}{y^2} \equiv \frac{-y^2}{y^2} \equiv -1 \bmod p.$$

  Daher ist -1 ein Quadrat modulo p, also $\left(\frac{-1}{p}\right) = 1$. Der vorangegangene Satz liefert dann $p \equiv 1 \bmod 4$.
- $\Longleftarrow$ Sei $p \equiv 1 \bmod 4$.
  - **1. Schritt:** Wir bestimmen $x, y \in \mathbb{Z}$ und ein $m \in \mathbb{N}$ mit

    $$x^2 + y^2 = mp \quad \text{und} \quad 1 \leq m < p.$$

    Aus $p \equiv 1 \bmod 4$ folgt $\left(\frac{-1}{p}\right) = 1$. Also gibt es ein $w \in \{1, \ldots, p-1\}$ mit $w^2 \equiv -1 \bmod p$. Für $x = w$ und $y = 1$ gilt dann

    $$x^2 + y^2 \equiv w^2 + 1^2 \equiv -1 + 1 \equiv 0 \bmod p$$

    und

    $$1 \leq m = \frac{x^2 + y^2}{p} \leq \frac{(p-1)^2 + 1}{p} = \frac{p^2 - 2p + 2}{p} < \frac{p^2}{p} = p.$$

  - **2. Schritt:** Ist $m = 1$, so sind wir fertig.
  - **3. Schritt:** Ist $m > 1$ (und damit $1 < m < p$), so finden wir mit dem nachfolgenden Lemma Zahlen $n, \widetilde{x}, \widetilde{y} \in \mathbb{Z}$ mit

    $$\widetilde{x}^2 + \widetilde{y}^2 = np \quad \text{und} \quad 1 \leq n < m.$$

    Wir ersetzen jetzt x, y, m durch $\widetilde{x}, \widetilde{y}, n$ und gehen zurück zum 2. Schritt.

  Es ist klar, dass man bei diesem Reduktionsprozess nach endlich vielen Schritten auf den Fall $m = 1$ und damit auf $x^2 + y^2 = p$ stößt. ■

LEMMA. *Sei p eine Primzahl, seien $x, y \in \mathbb{Z}$, sodass ein $m \in \mathbb{N}$ mit*

$$x^2 + y^2 = mp \quad \textit{und} \quad 1 < m < p$$

existiert. Man wählt $u, v \in \mathbb{Z}$ mit

$$u \equiv x \bmod m, \quad v \equiv y \bmod m, \quad |u| \leq \frac{m}{2}, \quad |v| \leq \frac{m}{2}.$$

(Ist zunächst $0 \leq u \leq m - 1$ und $u > \frac{m}{2}$, so ersetzt man u durch $u - m$. Dann gilt $|u| < \frac{m}{2}$. Analog geht man bei v vor.) Nun definiert man

$$n = \frac{u^2 + v^2}{m}, \quad \widetilde{x} = \frac{ux + vy}{m}, \quad \widetilde{y} = \frac{uy - vx}{m}.$$

Dann gilt

$$n \in \mathbb{N}, \quad \widetilde{x}, \widetilde{y} \in \mathbb{Z}, \quad \widetilde{x}^2 + \widetilde{y}^2 = np, \quad n \leq \frac{m}{2}.$$

Beweis:

- Modulo m gilt:

$$\begin{aligned} u^2 + v^2 &\equiv x^2 + y^2 \equiv 0 \bmod m, \\ ux + vy &\equiv x^2 + y^2 \equiv 0 \bmod m, \\ uy - vx &\equiv xy - yx \equiv 0 \bmod m. \end{aligned}$$

  Daher gilt

$$n = \frac{u^2 + v^2}{m} \in \mathbb{N}_0, \quad \widetilde{x} = \frac{ux + vy}{m} \in \mathbb{Z} \quad \text{und} \quad \widetilde{y} = \frac{uy - vx}{m} \in \mathbb{Z}$$

  und

$$\begin{aligned} \widetilde{x}^2 + \widetilde{y}^2 &= \frac{(ux + vy)^2 + (uy - vx)^2}{m^2} = \frac{u^2x^2 + 2uvxy + v^2y^2 + u^2y^2 - 2uvxy + v^2x^2}{m^2} = \\ &= \frac{u^2x^2 + u^2y^2 + v^2x^2 + v^2y^2}{m^2} = \frac{(u^2 + v^2)(x^2 + y^2)}{m^2} = \frac{u^2 + v^2}{m} \cdot \frac{x^2 + y^2}{m} = \\ &= np. \end{aligned}$$

  Nun ist

$$0 \leq n = \frac{u^2 + v^2}{m} \leq \frac{\frac{m^2}{4} + \frac{m^2}{4}}{m} = \frac{m}{2}.$$

  Wir müssen noch zeigen, dass $n > 0$ gilt.
- Ist $n = 0$, so ist $u = v = 0$. Damit ist $x \equiv y \equiv 0 \bmod m$. Es gibt also $x_1, y_1 \in \mathbb{Z}$ mit $x = mx_1$ und $y = my_1$. Dann ist

$$mp = x^2 + y^2 = m^2x_1^2 + m^2y_1^2 = m^2(x_1^2 + y_1^2), \quad \text{also} \quad m(x_1^2 + y_1^2) = p$$

  und damit $m \mid p$. Dies widerspricht aber unserer Voraussetzung $1 < m < p$. Also kann der Fall $n = 0$ nicht eintreten. Wir haben alles gezeigt. ■

Bestimmung von $x, y \in \mathbb{Z}$ mit $p = x^2 + y^2$ für ein Primzahl $p \equiv 1 \bmod 4$

Eingabe: Primzahl $p \equiv 1 \bmod 4$
Ausgabe: $x, y \in \mathbb{Z}$ mit $p = x^2 + y^2$

1: Bestimme (mit dem zuvor beschriebenen Verfahren) $w \in \mathbb{Z}$ mit $w^2 \equiv -1 \bmod p$ und $1 \leq w \leq p - 1$
2: $x, y \leftarrow w, 1$
3: $m \leftarrow \frac{x^2+y^2}{p}$
4: **while** $m > 1$ **do**
5: $\quad u, v \leftarrow x \bmod m, y \bmod m$
6: $\quad$ **if** $2u > m$ **then**
7: $\quad\quad u \leftarrow u - m$
8: $\quad$ **end if**
9: $\quad$ **if** $2v > m$ **then**
10: $\quad\quad v \leftarrow v - m$
11: $\quad$ **end if**
12: $\quad x, y, m \leftarrow \frac{ux+vy}{m}, \frac{uy-vx}{m}, \frac{u^2+v^2}{m}$
13: **end while**
14: **return** x, y

Hier ist eine zugehörige Python-Funktion:

```
def zqs(p):
  x,y=wurzel_minus1_modp(p),1
  m=(x**2+y**2)//p
  while m>1:
    u,v=x%m,y%m
    if 2*u>m:
      u=u-m
    if 2*v>m:
      v=v-m
    x,y,m=(u*x+v*y)//m,(u*y-v*x)//m,(u**2+v**2)//m
  return x,y
```

Wir wollen jetzt sehen, wann 2 ein Quadrat modulo p ist.

Beispiele: Durch Ausprobieren finden wir: 2 ist kein Quadrat modulo 3, 5, 11, 13, aber

$$3^2 \equiv 2 \bmod 7, \quad 6^2 \equiv 2 \bmod 17, \quad 5^2 \equiv 2 \bmod 23, \ldots$$

Allgemeiner haben wir alle ungerade Primzahlen $p < 100$ angeschaut:

$$\left(\frac{2}{p}\right) = 1 \quad \text{für} \quad p = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97,$$
$$\left(\frac{2}{p}\right) = -1 \quad \text{für} \quad p = 3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83.$$

Gibt es eine Gesetzmäßigkeit?

SATZ. *Für eine ungerade Primzahl p gilt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{falls } p \equiv 1, 7 \bmod 8, \\ -1, & \text{falls } p \equiv 3, 5 \bmod 8. \end{cases}$$

Beweis: Zwar gibt es elementare Beweise, wir wollen aber einen algebraischen geben. Dazu müssen wir aber annehmen, dass es einen Körper K mit p^2 Elementen und $\mathbb{F}_p \subseteq K$ gibt.

(1) Zunächst gilt
$$\{x \in K : x^p = x\} = \mathbb{F}_p,$$
denn einerseits gilt $\supseteq$, andererseits hat das Polynom $X^p - X$ höchstens p Nullstellen in K, woraus schon alles folgt.

(2) Es gilt $p^2 \equiv 1 \bmod 8$ und damit $8 | \#K^*$. Aus der Algebra-Vorlesung weiß man, dass jede endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist. Also gibt es ein $a \in K^*$ mit $\operatorname{ord}(a) = 8$. Dann ist $\operatorname{ord}(a^2) = 4$, $\operatorname{ord}(a^4) = 2$. Das einzige Element der Ordnung 2 ist aber -1, also haben wir $a^4 = -1$.

(3) Für $b = a + \frac{1}{a}$ gilt:
$$b^2 = a^2 + 2 + \frac{1}{a^2} = a^2 + 2 + \frac{a^2}{a^4} = 2.$$
Bis auf $\pm$ ist b in K als Wurzel aus 2 eindeutig bestimmt. Daher gilt $\left(\frac{2}{p}\right) = 1 \iff b \in \mathbb{F}_p$.

(4) Da in K die Aussage $1 \cdot p = 0$ gilt, folgt $\binom{p}{i} \cdot 1 = 0$ in K für $1 \le i \le p-1$ und daher mit dem binomischen Lehrsatz $(x+y)^p = x^p + y^p$ für $x, y \in K$. Also erhält man $b^p = a^p + \frac{1}{a^p}$. Wegen $a^8 = 1$ folgt aus $m \equiv n \bmod 8$ sofort $a^m = a^n$. Wir unterscheiden jetzt 4 Fälle:

$$\begin{aligned}
p \equiv 1 \bmod 8 \quad &\Rightarrow \quad b^p = a + \frac{1}{a} = b, \\
p \equiv 3 \bmod 8 \quad &\Rightarrow \quad b^p = a^3 + \frac{1}{a^3} = \frac{a^4}{a} + \frac{a}{a^4} = -b, \\
p \equiv 5 \bmod 8 \quad &\Rightarrow \quad b^p = a^5 + \frac{1}{a^5} = a^4 \cdot a + \frac{1}{a^4 \cdot a} = -b, \\
p \equiv 7 \bmod 8 \quad &\Rightarrow \quad b^p = a^7 + \frac{1}{a^7} = \frac{1}{a} + a = b.
\end{aligned}$$

Wir sehen also

$$\left(\frac{2}{p}\right) = 1 \quad \Longleftrightarrow \quad b \in \mathbb{F}_p \quad \Longleftrightarrow \quad b^p = b \quad \Longleftrightarrow \quad p \equiv 1, 7 \bmod 8,$$

was wir zeigen wollten. ■

Sind p und q verschiedene ungerade Primzahlen, so ist natürlich

$$\left(\frac{p}{q}\right) = \pm \left(\frac{q}{p}\right),$$

da das Legendre-Symbol hier nur die Werte ± 1 annehmen kann. Welches Vorzeichen gilt, gibt folgender Satz an, für den Gauß sechs verschiedene Beweise gegeben hat. (Wir werden den Satz nicht beweisen.)

Satz (Quadratisches Reziprozitätsgesetz). *Sind p und q verschiedene ungerade Primzahlen, so gilt*

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

d.h.

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4, \\ -\left(\frac{q}{p}\right), & \text{falls } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Beispiele: Wir berechnen Legendre-Symbole unter Verwendung des Reziprozitätsgesetzes und der Formeln für $\left(\frac{-1}{p}\right)$ und $\left(\frac{2}{p}\right)$:

$$\left(\frac{1009}{1033}\right) = \left(\frac{1033}{1009}\right) = \left(\frac{24}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right) = \left(\frac{1009}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Für $p = 10^{10} + 19$, $q = 10^{100} + 267$ gilt:

$$\begin{aligned} \left(\frac{p}{q}\right) &= -\left(\frac{1066246421}{p}\right) = -\left(\frac{53}{p}\right)\left(\frac{103}{p}\right)\left(\frac{195319}{p}\right) = -\left(\frac{p}{53}\right)\left(\frac{p}{103}\right)\left(\frac{p}{195319}\right) = \\ &= -\left(\frac{34}{53}\right)\left(\frac{85}{103}\right)\left(\frac{57857}{195319}\right) = -\left(\frac{2}{53}\right)\left(\frac{17}{53}\right)\left(\frac{5}{103}\right)\left(\frac{17}{103}\right)\left(\frac{47\cdot 1231}{195319}\right) = \\ &= \left(\frac{2}{17}\right)\left(\frac{3}{5}\right)\left(\frac{1}{17}\right)(-1)\left(\frac{34}{47}\right)(-1)\left(\frac{821}{1231}\right) = -\left(\frac{2}{47}\right)\left(\frac{17}{47}\right)\left(\frac{821}{1231}\right) = \\ &= -\left(\frac{13}{17}\right)\left(\frac{410}{821}\right) = -\left(\frac{-4}{17}\right)\left(\frac{2}{821}\right)\left(\frac{5}{821}\right)\left(\frac{41}{821}\right) = \left(\frac{1}{5}\right)\left(\frac{1}{41}\right) = 1. \end{aligned}$$

(Man sieht hier bereits einen Nachteil dieser Version des Reziprozitätsgesetzes: um es anzuwenden, muss man Primfaktorzerlegung durchführen.)

Eine theoretische Anwendung des Reziprozitätsgesetzes gibt folgender Satz:

Satz (Pepin). *Für $n \geq 1$ ist die Fermat-Zahl $F_n = 2^{2^n} + 1$ genau dann prim, wenn gilt*

$$3^{\frac{F_n-1}{2}} = 3^{2^{2^n-1}} \equiv -1 \bmod F_n.$$

Beweis:

- Gilt die Beziehung, so ist $3^{F_n-1} \equiv 1 \bmod F_n$. Daher ist

  $$\operatorname{ord}_{F_n}(3) \mid F_n - 1, \quad \text{aber} \quad \operatorname{ord}_{F_n}(3) \nmid \frac{F_n - 1}{2}.$$

  Dies bedeutet

  $$\operatorname{ord}_{F_n}(3) \mid 2^{2^n}, \quad \text{aber} \quad \operatorname{ord}_{F_n}(3) \nmid 2^{2^n-1}.$$

  Daher gilt

  $$\operatorname{ord}_{F_n}(3) = 2^{2^n} = F_n - 1.$$

  Alle Elemente aus $\{1, \ldots, F_n - 1\}$ sind also invertierbar modulo F_n, weswegen F_n eine Primzahl ist.

- Sei nun umgekehrt F_n eine Primzahl. Dann gilt

$$F_n \equiv 1 \bmod 4 \quad \text{und} \quad F_n = 4^{2^{n-1}} + 1 \equiv 2 \bmod 3$$

und damit (mit dem Satz von Euler)

$$3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \equiv \left(\frac{F_n}{3}\right) \equiv \left(\frac{2}{3}\right) \equiv -1 \bmod F_n,$$

was wir zeigen wollten. ■

Bemerkung: Bisher ist nur von folgenden Fermat-Zahlen bekannt, dass sie prim sind:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Es ist unklar, ob es weitere Fermat-Primzahlen gibt.

Bemerkung: Um einige der nachfolgenden Rechnungen kompakter schreiben zu können, führen wir für ungerade natürliche Zahlen n folgende Funktionen ein:

$$\varepsilon(n) = \frac{n-1}{2} \quad \text{und} \quad \omega(n) = \frac{n^2-1}{8},$$

sodass dann gilt

$$\varepsilon(n) \equiv \begin{cases} 0 \bmod 2 & \text{für } n \equiv 1 \bmod 4, \\ 1 \bmod 2 & \text{für } n \equiv 3 \bmod 4 \end{cases} \quad \text{und} \quad \omega(n) \equiv \begin{cases} 0 \bmod 2 & \text{für } n \equiv 1, 7 \bmod 8, \\ 1 \bmod 2 & \text{für } n \equiv 3, 5 \bmod 8. \end{cases}$$

Die Formeln des quadratischen Reziprozitätsgesetzes lassen sich dann auch in der Form

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\varepsilon(p)\varepsilon(q)}, \quad \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}, \quad \left(\frac{2}{p}\right) = (-1)^{\omega(p)}$$

schreiben.

LEMMA. *Für ungerade natürliche Zahlen a und b gilt*

$$\varepsilon(ab) \equiv \varepsilon(a) + \varepsilon(b) \bmod 2 \quad \textit{und} \quad \omega(ab) \equiv \omega(a) + \omega(b) \bmod 2$$

und damit

$$(-1)^{\varepsilon(ab)} = (-1)^{\varepsilon(a)} \cdot (-1)^{\varepsilon(b)} \quad \textit{und} \quad (-1)^{\omega(ab)} = (-1)^{\omega(a)} \cdot (-1)^{\omega(b)}.$$

Beweis: Mit $2 \mid a-1$, $2 \mid a^2-1$, $\frac{b-1}{2} \in \mathbb{Z}$ und $\frac{b^2-1}{8} \in \mathbb{Z}$ erhält man

$$\begin{aligned} \varepsilon(ab) &= \frac{ab-1}{2} = \frac{(a-1)(b-1)}{2} + \frac{a-1}{2} + \frac{b-1}{2} = (a-1)\cdot\frac{b-1}{2} + \varepsilon(a) + \varepsilon(b) \\ &\equiv \varepsilon(a) + \varepsilon(b) \bmod 2, \\ \omega(ab) &= \frac{a^2b^2-1}{8} = \frac{(a^2-1)(b^2-1)}{8} + \frac{a^2-1}{8} + \frac{b^2-1}{8} = (a^2-1)\frac{b^2-1}{8} + \omega(a) + \omega(b) \\ &\equiv \omega(a) + \omega(b) \bmod 2, \end{aligned}$$

was zu zeigen war. ■

3. Das Jacobi-Symbol

Wir verallgemeinern jetzt das Legendre-Symbol zum Jacobi-Symbol:

DEFINITION. *Für $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $b \equiv 1 \bmod 2$ mit der Faktorisierung $b = p_1 \dots p_r$, wo $p_1, \dots, p_r$ nicht notwendig verschiedene Primzahlen sind, wird das* **Jacobi-Symbol** $\left(\frac{a}{b}\right)$ *durch*

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$$

definiert, wo $\left(\frac{a}{p_i}\right)$ das Legendre-Symbol ist. (Das Jacobi-Symbol verallgemeinert also das Legendre-Symbol.) Ist $b = \prod_i p_i^{e_i}$ mit paarweise verschiedenen Primzahlen p_i und $e_i \in \mathbb{N}_0$, so kann man die Definition auch in der Form

$$\left(\frac{a}{b}\right) = \prod_{i} \left(\frac{a}{p_i}\right)^{e_i}$$

schreiben. Insbesondere ist dann

$$\left(\frac{a}{1}\right) = 1.$$

Achtung: Das Jacobi-Symbol $\left(\frac{a}{b}\right)$ wird über das Legendre-Symbol definiert, nicht über die Lösbarkeit einer Gleichung $x^2 \equiv a \bmod b$. (Beispielsweise ist $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = 1$, aber die Gleichung $x^2 \equiv 2 \bmod 9$ besitzt keine Lösung, da sie auch keine Lösung modulo 3 besitzt.)

Folgende Eigenschaften ergeben sich aus den entsprechenden Eigenschaften für des Legendre-Symbol:

SATZ. *Seien $a, a_1, a_2 \in \mathbb{Z}$ und $b, b_1, b_2 \in \mathbb{N}$ mit $b \equiv b_1 \equiv b_2 \equiv 1 \bmod 2$. Dann gilt für das Jacobi-Symbol:*

(1)
$$a_1 \equiv a_2 \bmod b \quad \Longrightarrow \quad \left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right),$$
insbesondere gilt also
$$\left(\frac{a}{b}\right) = \left(\frac{a \bmod b}{b}\right).$$

(2) *Das Jacobi-Symbol ist multiplikativ:*
$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right) \quad \text{und} \quad \left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).$$

(3)
$$\left(\frac{a}{b}\right) = 0 \quad \Longleftrightarrow \quad \operatorname{ggT}(a, b) > 1.$$

(4)
$$\left(\frac{0}{b}\right) = \begin{cases} 1 & \text{für } b = 1, \\ 0 & \text{für } b > 1. \end{cases}$$

(5) *Es gilt das quadratische Reziprozitätsgesetz für ungerade Zahlen $a, b \in \mathbb{N}$*
$$\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{falls } a \equiv 1 \bmod 4 \text{ oder } b \equiv 1 \bmod 4, \\ -\left(\frac{b}{a}\right) & \text{falls } a \equiv b \equiv -1 \bmod 4, \end{cases}$$
was auch in der Form
$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}} = \left(\frac{b}{a}\right)(-1)^{\varepsilon(a)\varepsilon(b)}$$
geschrieben werden kann.

(6) *Es gelten die Ergänzungssätze:*

$$\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{für } b \equiv 1 \bmod 4, \\ -1 & \text{für } b \equiv 3 \bmod 4, \end{cases} \qquad \left(\frac{2}{b}\right) = \begin{cases} 1 & \text{für } b \equiv 1, 7 \bmod 8, \\ -1 & \text{für } b \equiv 3, 5 \bmod 8. \end{cases}$$

Diese können auch in der Form

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} = (-1)^{\varepsilon(b)}, \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = (-1)^{\omega(b)}$$

geschrieben werden.

Beweis:

(0) Die Eigenschaften (1), (2), (3), (4) folgen schnell aus der Definition und den Eigenschaften des Legendre-Symbols.

(5) Sei $a = p_1 \dots p_r$ und $b = q_1 \dots q_s$. Da $\varepsilon(uv) \equiv \varepsilon(u) + \varepsilon(v) \bmod 2$ für ungerade natürliche Zahlen u, v gilt, folgt

$$\varepsilon(a)\varepsilon(b) = \varepsilon(\prod_i p_i)\varepsilon(\prod_j q_j) \equiv \left(\sum_i \varepsilon(p_i)\right)\left(\sum_j \varepsilon(q_j)\right) = \sum_{i,j} \varepsilon(p_i)\varepsilon(q_j) \bmod 2.$$

Das gewöhnliche Reziprozitätsgesetzt liefert nun $\left(\frac{p_i}{q_j}\right) = \left(\frac{q_j}{p_i}\right)(-1)^{\varepsilon(p_i)\varepsilon(q_j)}$, womit wir erhalten

$$\begin{aligned} \left(\frac{a}{b}\right) &= \left(\frac{\prod_i p_i}{\prod_j q_j}\right) = \prod_{i,j}\left(\frac{p_i}{q_j}\right) = \prod_{i,j}\left(\frac{q_j}{p_i}\right)(-1)^{\varepsilon(p_i)\varepsilon(q_j)} = \left(\frac{b}{a}\right)(-1)^{\sum_{i,j}\varepsilon(p_i)\varepsilon(q_j)} = \\ &= \left(\frac{b}{a}\right)(-1)^{\varepsilon(a)\varepsilon(b)}, \end{aligned}$$

was zu zeigen war.

(4) Für $b = p_1 \dots p_r$ gilt zunächst

$$\varepsilon(b) = \varepsilon(\prod_i p_i) \equiv \sum_i \varepsilon(p_i) \bmod 2 \quad \text{und} \quad \omega(b) = \omega(\prod_i p_i) \equiv \sum_i \omega(p_i) \bmod 2.$$

Benutzen wir jetzt $\left(\frac{-1}{p_i}\right) = (-1)^{\varepsilon(p_i)}$ und $\left(\frac{2}{p_i}\right) = (-1)^{\omega(p_i)}$, so folgt

$$\left(\frac{-1}{b}\right) = \prod_i \left(\frac{-1}{p_i}\right) = \prod_i (-1)^{\varepsilon(p_i)} = (-1)^{\sum_i \varepsilon(p_i)} = (-1)^{\varepsilon(b)}$$

und

$$\left(\frac{2}{b}\right) = \prod_i \left(\frac{2}{p_i}\right) = \prod_i (-1)^{\omega(p_i)} = (-1)^{\sum_i \omega(p_i)} = (-1)^{\omega(b)},$$

was zu zeigen war. ■

Achtung: Wir werden im nächsten Abschnitt sehen, dass sich die Euler-Formel

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$$

nicht auf das Jacobi-Symbol übertragen lässt.

Bemerkung: Die im letzten Satz angegebenen Eigenschaften des Jacobi-Symbols liefern Möglichkeiten für eine schnelle Berechnung. Wir werden eine Variante ausführen, wobei die grundlegenden Ideen zur Berechnung von $\left(\frac{a}{b}\right)$ (für $a \in \mathbb{Z}$, $b \in \mathbb{N}$ mit $b \equiv 1 \bmod 2$) die folgenden sind:

(1) Wir können a modulo b reduzieren, denn mit $a' = a \bmod b$ gilt

$$\left(\frac{a}{b}\right) = \left(\frac{a \bmod b}{b}\right) = \left(\frac{a'}{b}\right) \quad \text{und } 0 \le a' < b.$$

(2) Ist $a' = 0$, so sind wir wegen

$$\left(\frac{0}{b}\right) = \begin{cases} 1 & \text{für } b = 1, \\ 0 & \text{für } b > 1 \end{cases}$$

fertig. Daher beschränken wir uns im Folgenden auf den Fall $a' > 0$. Wir klammern die 2 so oft wie möglich aus, d.h. wir zerlegen

$$a' = 2^e \cdot \widetilde{a} \text{ mit } e \geq 0 \text{ und } \widetilde{a} \equiv 1 \bmod 2.$$

Insbesondere ist dann $\widetilde{a}$ eine ungerade natürliche Zahl (mit $1 \leq \widetilde{a} \leq a' < b$). Damit ergibt sich

$$\left(\frac{a'}{b}\right) = \left(\frac{2^e \cdot \widetilde{a}}{b}\right) = \left(\frac{2}{b}\right)^e \cdot \left(\frac{\widetilde{a}}{b}\right).$$

Nun gilt die Formel $\left(\frac{2}{b}\right) = (-1)^{\omega(b)}$, sodass wir erhalten

$$\left(\frac{a'}{b}\right) = (-1)^{e\omega(b)} \cdot \left(\frac{\widetilde{a}}{b}\right).$$

(3) $\widetilde{a}$ und b sind ungerade natürliche Zahlen, weswegen wir das quadratische Reziprozitätsgesetz anwenden können:

$$\left(\frac{\widetilde{a}}{b}\right) = (-1)^{\varepsilon(\widetilde{a})\varepsilon(b)} \left(\frac{b}{\widetilde{a}}\right).$$

Insgesamt erhalten wir daher:

$$\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right) = (-1)^{e\omega(b)} \left(\frac{\widetilde{a}}{b}\right) = (-1)^{e\omega(b)+\varepsilon(\widetilde{a})\varepsilon(b)} \left(\frac{b}{\widetilde{a}}\right) \text{ mit } \widetilde{a} \leq a' < b.$$

Wir haben also den „Nenner“ kleiner gemacht und können jetzt wieder mit (1) beginnen.

Wir illustrieren die obigen Überlegungen zunächst an Beispielen:

Beispiele: Wir wenden die in der Bemerkung skizzierten Ideen wiederholt an:

(1) Wir wollen $\left(\frac{24}{35}\right)$ berechnen.

$$\begin{aligned} \left(\frac{24}{35}\right) &= \left(\frac{2^3 \cdot 3}{35}\right) = \left(\frac{2}{35}\right)^3 \cdot \left(\frac{3}{35}\right) \overset{35\equiv 3 \bmod 8}{=} (-1)^3 \cdot \left(\frac{3}{35}\right) \overset{3\equiv 35\equiv 3 \bmod 4}{=} \\ &= (-1) \cdot (-\left(\frac{35}{3}\right)) \overset{35 \bmod 3 = 2}{=} \left(\frac{2}{3}\right) \overset{3\equiv 3 \bmod 8}{=} -1. \end{aligned}$$

(2) Wir wollen $\left(\frac{5407}{8627}\right)$ berechnen.

$$\begin{aligned} \left(\frac{5407}{8627}\right) &\overset{5407\equiv 8627\equiv 3 \bmod 4}{=} -\left(\frac{8627}{5407}\right) = -\left(\frac{8627 \bmod 5407}{5407}\right) = -\left(\frac{3220}{5407}\right) = \\ &= -\left(\frac{2^2 \cdot 805}{5407}\right) = -\left(\frac{2}{5407}\right)^2 \cdot \left(\frac{805}{5407}\right) \overset{805\equiv 1 \bmod 4}{=} \\ &= -\left(\frac{5407}{805}\right) = -\left(\frac{5407 \bmod 805}{805}\right) = -\left(\frac{577}{805}\right) \overset{805\equiv 1 \bmod 4}{=} \\ &= -\left(\frac{805}{577}\right) = -\left(\frac{805 \bmod 577}{577}\right) = -\left(\frac{228}{577}\right) = -\left(\frac{2^2 \cdot 57}{577}\right) = \\ &= -\left(\frac{2}{577}\right)^2 \cdot \left(\frac{57}{577}\right) \overset{57\equiv 1 \bmod 4}{=} -\left(\frac{577}{57}\right) = -\left(\frac{577 \bmod 57}{57}\right) = \\ &= -\left(\frac{7}{57}\right) \overset{57\equiv 1 \bmod 4}{=} -\left(\frac{57}{7}\right) = -\left(\frac{57 \bmod 7}{7}\right) = -\left(\frac{1}{7}\right) = -1. \end{aligned}$$

Der folgende Satz beschreibt eine systematische Vorgehensweise zur Berechnung des Jacobi-Symbols:

SATZ. *Sei $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ mit $b \equiv 1 \bmod 2$. Beginnend mit*

$$a_1 = a, \quad b_1 = b, \quad j_1 = 1$$

werden rekursiv Zahlen a_i, b_i, j_i definiert. Ist zu Beginn des i-ten Schritts bereits a_i, b_i, j_i definiert, so setzt man

$$a_i' = a_i \bmod b_i$$

und unterscheidet dann zwei Fälle:

- *Ist $a_i' = 0$, so beendet man die Konstruktion. Den aktuellen Index nennt man ℓ, sodass also $a_\ell' = 0$ gilt.*
- *Ist $a_i' > 0$, so zerlegt man*

  $$a_i' = 2^{e_i} \cdot \widetilde{a}_i \text{ mit } \widetilde{a}_i \equiv 1 \bmod 2$$

  und definiert

  $$j_{i+1} = (-1)^{e_i \omega(b_i)} \cdot (-1)^{\varepsilon(\widetilde{a}_i)\varepsilon(b_i)} \cdot j_i, \quad a_{i+1} = b_i, \quad b_{i+1} = \widetilde{a}_i.$$

Dann gilt für das Jacobi-Symbol

$$\left(\frac{a}{b}\right) = \begin{cases} j_\ell, \text{ falls } b_\ell = 1, \\ 0, \text{ falls } b_\ell > 1. \end{cases}$$

(Die Zahl ℓ mit $a_\ell' = 0$ nennen wir die Schrittzahl.)

Beweis:

(1) Wir betrachten den Fall $a_i' > 0$, d.h. $1 \le i \le \ell - 1$. Dann gilt mit den obigen Definitionen, der Formel für $\left(\frac{2}{b_i}\right)$ und dem quadratischen Reziprozitätsgesetz

$$\begin{aligned} \left(\frac{a_i}{b_i}\right) &= \left(\frac{a_i \bmod b_i}{b_i}\right) = \left(\frac{a_i'}{b_i}\right) = \left(\frac{2^{e_i} \cdot \widetilde{a}_i}{b_i}\right) = \left(\frac{2}{b_i}\right)^{e_i} \cdot \left(\frac{\widetilde{a}_i}{b_i}\right) = \\ &= \left((-1)^{\omega(b_i)}\right)^{e_i} \cdot (-1)^{\varepsilon(\widetilde{a}_i)\varepsilon(b_i)} \left(\frac{b_i}{\widetilde{a}_i}\right) = \frac{j_{i+1}}{j_i} \left(\frac{a_{i+1}}{b_{i+1}}\right), \end{aligned}$$

und damit

$$j_i \left(\frac{a_i}{b_i}\right) = j_{i+1} \left(\frac{a_{i+1}}{b_{i+1}}\right) \text{ für } 1 \le i \le \ell - 1.$$

(2) Mit der Formel aus (1) und $j_1 = 1$ folgt

$$\begin{aligned} \left(\frac{a}{b}\right) &= j_1 \left(\frac{a_1}{b_1}\right) = j_2 \left(\frac{a_2}{b_2}\right) = \cdots = j_{\ell-1} \left(\frac{a_{\ell-1}}{b_{\ell-1}}\right) = j_\ell \left(\frac{a_\ell}{b_\ell}\right) = \\ &= j_\ell \left(\frac{a_\ell \bmod b_\ell}{b_\ell}\right) = j_\ell \left(\frac{a_\ell'}{b_\ell}\right) = j_\ell \left(\frac{0}{b_\ell}\right) = \begin{cases} j_\ell & \text{im Fall } b_\ell = 1, \\ 0 & \text{im Fall } b_\ell > 1. \end{cases} \end{aligned}$$

Dies war zu zeigen. ■

Wir greifen nochmals die Beispiele von vorher auf:

Beispiele: Wir verwenden die Bezeichnungen des Satzes.

- Der i-te Schritt beginnt mit

  $$\left(\frac{a}{b}\right) = \left(\frac{a \bmod b}{b}\right) = \left(\frac{a'}{b}\right) \text{ mit } 0 \le a' < b,$$

  wobei $\left(\frac{a}{b}\right)$ im Fall $i \ge 2$ das letzte Symbol des vorangegangenen Schritts ist. (Gilt bereits $0 \le a < b$, schreiben wir dies nicht an, weil hier nichts zu tun ist.)
- Im Fall $a' > 0$ zerlegt man $a' = 2^e \cdot \widetilde{a}$ mit $\widetilde{a} \equiv 1 \bmod 2$. Dann ist

  $$\left(\frac{a'}{b}\right) = \left(\frac{2^e \cdot \widetilde{a}}{b}\right) = \left(\frac{2}{b}\right)^e \left(\frac{\widetilde{a}}{b}\right) = \begin{cases} \left(\frac{\widetilde{a}}{b}\right) & \text{im Fall } e \bmod 2 = 0 \text{ oder } b \bmod 8 \in \{1, 7\}, \\ -\left(\frac{\widetilde{a}}{b}\right) & \text{sonst .} \end{cases}$$

  Ist $e = 0$ schreiben wir dies nicht an, weil hier nichts passiert.

- Nun verwenden wir das Reziprozitätsgesetz

$$\left(\frac{\widetilde{a}}{b}\right) = \begin{cases} \left(\frac{b}{\widetilde{a}}\right) & \text{im Fall } \widetilde{a} \bmod 4 = 1 \text{ oder } b \bmod 4 = 1, \\ -\left(\frac{b}{\widetilde{a}}\right) & \text{im Fall } \widetilde{a} \bmod 4 = 3 \text{ und } b \bmod 4 = 3. \end{cases}.$$

  $\left(\frac{b}{\widetilde{a}}\right)$ ist das letzte Symbol des i-ten Schritts und damit das erste Symbol des $(i+1)$-ten Schritts.
- Im Fall $a' = 0$ benutzen wir

$$\left(\frac{0}{b}\right) = \begin{cases} 1, & \text{falls } b = 0, \\ 0, & \text{falls } b > 1 \end{cases}$$

  und sind dann fertig. Dies ist der letzte Schritt. (Man könnte eigentlich schon aufhören, wenn man auf $a' = 1$ stößt, weil ja dann $\left(\frac{1}{b}\right) = 1$ gilt. Da dies im Fall $\mathrm{ggT}(a,b) > 1$ aber nicht passiert, haben wir keine Abbruchbedingung im Fall $a' = 1$ eingeführt.)

$$\begin{aligned} \left(\frac{24}{35}\right) &\overset{\text{1. Schritt}}{=} \left(\frac{2^3 \cdot 3}{35}\right) = -\left(\frac{3}{35}\right) = \left(\frac{35}{3}\right) = \\ &\overset{\text{2. Schritt}}{=} \left(\frac{35 \bmod 3}{3}\right) = \left(\frac{2}{3}\right) = \left(\frac{2 \cdot 1}{3}\right) = -\left(\frac{1}{3}\right) = -\left(\frac{3}{1}\right) = \\ &\overset{\text{3. Schritt}}{=} -\left(\frac{3 \bmod 1}{1}\right) = -\left(\frac{0}{1}\right) = -1 \end{aligned}$$

$$\begin{aligned} \left(\frac{5407}{8627}\right) &\overset{\text{1. Schritt}}{=} -\left(\frac{8627}{5407}\right) = \\ &\overset{\text{2. Schritt}}{=} -\left(\frac{8627 \bmod 5407}{5407}\right) = -\left(\frac{3220}{5407}\right) = -\left(\frac{2^2 \cdot 805}{5407}\right) = -\left(\frac{805}{5407}\right) = -\left(\frac{5407}{805}\right) = \\ &\overset{\text{3. Schritt}}{=} -\left(\frac{5407 \bmod 805}{805}\right) = -\left(\frac{577}{805}\right) = -\left(\frac{805}{577}\right) = \\ &\overset{\text{4. Schritt}}{=} -\left(\frac{805 \bmod 577}{577}\right) = -\left(\frac{228}{577}\right) = -\left(\frac{2^2 \cdot 57}{577}\right) = -\left(\frac{57}{577}\right) = -\left(\frac{577}{57}\right) = \\ &\overset{\text{5. Schritt}}{=} -\left(\frac{577 \bmod 57}{57}\right) = -\left(\frac{7}{57}\right) = -\left(\frac{57}{7}\right) = \\ &\overset{\text{6. Schritt}}{=} -\left(\frac{57 \bmod 7}{7}\right) = -\left(\frac{1}{7}\right) = -\left(\frac{7}{1}\right) = \\ &\overset{\text{7. Schritt}}{=} -\left(\frac{7 \bmod 1}{1}\right) = -\left(\frac{0}{1}\right) = -1 \end{aligned}$$

Der Satz führt sofort zu folgendem Algorithmus:

Algorithmus zur Berechnung des Jacobi-Symbols:

Eingabe: $a \in \mathbb{Z}$, $b \in \mathbb{N}$ mit $b \equiv 1 \bmod 2$

Ausgabe: $\left(\frac{a}{b}\right)$

```
1:  j ← 1
2:  loop
3:      a ← a mod b
4:      if a = 0 then
5:          if b = 1 then
6:              return j
7:          else
8:              return 0
9:          end if
10:     end if
11:     e ← 0
12:     while a mod 2 = 0 do
13:         a ← ⌊a/2⌋, e ← e + 1
14:     end while
```

15: **if** $e \bmod 2 = 1$ und $b \bmod 8 \in \{3,5\}$ **then**
16: $j \leftarrow -j$
17: **end if**
18: **if** $a \bmod 4 = 3$ und $b \bmod 4 = 3$ **then**
19: $j \leftarrow -j$
20: **end if**
21: $a, b \leftarrow b, a$
22: **end loop**

Eine zugehörige Python-Funktion könnte so aussehen:

```
# Berechnung des Jacobi-Symbols. a ist eine ganze Zahl, b eine ungerade
# natuerliche Zahl.
def jac(a,b):
  j=1
  while True:
    a=a%b
    if a==0:
      if b>1:
        j=0
      return j
    e=0
    while a%2==0:
      a,e=a//2,e+1
    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
```

Das folgende Lemma dient zur Vorbereitung der Schrittzahlabschätzung:

LEMMA. *Mit den Notationen des vorangegangenen Satzes und* $q_i = \left\lfloor \frac{a_i}{b_i} \right\rfloor$ *(für* $1 \le i \le \ell$*) gelten folgende Aussagen:*

(1) $q_i \ge 1$ *für* $2 \le i \le \ell$.
(2) $b_1 \equiv b_2 \equiv \cdots \equiv b_\ell \equiv 1 \bmod 2$.
(3) $b = b_1 > b_2 > \cdots > b_{\ell-1} > b_\ell$ *(und damit* $b_\ell \ge 1$ *und* $b_{\ell-1} \ge 3$*).*
(4) *Für* $2 \le i \le \ell - 1$ *gilt:*
$$b_{i-1} = q_i b_i + 2^{e_i} b_{i+1}.$$

Beweis:

(1) Für $1 \le i \le \ell$ ist $a_i' = a_i \bmod b_i$ mit $0 \le a_i' < b_i$, also gilt mit $q_i = \left\lfloor \frac{a_i}{b_i} \right\rfloor$
$$a_i = q_i b_i + a_i'.$$
Für $1 \le i \le \ell - 1$ ist $a_i' = 2^{e_i} \widetilde{a}_i$ und
$$a_{i+1} = b_i, \quad b_{i+1} = \widetilde{a}_i.$$
Aus $1 \le \widetilde{a}_i < b_i$ folgt dann $b_{i+1} < a_{i+1}$, also $q_{i+1} \ge 1$. Daraus folgt die Behauptung.
(2) Dies ist klar wegen $b_1 = b \equiv 1 \bmod 2$ und $b_{i+1} = \widetilde{a}_i \equiv 1 \bmod 2$.
(3) Für $1 \le i \le \ell - 1$ ist $a_i' \ne 0$, sodass wir zerlegen können
$$a_i' = 2^{e_i} \cdot \widetilde{a}_i.$$
Dies impliziert insbesondere
$$1 \le \widetilde{a}_i \le a_i' < b_i.$$

Wegen $b_{i+1} = \widetilde{a}_i$ folgt dann

$$b_{i+1} < b_i \text{ für } 1 \leq i \leq \ell - 1,$$

sodass also gilt

$$b_\ell < b_{\ell-1} < \cdots < b_2 < b_1.$$

(4) Sei nun $2 \leq i \leq \ell - 1$. Wir haben wegen $a_i' = 2^{e_i}\widetilde{a}_i$ die Gleichung

$$a_i = q_i b_i + 2^{e_i}\widetilde{a}_i.$$

Nun ist $a_i = b_{i-1}$ und $\widetilde{a}_i = b_{i+1}$, sodass wir auch schreiben können

$$b_{i-1} = q_i b_i + 2^{e_i} b_{i+1}.$$

Dies war zu zeigen. ■

SATZ. *Sei $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ mit $b \equiv 1 \bmod 2$. Sind a_i, b_i, j_i für $1 \leq i \leq \ell$ die im vorangegangenen Satz definierten Zahlenfolgen, so gilt für die Schrittzahl ℓ (zur Berechnung des Jacobi-Symbols)*

$$\ell \leq 1 + \frac{\log b}{\log 2} \leq 1 + 3.322 \log_{10} b.$$

Beweis: Wir verwenden die Bezeichnungen und Aussagen des vorangegangenen Lemmas.

(1) Wir beweisen zunächst, dass

$$b_i \geq 2^{\ell - i} \text{ für } 1 \leq i \leq \ell$$

gilt:

- Es ist $b_\ell \geq 1 = 2^{\ell-\ell}$ und $b_{\ell-1} \geq 3 > 2 = 2^{\ell-(\ell-1)}$.
- Ist $2 \leq i \leq \ell - 1$ und die Aussage bereits für $i, i+1, i+2, \ldots, \ell$ gezeigt, so folgt mit der letzten Gleichung des Lemmas

$$\begin{aligned} b_{i-1} &= q_i b_i + 2^{e_i} b_{i+1} \geq q_i \cdot 2^{\ell-i} + 2^{e_i} \cdot 2^{\ell-(i+1)} = \\ &= 2^{\ell-(i-1)} \cdot \left(q_i \cdot \frac{1}{2} + 2^{e_i} \cdot \frac{1}{4} \right). \end{aligned}$$

  – *Fall $q_i = 1$:* Dann ist $b_{i-1} = b_i + 2^{e_i} b_{i+1}$. Da aber $b_{i-1} \equiv b_i \equiv b_{i+1} \equiv 1 \bmod 2$ gilt, folgt $e_i \geq 1$, und damit

$$q_i \cdot \frac{1}{2} + 2^{e_i} \cdot \frac{1}{4} \geq \frac{1}{2} + 2 \cdot \frac{1}{4} = 1.$$

  – *Fall $q_i \geq 2$:* Hier folgt direkt

$$q_i \cdot \frac{1}{2} + 2^{e_i} \cdot \frac{1}{4} > 1.$$

Insgesamt ergibt sich

$$b_{i-1} \geq 2^{\ell-(i-1)},$$

woraus dann die Behauptung durch Induktion folgt.

(2) Mit $b = b_1 \geq 2^{\ell-1}$ ergibt sich

$$\ell \leq 1 + \frac{\log b}{\log 2} \leq 1 + 3.322 \log_{10} b,$$

wie behauptet. ■

Beispiele:

(1) Für die 100-stelligen, wahrscheinlichen Primzahlen $p = 7^{118} + 160$ und $q = 10^{100} - 797$ wird das Jacobi-Symbol $\left(\frac{p}{q}\right) = 1$ in 124 Schritten berechnet.

(2) Für die folgenden 100-stelligen Zahlen a, b braucht der Algorithmus 303 Schritte zur Berechnung von $\left(\frac{a}{b}\right) = 1$:

a=95150347765515132057349145859332264584534161188573209629959092866063019658634997990333872141304697 41,
b=37145573298244638258433921651316369187598827328261684786589822600354303056414920154353392217998297 85.

Bemerkung: Wir betrachten nochmals das Verfahren zur Berechnung des Jacobi-Symbols. Mit den Bezeichungen des vorangegangenen Satzes hatten wir zu Beginn des i-ten Schritts die Zahlen a_i und b_i und damit

$$a_i' = a_i \bmod b_i$$

berechnet. Wir betrachten den Fall $a_i' > 0$.

- Wir haben dann zerlegt

$$a_i' = 2^{e_i} \cdot \widetilde{a}_i \text{ mit } \widetilde{a}_i \equiv 1 \bmod 2.$$

- Alternativ könnte man vor dem Ausklammern der 2-Potenzen zunächst testen, ob

$$a_i' \equiv 1 \bmod 2 \quad \text{und} \quad a_i' > \frac{b_i}{2}$$

gilt. Ist dies der Fall, so ist nämlich

$$\left(\frac{a_i'}{b_i}\right) = \left(\frac{-1}{b_i}\right)\left(\frac{-a_i'}{b_i}\right) = (-1)^{\varepsilon(b_i)}\left(\frac{b_i - a_i'}{b_i}\right)$$

und

$$0 < b_i - a_i' < \frac{b_i}{2} \text{ und } b_i - a_i' \equiv 0 \bmod 2.$$

Setzt man also $a_i'' = b_i - a_i'$, so gilt

$$\left(\frac{a_i'}{b_i}\right) = (-1)^{\varepsilon(b_i)}\left(\frac{a_i''}{b_i}\right) \text{ und } 0 < a_i'' < \frac{b_i}{2} \text{ und } a_i'' \equiv 0 \bmod 2.$$

Nun definiert man $\widetilde{a}_i$ durch

$$a_i'' = 2^{e_i} \cdot \widetilde{a}_i \text{ mit } \widetilde{a}_i \equiv 1 \bmod 2.$$

Durch Betrachten des Fall $a_i' \equiv 1 \bmod 2$ und $a_i' > \frac{b_i}{2}$ könnte so eventuell der Berechnungsprozess nochmals beschleunigt werden. Dazu haben wir dies Python-Funktion erstellt:

```
# Alternative Berechnung des Jacobi-Symbols
def jac2(a,b):
  j=1
  while True:
    a=a%b
    if a==0:
      if b>1:
        j=0
      return j
    if a%2==1 and 2*a>b: # Diese vier Zeilen wurden hinzugefuegt.
      a=b-a              #
      if b%4==3:         #
        j=-j             #
    e=0
    while a%2==0:
      a,e=a//2,e+1
    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
```

In Experimenten haben wir aber festgestellt, dass die Laufzeit bei `jac2(a,b)` annähernd doppelt so lang ist wie die bei `jac(a,b)`.

4. Der Solovay-Strassen-Primzahltest

Der Satz von Euler (für das Legendre-Symbol) besagt, dass für eine ungerade Primzahl p und eine ganze Zahl a die Kongruenz

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

gilt. Dabei können wir $\left(\frac{a}{p}\right)$ als Legendre-Symbol oder als Jacobi-Symbol deuten. Ist n eine ungerade natürliche Zahl, so können wir sowohl das Jacobi-Symbol $\left(\frac{a}{n}\right)$ als auch $a^{\frac{n-1}{2}} \bmod n$ berechnen und dann vergleichen. vergleichen.

Beispiel: Für $n = 15$ ist

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1, \quad \text{aber} \quad 2^{\frac{15-1}{2}} \equiv 2^7 \equiv 8 \bmod 15,$$

also

$$\left(\frac{2}{15}\right) \not\equiv 2^{\frac{15-1}{2}} \bmod 15,$$

sodass auf Grund des Satzes von Euler 15 keine Primzahl sein kann. Diese Idee wird zu einem Primzahltest ausgebaut werden.

Zusammengesetzte natürliche Zahlen n, die sich im Satz von Euler (für das Legendre-Symbol) wie Primzahlen verhalten, haben einen eigenen Namen:

Definition. *Eine zusammengesetzte ungerade natürliche Zahl n heißt* **Euler-Pseudoprimzahl zur Basis** *a, wenn gilt* $\mathrm{ggT}(n, a) = 1$ *und*

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

Die kleinste Euler-Pseudoprimzahl zur Basis 2 ist 561 (mit $2^{\frac{561-1}{2}} \equiv \left(\frac{2}{561}\right) \equiv 1 \bmod 561$).

Ob für eine ungerade natürliche Zahl n die Eigenschaft $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$ gilt, kann man schnell testen, da die Potenz $a^{\frac{n-1}{2}} \bmod n$ und das Jacobi-Symbol $\left(\frac{a}{n}\right)$ schnell berechnet werden können. Deswegen wurde auch hieraus ein Primzahltest gemacht. Er ist aber nicht nach Euler benannt, sondern nach den Erfindern Solovay und Strassen.

Solovay-Strassen-Primzahltest zur Basis a: Sei $n \geq 3$ eine ungerade natürliche Zahl und $a \in \mathbb{N}$ mit $\mathrm{ggT}(n, a) = 1$. Es wird getestet, ob

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

gilt.

- Gilt die Kongruenzgleichung, so sagt man, dass n den Solovay-Strassen-Test zur Basis a besteht. In diesem Fall ist n eine Primzahl oder eine Euler-Pseudoprimzahl zur Basis a.
- Gilt die Kongruenzgleichung nicht, so sagt man, dass n den Solovay-Strassen-Test zur Basis a nicht besteht. In diesem Fall ist n zusammengesetzt.

Interessant am Solovay-Strassen-Test ist, dass es hier das Phänomen der Carmichael-Zahlen wie beim Fermat-Test nicht gibt.

Wir betrachten jetzt zu n alle Zahlen a, sodass n den Solovay-Strassen-Test zur Basis a besteht, und nennen die zugehörige Menge $E(n)$:

SATZ. *Sei n eine ungerade natürliche Zahl und*

$$E(n) = \{(a \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^* : \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n\}.$$

Dann gilt:

(1) *$E(n)$ ist eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$.*
(2) *Ist $n = p$ prim, so gilt $E(n) = (\mathbb{Z}/n\mathbb{Z})^*$.*
(3) *Ist n zusammengesetzt, so ist $E(n) \subsetneq (\mathbb{Z}/n\mathbb{Z})^*$.*

Beweis:

(1) Natürlich ist $(1 \bmod n) \in E(n)$, außerdem ist klar, dass $E(n)$ abgeschlossen unter Multiplikation ist, was dann die Behauptung beweist.
(2) Dies besagt der Satz von Euler.
(3) Sei p ein Primteiler von n. Wir unterscheiden, ob p einfach oder mehrfach in n aufgeht.
   (a) Hier betrachten wir den Fall, dass p einfach in n aufgeht, d.h. wir haben $n = pm$ mit $m \geq 3$ und $p \nmid m$. Sei g_p eine Primitivwurzel modulo p. Wir wissen, dass dann $\left(\frac{g_p}{p}\right) = -1$ gilt. Wegen $\mathrm{ggT}(p, m) = 1$ finden wir mit dem chinesischen Restsatz ein $a \in \mathbb{Z}$ mit
   $$a \equiv \begin{cases} g_p \bmod p, \\ 1 \bmod m. \end{cases}$$
   Es folgt
   $$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{m}\right) = \left(\frac{g_p}{p}\right)\left(\frac{1}{m}\right) = -1.$$
   Modulo m ist
   $$a^{\frac{n-1}{2}} \equiv 1^{\frac{n-1}{2}} \equiv 1 \bmod m.$$
   Daher ist $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod m$ und damit auch $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n$. Somit ist $(a \bmod n) \notin E(n)$.
   (b) Sei jetzt $n = p^k m$ mit $k \geq 2$, $m \geq 1$ und $\mathrm{ggT}(p, m) = 1$. Wir betrachten $a = 1 + p^{k-1}m$. Natürlich ist $\mathrm{ggT}(a, n) = 1$. Weiter ist
   $$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)^k \left(\frac{a}{m}\right) = 1.$$
   Wegen $p^k \mid (p^{k-1})^2$ folgt aus
   $$a^{\frac{n-1}{2}} = (1 + p^{k-1}m)^{\frac{n-1}{2}} = 1 + \frac{n-1}{2} \cdot p^{k-1}m + \ldots$$
   sofort
   $$a^{\frac{n-1}{2}} \equiv 1 + \frac{n-1}{2} p^{k-1}m \not\equiv 1 \bmod p^k.$$
   Daher gilt auch in diesem Fall
   $$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n$$
   und somit $(a \bmod n) \notin E(n)$.

Dies beweist, dass $E(n) \subsetneq (\mathbb{Z}/n\mathbb{Z})^*$ gilt, wenn n zusammengesetzt ist. ■

Zum Vergleich erinnern wir nochmals an die Situation beim Fermat-Test. Wir betrachten alle Zahlen a (modulo n), sodass n den Fermat-Test zur Basis a besteht:

SATZ. *Sei n eine natürliche Zahl ≥ 2 und*

$$F(n) = \{(a \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^* : a^{n-1} \equiv 1 \bmod n\}.$$

Dann gilt:

(1) *$F(n)$ ist eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$.*
(2) *Ist $n = p$ prim, so gilt $F(n) = (\mathbb{Z}/n\mathbb{Z})^*$.*

(3) *Ist n zusammengesetzt, so gilt*

$$F(n) = (\mathbb{Z}/n\mathbb{Z})^* \quad \Longleftrightarrow \quad n \text{ ist Carmichael-Zahl.}$$

Im Sinn des letzten Satzes tritt das Phänomen der Carmichale-Zahlen beim Solovay-Strassen-Test nicht auf. Es gilt nämlich:

$$\begin{aligned} n \text{ prim} \quad &\Longleftrightarrow \quad E(n) = (\mathbb{Z}/n\mathbb{Z})^*, \\ n \text{ zusammengesetzt} \quad &\Longleftrightarrow \quad E(n) \subsetneq (\mathbb{Z}/n\mathbb{Z})^*. \end{aligned}$$

Nun kann man (grob) abschätzen, wie groß $E(n)$ höchstens sein kann im Fall, dass n zusammengesetzt ist. Das liegt daran, dass $E(n)$ eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ ist:

FOLGERUNG. *Ist n eine zusammengesetzte ungerade natürliche Zahl, so gilt*

$$|E(n)| \leq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^*| = \frac{1}{2}\varphi(n).$$

Beweis: Da $E(n)$ eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ ist, ist die Untergruppenordnung ein Teiler der Gruppenordnung, d.h. es gibt ein $d \in \mathbb{N}$ mit $|(\mathbb{Z}/n\mathbb{Z})^*| = d \cdot |E(n)|$. Da in unserem Fall $E(n) \neq (\mathbb{Z}/n\mathbb{Z})^*$ ist, folgt $d \geq 2$ und damit

$$\frac{|E(n)|}{|(\mathbb{Z}/n\mathbb{Z})^*|} = \frac{1}{d} \leq \frac{1}{2},$$

was wir zeigen wollten. ■

Auswirkung: Sei n eine zusammengesetzte natürliche Zahl. Es ist $\frac{\#E(n)}{\#(\mathbb{Z}/n\mathbb{Z})^*} \leq \frac{1}{2}$. Wir wählen zufällig und unabhängig Zahlen $a_1, \ldots, a_r$. Die Wahrscheinlichkeit, dass $a_i \in E(n)$ ist, ist also $\leq \frac{1}{2}$. Die Wahrscheinlichkeit, dass alle Zahlen $a_1, \ldots, a_r$ in $E(n)$ liegen, ist also $\leq (\frac{1}{2})^r$. Äquivalent ausgedrückt: Die Wahrscheinlichkeit, dass n die Solovay-Strassen-Tests zu den Basen $a_1, \ldots, a_r$ besteht, ist $\leq (\frac{1}{2})^r$. Für große r ist dies sehr unwahrscheinlich.
Interpretation: Je mehr Solovay-Strassen-Tests eine natürliche Zahl n besteht, desto unwahrscheinlicher ist es, dass die Zahl zusammengesetzt ist. Die Zahl ist also wahrscheinlich prim.

Diese Argumentation funktioniert beim Fermat-Test wegen der Existenz von Carmichael-Zahlen ($F(n) = (\mathbb{Z}/n\mathbb{Z})^*$) nicht.

Die folgende Tabelle enthält die Eulerschen Pseudoprimzahlen $\leq 10^5$ zu einigen Basen, also zusammengesetzte Zahlen n mit $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$ und $\mathrm{ggT}(n, a) = 1$:

a	Euler-Pseudoprimzahlen zur Basis a
2	561, 1105, 1729, 1905, 2047, 2465, 3277, 4033, 4681, 6601, 8321, 8481, 10585, 12801, 15841, 16705, 18705, 25761, 29341, 30121, 33153, 34945, 41041, 42799, 46657, 49141, 52633, 62745, 65281, 74665, 75361, 80581, 85489, 87249, 88357, 90751
3	121, 703, 1729, 1891, 2821, 3281, 7381, 8401, 8911, 10585, 12403, 15457, 15841, 16531, 18721, 19345, 23521, 24661, 28009, 29341, 31621, 41041, 44287, 46657, 47197, 49141, 50881, 52633, 55969, 63139, 63973, 74593, 75361, 79003, 82513, 87913, 88573, 93961, 97567
4	341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, 10261, 10585, 11305, 12801, 13741, 13747, 13981, 14491, 15709, 15841, 16705, 18705, 18721, 19951, 23001, 23377, 25761, 29341, 30121, 30889, 31417, 31609, 31621, 33153, 34945, 35333, 39865, 41041, 41665, 42799, 46657, 49141, 49981, 52633, 55245, 57421, 60701, 60787, 62745, 63973, 65077, 65281, 68101, 72885, 74665, 75361, 80581, 83333, 83665, 85489, 87249, 88357, 88561, 90751, 91001, 93961
5	781, 1541, 1729, 5461, 5611, 6601, 7449, 7813, 11041, 12801, 13021, 14981, 15751, 15841, 21361, 24211, 25351, 29539, 38081, 40501, 41041, 44801, 47641, 53971, 67921, 75361, 79381, 90241
6	217, 481, 1111, 1261, 1729, 2701, 3589, 3913, 5713, 6533, 10585, 11041, 11137, 14701, 15841, 17329, 18361, 20017, 21049, 29341, 34441, 39493, 41041, 43621, 46657, 46873, 49141, 49321, 49661, 52633, 54481, 58969, 74023, 74563, 75361, 76921, 83333, 83665, 87061, 88561, 92053, 94657, 94697, 97751, 97921
7	25, 325, 703, 2101, 2353, 2465, 3277, 4525, 11041, 13665, 14089, 19345, 20197, 29857, 29891, 38081, 39331, 46657, 49241, 58825, 64681, 76627, 78937, 79381, 87673, 88399, 88831, 89961, 92929

Wir haben gesehen, dass für zusammengesetzte Zahlen n die Gruppe $E(n)$ eine echte Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ ist. Der Index

$$[(\mathbb{Z}/n\mathbb{Z})^* : E(n)]$$

ist also ≥ 2. Die Tabelle behandelt alle zusammengesetzten natürlichen Zahlen < 100:

n	$\lvert(\mathbb{Z}/n\mathbb{Z})^*\rvert$	$\lvert E(n)\rvert$	$[(\mathbb{Z}/n\mathbb{Z})^* : \lvert E(n)\rvert]$
$9 = 3^2$	6	2	3
$15 = 3 \cdot 5$	8	2	4
$21 = 3 \cdot 7$	12	2	6
$25 = 5^2$	20	4	5
$27 = 3^3$	18	2	9
$33 = 3 \cdot 11$	20	2	10
$35 = 5 \cdot 7$	24	2	12
$39 = 3 \cdot 13$	24	2	12
$45 = 3^2 \cdot 5$	24	4	6
$49 = 7^2$	42	6	7
$51 = 3 \cdot 17$	32	2	16
$55 = 5 \cdot 11$	40	2	20
$57 = 3 \cdot 19$	36	2	18
$63 = 3^2 \cdot 7$	36	2	18
$65 = 5 \cdot 13$	48	8	6
$69 = 3 \cdot 23$	44	2	22
$75 = 3 \cdot 5^2$	40	2	20
$77 = 7 \cdot 11$	60	2	30
$81 = 3^4$	54	2	27
$85 = 5 \cdot 17$	64	8	8
$87 = 3 \cdot 29$	56	2	28
$91 = 7 \cdot 13$	72	18	4
$93 = 3 \cdot 31$	60	2	30
$95 = 5 \cdot 19$	72	2	36
$99 = 3^2 \cdot 11$	60	2	30

Wie klein kann der Index $[(\mathbb{Z}/n\mathbb{Z})^* : E(n)]$ sein? Hier sind alle Beispiele mit $[(\mathbb{Z}/n\mathbb{Z})^* : E(n)] < 5$ und $n \leq 100000$:

n	$\lvert(\mathbb{Z}/n\mathbb{Z})^*\rvert$	$\lvert E(n)\rvert$	$[(\mathbb{Z}/n\mathbb{Z})^* : \lvert E(n)\rvert]$
$9 = 3^2$	6	2	3
$15 = 3 \cdot 5$	8	2	4
$91 = 7 \cdot 13$	72	18	4
$561 = 3 \cdot 11 \cdot 17$	320	80	4
$703 = 19 \cdot 37$	648	162	4
$1105 = 5 \cdot 13 \cdot 17$	768	192	4
$1729 = 7 \cdot 13 \cdot 19$	1296	648	2
$1891 = 31 \cdot 61$	1800	450	4
$2465 = 5 \cdot 17 \cdot 29$	1792	896	2
$2701 = 37 \cdot 73$	2592	648	4
$2821 = 7 \cdot 13 \cdot 31$	2160	540	4
$6601 = 7 \cdot 23 \cdot 41$	5280	1320	4
$8911 = 7 \cdot 19 \cdot 67$	7128	1782	4
$10585 = 5 \cdot 29 \cdot 73$	8064	2016	4
$12403 = 79 \cdot 157$	12168	3042	4
$15841 = 7 \cdot 31 \cdot 73$	12960	6480	2
$18721 = 97 \cdot 193$	18432	4608	4
$29341 = 13 \cdot 37 \cdot 61$	25920	6480	4
$38503 = 139 \cdot 277$	38088	9522	4
$41041 = 7 \cdot 11 \cdot 13 \cdot 41$	28800	14400	2
$46657 = 13 \cdot 37 \cdot 97$	41472	20736	2
$49141 = 157 \cdot 313$	48672	12168	4
$52633 = 7 \cdot 73 \cdot 103$	44064	11016	4
$62745 = 3 \cdot 5 \cdot 47 \cdot 89$	32384	8096	4
$75361 = 11 \cdot 13 \cdot 17 \cdot 31$	57600	28800	2
$79003 = 199 \cdot 397$	78408	19602	4
$88831 = 211 \cdot 421$	88200	22050	4

Der Solovay-Strassen-Test zur Basis a scheint deutlich aufwändiger als der Fermat-Test zu sein, da neben $a^{\frac{n-1}{2}} \bmod n$ auch das Jacobi-Symbol $\left(\frac{a}{n}\right)$ berechnet werden muss. Nun ist aber

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{für } n \equiv 1,7 \bmod 8, \\ -1 & \text{für } n \equiv 3,5 \bmod 8, \end{cases}$$

sodass im Fall $a = 2$ die Berechnung des Jacobi-Symbols keinen großen Aufwand darstellt. Daher beschreiben wir nochmals den Solovay-Strassen-Test zur Basis 2 explizit:

Solovay-Strassen-Primzahltest zur Basis 2: Sei $n \geq 3$ eine ungerade natürliche Zahl. Gilt

$$2^{\frac{n-1}{2}} \equiv \begin{cases} 1 \bmod n & \text{im Fall } n \equiv 1,7 \bmod 8, \\ -1 \bmod n & \text{im Fall } n \equiv 3,5 \bmod 8, \end{cases}$$

so besteht n den Test, ist also eine Primzahl oder eine Euler-Pseudo-Primzahl zur Basis 2. Andernfall besteht n den Test nicht und ist daher zusammengesetzt.

Eine zugehörige Python3-Funktion könnte so aussehen:

```
def solovay_strassen_test_2(n):
  return (n%8 in [1,7] and pow(2,(n-1)//2,n)==1) or \
         (n%8 in [3,5] and pow(2,(n-1)//2,n)==n-1)
```

Beispiele: Hier sind alle ungeraden natürlichen Zahlen $\leq 10^5$, die den Fermat-Test zur Basis 2 bestehen, den Solovay-Strassen-Test zur Basis 2 aber nicht:

$$341, 645, 1387, 2701, 2821, 4369, 4371, 5461, 7957, 8911, 10261, 11305,$$
$$13741, 13747, 13981, 14491, 15709, 18721, 19951, 23001, 23377, 30889,$$
$$31417, 31609, 31621, 35333, 39865, 41665, 49981, 55245, 57421, 60701,$$
$$60787, 63973, 65077, 68101, 72885, 83333, 83665, 88561, 91001, 93961.$$

Abschwächung des Solovay-Strassen-Tests zur Basis 2: Im Solovay-Strassen-Test zur Basis 2 testet man für eine ungerade natürliche Zahl n, ob die Bedingung

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

erfüllt ist oder nicht.
Etwas abgeschwächt könnte man nur testen, ob

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

erfüllt ist oder nicht. Ist dies eine schwächere Bedingung, d.h. gibt es Zahlen mit

$$2^{\frac{n-1}{2}} \equiv \pm 1 \bmod n, \quad \text{aber} \quad 2^{\frac{n-1}{2}} \not\equiv \left(\frac{2}{n}\right) \bmod n?$$

Da man $\left(\frac{2}{n}\right)$ einfach durch $n \bmod 8$ ausdrücken kann, kann man die letzte Frage auch so stellen: Gibt es Zahlen n mit

- $n \equiv 1 \bmod 8$ und $2^{\frac{n-1}{2}} \equiv -1 \bmod n$?
- $n \equiv 3 \bmod 8$ und $2^{\frac{n-1}{2}} \equiv 1 \bmod n$?
- $n \equiv 5 \bmod 8$ und $2^{\frac{n-1}{2}} \equiv 1 \bmod n$?
- $n \equiv 7 \bmod 8$ und $2^{\frac{n-1}{2}} \equiv -1 \bmod n$?

Wir haben nun alle ungeraden natürlichen Zahlen $n \leq 10^6$ bestimmt, für die

$$2^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad \text{und} \quad 2^{\frac{n-1}{2}} \not\equiv \left(\frac{2}{n}\right) \bmod n$$

gilt:

n	$2^{\frac{n-1}{n}} \bmod n$	$\left(\frac{2}{n}\right)$	$n \bmod 8$
341	1	-1	5
5461	1	-1	5
10261	1	-1	5
15709	1	-1	5
31621	1	-1	5
49981	1	-1	5
65077	1	-1	5
83333	1	-1	5
137149	1	-1	5
176149	1	-1	5
194221	1	-1	5
215749	1	-1	5
219781	1	-1	5
276013	1	-1	5
282133	1	-1	5
534061	1	-1	5
587861	1	-1	5
611701	1	-1	5
653333	1	-1	5
657901	1	-1	5
665333	1	-1	5
688213	1	-1	5
710533	1	-1	5
722261	1	-1	5
738541	1	-1	5
742813	1	-1	5
769757	1	-1	5
950797	1	-1	5

Erstaunlicherweise kommt nur der Fall $n \equiv 5 \bmod 8$ vor. Warum?

- $n \equiv 1 \bmod 8$ und $2^{\frac{n-1}{2}} \equiv -1 \bmod n$: (Nicht möglich $\longrightarrow$ Satz)
- $n \equiv 3 \bmod 8$ und $2^{\frac{n-1}{2}} \equiv 1 \bmod n$: (Nicht möglich - Aufgabe 8)
- $n \equiv 5 \bmod 8$ und $2^{\frac{n-1}{2}} \equiv 1 \bmod n$: (Möglich)
- $n \equiv 7 \bmod 8$ und $2^{\frac{n-1}{2}} \equiv -1 \bmod n$: (Nicht möglich - Aufgabe 8)

SATZ. *Sei $n \in \mathbb{N}_{\geq 3}$ ungerade mit der Primfaktorzerlegung $n = \prod_{i=1}^{r} p_i^{e_i}$ und $\ell, u \in \mathbb{N}$ mit $n-1 = 2^\ell u$ mit $u \equiv 1 \bmod 2$. Es gebe ein $a_0 \in \mathbb{Z}$ mit*

$$a_0^{\frac{n-1}{2}} \equiv -1 \bmod n.$$

(1) *Für alle i gilt*

$$p_i \equiv 1 \bmod 2^\ell,$$

sodass Zahlen $\varepsilon_i \in \{0,1\}$ und $v_i \in \mathbb{N}_0$ existieren mit

$$p_i = 1 + \varepsilon_i \cdot 2^\ell + 2^{\ell+1} \cdot v_i.$$

(2) *Es ist*

$$\sum_{i=1}^{r} \varepsilon_i e_i \equiv 1 \bmod 2.$$

(3) *Für $a \in \mathbb{Z}$ gilt die Implikation*

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad \Longrightarrow \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n.$$

(Gilt also $a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$, so besteht n den Solovay-Strassen-Test zur Basis a.)

Beweis:

(1) Wählen wir $b_0 \in \mathbb{Z}$ mit $b_0 \equiv a_0^u \bmod n$, so folgt aus $\frac{n-1}{2} = 2^{\ell-1}u$ und $a_0^{\frac{n-1}{2}} \equiv -1 \bmod n$ sofort

$$b_0^{2^{\ell-1}} \equiv -1 \bmod n, \quad \text{also auch} \quad b_0^{2^{\ell-1}} \equiv -1 \bmod p_i$$

für alle i. Dann gilt aber

$$\operatorname{ord}_{p_i}(b_0) = 2^\ell.$$

Wegen $\operatorname{ord}_{p_i}(b_0) \mid p_i - 1$ ergibt sich $2^\ell \mid p_i - 1$, also

$$p_i \equiv 1 \bmod 2^\ell.$$

Betrachtet man die Binärentwicklung von p_i, so erhält man sofort die Darstellung

$$p_i = 1 + \varepsilon_i \cdot 2^\ell + 2^{\ell+1} \cdot v_i \text{ mit } \varepsilon_i \in \{0,1\} \text{ und } v_i \in \mathbb{N}_0.$$

(2) Für $\alpha, \beta \in \mathbb{Z}$ gilt

$$(1 + \alpha \cdot 2^\ell) \cdot (1 + \beta \cdot 2^\ell) \equiv 1 + (\alpha + \beta) \cdot 2^\ell \bmod 2^{\ell+1}.$$

Dies impliziert

$$n \equiv \prod_{i=1}^{r} (1 + \varepsilon_i \cdot 2^\ell)^{e_i} \equiv 1 + (\sum_{i=1}^{r} e_i \varepsilon_i) \cdot 2^\ell \bmod 2^{\ell+1}.$$

Da aber nach Wahl von ℓ natürlich

$$n \equiv 1 + 2^\ell \bmod 2^{\ell+1}$$

gilt, folgt

$$\sum_{i=1}^{r} e_i \varepsilon_i \equiv 1 \bmod 2,$$

wie behauptet.

(3) Sei nun $a \in \mathbb{Z}$ mit $a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$ und $b \in \mathbb{Z}$ mit $b \equiv a^u \bmod n$. Dann ist wegen $\frac{n-1}{2} = 2^{\ell-1}u$

$$a^{\frac{n-1}{2}} \equiv b^{2^{\ell-1}} \equiv \pm 1 \bmod n.$$

Wir unterscheiden zwei Fälle:

(a) Falls $a^{\frac{n-1}{2}} \equiv b^{2^{\ell-1}} \equiv -1 \bmod n$, folgt wegen $b \equiv a^u \bmod p_i$

$$\left(\frac{a}{p_i}\right) \equiv \left(\frac{b}{p_i}\right) \equiv b^{\frac{p_i-1}{2}} \equiv b^{\varepsilon_i 2^{\ell-1} + 2^\ell \cdot v_i} \equiv (b^{2^{\ell-1}})^{\varepsilon_i + 2v_i} \equiv (-1)^{\varepsilon_i + 2v_i} \equiv (-1)^{\varepsilon_i} \bmod p_i,$$

und damit

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i} = \prod_{i=1}^{r} (-1)^{\varepsilon_i e_i} = (-1)^{\sum_{i=1}^{r} e_i \varepsilon_i} = -1.$$

(b) Falls $a^{\frac{n-1}{2}} \equiv b^{2^{\ell-1}} \equiv 1 \bmod n$ folgt

$$\left(\frac{a}{p_i}\right) \equiv \left(\frac{b}{p_i}\right) \equiv b^{\frac{p_i-1}{2}} \equiv b^{\varepsilon_i \cdot 2^{\ell-1} + 2^\ell \cdot v_i} \equiv (b^{2^{\ell-1}})^{\varepsilon_i + 2v_i} \equiv 1 \bmod p_i,$$

und damit

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i} = 1.$$

Damit ist alles bewiesen. ■

FOLGERUNG. *Ist $n \in \mathbb{N}_{\geq 3}$ ungerade mit $2^{\frac{n-1}{2}} \equiv -1 \bmod n$, so gilt $\left(\frac{2}{n}\right) = -1$ und damit $n \equiv 3 \bmod 8$ oder $n \equiv 5 \bmod 8$.*

Erinnerung: Der Miller-Rabin-Primzahltest

Der Fermatsche Primzahltest untersucht, ob $a^{n-1} \equiv 1 \bmod n$ gilt. Leider gibt es zusammengesetzte Zahlen n, so dass alle a mit $\mathrm{ggT}(a,n) = 1$ diese Bedingung erfüllen, nämlich die Carmichael-Zahlen. Wir werden den Fermattest jetzt etwas verfeinern.

LEMMA. *Ist p eine Primzahl, a eine Zahl mit $a^2 \equiv 1 \bmod p$ und $a \not\equiv 1 \bmod p$, so gilt $a \equiv -1 \bmod p$.*

Beweis: Es ist $0 \equiv a^2 - 1 = (a-1)(a+1) \bmod p$, d.h. $p|(a-1)(a+1)$. Nach Voraussetzung ist $a \not\equiv 1 \bmod p$, d.h. $p \not| a-1$ und damit $p|a+1$, d.h. $a \equiv -1 \bmod p$. ■

Beispiel: Für zusammengesetzte Zahlen n gilt die Aussage des Lemmas im allgemeinen nicht, so ist z.B. $3^2 \equiv 1 \bmod 8$, aber $3 \not\equiv \pm 1 \bmod 8$.

LEMMA. *Sei p eine ungerade Primzahl und $p-1 = 2^\ell q$ mit $q \equiv 1 \bmod 2$. Sei a eine Zahl mit* $\mathrm{ggT}(a,p) = 1$ *und $b \equiv a^q \bmod p$.*
Dann gilt für b:
Entweder ist $b \equiv 1 \bmod p$ oder es gibt ein i mit $0 \le i \le \ell - 1$ und $b^{2^i} \equiv -1 \bmod p$.

Beweis: Der kleine Satz von Fermat zeigt

$$1 \equiv a^{p-1} \equiv a^{q \cdot 2^\ell} \equiv b^{2^\ell} \bmod p.$$

Ist $b \equiv 1 \bmod p$, so sind wir fertig. Sei also $b \not\equiv 1 \bmod p$. Dann gibt einen Index i mit $0 \le i \le \ell - 1$, so dass

$$b^{2^{i+1}} \equiv 1 \bmod p, \quad \text{aber} \quad b^{2^i} \not\equiv 1 \bmod p.$$

Damit gilt $(b^{2^i})^2 \equiv 1 \bmod p$, nach unserem Lemma also $b^{2^i} \equiv -1 \bmod p$, was zu zeigen war. ■

Beispiel: Für $p = 1009$ ist $p - 1 = 2^4 \cdot 63$. Für $a = 2$ ist

$$2^{63} \equiv 192, \quad 192^2 \equiv 540, \quad 540^2 \equiv 1008 \equiv -1 \bmod p.$$

Was passiert nun mit der Aussage des Lemmas, wenn man keine Primzahl hat?

Beispiele:

- $341 = 11 \cdot 31$ war eine Fermat-Pseudoprimzahl zur Basis 2. Nun ist $341 - 1 = 2^2 \cdot 85$. Wählt man $a = 2$ und $b \equiv a^{85} \equiv 32 \bmod 341$, so ist $b^2 \equiv 1 \bmod 341$, also kann 341 nach dem Lemma keine Primzahl sein.
- $561 = 3 \cdot 11 \cdot 17$ ist die kleinste Carmichael-Zahl. Nun ist $561 - 1 = 2^4 \cdot 35$. Wir wählen $a = 2$, erhalten $b \equiv a^{35} \equiv 263 \bmod 561$. Nun quadrieren wir:

  $$b^2 \equiv 166, \quad b^4 \equiv 67, \quad b^8 \equiv 1 \bmod 561,$$

  also kann 561 keine Primzahl sein.

Die vorstehenden Überlegungen führen zu folgendem Test:

Miller-Rabin-Primzahltest zur Basis a: (Dabei ist $a \in \mathbb{N}_{\ge 2}$.) Sei n eine ungerade natürliche Zahl mit $n > a$. Wir zerlegen

$$n - 1 = 2^\ell q \text{ mit } q \equiv 1 \bmod 2 \quad \text{und berechnen} \quad b = a^q \bmod n.$$

Gilt

$$b = 1 \quad \text{oder} \quad b^{2^i} \equiv -1 \bmod n \text{ für ein } i \text{ mit } 0 \le i \le \ell - 1,$$

so sagen wir, *n besteht den Miller-Rabin-Test zur Basis a.* Andernfalls ist n zusammengesetzt. (Die Potenzen $b^{2^i} \bmod n$ berechnet man natürlich durch sukzessives Quadrieren: b, b^2, $b^4 = (b^2)^2$, $b^8 = (b^4)^2$, $b^{16} = (b^8)^2$, ...)
Hier ist eine algorithmische Variante:

Miller-Rabin-Primzahltest zur Basis a:
Eingabe: Eine ungerade natürliche Zahl n und eine natürliche Zahl a mit $2 \le a \le n - 1$
Ausgabe: (n besteht den Miller-Rabin-Test zur Basis a) oder (n ist zusammengesetzt)

Zerlege $n-1 = 2^\ell q$ mit einer ungeraden Zahl q
$b \leftarrow a^q \bmod n$
if $b = 1$ oder $b = n-1$ **then**
    return n besteht den Miller-Rabin-Test zur Basis a
end if
for $i = 1, \ldots, \ell - 1$ **do**
    $b \leftarrow b^2 \bmod n$ ▷ Dann ist $b = (a^q)^{2^i} \bmod n$
    if $b = n-1$ **then**
        return n besteht den Miller-Rabin-Test zur Basis a
    end if
end for
return n ist zusammengesetzt

Besteht nun eine Zahl n einen Miller-Rabin-Test, so hofft man, dass n prim ist. Leider gibt es auch hier, analog zu den Fermat-Pseudoprimzahlen beim Fermattest, zusammengesetzte Zahlen, die einen Miller-Rabin-Test bestehen:

DEFINITION. *Eine zusammengesetzte ungerade natürliche Zahl n heißt* **Miller-Rabin-Pseudoprimzahl zur Basis** *a oder eine* **starke Pseudoprimzahl zur Basis** *a, wenn n den Miller-Rabin-Test zur Basis a besteht, d.h. ist $n-1 = 2^\ell \cdot q$ mit $q \equiv 1 \bmod 2$, so gilt für $b \equiv a^q \bmod n$:*

$$b \equiv 1 \bmod n \quad \textit{oder} \quad b^{2^i} \equiv -1 \bmod n \textit{ für ein } i \textit{ mit } 0 \le i \le \ell - 1.$$

Beispiel: Wir betrachten $n = 2047 = 23 \cdot 89$. Es ist

$$n - 1 = 2 \cdot 1023, \quad \text{insbesondere } \ell = 1.$$

Wir berechnen für $a = 2$

$$b = (2^{1023} \bmod n) = 1.$$

Also besteht n den Miller-Rabin-Test zur Basis 2. Die Zahl 2047 ist also eine Miller-Rabin-Pseudoprimzahl zur Basis 2.
Nun betrachten wir noch $a = 3$. Wir berechnen

$$b = (3^{1023} \bmod n) = 1565.$$

Da wir nur $b^{2^i} \bmod n$ für $0 \le i \le \ell - 1 = 0$ anschauen müssen und $b \not\equiv \pm 1 \bmod n$ ist, besteht n den Miller-Rabin-Test zur Basis 3 nicht.
Beispiele: In der folgenden Liste sind alle starken Pseudoprimzahlen $\le 10^5$ zu den Basen $a = 2, 3, 5, 7$ aufgeführt.

2	2047, 3277, 4033, 4681, 8321, 15841, 29341, 42799, 49141, 52633, 65281, 74665, 80581, 85489, 88357, 90751
3	121, 703, 1891, 3281, 8401, 8911, 10585, 12403, 16531, 18721, 19345, 23521, 31621, 44287, 47197, 55969, 63139, 74593, 79003, 82513, 87913, 88573, 97567
5	781, 1541, 5461, 5611, 7813, 13021, 14981, 15751, 24211, 25351, 29539, 38081, 40501, 44801, 53971, 79381
7	25, 325, 703, 2101, 2353, 4525, 11041, 14089, 20197, 29857, 29891, 39331, 49241, 58825, 64681, 76627, 78937, 79381, 87673, 88399, 88831

Im folgenden sind die zusammengesetzten Zahlen $n \le 10^7$ angegeben, die den Miller-Rabin-Test sowohl zur Basis 2 als auch zur Basis 3 bestehen:

$$1373653, 1530787, 1987021, 2284453, 3116107, 5173601, 6787327.$$

Für die folgende Tabelle haben wir wieder Primzahlen und Pseudoprimzahlen gezählt, mit folgenden Bezeichnungen:

$$\begin{aligned} \pi(x) &= \#\{p \le x : p \text{ ist Primzahl}\}, \\ \pi_{\mathrm{F},a}(x) &= \#\{n \le x : n \text{ ist Fermat-Pseudoprimzahl zur Basis } a\}, \\ \pi_{\mathrm{MR},a}(x) &= \#\{n \le x : n \text{ ist Miller-Rabin-Pseudoprimzahl zur Basis } a\}. \end{aligned}$$

N	$\pi(N)$	$\pi_{\mathrm{F},2}(N)$	$\pi_{\mathrm{F},3}(N)$	$\pi_{\mathrm{F},5}(N)$	$\pi_{\mathrm{F},7}(N)$	$\pi_{\mathrm{MR},2}(N)$	$\pi_{\mathrm{MR},3}(N)$	$\pi_{\mathrm{MR},5}(N)$	$\pi_{\mathrm{MR},7}(N)$
10^2	25	0	1	1	2	0	0	0	1
10^3	168	3	6	5	6	0	2	1	3
10^4	1229	22	23	20	16	5	6	5	6
10^5	9592	78	78	73	73	16	23	16	21
10^6	78498	245	246	248	234	46	73	64	66
10^7	664579	750	760	745	659	162	207	199	177
10^8	5761455	2057	2155	1954	1797	488	582	475	446

(In der Tabelle fehlen die Euler-Pseudoprimzahlen.)
Der entscheidende Unterschied zwischen Fermattest und Miller-Rabin-Test besteht nun darin, dass es beim Miller-Rabin-Test kein Analogon zu den Carmichael-Zahlen gibt.
Für eine ungerade natürliche Zahl $n \geq 3$ betrachten wir alle a (modulo n), sodass n den Miller-Rabin-Test zur Basis a besteht. (Sei $n-1 = 2^\ell q$ mit $q \equiv 1 \bmod 2$.)

$$\mathrm{MR}(n) = \{(a \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^* : \quad a^q \equiv 1 \bmod n \text{ oder } a^{2^i q} \equiv -1 \bmod n \text{ für ein } i \text{ mit } 0 \leq i \leq \ell - 1\}.$$

Im Unterschied zu $F(n)$ und $E(n)$ muss $\mathrm{MR}(n)$ keine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ sein. Es gilt aber:

Satz. *Sei n eine ungerade natürliche Zahl ≥ 3 und $n \neq 9$. Dann gilt:*

$$\begin{aligned} n \text{ prim} \quad &\Longleftrightarrow \quad \mathrm{MR}(n) = (\mathbb{Z}/n\mathbb{Z})^*, \\ n \text{ zusammengesetzt} \quad &\Longrightarrow \quad \#\mathrm{MR}(n) \leq \frac{1}{4}\#(\mathbb{Z}/n\mathbb{Z})^*. \end{aligned}$$

Beispiele: Hier sind die zusammengesetzten ungeraden Zahlen n mit $3 \leq n \leq 100$ und $\mathrm{MR}(n)$:

n	$\mathrm{MR}(n)$
9	$\{1, 8\}$
15	$\{1, 14\}$
21	$\{1, 20\}$
25	$\{1, 7, 18, 24\}$
27	$\{1, 26\}$
33	$\{1, 32\}$
35	$\{1, 34\}$
39	$\{1, 38\}$
45	$\{1, 44\}$
49	$\{1, 18, 19, 30, 31, 48\}$
51	$\{1, 50\}$
55	$\{1, 54\}$
57	$\{1, 56\}$
63	$\{1, 62\}$
65	$\{1, 8, 18, 47, 57, 64\}$
69	$\{1, 68\}$
75	$\{1, 74\}$
77	$\{1, 76\}$
81	$\{1, 80\}$
85	$\{1, 13, 38, 47, 72, 84\}$
87	$\{1, 86\}$
91	$\{1, 9, 10, 12, 16, 17, 22, 29, 38, 53, 62, 69, 74, 75, 79, 81, 82, 90\}$
93	$\{1, 92\}$
95	$\{1, 94\}$
99	$\{1, 98\}$

(Immer gilt $\{1, n-1\} \subseteq \mathrm{MR}(n)$.)
Auswirkung: Sei n eine zusammengesetzte natürliche Zahl $\neq 9$.
Es ist $\frac{\#\mathrm{MR}(n)}{\#(\mathbb{Z}/n\mathbb{Z})^*} \leq \frac{1}{4}$. Wir wählen zufällig und unabhängig Zahlen $a_1, \ldots, a_r$ (aus $(\mathbb{Z}/n\mathbb{Z})^*$).
Die Wahrscheinlichkeit, dass $a_i \in \mathrm{MR}(n)$ ist, ist also $\leq \frac{1}{4}$. Die Wahrscheinlichkeit, dass alle Zahlen $a_1, \ldots, a_r$ in $\mathrm{MR}(n)$ liegen, ist also $\leq (\frac{1}{4})^r$. Äquivalent ausgedrückt: Die Wahrscheinlichkeit, dass n die Miller-Rabin-Tests zu den Basen $a_1, \ldots, a_r$ besteht, ist $\leq (\frac{1}{4})^r$. Für große r ist dies sehr unwahrscheinlich.
Interpretation: Je mehr Miller-Rabin-Tests eine natürliche Zahl n besteht, desto unwahrscheinlicher ist es, dass die Zahl zusammengesetzt ist. Die Zahl ist also wahrscheinlich prim.
Besteht z.B. eine natürliche Zahl 25 Miller-Rabin-Tests, so ist die Wahrscheinlichkeit, dass n nicht prim ist, $< 10^{-15}$. Für die Praxis genügen diese Anforderungen.

5. Vergleich von Primzahltests

Um wahrscheinliche Primzahlen zu finden haben wir inzwischen den Fermat-Test, den Miller-Rabin-Test und den Solovay-Strassen-Primzahltest kennengelernt. Mathematisch besteht ein einfacher Zusammenhang zwischen den Tests, den wir nun darstellen wollen.

Satz. *Besteht eine ungerade natürliche Zahl n den Solovay-Strassen-Test zur Basis a, so auch den Fermat-Test zur Basis a, d.h. gilt mit* $\mathrm{ggT}(n, a) = 1$

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

wobei $\left(\frac{a}{n}\right)$ *das Jacobi-Symbol bezeichnet, so gilt auch*

$$a^{n-1} \equiv 1 \bmod n.$$

Beweis: Wegen $\mathrm{ggT}(a,n) = 1$ gilt $\left(\frac{a}{n}\right) = \pm 1$, sodass aus

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

durch Quadrieren sofort

$$a^{n-1} \equiv 1 \bmod n$$

folgt. ■

Bemerkung: Der Solovay-Strassen-Test ist also besser als der Fermat-Test. Hier sind die Zahlen ≤ 10000, die den Fermat-Test zur Basis 2 bestehen, nicht jedoch den Solovay-Strassen-Test zur Basis 2:

$$341 = 11 \cdot 31, \quad 645 = 3 \cdot 5 \cdot 43, \quad 1387 = 19 \cdot 73, \quad 2701 = 37 \cdot 73, \quad 2821 = 7 \cdot 13 \cdot 31,$$
$$4369 = 17 \cdot 257, \quad 4371 = 3 \cdot 31 \cdot 47, \quad 5461 = 43 \cdot 127, \quad 7957 = 73 \cdot 109, \quad 8911 = 7 \cdot 19 \cdot 67.$$

Satz. *Besteht eine ungerade natürliche Zahl n den Miller-Rabin-Test zur Basis a, so auch den Solovay-Strassen-Test zur Basis a. Ausführlich formuliert mit $n-1 = 2^\ell q$, $q \equiv 1 \bmod 2$ und $b = a^q \bmod n$ lautet dies: Gilt*

$$a^q \equiv 1 \bmod n \quad \textit{oder} \quad a^{2^k q} \equiv -1 \bmod n \textit{ für ein } k \textit{ mit } 0 \leq k \leq \ell - 1,$$

so gilt

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

wobei $\left(\frac{a}{n}\right)$ *das Jacobi-Symbol bezeichnet.*

Beweis:

(1) Wir schreiben $b = a^q \bmod n$ und setzen dann voraus, dass gilt

$$b = 1 \quad \text{oder} \quad b^{2^k} \equiv -1 \bmod n \text{ für ein } k \text{ mit } 0 \leq k \leq \ell - 1.$$

Wir wollen zeigen, dass $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$ gilt. Da q ungerade ist, gilt für die Jacobi-Symbole $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(2) Im Fall $b = 1$ gilt

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) = 1 \quad \text{und} \quad a^{\frac{n-1}{2}} \equiv a^{2^{\ell-1}q} \equiv b^{2^{\ell-1}} \equiv 1,$$

was die Gleichheit $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$ beweist.

(3) Nun betrachten wir den Fall, dass ein k existiert mit

$$b^{2^k} \equiv -1 \bmod n \text{ mit } 0 \leq k \leq \ell - 1.$$

(a) Dann gilt auch

$$b^{2^k} \equiv -1 \bmod p_i,$$

was sofort

$$\mathrm{ord}_{p_i}(b) = 2^{k+1}$$

impliziert. Insbesondere zeigt dies dann $2^{k+1} \mid p_i - 1$. Modulo p_i gilt mit dem Satz von Euler

$$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right) \equiv b^{\frac{p_i-1}{2}} \equiv b^{2^k \cdot \frac{p_i-1}{2^{k+1}}} \equiv (-1)^{\frac{p_i-1}{2^{k+1}}} \bmod p_i,$$

was nun sofort

$$\left(\frac{a}{p_i}\right) = (-1)^{\frac{p_i-1}{2^{k+1}}}$$

liefert.

(b) Mit $n = \prod_i p_i^{e_i}$ folgt aus (a)

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i} = (-1)^{\sum_i e_i \frac{p_i-1}{2^{k+1}}}.$$

(c) Für $u, v \in \mathbb{Z}$

$$\frac{uv-1}{2^{k+1}} = \frac{u-1}{2^{k+1}} + \frac{v-1}{2^{k+1}} + \frac{u-1}{2^{k+1}}\frac{v-1}{2^{k+1}} \cdot 2^{k+1},$$

woraus sofort

$$u, v \equiv 1 \bmod 2^{k+1} \quad \Longrightarrow \quad uv \equiv 1 \bmod 2^{k+1} \text{ und } \frac{uv-1}{2^{k+1}} \equiv \frac{u-1}{2^{k+1}} + \frac{v-1}{2^{k+1}} \bmod 2$$

folgt. Wir wenden dies auf $n = \prod_i p_i^{e_i}$ an, wobei wir $p_i \equiv 1 \bmod 2^{k+1}$ voraussetzen dürfen, und erhalten $n \equiv 1 \bmod 2^{k+1}$ und

$$\frac{n-1}{2^{k+1}} \equiv \sum_i e_i \frac{p_i-1}{2^{k+1}} \bmod 2.$$

Aus (b) folgt dann sofort

$$\left(\frac{a}{n}\right) = (-1)^{\sum_i e_i \frac{p_i-1}{2^{k+1}}} = (-1)^{\frac{n-1}{2^{k+1}}} = (-1)^{\frac{2^\ell q}{2^{k+1}}} = (-1)^{2^{\ell-k-1}}.$$

(d) Andererseits gilt modulo n

$$a^{\frac{n-1}{2}} \equiv a^{2^{\ell-1}q} \equiv b^{2^{\ell-1}} \equiv b^{2^k \cdot 2^{\ell-k-1}} \equiv (-1)^{2^{\ell-k-1}} \bmod n,$$

was zusammen mit (d) schließlich

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

liefert. ■

Bemerkung: Der Miller-Rabin-Test ist besser als der Solovay-Strassen-Test. Folgende Zahlen bestehen den Solovay-Strassen-Test zur Basis 2, nicht aber den Miller-Rabin-Test zur Basis 2.

$$561 = 3 \cdot 11 \cdot 17, \quad 1105 = 5 \cdot 13 \cdot 17, \quad 1729 = 7 \cdot 13 \cdot 19, \quad 1905 = 3 \cdot 5 \cdot 127,$$
$$2465 = 5 \cdot 17 \cdot 29, \quad 6601 = 7 \cdot 23 \cdot 41, \quad 8481 = 3 \cdot 11 \cdot 257.$$

6. Quadrate modulo $N = pq$ und die Goldwasser-Micali-Verschlüsselung

Für Primzahlen p kann man mit Hilfe des Legendre-Symbols $\left(\frac{a}{p}\right)$ schnell feststellen, ob a ein Quadrat modulo p ist oder nicht. Was passiert, wenn man statt einer Primzahl eine zusammengesetzte Zahl nimmt? Der einfacheren Darstellung halber beschränken wir uns auf RSA-Zahlen $N = pq$.

Satz. *Sei $N = pq$ mit verschiedenen ungeraden Primzahlen p und q. Genau dann ist $a \in \mathbb{Z}$ mit* $\mathrm{ggT}(a, N) = 1$ *ein Quadrat modulo N, wenn $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$ ist. Mit anderen Worten:*

$$\{b^2 \in (\mathbb{Z}/N\mathbb{Z})^* : b \in (\mathbb{Z}/N\mathbb{Z})^*\} = \{a \in (\mathbb{Z}/N\mathbb{Z})^* : \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1\}.$$

Beweis: Ist a (mit $\mathrm{ggT}(a, N) = 1$) ein Quadrat modulo N, also $a \equiv b^2 \bmod N$, so folgt $a \equiv b^2 \bmod p$, $a \equiv b^2 \bmod q$, was zusammen mit $\mathrm{ggT}(a, p) = 1$, $\mathrm{ggT}(a, q) = 1$ sofort $\left(\frac{a}{p}\right) = 1$, $\left(\frac{a}{q}\right) = 1$ liefert. Es gelte umgekehrt für $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, N) = 1$ die Aussage $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$. Dann ist a Quadrat modulo p, also $a \equiv b_p^2 \bmod p$, a ein Quadrat modulo q, also $a \equiv b_q \bmod p$. Mit den chinesischen Restsatz findet man ein $b \in \mathbb{Z}$ mit $b \equiv b_p \bmod p$ und $b \equiv b_q \bmod q$. Es folgt $a \equiv b^2 \bmod p$ und $a \equiv b^2 \bmod q$, was sofort $a \equiv b^2 \bmod N$ und damit die Behauptung liefert. ■

SATZ. *Sei $N = pq$ eine RSA-Zahl und*

$$\begin{aligned} M_{1,1} &= \{a \in (\mathbb{Z}/N\mathbb{Z})^* : \left(\frac{a}{p}\right) = 1, \left(\frac{a}{q}\right) = 1\}, \\ M_{1,-1} &= \{a \in (\mathbb{Z}/N\mathbb{Z})^* : \left(\frac{a}{p}\right) = 1, \left(\frac{a}{q}\right) = -1\}, \\ M_{-1,1} &= \{a \in (\mathbb{Z}/N\mathbb{Z})^* : \left(\frac{a}{p}\right) = -1, \left(\frac{a}{q}\right) = 1\}, \\ M_{-1,-1} &= \{a \in (\mathbb{Z}/N\mathbb{Z})^* : \left(\frac{a}{p}\right) = -1, \left(\frac{a}{q}\right) = -1\}. \end{aligned}$$

Dann gilt:

(1) *Die Mengen sind alle gleichmächtig. $\#M_{i,j} = \frac{1}{4}(p-1)(q-1)$.*
(2) *$M_{1,1}$ ist die Menge der Quadrate in $(\mathbb{Z}/N\mathbb{Z})^*$, d.h.*
$$M_{1,1} = \{b^2 : b \in (\mathbb{Z}/N\mathbb{Z})^*\}.$$
(3) *$M_{1,1} \cup M_{-1,-1}$ sind die Zahlen mit Jacobi-Symbol 1:*
$$M_{1,1} \cup M_{-1,-1} = \{a \in (\mathbb{Z}/N\mathbb{Z})^* : \left(\frac{a}{N}\right) = 1\}.$$
(4)
$$\frac{\#\{b^2 : b \in (\mathbb{Z}/N\mathbb{Z})^*\}}{\#\{a \in (\mathbb{Z}/N\mathbb{Z})^* : \left(\frac{a}{N}\right) = 1\}} = \frac{1}{2},$$
d.h. (nur) die Hälfte der Zahlen mit Jacobi-Symbol 1 sind Quadrate.

Beweis:

(1) Man zeigt zunächst, dass die Abbildung
$$\alpha : (\mathbb{Z}/N\mathbb{Z})^* \to \{(\pm 1, \pm 1)\}, \quad a \mapsto (\left(\frac{a}{p}\right), \left(\frac{a}{q}\right))$$
ein surjektiver Gruppenhomomorphismus ist. Dann ist
$$M_{i,j} = \alpha^{-1}((i,j)),$$
woraus die Gleichmächtigkeit folgt.
(2) Diese Aussage steht im letzten Satz.
(3) Dies folgt aus $\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$.
(4) Dies folgt aus (2) und (3). ■

Aktueller Wissensstand: $N = pq$ sei eine RSA-Zahl. Ist $\left(\frac{a}{N}\right) = -1$, so weiß man, dass a kein Quadrat modulo N ist. Ist $\left(\frac{a}{N}\right) = 1$, so ist $(a \bmod N) \in M_{1,1} \cup M_{-1,-1}$. Man kennt keinen Weg zu sagen, ob a Quadrat ist oder nicht, wenn man die Faktorisierung von N nicht kennt.

Goldwasser-Micali-Verschlüsselung:

(1) **Schlüsselerzeugung:** Zur Erstellung eines Schlüssels geht eine Person A folgendermaßen vor:
   (a) A wählt sich (mit Hilfe eines Primzahltests) große, verschiedene, ungerade Primzahlen p und q und berechnet $N = pq$. (Die Zahlen sollten so gewählt sein, dass sich N mit den gängigen Faktorisierungsverfahren praktisch nicht faktorisieren lässt.)
   (b) A wählt eine Zahl k mit $\left(\frac{k}{p}\right) = \left(\frac{k}{q}\right) = -1$.
   (c) Der **öffentliche Schlüssel** von A ist (N, k), der **private Schlüssel** p (oder q).
(2) **Verschlüsselung:** Will eine Person B eine Nachricht verschlüsselt an A schicken, geht sie folgendermaßen vor:
   (a) B besorgt sich den öffentlichen Schlüssel (N, k) von A.
   (b) B wandelt seine Nachricht nach einem vereinbarten Verfahren in eine Bitfolge $a_1, a_2, a_3, \ldots$, d.h. $a_i \in \{0, 1\}$, um.
   (c) Für jedes a_i wählt B eine Zufallszahl z_i.

(d) B berechnet

$$b_i = \begin{cases} z_i^2 \bmod N, & \text{falls } a_i = 0, \\ kz_i^2 \bmod N, & \text{falls } a_i = 1. \end{cases}$$

(e) Der Chiffretext ist die Zahlenfolge $b_1, b_2, b_3, \ldots$ und wird von B an A geschickt.

(3) **Entschlüsselung:**

(a) A erhält die Zahlenfolge $b_1, b_2, b_3, \ldots$

(b) A berechnet die Legendre-Symbole $\left(\frac{b_i}{p}\right)$ und damit

$$a_i = \begin{cases} 0 & \text{für } \left(\frac{b_i}{p}\right) = 1, \\ 1 & \text{für } \left(\frac{b_i}{p}\right) = -1. \end{cases}$$

$a_1, a_2, a_3, \ldots$ liefert nach Umwandlung die von B gesandte Nachricht.

Bemerkungen:

(1) Etwas kompakter kann man die Verschlüsselungsformeln in der Form

$$b_i = k^{a_i} z_i^2 \bmod N$$

und die Entschlüsselungsformeln in der Form

$$a_i = \frac{1}{2}(1 - \left(\frac{b_i}{p}\right))$$

schreiben.

(2) Die Goldwasser-Micali-Verschlüsselung hat eine starke Nachrichtenexpansion. m zu verschlüsselnde Bits liefern verschlüsselt m Zahlen der Länge N.

(3) Gilt $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$, so kann man $k = -1$ wählen, weil in diesem Fall $\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right) = -1$ gilt. Gilt $p \bmod 8, q \bmod 8 \in \{3, 5\}$, so kann man analog $k = 2$ wählen.

Beispiel: Wir wählen Primzahlen $p = 38459$ und $q = 72959$, die beide $\equiv 3 \bmod 4$ sind, sodass wir $k = -1$ wählen können. Dann ist $N = pq = 2805930181$. Der öffentliche Goldwasser-Micali-Schlüssel ist also

$$(N, k) = (2805930181, -1).$$

Wir wollen die Bitfolge 1,0,0,1,0 verschlüsseln.

a_i	z_i	$z_i^2 \bmod N$	b_i	$\left(\frac{b_i}{N}\right)$	$\left(\frac{b_i}{p}\right)$	$\left(\frac{b_i}{q}\right)$
1	918281569	639174607	2166755574	1	-1	-1
0	1234652636	865149599	865149599	1	1	1
0	1309591615	2131482269	2131482269	1	1	1
1	53942974	2250571703	555358478	1	-1	-1
0	78612957	321025512	321025512	1	1	1

Der Chiffrefolge ist also

$$2166755574, 865149599, 2131482269, 555358478, 321025512.$$

7. Quadratwurzelziehen modulo p - Das Tonelli-Verfahren

Mit dem Legendre-Symbol $\left(\frac{a}{p}\right)$ kann man entscheiden, ob die Gleichung $x^2 \equiv a \bmod p$ lösbar ist oder nicht. Nun wollen wir die Gleichung lösen, wenn $\left(\frac{a}{p}\right) = 1$ ist. Ist x_1 eine Lösung, so auch $x_2 \equiv -x_1 \equiv p - x_1 \bmod p$.

Beispiel: Für $p = 41$ gilt $\left(\frac{2}{41}\right) = 1$, also ist die Gleichung $x^2 \equiv 2 \bmod 41$ lösbar. Wir brauchen für das folgende Verfahren noch ein Nichtquadrat modulo 41. Wegen $\left(\frac{3}{41}\right) = -1$ wählen wir 3. Der Satz von Euler impliziert

$$2^{20} \equiv 1 \bmod 41 \quad \text{und} \qquad 3^{20} \equiv -1 \bmod 41.$$

Wir formen die erste Gleichung um:

$$2^{20} \equiv 1 \bmod 41 \quad \Longrightarrow \quad \left(2^{10}\right)^2 \equiv 1 \bmod 41 \quad \Longrightarrow \quad 2^{10} \equiv \pm 1 \bmod 41.$$

Man berechnet

$$2^{10} \equiv -1 \bmod 41.$$

Da rechts -1 steht, multiplizieren wir mit $3^{20} \equiv -1 \bmod 41$ und machen weiter:

$$2^{10} \cdot 3^{20} \equiv 1 \bmod 41 \quad \Longrightarrow \quad \left(2^5 \cdot 3^{10}\right)^2 \equiv 1 \bmod 41 \quad \Longrightarrow \quad 2^5 \cdot 3^{10} \equiv \pm 1 \bmod 41.$$

Man berechnet

$$2^5 \cdot 3^{10} \equiv 1 \bmod 41.$$

Da im Exponenten von 2 eine ungerade Zahl steht, sind für fast fertig: Wir multiplizieren die Gleichung noch mit 2 und erhalten

$$2 \equiv 2^6 \cdot 3^{10} \equiv \left(2^3 \cdot 3^5\right)^2 \equiv 14^2 \bmod 41.$$

Also sind 17 und $24 = 41 - 17$ die Quadratwurzeln von 2 modulo 41.

Die Ideen des Beispiels werden im folgenden Lemma allgemein dargestellt:

LEMMA. *Sei p eine ungerade Primzahl, $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 1$ und $n \in \mathbb{Z}$ mit $\left(\frac{n}{p}\right) = -1$. Im Folgenden sind x, y Zahlen aus $\mathbb{N}_0$.*

(1) *Es gilt $a^{\frac{p-1}{2}} n^0 \equiv 1 \bmod p$ und $n^{\frac{p-1}{2}} \equiv -1 \bmod p$.*
(2) *Ist $a^x n^y \equiv 1 \bmod p$, so ist y gerade.*
(3) *Ist $a^x n^y \equiv 1 \bmod p$ und ist x gerade, so kann man schreiben $\left(a^{\frac{x}{2}} n^{\frac{y}{2}}\right)^2 \equiv 1 \bmod p$, also gilt $a^{\frac{x}{2}} n^{\frac{y}{2}} \equiv \pm 1 \bmod p$, und damit*

$$a^{\frac{x}{2}} n^{\frac{y}{2}} \equiv 1 \bmod p \quad \text{oder} \quad a^{\frac{x}{2}} n^{\frac{y}{2}+\frac{p-1}{2}} \equiv 1 \bmod p.$$

(y ist nach (2) eine gerade Zahl.)
(4) *Ist $a^x n^y \equiv 1 \bmod p$ und x ungerade (y ist nach (2) gerade), so gilt*

$$a \equiv \left(\pm a^{\frac{x+1}{2}} n^{\frac{y}{2}}\right)^2 \bmod p$$

Beweis:

(1) Die Satz von Euler und die Voraussetzung liefern $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \bmod p$ und $n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \equiv -1 \bmod p$, was die Behauptung zeigt.
(2) Wir setzen die Relation $a^x n^y \equiv 1 \bmod p$ in das Legendre-Symbol ein und erhalten

$$1 = \left(\frac{1}{p}\right) = \left(\frac{a^x n^y}{p}\right) = \left(\frac{a}{p}\right)^x \left(\frac{n}{p}\right)^y = (-1)^y,$$

was zeigt, dass y gerade ist.
(3) Da nach Voraussetzung und (2) x und y gerade Zahlen sind, können wir schreiben

$$\left(a^{\frac{x}{2}} n^{\frac{y}{2}}\right)^2 \equiv a^x n^y \equiv 1 \bmod p,$$

was sofort

$$a^{\frac{x}{2}} n^{\frac{y}{2}} \equiv \pm 1 \bmod p$$

zeigt.
(a) Ist $a^{\frac{x}{2}} n^{\frac{y}{2}} \equiv 1 \bmod p$, so ist nichts zu zeigen.

(b) Ist $a^{\frac{x}{2}} n^{\frac{y}{2}} \equiv -1 \bmod p$, so multiplizieren wir die Gleichung mit $n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \equiv -1 \bmod p$ und erhalten

$$a^{\frac{x}{2}} n^{\frac{y}{2}+\frac{p-1}{2}} \equiv 1 \bmod p,$$

was zu zeigen war.

(4) Sei nun x ungerade. Dann gilt

$$a \equiv a \cdot 1 \equiv a \cdot a^x n^y \equiv a^{x+1} n^y \equiv \left(\pm a^{\frac{x+1}{2}} n^{\frac{y}{2}}\right)^2 \bmod p,$$

was die Behauptung beweist. ■

Beispiele:

(1) Die Gleichung $x^2 \equiv 23 \bmod 101$ soll gelöst werden.
Als Nichtquadrat modulo 101 wird 2 gewählt. Sei $p = 101$.
Mit dem Satz von Euler erhält man mit $\frac{p-1}{2} = 50$ die Gleichungen

$$23^{50} \equiv 1 \bmod p, \quad \text{und} \quad 2^{50} \equiv -1 \bmod p.$$

Die erste Gleichung wird der Reihe nach abgewandelt, bis der Exponent bei 23 ungerade ist.

$$\left(23^{25} \cdot 2^0\right)^2 \equiv 1 \bmod p \quad \overset{\text{ausrechnen}}{\longrightarrow} \quad 23^{25} \cdot 2^0 \equiv -1 \bmod p \quad \longrightarrow \quad 23^{25} \cdot 2^{50} \equiv 1 \bmod p$$

Es folgt

$$23 \equiv 23^{26} \cdot 2^{50} \equiv \left(23^{13} \cdot 2^{25}\right)^2 \equiv 86^2 \bmod p.$$

Die Quadratwurzeln aus 23 modulo 101 sind

$$15 \quad \text{und} \quad 86.$$

(2) Die Gleichung $x^2 \equiv 29 \bmod 1009$ soll gelöst werden.
Als Nichtquadrat modulo 1009 wird 11 gewählt. Sei $p = 1009$.
Mit dem Satz von Euler erhält man mit $\frac{p-1}{2} = 504$ die Gleichungen

$$29^{504} \equiv 1 \bmod p, \quad \text{und} \quad 11^{504} \equiv -1 \bmod p.$$

Die erste Gleichung wird der Reihe nach abgewandelt, bis der Exponent bei 29 ungerade ist.

$$\begin{array}{lcll}
\left(29^{252} \cdot 11^0\right)^2 \equiv 1 \bmod p & \overset{\text{ausrechnen}}{\longrightarrow} & 29^{252} \cdot 11^0 \equiv -1 \bmod p & \longrightarrow \quad 29^{252} \cdot 11^{504} \equiv 1 \bmod p \\
\left(29^{126} \cdot 11^{252}\right)^2 \equiv 1 \bmod p & \overset{\text{ausrechnen}}{\longrightarrow} & 29^{126} \cdot 11^{252} \equiv -1 \bmod p & \longrightarrow \quad 29^{126} \cdot 11^{756} \equiv 1 \bmod p \\
\left(29^{63} \cdot 11^{378}\right)^2 \equiv 1 \bmod p & \overset{\text{ausrechnen}}{\longrightarrow} & 29^{63} \cdot 11^{378} \equiv -1 \bmod p & \longrightarrow \quad 29^{63} \cdot 11^{882} \equiv 1 \bmod p
\end{array}$$

Es folgt

$$29 \equiv 29^{64} \cdot 11^{882} \equiv \left(29^{32} \cdot 11^{441}\right)^2 \equiv 821^2 \bmod p.$$

Die Quadratwurzeln aus 29 modulo 1009 sind

$$188 \quad \text{und} \quad 821.$$

Wir formalisieren die Vorgehensweise:

LEMMA. *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 1$, außerdem $n \in \mathbb{Z}$ mit $\left(\frac{n}{p}\right) = -1$. Sei $p - 1 = 2^\ell u$ mit $u \equiv 1 \bmod 2$. Beginnend mit $x_1 = \frac{p-1}{2}$, $y_1 = 0$ werden rekursiv Zahlen x_i, y_i definiert durch*

- *Ist $x_i \equiv 1 \bmod 2$, so hört man auf.*
- *Ist $x_i \equiv 0 \bmod 2$, so definiert man*

$$x_{i+1} = \frac{x_i}{2}, \quad y_{i+1} = \begin{cases} \frac{y_i}{2}, & \text{falls } a^{\frac{x_i}{2}} n^{\frac{y_i}{2}} \equiv 1 \bmod p, \\ \frac{y_i}{2} + \frac{p-1}{2}, & \text{falls } a^{\frac{x_i}{2}} n^{\frac{y_i}{2}} \equiv -1 \bmod p. \end{cases}$$

Dann gilt:

(1) *Für* $1 \leq i \leq \ell$ *ist*

$$x_i = \frac{p-1}{2^i} = 2^{\ell-i}u,$$

insbesondere ist x_ℓ *ungerade und* ℓ *der Index, mit dem die Konstruktion endet.*

(2)

$$a^{\frac{x_\ell+1}{2}} n^{\frac{y_\ell}{2}} \bmod p$$

ist eine Quadratwurzel von a *modulo* p*.*

Beweis: Die Aussagen folgen sofort aus dem vorangegangenen Lemma. ■

Beispiele:

(1) $p = 101$ und $a = 23$. Wegen $n \equiv 5 \bmod 8$ können wir $n = 2$ wählen.

i	x_i	y_i	$a^{\frac{x_i}{2}} n^{\frac{y_i}{2}} \bmod p$
1	50	0	100
2	25	50	-

Daher ist

$$a^{\frac{25+1}{2}} n^{\frac{50}{2}} \equiv 23^{13} \cdot 2^{25} \equiv 49 \cdot 10 \equiv 86 \bmod 101.$$

(2) $p = 1009$ und $a = 29$. Durch Probieren finden wir $\left(\frac{11}{p}\right) = -1$, sodass wir $n = 11$ wählen.

i	x_i	y_i	$a^{\frac{x_i}{2}} n^{\frac{y_i}{2}} \bmod p$
1	504	0	1008
2	252	504	1008
3	126	756	1008
4	63	882	-

Daher ist

$$a^{\frac{63+1}{2}} n^{\frac{882}{2}} \equiv 29^{32} \cdot 11^{441} \equiv 821 \bmod p$$

eine Quadratwurzel von 29 modulo 1009.

Das vorangegangene Lemma führt unmittelbar zu folgendem Algorithmus:

Tonelli-Algorithmus zum Quadratwurzelziehen modulo p:

Eingabe: p sei eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 1$

Ausgabe: w mit $w^2 \equiv a \bmod p$

1: Suche ein $n \in \mathbb{F}_p$ mit $\left(\frac{n}{p}\right) = -1$. (Beispielsweise durch Ausprobieren: $n = 2, 3, \dots$)
2: $x \leftarrow \frac{p-1}{2}$, $y \leftarrow 0$
3: **while** $x \bmod 2 = 0$ **do**
4: $\quad x \leftarrow \frac{x}{2}$, $y \leftarrow \frac{y}{2}$
5: $\quad$ **if** $a^x n^y \not\equiv 1 \bmod p$ **then**
6: $\quad\quad y \leftarrow y + \frac{p-1}{2}$
7: $\quad$ **end if**
8: **end while**
9: $w \leftarrow a^{\frac{x+1}{2}} n^{\frac{y}{2}} \bmod p$
10: **return** w

Bemerkungen:

(1) Ist $p - 1 = 2^\ell u$ mit $u \equiv 1 \bmod 2$, so zeigen die Formeln des letzten Lemmas, dass die Schrittzahl in etwa ℓ ist, d.h. man man braucht $x_1, \dots, x_\ell$ und $y_1, \dots, y_\ell$.

(2) Praktisch einfach, theoretisch unklar ist, wie man schnell ein n mit $\left(\frac{n}{p}\right) = -1$ findet.

(a) Im Fall $p \equiv 3 \bmod 4$ gilt $\left(\frac{-1}{p}\right) = -1$, sodass man $n = -1$ als Nichtquadrat modulo p wählen kann.

(b) Im Fall $p \equiv 5 \bmod 8$ gilt $\left(\frac{2}{p}\right) = -1$, sodass man $n = 2$ als Nichtquadrat modulo p wählen kann.
(c) Im Fall $p \equiv 1 \bmod 8$ kann man durch Probieren ein n finden.
(So wurde es in nachfolgender Python-Funktion gemacht.)

Das Tonelli-Verfahren liefert für ein paar Spezialfälle auch schöne Formeln:

SATZ. *Sei p eine Primzahl mit $p \equiv 3, 5, 7 \bmod 8$ und $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 1$. Definiert man*

$$w = \begin{cases} a^{\frac{p+1}{4}} \bmod p & \text{im Fall } p \equiv 3 \bmod 4, \\ a^{\frac{p+3}{8}} \bmod p & \text{im Fall } p \equiv 5 \bmod 8 \text{ und } a^{\frac{p-1}{4}} \equiv 1 \bmod p, \\ 2^{\frac{p-1}{4}} \cdot a^{\frac{p+3}{8}} \bmod p & \text{im Fall } p \equiv 5 \bmod 8 \text{ und } a^{\frac{p-1}{4}} \equiv -1 \bmod p, \end{cases}$$

so sind $\pm w$ die Quadratwurzeln von a modulo p.

Beweis:

(1) Sei $p \equiv 3 \bmod 4$, also $p = 3 + 4k$. Dann ist $p - 1 = 2 + 4k = 2^1 \cdot (1 + 2k)$. Wir beginnen mit

$$x_1 = \frac{p-1}{2} = 1 + 2k, \quad y_1 = 0.$$

Da x_1 ungerade ist, sind wir fertig und erhalten als Quadratwurzel

$$a^{\frac{x_1+1}{2}} n^{y_1} \equiv a^{\frac{p+1}{4}} \bmod p.$$

(2) Sei $p \equiv 5 \bmod 8$, also $p = 5 + 8k$. Dann ist $p - 1 = 2^2 \cdot (1 + 2k)$. Wir beginnen mit

$$x_1 = \frac{p-1}{2} = 2(1 + 2k), \quad y_1 = 0.$$

Nun müssen wir

$$a^{\frac{x_1}{2}} n^{\frac{y_1}{2}} \equiv a^{\frac{p-1}{4}} \bmod p$$

betrachten.

- Ist $a^{\frac{p-1}{4}} \equiv 1 \bmod p$, so ist

$$x_2 = \frac{p-1}{4} = 1 + 2k, \quad y_2 = 0,$$

also x_2 ungerade und daher

$$a^{\frac{x_2+1}{2}} n^{\frac{y_2}{2}} \equiv a^{\frac{p+3}{8}} \bmod p$$

eine Quadratwurzel von a modulo p.

- Ist $a^{\frac{p-1}{4}} \equiv -1 \bmod p$, so ist

$$x_2 = \frac{p-1}{4} = 1 + 2k, \quad y_2 = \frac{p-1}{2}.$$

Da x_2 ungerade ist, erhalten wir als Quadratwurzel

$$a^{\frac{x_2+1}{2}} n^{\frac{y_2}{2}} \equiv a^{\frac{p+3}{8}} n^{\frac{p-1}{4}} \bmod p.$$

Da $p \equiv 5 \bmod 8$ ist, ist 2 ein Nichtquadrat modulo p, sodass wir $n = 2$ wählen können. Damit folgt die Behauptung. ■

Bemerkung: Eine mögliche Python3-Funktion zum Tonelli-Algorithmus könnte so aussehen:

```
def sqrtp_tonelli(a,p):
  if a%p==0:
    return 0
  if jac(a,p)==-1:
    return "a ist kein Quadrat modulo p"
  if p%4==3:
    n=-1
  elif p%8==5:
```

```
    n=2
  else:
    n=3
    while jac(n,p)!=-1:
      n+=1
  x,y=(p-1)//2,0
  while x%2==0:
    x,y=x//2,y//2
    if (pow(a,x,p)*pow(n,y,p))%p!=1:
      y+=(p-1)//2
  w=(pow(a,(x+1)//2,p)*pow(n,y//2,p))%p
  return w
```

Dabei wird $n = -1$ im Fall $p \equiv 3 \bmod 4$ und $n = 2$ im Fall $p \equiv 4 \bmod 8$ gewählt. Für den Rest ($p \equiv 1 \bmod 8$) wird ein Nichtquadrat modulo p durch Probieren bestimmt.

8. Zum Finden von Nichtquadraten modulo p

Für das Tonelli-Verfahren zum Quadratwurzelziehen modulo p braucht man ein Nichtquadrat modulo p. Wie findet man ein solches?

Wie findet man ein $n \in \mathbb{Z}$ mit $\left(\frac{n}{p}\right) = -1$?

- **Fall $p \equiv 3$ oder $7 \bmod 8$:** Hier ist $p \equiv 3 \bmod 4$. In diesem Fall kann man $n = -1$ wählen.
- **Fall $p \equiv 5 \bmod 8$:** Hier kann man $n = 2$ wählen.
- **Fall $p \equiv 1 \bmod 8$:** Hier probiert man aus.

Bemerkung: Ist $p \equiv 1 \bmod 8$, so gilt für $n \in \mathbb{N}$ wegen $\left(\frac{-1}{p}\right) = 1$ natürlich

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

Bei der Suche nach kleinen Nichtquadraten kann man sich also auf natürliche Zahlen beschränken. Ist $n \in \mathbb{N}$ mit $\left(\frac{n}{p}\right) = -1$ und n zusammengesetzt, d.h. $n = n_1 n_2$ mit $1 < n_1 < n$, $1 < n_2 < n$, so folgt aus $-1 = \left(\frac{n}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)$, dass $\left(\frac{n_1}{p}\right) = -1$ oder $\left(\frac{n_2}{p}\right) = -1$ gilt, d.h. n ist nicht das kleinste Nichtquadrat modulo p. Bei der Suche nach dem kleinsten Nichtquadrat modulo p kann man sich also auf Primzahlen n beschränken, wegen $\left(\frac{2}{p}\right) = 1$ sogar auf ungerade Primzahlen.
Für folgende $n \in \mathbb{N}$ haben wir die ersten 10 Primzahlen $p \equiv 1 \bmod 8$ - so weit möglich - bestimmt, sodass

n das kleinste Nichtquadrat modulo p ist. (Wir haben alle Primzahlen $\leq 10^8$ betrachtet.)

n	p, sodass n das kleinste Nichtquadrat modulo p ist
2	
3	17, 41, 89, 113, 137, 233, 257, 281, 353, 401
5	73, 97, 193, 313, 337, 433, 457, 577, 673, 937
7	241, 409, 601, 769, 1249, 1321, 1489, 1609, 2089, 2161
11	1009, 1129, 1201, 1801, 2521, 3049, 3361, 3889, 4201, 4561
13	2689, 3529, 5569, 7561, 7681, 9241, 9601, 9769, 12049, 12721
17	8089, 8761, 13729, 19009, 21121, 21961, 24049, 28081, 31249, 33289
19	33049, 37489, 44641, 49009, 49921, 51769, 53089, 55441, 59929, 63361
23	53881, 92569, 102001, 130729, 144169, 166609, 173209, 176401, 187009, 197521
29	87481, 185641, 336361, 394969, 504001, 526681, 538561, 552841, 600601, 629281
31	483289, 561961, 601969, 709921, 842521, 911089, 1005481, 1266841, 1517569, 1655809
37	515761, 878641, 979969, 1195489, 1433041, 1672609, 1730089, 1859881, 2144041, 2211889
41	1083289, 2043001, 4280329, 5390449, 5829121, 6104641, 6500209, 6868801, 7504561, 7623529
43	7921489, 8254801, 9033649, 11182609, 11236681, 11400481, 16754929, 16889161, 17139721, 17264641
47	3818929, 6589969, 8465209, 10939009, 16570129, 22684561, 24583441, 28034449, 31241401, 36813841
53	9257329, 15861169, 23888929, 25970569, 38391721, 57935329, 59315881, 64404649, 70023409, 72388801
59	22000801, 69626041, 80017081, ...
61	68204761, ...
67	48473881, 93586249, ...

Da man in den Fällen $p \equiv 3, 5, 7 \bmod 8$ sofort ein Nichtquadrat modulo p angeben kann, wäre es schön, wenn dies auch im Fall $p \equiv 1 \bmod 8$ so ähnlich wäre. Wir fragen: Kann es eine endliche Menge $\{n_1, \ldots, n_r\}$ von ganzen Zahlen geben, sodass es für jede Primzahl $p \equiv 1 \bmod 8$ ein n_i in der Menge gibt mit

$$\left(\frac{n_i}{p}\right) = -1.$$

Leider kann es eine solche endliche Menge nicht geben, wie die nachfolgenden Überlegungen zeigen.

LEMMA. *Sei $\{n_1, \ldots, n_r\} \subseteq \mathbb{Z} \setminus \{0\}$ eine endliche Menge ganzer Zahlen. Für $i = 1, \ldots, r$ zerlegen wir*

$$n_i = (-1)^{a_i} \cdot 2^{b_i} \cdot m_i \quad \textit{mit} \quad a_i \in \{0, 1\}, \quad b_i \in \mathbb{N}_0, \quad m_i \in \mathbb{N} \textit{ ungerade.}$$

Dann folgt: Ist p eine Primzahl mit

$$p \equiv 1 \bmod 8\, m_1 \ldots m_r,$$

so gilt

$$\left(\frac{n_1}{p}\right) = \cdots = \left(\frac{n_r}{p}\right) = 1.$$

Beweis: Aus der Annahme folgt

$$p \equiv 1 \bmod 4, \quad p \equiv 1 \bmod 8, \quad p \equiv 1 \bmod m_1, \quad [\ldots], \quad p \equiv 1 \bmod m_r.$$

Daher ist

$$\left(\frac{-1}{p}\right) = 1, \quad \left(\frac{2}{p}\right) = 1,$$

und damit ergibt sich für $i = 1, \ldots, r$

$$\begin{aligned} \left(\frac{n_i}{p}\right) &= \left(\frac{(-1)^{a_i} \cdot 2^{b_i} \cdot m_i}{p}\right) = \left(\frac{-1}{p}\right)^{a_i} \cdot \left(\frac{2}{p}\right)^{b_i} \cdot \left(\frac{m_i}{p}\right) = \\ &= \left(\frac{m_i}{p}\right) \overset{p \equiv 1 \bmod 4}{=} \left(\frac{p}{m_i}\right) = \left(\frac{p \bmod m_i}{m_i}\right) = \left(\frac{1}{m_i}\right) = 1, \end{aligned}$$

was die Behauptung beweist. ■

FOLGERUNG. *Es gibt keine endliche Menge $N \subseteq \mathbb{Z}$, sodass für jede ungerade Primzahl p ein $n \in N$ existiert mit $\left(\frac{n}{p}\right) = -1$.*

Beweis: Angenommen, es gäbe eine solche Menge. Wir können $0 \notin N$ annehmen und schreiben $N = \{n_1, \ldots, n_r\}$ mit

$$n_i = (-1)^{a_i} \cdot 2^{b_i} \cdot m_i,$$

wie im vorangegangenen Lemma. Der Dirichletsche Primzahlsatz besagt, dass es zu $m_1, \ldots, m_r$ unendlich viele Primzahlen p gibt mit

$$p \equiv 1 \bmod 8\, m_1 \ldots m_r.$$

Dann folgt aber mit dem Lemma

$$\left(\frac{n_1}{p}\right) = \cdots = \left(\frac{n_r}{p}\right) = 1.$$

Dies ist aber ein Widerspruch dazu, dass ein $n_i \in N$ existieren sollte mit $\left(\frac{n_i}{p}\right) = -1$. Die Annahme ist also falsch. Es folgt die Behauptung. ■

Bemerkung: Aufgabe 13 enthält eine Variante der vorangegangenen Überlegungen.

9. Quadratwurzelziehen modulo p - II

LEMMA. *Sei p eine ungerade Primzahl und $Z \subseteq \mathbb{F}_p^*$ die Menge der Elemente von $\mathbb{F}_p^*$, deren Ordnung eine 2-Potenz ist, also*

$$Z = \{\overline{b} \in \mathbb{F}_p^* : \operatorname{ord}_p(b) = 2^i \text{ für ein } i \in \mathbb{N}_0\}.$$

Sei weiter $p - 1 = 2^\ell u$ mit $u \equiv 1 \bmod 2$, $n \in \mathbb{Z}$ mit $\left(\frac{n}{p}\right) = -1$ und $z \in \mathbb{Z}$ mit $z \equiv n^u \bmod p$. Dann gilt:

(1) *Z ist eine Untergruppe von $\mathbb{F}_p^*$, die auch so geschrieben werden kann:*

$$Z = \{\overline{b} \in \mathbb{F}_p^* : b^{2^i} \equiv 1 \bmod p \text{ für ein } i \in \mathbb{N}_0\} = \{\overline{b} \in \mathbb{F}_p^* : b^{2^\ell} \equiv 1 \bmod p\}.$$

(2) $\operatorname{ord}_p(z) = 2^\ell$.

(3) *$Z = \{\overline{z}^i : 0 \le i \le 2^\ell - 1\}$, d.h. $\overline{z}$ ist ein Erzeuger von Z, insbesondere gilt $\#Z = 2^\ell$.*

Beweis:

(1) (a) Aus $\operatorname{ord}_p(b) = 2^i$ folgt natürlich $b^{2^i} \equiv 1 \bmod p$. Gilt umgekehrt $b^{2^i} \equiv 1 \bmod p$, so folgt $\operatorname{ord}_p(b) \mid 2^i$, also ist $\operatorname{ord}_p(b) = 2^j$ für ein $j \in \mathbb{N}_0$ mit $j \le i$. Dies zeigt

$$Z = \{\overline{b} \in \mathbb{F}_p^* : \operatorname{ord}_p(b) = 2^i \text{ für ein } i \in \mathbb{N}_0\} = \{\overline{b} \in \mathbb{F}_p^* : b^{2^i} \equiv 1 \bmod p \text{ für ein } i \in \mathbb{N}_0\}.$$

(b) Sei $\overline{b} \in Z$, also $\operatorname{ord}_p(b) = 2^i$ für ein $i \in \mathbb{N}_0$. Der kleine Satz von Fermat liefert $b^{p-1} \equiv 1 \bmod p$, woraus $\operatorname{ord}_p(b) \mid p - 1$, also $\operatorname{ord}_p(b) \mid 2^\ell u$, und damit $\operatorname{ord}_p(b) \mid 2^\ell$ folgt. Dies impliziert $b^{2^\ell} \equiv 1 \bmod p$. Die Umkehrung haben wir bereits gezeigt.

(c) Die Untergruppeneigenschaft ist klar.

(2) Aus $\left(\frac{n}{p}\right) = -1$ und $z \equiv n^u \bmod p$ ergibt sich

$$z^{2^{\ell-1}} \equiv n^{2^{\ell-1}u} \equiv n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) = -1 \bmod p.$$

Daraus folgt aber

$$\operatorname{ord}_p(z) = 2^\ell,$$

woraus insbesondere

$$\#\{\overline{z}^i : 0 \le i \le 2^\ell - 1\} = 2^\ell \quad \text{und} \quad \{\overline{z}^i : 0 \le i \le 2^\ell - 1\} \subseteq Z$$

folgt.

(3) Wir betrachten das Polynom

$$f(x) = x^{2^\ell} - 1 \in \mathbb{F}_p[x].$$

Dann gilt

$$Z = \{\overline{b} \in \mathbb{F}_p : f(\overline{b}) = 0\}.$$

Da aber f als Polynom vom Grad 2^ℓ höchstens 2^ℓ Nullstellen haben kann, folgt

$$\#Z \leq 2^\ell,$$

und mit $\{\overline{z}^i : 0 \leq i \leq 2^\ell - 1\} \subseteq Z$ und $\#\{\overline{z}^i : 0 \leq i \leq \ell - 1\} = 2^\ell$ dann

$$Z = \{\overline{z}^i : 0 \leq i \leq 2^\ell - 1\}.$$

Dies beweist die Behauptungen. ■

Beispiele: In den folgenden Beispielen werden die Bezeichnungen des vorangegangenen Lemmas verwendet. Dabei wurde für n die kleinste natürliche Zahl gewählt, die kein Quadrat modulo p ist.

(1) $p = 13$, $\ell = 2$, $u = 3$ $n = 2$, $z = 8$

i	0	1	2	3
$z^i \bmod p$	1	8	12	5

(2) $p = 31$, $\ell = 1$, $u = 15$ $n = 3$, $z = 30$

i	0	1
$z^i \bmod p$	1	30

(3) $p = 101$, $\ell = 2$, $u = 25$ $n = 2$, $z = 10$

0	1	2	3
1	10	100	91

(4) $p = 1009$, $\ell = 4$, $u = 63$ $n = 11$, $z = 179$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$z^i \bmod p$	1	179	762	183	469	204	192	62	1008	830	247	826	540	805	817	947

(5) $p = 10009$, $\ell = 3$, $u = 1251$ $n = 7$, $z = 6382$

i	0	1	2	3	4	5	6	7
$z^i \bmod p$	1	6382	3303	792	10008	3627	6706	9217

SATZ. *Sei p eine ungerade Primzahl, $p - 1 = 2^\ell u$ mit $u \equiv 1 \bmod p$, $n \in \mathbb{Z}$ mit $\left(\frac{n}{p}\right) = -1$ und $z \in \mathbb{Z}$ mit $z \equiv n^u \bmod p$, sowie*

$$Z = \{\overline{b} \in \mathbb{F}_p^* : b^{2^\ell} \equiv 1 \bmod p\} = \{\overline{z}^i : 0 \leq i \leq 2^\ell - 1\}.$$

Für $a \in \mathbb{Z}$ mit $\mathrm{ggT}(p, a) = 1$ gilt dann:

(1) *$\overline{a}^u \in Z$, d.h. es gibt ein $x \in \mathbb{N}_0$ mit*

$$a^u \equiv z^x \bmod p.$$

(x ist ein diskreter Logarithmus von $\overline{a^u}$ zur Basis $\overline{z}$ in Z.)

(2) *Genau dann ist a ein Quadrat modulo p, wenn $x \equiv 0 \bmod 2$ gilt.*

(3) *Ist $x \equiv 0 \bmod 2$, so ist*

$$a^{\frac{p-u}{2}} \cdot z^{\frac{x}{2}} \bmod p$$

eine Quadratwurzel von a modulo p.

Beweis:

(1) Es ist

$$(a^u)^{2^\ell} \equiv a^{p-1} \equiv 1 \bmod p,$$

also $\overline{a^u} \in Z$, woraus die Aussage mit dem vorangegangenen Lemma folgt.

(2) Da u ungerade ist, folgt

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^u = \left(\frac{a^u}{p}\right) = \left(\frac{z^x}{p}\right) = \left(\frac{z}{p}\right)^x = \left(\frac{n^u}{p}\right)^x = \left(\frac{n}{p}\right)^{ux} = (-1)^{ux} = (-1)^x,$$

und damit die Behauptung.

(3) Sei nun x gerade. Mit $a^p \equiv a \bmod p$ und $p - u \equiv 0 \bmod 2$ ergibt sich

$$a \equiv a^p \equiv a^{p-u} \cdot a^u \equiv a^{p-u} \cdot z^x \equiv \left(a^{\frac{p-u}{2}} \cdot z^{\frac{x}{2}}\right)^2 \bmod p,$$

was zu zeigen war. ■

Beispiel: Für $p = 1009$ ist $p - 1 = 2^\ell u$ mit $\ell = 4$ und $u = 63$. $n = 11$ ist ein Nichtquadrat modulo p und $z = 179 = n^u \bmod p$ erzeugt die Untergruppe Z der Elemente mit 2-Potenzordnung.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$z^i \bmod p$	1	179	762	183	469	204	192	62	1008	830	247	826	540	805	817	947

Für die folgenden Beispiele brauchen wir zu a^u ein x mit $a^u \equiv z^x \bmod p$. Dies x finden wir durch Nachschauen in der Tabelle.

a	$a^u \bmod p$	x mit $a^u \equiv z^x \bmod p$	Quadratwurzel $a^{\frac{p-u}{2}} \cdot z^{\frac{x}{2}} \bmod p$, falls $x \equiv 0 \bmod p$
2	192	6	570
3	192	6	860
4	540	12	2
5	192	6	244
6	540	12	835
7	469	4	45
8	762	2	878
9	540	12	3
10	540	12	847
11	179	1	kein Quadrat modulo p
12	762	2	298
13	204	5	kein Quadrat modulo p
14	247	10	425
15	540	12	977
16	1008	8	1005
17	830	9	kein Quadrat modulo p
18	762	2	308
19	179	1	kein Quadrat modulo p
20	762	2	521

Wir erhalten folgenden Algorithmus:

Algorithmus zum Quadratwurzelziehen modulo p:
Eingabe: p ungerade Primzahl und $a \in \mathbb{Z}$
Ausgabe: Ein $w \in \mathbb{Z}$ mit $w^2 \equiv a \bmod p$ oder „a ist kein Quadrat modulo p“

1: **if** $a \equiv 0 \bmod p$ **then**
2: **return** 0
3: **end if**
4: $\ell \leftarrow 0$, $u \leftarrow p - 1$
5: **while** $u \bmod 2 = 0$ **do**
6: $\ell \leftarrow \ell + 1$, $u \leftarrow \frac{u}{2}$
7: **end while** ▷ Nun ist $p - 1 = 2^\ell u$ mit $u \equiv 1 \bmod 2$
8: Bestimme ein $n \in \mathbb{Z}$ mit $\left(\frac{n}{p}\right) = -1$ ▷ Beispielsweise durch Probieren $n = 2, 3, 4, 5, \ldots$
9: $z \leftarrow n^u \bmod p$
10: Bestimme ein x mit $a^u \equiv z^x \bmod p$ (und $0 \le x \le 2^\ell - 1$)

11: **if** $x \bmod 2 = 1$ **then**
12: **return** „a ist kein Quadrat modulo p“
13: **end if**
14: $w \leftarrow a^{\frac{p-u}{2}} \cdot z^{\frac{x}{2}} \bmod p$
15: **return** w

Bemerkungen:

(1) Ist 2^ℓ nicht zu groß, kann man in Zeile 10 des Algorithmus den Exponenten x durch Probieren finden. Muss man mehrere Quadratwurzeln modulo p bezeichnen kann man sich auch eine Tabelle der Gestalt $T(z^i \bmod p) = i$ (mit $0 \le i \le 2^\ell - 1$) anlegen.
(2) Die Gleichung $a^u \equiv z^x \bmod p$ mit unbekanntem x zu lösen, heißt, den diskreten Logarithmus von $a^u \bmod p$ zur Basis z modulo p zu berechnen. In unserer Situation gibt es dafür eine schnelle Lösung, bei der man nicht alle $x \in \{0, \ldots, 2^\ell - 1\}$ durchprobieren muss. Dies wird weiter unten dargestellt werden.

Beispiele:

(1) $p \equiv 3 \bmod 4$. Wir können dann schreiben $p = 3 + 4k$ und erhalten $p - 1 = 2 + 4k = 2^1 \cdot (1 + 2k)$, also $\ell = 1$ und $u = 1 + 2k = \frac{p-1}{2}$. Ist n ein Nichtquadrat modulo p, wobei wir hier $n = -1$ wählen können, so ist
$$z \equiv n^u \equiv n^{\frac{p-1}{2}} \equiv -1 \bmod p.$$
Wir wählen $z = -1$ und erhalten
$$Z = \{\overline{1}, \overline{-1}\}.$$
Es ist
$$p - u = p - \frac{p-1}{2} = \frac{p+1}{2}.$$
Es folgt
$$a \equiv a^p \equiv a^{p-u} \cdot a^u \equiv a^{\frac{p+1}{2}} \cdot a^{\frac{p-1}{2}} \equiv \left(a^{\frac{p+1}{4}}\right)^2 \cdot \left(\frac{a}{p}\right) \bmod p.$$
Die Formel zeigt sofort: Ist a ein Quadrat modulo p, also $\left(\frac{a}{p}\right) = 1$, so ist
$$a^{\frac{p+1}{4}}$$
eine Quadratwurzel von a modulo p.
(2) $p \equiv 5 \bmod 8$. Wir schreiben $p = 5 + 8k$ und erhalten
$$p - 1 = 4 + 8k = 2^2 \cdot (1 + 2k), \quad \text{also} \quad \ell = 2 \quad \text{und} \quad u = 1 + 2k = \frac{p-1}{4}.$$
Es ist
$$p - u = p - \frac{p-1}{4} = \frac{3p+1}{4}$$
und
$$a \equiv a^p \equiv a^{p-u} \cdot a^u \equiv a^{\frac{3p+1}{4}} \cdot a^u \equiv \left(a^{\frac{3p+1}{8}}\right)^2 \cdot a^u \bmod p.$$
Wegen $p \equiv 5 \bmod 8$ können wir $n = 2$ wählen und $z \equiv 2^u \equiv 2^{\frac{p-1}{4}} \bmod p$. Es ist
$$Z = \{\overline{1}, \overline{z}, \overline{z}^2, \overline{z}^3\}.$$
Es gibt ein $x \in \{0, 1, 2, 3\}$ mit
$$a^{\frac{p-1}{4}} \equiv a^u \equiv z^x \equiv \left(2^{\frac{p-1}{4}}\right)^x \bmod p.$$
Wir unterscheiden ein paar Fälle:
- Ist $a^{\frac{p-1}{4}} \equiv 1 \bmod p$, so ist $x = 0$ und
$$a \equiv \left(a^{\frac{3p+1}{8}}\right)^2 \bmod p.$$

- Ist $a^{\frac{p-1}{4}} \not\equiv 1 \bmod p$ und $\left(\frac{a}{p}\right) = 1$, so ist $a^u \equiv z^2 \equiv (2^{\frac{p-1}{4}})^2 \bmod p$, und es folgt
$$a \equiv \left(a^{\frac{3p+1}{8}}\right)^2 \cdot \left(2^{\frac{p-1}{4}}\right)^2 \equiv \left(a^{\frac{3p+1}{8}} \cdot 2^{\frac{p-1}{4}}\right)^2 \bmod p.$$
- Der Fall $\left(\frac{a}{p}\right) = -1$ interessiert uns hier nicht weiter.

(Man vergleiche diese Ergebnisse mit denen des Tonelli-Algorithmus. Wo ist der Unterschied?) Wir fassen das Ergebnis zusammen:

SATZ. *Sei p eine Primzahl mit $p \equiv 3, 5, 7 \bmod 8$ und $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 1$. Definiert man*
$$w = \begin{cases} a^{\frac{p+1}{4}} & \text{im Fall } p \equiv 3 \bmod 4, \text{ d.h. } p \equiv 3, 7 \bmod 8, \\ a^{\frac{3p+1}{8}} \bmod p & \text{im Fall } p \equiv 5 \bmod 8 \text{ und } a^{\frac{p-1}{4}} \equiv 1 \bmod p, \\ 2^{\frac{p-1}{4}} \cdot a^{\frac{3p+1}{8}} \bmod p & \text{im Fall } p \equiv 5 \bmod 8 \text{ und } a^{\frac{p-1}{4}} \equiv -1 \bmod p, \end{cases}$$
so sind $\pm w$ die Quadratwurzeln von a modulo p.

Bemerkung: In den angegebenen Fällen hatten wir auch Formeln mit dem Tonelli-Algorithmus hergeleitet. Die Ergebnisse sehen ähnlich aus, nur dass dort statt $a^{\frac{3p+1}{8}}$ der Ausdruck $a^{\frac{p+3}{8}}$ steht.

Ist 2^ℓ in $p - 1 = 2^\ell u$ klein, so kann man die Gleichung $a^u \equiv z^x \bmod p$ durch Probieren lösen, da man sich auf $0 \le x \le 2^\ell - 1$ beschränken kann. Ist 2^ℓ größer, kann man nachfolgendes Verfahren benutzen.

Beispiele: Zu gegebenem ℓ haben wir jeweils die kleinste Primzahl $p \equiv 1 \bmod 2^\ell$ bestimmt und dazu die Faktorisierung von $p - 1$ angegeben. Das Ergebnis ist in der zugehörigen Tabelle zu finden.

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 $G = \{g^i : 0 \le i \le 2^\ell - 1\}$, 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 $0 \le j \le \ell - 1$*
$$h_j = a \cdot \prod_{0 \le i \le j-1} (g^{2^i})^{y_i},$$
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 $0 \le j \le \ell - 1$*
$$y_j = \begin{cases} 0, & \text{falls } h_j^{2^{\ell-1-j}} = 1, \\ 1, & \text{sonst.} \end{cases}$$
(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.

Beweis:

(1) Für $a^{-1} \in G$ gibt es eine Zahl $y \in \mathbb{Z}$ mit $0 \le y \le 2^\ell - 1$ und $a^{-1} = g^y$. Ist $y = \sum_{i=0}^{\ell-1} y_i \cdot 2^i$ die Binärentwicklung von y, so ergibt sich unmittelbar die behauptete Darstellung.
(2) Klar.
(3) Dies ist ebenfalls klar.

(4) Wir potenzieren die Relation

$$1 = a \cdot g^{\sum_{i=0}^{\ell-1} y_i \cdot 2^i} = a \cdot \prod_{i=0}^{\ell-1} (g^{2^i})^{y_i}$$

mit $2^{\ell-1-j}$ (für $0 \leq j \leq \ell-1$) und erhalten

$$\begin{aligned} 1 &= \left(a \cdot \prod_{0 \leq i \leq \ell-1} (g^{2^i})^{y_i} \right)^{2^{\ell-1-j}} = \\ &= \left(a \cdot \prod_{0 \leq i \leq j-1} (g^{2^i})^{y_i} \right)^{2^{\ell-1-j}} \cdot (g^{2^{\ell-1}})^{y_j} \cdot \prod_{j+1 \leq i \leq \ell-1} (g^{2^{\ell+i-(j+1)}})^{y_i} = \\ &= h_j^{2^{\ell-1-j}} \cdot (g^{2^{\ell-1}})^{y_j}. \end{aligned}$$

Da g Ordnung 2^ℓ hat, ist $g^{2^{\ell-1}} \neq 1$. Daher folgt: Ist $y_j = 0$, so ist $h_j^{2^{\ell-1-j}} = 1$, ist $y_j = 1$, so ist $h_j^{2^{\ell-1-j}} \neq 1$. Dies zeigt die Behauptung.

(5) Dies folgt aus $g^{2^\ell} = 1$ aus

$$a = g^{-\sum_{i=0}^{\ell-1} y_i \cdot 2^i} = g^{2^\ell - \sum_{i=0}^{\ell-1} y_i \cdot 2^i}.$$

Dies war zu zeigen. Wir bemerken noch die Darstellung

$$2^\ell - \sum_{i=0}^{\ell-1} = 1 + (2^\ell - 1) - \sum_{i=0}^{\ell-1} y_i \cdot 2^i = 1 + \sum_{i=0}^{\ell-1} 2^i - \sum_{i=0}^{\ell-1} y_i \cdot 2^i = 1 + \sum_{i=0}^{\ell-1} (1 - y_i) \cdot 2^i,$$

die wir allerdings im Satz nicht angemerkt haben. ■

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** $0 \leq j \leq \ell - 1$ **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 $x \bmod 2^\ell$)

Hier sind Python-Funktionen zu den vorangegangenen Algorithmen:

```
# Diskrete Logarithmenberechnung 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 dlog2(a,g,p,l):
  g_j=g
  h=a
  x=2**l
  for j in range(l):
    if pow(h,2**(l-1-j),p)!=1:
      x=x-2**j
      h=(h*g_j)%p
    g_j=(g_j*g_j)%p
```

```
  return x%(2**l)
################################################################################
# Quadratwurzel modulo p - 2. Verfahren
def sqrtp_2(a,p):
  if a%p==0:
    return 0
  l,u=0,p-1
  while u%2==0:
    l,u=l+1,u//2
  # Bestimmung des kleinsten positiven Nichtquadrats durch Ausprobieren
  n=2
  while jac(n,p)!=-1:
    n=n+1
  z=pow(n,u,p) # z erzeugt die Untergruppe der Elemente mit 2-Potenz-Ordnung
  au=pow(a,u,p)
  if l<=10:
    for x in range(2**l):
      if pow(z,x,p)==au:
        break
  else:
    x=dlog2(au,z,p,l)
  if x%2==1:
    return "a ist kein Quadrat modulo p"
  w=(pow(a,(p-u)//2,p)*pow(z,x//2,p))%p
  return w
```

10. Die Gleichung $x^2 \equiv a \bmod N$ für $N = pq$

Wir haben bis jetzt gesehen, dass es praktisch leicht ist, die Gleichung $x^2 \equiv a \bmod p$ auf Lösbarkeit zu untersuchen und gegebenenfalls eine Lösung zu bestimmen. Wir wollen nun die Gleichung $x^2 \equiv a \bmod N$ anschauen, wobei N eine zusammengesetzte Zahl ist. Wir beschränken uns auf den Fall $N = pq$.

Satz. *Sei $N = pq$ mit verschiedenen ungeraden Primzahlen p und q und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, N) = 1$.*

(1) *Die Gleichung $x^2 \equiv a \bmod N$ ist genau dann lösbar in $\mathbb{Z}$, wenn für die Legendre-Symbole gilt: $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$.*

(2) *Gilt $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$, so gibt es $x_p, x_q \in \mathbb{Z}$ mit $x_p^2 \equiv a \bmod p$, $x_q^2 \equiv a \bmod q$. Für $\varepsilon_p, \varepsilon_q \in \{\pm 1\}$ definiert man Zahlen $x_{\varepsilon_p,\varepsilon_q}$ auf eine der folgenden Weisen:*

- $$x_{\varepsilon_p,\varepsilon_q} \equiv \begin{cases} \varepsilon_p x_p \bmod p, \\ \varepsilon_q x_q \bmod q \end{cases}$$
- *Wählt man $u, v \in \mathbb{Z}$ mit $up + vq = 1$ (erweiterter euklidischer Algorithmus), setzt man*
$$x_{\varepsilon_p,\varepsilon_q} = (\varepsilon_p x_p vq + \varepsilon_q x_q up) \bmod N \quad \text{mit} \quad \varepsilon_p, \varepsilon_q \in \{\pm 1\},$$

so sind die $x_{\varepsilon_p,\varepsilon_q}$ genau die Lösungen der Gleichung $x^2 \equiv a \bmod N$ modulo N. Insbesondere gibt es genau vier Lösungen modulo N.

Beweis:

(1) Gilt $x^2 \equiv a \bmod N$ für ein $x \in \mathbb{Z}$, so folgt $x^2 \equiv a \bmod p$ und $x^2 \equiv a \bmod q$, also wegen $\mathrm{ggT}(a, N) = 1$ dann $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$.

(2) Sei umgekehrt $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$. Dann gibt es $x_p, x_q \in \mathbb{Z}$ mit $x_p^2 \equiv a \bmod p$ und $x_q^2 \equiv a \bmod q$. Mit $up + vq = 1$ und $x_{\varepsilon_p,\varepsilon_q} = \varepsilon_p x_p vq + \varepsilon_q x_q up$ gilt wegen $vq \equiv 1 \bmod p$ und $up \equiv 1 \bmod q$

$$x_{\varepsilon_p,\varepsilon_q} \equiv \varepsilon_p x_p \bmod p \quad \text{und} \quad x_{\varepsilon_p,\varepsilon_q} \equiv \varepsilon_q x_q \bmod q,$$

was dann

$$x_{\varepsilon_p,\varepsilon_q}^2 \equiv x_p^2 \equiv a \bmod p \quad \text{und} \quad x_{\varepsilon_p,\varepsilon_q}^2 \equiv x_q^2 \equiv a \bmod q$$

liefert. Daher haben wir $p \mid x_{\varepsilon_p,\varepsilon_q}^2 - a$, $q \mid x_{\varepsilon_p,\varepsilon_q}^2 - a$, also $N \mid x_{\varepsilon_p,\varepsilon_q}^2 - a$, d.h. $x_{\varepsilon_p,\varepsilon_q}^2 \equiv a \bmod N$. Die Zahlen $x_{\varepsilon_p,\varepsilon_q}$ sind also Lösungen der Gleichung $x^2 \equiv a \bmod N$.

(3) Sei $x \in \mathbb{Z}$ mit $x^2 \equiv a \bmod N$. Es folgt $x^2 \equiv a \equiv x_p^2 \bmod p$. Also gibt es ein $\varepsilon_p \in \{\pm 1\}$ mit $x \equiv \varepsilon_p x_p \bmod p$. Analog gibt es ein $\varepsilon_q \in \{\pm 1\}$ mit $x \equiv \varepsilon_q x_q \bmod q$. Es folgt $x \equiv x_{\varepsilon_p,\varepsilon_q} \bmod p$ und $x \equiv x_{\varepsilon_p,\varepsilon_q} \bmod q$, woraus sofort $x \equiv x_{\varepsilon_p,\varepsilon_q} \bmod N$ folgt. Damit sehen wir, dass modulo N genau die Zahlen $x_{\varepsilon_p,\varepsilon_q}$ die Gleichung $x^2 \equiv a \bmod N$ lösen. ■

Bemerkungen:

(1) Mit Hilfe des Satzes kann man die Gleichung $x^2 \equiv a \bmod N$ schnell lösen, wenn man die Faktorisierung von $N = pq$ kennt.

(2) Die Form $x_{\varepsilon_p,\varepsilon_q} = (\varepsilon_p x_p vq + \varepsilon_q x_q up) \bmod N$ der Lösungen ergibt sich durch eine explizite Form des chinesischen Restsatzes aus den Lösungen $\varepsilon_p x_p$ modulo p und $\varepsilon_q x_q$ modulo q.

(3) Der Satz lässt sich leicht wie folgt verallgemeinern: Ist $N = p_1 \dots p_r$ mit paarweise verschiedenen ungeraden Primzahlen p_i, gilt $\left(\frac{a}{p_1}\right) = \dots = \left(\frac{a}{p_r}\right) = 1$, so gibt es $x_i \in \mathbb{Z}$ mit $x_i^2 \equiv a \bmod p_i$. Zu $\varepsilon_1, \dots, \varepsilon_r \in \{\pm 1\}$ findet man mit dem chinesischen Restsatz ein $x_{\varepsilon_1,\dots,\varepsilon_r} \in \mathbb{Z}$ mit

$$x_{\varepsilon_1,\dots,\varepsilon_r} \equiv \varepsilon_i x_i \bmod p_i \quad \text{für} \quad i = 1, \dots, r.$$

Dann sind die Lösungen der Gleichung $x^2 \equiv a \bmod N$ genau die Zahlen $x_{\varepsilon_1,\dots,\varepsilon_r}$ modulo N.

Beispiel: $N = 12193263122374638001 = pq$ mit $p = 1234567891$ und $q = 9876543211$. Die Gleichung $x^2 \equiv 5 \bmod N$ ist wegen $\left(\frac{5}{p}\right) = \left(\frac{5}{q}\right) = 1$ lösbar. Modulo p erhalten wir die Lösungen

$$x_{p,1} = 416740019, \quad x_{p,2} = 772827872,$$

modulo q die Lösungen

$$x_{q,1} = 317399324, \quad x_{q,2} = 9559143887,$$

woraus man mit dem chinesischen Restsatz die vier Lösungen

$$x_{11} = 11035184594165244164, \qquad x_{12} = 92713293520307307,$$
$$x_{21} = 12100549828854330694, \qquad x_{22} = 1158078528209393837$$

erhält.

Wir wollen jetzt umgekehrt zeigen, dass die Kenntnis von vier Lösungen von $x^2 \equiv a \bmod N$ mit $N = pq$ zur Faktorisierung von N führt:

LEMMA. *Sei $N = pq$ mit verschiedenen ungeraden Primzahlen p und q und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, N) = 1$. Hat die Gleichung $x^2 \equiv a \bmod N$ die vier (modulo N) verschiedenen Lösungen x_1, x_2, x_3, x_4, so gilt*

$$\{\mathrm{ggT}(x_1 - x_2, N), \mathrm{ggT}(x_1 - x_3, N), \mathrm{ggT}(x_1 - x_4, N)\} = \{1, p, q\}.$$

Beweis: Wir verwenden die Bezeichnungen des vorangegangenen Satzes. O.E.

$$\begin{aligned} x_1 &= +x_p vq + x_q up, \\ x_2 &= +x_p vq - x_q up, \\ x_3 &= -x_p vq + x_q up, \\ x_4 &= -x_p vq - x_q up. \end{aligned}$$

Dann ist

$$\begin{aligned} \mathrm{ggT}(x_1 - x_2, n) &= \mathrm{ggT}(2x_q up, pq) = p, \\ \mathrm{ggT}(x_1 - x_3, n) &= \mathrm{ggT}(2x_p vq, pq) = q, \\ \mathrm{ggT}(x_1 - x_4, n) &= \mathrm{ggT}(2x_1, pq) = 1, \end{aligned}$$

was wir zeigen wollten. ■

Bemerkung: Weiß man also, dass die zusammengesetzte Zahl N die Gestalt $N = pq$ hat, kennt man für ein $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, N) = 1$ vier Lösungen der Gleichung $x^2 \equiv a \bmod N$, so kann man N damit faktorisieren. Man sieht also, dass das Finden aller 4 Wurzeln ebenso schwer ist wie das Faktorisieren von N.

Bemerkung: Wir interpretieren das Vorangegangene etwas anders: Kennt man zu einer RSA-Zahl $N = pq$ zwei Zahlen x, y mit $\mathrm{ggT}(x, N) = \mathrm{ggT}(y, N) = 1$, $x \not\equiv \pm y \bmod N$ und $x^2 \equiv y^2 \bmod N$, so kennen wir zu $a = x^2 \bmod N$ alle Wurzeln modulo N, nämlich $x, -x, y, -y$. Dann erhält man sofort die nichttriviale Faktorzerlegung

$$N = \mathrm{ggT}(N, x - y) \cdot \mathrm{ggT}(N, x + y), \qquad \text{also} \qquad \{\mathrm{ggT}(N, x - y), \mathrm{ggT}(N, x + y)\} = \{p, q\}.$$

Bemerkung: Hätte man ein (schnelles) Verfahren, das bei Vorgabe von $N = pq$ und a mit $\mathrm{ggT}(a, N) = 1$ eine Lösung x mit $x^2 \equiv a \bmod N$ bestimmt oder sagt, dass keine existiert, so könnte man auf folgendem Weg (schnell) N faktorisieren:

(1) Man wählt zufällig b mit $0 \le b \le N - 1$ und $\mathrm{ggT}(b, N) = 1$ und berechnet $a \equiv b^2 \bmod N$.
(2) Das Verfahren liefert ein c mit $c^2 \equiv a \equiv b^2 \bmod N$.
(3) Mit Wahrscheinlichkeit $\frac{1}{2}$ ist $b \not\equiv \pm c \bmod N$ und damit ist $\mathrm{ggT}(b - c, N)$ ein nichttrivialer Teiler von N.
(4) Ist $b \equiv \pm c \bmod N$ so wählt man ein neues b.

11. Das Rabin-Verschlüsselungsverfahren

Die Schwierigkeit, Quadratwurzeln modulo einer zusammengesetzten Zahl N zu ziehen, wenn man die Faktorisierung von N nicht kennt, wird im Rabin-Verschlüsselungsverfahren ausgenutzt.

Rabin-Verschlüsselung:

(1) **Schlüsselerzeugung:** A wählt sich zwei verschiedene, große Primzahlen p und q mit $p \equiv q \equiv 3 \bmod 4$, berechnet $N = pq$ und gibt N als seinen öffentlichen Schlüssel bekannt. Mit dem erweiterten euklidischen Algorithmus berechnet A ganze Zahlen u, v mit $up + vq = 1$. Der private Schlüssel von A sind dann die Zahlen p, q, u, v. Nochmals:
   - Öffentlicher Schlüssel: N
   - Privater Schlüssel: p, q, u, v

(2) **Verschlüsselung:**
   (a) Man einigt sich auf ein Verfahren, wie man Text in eine Folge von Zahlen a_i mit $0 \le a_i \le N - 1$ umsetzt.
   (b) Will jemand die Zahlenfolge $a_1, a_2, a_3, \ldots$ mit dem öffentlichen Schlüssel von A verschlüsseln, berechnet er
   $$b_i = a_i^2 \bmod N$$
   und schickt die Zahlenfolge $b_1, b_2, b_3, \ldots$ an A.

(3) **Entschlüsselung:**
   (a) Mit seinem privaten Schlüssel p, q, u, v berechnet A zu jedem b_i für die vier Möglichkeiten $(\varepsilon_p, \varepsilon_q) = (\pm 1, \pm 1)$ die Zahlen
   $$c_{i,\varepsilon_p,\varepsilon_q} = \Big(\varepsilon_p \cdot (b_i^{\frac{p+1}{4}} \bmod p) \cdot vq + \varepsilon_q \cdot (b_i^{\frac{q+1}{4}} \bmod q) \cdot up\Big) \bmod N.$$

(b) Ist alles richtig gegangen, so gilt

$$a_i \in \{c_{i,+1,+1}, c_{i,+1,-1}, c_{i,-1,+1}, c_{i,-1,-1}\}.$$

A muss aus diesen 4 Möglichkeiten das richtige a_i auswählen. Die Entschlüsselung ist also zunächst nicht eindeutig.

(c) Man kann versuchen, die Entschlüsselung eindeutiger zu machen, indem man Redundanz einführt. Wir werden später eine andere Möglichkeit zeigen, wie man die Entschlüsselung eindeutig machen kann.

Bemerkungen:

(1) Bei RSA wird mit der Gleichung

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

verschlüsselt, mit

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

entschlüsselt, wobei $ed \equiv 1 \bmod (p-1)(q-1)$ gilt. Wegen der Bedingung $\mathrm{ggT}(e,(p-1)(q-1)) = 1$ muss e ungerade sein, $e = 3$ ist der kleinstmögliche Exponent (im Fall $p \equiv q \equiv 2 \bmod 3$). Bei der Rabin-Verschlüsselung ist die Verschlüsselungsgleichung

$$b_i = a_i^2 \bmod N$$

einfacher, dafür ist die Entschlüsselung aber komplizierter und zunächst nicht eindeutig.

(2) Bei der Schlüsselerzeugung wurde $p \equiv q \equiv 3 \bmod 4$ vorausgesetzt. Dadurch kann man die Wurzel aus b_i modulo p einfach in der Form $b_i^{\frac{p+1}{4}}$ angegeben, und analog modulo q. Im Allgemeinfall muss man ein Quadratwurzelverfahren verwenden um die Wurzel aus b_i modulo p zu ziehen.

(3) Die bei der Entschlüsselung verwendete Formel

$$c_{i,\varepsilon_p,\varepsilon_q} = \left(\varepsilon_p \cdot (b_i^{\frac{p+1}{4}} \bmod p) \cdot vq + \varepsilon_q \cdot (b_i^{\frac{q+1}{4}} \bmod q) \cdot up\right) \bmod N$$

kann man auch in der Form

$$c_{i,\varepsilon_p,\varepsilon_q} = \left(\varepsilon_p \cdot b_i^{\frac{p+1}{4}} \cdot vq + \varepsilon_q \cdot b_i^{\frac{q+1}{4}} \cdot up\right) \bmod N$$

schreiben.

(4) Warum funktioniert die Entschlüsselung? Mit $b_i \equiv a_i^2 \bmod N$ gilt auch $b_i \equiv a_i^2 \bmod p$ und damit modulo p

$$c_{i,\varepsilon_p,\varepsilon_q} \equiv \varepsilon_p b_i^{\frac{p+1}{4}} \equiv \varepsilon_p a_i^{\frac{p+1}{2}} \equiv \varepsilon_p a_i^{\frac{p-1}{2}} a_i \equiv \varepsilon_p \left(\frac{a_i}{p}\right) a_i \bmod p$$

und analog

$$c_{i,\varepsilon_p,\varepsilon_q} \equiv \varepsilon_q \left(\frac{a_i}{q}\right) a_i \bmod q.$$

Wählt man nun

$$\varepsilon_p = \begin{cases} \left(\frac{a_i}{p}\right), & \text{falls } \mathrm{ggT}(a_i,p) = 1, \\ 1, & \text{falls } p \mid a_i, \end{cases}$$

und

$$\varepsilon_q = \begin{cases} \left(\frac{a_i}{q}\right), & \text{falls } \mathrm{ggT}(a_i,q) = 1, \\ 1, & \text{falls } q \mid a_i, \end{cases}$$

so folgt

$$c_{i,\varepsilon_p,\varepsilon_q} \equiv a_i \bmod p \quad \text{und} \quad c_{i,\varepsilon_p,\varepsilon_q} \equiv a_i \bmod q$$

und damit

$$c_{i,\varepsilon_p,\varepsilon_q} = a_i,$$

was dann die Richtigkeit der Entschlüsselung zeigt.

Beispiel: Wir wählen $N = 30053021$ mit $N = pq$, $p = 5003$, $q = 6007$. Wir wollen „SONNENSCHEIN“ Rabin-verschlüsseln und wandeln es zunächst in der gewohnten Weise in eine Zahlenfolge a_i um (mit Blocklänge 4):

Text	SONN	ENSC	HEIN
a_i	19151414	5141903	8050914
$b_i = a_i^2 \bmod N$	3001697	21236659	2557394

Für die Entschlüsselung berechnen wir $u = 353$, $v = -294$ mit $up+vq = 1$ und dann mit den angegebenen Formeln

b_i	$c_{i,+1,+1}$	$c_{i,+1,-1}$	$c_{i,-1,+1}$	$c_{i,-1,-1}$
3001697	10901607 (J*PG)	12327462 (L***)	17725559 (Q***)	19151414 (SONN)
21236659	18970195 (R*A*)	5141903 (ENSC)	24911118 (X*KR)	11082826 (KH*Z)
2557394	22002107 (V UG)	674318 (**R)	29378703 (***C)	8050914 (HEIN)

Die ersten beiden Zeilen liefern SONN und ENSC, in der letzten gibt es zwei Möglichkeiten: V UG oder HEIN. Natürlich kann man im Zusammenhang die richtige Lösung erraten: SONNENSCHEIN.

12. Eine Variante der Rabin-Verschlüsselung

Kann man beim Verschlüsseln eine Eigenschaft von a_i mitübertragen, die die Entschlüsselung dann eindeutig macht?

Beispiel: Wird a_i zu $b_i = a_i^2 \bmod N$ Rabin-verschlüsselt, so könnte man neben b_i auch $a_i \bmod 4$ übertragen. Für das richtige $c_{i,\varepsilon_p,\varepsilon_q}$ muss dann

$$c_{i,\varepsilon_p,\varepsilon_q} \bmod 4 = a_i \bmod 4$$

gelten. Leider müssen die vier Zahlen $c_{i,\varepsilon_p,\varepsilon_q} \bmod 4$ aber nicht alle vier Möglichkeiten modulo 4 annehmen. Deswegen reicht dies nicht.

Es zeigt sich aber, dass die Zusatzinformation

$$\left(\frac{a_i}{N}\right) \quad \text{und} \quad a_i \bmod 2$$

reicht, um das richtige $c_{i,\varepsilon_p,\varepsilon_q}$ zu finden.

Lemma. *Sei $N = pq$ eine RSA-Zahl mit $p \equiv q \equiv 3 \bmod 4$. Sei $a_i \in \mathbb{Z}$ mit $\mathrm{ggT}(N, a_i) = 1$ und $0 \le a_i \le N-1$. Berechnet man*

$$b_i = a_i^2 \bmod N, \quad \left(\frac{a_i}{N}\right), \quad a_i \bmod 2,$$

kennt man $u, v \in \mathbb{Z}$ mit $up + vq = 1$, definiert man

$$c_i = \left(\left(b_i^{\frac{p+1}{4}} \bmod p\right) \cdot vq + \left(\frac{a_i}{N}\right) \cdot \left(b_i^{\frac{q+1}{4}} \bmod q\right) \cdot up\right) \bmod N,$$

so gilt

$$a_i = \begin{cases} c_i, & \text{falls } c_i \bmod 2 = a_i \bmod 2, \\ N - c_i, & \text{falls } c_i \bmod 2 \neq a_i \bmod 2. \end{cases}$$

Beweis: Wir rechnen modulo N:

$$\begin{aligned} c_i &\equiv b_i^{\frac{p+1}{4}} \cdot vq + \left(\frac{a_i}{N}\right) \cdot b_i^{\frac{q+1}{4}} \cdot up \equiv a_i^{\frac{p+1}{2}} \cdot vq + \left(\frac{a_i}{N}\right) \cdot a_i^{\frac{q+1}{2}} \cdot up \equiv \\ &\equiv a_i \cdot a_i^{\frac{p-1}{2}} \cdot vq + \left(\frac{a_i}{p}\right)\left(\frac{a_i}{q}\right) \cdot a_i \cdot a_i^{\frac{q-1}{2}} \cdot up \equiv \\ &\equiv a_i \cdot \left(\frac{a_i}{p}\right) \cdot vq + \left(\frac{a_i}{p}\right)\left(\frac{a_i}{q}\right) \cdot a_i \cdot \left(\frac{a_i}{q}\right) \cdot up \equiv \\ &\equiv \left(\frac{a_i}{p}\right) \cdot a_i \cdot (vq + up) \equiv \left(\frac{a_i}{p}\right) \cdot a_i \bmod N. \end{aligned}$$

Daraus folgt

$$a_i \equiv \left(\frac{a_i}{p}\right) \cdot c_i \bmod N.$$

- **Fall** $\left(\frac{a_i}{p}\right) = 1$**:** Dann ist $a_i \equiv c_i \bmod N$, also
$$a_i = c_i.$$
In diesem Fall gilt $a_i \bmod 2 = c_i \bmod 2$.
- **Fall** $\left(\frac{a_i}{p}\right) = -1$**:** Dann ist
$$a_i \equiv \left(\frac{a_i}{p}\right) \cdot c_i \equiv -c_i \equiv N - c_i \bmod N,$$
also
$$a_i = N - c_i.$$
In diesem Fall gilt $a_i \bmod 2 \neq c_i \bmod 2$, da N ungerade ist.

Man sieht also, dann man die beiden Fälle durch Vergleich von $a_i \bmod 2$ und $c_i \bmod 2$ unterscheiden kann. Damit folgt die Behauptung. ■

Das vorangegangene Lemma führt sofort zu folgender Variante der Rabin-Verschlüsselung:

Rabin-Verschlüsselung (II):

(1) **Schlüsselerzeugung:** A wählt sich zwei verschiedene, große Primzahlen p und q mit $p \equiv q \equiv 3 \bmod 4$, berechnet $N = pq$ und gibt N als seinen öffentlichen Schlüssel bekannt. Mit dem erweiterten euklidischen Algorithmus berechnet A ganze Zahlen u, v mit $up + vq = 1$. Der private Schlüssel von A sind dann die Zahlen p, q, u, v. Nochmals:
- Öffentlicher Schlüssel: N
- Privater Schlüssel: p, q, u, v

(2) **Verschlüsselung:**
(a) Man einigt sich auf ein Verfahren, wie man Text in eine Folge von Zahlen a_i mit $0 \leq a_i \leq N - 1$ umsetzt.
(b) Will jemand die Zahlenfolge $a_1, a_2, a_3, \ldots$ mit dem öffentlichen Schlüssel von A verschlüsseln, berechnet er
$$b_i = a_i^2 \bmod N, \quad j_i = \left(\frac{a_i}{N}\right), \quad m_i = a_i \bmod 2$$
und schickt die Zahlenfolge b_i, j_i, m_i an A.

(3) **Entschlüsselung:**
(a) A erhält die Zahlenfolgen b_i, j_i, m_i. Mit seinem privaten Schlüssel p, q, u, v berechnet A zunächst
$$c_i = \left(\left(b_i^{\frac{p+1}{4}} \bmod p\right) \cdot vq + j_i \cdot \left(b_i^{\frac{q+1}{4}} \bmod q\right) \cdot up\right) \bmod N.$$
Dann erhält A die Klartextfolge a_i durch
$$a_i = \begin{cases} c_i, & \text{falls } c_i \bmod 2 = m_i, \\ N - c_i, & \text{falls } c_i \bmod 2 \neq m_i. \end{cases}$$

Beispiel: Wir greifen nochmals das Beispiel bei der Rabin-Verschlüsselung auf. Wir haben gewählt $N = 30053021$ mit $N = pq$, $p = 5003$, $q = 6007$. Wir wollen wieder „SONNENSCHEIN“ verschlüsseln. Wir erhalten folgende Zahlenfolgen:

a_i	$b_i = a_i^2 \bmod N$	$j_i = \left(\frac{a_i}{N}\right)$	$m_i = a_i \bmod 2$	c_i	a_i
19151414	3001697	1	0	10901607	19151414
5141903	21236659	-1	1	5141903	5141903
8050914	2557394	1	0	22002107	8050914

13. Das Rabin-Williams-Verschlüsselungsverfahren

Eine andere Variante der Rabin-Verschlüsselung, bei der die Entschlüsselung eindeutig ist, geht auf Williams zurück:

Das Rabin-Williams-Verschlüsselungsverfahren:

(1) **Schlüsselerzeugung:** Zur Erstellung eines Schlüssels geht eine Person A folgendermaßen vor:
   (a) A wählt Primzahlen p, q mit $p \equiv 3 \bmod 8$ und $q \equiv 7 \bmod 8$ und berechnet $N = pq$. (Die Zahlen sollten so gewählt sein, dass N praktisch nicht faktorisiert werden kann.)
   (b) Außerdem berechnet A die Zahl $m = \frac{(p-1)(q-1)+4}{8}$.
   (c) A gibt N als seinen öffentlichen Schlüssel bekannt. N und m bilden den privaten Schlüssel von A.

(2) **Verschlüsselung:** Will eine Person B eine Nachricht verschlüsselt an A schicken, geht B so vor:
   (a) B besorgt sich den öffentlichen Schlüssel N von A.
   (b) B wandelt die Nachricht nach einem vereinbarten Schema in eine Zahlenfolge a_i mit $0 \leq a_i \leq \left\lfloor \frac{N}{8} \right\rfloor$ um.
   (c) B berechnet

$$b_i = \begin{cases} 16(2a_i+1)^2 \bmod N, & \text{falls } \left(\frac{2a_i+1}{N}\right) = 1, \\ 4(2a_i+1)^2 \bmod N, & \text{falls } \left(\frac{2a_i+1}{N}\right) = -1, \end{cases}$$

   was sich zusammengefasst auch in der Form

$$b_i = 2^{3+\left(\frac{2a_i+1}{N}\right)}(2a_i+1)^2 \bmod N$$

   schreiben lässt. (Im Fall $\left(\frac{2a_i+1}{N}\right) = 0$ ist $\mathrm{ggT}(N, 2a_i+1) \in \{p, q\}$. Tritt dieser Fall ein, sollte B der Person A mitteilen, dass er N faktorisiert hat.)
   (d) B schickt die Folge b_i, als den Chiffretext, an A.

(3) **Entschlüsselung:** A erhält die Zahlenfolge b_i von B.
   (a) A berechnet mit seinem privaten Schlüssel $m = \frac{(p-1)(q-1)+4}{8}$

$$c_i = b_i^m \bmod N,$$

   und damit

$$a_i = \begin{cases} \frac{c_i-4}{8}, & \text{falls } c_i \equiv 0 \bmod 4, \\ \frac{N-4-c_i}{8}, & \text{falls } c_i \equiv 1 \bmod 4, \\ \frac{c_i-2}{4}, & \text{falls } c_i \equiv 2 \bmod 4, \\ \frac{N-2-c_i}{4}, & \text{falls } c_i \equiv 3 \bmod 4. \end{cases}$$

   (b) Die Zahlenfolge a_i wandelt A nach dem vereinbarten Schema in Text um und erhält damit die von B gesandte Nachricht.

Bemerkung: Natürlich muss man beweisen, dass die Entschlüsselung wieder die Ausgangszahl ergibt. Wir verzichten hier aber darauf.

Beispiel: Für die Primzahlen $p = 1499$ und $q = 2039$ erhält man $N = 3056461$ und $m = 381616$. Wir wollen „HEUTE IST FREITAG“ mit unserer üblichen Umsetzung in Zahlen verschlüsseln. Wegen $\left\lfloor \frac{N}{8} \right\rfloor = 382057$ wählen wir Blocklänge 3.

Text	a_i	$\left(\frac{2a_i+1}{N}\right)$	b_i
HEU	80521	-1	48595
TE	200500	1	825429
IST	091920	1	1962993
FR	618	-1	7754
EIT	50920	1	991423
AG	10700	-1	1191065

Der Chiffretext ist also

$$48595, 825429, 1962993, 7754, 991423, 1191065.$$

Wir wollen dies wieder entschlüsseln:

b_i	$c_i = b_i^m \bmod N$	$c_i \bmod 4$	a_i
48595	322086	2	80521
825429	1604004	0	200500
1962993	2321097	1	91920
7754	2474	2	618
991423	407364	0	50920
1191065	3013659	3	10700

14. Das Fiat-Shamir-Identifikationsprotokoll

Die Sicherheit des folgenden Verfahrens beruht darauf, dass man praktisch keine Wurzeln modulo einer RSA-Zahl N ziehen kann, wenn man die Faktorisierung von N nicht kennt.

Schlüssel:

(1) Man braucht eine vertrauenswürdige Zentrale (TTP- trusted third party). Diese wählt verschiedene große Primzahlen p und q, berechnet $N = pq$ und gibt N öffentlich bekannt. N sollte praktisch nicht zu faktorisieren sein. (Außer der vertrauenswürdigen Zentrale selbst kann niemand Quadratwurzeln modulo N berechnen.)

(2) Jeder Teilnehmer A wählt sich geheim ein e_A mit $1 \le e_A \le N-1$ und $\mathrm{ggT}(N, e_A) = 1$ und berechnet $f_A = e_A^2 \bmod N$. Der Wert f_A wird veröffentlicht.

Das Identifikationsprotokoll: A will B davon überzeugen, dass er A ist, indem er B beweist, dass er eine Wurzel e_A von f_A modulo N kennt. Dazu werden die folgenden Schritte hinreichend oft wiederholt:

(1) A wählt zufällig a_i mit $1 \le a_i \le N-1$, berechnet $b_i = a_i^2 \bmod N$ und schickt b_i an B.

(2) B wählt zufällig $e_i \in \{0, 1\}$ und schickt e_i an A. (challenge)

(3) A setzt bzw. berechnet

$$c_i = \begin{cases} a_i & \text{im Fall } e_i = 0, \\ e_A a_i \bmod N & \text{im Fall } e_i = 1 \end{cases}$$

und schickt c_i an B. (response).

(4) B testet, ob gilt

$$c_i^2 \equiv \begin{cases} b_i \bmod N & \text{im Fall } e_i = 0, \\ f_A b_i \bmod N & \text{im Fall } e_i = 1. \end{cases}$$

Ist die Gleichung erfüllt, akzeptiert B den Schritt.

Ist nach einigen Wiederholungen alles gut gegangen, glaubt B, dass A eine Wurzel von f_A modulo N kennt.

Was passiert, wenn ein Außenstehender C vortäuscht, A zu sein, zwar f_A, aber keine Wurzel von f_A modulo N kennt?
C muss an B jeweils zwei Zahlen b_i und c_i senden, für die

$$c_i^2 \equiv b_i \bmod N \text{ im Fall } e_i = 0 \quad \text{ und } c_i^2 \equiv f_A b_i \bmod N \text{ im Fall } e_i = 1$$

gilt. Beide Gleichungen sind einfach zu erfüllen, aber C muss b_i festlegen, bevor er e_i kennt.

(1) Falls sich C auf $e_i = 0$ einstellt, wählt er b_i und $\widetilde{c}_i$ mit $b_i \equiv \widetilde{c}_i^2 \bmod N$ und schickt zunächst b_i an B.

(a) Kommt von B die Herausforderung $e_i = 0$, ist alles in Ordnung, wenn C die Zahl $c_i = \widetilde{c}_i$ an B schickt.

(b) Kommt von B aber $e_i = 1$, so muss C ein c_i mit $c_i^2 \equiv f_A b_i \equiv f_A \widetilde{c}_i^2 \bmod N$ finden, was aber nicht geht, da C keine Wurzel von f_A modulo N kennt.

(2) Falls sich C auf $e_i = 1$ einstellt, wählt er b_i und $\widetilde{c}_i$ mit $\widetilde{c}_i^2 \equiv f_A b_i \bmod N$ und schickt b_i an B.
   (a) Kommt von B die Herausforderung $e_i = 0$, so muss C ein c_i mit $b_i \equiv c_i^2 \bmod N$ finden, was aber wegen $\widetilde{c}_i^2 \equiv f_A b_i \equiv f_A c_i^2 \bmod N$ wieder auf die Kenntnis einer Wurzel von f_A modulo N hinausliefe. Das geht nicht.
   (b) Kommt von B die Herausforderung $e_i = 1$, schickt C den Wert $c_i = \widetilde{c}_i$ an B zurück und alles ist in Ordnung.

Die Wahrscheinlichkeit, dass etwas schief geht, ist also $\frac{1}{2}$. Nach einigen Wiederholungen sollte das auffallen.

Bemerkung: Das Verfahren ist auch ein Beispiel für einen zero-knowledge-Beweis (Beweis ohne Wissensvermittlung): A überzeugt B davon, dass er eine Wurzel von $f_A \bmod N$ kennt, B erhält allerdings keine explizite Kenntnis der Wurzel.

15. Formeln zum Wurzelziehen

Wir haben gesehen, dass man im Fall $p \equiv 3 \bmod 4$ für $a \in \mathbb{F}_p$ mit $\left(\frac{a}{p}\right) = 1$ eine Quadratwurzel von a einfach durch Potenzieren mit $\frac{p+1}{4}$ erhält: $a^{\frac{p+1}{4}}$ ist eine Quadratwurzel von a. Gibt es weitere Fälle, in denen man so einfach Quadratwurzeln berechnen kann?

LEMMA. *Sei G eine multiplikativ geschriebene, abelsche Gruppe und $Q = \{g^2 : g \in G\}$ die Untergruppe der Quadrate von G.*

(1) *Sei $a \in Q$.*
   (a) *Genau dann gibt es eine Quadratwurzel von a der Gestalt a^k (mit $k \in \mathbb{N}$), wenn $\operatorname{ord}(a)$ eine ungerade Zahl ist.*
   (b) *Ist $\operatorname{ord}(a)$ ungerade, so ist für jedes $k \in \mathbb{N}$ mit $\operatorname{ord}(a) \mid 2k-1$ das Element a^k eine Quadratwurzel von a, d.h. es gilt $(a^k)^2 = a$. Insbesondere gilt $(a^{\frac{\operatorname{ord}(a)+1}{2}})^2 = a$.*

(2) *Ist die Gruppenordnung $|Q|$ ungerade, so ist für jedes $a \in Q$*

$$a^{\frac{|G|+1}{2}}$$

eine Quadratwurzel von a.

(3) *Ist die Gruppenordnung $|Q|$ gerade, so gibt es ein Element $\varepsilon \in Q$ mit $\operatorname{ord}(\varepsilon) = 2$, und es ist $(\varepsilon^k)^2 \neq \varepsilon$ für alle $k \in \mathbb{N}$, d.h. keine Quadratwurzel von ε hat die Gestalt ε^k.*

Beweis:

(1) Für $k \in \mathbb{N}$ gelten die Äquivalenzen

$$(a^k)^2 = a \quad \Longleftrightarrow \quad a^{2k-1} = 1 \quad \Longleftrightarrow \quad \operatorname{ord}(a) \mid 2k-1.$$

Gibt es also ein $k \in \mathbb{N}$ mit $(a^k)^2 = a$, so ist $\operatorname{ord}(a)$ ungerade. Ist umgekehrt $\operatorname{ord}(a)$ ungerade und wählt man ein k mit $\operatorname{ord}(a) \mid 2k-1$, so gilt $(a^k)^2 = a$. Die Wahl $k = \frac{\operatorname{ord}(a)+1}{2}$ führt zur letzten Aussage.

(2) Ist $|Q|$ ungerade, so folgt aus $a^{|Q|} = 1$ sofort

$$(a^{\frac{|Q|+1}{2}})^2 = a^{|Q|+1} = a^{|Q|}a = a,$$

was die Behauptung beweist.

(3) Ist die Gruppenordnung $|Q|$ gerade, so gibt es (mindestens) ein Element $\varepsilon \in Q$ mit $\operatorname{ord}(\varepsilon) = 2$, d.h. $\varepsilon^2 = 1$ und $\varepsilon \neq 1$. Dann ist aber $(\varepsilon^k)^2 = 1 \neq \varepsilon$ für alle $k \in \mathbb{N}$, woraus die Behauptung folgt. ∎

SATZ. *Sei p eine ungerade Primzahl und $Q = \{a \in \mathbb{F}_p^* : \left(\frac{a}{p}\right) = 1\}$ die Untergruppe der Quadrate von $\mathbb{F}_p^*$. Sei weiter $\lambda : Q \to \mathbb{N}$ eine Funktion mit*

$$(a^{\lambda(a)})^2 = a \text{ für alle } a \in Q.$$

Dann gilt $p \equiv 3 \bmod 4$ und $a^{\lambda(a)} = a^{\frac{p+1}{4}}$.

Beweis: Es gilt $|Q| = \frac{p-1}{2}$. Das vorangegangene Lemma zeigt, dass $|Q|$ ungerade sein muss, was dann $p \equiv 3 \bmod 4$ impliziert. Nun gilt $(a^{\lambda(a)})^2 = a = (a^{\frac{p+1}{4}})^2$, was zu

$$a^{2\lambda(a)-2\frac{p+1}{4}} = 1 \Longrightarrow \operatorname{ord}_p(a) \mid 2(\lambda(a) - \frac{p+1}{4})$$

führt. Mit $|Q|$ ist auch $\operatorname{ord}_p(a)$ ungerade, sodass $\operatorname{ord}_p(a) \mid \lambda(a) - \frac{p+1}{4}$ und damit $a^{\lambda(a)-\frac{p+1}{4}} = 1$, also

$$a^{\lambda(a)} = a^{\frac{p+1}{4}}$$

folgt. ■

Wir wollen nun auch den Fall von Quadraten in $(\mathbb{Z}/N\mathbb{Z})^*$ mit einer RSA-Zahl $N = pq$ betrachten.

Satz. *Sei $N = pq$ eine RSA-Zahl und*

$$Q = \{b^2 \in (\mathbb{Z}/N\mathbb{Z})^* : b \in (\mathbb{Z}/N\mathbb{Z})^*\}$$

die Untergruppe der Quadrate von $(\mathbb{Z}/N\mathbb{Z})^*$, für die (bekanntlich)

$$Q = \{a \in (\mathbb{Z}/N\mathbb{Z})^* : \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1\} \quad \textit{und} \quad |Q| = \frac{(p-1)(q-1)}{4}$$

gilt.

(1) *Ist $p \equiv 3 \bmod 4$ und $q \equiv 3 \bmod 4$, so ist für $a \in Q$ die Zahl*

$$a^{\frac{(p-1)(q-1)+4}{8}}$$

eine Quadratwurzel von a. Sind $u, v \in \mathbb{Z}$ mit $up + vq = 1$, so gilt auch

$$a^{\frac{(p-1)(q-1)+4}{8}} = a^{\frac{p+1}{4}}vq + a^{\frac{q+1}{4}}up.$$

(2) *Ist $\lambda : Q \to \mathbb{N}$ eine Funktion mit*

$$(a^{\lambda(a)})^2 = a \textit{ für alle } a \in Q,$$

so ist $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$ und

$$a^{\lambda(a)} = a^{\frac{(p-1)(q-1)+4}{8}}.$$

Beweis:

(1) Sei $p \equiv q \equiv 3 \bmod 4$.

(a) Hier ist $|Q| = \frac{p-1}{2} \cdot \frac{q-1}{2}$ eine ungerade Zahl. Nach dem vorangegangenen Lemma ist dann für $a \in Q$

$$a^{\frac{|Q|+1}{2}} = a^{\frac{\frac{(p-1)(q-1)}{4}+1}{2}} = a^{\frac{(p-1)(q-1)+4}{8}}$$

eine Quadratwurzel von a.

(b) Der Einfachkeit halber verwenden wir jetzt die modulo-Schreibweise. Es ist

$$\frac{(p-1)(q-1)+4}{8} - \frac{p+1}{4} = \frac{(p-1)(q-3)}{8} = \frac{p-1}{2} \cdot \frac{q-3}{4}.$$

Es ist $\frac{q-3}{4} \in \mathbb{N}$. Für $a \in Q$ ist $\left(\frac{a}{p}\right) = 1$, also mit dem Satz von Euler $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \bmod p$. Mit $up \equiv 0 \bmod p$ und $vq \equiv 1 \bmod p$ erhalten wir schließlich modulo p

$$\begin{aligned} a^{\frac{(p-1)(q-1)+4}{8}} &\equiv a^{\frac{p+1}{4}+\frac{p-1}{2}\frac{q-3}{4}} \equiv a^{\frac{p+1}{4}} \cdot (a^{\frac{p-1}{2}})^{\frac{q-3}{4}} \equiv a^{\frac{p+1}{4}} \equiv \\ &\equiv a^{\frac{p+1}{4}}vq + a^{\frac{q+1}{4}}up \bmod p. \end{aligned}$$

Genauso ergibt sich

$$a^{\frac{(p-1)(q-1)+4}{8}} \equiv a^{\frac{p+1}{4}}vq + a^{\frac{q+1}{4}}up \bmod q,$$

was zusammen dann

$$a^{\frac{(p-1)(q-1)+4}{8}} \equiv a^{\frac{p+1}{4}}vq + a^{\frac{q+1}{4}}up \bmod N,$$

also die Behauptung ergibt.

(2) Sei jetzt $\lambda : Q \to \mathbb{N}$ eine Funktion mit $(a^{\lambda(a)})^2 = a$ für alle $a \in Q$. Nach dem vorangegangenen Lemma muss dann $|Q| = \frac{p-1}{2}\frac{q-1}{2}$ ungerade sein, was genau für $p \equiv q \equiv 3 \bmod 4$ der Fall ist. Der Rest folgt wie beim letzten Beweis. ■

16. Blum-Goldwasser-Verschlüsselung

LEMMA. *Sei p eine Primzahl mit $p \equiv 3 \bmod 4$ und*

$$Q = \{a \in \mathbb{F}_p^* : \left(\frac{a}{p}\right) = 1\}$$

die Untergruppe der Quadrate in $\mathbb{F}_p^*$.

(1) *Die Abbildung $Q \to Q$ mit $x \mapsto x^2$ ist bijektiv mit $x \mapsto x^{\frac{p+1}{4}}$ als Umkehrabbildung.*
(2) *Ist $x_0 \in Q$ und definiert man rekursiv $x_i = x_{i-1}^2$ für $i \geq 1$, so gilt $x_i = x_0^{2^i}$ und*

$$x_0 = x_i^{(\frac{p+1}{4})^i} = x_i^{(\frac{p+1}{4})^i \bmod (p-1)}.$$

Beweis:

(1) Für $x \in Q$ ist $x^{\frac{p-1}{2}} = \left(\frac{x}{p}\right) = 1$, sodass die Behauptung sofort aus

$$\left(x^2\right)^{\frac{p+1}{4}} = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}} \cdot x = x$$

folgt.

(2) Die Aussage $x_i = x_0^{2^i}$ folgt sofort durch Induktion. Die zweite Aussage ergibt sich ebenfalls durch Induktion, wobei der Fall $i = 0$ klar ist. Setzen wir

$$x_0 = x_{i-1}^{(\frac{p+1}{4})^{i-1}}$$

voraus, so folgt aus $x_i = x_{i-1}^2$ zunächst $x_{i-1} = x_i^{\frac{p+1}{4}}$, was eingesetzt dann

$$x_0 = x_i^{(\frac{p+1}{4})^i}$$

ergibt. Da man im Exponenten modulo $p-1$ rechnen darf, ist auch die zweite Aussage klar. ■

LEMMA. *Sei $N = pq$ eine RSA-Zahl mit Primzahlen $p \equiv q \equiv 3 \bmod 4$ und Q die Untergruppe der Quadrate in $(\mathbb{Z}/N\mathbb{Z})^*$, die sich auch in der Form*

$$Q = \{a \in (\mathbb{Z}/N\mathbb{Z})^* : \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1\}$$

schreiben lässt. Seien $u, v \in \mathbb{Z}$ mit $up + vq = 1$.

(1) *Die Abbildung $Q \to Q$ mit $x \mapsto x^2$ ist bijektiv mit Umkehrabbildung*

$$x \mapsto x^{\frac{(p-1)(q-1)+4}{8}},$$

die sich auch in der Form

$$x \mapsto x^{\frac{p+1}{4}}vq + x^{\frac{q+1}{4}}up$$

schreiben lässt.

(2) *Sei $x_0 \in \mathbb{Z}$ ein Quadrat modulo N mit $\mathrm{ggT}(x_0, N) = 1$. Rekursiv wird eine Folge x_i durch $x_i = x_{i-1} \bmod N$ definiert. Dann gilt $x_i = x_0^{2^i} \bmod N$ und*

$$x_{i-1} = x_i^{\frac{(p-1)(q-1)+4}{8}} \bmod N \quad (\textit{oder alternativ } x_{i-1} = x_i^{\frac{p+1}{4}}vq + x_i^{\frac{q+1}{4}}up \bmod N)$$

und

$$x_0 = x_i^{(\frac{(p-1)(q-1)+4}{8})^i} \bmod N \quad (\textit{oder alternativ } x_0 = vqx^{(\frac{p+1}{4})^i} + upx^{(\frac{q+1}{4})^i} \bmod N).$$

Dies kann man auch in der Form

$$x_0 = vq(x^{(\frac{p+1}{4})^i \bmod (p-1)} \bmod p) + up(x^{(\frac{q+1}{4})^i \bmod (q-1)} \bmod q) \bmod N$$

---

schreiben.

Beweis:

(1) Dies wurde praktisch bereits im letzten Abschnitt bewiesen.
(2) Die Darstellung

$$x_{i-1} = x_i^{\frac{(p-1)(q-1)+4}{8}} \bmod N \quad \text{ und damit } x_0 = x_i^{(\frac{(p-1)(q-1)+4}{8})^i} \bmod N$$

folgt sofort aus (1). Zur zweiten Darstellung: Aus $x_i \equiv x_{i-1}^2 \bmod p$ folgt mit dem letzten Lemma $x_0 \equiv x_i^{(\frac{p+1}{4})^i} \bmod p$, was sich wegen $vq \equiv 1 \bmod p$ und $up \equiv 0 \bmod p$ auch in der Form

$$x_0 \equiv vqx^{(\frac{p+1}{4})^i} + upx^{(\frac{q+1}{4})^i} \bmod p$$

schreiben lässt. Das gleiche gilt natürlich modulo q, was dann zusammengesetzt die Behauptung liefert. ■

Bemerkung: Mit den Bezeichnungen des vorangegangenen Lemmas gilt für Indizes $i < j$

$$x_j = x_i^{2^{j-i}} \bmod N \quad \text{ und } \quad x_i = x_j^{(\frac{(p-1)(q-1)+4}{8})^{j-i}} \bmod N.$$

(Beim praktischen Rechnen sollte man natürlich den Exponenten modulo $(p-1)(q-1)$ reduzieren oder getrennt modulo p und modulo q rechnen.)

Bei der im letzten Lemma betrachteten Zahlenfolge ist x_{i-1} eine Quadratwurzel von x_i. Wie wir zuvor gesehen haben, kann man aber Quadratwurzeln modulo N praktisch nicht berechnen, wenn man die Faktorisierung von N nicht kennt. Dies wird nun in folgendem Verschlüsselungsverfahren ausgenutzt.

Blum-Goldwasser-Verschlüsselung:

(1) **Schlüsselerzeugung:** A wählt sich Primzahlen $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$, setzt $N = pq$ und gibt N als seinen öffentlichen Schlüssel bekannt.
(2) **Verschlüsselung:** B will eine Nachricht an A schicken.
   (a) Es wird ein $n \in \mathbb{N}$ und ein Verfahren vereinbart, wie ein Text in eine Zahlenfolge $a_0, a_1, \ldots, a_{\ell-1}$ mit $a_i \in \{0, 1, \ldots, n-1\}$ übersetzt wird. (Im Fall $n = 2$ hat man eine Bitfolge.) B wandelt die Nachricht also in eine Zahlenfolge $a_0, a_1, \ldots, a_{\ell-1}$ mit $0 \le a_i \le n-1$ um.
   (b) B wählt eine Zufallszahl z mit $\mathrm{ggT}(z, N) = 1$, berechnet $x_0 = z^2 \bmod N$ und rekursiv $x_i = x_{i-1}^2 \bmod N$ für $i = 1, \ldots, \ell$ und dazu $z_i = x_i \bmod n$.
   (c) B berechnet nun $b_i = a_i + z_i \bmod n$ und schickt die Zahlenfolge $b_0, b_1, \ldots, b_{\ell-1}, x_\ell$ als Chiffretext an A.
(3) **Entschlüsselung:** A erhält die Zahlenfolge $b_0, \ldots, b_{\ell-1}, x_\ell$. *A* berechnet sich mit dem erweiterten euklidischen Algorithmus $u, v \in \mathbb{Z}$ mit $up + vq = 1$ und damit

$$x_0 = vqx_\ell^{(\frac{p+1}{4})^\ell \bmod (p-1)} + upx_\ell^{(\frac{q+1}{4})^\ell \bmod (q-1)} \bmod N,$$

oder mit der Formel

$$x_0 = x_\ell^{(\frac{(p-1)(q-1)+4}{8})^\ell \bmod (p-1)(q-1)} \bmod N,$$

dann rekursiv

$$z_i = x_i \bmod n, \quad a_i = b_i - z_i \bmod n, \quad x_{i+1} = x_i^2 \bmod N.$$

Bemerkung: Die Blum-Goldwasser-Verschlüsselung ist eine Stromchiffrierung, wobei mit $x_0 = z^2 \bmod N$, $x_i = x_{i-1}^2 \bmod N$, $z_i = x_i \bmod n$ eine Pseudozufallszahlenfolge erzeugt wird. Aus der Kenntnis von x_ℓ kann man nicht auf $x_{\ell-1}, x_{\ell-2}, \ldots$ schließen, wenn man keine Wurzeln ziehen kann.

Beispiel: Wir verwenden nur Großbuchstaben, die wir wie üblich mit $0, \dots, 25$ identifizieren. Wir wählen $n = 26$ und als öffentlichen Schlüssel $N = 5561$. Wir verschlüsseln `KRYPTOGRAPHIE`, wählen den Startwert $z = 1617$, dazu $x_0 = 1019 = z^2 \bmod N$.

	K	R	Y	P	T	O	G	R	A	P	H	I	E	
a_i	10	17	24	15	19	14	6	17	0	15	7	8	4	
x_i	1019	4015	4447	893	2226	225	576	3677	1538	2019	148	5221	4380	4511
z_i	5	11	1	9	16	17	4	11	4	17	18	21	12	13
b_i	15	2	25	24	9	5	10	2	4	6	25	3	16	
	P	C	Z	Y	J	F	K	C	E	G	Z	D	Q	

Der Chiffretext ist also `PCZYJFKCEGZDQ4511`.
Zum Entschlüsseln brauchen wir die Faktorisierung $N = 67 \cdot 83$. Da wir $\ell = 13$ Zeichen verschlüsselt haben, erhalten wir mit $x_\ell = 4511$

$$x_0 = x_\ell^{(\frac{(p-1)(q-1)+4}{8})^\ell} \bmod N = 4511^{677^{13}} \bmod N = 1019.$$

Der Rest ist klar.

17. Identitätsbasierte Kryptographie nach Cocks

Ist es möglich, ein Public-Key-Verschlüsselungsverfahren so zu konstruieren, dass man als öffentlichen Schlüssel einer Person beispielsweise einfach deren E-Mail-Adresse verwenden kann?
Bei den gängigen Public-Key-Verschlüsselungsverfahren wie RSA ist dies nicht der Fall.
Die Frage wurde 1984 von Shamir gestellt, erste Lösungen gab es 2001, eine mit elliptischen Kurven, die andere mit quadratischen Resten, die auf Cocks zurückgeht und hier vorgestellt werden soll.

Identitätsbasierte Verschlüsselung nach Cocks:

(1) **Vorbereitungen**

(a) Man braucht eine **vertrauenswürdige Zentrale** (**trusted third party**), die sich verschiedene ungerade Primzahlen p und q wählt mit $p \equiv 3 \bmod 8$ und $q \equiv 7 \bmod 8$, sodass $N = pq$ praktisch nicht zu faktorisieren ist. Die Wahl von p und q impliziert

$$\left(\frac{-1}{p}\right) = -1, \quad \left(\frac{-1}{q}\right) = -1, \quad \left(\frac{2}{N}\right) = -1.$$

(b) Man braucht eine Hashfunktion H, die beliebig langen Zeichenketten eine Zahl aus $\{0, 1, \dots, N-1\}$ zuordnet mit $\left(\frac{H(z)}{N}\right) = 1$. Ist $\widetilde{H}$ eine beliebige Hashfunktion mit Werten in $\mathbb{N}_0$, so kann man beispielsweise

$$H(z) = \begin{cases} \widetilde{H}(z) \bmod N, & \text{falls } \left(\frac{\widetilde{H}(z)}{N}\right) = 1, \\ 2\widetilde{H}(z) \bmod N, & \text{falls } \left(\frac{\widetilde{H}(z)}{N}\right) = -1 \end{cases}$$

wählen. (Der Fall $\left(\frac{\widetilde{H}(z)}{N}\right) = 0$ sollte praktisch nicht auftreten.) Durch die Wahl von N und die Definition von H ist gewährleistet, dass (praktisch immer)

$$\left(\frac{H(z)}{N}\right) = 1$$

gilt.

(2) **Schlüssel**

(a) Einer Person A ist eine Zeichenkette zugeordnet, beispielsweise die E-Mail-Adresse, das als **öffentlicher Schlüssel** verwendet werden soll. Daraus kann jeder berechnen

$$f_A = H(\text{E-Mail-Adresse}(A)).$$

Dies bezeichnen wir hier als öffentlichen Schlüssel von A.

(b) Die vertrauenswürdige Zentrale berechnet für A

$$e_A = f_A^{\frac{N+5-(p+q)}{8}} \bmod N$$

und gibt diese Zahl als **privaten Schlüssel** an A. (Es gilt $e_A^2 \equiv \pm f_A \bmod N$.)

(3) **Verschlüsselung**

(a) Eine Person B will eine Nachricht an eine Person A schicken. Er wandelt die Nachricht (nach einem vereinbarten Schema) in eine Bitfolge $a_i \in \{0,1\}$ um.

(b) B bestimmt den öffentlichen Schlüssel von A:

$$f_A = H(\text{E-Mail-Adresse}(A)).$$

(c) Für jedes a_i wählt B zufällig Zahlen x_i und y_i mit $0 \le x_i \le N-1$ und $0 \le y_i \le N-1$ und

$$\left(\frac{x_i}{N}\right) = \left(\frac{y_i}{N}\right) = (-1)^{a_i}.$$

Dann berechnet B

$$b_i = (x_i + \frac{f_A}{x_i}) \bmod N \quad \text{und} \quad c_i = (y_i - \frac{f_A}{y_i}) \bmod N$$

und schickt die Zahlenfolgen b_i, c_i (Chiffretext) an A.

(4) **Entschlüsselung**

(a) Mit seinem privaten Schlüssel e_A berechnet sich A aus den Zahlenfolgen b_i, c_i

$$a_i = \begin{cases} \frac{1}{2}(1 - (\frac{b_i+2e_A}{N})), & \text{falls } e_A^2 \equiv f_A \bmod N, \\ \frac{1}{2}(1 - (\frac{c_i-2e_A}{N})), & \text{falls } e_A^2 \equiv -f_A \bmod N. \end{cases}$$

Anschließend wandelt A die Bitfolge a_i in die Nachricht um.

Das folgende Lemma begründet das Funktionieren des obigen Verfahrens:

LEMMA. *Sei $N = pq$ eine RSA-Zahl mit $p \equiv 3 \bmod$ und $q \equiv 7 \bmod 8$, seien $e, f \in \mathbb{Z}$ mit*

$$\left(\frac{f}{N}\right) = 1 \quad \textit{und} \quad e \equiv f^{\frac{N+5-p-q}{8}} \bmod N.$$

(1) *Für $h \in \mathbb{Z}$ gilt die Implikation*

$$\left(\frac{h}{N}\right) = -1 \quad \Longrightarrow \quad \left(\frac{2h}{N}\right) = 1.$$

(2) *Es ist $\left(\frac{f}{p}\right) = \left(\frac{f}{q}\right)$.*

(3) *Es ist*

$$e^2 \equiv \begin{cases} f \bmod N, & \textit{falls } \left(\frac{f}{p}\right) = \left(\frac{f}{q}\right) = 1, \\ -f \bmod N, & \textit{falls } \left(\frac{f}{p}\right) = \left(\frac{f}{q}\right) = -1. \end{cases}$$

(4) *Ist $e^2 \equiv f \bmod N$ und sind $a \in \{0,1\}$, $x, b \in \mathbb{Z}$ mit*

$$\left(\frac{x}{N}\right) = (-1)^a \quad \textit{und} \quad b \equiv (x + \frac{f}{x}) \bmod N,$$

so gilt

$$\left(\frac{b+2e}{N}\right) = \left(\frac{x}{N}\right) \quad \textit{und} \quad a = \frac{1}{2}(1 - \left(\frac{b+2e}{N}\right)).$$

(5) *Ist $e^2 \equiv -f \bmod N$ und sind $a \in \{0,1\}$, $y, c \in \mathbb{Z}$ mit*

$$\left(\frac{y}{N}\right) = (-1)^a \quad \textit{und} \quad c \equiv (y - \frac{f}{y}) \bmod N,$$

so gilt

$$\left(\frac{c-2e}{N}\right) = \left(\frac{y}{N}\right) \quad \textit{und} \quad a = \frac{1}{2}(1 - \left(\frac{c-2e}{N}\right)).$$

Beweis:

(1) Wegen $p \equiv 3 \bmod 8$ und $q \equiv 7 \bmod 8$ ist $N \equiv 5 \bmod 8$, also $\left(\frac{2}{N}\right) = -1$, was sofort die Behauptung beweist.
(2) Wegen $\left(\frac{f}{N}\right) = 1$ und $\left(\frac{f}{N}\right) = \left(\frac{f}{p}\right)\left(\frac{f}{q}\right)$ folgt sofort $\left(\frac{f}{p}\right) = \left(\frac{f}{q}\right)$.
(3) Modulo p gilt

$$e^2 \equiv f^{\frac{N+5-(p+q)}{4}} \equiv f^{\frac{(p-1)(q-1)+4}{4}} \equiv f \cdot \left(f^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} \equiv f \cdot \left(\frac{f}{p}\right)^{\frac{q-1}{2}} \equiv \left(\frac{f}{p}\right) \cdot f \bmod p$$

und analog

$$e^2 \equiv \left(\frac{f}{q}\right) \cdot f \bmod q,$$

was wegen $\left(\frac{f}{p}\right) = \left(\frac{f}{q}\right)$ zu

$$e^2 \equiv \left(\frac{f}{p}\right) \cdot f \bmod N$$

zusammengefasst werden kann.
(4) Sei $e^2 \equiv f \bmod N$. Wegen

$$x \cdot (1 + \frac{e}{x})^2 \equiv x \cdot (1 + \frac{2e}{x} + \frac{e^2}{x^2}) \equiv x + 2e + \frac{f}{x} \equiv b + 2e \bmod N$$

gilt

$$\left(\frac{b+2e}{N}\right) = \left(\frac{x}{N}\right) = (-1)^a.$$

Der Rest folgt aus

$$a = \frac{1}{2}(1 - (-1)^a) \text{ für } a \in \{0, 1\}.$$

(5) Sei $e^2 \equiv -f \bmod N$. Wegen

$$y \cdot (1 - \frac{e}{y})^2 \equiv y \cdot (1 - \frac{2e}{y} + \frac{e^2}{y^2}) \equiv y - 2e - \frac{f}{y} \equiv c - 2e \bmod N$$

gilt

$$\left(\frac{c-2e}{N}\right) = \left(\frac{y}{N}\right) = (-1)^a.$$

Der Rest folgt aus

$$a = \frac{1}{2}(1 - (-1)^a) \text{ für } a \in \{0, 1\}.$$

Dies beweist die Behauptungen. ■

Beispiel: Wir wählen Primzahlen $p \equiv 3 \bmod 8$, $q \equiv 7 \bmod 8$ und berechnen $N = pq$:

$$\begin{aligned} p &= 64589236458273645892364582634852634854 19, \\ q &= 76903478590687345908673490857693847575 51, \\ N &= 49671369631576899026686401886421066442656606745398853283533620414605450538648869 \end{aligned}$$

Ist $z_1 \dots z_n$ eine Zeichenkette, so wählen wir

$$\widetilde{H}(z_1 \dots z_n) = \sum_{i=1}^{n} \text{ord}\,(z_i) \cdot 256^{n-i},$$

wobei hier $\text{ord}\,(z_i)$ den Unicode-Wert des Zeichens z_i bezeichnet, wie in Python3. Damit definieren wir

$$H(z_1 \dots z_n) = \begin{cases} \widetilde{H}(z_1 \dots z_n) \bmod N, & \text{falls } \left(\frac{\widetilde{H}(z_1 \dots z_n)}{N}\right) = 1, \\ 2\widetilde{H}(z_1 \dots z_n) \bmod N, & \text{falls } \left(\frac{\widetilde{H}(z_1 \dots z_n)}{N}\right) = -1. \end{cases}$$

Wir berechnen

$$h = \widetilde{H}(\text{wolfgang.ruppert@fau.de}) = 114396240425157978983067263436403491184206448318825360 37$$

Da $\left(\frac{h}{N}\right) = 1$ ist, ist

$$f = H(\text{wolfgang.ruppert@fau.de}) = 114396240425157978983067263436403491184206448318825360 37$$

der öffentliche Schlüssel. Den zugehörigen privaten Schlüssel erhält man aus der Formel

$$e = f^{\frac{N+5-p-q}{8}} \bmod N$$

mit dem Wert

$$e = 4944608884211242244995000278936719343619164986511949112508247435327558637680375 6.$$

Wir wollen nun die Zahl 2017 verschlüsseln. Die zugehörige Binärdarstellung ist

$$2017 = (1,1,1,1,1,1,0,0,0,0,1)_2.$$

Die einzelnen Bits bezeichnen wir mit $a_1, \ldots, a_{11}$. Für jedes a_i wählen wir Zufallszahlen x_i, y_i mit $\left(\frac{x_i}{N}\right) = \left(\frac{y_i}{N}\right) = (-1)^{a_i}$:

$$\begin{aligned}
x_1 &= 291884009586238713116361997015654066893099991288771150752449396692038655253950 00,\\
x_2 &= 224096300058687044945286415453585239995624406927660151331031803563852536776 23108,\\
x_3 &= 247856526763007415663535012035003610509249932325094233027324670788750472399035 05,\\
x_4 &= 327253723030393623748586345377809004391903264978240889786032432612867590034910 19,\\
x_5 &= 339272778054009773739062240819984578587796279126043641576987516860312161787699,\\
x_6 &= 384587699676143969123258071822043343567585234449630475072512618060078162217343 64,\\
x_7 &= 366330993630065440622220791328195691666094048562047150329079177676475648616810 48,\\
x_8 &= 128873742626914811380802012453009310584866683250330130950465851760173879933770 5,\\
x_9 &= 169105510803802111290428807465892004704715710805725801195326465801163424545195 11,\\
x_{10} &= 486352050564423628603447537401379973631152017075436163806581953970434822978464 35,\\
x_{11} &= 310245931342358149692693814648545340826130528788625092037142789662174023265189 61,\\
y_1 &= 338131873125183102471243467149736075643582869489733501650459711725356771679276 66,\\
y_2 &= 422308594784488087077871383730818021204992584233487080785354224945572123888419 53,\\
y_3 &= 470886410389818148586277454422586615382584369350065575005339050514047170463236 49,\\
y_4 &= 181775666949315622108271067512565751467030403860921475756313961379042171697298 39,\\
y_5 &= 715089368574216010908938705217712733057662850065698498993073277424657486246911 4,\\
y_6 &= 346748386284133377738174671851410174821593593384746280202291935481389681310382 44,\\
y_7 &= 373553074502812375699879160304712756086491407851316825386288577903023232440576 256,\\
y_8 &= 140233487250840383744420794207877902500805942919842292472715810095066972798625 72,\\
y_9 &= 156093502145344098437481218145370764759558447159863924338448264079315654455393 83,\\
y_{10} &= 383525248760014326077918110784221054660604814624202785853900011308084085704273 34,\\
y_{11} &= 244736696765553346333503370949718097699562191710339644703883034398654853995932 2
\end{aligned}$$

Nun werden mit den Formeln

$$b_i = (x_i + \frac{f}{x_i}) \bmod N \quad \text{und} \quad c_i = (y_i - \frac{f}{y_i}) \bmod N$$

die Zahlen b_i, c_i berechnet:

$$\begin{aligned}
b_1 &= 283884533815411740233773244384999709049881240012065796019557165306333478551379 20,\\
b_2 &= 217374293753129443181738684877048596111263211159916273803089806045772311745493 14,\\
b_3 &= 433306764312231393408237144148205280095089985342876957642226250548196780735396 23,\\
b_4 &= 382142566155031974304579573818847046077901517780979071840394068548564474656656 81,\\
b_5 &= 690374343628204910311860056335593365573137984802484364216204642605550171343988 5,\\
b_6 &= 263915790783570934192127855339724809586634475697816916061519128122519369838991 18,\\
b_7 &= 387106567275834871526265288802277495667969949452768998178570045158391835355405 68,\\
b_8 &= 271155353764876670534056894225543574744236752804291269922151170395904154110701 96,\\
b_9 &= 839565714606172418264557147078101802258296467738574602709029668166215663388 38,\\
b_{10} &= 160413400809546347875634960967300784343124690206133874468811704379674521063508 67,\\
b_{11} &= 464070520693722130968161499397484860763763595379944731754710918451072279084480 89,\\
c_1 &= 967019560574641374964217605962173136905145146852940095811415583594468219868263 4,\\
c_2 &= 755468761010917052669878071517915025144986248152942868367434103715862617952449 0,\\
c_3 &= 234819542420578848789346814897782461417177446116257543349644571818276053906597 1,\\
c_4 &= 439930571825976601125168162690114707385886363127943984845794464661769873700117 14,\\
c_5 &= 403828743468341540378084536445226115302928299075883780717329471309709982156471 9,\\
c_6 &= 720624164854920499385535346961725317347996432621289965153048006037400381020387 0,\\
c_7 &= 397205941209101625576746625545312855459276520870036510094570998705256646156887 56,\\
c_8 &= 493248558440485488886940107135922689307824714257965363936417922857909218218443 2,\\
c_9 &= 262280065115839774374546941576547002739441148810577590834123998898560269381046 19,\\
c_{10} &= 129776921462761791287190662868576907945246911101759801733392453904152993541499 22,\\
c_{11} &= 253659459184666718961198454074420071542797491211248411032685965330403589929299 84
\end{aligned}$$

Nun überprüft man, dass gilt $e^2 + f \equiv 0 \bmod N$, d.h. wir das Entschlüsseln brauchen wir $c_1, \ldots, c_{11}$. Man überprüft, dass tatsächlich

$$a_i = \frac{1}{2}(1 - \left(\frac{c_i - 2e}{N}\right)) \text{ für } i = 1, \ldots, 11$$

gilt.

Bemerkung: Die Zufallszahlen x_i und y_i müssen natürlich verschieden sein. Wäre $x_i = y_i$, so hätte man

$$b_i = x_i + \frac{f_A}{x_i} \bmod N \quad \text{und} \quad c_i = x_i - \frac{f}{y_i} \bmod N,$$

also

$$b_i + c_i \equiv 2 \bmod x_i \bmod N,$$

woraus man x_i und damit aus $\left(\frac{x_i}{N}\right) = (-1)^{a_i}$ auch a_i berechnen kann.

18. Quadratwurzeln modulo p^n

Bemerkung: Will man aus einer reellen Zahl $a > 0$ eine Quadratwurzel berechnen, kann man sich nach Wahl von $x_0 \in \mathbb{R}_{>0}$ durch

$$x_i = \frac{1}{2}(x_{i-1} + \frac{a}{x_{i-1}}) \text{ für } i \geq 1$$

eine Folge konstruieren, die gegen $\sqrt{a}$ konvergiert. Dies lässt sich auch für das Wurzelziehen modulo p^n anwenden:

LEMMA. *Sei p eine ungerade Primzahl $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 1$ und $x_0 \in \mathbb{Z}$ mit $x_0^2 \equiv a \bmod p$. Beginnend mit x_0 wird durch*

$$x_i = \frac{1}{2}(x_{i-1} + \frac{a}{x_{i-1}}) \bmod p^{2^i} \text{ für } i \geq 1$$

rekursiv eine Folge ganzer Zahlen x_i definiert, für die gilt

$$x_i^2 \equiv a \bmod p^{2^i} \text{ für alle } i \geq 0.$$

Beweis:

(1) Ganz allgemein gilt für $y = \frac{1}{2}(x + \frac{a}{x})$

$$y^2 - a = \frac{1}{4}(x^2 + 2a + \frac{a^2}{x^2}) - a = \frac{1}{4}(x^2 - 2a + \frac{a^2}{x^2}) = \frac{1}{4}(x - \frac{a}{x})^2 = \frac{1}{4x^2}(x^2 - a)^2.$$

(2) Wir beweisen dies durch Induktion. Für $i = 0$ gilt nach Voraussetzung $x_0^2 \equiv a \bmod p^{2^0}$ und damit insbesondere $\mathrm{ggT}(x_0, p) = 1$. Sei die Aussage nun bereits für $i-1$ bewiesen. Dann gilt

$$x_{i-1}^2 \equiv a \bmod p^{2^{i-1}}.$$

Insbesondere gilt $\mathrm{ggT}(x_{i-1}, p) = 1$, sodass

$$x_i = \frac{1}{2}(x_{i-1} + \frac{a}{x_{i-1}}) \bmod p^{2^i}$$

wohldefiniert ist. Dann ist

$$2x_i x_{i-1} \equiv x_{i-1}^2 + a \bmod p^{2^i}.$$

Es folgt modulo p^{2^i}

$$\begin{aligned}(x_{i-1}^2 - a)^2 &\equiv x_{i-1}^4 - 2ax_{i-1}^2 + a^2 \equiv x_{i-1}^4 + 2ax_{i-1}^2 + a^2 - 4ax_{i-1}^2 \equiv \\ &\equiv (x_{i-1}^2 + a)^2 - 4ax_{i-1}^2 \equiv 4x_i^2 x_{i-1}^2 - 4ax_{i-1}^2 \equiv \\ &\equiv 4x_{i-1}^2 \cdot (x_i^2 - a) \bmod p^{2^i},\end{aligned}$$

sodass ein $k_i \in \mathbb{Z}$ existiert mit

$$(x_{i-1}^2 - a)^2 = 4x_{i-1}^2 \cdot (x_i^2 - a) + p^{2^i} \cdot k_i.$$

Da $(x_{i-1}^2 - a)^2$ durch $(p^{2^{i-1}})^2 = p^{2^i}$ teilbar ist, folgt

$$x_i^2 - a \equiv 0 \bmod p^{2^i},$$

was zu beweisen war. ■

Beispiel: Wir beginnen mit $p = 13$, $a = -1$ und $x_0 = 8$. (Die Zahl $v_p(x)$ gibt an, wie oft p in x aufgeht.)

x_i	$v_p(x_i^2 - a)$
$x_0 = 8$	1
$x_1 = 99$	2
$x_2 = 28322$	4
$x_3 = 808904403$	8
$x_4 = 651495710876207647$	16
$x_5 = 1220420586853055768566061765292171 75$	32
$x_6 = 1829903588697063030071015872095552142523304062346723025310487382243166 36$	64

SATZ. *Sei p eine ungerade Primzahl, $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(p, a) = 1$.*

(1) *Die Gleichung $x^2 \equiv a \bmod p^n$ ist genau dann lösbar, wenn $\left(\frac{a}{p}\right) = 1$ ist.*

(2) *Im Fall $\left(\frac{a}{p}\right) = 1$, hat die Gleichung $x^2 \equiv a \bmod p^n$ genau zwei Lösungen modulo p^n. Ist x_1 eine Lösung mit $0 \leq x_1 \leq p^n - 1$, so $x_2 = p^n - x_1$ die zweite Lösung zwischen 0 und $p^n - 1$.*

Beweis:

(1) Ist $x^2 \equiv a \bmod p^n$ lösbar, so natürlich auch $x^2 \equiv a \bmod p$, was wegen $\mathrm{ggT}(p,a) = 1$ sofort $\left(\frac{a}{p}\right) = 1$ zeigt.

(2) Sei umgekehrt $\left(\frac{a}{p}\right) = 1$. Mit Hilfe des vorangegangenen Lemmas finden wir ganze Zahlen x_i mit

$$x_i^2 \equiv a \bmod p^{2^i}.$$

Wählen wir einen Index i mit $2^i \geq n$, so folgt offensichtlich

$$x_i^2 \equiv a \bmod p^n.$$

Dann ist

$$y_1 = x_i \bmod p^n$$

eine Lösung der Gleichung $x^2 \equiv a \bmod p^n$ mit $0 \leq y_1 \leq p^n - 1$ was die Lösbarkeit der Gleichung $x^2 \equiv a \bmod p^n$ zeigt.

(3) Sei y eine weitere Lösung, d.h. $y^2 \equiv a \bmod p^n$. Es folgt $y^2 \equiv y_1^2 \bmod p^n$ und damit

$$p^n \mid y^2 - y_1^2 = (y - y_1)(y + y_1).$$

Würde p in $y - y_1$ und $y + y_1$ aufgehen, so würde $p \mid 2y_1$, ein Widerspruch folgen. Also bleiben nur zwei Fälle:

$$y \equiv y_1 \bmod p^n \quad \text{oder} \quad y \equiv -y_1 \bmod p^n.$$

Zwischen 0 und $p^n - 1$ gibt es dann die beiden Lösungen y_1 und $p^n - y_1$. Dies beweist die Behauptung. ■

Dies führt sofort zu folgendem Algorithmus:

Quadratwurzel modulo p^n für eine ungerade Primzahl:

Eingabe: Ungerade Primzahl p, $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 1$

Ausgabe: $x \in \mathbb{Z}$ mit $x^2 \equiv a \bmod p^n$ und $0 \leq x \leq p^n - 1$

1: Bestimme mit einem Quadratwurzelalgorithmus eine Lösung x der Gleichung $x^2 \equiv a \bmod p$
2: $i \leftarrow 0$
3: **while** $2^i < n$ **do**
4: $\quad i \leftarrow i + 1$
5: $\quad x \leftarrow \frac{1}{2}(x + \frac{a}{x}) \bmod p^{2^i}$
6: **end while**
7: **return** $x \bmod p^n$

Wir wollen nun die Gleichung $x^2 \equiv a \bmod 2^n$ untersuchen, wobei wir $\mathrm{ggT}(a,2) = 1$ voraussetzen. Der Fall $n = 1$ ist klar, da dann $a \equiv 1 \equiv 1^2 \bmod 2$ gilt. Für $n = 2$ muss $a \equiv 1 \bmod 4$ gelten, da $1^2 \equiv 3^2 \equiv 1 \bmod 4$ gilt. Ist $n \geq 3$ und $x^2 \equiv a \bmod 2^n$, so folgt $x^2 \equiv a \bmod 8$. Wegen $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$ muss dann notwendigerweise $a \equiv 1 \bmod 8$ gelten. Das folgende Lemma zeigt, dass diese Bedingung auch hinreichend ist.

LEMMA. *Sei $a \in \mathbb{Z}$ mit $a \equiv 1 \bmod 8$ und $x_0 \in \mathbb{Z}$ mit $x_0^2 \equiv a \bmod 8$, z.B. $x_0 = 1$. Rekursiv wird dann durch*

$$x_i = \frac{1}{x_{i-1}} \cdot \frac{x_{i-1}^2 + a}{2} \bmod 2^{2^i+2}$$

eine Folge ganzer Zahlen definiert, die

$$x_i^2 \equiv a \bmod 2^{2^i+2}$$

erfüllen. (Alle x_i sind ungerade, sodass $\frac{x_{i-1}+a}{2}$ als ganze Zahl berechnet werden kann.)

Beweis: Wir nehmen an, wir wissen, dass $x_{i-1}^2 \equiv a \bmod 2^{2^{i-1}+2}$ gilt. (Für $i = 1$ ist dies die Voraussetzung.) Da a ungerade ist, ist es auch x_{i-1}, sodass $\frac{x_{i-1}^2+a}{2}$ eine ganze Zahl (2 ist ja nicht invertierbar modulo 2.) und x_{i-1} invertierbar modulo 2^{2^i+2} ist. Daher können wir definieren

$$x_i = \frac{1}{x_{i-1}} \cdot \frac{x_{i-1}^2 + a}{2} \bmod 2^{2^i+2}.$$

Multiplikation mit x_{i-1} und anschließendes Quadrieren liefert

$$x_{i-1}x_i \equiv \frac{x_{i-1}^2 + a}{2} \bmod 2^{2^i+2} \quad \text{und} \quad x_{i-1}^2 x_i^2 \equiv \left(\frac{x_{i-1}^2 + a}{2}\right)^2 \bmod 2^{2^i+2}.$$

Nach Multiplikation mit $4 = 2^2$ erhält man

$$4x_{i-1}^2 x_i^2 \equiv (x_{i-1}^2 + a)^2 \bmod 2^{2^i+4}.$$

Es folgt

$$\begin{aligned}(x_{i-1}^2 - a)^2 &\equiv x_{i-1}^4 - 2ax_{i-1}^2 + a^2 \equiv x_{i-1}^4 + 2ax_{i-1}^2 + a^2 - 4ax_{i-1}^2 \equiv \\ &\equiv (x_{i-1}^2 + a)^2 - 4ax_{i-1}^2 \equiv 4x_{i-1}^2 x_i^2 - 4ax_{i-1}^2 \equiv 4x_{i-1}^2(x_i^2 - a) \bmod 2^{2^i+4}.\end{aligned}$$

$x_{i-1}^2 - a$ ist durch $2^{2^{i-1}+2}$ teilbar, die linke Seite also durch 2^{2^i+4}, somit auch die rechte Seite. Daher muss $x_i^2 - a$ durch 2^{2^i+2} teilbar sein, wie behauptet. ■

Beispiel: Wir wählen $a = 17$ und berechnen die ersten Folgenglieder der im Lemma definierten Folge x_i:

x_i	$v_2(x_i^2 - a)$
$x_0 = 1$	4
$x_1 = 9$	6
$x_2 = 41$	7
$x_3 = 745$	11
$x_4 = 206569$	21
$x_5 = 13754377961$	37
$x_6 = 9629331466073876201$	67
$x_7 = 741279623515331529177541076053478549225$	131
$x_8 = 167964809619010748940859056355957030747918591173264760320123412936723094775529$	260

Kann man alle Lösungen der Gleichung $x^2 \equiv a \bmod 2^n$ beschreiben? Wir beginnen mit einem Beispiel:

Beispiel: Durch Probieren findet man, dass die Lösungen der Gleichung $x^2 \equiv 17 \bmod 2^{10}$ die Zahlen

$$233, \quad 279, \quad 745, \quad 791$$

sind. Außerdem gilt

$$233 + 791 = 2^{10} \quad \text{und} \quad 279 + 745 = 2^{10}$$

und

$$745 - 233 = 2^9 \quad \text{und} \quad 791 - 279 = 2^9.$$

SATZ. *Sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, 2) = 1$.*

(1) *Gilt $x^2 \equiv a \bmod 2^n$ mit $n \geq 3$, so ist $a \equiv 1 \bmod 8$.*
(2) *Sei nun $a \in \mathbb{Z}$ mit $a \equiv 1 \bmod 8$ und $n \geq 3$.*
   (a) *Es gibt ein $x_n \in \mathbb{Z}$ mit $x_n^2 \equiv a \bmod 2^n$ und $0 \leq x_n \leq 2^n - 1$.*
   (b) *Gilt $\widetilde{x}^2 \equiv a \bmod 2^n$, so folgt*

$$\widetilde{x} \equiv x_n \bmod 2^{n-1} \quad \text{oder} \quad \widetilde{x} \equiv -x_n \bmod 2^{n-1}.$$

   (c) *Gilt $\widetilde{x}^2 \equiv a \bmod 2^n$, so gilt auch $(\widetilde{x} + 2^{n-1})^2 \equiv a \bmod 2^n$.*

(d) *Die Gleichung* $x^2 \equiv a \bmod 2^n$ *hat für* $n \geq 3$ *(mit* $a \equiv 1 \bmod 8$*) modulo* 2^n *genau die vier Lösungen*

$$x_n, \quad -x_n, \quad x_n + 2^{n-1}, \quad -x_n + 2^{n-1}.$$

(Die Lösungen sind modulo 2^n *verschieden. Man kann die Lösungen auch als* $x_n, 2^{n-1} - x_n, 2^{n-1} + x_n, 2^n - x_n$ *schreiben.)*

Beweis:

(1) Dies wissen wir bereits.

(2) (a) Betrachtet man die Folge x_i des Lemmas, so gilt

$$x_i^2 \equiv a \bmod 2^{2^i+2}.$$

Wählt man nun einen Index i mit $2^i + 2 \geq n$, setzt man $y = x_i \bmod 2^n$, so folgt $y^2 \equiv a \bmod 2^n$. Im Weiteren wechseln wir die Bezeichnungen und schreiben x_n für y, sodass gilt

$$x_n^2 \equiv a \bmod 2^n.$$

(b) Es gelte $\widetilde{x}^2 \equiv a \bmod 2^n$. Dann folgt $\widetilde{x}^2 \equiv x_n^2 \bmod 2^n$, also $2^n \mid (\widetilde{x} - x_n)(\widetilde{x} + x_n)$. Es gilt

$$\mathrm{ggT}(\widetilde{x} - x_n, \widetilde{x} + x_n, 2^n) = \mathrm{ggT}(\widetilde{x} - x_n, \widetilde{x} + x_n, 2x_n, 2^n) = 2.$$

Daraus folgt aber

$$\widetilde{x} \equiv x_n \bmod 2^{n-1} \quad \text{oder} \quad \widetilde{x} \equiv -x_n \bmod 2^{n-1}.$$

(c) Mit $\widetilde{x}^2 \equiv a \bmod 2^n$ folgt auch für $n \geq 2$

$$(\widetilde{x} + 2^{n-1})^2 = \widetilde{x}^2 + \widetilde{x} \cdot 2^n + 2^{n+n-2} \equiv \widetilde{x}^2 \equiv a \bmod 2^n.$$

(d) Dass $x_n, -x_n, x_n + 2^{n-1}, -x_n + 2^{n-1}$ Lösungen sind, ist nach den vorangegangenen Aussagen klar. Dass die Lösungen paarweise verschieden sind, überlegt man sich auch leicht. Sei jetzt $\widetilde{x}$ eine Lösung von $\widetilde{x}^2 \equiv a \bmod 2^n$. Nach (3) folgt $\widetilde{x} \equiv \varepsilon x_n \bmod 2^{n-1}$ für ein $\varepsilon \in \{\pm 1\}$. Wir schreiben $\widetilde{x} = \varepsilon x_n + k \cdot 2^{n-1}$ mit $k \in \mathbb{Z}$. Da wir nur an Lösungen modulo 2^n interessiert sind, können wir $k \in \{0, 1\}$ annehmen, was dann sofort die Behauptung liefert. ■

Wir haben gesehen, wie man die Gleichung $x^2 \equiv a \bmod p^n$ im Fall $\mathrm{ggT}(p, a) = 1$ explizit lösen kann. Nun betrachten wir den Allgemeinfall der Gleichung $x^2 \equiv a \bmod p^n$:

SATZ. *Sei* p *eine Primzahl, auch* $p = 2$ *ist zugelassen, und* $n \in \mathbb{N}$. *Sei* $a \in \mathbb{Z}$ *mit* $0 \leq a \leq p^n - 1$.

(1) **Fall** $a = 0$**:** *Es gilt*

$$\begin{aligned} x^2 \equiv 0 \bmod p^n \quad &\iff \quad p^{\lceil \frac{n}{2} \rceil} \mid x \quad \iff \\ &\iff \quad x \bmod p^n \in \{p^{\lceil \frac{n}{2} \rceil} \cdot k : k \in \{0, 1, \ldots, p^{\lfloor \frac{n}{2} \rfloor} - 1\}\}. \end{aligned}$$

Insbesondere hat die Gleichung $x^2 \equiv 0 \bmod p^n$ *genau* $p^{\lfloor \frac{n}{2} \rfloor}$ *Lösungen modulo* p^n.

(2) **Fall** $a = p^\ell b$ **mit** $p \nmid b$ **und** $0 \leq \ell \leq n - 1$**:** *Die Gleichung* $x^2 \equiv a \bmod p^n$ *ist genau dann lösbar, wenn*

$$\ell \equiv 0 \bmod 2$$

und

$$\left(\frac{b}{p}\right) = 1 \text{ im Fall } p > 2 \quad \text{und} \quad b \equiv \begin{cases} 1 \bmod 2, & \text{falls } \ell = n - 1, \\ 1 \bmod 4, & \text{falls } \ell = n - 2, \\ 1 \bmod 8, & \text{falls } \ell \leq n - 3 \end{cases} \quad \text{im Fall } p = 2$$

gilt.

(3) **Fall $a = p^\ell b$ mit $p \nmid b$, $\ell \equiv 0 \bmod 2$ und $0 \le \ell \le n-1$:** *Seien $y_1, \dots, y_r$ die Lösungen von $y^2 \equiv b \bmod p^{n-\ell}$ mit $0 \le y_i \le p^{n-\ell} - 1$. Dabei ist*

$$r = \begin{cases} 2 & \text{im Fall } p > 2 \text{ und } \left(\frac{b}{p}\right) = 1, \\ 0 & \text{im Fall } p > 2 \text{ und } \left(\frac{b}{p}\right) = -1, \\ 1 & \text{im Fall } p = 2 \text{ und } \ell = n-1, \\ 2 & \text{im Fall } p = 2 \text{ und } \ell = n-2 \text{ und } b \equiv 1 \bmod 4, \\ 4 & \text{im Fall } p = 2 \text{ und } \ell \le n-3 \text{ und } b \equiv 1 \bmod 8, \\ 0 & \text{im Fall } p = 2 \text{ sonst.} \end{cases}$$

Dann gilt:

$$x^2 \equiv a \bmod p^n \iff x \bmod p^n \in \{p^{\frac{\ell}{2}} y_i + p^{n-\frac{\ell}{2}} k : 1 \le i \le r, k \in \{0, 1, \dots, p^{\frac{\ell}{2}-1}\}.$$

Insbesondere ist die Anzahl der Lösungen der Gleichung $x^2 \equiv a \bmod p^n$ genau

$$\begin{cases} 2p^{\frac{\ell}{2}} & \text{im Fall } p > 2 \text{ und } \left(\frac{b}{p}\right) = 1, \\ 0 & \text{im Fall } p > 2 \text{ und } \left(\frac{b}{p}\right) = -1, \\ 2^{\frac{\ell}{2}} & \text{im Fall } p = 2 \text{ und } b \equiv 1 \bmod 2, \ell = n-1, \\ 2^{\frac{\ell}{2}+1} & \text{im Fall } p = 2 \text{ und } b \equiv 1 \bmod 4, \ell = n-2, \\ 2^{\frac{\ell}{2}+2} & \text{im Fall } p = 2 \text{ und } b \equiv 1 \bmod 8, \ell \le n-3, \\ 0 & \text{im Fall } p = 2 \text{ sonst.} \end{cases}$$

Beweis:

(1) Für $x \in \mathbb{Z}$ gilt:

$$\begin{aligned} x^2 \equiv 0 \bmod p^n &\iff p^n \mid x^2 \iff n \le v_p(x^2) = 2v_p(x) \iff \\ &\iff \frac{n}{2} \le v_p(x) \iff \lceil \frac{n}{2} \rceil \le v_p(x) \iff p^{\lceil \frac{n}{2} \rceil} \mid x \iff \\ &\iff x \in \{p^{\lceil \frac{n}{2} \rceil} \cdot k : k \in \mathbb{Z}\} \iff \\ &\iff x \bmod p^n \in \{p^{\lceil \frac{n}{2} \rceil} \cdot k : k \in \{0, 1, \dots, p^{\lfloor \frac{n}{2} \rfloor} - 1\}\}. \end{aligned}$$

(2) Sei nun $a = p^\ell b$ mit $p \nmid b$ und $0 \le \ell \le n-1$.

(a) Wir betrachten den Fall $\ell \equiv 1 \bmod 2$. Wir nehmen an, die Gleichung wäre lösbar, d.h. es gäbe ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \bmod p^n$. Dann würde $x^2 \equiv 0 \bmod p^\ell$, also $p^\ell \mid x^2$ folgen. Da ℓ ungerade ist, würde auch $p^{\ell+1} \mid x^2$ folgen, woraus dann mit $x^2 \equiv a \bmod p^n$ die Gleichung $a \equiv 0 \bmod p^{\ell+1}$ folgen würde, im Widerspruch zur Voraussetzung. Wir können uns daher im Folgenden auf $\ell \equiv 0 \bmod 2$ beschränken.

(b) Sei also nun $\ell \equiv 0 \bmod 2$. Ist $x^2 \equiv a \bmod p^n$, so folgt $x^2 \equiv 0 \bmod p^\ell$, also $p^{\frac{\ell}{2}} \mid x$. Daher können wir ansetzen $x = p^{\frac{\ell}{2}} y$. Es gilt dann

$$x^2 \equiv a \bmod p^n \iff p^\ell y^2 \equiv p^\ell b \bmod p^n \iff y^2 \equiv b \bmod p^{n-\ell}.$$

Die Lösbarkeit (und die Lösungen) der Gleichung $y^2 \equiv b \bmod p^{n-\ell}$ haben wir aber bereits zuvor untersucht. Damit folgen sofort die angegebenen Lösbarkeitskriterium und die Formeln für die Anzahl r der Lösungen $y_1, \dots, y_r$ von $y^2 \equiv b \bmod p^{n-\ell}$.

(3) Seien $y_1, \dots, y_r$ die Lösungen von $y^2 \equiv b \bmod p^{n-\ell}$. Mit dem Ansatz $x = p^{\frac{\ell}{2}} y$ folgt:

$$\begin{aligned} x^2 \equiv a \bmod p^n &\iff p^\ell y^2 \equiv p^\ell b \bmod p^n \iff y^2 \equiv b \bmod p^{n-\ell} \iff \\ &\iff y \equiv y_i \bmod p^{n-\ell} \text{ für } 1 \le i \le r \iff \\ &\iff x \equiv p^{\frac{\ell}{2}} y_i \bmod p^{n-\frac{\ell}{2}} \text{ mit } 1 \le i \le r \iff \\ &\iff x = p^{\frac{\ell}{2}} y_i + p^{n-\frac{\ell}{2}} \cdot k \text{ mit } k \in \mathbb{Z} \text{ und } 1 \le i \le r \iff \\ &\iff x \bmod p^n \in \{p^{\frac{\ell}{2}} y_i + p^{n-\frac{\ell}{2}} \cdot k : k \in \{0, 1, \dots, p^{\frac{\ell}{2}} - 1\}, 1 \le i \le r\}. \end{aligned}$$

Diese Aussage war zu zeigen. Die Anzahl der Lösungen von $x^2 \equiv a \bmod p^n$ modulo p^n ist dann $r \cdot p^{\frac{\ell}{2}}$, woraus sofort die angegebenen Formeln folgen. ■

Nun kommen wir zur allgemeinen Gleichung $x^2 \equiv a \bmod N$ mit einer (beliebigen) natürlichen Zahl N und einer (beliebigen) ganzen Zahl a. Kennt man die Primfaktorzerlegung $N = \prod_{i=1}^{r} p_i^{e_i}$ der Zahl N, so kann man die Gleichung $x^2 \equiv a \bmod N$ auf die Gleichungen $x^2 \equiv a \bmod p_i^{e_i}$ mit Hilfe des chinesischen Restsatzes zurückführen. Eine explizite Version findet sich im folgenden Satz:

SATZ. *Für $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ sei*

$$\mathcal{L}(a, m) = \{x \in \mathbb{Z} : 0 \leq x \leq m-1 \text{ und } x^2 \equiv a \bmod m\}.$$

Sei $N \in \mathbb{N}_{\geq 2}$ und $a \in \mathbb{Z}$. Die Primfaktorzerlegung von N sei

$$N = \prod_{i=1}^{r} p_i^{e_i}.$$

Dazu wird definiert

$$M_i = \prod_{\substack{1 \leq j \leq r \\ j \neq i}} p_j^{e_j} \quad \text{und} \quad N_i = \frac{1}{M_i} \bmod p_i^{e_i}.$$

Dann ist die Abbildung

$$f : \mathcal{L}(a, N) \to \mathcal{L}(a, p_1^{e_1}) \times \cdots \times \mathcal{L}(a, p_r^{e_r}), \quad x \mapsto (x \bmod p_1^{e_1}, \ldots, x \bmod p_r^{e_r})$$

bijektiv mit der Umkehrabbildung

$$g : \mathcal{L}(a, p_1^{e_1}) \times \cdots \times \mathcal{L}(a, p_r^{e_r}) \to \mathcal{L}(a, N), \quad (x_1, \ldots, x_r) \mapsto \sum_{i=1}^{r} x_i N_i M_i \bmod N.$$

Beweis:

(1) Ist $x \in \mathcal{L}(a, N)$, so ist $0 \leq x \leq N-1$ und $x^2 \equiv a \bmod N$. Es folgt $x^2 \equiv a \bmod p_i^{e_i}$, und damit natürlich auch $(x \bmod p_i^{e_i})^2 \equiv a \bmod p_i^{e_i}$. Dies zeigt, dass die Abbildung f wohldefiniert ist.

(2) Sei $(x_1, \ldots, x_r) \in \mathcal{L}(a, p_1^{e_1}) \times \cdots \times \mathcal{L}(a, p_r^{e_r})$. Dann ist $x_i^2 \equiv a \bmod p_i^{e_i}$ und wegen

$$g(x_1, \ldots, x_r) \equiv \sum_{i=1}^{r} x_i N_i M_i \equiv x_i \bmod p_i^{e_i}$$

auch

$$g(x_1, \ldots, x_r)^2 \equiv x_i^2 \equiv a \bmod p_i^{e_i}.$$

Daraus folgt sofort

$$g(x_1, \ldots, x_r)^2 \equiv a \bmod N, \quad \text{also} \quad g(x_1, \ldots, x_r) \in \mathcal{L}(a, N).$$

Daher ist auch g wohldefiniert.

(3) Durch Betrachtung von $f \circ g$ und $g \circ f$ sieht man, dass f und g invers zueinander sind. Die Behauptungen folgen. ■

Bemerkung: Wollen wir die Gleichung $x^2 \equiv a \bmod N$ lösen, kennen wir die Faktorisierung von N, also $N = \prod_{i=1}^{r} p_i^{e_i}$, so bestimmen wir zunächst $\mathcal{L}(a, p_i^{e_i})$ für $i = 1, \ldots, r$ und erhalten dann mit Hilfe des chinesischen Restsatzes $\mathcal{L}(a, N)$. Daher lässt sich die Gleichung $x^2 \equiv a \bmod N$ schnell lösen, wenn man die Faktorisierung von N kennt.

Beispiel: Wir betrachten $N = 600 = 2^3 \cdot 3 \cdot 5^2$ und $a = 100$. Es ist

$$\begin{aligned} \mathcal{L}(100, 2^3) &= \mathcal{L}(4, 8) = \{2, 6\}, \\ \mathcal{L}(100, 3) &= \mathcal{L}(1, 3) = \{1, 2\}, \\ \mathcal{L}(100, 5^2) &= \mathcal{L}(0, 5^2) = \{0, 5, 10, 15, 20\} \end{aligned}$$

und

$$\mathcal{L}(100, 600) = \{10, 50, 70, 110, 130, 170, 190, 230, 250, 290, 310, 350, 370, 410, 430, 470, 490, 530, 550, 590\}.$$

18.1. Anhang. Es gibt auch eine Formel, mit der man $x^2 \equiv a \bmod p^n$ lösen kann, wenn man bereits eine Lösung $x_1^2 \equiv a \bmod p$ kennt.

SATZ (Tonelli-Formel). *Sei p eine ungerade Primzahl, $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 1$ und $x_1 \in \mathbb{Z}$ mit $x_1^2 \equiv a \bmod p$. Dann gilt für*

$$x_n = a^{\frac{p^n - 2p^{n-1}+1}{2}} \cdot x_1^{p^{n-1}} \bmod p^n \quad \text{die Gleichung} \quad x_n^2 \equiv a \bmod p^n.$$

Beweis:

(1) Zunächst zeigen wir die Implikation

$$x \equiv 1 \bmod p \quad \Longrightarrow \quad x^{p^{n-1}} \equiv 1 \bmod p^n$$

durch Induktion, wobei der Induktionsanfang klar ist. Es gelte also $x^{p^{n-1}} \equiv 1 \bmod p^n$, d.h. $x^{p^{n-1}} = 1 + kp^n$ für ein $k \in \mathbb{Z}$. Es folgt

$$x^{p^n} = (x^{p^{n-1}})^p = (1+kp^n)^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} k^i p^{ni} + k^p p^{np} \equiv 1 \bmod p^{n+1},$$

was die Behauptung durch Induktion beweist.

(2) Mit $a^{p-1} \equiv 1 \bmod p$ und $x_1^2 \equiv a \bmod p$ erhalten wir

$$1 \equiv a^{p-1} \equiv a^{p-2} \cdot a \equiv a^{p-2} \cdot x_1^2 \bmod p.$$

Potenzieren wir mit p^{n-1}, so folgt aus (1)

$$1 \equiv \left(a^{p-2} \cdot x_1^2\right)^{p^{n-1}} \equiv a^{p^n - 2p^{n-1}} \cdot x_1^{2p^{n-1}} \bmod p^n,$$

womit sich ergibt

$$a \equiv a \cdot 1 \equiv a \cdot a^{p^n - 2p^{n-1}} \cdot x_1^{2p^{n-1}} \equiv a^{p^n - 2p^{n-1}+1} \cdot x_1^{2p^{n-1}} \equiv \left(a^{\frac{p^n - 2p^{n-1}+1}{2}} \cdot x_1^{p^{n-1}}\right)^2 \bmod p^n.$$

Dies war zu zeigen. ■

SATZ. *Ist p eine Primzahl $p \equiv 3 \bmod 4$ und $a \in \mathbb{Z}$. Für $n \in \mathbb{N}$ sei*

$$x_n = a^{\frac{3p^n - 3p^{n-1}+2}{4}}.$$

Dann gilt

$$x_n^2 \equiv \begin{cases} a \bmod p^n, & \text{falls } \left(\frac{a}{p}\right) = 1, \\ -a \bmod p^n, & \text{falls } \left(\frac{a}{p}\right) = -1. \end{cases}$$

Beweis:

(1) Sei $\left(\frac{a}{p}\right) = 1$. Dann wissen wir, dass $x_1 \equiv a^{\frac{p+1}{4}} \bmod p$ eine Lösung der Gleichung $x^2 \equiv a \bmod p$ ist. Setzt man dies in die Formel aus dem letzten Satz ein, so erhält man mit

$$\frac{p^n - 2p^{n-1}+1}{2} + \frac{p+1}{4} p^{n-1} = \frac{2(p^n - 2p^{n-1}+1) + (p^n + p^{n-1})}{4} = \frac{3p^n - 3p^{n-1}+2}{4}$$

die zu beweisende Formel.

(2) Wegen $p \equiv 3 \bmod$ ist $\left(\frac{-1}{p}\right) = -1$. Sei jetzt $\left(\frac{a}{p}\right) = -1$. Dann ist $\left(\frac{-a}{p}\right) = 1$. Wir können also $-a$ in die Formel einsetzen und erhalten

$$-a \equiv \left((-a)^{\frac{3p^n - 3p^{n-1}+2}{4}}\right)^2 \equiv (-1)^{\frac{3p^n - 3p^{n-1}+2}{2}} a^{\frac{3p^n - 3p^{n-1}+2}{2}} \equiv \left(a^{\frac{3p^n - 3p^{n-1}+2}{4}}\right)^2 \bmod p^n,$$

was den Rest beweist wegen $\frac{3p^n - 3p^{n-1}+2}{2} \in 2\mathbb{Z}$. ■

Bemerkung: Ist $N \in \mathbb{N}$ mit der Primfaktorzerlegung $N = \prod_{i=1}^{r} p_i^{e_i}$ (mit $e_i \geq 1$) und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, N) = 1$, so sieht man mittels des chinesischen Restsatzes sofort, dass die Gleichung $x^2 \equiv a \bmod N$ genau dann lösbar ist, wenn $x^2 \equiv a \bmod p_i^{e_i}$ für alle i lösbar ist.

SATZ. *Für $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ sei*

$$\mathcal{L}(a, m) = \{x \in \mathbb{Z} : 0 \leq x \leq m-1 \text{ und } x^2 \equiv a \bmod m\}.$$

Sei $N \in \mathbb{N}_{\geq 2}$ und $a \in \mathbb{Z}$. Die Primfaktorzerlegung von N sei

$$N = \prod_{i=1}^{r} p_i^{e_i}.$$

Dazu wird definiert

$$M_i = \prod_{\substack{1 \leq j \leq r \\ j \neq i}} p_j^{e_j} \quad \text{und} \quad N_i = \frac{1}{M_i} \bmod p_i^{e_i}.$$

Dann ist

$$f : \mathcal{L}(a, N) \to \mathcal{L}(a, p_1^{e_1}) \times \cdots \times \mathcal{L}(a, p_r^{e_r}), \quad x \mapsto (x \bmod p_1^{e_1}, \ldots, x \bmod p_r^{e_r})$$

bijektiv mit Umkehrabbildung

$$g : \mathcal{L}(a, p_1^{e_1}) \times \cdots \times \mathcal{L}(a, p_r^{e_r}) \to \mathcal{L}(a, N), \quad (x_1, \ldots, x_r) \mapsto \sum_{i=1}^{r} x_i N_i M_i \bmod N.$$

Beweis:

(1) Ist $x \in \mathcal{L}(a, N)$, so ist $0 \leq x \leq N-1$ und $x^2 \equiv a \bmod N$. Es folgt $x^2 \equiv a \bmod p_i^{e_i}$, und damit natürlich auch $(x \bmod p_i^{e_i})^2 \equiv a \bmod p_i^{e_i}$. Dies zeigt, dass die Abbildung f wohldefiniert ist.

(2) Sei $(x_1, \ldots, x_r) \in \mathcal{L}(a, p_1^{e_1}) \times \cdots \times \mathcal{L}(a, p_r^{e_r})$. Dann ist $x_i^2 \equiv a \bmod p_i^{e_i}$ und wegen

$$g(x_1, \ldots, x_r) \equiv \sum_{i=1}^{r} x_i N_i M_i \equiv x_i \bmod p_i^{e_i}$$

auch

$$g(x_1, \ldots, x_r)^2 \equiv a \bmod p_i^{e_i}.$$

Daraus folgt sofort

$$g(x_1, \ldots, x_r)^2 \equiv a \bmod N, \quad \text{also} \quad g(x_1, \ldots, x_r) \in \mathcal{L}(a, N).$$

Daher ist auch g wohldefiniert.

(3) Durch Betrachtung von $f \circ g$ und $g \circ f$ sieht man, dass f und g invers zueinander sind. ■

TABELLE 1. Primzahlen $p \equiv 1 \bmod 2^\ell$

ℓ	$p \equiv 1 \bmod 2^\ell$	$p-1$
1	3	2
2	5	2^2
3	17	2^4
4	17	2^4
5	97	$2^5 \cdot 3$
6	193	$2^6 \cdot 3$
7	257	2^8
8	257	2^8
9	7681	$2^9 \cdot 3 \cdot 5$
10	12289	$2^{12} \cdot 3$
11	12289	$2^{12} \cdot 3$
12	12289	$2^{12} \cdot 3$
13	40961	$2^{13} \cdot 5$
14	65537	2^{16}
15	65537	2^{16}
16	65537	2^{16}
17	786433	$2^{18} \cdot 3$
18	786433	$2^{18} \cdot 3$
19	5767169	$2^{19} \cdot 11$
20	7340033	$2^{20} \cdot 7$
21	23068673	$2^{21} \cdot 11$
22	104857601	$2^{22} \cdot 5^2$
23	167772161	$2^{25} \cdot 5$
24	167772161	$2^{25} \cdot 5$
25	167772161	$2^{25} \cdot 5$
26	469762049	$2^{26} \cdot 7$
27	2013265921	$2^{27} \cdot 3 \cdot 5$
28	3221225473	$2^{30} \cdot 3$
29	3221225473	$2^{30} \cdot 3$
30	3221225473	$2^{30} \cdot 3$
31	75161927681	$2^{31} \cdot 5 \cdot 7$
32	77309411329	$2^{33} \cdot 3^2$
33	77309411329	$2^{33} \cdot 3^2$
34	206158430209	$2^{36} \cdot 3$
35	206158430209	$2^{36} \cdot 3$
36	206158430209	$2^{36} \cdot 3$
37	2061584302081	$2^{37} \cdot 3 \cdot 5$
38	2748779069441	$2^{39} \cdot 5$
39	2748779069441	$2^{39} \cdot 5$
40	6597069766657	$2^{41} \cdot 3$
41	6597069766657	$2^{41} \cdot 3$
42	39582418599937	$2^{42} \cdot 3^2$
43	79164837199873	$2^{43} \cdot 3^2$
44	263882790666241	$2^{44} \cdot 3 \cdot 5$
45	1231453023109121	$2^{45} \cdot 5 \cdot 7$
46	1337006139375617	$2^{46} \cdot 19$
47	3799912185593857	$2^{47} \cdot 3^3$
48	4222124650659841	$2^{48} \cdot 3 \cdot 5$
49	7881299347898369	$2^{50} \cdot 7$
50	7881299347898369	$2^{50} \cdot 7$

ℓ	$p \equiv 1 \bmod 2^\ell$	$p-1$
51	31525197391593473	$2^{52} \cdot 7$
52	31525197391593473	$2^{52} \cdot 7$
53	180143985094819841	$2^{55} \cdot 5$
54	180143985094819841	$2^{55} \cdot 5$
55	180143985094819841	$2^{55} \cdot 5$
56	1945555039024054273	$2^{56} \cdot 3^3$
57	4179340454199820289	$2^{57} \cdot 29$
58	15564440312192434177	$2^{59} \cdot 3^3$
59	15564440312192434177	$2^{59} \cdot 3^3$
60	35740566642812256257	$2^{60} \cdot 31$
61	83010348331692982273	$2^{63} \cdot 3^2$
62	83010348331692982273	$2^{63} \cdot 3^2$
63	83010348331692982273	$2^{63} \cdot 3^2$
64	221360928884514619393	$2^{66} \cdot 3$
65	221360928884514619393	$2^{66} \cdot 3$
66	221360928884514619393	$2^{66} \cdot 3$
67	1328165573307087716353	$2^{67} \cdot 3^2$
68	9149585060559937601537	$2^{68} \cdot 31$
69	13576803638250229989377	$2^{69} \cdot 23$
70	46043073207979040833537	$2^{70} \cdot 3 \cdot 13$
71	92086146415958081667073	$2^{71} \cdot 3 \cdot 13$
72	188894659314785808547841	$2^{75} \cdot 5$
73	188894659314785808547841	$2^{75} \cdot 5$
74	188894659314785808547841	$2^{75} \cdot 5$
75	188894659314785808547841	$2^{75} \cdot 5$
76	438235609610303075830988 9	$2^{77} \cdot 29$
77	438235609610303075830988 9	$2^{77} \cdot 29$
78	453347182355485940514816 1	$2^{78} \cdot 3 \cdot 5$
79	217606647530633251447111 69	$2^{81} \cdot 3^2$
80	217606647530633251447111 69	$2^{81} \cdot 3^2$
81	217606647530633251447111 69	$2^{81} \cdot 3^2$
82	628641426199607170847211 53	$2^{82} \cdot 13$
83	193428131138340667952988 161	$2^{85} \cdot 5$
84	193428131138340667952988 161	$2^{85} \cdot 5$
85	193428131138340667952988 161	$2^{85} \cdot 5$
86	673129896361425524476398 7969	$2^{86} \cdot 3 \cdot 29$
87	116056878683004400771792 89601	$2^{87} \cdot 3 \cdot 5^2$
88	188785855991020491922116 44417	$2^{88} \cdot 61$
89	315674710017771970099276 67713	$2^{89} \cdot 3 \cdot 17$
90	346623210999906474697175 478273	$2^{92} \cdot 7$
91	346623210999906474697175 478273	$2^{92} \cdot 7$
92	346623210999906474697175 478273	$2^{92} \cdot 7$
93	287202089114208223776596 819969	$2^{93} \cdot 29$
94	851702747028341629130597 466113	$2^{94} \cdot 43$
95	305028425679917699735144 2087937	$2^{95} \cdot 7 \cdot 11$
96	451600526331306724283200 5169153	$2^{96} \cdot 3 \cdot 19$
97	136272439524534660660895 59457793	$2^{98} \cdot 43$
98	136272439524534660660895 59457793	$2^{98} \cdot 43$
99	138807740724991119463889 000988673	$2^{99} \cdot 3 \cdot 73$
100	209162349037657851246956 028887041	$2^{100} \cdot 3 \cdot 5 \cdot 11$