Norbert Klingen

Primzahlen und Faktorisierung

Universität zu Köln 2004/05

Letzte Änderung: 26.10.2025 22:32

Inhaltsverzeichnis

Einleitung

Gegenstand dieser Vorlesung sind die Primzahlen und die Zerlegung natürlicher Zahlen in ihre Primfaktoren. Dies ist theoretisch recht unproblematisch, in der praktischen Durchführung jedoch von großer Komplexität. Auf dieser Tatsache beruht das wachsende Interesse der Informatiker an der Primzerlegung. So ist die Primzerlegung z. B. von großer Bedeutung in der Kryptographie (etwa Public Key Kryptosysteme).

So ist es ein Ziel dieser Vorlesung, nicht nur in die elementare Zahlentheorie einzuführen, sondern dabei zugleich ein besonderes Augenmerk auf die algorithmischen Aspekte zu legen und die Grundprinzipien der Anwendungen in der Kryptographie zu verdeutlichen.

Die Vorlesung ist dabei möglichst voraussetzungslos konzipiert und richtet sich so an Hörer aller Semester. Die benötigten Voraussetzungen umfassen nur wenige algebraische Grundbegriffe aus den Grundvorlesungen, die bei Bedarf auch kurz rekapituliert werden können.

§1 Eindeutige Primzerlegung und Euklids Algorithmus

Gemäß einer gängigen Definition gilt:

Definition: Eine *Primzahl* ist eine natürliche Zahl ≥ 2, die nicht in zwei kleinere Faktoren zerlegt werden kann: p ist *unzerlegbar*.

Bereits 300 v. Chr. hat Euklid in Buch VII seiner 'Elemente' als Proposition 30 die folgende stärkere Charakterisierung von Primzahlen bewiesen:

(1.1) Proposition: *Eine natürliche Zahl p ist genau dann eine Primzahl, wenn für alle natürlichen Zahlen a, b gilt:*

$$p \mid ab \Longrightarrow p \mid a \vee p \mid b\,. \qquad (*)$$

(Dabei steht $p \mid a$ für p teilt a.)

Eine Zahl mit der Eigenschaft $(*)$ ist sicher eine Primzahl im Sinne unserer obigen Definition, denn wäre p zerlegbar: $p = ab$, so folgte erst recht $p \mid ab$, also nach $(*)$ $p \mid a$ oder $p \mid b$. Dann wäre aber einer der beiden Faktoren nicht kleiner als p; p ist unzerlegbar.

Dass umgekehrt Eigenschaft $(*)$ von Proposition (1.1) nicht so selbstverständlich aus der obigen Definition folgt, erkennt man an einer Reihe von interessanten Konsequenzen, die man aus (1.1) ziehen kann (siehe unten), und der Tatsache, dass in beliebigen Ringen $(*)$ nicht aus der Unzerlegbarkeit gefolgert werden kann.

Konsequenzen von (1.1):

A) Eindeutige Primzerlegung:
Natürliche Zahlen sind (bis auf die Reihenfolge) eindeutig als Produkt von Primzahlen darstellbar.

Genauer gesagt impliziert (1.1) die *Eindeutigkeit* der Primzerlegung; die *Existenz* beruht darauf, dass es in $\mathbb{N}$ keine unendlich lange absteigende Kette von Zahlen gibt: Spaltet man von einer natürlichen Zahl evtentuelle Teiler so oft wie möglich ab, so ist dies nur endlich oft möglich, und man endet mit einer Primzerlegung von a.

Wäre nun die Eindeutigkeit der Primzerlegung verletzt, so gäbe es eine kleinste natürliche Zahl mit zwei wesentlich verschiedenen Primzerlegungen:

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s\,.$$

Nach (1.1) müsste p_1 einen der Faktoren q_i teilen, und dann, da letzterer unzerlegbar ist, damit übereinstimmen: $p_1 = q_i$. Dividiert man die Zerlegungen durch diese Primzahl, so erhielte man zwei wesentlich verschiedene Zerlegungen für eine kleinere Zahl

$$\frac{n}{p_1} = p_2 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot \hat{q}_i \cdot \ldots \cdot q_s\,,$$

im Widerspruch zur Minimalität von n.

B) Irrationalität von Quadratwurzeln:
Ist a eine natürliche Zahl und p eine Primzahl mit $p \nmid a$, so ist $\sqrt{pa}$ irrational.

Beweis: Wäre $\sqrt{pa}$ doch als Bruch $\sqrt{pa} = \frac{m}{n}$ $(m, n \in \mathbb{N}_+)$ darstellbar, so könnte man durch Kürzen erreichen: p teilt nicht zugleich n *und* m. Man erhielte so eine Darstellung der Form $pan^2 = m^2$. Damit gilt $p \mid m^2$, also nach (1.1) $p \mid m$, woraus natürlich $p^2 \mid m^2 = pan^2$ folgte. Dies ergibt $p \mid an^2$, also folgt wieder aus $(*)$: $p \mid a$ (Widerspruch zur Voraussetzung) oder $p \mid n$ (Widerspruch, da p bereits m teilt).

Wir betrachten die folgenden Unterringe von $\mathbb{R}$:

$$\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\} \quad \text{und} \quad \mathbb{Q}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Q}\}$$

Der zweite Ring ist sogar ein Körper; dazu zeigt man, dass das Inverse $1/\alpha$ einer Zahl $\alpha = a + b\sqrt{10} \neq 0$ $(a, b \in \mathbb{Q})$ wieder zu $\mathbb{Q}[\sqrt{10}]$ gehört. Wir bemerken zunächst, dass die Darstellung eines $\alpha \in \mathbb{Q}[\sqrt{10}]$ als $\alpha = a + b\sqrt{10}$ eindeutig ist:

$$\alpha = a + b\sqrt{10} = 0 \iff (a, b) = (0, 0)\,.$$

Begründung: $\alpha = 0 \iff a = -b\sqrt{10}$. Wäre $b \neq 0$, so ergäbe sich $\sqrt{10} = -a/b \in \mathbb{Q}$. Widerspruch zu B). Also ist $b = 0$ und dann auch $a = -b\sqrt{10} = 0$.
Nun erhalten wir die gewünschte Darstellung des Inversen durch Erweitern mit dem (algebraisch) *Konjugierten*[1] $\bar{\alpha} := a - b\sqrt{10}$ von α:

$$\frac{1}{a + b\sqrt{10}} = \frac{a - b\sqrt{10}}{(a + b\sqrt{10})(a - b\sqrt{10})} = \frac{a - b\sqrt{10}}{a^2 - 10b^2}\,.$$

Da der Nenner $a^2 - 10b^2$ rational ist, erhält man insgesamt die gewünschte Darstellung.

Im Ring $\mathbb{Z}[\sqrt{10}]$ kann man nun wie üblich Teilbarkeit definieren. Aber der Begriff der Unzerlegbarkeit muss in beliebigen Ringen etwas anders gefasst werden. In $\mathbb{N}$ haben wir unter einer Zerlegung einer Zahl eine Darstellung als Produkt *mit zwei kleineren Faktoren* verstanden. Dies bedeutete, dass wir $+1$ nicht als Faktor zugelassen haben. Dies ist sinnvoll, da $+1$ immer als Faktor gewählt werden könnte, da sie jede Zahl teilt. Im Ring $\mathbb{Z}$ gilt dasselbe auch noch für -1.

Im Ring $\mathbb{Z}[\sqrt{10}]$ gibt es neben ± 1 aber noch weitere Zahlen, die die 1 und damit jedes Ringelement teilen; z. B. $3 + \sqrt{10}$: Es gilt nämlich

$$(3 + \sqrt{10})(-3 + \sqrt{10}) = -9 + 10 = 1\,.$$

Man nennt die Teiler der 1 auch die *Einheiten*; sie sind die Zahlen, deren Inverse ebenfalls in dem Ring liegen.

Man nennt nun ein Ringelement α *zerlegbar*, wenn es Produkt von zwei Nichteinheiten ist, und entsprechend *unzerlegbar*, wenn in jeder Produktzerlegung mindestens einer der Faktoren eine Einheit ist.

C) *Im Ring $\mathbb{Z}[\sqrt{10}]$ folgt aus Unzerlegbarkeit nicht die Eigenschaft $(*)$ von (1.1).*

Dazu betrachten wir die folgenden zwei Zerlegungen von 6:

$$6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})\,.$$

In dieser Zerlegung sind alle auftretenden Faktoren unzerlegbar (!), aber keiner teilt einen der anderen. Dann kann aber für sie (1.1) nicht gelten!
Dass keiner der 4 Faktoren einen der anderen teilt, rechnet man einfach nach, indem man in $\mathbb{Q}[\sqrt{10}]$ die Quotienten berechnet und feststellt, dass diese nicht in $\mathbb{Z}[\sqrt{10}]$ liegen.

Um die Unzerlegbarkeit zu überprüfen, benutzt man die folgende Überlegung, die das Problem ein wenig auf $\mathbb{Z}$ zurückspielt:

$$\alpha = \beta \cdot \gamma \Longrightarrow \bar{\alpha} = \bar{\beta} \cdot \bar{\gamma} \Longrightarrow \alpha\bar{\alpha} = \beta\bar{\beta} \cdot \gamma\bar{\gamma}\,.$$

[1] Nicht konjugiert-komplexen!

Wie wir oben gesehen haben, ist stets $\alpha\bar{\alpha} = a^2 - 10b^2 \in \mathbb{Z}$, so dass aus einer Zerlegung von α in $\mathbb{Z}[\sqrt{10}]$ eine bestimmte Zerlegung von $\alpha\bar{\alpha}$ in $\mathbb{Z}$ folgt. Man zeigt dann, das letztere nicht existieren kann. Z. B. durchgeführt für $4 + \sqrt{10}$:

$$4 + \sqrt{10} = (a + b\sqrt{10})(c + d\sqrt{10}) \Longrightarrow (4 + \sqrt{10})(4 - \sqrt{10}) = 6 = (a^2 - 10b^2)(c^2 - 10d^2)\,.$$

In $\mathbb{Z}$ kennen wir nun alle möglichen Zerlegungen der 6. Wäre einer der Faktoren gleich ± 1, etwa $a^2 - 10b^2 = \pm 1$, d. h. $(a + b\sqrt{10}) \cdot [\pm(a - b\sqrt{10})] = 1$, so wäre $a + b\sqrt{10}$ eine Einheit und würde *jedes* andere Element in $\mathbb{Z}[\sqrt{10}]$ teilen, Widerspruch zum oben Gezeigten. Es bleibt noch die Möglichkeit, dass einer der Faktoren ± 2 ist, etwa $a^2 - 10b^2 = \pm 2$.

Nun ist eine Quadratzahl entweder durch 5 teilbar, oder sie lässt bei Division durch 5 den Rest ± 1. Damit ist $a^2 - 10b^2 \equiv a^2 \equiv 0, \pm 1$ modulo 5, in keinem Falle also $= \pm 2$.

Auf diese Weise zeigt man, dass im Ring $\mathbb{Z}[\sqrt{10}]$ die Elemente 2, 3, $4 + \sqrt{10}$ und $4 - \sqrt{10}$ unzerlegbar sind, aber nicht $(*)$ erfüllen.

Bevor wir zu einem Beweis von (1.1) kommen, sei noch (zur mathematischen Unterhaltung) das folgende Thema angeschnitten:

D1) Pythagoreische Tripel:

Natürliche Zahlen x, y, z mit $x^2 + y^2 = z^2$.

Pythagoreische Tripel sind natürliche Zahlen, die (gemäß dem Satz des Pythagoras) als Kantenlängen eines rechtwinkligen Dreiecks auftreten. Das bekannteste pythagoreische Tripel ist wohl $(3, 4, 5)$: $3^2 + 4^2 = 5^2$.

Pythagoreische Tripel treten auf bei Diophantos (250 n. Chr.), aber auch schon bei Euklid (300 v. Chr.). Archäologische Untersuchungen dieses Jahrhunderts haben sogar gezeigt, dass bereits 1500 v. Chr. den Babyloniern 'pythagoreische' Tripel bekannt waren; auf Tontäfelchen fand man Listen von pythagoreischen Tripeln, unter ihnen $3^2 + 4^2 = 5^2$, aber auch (!)

$$\begin{array}{rcrcr} 4961^2 & + & 6480^2 & = & 8161^2 \\ 24\,611\,521 & + & 41\,990\,400 & = & 66\,601\,921\,. \end{array}$$

Bei solch großen Zahlen muss man annehmen, dass sie nach einem System und nicht durch Zufall bzw. Probieren gefunden wurden.

D2) Pythagoreische Tripel:

a) Ist (x, y, z) ein pythagoreisches Tripel, so auch $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ mit $d = \mathrm{ggT}(x, y)$.

Pythagoreische Tripel mit $d = \mathrm{ggT}(x, y) = 1$ nennt man primitiv.

b) Die primitiven pythagoreischen Tripel (x, y, z) sind genau die Tripel der nachfolgenden Gestalt, evtl. mit vertauschten Rollen von x und y:

$$x = a^2 - b^2\,,\ y = 2ab\,,\ z = a^2 + b^2 \quad \textit{mit} \quad a, b \in \mathbb{N}\,,\ a > b > 0 \ \textit{teilerfremd}\,,\ 2 \mid ab\,.$$

a) Für gemeinsame Primteiler p von x und y folgt $p \mid x^2 + y^2 = z^2$, also $p \mid z$, und dann ist $(x/p, y/p, z/p)$ wieder ein pythagoreisches Tripel. Iteration ergibt a).

b) Man braucht also nur die pythagoreischen Tripel zu beschreiben, bei denen x und y teilerfremd sind, die sog. *primitiven* Tripel. Dass die angebenen Tripel pythagoreisch sind, rechnet man einfach nach. Außerdem sind sie primitiv, denn ein gemeinsamer Primteiler $p \neq 2$ von $x = a^2 - b^2$ und $y = 2ab$ ist wegen $p \mid y$ Teiler von (o. E.) a, also von a^2, dann von $b^2 = a^2 - x$, also von b, und wäre damit ein gemeinsamer Primteiler von a und b; Widerspruch. Für $p = 2$ schließt man genauso, da $2 \mid ab$ gilt.

Sei also nun (x, y, z) ein primitives pythagoreisches Tripel. Dann gilt:

Eine der beiden Zahlen x, y ist gerade;

Ist y gerade, so sind x und z ungerade.

Denn: Wären x, y ungerade, so wären ihre Quadrate von der Form $(2k + 1)^2 = 4l + 1$ $(k, l \in \mathbb{N})$, also $z^2 = x^2 + y^2 = 4m + 2$ für ein $m \in \mathbb{N}$. Damit wäre z^2, also auch z gerade, dann aber $z^2 = (2n)^2 = 4n^2 \neq 4m + 2$. Widerspruch.

Ist nun y gerade, so muss also x ungerade sein. Dann muss aber auch z ungerade sein, da sonst 2 ein Teiler von $z^2 - y^2 = x^2$, also ein Teiler von x wäre.

Seien also im Folgenden (o. E.) $y = 2m$ gerade und x, z ungerade. Dann sind $x+z$ und $x-z$ gerade, und wir erhalten

$$4m^2 = y^2 = z^2 - x^2 = (z-x)(z+x)\,,\ m^2 = \frac{z+x}{2} \cdot \frac{z-x}{2} = A \cdot B\,.$$

Nun sind die letzten beiden Faktoren A, B teilerfremd, denn ein gemeinsamer Primteiler p wäre Teiler von $A + B = z$ und von $A - B = x$; Widerspruch.

Aus der eindeutigen Primzerlegung entnehmen wir:

Ist ein Quadrat Produkt teilerfremder Zahlen, so sind diese notwendig Quadrate.

Also sind $A = a^2$ und $B = b^2$ Quadrate natürlicher Zahlen a, b. Damit erhalten wir $m^2 = a^2b^2$, also $m = ab$ und daher

$$x = A - B = a^2 - b^2\,,\ y = 2m = 2ab\,,\ z = A + B = a^2 + b^2\,,$$

mit $a, b \in \mathbb{N}$, a, b teilerfremd, a oder b gerade (da andernfalls $a^2 + b^2 = z$ gerade) und schließlich $a > b$, da $a^2 = A > B = b^2$.

Nach diesem Abstecher kommen wir nun zurück zum Beweis von Proposition (1.1). Dieser beruht entscheidend auf dem folgenden

(1.2) Lemma: (Euklid) *Der größte gemeinsame Teiler $d = \mathrm{ggT}(a, b)$ zweier natürlicher Zahlen $a, b \in \mathbb{N}$ besitzt eine Darstellung als Vielfachsumme*

$$d = xa + yb \text{ mit } x, y \in \mathbb{Z}\,.$$

Wir zeigen zunächst (1.2)⇒(1.1): Ist p ein Teiler von ab und kein Teiler von a, so ist $1 = \mathrm{ggT}(p, a)$ und daher nach (1.2) $1 = xa + yp$. Nach Multiplikation mit b erhalten wir $b = xab + ypb$. Da $p \mid ab$ vorausgesetzt ist, folgt nun, dass p ein Teiler von b sein muss.

Wir geben nun einen algorithmischen Beweis von (1.2):

(1.3) Euklidischer Algorithmus:
Für eine reelle Zahl x bezeichne $\lfloor x \rfloor$ die größte ganze Zahl $\leq x$.
Für zwei natürliche Zahlen $a, b \in \mathbb{N}$ berechnen wir die folgenden Zahlenfolgen:

$$\begin{aligned}
&a_0 = a\,,\ a_1 = b\,, && a_{i+1} = a_{i-1} - q_i a_i \quad \text{mit } q_i = \lfloor \tfrac{a_{i-1}}{a_i} \rfloor \\
&x_0 = 1\,,\ x_1 = 0\,, && x_{i+1} = x_{i-1} - q_i x_i\,, \\
&y_0 = 0\,,\ y_1 = 1\,, && y_{i+1} = y_{i-1} - q_i y_i\,,
\end{aligned}$$

Der Algorithmus endet, wenn $a_{i+1} = 0$ erreicht ist (denn dann ist q_{i+1} nicht mehr definiert). Wenn dies der Fall ist, gilt:

$$a_i = \mathrm{ggT}(a, b) = x_i a + y_i b\,.$$

Diese Form des Euklidischen Algorithmus (nach D. E. Knuth) berechnet den ggT sowie gleichzeitig seine Darstellung als $\mathbb{Z}$-Linearkombination der Ausgangszahlen.

Beweis: 1) Der Algorithmus endet:
Nach Definition von q_i ist a_{i+1} der Rest bei Division von a_{i-1} durch a_i, also $0 \leq a_{i+1} < a_i$. Da die a_i natürliche Zahlen sind, muss schließlich $a_{i+1} = 0$ erreicht werden.

2) Ist $a_{i+1} = 0$ und $d := a_i$, so ist d gemeinsamer Teiler von a und b:
Wir zeigen (absteigend) induktiv $d \mid a_j$ für alle $j = i+1, i, \ldots, 1, 0$. (Dann gilt natürlich $d \mid a_0 = a$ und $d \mid a_1 = b$.)
Der Induktionsanfang ist klar: $d \mid 0 = a_{i+1}$.
Sei nun d ein Teiler aller a_k mit $k \geq j$. Dann ist d auch ein Teiler von $a_{j+1} + q_j a_j = a_{j-1}$. Damit ist auch der Induktionsschritt bewiesen.

3) $d = x_i a + y_i b$:
Wir zeigen induktiv $a_j = x_j a + y_j b$ für $j = 0, 1, \ldots, i$. (Daraus folgt $d = a_i = x_i a + y_i b$.) Für $j = 0$ und $j = 1$ ist die Induktionsbehauptung unmittelbar aus der Definition ablesbar. Und aufgrund der gleichartigen Definition von a_{j+1}, x_{j+1} und y_{j+1} erhält man unmittelbar den Induktionsschritt.

4) $d = \mathrm{ggT}(a, b)$:
Nach 2) ist d ein gemeinsamer Teiler von a und b. Ist $d' \in \mathbb{N}$ irgendein weiterer gemeinsamer Teiler von a und b, so ist d' nach 3) auch ein Teiler von d. Damit ist d der größte gemeinsame Teiler von a und b.

§2 Primzahlhäufigkeit, Riemannsche Zetafunktion, perfekte Zahlen und Mersenne Primzahlen

(2.1) Satz: (Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis: Seien $p_1, \ldots, p_r$ irgendwelche Primzahlen. Wir bilden die Zahl

$$N = \prod_{i=1}^{r} p_i + 1 = p_1 \cdot \ldots \cdot p_r + 1\,.$$

Diese natürliche Zahl > 1 besitzt einen Primteiler q. Dieser muss von $p_1, \ldots, p_r$ verschieden sein, denn wäre $q = p_i$, so wäre q Teiler von N und von $p_1 \cdot \ldots \cdot p_r$, also

$$q \mid 1 = N - p_1 \cdot \ldots \cdot p_r\,. \quad \text{Wid.}$$

Also gibt es zu endlich vielen Primzahlen stets noch eine weitere davon verschiedene; die Menge der Primzahlen ist unendlich.

Diese Euklid'sche Aussage ist noch recht grob. Es hat die Mathematiker immer herausgefordert, hier genauere Angaben zu machen. Man studierte die Funktion

$$\pi(x) = \#\{p \le x \mid p \text{ Primzahl}\} \quad (x \in \mathbb{R})\,,$$

die die Anzahl der Primzahlen unterhalb einer reellen Grenze x angibt. Man fragte sich

$$\text{Wie wächst } \pi(x)\,?$$

Diese Frage beantwortet der

(2.2) Primzahlsatz: *Es gilt*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1\,, \text{ in Zeichen: } \pi(x) \sim \frac{x}{\log x}\,.$$

Dieser Satz kann hier nicht bewiesen werden. Sein Beweis gehört zur analytischen Zahlentheorie. Er beruht auf dem Zusammenhang der Primzahlverteilung mit der Riemann'schen Zetafunktion (siehe später).

Dieser Satz gibt eine Approximation für $\pi(x)$ durch $x/\log x$; er besagt aber nicht, dass die Differenz gegen 0 geht, sondern nur, dass die relative Abweichung gegen 0 strebt.

Historisches zum Primzahlsatz

Euklid (300 v. Chr.):

$$\pi(x) \to \infty \quad (x \to \infty)$$

Euler (1737):

$$\sum_p 1/p = \infty.$$

Legendre (1798, genauer 1808):

$$\pi(x) \text{ ungefähr } \frac{x}{\log x - B}$$

Gauß (1849 in einem Brief an Encke, 1863 posthum veröffentlicht):

$$\frac{1}{\log x} \text{ ist die Dichte der Primzahlen}$$
$$\pi(x) \text{ ungefähr } \int_2^x \frac{1}{\log t} dt$$

[Diese auf empirische Untersuchungen gestützte Vermutung von Gauß geht wohl bis in das Jahr 1791 zurück. (Gauß 14 Jahre alt!)]
Tschebyscheff (1851/52):

$$\text{Wenn } \lim_{x\to\infty} \frac{\pi(x)}{x/\log x} \text{ existiert, so ist er gleich 1.}$$
$$\text{Für } x \gg 0: \quad 0.92\ldots < \frac{\pi(x)}{x/\log x} < 1.055\ldots$$

Erst Riemann's Methoden aus dem Jahre 1859 ermöglichten den Beweis des Primzahlsatzes. Seine Beweisskizzen wurden streng durchgeführt von Hadamard (1893) und v. Mangoldt (1894). 1896 wurde der Primzahlsatz von Hadamard und unabhängig von de la Vallée-Poussin bewiesen.

(2.3) Proposition/Definition: *Die Riemann'sche Zetafunktion ist definiert als*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \textit{für } s \in]1, \infty[\,.$$

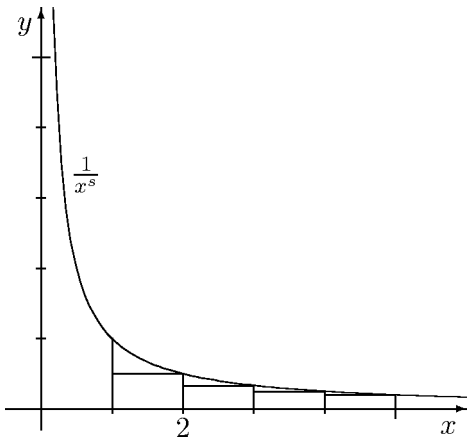
Beweis: Wir müssen zeigen, dass die angegebene Reihe konvergiert. Es ist eine Reihe mit positiven Gliedern; es genügt ihre Beschränktheit zu beweisen. Diese zeigt sich unmittelbar, wenn man

$$\zeta(s) - 1 = \sum_{n=2}^{\infty} \frac{1}{n^s}$$

als Untersumme des uneigentlichen Integrals

$$\int_1^{\infty} \frac{1}{x^s}\, dx$$

erkennt (siehe Skizze).



Dieses uneigentliche Integral ist für $s > 1$ konvergent:

$$\int_1^{\infty} \frac{1}{x^s}\, dx = \lim_{a\to\infty} \int_1^a x^{-s}\, dx = \lim_{a\to\infty} \frac{1}{s-1}(1 - \frac{1}{a^{s-1}}) = \frac{1}{s-1}\,.$$

Man erhält so eine Abschätzung für $\zeta(s)$ nach oben: $\zeta(s) \le 1 + \frac{1}{s-1}$. Auf dieselbe Weise kann man auch eine Abschätzung nach unten nachweisen, indem man nämlich die komplette Zetareihe selbst als *Obersumme* des obigen Integrals erkennt und daraus $\zeta(s) \ge 1/(s-1)$ abliest. Insgesamt erhält man so

$$\frac{1}{s-1} \le \zeta(s) \le 1 + \frac{1}{s-1} \text{ für } s > 1\,.$$

Die Abschätzung nach unten zeigt $\lim_{s\to 1+} \zeta(s) = \infty$. (Siehe unten (2.5).)

Genau genommen war Riemann's entscheidender Beitrag nicht die Einführung dieser Funktion (diese war bereits von Dirichlet für reelles s betrachtet worden), sondern ihre Ausdehnung zu einer Funktion einer *komplexen* Veränderlichen und dort ihre analytische Fortsetzung auf die ganze komplexe Zahlenebene. Dies erst führte zum entscheidenden Durchbruch und dem Beweis

des Primzahlsatzes 30 Jahre später. Dieser basierte nämlich auf dem Nachweis, dass die Zetafunktion keine Nullstelle mit Realteil 1 besitzt.
In seiner Arbeit aus dem Jahre 1859 'Ueber die Anzahl der Primzahlen unter einer gegebenen Größe' schreibt Riemann:

Bei dieser Untersuchung diente mir als Ausgangspunkt die von Euler gemachte Bemerkung, dass das Produkt

$$\prod \frac{1}{1-\frac{1}{p^s}} = \sum \frac{1}{n^s}\,, \qquad (*)$$

wenn für p alle Primzahlen, für n alle ganzen Zahlen gesetzt werden. Die Function der complexen Veränderlichen s, welche durch diese beiden Ausdrücke, so lange sie convergiren, dargestellt wird, bezeichne ich durch $\zeta(s)$. Beide convergiren nur, so lange der relle Theil von s grösser als 1 ist; es lässt sich indess leicht ein immer gültig bleibender Ausdruck der Function finden.

Diese auf Euler zurückgehende Beziehung $(*)$ bezeichnet man auch als Eulerproduktdarstellung der Zetafunktion:

(2.4) Satz: (Eulerprodukt) *Für $s > 1$ konvergiert das nachfolgende unendliche Produkt und stellt die Zetafunktion dar:*

$$\zeta(s) = \prod_{p \text{ Primzahl}} \frac{1}{1-\frac{1}{p^s}}\,.$$

Zum *Beweis* vergleichen wir ein Partialprodukt mit einem Anfangsabschnitt der Zetareihe. Sei $N \in \mathbb{N}$ beliebig vorgegeben und $p_1, \ldots, p_t$ gerade die Menge der Primzahlen $\leq N$.
Da für $s > 1$ und beliebige Primzahlen p die Abschätzung $0 \leq p^{-s} < 1$ gilt, ist die geometrische Reihe mit Quotient p^{-s} konvergent und es gilt

$$\begin{aligned}\prod_{p\leq N} \frac{1}{1-p^{-s}} &= \prod_{i=1}^{t}\sum_{n=0}^{\infty} p_i^{-sn} = \sum_{n_1,\ldots,n_t\in\mathbb{N}} \prod_{i=1}^{t}(\frac{1}{p_i^{n_i s}}) = \sum_{n_1,\ldots,n_t\in\mathbb{N}} \frac{1}{(p_1^{n_1}\cdot\ldots\cdot p_t^{n_t})^s} \\ &= \sum_{n\in\mathcal{N}} \frac{1}{n^s} \quad \text{mit } \mathcal{N} = \{n \in \mathbb{N} \mid \text{alle Primteiler von } n \text{ sind} \leq N\}\,.\end{aligned}$$

Es sei hier betont, dass in der letzten Gleichung die eindeutige Primzerlegung wesentlich benutzt wurde. Nun umfasst $\mathcal{N}$ insbesondere alle Zahlen $n \leq N$, so dass folgt

$$\left|\prod_{p\leq N} \frac{1}{1-\frac{1}{p^s}} - \sum_{n\in\mathbb{N}} \frac{1}{n^s}\right| = \sum_{n\notin\mathcal{N}} \frac{1}{n^s} \leq \sum_{n\geq N} \frac{1}{n^s}\,.$$

Als Restabschnitte der konvergenten Zetareihe konvergieren (für $N \to \infty$) die letztgenannten Reihen gegen 0, womit (2.4) bewiesen ist.

Aus dem Zusammenhang zwischen Eulerprodukt und Zetareihe und der Divergenz der harmonischen Reihe ('$= \zeta(1)$') kann man folgern

(2.5) Korollar: *Die Reihe der Inversen der Primzahlen divergiert:*

$$\sum_{p \text{ Primzahl}} \frac{1}{p} \text{ divergiert.}$$

Dass dagegen die Reihe der inversen Quadrate $\sum_n 1/n^2 = \zeta(2)$ konvergiert, kann man lax etwa so formulieren:

Die Primzahlen liegen dichter als die Quadratzahlen.

Beweis von (2.5): Wir betrachten den Logarithmus der Zetafunktion

$$\log \zeta(s) = - \sum_{p \text{ Primzahl}} \log(1 - p^{-s}) = \sum_{p,n \geq 1} \frac{1}{np^{ns}} \, .$$

Die letztgenannte Reihe konvergiert im Bereich $s > 1$, da sie majorisiert wird durch

$$\sum_{p,n \geq 1} \frac{1}{np^{ns}} \leq \sum_{p,n \geq 1} \frac{1}{p^{ns}} = \sum_{p} \frac{p^{-s}}{1 - p^{-s}} \, .$$

Für $s > 1$ ist $p^{-s} \leq \frac{1}{2}$ und $\frac{1}{1-p^{-s}} \leq 2$, so dass man schließlich

$$\log \zeta(s) \leq 2 \sum_{p} p^{-s} \leq 2\zeta(s)$$

erhält. Dies zeigt, dass die Reihe für $\log \zeta(s)$ im Bereich $s > 1$ beschränkt bleibt, also konvergiert, so dass $\zeta(s)$ in diesem Bereich keine Nullstelle hat.

Dieselben Überlegungen zeigen für $s \geq \frac{1}{2}$

$$0 \leq \log \zeta(s) - \sum_{p} p^{-s} = \sum_{p,n \geq 2} \frac{1}{np^{ns}} \leq \frac{1}{2} \sum_{p,n \geq 2} \frac{1}{p^{ns}} \leq \frac{1}{2} \sum_{p} \frac{p^{-2s}}{1 - p^{-s}} \leq c\zeta(2s)$$

mit $c = \frac{1}{2} \max\limits_{s \geq 1/2, p} \frac{1}{1-p^{-s}} = \frac{1}{2} \frac{1}{1-2^{-1/2}} = \frac{1}{2-\sqrt{2}}$. Damit bleibt die Differenz $\log \zeta(s) - \sum_p p^{-s}$ für $s \to 1$ durch $c\zeta(2)$ beschränkt, so dass mit $\zeta(s)$ und $\log \zeta(s)$ auch $\sum_p p^{-s}$ für $s \to 1+$ divergieren muss. Dann muss aber Behauptung von (2.5) gelten, denn andernfalls folgte für $s \geq 1$

$$\infty > \sum_{p} 1/p \geq \sum_{p} \frac{1}{p^s}$$

und damit die Konvergenz von $\sum_p 1/p^s$ im gesamten Bereich $s \geq 1$, Wid.

Eine der ältesten systematischen Methoden zur Erzeugung einer Liste der ersten Primzahlen, ist das sog. Sieb des Eratosthenes, das ich hier in algorithmischem Gewande angeben möchte:

(2.6) Algorithmus: (Sieb des Eratosthenes)

```
Read N
FOR i := 2 TO N DO a_i ← 1
p ← 2
WHILE p^2 ≤ N DO
    Write p
    k ← 2
    WHILE kp ≤ N DO
        a_kp ← 0
        k ← k + 1
    ENDWHILE
    REPEAT
        p ← p + 1
    UNTIL a_p = 1
ENDWHILE
WHILE p ≤ N DO
    Write p
    REPEAT
        p ← p + 1
```

```
    UNTIL a_p = 1 OR p > N
ENDWHILE
```

Die ursprünglich alle mit '1' markierten Zahlen n von 2 bis N werden im Laufe des Algorithmus zum Teil mit '0' markiert ('sie fallen durchs Sieb'); die am Ende des Algorithmus mit 1 markierten Zahlen ('die im Sieb übrigbleibenden') sind genau die Primzahlen $\leq N$.

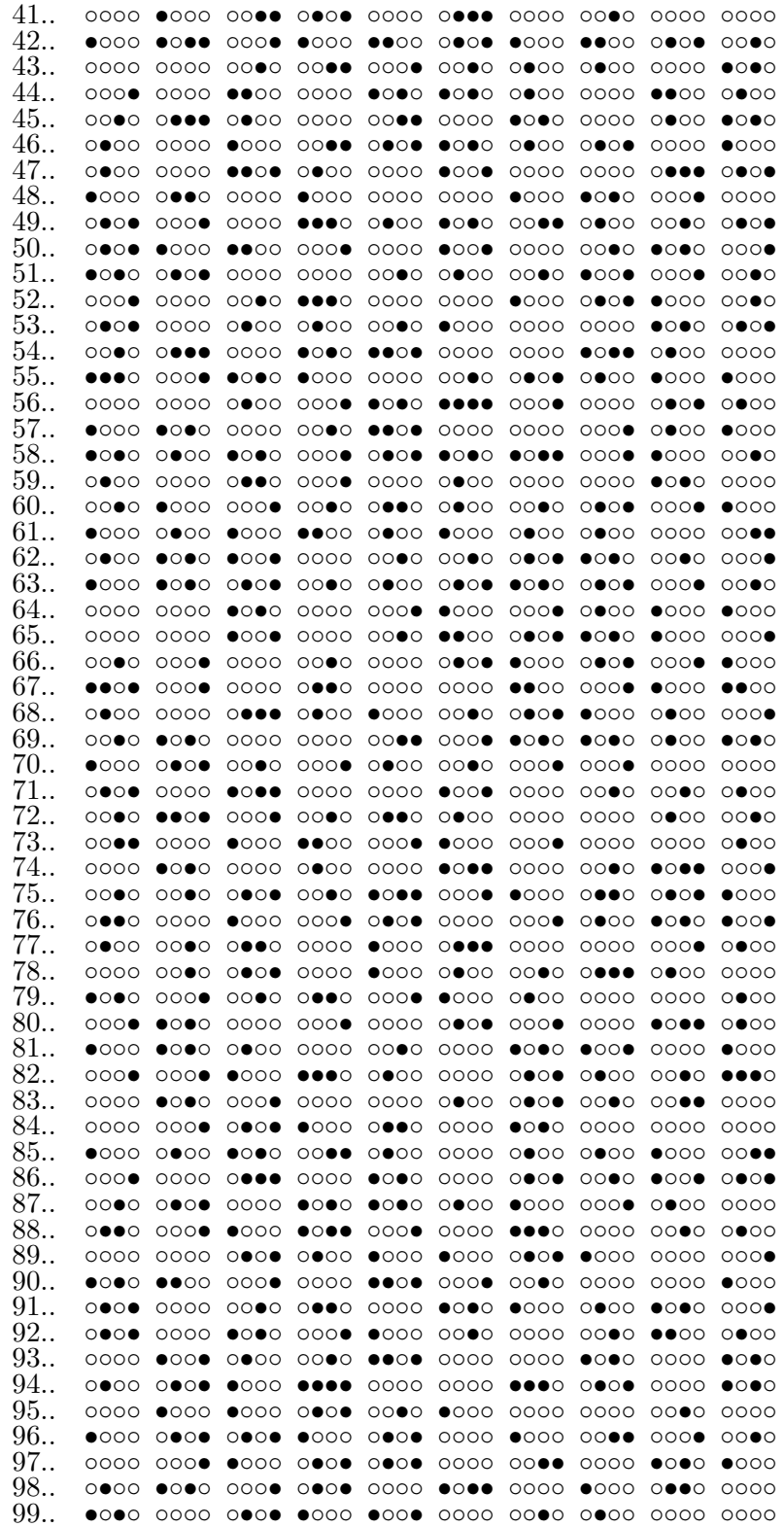
Beweis: 1) Ist n eine Primzahl, so ist $a_n = 1$, da nie $n = kp$ mit $k \geq 2$ und $p \geq 2$ ist.
2) Ist $n \leq N$ keine Primzahl, dann gilt für den kleinsten Primteiler p von n: $p^2 \leq n \leq N$, denn $n = pk$ mit $p \leq k$ impliziert $n = pk \geq pp$ (und zugleich $k \geq 2$). Also ist $n = kp$ mit $p^2 \leq N$ und $k \geq 2$, so dass $a_n = a_{kp} = 0$ gesetzt wird.
Damit sind die am Ende des Algorithmus verbleibenden n mit $a_n = 1$ genau die Primzahlen unterhalb N.

Nachfolgend ist das Ergebnis dieses Algorithmus für $N = 10000$ abgedruckt, jedoch sind nicht – wie in (2.6) angegeben – die Primzahlen selbst ausgedruckt, sondern, um Platz zu sparen, Markierungen für die a_n, und zwar für die mit ungeradem, nicht durch 5 teilbarem $n \geq 3$. (Nicht erfasst sind in der folgenden Tabelle also die Primzahlen 2 und 5.)

Die Primzahlen $< 10\,000$

Jede Zeile repräsentiert alle Zahlen eines Hunderterblocks mit den Endziffern 1, 3, 7, 9. Die Hunderter sind am Zeilenanfang angegeben. Ein • repräsentiert eine Primzahl und ein ∘ zeigt an, dass die ensprechende Zahl zerlegbar ist.

0..	•• ∘	••••	∘•∘•	•∘•∘	•••∘	∘•∘•	•∘•∘	••∘•	∘•∘•	∘∘•∘
1..	••••	∘•∘∘	∘∘•∘	•∘••	∘∘∘•	•∘•∘	∘••∘	∘•∘•	•∘∘∘	••••
2..	∘∘∘∘	•∘∘∘	∘•••	∘•∘•	•∘∘∘	•∘•∘	∘•∘•	•∘•∘	••∘∘	∘•∘∘
3..	∘∘•∘	•••∘	∘∘∘∘	•∘•∘	∘∘••	∘•∘•	∘∘•∘	∘•∘•	∘•∘•	∘∘•∘
4..	•∘∘•	∘∘∘•	•∘∘∘	••∘•	∘•∘•	∘∘•∘	•••∘	∘∘∘•	∘∘•∘	•∘∘•
5..	∘•∘•	∘∘∘∘	••∘∘	∘∘∘∘	•∘•∘	∘∘•∘	∘•∘•	•∘•∘	∘∘•∘	∘•∘•
6..	•∘•∘	∘•••	∘∘∘∘	•∘∘∘	•••∘	∘•∘•	•∘∘∘	∘•••	∘•∘∘	•∘∘∘
7..	•∘∘•	∘∘∘•	∘∘•∘	∘•∘•	∘•∘∘	•∘•∘	•∘∘•	∘•∘∘	∘∘•∘	∘∘•∘
8..	∘∘∘•	•∘∘∘	••••	∘∘∘•	∘∘∘∘	∘•••	∘•∘∘	∘∘•∘	•••∘	∘∘∘∘
9..	∘∘•∘	•∘∘•	∘∘∘•	∘∘•∘	•∘•∘	∘•∘∘	∘∘•∘	•∘•∘	∘•∘∘	•∘•∘
10..	∘∘∘•	∘•∘•	•∘∘∘	••∘•	∘∘∘•	•∘∘∘	••∘•	∘∘∘∘	∘∘•∘	•••∘
11..	∘•∘•	∘∘•∘	∘•∘•	∘∘∘∘	∘∘∘∘	••∘∘	∘•∘∘	•∘∘∘	•∘•∘	∘•∘∘
12..	•∘∘∘	∘••∘	∘•∘•	•∘•∘	∘∘∘•	∘∘∘•	∘∘∘∘	∘∘••	∘•∘•	•∘•∘
13..	•••∘	∘∘∘•	•∘•∘	∘∘∘∘	∘∘∘∘	∘∘∘∘	•∘•∘	∘•∘∘	•∘∘∘	∘∘∘•
14..	∘∘∘•	∘∘∘∘	∘•••	∘•∘•	∘∘•∘	•••∘	∘∘∘∘	•∘∘∘	••••	∘•∘•
15..	∘∘∘∘	•∘∘∘	∘•∘∘	•∘∘∘	∘•∘•	∘•∘•	∘∘•∘	•∘∘•	∘•∘∘	∘∘•∘
16..	•∘••	∘•∘•	•∘•∘	∘∘•∘	∘∘∘∘	∘∘•∘	∘•••	∘∘∘∘	∘∘∘∘	∘•••
17..	∘∘∘•	∘∘∘∘	••∘∘	∘•∘∘	•∘•∘	∘•∘•	∘∘∘∘	∘∘•∘	∘•••	∘∘∘∘
18..	•∘∘∘	•∘∘∘	∘•∘∘	•∘∘∘	∘∘•∘	∘∘∘∘	•∘•∘	••••	∘∘∘•	∘∘∘∘
19..	•∘•∘	∘•∘∘	∘∘∘∘	••∘∘	∘∘∘•	•∘∘∘	∘∘∘∘	∘•∘•	∘∘•∘	∘•••
20..	∘•∘∘	•∘•∘	∘∘••	∘∘∘•	∘∘∘∘	∘•∘∘	∘•∘•	∘∘∘∘	••••	∘∘∘•
21..	∘∘∘∘	••∘∘	∘∘∘•	•∘•∘	••∘∘	∘•∘∘	•∘∘∘	∘∘∘•	∘∘∘∘	∘∘∘∘
22..	∘•••	∘•∘∘	•∘∘∘	∘∘••	∘•∘∘	•∘∘∘	∘∘••	∘•∘∘	•∘•∘	∘•••
23..	∘∘∘•	•∘∘∘	∘∘∘∘	∘•∘•	•∘•∘	•∘•∘	∘∘∘∘	•∘•∘	•••∘	∘•∘•
24..	∘∘∘∘	•∘•∘	∘•∘∘	∘∘•∘	•∘•∘	∘∘∘•	∘∘•∘	∘•••	∘∘∘∘	∘∘∘∘
25..	∘•∘∘	∘∘∘∘	•∘∘∘	•∘∘•	∘•∘•	•∘•∘	∘∘∘∘	∘∘∘•	∘∘∘∘	••∘∘
26..	∘∘∘•	∘∘•∘	•∘∘∘	∘•∘∘	∘∘•∘	∘∘••	∘•∘∘	•∘•∘	∘•••	∘•∘•
27..	∘∘•∘	••••	∘∘∘•	•∘∘∘	•∘∘•	∘•∘∘	∘∘•∘	∘∘•∘	∘∘∘•	•∘•∘
28..	•••∘	∘∘∘•	∘∘∘∘	∘•••	∘•∘∘	•∘•∘	•∘∘∘	∘∘∘•	∘∘•∘	∘∘•∘
29..	∘•∘•	∘∘•∘	∘∘•∘	∘∘∘•	∘∘∘∘	∘•••	∘•∘•	•∘∘∘	∘∘∘∘	∘∘∘•
30..	•∘∘∘	•∘∘•	∘•∘∘	∘∘•∘	•∘∘•	∘∘∘∘	•∘•∘	∘∘∘•	∘•∘•	∘∘∘∘
31..	∘∘∘•	∘∘∘•	•∘∘∘	∘∘•∘	∘∘∘∘	∘∘∘∘	∘•••	∘∘∘∘	•∘•∘	•∘∘∘
32..	∘•∘•	∘∘•∘	•∘∘•	∘∘∘∘	∘∘∘∘	••••	∘∘∘∘	•∘∘∘	∘∘∘∘	∘∘∘•
33..	•∘•∘	∘•∘•	∘•∘•	•∘∘∘	∘•••	∘∘∘•	•∘∘∘	••∘∘	∘∘∘•	•∘∘∘
34..	∘∘•∘	∘•∘∘	∘∘∘∘	∘•∘∘	∘∘∘•	∘∘•∘	••••	∘∘∘∘	∘∘∘∘	•∘∘•
35..	∘∘∘∘	•∘•∘	∘∘••	∘•∘•	•∘•∘	∘∘••	∘∘∘∘	•∘∘∘	••∘∘	∘•∘∘
36..	∘∘•∘	∘•••	∘•∘∘	•∘•∘	∘•∘∘	∘∘∘•	∘∘∘∘	•••∘	∘∘∘∘	•∘•∘
37..	•∘∘•	∘∘∘•	∘∘•∘	∘•∘•	∘∘∘∘	∘∘∘∘	•∘••	∘∘∘•	∘∘∘∘	∘•••
38..	∘•∘∘	∘∘∘∘	••∘∘	∘•∘∘	∘∘•∘	••∘∘	∘•∘∘	∘∘•∘	•∘∘•	∘∘∘∘
39..	∘∘•∘	•∘••	∘•∘•	•∘∘∘	∘•••	∘∘∘∘	∘∘•∘	∘∘∘∘	∘∘∘•	∘∘∘∘
40..	•••∘	∘•∘•	•∘•∘	∘∘∘∘	∘∘∘•	•∘•∘	∘∘∘∘	∘•∘•	∘∘∘∘	••∘•



Insgesamt gibt es 1229 Primzahlen unter 10 000. Zum Vergleich: $\frac{x}{\log x}$ hat für $x = 10000$ den gerundeten Wert 1085,7, und

$$\int_2^{10000} \frac{1}{\log t}\, dt \approx 1245{,}1\,.$$

Mit dem Sieb des Eratosthenes verbunden ist die folgende

(2.7) Proposition: (Legendres Formel für $\pi(x)$)
Für eine reelle Zahl x ist die Anzahl der Primzahlen unterhalb x gegeben durch

$$\pi(x) = \lfloor x \rfloor - 1 + \pi(\sqrt{x}) - \sum_{p \le \sqrt{x}} \lfloor \frac{x}{p} \rfloor + \sum_{p<q\le\sqrt{x}} \lfloor \frac{x}{pq} \rfloor - \sum_{p_1<p_2<p_3\le\sqrt{x}} \lfloor \frac{x}{p_1p_2p_3} \rfloor + - \dots .$$

Beweis: Es ist $1 + \pi(x) = \lfloor x \rfloor - z$, wo z die Anzahl der zerlegbaren natürlichen Zahlen $\le x$ bezeichnet. z ist also die Anzahl der mit '0' markierten (durch das Sieb gefallenen) Zahlen $\le N = \lfloor x \rfloor$ im obigen Algorithmus. Nun werden gerade die Zahlen n mit $a_n = 0$ markiert, für die $n = kp \le x$ ist mit $p \le \sqrt{x}$ und $2 \le k$. Die möglichen Werte von k sind damit $2, \dots, \lfloor \frac{x}{p} \rfloor$, also sind dies gerade $\lfloor \frac{x}{p} \rfloor - 1$ viele Werte von n. Dies liefert zunächst die Zahl

$$\sum_{p\le\sqrt{x}} (\lfloor \frac{x}{p} \rfloor - 1) = \sum_{p\le\sqrt{x}} \lfloor \frac{x}{p} \rfloor - \pi(\sqrt{x}) .$$

Nun hat man aber in dieser Summe alle Zahlen mit zwei Primteilern $\le \sqrt{x}$ doppelt gezählt, so dass man deren Anzahl wieder abziehen muss. Dann hat man aber die mit drei verschiedenen Primteilern $\le \sqrt{x}$ zuviel abgezogen, etc. Dies ergibt dann

$$z = -\pi(\sqrt{x}) + \sum_p \lfloor \frac{x}{p} \rfloor - \sum_{p<q} \lfloor \frac{x}{pq} \rfloor + \sum_{p_1<p_2<p_3} \lfloor \frac{x}{p_1p_2p_3} \rfloor - + \dots ,$$

woraus die behauptete Formel folgt.

Etwa für $x = 50$ ergibt sich (mit den 4 Primzahlen 2, 3, 5 und 7 unterhalb $\sqrt{50}$)

$$\begin{aligned} \pi(50) &= -1 + 4 + 50 \\ &\quad -\lfloor \frac{50}{2} \rfloor - \lfloor \frac{50}{3} \rfloor - \lfloor \frac{50}{5} \rfloor - \lfloor \frac{50}{7} \rfloor \\ &\quad +\lfloor \frac{50}{2\cdot 3} \rfloor + \lfloor \frac{50}{2\cdot 5} \rfloor + \lfloor \frac{50}{2\cdot 7} \rfloor + \lfloor \frac{50}{3\cdot 5} \rfloor + \lfloor \frac{50}{3\cdot 7} \rfloor + \lfloor \frac{50}{5\cdot 7} \rfloor \\ &\quad -\lfloor \frac{50}{2\cdot 3\cdot 5} \rfloor - \lfloor \frac{50}{2\cdot 3\cdot 7} \rfloor - 0 - \dots + 0 \\ &= -1 + 4 + 50 - 25 - 16 - 10 - 7 + 8 + 5 + 3 + 3 + 2 + 1 - 1 - 1 = 15 \end{aligned}$$

Zum Abschluss dieses Paragraphen kommen wir zu den *perfekten* Zahlen. Dieser Begriff stammt ebenfalls bereits von den alten Griechen.

(2.8) Definition: Eine natürliche Zahl n heißt *perfekt*, wenn sie die Summe ihrer echten Teiler ist:

$$n = \sum_{\substack{d|n \\ d\ne n}} d .$$

bzw. äquivalent, wenn die Summe aller Teiler (bezeichnet mit $\sigma(n)$) gleich $2n$ ist:

$$\sigma(n) := \sum_{d|n} d = 2n .$$

Die ersten Beispiele sind

$$\begin{aligned} 6 &= 1 + 2 + 3 \\ 28 &= 1 + 2 + 4 + 7 + 14 \\ 496 &= 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 \\ 8128 &= \dots . \end{aligned}$$

Bis heute ist nicht bekannt, ob es unendlich viele perfekte Zahlen gibt (man vermutet: ja), und auch nicht, ob es irgendeine ungerade perfekte Zahl gibt (man vermutet: nein).

Studiert man die Primzerlegung einiger perfekter Zahlen, so stellt man Merkwürdigkeiten fest:

$$\begin{array}{rcrcl} 6 & = & 2 \cdot 3 & = & 2^1 \cdot (2^2 - 1) \\ 28 & = & 4 \cdot 7 & = & 2^2 \cdot (2^3 - 1) \\ 496 & = & 16 \cdot 31 & = & 2^4 \cdot (2^5 - 1) \\ 8128 & = & 64 \cdot 127 & = & 2^6 \cdot (2^7 - 1) \end{array}$$

Euler bewies die folgende Charakterisierung gerader perfekter Zahlen:

(2.9) Satz: *Für eine natürliche Zahl $m \in \mathbb{N}$ sind äquivalent:*

(i) *m ist eine gerade perfekte Zahl.*

(ii) *$m = 2^{n-1}(2^n - 1)$ mit einer Primzahl $2^n - 1$.*

Primzahlen dieser speziellen Bauart sind benannt nach dem französischen Mönch *Marin Mersenne* (1588-1648):

(2.10) Definition: Eine *Mersenne-Primzahl* ist eine Primzahl der Form $M(n) = 2^n - 1$.

Beweis von (2.9): (ii) $\Rightarrow$ (i): Ist $m = 2^{n-1}M(n)$ mit einer Primzahl $M(n)$, so hat m die Teiler

$$1, 2, 4, 8, \ldots, 2^{n-1}, M(n), 2M(n), 4M(n), \ldots, 2^{n-1}M(n)\,.$$

Die Summe aller Teiler ist also

$$\sigma(m) = \sum_{d|m} d = (1 + 2 + 4 + \ldots + 2^{n-1})(1 + M(n)) = \frac{2^n - 1}{2 - 1} \cdot 2^n = 2^n(2^n - 1) = 2m\,.$$

Damit ist $2m$ die Summe *aller*, und m die Summe aller *echten* Teiler, m also perfekt. m ist auch gerade, denn sonst wäre $n = 1$, also M(n)=1; aber $M(n)$ ist als Primzahl vorausgesetzt.

(i) $\Rightarrow$ (ii): Sei m eine gerade perfekte Zahl. Also $m = 2^a \cdot M$ mit $a \geq 1$ und M ungerade. Wie oben berechnen wir die Teilersumme von m aus der Teilersumme $\sigma(M)$ von M (wegen der Teilerfremdheit der Zerlegung $m = 2^a M$):

$$2m = \sum_{d|m} d = (1 + 2 + \ldots + 2^a) \cdot \sigma(M) = (2^{a+1} - 1) \cdot \sigma(M)\,.$$

Dies ergibt für die Teilersumme von M:

$$\sigma(M) = \frac{2m}{2^{a+1} - 1} = \frac{2^{a+1} \cdot M}{2^{a+1} - 1} = M + \frac{M}{2^{a+1} - 1}\,. \qquad (*)$$

Nun sind $\sigma(M)$ und M ganze Zahlen, also auch $M/(2^{a+1} - 1)$. Damit ist dies ein Teiler von M. Da S_M die Summe *aller* Teiler ist, besagt $(*)$, dass M und $M/(2^{a+1} - 1)$ sämtliche Teiler von M sind; mit nur zwei Teilern muss M eine Primzahl sein und $M/(2^{a+1} - 1) = 1$. Damit ist gezeigt:

$$M = 2^{a+1} - 1 \quad \text{und} \quad M \text{ ist Primzahl.}$$

m hat also die in (ii) behauptete Form. □

(2.11) Bemerkung: Nicht alle Zahlen $M(n) = 2^n - 1$ sind Primzahlen:
Ist $M(n)$ eine Primzahl, so ist n eine Primzahl.
Aber auch hier gilt nicht die Umkehrung.

Beweis: Sei $n = ab$ zusammengesetzt mit $2 \leq a, b < n$. Dann gilt

$$M(n) = 2^{ab} - 1 = \frac{(2^a)^b - 1}{2^a - 1} \cdot (2^a - 1) = (1 + 2^a + 2^{2a} + \ldots + 2^{a(b-1)})(2^a - 1)\,.$$

Damit ist $2^a - 1$ ein echter Teiler von $M(n)$; $M(n)$ also keine Primzahl.
Aber nicht jedes $M(p)$ (p Primzahl) ist selbst prim: $M(11) = 2047 = 23 \cdot 89$.

§3 Pseudoprimzahlen

Bei der Untersuchung der Mersenne'schen Zahlen $M(p)$ mit Primzahlindex bemerkte Fermat – soweit ihm die Primzerlegungen bekannt waren – folgende Tatsache (siehe unten Satz (3.4)):

$$p, q \text{ Primzahlen},\ q \mid M(p) \Longrightarrow q \equiv 1 \bmod p\,. \qquad (*)$$

Diese Aussage schränkt die möglichen Primfaktoren für Mersenne-Zahlen $M(p)$ stark ein und erleichtert so den Primzahlnachweis für $M(p)$ wesentlich.
Aus der Gültigkeit von $(*)$ folgt dann auch für beliebige Teiler d:

$$p \text{ Primzahl},\ d \mid M(p) \Longrightarrow d \equiv 1 \bmod p\,,$$

denn für jeden Primteiler $q \mid d$ gilt $q \equiv 1 \bmod p$, dann natürlich auch für das Produkt d.
Insbesondere muss $M(p)$ selbst kongruent 1 sein modulo p:

$$M(p) = 2^p - 1 \equiv 1 \bmod p\,.$$

Dies bedeutet für jede *Primzahl* p: $2^p \equiv 2 \bmod p$. Es gilt jedoch noch wesentlich mehr:

(3.1) Satz: *Für eine natürliche Zahl n sind äquivalent:*

(i) n ist eine Primzahl.

(ii) Für alle $1 \leq a \leq n-1$ gilt: $a^{n-1} \equiv 1 \bmod n$.

Beweis: (i)⇒(ii): Ist $n = p$ eine Primzahl, so gilt für alle natürlichen Zahlen n mit $p \nmid n$:

$$n^{p-1} \equiv 1 \bmod p\,.$$

Dies ist der sog. kleine Satz von Fermat, der aus der Algebra bekannt[2)] ist. Zur Erinnerung: p Primzahl $\Longrightarrow$ $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist ein Körper $\Longrightarrow$ $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ ist eine Gruppe der Ordnung $p-1$ $\Longrightarrow$ $a^{p-1} = 1$ für $a \in \mathbb{F}_p^\times$, also insbesondere $n^{p-1} \equiv 1 \bmod p$ für alle natürlichen Zahlen n mit $1 \leq n \leq p-1$.

(ii)⇒(i): Wäre n keine Primzahl, also $n = rs$ mit $2 \leq r \leq n-1$, so folgte aus (ii) $r^{n-1} \equiv 1 \bmod n$, also erst recht $r^{n-1} \equiv 1 \bmod r$. Nun gilt aber $r^{n-1} \equiv 0 \bmod r$, ein Widerspruch für $r > 1$. Damit muss also n eine Primzahl sein. □

Nun zeigt sich, dass für zusammengesetzte Zahlen n die Bedingung (ii) sehr oft schon für $a = 2$ oder zumindest für sehr viele a verletzt ist. Dies bedeutet, dass eine Zahl n, für die für ein

---

[2)] Man kann dies auch im Rahmen der elementaren Zahlentheorie durch Kongruenzrechnungen beweisen: Man zeigt zunächst für $a, b \in \mathbb{Z}$: $(a+b)^p \equiv a^p + b^p \bmod p$. Wegen $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ genügt es zu zeigen, dass die Binomialkoeffizienten $\binom{p}{i}$ für $0 < i < p$ durch p teilbar sind. Nun gilt für $i > 0$ $\binom{p}{i} = p \cdot \frac{(p-1)(p-2)\cdot\ldots\cdot(p-i+1)}{i!}$, wobei der zweite Faktor für $i < p$ eine ganze Zahl ist (denn alle Primfaktoren von $i!$ lassen sich wegkürzen, aber wegen $i < p$ nicht gegen p).
Aus $(a+b)^p \equiv a^p + b^p$ ergibt sich für alle $n \in \mathbb{N}$ $n^p = (1 + \cdots + 1)^p \equiv 1^p + \ldots + 1^p = n \bmod p$. Für $p \nmid n$ erhält man daraus

$$n^p \equiv n \bmod p \iff p \mid n(n^{p-1} - 1) \iff p \mid n^{p-1} - 1 \iff n^{p-1} \equiv 1 \bmod p\,.$$

a Bedingung (ii) gilt, schon mit beachtlicher Wahrscheinlichkeit eine Primzahl ist. Dies führte zu der folgenden

(3.2) Definition: Sei n eine natürliche Zahl und $1 \leq a \leq n-1$. Dann definieren wir:

$$n \text{ ist } a\text{-Pseudoprimzahl} \iff a^{n-1} \equiv 1 \bmod n\,.$$

Diese Definition ist dadurch motiviert, dass
1) eine Zahl, die a-Pseudoprimzahl ist, mit beachtlicher Wahrscheinlichkeit selbst prim ist;
2) eine Zahl, die nicht a-Pseudoprimzahl ist, notwendig zerlegbar ist;
3) der Test, ob eine Zahl a-Pseudoprimzahl ist, mit geringem Rechenaufwand durchführbar ist.
Die letzte Tatsache beruht darauf, dass die Potenzierung schnell durchführbar ist:

(3.3) Algorithmus: (2-adische Potenzierung)
`Read` a, n
$p \leftarrow 1$
`WHILE` $n \neq 0$ `DO`
  `IF` n `odd THEN` $p \leftarrow p \cdot a$
  $n \leftarrow \lfloor \frac{n}{2} \rfloor$
  $a \leftarrow a^2$
`ENDWHILE`
`Write` p

Für natürliche Zahlen a, n als Input endet Algorithmus (3.3) nach endlich vielen Schritten, und der Output ist dann die Potenz $p = a^n$.

Beweis: Der Algorithmus endet, weil bei jedem Schritt die natürliche Zahl n verkleinert wird, also schließlich die Abbruchbedingung $n = 0$ erfüllt ist. (Man kann leicht die Anzahl der Schleifendurchläufe abzählen; s. u.)

Wir zeigen nun per Induktion über n, dass für jeden Startwert p die WHILE-Schleife diesen Wert p mit a^n multipliziert. (Also liefert der Algorithmus bei $p = 1$ als Ergebnis $p = a^n$.)

Induktionsanfang $n = 0$: Dann geschieht in der Schleife nichts; p wird also mit $1 = a^0$ multipliziert.
Induktionsschritt: Die Induktionsbehauptung gelte für Exponenten kleiner als n.
1. n ungerade:
Dann erfolgen im ersten Zyklus der While-Schleife die folgenden Setzungen:

$$p \leftarrow p \cdot a\,, \quad n \leftarrow \frac{n-1}{2}\,, \quad a \leftarrow a^2$$

Nach Induktionsvoraussetzung wird im weiteren Verlauf der WHILE-Schleife der nun gültige Startwert pa multipliziert mit $(a^2)^{(n-1)/2} = a^{n-1}$, also endet die Schleife mit

$$p \cdot a \cdot a^{n-1} = p \cdot a^n\,.$$

2. n gerade: Dann sind die ersten Schritte:

$$n \leftarrow \frac{n}{2}\,, \quad a \leftarrow a^2$$

und nach Induktionsvoraussetzung wird dann der (unveränderte) Startwert p mit $(a^2)^{n/2} = a^n$ multipliziert.

In Kurzform kann man den Grundgedanken des Algorithmus an den folgenden Gleichungen verdeutlichen:

$$a^8 = (((a^2)^2)^2 \text{ und } a^{23} = a \cdot (a^2)^{11} = a \cdot a^2 \cdot (a^4)^5 = \dots\,.$$

Hinter diesem Algorithmus steht also die 2-adische Entwicklung des Exponenten. Dies erklärt auch den Namen.

Man erkennt leicht, dass die WHILE-Schleife im Algorithmus k-mal durchlaufen wird mit $k = \lceil \log_2(n) \rceil$, der kleinsten ganzen Zahl oberhalb des Logarithmus von n zur Basis 2. Dies zeigt, dass zur Potenzierung mit n nicht n, sondern höchstens $2\log_2(n)$ viele Multiplikationen nötig sind. Die letzte Zahl ist proportional zu $\log_{10}(n)$, der Stellenzahl von n. Damit ist eine solche Potenzierung auch für 100-stellige Zahlen vom Aufwand her unproblematisch.

Problematischer ist da schon die Größe des Ergebnisses. Nun wird dieser Algorithmus aber vornehmlich nicht für Potenzierungen in $\mathbb{N}$, sondern für *Potenzierungen modulo N* verwendet: Vom Ergebnis des Produktes wird der Rest modulo N genommen. Dabei liegen dann natürlich alle Ergebnisse im Bereich $0 \le x < N$; es gibt keine Überlaufprobleme.

Wir beenden diesen Paragraphen mit dem Nachweis der eingangs beschriebenen Beobachtung von Fermat:

(3.4) Satz: *Ist p eine Primzahl, so gilt für jede natürliche Zahl d:*

$$d \mid M(p) = 2^p - 1 \Longrightarrow d \equiv 1 \bmod p\,.$$

(3.5) Lemma: *Ist $a \ge 2$ eine natürliche Zahl und sind $n, m \in \mathbb{N}_+$ beliebig, so gilt*

$$\mathrm{ggT}(a^n - 1, a^m - 1) = a^{\mathrm{ggT}(n,m)} - 1\,.$$

Beweis: Sei $d = \mathrm{ggT}(n,m)$, also $n = dn'$, $m = dm'$ mit teilerfremden n', m'. Dann gilt

$$a^n - 1 = (a^d - 1) \cdot \frac{a^{dn'} - 1}{a^d - 1} \quad \text{und} \quad \frac{a^{dn'} - 1}{a^d - 1} = 1 + a^d + a^{2d} + \ldots + a^{d(n'-1)} \in \mathbb{N}\,.$$

Die Behauptung ist also äquivalent zu:

$$\frac{a^{dn'} - 1}{a^d - 1} \quad \text{und} \quad \frac{a^{dm'} - 1}{a^d - 1} \quad \text{sind teilerfremd.}$$

Diese Tatsache folgt (mit $A = a^d$) aus

$$m, n \text{ teilerfremd} \Longrightarrow A_n = \frac{A^n - 1}{A - 1}\,, A_m = \frac{A^m - 1}{A - 1} \text{ teilerfremd}\,. \qquad (*)$$

Wir können o. E. $m \ge n$ annehmen und beweisen $(*)$ per Induktion über m. Ist $m = 1$, also $m = n = 1$, so ist $A_m = A_n = 1$ und die Behauptung klar. Sei nun $m \ge 2$ und es gelte die Behauptung $(*)$ für alle kleineren Indizes. Wegen der Teilerfremdheit gilt $m > n \ge 1$.

Ist p ein gemeinsamer Primteiler von A_n und $A_m = 1 + A + A^2 + \ldots + A^{m-1} = 1 + AA_{m-1}$ ($m - 1 \ge 1$!), so kann p kein Teiler von A sein. Also gilt

$$p \mid A_m - A_n = \frac{A^m - A^n}{A - 1} = A^n \cdot \frac{A^{m-n} - 1}{A - 1} = A^n \cdot A_{m-n} \underset{p \nmid A}{\Longrightarrow} p \mid A_{m-n}\,.$$

Damit ist p gemeinsamer Teiler von A_n und A_{m-n}, obwohl n und $m - n$ kleiner als m und teilerfremd sind (wegen $\mathrm{ggT}(n,m) = 1$), ein Widerspruch zur Induktionsvoraussetzung.

Wir kommen nun zum *Beweis* von (3.4): Wie schon eingangs des Paragraphen bemerkt, genügt es, (3.4) für Primteiler q von $M(p)$ zu beweisen; gelte also $q \mid M(p) = 2^p - 1$ mit einer (notwendig ungeraden) Primzahl q. Dann gilt nach (3.1) $2^{q-1} \equiv 1 \bmod q$, also

$$q \mid 2^{q-1} - 1 \text{ und } q \mid M(p) = 2^p - 1\,.$$

Mit Lemma (3.5) erhalten wir daraus

$$q \mid \mathrm{ggT}(2^p - 1, 2^{q-1} - 1) = 2^{\mathrm{ggT}(p,q-1)} - 1\,.$$

1. Fall: $\mathrm{ggT}(p, q-1) = 1$, dann folgt $q \mid 2^1 - 1 = 1$; Widerspruch.
2. Fall: $\mathrm{ggT}(p, q-1) = p$, dann folgt $p \mid q - 1$, also wie behauptet: $q \equiv 1 \bmod p$.

Zum Ende dieses Paragraphen noch die folgende kleine

(3.6) Bemerkung: Die Dezimaldarstellung einer geraden perfekten Zahl endet auf 6 oder 28.

Beweis: Sei n eine gerade perfekte Zahl, also gilt nach (2.11) und (2.10) $n = 2^{p-1}(2^p - 1)$ mit einer Primzahl p. Für $p = 2$ ergibt sich $n = 6$ und die Behauptung stimmt. Für $p > 2$ unterscheiden wir zwei Fälle: 1) $p \equiv 1 \bmod 4$ und 2) $p \equiv 3 \bmod 4$.

1) $p - 1 = 4k$ mit $k \in \mathbb{N}$. Wir zeigen, dass in diesem Fall $n \equiv 6 \bmod 10$ ist. Es ist

$$\begin{aligned} &2^{p-1} \equiv 16^k \equiv 6^k \equiv 6 \equiv \bmod 10 \text{ und dann} \\ &2^p - 1 = 2 \cdot 2^{p-1} - 1 \equiv 2 \cdot 6 - 1 \equiv 1 \bmod 10\,, \end{aligned}$$

und daher $n \equiv 6 \bmod 10$.

2) $p - 1 = 4k + 2$ mit $k \in \mathbb{N}$. Wie oben kann man zeigen, dass dann $n \equiv 8 \bmod 10$ ist. Wir müssen aber schärfer zeigen: $n \equiv 28 \bmod 100$. Aus $16^k \equiv 6 \bmod 10$ folgt $16^k \equiv 10a + 6 \bmod 100$, also gilt

$$\begin{aligned} 2^{p-1} &= 16^k \cdot 4 \equiv (10a + 6) \cdot 4 \equiv 40a + 24 \bmod 100\,, \text{ dann} \\ 2^p - 1 &\equiv 80a + 47 \bmod 100\,, \text{ und damit} \\ n &\equiv (40a + 24)(80a + 47) = [10(4a + 2) + 4][10(8a + 4) + 7] \\ &\equiv 10(28a + 14 + 32a + 16) + 28 \equiv 28 \bmod 100\,. \end{aligned}$$

§4 Eulers φ-Funktion, das RSA-Public-Key-Kryptosystem

In §3 haben wir gesehen

$$a^{p-1} \equiv 1 \bmod p \text{ für Primzahlen } p \text{ und } p \nmid a\,.$$

Wir wollen dieses Ergebnis nun für Nicht-Primzahlen untersuchen. Dazu benötigen wir die folgenden grundlegenden Definitionen:

(4.1) Definition: a) Wir definieren für $n \in \mathbb{N}$, $n \geq 2$, die *prime Restklassengruppe modulo n* als Einheitengruppe des Ringes $\mathbb{Z}/n\mathbb{Z}$:

$$\mathcal{P}(n) := (\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{es gibt ein } \bar{b} \in \mathbb{Z}/n\mathbb{Z} \text{ mit } \bar{a} \cdot \bar{b} = \bar{1}\}$$

b) Die *Euler'sche φ-Funktion* wird definiert als Ordnung dieser Gruppe:

$$\varphi(n) := \#\mathcal{P}(n)\,,$$

c) und schließlich sei

$$\lambda(n) = \exp(\mathcal{P}(n)) := \min\{k \in \mathbb{N}_+ \mid \bar{a}^k = 1 \text{ für alle } \bar{a} \in \mathcal{P}(n)\}\,.$$

der *Exponent* von $\mathcal{P}(n)$.

(4.2) Bemerkung: Sei $n \geq 2$ eine natürliche Zahl. Dann gilt

$$\mathcal{P}(n) = (\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a, n) = 1\}$$

und damit für $a \in \mathbb{Z}$

$$\mathrm{ggT}(a, n) = 1 \implies a^{\lambda(n)} \equiv a^{\varphi(n)} \equiv 1 \bmod n\,.$$

Beweis: ad $\subseteq$: Ist $\bar{a}\bar{b} = \bar{1}$, also $ab = 1 + kn$ mit $k \in \mathbb{Z}$, so ist ein gemeinsamer Teiler von a und n auch ein Teiler von $1 = ab - kn$, also haben a und n den ggT 1.

ad $\supseteq$: Nach dem Lemma von Euklid (1.2) existiert eine Darstellung $1 = \mathrm{ggT}(a,n) = xa + yn$, d. h. $ax \equiv 1 \bmod n$ für eine Zahl $x \in \mathbb{Z}$. Mithin ist $\bar{x}$ Inverses zu $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$ und $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times = \mathcal{P}(n)$. Die letzte Behauptung folgt unmittelbar aus dem Satz von Lagrange. □

Fundamentale Basis für die Strukturuntersuchung der primen Restklassengruppen ist

(4.3) Satz: (Chinesischer Restsatz)
Sind $n_1, \ldots, n_r \in \mathbb{N}_+$ paarweise teilerfremde Zahlen und $a_1, \ldots, a_r \in \mathbb{Z}$ beliebig, so gibt es stets eine Lösung x des folgenden Kongruenzensystems

$$x \equiv a_i \bmod n_i \quad (i = 1, \ldots, r)\,.$$

Die Lösung x ist eindeutig bestimmt modulo $N = \prod_{i=1}^{r} n_i$.

Beweis: (konstruktiv) Wir setzen $N := \prod_{i=1}^{r} n_i$ sowie $N_i := \frac{N}{n_i} = \prod_{j \neq i} n_j$. Für jedes i ist dann $\mathrm{ggT}(N_i, n_i) = 1$, denn angenommen es gibt eine Primzahl p mit $p \mid N_i = \prod_{j \neq i} n_j$ und $p \mid n_i$, so gibt es ein $j \neq i$ mit $p \mid n_j$ und $p \mid n_i$, im Widerspruch zur Voraussetzung.

Nach Bem. (4.2) existiert daher zu N_i ein N_i' mit $N_i N_i' \equiv 1 \bmod n_i$. Mit diesen Größen erhalten wir die folgende konstruktive Lösung der simultanen Kongruenzen:

$$\bigwedge_{i=1}^{r} x \equiv a_i \bmod n_i \iff x \equiv \sum_{i=1}^{r} N_i N_i' a_i \bmod N\,.$$

Wir setzen $A := \sum_{j=1}^{r} N_j N_j' a_j$. Da die n_i teilerfremd sind, ist $N = \prod_i n_i = \mathrm{kgV}\{n_i \mid 1 \leq i \leq r\}$ und daher gilt

$$\begin{aligned} x \equiv A \bmod N \quad &\iff \quad N = \mathrm{kgV}(n_i) \mid x - A \iff \bigwedge_i n_i \mid x - A \\ &\iff \quad \bigwedge_i \; x \equiv A = \sum_{j \neq i} \underbrace{N_j}_{\equiv 0} N_j' a_j + \underbrace{N_i N_i'}_{\equiv 1} a_i \bmod n_i \\ &\iff \quad \bigwedge_i \; x \equiv a_i \bmod n_i \end{aligned}$$

(4.4) Zusatz: *Sind $n_1, \ldots, n_r \in \mathbb{N}_+$ beliebig und $a_1, \ldots, a_r \in \mathbb{Z}$, so gilt:*

$$x \equiv a_i \bmod n_i \ (i = 1, \ldots, r) \text{ lösbar} \iff a_i \equiv a_j \bmod \mathrm{ggT}(n_i, n_j) \ (1 \leq i < j \leq r).$$

Beweis: $\underline{\Rightarrow}$: Die angegebenen Bedingungen sind selbstverständlich notwendig für die Lösbarkeit: Sei $d_{ij} = \mathrm{ggT}(n_i, n_j)$, dann folgt aus $x \equiv a_i \bmod n_i$ natürlich $x \equiv a_i \bmod d_{ij}$ für alle i, j, also wie behauptet

$$a_i \equiv x \equiv a_j \bmod d_{ij}\,.$$

$\underline{\Leftarrow}$: Wir betrachten die Primzerlegungen

$$n_i = \prod_p p^{k_i(p)}\,, \quad \mathrm{ggT}(n_i, n_j) = \prod_p p^{\min(k_i(p), k_j(p))}$$

Aufgrund der Eindeutigkeitsaussage in (4.3) spalten wir die Kongruenzen modulo n_i nach ihren Primzahlpotenzmoduln auf:

$$x \equiv a_i \bmod n_i \iff \bigwedge_p x \equiv a_i \bmod p^{k_i(p)}\,. \tag{1}$$

Aufgrund der vorausgesetzten Kongruenzen zwischen den a_i gilt

$$a_i \equiv a_j \bmod p^{\min(k_i(p), k_j(p))} \text{ für alle } p, i, j\,. \tag{2}$$

Für jede Primzahl p wählen wir nun $\nu(p)$ als einen Index i mit der höchsten p-Potenz in n_i, also

$$\bigwedge_{1\le i\le r} k_{\nu(p)}(p) \ge k_i(p)\,. \tag{3}$$

Dann folgt aus (2)

$$a_{\nu(p)} \equiv a_i \bmod p^{k_i(p)} \text{ für alle } p \text{ und alle } i \tag{2'}$$

und wir erhalten

$$\begin{aligned} x \equiv a_i \bmod n_i \ (i=1,\dots,r) \quad &\underset{(1)}{\iff} \quad x \equiv a_i \bmod p^{k_i(p)} \text{ für alle } p,i \\ &\underset{(2')}{\iff} \quad x \equiv a_{\nu(p)} \bmod p^{k_i(p)} \text{ für alle } p,i\,. \\ &\underset{(3)}{\iff} \quad x \equiv a_{\nu(p)} \bmod p^{k_{\nu(p)}(p)} \text{ für alle } p\,. \end{aligned}$$

Das letzte simultane Kongruenzensystem (aus den endlich vielen Kongruenzen mit $k_{\nu(p)}(p) \neq 0$) ist nach (4.3) lösbar, da die Moduln als Potenzen verschiedener Primzahlen teilerfremd sind.

Damit ist (4.4) vollständig bewiesen; dieser Beweis ist ebenfalls konstruktiv: Man zerlegt die gegebenen Kongruenzen in Kongruenzen nach Primzahlpotenzmoduln und überprüft, ob die mit gleicher Primzahl Widersprüche enthalten. Ist dies nicht der Fall, braucht man für jede Primzahl nur noch die Kongruenz mit dem höchsten Exponenten zu betrachten, und löst diese dann gemäß (4.3).

Wir kommen zurück zur angestrebten Strukturbestimmung der primen Restklassengruppen. Als Vorbereitung weisen wir die zunächst die folgenden Eigenschaften des Exponenten nach.

(4.5) Lemma: *a) Für jede endliche Gruppe G gilt*

$$\exp(G) := \min\{k \in \mathbb{N}_+ \mid a^k = 1 \text{ für alle } a \in G\} = \mathrm{kgV}\{\mathrm{ord}(a) \mid a \in G\}$$

b) Ist G eine Gruppe und sind $U_1, U_2 \le G$ Untergruppen mit der Eigenschaft $u_1u_2 = u_2u_1$ für alle $u_i \in U_i$, so gilt:

$$\exp(U_1U_2) = \mathrm{kgV}(\exp(U_1), \exp(U_2))\,.$$

Insbesondere: $\exp(G \times H) = \mathrm{kgV}(\exp(G), \exp(H))$ *für beliebige endliche Gruppen G, H.*
c) Ist A eine endliche abelsche Gruppe, so gilt

$$\exp(A) = \max\{\mathrm{ord}(a) \mid a \in A\}\,. \tag{1}$$

Beweis: a) Wegen der Endlichkeit von G sind Minimum und kgV wohldefiniert. Nun gilt für $a \in G$ und $k \in \mathbb{N}_+$: $a^k = 1 \iff \mathrm{ord}(a) \mid k$ und folglich

$$\min\{k \in \mathbb{N}_+ \mid \bigwedge_{a\in G} a^k = 1\} = \min\{k \in \mathbb{N}_+ \mid \bigwedge_{a\in G} \mathrm{ord}(a) \mid k\} = \mathrm{kgV}\{\mathrm{ord}(a) \mid a \in G\}\,.$$

b) Wegen der elementweisen Vertauschbarkeit von U_1 und U_2 ist $V = U_1U_2$ eine Untergruppe von G und es gilt für beliebige $k \in \mathbb{Z}$:

$$\begin{aligned} \exp(U_1U_2) \mid k \quad &\iff \quad \bigwedge_{u_1u_2\in U_1U_2} 1 = (u_1u_2)^k = u_1^k u_2^k \iff \bigwedge_{u_1\in U_1} u_1^k = 1 \ \wedge \bigwedge_{u_2\in U_2} u_2^k = 1 \\ &\iff \quad \exp(U_1) \mid k \ \wedge \ \exp(U_2) \mid k \iff \mathrm{kgV}(\exp(U_1), \exp(U_2)) \mid k\,. \end{aligned}$$

c) Sei $a \in A$ mit maximaler Ordnung $m = \mathrm{ord}(a)$. Wir müssen zeigen, dass für *alle* $b \in A$ $b^m = 1$ gilt. Sei $n = \mathrm{ord}(b)$ die Ordnung eines beliebigen Elementes $b \in A$. Wir setzen $d = \mathrm{ggT}(m,n)$. Dann haben $x = a^d$ bzw. $y = b^d$ die Ordnungen $m' = \frac{m}{d}$ bzw. $n' = \frac{n}{d}$. Diese sind

teilerfremd. Daher hat xy die Ordnung $n'm'$, denn es gilt allgemein für zwei Elemente x, y einer beliebigen Gruppe G:

$$xy = yx \ \wedge \ \mathrm{ggT}(\mathrm{ord}(x), \mathrm{ord}(y)) = 1 \implies \mathrm{ord}(xy) = \mathrm{ord}(x) \cdot \mathrm{ord}(y) \tag{2}$$

Wegen der Vertauschbarkeit von x und y sowie der Teilerfremdheit ihrer Ordnungen gilt für beliebiges $k \in \mathbb{Z}$:

$$1 = (xy)^k \implies \begin{cases} 1 = (xy)^{k \cdot \mathrm{ord}(x)} = y^{k \cdot \mathrm{ord}(x)} \implies \mathrm{ord}(y) \mid k \cdot \mathrm{ord}(x) \implies \mathrm{ord}(y) \mid k \\ 1 = (xy)^{k \cdot \mathrm{ord}(y)} = x^{k \cdot \mathrm{ord}(y)} \implies \mathrm{ord}(x) \mid k \cdot \mathrm{ord}(y) \implies \mathrm{ord}(x) \mid k \end{cases}$$

Also folgt $\mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y)) \mid k$. Wegen der Teilerfremdheit von $\mathrm{ord}(x)$ und $\mathrm{ord}(y)$ gilt schließlich $\mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y)) = \mathrm{ord}(x) \cdot \mathrm{ord}(y)$, womit die Behauptung (2) bewiesen ist.

Aus $xy = (ab)^d$ und $\mathrm{ord}(xy) = n'm'$ folgt $\mathrm{ord}(ab) = d \cdot n'm' = n' \cdot m$. Wegen der Maximalität von $m = \mathrm{ord}(a)$ muss $n' = 1$ und damit $d = \mathrm{ggT}(n, m) = n$ sein; dies heißt aber $\mathrm{ord}(b) = n \mid m$ und $b^m = 1$. Damit ist (1) bewiesen.

Man beachte, dass in (2) keine der beiden Voraussetzungen verzichtbar ist, auch dann nicht, wenn man in (2) die Behauptung abändert zu $\mathrm{ord}(xy) = \mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y))$[3)].

(4.6) Satz: (Struktur von $\mathcal{P}(n)$)

a) *Für teilerfremde natürliche Zahlen $n, m \geq 2$ gilt*

$$\begin{aligned} \mathbb{Z}/nm\mathbb{Z} &\xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\,, \quad a \bmod nm \mapsto (a \bmod n, a \bmod m)\,. \\ \mathcal{P}(n \cdot m) &\xrightarrow{\sim} \mathcal{P}(n) \times \mathcal{P}(m)\,, \quad a \bmod nm \mapsto (a \bmod n, a \bmod m)\,. \end{aligned}$$

Induktiv ergibt sich daher bei bekannter Primzerlegung $n = \prod_{i=1}^{r} p_i^{k_i}$ von n:

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} \prod_{i=1}^{r} \mathbb{Z}/p_i^{k_i}\mathbb{Z} \\ \mathcal{P}(n) &\xrightarrow{\sim} \prod_{i=1}^{r} \mathcal{P}(p_i^{k_i}) \\ \varphi(n) &= \prod_{i=1}^{r} \varphi(p_i^{k_i}) \\ \lambda(n) &= \mathrm{kgV}(\lambda(p_i^{k_i})) \end{aligned}$$

b) *Für p prim und $k \geq 1$ ist gilt $\varphi(p^k) = p^{k-1}(p-1)$.*

c) *Für $p \neq 2$ und $k \geq 1$ ist $\mathcal{P}(p^k)$ zyklisch und somit $\lambda(p^k) = \varphi(p^k) = p^{k-1}(p-1)$.*

d) *$\mathcal{P}(2) = \{1\}$ und $\mathcal{P}(4) = \{-1, 1\}$ sind ebenfalls zyklisch, aber:*

$$k \geq 3 \implies \mathcal{P}(2^k) = \langle -\bar{1} \rangle \times \langle \bar{5} \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}\,,$$

also

$$\lambda(2^k) = \begin{cases} 1 & k = 1 \\ 2 & k = 2 \\ 2^{k-2} & k \geq 3 \end{cases}$$

[3)] Gegenbeispiele:
1. $G = S_3$ symmetrische Gruppe, $x = (1,2)$ Transposition und $y = (1,2,3)$ 3-Zyklus haben teilerfremde Ordnung 2 bzw. 3, aber $x \circ y = (2,3)$ hat nicht die Ordnung 6.
2. $G \neq 1$, $x \neq 1$ beliebig und $y = x^{-1}$. x, y sind vertauschbar, aber die Ordnung von $xy = 1$ ist weder $\mathrm{ord}(x) \cdot \mathrm{ord}(y) = \mathrm{ord}(x)^2$ noch $\mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y)) = \mathrm{ord}(x)$.

Beweis: a) Wir betrachten den natürlichen Homomorphismus

$$\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\,, \quad a \bmod nm \mapsto (a \bmod n, a \bmod m)\,.$$

Nach dem Chinesischen Restsatz (4.3) ist dieser für teilerfremde n, m ein Ringisomorphismus und er bildet die jeweiligen 1-Elemente aufeinander ab. Ein solcher Ringisiomorphismus induziert dann natürlich einen Gruppenisomorphismus der Einheitengruppen.
Die weiteren Aussagen von a) ergeben sich daraus durch vollständige Induktion, wobei die Behauptung über λ aus Lemma (4.5),b) folgt.

b) Nach (4.2) ist allgemein $\varphi(n) = \#\{1 \le a \le n \mid \mathrm{ggT}(a,n) = 1\}$ und dies läßt sich für Primzahlpotenzen $n = p^k$ einfach abzählen, denn eine Zahl $a \in \mathbb{Z}$ ist genau dann teilerfremd zu p^k, wenn sie nicht durch p teilbar ist, also

$$\mathcal{P}(p^k) = \{1, \ldots, p^k\} \setminus \{pm \mid 1 \le pm \le p^k\} = \{1, \ldots, p^k\} \setminus \{pm \mid 1 \le m \le p^{k-1}\}\,,$$

woraus man die behauptete Abzählung $\varphi(p^k) = p^k - p^{k-1}$ abliest.

c) Wir zeigen die Behauptung zunächst für $k = 1$. In diesem Fall ist $\mathcal{P}(p) = \mathbb{F}_p^\times$ die Multiplikationsgruppe eines endlichen Körpers. Diese sind zyklisch. Es gilt allgemeiner:

Endliche Untergruppen A in der Multiplikationsgruppe $K^\times$ eines Körpers sind zyklisch.

Beweis: Sei $a \in A$ mit $m = \mathrm{ord}(a)$ maximal, dann gilt nach (4.5),c) $m = \exp(A)$ und damit für $x^m = 1$ für alle $x \in A$. A besteht also nur aus Wurzeln des Polynoms $X^m - 1$ (aus m-ten Einheitswurzeln). In einem Körper hat ein Polynom vom Grad m bekanntlich höchstens m Wurzeln (Polynomdivision), also folgt: $\#A \le m = \mathrm{ord}(a) = \#\langle a\rangle$ und somit ist $A = \langle a\rangle$ zyklisch.

ad c) mit $k \ge 2$: Wegen $\mathrm{ggT}(a, p^k) = 1 \iff \mathrm{ggT}(a,p) = 1$ ist $\mathcal{P}(p^k) \twoheadrightarrow \mathcal{P}(p) = \mathbb{F}_p^\times$ ein Epimorphismus auf zyklische Gruppe $\mathbb{F}_p^\times$. Sei u ein Erzeugendes für $\mathbb{F}_p^\times$, eine sog. *Primitivwurzel* $\bmod p$. Wir wählen ein Urbild $v \in \mathcal{P}(p^k)$ von u. Wegen $\mathrm{ord}(u) = p-1$ muss $\mathrm{ord}(v)$ ein Vielfaches von $p-1$ sein. Wegen $\mathrm{ord}(v) \mid \#\mathcal{P}(p^k) = p^{k-1} \cdot (p-1)$ folgt $\mathrm{ord}(v) = p^\mu \cdot (p-1)$ mit $0 \le \mu < k$. Dann hat das Element $w = v^{p^\mu} \in \mathcal{P}(p^k)$ die genaue Ordnung $p-1$.

Wir wollen nun zeigen, dass das Element $x = 1 + \bar{p} \in \mathcal{P}(p^k)$ die Ordnung p^{k-1} hat:

$$\mathrm{ord}(1 + p \bmod p^k) = p^{k-1}\,. \tag{4}$$

Gemäß (2) hat dann das Element $x \cdot w \in \mathcal{P}(p^k)$ die Ordnung $p^{k-1} \cdot (p-1) = \#\mathcal{P}(p^k)$, erzeugt also $\mathcal{P}(p^k)$.

Zum Beweis von (4) zeigen wir per Induktion über i:

$$(1+p)^{p^i} \equiv 1 + p^{i+1} \bmod p^{i+2} \quad \text{für } i \ge 0\,. \tag{5}$$

Der Fall $i = 0$ ist klar. Sei $i \ge 0$ und $(1+p)^{p^i} = 1 + p^{i+1} + ap^{i+2}$ für ein $a \in \mathbb{Z}$. Dann folgt

$$\begin{aligned}(1+p)^{p^{i+1}} &= (1 + p^{i+1}(1+ap))^p \\ &= 1 + p \cdot p^{i+1}(1+ap) + \binom{p}{2} p^{2i+2}(1+ap)^2 + \ldots \\ &\equiv 1 + p^{i+2} \bmod p^{i+3}\,,\end{aligned}$$

denn für $p \ne 2$ ist p ein Teiler von $\binom{p}{2}$.

Mit $i = k-1$ folgt aus (5) zunächst$(1+p)^{p^{k-1}} \equiv 1 \bmod p^k$; die Ordnung von $1 + p \bmod p^k$ ist also ein Teiler von p^{k-1}. Die Ordnung kann aber kein echter Teiler sein, da für $i < k-1$, also $i + 2 \le k$ folgt

$$(1+p)^{p^i} \equiv 1 + p^{i+1} \pmod{p^{i+2}} \not\equiv 1 \pmod{p^{i+2}} \not\equiv 1 \pmod{p^k}\,.$$

Damit ist (4) bewiesen und wie bereits gezeigt folgt daraus c).

d) Wir zeigen zunächst induktiv

$$5^{2^i} \equiv 1 + 2^{i+2} \bmod 2^{i+3} \text{ für } i \geq 0\,. \tag{6}$$

$i = 0$ ist wieder klar. Sei $i \geq 0$ und $5^{2^i} = 1 + 2^{i+2} + 2^{i+3}a$ mit $a \in \mathbb{Z}$. Dann folgt

$$5^{2^{i+1}} = (1 + 2^{i+2}(1+2a))^2 = 1 + 2^{i+3}(1+2a) + 2^{2i+4}(1+2a)^2 \equiv 1 + 2^{i+3} \bmod 2^{i+4}\,.$$

Daraus folgt wie beim Beweis von (4), dass 5 mod 2^k die Ordnung 2^{k-2} hat (für $k \geq 2$).

Läge nun -1 mod 2^k in der von 5 mod 2^k erzeugten Untergruppe, so existierte ein i, $0 < i < 2^{k-2}$, mit

$$\begin{aligned}
&-1 \equiv 5^i \bmod 2^k \implies 5^{2i} \equiv 1 \bmod 2^k \\
&\implies \operatorname{ord}(\bar{5}) = 2^{k-2} \mid 2i \implies 2^{k-3} \mid i \implies 2^{k-3} = i \\
&\implies -1 \equiv 5^{2^{k-3}} \equiv 1 + 2^{k-1} \bmod 2^k \implies -1 \equiv 1 \bmod 2^{k-1} \implies k - 1 \leq 1
\end{aligned}$$

im Widerspruch zu $k \geq 3$. $\mathcal{P}(2^k)$ hat also die behauptete Struktur als direktes Produkt einer zyklischen Gruppe der Ordnung 2 und einer der Ordnung 2^{k-2} (mit den explizit angegebenen Erzeugenden). Die angegebenen Formeln für $\lambda(2^k)$ ergeben sich damit unmittelbar.

Wir wollen nun die Grundidee des *RSA-Public-Key-Kryptosystems* darstellen (benannt nach Rivest-Shamir-Adleman: A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM* **21** (1978) 120-126).

Zunächst stellt man Buchstaben durch Zahlen dar (wie in jedem PC), sodann werden Sequenzen von Buchstaben zu (etwa 100-stelligen) Zahlen zusammengefasst. So stellt eine zu übermittelnde Nachricht eine natürliche Zahl dar. Chiffrierung ist dann eine injektive Abbildung c im Bereich $\mathbb{N}$ und die Dechiffrierung erfolgt durch die Umkehrabbildung $d = c^{-1}$.

Der Sender muss die Chiffrierfunktion und der Empfänger die Dechiffrierfunktion kennen. Üblicherweise müssen beide geheimgehalten werden, da man aus der Chiffrierfunktion c (etwa einem Codebuch) leicht die Dechiffrierfunktion d gewinnen konnte (etwa durch Umordnen des Codebuchs). Das Neuartige an Public-Key-Kryptosystemen ist, dass der Schlüssel c *öffentlich* bekannt gemacht werden kann – ohne dass dadurch der Dechriffrierschlüssel d preisgegeben wird.

Leicht berechenbare Funktionen c, deren Umkehrfunktion (oder allgemeiner -relation) d nur schwer berechenbar ist, werden auch als *one-way-functions* bezeichnet. Man ist überzeugt, dass die Multiplikation

$$m : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

eine solche 'Einbahnstraßen-Funktion' ist. Die Multiplikation natürlicher Zahlen ist schnell durchführbar, während die Zerlegung einer gegebenen Zahl in (Prim-)Faktoren aufwendig ist. Ein Nachweis, dass die Primzerlegung nicht in polynomialer Zeit (bzgl. der Stellenzahl) möglich ist, ist jedoch (noch) nicht erbracht.

Das RSA-Verfahren macht sich die oben entwickelten fundamentalen Eigenschaften von $\lambda(n)$ und $\varphi(n)$ zunutze. Man startet mit einer Zahl N. Alle Rechnungen werden modulo N durchgeführt. Außerdem ist eine Zahl c gewählt, und die Chiffrierfunktion ist dann die Potenzierung modulo N mit c:

$$a \bmod N \mapsto a^c \bmod N\,.$$

Diese ist schnell durchführbar (vgl. Algorithmus (3.3)). N und c sind öffentlich bekannt!

Hat man nun c teilerfremd zu $\varphi(N)$ gewählt, so ist diese Chiffrierfunktion umkehrbar (zumindest für a prim zu N). Man bestimmt dafür zu c ein d mit

$$cd \equiv 1 \bmod \varphi(N)\,.$$

Ein solches d existiert gemäß der Charakterisierung der primen Restklassen Bemerkung (4.2). Man bestimmt d (siehe Beweis von (4.2)) mit dem Euklidischen Algorithmus (1.3), der eine Darstellung $1 = \mathrm{ggT}(c, \varphi(N)) = xc + y\varphi(N)$ liefert. Dann ist $xc \equiv 1 \bmod \varphi(N)$, und jedes $d \equiv x \bmod \varphi(N)$ leistet das Geforderte.

Es gilt dann nach (4.2) (für alle zu N teilerfremden a)

$$a^{cd} = a^{\varphi(N)\cdot k+1} \equiv a \bmod N\,,$$

so dass aus der verschlüsselten Nachricht $a^c \bmod N$ durch Potenzierung mit d die Originalnachricht $a^{cd} \bmod N = a \bmod N$ zurückgewonnen werden kann. Die Dechiffrierfunktion ist also ebenfalls eine Potenzierung modulo N, jedoch mit einem anderen Exponenten.

Ob dies ein praktikables Kryptosystem ist, hängt davon ob, wie schwierig es ist, aus dem Chiffrierschlüssel c den Dechiffrierschlüssel d zu bestimmen. Wir haben gesehen, dass d *bei Kenntnis von* $\varphi(N)$ mit dem Euklidischen Algorithmus aus c bestimmt werden kann. Da N öffentlich bekannt ist, hängt alles davon ab, wie aufwendig es ist, den Wert der Eulerschen φ-Funktion $\varphi(N)$ zu berechnen. Gemäß Satz (4.6) ist dies kein Problem, *wenn die Primzerlegung von N bekannt ist.* Man wird daher N als Produkt von zwei (geheimzuhaltenden) Primzahlen p und q ansetzen. In diesem Falle ist die Kenntnis von $\varphi(N)$ gleichbedeutend mit der Kenntnis der beiden Primzahlen p und q, d. h. der Primzerlegung von N:

(4.7) Bemerkung: Ist N das Produkt zweier Primzahlen, so ist aus $\varphi(N)$ unmittelbar die Primzerlegung von N ablesbar.

Beweis: Ist $N = pq$, so gilt gemäß (4.6) a) $\varphi(N) = (p-1)(q-1) = N - p - q + 1$, also

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

Damit ist $p + q$ durch $\varphi(N)$ und N unmittelbar bestimmt. Nun gilt weiter

$$(p-q)^2 = (p+q)^2 - 4pq = (N - \varphi(N) + 1)^2 - 4N\,,$$

also ist auch $p - q$ durch N und $\varphi(N)$ unmittelbar bestimmbar. Damit sind aber auch p und q bekannt.

Das RSA-Verfahren ist also in demselben Maße als sicher anzusehen, wie es schwierig ist, die Zerlegung einer Zahl in zwei Primfaktoren in begrenzter Zeit durchzuführen. Beim heutigen Kenntnisstand und mit der verfügbaren Hardware ist es zwar durchaus möglich, zwei 100-stellige Primzahlen p und q zu erzeugen, aber praktisch unmöglich, deren 200-stelliges Produkt N zu faktorisieren.

Nun hatten wir oben gesehen, dass die Dechriffrierung $a \equiv a^{cd} \bmod N$ nur gesichert ist für 'Nachrichten' a, *die teilerfremd sind zu N*. Für $N = pq$ mit zwei Primzahlen bedeutet dies, dass a kein Vielfaches von p oder q sein darf. Bei etwa 100-stelligen Primzahlen p und q ist die relative Häufigkeit der Vielfachen von p oder q unterhalb N etwa $2 \cdot 10^{100}/10^{200} = 2 \cdot 10^{-100}$; die Wahrscheinlichkeit, dass eine 'Nachricht' a auftritt, die nicht prim zu N ist und so nicht entschlüsselt werden kann, ist also unvergleich viel geringer als etwa die Wahrscheinlichkeit eines Hardwarefehlers.

Eine andere Möglichkeit, diesem Problem zu begegnen, ist es, die 'Nachrichten' a in ihrer Stellenzahl so zu begrenzen, dass $a < p$ und $a < q$ gilt, also a mit Sicherheit zu N teilerfremd ist. Bei etwa 100-stelligen Primzahlen könnten so Textblöcke der Länge 50 (jeder Buchstabe 2 Ziffern) zugrundegelegt werden.

(4.8) RSA-Public-Key-Kryptosystem (Grundidee)
A) Installation des Systems:
Man konstruiert zwei 'große' Primzahlen p, q (Stellenzahl etwa 100), und bildet $N = p \cdot q$.
(Bei der Wahl von p und q ergreift man noch gewisse 'Vorsichtsmaßnahmen', damit N nicht mit

einigen der noch vorzustellenden Faktorisierungsalgorithmen (siehe §5) zerlegt werden kann. So sollen $p-1$ und $q-1$ große Primfaktoren enthalten und nur einen kleinen ggT haben.)

Man wählt nun den Chiffrierschlüssel c teilerfremd zu $\varphi(N) = (p-1)(q-1)$ und berechnet den Dechiffrierschlüssel d mit $cd \equiv 1 \bmod \varphi(N)$.

• Man gibt N und c als öffentlichen Schlüssel bekannt.
• d hält der Empfänger geheim.
• p, q und $\varphi(N)$ werden vernichtet!

B) Chiffrierung:
Soll einem Empfänger E eine Nachricht a zugeschickt werden, so berechnet man mit dem *öffentlich bekannten* Schlüssel $c = c_E$, $N = N_E$ von E die chiffrierte Nachricht $a^c \bmod N$.
E dechiffriert diese mit dem nur ihm bekannten Schlüssel d: $a^{cd} \equiv a \bmod N$.
Auf diese Weise kann jeder an E eine verschlüsselte Nachricht senden, ohne je Kontakt mit ihm zu haben; lediglich der in einem 'Schlüsselbuch' (wie einem Telefonbuch) öffentlich gemachte Schlüssel c, N wird benötigt.

C) Signatur:
Man kann dasselbe System auch verwenden für eine elektronische Unterschrift: Der Empfänger E übermittelt an den Absender A einen Kontrolltext a, dieser wird von A mit seinem geheimen Schlüssel $d = d_A$ 'dechiffriert' $a^d \bmod N$ und an E zurückgesandt. E kann nun diese Chiffre dem öffentlich bekannten Schlüssel $c = c_A$ des vorgeblichen Senders A unterwerfen und erhält den Quelltext zurück und damit den Nachweis, dass A der Sender war.

D) Man kann B) und C) auch kombinieren. Dies wird hier der Einfachheit halber für übereinstimmendes N erläutert.
Sender A unterwirft eine Nachricht a zunächst seiner 'Dechiffrierung': $a^{d_A} \bmod N$, und verschlüsselt dies dann mit dem öffentlichen Schlüssel c_E des Empfängers E. Die chiffrierte Nachricht ist also $a^{d_A c_E} \bmod N$. Diese kann nun E dechiffrieren und erhält wieder $a^{d_A} \bmod N$. Wendet er darauf den öffentlichen Schlüssel c_A des (vorgeblichen) Senders A an, so erhält er den Klartext $a^{d_A c_A} = a \bmod N$ zurück und weiß zugleich, dass die Nachricht von A stammen muss.

§5 Faktorisierung

Wie wir gesehen haben, hängt die Sicherheit des RSA-Verfahrens eng mit der Primzerlegung zusammen. In diesem Paragraphen sollen daher kurz einige Faktorisierungsalgorithmen beschrieben werden. Als erstes das (im guten Sinne) 'naive' Verfahren der Division durch kleinere Primfaktoren. Dies führt im Prinzip zum Ziel, jedoch mit sehr großem Aufwand. Es wird daher in der Regel nur verwandt, um die 'kleinen Primteiler' zu bestimmen, d. h. man baut eine Schranke ein, bis zu der Primfaktoren gesucht werden. Kombiniert man dies mit den Grundgedanken des Siebes des Eratosthenes, so erhält man den folgenden Algorithmus (5.1). Er liefert als Ergebnis eine Produktzerlegung von n

$$n = \prod_{i=1}^{r} p_i^{e_i} \cdot f$$

mit verschiedenen Primzahlen p_i, Exponenten $e_i \geq 1$ und einem Faktor f, der keine Primteiler $\leq pmax$ besitzt.

(5.1) Algorithmus: (Kleine Primfaktoren)

```
PROCEDURE spalte-ab(f, d, i)
    i ← i + 1
    p_i ← d
    e_i ← 0
    REPEAT
        f ← f/d
        e_i ← e_i + 1
    UNTIL f mod d ≠ 0
```

```
ENDPROCEDURE
Read n                  (die zu zerlegende Zahl)
Read pmax               (Schranke für die Primfaktoren)
i ← 0                    (Index für die Primfaktoren)
f ← n                    (noch zu zerlegende Zahl)
FOR d = 2 TO 3 DO
    IF f mod d = 0 THEN spalte-ab(f, d, i)
ENDFOR
d ← 5
incr ← 2                        (Mindestabstand zur nächsten Primzahl)
WHILE d ≤ pmax AND d² ≤ f DO
    IF f mod d = 0 THEN spalte-ab(f, d, i)
    d ← d + incr
    incr ← 6 − incr                  (incr abwechselnd 2, 4, 2, 4, ...)
ENDWHILE
IF d² > f AND f > 1 THEN                          (*)
    i ← i + 1
    p_i ← f
    e_i ← 1
    f ← 1
ENDIF
r ← i
FOR i = 1 TO r DO Write p_i, e_i
Write f
```

Einige erläuternde Bemerkungen zur Begründung.
a) Immer wenn das Unterprogramm *spalte-ab(f, d, i)* aufgerufen wird, ist d der kleinste Primteiler von f, und wenn es beendet ist, hat f keinen Primteiler $\leq d$ mehr:
Wir beweisen dies induktiv: Die Behauptung ist einsichtig für $d = 2, 3$. Danach wird d mit $d = 5$ beginnend abwechselnd um 2 bzw. 4 erhöht; d durchläuft so alle ungeraden, nicht durch 3 teilbaren Zahlen und somit alle noch möglichen Teiler von f. Sei nun die Behauptung für d_0 richtig. Danach wird d_0 vergrößert zu d und das Programm *spalte-ab* wird erst wieder aufgerufen, wenn das vergrößerte d ein Teiler von f ist. Da nach Induktionsvoraussetzung f keinen Primteiler $\leq d_0$ hat und d der erste Teiler $> d_0$ von f ist, muss d der kleinste Primteiler von f sein. Da dieser im Unterprogramm *spalte-ab* so oft wie möglich abgespalten wird, hat f nach Ablauf des Unterprogramms d nicht mehr als Primteiler, und kleinere kamen ohnehin nicht mehr in Frage: f hat somit keine Primteiler $\leq d$ mehr.

b) Die WHILE-Schleife wird abgebrochen, wenn $d > pmax$ ist (weil größere Primteiler nicht gesucht werden), oder wenn $d^2 > f$ ist. Ist Letzteres der Fall und $f > 1$ (siehe $(*)$), so muss f selbst eine Primzahl sein: Nach der zuvor bewiesenen Bemerkung a) hat f keine Primteiler $< d$ mehr, also erst recht keine Primfaktoren $\leq \sqrt{f} (< d)$. Dann ist aber f selbst eine Primzahl (vgl. Sieb des Eratosthenes (2.6), Beweisschritt 2)).

Algorithmus (5.1) wird stets eingesetzt, um zunächst 'kleine' Primfaktoren abzuspalten. Für Zahlen mit großen Primfaktoren wird man zunächst überprüfen, ob sie evtl. selbst prim sind (Pseudoprimzahltest), und erst wenn sie nachweislich zerlegbar sind, wird man weitere Faktorisierungsalgorithmen anwenden.

- *Bei den folgenden Faktorisierungsalgorithmen wird stets vorausgesetzt, dass die zu zerlegende Zahl nachweislich zerlegbar ist.*

Denn auf Primzahlen angewendet haben sie eine unzumutbare große Laufzeit – oder enden evtl. gar nicht.

Während (5.1) kleine Primfaktoren suchte, werden in dem nachfolgenden Algorithmus große Faktoren (in der Nähe von $\sqrt{n}$) gesucht. Dieser Algorithmus ist nicht übermäßig praktikabel, macht aber einige der zu besseren Verfahren führenden Ideen deutlich. Die Grundidee geht auf Fermat zurück und besteht in der folgenden simplen

(5.2) Bemerkung: Ist n eine ungerade natürliche Zahl, so gilt:

$$n \text{ ist zerlegbar } \iff n = x^2 - y^2 \text{ mit } x, y \in \mathbb{Z}\,,\ 0 \le y \le x - 2\,.$$

Beweis: $\Leftarrow$: $n = x^2 - y^2 = (x + y) \cdot (x - y)$ mit $a := x + y \ge b := x - y \ge 2$; n ist also zerlegbar.
$\Rightarrow$: Auch die Umkehrung ergibt sich aus dieser simplen binomischen Formel, indem man von einer Zerlegung $n = a \cdot b$ mit $a \ge b \ge 2$ ausgehend x, y so bestimmt, dass $x+y = a$ und $x-y = b$ ist:

$$x = \frac{a+b}{2}\,,\ y = \frac{a-b}{2}\,.$$

Ist nun n ungerade, so sind auch a und b ungerade, deren Summe und Differenz also gerade, so dass x, y ganze Zahlen sind mit $n = a \cdot b = (x+y)(x-y) = x^2 - y^2$. Schließlich gilt $y \ge 0$ wegen $a = x + y \ge b = x - y$ und $x - 2 \ge y$ wegen $b = x - y \ge 2$.

Eine Zerlegung einer (o. E.) ungeraden Zahl n zu finden, ist also gleichbedeutend mit einer Darstellung von n als Differenz von Quadratzahlen. Ausgehend von $x = \lceil \sqrt{n} \rceil$ und $y = 0$ untersucht man, ob $r := x^2 - y^2 - n = 0$ wird. Ist $r > 0$, so vergrößert man y um 1, wodurch sich r um $\Delta_y r = 2y + 1$ verkleinert und $\Delta_y r$ um 2 erhöht. Ist $r < 0$, so vergrößert man x um 1, wodurch sich r um $\Delta_x r = 2x + 1$ sowie $\Delta_x r$ um 2 vergrößert. Ist $r = 0$, so ist eine gewünschte Darstellung $n = x^2 - y^2$ gefunden.

(5.3) Algorithmus: (Große Faktoren zerlegbarer ungerader Zahlen)

```
Read n                          (ungerade zerlegbare Zahl)
x ← ⌈√n⌉
Δxr ← 2x + 1
Δyr ← 1                                  (y = 0)
r ← x² − n
WHILE r ≠ 0 DO
    WHILE r > 0 DO
        r ← r − Δyr
        Δyr ← Δyr + 2                    (y wächst um 1)
    ENDWHILE
    IF r < 0 THEN
        r ← r + Δxr
        Δxr ← Δxr + 2
    ENDIF
ENDWHILE
a ← (Δxr + Δyr − 2)/2                    (= ((2x + 1) + (2y + 1) − 2)/2)
b ← (Δxr − Δyr)/2                        (= ((2x + 1) − (2y + 1))/2)
Write a, b
```

Man kann die Zahl der Schleifendurchläufe halbieren, indem man beachtet, dass für ungerades n die Zahlen x, y unterschiedliche Parität (gerade/ungerade) haben müssen. Man wählt also den Startwert y gleich 0 oder 1, je nach Parität von $x = \sqrt{\lceil n \rceil}$. Sodann erhöht man bei festem x das y immer um 2 und $\Delta_y r$ um 8. Der Fall $r < 0$ erfordert dann jedoch eine Sonderbehandlung, da hier neben der Änderung von x um 1 auch y nur um 1 wächst; die simple arithmetische Folge der $\Delta_y r$ wird gestört.

Eine weitere Modifikation liegt in der Überlegung, dass die y-Schleife (in der y erhöht wird), nicht zum Ziel $r = 0$ ($\iff x^2 - n = y^2$) führen kann, wenn $x^2 - n$ *kein Quadrat* ist. Dies kann

man für 'kleine' natürliche Zahlen n bequem testen: Ist die Stellenzahl von n kleiner als die Mantissenlänge der verarbeitbaren reellen Zahlen, so kann man testen, ob $\sqrt{x^2-n}$ ganzzahlig ist.

Man beachte, dass dagegen (5.3) zwar viele Schleifendurchläufe erfordert, aber nur sehr einfache algebraische Operationen (keine Multiplikationen). Dennoch ist der Algorithmus in dieser Form nicht sehr praktikabel. Wir werden jedoch seine Grundideen später weiterentwickeln.

Ein Ansatz liegt darin, statt der gesuchten Gleichheit $x^2 - y^2 = n$ nur die Kongruenz $x^2 \equiv y^2 \bmod n$ zu lösen. Eine Lösung dieser Kongruenz ergibt die Teilbarkeitsaussage $n \mid (x+y)(x-y)$ und so (bei zerlegbarem n!) eine gute Wahrscheinlichkeit dafür, dass $\mathrm{ggT}(n, x+y)$ und $\mathrm{ggT}(n, x-y)$ echte Teiler von n sind. Dies führt auf die Untersuchung *quadratischer Reste* modulo n und das Gaußsche *Reziprozitätsgesetz*, eine der Wurzeln der modernen algebraischen Zahlentheorie.

Hier sollen nun noch weitere einfache Faktorisierungsmethoden vorgestellt werden.

1. Pollard's ρ: Die erste davon ist *Pollard's ρ-Methode*. Ihr Grundgedanke ist der folgende: Man erzeugt eine rekursive Zahlenfolge x_i modulo der zu zerlegenden Zahl n. Jede derartige Folge muss schließlich (spätestens nach n Schritten) periodisch werden (da es nur n Reste modulo n gibt). (Nach einer 'Vorperiode' unbekannter Länge wird eine solche Folge dann zyklisch; eine graphische Darstellung einer solchen Folge ähnelt dem griechischen ρ. Daher der Name!) Ist nun n zerlegbar und d ein Teiler von n, so ist diese Zahlfolge erst recht modulo d periodisch (und dies mit einer Periodenlänge, die d teilt). Man sucht also Teiler d von n unter den Teilern der Differenzen $x_i - x_j$ und berechnet daher $\mathrm{ggT}(n, x_i - x_j)$ $(i < j)$.

Da man weder die Vor-, noch die Periodenlänge kennt, muss i unbegrenzt wachsen und die Differenzen $j - i$ alle natürlichen Zahlen durchlaufen. Dies ergibt im allgemeinen einen nicht zu bewältigenden Suchaufwand. Ist aber die Folge x_i durch eine einfache Rekursion gegeben ($x_{i+1} = f(x_i)$, f ein ganzzahliges Polynom), so kann man diese Suche erleichtern.

Floyd's cycle-finding algorithm untersucht bei wachsendem i die Differenzen $x_i - x_{2i}$. Ist $x_i \equiv x_{2i} \bmod d$, so ist die Folge (da einfach rekursiv) offenbar periodisch mit einer Periodenlänge l, die $2i - i = i$ teilt, und einer Vorperiodenlänge $v < i$. Hat umgekehrt die Folge modulo d die Vorperiodenlänge v und die Periodenlänge l, so muss $x_i \equiv x_{2i} \bmod d$ gelten für $i > v$ und $2i - i = i = kl$ $(k \in \mathbb{N})$, also $k > v/l$ und $i \geq (\lfloor \frac{v}{l} \rfloor + 1)l$. Indem man x_i und x_{2i} parallel berechnet, kann man großen Speicheraufwand vermeiden, muss dafür aber eine Doppelberechnung der x_ν in Kauf nehmen.

Eine Verbesserung dieses Suchalgorithmus stammt von *Brent*. Er vermeidet ebenfalls die Speicherung vieler Werte, zugleich aber auch die Doppelberechnung in Floyd's Methode. Brent berechnet

$$x_i - x_j \text{ für } i = 2^n - 1 \text{ und } 2^{n-1} + 1 \leq j - i \leq 2^n\,, \text{ also } 2^n + 2^{n-1} \leq j \leq 2^{n+1} - 1\,.$$

Dies bedeutet explizit die Berechnung folgender Differenzen

$$x_1 - x_3\,, \quad x_3 - x_6, x_3 - x_7\,, \quad x_7 - x_{12}, x_7 - x_{13}, x_7 - x_{14}, x_7 - x_{15}\,, \quad x_{15} - x_{24}, \ldots$$

Man erkennt unmittelbar an der Definition, dass i über alle Grenzen wächst und $j - i$ alle natürlichen Zahlen durchläuft. Der Vorteil dieses Verfahrens ist, dass alle Werte nur einmal berechnet werden und man immer nur einen Vergleichswert x_i speichern muss.

Neben der Berechnung der $x_i - x_j$ sind außerdem viele ggT-Berechnungen nötig. Diese sind zwar mit Euklid's Algorithmus schnell durchführbar, aber es kann viel Aufwand in die (wenig informative) Berechnung von $\mathrm{ggT}(n, x_i - x_j) = 1$ fließen. Man berechnet daher *Produkte* $Q = \prod (x_i - x_j)$ mehrerer aufeinanderfolgender $x_i - x_j$ und dann $\mathrm{ggT}(n, Q)$. Ist dieser 1, so müssen auch die einzelnen $\mathrm{ggT}(n, x_i - x_j) = 1$ sein und man sucht weiter. Ist $\mathrm{ggT}(n, Q) \neq 1$ und $\neq n$, so hat man einen echten Teiler von n gefunden. Ist aber $\mathrm{ggT}(n, Q) = n$, so muss man die einzelnen Faktoren $x_i - x_j$ von Q erneut berechnen und die ggT's einzeln bestimmen.

Ob dieser Algorithmus sinnvoll ist, hängt entscheidend davon ab, wieviele $x_i - x_j$ man berechnen muss, bis man einen Teiler von n gefunden hat. Es war Pollard's Beobachtung, dass für

eine Zufallsfolge von Zahlen eine Periode modulo p nach durchschnittlich $C\sqrt{p}$ Zyklen auftritt. Dies gilt nicht für alle wie oben konstruierten Folgen; etwa für lineare Polynome und für X^2 bzw. X^2-2 nicht. Empirische Untersuchungen bestätigen dies jedoch für alle anderen Polynome X^2+a.

2. Pollard's $p-1$-Methode: Ein weiterer Faktorisierungsalgorithmus ist *Pollard's $p-1$-Methode*. Er ist darauf gerichtet, Primfaktoren p einer zerlegbaren Zahl n zu finden, für die $p-1$ seinerseits nur kleine Primfaktoren besitzt. Wir wollen letzteres in der Form $p-1 \mid k!$ voraussetzen, etwa mit $k=10000$. Wir betonen wieder, dass n zuvor als zerlegbar nachgewiesen sein muss!

Besitzt n einen derartigen Primteiler p, so gilt für beliebiges a prim zu n folgendes:

$$m := a^{k!} \bmod n \Longrightarrow m \bmod p = a^{k!} \bmod p = (a^{p-1})^{k'} \underset{(3.1)}{\equiv} 1 \bmod p\,.$$

Hat also n einen Primteiler p mit $p-1 \mid k!$, so ist dieser als Teiler von $m := a^{k!}-1 \bmod n$ zu finden.

Man geht dazu folgendermaßen vor: Man berechne sukzessive $m_l := a^{l!} \bmod n$ gemäß der Rekursion $m_{l+1} = m_l^{l+1} \bmod n$ und dann (nicht unbedingt für jedes l, sondern nur in gewissen Abständen) $\mathrm{ggT}(m_l-1, n)$. Ist dieser ggT $\neq 1$ und $\neq n$, so hat man einen echten Teiler von n gefunden; ist er $=1$, so rechne man weiter; ist er $=n$, so macht es keinen Sinn weitere m_l zu berechnen, denn

$$\mathrm{ggT}(n, m_l-1) = n \iff m_l \equiv 1 \bmod n \implies m_{l+1} = m_l^{l+1} \equiv 1 \bmod n\,.$$

Man berechnet dann die zuvor ausgelassenen ggTs in der Hoffnung, dass dabei ein echter Teiler von n gefunden wird. Andernfalls muss man die zugrundegelegte Basis a verändern, oder einen anderen Faktorisierungsalgorithmus anwenden.

(5.4) Algorithmus: (Pollard's $p-1$-Methode)

```
Read n, a, k
m ← a
mggt ← m          (Letzter Wert für m bei ggT-Berechnung)
abst ← 10         (Abstand für ggT-Berechnungen)
g ← 1             (gefundener Teiler von n)
i ← 1
WHILE i < k AND g = 1 DO
    i ← i + 1
    m ← m^i mod n              (siehe Algorithmus (3.3))
    IF i mod abst = 0 THEN
        g ← ggT(m − 1, n)      (siehe Algorithmus (1.3))
        IF g = n THEN
            m ← mggt
            k ← i
            i ← i − abst
            abst ← 1
        ELSE
         mggt ← m
        ENDIF
    ENDIF
ENDWHILE
IF 1 < g < n THEN Write g ELSE Write 'Kein Faktor gefunden.'
```

§6 Quadratische Reste, starke Pseudoprimzahlen

In §3 haben wir die sog. Pseudoprimzahlen eingeführt. Ihre Bedeutung war durch Satz (3.1) gegeben. Ist eine Zahl n für ein a keine a-Pseudoprimzahl, so ist sie zerlegbar. Und umgekehrt: Wenn n zerlegbar ist, so gibt es ein a, für das n den a-Pseudoprimzahltest *nicht* erfüllt. Allerdings zeigte der Beweis von (3.1), dass a dabei ein Teiler n ist.

Nun ist aber ein Pseudoprimzahltest nur dann sinnvoll, wenn die Zahl a teilerfremd zu n ist: Ist nämlich $\mathrm{ggT}(a,n) \neq 1$ (was schnell überprüfbar ist), so ist schon damit klar, dass n zerlegbar ist; mit dem ggT ist sogar schon ein Teiler von n gefunden.

Man führt also Pseudoprimzahltests nur für Basen a durch, die zu n teilerfremd sind. Allerdings kann es dann passieren, dass alle Tests positiv sind, aber n dennoch nicht prim.

(6.1) Definition: Eine Zahl n heißt *Carmichael-Zahl*, wenn sie für alle zu n teilerfremden Zahlen a eine a-Pseudoprimzahl, aber dennoch keine Primzahl ist.

(6.2) Satz: *a) Sei n eine zerlegbare Zahl. Dann sind äquivalent:*

(i) n ist Carmichael-Zahl.

(ii) $\lambda(n) \mid n-1$.

(iii) n ist quadratfrei und für alle Primteiler p von n gilt: $p-1 \mid n-1$.

b) Carmichael-Zahlen sind ungerade und haben mindestens 3 Primfaktoren.

Beweis: a) Gemäß Definition ist $\lambda(n)$ der Exponent der primen Restklassengruppe $\mathcal{P}(n)$, also gilt

$$\lambda(n) \mid n-1 \iff \bigwedge_{a \in \mathcal{P}(n)} a^{n-1} \equiv 1 \bmod n\,,$$

und Letzteres charakterisiert gerade die Carmichael-Zahlen. Damit ist (i)⇔(ii) bewiesen.

(ii)⇐(iii): Sei $n = p_1 \cdot \ldots \cdot p_r$ mit verschiedenen Primzahlen p_i und $p_i - 1 \mid n-1$ für alle i. Dann folgt gemäß (4.6),a)

$$\lambda(n) = \mathrm{kgV}(p_1 - 1, \ldots, p_r - 1) \mid n-1\,.$$

(ii)⇒(iii): Wir zeigen zunächst, dass n ungerade sein muss. Wäre n gerade, also $n-1$ ungerade, so folgte

$$(-1)^{n-1} \equiv -1 \bmod n\,,$$

während für eine Carmichael-Zahl $a^{n-1} \equiv 1 \bmod n$ gelten muss. Also folgte $-1 \equiv 1 \bmod n$, $\eth n = 2$. Carmichael-Zahlen sind aber nicht prim.

Sei nun p ein Primteiler von n und $n = p^k \cdot m$ mit $k \geq 1$ und $p \nmid m$. Da n ungerade ist, ist $p \neq 2$ und damit die prime Restklassengrupp $\mathcal{P}(p^k)$ gemäß (4.6),b) zyklisch. Sei w ein Erzeuger von $\mathcal{P}(p^k)$, also $\mathrm{ord}(w \bmod p^k) = p^{k-1}(p-1)$.

Nach dem Chinesischen Restsatz wählen wir nun ein $a \in \mathcal{P}(n)$ mit $a \equiv w \bmod p^k$ und $a \equiv 1 \bmod m$. Aus $a^{n-1} \equiv 1 \bmod n$ folgt erst recht $1 \equiv a^{n-1} \equiv w^{n-1} \bmod p^k$, also $\mathrm{ord}(w \bmod p^k) = p^{k-1}(p-1) \mid n-1$. Damit gilt $p-1 \mid n-1$, wie in (iii) behauptet. Darüberhinaus folgt $p^{k-1} \mid n-1$. Wegen $p \mid n$ kann Letzteres nur gelten, wenn $k = 1$ ist; n ist also quadratfrei.

b) Dass n ungerade sein muss, haben wir bereits unter a) (ii)⇒(iii) gezeigt. Sei nun $n = pq$ mit $p < q$ Primzahlen. Dann ist $\lambda(n) = \mathrm{kgV}(p-1, q-1)$. Wäre n Carmichael-Zahl, so folgte $q-1 \mid \mathrm{kgV}(p-1,q-1) \mid pq-1$. Also wäre $\frac{pq-1}{q-1} = p + \frac{p-1}{q-1}$ ganzzahlig, was für $p < q$ nicht möglich ist.

(6.3) Bemerkung: (Konstruktion von Carmichael-Zahlen)
Es sei t eine natürliche Zahl, so dass $p_1 = 6t+1$, $p_2 = 12t+1$ und $p_3 = 18t+1$ drei Primzahlen sind. Dann ist $n = p_1 p_2 p_3$ eine Carmichael-Zahl.
Zum Beispiel $t = 1$, $p_1 = 7$, $p_2 = 13$, $p_3 = 19$ und $n = 1729$.

Beweis: Es gilt

$$\begin{aligned} n-1 &= (6t+1)(12t+1)(18t+1)-1 = 36t(36t^2+11t+1)\,, \text{ und} \\ \lambda(n) &= \mathrm{kgV}(\lambda(p_1),\lambda(p_2),\lambda(p_3)) = \mathrm{kgV}(p_1-1,p_2-1,p_3-1) \\ &= \mathrm{kgV}(6t,12t,18t) \mid 36t\,, \end{aligned}$$

also ist $\lambda(n)$ ein Teiler von $n-1$ und n eine Carmichael-Zahl

Wir wollen nun den Begriff der a-Pseudoprimzahl so verschärfen, dass es das Carmichael-Problem nicht mehr gibt. Es sei n für alle a mit $\mathrm{ggT}(a,n)=1$ eine a-Pseudoprimzahl, also $a^{n-1}\equiv 1 \bmod n$. Ist $n=2m+1$ ungerade, so erhält man

$$n \mid a^{n-1}-1 = a^{2m}-1 = (a^m+1)(a^m-1)\,.$$

Ist nun n tatsächlich eine Primzahl, so folgte daraus

$$n \mid a^m+1 \ \vee \ n \mid a^m-1\,,$$

während bei zerlegbarem n dies nicht notwendig der Fall sein muss.

Man kann also für ungerades n die a-Pseudoprimzahlbedingung $a^{n-1}\equiv 1 \bmod n$ verschärfen zu $a^{(n-1)/2}\equiv \pm 1 \bmod n$. Diese Überlegung kann man nun für gerades $m=(n-1)/2$ fortsetzen:

Sei also $n=2^\alpha t+1$ mit $\alpha \geq 0$ und ungeradem t. Dann gilt

$$\begin{aligned} a^{n-1}-1 &= a^{2^\alpha t}-1 = (a^{2^{\alpha-1}t}+1)(a^{2^{\alpha-1}t}-1) \\ &= (a^{2^{\alpha-1}t}+1)(a^{2^{\alpha-2}t}+1)(a^{2^{\alpha-2}t}-1) \\ &= (a^{2^{\alpha-1}t}+1)(a^{2^{\alpha-2}t}+1)(a^{2^{\alpha-3}t}+1)\cdots(a^{2t}+1)(a^t+1)\cdot(a^t-1) \qquad (*) \end{aligned}$$

und n kann nur dann eine Primzahl sein, wenn n einen der in $(*)$ auftretenden Faktoren teilt, d. h. es gilt

$$n=2^\alpha t+1 \text{ Primzahl } \implies a^t\equiv 1 \bmod n \text{ oder } a^{2^\beta t}\equiv -1 \bmod n \text{ für ein } 0\leq\beta\leq\alpha-1\,.$$

(6.4) Definition: Sei $n=2^\alpha t+1$ mit $\alpha\geq 0$ und t ungerade sowie a prim zu n. Dann nennen wir n eine *starke a-Pseudoprimzahl*, wenn eine der folgenden Kongruenzen erfüllt ist:

$$a^t\equiv 1 \bmod n \text{ oder } a^{2^\beta t}\equiv -1 \bmod n \text{ für ein } 0\leq\beta\leq\alpha-1\,.$$

Die Definition ist so gefasst, dass formal n auch gerade sein kann. Für gerades n ist $\alpha=0$ und $t=n-1$, so dass sich hier der Begriff *starke a-Pseudoprimzahl* reduziert auf gewöhnliche *a-Pseudoprimzahl*.

Dies und die Vorüberlegungen zur Definition (6.4) (siehe Formel $(*)$) zeigen unmittelbar:

(6.5) Bemerkung: Es gilt für $n\in\mathbb{N}$ und alle $a\in\mathcal{P}(n)$:

$$n \text{ Primzahl } \implies n \text{ starke } a\text{-Pseudoprimzahl } \implies n \text{ } a\text{-Pseudoprimzahl}$$

Die letzte Implikation lässt sich nicht umkehren, da es sogar Carmichael-Zahlen gibt, die keine starken a-Pseudoprimzahlen sind. Z. B. ist $561=3\cdot 11\cdot 17$ eine Carmichael-Zahl, denn n ist ungerade, quadratfrei und $2\mid 560$, $10\mid 560$ und $16\mid 560$ (vgl. (6.2),(iii)), aber n ist keine starke 2-Pseudoprimzahl:

$$n-1=560=2^4\cdot 35\,,\ \text{also } t=35\,,\ \alpha=4\,,$$

und man berechnet mittels (3.3) folgende Kongruenzen modulo 561:

$$\begin{aligned} 2^{35} &\equiv 263 \not\equiv \pm 1\,, \\ 2^{70} &\equiv 263^2 \equiv 166 \not\equiv -1\,, \\ 2^{140} &\equiv 166^2 \equiv 67 \not\equiv -1\,, \\ 2^{280} &\equiv 67^2 \equiv 1 \not\equiv -1\,. \end{aligned}$$

Damit ist 561 keine starke 2-Pseudoprimzahl, obwohl 561 als Carmichael-Zahl nicht nur für $a = 2$, sondern sogar für alle a mit $\mathrm{ggT}(a, n) = 1$ eine a-Pseudoprimzahl ist.

Es sei noch bemerkt, dass der starke Pseudoprimzahltest nicht aufwendiger ist als der gewöhnliche. Statt direkt $a^{n-1} \bmod n$ zu berechnen, muss man $a^t \bmod n$ sowie dessen Quadrate berechnen und jeweils überprüfen, ob die Kongruenz zu ± 1 (für t) bzw. zu -1 (für die folgenden Quadrate) gegeben ist. Sobald dies einmal der Fall ist, ist n stark a-pseudoprim, sonst nicht. Hier ein konkretes Pascal-Programm, das dies leistet.

```
PROGRAM probable_prime;
uses primz;

VAR t,alpha,p,a,m,n:longint;
    pseudoprim:boolean;

FUNCTION mult(a,m,n:longint):longint;
VAR summe:longint;
BEGIN
   summe:=0;
   WHILE m<>0 DO
   BEGIN
      IF m mod 2 =1 then summe:=(summe+a) mod n;
      m:=m div 2;
      a:=(a+a) mod n ;
   END;
   mult:=summe;
END;

FUNCTION potenz(a,m,n:longint):longint;
VAR p:longint;
BEGIN
   p:=1;
   WHILE m<>0 DO
   BEGIN
     IF m mod 2  = 1 THEN p:=mult(p,a,n);
     m:= m div 2;
     a:=mult(a,a,n);
   END;
   potenz:=p;
END;

BEGIN
   Writeln('Ungerade Zahl n und Basis a eingeben: ');
   Readln(n,a);
   t:= n-1;
   alpha:=0;
```

```
   WHILE t mod 2 =0 DO BEGIN t:= t div 2; alpha:=alpha+1; END;
     Writeln(alpha);
   pseudoprim:=false;
   p:=potenz(a,t,n);
   IF (p=n-1) OR (p=1) THEN pseudoprim:=true;
   alpha:=alpha-1;
   WHILE (not pseudoprim) AND (alpha<>0) AND (p>1) DO
   BEGIN
     Writeln(alpha);
     p:=mult(p,p,n);
     alpha:=alpha-1;
     if p=n-1 then pseudoprim:=true;
   END;
   IF pseudoprim THEN Writeln(n,' ist wahrscheinlich prim.')
                 ELSE Writeln(n,' ist zerlegbar.');
END.
```

In diesem Programm ist die Funktion `potenz` eine Implementierung des Algorithmus (3.3) zur Potenzierung modulo n. Auf denselben Grundideen beruht die darin benutzte Funktion `mult` zur Multiplikation modulo n. (Auf die gewöhnliche Multiplikation natürlicher Zahlen angewandt auch als *Bauern-Multiplikation* bekannt: Schnelle Multiplikation allein mittels der Addition.)

Zum angestrebten Beweis, dass es das Analogon der Carmichael-Zahlen nicht gibt, benötigen wir den Begriff der quadratischen Reste:

(6.6) Definition: Sei p eine ungerade Primzahl und a eine natürliche Zahl mit $p \nmid a$. Dann definieren wir: a quadratischer Rest modulo $p \iff a \equiv x^2 \bmod p$ für ein x.

Zum Beispiel sind die quadratischen Reste modulo 7 gegeben durch 1, 2 und 4: $(\pm 1)^2 \equiv 1$, $(\pm 2)^2 \equiv 4$ und $(\pm 3)^2 \equiv 2$ modulo 7.

(6.7) Bemerkung: Ist p eine ungerade Primzahl, so gilt:
a) $x^2 \equiv y^2 \bmod p \iff x \equiv \pm y \bmod p$.
b) Es gibt $(p-1)/2$ quadratische Reste und genausoviele Nichtreste.

Beweis: a) Für eine Primzahl p gilt

$$p \mid x^2 - y^2 = (x+y)(x-y) \iff p \mid x+y \vee p \mid x-y\,.$$

b) Für $p \neq 2$ ist stets $x \not\equiv -x$ für alle $x \in \mathcal{P}(p)$, so dass zwei verschiedene $x \in \mathcal{P}(p)$ dasselbe Quadrat modulo p haben. Also gibt es halb soviele Quadrate wie es überhaupt prime Restklassen in $\mathcal{P}(p)$ gibt, d. h. $(p-1)/2$.

Den Zusammenhang zwischen quadratischen Resten und den Pseudoprimzahltests stellt das folgende Resultat von Euler her:

(6.8) Satz: (Euler) *Sei p eine ungerade Primzahl und a mit $p \nmid a$.*
Dann gilt: a quadratischer Rest modulo $p \iff a^{(p-1)/2} \equiv 1 \bmod p$.

Beweis: $\Rightarrow$: Ist $a \equiv x^2 \bmod p$ quadratischer Rest, so folgt gemäß (3.1)

$$a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \bmod p\,.$$

ad $\Leftarrow$: Sei $p = 2m+1$, also $m = (p-1)/2$, und a nicht quadratischer Rest. Wir zeigen dann zunächst $a^m \equiv (p-1)! \bmod p$: Dazu gruppieren wir in dem Produkt $(p-1)! = \prod_{i=1}^{p-1} i$ die Faktoren paarweise wie folgt: Wegen der Gruppeneigenschaft von $\mathcal{P}(p) = \mathbb{F}_p^\times$ gibt es zu jedem $1 \leq i < p$ genau ein i' mit $ii' \equiv a \bmod p$. Dabei kann nie $i \equiv i' \bmod p$ sein, da sonst $a \equiv i^2 \bmod p$ ein quadratischer Rest wäre. Also kann man in obigem Produkt $(p-1)/2 = m$ Paare $ii' \equiv a$ zusammenfassen, so dass insgesamt $(p-1)! \equiv a^m \bmod p$ folgt.

Die Behauptung von Satz (6.8) ergibt sich dann aus dem nachfolgenden Satz, denn für Primzahlen $p \neq 2$ erhalten wir $a^m \equiv (p-1)! \equiv -1 \not\equiv 1 \bmod p$.

(6.9) Satz: (Wilson) *Eine Zahl n ist genau dann Primzahl, wenn $(n-1)! \equiv -1 \bmod n$ ist.*

Beweis: Sei n zerlegt, also $n = pa$ mit $2 \leq p \leq a$ und p Primzahl. Im Falle $a = 2$, also $n = 4$, gilt $(n-1)! = 3! \equiv 2 \not\equiv -1 \bmod 4$.
Sei also jetzt $a > 2$. Dann gilt:

$$(n-1)! = a! \cdot \prod_{k=a+1}^{n-1} k\,.$$

Das letztgenannte Produkt enthält $n-1-a$ aufeinanderfolgende Faktoren. Nun ist $n-1-a = (p-1)a-1 \geq a-1 \geq p-1$. In dieser Ungleichungskette kann nicht überall Gleichheit gelten, da sonst $p-1 = 1$ und $a = p$, also $a = 2$ wäre. Also ist die Anzahl der Faktoren $n-1-a > p-1$, das obige Produkt enthält also mindestens p aufeinanderfolgende Faktoren. Mindestens einer davon ist dann durch p teilbar, also auch das Produkt. Damit folgt insgesamt

$$n = ap \mid a! \cdot p \mid (n-1)!\,,$$

so dass in diesem Falle $(n-1)! \equiv 0 \not\equiv 1 \bmod n$ ist.

Sei nun $n = p$ eine Primzahl. Ähnlich wie im Beweis von (6.8) wollen wir in dem Produkt für $(p-1)!$ die Faktoren in Paaren gruppieren, und diesmal so, dass $ii' \equiv 1 \bmod p$ ist. Hierbei kann nun $i \equiv i' \bmod p$ auftreten, aber dann ist $i^2 \equiv 1 \bmod p$, also $i = i' = 1$ oder $i = i' \equiv -1$. So erhält man

$$(p-1)! \equiv 1 \cdot (-1) \cdot \prod_i (ii') \equiv -1 \bmod p\,.$$

Wir wollen nun zeigen, dass eine Zahl n, die für alle a mit $\mathrm{ggT}(a,n) = 1$ eine starke a-Pseudoprimzahl ist, bereits tatsächlich prim sein muss.

(6.10) Satz: *Es gilt:*

$$n \text{ Primzahl} \iff \bigwedge_{a \in \mathcal{P}(n)} n \text{ starke } a\text{-Pseudoprimzahl}\,.$$

Beweis: $\Rightarrow$ gilt gemäß (6.5). Zum Beweis von $\Leftarrow$ muss man ausgehend von einem zerlegbaren n ein dazu primes a finden, so dass n keine starke a-Pseudoprimzahl ist.

1. Fall: n keine Carmichael-Zahl

Dann gibt es ein $a \in \mathcal{P}(n)$, so dass n keine a-Pseudoprimzahl, also erst recht keine starke a-Pseudoprimzahl ist.

2. Fall: n Carmichael-Zahl

Gemäß (6.2) ist n ungerade und quadratfrei, also $n = p \cdot m$ mit $p \neq 2$ Primzahl und $p \nmid m$, $m > 1$ ungerade. Weiter gilt $p-1 \mid n-1$. Setzen wir $n = 2^\alpha t + 1$, $p = 2^\beta u + 1$ mit $\alpha, \beta \geq 1$ und u, t ungerade, so gilt:

$$p-1 \mid n-1 \iff \beta \leq \alpha \ \wedge\ u \mid t\,.$$

Wir wählen nun a_p als quadratischen Nichtrest modulo p (existiert für ungerades p nach (6.7)). Gemäß (6.8) ist daher $a_p^{\frac{p-1}{2}} \not\equiv 1 \bmod p$ und wegen $(a_p^{\frac{p-1}{2}})^2 = a_p^{p-1} \equiv 1 \bmod p$ erhalten wir schließlich

$$a_p^{\frac{p-1}{2}} \equiv -1 \bmod p\,.$$

Nach dem Chinesischen Restsatz existiert ein $a \in \mathcal{P}(n)$ mit $a \equiv a_p \bmod p$, $a \equiv 1 \bmod m$. Wir wollen nun zeigen, dass n keine starke a-Pseudoprimzahl ist. Zunächst gilt

$$a^{2^{\beta-1}u} = a^{\frac{p-1}{2}} \equiv -1 \bmod p \implies a^{2^{\beta-1}t} \equiv (-1)^{\frac{t}{u}} \equiv -1 \bmod p\,. \tag{1}$$

Insbesondere folgt daraus

$$a^t \not\equiv 1 \bmod p \quad \text{und erst recht} \quad a^t \not\equiv 1 \bmod n \tag{2}$$

Und wegen $a \equiv 1 \bmod m \implies a^k \equiv 1 \not\equiv -1 \bmod m$ ($m > 2$!) gilt natürlich auch

$$a^k \not\equiv -1 \bmod n \text{ für alle } k\,. \tag{3}$$

Damit ist n keine starke a-Pseudoprimzahl.

Ob und inwieweit Satz (6.10) als Primzahltest geeignet und tatsächlich besser ist als der einfache Pseudoprimzahltest, hängt entscheidend davon ab, wie leicht bei einer zerlegbaren Zahl n ein a zu finden ist, für das n keine starke a-Pseudoprimzahl ist. Der Beweis von (6.10) zeigt, dass diese Frage mit quadratischen Resten zusammenhängt. Daher wollen wir zunächst diese etwas genauer studieren.

§7 Das quadratische Reziprozitätsgesetz

(7.1) Definition: Ist $p \neq 2$ eine ungerade Primzahl und a eine ganze Zahl, so definiert man das *Legendre-Symbol*

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{für } p \mid a, \\ +1 & \text{für } p \nmid a,\ a \text{ quadratischer Rest modulo } p, \\ -1 & \text{für } p \nmid a,\ a \text{ nicht quadratischer Rest modulo } p, \end{cases}$$

(7.2) Bemerkung: Ist $p \neq 2$ eine ungerade Primzahl und sind a, b ganze Zahlen, so gilt:

$$\begin{aligned} a \equiv b \bmod p \quad &\Rightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right), \\ p \nmid a \quad &\Rightarrow \quad \left(\frac{a^2}{p}\right) = 1\,, \\ \left(\frac{ab}{p}\right) \quad &= \quad \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \end{aligned}$$

Die ersten beiden Behauptungen ergeben sich unmittelbar aus der Definition. Auch die Multiplikativität des Legendre-Symbols (bei festem Modul) ist ohne weitere Hilfsmittel nachzuweisen (Übung), sie folgt aber unmittelbar aus dem Eulerschen Satz (6.8) bzw. dem daraus abgeleiteten folgenden

(7.3) Korollar: (Euler) *$p \neq 2$ ungerade Primzahl, $a \in \mathbb{Z}$. Dann gilt*

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

Beweis: Ist p ein Teiler von a, so sind beide Seiten 0 modulo p. Für $p \nmid a$ nimmt die linke Seite nur die Werte ± 1 an, je nachdem ob a quadratischer Rest modulo p ist. Dasselbe gilt auch für die rechte Seite von (7.3), denn es gilt $p \mid a^{p-1} - 1 = (a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1)$, also hat auch $a^{(p-1)/2}$ modulo p nur die Werte ± 1. Satz (6.8) gibt dann die behauptete Gleichheit.

Als weiteres Korollar erhalten wir aus (7.3)

(7.4) Korollar: *Für eine ungerade Primzahl p gilt*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \textit{für } p \equiv 1 \bmod 4, \\ -1 & \textit{für } p \equiv -1 \bmod 4. \end{cases}$$

Die nun folgende Methode zur Berechnung des Legendre-Symbols geht auf Gauß zurück. Sie ist zugleich ein wichtiger Schritt im Beweis des quadratischen Reziprozitätsgesetzes.

(7.5) Satz: (Gauß) *Sei $p = 2m + 1$ eine ungerade Primzahl und $a \in \mathbb{N}$ mit $p \nmid a$. Weiter seien für die ungeraden Zahlen $0 < k_1, \ldots, k_m < p$ die r_i $(i = 1, \ldots, m)$ definiert als*

$$r_i \equiv ak_i \bmod p\,,\ 0 < r_i < p\,.$$

Ist dann t die Anzahl der geraden Reste r_i, so gilt

$$\left(\frac{a}{p}\right) = (-1)^t\,.$$

Beweis: O. E. seien die k_i so nummeriert, dass $r_1, \ldots, r_t$ gerade und $r_{t+1}, \ldots, r_m$ ungerade sind. Also sind

$$0 < p - r_1, \ldots, p - r_t, r_{t+1}, \ldots, r_m < p \text{ ungerade.}$$

Wir zeigen, dass diese untereinander verschieden sind: Da die k_i modulo p inäquivalent sind, gilt dies auch für die $r_i \equiv ak_i$ $(a \in \mathcal{P}(p))$. Also sind $p - r_1, \ldots, p - r_t$ untereinander verschieden; ebenso die $r_{t+1}, \ldots, r_m$. Angenommen es gälte

$$p - r_i = r_j \text{ mit } 1 \le i \le t < j \le m\,.$$

Dann folgt

$$p = r_i + r_j \equiv ak_i + ak_j \equiv a(k_i + k_j) \bmod p\,.$$

Wegen $p \nmid a$ folgt $p \mid k_i + k_j$. Aber $0 < k_i + k_j < 2p$, also $p = k_i + k_j$. Dies ist aber nicht möglich, da k_i, k_j und p ungerade sind.

Damit ist gezeigt, dass $p - r_1, \ldots, p - r_t, r_{t+1}, \ldots, r_m$ verschiedene ungerade Zahlen zwischen 0 und p (ausschließlich) sind. Da ihre Anzahl gerade m ist, sind es genau die Zahlen $k_1, \ldots, k_m$. Daraus folgt

$$\begin{aligned}\prod_{i=1}^{m} k_i &= \prod_{i=1}^{t}(p - r_i) \prod_{j=t+1}^{m} r_j \equiv \prod_{i=1}^{t}(-r_i) \prod_{j=t+1}^{m} r_j \equiv (-1)^t \prod_{i=1}^{m} r_i \\ &\equiv (-1)^t \prod_{i=1}^{m}(ak_i) \equiv (-1)^t a^m \prod_{i=1}^{m} k_i \mod p\,.\end{aligned}$$

Kürzt man in dieser Kongruenz durch das Produkt (welches prim ist zu p), so folgt

$$1 \equiv (-1)^t \cdot a^m \bmod p$$

und damit aus Korollar (7.3) die Behauptung.

Als eine erste Anwendung des Gauß'schen Kriteriums berechnen wir den quadratischen Restcharakter von 2:

(7.6) Korollar: *Für ungerade Primzahlen p gilt:*

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{für } p \equiv \pm 1 \bmod 8 \\ -1 & \text{für } p \equiv \pm 3 \bmod 8 \end{cases}.$$

Zum *Beweis* untersuchen wir die Reste $r_i \equiv 2 \cdot (2i - 1) = 4i - 2 \bmod p$ für $1 \le i \le \frac{p-1}{2}$. Nun ist $r_i = 4i - 2$ (und damit gerade), solange $4i - 2 < p$, d. h. $i < \frac{p+2}{4}$ ist. Die weiteren Zahlen $4i - 2$ liegen zwischen p und $2p$, also ist für sie $r_i = 4i - 2 - p$ ungerade. Damit ist die Anzahl t der geraden positiven Reste von $2(2i - 1)$ modulo p gegeben durch

$$t = \lfloor \frac{p + 2}{4} \rfloor\,.$$

Wir untersuchen nun die verschiedenen Möglichkeiten für p modulo 8 (k bezeichne dabei eine natürliche Zahl)

$$\begin{aligned} p = 8k+1 &\Rightarrow t = \lfloor \frac{8k+3}{4} \rfloor = 2k\,, \\ p = 8k+3 &\Rightarrow t = \lfloor \frac{8k+5}{4} \rfloor = 2k+1\,, \\ p = 8k+5 &\Rightarrow t = \lfloor \frac{8k+7}{4} \rfloor = 2k+1\,, \\ p = 8k+7 &\Rightarrow t = \lfloor \frac{8k+9}{4} \rfloor = 2k+2\,, \end{aligned}$$

und entnehmen daraus

$$t \text{ gerade} \iff p \equiv \pm 1 \bmod 8\,.$$

Dies ist angesichts von Satz (7.5) genau die Behauptung.

Satz (7.5) ist nun auch die Basis des Gauß'schen Reziprozitätsgesetzes (von C. F. Gauß im Alter von 19 Jahren entdeckt):

(7.7) Satz: (Quadratisches Reziprozitätsgesetz) *Sind p, q ungerade Primzahlen, so gilt:*

$$\begin{aligned} \left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right) \quad \textit{für } p \equiv q \equiv -1 \bmod 4\,, \\ \left(\frac{p}{q}\right) &= +\left(\frac{q}{p}\right) \quad \textit{sonst}\,. \end{aligned}$$

Beweis: Die Aussage ist wahr (aber uninteressant) für $p = q$. Sei also im folgenden $p \neq q$. Wir benutzen Satz (7.5) und definieren dazu die folgenden Mengen:

$$\begin{aligned} T &= \{0 < r < p \mid r \text{ gerade},\ r \equiv qk \bmod p \text{ für ein ungerades } 0 < k < p\} \\ T' &= \{0 < r' < q \mid r' \text{ gerade},\ r' \equiv pk' \bmod q \text{ für ein ungerades } 0 < k' < q\} \end{aligned}$$

Gemäß Satz (7.5) gilt dann

$$\left(\frac{q}{p}\right) = (-1)^t \text{ mit } t = \#T\,, \qquad \left(\frac{p}{q}\right) = (-1)^{t'} \text{ mit } t' = \#T'$$

und folglich

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{t+t'}\,.$$

Zum Beweis des quadratischen Reziprozitätsgesetzes ist die Parität von $t + t'$ zu bestimmen. Nun ist

$$t + t' = \#(T \,\dot\cup\, (-T')) = \#\{r \mid r \in T \vee -r \in T'\}\,.$$

Wir geben eine andere Beschreibung für $T \,\dot\cup\, (-T')$: Dazu sei

$$M = \{r = qk - pk' \mid 0 < k < p\,,\ 0 < k' < q\,,\ k, k' \text{ ungerade}\}\,.$$

Für diese Menge gilt:
- Alle Zahlen in M sind gerade, denn q, k, p, k' sind ungerade;
- $0 \notin M$, da sonst $qk = pk'$ und wegen $p \neq q$ dann $p \mid k$ folgen würde.
- für verschiedene Paare (k, k') sind $qk - pk'$ voneinander verschieden, denn:

$$\begin{aligned} &qk - pk' = qk_1 - pk_1' \iff q(k - k_1) = p(k' - k_1') \\ &\Longrightarrow k \equiv k_1 \bmod p \ \wedge\ k' \equiv k_1' \bmod q \Longrightarrow k = k_1 \ \wedge\ k' = k_1'\,. \end{aligned} \qquad (*)$$

Es gilt dann

$$T \dot\cup (-T') = \{r \in M \mid -q < r < p\}\,.$$

Beweis: Ist $r \in M$ mit $0 \le r < p$, so ist $r \neq 0$ gerade und $r = qk - pk' \equiv qk \bmod p$ mit $0 < k < p$ ungerade, also $r \in T$. Sei umgekehrt $r \in T$, also $0 < r < p$ gerade und $r \equiv qk \bmod p$ mit $0 < k < p$ ungerade. Als kleinster positiver Rest von qk modulo p ist $r \le qk$ und damit folgt $r = qk - pk'$ für ein $k' \ge 0$. k' muss ungerade sein, da r gerade und q, k ungerade sind. Außerdem ist $k' = (qk - r)/p < (qp - r)/p < q$. Genauso geht man für $-r = pk' - qk$ und q vor. Insgesamt ist so gezeigt:

$$0 < r < p \wedge r \in M \iff r \in T\,, \qquad -q < r < 0 \wedge r \in M \iff -r \in T'\,.$$

Nun gibt es auf den positiven ungeraden Resten $0 < k < p$ modulo p eine natürliche Involution gegeben durch $k \mapsto p - 1 - k$, und entsprechend für q. Diese Involutionen induzieren eine Involution c auf M:

$$c : M \to M\,, \quad r = qk - pk' \mapsto q(p - 1 - k) - p(q - 1 - k') = p - q - r$$

Diese Involution bildet $M_0 := T \dot\cup (-T')$ in sich ab und induziert so eine Involution c auf M_0:

$$\begin{aligned} -q < r < p \quad &\iff \quad q > -r > -p \\ &\iff \quad p - q + q > p - q - r > p - q - p \\ &\iff \quad -q < p - q - r < p\,. \end{aligned}$$

Damit zerfällt M_0 disjunkt in die Menge M_0^c der Fixpunkte unter der Involution c und zweielementige Mengen von Elementen $\{a, a^c\}$. Dies bedeutet

$$t + t' = \#M_0 \equiv \#M_0^c \bmod 2\,.$$

Wir berechnen nun $\#M_0^c$. Zunächst gibt es in M höchstens einen Fixpunkt unter c, denn

$$\begin{aligned} & qk - pk' = q(p - 1 - k) - p(q - 1 - k') \\ \underset{(*)}{\iff} \quad & k = p - 1 - k \wedge k' = q - 1 - k' \iff k = \frac{p-1}{2} \wedge k' = \frac{q-1}{2}\,. \end{aligned}$$

Nun liegt $qk - pk'$ aber nur dann in M, wenn k und k' beide ungerade sind, d. h. es gibt dann und nur dann (genau) einen Fixpunkt in M, wenn $(p-1)/2$ und $(q-1)/2$ ungerade sind, wenn also $p \equiv q \equiv 3 \bmod 4$ ist. Dieser Fixpunkt liegt dann aber notwendig in M_0, denn

$$r = q \cdot \frac{p-1}{2} - p \cdot \frac{q-1}{2} = \frac{p-q}{2} \text{ und } -q < \frac{p-q}{2} < p\,.$$

Also ist gezeigt

$$t + t' \equiv \#M_0^c = \begin{cases} 1 & \text{falls } p \equiv q \equiv 3 \bmod 4, \\ 0 & \text{sonst.} \end{cases}$$

Damit folgt die Behauptung von (7.7)

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{t+t'} = \begin{cases} -1 & \text{falls } p \equiv q \equiv 3 \bmod 4, \\ +1 & \text{sonst.} \end{cases}$$

Beispiel für eine Berechnung des Legendre-Symbols:

$$\begin{aligned} \left(\tfrac{8039}{4363}\right) &= \left(\tfrac{-687}{4363}\right) = \left(\tfrac{-1}{4363}\right)\left(\tfrac{687}{4363}\right) = -\left(\tfrac{3}{4363}\right)\left(\tfrac{229}{4363}\right) \\ &= \left(\tfrac{4363}{3}\right)\left(\tfrac{4363}{229}\right) = \left(\tfrac{1}{3}\right)\left(\tfrac{12}{229}\right) = \left(\tfrac{2}{229}\right)^2\left(\tfrac{3}{229}\right) \\ &= \left(\tfrac{229}{3}\right) = \left(\tfrac{1}{3}\right) = +1 \end{aligned}$$

Man sieht, dass man durch das Reziprozitätsgesetz sehr schnell den Modul p reduzieren und so das Legendresymbol $\left(\frac{a}{p}\right)$ berechnen kann. Einen Nachteil hat diese Rechnung jedoch immer noch: Man muss an vielen Stellen vor der Anwendung des Reziprozitätsgesetzes die Primzerlegung des 'Zählers' a herstellen. Damit kann die Berechnung des Legendre-Symbols in dieser Form nicht sehr nützlich für Faktorisierungsalgorithmen oder Pseudoprimzahltests sein!

Dieses Problem wird gelöst durch die folgende einfache erweiterte Definition des Legendre-Symbols:

(7.8) Definition: Für eine ungerade natürliche Zahl b und $a \in \mathbb{Z}$ beliebig definieren wir das *Jacobi-Symbol* durch

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1 \cdots p_r}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right) \text{ für } b = p_1 \cdots p_r\,,\ p_i > 2 \text{ Primzahlen}\,.$$

Das Legendre-Symbol wird also zum Jacobi-Symbol ausgeweitet, indem man die Multiplikativität auch im 'Nenner' erzwingt.

Vorsicht: Ist a prim zu b und quadratischer Rest modulo b, so ist $\left(\frac{a}{m}\right) = 1$, aber i. a. *nicht umgekehrt*! Ist jedoch b prim, so gilt auch die Umkehrung.

Der Vorzug des Jacobi-Symbols besteht darin, dass es dieselben Gesetzmäßigkeiten besitzt wie das Legendre-Symbol, *aber nicht jeweils überprüft werden muss, ob die 'Nenner' prim sind*! Es müssen jeweils lediglich Vorzeichen und Zweierpotenzen abgespalten werden, damit die Argumente ungerade natürliche Zahlen sind.

(7.9) Satz: (Eigenschaften des Jacobi-Symbols)
Für ungerade natürliche Zahlen b, b' und $a, a' \in \mathbb{Z}$ gelten die folgenden Gesetzmäßigkeiten:

a) $\left(\frac{a}{b}\right) \in \{-1, 0, +1\}$, $\left(\frac{a}{b}\right) = 0 \iff \text{ggT}(a, b) \neq 1$

b) $a \equiv a' \bmod b \Longrightarrow \left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$

c) $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)\,, \quad \left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$

d) $\left(\frac{-1}{b}\right) = +1 \iff b \equiv 1 \bmod 4\,, \quad \left(\frac{-1}{b}\right) = -1 \iff b \equiv -1 \bmod 4$

e) $\left(\frac{2}{b}\right) = +1 \iff b \equiv \pm 1 \bmod 8\,, \quad \left(\frac{2}{b}\right) = -1 \iff b \equiv \pm 3 \bmod 8$

f) $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ *falls* $a \equiv 1 \bmod 4 \vee b \equiv 1 \bmod 4, a$ *ungerade,*
$\left(\frac{a}{b}\right) = -\left(\frac{b}{a}\right)$ *falls* $a \equiv b \equiv -1 \bmod 4$.

Beweis: a) folgt aus den entsprechenden Eigenschaften des Legendre-Symbols, ebenso b), denn $a \equiv a' \bmod b \Rightarrow a \equiv a' \bmod p_i$ $(i = 1, \ldots, r)$.
c) Die Multiplikativität im unteren Argument ist durch die Definition erzwungen, die Multiplikativität im oberen Argument galt bereits für das Legendre-Symbol.
Auch d) und f) ergeben sich aus den bekannten Gesetzmäßigkeiten für das Legendre-Symbol, wenn man benutzt

$$b = p_1 \cdots p_r \equiv 1 \bmod 4 \iff \#\{i \mid p_i \equiv -1 \bmod 4\} \text{ gerade}$$

Für e) benutzt man eine entsprechende Überlegung modulo 8.

Aufgrund dieser Gesetzmäßigkeiten für das Jacobi-Symbol kann man die obige Berechnung wie folgt abkürzen:

$$\begin{aligned}\left(\tfrac{8039}{4363}\right) &= \left(\tfrac{-687}{4363}\right) = -\left(\tfrac{687}{4363}\right) = \left(\tfrac{4363}{687}\right) = \left(\tfrac{241}{687}\right) \\ &= \left(\tfrac{687}{241}\right) = \left(\tfrac{-36}{241}\right) = \left(\tfrac{-1}{241}\right)\left(\tfrac{6}{241}\right)^2 = +1\,;\end{aligned}$$

insbesondere sind keine Primzerlegungen nötig. Lediglich Zweierpotenzen müssen gegebenenfalls abgespalten werden.

Wir wollen nun mit Hilfe des Jacobi-Symbols einen probabilistischen Primzahltest konzipieren, bei dem die Wahrscheinlichkeit, dass eine zerlegbare Zahl als prim erscheint, abgeschätzt werden kann.

(7.10) Satz: *Sei $n \geq 3$ ungerade. Dann gilt:*
a) n Primzahl $\iff a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$ *für alle* $a \in \mathcal{P}(n)$,
b) Sei A die Menge der $a \in \mathcal{P}(n)$, für die $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$ *erfüllt ist. Dann gilt für die relative Häufigkeit von A in $\mathcal{P}(n)$:*

$$n \text{ zerlegt} \implies \frac{\#A}{\#\mathcal{P}(n)} \leq \frac{1}{2}\,.$$

Ist also n zerlegbar, so ist die Wahrscheinlichkeit dafür, dennoch den probabilistischen Primzahltest aus a) für ein beliebig gewähltes $a \in \mathcal{P}(n)$ zu bestehen $\leq \frac{1}{2}$, bei k Iterationen dann $\leq \frac{1}{2^k}$.

Beweis: a) Es ist nur '$\Leftarrow$' zu beweisen. Aus der Voraussetzung folgt $a^{n-1} \equiv 1 \bmod n$ für alle $a \in \mathcal{P}(n)$, n ist also eine a-Pseudoprimzahl für alle a. Wäre nun n nicht prim, so wäre n eine Carmichael-Zahl (Def. (6.1)) und somit $n = p \cdot m$ mit $p \neq 2$ Primzahl und $p \nmid m$, $m > 2$ ungerade (Satz (6.2)). Sei a_p ein quadratischer Nichtrest modulo p und $a \in \mathcal{P}(n)$ mit

$$a \equiv \begin{cases} a_p & \bmod p, \\ 1 & \bmod m. \end{cases}$$

Dann gilt $\left(\frac{a}{p}\right) = \left(\frac{a_p}{p}\right) = -1$ und $\left(\frac{a}{m}\right) = 1$, zusammen also $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{m}\right) = -1$. Gemäß der Voraussetzung muss dann $a^{\frac{n-1}{2}} \equiv -1 \bmod n$, insbesondere $a^{\frac{n-1}{2}} \equiv -1 \bmod m$ sein. Dies widerspricht aber der Wahl von a: $a \equiv 1 \bmod m$.

b) A ist der Kern des Homomorphismus

$$\mathcal{P}(n) \to \mathcal{P}(n)\,, \quad a \mapsto a^{\frac{n-1}{2}} \cdot \left(\frac{a}{n}\right)\,.$$

Nach a) ist dieser Kern genau dann trivial, wenn n prim ist. Andernfalls ist sein Index in $\mathcal{P}(n)$ mindestens 2, seine relative Häufigkeit in $\mathcal{P}(n)$ also höchstens $\frac{1}{2}$.

§8 Primzahlnachweise

(8.1) Definition: Eine Zahl $w \in \mathbb{Z}$ heißt *Primitivwurzel* modulo n, wenn $w \bmod n$ die prime Restklassengruppe erzeugt:

$$w \text{ Primitivwurzel modulo } n \iff \mathcal{P}(n) = \langle w \bmod n \rangle\,,$$

oder m. a. W., wenn w prim ist zu n und $\operatorname{ord}(w \bmod n) = \varphi(n)$.
Eine Primitivwurzel mod n existiert also genau dann, wenn $\mathcal{P}(n)$ zyklisch ist.

Der folgende Satz ist in wesentlichen Teilen ein Korollar zu Satz (4.6):

(8.2) Satz: *Folgende Aussagen sind äquivalent:*

(i) Es gibt eine Primitivwurzel modulo n.

(ii) n ist eine der Zahlen 2, 4, p^k oder $2p^k$ mit einer ungeraden Primzahl p.

Beweis: (ii)⇒(i) wurde für $n = 2, 4, p^k$ ($p \neq 2$ Primzahl) in Satz (4.6) bewiesen. Wegen $\varphi(2p^k) = \varphi(p^k)$ für Primzahlen $p \neq 2$ ist $\mathcal{P}(2p^k) \simeq\!\!\to \mathcal{P}(p^k)$ und daher auch zyklisch. Überdies gilt: Ist w eine Primitivwurzel modulo p^k, so ist w oder $w+p^k$ ungerade und damit eine Primitivwurzel modulo $2p^k$.

Zum Beweis von (i)⇒(ii) muss man zeigen, dass alle anderen $\mathcal{P}(n)$ nicht zyklisch sind. Bereits aus Satz (4.6) ist bekannt, dass $\mathcal{P}(2^k)$ ($k \geq 3$) nicht zyklisch ist. Bleibt also zu zeigen:
Sind $k, l > 2$ teilerfremd, so ist $\mathcal{P}(kl)$ nicht zyklisch.

Beweis: Gemäß (4.6),a) ist die natürliche Abbildung $a \bmod kl \mapsto (a \bmod k, a \bmod l)$ ein Isomorphismus $\mathcal{P}(kl) \simeq\!\!\to \mathcal{P}(k) \times \mathcal{P}(l)$. Daher gilt gemäß Lemma (4.5),b):

$$\exp(\mathcal{P}(kl)) = \exp(\mathcal{P}(k) \times \mathcal{P}(l)) = \mathrm{kgV}(\exp(\mathcal{P}(k)), \exp(\mathcal{P}(l)) \mid \mathrm{kgV}(\varphi(k), \varphi(l))\,.$$

Nun sind für $k > 2$ und $l > 2$ sowohl $\varphi(k)$ als auch $\varphi(l)$ gerade, so dass gilt:

$$\mathrm{kgV}(\varphi(k), \varphi(l)) < \varphi(k)\varphi(l) = \varphi(kl)\,.$$

Es kann also kein $a \bmod kl$ die Ordnung $\varphi(kl)$ haben, d. h. es gibt keine Primitivwurzel modulo kl.

Wir wollen nun unsere Resultate über Primitivwurzeln benutzen für Primzahl*nachweise*. Die wichtigen Pseudoprimzahltests (§6,7) sind probabilistischer Natur: Sie liefern als Ergebnis entweder, dass eine Zahl nachweislich zerlegbar ist, oder aber, dass sie mit (hoher) Wahrscheinlichkeit prim ist; sie liefern im letzteren Fall aber keine Gewissheit, dass eine Primzahl vorliegt. Die folgenden Überlegungen zeigen, wie man dann einen Primzahl*nachweis* führen kann. Sie sollten aber nur angewendet werden, wenn die Zahl etliche Pseudoprimzahltests 'bestanden' hat.

Im Kern stellen diese Überlegungen eine Reduktion dar: Ist die Primzerlegung von $n-1$ (weitgehend) bekannt, so kann man für die (wahrscheinliche) Primzahl n die Primzahleigenschaft *nachweisen*. Man erhält so eine Reduktion des Primzahlnachweises für n auf die Primteiler von $n-1$. Kern der Überlegungen ist die folgende Äquivalenz

$$\mathrm{ord}(a \bmod n) = n-1 \iff n \text{ Primzahl } \wedge\ a \text{ Primitivwurzel modulo } n\,.$$

'⇐': Ist n eine Primzahl und a eine Primitivwurzel modulo n, so ist $\mathrm{ord}(a \bmod n) = \varphi(n) = n-1$.
'⇒': Es ist $n-1 = \mathrm{ord}(a \bmod n) \mid \varphi(n) \leq n-1$, also $\mathrm{ord}(a \bmod n) = \varphi(n) = n-1$. Die erste Gleichheit besagt aber gerade, dass a eine Primitivwurzel modulo n ist, und die zweite Gleichheit $\varphi(n) = n-1$ bedeutet, dass alle Restklassen $1, \ldots, n-1$ zu n teilerfremd sind, dass n also eine Primzahl ist.

Da es für Primzahlen n stets Primitivwurzeln a gibt, gilt also:

$$n \text{ Primzahl} \iff \bigvee_{a \in \mathcal{P}(n)} \mathrm{ord}(a \bmod n) = n-1\,.$$

Man kann also versuchen, für ein a die Eigenschaft $\mathrm{ord}(a \bmod n) = n-1$ nachzuweisen. Dazu zeigt man zunächst, dass $a^{n-1} \equiv 1 \bmod n$, also n eine a-Pseudoprimzahl (Def. (3.2)) ist. Der Nachweis, dass die Ordnung von $a \bmod n$ genau $n-1$ ist, ist dann relativ leicht durchzuführen, *wenn die Primzerlegung von* $n-1$ *bekannt ist*:

- Ist $a^{n-1} \equiv 1 \bmod n$ und $n-1 = p_1^{\nu_1} \cdots p_r^{\nu_r}$ die Primzerlegung von $n-1$, so gilt:

$$\mathrm{ord}(a \bmod n) = n-1 \iff a^{(n-1)/p_i} \not\equiv 1 \bmod n \text{ für alle } i\,.$$

Denn, nach Voraussetzung ist die Ordnung von $a \bmod n$ ein Teiler von $n-1$ und genau dann ein *echter* Teiler von $n-1$, wenn für ein p_i $a^{(n-1)/p_i} \equiv 1 \bmod n$ ist.

Fasst man beide Überlegungen zusammen, so erhält man für Zahlen n mit bekannter Primzerlegung $n-1 = p_1^{\nu_1} \cdots p_r^{\nu_r}$ von $n-1$:

$$n \text{ Primzahl} \iff \bigvee_{a \in \mathcal{P}(n)} a^{n-1} \equiv 1 \bmod n \ \wedge \ \bigwedge_{i=1}^{r} a^{(n-1)/p_i} \not\equiv 1 \bmod n\,. \qquad (*)$$

Ein Primzahlnachweis für eine (wahrscheinliche) Primzahl n erfordert also den Nachweis der rechten Seite von $(*)$ (wozu alle Primteiler von $n-1$ bekannt sein müssen). Nun kann die Verifikation dieser Eigenschaft aus zwei Gründen misslingen: Entweder ist n keine Primzahl (was sehr unwahrscheinlich sein sollte) oder a wurde falsch gewählt, d. h. a ist keine Primitivwurzel modulo n. Letzteres kann natürlich sehr wohl eintreten: Unter den $n-1$ primen Restklassen modulo einer Primzahl n gibt es $\varphi(n-1)$ viele Primitivwurzeln. Je kleiner $\varphi(n-1)$ ist, desto schwieriger der Nachweis der rechten Seite von $(*)$.

Hier hilft nun die nachfolgende Verschärfung von $(*)$, derzufolge man die Quantoren in $(*)$ vertauschen kann (was natürlich a priori nicht klar ist). Dies bedeutet dann, dass man nicht unbedingt eine Primitivwurzel a modulo n finden muss, um die Primzahleigenschaft nachzuweisen.

(8.3) Proposition: *Es sei n eine natürliche Zahl und $n-1 = p_1^{\nu_1} \cdots p_r^{\nu_r}$ die Primzerlegung von $n-1$. Dann gilt:*

$$n \textit{ ist Primzahl} \iff \bigwedge_{i=1}^{r} \bigvee_{a_i \in \mathbb{Z}} a_i^{n-1} \equiv 1 \bmod n \ \wedge \ a_i^{(n-1)/p_i} \not\equiv 1 \bmod n\,.$$

Beweis: Nach den obigen Überlegungen ist nur '$\Leftarrow$' zu beweisen. Wegen $a_i^{n-1} \equiv 1 \bmod n$ ist a_i teilerfremd zu n, also $a_i \in \mathcal{P}(n)$, und für $d_i = \operatorname{ord}(a_i \bmod n)$ gilt nach Voraussetzung

$$d_i \mid n-1 = p_1^{\nu_1} \cdots p_r^{\nu_r}\,, \text{ aber } d_i \nmid \frac{n-1}{p_i}\,, \text{ also } p_i^{\nu_i} \mid d_i\,.$$

Nun sind aber alle d_i Teiler von $\varphi(n)$, so dass folgt

$$p_i^{\nu_i} \mid \varphi(n) \text{ für alle } i\,,$$

also

$$n-1 = p_1^{\nu_1} \cdots p_r^{\nu_r} \mid \varphi(n) \le n-1\,.$$

Damit ist $n-1 = \varphi(n)$ und n eine Primzahl.

(8.4) Beispiel: $n = 61\,89700\,19642\,69013\,74495\,62111$ ist eine Primzahl.

Nachweis: Zunächst spalten wir von $n-1$ 'kleine' Primfaktoren ab (Algorithmus (5.1), etwa mit $p_{\max} = 31607$, dem größten Eintrag einer mit dem Sieb des Erathostenes erstellten Primzahltafel. Man erhält dann die Zerlegung

$$n-1 = 2 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89 \cdot 353 \cdot 397 \cdot 683 \cdot 2113 \cdot 2931542417$$

wobei alle Faktoren, außer evtl. dem letzten, Primzahlen sind. Der letzte Faktor $m = 2931542417$ besitzt keine Primteiler ≤ 31607. Wegen $\sqrt{2931542417} > 31607$ ist damit aber noch nicht sicher, ob m ebenfalls prim ist.

Um dies zu überprüfen, benutzen wir erneut das obige Kriterium und bestimmen die 'kleinen' Primfaktoren von $m-1 = 2931542416$. Wir erhalten (mit demselben $p_{\max} = 31607$) eine vollständige Primzerlegung

$$m-1 = 2^4 \cdot 11 \cdot 1913 \cdot 8707\,.$$

Wir wollen nun zeigen, dass m prim ist, indem wir (8.3) anwenden. Wir finden $2^{m-1} \equiv 1 \bmod m$, aber auch $2^{\frac{m-1}{2}} \equiv 1 \bmod m$, so dass $a = 2$ nicht geeignet ist. (Dies ergibt sich auch daraus, dass

$m \equiv 17 \equiv 1 \bmod 8$ und somit $\left(\frac{2}{m}\right) \underset{=}{=} +1$ ist, siehe (7.3).) Aber bereits $a = 3$ erfüllt alle Bedingungen von (8.3) (bzw. bereits der Vorstufe $(*)$): 3 ist Primitivwurzel mod m und m prim.

Damit ist die obige Zerlegung von $n-1$ die vollständige Primzerlegung, und wir können nun (8.3) auf n anwenden. Wieder finden wir 3 als Primitivwurzel mod n, indem wir $3^{n-1} \equiv 1 \bmod n$ nachweisen, sowie für alle 11 Primfaktoren p_i von $n-1$ zeigen $3^{\frac{n-1}{p_i}} \not\equiv 1 \bmod n$. Damit ist n nachweislich prim.

Der Primzahlnachweis für $n = 61\,89700\,19642\,69013\,74495\,62111$ besteht aus einer Hierarchie von Primzahlnachweisen, deren einzelne Schritte mit den nachstehenden Angaben leicht überprüfbar sind. Die nachfolgenden Fakten stellen sozusagen ein 'Primzahlzertifikat' dar:
a) Primzerlegung $2931542416 = 2^4 \cdot 11 \cdot 1913 \cdot 8707$;
b) 2931542417 ist prim gemäß (8.3) mit $a_i = a = 3$;
c) Primzerlegung $n-1 = 61\,89700\,19642\,69013\,74495\,62110 = 2 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89 \cdot 353 \cdot 397 \cdot 683 \cdot 2113 \cdot 2931542417$,
d) $n = 61\,89700\,19642\,69013\,74495\,62111$ ist prim gemäß (8.3) mit $a_i = a = 3$.

Anmerkung: Man erhält eine deutliche Erleichterung, wenn man bei der Abspaltung der 'kleinen' Primfaktoren etwa eine Primzahltafel bis zu der etwas größeren Schranke $p_{\max} = 2^{16} = 65536$ zur Verfügung hat. Dann erhält man wie oben

$$n - 1 = 2 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89 \cdot 353 \cdot 397 \cdot 683 \cdot 2113 \cdot 2931542417$$

wobei nun der letzte Faktor m keinen Primfaktor $\le p_{\max} = 2^{16}$ enthält. Wegen $m \le 2^{32} = p_{\max}^2$ zeigt somit bereits Algorithmus (5.1), dass m prim ist.

Man kann nun die Voraussetzung von (8.3) noch ein wenig abschwächen, so dass man nicht sämtliche Primteiler von $n-1$ benötigt.

(8.5) Satz: *Es sei $n \ge 2$ eine natürliche Zahl und für $n-1$ sei eine partielle Zerlegung bekannt:*

$$n - 1 = A \cdot B\,,\ A = p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}\ \textit{Primzerlegung.}$$

Dann gilt im Falle $A \ge \sqrt{n}$:

$$n\ \textit{Primzahl} \iff \bigwedge_{i=1}^{r} \bigvee_{a_i \in \mathbb{Z}} a_i^{n-1} \equiv 1 \bmod n\ \wedge\ \mathrm{ggT}(a_i^{(n-1)/p_i} - 1, n) = 1\,.$$

Beweis: '$\Rightarrow$' ist eine Abschwächung von (8.3), denn für eine Primzahl n gilt $a_i^{(n-1)/p_i} \not\equiv 1 \bmod n \iff \mathrm{ggT}(a_i^{(n-1)/p_i} - 1, n) = 1$.
Für '$\Leftarrow$' fixieren wir zunächst einen beliebigen Primteiler p von n und setzen dann $n_i := \mathrm{ord}(a_i \bmod p)$. Dann gilt

$$n_i \mid p - 1\,. \tag{1}$$

Andererseits gilt nach Voraussetzung $a_i^{n-1} \equiv 1 \bmod n$, also erst recht $a_i^{n-1} \equiv 1 \bmod p$. Dies bedeutet

$$n_i \mid n - 1\,. \tag{2}$$

Schließlich folgt aus $\mathrm{ggT}(a_i^{(n-1)/p_i} - 1, n) = 1$ insbesondere $p \nmid a_i^{(n-1)/p_i} - 1$, oder mit anderen Worten $a_i^{(n-1)/p_i} \not\equiv 1 \bmod p$. Dies bedeutet

$$n_i \nmid \frac{n-1}{p_i}\,. \tag{3}$$

Angesichts der Faktorisierung von $n-1$ folgt aus (2) und (3)

$$p_i^{\nu_i} \mid n_i\,,$$

also mit (1) $p_i^{\nu_i} \mid p-1$ für alle i und folglich $A \mid p-1$:

$$p \equiv 1 \bmod A \quad \text{für alle Primteiler } p \text{ von } n. \tag{4}$$

Ist nun $A \geq \sqrt{n}$, so folgt daraus

$$p > p-1 \geq A \geq \sqrt{n} \text{ für jeden Primteiler } p \text{ von } n\,,$$

und n muss prim sein, denn eine zerlegbare Zahl n besitzt stets einen Primteiler $p \leq \sqrt{n}$.

Anmerkungen:
1. Man beachte, dass (4) *ohne* die Voraussetzung $A \geq \sqrt{n}$ bewiesen wurde. Die Gültigkeit der rechten Seite von (8.5) liefert dann zwar keinen Primzahlnachweis mehr für n, aber (4) zeigt, dass n nur Primfaktoren $p \equiv 1 \bmod A$ besitzen kann.
2. Unter Verwendung von (8.5) ist in Beispiel (8.4) der Primzahlnachweis von m nicht nötig: Man wendet (8.5) auf die gefundene partielle Primzerlegung von $n-1$ an mit $B = m$. Da $B^2 = m^2 < n$ ist, ist die Voraussetzung $A \geq \sqrt{n}$ erfüllt und man muss dann für die 10 Primteiler von A die Bedingungen der rechten Seite von (8.5) nachweisen.

Abschließend wollen wir nun zeigen, wie man diese Resultate benutzen kann, um besonders effiziente Primzahlnachweise *für spezielle Zahlen* zu entwickeln.

Wir betrachten Zahlen der speziellen Gestalt $n = 2^a \pm 1$ und untersuchen diese auf Primalität. Bei der Diskussion der Mersenne-Zahlen hatten wir bereits gezeigt

$$2^a - 1 \text{ Primzahl } \implies a = p \text{ Primzahl}\,,$$

als Mersenne-Primzahlen kommen also nur Zahlen der Form $2^p - 1$, p prim, in Frage. Für Mersenne-Zahlen gibt es besonders effiziente Algorithmen zum Nachweis der Primalität (Lucas-Folgen). Sie sind der Grund dafür, dass die größten bekannten Primzahlen bislang immer Mersenne-Primzahlen sind.

Wir wollen hier die 'Gegenstücke' dazu betrachten, die Zahlen der Form $n = 2^a + 1$. Für diese gilt:

$$2^a + 1 \text{ Primzahl } \implies a = 2^k \text{ 2-Potenz.}$$

Der Beweis dieser Tatsache beruht auf derselben Überlegung wie früher für die Mersenne'schen Zahlen. Angenommen a ist keine 2-Potenz, also $a = b \cdot c$ mit einer *ungeraden* Zahl $c > 1$. Dann gilt

$$2^a + 1 = 2^{bc} + 1 = \frac{(2^b)^c - (-1)^c}{2^b - (-1)} \cdot (2^b + 1)\,,$$

wobei der erste Faktor aufgrund der bekannten Formel

$$\frac{x^n - y^n}{x - y} = x^{n-1} + x^{n-2}y + \ldots + y^{n-1}$$

eine ganze Zahl ist. Wegen $1 < 2^b + 1 < 2^a + 1$ wäre $2^b + 1$ ein *echter* Teiler und $2^a + 1$ damit zerlegbar.

Wir betrachten also im folgenden die *Fermat-Zahlen*

$$F_k = 2^{2^k} + 1 \ (k = 0, 1, 2, \ldots)$$

und wollen diese auf Primalität untersuchen. Die ersten davon sind Primzahlen:

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

(8.6) Satz: *Für $k \in \mathbb{N}$, $k \geq 1$ gilt:*

$$F_k = 2^{2^k} + 1 \textit{ ist Primzahl} \iff 3^{(F_k-1)/2} \equiv -1 \bmod F_k\,.$$

Da $(F_k - 1)/2 = 2^{2^k - 1}$ eine 2-Potenz ist, kann die rechte Seite durch $2^k - 1$-faches Quadrieren modulo F_k berechnet werden.

Beweis: '$\Leftarrow$' ist die schwache Vorstufe $(*)$ von (8.3), denn: $3^{(F_k-1)/2} \equiv -1 \bmod F_k \Rightarrow 3^{F_k-1} \equiv +1 \bmod F_k$, womit dann beide Forderungen in $(*)$ (für den einzigen Primteiler $p = 2$ von $F_k - 1$) erfüllt sind.

'$\Longrightarrow$': Mit dem Beweis dieser Richtung, zeigen wir nun, dass die sehr scharfe Forderung von $(*)$ tatsächlich erfüllt sein *muss*, und zwar für die (von k unabhängige) Basis $a = 3$:
Sei F_k eine Primzahl. Dann gilt nach (7.3)

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

Wir berechnen daher das Legendre-Symbol von 3 modulo F_k. Mit dem quadratischen Reziprozitätsgesetz (7.7) bzw. (7.9),f) erhalten wir wegen $F_k \equiv 1 \bmod 4$

$$\left(\frac{3}{F_k}\right) = \left(\frac{F_k}{3}\right) = \left(\frac{-1}{3}\right) = -1\,.$$

Dabei folgt die vorletzte Gleichheit für $k \geq 1$ aus

$$F_k = 2^{2^k} + 1 \equiv (-1)^{2^k} + 1 = 1 + 1 \equiv -1 \bmod 3\,.$$

Anmerkung: Für $k \geq 2$ erhält man dieselbe Aussage wie (8.6) mit der Basis 5 statt 3.

Unter Verwendung dieses Kriteriums zeigt man nun leicht:

$$F_4 = 65537 \text{ ist prim, aber } F_5 = 4\,294\,967\,297 \text{ ist zerlegbar.}$$

Die Zerlegbarkeit von F_5 wurde bereits von Euler gezeigt, der 641 als Teiler von F_5 nachwies.

§9 Der $(p+1)$-Primzahltest; Mersenne-Primzahlen

Die Basis des oben dargestellten Primzahltestes war die Gruppe $\mathcal{P}(n)$, deren bekannte Ordnung $\#\mathcal{P}(n) = \varphi(n) \leq n-1$ und Struktur ($\mathcal{P}(p) = \mathbb{F}_p^\times$ zyklisch) sowie die darauf aufbauende Tatsache (siehe S. 41)

$$n \text{ prim} \iff \bigvee_{a \in \mathcal{P}(n)} \operatorname{ord}(a \bmod n) = n - 1\,. \qquad (*)$$

Dies hatte einen Primzahltest für solche Zahlen n zur Folge, für die $n-1$ (fast) vollständig in Primfaktoren zerlegt werden konnte (siehe (8.3) und (8.5)). Dazu gehörten insbesondere die Zahlen der Form $n = 2^m + 1$.

Wir wollen nun ein Gegenstück dazu kennenlernen, bei dem man eine Faktorisierung von $n+1$ benötigt. Dazu konstruieren wir eine andere Gruppe $G(n)$ (keine standardisierte Bezeichnung) mit der Eigenschaft:

$$n \text{ prim} \iff \bigvee_{\xi \in G(n)} \operatorname{ord}(\xi) = n + 1\,.$$

Dabei ist analog zu oben $G(p)$ zyklisch von der Ordnung $p+1$.

Wir wollen zunächst diese Gruppe für $n = p > 2$ prim konstruieren. Es sei $\mathbb{F}_p$ der Primkörper von p Elementen und $D \in \mathbb{Z}$ mit $\left(\frac{D}{p}\right) = -1$ ein quadratischer Nichtrest, also $\alpha = (D \bmod p) \in \mathbb{F}_p$ kein Quadrat. Dann ist $K = \mathbb{F}_p[\sqrt{\alpha}]$ eine quadratische Körpererweiterung, also $\#K = p^2$. Als Multiplikationsgruppe eines endlichen Körpers ist $K^\times$ eine zyklische Gruppe (siehe Beweis von Satz (4.6),c)) der Ordnung $p^2 - 1 = (p+1)(p-1)$. Diese enthält eine (zyklische) Untergruppe der Ordnung $p+1$. Wir wollen diese als die sog. *Normeinsuntergruppe* beschreiben. Dazu betrachten wir folgende Abbildungen von $K = \mathbb{F}_p[\sqrt{\alpha}]$:

1) Die Konjugation $K \to K$: $\xi = x + y\sqrt{\alpha} \mapsto \bar{\xi} = x - y\sqrt{\alpha}$.
2) Die Spur $\mathrm{Tr} : K \to k$: $\xi \mapsto \xi + \bar{\xi}$.
3) Die Norm $\mathcal{N} : K^\times \to k^\times$: $\xi \mapsto \xi \cdot \bar{\xi}$.

Die Konjugation ist der einzige nicht-triviale Körperautomorphismus von K, der $k = \mathbb{F}_p$ elementweise festlässt; Tr ist ein additiver Homomorphismus und $\mathcal{N}$ ein multiplikativer vom Erweiterungskörper in den Grundkörper. Die Konjugation kann auch als der sog. *Frobeniusautomorphismus* $\xi \mapsto \xi^p$ beschrieben werden. Um dies zu sehen, zeigt man zunächst, dass $\xi \mapsto \xi^p$ ein Homomorphismus ist und dass für $\xi = x \bmod p \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ gilt: $\xi^p = x^p \bmod p = x \bmod p = \xi$ (vgl. Fußnote auf S. 15). Aus Anzahlgründen sind die $\xi \in k$ *genau* die Fixpunkte des Frobeniusautomorphismus. Dieser ist also auch ein nicht-trivialer Automorphismus, der k fest lässt, muss also gleich der Konjugation sein. Damit folgt dann: $\mathcal{N}\xi = \xi \cdot \bar{\xi} = \xi^{p+1}$.

Die Normeinsgruppe ist der Kern der Normabbildung:

$$\{\xi \in K \mid \mathcal{N}\xi = 1\} = \{\xi \in K \mid \xi^{p+1} = 1\}\,.$$

Diese Gruppe besteht aus allen Elementen von $K^\times$, deren Ordnung $p+1$ teilt. Da $K^\times$ zyklisch von der Ordnung $p^2 - 1 = (p+1)(p-1)$ ist, hat diese die genaue Ordnung $p+1$.

Wir fassen zusammen

(9.1) Proposition: *Sei $p > 2$ eine Primzahl und $D \in \mathbb{Z}$ ein quadratischer Nichtrest modulo p. Sei $\alpha = D \bmod p \in \mathbb{F}_p$ und $K = \mathbb{F}_p[\sqrt{\alpha}]$ die entsprechende quadratische Körpererweiterung. Dann ist die Normeinsuntergruppe*

$$\{\xi \in \mathbb{F}_p[\sqrt{\alpha}] \mid \mathcal{N}\xi = 1\}$$

eine zyklische Untergruppe der Ordnung $p+1$.

Wir wollen diese Konstruktion nun von Primzahlen p auf beliebige Zahlen n und weitgehend beliebige D ausweiten. Wir betrachten teilerfremde $n, D \in \mathbb{N}$ und konstruieren einen Erweiterungsring von $R = \mathbb{Z}/n\mathbb{Z}$:

$$Z(n,D) = \left\{A \in M_2(R) \mid A = \begin{pmatrix} x & Dy \\ y & x \end{pmatrix},\ x, y \in R = \mathbb{Z}/n\mathbb{Z}\right\}.$$

Dies ist offensichtlich ein Ring mit Eins; er ist sogar kommutativ. Jedes Element in $Z(n,D)$ ist eindeutig darstellbar als $A = xE + yW$ mit der Einheitsmatrix E und der Matrix

$$W = \begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix}.$$

Damit ist R vermöge der Abbildung $x \mapsto xE$ ein Unterring von $Z(n,D)$. Wegen $W^2 = DE$ ist W eine Quadratwurzel aus D. Die Multiplikation in $Z(n,D)$ lautet wie folgt:

$$(x_1E + y_1W)(x_2 + y_2W) = (x_1x_2 + Dy_1y_2)E + (x_1y_2 + x_2y_1)W$$

und ist genau die Multiplikation von Termen der Form $x + y\sqrt{D}$, wie wir sie für quadratische Körpererweiterungen kennen. Nur dass die obigen Überlegungen für Ringe und auch dann gelten, wenn $D \in R$ ein Quadrat in R ist!

Wir betrachten vorweg den (für uns weniger interessanten) Fall, dass D ein Quadrat modulo n ist:

(9.2) Proposition: *Seien $n \in \mathbb{N}$ ungerade und $D \in \mathcal{P}(n)$ ein Quadrat in $\mathcal{P}(n)$: $D \equiv a^2 \bmod n$ für ein $a \in \mathcal{P}(n)$. Dann gilt:*

$$Z(n,D) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\,,\ xE + yW \mapsto (x + ay, x - ay)\,.$$

Beweis: Die angegebene Abbildung ist bijektiv mit der Umkehrabbildung

$$(u,v) \mapsto \frac{u+v}{2}E + \frac{u-v}{2a}W\,.$$

(Beachten Sie, dass nicht nur a, sondern auch 2 modulo n invertierbar, also $2a$ Einheit in R ist.) Zur Homomorphie beachte man, dass alle Matrizen simultane Eigenvektoren besitzen:

$$\begin{pmatrix} x & a^2y \\ y & x \end{pmatrix} \begin{pmatrix} \pm a \\ 1 \end{pmatrix} = (x \pm ay) \cdot \begin{pmatrix} \pm a \\ 1 \end{pmatrix} .$$

Die Eigenwerte sind $x \pm ay$, und diese hängen (bei unveränderlichen Eigenvektoren!) homomorph von der Matrix A ab. □

Uns wird im folgenden vornehmlich der Fall interessieren, dass D kein Quadrat in $R = \mathbb{Z}/n\mathbb{Z}$ ist. Wir betrachten in Analogie zum Körperfall folgende Abbildungen von $Z(n, D)$:

1) Die Konjugation: $\xi = x + yW \mapsto \bar{\xi} = x - yW$.

2) Die Spur Tr: $\xi = x + yW \mapsto \xi + \bar{\xi} = 2x$.

3) Die Norm $\mathcal{N}$: $\xi = x + yW \mapsto \xi \cdot \bar{\xi} = x^2 - y^2 D$.

Man beachte, dass Tr die übliche Matrixspur (Summe der Diagonalelemente) und $\mathcal{N}$ die Determinante ist! Tr ist additiv, $\mathcal{N}$ multiplikativ. Die Bilder liegen im Grundring R.

Wir betrachten nun in diesen Ringen die Einheitengruppe $U(n, D) = Z(n, D)^\times$. Es gilt

$$U(n, D) = \{A \in Z(n, D) \mid \det A \in R^\times = \mathcal{P}(n)\} ,$$

denn mit A hat auch die Adjunkte A^{ad} (gebildet aus den $(n-1)$-reihigen Unterdeterminanten) Koeffizienten in $R = \mathbb{Z}/n\mathbb{Z}$ und es gilt

$$A \cdot A^{\mathrm{ad}} = \det A \cdot E .$$

Wenn also $\det A$ zu $\mathcal{P}(n) = (\mathbb{Z}/n\mathbb{Z})^\times$ gehört, ist $A^{-1} = \frac{1}{\det A} \cdot A^{\mathrm{ad}} \in Z(n, D)$ und A eine Einheit in $Z(n, D)$.

In $U(n, D)$ betrachten wir nun die Normeinsuntergruppe

$$U_1(n, D) = \{A \in Z(n, D) \mid \det A = 1\} .$$

Aus dem Chinesischen Restsatz erhält man für teilerfremde n_1, n_2:

$$\begin{aligned} Z(n_1 n_2, D) &\simeq Z(n_1, D) \times Z(n_2, D) , \\ U(n_1 n_2, D) &\simeq U(n_1, D) \times U(n_2, D) , \\ U_1(n_1 n_2, D) &\simeq U_1(n_1, D) \times U_1(n_2, D) . \end{aligned}$$

Wir brauchen diese Strukturen also nur für Primzahlpotenzen $n = p^k$ zu studieren. Den Fall $k = 1$, d. h. $n = p$ prim, haben wir im wesentlichen bereits oben erledigt:

$$Z(p, D) \simeq \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \text{falls } \left(\frac{D}{p}\right) = +1 \\ \mathbb{F}_p[\sqrt{D}] \simeq \mathbb{F}_{p^2} & \text{falls } \left(\frac{D}{p}\right) = -1 \end{cases}$$

Für die Gruppen ergibt sich so in den entsprechenden Fällen

$$U(p, D) \simeq \begin{cases} \mathbb{F}_p^\times \times \mathbb{F}_p^\times \simeq C_{p-1} \times C_{p-1} \\ \mathbb{F}_{p^2}^\times \simeq C_{p^2-1} \end{cases}$$

wobei C_d die zyklische Gruppe der Ordnung d bezeichne. Für U_1, den Kern der Determinante, ergibt sich dann

$$U_1(p, D) \simeq \begin{cases} \mathbb{F}_p^\times \simeq C_{p-1} \\ C_{p+1} \end{cases}$$

Begründung: Im ersten Fall $\left(\frac{D}{p}\right) = 1$ gilt $U(p, D) \simeq \mathbb{F}_p^\times \times \mathbb{F}_p^\times$ vermöge $\xi = xE + yW \mapsto (u, v) = (x + ay, x - ay)$ und $\det \xi = x^2 - a^2y^2 = (x + ay)(x - ay)$. Folglich haben wir $\xi \in U_1(p, D) \iff$

$1 = \det\xi = u \cdot v \iff v = u^{-1}$ und damit $U_1(p,D) \simeq \mathbb{F}_p^\times$ vermöge $\xi \mapsto u$. Den zweiten Fall $\left(\frac{D}{p}\right) = -1$ haben wir in (9.1) behandelt.

Wir wollen nun die Struktur von U_1 im allgemeinen Fall $n = p^k$ untersuchen.

(9.3) Satz: *Sei $p > 2$ eine Primzahl, $n \in \mathbb{N}$ und $D \in \mathbb{Z}$ mit $p \nmid D$. Dann gilt:*

$$U_1(p^k, D) \begin{cases} \text{zyklisch von der Ordnung } p^{k-1}(p-1)\,, & \text{falls } \left(\frac{D}{p}\right) = +1, \\ \text{zyklisch von der Ordnung } p^{k-1}(p+1)\,, & \text{falls } \left(\frac{D}{p}\right) = -1, \end{cases}$$

oder kompakt zusammengefasst

$$U_1(p^k, D) \text{ ist zyklisch von der Ordnung } p^{k-1}\Big(p - \left(\frac{D}{p}\right)\Big)$$

Als ersten Schritt zeigen wir

(9.4) Lemma: *Ist $D \in \mathbb{Z}$ ein quadratischer Rest modulo p: $\left(\frac{D}{p}\right) = +1$, so ist D auch ein quadratischer Rest modulo aller p^k:*

$$D \equiv a_k^2 \bmod p^k\,.$$

Beweis: Wir konstruieren a_k induktiv. a_1 existiert nach Voraussetzung. Ausgehend von $k \geq 1$ und $D = a_k^2 + p^k b$ setzen wir an $a_{k+1} = a_k + p^k c$. Dann gilt modulo p^{k+1}

$$a_{k+1}^2 = a_k^2 + 2p^k a_k c + p^{2k} c \equiv D - p^k b + 2p^k a_k c = D + p^k(2a_k c - b)\,.$$

Wählt man nun c so, dass $2a_k c \equiv b \bmod p$ (möglich wegen $p \nmid 2a_k$), so hat man a_{k+1} wie gewünscht.

Beweis von (9.3): 1. Fall $\left(\frac{D}{p}\right) = 1$: Nach dem Lemma ist D ein Quadrat modulo p^k und nach (9.2) sowie den nachfolgenden Bemerkungen gilt dann

$$\begin{aligned} Z(p^k, D) &\simeq \mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/p^k\mathbb{Z}\,, \\ U(p^k, D) &\simeq \mathcal{P}(p^k) \times \mathcal{P}(p^k)\,, \\ U_1(p^k, D) &\simeq \{(u,v) \in \mathcal{P}(p^k) \times \mathcal{P}(p^k) \mid uv \equiv 1 \bmod p^k\} \simeq \mathcal{P}(p^k)\,. \end{aligned}$$

Damit ist dann $U_1(p^k, D) \simeq \mathcal{P}(p^k)$ zyklisch von der Ordnung $p^{k-1}(p-1)$ (vgl. Satz (4.6),c)).

2. Fall $\left(\frac{D}{p}\right) = -1$: Wir beweisen zunächst die Behauptung über die Ordnung per Induktion über k. Der Induktionsanfang $k = 1$ ist in Satz (9.1) enthalten.

$k \geq 1\,,\ k \to k+1$: Die natürliche Projektion

$$Z(p^{k+1}, D) \twoheadrightarrow Z(p^k, D)$$

bildet die Einheitengruppen ineinander ab:

$$U(p^{k+1}, D) \to U(p^k, D)\,.$$

Dieser Homomorphismus ist surjektiv, denn

$$\xi \in U(p^k, D) \implies \det\xi \in \mathcal{P}(p^k) \iff p \nmid \det\xi \implies \det\xi \in \mathcal{P}(p^{k+1})\,,$$

und jedes Urbild von ξ in $Z(p^{k+1}, D)$ gehört also zu $U(p^{k+1}, D)$.

Dieser Epimorphismus der Einheitengruppen bildet nun die Normeinsuntergruppen ineinander ab:

$$U_1(p^{k+1}, D) \to U_1(p^k, D)\,.$$

denn $\det \xi \equiv 1 \bmod p^{k+1} \implies \det \xi \equiv 1 \bmod p^k$.

Auch diese Abbildung ist surjektiv: Sei $\xi = x + yW \in U_1(p^k, D)$, also

$$\det \xi = x^2 - y^2 D \equiv 1 \bmod p^k \,. \tag{1}$$

Gesucht ist nun $\tilde{x} + \tilde{y}W$ mit

$$\tilde{x} \equiv x \,,\ \tilde{y} \equiv y \bmod p^k \tag{2}$$
$$\tilde{x}^2 + \tilde{y}^2 D \equiv 1 \bmod p^{k+1} \tag{3}$$

Gemäß (2) setzen wir $\tilde{x} = x + p^k u$ und $\tilde{y} = y + p^k v$ mit geeigneten u, v. Voraussetzung (1) besagt $x^2 - y^2 D = 1 + p^k w$, also gilt

$$\begin{aligned} \tilde{x}^2 - \tilde{y}^2 D &= (x + p^k u)^2 - D(y + p^k v)^2 \\ &= x^2 - Dy^2 + p^k(2xu - 2yv) + p^{2k}(u^2 - v^2) \\ &\equiv 1 + p^k(w + 2xu + 2yv) \bmod p^{k+1} \\ &\equiv 1 \bmod p^{k+1} \end{aligned}$$

falls $w + 2xu + 2yv \equiv 0 \bmod p$.

Eine solche Wahl von u, v ist möglich: Im Fall $p \nmid x$ können wir u so wählen, dass $2xu \equiv -w \bmod p$ ist, und erhalten mit $v = 0$ die gewünschte Kongruenz. Im Falle $p \nmid y$ argumentiert man mit vertauschten Rollen. Einer dieser beiden Fälle muss eintreten, denn wäre p gemeinsamer Teiler von x und y, so auch von $\det \xi = x^2 - y^2 D$, im Widerspruch zu $\det \xi \in \mathcal{P}(p^k)$.

Also induzieren die natürlichen Projektionen Epimorphismen

$$\pi_{k+1} : U_1(p^{k+1}, D) \twoheadrightarrow U_1(p^k, D) \,,\ \xi = x + yW \mapsto \xi' = x + yW \bmod p^k \,.$$

Wir wollen deren Kern bestimmen:

$$\xi \in \operatorname{Ke} \pi_{k+1} \iff \xi \equiv E \bmod p^k \iff x \equiv 1 \,,\ y \equiv 0 \bmod p^k \iff x = 1 + p^k u \,,\ y = p^k v \,.$$

Wegen $\xi \in U_1(p^{k+1}, D)$ gilt dann

$$\begin{aligned} x^2 - y^2 D \equiv 1 \bmod p^{k+1} &\iff 1 + 2p^k u + p^{2k} u^2 - p^{2k} v^2 D \equiv 1 \bmod p^{k+1} \\ &\implies 1 + 2p^k u \equiv 1 \bmod p^{k+1} \\ &\iff u \equiv 0 \bmod p \,. \end{aligned}$$

Damit folgt

$$\begin{aligned} \operatorname{Ke} \pi_{k+1} &= \{x + yW \in U_1(p^{k+1}, D) \mid x \equiv 1 \bmod p^{k+1} \,,\ y = p^k v \bmod p^{k+1}\} \\ &= \{1 + p^k v W \mid v \in \mathbb{Z}/p\mathbb{Z}\} \,. \end{aligned}$$

Der Kern ist also zyklisch von der Ordnung p und jedes Element in $U_1(p^k, D)$ hat genau p Urbilder in $U_1(p^{k+1}, D)$. Es folgt induktiv

$$\#U_1(p^{k+1}, D) = p \cdot \#U_1(p^k, D) = p \cdot p^{k-1}(p+1) = p^k(p+1) \,.$$

Nachdem nun die Ordnung von $U_1(p^k, D) = p^{k-1}(p+1)$ bestimmt ist, beweisen wir auch die Zyklizität von $U_1(p^k, D)$ induktiv.

$\underline{k = 1}$: Dies ist bereits in Satz (9.1) enthalten.

$\underline{k = 2}$: Wir zeigen: Ist $\xi \in U_1(p^2, D)$ ein Urbild eines Erzeugers $\xi' \in U_1(p, D)$, so ist ξ oder $\xi + pW$ ein Erzeuger von $U_1(p^2, D)$.

Zunächst gilt ord $\xi \mid p(p+1) = \#U_1(p^2, D)$, aber

$$\xi^p = 1 \implies \xi'^p = 1 \implies \text{ord } \xi' = p + 1 \mid p \,, \text{ Widerspruch!}$$

Also ist $\xi^p \neq 1$ und ξ hat die gewünschte Ordnung $p(p+1)$ genau dann, wenn $\xi^{p+1} \neq 1$ ist. Sollte $\xi^{p+1} = 1$ sein, so betrachten wir statt ξ das Urbild $\xi + pW$ von ξ'. Für dieses gilt $(\xi + pW)^{p+1} \neq 1$, denn:

$$(\xi + pW)^{p+1} \equiv \xi^{p+1} + (p+1)pW\xi^p \equiv 1 + pW\xi^p \bmod p^2 .$$

Da $\det W\xi^p = \det W = -D$ kein Vielfaches von p ist, kann auch $W\xi^p$ nicht durch p teilbar sein, so dass gilt:

$$(\xi + pW)^{p+1} \equiv 1 + pW\xi^p \not\equiv 1 \bmod p^2 .$$

Wir kommen nun zum Induktionsschritt $k \geq 2, k \to k+1$:
Sei $\xi \in U_1(p^{k+1}, D)$ ein beliebiges Urbild eines Erzeugers von $U_1(p^k, D)$, also

$$\langle \xi \bmod p^k \rangle = U_1(p^k, D) .$$

Dann gilt

$$p^{k-1}(p+1) = \#U_1(p^k, D) = \operatorname{ord}(\xi \bmod p^k) \mid \operatorname{ord} \xi \mid \#U_1(p^{k+1}, D) = p^k(p+1) .$$

Um zu zeigen, dass ξ selbst ein Erzeugendes von $U_1(p^{k+1}, D)$ ist, muss man also nur zeigen, dass $\xi^{p^{k-1}(p+1)} \neq 1$ ist. Da $\xi \bmod p^k$ $U_1(p^k, D)$ erzeugt, gilt

$$\xi^{p^{k-2}(p+1)} \not\equiv 1 \bmod p^k ,$$

Andererseits muss wegen $\#U_1(p^{k-1}, D) = p^{k-2}(p+1)$ $(k \geq 2!)$ gelten

$$\xi^{p^{k-2}(p+1)} \equiv 1 \bmod p^{k-1} .$$

Beide Kongruenzen zusammen ergeben

$$\xi^{p^{k-2}(p+1)} = 1 + p^{k-1}A , \quad A \in Z(p^{k+1}, D) , \ p \nmid A .$$

Dann folgt aber

$$\xi^{p^{k-1}(p+1)} = (1 + p^{k-1}A)^p \equiv 1 + p^k A \bmod p^{k+1} \not\equiv 1 \bmod p^{k+1} ,$$

und der Induktionsschritt ist bewiesen.

Mit dem Chinesischen Restsatz erhalten wir aus (9.3) das folgende

(9.5) Korollar: *Ist $n \geq 3$ ungerade mit der Primzerlegung $n = \prod_{i=1}^r p_i^{\nu_i}$ und D teilerfremd zu n, so gilt:*

$$U_1(n, D) \simeq \prod_{i=1}^{r} U_1(p_i^{\nu_i}, D)$$

ist direktes Produkt zyklischer Gruppen der Ordnungen

$$p_i^{\nu_i - 1}(p_i - \left(\frac{D}{p_i}\right)) .$$

Hieraus erhalten wir in Analogie zum $p-1$-Kriterium, p. 41 das folgende $(p+1)$-Primzahlkriterium:

(9.6) Satz: *Sei $n \geq 3$ ungerade und D eine natürliche Zahl mit $\left(\frac{D}{p}\right) = -1$. Dann gilt:*

$$n \text{ Primzahl} \iff \bigvee_{\xi \in U_1(n,D)} \operatorname{ord} \xi = n+1$$

Beweis: ' $\Longrightarrow$ ': Sei $n = p$ Primzahl. Wegen $\left(\frac{D}{p}\right) = -1$ ist dann $U_1(p, D)$ zyklisch von der Ordnung $p+1$. Man wähle ξ als Erzeuger von $U_1(p, D)$ und alle Forderungen sind erfüllt.

'$\Longleftarrow$': Sei $n = \prod_{i=1}^{r} p_i^{k_i}$ die Primzerlegung von n. Dann ist $U_1(n,D)$ direktes Produkt zyklischer Gruppen der Ordnungen $p_i^{k_i-1}(p_i \mp 1)$ (siehe Korollar (9.5)) und hat den Exponenten (siehe (4.2) und (4.5),b))

$$\exp U_1(n,D) = \operatorname*{kgV}_{i=1}^{r} \left(p_i^{k_i-1}(p_i \mp 1)\right).$$

Nach Voraussetzung enthält $U_1(n,D)$ ein Element der Ordnung $n+1$, $n+1$ ist also Teiler dieses Exponenten. Da n ungerade ist, sind alle $p_i \geq 3$ ungerade und $p_i \mp 1$ gerade. Also gilt

$$n+1 \mid \exp U_1(n,D) = 2 \cdot \operatorname*{kgV}_{i=1}^{r} \left(p_i^{k_i-1} \cdot \frac{p_i \mp 1}{2}\right).$$

Wir schätzen nun diesen kgV durch das Produkt ab:

$$n+1 \mid \exp U_1(n,D) \leq 2 \cdot \prod_{i=1}^{r} p_i^{k_i} \cdot \prod_{i=1}^{r} \frac{1 \mp \frac{1}{p_i}}{2} = 2n \prod_{i=1}^{r} \frac{1 \mp \frac{1}{p_i}}{2}$$

In diesem letzten Produkt sind zunächst alle Faktoren < 1, denn $1 \mp \frac{1}{p_i} \leq 1 + \frac{1}{p_i} < 2$, also ist das Produkt kleiner gleich jedem Partialprodukt. Wegen $p_1 \geq 3$ und $p_2 \geq 5$ erhielte man im Falle $r \geq 2$ den Widerspruch

$$n+1 \mid \exp U_1(n,D) \leq 2n \cdot \frac{2}{3} \cdot \frac{3}{5} = n \cdot \frac{4}{5} < n\,.$$

Es muss also $r = 1$ und damit $n = p^k$ eine Primzahlpotenz sein. Dann folgt

$$n+1 = p^k + 1 \mid \#U_1(p^k,D) = p^{k-1}(p \mp 1)$$

Wegen der Teilerfremdheit von p^k+1 und p^{k-1} müsste dann $p^k + 1 \mid p \mp 1$ gelten, was nur für $k = 1$ (und den zweiten Fall $p+1$) möglich ist. Damit ist $n = p$ prim. □

(9.7) Satz: *Es sei $n \geq 3$ eine natürliche Zahl und $D \in \mathbb{Z}$ mit $\left(\frac{D}{p}\right) = -1$. Für $n+1$ sei eine partielle Zerlegung bekannt:*

$$n+1 = A \cdot B\,,\ A = p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r} \text{ Primzerlegung.}$$

Dann gilt im Falle $A > B$:

$$n \text{ Primzahl} \iff \bigwedge_{i=1}^{r} \bigvee_{\xi_i \in Z(n,D)} \xi_i \bar{\xi}_i \equiv 1 \bmod n \ \wedge\ \xi_i^{n+1} \equiv 1 \bmod n \ \wedge\ \operatorname{ggT}\left(\xi_i^{(n+1)/p_i} - 1, n\right) = 1\,.$$

Dabei wollen wir hier den ggT eines $\xi \in Z(n,D)$ und der Zahl $n \in \mathbb{N}$ innerhalb $\mathbb{N}$, und das bedeutet, komponentenweise bilden: $\operatorname{ggT}(\xi, n) = \operatorname{ggT}(x + yW, n) = \operatorname{ggT}\{\operatorname{ggT}(x,n), \operatorname{ggT}(y,n)\}$.

Beweis: Zunächst formen wir (9.6) um zu:

$$n \text{ Primzahl} \iff \bigvee_{\xi \in Z(n,D)} \xi\bar{\xi} \equiv 1 \bmod n \ \wedge\ \xi^{n+1} \equiv 1 \bmod n \ \wedge \bigwedge_{\substack{q \text{ prim} \\ q \mid n+1}} \xi^{\frac{n+1}{q}} \not\equiv 1 \bmod n\,.$$

Damit ist von Satz (9.7) die Richtung $\Longrightarrow$ bewiesen (sogar mit einem von i unabhängigen $\xi_i = \xi$), denn für eine Primzahl $n = p$ und $\xi = x + yW \in Z(n,D)$ gilt

$$\xi \not\equiv 1 \bmod p \iff p \nmid \xi - 1 = (x-1) + yW \iff p \nmid x - 1 \ \vee\ p \nmid y \iff \operatorname{ggT}(\xi - 1, p) = 1\,.$$

Für die Umkehrung $\Longleftarrow$ schließen wir genauso wie bei (8.5). Wir fixieren einen beliebigen Primteiler p von n. Dann ist $\xi \bmod p$ ein Element in $U_1(p,D)$ und für die Ordnung $n_i := \operatorname{ord}(\xi_i \bmod p)$ muss gelten

$$n_i \mid p - \left(\frac{D}{p}\right)\,. \tag{1}$$

Andererseits gilt nach Voraussetzung $\xi_i^{n+1} \equiv 1 \bmod n$, also erst recht $\xi_i^{n+1} \equiv 1 \bmod p$. Dies bedeutet

$$n_i \mid n+1\,. \tag{2}$$

Schließlich folgt aus $\mathrm{ggT}(\xi_i^{(n+1)/p_i}-1, n) = 1$ (bei unserer obigen Deutung des ggT) $p \nmid \xi_i^{(n+1)/p_i} - 1$, oder mit anderen Worten $\xi_i^{(n+1)/p_i} \not\equiv 1 \bmod p$. Dies bedeutet

$$n_i \nmid \frac{n+1}{p_i}\,. \tag{3}$$

Angesichts der Faktorisierung von $n+1$ folgt aus (2) und (3)

$$p_i^{\nu_i} \mid n_i\,,$$

also mit (1) $p_i^{\nu_i} \mid p - \left(\frac{D}{p}\right)$ für alle i und folglich $A \mid p - \left(\frac{D}{p}\right)$:

$$p \equiv \left(\frac{D}{p}\right) \bmod A \quad \text{für alle Primteiler } p \text{ von } n. \tag{4}$$

Ist nun $A > B$, also $A > \sqrt{n+1}$, so folgt daraus

$$p - \left(\frac{D}{p}\right) \geq A > \sqrt{n+1} \text{ für jeden Primteiler } p \text{ von } n\,. \tag{5}$$

Speziell

$$p > p-1 > \sqrt{n} \text{ für jeden Primteiler } p \mid n \text{ mit } \left(\frac{D}{p}\right) = +1\,. \tag{6}$$

Wir nehmen an, n sei zerlegbar. Dann gilt für den kleinsten Primteiler p von n: $p \leq \sqrt{n}$, und daher nach (6) $\left(\frac{D}{p}\right) = -1$. Gemäß (5) folgt dann

$$p+1 = p - \left(\frac{D}{p}\right) > \sqrt{n+1} > \sqrt{n} \geq p \iff (p+1)^2 > n+1 \ \wedge\ n \geq p^2 \iff p^2+2p > n \geq p^2\,.$$

Da p Teiler von n ist, folgt

$$p(p+2) > n = kp \geq p^2 \implies p+2 > k \geq p\,.$$

Mithin ist $k = p \ \vee\ k = p+1$ bzw. $n = p^2 \ \vee\ n = p(p+1)$. Im letzten Falle wäre $p+1$ gerade und $p > 2$ nicht der kleinste Primteiler von n, während sich im ersten Falle $\left(\frac{D}{n}\right) = \left(\frac{D}{p^2}\right) = +1$ ergibt, im Widerspruch zur Voraussetzung $\left(\frac{D}{p}\right) = -1$. Damit kann n nicht zerlegbar sein. □

Wir wollen nun den Extremfall von (9.7) betrachten, dass nämlich $n+1$ vom einfachsten vollständig zerlegten Typ ist: $n+1 = 2^k$ und daher $n = 2^k - 1$. n ist also eine Mersenne-Zahl und diese kann nur prim sein, wenn auch k prim ist (siehe Bemerkung (2.11)). Wir wollen also auf die Mersenne-Zahlen $M_q = 2^q - 1$ den obigen Primzahltest anwenden. Dabei lassen wir die Mersenne-Primzahl $M_2 = 2^2 - 1 = 3$ außer Betracht. Zur Anwendung des Primzahltests wählen wir ein D mit $\left(\frac{D}{n}\right) = -1$. Dabei können wir (unabhängig von $n = 2^q - 1$) $D = 3$ wählen:

(9.8) Lemma: *Ist $q \geq 3$ ungerade, so gilt $\left(\frac{3}{M_q}\right) = -1$.*

Beweis: Es ist $M_q = 2^q - 1 \equiv -1 \bmod 4$, also nach dem quadratischen Reziprozitätsgesetz für das Jacobisymbol

$$\left(\frac{3}{M_q}\right) = -\left(\frac{M_q}{3}\right)$$

Modulo 3 gilt nun $M_q = 2^q - 1 \equiv (-1)^q - 1 \equiv -1 - 1 \equiv 1 \bmod 3$ (q ist ungerade!). Also folgt die Behauptung

$$\left(\frac{3}{M_q}\right) = -\left(\frac{M_q}{3}\right) = -\left(\frac{1}{3}\right) = -1\,.$$

Aber nicht nur D, sondern auch das in Satz (9.7) geforderte ξ ist universell wählbar, denn wenn M_q eine Mersenne-Primhahl ist, hat das Element $\xi = 2 + \sqrt{3} = 2 + W \in U_1(M_q, 3)$ die geforderten Eigenschaften:

(9.9) Satz: *Sei M_q eine Mersenne-Primzahl (mit $q \geq 3$ ungerade). Dann gilt:*

$$2 + \sqrt{3} \in U_1(M_q, 3) \subset \mathbb{F}_{M_q}[\sqrt{3}]^\times \text{ hat die Ordnung } 2^q = M_q + 1\,.$$

Beweis: Das Element $\xi = 2 + \sqrt{3}$ hat die Norm $\mathcal{N}\xi = 4 - 3 = 1$, gehört also zur Gruppe $U_1(M_q, 3)$ von der Ordnung $M_q + 1 = 2^q$. Die Ordnung von ξ ist somit eine Potenz von 2. Wäre die Ordnung von ξ kleiner als 2^q, so wäre ξ eine Potenz eines Erzeugers mit geradem Exponenten und damit ein Quadrat. Also $\xi = \zeta^2$ mit $\zeta = x + y\sqrt{3} \in U_1(M_q, 3)$. Dies ergibt

$$1 = x^2 - 3y^2 \text{ und } 2 + \sqrt{3} = \zeta^2 = (x^2 + 3y^2) + 2xy\sqrt{3} = (2x^2 - 1) + 2xy\sqrt{3}$$

also $2x^2 - 1 = 2$ bzw. $2x^2 = 3$ im Körper $\mathbb{F}_{M_q}$. 2 und 3 unterscheiden sich damit um ein Quadrat modulo M_q, sind also beide qudratische Reste oder beide quadratische Nichtreste. Aber dies ist falsch, denn $\left(\frac{3}{M_q}\right) = -1$ und wegen $M_q = 2^q - 1 \equiv -1 \bmod 8$ gilt $\left(\frac{2}{M_q}\right) = +1$ (Ergänzungssatz (7.6)). □

Dieser Satz zeigt, welches ξ man wählen kann, um mit Satz (9.6) einen Primzahlnachweis für eine Mersenne-Zahl zu führen. Setzt man dies um, erhält man das folgende, erstaunlich einfach zu formulierende und überprüfende Kriterium für Mersenne-Primzahlen:

(9.10) Satz: *Sei $q \geq 3$ ungerade und $M_q = 2^q - 1$ eine Mersenne-Zahl. Wir definieren rekursiv die Folge*

$$u_0 = 4\,, \quad u_{k+1} = u_k^2 - 2\,.$$

Dann gilt:

$$M_q \textit{ ist prim} \iff u_{q-2} \equiv 0 \bmod M_q\,.$$

Beweis: Sei $D = 3$ und angesichts (9.9) wählen wir

$$\xi = 2 + W = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \in U_1(M_q, 3)\,.$$

Dabei ist $W = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$ die Matrix in $Z(M_q, 3)$ mit $W^2 = 3E = 3$ (vgl. die Definition von $Z(n, D)$, p. 46). Nach (9.8) gilt $\left(\frac{D}{M_q}\right) = -1$ und wir erhalten aus (9.9) und (9.6)

$$M_q \text{ ist prim} \iff \operatorname{ord}(\xi) = M_q + 1 = 2^q\,.$$

Nach (9.3) ist $\#U_1(M_q, 3) = M_q + 1 = 2^q$ und daher ord ξ eine Potenz von 2. Damit folgt

$$M_q \text{ ist prim} \iff \operatorname{ord}(\xi) \not| \, 2^{q-1} \iff \xi^{2^{q-1}} \not\equiv 1 \bmod M_q\,.$$

Wir definieren rekursiv $\xi_0 = \xi$ und $\xi_k = (\xi_{k-1})^2$, also $\xi_k = \xi^{2^k}$, und unser Kriterium lautet

$$M_q \text{ prim} \iff \xi_{q-1} \not\equiv 1 \bmod M_q\,. \qquad (*)$$

Wir setzen nun $\xi_k = x_k + y_k W$ und erhalten Rekursionsformeln für x_k, y_k:

$$x_{k+1} + y_{k+1}W = (x_k + y_k W)^2 = (x_k^2 + 3y_k^2) + 2x_k y_k W\,,$$

zusammen mit $1 = \mathcal{N}\xi_k = x_k^2 - 3y_k^2$ führt dies zu

$$x_{k+1} = x_k^2 + 3y_k^2 = 2x_k^2 - 1\,.$$

Damit erfüllt $u_k = 2x_k$ genau die im Satz angegebene Rekursion:

$$u_{k+1} = 2x_{k+1} = 4x_k^2 - 2 = u_k^2 - 2\,.$$

Da M_q ungerade ist, besagt die Bedingung $u_{q-2} \equiv 0 \bmod M_q$ nichts anderes als $x_{q-2} \equiv 0 \bmod M_q$, und es folgt dann

$$\xi_{q-2} = y_{q-2}W \in Z(M_q, 3) \implies \xi_{q-1} = 3y_{q-2}^2 \equiv -\mathcal{N}(\xi_{q-2}) \equiv -1 \not\equiv 1 \bmod M_q\,.$$

Also ist $\xi_{q-1} \not\equiv 1 \bmod M_q$ und M_q ist prim nach $(*)$.

Umgekehrt sei M_q prim. Dann ist gemäß $(*)$ $\xi_{q-1} \neq 1$. Dann folgt aber $\xi_{q-1} = -1$, da $Z(M_q, 3) = \mathbb{F}_{M_q}[\sqrt{3}] =: k$ ein Körper ist. Also folgt:

$$\begin{aligned} -1 = \xi_{q-1} = \xi_{q-2}^2 &= x_{q-2}^2 + 3y_{q-2}^2 + 2x_{q-2}y_{q-2}\sqrt{3} \\ \iff x_{q-2}^2 + 3y_{q-2}^2 \equiv -1 \bmod M_q &\ \wedge\ 2x_{q-2}y_{q-2} \equiv 0 \bmod M_q \end{aligned}$$

Wegen $\left(\frac{3}{M_q}\right) = -1$ ((9.8)) und $\left(\frac{-1}{M_q}\right) = -1$ ($M_q = 2^q - 1 \equiv -1 \bmod 4$) gilt $\left(\frac{-3}{M_q}\right) = +1$. Also ist -3 ein Quadrat in $k^\times$ und es gibt ein y mit

$$3y^2 \equiv -1 \bmod M_q\,.$$

Dann sind $\pm y\sqrt{3}$ zwei Lösungen der obigen Gleichung $\xi_{q-2}^2 = \xi_{q-1} = -1$. Im Körper k kann es keine weiteren Lösungen geben, also folgt

$$\pm y\sqrt{3} \equiv \xi_{q-2} = x_{q-2} + y_{q-2}\sqrt{3} \bmod M_q \implies x_{q-2} \equiv 0 \bmod M_q \iff u_{q-2} \equiv 0 \bmod M_q\,.$$

Literatur — Eine Auswahl

[AKS] Agrawal, Manindra; Kayal, Neeraj; Saxena, Nitin: *PRIMES is in P*, Ind. Inst. Techn. Kanpur, Preprint 6. 8. 2002, Revised Version: `http://www.cse.iitk.ac.in/news/primality_v3.pdf`

[BH] Bosma, Wieb, Hulst, Marc-Paul: *Faster primality testing*, in: Advances in cryptology - Eurocrypt '89, Springer Lect. Notes Comp. Sci 434 (1990), pp. 652-656

[Bu] Buchmann, Johannes: *Einführung in die Kryptographie*, Springer Lehrbuch, Springer Berlin-Heidelberg-New York, 1999

[Br] Bressoud, David M.: *Factorization and Primality Testing*, Springer Berlin-Heidelberg-New York, 1989

[CL1] Cohen, H., Lenstra, H. W. Jr.: Primality testing and Jacobi sums, *Math. Comp.* **42** (1984) 297–330

[CL2] Cohen, H., Lenstra, H. W. Jr.: Implementation of a new primality test, *Math. Comp.* **48** (1987) 103–121; *Supplement* S1–S4

[Fo] Forster, Otto: *Algorithmische Zahlentheorie*, vieweg Lehrbuch Mathematik, Braunschweig/Wiesbaden 1996

[Di] Dixon, John D.: Factorization and primality testing, *Am. Math. monthly* **91** (1984) 333-352

[Ko1] Koblitz, N.: *A Course in Number Theory and Cryptography*, Springer Berlin-Heidelberg-New York, 1987

[Ko2] Koblitz, N.: *Algebraic Aspects of Cryptography*, Springer Berlin-Heidelberg-New York, 1998

[LAK] Lenstra, A. K.: *Primality testing*, in: Proc. Symp. Appl. Math. 42 (1990), pp. 13–25

[LHW] Lenstra, H. W. Jr.: Factoring integers with elliptic curves, *Ann. Math.* **126** (1987) 649–673

[Ne] Nebe, Gabriele: Faktorisieren ganzer Zahlen, in: *Jber. d. Dt. Math.-Verein.* **102** (2000) 1–14

[Po] Pomerance, C.: The quadratic sieve factoring algorithm, in: *Advances in Cryptology - Eurocrypt 1984*, Springer Lect. Notes Comp. Sci. 209 (1985), pp. 169–182

[Ri] Riesel, Hans: *Prime Numbers and Computer Methods for Factorization*, Second Edition, Birkhäuser, Boston, Inc., 1994

Und abschließend ein Buch, das man gut in den Ferien am Strand oder im Liegestuhl lesen kann:

[Si] Singh, Simon: *Geheime Botschaften*, Carl Hanser Verlag 2000