Zahlentheorie und Primzahltests

Prof. Udo Hebisch

SS 2020

Dieses Skript enthält nur den "roten Faden"
der Vorlesung.
Wesentliche Inhalte werden ausschließlich
in der Vorlesung vermittelt. Daher ist dieses
Skript nicht zum Selbststudium gedacht, sondern
nur als "Erinnerungsstütze".

Inhaltsverzeichnis

1 Natürliche Zahlen und Primzahlen

> Primzahlen erfordern unsere ungeteilte Aufmerksamkeit..
> Brigitte Fuchs

1.1 Natürlichen Zahlen und Induktion

Obwohl wir in dieser Vorlesung generell Vertrautheit mit dem Rechnen im Körper der komplexen Zahlen $\mathbb{C}$ voraussetzen, beginnen wir mit einer axiomatischen Definition der natürlichen Zahlen $\mathbb{N}_0$. Dies geschieht, um zu zeigen, daß viele Grundbegriffe und Probleme der Zahlentheorie elementar formuliert werden können, obwohl zu ihrer Lösung oft sehr starke mathematische Hilfsmittel benötigt werden.

Definition 1.1 Die Menge $\mathbb{N}_0$ der *natürlichen Zahlen* läßt sich eindeutig durch die *Peano-Axiome* (Giuseppe Peano, 1858 - 1932) charakterisieren:

(P1) $0 \in \mathbb{N}_0$.

(P2) Es gibt eine Funktion $' : \mathbb{N}_0 \to \mathbb{N}_0$, die jeder natürlichen Zahl $n \in \mathbb{N}_0$ eindeutig einen *Nachfolger* $n' \in \mathbb{N}_0$ zuordnet.

(P3) Die Nachfolgerfunktion ist injektiv, also $n' = m'$ impliziert $n = m$ für alle $n, m \in \mathbb{N}_0$.

(P4) 0 ist nicht Nachfolger einer natürlichen Zahl, also $0 \neq n'$ für alle $n \in \mathbb{N}_0$.

(P5) (**Induktionsaxiom**) Für jede Teilmenge $N \subseteq \mathbb{N}_0$ mit $0 \in N$ (**Induktionsbeginn**) und der Eigenschaft, daß für alle $n \in \mathbb{N}_0$ aus $n \in N$ stets $n' \in N$ folgt (**Induktionsschritt**), gilt bereits $N = \mathbb{N}_0$ (**Induktionsschluß**).

Bemerkung 1.2 Die Nachfolgerfunktion wird bei vielen Autoren auch als $succ(n)$ (von lat. succedere = nachfolgen) anstelle von n' notiert. Durch die folgende Verabredung wird sie aber entbehrlich und in späteren Abschnitten auch nicht wieder auftauchen.

Man verabredet die üblichen *dezimalen Schreibweisen* für die iterierten Nachfolger der Zahl 0: $1 = 0'$, $2 = 1' = (0')'$, usw. Berücksichtigt man nun noch die gleich definierte Additon für natürliche Zahlen (vgl. (2)), so kann man stets n' durch das gewohnte $n + 1$ ersetzen. Den außer für 0 stets existierenden und wegen (P3)

eindeutig bestimmten *Vorgänger* der natürlichen Zahl n bezeichnet man dann auch mit $n-1$, also $(n-1)' = n$.

Man kann in diesem Axiomensystem auch die 0 durch die 1 ersetzen, um die Menge $\mathbb{N} = \mathbb{N}_0 \setminus \{0\} = \{1, 2, 3, \ldots\}$ zu charakterisieren. Der Einschluß der Null unter die "natürlichen" Zahlen hat den Vorteil, daß dann auch die Mächtigkeit der leeren Menge eine natürliche Zahl ist.

Wegen des Induktionsaxioms kann man jetzt folgende *induktiven* oder *rekursiven* Definitionen für Operationen und Relationen auf den natürlichen Zahlen geben (erstmals durch Hermann Günther Graßmann (1809 - 1877) im Jahr 1861).

Definition 1.3 a) Die *Addition* $n+k$ werde für zwei beliebige natürliche Zahlen n und k definiert durch

$$\begin{aligned} (1) \quad n+0 &= n \text{ für } k=0 \\ (2) \quad n+m' &= (n+m)' \text{ für } k=m'. \end{aligned}$$

b) Die *Multiplikation* $n \cdot k$ werde für zwei beliebige natürliche Zahlen n und k mit Hilfe der Addition definiert durch

$$\begin{aligned} (3) \quad n \cdot 0 &= 0 \text{ für } k=0 \\ (4) \quad n \cdot m' &= (n \cdot m) + n \text{ für } k=m'. \end{aligned}$$

Wie üblich soll im folgenden die Multiplikation stärker binden als die Addition und die Klammern in $(n \cdot m)$ werden daher fortgelassen.

c) Ebenfalls mit Hilfe der Addition läßt sich die übliche *Ordnungsrelation* $n \leq m$ für zwei beliebige natürliche Zahlen n und m definieren durch

$$(5) \quad n \leq m \Longleftrightarrow n+k=m \text{ für ein } k \in \mathbb{N}_0.$$

Ist hierbei $k \neq 0$ so schreibt man $n < m$.

d) Schließlich definiert man *Potenzen* n^k für zwei beliebige natürliche Zahlen n und k mit Hilfe der Multiplikation durch

$$\begin{aligned} (6) \quad n^0 &= 1 \text{ für } k=0 \\ (7) \quad n^{m'} &= (n^m) \cdot n \text{ für } k=m'. \end{aligned}$$

Bemerkung 1.4 Wegen der Kürzbarkeit der Addition (vgl. Aufgabe 1.6 d)) ist die natürliche Zahl k in (5) sogar eindeutig durch m und n bestimmt. Man schreibt daher auch $k = m - n$.

Zur Demonstration eines Induktionsbeweises und als nützliche Hilfe bei der Lösung von Aufgabe 1.6 zeigen wir das folgende Lemma.

Lemma 1.5 *Für alle* $m, n \in \mathbb{N}_0$ *gilt* $m' + n = m + n'$.

Beweis: Es sei $m \in \mathbb{N}_0$ eine beliebige natürliche Zahl und $N = \{n \in \mathbb{N}_0 \mid m' + n = m + n'\}$. Dann ist also $N = \mathbb{N}_0$ zu zeigen. Wegen (1) und (2) gilt $m' + 0 = m' = (m + 0)' = m + 0'$ und damit jedenfalls $0 \in N$. Sei nun $n \in N$. Mit (2) folgt dann $m' + n' = (m' + n)' = (m + n')' = m + (n')'$ und damit auch $n' \in N$. Mit (P5) ergibt sich daher $N = \mathbb{N}_0$. ◇

Wenn man die technische Durchführung der folgenden fünf Aufgaben als zu "eintönig" empfindet, sollte man sich mindestens überlegen, bei welchen Aussagen die Axiome (P3) bzw. (P4) in die entsprechenden Beweise wesentlich eingehen.

Aufgabe 1.6 Zeigen Sie mittels vollständiger Induktion unter Benutzung von Lemma 1.5, daß $(\mathbb{N}_0, +, 0)$ ein *kommutatives und kürzbares Monoid* ist, d. h. es gelten die folgenden Aussagen.

a) Die Addition ist *assoziativ* gemäß $(n+m)+\ell = n+(m+\ell)$ für alle $n, m, \ell \in \mathbb{N}_0$, $(\mathbb{N}_0, +)$ ist also eine *Halbgruppe*.

b) 0 ist *neutrales Element* der Addition gemäß $0 + n = n = n + 0$ für alle $n \in \mathbb{N}_0$, $(\mathbb{N}_0, +, 0)$ ist also ein *Monoid*.

c) Die Addition ist *kommutativ* gemäß $n + m = m + n$ für alle $n, m \in \mathbb{N}_0$.

d) Die Additon ist *kürzbar* gemäß $n + k = m + k \Longrightarrow n = m$ für alle $n, m, k \in \mathbb{N}_0$.

Zusätzlich gilt noch:

e) Es ist $m + n \neq 0$ für alle $m, n \in \mathbb{N}$, d. h. es gilt die Implikation $n + m = 0 \Longrightarrow n = m = 0$ für alle $n, m \in \mathbb{N}_0$.

Aufgabe 1.7 Zeigen Sie mittels vollständiger Induktion, daß in $(\mathbb{N}_0, +, \cdot)$ die Multiplikation *distributiv* gegenüber der Addition ist, d. h. es gelten $(n+m) \cdot k = n \cdot k + m \cdot k$ und (wegen der Kommutativität der Multiplikation dann auch) $k \cdot (n + m) = k \cdot n + k \cdot m$ für alle $n, m, k \in \mathbb{N}_0$.

Aufgabe 1.8 Zeigen Sie mittels vollständiger Induktion, daß $(\mathbb{N}_0, \cdot, 1)$ ein *kommutatives Monoid* mit *absorbierendem Nullelement* 0 ist, d. h. es gelten die folgenden Aussagen. (Die Aussagen der Aufgaben 1.6 und 1.7 dürfen dabei verwendet werden.)

a) $0 \cdot n = 0 = n \cdot 0$ für alle $n \in \mathbb{N}_0$.

b) 1 ist *neutrales Element* der Multiplikation gemäß $1 \cdot n = n = n \cdot 1$ für alle $n \in \mathbb{N}_0$.

c) Die Multiplikation ist *kommutativ* gemäß $n \cdot m = m \cdot n$ für alle $n, m \in \mathbb{N}_0$.

d) Die Multiplikation ist *assoziativ* gemäß $(n \cdot m) \cdot \ell = n \cdot (m \cdot \ell)$ für alle $n, m, \ell \in \mathbb{N}_0$.

Zusätzlich gelten noch:

e) Es ist $n \cdot m \neq 0$ für alle $m, n \in \mathbb{N}$, d. h. es gilt die Implikation $n \cdot m = 0 \Longrightarrow n = 0$ oder $m = 0$ für alle $n, m \in \mathbb{N}_0$.

f) Jede natürliche Zahl $k \neq 0$ ist *multiplikativ kürzbar* gemäß $n \cdot k = m \cdot k \Longrightarrow n = m$ für alle $n, m \in \mathbb{N}_0$.

Aufgabe 1.9 Zeigen Sie die folgenden *Potenzrechenregeln* für alle natürlichen Zahlen a, b, n, m

$$
\begin{aligned}
&(8) \quad a^n \cdot a^m &&= a^{n+m},\\
&(9) \quad (a \cdot b)^n &&= a^n \cdot b^n,\\
&(10) \quad (a^n)^m &&= a^{n \cdot m}.
\end{aligned}
$$

Aufgabe 1.10 Zeigen Sie, daß $(\mathbb{N}_0, \leq)$ eine *linear geordnete Menge* ist, daß also $\leq$ reflexiv, transitiv und antisymmetrisch ist und für alle $n, m \in \mathbb{N}_0$ bereits $n \leq m$ oder $m \leq n$ gilt. Weiterhin sind sowohl die Addition als auch die Multiplikation *monoton* bezüglich $\leq$, d. h. für alle $n, m, k \in \mathbb{N}_0$ gilt die Implikation $n \leq m \Longrightarrow n + k \leq m + k$ und $n \cdot k \leq m \cdot k$. Für $k \neq 0$ gilt sogar schärfer $n < m \Longrightarrow n + k < m + k$ und $n \cdot k < m \cdot k$.

Bemerkung 1.11 Wir setzen im folgenden den Umgang mit dem in den vorhergehenden Aufgaben betrachteten *partiell geordneten Halbring* $(\mathbb{N}_0, +, \cdot, \leq)$ als bekannt voraus und verwenden Begriffsbildungen aus der Theorie partiell geordneter Mengen. Insbesondere ist 0 kleinstes Element von $(\mathbb{N}_0, \leq)$, während kein größtes Element existiert.

Für jede endliche Menge $\{n_1, n_2, \ldots, n_k\}$ natürlicher Zahlen seien die *Summe* $\sum_{i=1}^{k} n_i$ bzw. das *Produkt* $\prod_{i=1}^{k} n_i$ definiert durch $\sum_{i=1}^{k} n_i = 0$ bzw. $\prod_{i=1}^{k} n_i = 1$ für $k = 0$ sowie $\sum_{i=1}^{k} n_i = n_k + \sum_{i=1}^{k-1} n_i$ bzw. $\prod_{i=1}^{k} n_i = n_k \cdot \prod_{i=1}^{k-1} n_i$ für $k > 0$.

Als letzte Übung zur vollständigen Induktion beweisen wir noch eine Eigenschaft der natürlichen Zahlen, die später häufiger gebraucht werden wird. Zur Vereinfachung des Beweises benutzen wir die folgende gleichwertige Variante des Induktionsaxioms.

Lemma 1.12 *Bei Gültigkeit von (P1) - (P4) ist das folgende Axiom (P5*) gleichwertig zu (P5).*

(P5) Für jede Teilmenge $M \subseteq \mathbb{N}_0$ mit $0 \in M$ und der Eigenschaft, daß für alle $n \in \mathbb{N}_0$ aus $0, 1, \ldots, n \in M$ stets $n' \in M$ folgt, gilt bereits $M = \mathbb{N}_0$.*

Beweis: (P5*) $\Longrightarrow$ (P5): Erfülle die Menge N also die Voraussetzungen von (P5). Dann gilt also $0 \in N$ und aus $0, 1, \ldots, n \in N$ folgt stets $n' \in N$, da dies ja schon aus $n \in N$ folgt. Also erfüllt N die Voraussetzungen von (P5*) und daher gilt $N = \mathbb{N}_0$.

(P5) $\Longrightarrow$ (P5*): Erfülle die Menge N nun die Voraussetzungen von (P5*). Dann gilt jedenfalls $0 \in N$. Sei nun $n \in N$ beliebig. Da N die Voraussetzungen von (P5*) erfüllt, folgt aus $0 \in N$ auch $1 = 0' \in N$. Dann impliziert $0, 1 \in N$ aber auch $2 = 1' \in N$. Nach n-maliger Anwendung dieses Schlusses erhält man $0, 1, \ldots, n \in N$ und dies impliziert jetzt $n' \in N$. Daher erfüllt N die Voraussetzungen von (P5) und dies impliziert $N = \mathbb{N}_0$. ◇

Satz 1.13 *Jede nichtleere Teilmenge natürlicher Zahlen besitzt ein kleinstes Element.*

Beweis: Angenommen, es existiert eine nichtleere Teilmenge M der natürlichen Zahlen ohne kleinstes Element. Betrachte das Komplement $N = \mathbb{N}_0 \setminus M$. Dann gilt $0 \in N$, da sonst $0 \in M$ sicherlich kleinstes Element von M wäre, denn es ist ja sogar kleinstes Element von $\mathbb{N}_0$. Sei nun $n \in N$ so, daß alle natürlichen Zahlen $0, 1, \ldots, n$ ebenfalls in N liegen. Wäre $n' \in M$, dann wäre n' kleinstes Element von M, denn alle in $\mathbb{N}_0$ kleineren Elemente $0, 1, \ldots, n$ liegen ja im Komplement N. Also muß auch $n' \in N$ liegen. Aus (P5*) folgt daher $N = \mathbb{N}_0$ und damit der Widerspruch $M = \emptyset$. ◇

Bemerkung 1.14 In der Ordnungstheorie nennt man partiell geordnete Mengen $(M, \leq)$, für die jede nichtleere Teilmenge von M ein kleinstes Element besitzt,

wohlgeordnet. Auf derartigen Mengen gilt eine Verallgemeinerung des Induktionsaxioms, die sogenannte *transfinite Induktion*. Für die natürlichen Zahlen stimmt sie aber mit der durch (P5) beschriebenen Induktion überein.

Ähnlich wie (P5*) gibt es zahlreiche weitere gleichwertige Varianten zu (P5).

Bemerkung 1.15 Mit Hilfe des Induktionsaxioms lassen sich auch rekursiv Funktionen $f : \mathbb{N}_0 \to \mathbb{N}_0$ definieren, beispielsweise die *Fakultät* $f(n) = n!$ gemäß

$$0! = 1 \tag{11}$$
$$(n+1)! = (n+1) \cdot n! \tag{12}$$

und damit dann weiter die *Binomialkoeffizienten*

$$\binom{n}{m} = \frac{n!}{m! \cdot (n-m)!} \text{ für } n, m \in \mathbb{N}_0, n \geq m \tag{13}$$

oder die *Fibonacci-Zahlen* $f(n) = \phi_n$ (Fibonacci = Leonardo von Pisa, ca. 1180 - 1250) gemäß

$$\phi_1 = 1, \phi_0 = 0 \tag{14}$$
$$\phi_n = \phi_{n-1} + \phi_{n-2} \tag{15}$$

oder die *Catalan-Zahlen* (Eugène Charles Catalan, 1814 - 1894) $f(n) = C_n$ gemäß

$$C_1 = 1, C_0 = 0 \tag{16}$$
$$C_n = \sum_{k=1}^{n-1} C_k \cdot C_{n-k}. \tag{17}$$

Auch Funktionen, die von mehreren natürlichen Zahlen abhängen, lassen sich rekursiv definieren, beispielsweise die *Partitionszahlen* $p(n, k)$ gemäß

$$p(n, n) = p(n, 1) = 1 \text{ für } n \in \mathbb{N} \tag{18}$$
$$p(n, k) = p(n-1, k-1) + p(n-k, k) \text{ für } n, k \in \mathbb{N}, n > k > 1. \tag{19}$$

Ein sehr berühmtes Beispiel einer rekursiv definierten Funktion ist die *Ackermann-Funktion* (Wilhelm Ackermann, 1896 - 1962) in der folgenden Formulierung, die Rózsa Péter (1905 - 1977) im Jahr 1955 angab:

$$
\begin{aligned}
(20) \qquad a(0,n) &= n+1 \text{ für } n \in \mathbb{N}_0 \\
(21) \qquad a(m+1,0) &= a(m,1) \text{ für } m \in \mathbb{N}_0 \\
(22) \qquad a(m+1,n+1) &= a(m,a(m+1,n)) \text{ für } m,n \in \mathbb{N}_0.
\end{aligned}
$$

Ackermann hatte sie bereits 1928 in einer etwas komplizierteren Form als dreistellige Funktion definiert. Sie war das erste Beispiel einer rekursiven Funktion, die nicht *primitiv rekursiv* ist: bei der Berechnung von $a(m,n)$ reicht es nicht aus, die Funktionswerte $a(m',n')$ für alle Werte $m' < m$ und $n' \leq n$ zu ermitteln. Vielmehr kann der Wert des zweiten Argumentes in Abhängigkeit vom ersten Argument beliebig groß werden. Dies führt zu einem außerordentlich raschen Anwachsen der Werte der hieraus abgeleiteten Funktion $f(n) = a(n,n)$.

Aufgabe 1.16 a) Zeigen Sie, daß die Binomialkoeffizienten die folgende rekursive Darstellung besitzen

$$
\begin{aligned}
(23) \qquad \binom{n}{n} &= \binom{n}{0} = 1 \\
(24) \qquad \binom{n+1}{m} &= \binom{n}{m} + \binom{n}{m-1} \text{ für } 0 < m \leq n.
\end{aligned}
$$

b) Für $n > m$ gilt $\binom{n}{m} = \sum_{k=0}^{m} \binom{n-m-1+k}{k}$.

c) Für $n > 1$ gilt $2^n < \binom{2n}{n}$.

Aufgabe 1.17 Beweisen Sie durch vollständige Induktion den *Binomischen Satz* für alle $a, b, n \in \mathbb{N}_0$

$$(25) \quad (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Hieraus folgen dann weiter

a) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$,

b) $\sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$,

c) $\sum_{k=0}^{n} \binom{n}{k} 2^k = 3^n$,

d) $\sum_{k=0}^{n} \binom{n}{k} k = n2^{n-1}$ für $n > 0$.

Aufgabe 1.18 Zeigen Sie die folgenden Aussagen für Fibonacci-Zahlen:

a) $\phi_{n+2} - 1 = \sum_{i=1}^{n} \phi_i$.

b) $\phi_{2n} = \sum_{i=1}^{n} \phi_{2i-1}$.

c) $\phi_{2n+1} - 1 = \sum_{i=1}^{n} \phi_{2i}$.

d) $\phi_n \phi_{n+1} = \sum_{i=1}^{n} \phi_i^2$.

e) $\phi_{2n} + 1 = \phi_1 - \phi_2 + \phi_3 - \phi_4 + \ldots + \phi_{2n+1}$.

f) $1 - \phi_{2n-1} = \phi_1 - \phi_2 + \phi_3 - \phi_4 + \ldots - \phi_{2n}$.

g) $\phi_n^2 = \phi_{n-1}\phi_{n+1} + (-1)^{n+1}$.

h) $\phi_{n+m} = \phi_{n-1}\phi_m + \phi_n \phi_{m+1}$.

Aufgabe 1.19 Beweisen Sie mit vollständiger Induktion (natürlich ist jetzt im Körper $\mathbb{R}$ der reellen Zahlen zu rechnen!) die folgende explizite Darstellung der Fibonacci-Zahlen (Jacques Philippe Marie Binet, 1786 - 1856)

$$\phi_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{\sqrt{5}+1}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right\}. \tag{26}$$

Aufgabe 1.20 Zeigen Sie, daß die Catalan-Zahlen die folgende explizite Darstellung besitzen:

$$C_n = \frac{1}{n+1} \binom{2n}{n}. \tag{27}$$

Es dürfen analytische Hilfsmittel, z. B. erzeugende Funktionen benutzt werden.

Aufgabe 1.21 Geben Sie explizite Formeln für die Werte $a(1,n), a(2,n)$ und $a(3,n)$ der Ackermann-Funktion an. Hinweis: Berechnen Sie zunächst jeweils $a(1,0), a(2,0)$ und $a(3,0)$ und beweisen Sie dann allgemeine Formeln durch Induktion.

1.2 Teilbarkeit, Primzahlen und der Hauptsatz

So wie die partielle Ordnung $\leq$ mit Hilfe der Addition definiert wurde (vgl. Definition 1.3), kann man auch mit Hilfe der Multiplikation eine partielle Ordnung $|$ auf $\mathbb{N}_0$ definieren:

Definition 1.22 Für $n, m \in \mathbb{N}_0$ sei

(28) $n \mid m \iff n \cdot k = m$ für ein $k \in \mathbb{N}_0$.

Man sagt dann, n *teilt* m oder n ist ein *Teiler* von m oder m ist ein *Vielfaches* von n. Gilt $2 \mid n$, so heißt n *gerade*, andernfalls *ungerade*. Ein Teiler n von m mit $n \neq m$ heißt ein *echter Teiler* von m.

Lemma 1.23 *a) Die Teilbarkeitsrelation $|$ ist eine partielle Ordnungsrelation auf $\mathbb{N}_0$.*

b) 0 ist größtes und 1 ist kleinstes Element der partiell geordneten Menge $(\mathbb{N}_0, |)$.

c) $d \mid a$ und $d \mid b \Longrightarrow d \mid (xa + yb)$ für alle $d, a, b, x, y \in \mathbb{N}_0$.

d) Aus $d \mid a$ und $a \neq 0$ folgt $d \leq a$. Jede von 0 verschiedene natürliche Zahl hat also nur endlich viele verschiedene Teiler.

Beweis: a) Wegen $a \cdot 1 = a$ ist $|$ reflexiv. Aus $a \cdot x = b$ und $b \cdot y = c$ folgt $a \cdot (x \cdot y) = c$, also ist $|$ auch transitiv. Zum Nachweis der Antisymmetrie gelte $a \cdot x = b$ und $b \cdot y = a$ für $a, b, x, y \in \mathbb{N}_0$. Aus $a = 0$ würde $b = 0 = a$ folgen und ebenso aus $b = 0$ auch $a = 0 = b$. Es bleiben also $a, b \in \mathbb{N}$ zu betrachten. Dann gilt auch $x, y \in \mathbb{N}$ und alle Elemente sind in $(\mathbb{N}_0, \cdot, 1)$ kürzbar. Also folgt aus $a = a \cdot (x \cdot y)$ sofort $1 = x \cdot y$ und damit in $\mathbb{N}$ sofort $x = y = 1$.

b) Wegen $n \cdot 0 = 0$ gilt $n \mid 0$, wegen $1 \cdot n = n$ gilt $1 \mid n$ für alle $n \in \mathbb{N}_0$.

c) Aus $a = d \cdot a'$ und $b = d \cdot b'$ folgt $xa + yb = d \cdot (xa' + yb')$.

d) Aus $a = d \cdot b$ und $a \neq 0$ folgt $b \neq 0$, also $1 \leq b$. Mit der Monotonie der Multiplikation (vgl. Aufgabe 1.10) ergibt sich hieraus $d \leq d \cdot b = a$. $\diamond$

Aufgabe 1.24 Für $n \in \mathbb{N}_0$ gilt $30 \mid (n^5 - n)$.

Aufgabe 1.25 Zeigen Sie, daß eine natürliche Zahl genau dann durch 3 teilbar ist, wenn ihre Quersumme durch 3 teilbar ist. Untersuchen Sie, ob diese Aussage auch für andere Ziffern aus $\{2, \ldots, 9\}$ gilt.

Definition 1.26 Zwei natürliche Zahlen $n, m \in \mathbb{N}$ heißen *teilerfremd* oder *relativ prim*, wenn 1 ihr einziger gemeinsamer Teiler ist.

Aufgabe 1.27 a) Zeigen Sie, daß je zwei aufeinander folgende Fibonacci-Zahlen teilerfremd sind.

b) Für $n, m \in \mathbb{N}$ gilt $\phi_m \mid \phi_{mn}$.

Definition 1.28 Eine natürliche Zahl $n > 1$ heißt *Primzahl*, wenn n nur die (trivialen) Teiler 1 und n besitzt, andernfalls nennt man n *zusammengesetzt*. Die Menge aller Primzahlen werde mit $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ (vgl. Abschnitt 7.1) bezeichnet.

Ist $p \in \mathbb{P}$ und $n \in \mathbb{N}$, so versteht man unter der *p-Bewertung* $k = v_p(n)$ *von* n den größten Exponenten $k \in \mathbb{N}_0$, für den p^k Teiler von n ist. Man schreibt dann $p^{v_p(n)} || n$. Für $n = 0$ setzt man $v_p(0) = \infty$.

Schließlich bezeichne $\pi(x)$ für jede (positive) reelle Zahl x die Anzahl der Primzahlen $p \in \mathbb{P}$ mit $p \leq x$.

Aufgabe 1.29 Man zeige für alle $n \in \mathbb{N}$ und $p \in \mathbb{P}$

$$v_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

Hierbei sei die *Gauss-Klammer* $[x]$ (Carl Friedrich Gauss, 1777 - 1855) für alle nichtnegativen reellen Zahlen x die größte natürliche Zahl, die kleiner oder gleich x ist.

Die Summe auf der rechten Seite ist natürlich stets endlich!

Die folgenden beiden Aussagen finden sich bereits in den “Elementen” des Euklid (365 - 300 v. Chr.).

Lemma 1.30 *Jede natürliche Zahl $n > 1$ besitzt eine Primzahl als Teiler. Insbesondere ist der kleinste Teiler $p > 1$ von n eine Primzahl.*

Beweis: Betrachte zu $n > 1$ die Menge M aller Teiler $m > 1$ von n. Wegen $n \in M$ ist M nicht leer, besitzt also nach Satz 1.13 ein kleinstes Element p. Jede natürliche Zahl k mit $1 < k < p$ kann dann nicht p teilen, da k wegen der Transitivität der Teilbarkeitsrelation sonst auch ein Teiler von n und kleiner als p wäre. Also ist p eine Primzahl. ◇

Folgerung 1.31 *Jede natürliche Zahl $n > 1$ besitzt eine Primfaktorzerlegung*

$$n = p_1 \cdots p_k \tag{29}$$

mit (nicht notwendig verschiedenen) Primfaktoren $p_i \in \mathbb{P}$, die $p_1 \leq p_2 \leq \cdots \leq p_k$ erfüllen.

Beweis: Nach Lemma 1.30 existiert eine kleinste Primzahl $p_1 \in \mathbb{P}$ mit $n = p_1 \cdot n_1$ und $n_1 \in \mathbb{N}$. Damit gilt $n_1 < n$. Ist $n_1 > 1$, so existiert eine kleinste Primzahl $p_2 \in \mathbb{P}$ mit $n_1 = p_2 \cdot n_2$ und daher $n_2 < n_1 < n$. So fortfahrend, muß man nach endlich vielen Schritten zu $n_k = 1$ gelangen. Damit ist dann die Zerlegung $n = p_1 \cdots p_k$ gefunden. ◇

Definition 1.32 Die für jede natürliche Zahl $n > 1$ im Beweis von Folgerung 1.31 gefundene Primfaktorzerlegung (29) nennt man die *kanonische Zerlegung* von n. Man faßt noch gleiche Faktoren p_i zu Potenzen zusammen und schreibt mit Hilfe der p-Bewertungen $v_p(n)$

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)} \tag{30}$$

als formal unendliches Produkt. Diese Darstellung gilt auch für $n = 1$ und mit der zusätzlichen Verabredung $v_p(0) = \infty$ aus Definition 1.28 für $n = 0$.

Der folgende Satz ist der zentrale Satz der elementaren Zahlentheorie. Der hier angegebene Beweis der Eindeutigkeit geht auf Ernst Zermelo (1871 - 1953) zurück und findet sich beispielsweise in [12]. Im Unterschied zu vielen anderen Beweisen wird nur innerhalb der natürlichen Zahlen argumentiert und die negativen Zahlen werden nicht benutzt.

Satz 1.33 (Hauptsatz der Arithmetik) *Jede natürlich Zahl $n > 1$ besitzt eine Primfaktorzerlegung gemäß (30) und diese Zerlegung ist bis auf die Reihenfolge der Faktoren eindeutig.*

Beweis: Wegen Folgerung 1.31 ist nur noch die Eindeutigkeit der Faktoren zu zeigen, die natürlich wegen der Kommutativität der Multiplikation stets beliebig vertauscht werden können. Angenommen, es existieren natürliche Zahlen, die außer der kanonischen Zerlegung noch eine weitere Zerlegung besitzen. Sei $n > 1$ die kleinste unter ihnen, die nach Satz 1.13 dann existieren muß. Insbesondere kann n keine Primzahl sein, da jede Primzahl nur die eindeutige Zerlegung $n = n$ besitzt. Sei weiterhin p der kleinste Primteiler von n und $n = p \cdot k$ die kanonische Zerlegung, wobei die weiteren Primfaktoren in k zusammengefaßt seien. Es gilt $k < n$ und damit hat k eine eindeutige Primfaktorzerlegung. Sei nun $n = q \cdot \ell$ eine weitere, von der kanonischen Zerlegung verschiedene Zerlegung von n mit q als kleinster Primzahl in dieser Zerlegung und ℓ als Produkt der restlichen Primfaktoren. Wieder gilt $\ell < n$ und ℓ besitzt folglich eine eindeutige Primfaktorzerlegung. Nun würde $p = q$ wegen der multiplikativen Kürzbarkeit zu $k = \ell$ und damit zur Übereinstimmung der beiden Primfaktorzerlegungen führen. Da p kleinster Primteiler von n ist, gilt $p < q$ und damit $\ell < k$. Also existieren $r, s \in \mathbb{N}$ mit $p + r = q$ und $\ell + s = k$. Aus den Distributivgesetzen folgt $p \cdot \ell + p \cdot s = p \cdot k = n$ und $p \cdot \ell + r \cdot \ell = q \cdot \ell = n$. Also gilt $p \cdot \ell + p \cdot s = p \cdot \ell + r \cdot \ell$ und aus der additiven Kürzbarkeit folgt $p \cdot s = r \cdot \ell$. Die natürlichen Zahlen r, ℓ und $r \cdot \ell$ sind sämtlich kleiner als n, besitzen also eindeutige Primfaktorzerlegungen. Nun ist p ein Teiler des Produktes $r \cdot \ell$, kommt aber unter den Primfaktoren von ℓ nicht vor, da $p < q$ gilt und q der kleinste Primfaktor der Zerlegung von $n = q \cdot \ell$ ist. Also muß p als Primfaktor von $r \cdot \ell$ ein Teiler von r sein. Dann ist p aber auch ein Teiler von $p + r = q$. Dies ist unmöglich, da q und $p < q$ Primzahlen sind. ◇

Folgerung 1.34 *Seien $n, a, b \in \mathbb{N}$ sowie n und a teilerfremd. Aus $n \mid ab$ folgt dann $n \mid b$.*

Speziell für Primzahlen p gilt

(31) $p \mid ab \Longrightarrow p \mid a$ *oder* $p \mid b$.

Beweis: Jeder Primfaktor von n kommt in der Primfaktorzerlegung von ab, aber nicht in der von a vor. Daher muß er in der Primfaktorzerlegung von b vorkommen.

Speziell für Primzahlen $n = p$ folgt hieraus: Ist p kein Teiler von a, so sind p und a schon teilerfremd. Also gilt dann $p \mid b$. ◇

Folgerung 1.35 *Sind $m, n \in \mathbb{N}$ teilerfremd so gilt für alle $a \in \mathbb{N}$*

(32) $m \mid a, n \mid a \Longrightarrow mn \mid a$

Beweis: Die Primfaktoren von n sind von allen Primfaktoren von m verschieden. Alle diese Primfaktoren kommen aber unter den Primfaktoren von a vor. ◇

Folgerung 1.36 *Gilt für $n, n_1, n_2 \in \mathbb{N}$ die Zerlegung $n = n_1 n_2$ mit teilerfremden n_1 und n_2, so existiert für jeden Teiler d von n eine eindeutige Zerlegung $d = d_1 d_2$ mit $d_i \mid n_i$.*

Beweis: Betrachte die Primfaktoren p_i der Primfaktorzerlegung von d. Wegen $p_i \mid n = n_1 n_2$ gilt $p_i \mid n_1$ oder $p_i \mid n_2$, wegen der Teilerfremdheit von n_1 und n_2 aber nicht beides gleichzeitig. Dann besteht d_1 genau aus den Primfaktoren, die n_1 teilen, und d_2 aus den anderen. ◇

Bemerkung 1.37 Man kann auch umgekehrt aus der Eigenschaft (31) für alle Primzahlen p und alle natürlichen Zahlen a, b den Hauptsatz der Arithmetik beweisen. Daher sind beide Aussagen gleichwertig.

Man nennt in kommutativen Ringen mit Einselement allgemein Elemente p, die (31) erfüllen *prim*, während Elemente, die entsprechend Definition 1.28 nur triviale Teiler besitzen, *irreduzibel* genannt werden. Im Halbring $(\mathbb{N}_0, +, \cdot)$ (und auch im Ring $(\mathbb{Z}, +, \cdot)$) stimmen also beide Begriffe überein. Dies ist aber in allgemeinen Ringen nicht mehr der Fall.

Aufgabe 1.38 Zeigen Sie, daß für alle $p \in \mathbb{P}$ und $\alpha, \beta, n, m \in \mathbb{N}$ gilt:

i) $p^\alpha || n, p^\beta || m \Longrightarrow p^{\alpha+\beta} || nm$,

ii) $p^\alpha || n, p^\beta || m, \alpha < \beta \Longrightarrow p^\alpha || n \pm m$.

Zeigen Sie durch ein Gegenbeispiel, daß ii) für $\alpha = \beta$ falsch werden kann.

Aufgabe 1.39 a) Zeigen Sie durch Vergleich mit der divergenten harmonischen Reihe, daß das Produkt

$$\prod_{p \in \mathbb{P}} (1 - \frac{1}{p})^{-1} = \prod_{p \in \mathbb{P}} \left(\sum_{\nu=0}^{\infty} \left(\frac{1}{p} \right)^\nu \right)$$

gegen ∞ divergiert. (Wie schon Leonhard Euler (1707 - 1783) bemerkte, folgt hieraus ebenfalls die Unendlichkeit von $\mathbb{P}$).

b) Zeigen Sie unter Benutzung von $x > -\frac{1}{2}\log(1-x)$ für $x \leq \frac{1}{2}$, daß auch

$$\sum_{p\in\mathbb{P}} \frac{1}{p}$$

divergiert, daß es also "wesentlich mehr" Primzahlen gibt, als Quadratzahlen.

Bemerkung 1.40 Im Unterschied hierzu ist

$$\sum_{(p,p+2)\text{ Primzahlzwillinge}} \left(\frac{1}{p}+\frac{1}{p+2}\right) = 1.90216054...$$

konvergent (vgl. Bemerkung 1.87).

Definition 1.41 Jede Funktion $f : \mathbb{N} \to \mathbb{C}$ heißt eine *zahlentheoretische* Funktion, sie heißt *multiplikativ*, wenn sie

$$(33)\quad f(1) = 1 \text{ und } f(n \cdot m) = f(n) \cdot f(m)$$

für teilerfremde $n, m \in \mathbb{N}$ erfüllt.

Beispiel 1.42 Es sei $k \in \mathbb{N}_0$. Die *k-te Teilersummenfunktion* $\sigma_k : \mathbb{N} \to \mathbb{N}$ ist definiert durch

$$(34)\quad \sigma_k(n) = \sum_{1\leq d\leq n,\ d|n} d^k.$$

Also zählt σ_0 die Anzahl der Teiler von n, während σ_1 alle Teiler aufsummiert.

Wegen $\sigma_k(1) = 1$ und Folgerung 1.36 ist σ_k multiplikativ für alle $k \in \mathbb{N}_0$.

Für Primzahlpotenzen $p^m, m \in \mathbb{N}_0$ ist $\sigma_0(p^m) = m+1$ und $\sigma_1(p^m) = 1+p+p^2+\ldots+p^m = \frac{p^{m+1}-1}{p-1}$.

1.3 Primzahlen besonderer Bauart

Auch die nächste Aussage findet sich schon bei Euklid.

Lemma 1.43 $\mathbb{P}$ *ist unendlich, d. h.* $\pi(x)$ *wächst unbeschränkt.*

Beweis: Wäre $\mathbb{P} = \{p_1, \ldots, p_k\}$ endlich, dann wäre $n = 1 + \Pi_{i=1}^{k} p_1 > 1$ durch keine der Primzahlen aus $\mathbb{P}$ teilbar im Widerspruch zu Lemma 1.30. $\diamond$

Bemerkung 1.44 a) Man bezeichnet für jede Primzahl p mit $p\# + 1$ die Zahl $p_1 \cdots p_k + 1$, wobei $p_1 < p_2 < \ldots < p_k = p$ alle verschiedenen Primzahlen $p_i \leq p$ seien. Es stellt sich daher im Beweis von Lemma 1.43 die Frage, wann $N = p\#+1$ selbst schon eine Primzahl ist. Diese wird dann eine *euklidische Primzahl* genannt. Es ist bekannt, daß für $N \leq 10^{10000}$ dies genau für $p = 2$, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3329, 4547, 4787, 11549, 13649, 18523, 24029 der Fall ist. Ob es unendlich viele euklidische Primzahlen gibt, ist noch ungeklärt (vgl. auch 7.4 für weitere Primzahlen in dieser Folge).

Entsprechendes gilt für die Zahlen $N = p\# - 1$ und $N \leq 10^{10000}$. Genau für $p = 3$, 5, 11, 13, 41, 89, 317, 991, 1873, 2053, 2377, 4093, 4297, 4583, 6569, 13033, 15877 sind dies Primzahlen (vgl. auch 7.4).

b) Untersucht man analog die Zahlen $N = n! + 1$ mit $N \leq 10^{10000}$, so findet man genau für $n = 1, 2, 3, 11, 27, 37, 41, 73, 77, 116, 154, 320, 340, 399, 427, 872, 1477$ Primzahlen (vgl. auch 7.3 für weitere Primzahlen in dieser Folge).

Untersucht man $N = n! - 1$ mit $N \leq 10^{10000}$, so findet man genau für $n = 3, 4, 6, 7, 12, 14, 30, 32, 33, 38, 94, 166, 324, 379, 469, 546, 974, 1963$ Primzahlen (vgl. auch 7.3 für weitere Primzahlen in dieser Folge).

Aufgabe 1.45 Es sei $(p_k)_{k\in\mathbb{N}}$ die Folge der Primzahlen in ihrer natürlichen Reihenfolge. Zeigen Sie, daß $p_{k+1} < p_k^k + 1$ und $p_k < 2^{2^k}$ für alle $k > 1$ gelten.

Definition 1.46 Eine ungerade Primzahl $p = 2m + 1, m \in \mathbb{N}$ heißt *Germain-Primzahl* (Sophie Germain, 1776 - 1831), wenn auch $q = 2p + 1 = 4m + 3 = 4(m + 1) - 1$ eine Primzahl ist (vgl. 7.2 und 7.5).

Dagegen heißt p wie oben eine *Stern-Primzahl* (Moritz Abraham Stern, 1807 - 1894), wenn auch $q = 4p + 1 = 8m + 5$ eine Primzahl ist (vgl. 7.2).

Bemerkung 1.47 a) Sophie Germain bewies für die heute nach ihr benannten Primzahlen p die Aussage des großen Fermatschen Satzes: Es gibt keine ganzen Zahlen x, y, z, die von 0 verschieden sind und keine Vielfachen von p, so daß die Gleichung

$$x^p + y^p = z^p$$

gilt.

b) Germain-Primzahlen sind in der Kryptographie zur Konstruktion von Stromchiffren von Interesse. Daher macht es Sinn, unter den Primzahlen aus Bemerkung 1.44 nach ihnen zu suchen.

Sei $q = N_n = n! - 1$ Primzahl. Wann ist auch $p = (N_n - 1)/2 = (n! - 2)/2$ eine Primzahl? Man erhält $(N_3 - 1)/2 = 2$, $(N_4 - 1)/2 = 11$, $(N_6 - 1)/2 = 359$ sind prim, aber $(N_7 - 1)/2 = 2519 = 11 \cdot 229$ nicht. Auch die im Forschungsproblem [3], 5.5.1 genannten Zahlen $(N_{12} - 1)/2, (N_{14} - 1)/2, (N_{30} - 1)/2, (N_{32} - 1)/2$, sowie $(N_{33} - 1)/2$ und $(N_{38} - 1)/2$ sind keine Primzahlen.

Sei $P_p = p\# - 1$. Dann kann man auch P_p und $(P_p - 1)/4$, falls beides Primzahlen sind, zur Konstruktion guter Stromchiffren verwenden. Man erhält $P_3 = 5 = 4 \cdot 1 + 1$, $P_5 = 29 = 4 \cdot \mathbf{7} + 1$, $P_{11} = 2309 = 4 \cdot \mathbf{577} + 1$, $P_{13} = 30029 = 4 \cdot \mathbf{7507} + 1$.

Forschungsproblem: (Vgl. [3], 5.5.2) Ist $(P_{317} - 1)/4$ prim? Die dort ebenfalls genannten Zahlen $(P_{41} - 1)/4$ und $(P_{89} - 1)/4$ sind jedenfalls nicht prim.

Ebenfalls in [3] findet man das folgenden Forschungsproblem für Primzahlen (zur Konstruktion guter Stromchiffren) gestellt, die in Analogie zu den Germain-Primzahlen gebildet werden:

Forschungsproblem: (Vgl. [3], 5.2.4 - 5.2.7) Für $k = 4, 8, 16, 32$ finde große Primzahlen p, so daß auch $q = k \cdot p + 1$ eine Primzahl ist (vgl. auch Satz 4.23).

c) Stern bewies 1830 den Satz 4.6 für die nach ihm benannten Primzahlen.

1.4 Primzahltests und Faktorisierung

Aus dem Hauptsatz der Arithmetik ergeben sich für natürliche Zahlen die beiden folgenden (wegen der Unendlichkeit von $\mathbb{P}$ nichttrivialen!) Problemstellungen.

Primzahltest Man gebe einen Algorithmus an, der für jedes $n \in \mathbb{N}$ (möglichst effizient) feststellt, ob $n \in \mathbb{P}$ gilt oder nicht.

Faktorisierung Man gebe einen Algorithmus an, der für beliebiges $n \in \mathbb{N}$ (möglichst effizient) sämtliche Primfaktoren ermittelt.

Bemerkung 1.48 Da für eine natürliche Zahl $n = a \cdot b$ mit $a, b \in \mathbb{N}$ aus $a \leq \sqrt{n}$ wegen der Monotonie der Multiplikation sofort $\sqrt{n} \leq b$ folgt, existiert eine Bijektion $a \leftrightarrow b$ zwischen diesen Teilern. Man braucht also beim Primzahltest für eine natürliche Zahl n "nur" die Primzahlen $p \in \mathbb{P}$ mit $p \leq \sqrt{n}$ als mögliche Teiler von n durch "Probedivision" auszuschließen. Da man außerdem an der letzten Stelle der (dezimalen oder binären) Darstellung von n direkt ablesen kann, ob n gerade ist oder nicht, darf bei allen Primzahltests davon ausgegangen werden, daß n ungerade ist und daher auch nur ungerade Teiler haben kann.

Algorithmus 1.49 Trivialer Primzahltest

Eingabe: $n > 1$ ungerade

Ausgabe: true, falls $n \in \mathbb{P}$, sonst false

```
w:=[sqrt[n]]
for k:=3(2)w
   if [n/k]*k=n then false, stop endif
endfor
true, stop
```

Man kann diesen Algorithmus, wie oben schon bemerkt, dadurch verbessern, daß man die Laufvariable k nicht alle ungeraden Zahlen unterhalb $\sqrt{n}$ durchlaufen läßt, sondern nur die betreffenden Primzahlen, die man dann aber zunächst ermitteln müßte. Hilfreich wäre dazu eine hinreichend lange Liste der ersten Primzahlen. Auch hierfür wurde bereits durch einen antiken griechischen Mathematiker ein Algorithmus angegeben:

Algorithmus 1.50 Sieb des Eratosthenes (um 270 - 196 v. Chr.)

Eingabe: $n > 1$

Ausgabe: *Lp = Liste aller* $p \in \mathbb{P}$ *mit* $p \leq n$

```
w:=[sqrt(n)]
L := (2,3,...,n)
Lp :={}
do
   entferne erstes Element p aus L,
   streiche alle Vielfachen von p aus L,
   Lp:= Lp + {p}
   if p>sqrt(n) then Lp:=Lp + L, stop endif
od
```

Aufgabe 1.51 a) Modifizieren Sie den Algorithmus 1.49 so, daß er auch für gerade natürliche Zahlen $n > 1$ arbeitet und als Ausgabe den kleinsten Primteiler von n liefert.

b) Benutzen Sie den Algorithmus aus Teil a) zur Konstruktion eines Faktorisierungsalgorithmus, der die im Beweis von Folgerung 1.31 konstruierte Faktorisierung von $n > 1$ berechnet.

Bemerkung 1.52 In 7.9 ist eine Tabelle der Primfaktorzerlegungen der ersten Fibonacci-Zahlen angegeben. Der Eintrag für $n = 19$ zeigt, daß die Vermutung "n prim $\Longrightarrow \phi_n$ prim" falsch ist. Trotzdem besteht ein Zusammenhang zwischen Teilbarkeiten der Indizes und der zugehörigen Fibonacci-Zahlen. Welcher ist es? Beweisen Sie Ihre Vermutung!

1.5 Mersenne-Zahlen, vollkommene Zahlen und Fermat-Zahlen

Statt einen universellen Algorithmus anzugeben, der die oben gestellten Probleme für alle natürlichen Zahlen löst, beschränkt man sich oft darauf, das jeweilige Problem für Zahlen einer ganz bestimmten Form zu lösen.

Ein auf Pierre de Fermat (1601 - 1665) zurückgehender Faktorisierungsalgorithmus, insbesondere für Zahlen der Form $n = p \cdot q$ mit verschiedenen Primzahlen p und q (solche Zahlen n werden beispielsweise in der Kryptographie beim RSA–Kryptosystem als öffentliche Schlüssel benutzt), beruht auf folgender Aussage.

Lemma 1.53 *a) Jede ungerade natürliche Zahl n ist Differenz zweier Quadratzahlen.*

b) Ist n ungerade und keine Quadratzahl, so besteht eine Bijektion zwischen allen Darstellungen von n als Differenz zweier Quadratzahlen und den Teilern q von n mit $q > \sqrt{n}$.

Beweis: a) Es ist $n = 2k + 1 = (k + 1)^2 - k^2$.

b) Gilt $n = a^2 - b^2 = (a + b)(a - b)$ mit $b \neq 0$, so folgt $n = pq$ für $q = a + b > \sqrt{n} > p = a - b$. Umgekehrt liefern dann $a = \frac{q+p}{2}$ und $b = \frac{q-p}{2}$ die Darstellung $n = a^2 - b^2$. Offensichtlich bestimmen q und (a, b) sich gegenseitig eindeutig. $\diamond$

Gilt nun $n = pq$ mit ungeraden Primzahlen $p < q$, die beide "in der Nähe" von $\sqrt{n}$ liegen, so kann man wie folgt nach ihnen suchen. Man setzt $n = p \cdot q =$

$a^2 - b^2 = (a-b)\cdot(a+b)$, woraus $p = a - b$, $q = a + b$ und insbesondere $a > \sqrt{n}$ folgt. Nun prüft man für $a = [\sqrt{n}] + 1, [\sqrt{n}] + 2, \ldots, \frac{n-1}{2}$, wann $a^2 - n = b^2$ eine (kleine) Quadratzahl ist. Ist dies der Fall, so hat man mit a und b auch p und q gefunden.

Beispiel 1.54 Zur Faktorisierung von $n = 200819$ beginnt man also mit $a = [\sqrt{200819}] + 1 = 449$. Es ist aber $449^2 - 200819 = 782$ keine Quadratzahl. Daher fährt man mit $a = 450$ fort. Man erhält $450^2 - 200819 = 1681 = 41^2$, woraus $200819 = (450 + 41)(450 - 41) = 491 \cdot 409$ folgt.

Aufgabe 1.55 Faktorisieren Sie mittels Fermat-Faktorisierung die Zahlen i) 8633, ii) 88169891, iii) 305321, iv) 809009, v) 4601 und vi) 92296873.

Aufgabe 1.56 Führen Sie eine iterierte Fermat-Faktorisierung durch, um die jeweilige Primfaktorzerlegung der folgenden Zahlen zu erhalten: i) 200583, ii) 3786965 und iii) 13717.

Aufgabe 1.57 Formulieren Sie einen entsprechenden Faktorisierungsalgorithmus für derartige ungerade natürliche Zahlen $n = pq$.

Die folgenden einfachen Überlegungen führen direkt zu Fragen, die den augenblicklichen Stand in einem Teilbereich der Primzahlforschung betreffen.

Lemma 1.58 *Für alle $a \in \mathbb{N}$ und $n, m \in \mathbb{N}$ gilt*

(35) $a^{mn} - 1 = (a^m - 1)(a^{m(n-1)} + \ldots + a^{2m} + a^m + 1)$.

Ist n ungerade, so gilt

(36) $a^{mn} + 1 = (a^m + 1)(a^{m(n-1)} - a^{m(n-2)} + \ldots + a^{2m} - a^m + 1)$.

Beweis: Sei zunächst $m = 1$. Multipliziert man $b = a^{n-1} + \ldots + a^2 + a + 1$ mit a und zieht davon wieder b ab, so erhält man $a^n - 1 = ab - b = (a-1)b$, also die Behauptung. Im Fall $m > 1$ ersetzt man a durch a^m und erhält mit den Potenzrechenregeln dann auch hierfür die Behauptung.

Auch bei der zweiten Gleichung reicht es, den Fall $m = 1$ zu zeigen. Multipliziert man $b = a^{n-1} - a^{n-2} + \ldots + a^2 - a + 1$ mit a und addiert dazu b so erhält man $a^n + 1 = ab + b = (a+1)b$. ◇

Eine natürliche Zahl der Form $a^n - 1$ mit $n > 1$ kann also nur für $a = 2$ Primzahl sein, und dann auch nur, wenn n selbst schon eine Primzahl ist.

Definition 1.59 Eine Primzahl der Form $M_p = 2^p - 1$ mit $p \in \mathbb{P}$ heißt eine *Mersennesche Primzahl* (Marin Mersenne, 1588-1648).

Bemerkung 1.60 Für $p = 2, 3, 5, 7$ ergeben sich die Primzahlen $M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127$, für $p = 11$ gilt jedoch $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$.

Indem man die (beispielsweise durch das Sieb des Eratosthemes gefundene) Liste der ersten Primzahlen systematisch durchgeht und für alle Primzahlen p hieraus den in Satz 3.21 beschriebenen Primzahltest auf $M_p = 2^p - 1$ anwendet, hat man inzwischen 50 Mersennesche Primzahlen gefunden (vgl. Abschnitt 7.11), und es wird vermutet, daß es sogar unendlich viele gibt.

In Analogie zu den Mersenne-Zahlen hat Catalan rekursiv die folgenden, Catalan-Mersenne-Zahlen definiert

$$C(0) = 2, C(k+1) = 2^{C(k)} - 1.$$

Neben $C(0) = 2$ sind auch $C(1) = 3$, $C(2) = 7$, $C(3) = 127$ und $C(4) = 170141183460469231731687303715884105727$ prim, über $C(5)$ weiß man nicht ob sie prim ist, aber wenn nicht, so hat sie keinen Primfaktor unterhalb von 10^{51}. Die weiteren Zahlen dieser Folge liegen wohl für immer jenseits aller Berechnungsmöglichkeiten.

Die Zahlen $C(n)$ bilden eine Teilfolge der *doppelten Mersenne-Zahlen* $M_{M_n} - 1$. Diese können natürlich nur Primzahlen sein, wenn M_n und daher auch n Primzahlen sind. Für $p = 2, 3, 5, 7$ erhält man tatsächlich (Mersennesche) Primzahlen, für $p = 13, 17, 19, 31$ hat man gezeigt, daß sie zusammengesetzt sind und man hat jeweils einen Primfaktor gefunden. Der nächste Kandidat für $p = 61$ ist ungefähr $1.695 \cdot 10^{10694127911065419641}$ und damit auch weit jenseits aller heute bekannten Primzahltests. Es existiert aber kein Primfaktor unterhalb von $4 \cdot 10^{33}$.

Euler hat den folgenden Satz gezeigt, den wir mit etwas mehr Hilfsmitteln als Folgerung 2.89 beweisen werden.

Satz 1.61 *Ist $k \in \mathbb{N}$ und sind $p = 4k+3$ und $q = 2p+1$ prim (und damit p eine Germain-Primzahl, vgl. Definition 1.46) so ist q ein echter Teiler von M_p (vgl. auch Aufgabe 2.55).*

Bemerkung 1.62 Wenn es also unendlich viele Germain-Primzahlen der Form $p = 4k + 3$ gibt (vgl. Aufgabe 1.82), so gibt es auch unendlich viele zusammengesetzte Mersenne-Zahlen (vgl. Folgerung 2.90).

Jedenfalls gilt damit $23 \mid M_{11},\ 47 \mid M_{23},\ 167 \mid M_{83}, 263 \mid M_{131},\ 359 \mid M_{179},\ 383 \mid M_{191},\ 479 \mid M_{239}, 503 \mid M_{251}$ usw.

Außerdem gelten beispielsweise $q = 223 \mid M_{37}$ (also $q = 6p + 1$), $q = 233 \mid M_{29}$ (also $q = 8p + 1$) und $q = 431 \mid M_{43}$ (also $q = 10p + 1$).

Wegen ihrer besonderen Darstellung im Binärsystem (ein Bitstring aus p Einsen, vgl. Definition 1.70) und des speziell auf sie zugeschnittenen sehr schnellen Primzahltests (Lucas-Lehmer-Test), (Francois Edouard Anatole Lucas, 1842 - 1891, Derrick Henry Lehmer, 1905 - 1991) ist die jeweilige"Rekordprimzahl" schon seit 1876 mit nur 2 kurzen Unterbrechungen stets eine Mersennesche Primzahl. Vom Juni 1951 bis zum Januar 1952 waren nacheinander die Zahlen $180 \cdot (2^{127} - 1) + 1, 934 \cdot (2^{127} - 1) + 1$ und $(2^{148} + 1)/17$, vom 6. August 1989 bis zum 18. Februar 1992 war die Zahl $391581 \cdot 2^{216193} - 1$ Rekordhalter.

Aufgabe 1.63 Zeigen Sie, daß eine Mersennesche Primzahl M_p nicht Summe von zwei Quadratzahlen sein kann. Hinweis: Betrachten Sie die Teilbarkeit durch 4.

Die Mersenneschen Primzahlen sind eng mit den vollkommenen oder perfekten Zahlen verbunden.

Definition 1.64 Eine natürliche Zahl n heißt *vollkommen* oder *perfekt*, wenn sie gleich der Summe ihrer echten Teiler ist, wenn also gilt

$$\sigma_1(n) = 2n.$$

Bemerkung 1.65 Die kleinsten, schon bei den Babyloniern und Ägyptern bekannten vollkommenen Zahlen sind $6 = 1 + 2 + 3$ und $28 = 1 + 2 + 4 + 7 + 14$. Bei Nikomachus von Gerasa (um 100 n. Chr.) finden sich dann 496 und 8128. Man kennt wegen des folgenden Satzes 1.66, dessen eine Richtung sich bereits als Satz 36 im IX. Buch der "Elemente" des Euklid findet, weitere, die sämtlich gerade sind.

Bis heute ist keine ungerade perfekte Zahl bekannt und man weiß nicht, ob es überhaupt eine gibt. Man weiß aber ([16], Remark 6.2.5), daß eine ungerade vollkommene Zahl das Produkt aus einer Quadratzahl und einem weiteren einzelnen Primfaktor in ungerader Potenz sein müßte, insgesamt mindestens acht verschiedene Primteiler besitzen und mindestens 29 Primfaktoren haben müßte. Sie wäre größer als 10^{300}, ihr größte Primfaktor größer als $5 \cdot 10^5$ und der zweitgrößte größer als 10^3.

Satz 1.66 (Satz von Euklid und Euler) *Es sei $n = 2^m u$, $m, u \in \mathbb{N}$, $u > 1$ ungerade. Genau dann ist n vollkommen, wenn $u = 2^{m+1} - 1$ eine Mersennesche Primzahl ist.*

Beweis: Der Teil von Euklid: Sei $u = 2^{m+1}-1$ eine Primzahl. Dann sind die Teiler von $n = 2^m u$ genau die Zweierpotenzen $1, 2, 2^2, \ldots, 2^m$ und diese Zweierpotenzen multipliziert mit u, also $u, 2u, \ldots, 2^m u = n$. Summiert man nun über die Teiler, so erhält man $\sum_{k=0}^{m} 2^k + u \sum_{k=0}^{m} 2^k$. Die erste Summe ist gerade $2^{m+1} - 1 = u$, die zweite $u(2^{m+1} - 1)$. Zusammen ergibt sich als Teilersumme genau $2n$, d. h. n ist vollkommen.

Umkehrung von Euler: Es sei $n = 2^m u$ vollkommen, $u > 1$ ungerade. Da 2^m und u teilerfremd sind, gilt $2^{m+1}u = 2n = \sigma_1(n) = \sigma_1(2^m)\sigma_1(u) = (2^{m+1} - 1)\sigma_1(u) = (2^{m+1} - 1)(\sigma_1(u) - u) + (2^{m+1} - 1)u$. Hieraus folgt $u = (2^{m+1} - 1)(\sigma_1(u) - u)$, also ist $d = \sigma_1(u) - u$ ein echter Teiler von u. Andererseits ist $\sigma_1(u) - u$ aber genau die Summe aller echten Teiler von u. Also hat u nur diesen einen echten Teiler und daher ist $\sigma_1(u) - u = d = 1$, also $\sigma_1(u) = u + 1$. Folglich ist $u = 2^{m+1} - 1$ eine Primzahl. ◇

Aufgabe 1.67 Zeigen Sie, daß eine Primzahlpotenz $n = p^k$ mit $k \geq 1$ keine vollkommene Zahl sein kann, daß eine ungerade vollkommene Zahl also mindestens zwei verschiedene Primteiler haben muß.

Aufgabe 1.68 Ist $(p, p+2)$ ein Paar von Primzahlzwillingen, so ist $n = p(p+2)$ keine vollkommene Zahl.

Aufgabe 1.69 Sind m und n vollkommene Zahlen, dann ist auch nm vollkommen.

Wie in Lemma 1.58 gezeigt, ist $a^n - 1$ stets durch $a - 1$ teilbar. Sucht man daher für $a \neq 2$ nach Primzahlen, so kann man untersuchen, wann $p = \frac{a^n-1}{a-1}$ eine Primzahl ist. Betrachtet man diese Zahlen zur Basis $b = a$, so besitzen sie die b-adische Darstellung $(111 \ldots 111)_b$ aus n Einsen.

Definition 1.70 Es seien $n, b \in \mathbb{N}$ und $b > 1$. Unter der *repetitiven Eins* $R_b n$ versteht man die b-adische natürliche Zahl, die aus n Einsen besteht. Speziell für $b = 10$ schreibt man auch kurz Rn.

Bemerkung 1.71 a) Für $b = 2$ handelt es sich bei den repetitiven Einsen gerade um die Mersenne-Zahlen.

b) Ist $n = m \cdot k$ mit $m, k > 1$ keine Primzahl, so ist $R_b n$ wegen $R_b n = R_b m \cdot (b^{(k-1)m} + \ldots + b^{2m} + b^m + 1)$ sicherlich ebenfalls keine Primzahl.

c) Für $b = 10$ ist $R1 = 1, R2 = 11$ prim, $R3 = 111 = 3 \cdot 37$, $R4 = 1111 = 11 \cdot 101$, $R5 = 11111 = 41 \cdot 271$, $R6 = 111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$, $R7 = 1111111 = 239 \cdot 4549$, $R8 = 11111111 = 11 \cdot 73 \cdot 101 \cdot 137$, $R9 = 111111111 = 3 \cdot 3 \cdot 37 \cdot 333667$, $R10 = 1111111111 = 11 \cdot 41 \cdot 271 \cdot 9091$. Es ist bekannt, daß für Primzahlen $p \leq 10000$ nur $R2, R19, R23, R317$ und $R1031$ Primzahlen sind.

d) Repetitive Einsen für die Basen 2, 3 und 5 werden in den Aufgaben 2.48, 2.49 und 2.50 betrachtet.

Aufgabe 1.72 Analog zu den dezimalen repetitiven Einsen kann man die "fast"repetitiven Dreien $31, 331, 3331, \ldots$ (vgl. 7.1) bilden. Untersuchen Sie einige der folgenden Glieder dieser Folge, ob es sich ebenfalls um Primzahlen handelt.

Eine andere Klasse von natürlichen Zahlen, die sehr intensiv mit Faktorisierungsalgorithmen bearbeitet werden, wurde von Pierre de Fermat erstmals untersucht. Auch hier ist der Ausgangspunkt eine einfache Beobachtung.

Lemma 1.73 *Ist $m \in \mathbb{N}$ keine Zweierpotenz, dann ist $2^m + 1$ zusammengesetzt.*

Beweis: Es sei $m = v \cdot u$ mit $v \in \mathbb{N}$ und ungeradem $u > 1$. Dann ist $2^v + 1 \neq 1$ nichttrivialer Teiler von

$$2^m + 1 = 2^{v \cdot u} + 1 = (2^v + 1)(2^{v(u-1)} - 2^{v(u-2)} + - \ldots + 2^{2v} - 2^v + 1).$$

◇

Definition 1.74 Für $k \in \mathbb{N}_0$ heißt $F_k = 2^{2^k} + 1$ die k-te *Fermat-Zahl*.

Bemerkung 1.75 $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ und $F_4 = 65537$ sind die einzigen bis heute bekannten Primzahlen unter den Fermat-Zahlen. Fermat nahm irrtümlich an, daß alle Fermat-Zahlen prim sind. Die Faktorisierung von $F_5 = 4294967297 = 641 \cdot 6700417$ lag damals nämlich außerhalb seiner rechnerischen Möglichkeiten und gelang erst Leonard Euler. Allerdings wäre ihm eine Widerlegung der Eigenschaft von F_5, eine Primzahl zu sein, mit Hilfe des kleinen Fermatschen Satzes (Satz 2.54) durchaus möglich gewesen.

Der aktuelle Stand der Forschung über die Fermat-Zahlen zeigt stets schön die Möglichkeiten beim Faktorisierungsproblem für eine beliebige natürliche Zahl. Jede Fermat-Zahl fällt nämlich in genau eine der fünf Klassen (vgl. 7.13 und 7.14):

1. $n = F_k$ ist eine Primzahl.

2. $n = F_k$ ist eine zusammengesetzte Zahl mit vollständig bekannten Primfaktoren.

3. $n = F_k$ ist eine zusammengesetzte Zahl, von der man einen oder mehrere, aber noch nicht alle Primfaktoren kennt.

4. $n = F_k$ ist eine zusammengesetzte Zahl, man kennt aber noch keinen einzelnen Primfaktor.

5. Es ist unbekannt, ob $n = F_k$ zusammengesetzt ist oder eine Primzahl.

Die Fermat-Zahlen sind eng mit einem klassischen geometrischen Problem verknüpft:

Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^m \cdot p_1 \dots p_k$ gilt mit $m, k \in \mathbb{N}_0$ und paarweise verschiedenen primen Fermat-Zahlen p_i.

Aufgabe 1.76 Zeigen Sie, daß für die Fermat-Zahlen F_k, $k \in \mathbb{N}$ gilt

(37) $F_k = F_{k-1} \cdots F_2 \cdot F_1 \cdot F_0 + 2.$

Folgerung 1.77 *Für verschiedene Fermat-Zahlen F_n, F_m mit $n \neq m$ gilt $ggT(F_n, F_m) = 1$.*

Beweis: Sei $d = ggT(F_m, F_n)$ für $m < n$. Dann teilt d also F_n und F_m und daher nach Aufgabe 1.76 auch $F_n - 2$. Also gilt $d \mid 2$. Da aber alle Fermat-Zahlen ungerade sind, ist $d = 2$ ausgeschlossen. Daher bleibt nur $d = ggT(F_m, F_n) = 1$.$\diamond$

Polya merkte dazu augenzwinkernd an, daß hieraus nochmals folgt, daß es unendlich viele Primzahlen geben muß, denn jede Fermat-Zahl hat mindestens einen Primteiler und alle derartigen Primzahlen müssen paarweise verschieden sein.

Bemerkung 1.78 Ähnlich wie man die repetitiven Einsen als Verallgemeinerung der Mersenne-Zahlen auffassen kann, kann man die Zahlen der Form $F_n(b) = GF(n,b) = b^N + 1$ mit $N = 2^n$ als *verallgemeinerte Fermat-Zahlen* betrachten. Im Unterschied zu den Fermat-Zahlen ergeben sich für Basen $b \neq 2$ zahlreiche weitere Primzahlen. Man sieht leicht, daß hierzu die Basis b gerade und der Exponent N eine Zweierpotenz sein muß, vgl. Lemma 1.73. So sind etwa $F_{18}(24518) = 24518^{262144} + 1$, $F_{17}(1372930) = 1372930^{131072} + 1$ und $F_{17}(1361244) = 1361244^{131072} + 1$ verallgemeinerte Fermat-Primzahlen mit mehr als 800000 Stellen.

Ebenfalls verwandt mit den Fermat-Zahlen sind die *Cullen-Zahlen* $C_n = n \cdot 2^n + 1$, die von James Cullen (1867 - 1933) 1905 für $n = 1, \ldots, 99$ untersucht wurden. Er fand, daß hierunter nur $C_1 = 3$ eine Primzahl ist. Die nächste Primzahl in dieser Folge ist C_{141} und wurde 1958 von Raphael M. Robinson (1911 - 1995) entdeckt. Man hat bis $n = 6384000$ alle Cullen-Zahlen untersucht und nur noch für $n = 4713,\ 5795,\ 6611, 18496, 32292, 32469, 59656, 90825, 262419, 361275,\ 481899,$ 1354828 und 6328548 Primzahlen gefunden.

Die zu den Cullen-Zahlen analogen *Woodall-Zahlen*, benannt nach H. J. Woodall, der sie 1917 untersuchte, $C'_n = n \cdot 2^n - 1$ sind etwas häufiger prim, nämlich unterhalb von $n = 6640000$ für $n = 2,\ 3,\ 6,\ 30,\ 75,\ 81,\ 115,$ $123, 249, 362, 384, 462, 512, 751, 882, 5312, 7755, 9531, 12379, 15822, 18885, 22971,$ 23005, 98726, 143018, 151023, 667071, 1195203, 1268979, 2013992, 2367906 und 3752948.

Ähnlich wie die verallgemeinerten Fermat-Zahlen hat man auch verallgemeinerte Cullen-Zahlen $n \cdot b^n + 1$ und verallgemeinerte Woodall-Zahlen $n \cdot b^n - 1$ für Basen $b \neq 2$ untersucht.

Bei der Suche nach allgemeinen Formeln, die stets Primzahlen liefern, wurde auch die kuriose Formel $p(n) = n^2 - 79n + 1601$ gefunden, die für $n = 0, \ldots, 79$ stets Primzahlen liefert, aber für $n = 80$ dann $p(80) = 1681 = 41^2$. Daß man auf diese einfache Weise auch keinen Erfolg haben kann, zeigt der folgende Satz.

Satz 1.79 *Es existiert kein Polynom $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ vom Grad $n \geq 1$, so daß $f(m) \in \mathbb{P}$ für alle $m \in \mathbb{N}_0$ gilt.*

Beweis: Sei $f(x)$ ein derartiges Polynom. Dann ist jedenfalls $f(0) = a_0 = p$ eine Primzahl. Für jedes $m \in \mathbb{N}$ folgt daraus $f(mp) = a_n(mp)^n + \ldots + a_1(mp) + p = g(m) \cdot p + p = (g(m) + 1)p$ für $g(x) = \sum_{i=1}^{n} a_i p^{i-1} x^i$. Damit $f(mp)$ eine Primzahl ist, muß also $g(m) = 0$ für alle $m \in \mathbb{N}$ gelten. Dann ist aber $g(x)$ das Nullpolynom und nicht wie $f(x)$ vom Grad $n \geq 1$. ◇

Bemerkung 1.80 Von W. H. Mills konnte 1947 aber folgende Aussage gezeigt werden:

Es gibt ein $\alpha > 1$ in $\mathbb{R}$, so daß die Funktion $f : \mathbb{N} \to \mathbb{Z}$ mit $f(n) = [\alpha^{3^n}]$ für alle $n \in \mathbb{N}$ nur Primzahlwerte annimmt.

Allerdings ist kein Verfahren zur Bestimmung von α bekannt!

Ein nur mit umfangreichen ([6], S. 58–90) analytischen Hilfsmitteln zu beweisendes Resultat in ähnlicher Richtung ist von J. P. G. L. Dirichlet (1805 - 1859) gezeigt worden:

Sind a und b teilerfremde natürliche Zahlen, so gibt es stets unendlich viele Primzahlen der Form $a \cdot n + b$ mit $n \in \mathbb{N}_0$.

Dagegen weiß man nicht, ob das quadratische Polynom $f(n) = n^2 + 1$ unendlich viele Primzahlen liefert oder nicht.

Aufgabe 1.81 Zeigen Sie: Sind a und b nicht teilerfremd, so gibt es höchstens eine Primzahl der Form $a \cdot n + b$.

Aufgabe 1.82 Zeigen Sie durch eine geeignete Modifikation des Beweises von Euklid:

Es gibt uendlich viele Primzahlen der Form $p = 6n - 1$.

Gilt der Beweis auch für Primzahlen der Form $p = 4n - 1$?

1.6 Verteilung der Primzahlen und der Primzahlsatz

Die Unregelmäßigkeit des Wachstums der monotonen und stückweise konstanten Primzahlverteilungsfunktion $\pi(x)$ wird durch die beiden folgenden Aussagen näher beleuchtet.

Lemma 1.83 *Es gibt beliebig große Lücken zwischen zwei aufeinander folgenden Primzahlen, d. h. es gibt beliebig große Intervalle, auf denen $\pi(x)$ konstant ist.*

Beweis: Für $n > 1$ sind die aufeinander folgenden natürlichen Zahlen

$$n! + 2, n! + 3, \ldots, n! + n$$

nacheinander teilbar durch $2, 3, \ldots, n$, also keine Primzahlen. ◇

Bemerkung 1.84 Tatsächlich findet man große Lücken aber nicht erst bei derartig großen Zahlen. So gibt es etwa zwischen 1327 und 1361, zwischen 8467 und 8501, zwischen 9551 und 9587 keine Primzahlen.

Lemma 1.85 *Für $n > 2$ liegt zwischen n und $n!$ stets eine Primzahl.*

Beweis: Jede Primzahl $p \leq n$ teilt $n!$ und daher nicht $n! - 1$, da sie sonst auch $n! - (n! - 1) = 1$ teilen müßte. Der kleinste, nach Lemma 1.30 existierende Primteiler p von $n! - 1$ erfüllt daher $n < p \leq n! - 1 < n!$. ◇

Bemerkung 1.86 Pafnuti Lwowitsch Tschebyscheff (1821 - 1894) konnte sogar zeigen, daß zwischen n und $2n - 2$ für $n > 1$ stets eine Primzahl liegt.

Die Aussage "zwischen n und $2n$ liegt stets eine Primzahl" war 1845 von J. Bertrand (1822 - 1900) für $n \leq 6000000$ überprüft worden und hieß danach auch *Bertrandsches Postulat*.

Eine noch offene Frage ist, ob es zwischen n^2 und $(n+1)^2$ ebenfalls immer eine Primzahl gibt.

Bemerkung 1.87 Da von zwei aufeinander folgenden natürlichen Zahlen genau eine Zahl gerade ist und die andere ungerade, kann es außer im Fall $p = 2$ und $p + 1 = 3$ keine weiteren unmittelbar benachbarten Primzahlen geben. Sind aber p und $p + 2$ (ungerade) Primzahlen, so spricht man von *Primzahlzwillingen*. Hier springt $\pi(x)$ innerhalb eines Intervalls der Länge 2 zweimal um 1. Mit $\pi_2(x)$ wird die Anzahl aller Primzahlzwillinge $(p, p + 2)$ mit $p + 2 \leq x$ bezeichnet (vgl. 7.1).

Es besteht die durch viele Indizien gestützte, aber bisher noch unbewiesene

Vermutung: Es gibt unendlich viele Primzahlzwillinge.

Man vermutet sogar, daß gilt

$$\pi_2(x) \sim \frac{x}{\log^2(x)} \cdot 2 \prod_{p \in \mathbb{P}, p > 2} \left(1 - \frac{1}{(p-1)^2}\right).$$

Aufgabe 1.88 Zeigen Sie, daß das unendliche Produkt

$$\prod_{p \in \mathbb{P}, p > 2} \left(1 - \frac{1}{(p-1)^2}\right)$$

konvergiert.

Wegen dieser Unregelmäßigkeiten ist man an einer möglichst guten Approximation von $\pi(x)$ durch "einfachere" Funktionen $f(x)$ interessiert. Als Anregung für solche Funktionen diene die folgende Tabelle, deren drei letzten Spalten zur Übung ausgefüllt werden sollten. Es ist $li(x)$ der *Integrallogarithmus* definiert durch

$$li(x) = \int_2^x \frac{dt}{\log(t)}.$$

Hier und im folgenden bedeutet log wie in der Zahlentheorie üblich, den natürlichen Logarithmus zur Basis e.

x	$\pi(x)$	$li(x)$	$\frac{x}{log(x)}$	$\pi(x) \cdot \frac{\log(x)}{x}$	$\pi(x)/li(x)$
10^3	168	178			
10^4	1229	1246			
10^5	9592	9630			
10^6	78498	78628			
10^7	664579	664918			

Diese numerischen Ergebnisse legen den folgenden Satz nahe, der sich (allerdings mit erheblichem analytischem Aufwand) auch beweisen läßt.

Satz 1.89 Primzahlsatz

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1.$$

Unter einer Abschätzung des *Restgliedes* im Primzahlsatz versteht man dann die Angabe der Größenordnung der Differenz $\pi(x) - f(x)$ mit Hilfe der O-Notation.

Definition 1.90 Es seien $f, g : \mathbb{R}^+ \to \mathbb{C}$ beliebige Funktionen. Existieren dann $x_0, c \in \mathbb{R}^+$ mit

$$|f(x)| \leq c \cdot g(x)$$

für alle $x \geq x_0$, so schreibt man $f(x) = O(g(x))$.

Bemerkung 1.91 Bereits Gauss vermutete den Primzahlsatz in der Form

$$\lim_{x\to\infty} \frac{\pi(x)}{li(x)} = 1.$$

Wegen

$$li(x) = \frac{x}{\log(x)} + O\left(\frac{x}{\log^2(x)}\right)$$

sind beide Versionen gleichwertig, allerdings gestattet $li(x)$ die bessere Restgliedabschätzung.

Der erste Beweis des Primzahlsatzes erfolgte 1896 durch Jacques-Salomon Hadamard (1865 - 1963) und Charles Jean de la Vallée-Poussin (1866 - 1962) unabhängig voneinander. Sie benutzten dabei die von Bernhard Riemann (1826 - 1866) eingeführte *Riemannsche Zetafunktion*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \ s \in \mathbb{C}.$$

Die bis heute unbewiesene, von Riemann 1859 formulierte *Riemannsche Vermutung* besteht in der Aussage, daß sämtliche Nullstellen der Zetafunktion innerhalb des Streifens $0 < Re(s) < 1$ auf der *kritischen Geraden* $Re(s) = \frac{1}{2}$ liegen.

Aus der Riemannschen Vermutung würde u. a. eine drastische Verschärfung für die Abschätzung des Restgliedes im Primzahlsatz folgen:

$$\pi(x) = li(x) + O(\sqrt{x}\log(x)).$$

Die beste bis heute bewiesene Version des Primzahlsatzes liefert dagegen:

$$\pi(x) = li(x) + O\left(x \cdot exp\left(-c\log^{3/5}(x) \cdot log(log(x))^{-1/5}\right)\right)$$

für eine geeignete Konstante $c > 0$.

Bereits 1852 konnte Tschebyscheff elementar zeigen, daß $\pi(x)$ und $\frac{x}{\log(x)}$ jedenfalls in derselben Größenordnung liegen. Er zeigte allerdings ein besseres Ergebnis als im folgenden Satz, nämlich

$$0.89\frac{n}{\log(n)} \leq \pi(n) \leq 1.11\frac{n}{\log(n)}$$

für hinreichend große n.

Satz 1.92 (Satz von Tschebyscheff) *Für alle natürlichen Zahlen $n \geq 4$ gilt*

$$\frac{1}{4}\frac{n}{\log(n)} \leq \pi(n) \leq 6\frac{n}{\log(n)}.$$

Beweis: Die linke Ungleichung in

$$(38) \quad 2^n < \binom{2n}{n} = \frac{(2n)!}{(n!)^2} < 4^n$$

folgt aus Aufgabe 1.16, die rechte aus dem binomischen Satz (vgl. Aufgabe 1.17). Durch Logarithmieren erhält man hieraus (die Logarithmusfunktion ist streng monoton wachsend!)

$$n\log(2) < \log((2n)!) - 2\log(n!) < 2n\log(2). \tag{39}$$

Sei nun

$$n! = \prod_{p\le n} p^{v_p(n!)}$$

die Primfaktorzerlegung von $n!$, also nach Logarithmieren

$$\log(n!) = \sum_{p\le n} v_p(n!)\log(p).$$

Nach Aufgabe 1.29 gilt

$$v_p(n!) = \sum_{m\ge 1}\left[\frac{n}{p^m}\right], \tag{40}$$

wobei die Summe für jedes $p\in\mathbb{P}$ nur von 1 bis $\left[\frac{\log(n)}{\log(p)}\right]$ läuft. Hieraus folgt

$$\log((2n)!) - 2\log(n!) = \sum_{p\le 2n}\sum_{m=1}^{\left[\frac{\log(2n)}{\log(p)}\right]}\left(\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right]\right)\log(p). \tag{41}$$

Wegen $[2x]-2[x]=0$, falls $x-[x]<\frac{1}{2}$, und $[2x]-2[x]=1$, falls $x-[x]\ge\frac{1}{2}$, kann man die innere Summe durch die Anzahl ihrer Glieder nach oben abschätzen und erhält:

$$n\log(2) < \sum_{p\le 2n}\left[\frac{\log(2n)}{\log(p)}\right]\log(p) \le \pi(2n)\log(2n). \tag{42}$$

Hieraus folgt wegen $\frac{1}{2} < \log(2)$

$$\frac{1}{4}\frac{2n}{\log(2n)} < \frac{n\log(2)}{\log(2n)} < \pi(2n),$$

also die linke Ungleichung des Satzes für gerade natürliche Zahlen. Wegen $\frac{n\log(2)}{2n+1} > \frac{1}{4}$ für $n\ge 2$ folgt aber auch für ungerade natürliche Zahlen

$$\frac{1}{4}\frac{2n+1}{\log(2n+1)} < \frac{1}{4}\frac{2n+1}{\log(2n)} < \frac{n\log(2)}{\log(2n)} < \pi(2n) \le \pi(2n+1).$$

Die rechte Ungleichung erhält man über eine Abschätzung der Funktion

$$\theta(x) = \sum_{p\in\mathbb{P},\ p\le x} \log(p).$$

Da für alle Primzahlen $n < p < 2n$ gilt $[\frac{2n}{p}] - 2[\frac{n}{p}] = 1 - 0 = 1$, erhält man aus (41)

$$\theta(2n) - \theta(n) = \sum_{n<p<2n} \log(p) \le \log((2n)!) - 2\log(n!) < 2n\log(2).$$

Hieraus ergibt sich für Zweierpotenzen

$$\theta(2^{k+1}) - \theta(2^k) < 2^{k+1}\log(2).$$

Mit $\theta(1) = 0$ folgt dann durch Summation über k

$$\theta(2^{k+1}) < 2^{k+2}\log(2).$$

Betrachte nun natürliche Zahlen zwischen zwei Zweierpotenzen, also $2^k \le n < 2^{k+1}$, und ein beliebiges $y < n$. Dann gilt

$$\begin{aligned}(\pi(n) - \pi(y))\log(y) &= \sum_{y<p\le n} \log(y)\\ &\le \sum_{y<p\le n} \log(p)\\ &\le \theta(n) \le \theta(2^{k+1}) \le 2^{k+2}\log(2) \le 4n\log(2).\end{aligned}$$

Wählt man $y = n^{2/3}$, also $\log(y) = \frac{2}{3}\log(n)$, so erhält man wegen $\pi(y) \le y = n^{2/3}$ die Abschätzung

$$\pi(n) \le n^{2/3} + \frac{3}{2}\frac{4n\log(2)}{\log(n)} = \frac{n}{\log(n)}\left(\frac{\log(n)}{n^{1/3}} + 6\log(2)\right).$$

Da nun die Funktion $f(x) = \frac{\log(x)}{x^{1/3}}$ bei $x = e^3$ ihr Maximum annimmt, gilt

$$\frac{\log(n)}{n^{1/3}} + 6\log(2) < \frac{3}{e} + 6\log(2) < 6$$

und damit auch die rechte Ungleichung des Satzes. ◇

Für das oben schon erwähnte RSA-Verfahren benutzt man zufällig gewählte Primzahlen p und q mit üblicherweise 100 Dezimalstellen. Man mache sich anhand des Satzes von Tschebyscheff klar, daß es "hinreichend viele" verschiedene Primzahlen dieser Art gibt.

2 Ganze Zahlen und der euklidische Algorithmus

2.1 Die ganzen Zahlen

Obwohl wir das Rechnen im Ring der ganzen Zahlen $(\mathbb{Z}, +, \cdot)$ als bekannt voraussetzen wollen, sei hier noch einmal kurz die Konstruktion dieses Ringes aus dem Halbring $(\mathbb{N}_0, +, \cdot)$ der natürlichen Zahlen angegeben. Für Paare $(a, b), (c, d) \in Z = \mathbb{N}_0 \times \mathbb{N}_0$ werde die Relation $\sim$ definiert durch

$$(43) \quad (a, b) \sim (c, d) \Longleftrightarrow a + d = b + c.$$

Aufgabe 2.1 Zeigen Sie, daß $\sim$ eine Äquivalenzrelation auf Z ist, die außerdem

$$(44) \quad (a, b) \sim (c, d) \Longrightarrow (a + x, b + y) \sim (c + x, d + y)$$

für alle $(a, b), (c, d), (x, y) \in Z$ erfüllt.

Auf der Menge $\mathbb{Z} = Z/_\sim = \{[a, b] \mid (a, b) \in Z\}$ aller Äquivalenzklassen $[a, b] = \{(c, d) \in Z \mid (a, b) \sim (c, d)\}$ werden eine Addition gemäß

$$(45) \quad [a, b] + [c, d] = [a + c, b + d]$$

und eine Multiplikation gemäß

$$(46) \quad [a, b] \cdot [c, d] = [a \cdot c + b \cdot d, a \cdot d + b \cdot c]$$

erklärt.

Aufgabe 2.2 Zeigen Sie, daß $(\mathbb{Z}, +, \cdot)$ ein kommutativer und nullteilerfreier Ring mit Einselement $[1, 0]$ ist. Das Nullelement ist $[0, 0]$, das additiv Inverse zu $[a, b]$ ist $[b, a]$.

Daher gilt $[a, b] = [a, 0] + [0, b] = [a, 0] - [b, 0]$ für alle $[a, b] \in \mathbb{Z}$. Identifiziert man nun $[a, 0] \in \mathbb{Z}$ mit $a \in \mathbb{N}_0$, so gelangt man zu der üblichen (dezimalen) Notation der ganzen Zahlen $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$.

Auch die Ordnungsrelation $\leq$ kann von $\mathbb{N}_0$ auf $\mathbb{Z}$ fortgesetzt werden durch

(47) $a \leq b \Longleftrightarrow a + n = b$ für ein $n \in \mathbb{N}_0$.

Aufgabe 2.3 Zeigen Sie, daß $\leq$ eine lineare Ordnungsrelation auf $\mathbb{Z}$ ist, für die die Addition monoton ist. Bezüglich der Multiplikation gilt $a \leq b \Longrightarrow a \cdot c \leq b \cdot c$, falls $0 \leq c$.

Schließlich definiert man noch den *Betrag* einer ganzen Zahl a durch $|a| = a$, falls $0 \leq a$, und $|a| = -a$, sonst.

2.2 Der Euklidische Algorithmus

In diesem Kapitel soll hauptsächlich die Teilbarkeitsrelation auf dem Ring $\mathbb{Z}$ der ganzen Zahlen untersucht werden. Sie wird vollkommen analog zu der Teilbarkeit für natürliche Zahlen (vgl. Definition 1.22) erklärt und setzt diese offensichtlich fort. Sie hat aber etwas andere Eigenschaften, wie das folgende Lemma zeigt.

Definition 2.4 Für Elemente $a, b \in \mathbb{Z}$ wird die *Teilbarkeit* $|$ definiert durch

(48) $a \mid b \Longleftrightarrow a \cdot x = b$ für ein $x \in \mathbb{Z}$.

Gilt $a \mid b$ und $b \mid a$, so heißen a und b *assoziiert* zueinander.

Lemma 2.5 *a) Die Teilbarkeitsrelation $|$ ist reflexiv und transitiv auf $\mathbb{Z}$. Sind a und b aus $\mathbb{Z}$ assoziiert zueinander, so gilt $a = \pm b$.*

b) $a \mid b \Longleftrightarrow -a \mid b \Longleftrightarrow a \mid -b$ für alle $a, b \in \mathbb{Z}$.

c) $a \mid 0$ und $1 \mid a$ für alle $a \in \mathbb{Z}$.

d) $d \mid a$ und $d \mid b \Longrightarrow d \mid (xa + yb)$ für alle $d, a, b, x, y \in \mathbb{Z}$.

e) Aus $d \mid a$ und $a \neq 0$ folgt $\mid d \mid \leq \mid a \mid$. Jede von 0 verschiedene ganze Zahl hat also nur endlich viele verschiedene Teiler.

Beweis: Analog zum Beweis von Lemma 1.23. $\diamond$

Definition 2.6 Es sei A eine nichtleere Teilmenge von $\mathbb{Z}$. Eine ganze Zahl d heißt ein *größter gemeinsamer Teiler von* A, geschrieben: $d = ggT(A)$, wenn die beiden folgenden Bedingungen erfüllt sind.

(ggT1) d ist gemeinsamer Teiler von allen $a \in A$, d. h. $d \mid a$ für alle $a \in A$.

(ggT2) Ist t gemeinsamer Teiler von allen $a \in A$, so gilt $t \mid d$.

Bemerkung 2.7 a) Stets sind 1 und -1 gemeinsame Teiler von A.

b) Für $A = \{0\}$ ist 0 gemeinsamer Teiler von A, woraus sich mit (ggT2) dann auch $0 = ggT(0)$ ergibt.

c) Existiert ein $a \neq 0$ in A, so ist 0 niemals gemeinsamer Teiler von A. Der $ggT(A)$ ist dann unter den endlich vielen Teilern von a zu suchen.

d) Gilt $d = ggT(A)$, so ist jeder andere größte gemeinsame Teiler von A assoziiert zu d, der $ggT(A)$ ist also nur bis auf das Vorzeichen eindeutig bestimmt.

Satz 2.8 (Division mit Rest) *Zu $a, b \in \mathbb{Z}$, $b \neq 0$ existieren eindeutig bestimmte ganze Zahlen q und r mit $0 \leq r < |b|$ und $a = qb + r$.*

Beweis: Wegen $b \neq 0$ ist $0 < |b|$ und die ganzen Zahlen lassen sich in disjunkte nach rechts halboffene Intervalle der Länge $|b|$ zerlegen. In genau einem dieser Intervalle liegt a. Es gibt also eine eindeutig bestimmte ganze Zahl q mit $a \in [qb, qb + |b|)$. Dann gilt für $r = a - qb$ aber $0 \leq r < |b|$. ◇

Der folgende Satz sichert nicht nur die Existenz des $ggT(A)$ für jede nichtleere endliche Teilmenge A von $\mathbb{Z}$, er erlaubt auch eine explizite Berechnung. Er wurde, für natürliche Zahlen $a, b \neq 0$, bereits von Euklid in seinen "Elementen" bewiesen.

Satz 2.9 (Euklidischer Algorithmus) *Es seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Führt man iteriert Divisionen mit Rest gemäß dem folgenden Schema aus, so bricht das Verfahren nach endlich vielen Schritten ab, weil die letzte Division aufgeht. Der letzte Rest $r_n \neq 0$ ist der größte gemeinsame Teiler von a und b.*

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\dots \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

Beweis: Für die Divisionsreste gilt $|b| > r_1 > r_2 > \ldots > r_n \geq 0$, das Verfahren muß also nach spätestens $|b|$ Schritten abbrechen. Aus der letzten Gleichung liest man $r_n \mid r_{n-1}$ (und wegen $r_n < r_{n-1}$ auch $q_{n+1} > 1$) ab, dann aus der vorletzten Gleichung $r_n \mid r_{n-2}$ usw. Aus der zweiten Gleichung ergibt sich schließlich $r_n \mid b$ und aus der ersten $r_n \mid a$. Also ist r_n gemeinsamer Teiler von a und b.

Löst man die ersten n Gleichungen nach den jeweiligen Divisionsresten auf, so erhält man

$$\begin{aligned} r_1 &= a - q_1 b \\ r_2 &= b - q_2 r_1 \\ r_3 &= r_1 - q_3 r_2 \\ &\ldots \\ r_n &= r_{n-2} - q_n r_{n-1} \end{aligned}$$

Ist nun t ein gemeinsamer Teiler von a und b, so folgt aus der ersten Gleichung $t \mid r_1$, dann aus der zweiten $t \mid r_2$ usw. Aus der letzten Gleichung erhält man schließlich $t \mid r_n$. Dies zeigt $r_n = ggT(a, b)$.

Weiterhin liest man aus der ersten Gleichung ab, daß $x_1, y_1 \in \mathbb{Z}$ existieren mit $r_1 = x_1 a + y_1 b$. Setzt man dies in die zweite Gleichung ein, so erhält man $x_2, y_2 \in \mathbb{Z}$ mit $r_2 = x_2 a + y_2 b$. So fortfahrend gelangt man schließlich zu $x, y \in \mathbb{Z}$ mit $r_n = xa + yb$. Damit ist auch die nächste Folgerung bewiesen, die auch als Lemma von Bezout bekannt ist (Etienne Bezout, 1730 - 1783). ◇

Folgerung 2.10 *Für $a, b \in \mathbb{Z}$ mit $d = ggT(a, b)$ existieren $x, y \in \mathbb{Z}$ mit $d = xa + yb$. Diese können mit dem Euklidischen Algorithmus bestimmt werden.*

Aufgabe 2.11 Zeigen Sie, daß für die Divisionsreste im Euklidischen Algorithmus gilt $r_{k+2} < \frac{1}{2} r_k$ für $k = 1, \ldots, n-2$. Es gibt daher höchstens $2 \cdot \log_2(a)$ Divisionen.

Aufgabe 2.12 Bestimmen Sie ggT$(14345, 16289)$ und ggT$(142241, 153049)$.

Die folgende Realisierung des Euklidischen Algorithmus benötigt nur 10 Speicherplätze.

Algorithmus 2.13 Euklidischer Algorithmus

Eingabe: ganze Zahlen a, b

Ausgabe: $d = ggT(a, b), x, y \in \mathbb{Z}$ mit $d = xa + yb$

```
z:= a; z1:=b; x:=1; x1:=0; y:=0; y1:=1;
while z1 ungleich 0 do
   w:= [z/z1]; z2:= z-w*z1;
   x2 := x - w*x1; y2 := y - w*y1;
   z := z1; z1:=z2; x:=x1; x1:=x2; y:= y1; y1:= y2;
od
d:=z;
d,x,y, stop
```

Satz 2.14 (G. Lamé, 1845) *Es seien $n, a, b \in \mathbb{N}$ und $n > 3$.*

a) Für $a = \phi_n$ und $b = \phi_{n-1}$ benötigt der Euklidische Algorithmus genau $n-2$ Divisionen mit Rest.

b) Gilt $b < a < \phi_n$, so benötigt der Euklidische Algorithmus weniger als $n-2$ Divisionen mit Rest.

Beweis: Wegen $\phi_k = \phi_{k-1} + \phi_{k-2}$ für $k = n, n-1, \ldots, 4$ sind dies genau die Divisionen mit Rest, die im Euklidischen Algorithmus für $a = \phi_n$ und $b = \phi_{n-1}$ durchgeführt werden. Es ist jeweils $q = 1$ und $r = \phi_{k-2} < \phi_{k-1}$ eindeutig bestimmt. Dies sind also $n-3$ Divisionen. Mit $\phi_3 = 2\phi_2$ terminiert dann der Euklidische Algorithmus nach genau $n-2$ Divisionen mit Rest.

b) Betrachte $b < a$ aus $\mathbb{N}$, so daß der Euklidische Algorithmus $m \geq n-2$ Divisionen mit Rest benötigt. Dann ist $a \geq \phi_n$ zu zeigen. Seien $a_0 = a$, $a_1 = b$ und $a_i = q_{i+1}a_{i+1} + a_{i+2}$ für $i = 0, 1, \ldots, m-1$ die dabei berechneten Divisionen. Es ist insbesondere $a_{m+1} = 0 < a_m < a_{m-1} < \ldots < a_1 = b$, also $q_{i+1} \geq 1$ für alle i und $q_m > 1$, da sonst wegen $a_{m-1} = a_m$ die Division bereits mit $a_{m-2} = q_{m-1}a_{m-1} + a_m = (q_{m-1}+1)a_{m-1}$ nach $m-1$ Schritten beendet gewesen wäre. Im Fall $m > n-2$ gilt $a_{n-2} > a_m \geq 1 = \phi_2$ und wegen $a_{n-1} \geq a_m \geq 1$ folgt auch $a_{n-3} = q_{n-2}a_{n-2} + a_{n-1} \geq 1 + 1 = \phi_3$. Im Fall $m = n-2$, also $m+1 = n-1$ gilt auch noch $a_{n-2} = a_m \geq 1 = \phi_2$ und mit $q_m = q_{n-2} \geq 2$ folgt ebenfalls $a_{n-3} = q_{n-2}a_{n-2} + a_{n-1} \geq 2 = \phi_3$. Sei $i \in \{2, \ldots, n-1\}$ und $a_{n-j} \geq \phi_j$ für $j = 2, \ldots, i$ bereits gezeigt. Dann folgt $a_{n-i-1} = q_{n-i}a_{n-i} + a_{n-i+1} \geq \phi_i + \phi_{i-1} = \phi_{i+1}$. Insgesamt folgt damit $a = a_0 \geq \phi_n$. $\diamond$

Aufgabe 2.15 Es sei $b > 1$ eine natürliche Zahl. Zeigen Sie, daß für jede natürliche Zahl $a > 0$ ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte Zahlen $a_i \in \{0, \ldots, b-1\}$ für $i = 0, \ldots, n$ und $a_n \neq 0$ existieren, so daß

$$a = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0 \tag{49}$$

gilt. Man nennt $(a_n a_{n-1} \dots a_1 a_0)_b$ auch die *Darstellung von a zur Basis b* und läßt die Klammern sowie den Index b oft fort. Speziell für $b = 10$ ergibt sich die *Dezimaldarstellung* und für $b = 2$ die *Binärdarstellung*.

Schreibt man in (49) auch die Exponenten $n, n-1, \dots$ in der Form (49) und dann weiter auch die darin vorkommenden Exponenten usw., so gelangt man schließlich zur *iterierten Darstellung von a zur Basis b*.

Definition 2.16 Es sei $b > 1$ eine natürliche Zahl. Die Funktion $a_b : \mathbb{N} \to \mathbb{N}$ werde wie folgt erklärt. $a_b(n)$ entstehe aus der iterierten Darstellung von n zur Basis b dadurch, daß in dieser Darstellung überall b durch $b + 1$ ersetzt wird. Insbesondere ist $a_b(n) = n$ für alle $n < b$.

Die *Goodstein-Folge $g_b(n)$ zum Keim n* (Reuben Goodstein, 1912 - 1985) ist rekursiv definiert durch $g_1(n) = n$ und $g_b(n) = a_b(g_{b-1}(n)) - 1$ für $b > 1$.

Beispiel 2.17 Die Zahl $n = 42$ besitzt die Binärdarstellung $42 = 2^5 + 2^3 + 2$ und wegen $5 = 2^2 + 1$ und $3 = 2 + 1$ daher die iterierte Binärdarstellung $42 = 2^{2^2+1} + 2^{2+1} + 2$. Daher ist $a_2(42) = 3^{3^3+1} + 3^{3+1} + 3$ und somit $g_2(42) = 3^{3^3+1} + 3^{3+1} + 3 - 1 = 3^{28} + 3^4 + 2$. Dies ist eine Zahl mit 14 Dezimalstellen. Hieraus ergibt sich $g_3(42) = 4^{4^4+1} + 4^{4+1} + 2 - 1$, eine Zahl mit 155 Dezimalstellen. Das Folgeglied $g_4(42) = 5^{5^5+1} + 5^{5+1} + 1 - 1 = 5^{3126} + 5^6$ hat bereits 2185 Dezimalstellen.

Aufgabe 2.18 Berechnen Sie die Goodstein-Folgen zum Keim $n = 2$ und $n = 3$. Stellen Sie eine Vermutung auf.

2.3 Die Restklassenringe

Definition 2.19 Für $m \in \mathbb{N}_0$ werde die *Kongruenz modulo m* definiert durch

$$a \equiv b \bmod m \iff m \mid (a - b). \tag{50}$$

Aufgabe 2.20 Zeigen Sie, daß die Kongruenz modulo m stets eine Kongruenzrelation auf dem Ring $(\mathbb{Z}, +, \cdot)$ ist.

Für $m \neq 0$ sind zwei ganze Zahlen a und b genau dann kongruent modulo m, wenn sie bei Division durch m denselben Rest liefern.

Aufgabe 2.21 Für die natürlichen Zahlen $a, b \in \mathbb{N}$ mit $a > 1$ gelte $a \mid b$. Dann gilt auch die Äquivalenz

$$(a-1) \mid (b-1) \Longleftrightarrow (a-1) \mid (\frac{b}{a} - 1).$$

Lemma 2.22 *Es sei $m \in \mathbb{N}_0$. Auf der Menge $\mathbb{Z}/m\mathbb{Z} = \{[a]_m \mid a \in \mathbb{Z}\}$ der Restklassen $[a]_m = \{b \in \mathbb{Z} \mid a \equiv b \bmod m\}$ werde eine Addition gemäß*

(51) $[a]_m + [b]_m = [a+b]_m$

und eine Multiplikation gemäß

(52) $[a]_m \cdot [b]_m = [a \cdot b]_m$

definiert. Dann ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit dem Nullelement $[0]_m$ und Einselement $[1]_m$.

Beweis: Aus Aufgabe 2.20 folgt, daß die Addition und die Multiplikation unabhängig von der Wahl der Repräsentanten der Restklassen sind. Dann übertragen sich alle behaupteten Eigenschaften von dem Ring $(\mathbb{Z}, +, \cdot)$ auf den Ring $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$. ◇

Bemerkung 2.23 Für $m = 1$ und jedes $a \in \mathbb{Z}$ gilt $[a]_1 = \mathbb{Z}$, d. h. $(\mathbb{Z}/1\mathbb{Z}, +, \cdot)$ ist der *Nullring*, der nur aus einem Element besteht. Alle anderen Restklassenringe sind mindestens zweielementig und in ihnen gilt $[0]_m \neq [1]_m$.

Für $m = 0$ folgt wegen der Nullteilerfreiheit von $(\mathbb{Z}, +, \cdot)$ bereits $[a]_0 = \{a\}$ für alle $a \in \mathbb{Z}$, d. h. der Ring $(\mathbb{Z}/0\mathbb{Z}, +, \cdot)$ ist isomorph zu $(\mathbb{Z}, +, \cdot)$.

Für alle $m > 1$ ist $\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$ und man nennt $0, 1, \ldots, m-1$ das *kleinste nichtnegative Restsystem modulo m*. Dagegen spricht man bei $-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{m-3}{2}, \frac{m-1}{2}$ bei ungeradem m bzw. $-\frac{m-2}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{m-2}{2}, \frac{m}{2}$ bei geradem m vom *absolut kleinsten Restsystem*.

Definition 2.24 Es sei $m \in \mathbb{N}$. Die Gruppe der Einheiten in dem Monoid $(\mathbb{Z}/m\mathbb{Z}, \cdot, [1]_m)$ heißt die Gruppe der *primen Restklassen* oder kurz die *prime Restklassengruppe* modulo m. Sie wird mit $(\mathbb{Z}/m\mathbb{Z})^*$ bezeichnet und $\varphi(m)$ sei die Anzahl ihrer Elemente. Dann heißt $\varphi : \mathbb{N} \to \mathbb{N}$ die *Eulersche φ-Funktion*.

Satz 2.25 *Es sei $m \in \mathbb{N}$. Für $a \in \mathbb{Z}$ liegt $[a]_m$ genau dann in $(\mathbb{Z}/m\mathbb{Z})^*$, wenn $ggT(a,m) = 1$ gilt.*

Beweis: Gilt $ggT(a,m) = 1$, so existieren $x, y \in \mathbb{Z}$ mit $xa + ym = 1$, woraus sofort $[x]_m[a]_m = [1]_m$, also die Invertierbarkeit von $[a]_m$ folgt. Umgekehrt folgt aus $[xa]_m = [x]_m[a]_m = [1]_m$ sofort $m \mid (xa - 1)$, also $xa - 1 = ym$ für ein $y \in \mathbb{Z}$. Also gilt $xa - ym = 1$ und jeder gemeinsame Teiler von a und m muß 1 teilen, d. h. a und m sind relativ prim. ◇

Folgerung 2.26 *a) Für $n > 1$ ist $\varphi(n)$ die Anzahl der zu n teilerfremden Zahlen k mit $1 \leq k < n$. Insbesondere gilt $\varphi(p) = p - 1$ für $p \in \mathbb{P}$.*

b) Genau dann gilt $(\mathbb{Z}/m\mathbb{Z})^* = \mathbb{Z}/m\mathbb{Z} \setminus \{[0]_m\}$ und damit ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ dann ein endlicher Körper $\mathbb{F}_m$, wenn m eine Primzahl ist.

Beweis: a) Klar.

b) m ist genau dann eine Primzahl, wenn jede natürliche Zahl $1 \leq k < m$ teilerfremd zu m ist, wenn also jede von $[0]_m$ verschiedene Restklasse invertierbar ist. ◇

Folgerung 2.27 *Für $a, n \in \mathbb{N}, a > 1$ ist a im Restklassenring $R = \mathbb{Z}/(a^n - 1)\mathbb{Z}$ invertierbar und hat in der primen Restklassengruppe $R^* = (\mathbb{Z}/(a^n - 1)\mathbb{Z})^*$ die Ordnung n. Weierhin gilt für alle $m \in \mathbb{N}$ dann $n \mid m \iff a^n - 1 \mid a^m - 1$.*

Beweis: Wegen $a^n - 1 = 0$ im Restklassenring R gilt $a^n = 1$, d. h. a liegt in der Gruppe R^*. Weiterhin würde $a^k = 1$ für ein $k \leq n$ zu $a^k - 1 = 0$ und daher zu $a^n - 1 \mid a^k - 1$ führen, was wegen $a > 1$ nur für $k = n$ möglich ist. Daher ist n die Ordnung von a in R^*.

Aus $a^n - 1 \mid a^m - 1$ folgt aber $a^m = 1$ in R^* und daher $n \mid m$. Die Umkehrung wurde schon in Lemma 1.58 gezeigt. ◇

Aufgabe 2.28 Zeigen Sie, daß für jede Primzahl p und $k = 1, \ldots, p-1$ gilt

$$\binom{p}{k} \equiv 0 \bmod p.$$

Hieraus folgt dann weiter für alle $a, b \in \mathbb{Z}/p\mathbb{Z}$

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

Folgerung 2.29 (Satz von Wilson, 1741 - 1793) *Die natürliche Zahl $n > 1$ ist genau dann prim, wenn $(n-1)! \equiv -1 \bmod n$ gilt.*

Beweis: Der Satz gilt für $1 < n < 5$, wie man leicht nachprüft. Sei also $n \geq 5$ und n prim, also insbesondere ungerade. Die $n-3$ Elemente $2 \leq a \leq n-2$ des Körpers $\mathbb{F}_n$ können dann in Paaren (a, a^{-1}) mit $a \neq a^{-1}$ zusammengefaßt werden, denn $a = a^{-1} \iff a^2 = 1 \iff a^2 - 1 = 0$ ist in dem Körper $\mathbb{F}_n$ nur für $a = 1$ und $a = -1 = n-1$ möglich. Es folgt $(n-2)! = \prod_{k=2}^{n-2} k \equiv 1 \bmod n$, woraus $(n-1)! \equiv n-1 \equiv -1 \bmod n$ folgt.

Ist $n = ab$ mit $1 < a, b < n$ zusammengesetzt, so gilt natürlich $a \mid (n-1)!$. Wäre nun auch noch n ein Teiler von $(n-1)!+1$, so wäre a als Teiler von n ebenfalls ein Teiler von $(n-1)!+1$. Dies ist aber nur für $a = 1$ möglich. ◇

Folgerung 2.30 *Seien $m \in \mathbb{N}$ und $a, c \in \mathbb{Z}$. Die lineare Kongruenz*

$$ax \equiv c \bmod m \tag{53}$$

hat genau dann eine Lösung $x \in \mathbb{Z}$, wenn $d = ggT(a, m) \mid c$ gilt. In diesem Fall ist die Kongruenz gleichwertig zu

$$\frac{a}{d}x \equiv \frac{c}{d} \bmod \frac{m}{d} \tag{54}$$

und deren Lösung $[x]$ ist eindeutig bestimmt. Also sind

$$[x]_m, [x + \frac{m}{d}]_m, \ldots, [x + (d-1)\frac{m}{d}]_m$$

alle Lösungen modulo m.

Beweis: Die Bedingungen $d \mid m$ und $d \mid a$ sowie $ax \equiv c \bmod m \iff m \mid (ax - c)$ zeigen, daß die Kongruenz (53) nur dann eine Lösung haben kann, wenn $d \mid c$ gilt. In diesem Fall ist die Kongruenz also äquivalent zu $\frac{m}{d} \mid (\frac{a}{d}x - \frac{c}{d})$, also zu (54). Diese Kongruenz hat wegen der Teilerfremdheit von $\frac{a}{d}$ und $\frac{m}{d}$ genau eine Lösung $[x]$ in der primen Restklassengruppe modulo $\frac{m}{d}$. Diese Restklasse spaltet sich modulo m genau zu den angegebenen Lösungen auf. ◇

Satz 2.31 (Chinesischer Restsatz) *Seien $n \in \mathbb{N}$ und $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd. Dann gibt es zu $a_1, \ldots, a_n \in \mathbb{Z}$ ein $x \in \mathbb{Z}$, das alle Kongruenzen*

$$x \equiv a_1 \bmod m_1, \ldots, x \equiv a_n \bmod m_n$$

erfüllt. Dieses x ist modulo $m_1 \cdots m_n$ eindeutig bestimmt und mit x ist auch jeder Repräsentant von $[x]_{m_1 \cdots m_n}$ eine Lösung.

Beweis: *Eindeutigkeit:* Sind $x, y \in \mathbb{Z}$ Lösungen der Kongruenzen, so folgt $m_i \mid (x-y)$ für $i = 1, \ldots, n$. Da die m_i paarweise teilerfremd sind, liefert Folgerung 1.35 $m_1 \cdots m_n \mid (x - y)$, also die behauptete Eindeutigkeit.

Existenz: Sei $M = m_1 \cdots m_n$ und $M_i = M/m_i$ für $i = 1, \ldots, n$. Wegen $ggT(M_i, m_i) = 1$ kann mit dem Euklidischen Algorithmus ein $N_i \in \mathbb{Z}$ bestimmt werden mit $M_i N_i \equiv 1 \bmod m_i$. Sei $x = \sum_{i=1}^{n} a_i M_i N_i$. Dann gilt $m_i \mid a_j M_j N_j$ für $i, j = 1, \ldots, n$ und $i \neq j$, also $x \equiv a_i M_i N_i \equiv a_i \bmod m_i$. ◇

Beispiel 2.32 Kurt Gödel (1906 - 1978) definierte im Jahr 1931 die folgende *Gödel-Funktion* $g : {\mathbb{N}_0}^3 \to \mathbb{N}_0$ durch

$$g(a, b, c) = a \bmod (1 + b \cdot (c + 1))$$

für alle $a, b, c \in \mathbb{N}_0$. Sie hat die folgende Eigenschaft:

Zu $a_1, \ldots, a_n \in \mathbb{N}_0, n \geq 2$ existieren stets Zahlen $x, y \in \mathbb{N}_0$ mit $a_i = g(x, y, i)$ für $i = 1, \ldots, n$.

Zum Beweis zeigt man zunächst, daß für $y = (n!)^\ell \geq \max\{a_1, \ldots, a_n\}$ die Zahlen $1 + y(i + 1)$ für $i = 1, \ldots, n$ paarweise teilerfremd sind. Gäbe es nämlich eine Primzahl p, die sowohl $1 + y(i + 1)$ als auch $1 + y(i + k + 1)$ für ein k mit $1 \leq k \leq n - 1$ teilt, so wäre p auch ein Teiler der Differenz $y \cdot k$. Wäre aber p ein Teiler von y, dann auch von $y(i + 1)$ und gleichzeitig von $1 + y(i + 1)$, was unmöglich ist. Wäre andererseits p ein Teiler von $k \leq n - 1$, dann auch von $y = (n!)^\ell$, was, wie schon gezeigt, unmöglich ist.

Nach dem Chinesischen Restsatz gibt es dann eine Zahl $x \in \mathbb{N}_0$ mit der gewünschten Eigenschaft.

Aufgabe 2.33 Lösen Sie das folgende Gleichungssystem im Restklassenring $(\mathbb{Z}/(23), +, \cdot)$.

$$\begin{array}{rcrcrcr} 3x_1 & & & + & 19x_3 & = & 11 \\ 2x_1 & + & 14x_2 & + & 12x_3 & = & 2 \\ 17x_1 & + & 10x_2 & + & 5x_3 & = & 17 \end{array}$$

Aufgabe 2.34 Lösen Sie das folgende Gleichungssystem im Restklassenring $(\mathbb{Z}/(23), +, \cdot)$.

$$\begin{array}{rcrcrcr} 9x_1 & + & 2x_2 & + & 20x_3 & = & 9 \\ 2x_1 & + & 4x_2 & + & 20x_3 & = & 9 \\ x_1 & + & 5x_2 & + & 3x_3 & = & 14 \end{array}$$

Aufgabe 2.35 Bestimmen Sie alle Werte der Parameter $a, b \in \mathbb{Z}/(6)$, für welche die Matrix

$$M(a,b) = \begin{pmatrix} a & 2 \\ 2 & b \end{pmatrix}$$

invertierbar ist und geben Sie die jeweilige Inverse an.

Aufgabe 2.36 Begründen Sie, warum das System der Kongruenzen

$$\begin{array}{rcrcr} x & \equiv & 1 & \mod & 25 \\ x & \equiv & 2 & \mod & 7 \\ x & \equiv & 4 & \mod & 9 \\ x & \equiv & 7 & \mod & 38 \end{array}$$

modulo $25 \cdot 7 \cdot 9 \cdot 38$ eindeutig lösbar ist und bestimmen Sie die kleinste natürliche Zahl x, welche diese vier Kongruenzen erfüllt.

Folgerung 2.37 *Seien $n \in \mathbb{N}$ und $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd. Die Abbildung $f([x]_{m_1 \cdots m_n}) = ([x]_{m_1}, \ldots, [x]_{m_n})$ vermittelt Bijektionen*

$$f : \mathbb{Z}/m_1 \cdots m_n\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z},$$

$$f : (\mathbb{Z}/m_1 \cdots m_n\mathbb{Z})^* \to (\mathbb{Z}/m_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/m_n\mathbb{Z})^*.$$

Satz 2.38 *a) Die Eulersche φ-Funktion ist multiplikativ.*

b) Für Primzahlpotenzen p^k gilt $\varphi(p^k) = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$.

c) Für beliebiges $n \in \mathbb{N}$ gilt

$$\varphi(n) = n \prod_{p \in \mathbb{P},\ p|n} \left(1 - \frac{1}{p}\right). \tag{55}$$

d) Für beliebiges $n \in \mathbb{N}$ gilt

$$\sum_{d|n} \varphi(d) = n. \tag{56}$$

Beweis: a) Dies folgt unmittelbar aus der Definition der φ-Funktion und der zweiten Formel aus Folgerung 2.37.

b) Zwischen 1 und p^k sind alle Zahlen teilerfremd zu p^k außer den Vielfachen von p. Dies sind aber genau $p^k/p = p^{k-1}$ Stück.

c) Man wende a) und b) auf die Primfaktorzerlegung von n an.

d) Sei $f(n) = \sum_{d|n} \varphi(d)$. Dann ist also $f(n) = n$ zu zeigen. Klar ist $f(1) = \varphi(1) = 1$. Seien $m, n \in \mathbb{N}$ teilerfremd. Dann existieren nach Folgerung 1.36 zu jedem Teiler $d \mid nm$ eindeutig bestimmte Teiler $d_1 \mid n$ und $d_2 \mid m$ mit $d = d_1 d_2$. Wegen $ggT(n, m) = 1$ gilt auch $ggT(d_1, d_2) = 1$ und daher nach a) $\varphi(d) = \varphi(d_1)\varphi(d_2)$. Nun folgt $f(nm) = \sum_{d|nm} \varphi(d) = \sum_{d_1|n} \sum_{d_2|m} \varphi(d_1)\varphi(d_2) = \left(\sum_{d_1|n} \varphi(d_1)\right) \left(\sum_{d_2|n} \varphi(d_2)\right) = f(n)f(m)$. Also ist f multiplikativ. Es reicht daher, $f(p^k) = p^k$ für Primzahlpotenzen p^k zu zeigen. Da die Teiler von p^k aber gerade die Potenzen p^j für $j = 0, \ldots, k$ sind, gilt $f(p^k) = \sum_{j=0}^{k} \varphi(p^j) = 1 + \sum_{j=1}^{k} (p^j - p^{j-1}) = p^k$. ◇

Aufgabe 2.39 Zeigen Sie, daß für natürliche Zahlen $n = p \cdot q$ mit genau zwei Primfaktoren $p, q \in \mathbb{P}$ die Kenntnis von $\varphi(n)$ gleichwertig mit der Kenntnis von p und q ist.

Aufgabe 2.40 a) Geben Sie eine streng monoton wachsende Folge $(n_k)_{k\in\mathbb{N}}$ an mit

$$\lim_{k\to\infty} \frac{\varphi(n_k)}{n_k} = 1.$$

b) Geben Sie eine streng monoton wachsende Folge $(n_k)_{k\in\mathbb{N}}$ an mit

$$\lim_{k\to\infty} \frac{\varphi(n_k)}{n_k} = 0.$$

Aufgabe 2.41 Beweisen Sie, daß für $m, n \in \mathbb{N}$ gilt

$$\varphi(mn)\varphi(ggT(m, n)) = \varphi(m)\varphi(n)ggT(m, n).$$

2.4 Konsequenzen für das Faktorisierungsproblem

Lemma 2.42 *Seien $a, b, c, m \in \mathbb{N}$ mit $ggT(b, m) = 1$ und $d = ggT(a, c)$.*

a) Aus $b^a \equiv 1 \bmod m$ und $b^c \equiv 1 \bmod m$ folgt dann $b^d \equiv 1 \bmod m$.

b) Sei $m > 2$. Aus $b^a \equiv -1 \bmod m$ und $b^c \equiv \pm 1 \bmod m$ folgt dann $b^d \equiv -1 \bmod m$ und a/d ist ungerade.

Beweis: a) Es sei $d = xa+yc$ die mit dem Euklidischen Algorithmus berechenbare Darstellung von $d = ggT(a, c)$. Wegen $ggT(b, m) = 1$ liegt $[b]_m$ in der primen Restklassengruppe modulo m. Dort gilt $[b^d] = [b^{xa+yc}] = [b^a]^x \cdot [b^c]^y = [1]^x \cdot [1]^y = [1]$.

b) Der Beweis verläuft analog zum Beweis von a) bis zu $[b^d] = [b^a]^x \cdot [b^c]^y = [-1]^x \cdot [\pm 1]^y = [\pm 1]$. Wegen $[b^d]^{a/d} = [b^a] = [-1]$ kann, da $m > 2$ ist, nicht $[b^d] = [1]$ gelten und a/d muß ungerade sein. ◇

Lemma 2.43 (Legendre, 1830) *Seien $b, n \in \mathbb{N}$ und $p \in \mathbb{P}$.*

a) Falls p ein Teiler von $b^n - 1$ ist, so gilt entweder (i) p teilt schon $b^d - 1$ für einen echten Teiler d von n oder (ii) $p \equiv 1 \bmod n$.

Sind p und n beide ungerade, so gilt im Fall (ii) sogar $p \equiv 1 \bmod 2n$.

b) Falls $p > 2$ ein Teiler von $b^n + 1$ ist, so gilt entweder (i) p teilt schon $b^d + 1$ für einen echten Teiler d von n, für den n/d ungerade ist, oder (ii) $p \equiv 1 \bmod 2n$.

Beweis: a) Es gilt $b^n \equiv 1 \bmod p$, also insbesondere $ggT(b, p) = 1$, und nach Satz 2.54 daher auch $b^{p-1} \equiv 1$ *mod* p. Aus Lemma 2.42 a) folgt $b^d \equiv 1 \bmod p$ für $d = ggT(n, p-1)$. Im Fall $d < n$ folgt die Behauptung (i), im Fall $n = d = ggT(n, p-1)$ folgt $n \mid p-1$, also (ii).

Sind im Fall (ii) p und n ungerade, so folgt aus $n \mid p-1$ sofort $2n \mid p-1$, da $p-1$ ja gerade ist.

b) Man wende Lemma 2.42 b) für $a = n$ und $c = (p-1)/2$ an, wobei man beachte, daß aus $x^2 \equiv 1 \bmod p$ schon $x \equiv \pm 1 \bmod p$ folgt. Das Polynom $f(x) = x^2 - 1 \in \mathbb{F}_p[x]$ kann nämlich nach Satz 5.9 nur die Nullstellen $x = 1$ und $x = -1$ haben. ◇

Folgerung 2.44 *Es sei p ein Primteiler der Fermat-Zahl $F_n = 2^{2^n} + 1$, $n > 1$. Dann gilt $p = k \cdot 2^{n+2} + 1$ für ein $k \in \mathbb{N}$.*

Beweis: Sei p (ungerader) Primfaktor von $F_n = 2^t + 1$ mit $t = 2^n$ und $n > 1$. In Lemma 2.43 b) kann (i) nicht eintreten, da für jeden echten Teiler $d \mid t = 2^n$ der Quotient t/n niemals ungerade sein kann. Also gilt $p \equiv 1 \bmod 2t$ und daher $p \equiv 1 \bmod 2^{n+1}$. Hieraus folgt wegen $n > 1$ noch $p \equiv 1 \bmod 8$ und wegen $2^{2^n} \equiv -1 \bmod p$ ist $ord_p(2) = 2^{n+1}$.

Nun zeigt Satz 2.88, daß 2 ein quadratischer Rest modulo p ist. Also ist $ord_p(2) = 2^{n+1}$ ein Teiler von $\frac{p-1}{2}$. Es folgt $p - 1 = k \cdot 2^{n+2}$. ◇

Bemerkung 2.45 Bei der Faktorisierung von Fermat-Zahlen benötigt man daher Kenntnisse über Primzahlen dieser Form (vgl. 7.12). So findet man leicht den Primteiler $p = 5 \cdot 2^7 + 1 = 641$ von $F_5 = 2^{2^5} + 1$. Auch für einige größere Werte von n hat man schnell Erfolg: $p = 1071 \cdot 2^8 + 1 = 274177$ teilt F_6, $p = 1188 \cdot 2^{11} + 1 = 2424833$ teilt F_9, $p = 11131 \cdot 2^{12} + 1 = 45592577$ teilt F_{10}, $p = 39 \cdot 2^{13} + 1 = 319489$ und $q = 119 \cdot 2^{13} + 1 = 974849$ teilen F_{11}, $p = 7 \cdot 2^{14} + 1 = 114689$ teilt F_{12}. Allerdings hat beispielsweise F_{11} auch einen Primfaktor mit 564 Dezimalstellen, der auf diese Weise nur schwer zu finden sein dürfte.

Beispiel 2.46 a) Um die Mersenne-Zahl $2^{11} - 1 = 2047$ zu faktorisieren gelte also $p \mid 2^{11} - 1$ für eine ungerade Primzahl p. Da Fall (i) nicht eintreten kann, folgt aus (ii) $p \equiv 1 \bmod 22$. Wegen $[\sqrt{2047}] = 45$ kommt nur $p = 23$ in Frage. Mit $2047/23 = 89$ ist daher die Faktorisierung $2047 = 23 \cdot 89$ gefunden.

b) Die entsprechende Überlegung für $2^{13} - 1 = 8191$ zeigt, daß Primfaktoren $p \equiv 1 \bmod 26$ unterhalb von $[\sqrt{8191}] = 90$ zu überprüfen sind. Dies sind $p = 53$ und $p = 79$, die beide keine Teiler von 8191 sind. Daher ist $M_{13} = 8191$ eine Mersennesche Primzahl. Statt der 23 ungeraden Primzahlen unterhalb von 90 sind also nur 2 zu testen.

c) Beim entsprechenden Test für $2^{17} - 1 = 131071$ sind die Primzahlen $p \equiv 1 \bmod 34$ unterhalb 362 zu prüfen. Dies sind $p = 103, 137, 239, 307$. Da sie keine Teiler sind, ist auch $M_{17} = 131071$ eine Mersennesche Primzahl.

d) Beim entsprechenden Test für $2^{19} - 1 = 524287$ sind die Primzahlen $p \equiv 1 \bmod 38$ unterhalb 724 zu prüfen. Dies sind $p = 191, 229, 419, 457, 571, 647$. Da sie keine Teiler sind, ist auch $M_{19} = 524287$ eine Mersennesche Primzahl.

e) Beim entsprechenden Test für $2^{23} - 1 = 8388607$ sind die Primzahlen $p \equiv 1 \bmod 46$ unterhalb 2896 zu prüfen. Schon bei $p = 47$ hat man einen Teiler gefunden. Also ist $M_{23} = 8388607 = 47 \cdot 178481$ keine Mersennesche Primzahl.

f) Beim entsprechenden Test für $2^{29} - 1 = 536870911$ sind die Primzahlen $p \equiv 1 \bmod 58$ unterhalb 23170 zu prüfen. Dies sind $p = 59, 233, \ldots$. Mit $p = 233$ hat man einen Teiler gefunden. Also ist $M_{29} = 536870911 = 233 \cdot 2304167 = 233 \cdot 1103 \cdot 2089$ keine Mersennesche Primzahl.

Beispiel 2.47 Zur Faktorisierung von $2^{35} - 1 = 34359738367$ werden zunächst die Primfaktoren p von $2^d - 1$ für die echten Teiler $d = 1, 5, 7$ von 35 untersucht. Dies sind $p = 31$ für $d = 5$ und $p = 127$ für $d = 7$. Beides sind Primfaktoren und es ist $(2^{35} - 1)/(31 \cdot 127) = 8727391$. Für alle weiteren Primfaktoren p muß nun Fall (ii) eintreten, d. h. $p \equiv 1 \bmod 70$ gelten. Schon für $p = 71$ erhält man

$8727391/71 = 122921$. Wegen $[\sqrt{122921}] = 350$ bleiben jetzt noch $p = 71, 211, 281$ zu testen. Da dies keine Teiler mehr sind, ist 122921 prim und $2^{35} - 1 = 31 \cdot 71 \cdot 127 \cdot 122921$ die gesuchte Faktorisierung.

Aufgabe 2.48 Faktorisieren Sie analog $2^n - 1$ für i) $n = 15$, ii) $n = 20$, iii) $n = 21$, iv) $n = 30$, v) $n = 33$, vi) $n = 60$.

Aufgabe 2.49 Faktorisieren Sie analog $3^n - 1$ für i) $n = 12$, ii) $n = 15$, iii) $n = 24$.

Durch Streichen eines Faktors 2 erhält man die Faktorisierungen der repetitiven Einsen $R_3 n$.

Aufgabe 2.50 Faktorisieren Sie analog $5^n - 1$ für i) $n = 9$, ii) $n = 10$, iii) $n = 12$.

Durch Streichen eines Faktors 4 erhält man die Faktorisierungen der repetitiven Einsen $R_5 n$.

Beispiel 2.51 Zur Faktorisierung von $n = 2^{24}+1 = 16777217$ sind die Primteiler von 2^d+1 zu untersuchen, wenn $\frac{24}{d}$ ungerade ist. Die einzige Möglichkeit ist $d = 8$. Es ist $2^8 + 1 = 257$ selbst prim und Teiler von n. Jeder andere Primteiler p von n erfüllt also $p \equiv 1 \bmod 48$. Die kleinste Primzahl dieser Bauart ist $p = 97$. Wegen $16777217/(257 \cdot 97) = 673$ ist damit schon die Primfaktorzerlegung $16777217 = 97 \cdot 257 \cdot 673$ gefunden.

Mehrere effiziente Faktorisierungsalgorithmen beruhen auf der folgenden simplen Beobachtung. Man sucht mit den Algorithmen systematisch nach ganzen Zahlen a, b, welche die Kongruenzen (57) erfüllen.

Lemma 2.52 *Gibt es für ein $n \in \mathbb{N}$ Zahlen $a, b \in \mathbb{Z}$ mit*

(57) $a^2 \equiv b^2$ *mod* n *und* $a \not\equiv \pm b \bmod n$,

dann sind $ggT(a + b, n)$ und $ggT(a - b, n)$ nichttriviale Teiler von n.

Beweis: Aus $a \not\equiv \pm b \bmod n$ folgt $n \not| (a + b)$ und $n \not| (a - b)$. Aus $a^2 \equiv b^2 \bmod n$ folgt aber $n \mid (a^2 - b^2) = (a + b)(a - b)$, d. h. $a^2 - b^2 = k \cdot n$. Also haben sowohl $a + b$ und n als auch $a - b$ und n einen nichttrivialen gemeinsamen Teiler. ◇

So kann man beispielsweise die in Beispiel 1.54 benutzte Fermat-Faktorisierung oft dadurch beschleunigen, indem man kleine Werte für $k \in \mathbb{N}$ probiert, z. B. $k = 3$.

2.5 Kleiner Fermatscher Satz und Carmichael-Zahlen

Satz 2.53 *Ist $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ teilerfremd zu n, so gilt*

(58) $a^{\varphi(n)} \equiv 1 \bmod n$.

Beweis: Folgt aus Satz 5.2 im Anhang. ◇

Satz 2.54 (Kleiner Fermatscher Satz) *Ist $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ teilerfremd zu p, so gilt*

(59) $a^{p-1} \equiv 1 \bmod p$.

Für alle $a \in \mathbb{Z}$ gilt $a^p \equiv a \bmod p$.

Beweis: Man wende den Satz 2.53 auf eine Primzahl an. Für die letzte Aussage multipliziere man im Fall $ggT(a,p) = 1$ die Gleichung noch einmal mit a, im Fall $p \mid a$ steht auf beiden Seiten 0. ◇

Aufgabe 2.55 Es sei p eine ungerade Primzahl und $M_p = 2^p - 1$ die zugeörige Mersenne-Zahl. Zu jedem Primteiler q von M_p existiert dann ein $k \in \mathbb{N}$ mit $q = 2kp + 1$.

Folgerung 2.56 *Ist p Primzahl und kein Teiler von $a \in \mathbb{Z}$, so folgt aus $n \equiv n' \bmod p-1$ bereits $a^n \equiv a^{n'} \bmod p$.*

Beweis: Gelte $n > n'$. Wegen $p - 1 \mid n - n'$ gilt $n = n' + k(p-1)$ für ein $k \in \mathbb{N}$. Dann folgt aus $a^{p-1} \equiv 1$ *mod* p sofort $a^{k(p-1)} \equiv 1 \bmod p$ und dann weiter $a^n = a^{n'+k(p-1)} \equiv a^{n'} \bmod p$. ◇

Folgerung 2.57 *Für $n, n', m \in \mathbb{N}$ und $a \in \mathbb{Z}$ gelte $ggT(a,m) = 1$ und n' sei der kleinste positive Rest von n modulo $\varphi(m)$. Dann gilt $a^n \equiv a^{n'} \bmod m$.*

Beweis: Es gelte also $n = n' + k\varphi(m)$ mit einem $k \in \mathbb{N}$. Aus $a^{\varphi(m)} \equiv 1 \bmod m$ folgt dann $a^{k\varphi(m)} \equiv 1 \bmod m$ und damit $a^n = a^{n'+k\varphi(m)} \equiv a^{n'} \bmod m$ ◇

Folgerung 2.58 *Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ teilerfremd. Genau dann ist n prim, wenn $(x+a)^n \equiv x^n + a \bmod n$ gilt, d. h. wenn die Polynome $(x+a)^n$ und $x^n + a$ im Polynomring $(\mathbb{Z}/n\mathbb{Z})[x]$ gleich sind.*

Beweis: Ist n prim, so gilt nach dem Kleinen Fermatschen Satz 2.54 $a^n \equiv a \bmod n$ und n teilt den Binomialkoeffizienten $\binom{n}{k}$ für $k = 1, ..., n-1$ wegen Aufgabe 2.28. Mit dem Binomischen Satz (vgl. Aufgabe 1.17) folgt daher $(x+a)^n \equiv x^n + a^n \equiv x^n + a \bmod n$.

Gelte umgekehrt

$$(60) \quad (x+a)^n = \sum_{k=0}^{n} \binom{n}{k} a^k x^{n-k} \equiv x^n + a \bmod n$$

und sei p Primteiler von n. Für den Koeffizienten $\binom{n}{p} a^p$ von x^{n-p} in dieser Summe gilt $\binom{n}{p} \not\equiv 0 \; mod \; n$, da n diesen Binomialkoeffizienten wegen $p \mid n$ nicht mehr teilen kann. Wegen $ggT(a,n) = 1$ ist aber a in $\mathbb{Z}/n\mathbb{Z}$ invertierbar und daher auch $\binom{n}{p} a^p \not\equiv 0 \bmod n$. Dann kann aber nur $p = n$ gelten, da alle anderen Koeffizienten verschwinden. ◇

Diese Folgerung ist die Grundlage des auf Agrawal, Kayal und Saxana zurückgehenden sogenannten AKS-Primzahltests. Dieser 2002 erstmals veröffentlichte Algorithmus war der erste deterministische Primzahltest mit polynomialer Laufzeit. Mittlerweile führten Verbesserungen durch andere Autoren zu einem Laufzeitverhalten von $\mathcal{O}((\log(n)^{6+\varepsilon})$ mit einem beliebig kleinen $\varepsilon > 0$. Zur Behandlung dieses Algorithmus werden verschiedene Hilfsaussagen benötigt, die wir schon hier zusammenstellen.

Für zusammengesetztes $n \in \mathbb{N}$ und beliebiges $a \in \mathbb{Z}$ werden die Polynome $(x+a)^n$ und $x^n + a$ in $(\mathbb{Z}/n\mathbb{Z})[x]$ im allgemeinen noch nicht gleich sein. Man kann aber prüfen, ob sie bei Division durch das Polynom $x^r - 1$ für ein $r \in \mathbb{N}$ mit $ggT(r,n) = 1$ denselben Rest lassen. Man schreibt dies dann in der Form (61). In diesem Fall erhält man:

Lemma 2.59 AKS1 *Seien $r, n \in \mathbb{N}$, $n > 2$ mit $ggT(r,n) = 1$ und $a \in \mathbb{Z}$ sowie p ein Primteiler von n. Aus*

$$(61) \quad (x+a)^n \equiv x^n + a \bmod (n, x^r - 1)$$

folgt dann

$$(62)\quad (x^m + a)^{n^i p^j} \equiv x^{mn^i p^j} + a \bmod (p, x^r - 1)$$

für alle $m \in \mathbb{N}$ *und* $i, j \in \mathbb{N}_0$.

Beweis: Sei zunächst $m = 1$. Wegen $p \mid n$ folgt aus (61) jedenfalls $(x + a)^n \equiv x^n + a \bmod (p, x^r - 1)$, also die Behauptung für $j = 0$ und $i = 0, 1$. Hieraus folgt mit

$$x^r - 1 \mid x^{kr} - 1 = (x^r - 1)(x^{r(k-1)} + x^{kr(k-2)} + \ldots + 1)$$

für alle $k \in \mathbb{N}$ aber durch Induktion nach $i \in \mathbb{N}_0$

$$\begin{aligned}(x + a)^{n^{i+1}} &= ((x + a)^{n^i})^n \\ &\equiv (x^{n^i} + a)^n \bmod (n, x^r - 1) \\ &\equiv x^{n^{i+1}} + a + nf(x^{n^i}) + (x^{n^i r} - 1)h(x^{n^i}) \bmod (n, x^r - 1) \\ &\equiv x^{n^{i+1}} + a \bmod (n, x^r - 1).\end{aligned}$$

Also gilt $(x + a)^{n^i} \equiv x^{n^i} + a \bmod (n, x^r - 1)$ und damit wegen $p \mid n$ auch $(x+a)^{n^i} \equiv x^{n^i} + a \bmod (p, x^r - 1)$ für alle $i \in \mathbb{N}_0$. Durch wiederholte Anwendung von Folgerung 2.58 erhält man $(x+a)^{n^i p^j} \equiv x^{n^i p^j} + a \bmod (p, x^r - 1)$ für alle $i, j \in \mathbb{N}_0$. Ersetzt man hierin x durch x^m, so gilt $(x^m+a)^{n^i p^j} \equiv x^{mn^i p^j} + a \bmod (p, x^{mr} - 1)$ und wegen $x^r - 1 \mid x^{mr} - 1$ dann die Behauptung. ◇

Wegen $ggT(r, n) = 1$ und $p \mid n$ liegen n und p in der primen Restklassengruppe $(\mathbb{Z}/r\mathbb{Z})^*$ und erzeugen dort eine Untergruppe U. Sei $d = \frac{\varphi(r)}{|U|}$. Da U die von n erzeugte Untergruppe umfaßt, gilt für $t = ord_r(n)$ nach dem Satz von Lagrange $t \mid |U|$ also $d \mid \frac{\varphi(r)}{t}$. Sei weiterhin $m_1, \ldots, m_d$ ein Repräsentantensystem von $(\mathbb{Z}/r\mathbb{Z})^*/U$, also $(\mathbb{Z}/r\mathbb{Z})^* = \bigcup_{k=1}^{d} m_k U$. Mit diesen Bezeichnungen gilt das folgende Lemma.

Lemma 2.60 AKS2 *Es gibt* $0 \le i, j, h, l \le \left\lfloor \sqrt{\frac{\varphi(r)}{d}} \right\rfloor$ *mit* $(i, j) \ne (h, l)$, *so daß die Kongruenz* $n^i p^j \equiv n^h p^l \bmod r$ *gilt. Außerdem hat man*

$$(x^{m_k} + a)^{n^i p^j} \equiv (x^{m_k} + a)^{n^h p^l} \bmod (p, x^r - 1)$$

für alle $k = 1, \ldots, d$.

Beweis: Die Anzahl der Paare (i,j) mit $0 \le i,j \le \left[\sqrt{\frac{\varphi(r)}{d}}\right]$ ist

$$\left(\left[\sqrt{\frac{\varphi(r)}{d}}\right]+1\right)^2 > \frac{\varphi(r)}{d}.$$

Die Restklassen $n^i p^j \bmod r$ liegen in der Gruppe U der Ordnung $\frac{\varphi(r)}{d}$. Also gibt es $(i,j) \neq (h,l)$ mit $n^i p^j \equiv n^h p^l \bmod r$, also $n^i p^j = n^h p^l + qr$ mit einem $q \in \mathbb{Z}$. Es folgt $x^{n^i p^j} = x^{n^h p^l + qr} \equiv x^{n^h p^l} \bmod x^r - 1$ und dann mit Lemma 2.59 die letzte Aussage. ◇

Sei p wie bisher Primteiler von n und $s \in \mathbb{N}$, $s > 1$ so, daß $ggT(a,n) = 1$ für alle $a = 1, \ldots, s$ gilt. Dann gilt $p > s$, da sonst $a = p$ nicht teilerfremd zu n sein kann. Daher sind die linearen Polynome $x + a \in (\mathbb{Z}/p\mathbb{Z})[x]$ für $a = 1, \ldots, s$ paarweise verschieden. Setzt man für $e = (e_1, \ldots, e_s) \in \mathbb{N}_0^s$ nun

$$f_e = \prod_{a=1}^{s} (x+a)^{e_a} \in (\mathbb{Z}/p\mathbb{Z})[x],$$

so folgt $f_e \neq f_e'$ für $e \neq e'$. Sei ζ eine primitive r-te Einheitswurzel über $(\mathbb{Z}/p\mathbb{Z})[x]$, d. h. es gelte $\zeta \in K \supseteq \mathbb{Z}/p\mathbb{Z}$ und $|\{\zeta, \zeta^2, \ldots, \zeta^r = 1\}| = r$ in einem Körper K. Jedem Polynom f_e werde nun der Vektor

$$\tilde{f}_e = (f_e(\zeta^{m_1}), \ldots, f_e(\zeta^{m_d})) \in K^d$$

zugeordnet. Dann gilt das folgende Lemma.

Lemma 2.61 AKS3 *Ist $e \neq e'$ und $\max(grad(f_e), grad(f_{e'})) < \varphi(r)$, so gilt $\tilde{f}_e \neq \tilde{f}_{e'}$.*

Beweis: Wegen Lemma 2.59 gilt

$$\begin{aligned} f_e(x^{m_k})^{n^i p^j} &= \prod_{a=1}^{s} (x^{m_k} + a)^{n^i p^j e_a} \\ &\equiv \prod_{a=1}^{s} (x^{m_k n^i p^j} + a)^{e_a} \bmod (p, x^r - 1) \\ &\equiv f_e(x^{m_k n^i p^j}) \bmod (p, x^r - 1). \end{aligned}$$

Wegen $\zeta^r = 1$ folgt $f_e(\zeta^{m_k})^{n^i p^j} = f_e(\zeta^{m_k n^i p^j})$.

Gilt nun $\tilde{f}_e = \tilde{f}_{e'}$, also $f_e(\zeta^{m_k}) = f_{e'}(\zeta^{m_k})$ für $k = 1, \ldots, d$, so auch $f_e(\zeta^{m_k n^i p^j}) = f_{e'}(\zeta^{m_k n^i p^j})$. Also ist $\zeta^{m_k n^i p^j}$ Nullstelle von $g = f_e - f_{e'} \in \mathbb{Z}/p\mathbb{Z}$. Wegen $(\mathbb{Z}/r\mathbb{Z})^* =$

$\bigcup_{k=1}^{d} m_k U$ und $|(\mathbb{Z}/r\mathbb{Z})^*| = \varphi(r) \leq r$ hat man also $\varphi(r)$ verschiedene Nullstellen von g. Wegen $grad(g) < \varphi(r)$ ist g daher das Nullpolynom, d. h. $f_e = f_{e'}$, also $e = e'$. ◇

Nach dem Kleinen Fermatschen Satz ist eine natürliche Zahl $n > 1$ also dann zusammengesetzt, wenn es eine ganze Zahl $1 < a < n$ mit $ggT(a, n) = 1$ gibt, für die $a^{n-1} \not\equiv 1 \bmod n$ gilt. Er liefert daher einen "negativen" Primzahltest. Man kann aber umgekehrt aus $a^{n-1} \equiv 1 \bmod n$ für alle derartigen Zahlen a nicht schließen, daß $n \in \mathbb{P}$ gilt. Dies wird durch die folgenden Überlegungen gezeigt.

Definition 2.62 Eine zusammengesetzte natürliche Zahl n heißt *pseudoprim* zur Basis $a \in \mathbb{N}$, $1 < a < n$, wenn

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

erfüllt ist, sie heißt *Carmichael-Zahl* (Robert Daniel Carmichael, 1879 - 1967), wenn (63) für alle derartigen a mit $ggT(a, n) = 1$ gilt.

Bemerkung 2.63 a) Es ist $n = 341 = 11 \cdot 31$ die kleinste Pseudoprimzahl zur Basis 2. Unterhalb von 341 erfüllen also tatsächlich nur die Primzahlen p die Bedingung $2^{p-1} \equiv 1 \bmod p$. Dies ist wohl auch der Grund dafür, daß diese Bedingung bei vielen antiken Mathematikern als ("Chinesischer") Primzahltest angesehen wurde.

b) $n = 341, 561 = 3 \cdot 11 \cdot 17$ und $645 = 3 \cdot 5 \cdot 43$ sind die einzigen Pseudoprimzahlen zur Basis 2 unterhalb von 1000. Wegen $3^{340} \not\equiv 1 \bmod 341$ und $3^{644} \not\equiv 1 \bmod 645$ sind dies aber keine Pseudoprimzahlen zur Basis 3. Dagegen gelten $a^{561} = (a^{187})^3 \equiv a^{187} = a(a^{93})^2 \equiv a^3 \equiv a \bmod 3$, $a^{561} = (a^{51})^{11} \equiv a^{51} = a^7(a^{11})^4 \equiv a^{11} \equiv a \bmod 11$ und $a^{561} = (a^{33})^{17} \equiv a^{33} = a^{16}a^{17} \equiv a^{16}a \equiv a \bmod 17$, woraus mit dem chinesischen Restsatz $a^{561} \equiv a \bmod 561$ für jede Basis a folgt. Daher ist 561 eine Carmichael-Zahl.

c) $161038 = 2 \cdot 73 \cdot 1103$ ist eine gerade Pseudoprimzahl zur Basis 2 (vgl. hierzu auch Aufgabe 2.69).

Lemma 2.64 (Cipolla, 1904) *Sei $a \in \mathbb{N}$, $1 < a$, und p ungerade Primzahl mit $p \nmid a(a^2-1)$. Dann ist $n = (a^{2p}-1)/(a^2-1)$ pseudoprim zur Basis a. Insbesondere gibt es unendlich viele Pseudoprimzahlen zur Basis a.*

Beweis: Wegen $n = ((a^p - 1)/(a-1))((a^p+1)/(a+1))$ ist n zusammengesetzt. Weiterhin gilt

$$\begin{aligned} n-1 &= (a^{2p}-1)/(a^2-1) - (a^2-1)/(a^2-1) \\ &= (a^{2p} - 1 - a^2 + 1)/(a^2-1) \\ &= a^2(a^{2p-2}-1)/(a^2-1) \\ &= a^2(a^{p-1}+1)((a^{p-1}-1)/(a^2-1)). \end{aligned}$$

Falls a gerade ist, so ist auch a^2 und damit $n-1$ gerade, falls a ungerade ist, so ist $a^{p-1}+1$ gerade und damit ebenfalls $n-1$. Aus $p \not| a$ folgt $a^{p-1} \equiv 1 \; mod \; p$ nach Satz 2.54. Wegen $p \not| (a^2-1)$ folgt $p \mid n-1$, also insgesamt $2p \mid n-1$. Wegen $n(a^2-1) = a^{2p} - 1$ ist $a^{2p} \equiv 1 \; mod \; n$ und daher erst recht $a^{n-1} \equiv 1 \; mod \; n$. ◇

Beispiel 2.65 Für $a = 2$ und $p = 5$ erhält man das oben schon angegebene Beispiel $n = (2^{10}-1)/3 = 341 = 11 \cdot 31$, für $a = 2$ und $p = 7 \not| 6 = 2 \cdot (2^2 - 1)$ ist $n = (2^{14}-1)/3 = 5461 = 43 \cdot 127$ pseudoprim zur Basis 2.

Wegen $3^{90} = (3^6)^{15} = 729^{15} \equiv 1^{15} = 1 \; mod$ 91 ist 91 pseudoprim zur Basis 3, wegen $2^{90} \equiv 64 \; mod$ 91 aber nicht pseudoprim zur Basis 2.

Wegen $4^{14} = (4^2)^7 = 16^7 \equiv 1^7 = 1 \; mod$ 15 ist 15 pseudoprim zur Basis 4.

Lemma 2.66 *Es sei $n \in \mathbb{N}$ zusammengesetzt und ungerade.*

i) Für $a \in \mathbb{N}$, $1 < a < n$ mit $ggT(a,n) = 1$ ist n genau dann pseudoprim zur Basis a, wenn die Ordnung von a in der primen Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ ein Teiler von $n-1$ ist.

ii) Ist n pseudoprim zu den Basen a und b mit $ggT(a,n) = ggT(b,n) = 1$, so ist n auch pseudoprim zur Basis ab und zur Basis ab^{-1}, wobei b^{-1} das Inverse von b modulo n bezeichnet.

iii) Gilt für eine einzelne Basis $a \in (\mathbb{Z}/n\mathbb{Z})^*$ die Gleichung (63) nicht, so gilt sie auch für mindestens die Hälfte aller $a \in (\mathbb{Z}/n\mathbb{Z})^*$ nicht.

Beweis: i) Folgt unmittelbar aus Satz 5.2.

ii) Folgt aus den Potenzrechenregeln in $(\mathbb{Z}/n\mathbb{Z})^*$.

iii) Sei $\{a_1, \ldots, a_k\}$ die Menge aller Basen $0 < a_i < n$, für die n pseudoprim zur Basis a_i ist. Wäre nun n pseudoprim zur Basis aa_i für ein i mit $1 \le i \le n$, dann wäre nach ii) n auch pseudoprim zur Basis $a \equiv (aa_i)a_i^{-1} \; mod \; n$, was nicht der Fall ist. Also ist n mindestens zu diesen k Basen nicht pseudoprim. ◇

Bemerkung 2.67 Die kleinste Carmichael-Zahl ist $n = 561 = 3 \cdot 11 \cdot 17$ (vgl. Abschnitt 7.18), denn sie ist quadratfrei und $n - 1 = 560$ ist durch $2 = 3 - 1$, $10 = 11 - 1$ und $16 = 17 - 1$ teilbar (vgl. den folgenden Satz). 1992 haben Alford, Granville und Pomerance gezeigt, daß es unendlich viele Carmichael-Zahlen gibt (vgl. Abschnitt 7.19). Im Juli 2012 wurde eine Carmichael-Zahl mit fast 300 Milliarden Dezimalstellen und mehr als 10 Milliarden Primfaktoren konstruiert.

Satz 2.68 *Es sei n eine zusammengesetzte ungerade natürliche Zahl.*

i) Ist n teilbar durch eine Quadratzahl $p^2 > 1$, so ist n keine Carmichael-Zahl.

ii) Ist n quadratfrei, so ist n genau dann eine Carmichael-Zahl, wenn für jeden Primteiler p von n bereits $(p-1) \mid (n-1)$ gilt.

Beweis: i) Gelte $p^2 \mid n$ und sei g ein erzeugendes Element von $(\mathbb{Z}/p^2\mathbb{Z})^*$, also $k = p(p-1)$ der kleinste Exponent, für den $g^k = 1$ gilt. Weiterhin sei m das Produkt aller Primteiler $q \neq p$ von n. Nach dem Chinesischen Restsatz (Satz 2.31) gibt es eine ganze Zahl b so daß $b \equiv g \ mod \ p^2$ und $b \equiv 1 \ mod \ m$ gleichzeitig erfüllt sind. Dann ist b wie g ein erzeugendes Element von $(\mathbb{Z}/p^2\mathbb{Z})^*$ und es gilt $ggT(b,n) = 1$, da b weder durch p noch durch einen Primteiler von m teilbar ist. Wäre nun n pseudoprim zur Basis b, so würde aus $b^{n-1} \equiv 1 \ mod \ n$ auch $b^{n-1} \equiv 1 \ mod \ p^2$ folgen und damit $p(p-1) \mid n-1$, also $n - 1 \equiv 0 \ mod \ p$. Es ist wegen $p \mid n$ aber $n - 1 \equiv -1 \ mod \ p$. Also ist n nicht pseudoprim zur Basis b und daher keine Carmichael-Zahl.

ii) Gelte also $(p-1) \mid (n-1)$ für jeden Primteiler p von n. Sei b eine Basis mit $ggT(b,n) = 1$. Dann ist b^{n-1} eine Potenz von b^{p-1} für jeden Primteiler p von n, also insbesondere $b^{n-1} \equiv 1 \ mod \ p$. Also wird $b^{n-1} - 1$ von allen Primteilern p von n geteilt und damit, da n quadratfrei ist, von n selbst. Also gilt $b^{n-1} \equiv 1 \ mod \ n$ und n ist Carmichael-Zahl.

Gibt es andererseits einen Primteiler p von n so, daß $p-1$ kein Teiler von $n-1$ ist, so sei wie im Beweis von i) g ein erzeugendes Element von $(\mathbb{Z}/p\mathbb{Z})^*$. Sei ebenso b eine Lösung der Kongruenzen $b \equiv g \ mod \ p$ und $b \equiv 1 \ mod \ n/p$. Dann gilt $ggT(b,n) = 1$ und $b^{n-1} \equiv g^{n-1} \ mod \ p$. Weil aber die Ordnung $p-1$ von g kein Teiler von $n-1$ ist, gilt $1 \not\equiv g^{n-1} \equiv b^{n-1} \ mod \ n$. Damit ist n keine Carmichael-Zahl. ◇

Aufgabe 2.69 Es sei $n \in \mathbb{N}$ eine quadratfreie Zahl. Ist n gerade, dann ist es keine Carmichael-Zahl. Zeigen Sie weiter, daß n genau dann eine Carmichael-Zahl ist, wenn für jeden Primteiler p von n bereits $p-1$ ein Teiler von $\frac{n}{p} - 1$ ist.

Aufgabe 2.70 Prüfen Sie, ob es sich bei $172081, 552721$ und 847757 jeweils um eine Carmichael-Zahl handelt.

Folgerung 2.71 *Eine Carmichael-Zahl ist das Produkt von mindestens drei verschiedenen Primzahlen.*

Beweis: Da eine Carmichael-Zahl quadratfrei ist, kann sie nur aus verschiedenen Primfaktoren zusammengesetzt sein. Es bleibt der Fall $n = pq$ mit $p < q$ prim auszuschließen. Wäre n nun eine Carmichael-Zahl, so wäre $n-1 \equiv 0 \; mod \; (q-1)$. Es ist aber $n-1 = p(q-1+1)-1 \equiv p-1 \not\equiv 0 \; mod \; (q-1)$ wegen $0 < p-1 < q-1$. $\diamond$

Aufgabe 2.72 Sind für ein $m \in \mathbb{N}$ die Zahlen

$$p_1 = 6m+1, \quad p_2 = 12m+1, \quad p_3 = 18m+1$$

prim, so ist $n = p_1 p_2 p_3$ eine Carmichael-Zahl.

Aufgabe 2.73 Bestimmen Sie alle Carmichael-Zahlen der Form $3pq$ und $5pq$ für Primzahlen p und q.

Definition 2.74 Eine Primzahl p heißt *Wieferich-Primzahl zur Basis* $a > 1$ (Arthur Wieferich, 1884 - 1954), wenn

(64) $a^{p-1} \equiv 1 \; mod \; p^2$

gilt, andernfalls heißt sie *Nicht-Wieferich-Primzahl zur Basis* a.

Bemerkung 2.75 a) Die einzigen Wieferich-Primzahlen zur Basis 2 unterhalb von $6 \cdot 10^9$ sind 1093 und 3511.

b) Die einzigen Wieferich-Primzahlen zur Basis 3 unterhalb von 2^{30} sind 11 und 10006003.

Forschungsproblem: Zu welchen Basen $a > 1$ gibt es unendlich viele Wieferich-Primzahlen bzw. Nicht-Wieferich-Primzahlen?

2.6 Quadratische Reste und das Reziprozitätsgesetz

Betrachte im endlichen Körper $\mathbb{F}_p$ für eine ungerade Primzahl p und ein $a \in \mathbb{F}_p^*$ alle Lösungen der quadratischen Gleichung $x^2 - a = 0$. Wegen Satz 5.9 existieren höchstens zwei Lösungen. Existiert mit $b \in \mathbb{F}_p$ eine Lösung, dann ist $-b \neq b$ die zweite Lösung. Daher kann man (im Falle der Existenz) eine Lösung unter den Resten $b = 1, 2, \ldots, (p-1)/2$ modulo p finden, indem man deren Quadrate berechnet. Diese Quadrate sind paarweise verschieden, denn für $b \neq c$ folgt aus $b^2 = c^2$ sofort $b^2 - c^2 = (b-c)(b+c) = 0$ und daher wegen der Nullteilerfreiheit $b + c = 0$, also $b = -c$, was unter diesen Resten unmöglich ist. Also sind stets genau die Hälfte aller Elemente von $\mathbb{F}_p^*$ Quadrate, die andere Hälfte nicht. Man nennt die Quadrate auch *quadratische Reste modulo p* und die übrigen Elemente *(quadratische) Nichtreste modulo p*.

Beispiel 2.76 a) Für $p = 11$ erhält man so die $(11-1)/2 = 5$ Quadrate $1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 5$ und $5^2 = 3$. Die restlichen 5 Elemente $2, 6, 7, 8, 10 = -1$ sind keine Quadrate.

b) Für $p = 13$ erhält man die 6 Quadrate $1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 3, 5^2 = 12 = -1$ und $6^2 = 10$. Die restlichen 6 Elemente $2, 5, 6, 7, 8, 11$ sind keine Quadrate.

Bemerkung 2.77 a) Für die Primzahl $p = 2$ ist natürlich $a = 1$, das einzige Element aus $\mathbb{Z}/(p)^*$, ein quadratischer Rest und es existieren keine Nichtreste modulo p. Daher wird bei den folgenden Definitionen und Sätzen stets $p > 2$ vorausgesetzt.

b) Für zusammengesetzte Zahlen n ist die Frage nach Quadratwurzeln in $\mathbb{Z}/(n) \setminus \{0\}$ komplizierter. Wegen der Nullteiler ist Satz 5.9 nicht anwendbar und das Polynom $f(x) = x^2 - a$ kann mehr als zwei verschiedene Nullstellen haben. Für $n = 15 = 3 \cdot 5$ sind beispielsweise neben $x_1 = 1$ und $x_2 = -1$ auch $x_3 = 4$ und $x_4 = -4$ derartige Nullstellen von $f(x) = x^2 - 1$. Es gibt also i. a. weniger quadratische Reste als Nicht-Reste modulo n. Für $n = 15$ sind genau die Restklassen $1, 4, 6, 9$ und 10 quadratische Reste, die anderen neun Restklassen sind Nicht-Reste modulo n. Das Jacobi-Symbol aus Definition 2.95 gibt daher nicht unbedingt Auskunft darüber, ob ein Element $a \in \mathbb{Z}/(n)$ eine Quadratwurzel besitzt.

Für $n = 6 = 2 \cdot 3$ sind dagegen $1 = 1^2 = 5^2$, $3 = 3^2$ und $4 = 4^2 = 2^2$ drei quadratische Reste, denen nur die beiden Nicht-Reste 2 und 5 gegenüberstehen. Man kann aber die Anzahl der quadratischen Reste modulo n dadurch reduzieren, daß man sie auf zu n teilerfremde Restklassen einschränkt.

Definition 2.78 Es sei $p > 2$ eine Primzahl und $a \in \mathbb{Z}$. Das *Legendre-Symbol* (Adrien-Marie Legendre, 1752 - 1833) $\left(\frac{a}{p}\right)$ wird definiert durch

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p \mid a, \\ 1 & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist}, \\ -1 & \text{falls } a \text{ ein Nichtrest modulo } p \text{ ist.} \end{cases} \tag{65}$$

Lemma 2.79 (Euler-Kriterium) *Für Primzahlen $p > 2$ und $a \in \mathbb{Z}$ gilt*

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

Beweis: Die Rechnungen erfolgen in $\mathbb{F}_p$. Für $p \mid a$ steht auf beiden Seiten 0. Sei also a teilerfremd zu p, d. h. $a \in \mathbb{F}_p^*$. Nach dem kleinen Fermatschen Satz gilt $(a^{(p-1)/2})^2 = a^{p-1} = 1$, also ist $a^{(p-1)/2} = \pm 1$. Nach Satz 5.6 existiert ein erzeugendes Element g von $\mathbb{F}_p^*$, also $a = g^k$ für ein $k \in \mathbb{N}$ mit $1 \leq k \leq p-1$. Ist dabei k gerade, so gilt $a = (g^{k/2})^2$, d. h. a ist quadratischer Rest modulo p. Umgekehrt folgt aus $a = b^2$ für ein $b \in \mathbb{F}_p^*$ auch $b = g^\ell$ für ein $\ell \in \mathbb{N}$ mit $1 \leq \ell \leq p-1$ und damit $g^k = a = b^2 = g^{2\ell}$, also ist k gerade. Nun ist $a^{(p-1)/2} = g^{k(p-1)/2} = 1$ genau dann, wenn $k(p-1)/2$ teilbar durch $p-1$ ist, also genau dann, wenn k gerade ist. Daher sind beide Seiten der Kongruenz gleich ± 1 und genau dann gleich $+1$, wenn k gerade ist. ◇

Folgerung 2.80 (Francois Proth, 1852 - 1879) *Es sei $m = k2^n + 1$ mit ungeradem k und $k < 2^n$. Weiterhin existiere ein $a \in \mathbb{N}$ mit $\left(\frac{a}{m}\right) = -1$. Genau dann ist m Primzahl, wenn*

$$a^{(m-1)/2} \equiv -1 \ mod \ m$$

gilt.

Beweis: Ist m Primzahl, so folgt die Behauptung aus Lemma 2.79. Für die Umkehrung betrachte einen beliebigen Primteiler q von m. Dann hat man auch

$$a^{(m-1)/2} \equiv -1 \ mod \ q.$$

Daher gilt $ord_q(a) \mid q-1$ und $ord_q(a) \mid m-1$, aber $ord_q(a) \nmid (m-1)/2$. Es folgt $2^n \mid ord_q(a)$ und $q = t \cdot ord_q(a) + 1 \geq 2^n + 1 > \sqrt{m}$. Also ist $m = q$ prim. ◇

Bemerkung 2.81 Dieser Satz wird auch als *Proth's Primzahltest* bezeichnet. Er wurde von Proth 1878 veröffentlicht und ist eine Verallgemeinerung von Pepin's Test (Folgerung 3.9).

Man nennt daher Primzahlen der Form $k \cdot 2^n + 1$ mit ungeradem $k < 2^n$ auch *Prothsche Primzahlen*. Für $k = n$ ergeben sie die Cullen-Zahlen, für $k = 1$ die Fermat-Zahlen. Die ersten Prothschen Primzahlen sind $3 = 1 \cdot 2^1 + 1$, $5 = 1 \cdot 2^2 + 1$, $13 = 3 \cdot 2^2 + 1$, $17 = 1 \cdot 2^4 + 1$, $41 = 5 \cdot 2^3 + 1$, $97 = 3 \cdot 2^5 + 1$. Große Prothsche Primzahlen findet man im Anhang 7.12.

Sierpinski suchte ein $k \in \mathbb{N}$ für das $k2^n + 1$ für kein $n \in \mathbb{N}$ eine Primzahl ist. Er fand ein derartiges k in der Zahl 201446503145165177 und stellte daraufhin die Frage nach dem minimalen k^+ mit dieser Eigenschaft. Man konnte mittlerweile $k^+ \leq 78557$ zeigen und hat noch für 5 kleinere Werte von k bisher keine Primzahl der Form $k2^n + 1$ mit $n \leq 100000$ gefunden, allerdings auch noch nicht beweisen können, daß es keine geben kann. Es sind dies die folgenden Werte von k:

21181
22699
24737
55459
67607

Ein entsprechendes k für Zahlen der Form $k2^n - 1$ wurde von Hans Riesel (1929 -) mit $k = 509203$ ebenfalls gefunden. Hier sind noch 49 mögliche Kandidaten für ein kleineres k zu untersuchen.

2293, 9221, 23669, 31859, 38473,
46663, 67117, 74699, 81041, 93839,
97139, 107347, 121889, 129007, 143047,
146561, 161669, 192971, 206039, 206231,
215443, 226153, 234343, 245561, 250027,
315929, 319511, 324011, 325123, 327671,
336839, 342847, 344759, 362609, 363343,
364903, 365159, 368411, 371893, 384539,
386801, 397027, 409753, 444637, 470173,
474491, 477583, 485557, 494743

Für $p > 2$ sei $R_p^+ = \{1, 2, \ldots, \frac{1}{2}(p-1)\}$ und $S = \{\frac{1}{2}(p+1), \ldots, p-1\}$ eine disjunkte Zerlegung von $\{1, 2, \ldots, p-1\}$ in zwei gleich große Teilmengen und $R_p^- = S - p = \{-1, -2, \ldots, -\frac{1}{2}(p-1)\}$. Dann ist $R_p^+ \cup R_p^-$ ein Repräsentantensystem der

Restklassen von $\mathbb{Z}/(p)^*$ mit betragsmäßig kleinstmöglichen Repräsentanten. Ist $r \in R_p^+$ und $a \in \mathbb{Z}$ teilerfremd zu p, so ist auch ra teilerfremd zu p und es gibt genau einen Repräsentanten $r_a \in R_p^+$, so daß $ra \equiv \varepsilon(r,a)r_a \; mod \; p$ gilt, wobei das Vorzeichen $\varepsilon(r,a) \in \{-1,+1\}$ geeignet gewählt werde. Dabei gilt auch $r_a \equiv \varepsilon(r,a)ra \; mod \; p$.

Es ist also $\varepsilon(r,a) = -1$ genau dann, wenn der Repräsentant von ra negativ ist. Durchläuft nun bei fest gewähltem a der Parameter r den positiven Teil R_p^+ des Repräsentantensystems und ist n die Anzahl der Produkte $R_p^+ a = \{a, 2a, \ldots, \frac{1}{2}(p-1)a\}$, die einen Repräsentanten im negativen Teil besitzen, so gilt daher

$$\prod_{r \in R_p^+} \varepsilon(r,a) = (-1)^n.$$

Lemma 2.82 *Ist $p > 2$ Primzahl und $a \in \mathbb{Z}$ teilerfremd zu p, so definiert $\pi_a : R_p^+ \to R_p^+$ gemäß $\pi_a(r) = r_a$ eine Permutation von R_p^+.*

Beweis: Wegen der Endlichkeit von R_p^+ reicht es, die Injektivität zu zeigen. Gelte also $r_a = s_a$ für $r, s \in R_p^+$, also $\varepsilon(r,a)ra \equiv \varepsilon(s,a)sa \; mod \; p$. Da a und p teilerfremd sind, ist a kürzbar und es folgt $p \mid (\varepsilon(r,a)a - \varepsilon(s,a)s)$ in $\mathbb{Z}$. Es ist aber

$$|\varepsilon(r,a)a - \varepsilon(s,a)s| \leq |\varepsilon(r,a)r| + |\varepsilon(s,a)s| = r + s < (p-1),$$

wegen $r, s \in R_p^+$. Es folgt $\varepsilon(r,a)r = \varepsilon(s,a)s$ und wegen $r, s > 0$ muß $\varepsilon(r,a) = \varepsilon(s,a)$ und damit $r = s$ gelten. $\diamond$

Lemma 2.83 (Gauß, 1796) *Sei $p > 2$ prim und $a \in \mathbb{Z}$ teilerfremd zu p. Bezeichnet n die Anzahl der negativen Repräsentanten von $\{a, 2a, \ldots, \frac{1}{2}(p-1)a\}$ in dem betragsmäßig kleinsten Repräsentantensystem von $\mathbb{Z}/(p)^*$, so gilt*

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

Beweis: Alle Rechnungen erfolgen im Körper $\mathbb{Z}/(p)$. Wegen der Bijektivität von π_a gilt

$$\prod_{r \in R_p^+} r_a = \prod_{r \in R_p^+} r = (\frac{1}{2}(p-1))!.$$

Es folgt

$$a^{\frac{p-1}{2}}(\frac{1}{2}(p-1))! = \prod_{r \in R_p^+} ra = \prod_{r \in R_p^+} \varepsilon(r,a)r_a = (-1)^n(\frac{1}{2}(p-1))!.$$

Wegen $p \not| (\frac{1}{2}(p-1))!$ kann man kürzen und erhält

$$a^{\frac{p-1}{2}} = (-1)^n,$$

woraus mit dem Euler-Kriterium die Behauptung folgt. $\diamond$

Beispiel 2.84 Bei der Berechnung von $(\frac{7}{13})$ ist $R_{13}^+ = \{1,2,3,4,5,6\}$ und $R_{13}^+ \cdot 7 = \{7,14,21,28,35,42\}$. Wegen $7 \equiv -6, 14 \equiv 1, 21 \equiv -5,\ 28 \equiv 2, 35 \equiv -4, 42 \equiv 3\ mod\ 13$ ist $n = 3$ und daher $(\frac{7}{13}) = -1$, d. h. 7 ist ein quadratischer Nichtrest modulo 13, wie in Beispiel 2.76 b) schon festgestellt.

Lemma 2.85 *Das Legendre-Symbol hat für $p > 2$ die folgenden Eigenschaften:*

i) $a \equiv b\ mod\ p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

iii) $ggT(b,p) = 1 \implies \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

iv) $\left(\frac{1}{p}\right) = 1$ *und* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Beweis: i) folgt unmittelbar aus der Definition.

ii) folgt aus Lemma 2.79 nach den Potenzrechenregeln in $(\mathbb{F}_p^*, \cdot)$.

iii) folgt sofort aus ii).

iv) Die erste Formel folgt aus $1^2 = 1$, die zweite für $a = -1$ aus Lemma 2.79. $\diamond$

Bemerkung 2.86 Wegen iv) existiert genau für Primzahlen $p \equiv 1\ mod\ 4$ in $\mathbb{F}_p$ bereits eine Quadratwurzel aus -1 (vgl. Beispiel 2.76) b)). Für die Primzahlen $p \equiv 3\ mod\ 4$ (vgl. Beispiel 2.76) a)) kann man eine Quadratwurzel i aus -1 in derselben Weise adjungieren, wie man dies für den Körper $\mathbb{R}$ der reellen Zahlen macht, um den Körper $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ der komplexen Zahlen zu erhalten. Auf diese Weise entstehen dann Körper $\mathbb{F}_p(i) = \mathbb{F}_p + \mathbb{F}_p i$.

Aufgabe 2.87 Bestimmen Sie für $p \equiv 3\ mod\ 4$ in $\mathbb{F}_p(i)$ das Inverse von $a = 1+i$.

Satz 2.88 *Für ungerade Primzahlen p gilt*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Es ist also 2 genau dann quadratischer Rest modulo p, wenn $p \equiv \pm 1$ mod 8 gilt, und genau dann quadratischer Nicht-Rest, wenn $p \equiv \pm 3$ mod 8 gilt.

Beweis: Setze $f(n) = (-1)^{(n^2-1)/8}$ für ungerades n und $f(n) = 0$ für gerades n. Dann ist also $f(p) = \left(\frac{2}{p}\right)$ für alle Primzahlen $p = 2k+1$ zu zeigen. Offensichtlich gilt $f(n)^p = f(n)$, da p ungerade und $f(n) \in \{-1, 0, 1\}$ ist. Außerdem hat man $f(n) = 0 = f(p) \cdot 0 = f(p)f(pn)$ für gerades n, $f(1) = 1 = f(p)f(1 \cdot p), f(3) = -1 = f(p) \cdot (-1)f(p) = f(p)f(3p), f(5) = -1 = f(p) \cdot (-1)f(p) = f(p)f(5p)$ und $f(7) = 1 = f(p)f(7p)$. Wegen $p^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$ gilt $p^2 \equiv 1$ *mod* 8. Daher existiert im Körper $\mathbb{F}_{p^2}$ eine primitive 8-te Einheitswurzel ξ. Insbesondere gilt $\xi^4 = -1$. Definiere die *Gauss'sche Summe* $G = \sum_{j=0}^{7} f(j)\xi^j$. Dann ist $G^p = \sum_{j=0}^{7} f(j)^p \xi^{pj} = \sum_{j=0}^{7} f(j)\xi^{pj}$. Wegen $\xi^5 = \xi^4\xi = -\xi, \xi^6 = -\xi^2$ und $\xi^7 = -\xi^3$ gilt also $G = \xi - \xi^3 - \xi^5 + \xi^7 = 2(\xi - \xi^3)$ und $G^2 = 4(\xi^2 - 2\xi^4 + \xi^6) = 8$, was insbesondere $G \neq 0$ in $\mathbb{F}_{p^2}$ bedeutet. In $\mathbb{F}_{p^2}$ ergibt sich daher einerseits

$$G^p = (G^2)^{(p-1)/2} G = 8^{(p-1)/2} G = \left(\frac{8}{p}\right) G = \left(\frac{2}{p}\right) G.$$

Andererseits hat man

$$G^p = \sum_{j=0}^{7} f(p)f(pj)\xi^{pj} = f(p) \sum_{j'=0}^{7} f(j')\xi^{j'} = f(p)G.$$

Also gilt $\left(\frac{2}{p}\right) G = f(p)G$. Division durch $G \neq 0$ liefert nun die Behauptung. ◇

Folgerung 2.89 *Sind $p = 4k+3$ mit $k \in \mathbb{N}$ und $q = 2p+1$ prim, so ist q echter Teiler von M_p.*

Beweis: Wegen $q = 8k + 7$ ist 2 quadratischer Rest modulo q. Also gilt $2^p = 2^{(q-1)/2} \equiv 1$ *mod* q und wegen $q = 2p + 1 < 2^p - 1 = M_p$ für $p > 3$ ist q echter Teiler von M_p. ◇

Folgerung 2.90 *a) Ist p Primzahl mit $p \equiv 1$ mod 4 und $q = 2p - 1$ ebenfalls prim, so ist $n = pq$ pseudoprim zur Basis 2.*

b) Aus $2^{n-1} \equiv 1$ mod n und $M_n = 2^n - 1$ folgt $2^{M_n - 1} \equiv 1$ mod M_n. Mit n ist daher auch M_n pseudoprim zur Basis 2.

c) Jede Mersenne-Zahl M_n ist also entweder eine Mersennesche Primzahl oder pseudoprim zur Basis 2.

Beweis: Aus $p = 4k+1$ folgt $q = 2p-1 = 8k+1$ und daher $(\frac{2}{q}) = 1$. Es gilt also nach Lemma 2.79 $2^{p-1} = 2^{(q-1)/2} \equiv 1 \; mod \; q$. Aus $2^{p-1} \equiv 1 \; mod \; p$ folgt damit $2^{p-1} \equiv 1 \; mod \; n$, und wegen $n-1 = (2p+1)(p-1)$ gilt erst recht $2^{n-1} \equiv 1 \; mod \; n$.

b) Es gilt $2^n - 1 = M_n \equiv 0 \; mod \; M_n$, also $2^n \equiv 1 \; mod \; M_n$. Wegen $M_n - 1 = 2^n - 2 = 2(2^{n-1}-1) \equiv 0 \; mod \; n$ gilt $n \mid M_n - 1$. Es folgt $2^{M_n-1} = (2^n)^{(M_n-1)/n} \equiv 1 \; mod \; M_n$. Ist dann noch n zusammengesetzt, so nach Lemma 1.58 auch M_n.

c) Für $n = 2$ ist $M_2 = 3$ eine Primzahl. Ist $n > 2$ Primzahl, so gilt nach dem kleinen Fermatschen Satz $2^{n-1} \equiv 1 \; mod \; n$ und damit ist entweder M_n eine Primzahl oder, falls sie zusammengesetzt ist, nach b) pseudoprim zur Basis 2. ◇

Lemma 2.91 *Jede zusammengesetzte Fermat-Zahl $F_k = 2^{2^k} + 1$ ist pseudoprim zur Basis 2.*

Beweis: Es gilt $2^{2^k} \equiv -1 \; mod \; F_k$ und daher $2^{F_k-1} = 2^{2^{2^k}} \equiv 1 \; mod \; F_k$ durch wiederholtes Quadrieren. ◇

Aufgabe 2.92 Es seien p und $q = 2p-1$ Primzahlen. Für jeden quadratischen Rest a modulo q ist dann $n = pq$ pseudoprim zur Basis a.

Satz 2.93 (Quadratisches Reziprozitätsgesetz) *Für verschiedene ungerade Primzahlen p und q gilt*

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right).$$

Beweis: Sei p^k Potenz von p mit $p^k \equiv 1 \; mod \; q$, beispielsweise $k = q-1$. Der Köper $\mathbb{F}_{p^k}$ enthält dann eine primitive q-te Einheitswurzel, etwa ξ. Definiere die Gauss'sche Summe $G = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^j$. Durch eine längere Rechnung kann man

$$G^2 = (-1)^{(q-1)/2} q,$$

also insbesondere $G^2 = \pm q$ und damit $G \neq 0$ zeigen. Dann ergibt sich

$$\begin{aligned} G^p &= (G^2)^{(p-1)/2} G = \left((-1)^{(q-1)/2} q\right)^{(p-1)/2} G \\ &= (-1)^{(p-1)(q-1)/4} q^{(p-1)/2} G = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right) G. \end{aligned}$$

Da $(\frac{j}{q})^p = (\frac{j}{q})$ gilt, hat man andererseits

$$G^p = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^{pj} = \sum_{j=0}^{q-1} \left(\frac{p}{q}\right)\left(\frac{pj}{q}\right) \xi^{pj} = \left(\frac{p}{q}\right) G.$$

Gleichsetzen beider Darstellungen von G^p und Kürzen durch $G \neq 0$ liefert die Behauptung. ◇

Beweis: Seien n und m die nach dem Lemma von Gauß bestimmten Zahlen mit

$$\left(\frac{q}{p}\right) = (-1)^n \text{ und } \left(\frac{p}{q}\right) = (-1)^m.$$

Dann ist zu zeigen

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{n+m}.$$

Dies ist gleichwertig dazu, daß

$$\frac{p-1}{2}\frac{q-1}{2} = n + m + 2k$$

für ein $k \in \mathbb{N}_0$ gilt. Dabei ist n die Anzahl der $\frac{p-1}{2}$ Zahlen aus $\{q, 2q, \ldots, \frac{1}{2}(p-1)q\}$, die einen negativen Repräsentanten besitzen. Dies sind genau die Zahlen rq mit $r \in R_p^+$, für die ein eindeutig bestimmtes $s \in \mathbb{Z}$ existiert mit

$$(66) \quad -\frac{1}{2}p < rq - sp < 0.$$

Hierbei ist jedenfalls $0 < s$, da r, q und p positiv sind, und $0 < r < \frac{1}{2}p$. Es folgt

$$sp < rq + \frac{1}{2}p < \frac{1}{2}pq + \frac{1}{2}p = \frac{1}{2}p(q+1),$$

also $s < \frac{1}{2}(q+1)$ und daher $s \leq \frac{1}{2}(q-1)$ oder $s \in R_q^+$. Es ist also n die Anzahl der Paare $(r, s) \in R_p^+ \times R_q^+$ mit (66).

Entsprechend ist $m \leq \frac{q-1}{2}$ die Anzahl der Paare $(r, s) \in R_p^+ \times R_q^+$ mit $-\frac{1}{2}q < sp - rq < 0$ oder (nach Multiplikation mit -1)

$$0 < rq - sp < \frac{1}{2}q.$$

Wäre $(r', s') \in R_p^+ \times R_q^+$ ein Paar mit $r'q - s'p = 0$, so würde $\frac{p}{q} = \frac{r'}{s'}$ mit $1 \leq s' \leq \frac{1}{2}(q-1)$ folgen, was unmöglich ist, da sich der Nenner q des Bruches nicht durch Kürzen verkleinern läßt.

Daher ist $m+n$ genau die Anzahl der Paare $(r,s) \in R_p^+ \times R_q^+$ mit

$$-\frac{1}{2}p < rq - sp < \frac{1}{2}q.$$

Es ist dies also die Anzahl der Gitterpunkte mit ganzzahligen Koordinaten, die im abgeschlossenen Rechteck mit den Eckpunkten $(1,1), (\frac{1}{2}(p-1),1), (\frac{1}{2}(p-1), \frac{1}{2}(q-1)), (1, \frac{1}{2}(q-1))$ und gleichzeitig im Innern des Parallelstreifens zwischen den beiden Geraden $qx-py = -\frac{1}{2}p$ und $qx-py = \frac{1}{2}q$ liegen. Im abgeschlossenen Rechteck liegen genau $\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ Gitterpunkte und dieses setzt sich zusammen als disjunkte Vereinigung des offenen Parallelstreifens mit zwei abgeschlossenen Dreiecken. Beide Dreiecke sind aber kongruent, besitzen also gleich viele Gitterpunkte. Ist $k \in \mathbb{N}_0$ die Anzahl der Gitterpunkte eines der beiden Dreiecke, so gilt die zu beweisende Gleichung. ◇

Aufgabe 2.94 a) Es sei $p > 5$ prim. Zeigen Sie, daß -3 genau dann ein quadratischer Nicht-Rest modulo p ist, wenn $p \equiv 1 \; mod \; 3$ gilt.

a) Es sei p eine ungerade Primzahl, für die auch $M_p = 2^p - 1$ eine Mersennesche Primzahl ist. Dann ist 3 ein quadratischer Nicht-Rest modulo M_p.

Definition 2.95 Es seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ ungerade mit der Primfaktorzerlegung $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Das *Jacobi-Symbol* $\left(\frac{a}{n}\right)$ ist dann definiert als Produkt von Legendre-Symbolen gemäß

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Satz 2.96 *Sind n und m ungerade natürliche Zahlen, so gelten*

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$$

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

Beweis: Jedenfalls gilt die erste Gleichung, wenn n ungerade Primzahl ist. Definiere $f(n) = (-1)^{(n^2-1)/8}$. Durch Betrachten aller Möglichkeiten für ungerade Zahlen n, m modulo 8 beweist man $f(nm) = f(n)f(m)$ für ungerade Zahlen. Besitzt nun n die Primfaktorzerlegung $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, so folgt

$$f(n) = f(p_1)^{\alpha_1} \cdots f(p_k)^{\alpha_k} = \left(\frac{2}{p_1}\right)^{\alpha_1} \cdots \left(\frac{2}{p_k}\right)^{\alpha_k} = \left(\frac{2}{n}\right).$$

In der zweiten Gleichung steht auf beiden Seiten 0, wenn n und m nicht teilerfremd sind. Gelte also $ggT(n,m) = 1$. Seien $m = p_1 \cdots p_r$ und $n = q_1 \cdots q_s$ die Primfaktorzerlegungen (eventuell mit Wiederholungen). Geht man von $\left(\frac{m}{n}\right) = \prod_{i,j}\left(\frac{p_i}{q_j}\right)$ zu $\left(\frac{n}{m}\right) = \prod_{i,j}\left(\frac{q_j}{p_i}\right)$ über, muß man das Reziprozitätsgesetz für das Legendre-Symbol $r \cdot s$-mal anwenden. Die Anzahl der Vorzeichen (-1) dabei ist die Anzahl, in denen $p_i \equiv 3 \ mod\ 4$ mit $q_j \equiv 3 \ mod\ 4$ zusammentrifft. Also gilt $(\frac{m}{n}) = (\frac{n}{m})$, falls nicht eine ungerade Anzahl mal $p_i \equiv 1 \ mod\ 4$ in m und ebenfalls eine ungerade Anzahl mal $q_j \equiv 3 \ mod\ 4$ in n vorkommt. Aber dies ist genau dann der Fall, wenn m und n selbst kongruent 3 modulo 4 sind. Also gilt $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)$ bis auf diesen Fall. Dies ist aber gerade die Behauptung. ◇

Bemerkung 2.97 Wie schon in Bemerkung 2.77 angedeutet, gibt das Jacobi-Symbol nicht unbedingt die korrekte Auskunft darüber, ob für eine zusammengesetzte ungerade Zahl n ein Element $a \in \mathbb{Z}/(n)^*$ ein quadratischer Rest oder ein quadratischer Nicht-Rest ist. Für $n = 15$ ist nämlich $a = 2$ ein quadratischer Nicht-Rest, obwohl

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$$

gilt. Es gilt aber das folgende Lemma.

Lemma 2.98 *Es sei $n \in \mathbb{N}$ eine ungerade zusammengesetzte Zahl. Ist $a \in \mathbb{Z}/(n)^*$ ein quadratischer Rest, so gilt $(\frac{a}{n}) = 1$.*

Beweis: Es sei $b \in \mathbb{Z}$ mit $b^2 \equiv a \ mod\ n$. Für jeden Primteiler p von n gilt dann $b^2 \equiv a \ mod\ p$, also $(\frac{a}{p}) = 1$ für das jeweilige Legendre-Symbol. Dann gilt aber auch $(\frac{a}{n}) = 1$ für das daraus durch Multiplikation entstehende Jacobi-Symbol. ◇

Aufgabe 2.99 Berechnen Sie die Jacobi-Symbole

i) $\left(\frac{4060}{341}\right)$, ii) $\left(\frac{2584}{253}\right)$, iii) $\left(\frac{221}{383}\right)$, iv) $\left(\frac{2333}{3673}\right)$.

Definition 2.100 Es sei n eine zusammengesetzte ungerade natürliche Zahl und $a \in \mathbb{N}$ mit $1 < a < n$ und $ggT(a,n) = 1$. Gilt dann

$$(67) \quad a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \ mod\ n,$$

so heißt n *Euler-pseudoprim* zur Basis a.

Lemma 2.101 *Ist n Euler-pseudoprim zur Basis a, dann ist n auch pseudoprim zur Basis a.*

Beweis: Quadrieren von (67) liefert stets (63). ◇

Bemerkung 2.102 Die Umkehrung von Lemma 2.101 gilt nicht. Es ist nämlich die zusammengesetzte ungerade Zahl $n = 21 = 3 \cdot 7$ zur teilerfremden Basis $a = 8 = 2^3$ wegen $a^2 = 64 \equiv 1 \bmod 21$ und damit $a^{n-1} = 8^{20} \equiv 1^{10} = 1 \bmod n$ pseudoprim. Weiterhin gilt schon $a^{(n-1)/2} = 8^{10} \equiv 1 \bmod n$, aber

$$\left(\frac{8}{21}\right) = \left(\frac{8}{3}\right)\left(\frac{8}{7}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{7}\right) = \left(\frac{2}{3}\right) = (-1)^{(9-1)/8} = -1.$$

Also ist (67) nicht erfüllt und daher $n = 21$ nicht Euler-pseudoprim zur Basis $a = 8$.

Zusammengesetzte Zahlen, die Euler-pseudoprim für jede zu ihnen teilerfremde Basis sind, heißen auch *absolut Euler-pseudoprim*. Sie entsprechen den Carmichael-Zahlen bei pseudoprimen Zahlen.

Bei manchen Autoren heißen die hier definierten Euler-Pseudoprimzahlen auch genauer Euler-Jacobi-Pseudoprimzahlen. Dann werden die Euler-Pseudoprimzahlen ohne Benutzung des Jacobi-Symbols definiert, indem auf der rechten Seite von (67) einfach ± 1 geschrieben wird. In diesem schwächeren Sinn wäre dann $n = 21$ zwar Euler-pseudoprim, aber eben nicht Euler-Jacobi-pseudoprim.

Die zusammengesetzte Zahl $n = 15 = 3 \cdot 5$ und die Basis $a = 11$ liefern wegen $11^2 = 121 \equiv 1 \; mod \; 15$ und damit $a^{(n-1)} = 11^{14} \equiv 1 \; mod \; n$ eine Pseudoprimzahl zur Basis a, die wegen $a^{(n-1)/2} = 11^7 \equiv 11 \not\equiv \left(\frac{a}{n}\right) \; mod \; n$ auch keine Euler-Pseudoprimzahl zur Basis a im schwächeren Sinn ist.

Lemma 2.66 iii) und Lemma 2.101 liefern die Grundlage für den probabilistischen Primzahltest nach Solovay und Strassen im Abschnitt 3.6.

Definition 2.103 Es sei n eine ungerade zusammengesetzte Zahl und $n - 1 = m2^k$ mit ungeradem m. Dann heißt n *streng (oder stark) pseudoprim zur Basis* a, $1 < a < n$, wenn entweder $a^m \equiv 1 \; mod \; n$ gilt oder $a^{m2^j} \equiv -1 \; mod \; n$ für ein j mit $0 \leq j < k$.

Selfridge konnte den folgenden Satz zeigen (vgl. [15], 15.2.4):

Satz 2.104 *Ist n streng pseudoprim zur Basis a, dann ist n auch Euler-pseudoprim zur Basis a.*

Auf diesem Konzept basiert der probabilistische Primzahltest nach Miller und Rabin.

Bemerkung 2.105 Bezeichne $p_1 = 2, p_2 = 3, \ldots, p_k$ die ersten k Primzahlen und ψ_k die kleinste natürliche Zahl, die gleichzeitig eine strenge Pseudoprimzahl zu den Basen p_1 bis p_k ist. Damit ist jede natürliche Zahl $1 < n < \psi_k$, die gleichzeitig für die Basen $a = p_1$ bis $a = p_k$ die Bedingungen aus Definition 2.103 erfüllt, eine Primzahl.

k	ψ_k	Faktorisierung
1	2047	$23 \cdot 89$
2	1373653	$829 \cdot 1657$
3	25326001	$2251 \cdot 11251$
4	3215031751	$151 \cdot 751 \cdot 28351$
5	2152302898747	$6763 \cdot 10627 \cdot 29947$
6	3474749660383	$1303 \cdot 16927 \cdot 157543$
7	341550071728321	$10670053 \cdot 32010157$

3 Primzahltests

3.1 Iterative Erzeugung großer Primzahlen

Der folgende Satz bildet die Grundlage für ein Verfahren zur Erzeugung großer Primzahlen.

Satz 3.1 (Pocklington's Theorem) *Es sei p eine ungerade Primzahl, k eine zu p teilerfremde natürliche Zahl mit $1 < k < 2(p+1)$ und $n = 2kp + 1$. Genau dann ist n prim, wenn eine natürliche Zahl a mit $1 < a < n$ existiert, so daß $a^{kp} \equiv -1$ mod n und $ggT(a^k + 1, n) = 1$ gelten.*

Algorithmus zur Erzeugung großer Primzahlen:

i) Wähle eine Primzahl p_1 mit $d_1 = 5$ Dezimalstellen.

ii) Finde ein $k_1 < 2(p_1 + 1)$, so daß $p_2 = 2k_1p_1 + 1$ entweder $d_2 = 2d_1$ oder $d_2 = 2d_1 - 1$ Dezimalstellen hat und ein $a_1 < p_2$ mit $a_1^{k_1p_1} \equiv -1$ *mod* p_2 und $ggT(a_1^{k_1} + 1, p_2) = 1$ existiert.

Nach Pocklington's Theorem ist p_2 prim.

iii) Wiederhole i) und ii) mit p_2 anstelle von p_1, um eine Folge von Primzahlen $p_3, p_4, \ldots$ zu erzeugen. Nach 5 Schritten kann man k_5 so wählen, daß $2k_5p_5 + 1$ 100 Dezimalstellen besitzt.

3.2 Der AKS-Primzahltest

Dieser deterministische polynomiale Primzahltest wurde von Agrawal, Kayal und Saxana 2002 veröffentlicht und beruht auf dem folgenden AKS-Kriterium.

Satz 3.2 AKS-Kriterium *Seien $n, r \in \mathbb{N}$ teilerfremd und $n > 2$. Weiterhin sei $s \in \mathbb{N}$, $s > 1$ so, daß $ggT(a, n) = 1$ gilt für $a = 1, \ldots, s$ und*

$$\binom{\varphi(r) + s - 1}{s} > n^{2d\left\lfloor\sqrt{\frac{\varphi(r)}{d}}\right\rfloor} \tag{68}$$

für alle Teiler $d \mid \frac{\varphi(r)}{t}$, *wenn* $t = ord_r(n)$ *die Ordnung von* n *in* $(\mathbb{Z}/r\mathbb{Z})^*$ *ist. Gilt dann*

(69) $(x+a)^n \equiv x^n + a \ mod \ (n, x^r - 1)$

für alle $a = 1, \ldots, s$, *so ist* n *eine Primzahlpotenz.*

Beweis: Der Beweis folgt aus den Lemmata 2.60 und 2.61, ist aber etwas langwieriger! ◇

Damit kann man folgenden Primzahltest formulieren.

Algorithmus 3.3 AKS-Primzahltest

Eingabe: $n > 2$ *natürliche Zahl*

Ausgabe: *entweder "n ist prim" oder "n ist zusammengesetzt"*

```
Es sei l die Binaerstellenzahl von n.
Schritt 1: Pruefe durch hoechstens l Divisionen,
           ob n eine Zweierpotenz ist.
           Dann ist n zusammengesetzt, stop
Schritt 2: e=4*l^2, N=2n(n-1)(n^2-1)...(n^e-1),
           suche kleinste Primzahl r, die N nicht teilt
Schritt 3: wenn n=p fuer Primzahl p<r dann ist n prim, stop
Schritt 4: wenn p|n fuer eine Primzahl p<r
           dann ist n zusammengesetzt, stop
Schritt 5: sind fuer ein a=1,...,r  die Polynome
           (x+a)^n und x^n + a
           inkongruent modulo (n,x^r-1),
           dann ist n zusammengesetzt, stop
Schritt 6: s=Logarithmus von n zur Basis r,
           ist die m-te Wurzel aus n ganzzahlig fuer ein 1<m<s,
           dann ist n  zusammengesetzt, stop
Schritt 7: n ist prim
```

Satz 3.4 *Der AKS-Primzahltest entscheidet in polynomialer Laufzeit für jede (ungerade) natürliche Zahl* $n > 1$, *ob sie Primzahl ist oder nicht.*

Beweis: Schritt 1 erfordert höchstens l Probedivisionen.

Schritt 2: Die Anzahl der Multiplikationen im Produkt

$$N = 2n(n-1)(n^2-1)\cdots(n^{4l^2}-1)$$

ist polynomial in l und kann daher durch ein ganzzahliges Polynom in l nach oben abgeschätzt werden. Wegen

$$\log_2(N) \leq 1+\log_2(n)+(\log_2(n))\sum_{i=1}^{4l^2} i \leq 1+l+l\left(\frac{(4l^2+1)4l^2}{2}\right) \leq 1+l(16l^4+1)$$

ist $k = [\log_2(N)]$ ebenfalls polynomial in l. Nach einem Satz von Tschebyscheff gilt für $k \geq 2$

$$\prod_{p\in\mathbb{P}, p\leq 2k} p > 2^k.$$

Wegen $N < 2^k$ gibt es also eine Primzal $p \leq 2k$ mit $p \not| N$. Da $2k$ polynomial in l ist, kann mit dem Sieb des Eratosthenes die Liste L aller dieser Primzahlen und darin die kleinste derartige Primzahl r in polynomialer Laufzeit gefunden werden. Insbesondere ist r auch kein Teiler von n und r ungerade.

Schritt 3/4: Dieser Test erfordert wegen der Länge von L ebenfalls nur polynomiale Laufzeit in l.

Schritt 5: Es wird gezeigt, daß die Voraussetzungen des AKS-Kriteriums erfüllt sind. Zunächst gilt $t = ord_r(n) > 4l^2$, denn aus $n^i \equiv 1 \; mod \; r$ für ein $1 \leq i \leq 4l^2$ würde $r \mid n^i - 1 \mid N$ folgen. Sei nun $s = r$. Wegen Schritt 3 und 4 gilt jetzt $1 = ggT(a,n)$ für alle $a = 1,\ldots,s$. Aus $r \geq 3$ folgt $\varphi(r) = r-1 \geq 2$ und daher

$$\binom{\varphi(r)+s-1}{s} = \binom{\varphi(r)+r-1}{r} = \binom{2\varphi(r)}{\varphi(r)+1} \geq 2^{\varphi(r)}.$$

Wegen $d \leq \frac{\varphi(r)}{t} < \frac{\varphi(r)}{4l^2}$ gilt

$$2d\left[\sqrt{\frac{\varphi(r)}{d}}\right] \leq 2d\sqrt{\frac{\varphi(r)}{d}} = \sqrt{4d\varphi(r)} < \frac{\varphi(r)}{l} < \frac{\varphi(r)}{\log_2(n)}$$

und damit insgesamt

$$\binom{\varphi(r)+s-1}{s} \geq 2^{\varphi(r)} = n^{\frac{\varphi(r)}{\log_2(n)}} > n^{2d\left[\sqrt{\frac{\varphi(r)}{d}}\right]}.$$

Damit sind die Voraussetzungen des AKS-Kriteriums erfüllt. Tritt nun in Schritt 5 eine Inkongruenz auf, so ist n zusammengesetzt. Insgesamt ist diese Überprüfung polynomial in l, denn die Anzahl der zu berechnenden Kongruenzen ist

durch $r \leq 2k$ beschränkt und die Berechnung von $(x+a)^n$ modulo $(n, x^r - 1)$ erfordert zunächst höchstens $2l$ Multiplikationen durch wiederholtes Quadrieren und Multiplizieren. Dabei werden Polynome vom Grad kleiner r, welche polynomial in l sind, mit Koeffizienten der Größe höchstens n, die also ebenfalls eine in l polynomiale Bitlänge haben, multipliziert. Insgesamt ist der Aufwand also polynomial in l.

Schritt 6: Wenn dieser Schritt erreicht wird, war das AKS-Kriterium anwendbar und n ist eine Primzahlpotenz. Nun erfolgt noch der Test, ob n eine echte Potenz ist. Weil alle Primzahlen $p \leq r$ keine Teiler von n sind, bleibt die Ganzzahligkeit von $\sqrt[m]{n}$ höchstens für solche m mit $1 < m < \log_r(n) \leq l$ zu prüfen. Für festes m muß dabei $a^m = n$ nur für solche $a \in \mathbb{N}$ geprüft werden, für die $1 < a \leq \log_m(n) \leq l$ gilt. Endet jeder dieser in polynomialer Laufzeit auszuführender Test negativ, so ist n prim. ◇

3.3 Primzahltest nach Pollard

Der folgende Satz beruht auf der Tatsache, daß Carmichaelzahlen mindestens drei Primfaktoren haben müssen (vgl. Folgerung 2.71).

Satz 3.5 *Es gibt eine positive Konstante C, so daß für alle natürlichen Zahlen $n > C$ gilt: Es ist n genau dann prim, wenn gleichzeitig gelten*

1. n ist keine Quadratzahl,

2. n besitzt keinen Primteiler $p \leq n^{1/3}$,

3. $k^{n-1} \equiv 1 \ mod \ n$ für alle natürlichen Zahlen $k < n^{1/5}$.

Beweis: Ist n prim, so sind 1. und 2. trivialerweise erfüllt, und 3. folgt aus dem kleinen Fermatschen Satz.

Sind umgekehrt die drei Bedingungen erfüllt, so gilt für jeden Primfaktor p von n wegen 2. bereits $p > n^{1/3}$, n kann also höchstens zwei Primfaktoren besitzen, die wegen 1. dann aber verschieden sein müssen. Gelte also $n = pq$ mit

$$n^{1/3} < q < p < n^{2/3}.$$

Dann gibt es (nach einem Satz von Burgess) eine positive Konstante C, so daß für alle $n > C$ und alle Primteiler p von n eine Primitivwurzel $k < n^{1/5}$ modulo p existiert, d. h. es gelten $k^{p-1} \equiv 1 \ mod \ p$, aber $k^m \not\equiv 1 \ mod \ p$ für alle $0 < m < p-1$. Wegen 3. gilt aber $k^{n-1} \equiv 1 \ mod \ n$, also erst recht $k^{n-1} \equiv 1 \ mod \ p$. Es folgt

$(p-1) \mid (n-1) = pq - 1 = (p-1)q + (q-1)$. Dann wäre aber $p-1$ ein Teiler von $q-1$, was wegen $q < p$ unmöglich ist. Also ist n prim. $\diamond$

Der auf diesem Satz basierende Pollardsche Primzahltest läuft also folgendermaßen ab. Zuerst wird geprüft, ob n eine Quadratzahl ist. Wenn nicht, werden Probedivisionen mit den Primzahlen $p \leq n^{1/3}$ durchgeführt. Hier liegt die entscheidende Verbesserung gegenüber dem trivialen Primzahltest. Zuletzt werden die Zahlen k unterhalb von $n^{1/5}$ gemäß 3. überprüft. Dabei kommt der schnelle Algorithmus "Quadrieren und multiplizieren" zum Einsatz.

3.4 Primzahltest für Fermat-Zahlen

Der übliche Primzahltest für Fermat-Zahlen beruht auf dem folgenden Satz. Die Gleichwertigkeit von a) und c) wurde von Lehmer nach Ergebnissen von Lucas bewiesen, die Gleichwertigkeit von b) und a) später von Brillhart und Selfridge (vgl. [2]).

Satz 3.6 *Es sei $n \in \mathbb{N}$ und $n-1 = \prod p_i^{k_i}$ die Primfakterzerlegung von $n-1$. Dann sind die folgenden Aussagen gleichwertig.*

a) n ist eine Primzahl.

b) Zu jedem Primteiler $p_i \mid (n-1)$ existiert ein $a_i \in \mathbb{N}$ mit $ggT(a_i, n) = 1$, so daß gilt

$$a_i^{n-1} \equiv 1 \ mod\ n \quad und \quad a_i^{(n-1)/p_i} \not\equiv 1 \ mod\ n.$$

c) Es gibt ein $a \in \mathbb{N}$ mit $ggT(a, n) = 1$, so daß für jeden Primteiler $p \mid (n-1)$ gilt

$$a^{n-1} \equiv 1 \ mod\ n \quad und \quad a^{(n-1)/p} \not\equiv 1 \ mod\ n.$$

Beweis: a) $\Longrightarrow$ c): Ist n eine Primzahl, dann erfüllt jede Primitivwurzel a modulo n beide Bedingungen.

c) $\Longrightarrow$ b): Klar.

b) $\Longrightarrow$ a): Sei zu jedem $p_i^{k_i}$ ein derartiges a_i gefunden und bezeichne $\ell_i = ord_n(a_i)$ die Ordnung von a_i in $(\mathbb{Z}/n\mathbb{Z})^*$. Dann gilt offensichtlich $\ell_i \mid (n-1)$, aber $\ell_i \nmid (n-1)/p_i$, also $p_i^{k_i} \mid \ell_i$. Es folgt nach dem Satz von Euler $p_i^{k_i} \mid \ell_i \mid \varphi(n)$ für alle i, d. h. $(n-1) \mid \varphi(n) \leq n-1$. Dies zeigt $\varphi(n) = n-1$ und damit ist n prim. $\diamond$

Bemerkung 3.7 a) Dieser Satz ist auch die Grundlage für sogenannte *Primzahlzertifikate*. Dabei wird für die betreffende Primzahl n rekursiv eine Liste aller Primteiler p_i von $n-1$ erzeugt und jeweils ein Element a_i angegeben, so daß b) erfüllt ist. Anhand dieser Liste kann dann sehr schnell überprüft werden, ob Teil b) dieses Satzes gilt und damit n prim ist. Die Erstellung eines derartigen Zertifikates ist allerdings um einige Größenordnungen aufwendiger als die weiter unten beschriebenen probabilistischen Primzahltests.

b) Mit diesem Satz kann man z. B. beweisen, daß

$$n = 22708823198678103974314518195029102158525052496759285596453269189798311427475159776411276642277139650833937$$

mit $n-1 = 2^4 \cdot 104729^8 \cdot 224737^8 \cdot 350377^4$ eine 107-stellige Primzahl ist, sobald diese Primfaktorzerlegung bekannt ist. Man benötigt dazu natürlich eine entsprechende Langzahlarithmetik.

Lemma 3.8 (Richelot, 1832) *Ist $p = 2^m + 1$ prim, also eine Fermatsche Primzahl, so ist jeder quadratische Nicht-Rest eine Primitivwurzel modulo p.*

Beweis: Da $p-1$ eine Zweierpotenz ist, ist $ord_p(a)$ für jedes Element von $(\mathbb{Z}/p\mathbb{Z})^*$ eine Zweierpotenz. Ist nun a ein Nicht-Rest, also $-1 = \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ mod\ p$, so kann die Ordnung nicht kleiner als $p-1$ sein, d. h. a ist eine Primitivwurzel. ◇

Folgerung 3.9 (Pepins Test, 1877) *Es sei $n \in \mathbb{N}$. Die Fermat-Zahl $F_n = 2^{2^n} + 1$ ist genau dann prim, wenn gilt*

$$3^{2^{2^n-1}} \equiv -1 \ mod\ F_n. \tag{70}$$

Beweis: Ist F_n prim, so existieren nach Satz 5.6 in $(\mathbb{Z}/F_n\mathbb{Z})^*$ genau $\varphi(F_n - 1) = 2^{2^n-1}$ Primitivwurzeln. Diese müssen mit sämtlichen Nicht-Resten, von denen es genau so viele gibt, übereinstimmen. Es gelten $F_n \equiv 1 \ mod\ 4$ und $F_n \equiv 2 \ mod\ 3$. Mit dem quadratischen Reziprozitätsgesetz erhält man

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Also ist 3 Nicht-Rest und daher Primitivwurzel. Dies zeigt (70).

Die Umkehrung ergibt sich aus Satz 3.6 mit $a = 3$ und dem einzigen Primteiler 2 von $F_n - 1$. ◇

Bemerkung 3.10 Pepin hatte ursprünglich die Aussage für 5 anstelle von 3 bewiesen, dazu aber bemerkt, daß 5 auch durch 10 ersetzt werden könne.

3.5 Lucas-Lehmer-Test für Mersenne-Zahlen

Ausgangspunkt dieses speziell auf Mersenne-Zahlen zugeschnittenen Primzahltests sind die von Lucas eingeführten Folgen. Er war durch seine Untersuchungen zur Faktorisierung der Fibonacci-Zahlen (vgl. 7.9) auf sie gestoßen.

Definition 3.11 Es seien a, b und $D = a^2 - 4b$ von 0 verschiedene ganze Zahlen und

$$(71) \quad \alpha = \frac{a + \sqrt{D}}{2} \text{ und } \beta = \frac{a - \sqrt{D}}{2}$$

die beiden verschiedenen Nullstellen der quadratischen Gleichung $x^2 - ax + b = 0$. Die Folgen $U(a,b) = (U_k(a,b))_{k\in\mathbb{N}_0}$ und $V(a,b) = (V_k(a,b))_{k\in\mathbb{N}_0}$ mit

$$(72) \quad U_k(a,b) = \frac{\alpha^k - \beta^k}{\alpha - \beta} \quad \text{und} \quad V_k(a,b) = \alpha^k + \beta^k$$

heißen die *zum Paar* (a,b) *gehörenden Lucas-Folgen.*

Bemerkung 3.12 a) Nach den Vietaschen Wurzelsätzen (Francois Vieta,1540 - 1603) gelten also $\alpha + \beta = a, \alpha \cdot \beta = b$ und $\alpha - \beta = \sqrt{D}$.

b) Weiterhin gelten $U_0(a,b) = 0, U_1(a,b) = 1, V_0(a,b) = 2$ und $V_1(a,b) = a$. Für $k \geq 2$ hat man die Rekursionen

$$(73) \quad U_k(a,b) = aU_{k-1}(a,b) - bU_{k-2}(a,b) \quad \text{und} \quad V_k(a,b) = aV_{k-1}(a,b) - bV_{k-2}(a,b)$$

Hieraus ergeben sich weitere Werte:

k	$U_k(a,b)$	$V_k(a,b)$
2	a	$a^2 - 2b$
3	$a^2 - b$	$a(a^2 - 3b)$
4	$a(a^2 - 2b)$	$a^4 - 4a^2b + 2b^2$
5	$a^4 - 3a^2b + b^2$	$a(a^4 - 5a^2b + 5b^2)$
6	$a(a^2 - 3b)(a^2 - b)$	$a^6 - 6a^4b + 9a^2b^2 - 2b^3$

c) Für $a = 1, b = -1$ ist $U(1,-1)$ gerade die Folge der Fibonacci-Zahlen, während die entsprechende Folge $V(1,-1)$ als *Lucas-Folge* bezeichnet wird. Sie beginnt

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, ...$$

d) Für $a = 3, b = 2$ erhält man $U_k(3,2) = 2^k - 1$ und $V_k(3,2) = 2^k + 1$.

e) Für $a = 2, b = -1$ erhält man die *Pell-Folgen*

$$(74) \quad U(2,-1) \ : \ 0, 1, 2, 5, 12, 29, 70, \ldots$$
$$(75) \quad V(2,-1) \ : \ 2, 2, 6, 14, 34, 82, 198, \ldots$$

f) Für $a = 2, b = -2$, also $\alpha = 1 + \sqrt{3}$, $\beta = 1 - \sqrt{3}$ und $D = 12$ erhält man die *Lehmer-Folgen*

$$(76) \quad U(2,-2) \ : \ 0, 1, 2, 6, 16, 44, 120, \ldots$$
$$(77) \quad V(2,-2) \ : \ 2, 2, 8, 20, 56, 152, \ldots$$

Lemma 3.13 *Es seien $U_k = U_k(a,b)$ und $V_k = V_k(a,b)$ zu einem Paar (a,b) gehörende Lucas-Folgen. Dann gelten für alle $n, m \in \mathbb{N}$*

$$(78) \quad 2U_{n+m} = U_nV_m + U_mV_n$$
$$(79) \quad 2b^mU_{n-m} = U_nV_m - U_mV_n \quad (n > m)$$
$$(80) \quad 2V_{n+m} = V_nV_m + DU_nU_m$$
$$(81) \quad V_{2n} = V_n^2 - 2b^n$$
$$(82) \quad 4b^n = V_n^2 - D \cdot U_n^2$$

Beweis: (78): Es ist

$$\begin{aligned} U_nV_m + U_mV_n &= \frac{\alpha^n - \beta^n}{\alpha - \beta}(\alpha^m + \beta^m) + \frac{\alpha^m - \beta^m}{\alpha - \beta}(\alpha^n + \beta^n) \\ &= \frac{2}{\alpha - \beta}(\alpha^{n+m} - \beta^{n+m}) = 2U_{n+m}. \end{aligned}$$

(79): Nach Definition ist

$$2b^mU_{n-m} = 2(\alpha\beta)^m \frac{\alpha^{n-m} - \beta^{n-m}}{\sqrt{D}} = 2\frac{\alpha^n\beta^m - \alpha^m\beta^n}{\sqrt{D}}.$$

Außerdem ist

$$U_nV_m - U_mV_n = \frac{\alpha^n - \beta^n}{\sqrt{D}}(\alpha^m + \beta^m) - \frac{\alpha^m - \beta^m}{\sqrt{D}}(\alpha^n + \beta^n) = 2\frac{\alpha^n\beta^m - \alpha^m\beta^n}{\sqrt{D}}.$$

Also gilt (79).

(80): Mit $U_k = \frac{\alpha^k - \beta^k}{\sqrt{D}}$ folgt

$$DU_nU_m = (\alpha^n - \beta^n)(\alpha^m - \beta^m) = \alpha^{n+m} + \beta^{n+m} - (\alpha^n\beta^m + \alpha^m\beta^n).$$

Nach Definition gilt

$$V_nV_m = (\alpha^n + \beta^n)(\alpha^m + \beta^m) = \alpha^{n+m} + \beta^{n+m} + (\alpha^n\beta^m + \alpha^m\beta^n).$$

Addiert man beide Gleichungen, so ergibt sich (80).

(81): Nach Definition ist

$$V_{2n} = \alpha^{2n} + \beta^{2n} = (\alpha^n + \beta^n)^2 - 2(\alpha\beta)^n = V_n^2 - 2b^n,$$

also gilt (81).

(82): Setzt man in (80) $n = m$ so ergibt sich $2V_{2n} = V_n^2 + DU_n^2$. Mit (81) erhält man $V_n^2 + DU_n^2 = 2V_n^2 - 4b^n$, woraus (82) folgt. ◇

Aufgabe 3.14 Rechnen Sie die in Bemerkung 3.12 f) angegebenen Werte der Lehmer-Folgen explizit nach.

Lemma 3.15 *Es seien $U_k = U_k(a,b)$ und $V_k = V_k(a,b)$ die zum Paar (a,b) gehörenden Lucas-Folgen. Für Primzahlen p gilt dann $V_p \equiv a \ mod\ p$ und bei $p > 2$ gilt $U_p \equiv D^{(p-1)/2} \equiv \left(\frac{D}{p}\right) \ mod\ p$.*

Beweis: Es ist $V_p = \alpha^p + \beta^p \equiv (\alpha + \beta)^p \equiv a^p \equiv a \ mod\ p$ nach dem kleinen Fermatschen Satz.

Bei ungeradem $p > 2$ gilt auch $U_p = \frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv \frac{(\alpha-\beta)^p}{\alpha-\beta} \equiv (\alpha - \beta)^{p-1} \equiv D^{(p-1)/2} \ mod\ p$. Die weitere Gleichung folgt mit dem Euler-Kriterium für Legendre-Symbole. ◇

Beispiel 3.16 Aus den in Bemerkung 3.12 f) angegebenen Werten folgt für die Primzahlen $p = 2, 3, 5$:

$V_2 = 8 \equiv 0 \equiv 2 \ mod\ 2$, $V_3 = 20 \equiv 2 \ mod\ 3$, $V_5 = 152 \equiv 2 \ mod\ 5$.

$U_3 = 6 \equiv 0 \equiv (\frac{12}{3}) \ mod\ 3$, $U_5 = 44 \equiv -1 \equiv (\frac{3}{5}) \equiv (\frac{12}{5}) \ mod\ 5$, $U_6 = 120 \equiv 0 \ mod\ 5$.

Lemma 3.17 *Für ungerade Primzahlen p und die Lehmer-Folge $U_k = U_k(2,-2)$ gilt $p \mid U_m$ spätestens für $m = p+1$. Ist μ das kleinste m mit dieser Eigenschaft, so gilt $p \mid U_n \Longleftrightarrow n = k\mu$ für ein $k \in \mathbb{N}$. Man nennt μ dann auch den Rang von p.*

Beweis: Aus (78) und (79) folgen wegen $U_1 = 1$ und $V_1 = a = 2$ sofort $2U_{p+1} = U_pV_1 + U_1V_p = 2U_p + V_p$ und $-4U_{p-1} = U_1V_p - U_pV_1 = V_p - 2U_p$ und damit wegen Lemma 3.15 $-8U_{p-1}U_{p+1} = V_p^2 - 4U_p^2 \equiv 4 - 4\left(\frac{3}{p}\right)^2 \equiv 0 \; mod \; p$. Wegen $p \not| -8$ gilt $p \mid U_{p-1}$ oder $p \mid U_{p+1}$.

Sei nun $\mu \leq p+1$ wie angegeben. Aus (78) folgt wegen $U_{2\mu} = U_\mu V_\mu$ sofort $p \mid U_{2\mu}$. Gelte also $p \mid U_{\ell\mu}$ für $\ell = 1, \ldots, k$. Dann folgt wiederum aus (78) $2U_{(k+1)\mu} = U_{k\mu}V_\mu + U_\mu V_{k\mu}$, also auch $p \mid 2U_{(k+1)\mu}$ und daher $p \mid U_{(k+1)\mu}$, weil p ungerade ist.

Gilt umgekehrt $p \mid U_n$, so liefert Division mit Rest $n = q\mu + r$ für ein $0 \leq r \leq \mu - 1$. Mit $r = n - q\mu$ folgt aus (79) $2(-2)^{q\mu}U_r = U_nV_{q\mu} - U_{q\mu}V_n$. Hieraus ergibt sich $p \mid 2(-2)^{q\mu}U_r$ und daraus wegen $p \not| 2(-2)^{q\mu}$ sofort $p \mid U_r$. Wegen der Minimalität von μ und $r < \mu$ folgt $r = 0$. ◇

Definition 3.18 Die *Mersenne-Testfolge* (L_n) werde rekursiv definiert durch $L_1 = 4$ und $L_n = L_{n-1}^2 - 2$.

Lemma 3.19 *Ist (L_n) die Mersenne-Testfolge und (V_n) die Lehmer-Folge, so gilt für $n \in \mathbb{N}$*

$$2^{2^{n-1}} L_n = V_{2^n}.$$

Beweis: Der Beweis erfolgt durch Induktion nach n. Es ist $2L_1 = 8 = V_2$ für $n = 1$. Gelte die Behauptung also für ein $n \in \mathbb{N}$. Dann folgt mit (81)

$$\begin{aligned} V_{2^{n+1}} &= V_{2\cdot 2^n} = (V_{2^n})^2 + (-2)^{2^n+1} = (2^{2^{n-1}} L_n)^2 + (-2)\cdot 2^{2^n} \\ &= 2^{2^n}(L_n^2 - 2) = 2^{2^n} L_{n+1} \end{aligned}$$

Also gilt die Behauptung für alle $n \in \mathbb{N}$. ◇

Bemerkung 3.20 Die Werte der Mersenne-Testfolge sind $L_1 = 4, L_2 = 14, L_3 = 194, L_4 = 37634, L_5 = 1416317954, L_6 = 2005956546822746114, \ldots$.

Für die ersten Mersenneschen Primzahlen $M_3 = 7$, $M_5 = 31$ und $M_7 = 127$ gilt

$L_1 \equiv 4 \; mod \; M_3$, $L_2 \equiv 0 \; mod \; M_3$

$L_1 \equiv 4 \; mod \; M_5$, $L_2 \equiv 14 \; mod \; M_5$, $L_3 \equiv 8 \; mod \; M_5$, $L_4 \equiv 0 \; mod \; M_5$,

$L_1 \equiv 4 \; mod \; M_7$, $L_2 \equiv 14 \; mod \; M_7$, $L_3 \equiv 67 \; mod \; M_7$, $L_4 \equiv 42 \; mod \; M_7$, $L_5 \equiv 111 \; mod \; M_7$, $L_6 \equiv 0 \; mod \; M_7$,

also $M_p \mid L_{p-1}$ für $p = 3, 5, 7$.

Für die ersten zusammengesetzten Mersenne-Zahlen $M_4 = 15$ und $M_6 = 63$ dagegen gilt

$L_1 \equiv 4 \; mod \; M_4$, $L_2 \equiv 14 \; mod \; M_4$, $L_3 \equiv 14 \not\equiv 0 \; mod \; M_4$,

$L_1 \equiv 4 \; mod \; M_6$, $L_2 \equiv 14 \; mod \; M_6$, $L_3 \equiv 5 \; mod \; M_6$, $L_4 \equiv 23 \; mod \; M_6$, $L_5 \equiv 23 \; mod \; M_6$,

also $M_n \not| \; L_{n-1}$ für $n = 4, 6$.

Diese (und weitere numerische) Beispiele legen den Satz 3.21 nahe.

Satz 3.21 (Lucas-Lehmer-Test) *Es sei $p > 2$ eine Primzahl und die Folge (L_n) rekursiv definiert durch $L_1 = 4$ und $L_n = L_{n-1}^2 - 2$ für $n > 1$. Genau dann ist die Mersenne-Zahl $M_p = 2^p - 1$ prim, wenn $M_p \mid L_{p-1}$ gilt.*

Beweis: Gelte $M_p \mid L_{p-1}$. Dies impliziert $M_p \mid V_{2^{p-1}}$. Außerdem sind alle Primfaktoren von M_p ungerade. Ist q ein solcher Primteiler und μ sein Rang, so folgt aus (78) $q \mid U_{2^p}$, also insbesondere $\mu \leq 2^p$, denn es gilt $q \mid M_p \mid V_{2^{p-1}}$ und $2U_{2^p} = 2U_{2^{p-1}}V_{2^{p-1}}$. Wegen Lemma 3.17 gilt $\mu \mid 2^p$. Also ist $\mu = 2^k$ für ein $0 \leq k \leq p$. Wäre $k \leq p-1$, so würde $\mu \mid 2^{p-1}$ und $q \mid U_{2^{p-1}}$ folgen. Aus $q \mid U_{2^{p-1}}$ und $q \mid V_{2^{p-1}}$ ergibt sich aber mit (82) der Widerspruch $q \mid 4 \cdot (-2)^{2^{p-1}}$. Also gilt $\mu = 2^p$ und daher $2^p \leq q + 1$, d. h. $M_p = 2^p - 1 \leq q$. Daher ist $M_p = q$ eine Primzahl.

Sei jetzt M_p eine (ungerade) Primzahl. Zu zeigen ist $M_p \mid L_{p-1}$ oder gleichwertig $M_p \mid V_{2^{p-1}}$. Wegen $2^{p-1} = (M_p + 1)/2$ ist dies gleichwertig zu $V_{(M_p+1)/2} \equiv 0 \; mod \; M_p$, was wegen der Nullteilerfreiheit von $\mathbb{F}_{M_p}$ wiederum gleichwertig zu $(V_{(M_p+1)/2})^2 \equiv 0 \; mod \; M_p$ ist. Da die Behauptung für $p = 3$ und $p = 5$ in Bemerkung 3.20 schon gezeigt wurde, sei nun $p > 5$. Dann ist $M_p = 2^p - 1 = 2^{3+(p-3)} - 1 = 8 \cdot 2^{p-3} - 1$, und daher $1 = \left(\frac{2}{M_p}\right) \equiv 2^{(M_p-1)/2} \; mod \; M_p$ nach Satz 2.88. Dies impliziert $(-2)^{(M_p+1)/2} = (-1)^{(M_p+1)/2} \cdot 2^{(M_p+1)/2} = 2^{(M_p+1)/2} \equiv 2 \; mod \; M_p$. Aus (81) folgt nun $V_{M_p+1} = (V_{(M_p+1)/2})^2 - 2 \cdot (-2)^{(M_p+1)/2} \equiv (V_{(M_p+1)/2})^2 - 4 \; mod \; M_p$. Es bleibt $V_{M_p+1} \equiv -4 \; mod \; M_p$ für $p > 5$ zu zeigen.

Wegen $M_p = 2^p - 1 \equiv (-1)^p - 1 = -2 \equiv 1 \; mod \; 3$ ist $\left(\frac{M_p}{3}\right) = \left(\frac{1}{3}\right) = 1$ und damit mit dem Reziprozitätsgesetz $\left(\frac{12}{M_p}\right) = \left(\frac{3}{M_p}\right) = \left(\frac{M_p}{3}\right)(-1)^{(M_p-1)/2} = -1$. Aus (80) folgt mit $n = M_p$ und $m = 1$ sofort $2V_{M_p+1} = V_{M_p}V_1 + 12U_{M_p}U_1$ und mit $U_1 = 1$ und $V_1 = a = 2$ daher $V_{M_p+1} = V_{M_p} + 6U_{M_p}$ und somit nach Lemma 3.15 $V_{M_p+1} \equiv 2 + 6 \cdot \left(\frac{12}{M_p}\right) \equiv 2 + 6 \cdot (-1) \equiv -4 \; mod \; M_p$. ◇

Zum Testen von M_p berechnet man also die Folge L_n modulo M_p für $n = 1, 2, \ldots, p-1$ und prüft, ob sich 0 ergibt.

Bemerkung 3.22 Der von Mathematica in der Funktion "PrimeQ[N]" benutzte Primzahltest testet zunächst, ob N den strengen Pseudoprimzahltest für die Basen 2 und 3 besteht. Anschließend wird ein Lucas-Lehmer-Test mit einer geeigneten Lucasfolge durchgeführt. Es ist bekannt, daß keine zusammengesetzte Zahl $N < 10^{16}$ diesen gesamten Test besteht. Für größere N ist dieser Test allerdings nur probabilistisch. Will man dafür eine Primzahl mit Sicherheit nachweisen, muß man einen Zertifikatstest durchführen, der allerdings erheblich länger dauern kann.

3.6 Solovay-Strassen-Test

Dies ist ein probabilistischer Primzahltest. Eine Zahl n, die diesen Test besteht ist lediglich mit einer sehr hohen (vorgebbaren) Wahrscheinlichkeit eine Primzahl. Meist führt man bei derartigen probabilistischen Primzahltest vor dem eigentlichen Test noch Probedivisionen mit "den kleinen Primzahlen" durch, um im Falle eines Irrtums jedenfalls keine kleinen Primteiler zu haben.

Der folgende Primzahltest beruht auf Lemma 2.66 c) und Lemma 2.101.

Man gebe eine Irrtumswahrscheinlichkeit $\varepsilon > 0$ vor, so daß für eine zu testende Zahl n die Aussage "n ist eine Primzahl" nach Ausführung des Algorithmus nur mit höchstens dieser Wahrscheinlichkeit falsch sein darf. Man bestimme $k \in \mathbb{N}$ mit $(\frac{1}{2})^k < \varepsilon$.

Algorithmus 3.23 Solovay-Strassen-Primzahltest

Eingabe: $n > 1$ *ungerade natürliche Zahl,* k

Ausgabe: *entweder "n ist prim" (mit Irrtumswahrscheinlichkeit* $< (\frac{1}{2})^k$*) oder "n ist zusammengesetzt (mit Sicherheit)*

```
for i:=1(1)k do
   waehle zufaellig ein a zwischen 1 und n-1
   ls := a^((n-1)/2) mod n; rs := (a/n) mod n;
   if ls =/= rs then n ist zusammengesetzt, stop
   od
n ist prim, stop
```

3.7 Miller-Rabin-Test

Auch dies ist ein probabilistischer Primzahltest. Er berücksichtigt aber die Carmichael-Zahlen und erreicht daher schneller kleinere Irrtumswahrscheinlichkeiten.

Lemma 3.24 *Es sei p eine ungerade Primzahl und $p-1 = 2^\ell q$ mit ungeradem q. Sei weiter $a \in \mathbb{N}$ mit $ggT(a,p) = 1$ und $b = a^q \ mod\ p$. Dann gilt entweder $b \equiv 1 \ mod\ p$ oder es gibt einen Exponenten $0 \leq k \leq \ell - 1$ mit $b^{2^k} \equiv -1 \ mod\ p$.*

Beweis: Im Fall $b \equiv 1 \ mod\ p$ ist die Behauptung richtig. Gelte also $b^{2^0} = b \not\equiv 1 \ mod\ p$. Nach dem kleinen Fermatschen Satz gilt aber $1 \equiv a^{p-1} = a^{2^\ell q} = b^{2^\ell} \ mod\ p$. Also existiert ein Exponent $0 \leq k \leq \ell - 1$ mit $b^{2^k} \not\equiv 1 \ mod\ p$ und $b^{2^{k+1}} \equiv 1 \ mod\ p$, also $(b^{2^k})^2 \equiv 1 \ mod\ p$. Dann gilt in dem Körper $\mathbb{F}_p$ aber $b^{2^k} \equiv -1 \ mod\ p$. ◇

Der Test beruht nun auf dem von Miller und Rabin bewiesenen Satz:

Satz 3.25 *Die Wahrscheinlichkeit dafür, daß für eine zusammengesetzte Zahl n bei einem zufällig gewählten a mit $ggT(a,n) = 1$ die Aussage des Lemmas 3.24 für $b = a^q$ ebenfalls richtig ist, ist kleiner als $\frac{1}{4}$.*

Den etwas umfangreicheren Beweis dieses Satzes kann man in [10], Proposition V.1.7 oder [13], Satz 8.33 nachlesen.

Man gebe eine Irrtumswahrscheinlichkeit $\varepsilon > 0$ vor, so daß für eine zu testende Zahl n die Aussage "n ist eine Primzahl" nach Ausführung des Algorithmus nur mit höchstens dieser Wahrscheinlichkeit falsch sein darf. Man bestimme $k \in \mathbb{N}$ mit $(\frac{1}{4})^k < \varepsilon$.

k	$(1/4)^k$
10	$< 10^{-6}$
25	$< 10^{-15}$
30	$< 10^{-18}$
50	$< 10^{-30}$
100	$< 10^{-60}$
168	$< 10^{-101}$
1000	$< 10^{-602}$

Algorithmus 3.26 Miller-Rabin-Primzahltest

Eingabe: $n > 1$ *ungerade natürliche Zahl,* k

Ausgabe: *entweder "n ist prim" (mit Irrtumswahrscheinlichkeit* $< (\frac{1}{4})^k$*) oder "n ist zusammengesetzt" (mit Sicherheit)*

```
zerlege n-1=2^l*q mit ungeradem q;
for i:=1(1)k do
   waehle zufaellig ein a zwischen 1 und n-1
     b:= a^q mod n;
     if b=+1 or b=-1 then next i
     else
(1)     b:=b*b;
          if b=-1 then next i
             else if b=1 then n ist zusammengesetzt, stop
                  endif
          endif
        goto (1)
     endif
   endfor
n ist prim, stop
```

4 Primzahlen und Primitivwurzeln

Bei der Erzeugung guter Stromchiffren in der Kryptographie werden (große) Primzahlen p benötigt, zu denen "kleine Elemente" wie $a = 2, 3, 5, \ldots \in \mathbb{F}_p$ Primitivwurzeln modulo p sind oder zumindest eine große Ordnung $ord_p(a)$ in $\mathbb{F}_p^*$ besitzen. In diesem Abschnitt werden einige Ergebnisse über derartige Primzahlen zusammengestellt.

Definition 4.1 Es seien $n, a \in \mathbb{N}$. Falls ein $k \in \mathbb{N}$ mit $a^k \equiv -1 \; mod \; n$ existiert, heißt das kleinste derartige k die *negative Ordnung* von a modulo n, in Zeichen $nord_n(a) = k$.

Natürlich hat jede Primitivwurzel a eine negative Ordnung, da sich $-1 \in (\mathbb{Z}/n\mathbb{Z})^*$ ja als geeignete Potenz a^k darstellen läßt.

Zunächst einige Beispielrechnungen für kleine ungerade Primzahlen:

Beispiel 4.2 Betrachte die Potenzen $\{a, a^2, a^3, \ldots\}$ in $\mathbb{F}_p$.

i) $a = 2$: $p = 3$ $\{2 = -1, 2^2 = 1\}$, also ist 2 Primitivwurzel und $nord_3(2) = 1 = ord_3(2)/2$.

$p = 5$ $\{2, 2^2 = -1, 2^3 = 3 = -2, 2^4 = 1\}$, also ist 2 Primitivwurzel und $nord_5(2) = 2 = ord_5(2)/2$.

$p = 7$ $\{2, 2^2 = 4 = -3, 2^3 = 1\}$, also $ord_7(2) = 3 = (p-1)/2$ und 2 ist keine Primitivwurzel und hat keine negative Ordnung modulo 7.

$p = 11$ $\{2, 2^2 = 4, 2^3 = 8 = -3, 2^4 = 5, 2^5 = -1, 2^6 = -2, 2^7 = -4, 2^8 = 3, 2^9 = 6 = -5, 2^{10} = 1\}$, also ist 2 Primitivwurzel und $nord_{11}(2) = 5 = ord_{11}(2)/2$.

$p = 13$ $\{2, 2^2 = 4, 2^3 = 8 = -5, 2^4 = 3, 2^5 = 6, 2^6 = -1, 2^7 = -2, 2^8 = -4, 2^9 = -8 = 5, 2^{10} = 10 = -3, 2^{11} = -6, 2^{12} = 1\}$, also ist 2 Primitivwurzel und $nord_{13}(2) = 6 = ord_{13}(2)/2$.

$p = 17$ $\{2, 2^2 = 4, 2^3 = 8, 2^4 = -1, \ldots, 2^8 = 1\}$, also $ord_{17}(2) = 8 = (p-1)/2$ und 2 ist keine Primitivwurzel, aber es gilt $nord_{17}(2) = 4 = ord_{17}(2)/2$.

ii) $a = 3$: $p = 5$ $\{3, 3^2 = 4 = -1, 3^3 = -3 = 2, 3^4 = 1\}$, also ist 3 Primitivwurzel und $nord_5(3) = 2 = ord_5(3)/2$.

$p = 7$ $\{3, 3^2 = 2, 3^3 = 6 = -1, 3^4 = -3, 3^5 = -2, 3^6 = 1\}$, also ist 3 Primitivwurzel und $nord_7(3) = 3 = ord_7(3)/2$.

$p = 11$ $\{3, 3^2 = 9 = -2, 3^3 = -6 = 5, 3^4 = 4, 3^5 = 1\}$, also ist $ord_{11}(3) = 5 = (p-1)/2$ und 3 ist keine Primitivwurzel und hat keine negative Ordnung modulo 11.

Satz 4.3 *Es sei $n \in \mathbb{N}$. Falls eine natürliche Zahl a mit $1 \leq a \leq n-1$ und $ggT(a,n) = 1$ eine negative Ordnung modulo n besitzt, so gilt $ord_n(a) = 2nord_n(a)$.*

Beweis: Aus $a^{nord_n(a)} \equiv -1 \; mod \; n$ folgt $a^{2nord_n(a)} \equiv 1 \; mod \; n$, also $ord_n(a) \mid 2nord_n(a)$. Zeige $ord_n(a) \geq 2nord_n(a)$. Andernfalls würde $2nord_n(a) > ord_n(a) > nord_n(a)$ oder sogar $nord_n(a) > ord_n(a)$ gelten. Mit $k = ord_n(a) - nord_n(a)$ im ersten und $k = nord_n(a) - ord_n(a)$ im zweiten Fall wäre $1 \leq k < nord_n(a)$ und $a^k \equiv -1 \; mod \; n$ im Widerspruch zur Minimalität von $nord_n(a)$. ◇

Lemma 4.4 *Gilt $a^k \equiv -1 \; mod \; n$ für ein $k \in \mathbb{N}$, so gilt $nord_n(a) \mid k$ und $k/nord_n(a)$ ist ungerade.*

Beweis: Sei $k = h \cdot nord_n(a) + \ell$ mit $0 \leq \ell < nord_n(a)$. Aus $a^k \equiv (a^{nord_n(a)})^h a^\ell \; mod \; n$ folgt $a^\ell \equiv (-1)^{h+1} \; mod \; n$. Wegen $\ell < nord_n(a)$ und der Minimalität von $nord_n(a)$ muß h ungerade sein. Angenommen, $\ell > 0$. Dann zeigt $a^\ell \equiv 1 \; mod \; n$ bereits $ord_n(a) \leq \ell < nord_n(a)$, einen Widerspruch zu Satz 4.3. Also gilt $\ell = 0$ und damit die Behauptung. ◇

Satz 4.5 *Es sei $n > 4$ eine natürliche Zahl, so daß in $(\mathbb{Z}/n\mathbb{Z})^*$ ein primitives Element existiert. Genau dann ist a eine Primitivwurzel modulo n, wenn $nord_n(a) = \varphi(n)/2$ gilt.*

Beweis: Da eine Primitivwurzel modulo n existiert und wegen $n > 4$ gilt nach Satz 5.7 $n = p^k$ oder $n = 2p^k$ für eine ungerade Primzahlpotenz p^k. Dann ist aber $\varphi(n) = p^{k-1}(p-1)$ gerade. Daher läßt sich $a^{\varphi(n)} \equiv 1 \; mod \; n$ zerlegen gemäß

$$(a^{\varphi(n)/2} + 1)(a^{\varphi(n)/2} - 1) \equiv 0 \; mod \; n.$$

Wenn a Primitivwurzel ist, kann nicht schon $a^{\varphi(n)/2} \equiv 1 \; mod \; n$ gelten. Also muß $a^{\varphi(n)/2} \equiv -1 \; mod \; n$ sein und damit die negative Ordnung von a modulo n existieren. Wegen $ord_n(a) = \varphi(n)$ folgt mit Satz 4.3 $nord_n(a) = \varphi(n)/2$.

Umgekehrt folgt aus $nord_n(a) = \varphi(n)/2$ mit Satz 4.3 sofort $ord_n(a) = \varphi(n)$, und damit ist a erzeugendes Element von $(\mathbb{Z}/n\mathbb{Z})^*$. ◇

4.1 Der Fall 2 modulo q

Lemma 4.6 *Sind p und $q = 4p + 1$ ungerade Primzahlen, also p eine Stern-Primzahl, dann ist 2 eine Primitivwurzel modulo q.*

Beweis: Da $p = 2k + 1$ ungerade ist, gilt $q = 8k + 5 > 11$, also $q \equiv -3 \; mod \; 8$. Also ist 2 nach Satz 2.88 ein quadratischer Nicht-Rest modulo q und hat eine negative Ordnung $nord_q(2) \mid (q-1)/2 = 2p$. Wegen $q > 11$ ist $2^2 = 4 \neq -1$ und daher $nord_q(2) \neq 2$. Auch $nord_q(2) = p$ würde zu $-1 \equiv 2^p \; mod \; q$ und damit zu $1 \equiv 2^{2p} = 2^{(q-1)/2} \equiv -1 \; mod \; q$ führen, was wegen $q \neq 2$ nicht richtig ist. Also gilt $nord_q(2) = 2p = (q-1)/2 = \varphi(q)/2$. Mit Satz 4.5 folgt die Behauptung. ◇

Beispiel 4.7 Einige kleine Werte für Stern-Primzahlen $q = 4p + 1$ erhält man für $p = 3, 7, 13, 37, 43, 67, 73, 79, 97, 127, 139, 163, 193, 199$. Von diesen sind alle bis auf $p = 3$ auch kongruent 1 modulo 3 (vgl. Lemma 4.14).

Lemma 4.8 *Sind $p = 2k-1$ und $q = 4k-1$ ungerade Primzahlen mit ungeradem k, also p eine Germain-Primzahl, dann ist 2 eine Primitivwurzel modulo q.*

Beweis: Mit ungeradem $k = 2m + 1$ gilt $q = 4(2m + 1) - 1 = 8m + 3$, also $q \equiv 3 \; mod \; 8$. Wiederum nach Satz 2.88 ist 2 quadratischer Nicht-Rest modulo q und hat eine negative Ordnung $nord_q(2) \mid (q-1)/2 = (4k-2)/2 = p$. Es folgt $nord_q(2) = p = (q-1)/2 = \varphi(q)/2$, also mit Satz 4.5 die Behauptung. ◇

Beispiel 4.9 Einige kleine Werte für Germain-Primzahlen dieser Art erhält man für $p = 5, 29, 41, 53, 89$. Alle diese Primzahlen p sind kongruent 1 modulo 4 (vgl. Satz 4.21). Es ist $p = 3 = 2k - 1$ mit geradem k und $q = 4k - 1 = 7$, also p ebenfalls eine Germain-Primzahl. Aber 2 ist keine Primitivwurzel modulo 7. Dasselbe gilt mit der Germain-Primzahl $p = 11 = 2k - 1$ für $k = 6$ und $q = 23$.

Lemma 4.10 *a) Ist $q = 4k + 1$ und k ungerade mit der Primfaktorzerlegung $k = p_1 p_2$, so ist 2 genau dann eine Primitivwurzel modulo q, wenn gilt*

$$2^{2p_1p_2} \equiv -1 \; mod \; q, 2^{2p_1} \not\equiv -1 \; mod \; q, 2^{2p_2} \not\equiv -1 \; mod \; q.$$

b) Ist $q = 4k - 1$ und k ungerade und gilt die Primfaktorzerlegung $2k - 1 = p_1 p_2$, so ist 2 genau dann eine Primitivwurzel modulo q, wenn gilt

$$2^{p_1p_2} \not\equiv 1 \; mod \; q, 2^{p_1} \not\equiv -1 \; mod \; q, 2^{p_2} \not\equiv -1 \; mod \; q.$$

Beweis: a) Nach Voraussetzung existiert $nord_q(2)$ und teilt $2p_1p_2$, aber weder $2p_1$ noch $2p_2$. Also gilt $nord_q(2) = 2p_1p_2$. Da $ord_q(2) = 2nord_q(2)$ ein Teiler von $\varphi(q) = q - 1 = 4p_1p_2$ ist, kann nur Gleichheit gelten, woraus mit Satz 4.5 die Behauptung folgt.

b) Analog. ◇

Beispiel 4.11 a) Für $k = 3 \cdot 5$ ist $q = 4k + 1 = 61$ eine Primzahl, für die 2 Primitivwurzel ist. Es ist nämlich $2^{30} = 1073741824 \equiv -1, 2^6 = 64 \equiv 3, 2^{10} = 1024 \equiv 48$ modulo 61.

Für $k = 3 \cdot 13$ ist $q = 4k+1 = 157$ eine Primzahl, für die 2 keine Primitivwurzel ist, da 5 die kleinste Primitivwurzel modulo 157 ist. Es ist nämlich $2^{26} = 67108864 \equiv -1$ modulo 157.

b) Für $k = (3 \cdot 5 + 1)/2 = 8$ ist $q = 4k - 1 = 31$ eine Primzahl, für die 2 keine Primitivwurzel ist, da 3 die kleinste Primitivwurzel modulo 31 ist. Es ist nämlich $2^{15} = 32768 \equiv 1$ modulo 31.

Für $k = (3 \cdot 11 + 1)/2 = 17$ ist $q = 4k - 1 = 67$ eine Primzahl, für die 2 Primitivwurzel ist. Es ist nämlich $2^{33} = 8589934592 \equiv -1, 2^3 = 8, 2^{11} = 2048 \equiv 38$ modulo 67.

4.2 Der Fall 3 modulo q

Lemma 4.12 *a) Es sei $p = 4t + 1$ prim. Ist 3 eine Primitivwurzel modulo p, dann gilt $t = 3k + 1$ für ein $k \in \mathbb{N}_0$, also $p = 12k + 5$.*

b) Es sei $p = 4t - 1$ prim. Ist 3 eine Primitivwurzel modulo p, dann gilt $t = 3k + 2$ für ein $k \in \mathbb{N}_0$, also $p = 12k + 7$.

Beweis: a) Im Fall $t = 3k + 2$ würde $p = 12k + 9 = 3(4k + 3)$ folgen, also p keine Primzahl sein. Im Fall $t = 3k$ gilt

$$\left(\frac{3}{p}\right) = (-1)^{(3-1)/2\cdot(p-1)/2}\left(\frac{p}{3}\right) = (-1)^{2t}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \left(\frac{12k+1}{3}\right) = 1.$$

Als quadratischer Rest kann 3 daher keine Primitivwurzel sein. Also bleibt nur der Fall $t = 3k + 1$ wie behauptet.

b) Im Fall $t = 3k + 1$ würde $p = 12k + 3 = 3(4k + 1)$ folgen, also p keine Primzahl sein. Im Fall $t = 3k$ gilt

$$\left(\frac{3}{p}\right) = (-1)^{(3-1)/2\cdot(p-1)/2}\left(\frac{p}{3}\right) = (-1)^{2t-1}\left(\frac{p}{3}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{12k-1}{3}\right) = 1.$$

Als quadratischer Rest kann 3 daher keine Primitivwurzel sein. Also bleibt nur der Fall $t = 3k + 2$ wie behauptet. ◇

Bemerkung 4.13 a) Laut Anhang ist 6 kleinste Primitivwurzel modulo $p = 41 = 4 \cdot 10 + 1$ und $t = 10 = 3 \cdot 3 + 1$. Die Bedingung $p = 4t + 1$ und $t = 3k + 1$ ist also nicht hinreichend dafür, daß 3 eine Primitivwurzel modulo p ist.

b) Laut Anhang ist 5 kleinste Primitivwurzel modulo $p = 103 = 4 \cdot 26 - 1$ und $t = 26 = 3 \cdot 8 + 2$. Die Bedingung $p = 4t - 1$ und $t = 3k + 2$ ist also nicht hinreichend dafür, daß 3 eine Primitivwurzel modulo p ist.

Lemma 4.14 (Stern, 1830) *Ist $p \equiv 1$ mod 3 Primzahl und $q = 4p+1$ ebenfalls, also p eine Stern-Primzahl, so ist 3 Primitivwurzel modulo q.*

Beweis: Es ist nach dem Euler-Kriterium und dem Quadratischen Reziprozitätsgesetz

$$3^{(q-1)/2} \equiv \left(\frac{3}{q}\right) = (-1)^{(3-1)/2 \cdot (q-1)/2} \left(\frac{q}{3}\right) = (-1)^{2p} \left(\frac{q}{3}\right) = \left(\frac{q}{3}\right)$$

und weiter wegen $4p + 1 \equiv p + 1 \equiv 2$ *mod* 3

$$\left(\frac{q}{3}\right) = \left(\frac{4p+1}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{(9-1)/8} = -1.$$

Daher ist 3 quadratischer Nicht-Rest modulo q und hat eine negative Ordnung $nord_q(3) \mid (q-1)/2 = 2p$. Wegen $p > 3$ gilt $q = 4p + 1 > 13$ und daher $3^2 = 9 \not\equiv -1$ *mod* q. Auch $nord_q(3) = p$ würde zu $-1 \equiv 3^p$ *mod* q und damit zu $1 \equiv 3^{2p} \equiv 3^{(q-1)/2} \equiv -1$ *mod* q führen. Daher bleibt nur $nord_q(3) = (q-1)/2 = \varphi(q)/2$, was mit Satz 4.5 die Behauptung liefert. ◇

Satz 4.15 *Sei $q = 4t + 1$ Primzahl mit $t = 3k + 1 = 2^m t'$ und t' ungerade. Dann gilt $ord_q(3) = 2^{m+2} t_1$ für einen Teiler $t_1 \mid t'$.*

Für Primzahlen t' folgt:

Folgerung 4.16 *Sei $q = 4t + 1$ Primzahl mit $t = 3k + 1 = 2^m t'$ und t' ungerade Primzahl. Gilt $3^{2^{m+1}} \not\equiv -1$ mod q, so ist 3 eine Primitivwurzel modulo p.*

Folgerung 4.17 (Tschebyscheff, 1849) *Sei $q = 4t + 1$ Primzahl mit $t = 3k + 1 = 2^m t'$ und $t' > 3^{2^{m+1}}/2^{m+2}$ ungerade Primzahl. Dann ist 3 eine Primitivwurzel modulo $q = 4t'2^m + 1$.*

Beweis: Wegen $t' > 3^{2^{m+1}}/2^{m+2}$ ist $q > 3^{2^{m+1}} + 1$ und daher $3^{2^{m+1}} \not\equiv -1 \; mod \; q$. ◇

Definition 4.18 Eine Primzahl $q = 4t + 1$ mit $t = 3k + 1 = 2^m t'$ und $t' > 3^{2^{m+1}}/2^{m+2}$ prim heißt eine *Tschebyscheff-Primzahl.*

Folgerung 4.19 *Ist $q = 4t - 1$ prim mit $t = 3k + 2$ und $p = 2k + 1$ prim, so ist 3 genau dann eine Primitivwurzel modulo q, wenn gilt*

$$3^p \not\equiv -1 \; mod \; q, \; 3^{3p} \not\equiv 1 \; mod \; q.$$

4.3 Primitivwurzeln bei speziellen Primzahlen

Für Germain-Primzahlen hat man folgende Resultate.

Satz 4.20 *Es sei p eine Germain-Primzahl und $q = 2p + 1$. Dann gilt für jedes Element $2 \leq a \leq q - 2$ aus $\mathbb{F}_q$ schon $ord_q(a) = q - 1$ oder $ord_q(a) = (q - 1)/2$.*

Beweis: Da $ord_q(a)$ die Gruppenordnung $q - 1 = 2p$ teilt, kann diese Ordnung nur $2, p = (q - 1)/2$ oder $2p = q - 1$ sein. Wegen $a + 1 \neq 0$ und $a - 1 \neq 0$ in $\mathbb{F}_q$ folgt mit der Nullteilerfreiheit $a^2 \not\equiv 1 \; mod \; q$, d. h. $ord_q(a) \neq 2$. ◇

Satz 4.21 *Sei p eine Germain-Primzahl und $q = 2p + 1$.*

a) 2 ist Primtivwurzel modulo q genau dann, wenn $p \equiv 1 \; mod \; 4$ gilt.

b) Für $q > 7$ ist 3 keine Primitivwurzel modulo q.

c) 5 ist Primitivwurzel modulo q genau dann, wenn $p \equiv 1 \; mod \; 10$ oder $p \equiv 3 \; mod \; 10$ gilt.

d) 7 ist Primitivwurzel modulo q genau dann, wenn $p \equiv 5 \; mod \; 14$ oder $p \equiv 5 \; mod \; 11$ gilt.

Bemerkung 4.22 a) Für kleine Germain-Primzahlen $p \equiv 1 \; mod \; 4$ ist 2 Primitivwurzel modulo $q = 2p + 1$ für $p = 29, 41, 53, 89$.

b) Bei $q = 7$ ist 3 kleinste Primitivwurzel modulo 7.

c) Für $p = 11, 23, 83$ ist 5 kleinste Primitivwurzel modulo $q = 2p + 1$. Dies ist aber auch bei $q = 73, 97, 103, 157, 193$ der Fall, die alle keine Germain-Primzahlen sind.

d) Für $p = 179$ ist 7 kleinste Primitivwurzel modulo $q = 359$. Dies ist aber schon bei $q = 71, 239, 241$ der Fall, die alle keine Germain-Primzahlen sind.

Für Tschebyscheff-Primzahlen sind die folgenden Aussagen bekannt.

Satz 4.23 *In den folgenden Fällen ist* 3 *Primitivwurzel modulo* q*.*

a) Es sind $p > 11$ *und* $q = 8p + 1$ *prim.*

b) Es sind $p > 411$ *und* $q = 16p + 1$ *prim.*

c) Es sind $p > 1345211$ *und* $q = 32p + 1$ *prim.*

Forschungsproblem: Ist für eine der beiden Primzahlen $p = 114(2^{127} - 1) + 1$ bzw. $180(2^{127})^2 + 1$ die Zahl 2 eine Primitivwurzel modulo p?

4.4 Primitivwurzeln bei Primzahlzwillingen

Definition 4.24 Sind p und $p+2$ Primzahlzwillinge mit $p = 4k-1$ und $p+2 = 4k+1$, so haben sie *dasselbe Geschlecht*, andernfalls verschiedenes Geschlecht.

Bemerkung 4.25 Haben also $p = 4k-1$ und $p+2 = 4k+1$ dasselbe Geschlecht und ist k gerade, so gilt $\left(\frac{2}{p}\right) = 1 = \left(\frac{2}{p+2}\right)$, d. h. 2 ist für beide Primzahlen quadratischer Rest und damit für keine der beiden eine Primitivwurzel. Ist dagegen in diesem Fall k ungerade, so kann 2 für beide gleichzeitig eine Primitivwurzel sein.

Haben dagegen p und $p + 2$ verschiedenes Geschlecht, so gilt $p = 4k + 1$ und $p + 2 = 4k + 3 = 4(k + 1) - 1$, d. h. genau für eine der beiden Primzahlen ist 2 quadratischer Rest, für die andere quadratischer Nicht-Rest. Für höchstens eine von ihnen kann daher 2 Primitivwurzel sein.

Für die folgenden Probleme vgl. [3], 5.6.5 - 5.6.8.

Forschungsproblem: Finde große Primzahlzwillinge mit gemeinsamer Primitivwurzel 2.

Forschungsproblem: Finde Kriterien dafür, daß von zwei Primzahlzwillingen mit unterschiedlichem Geschlecht für eine der Primzahlen 2 eine Primitivwurzel ist.

Forschungsproblem: Finde große Primzahlzwillinge $(p, p+2)$ für die $ord_p(2)$ und $ord_{p+2}(2)$ groß sind.

Forschungsproblem: Untersuche diese Fragen speziell für die Primzahlzwillinge $1639494 \cdot (2^{4423} - 1) \pm 1$ und $2445810 \cdot (2^{4253} - 1) \pm 1$.

Satz 4.26 *Seien p und $p+2$ Primzahlzwillinge.*

a) Gilt $p \equiv 1$ mod 4, dann kann 3 gemeinsame Primitivwurzel von ihnen sein, andernfalls nicht.

b) Gilt $p \equiv -1$ mod 4, dann ist für keine von beiden Primzahlen 3 Primitivwurzel.

Bemerkung 4.27 Für $p = 71$ ist 7 kleinste Primitivwurzel modulo 71 und für $p + 2 = 73$ ist 5 kleinste Primitivwurzel modulo 73.

Forschungsproblem: a) Welcher Bruchteil aller Primzahlzwillinge hat 3 als gemeinsame Primitivwurzel?

b) Finde große Primzahlzwillinge mit gemeinsamer Primitivwurzel 3.

c) Finde große Primzahlzwillinge p und $p+2$, so daß $ord_p(3)$ und $ord_{p+2}(3)$ groß sind.

5 Algebraische Hilfsmittel

In diesem Abschnitt sind ohne Beweise einige fundamentale Sätze der Algebra zusammengestellt, die im Skript an verschiedenen Stellen benutzt werden. Diese Aussagen werden in der Vorlesung "Klassische Algebra" bewiesen.

Satz 5.1 *Ist $(S, \cdot, e)$ ein Monoid, so ist $U = \{a \in S \mid$ es gibt ein $b \in S$ mit $ab = e = ba\}$ eine Untergruppe von $(S, \cdot, e)$, die Gruppe der Einheiten von $(S, \cdot, e)$. Man schreibt $U = S^*$.*

Satz 5.2 *Ist $(G, \cdot)$ eine endliche Gruppe der Ordnung $n = |G|$, so gilt $a^n = e$ für jedes $a \in G$ und das Einselement e von $(G, \cdot)$.*

Gilt $a^k = e$ für ein $a \neq e$ aus G, so folgt $k \mid n$.

Satz 5.3 *Es sei $(S, *, e)$ ein Monoid, $a \in S$ und $n \in \mathbb{N}_0$. Der folgende Algorithmus berechnet a^n in höchstens $1 + \log_2(n)$ Multiplikationen.*

Algorithmus 5.4 **Quadrieren und Multiplizieren**

Eingabe: $a \in S$, $n \in \mathbb{N}_0$

Ausgabe: $P = a^n$

```
P:=e;
if n > 0 then
   b:=a; t:=n;
   while t > 1 do
      if t ungerade then P:=P*b endif
      b:= b*b; t:= [t/2];
      od
   P:=P*b;
   endif
P, stop
```

Satz 5.5 *Es sei $(R, +, \cdot)$ ein Ring. Dann gelten für alle $a, b \in R$*

$0 \cdot a = 0 = a \cdot 0$,

$(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,

$(-a) \cdot (-b) = a \cdot b$.

Satz 5.6 *Zu jeder Primzahlpotenz $q = p^k$ für $p \in \mathbb{P}$ und $k \in \mathbb{N}$ gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ mit q Elementen. Seine multiplikative Gruppe $\mathbb{F}_q^*$ ist zyklisch. Jedes erzeugende Element dieser zyklischen Gruppe heißt ein primitives Element von $\mathbb{F}_q$ oder eine Primitivwurzel modulo q. Ist g ein erzeugendes Element von $\mathbb{F}_q^*$, so ist g^k genau dann ebenfalls ein erzeugendes Element, wenn $ggT(k, q-1) = 1$ gilt. Insbesondere existieren genau $\varphi(q-1)$ verschiedene erzeugende Elemente von $\mathbb{F}_q^*$.*

Satz 5.7 *Die prime Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ ist genau für $n = 1, 2, 4$ und $n = p^k, 2p^k$ für ungerade Primzahlen p und $k \in \mathbb{N}$ zyklisch, besitzt also eine Primitivwurzel modulo n.*

Satz 5.8 *Zu Polynomen $a(x), b(x) \in K[x]$ über einem Körper K mit $b(x) \neq 0$ existieren Polynome $q(x), r(x) \in K[x]$ mit $a(x) = q(x)b(x) + r(x)$ und $r(x) = 0$ oder $grad(r(x)) < grad(b(x))$.*

Satz 5.9 *Ist $f(x) \in K[x]$ ein Polynom über einem Körper K vom Grad $n \geq 1$, so hat $f(x)$ in jedem Erweiterungskörper E von K höchstens n Nullstellen.*

Satz 5.10 *Ein Polynom $f(x) \in K[x]$ vom Grad m über einem Primkörper $K = \mathbb{Z}/(p)$ vom ist genau dann irreduzibel, wenn $\mathrm{ggT}(f(x), x^{p^k} - x) = 1$ für jedes $k \in \{1, \ldots, [\frac{m}{2}]\}$ gilt.*

6 Lösungen zu ausgewählten Aufgaben

Lösung 6.1 zu Aufgabe 1.6 a) Für beliebige $m, n \in \mathbb{N}_0$ betrachte $N = \{\ell \in \mathbb{N}_0 \mid (n+m)+\ell = n+(m+\ell)\}$. Dann ist $N = \mathbb{N}_0$ zu zeigen.

Wegen (1) gilt jedenfalls $0 \in N$. Sei also $\ell \in N$. Dann folgt mit (2) $(n+m)+\ell' = ((n+m)+\ell)' = (n+(m+\ell))' = n+(m+\ell)' = n+(m+\ell')$, also auch $\ell' \in N$. Mit (P5) erhält man $N = \mathbb{N}_0$.

b) Es sei $N = \{n \in \mathbb{N}_0 \mid n+0 = n = 0+n\}$. Dann ist $N = \mathbb{N}_0$ zu zeigen. Wegen (1) gilt jedenfalls $0+0 = 0$, also $0 \in N$.

Gelte nun $n \in N$ für irgend eine natürliche Zahl n, also insbesondere $0+n = n$. Aus (2) folgt dann aber $0+n' = (0+n)' = n'$ und $n'+0 = n'$ gilt wegen (1) in jedem Fall. Damit hat man aber auch $n' \in N$ und mit (P5) folgt $N = \mathbb{N}_0$.

c) Sei m eine beliebige natürliche Zahl und $N = \{n \in \mathbb{N}_0 \mid n+m = m+n\}$. Nach b) gilt jedenfalls $0 \in N$. Gelte nun $n \in N$ für eine natürliche Zahl n. Dann folgt $n'+m = n+m' = (n+m)' = (m+n)' = m+n'$ nach Lemma 1.5 und (2). Also gilt auch $n' \in N$ und mit (P5) folgt $N = \mathbb{N}_0$.

d) Betrachte $N = \{k \in \mathbb{N}_0 \mid n+k = m+k \Longrightarrow n = m \text{ für alle } n, m \in \mathbb{N}_0\}$. Wiederum ist $0 \in N$ offensichtlich. Gelte also $k \in N$ und $n+k' = m+k'$, also $(n+k)' = (m+k)'$ wegen (2). Nun liefert (P3) $n+k = m+k$ und $k \in N$ schließlich $n = m$. Also gilt auch $k' \in N$ und mit (P5) folgt $N = \mathbb{N}_0$.

e) Sei $m \in \mathbb{N}$ beliebig. Wir nehmen an, daß $N = \{n \in \mathbb{N} \mid m+n = 0\}$ nicht leer ist. Dann existiert nach Satz 1.13 ein kleinstes Element $n \in N \subseteq \mathbb{N}$. Also gibt es ein $k \in \mathbb{N}_0$ mit $n = k'$. Es folgt $m+k = \ell \neq 0$, da k kleiner ist als n. Hieraus ergibt sich $0 = m+n = m+k' = (m+k)' = \ell'$ im Widerspruch zu (P4).

Lösung 6.2 zu Aufgabe 1.7 Seien $m, n \in \mathbb{N}_0$ beliebig und $N = \{k \in \mathbb{N}_0 \mid (n+m)\cdot k = n\cdot k + m\cdot k\}$. Dann gilt wegen (3) und (1) jedenfalls $0 \in N$. Für $k \in N$ folgt mit (4) und Aufgabe 1.6 $(n+m)\cdot k' = (n+m)\cdot k + (n+m) = n\cdot k + n + m\cdot k + m = n\cdot k' + m\cdot k'$, also auch $k' \in N$. Mit (P5) folgt $N = \mathbb{N}_0$.

Das zweite Distributivgesetz folgt dann aus der Kommutativität der Multiplikation gemäß Aufgabe 1.8.

Lösung 6.3 zu Aufgabe 1.8 a) Betrachte $N = \{n \in \mathbb{N}_0 \mid 0\cdot n = 0 = n\cdot 0\}$. Wegen (1) gilt dann $0 \in N$. Sei also $n \in N$. Dann gilt $0\cdot n' = 0\cdot n + 0 = 0\cdot n = 0 = 0\cdot n'$, also auch $n' \in N$. Mit (P5) folgt $N = \mathbb{N}_0$.

b) Jedenfalls gilt $n \cdot 1 = n \cdot 0' = n \cdot 0 + n = 0 + n = n$ für alle $n \in \mathbb{N}_0$. Sei $N = \{n \in \mathbb{N}_0 \mid 1 \cdot n = n\}$. Wegen $1 \cdot 0 = 0$ gilt jedenfalls $0 \in N$. für $n \in N$ folgt $1 \cdot n' = 1 \cdot n + 1 = n + 1 = n'$, also auch $n' \in N$. Mit (P5) folgt $N = \mathbb{N}_0$.

c) Sei $m \in \mathbb{N}_0$ beliebig. Betrachte $N = \{n \in \mathbb{N}_0 \mid n \cdot m = m \cdot n\}$. Dann gilt jedenfalls $0 \in N$. Für $n \in N$ folgt mit dem rechtsseitigen Distributivgesetz $n' \cdot m = (n + 1) \cdot m = n \cdot m + 1 \cdot m = m \cdot n + m = m \cdot n'$.

d) Es seien $n, m \in \mathbb{N}_0$ beliebig. Betrachte $N = \{\ell \in \mathbb{N}_0 \mid (n \cdot m) \cdot \ell = n \cdot (m \cdot \ell)\}$. Jedenfalls gilt $0 \in N$. Für $\ell \in N$ folgt $(n \cdot m) \cdot \ell' = (n \cdot m) \cdot \ell + n \cdot m = n \cdot (m \cdot \ell) + n \cdot m = n \cdot (m \cdot \ell + m) = n \cdot (m \cdot \ell')$, also auch $\ell' \in N$. (P5) zeigt nun $N = \mathbb{N}_0$.

e) Angenommen, es ist $0 = n \cdot m$ für $n, m \in \mathbb{N}$. Dann existiert ein $k \in \mathbb{N}_0$ mit $m = k'$, also $0 = n \cdot k' = n \cdot k + n$. Aus Aufgabe 1.6 e) folgt dann der Widerspruch $n = 0$.

f) Es sei $k \in \mathbb{N}$. Angenommen, es gibt $n \neq m$ in $\mathbb{N}_0$ mit $n \cdot k = m \cdot k$. Es darf $n \leq m$ angenommen werden (vgl. Aufgabe 1.10). Also existiert ein $\ell \in \mathbb{N}$ mit $m = n + \ell$. Es folgt $n \cdot k + 0 = n \cdot k = m \cdot k = (n + \ell) \cdot k = n \cdot k + \ell \cdot k$. Aus der Kürzbarkeit der Addition folgt $\ell \cdot k = 0$. Dies steht im Widerspruch zu e), wegen $k, \ell \in \mathbb{N}$.

Lösung 6.4 zu Aufgabe 1.9 (8): Seien $a, n \in \mathbb{N}_0$. Betrachte $N = \{m \in \mathbb{N}_0 \mid a^n \cdot a^m = a^{n+m}\}$. Wegen $a^0 = 1$ gilt jedenfalls $0 \in N$. Für $m \in N$ folgt $a^n \cdot a^{m'} = a^n \cdot (a^m \cdot a) = (a^n \cdot a^m) \cdot a = a^{n+m} \cdot a = a^{(n+m)'} = a^{n+m'}$, also auch $m' \in N$. Mit (P5) folgt $N = \mathbb{N}_0$.

(9): Seien $a, b \in \mathbb{N}_0$. Betrachte $N = \{n \in \mathbb{N}_0 \mid (a \cdot b)^n = a^n \cdot b^n\}$. Wegen $(a \cdot b)^0 = 1 = 1 \cdot 1 = a^0 \cdot b^0$ gilt $0 \in N$. Für $n \in N$ folgt $(a \cdot b)^{n'} = (a \cdot b)^n \cdot a \cdot b = a^n \cdot b^n \cdot a \cdot b = a^n \cdot a \cdot b^n \cdot b = a^{n'} \cdot b^{n'}$, also auch $n' \in N$. Mit (P5) folgt $N = \mathbb{N}_0$.

(10): Seien $a, n \in \mathbb{N}_0$. Betrachte $N = \{m \in \mathbb{N}_0 \mid (a^n)^m = a^{n \cdot m}\}$. Wegen $(a^n)^0 = a^0$ gilt $0 \in N$. Für $m \in N$ folgt $(a^n)^{m'} = (a^n)^m \cdot a^n = a^{n \cdot m} \cdot a^n = a^{n \cdot m + n} = a^{n \cdot m'}$, also auch $m' \in N$. Mit (P5) folgt $N = \mathbb{N}_0$.

Lösung 6.5 zu Aufgabe 1.10 Wegen $n + 0 = n$ gilt $n \leq n$, also ist $\leq$ reflexiv.

Gelte $n \leq m$ und $m \leq n$. Dann existieren $k, \ell \in \mathbb{N}_0$ mit $n + k = m$ und $m + \ell = n$, also $n + k + \ell = n = n + 0$. Aus der Kürzbarkeit der Addition folgt $k + \ell = 0$. Aufgabe 1.6 e) zeigt nun $k = \ell = 0$, also $n = m$. Daher ist $\leq$ antisymmetrisch.

Gelte $n \leq m$ und $m \leq \ell$, also $n + k_1 = m$ und $m + k_2 = \ell$. Dann folgt $n + (k_1 + k_2) = (n + k_1) + k_2 = m + k_2 = \ell$, also auch $n \leq \ell$. Damit ist $\leq$ auch transitiv.

Wegen $0+n=n$ für alle $n \in \mathbb{N}_0$ ist 0 kleinstes Element in $(\mathbb{N}_0, \leq)$.

Wegen $n \leq n+1$ und $n \neq n+1$ ist kein $n \in \mathbb{N}_0$ größtes Element.

Sei nun $m \in \mathbb{N}_0$ beliebig. Angenommen, die Menge $N = \{n \in \mathbb{N}_0 \mid \text{es gilt weder } m \leq n \text{ noch } n \leq m\}$ sei nicht leer. Dann gibt es nach Satz 1.13 ein kleinstes Element $n \in N$. Natürlich ist $n \neq 0$, da $0 \leq m$ gilt. Also gilt $n = k+1$ für ein $k \in \mathbb{N}_0$, insbesondere also $k \leq n$. Hieraus folgt $k \notin N$, da n kleinstes Element von N ist. Also gilt $k \leq m$ oder $m \leq k$. Aus $m \leq k \leq n$ würde der Widerspruch $n \notin N$ folgen. Es muß also $k \leq m$ und $k \neq m$ gelten, d. h. es gibt ein $\ell \in \mathbb{N}$ mit $k+\ell = m$. Daher gibt es ein $p \in \mathbb{N}_0$ mit $\ell = p'$. Es folgt $m = k+p' = k+1+p = n+p$, also $n \leq m$, ebenfalls ein Widerspruch. Also ist N leer.

Nachweis der Monotoniebehauptungen:

Aus $n \leq m$ folgt $m = n+\ell$ für ein $\ell \in \mathbb{N}_0$ und damit weiter $m+k = n+\ell+k = n+k+\ell$ also auch $n+k \leq m+k$ sowie $m \cdot k = (n+\ell)\cdot k = n\cdot k + \ell \cdot k$ also auch $n \cdot k \leq m \cdot k$.

Lösung 6.6 zu Aufgabe 1.16 a) Wegen $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$ ist $\binom{n}{n} = \binom{n}{0} = \frac{n!}{0!n!} = \frac{1}{0!} = 1$.

Es ist $\binom{n}{m} = \frac{n!}{m!(n-m)!} = \frac{n!}{m!} \cdot \frac{n-m+1}{(n-m+1)!}$ und $\binom{n}{m-1} = \frac{n!}{(m-1)!(n-m+1)!} = \frac{n!}{m!}\frac{m}{(n-m+1)!}$ Die Summe ist also $\frac{n!}{m!(n+1-m)!} \cdot n - m + 1 + m = \frac{(n+1)!}{m!(n+1-m)!} = \binom{n+1}{m}$.

b) Für $n=2$ gilt $2^2 = 4 < 6 = \frac{4\cdot 3}{2} = \binom{4}{2}$.

Aus $2^n < \binom{2n}{n}$ folgt dann $\binom{2(n+1)}{n+1} = \frac{(2n+2)(2n+1)(2n)!}{(n+1)n!(n+1)n!} = 2\frac{2n+1}{n+1}\binom{2n}{n} > 2\cdot 2^n = 2^{n+1}$, womit die Aussage für alle $n > 1$ richtig ist.

Lösung 6.7 zu Aufgabe 1.17 Für $n=0$ ist wegen $(a+b)^0 = 1 = \binom{0}{0} a^0 b^0$ die Behauptung richtig. Sei sie für ein $n \in \mathbb{N}_0$ richtig. Dann folgt

$$(a+b)^{n+1} = (a+b)^n \cdot (a+b) = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}.$$

Nun ist aber nach Aufgabe 1.16

$$\begin{aligned}
&\sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k}+\sum_{k=0}^{n}\binom{n}{k}a^{k}b^{n+1-k}\\
=\;&\sum_{k=1}^{n+1}\binom{n}{k-1}a^{k}b^{n+1-k}+\sum_{k=0}^{n}\binom{n}{k}a^{k}b^{n+1-k}\\
=\;&a^{n+1}+\sum_{k=1}^{n}\left\{\binom{n}{k-1}+\binom{n}{k}\right\}a^{k}b^{n+1-k}+b^{n+1}\\
=\;&\sum_{k=0}^{n+1}\binom{n+1}{k}a^{k}b^{n+1-k}.
\end{aligned}$$

a) Dies ergibt sich unmittelbar mit $a = b = 1$.

b) Dies ergibt sich ebenso mit $a = 1$ und $b = 2$.

c) Wie ebenfalls schon in der Lösung zu Aufgabe 1.16 gezeigt wurde, folgt unmittelbar aus der Definition der Binomialkoeffizienten

$$\binom{n}{k}=\binom{n}{n-k}.$$

Aus der für $n \in \mathbb{N}_0$ und $0 \le k \le n$ gültigen Gleichung

$$\binom{n}{k}k+\binom{n}{k}(n-k)=\binom{n}{k}n$$

erhält man durch Summation über k und unter Benutzung von a)

$$\sum_{k=0}^{n}\binom{n}{k}k+\sum_{k=0}^{n}\binom{n}{k}(n-k)=n\sum_{k=0}^{n}\binom{n}{k}=n2^{n}.$$

Für die zweite Summe gilt aber nach der obigen Bemerkung

$$\sum_{k=0}^{n}\binom{n}{k}(n-k)=\sum_{k=0}^{n}\binom{n}{n-k}(n-k)=\sum_{m=0}^{n}\binom{n}{m}m,$$

wenn man $m = n-k$ setzt und in umgekehrter Reihenfolge summiert. Das zeigt, daß die erste Summe gleich der zweiten ist und folglich die Hälfte der rechten Seite. Dies war gerade zu zeigen.

Lösung 6.8 zu Aufgabe 1.18 a) Wegen $\phi_i = \phi_{i+2} - \phi_{i+1}$ gilt

$$\sum_{i=1}^{n}\phi_i=\sum_{i=1}^{n}(\phi_{i+2}-\phi_{i+1})=\phi_{n+2}-\phi_1.$$

b) Wegen $\phi_{2i-1} = \phi_{2i} - \phi_{2i-2}$ gilt

$$\sum_{i=1}^{n} \phi_{2i-1} = \sum_{i=1}^{n} (\phi_{2i} - \phi_{2i-2}) = \phi_{2n} - \phi_0.$$

c) Wegen $\phi_{2i} = \phi_{2i+1} - \phi_{2i-1}$ gilt

$$\sum_{i=1}^{n} \phi_{2i} = \sum_{i=1}^{n} (\phi_{2i+1} - \phi_{2i-1}) = \phi_{2n+1} - \phi_1.$$

d) Wegen $\phi_i = \phi_{i+1} - \phi_{i-1}$ gilt $\phi_i \cdot \phi_{i+1} - \phi_{i-1} \cdot \phi_i = \phi_i(\phi_{i+1} - \phi_{i-1}) = \phi_i^2$. Hieraus folgt

$$\sum_{i=1}^{n} \phi_i^2 = \sum_{i=1}^{n} (\phi_i \cdot \phi_{i+1} - \phi_{i-1} \cdot \phi_i) = \phi_n \cdot \phi_{n+1} - \phi_0 \cdot \phi_1.$$

e) Aus b) und c) folgt

$$\sum_{i=1}^{n} (\phi_{2i-1} - \phi_{2i}) + \phi_{2n+1} = \sum_{i=1}^{n+1} \phi_{2i-1} - \sum_{i=1}^{n} \phi_{2i} = \phi_{2n+2} - \phi_{2n+1} + 1.$$

f) Aus b) und c) folgt

$$\sum_{i=1}^{n} (\phi_{2i-1} - \phi_{2i}) = \sum_{i=1}^{n} \phi_{2i-1} - \sum_{i=1}^{n} \phi_{2i} = \phi_{2n} - \phi_{2n+1} + 1 = 1 - \phi_{2n-1}.$$

g) Für $n = 1$ gilt $\phi_1^2 = 1$ und $\phi_0 \cdot \phi_2 + (-1)^2 = 0 + 1 = 1$, also ist die Behauptung richtig. Gelte sie nun für ein $n \in \mathbb{N}$. Dann folgt

$$\begin{aligned}
\phi_{n+1}^2 &= (\phi_n + \phi_{n-1})\phi_{n+1} \\
&= \phi_n\phi_{n+1} + \phi_{n-1}\phi_{n+1} \\
&= \phi_n\phi_{n+1} + \phi_n^2 + (-1)^{n+2} \\
&= \phi_n(\phi_{n+1} + \phi_n) + (-1)^{n+2} \\
&= \phi_n\phi_{n+2} + (-1)^{n+2}.
\end{aligned}$$

Also gilt die Behauptung auch für $n + 1$ und damit für alle $n \in \mathbb{N}$.

Lösung 6.9 zu Aufgabe 1.19 Für $n = 0$ ergibt sich jedenfalls $\phi_0 = 0$ und für $n = 1$ auch $\phi_1 = 1$. Gelte die Formel also für zwei aufeinander folgende natürliche Zahlen $n-1$ und n. Wir schreiben

$$\alpha = \left(\frac{\sqrt{5}+1}{2}\right) \quad \text{und} \quad \beta = \left(\frac{1-\sqrt{5}}{2}\right).$$

Dann gilt also $\phi_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$ und $\phi_{n-1} = \frac{1}{\sqrt{5}}(\alpha^{n-1} - \beta^{n-1})$, und wir rechnen nach $\alpha^2 = \alpha + 1$ und $\beta^2 = \beta + 1$. Hieraus folgt

$$\begin{aligned}
\phi_{n+1} &= \phi_n + \phi_{n-1} \\
&= \frac{1}{\sqrt{5}}\left(\alpha^n - \beta^n + \alpha^{n-1} - \beta^{n-1}\right) \\
&= \frac{1}{\sqrt{5}}\left(\alpha^{n-1}(\alpha+1) - \beta^{n-1}(\beta+1)\right) \\
&= \frac{1}{\sqrt{5}}\left(\alpha^{n+1} - \beta^{n+1}\right),
\end{aligned}$$

also die Formel auch für $n+1$.

Lösung 6.10 zu Aufgabe 1.21 Zunächst ist es instruktiv, die Funktionswerte $a(m,n)$ für einige kleine Werte von m und n zu ermitteln:

$a(0,0) = 1, a(0,1) = 2, \ldots$ ergeben sich alle aus der ersten Definitionsgleichung.

$a(1,0) = a(0,1) = 2$ folgt hieraus mit der zweiten Gleichung,

$a(1,1) = a(0,a(1,0)) = a(0,a(0,1)) = a(0,1) + 1 = 3$ ergibt sich dann mit der dritten Gleichung.

$a(1,2) = a(0,a(1,1)) = a(0,a(0,a(1,0))) = a(1,1) + 1 = 4$ ergibt sich hieraus wiederum mit der dritten Gleichung.

Daher liefert vollständige Induktion mit der dritten Gleichung die Werte

$$a(1,n) = a(0,a(1,n-1)) = a(1,n-1) + 1 = n + 2.$$

Es ist dann wegen der zweiten Gleichung $a(2,0) = a(1,1) = 3$ und hieraus ergibt sich mit der dritten Gleichung $a(2,1) = a(1,a(2,0)) = a(2,0) + 2 = 3 + 2 = 5$.

Nun liefert vollständige Induktion mit der dritten Gleichung die Werte

$$a(2,n) = a(1,a(2,n-1)) = a(2,n-1) + 2 = 3 + 2 \cdot n.$$

Wiederum wegen der zweiten Gleichung ist $a(3,0) = a(2,1) = 5$ und wegen der dritten Gleichung dann $a(3,1) = a(2,a(3,0)) = 3 + 2 \cdot a(3,0) = 13$.

Nun liefert vollständige Induktion mit der dritten Gleichung $a(3,n) = a(2,a(3,n-1)) = 2 \cdot a(3,n-1) + 3 \cdot 1 = 2^n \cdot a(3,0) + 3 \cdot (1 + 2 + \cdots + 2^{n-1})$. Dies kann man vereinfachen zu

$$a(3,n) = 5 \cdot 2^n + 3 \cdot 2^n - 1 = 8 \cdot 2^n - 3 = 2^{n+3} - 3.$$

Weiterhin ist $a(4,0) = a(3,1) = 13$ und $a(4,1) = a(3,a(4,0)) = 2^{16} - 3 = 65533$ sowie $a(4,2) = a(3,a(4,1)) = 2^{65536} - 3$, eine Dezimalzahl mit 19729 Stellen.

Man kann noch durch Induktion zeigen, daß $a(4,n) = 2^{2^{\cdots^2}} - 3$ gilt, wobei der Exponententurm aus insgesamt $n+3$ Zweien besteht.

Außer $a(5,0) = a(4,1) = 65533$ lassen sich daher numerisch keine weiteren Werte der Ackermann-Funktion mehr darstellen. Trotzdem ist die Ackermann-Funktion eine *berechenbare Funktion*, da jeder ihrer Funktionswerte (im Prinzip) in endlicher Zeit berechnet werden kann. Jedoch reicht schon bei kleinen Werten von n und m der Platz im gesamten Universum nicht aus, um die benötigten Zwischenwerte zu speichern und die Rechenzeit würde auch sehr bald die Lebensdauer des Universums übersteigen.

Es wurden aber auch noch Funktionen konstruiert, die wesentlich schneller wachsen als die Ackermann-Funktion und die prinzipiell nicht mehr berechenbar sind. Eine derartige Funktion, die man "Fleißiger Biber" nennt, wird in der Automatentheorie angegeben.

Lösung 6.11 zu Aufgabe 1.24 Wegen $30 = 2 \cdot 3 \cdot 5$ ist $m = n^5 - n = n(n^4-1) = n(n^2-1)(n^2+1) = (n-1)n(n+1)(n^2+1)$ genau dann durch 30 teilbar, wenn m durch $2, 3$ und 5 teilbar ist. Von den drei aufeinander folgenden Zahlen $n-1, n$ und $n+1$ ist aber genau eine durch 3 teilbar und mindestens eine durch 2. Es bleibt daher nur noch die Teilbarkeit von m durch 5 zu zeigen. Zu n existiert aber genau ein $k \in \mathbb{N}$, so daß $n = 5k, n = 5k+1, n = 5k+2, n = 5k+3$ oder $n = 5k+4$ gilt. Im ersten Fall ist n durch 5 teilbar, im zweiten Fall $n-1$ und im letzten Fall $n+1$. Im Fall $n = 5k+2$ gilt $n^2+1 = (5k+2)+1 = 25k^2+10k+5$ und diese Zahl ist durch 5 teilbar. Im Fall $n = 5k+3$ gilt $n^2+1 = (5k+3)^2+1 = 25k^2+30k+10$ und auch diese Zahl ist durch 5 teilbar. Daher ist m stets durch 5 teilbar.

Lösung 6.12 zu Aufgabe 1.27 Gilt $d \mid \phi_{n+1}$ und $d \mid \phi_n$ für $n \in \mathbb{N}_0$, so folgt für $n = 0$ sofort $d \mid \phi_1 = 1$, also $d = 1$. Für $n > 0$ gilt aber auch $d \mid \phi_{n-1} = \phi_{n+1} - \phi_n$. So fortfahrend gelangt man auch jetzt schließlich zu $d \mid \phi_1$ und damit zu $d = 1$.

Lösung 6.13 zu Aufgabe 1.29 Wegen $[\frac{n}{p^k}] = 0$ für $p^k > n$, also für $k\log(p) > \log(n)$ läuft die Summe auf der rechten Seite stets nur von 1 bis $m = [\frac{\log(n)}{\log(p)}]$, ist also immer endlich.

Zu ermitteln ist die Anzahl der Primfaktoren p in der Primfaktorzerlegung von $n!$. Sammle also alle Primfaktoren p unter den Zahlen von 1 bis n ein. Zunächst kann p einmal als Faktor aus jeder p-ten Zahl von 1 bis n entfernt werden. Dies sind insgesamt $[\frac{n}{p}]$ Faktoren p. Dann kann p aber noch jeweils ein zweites Mal aus jeder p^2-ten Zahl von 1 bis n entfernt werden. Dies liefert nochmals genau $[\frac{n}{p^2}]$ Faktoren p., usw. Zuletzt kann p noch genau einmal aus $p^m \leq n$ als Faktor entfernt werden. Insgesamt steckte p genau $\sum_{k=1}^{m} \left[\frac{n}{p^k}\right]$ Mal als Faktor im Produkt $1 \cdot 2 \cdot 3 \cdots n = n!$.

Lösung 6.14 zu Aufgabe 1.38 i) Aus $p^\alpha || n$ folgt $n = p^\alpha n_p$ mit $p \not| n_p$, aus $p^\beta || m$ folgt $m = p^\beta m_p$ mit $p \not| m_p$. Also gilt auch $p \not| n_p m_p$ und $nm = p^{\alpha+\beta} n_p m_p$, was $p^{\alpha+\beta} || nm$ zeigt.

ii) Wegen $\alpha < \beta$ gilt $p^\beta = p^\alpha \cdot p^{\beta-\alpha}$ und damit (mit den Zerlegungen wie in i)) $n \pm m = p^\alpha n_p \pm p^\alpha p^{\beta-\alpha} m_p = p^\alpha(n_p \pm p^{\beta-\alpha} m_p)$, also $p^\alpha \mid n \pm m$. Wegen $p \mid p^{\beta-\alpha}$ hat man $p \not| n_p \pm p\beta - \alpha m_p$, da sonst $p \mid n_p$ folgen würde. Also gilt $p^\alpha || n \pm m$.

Es ist $2^2 || 12$ und $2^2 || 4$, aber wegen $2^3 || 8 = 12 - 4$ nicht $2^2 || 8$.

Lösung 6.15 zu Aufgabe 1.39 a) Es ist $\frac{1}{1-\frac{1}{p}} = \sum_{\alpha \in \mathbb{N}_0} \frac{1}{p^\alpha}$ und damit

$$\prod_{\nu=1}^{k} \frac{1}{1-\frac{1}{p_\nu}} = \sum_{\alpha_1,\ldots,\alpha_k \in \mathbb{N}_0} \frac{1}{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}.$$

Wegen der Eindeutigkeit der Primfaktorzerlegung kommt im Nenner der Summe auf der rechten Seite jedes $n \in \mathbb{N}$ für hinreichend großes k genau einmal vor. Daher gibt es zu jeder Partialsumme der harmonischen Reihe $\sum_{n=1}^{m} \frac{1}{n}$ ein $k \in \mathbb{N}$, so daß das Teilprodukt der linken Seite größer als diese Partialsumme ausfällt. Daher divergiert die Folge dieser Teilprodukte ebenso wie die harmonische Reihe gegen ∞.

b) Logarithmiert man die Teilprodukte auf der linken Seite in Teil a), so erhält man

$$\log\left(\prod_{\nu=1}^{k} \frac{1}{1-\frac{1}{p_\nu}}\right) = \sum_{\nu=1}^{k} -\log(1-\frac{1}{p_\nu}) < 2\sum_{\nu=1}^{k} \frac{1}{p_\nu}.$$

Wegen der Monotonie der Logarithmusfunktion und Teil a) divergiert die linke Seite gegen ∞, also auch die rechte Seite dieser Ungleichung.

Lösung 6.16 zu Aufgabe 1.45 Aus dem Beweis von Lemma 1.43 folgt $p_{k+1} \leq p_1 \cdot p_2 \cdots p_k + 1 < p_k^k + 1$ für $k > 1$. Für $k = 1$ gilt jedenfalls $p_1 = 2 < 4 = 2^2 = 2^{2^1}$. Gelte also $p_k < 2^{2^k}$ für $k \leq n$ in $\mathbb{N}$. Dann folgt $p_{n+1} \leq p_1 \cdot p_2 \cdots p_n < 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^n} \leq 2^{2^{n+1}}$.

Lösung 6.17 zu Aufgabe 1.55

i) $a = [\sqrt{8633}] + 1 = 93$ liefert $93^2 - 8633 = 16 = 4^2$. Daraus folgt $8633 = (93-4)(93+4) = 89 \cdot 97$. Fermatfaktorisierung benötigt also nur einen Schritt, während 89 beim trivialen Primzahltest erst als 24. Primzahl gefunden wird.

ii) $a = [\sqrt{88169891}] + 1 = 9390$ liefert $9390^2 - 88169891 = 2209 = 47^2$. Daraus folgt $88169891 = 9343 \cdot 9437$. Nach dem Primzahlsatz liegen unterhalb von 9343 ungefähr $\frac{9343}{\log(9343)} \sim 1022$ Primzahlen, die beim trivialen Primzahltest überprüft werden müßten.

iii) $a = [\sqrt{305321}] + 3 = 555$ liefert $555^2 - 305321 = 52^2$, also $305321 = 503 \cdot 607$ nach 3 Schritten, wobei 503 die 96. Primzahl ist.

iv) $a = [\sqrt{809009}] + 4 = 903$ liefert $903^2 - 809009 = 6400 = 80^2$, also $809009 = 823 \cdot 983$ nach 4 Schritten, wobei 823 die 143. Primzahl ist.

v) $a = [\sqrt{4601}] + 8 = 75$ liefert $75^2 - 4601 = 1024 = 32^2$, also $4601 = 43 \cdot 107$ nach 8 Schritten, wobei 43 die 14. Primzahl ist.

vi)$a = [\sqrt{92296873}] + 6 = 9613$ liefert $9613^2 - 92296873 = 112896 = 336^2$, also $92296873 = 9277 \cdot 9949$ nach 6 Schritten. Nach dem Primzahlsatz liegen unterhalb von 9277 ungefähr $\frac{9277}{\log(9277)} \sim 1015$ Primzahlen, die beim trivialen Primzahltest überprüft werden müßten.

Lösung 6.18 zu Aufgabe 1.56

i) $a = [\sqrt{200583}] + 1 = 448$ liefert $448^2 - 2000583 = 11^2$. Daraus folgt $200583 = 437 \cdot 459$.

$a = [\sqrt{437}] + 1 = 21$ liefert $21^2 - 437 = 2^2$. Daraus folgt $437 = 19 \cdot 23$, also die Primfaktorzerlegung von 437.

$a = [\sqrt{459}] + 1 = 22$ liefert $22^2 - 459 = 5^2$. Daraus folgt $459 = 17 \cdot 27$, also die Primfaktorzerlegung $459 = 3^3 \cdot 17$.

Damit ist $200583 = 3^3 \cdot 17 \cdot 19 \cdot 23$ die vollständige Primfaktorzerlegung.

ii) $a = [\sqrt{3786965}] + 1 = 1947$ liefert $1947^2 - 3786965 = 62^2$. Daraus folgt $3786965 = 1885 \cdot 2009$.

$a = [\sqrt{1885}] + 4 = 47$ liefert $47^2 - 1885 = 18^2$. Daraus folgt $1885 = 29 \cdot 65$, also die Primfaktorzerlegung $1885 = 5 \cdot 13 \cdot 29$.

$a = [\sqrt{2009}] + 1 = 45$ liefert $45^2 - 2009 = 4^2$. Daraus folgt $2009 = 41 \cdot 49$, also die Primfaktorzerlegung $2009 = 7^2 \cdot 41$.

Damit ist $3786965 = 5 \cdot 7^2 \cdot 13 \cdot 29 \cdot 41$ die vollständige Primfaktorzerlegung.

iii) $a = [\sqrt{13717}]+64 = 181$ liefert $181^2-13717 = 138^2$ nach 64 Schritten. Daraus folgt $13717 = 43 \cdot 319$.

$a = [\sqrt{319}] + 3 = 20$ liefert $20^2 - 319 = 9^2$ nach 3 Schritten. Daraus folgt $319 = 11 \cdot 29$, also die vollständige Primfaktorzerlegung $13717 = 11 \cdot 29 \cdot 43$.

Lösung 6.19 zu Aufgabe 1.63 Ist die Mersennezahl $M_p = 2^p-1$ eine Primzahl, so ist $p \geq 2$ eine Primzahl und daher 2^p durch 4 teilbar. Gilt nun $M_p = a^2 + b^2$ mit natürlichen Zahlen a und b, so ist folglich $a^2 + b^2 + 1 = 2^p$ durch 4 teilbar. Dabei ist a^2 genau dann durch 4 teilbar, wenn $a = 2k$ gerade ist, da sonst $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ nicht durch 4 teilbar ist. Dasselbe gilt für b^2. In keinem der vier möglichen Fälle für a und b, gerade oder ungerade zu sein, ist daher die Summe $a^2 + b^2 + 1$ durch 4 teilbar. Dieser Widerspruch zeigt, daß M_p nicht die Summe von zwei Quadraten sein kann. (Weil M_p eine Primzahl sein soll, ist es natürlich auch selbst kein Quadrat.)

Lösung 6.20 zu Aufgabe 1.67 Die echten Teiler von $n = p^k$ für eine Primzahl p und $k \in \mathbb{N}$ sind genau $1, p, p^2, \ldots, p^{k-1}$. Die Summe der echten Teiler ist daher $\frac{p^k-1}{p-1} < p^k = n$. Also ist n nicht vollkommen.

Lösung 6.21 zu Aufgabe 1.76 Für $n = 1$ gilt jedenfalls $F_1-2 = 5-2 = 3 = F_0$. Gelte also $F_{n-1} - 2 = 2^{2^{n-1}} - 1 = F_{n-2} \cdots F_0$. Dann folgt

$$F_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) = F_{n-1} \cdot F_{n-2} \cdots F_0.$$

Lösung 6.22 zu Aufgabe 1.81 Die Aussage ist offensichtlich richtig für $a = 0$ (dann müsste b eine Primzahl sein) oder $b = 0$ (dann müsste a eine Primzahl und $n = 1$ sein). Seien also $a, b \in \mathbb{N}$. Haben a und b einen gemeinsamen Teiler $d > 1$, so gilt $d \mid n \cdot a + 1 \cdot b = an + b$ nach Lemma 1.23 c). Damit kann $an + b$ nur dann Primzahl sein, wenn $d = an + b$ selbst Primzahl ist und dann auch nur für genau ein $n \in \mathbb{N}_0$.

Lösung 6.23 zu Aufgabe 1.82

Jede ungerade Primzahl ist von der Form $p = 6n + 1$ oder $q = 6n - 1$, denn jede andere ungerade Zahl hat die Form $6n + 3$ und damit den Teiler 3. Das Produkt von zwei (und damit von endlich vielen) Zahlen der ersten Form, also $(6n + 1)(6m+1) = 36nm+6(n+m)+1$, ist wieder eine (allerdings zusammengesetzte) Zahl dieser Form.

Ist nun $\{q_1, \ldots, q_k\}$ eine endliche Liste von Primzahlen der zweiten Form, so ist die ungerade Zahl $N = 2 \cdot 3 \cdot q_1 \cdots q_k - 1 > 1$ ebenfalls von dieser Form und besitzt nur Primfaktoren, die von allen Primzahlen $q_1, \ldots, q_k$ verschieden sind. Da sie aber nicht nur Primfaktoren der ersten Form besitzen kann, existiert ein Primfaktor der zweiten Form, der von allen q_i verschieden ist. Also kann die gegebene Liste erweitert werden.

Jede ungerade Primzahl ist auch entweder von der Form $p = 4n+1$ oder $q = 4n-1$ und das Produkt von zwei Zahlen der ersten Form ist ebenfalls wieder von dieser Form.

Nun kann man mit $N = 4 \cdot q_1 \cdots q_k - 1$ die selben Schlüsse wie oben durchführen.

Lösung 6.24 zu Aufgabe 2.1 Wegen $a + b = b + a$ für alle $a, b \in \mathbb{N}_0$ ist $\sim$ reflexiv. Da $a + d = b + c$ stets $c + b = d + a$ impliziert, ist $\sim$ symmetrisch. Aus $a + d = b + c$ und $c + f = d + e$ folgt $a + d + c + f = b + c + d + e$ und damit $a + f + (c + d) = b + e + (c + d)$. Bisher wurde nur die Assoziativität und Kommutativität der Addition verwendet. Mit der Kürzbarkeit folgt jetzt $a + f = b + e$, also ist $\sim$ auch transitiv.

Aus $a+d = b+c$ folgt $a+d+x+y = b+c+x+y$ und daher auch $(a+x)+(d+y) = (b + y) + (c + x)$, womit auch (44) gezeigt ist.

Lösung 6.25 zu Aufgabe 2.2 Die Addition ist repräsentantenunabhängig:

Seien $[a, b] = [a', b']$ und $[c, d] = [c', d']$ beliebige Klassen. Dann gelten $a+b' = a'+b$ und $c + d' = c' + d$. Hieraus folgt $(a + c) + (b' + d') = (a' + c') + (b + d)$, also $[a + c, b + d] = [a' + c', b' + d']$, wobei wiederum nur die Assoziativität und Kommutativität der Addition benutzt wurden.

Da die Addition (45) komponentenweise erfolgt, übertragen sich die Assoziativität und Kommutativität von $(\mathbb{N}_0, +)$ auf $(\mathbb{Z}, +)$.

Wegen $a + (b + c) = b + (a + c)$ für alle $a, b, c \in \mathbb{N}_0$ gilt $(a, b) \sim (a + c, b + c)$ und daher $[a, b] = [a + c, b + c]$. Folglich ist $[c, c]$ neutrales Element der Addition von $(\mathbb{Z}, +)$.

Wegen $[a,b]+[b,a]=[a+b,a+b]$ ist dann $[b,a]$ additiv invers zu $[a,b]$ und daher $(\mathbb{Z},+)$ eine abelsche Gruppe.

Die Multiplikation ist repräsentantenunabhängig:

Seien wieder $[a,b]=[a',b']$ und $[c,d]$ beliebige Klassen. Dann gelten $a+b'=a'+b$ und damit $ac+b'c=bc+a'c$ sowie $ad+b'd=bd+a'd$ nach den Distributivgesetzen in $(\mathbb{N}_0,+,\cdot)$. Addition liefert $(a'c+b'd)+(bc+ad)=a'd+b'c)+(bd+ac)$, also $(a'c+b'd,a'd+b'c)\sim(ac+bd,ad+bc)$. Dies zeigt $[a,b]\cdot[c,d]=[a',b']\cdot[c,d]$, also die Unabhängigkeit der Multiplikation vom linken Repräsentanten. Die Unabhängigkeit vom rechten Repräsentanten folgt analog.

Wegen der Kommutativität der Addition und der Multiplikation auf $\mathbb{N}_0$ ist auch die Multiplikation (46) kommutativ.

Die Multiplikation ist assoziativ:

Sowohl für $([a,b][c,d])[e,f]$ als auch für $[a,b]([c,d][e,f])$ ergibt sich $[ace+bde+adf+bcf,acf+bdf+ade+bce]$.

Wegen $[a,b]\cdot[1,0]=[a,b]$ ist $[1,0]$ Einselement von $(\mathbb{Z},\cdot)$.

Die Multiplikation ist distributiv gegenüber der Addition:

Wegen der Kommutativit der Multiplikation reicht es, ein Distributivgesetz zu zeigen.

Es gilt $[a,b]([c,d]+[e,f])=[a,b][c+e,d+f]=[ac+ae+bd+bf,ad+af+bc+be]$ und $[a,b][c,d]+[a,b][e,f]=[ac+bd+ae+bf,ad+bc+af+be]$, also die Gleichheit.

$(\mathbb{Z},+,\cdot)$ ist nullteilerfrei, denn aus $a\cdot b=0$ folgt $|a|\cdot|b|=|a\cdot b|=0$ und die Nullteilerfreiheit von $(\mathbb{N}_0,+\cdot)$ liefert $|a|=0$ oder $|b|=0$, also $a=0$ oder $b=0$.

Lösung 6.26 zu Aufgabe 2.3 Daß $\leq$ eine partielle Ordnung auf $\mathbb{Z}$ ist, folgt genau wie in Lösung 6.5.

Ebenso folgt die Monotonie der Addition genau wie in Lösung 6.5.

Wegen der Monotonie der Addition ist $\leq$ genau dann linear, wenn für alle $a\in\mathbb{Z}$ gilt $a\leq 0$ oder $0\leq a$. Denn gilt für $a,b\in\mathbb{Z}$ dann $0\leq b-a$, so folgt durch Addition von a sofort $a\leq b$, gilt dagegen $b-a\leq$, so folgt $b\leq a$.

Nach Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}_0$ existieren für jedes $a\in\mathbb{Z}$ aber natürliche Zahlen $n,m\in\mathbb{N}_0$ mit $a=n-m$. Daher gilt $m\leq n$ oder $n\leq m$ in $(\mathbb{N}_0,\leq)$. Im ersten

Fall folgt $0 \leq n - m = a$, im zweiten $0 \leq m - n = -a$, wegen der Monotonie der Addition also $a \leq 0$.

Aus $a \leq b$ folgt $0 \leq b - a$ und damit $0 \leq (b - a) \cdot c = b \cdot c - a \cdot c$, da die Multiplikation in $\mathbb{N}_0$ monoton bezüglich $\leq$ ist.

Lösung 6.27 zu Aufgabe 2.11 Für $k = 1, \ldots, n-2$ gilt entweder $r_{k+1} \leq \frac{1}{2} r_k$, woraus dann $r_{k+2} < r_{k+1} \leq \frac{1}{2} r_k$ folgt, oder es gilt $r_{k+1} > \frac{1}{2} r_k$, woraus sich dann die Division mit Rest $r_k = 1 \cdot r_{k+1} + r_{k+2}$ ergibt, was zu $r_{k+2} = r_k - r_{k+1} < \frac{1}{2} r_k$ führt. In jedem Fall gilt die Behauptung.

Lösung 6.28 zu Aufgabe 2.12 Mit $a = 16289$ und $b = 14345$ liefert der Euklidische Algorithmus die folgenden 10 Berechnungsschritte

$$\begin{aligned}
16289 &= 1 \cdot 14345 + 1944 \\
14345 &= 7 \cdot 1944 + 737 \\
1944 &= 2 \cdot 737 + 470 \\
737 &= 1 \cdot 470 + 267 \\
470 &= 1 \cdot 267 + 203 \\
267 &= 1 \cdot 203 + 64 \\
203 &= 3 \cdot 64 + 11 \\
64 &= 5 \cdot 11 + 9 \\
11 &= 1 \cdot 9 + 2 \\
9 &= 4 \cdot 2 + 1
\end{aligned}$$

Daher sind die beiden Zahlen teilerfremd.

Mit $a = 153049$ und $b = 142241$ liefert der Euklidische Algorithmus die folgenden 5 Berechnungsschritte

$$\begin{aligned}
153049 &= 1 \cdot 142241 + 10808 \\
142241 &= 13 \cdot 10808 + 1737 \\
10808 &= 6 \cdot 1737 + 386 \\
1737 &= 4 \cdot 386 + 193 \\
386 &= 2 \cdot 193
\end{aligned}$$

Daher ist $\mathrm{ggT}(153049, 142241) = 193$.

Lösung 6.29 zu Aufgabe 2.18 Für $n = 2$ ist $g_1(2) = 2 = 2^1$ in iterierter Darstellung zur Basis 2. Daraus folgt $g_2(2) = a_2(2^1) - 1 = 3 - 1 = 2$ in iterierter Darstellung zur Basis 3. Damit ergibt sich $g_3(2) = a_3(2) - 1 = 2 - 1 = 1$ und schließlich $g_4(2) = a_4(1) - 1 = 1 - 1 = 0$. Dann gilt aber $g_b(2) = 0$ für alle weiteren Folgeglieder.

Für $n = 3$ ist $g_1(3) = 3 = 2^1 + 1$ und daher $g_2(3) = 3^1 + 1 - 1 = 3^1$. Es folgen $g_3(3) = 4^1 - 1 = 3$ und weiter $g_4(3) = 3 - 1 = 2$, $g_5(3) = 2 - 1 = 1$ sowie $g_6(3) = 1 - 1 = 0$ und daher $g_b(3) = 0$ für alle weiteren Folgeglieder.

Für $n = 4$ lauten die ersten Folgeglieder

$$\begin{aligned}
g_1(4) &= 4 \\
g_2(4) &= a_2(2^2) - 1 = 3^3 - 1 = 26 \\
g_3(4) &= a_3(2 \cdot 3^2 + 2 \cdot 3^1 + 2) - 1 = 2 \cdot 4^2 + 2 \cdot 4^1 + 1 = 41 \\
g_4(4) &= a_4(2 \cdot 4^2 + 2 \cdot 4^1 + 1) - 1 = 2 \cdot 5^2 + 2 \cdot 5^1 = 60 \\
g_5(4) &= a_5(2 \cdot 5^2 + 2 \cdot 5^1 + 0) - 1 = 2 \cdot 6^2 + 2 \cdot 6 - 1 = 83.
\end{aligned}$$

Jetzt kann man durch Induktion zeigen, daß alle Folgeglieder $g_b(4)$ für $b \geq 2$ von der Form $g_b(4) = x_b \cdot (b+1)^2 + y_b \cdot (b+1) + z_b$ mit natürlichen Zahlen $x_b \leq 2$, $y_b, z_b \leq b$ sind. Jeder Basis b kann also eindeutig solch ein Tripel (x_b, y_b, z_b)

zugeordnet werden.

b	(x_b, y_b, z_b)
2	$(2,2,2)$
3	$(2,2,1)$
4	$(2,2,0)$
5	$(2,1,5)$
6	$(2,1,4)$
7	$(2,1,3)$
$\dots$	$\dots$
10	$(2,1,0)$
11	$(2,0,11)$
12	$(2,0,10)$
$\dots$	$\dots$
22	$(2,0,0)$
23	$(1,23,23)$
$\dots$	$\dots$
46	$(1,23,0)$
47	$(1,22,47)$
48	$(1,22,46)$
$\dots$	$\dots$
$3 \cdot 2^{27} - 2$	$(1,0,0)$
$3 \cdot 2^{27} - 1$	$(0, 3 \cdot 2^{27} - 1, 3 \cdot 2^{27} - 1)$
$\dots$	$\dots$
$3 \cdot 2^{27} \cdot 2^{3 \cdot 2^{27}-2} - 1$	$(0,1,0)$
$\dots$	$\dots$

Definiert man auf diesen Tripeln (x_b, y_b, z_b) eine naheliegende Ordnung, so kann man zeigen, daß die Folge dieser Tripel mit wachsendem b streng monoton gegen $(0,0,0)$ geht. Hieraus folgt $g_b(4) = 0$ für ein hinreichend großes b. Eine genauere Analyse zeigt, daß dies erstmals bei $b = 3 \cdot 2^{27} \cdot 2^{3 \cdot 2^{27}-1} - 2 = 3 \cdot 2^{402653211} - 2$ der Fall ist. Diese Zahl besitzt im Dezimalsystem ungefähr 130 Millionen Stellen.

Man kann daher vermuten, daß die Goodstein-Folge $g_b(n)$ für jeden Keim n eine Nullfolge ist. Dies kann man auch beweisen, allerdings benötigt man dazu transfinite Ordinalzahlen und transfinite Induktion. Die Induktion allein über natürliche Zahlen reicht dazu nachweislich nicht aus. Dies haben Laurence Kirby und Jeffrey Paris 1981 gezeigt. Genauer: *Die Funktion, die jedem Keim n die kleinste Basis b mit $g_b(n) = 0$ zuordnet, wächst schneller als jede durch vollständige Induktion definierbare Funktion.*

Lösung 6.30 zu Aufgabe 2.20 Die Aussagen ergeben sich aus Lemma 2.5:

Wegen $m \mid 0 = a - a$ für alle $a \in \mathbb{Z}$ ist $\equiv$ reflexiv.

Wegen $m \mid a - b \Longleftrightarrow m \mid b - a = -(a - b)$ ist $\equiv$ symmetrisch.

Wegen $m \mid a - b$ und $m \mid b - c \Longrightarrow m \mid a - c = (a - b) + (b - c)$ ist $\equiv$ transitiv, also eine Äquivalenzrelation.

Wegen $m \mid a - b \Longrightarrow m \mid (a + c) - (b + c)$ und $m \mid (a - b) \cdot c = a \cdot c - b \cdot c$ ist $\equiv$ mit der Addition und der Multiplikation verträglich, also eine Kongruenzrelation.

Gelten $a = q_1 \cdot m + r$ und $b = q_2 \cdot m + r$, so folgt $m \mid (b - a) = (q_2 - q_1) \cdot m$. Gilt umgekehrt $b - a = k \cdot m$ und $b = q \cdot m + r$ mit $0 \leq r < m$, so folgt $a = (q - k) \cdot m + r$.

Lösung 6.31 zu Aufgabe 2.21 Aus $a \mid b$ folgt

$$b - 1 = b - \frac{b}{a} + \frac{b}{a} - 1 = \frac{b}{a}(a - 1) + (\frac{b}{a} - 1) \equiv (\frac{b}{a} - 1) \; mod \; (a - 1).$$

Also teilt $a - 1$ genau dann $b - 1$, wenn $a - 1$ auch $\frac{b}{a} - 1$ teilt.

Lösung 6.32 zu Aufgabe 2.33 Man kann bei der Auflösung des linearen Gleichungssystems generell die benötigten Inversen der Koeffizienten stets mit Hilfe des Euklidischen Algorithmus aus der Linearkombination des jeweiligen größten gemeinsamen Teilers berechnen. Man kann aber bei diesem einfachen Modul die Inversen schneller durch elementare Überlegungen ermitteln.

Wegen $2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6 = 24 = 1$ in $\mathbb{Z}/(23)$ gilt dort $2^{-1} = 12, 3^{-1} = 8$ und $4^{-1} = 6$. Damit sind schon die acht Inversen von 1 und -1 und $2, 3, 4, 6, 8, 12$ und daher wegen $(-a)^{-1} = ((-1) \cdot a))^{-1} = (-1)^{-1} \cdot a^{-1} = -a^{-1}$ auch die weiteren sechs Inversen von $11 = -12, 15 = -8, 17 = -6, 19 = -4, 20 = -3$ und $21 = -2$ bekannt. Die noch fehlenden acht Inversen ergeben sich aus zwei weiteren Produkten. Wegen $5 \cdot 9 = 45 = -1$ gilt $5^{-1} = -9 = 14$, wegen $7 \cdot 10 = 70 = -1$ gilt $7^{-1} = -10 = 13$.

Durch Multiplikation der einzelnen Gleichungen mit den Inversen der Koeffizienten von x_1 erhält man das äquivalente Gleichungssystem

$$\begin{array}{rcrcrcr} x_1 & & & + & 14x_3 & = & 19 \\ x_1 & + & 7x_2 & + & 6x_3 & = & 1 \\ x_1 & + & 6x_2 & + & 3x_3 & = & 1 \end{array}$$

Subtrahiert man nun die dritte Gleichung von der zweiten, so ergibt sich $x_2 + 3x_3 = 0$, also $x_2 = 20x_3 = -3x_3$. Aus der ersten Gleichung erhält man $x_1 = 19 + 9x_3 = -4 + 9x_3$.

Setzt man dies in die zweite Gleichung ein, so ergibt sich

$$19 + 9x_3 - 21x_3 + 6x_3 = 19 - 6x_3 = 1,$$

woraus dann $6x_3 = 18$ und damit $x_3 = 3$ folgt. Die eindeutige Lösung ist daher $(x_1, x_2, x_3) = (0, 14, 3)$.

Lösung 6.33 zu Aufgabe 2.34 Wegen $2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6 = 24 = 1$ in $\mathbb{Z}/(23)$ gilt dort $2^{-1} = 12, 3^{-1} = 8$ und $4^{-1} = 6$.

Subtrahiert man die zweite Gleichung von der ersten, so erhält man $7x_1 - 2x_2 = 0$ oder $2x_2 = 7x_1$. Multiplikation mit 12 liefert $x_2 = 15x_1$.

Addiert man die zweite und die dritte Gleichung, so erhält man $3x_1 + 9x_2 = 0$. Multiplikation mit 3^{-1} liefert $x_1 = -3x_2$.

Setzt man dies in die dritte Gleichung ein, so erhält man $7x_1 + 3x_3 = 14$. Nach Multiplikation mit $3^{-1} = 8$ ergibt dies $x_3 = 20 - 10x_1$.

Wählt man $x_1 = t$ als Parameter, so erhält man sämtliche Lösungen des linearen Gleichungssystems als

$$(x_1, x_2, x_3) = (t, 15t, 20 + 13t), \ t \in \mathbb{Z}/(23).$$

Lösung 6.34 zu Aufgabe 2.35 Die Matrix $M(a, b) = \begin{pmatrix} a & 2 \\ 2 & b \end{pmatrix}$ ist genau dann invertierbar, wenn ihre Determinante $\det(M(a, b)) = ab - 4$ im Restklassenring $(\mathbb{Z}/(6), +, \cdot)$ invertierbar ist, also in der primen Restklassengruppe $\mathbb{Z}/(6)^*$ liegt. Die Inverse lautet dann

$$M(a, b)^{-1} = \det(M(a, b))^{-1} \begin{pmatrix} b & -2 \\ -2 & a \end{pmatrix}.$$

Wegen $\mathbb{Z}/(6)^* = \{1, 5\}$ ist dies genau dann der Fall, wenn $ab = 5 = -1$ oder $ab = 9 = 3$ gilt. Im ersten Fall sind also a und b selbst invertierbar, d. h. es ergeben sich die Kombinationen

1. $a = 1$, $b = -1$, $\det(M(1, -1)) = 1$ und $M(1, -1)^{-1} = \begin{pmatrix} -1 & -2 \\ -2 & 1 \end{pmatrix}$.

2. $a = -1$, $b = 1$, $\det(M(1, -1)) = 1$ und $M(-1, 1)^{-1} = \begin{pmatrix} 1 & -2 \\ -2 & -1 \end{pmatrix}$.

Im zweiten Fall sind a und b beide ungerade. Damit ergeben sich die Kombinationen

3. $a = 1$, $b = 3$, $\det(M(1,3)) = -1$ und $M(1,3)^{-1} = \begin{pmatrix} 3 & 2 \\ 2 & -1 \end{pmatrix}$.

4. $a = -1$, $b = 3$, $\det(M(-1,3)) = -1$ und $M(-1,3)^{-1} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$.

5. $a = 3$, $b = 1$, $\det(M(3,1)) = -1$ und $M(3,1)^{-1} = \begin{pmatrix} -1 & 2 \\ 2 & 3 \end{pmatrix}$.

6. $a = 3$, $b = -1$, $\det(M(3,-1) = -1$ und $M(3,-1)^{-1} = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$

7. $a = 3$, $b = 3$, $\det(M(3,3)) = -1$ und $M(3,3)^{-1} = \begin{pmatrix} 3 & -2 \\ -2 & 3 \end{pmatrix}$.

Lösung 6.35 zu Aufgabe 2.36 Mit den Bezeichnungen des Beweises von Satz 2.31 hat man $a_1 = 1, a_2 = 2, a_3 = 4, a_4 = 7$ und $m_1 = 25 = 5 \cdot 5, m_2 = 7, m_3 = 9 = 3 \cdot 3, m_4 = 2 \cdot 19$. Insbesondere sind die Module m_i teilerfremd. Daher ist das System dieser vier Kongruenzen modulo $M = 25 \cdot 7 \cdot 9 \cdot 38 = 59850$ eindeutig lösbar.

Weiterhin ist $M_1 = 2394, M_2 = 8550, M_3 = 6650$ und $M_4 = 1575$. Mit dem Euklidischen Algorithmus bestimmt man nun die jeweiligen Inversen N_i modulo m_i zu $N_1 = 4, N_2 = 5, N_3 = 8, N_4 = 9$ und damit eine Lösung zu

$$x' = 1 \cdot 2394 \cdot 4 + 2 \cdot 8550 \cdot 5 + 4 \cdot 6650 \cdot 8 + 7 \cdot 1575 \cdot 9 = 407101.$$

Eine weitere Division mit Rest durch M liefert dann die kleinste positive Lösung $x = 48001$.

Lösung 6.36 zu Aufgabe 2.39 Kennt man Primzahlen p und q mit $n = p \cdot q$, so erhält man $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1) = p \cdot q - (p+q) + 1 = n - (p+q) + 1$. Es gilt für derartige n also insbesondere stets $-(p+q) = \varphi(n) - n - 1$.

Kennt man andererseits für ein derartiges n auch $\varphi(n)$, dann kennt man die Koeffizienten der quadratischen Gleichung $(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 + (\varphi(n) - n - 1)x + n = 0$. Die Lösungen dieser quadratischen Gleichung sind dann gerade p und q.

Lösung 6.37 zu Aufgabe 2.40 a) Wähle beispielsweise $n_k = p_k$, die k-te Primzahl.

b) Wähle beispielsweise $n_k = k!$.

Lösung 6.38 zu Aufgabe 2.41 Aus Satz 2.38 b) folgt für alle Primzahlen p und Exponenten $\alpha, \beta \in \mathbb{N}$ sofort $\varphi(p^\alpha) = p^{\alpha-1}(p-1) = p^{\alpha-1}\varphi(p)$ und daher auch $\varphi(p^{\alpha+\beta}) = p^{\alpha+\beta-1}\varphi(p) = p^\alpha(p^{\beta-1}\varphi(p)) = p^\alpha\varphi(p^\beta) = p^\beta\varphi(p^\alpha)$. Durch Multiplikation mit $\varphi(p^\beta)$ erhält man hieraus

$$\varphi(p^{\alpha+\beta})\varphi(p^\beta) = \varphi(p^\alpha)\varphi(p^\beta)p^\beta. \tag{83}$$

Jedenfalls gilt

$$\varphi(mn)\varphi(ggT(m,n)) = \varphi(m)\varphi(n)ggT(m,n) \tag{84}$$

nach Satz 2.38 a) für $d = ggT(m,n) = 1$. Sei nun $d > 1$ und p ein beliebiger Primteiler von d. Mit den höchsten Exponenten $\alpha = v_p(m), \beta = v_p(n)$ und $\gamma = v_p(d)$ darf man, eventuell nach Vertauschung von m und n, dann $\alpha \geq \beta$ und daher $\gamma = \beta$ annehmen. Mit $m = p^\alpha m'$, $n = p^\beta n'$ und $d = p^\beta d'$ gilt dann $d' = ggT(m',n')$. Daher folgt aus der Multiplikativität von φ weiter $\varphi(m) = \varphi(p^\alpha)\varphi(m')$, $\varphi(n) = \varphi(p^\beta)\varphi(n')$, $\varphi(d) = \varphi(p^\beta)\varphi(d')$ und $\varphi(mn) = \varphi(p^\alpha p^\beta m'n') = \varphi(p^{\alpha+\beta})\varphi(m'n')$.

Nun ist (84) gleichwertig zu

$$\varphi(p^{\alpha+\beta})\varphi(m'n')\varphi(p^\beta)\varphi(d') = \varphi(p^\alpha)\varphi(m')\varphi(p^\beta)\varphi(n')p^\beta d'$$

und dies ist wegen (83) gleichwertig zu

$$\varphi(m'n')\varphi(ggT(m',n')) = \varphi(m')\varphi(n')ggT(m',n').$$

Also folgt (84) durch Induktion über die Anzahl der Primteiler von $ggT(m,n)$.

Lösung 6.39 zu Aufgabe 2.48 Man kann die folgenden Faktorisierungen für kleinere Exponenten benutzen:

$2^2 - 1 = 3$,

$2^3 - 1 = 7$,

$2^4 - 1 = 15 = 3 \cdot 5$,

$2^5 - 1 = 31$,

$2^6 - 1 = 63 = 3^2 \cdot 7$,

$2^7 - 1 = 127$,

$2^8 - 1 = 255 = 3 \cdot 5 \cdot 17$,

$2^9 - 1 = 511 = 7 \cdot 73$,

$2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$,

$2^{11} - 1 = 2047 = 23 \cdot 89$,

$2^{12} - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$,

$2^{13} - 1 = 8191$,

$2^{14} - 1 = 3 \cdot 43 \cdot 127$.

i) $2^{15} - 1 = 32767 = 7 \cdot 31 \cdot 151$,

ii) $2^{20} - 1 = 1048575 = 3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$,

iii) $2^{21} - 1 = 2097151 = 7^2 \cdot 127 \cdot 337$,

iv) $2^{30} - 1 = 1073741823 = 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$,

v) $2^{33} - 1 = 8589934591 = 7 \cdot 23 \cdot 89 \cdot 599479$,

vi) $2^{60} - 1 = 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$.

Lösung 6.40 zu Aufgabe 2.49 Man kann die folgenden Faktorisierungen für kleinere Exponenten benutzen:

$3^1 - 1 = 2$,

$3^2 - 1 = 8 = 2^3$,

$3^3 - 1 = 26 = 2 \cdot 13$,

$3^4 - 1 = 80 = 2^4 \cdot 5$,

$3^5 - 1 = 242 = 2 \cdot 11^2$,

$3^6 - 1 = 728 = 2^3 \cdot 7 \cdot 13$,

$3^7 - 1 = 2186 = 2 \cdot 1093$,

$3^8 - 1 = 6560 = 2^5 \cdot 5 \cdot 41$,

$3^9 - 1 = 19682 = 2 \cdot 13 \cdot 757$,

$3^{10} - 1 = 59048 = 2^3 \cdot 11^2 \cdot 61$.

i) $3^{12} - 1 = 531440 = 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 73$,

ii) $3^{15} - 1 = 14348906 = 2 \cdot 11^2 \cdot 13 \cdot 4561$,

iii) $3^{24} - 1 = 282429536480 = 2^5 \cdot 5 \cdot 7 \cdot 13 \cdot 41 \cdot 73 \cdot 6481$.

Lösung 6.41 zu Aufgabe 2.50 Man kann die folgenden Faktorisierungen für kleinere Exponenten benutzen:

$5^1 - 1 = 4 = 2^2$,

$5^2 - 1 = 24 = 2^3 \cdot 3$,

$5^3 - 1 = 124 = 2^2 \cdot 31$,

$5^4 - 1 = 624 = 2^4 \cdot 3 \cdot 13$,

$5^5 - 1 = 3124 = 2^2 \cdot 11 \cdot 71$,

$5^6 - 1 = 15624 = 2^3 \cdot 3^2 \cdot 7 \cdot 31$.

i) $5^9 - 1 = 1953124 = 2^2 \cdot 19 \cdot 31 \cdot 829$,

ii) $5^{10} - 1 = 9765624 = 2^3 \cdot 3 \cdot 11 \cdot 71 \cdot 521$,

iii) $5^{12} - 1 = 244140624 = 2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$.

Lösung 6.42 zu Aufgabe 2.55 Da q Teiler von $2^p - 1$ ist, gilt $2^p \equiv 1 \bmod q$. Nach dem Kleinen Fermatschen Satz gilt auch $2^{q-1} \equiv 1 \bmod q$. Da $q - 1$ gerade ist, kann $q - 1$ kein Teiler von p sein. Daher ist $q - 1$ ein Vielfaches der ungeraden Zahl p, aber selbst gerade. Es gibt daher eine natürliche Zahl k mit $q - 1 = 2kp$.

Lösung 6.43 zu Aufgabe 2.69 Eine gerade, quadratfreie und zusammengesetzte Zahl besitzt mindestens einen ungeraden Primfaktor p. Für diesen ist aber $p - 1$ gerade und kann daher nicht die ungerade Zahl $n - 1$ teilen. Also ist n keine Carmichael-Zahl.

Der Rest folgt aus Aufgabe 2.21 (mit $a = p$ und $b = n$) und Satz 2.68 ii).

Lösung 6.44 zu Aufgabe 2.72 Offensichtlich ist n ungerade und als Produkt von drei verschiedenen Primzahlen quadratfrei. Wegen

$$n-1 = (6m+1)(12m+1)(18m+1) - 1 = 36m(36m^2+11m+1)$$

gilt auch $(p_i-1) \mid 36m \mid (n-1)$. Also ist n nach Satz 2.68 ii) eine Carmichael-Zahl.

Für $m = 1$ erhält man $n = 1729 = 7 \cdot 13 \cdot 19$. Für $m = 2$ ist $p_2 = 25$ keine Primzahl und $n = 13 \cdot 5^2 \cdot 19$ nicht quadratfrei, also keine Carmichael-Zahl. Für $m = 3$ ist $p_3 = 55 = 5 \cdot 11$ keine Primzahl und $n = 19 \cdot 37 \cdot 55 = 38665$ wegen des Primfaktors $p = 11$ mit $p - 1 = 10 \not| n - 1$ keine Carmichael-Zahl. Erst für $m = 6$ erhält man wieder eine Carmichael-Zahl $n = 294409 = 37 \cdot 73 \cdot 109$

Lösung 6.45 zu Aufgabe 2.70 i) Es ist $n = 172081 = 7 \cdot 13 \cdot 31 \cdot 61$ wie man leicht mit Probedivisionen durch $2, 3, 5, 7, 11, 13, 19, 23, 29$ und 31 ermittelt. Daher ist n quadratfrei. Weiterhin gilt $n - 1 = 172080 = 2^4 \cdot 3^2 \cdot 5 \cdot 239$ wie man ebenfalls leicht mit Probedivisionen durch $2, 3$ und 5 feststellt. Da $6 = 7-1, 12 = 13-1, 30 = 31-1$ und $60 = 61-1$ jeweils Teiler von $n-1$ sind, handelt es sich bei $n = 172081$ um eine Carmichael-Zahl.

ii) Es ist $n = 552721 = 13 \cdot 17 \cdot 41 \cdot 61$ wie man ebenfalls mit Probedivisionen durch alle Primzahlen bis 41 ermittelt. Also ist n quadratfrei. Weiterhin ist $n - 1 = 552720 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 329$ wie man mit Probedivisionen durch $2, 3, 5$ und 7 feststellt. Daß 329 eine Primzahl ist, entnimmt man 7.1. Da $12 = 13 - 1, 16 = 17 - 1, 40 = 41 - 1$ und $60 = 61 - 1$ jeweils Teiler von $n - 1$ sind, handelt es sich auch bei $n = 552721$ um eine Carmichael-Zahl.

iii) Es ist $n = 847757 = 23 \cdot 29 \cdot 31 \cdot 41$ wie man mit Probedivisionen durch alle Primzahlen bis 31 ermittelt. Also ist n quadratfrei. Weiterhin ist $n - 1 = 847756 = 2^2 \cdot 7 \cdot 13 \cdot 17 \cdot 137$ wie man mit Probedivisionen durch $2, 3, 5, 7, 11, 13$ und 17 feststellt. Da aber $22 = 23 - 1$ kein Teiler von $n - 1$ ist, handelt es sich bei $n = 847757$ um keine Carmichael-Zahl.

Lösung 6.46 zu Aufgabe 2.92 Die Lösung orientiert sich am Beweis von Folgerung 2.90. Da a quadratischer Rest modulo q ist, gilt nach dem Euler-Kriterium (Lemma 2.79)

$$a^{p-1} \equiv a^{(q-1)/2} \equiv 1 \bmod q$$

und nach dem Kleinen Fermatschen Satz (Satz 2.54) auch

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

Es folgt $a^{p-1} \equiv 1 \bmod n$ und wegen $n-1 = pq-1 = 2p^2-p-1 = (2p+1)(p-1)$ auch $a^{n-1} \equiv 1$ modulo n. Also ist n pseudoprim zur Basis a.

Lösung 6.47 zu Aufgabe 2.99 i) Wegen $341 = 11 \cdot 31$ und $4060 \equiv 1 \bmod 11$ sowie $4060 \equiv 30 \equiv -1 \bmod 31$ gilt

$$\left(\frac{4060}{341}\right) = \left(\frac{4060}{11}\right)\left(\frac{4060}{31}\right) = \left(\frac{1}{11}\right)\left(\frac{-1}{31}\right) = (-1)^{\frac{31-1}{2}} = (-1)^{15} = -1.$$

ii) Wegen $253 = 11 \cdot 23$ und $2584 \equiv 10 \equiv -1 \bmod 11$ sowie $2584 \equiv 8 \equiv 2^3 \bmod 23$ gilt

$$\left(\frac{2584}{253}\right) = \left(\frac{2584}{11}\right)\left(\frac{2584}{23}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{23}\right)^3 = \left(\frac{-1}{11}\right)\left(\frac{2}{23}\right).$$

Daraus folgt dann

$$\left(\frac{2584}{253}\right) = (-1)^{\frac{11-1}{2}} \cdot (-1)^{\frac{(23-1)(23+1)}{8}} = (-1) \cdot 1 = -1.$$

iii) Da 383 eine Primzahl ist, sind wegen $221 = 13 \cdot 17$ die beiden folgenden Jacobi-Symbole miteinander zu multiplizieren, die sich jeweils mit dem Reziprozitätsgesetz vereinfachen lassen.

$$\left(\frac{17}{383}\right) = (-1)^{\frac{(17-1)(383-1)}{4}} \left(\frac{383}{17}\right) = 1 \cdot \left(\frac{3}{17}\right)^2 = 1,$$

wobei $383 \equiv 9 \equiv 3^2 \bmod 17$ benutzt wurde, und

$$\left(\frac{13}{383}\right) = (-1)^{\frac{(13-1)(383-1)}{4}} \left(\frac{383}{13}\right) = \left(\frac{6}{13}\right) = -1.$$

Dabei kann der letzte Wert aus Beispiel 2.76 b) übernommen oder als Produkt der Legendre-Symbole $\left(\frac{2}{13}\right) = (-1)^{\frac{169-1}{8}} = (-1)^{21} = -1$ und $\left(\frac{3}{13}\right) = 1$ (wegen $4^2 \equiv 3 \bmod 13$) ermittelt werden.

iv) Da 2333 und 3673 Primzahlen sind (vgl. 7.1) und $3673 \equiv 1340 \bmod 2333$ sowie $1340 = 2^2 \cdot 5 \cdot 67$ gelten, liefert das Reziprozitätsgesetz zunächst

$$\left(\frac{2333}{3673}\right) = (-1)^{\frac{2332 \cdot 3672}{4}} \left(\frac{3673}{2333}\right) = \left(\frac{5}{2333}\right)\left(\frac{67}{2333}\right).$$

Diese beiden Legendre-Symbole kann man ebenfalls wieder nach dem Reziprozitätsgesetz vereinfachen:

$$\left(\frac{5}{2333}\right) = (-1)^{\frac{4 \cdot 2332}{4}} \left(\frac{2333}{5}\right) = \left(\frac{3}{5}\right) = -1,$$

da 3 offensichtlich kein quadratischer Rest modulo 5 ist. (Es sind $1^2 = 1 = 4^2$ und $2^2 = 4 = 3^2$ sämtliche Quadrate in $\mathbb{Z}/(5)^*$.)

$$\left(\frac{67}{2333}\right) = (-1)^{\frac{66 \cdot 2332}{4}} \left(\frac{2333}{67}\right) = \left(\frac{55}{67}\right) = \left(\frac{5}{67}\right)\left(\frac{11}{67}\right) = (-1) \cdot (-1) = 1.$$

Auch die letzten beiden Legendre-Symbole können mit dem Reziprozitätsgesetz ermittelt werden:

$$\left(\frac{5}{67}\right) = (-1)^{\frac{4\cdot 66}{4}} \left(\frac{67}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

$$\left(\frac{11}{67}\right) = (-1)^{\frac{10\cdot 66}{4}} \left(\frac{67}{11}\right) = (-1) \cdot \left(\frac{1}{11}\right) = -1.$$

Insgesamt erhält man also

$$\left(\frac{2333}{3673}\right) = -1.$$

7 Anhang

7.1 Primzahlen, Primzahlzwillinge und -drillinge bis 4000

Primzahlzwillinge sind hervorgehoben.

2	**3**	**5**	**7**	**11**	**13**	**17**	**19**	23	**29**
31	37	**41**	**43**	47	53	**59**	**61**	67	**71**
73	79	83	89	97					
101	**103**	**107**	**109**	113	127	131	**137**	**139**	**149**
151	157	163	167	173	**179**	**181**	**191**	**193**	**197**
199									
211	223	**227**	**229**	233	**239**	**241**	251	257	263
269	**271**	277	**281**	**283**	293				
307	**311**	**313**	317	331	337	**347**	**349**	353	359
367	373	379	383	389	397				
401	409	**419**	**421**	**431**	**433**	439	443	449	457
461	**463**	467	479	487	491	499			
503	509	**521**	**523**	541	547	557	563	**569**	**571**
577	587	593	**599**						
601	607	613	**617**	**619**	631	**641**	**643**	647	653
659	**661**	673	677	683	691				
701	709	719	727	733	739	743	751	757	761
769	773	787	797						
809	**811**	**821**	**823**	**827**	**829**	839	853	**857**	**859**
863	877	**881**	**883**	887					
907	911	919	929	937	941	947	953	967	971
977	983	991	997						
1009	1013	**1019**	**1021**	**1031**	**1033**	1039	**1049**	**1051**	**1061**
1063	1069	1087	**1091**	**1093**	1097				
1103	1109	1117	1123	1129	**1151**	**1153**	1163	1171	1181
1187	1193								
1201	1213	1217	1223	**1229**	**1231**	1237	1249	1259	**1277**
1279	1283	**1289**	**1291**	1297					
1301	**1303**	1307	**1319**	**1321**	1327	1361	1367	1373	1381
1399									
1409	1423	**1427**	**1429**	1433	1439	1447	**1451**	**1453**	1459
1471	**1481**	**1483**	**1487**	**1489**	1493	1499			
1511	1523	1531	1543	1549	1553	1559	1567	1571	1579
1583	1597								
1601	**1607**	**1609**	1613	**1619**	**1621**	1627	1637	1657	1663
1667	**1669**	1693	**1697**	**1699**					

1709	**1721**	**1723**	1733	1741	1747	1753	1759	1777	1783
1787	**1789**								
1801	1811	1823	1831	1847	1861	1867	**1871**	**1873**	**1877**
1879	1889								
1901	1907	1913	**1931**	**1933**	**1949**	**1951**	1973	1979	1987
1993	**1997**	**1999**							
2003	2011	2017	**2027**	**2029**	2039	2053	2063	2069	**2081**
2083	**2087**	**2089**	2099						
2111	**2113**	**2129**	**2131**	2137	**2141**	**2143**	2153	2161	2179
2203	2207	2213	2221	**2237**	**2239**	2243	2251	**2267**	**2269**
2273	2281	2287	2293	2297					
2309	**2311**	2333	**2339**	**2341**	2347	2351	2357	2371	2377
2381	**2383**	2389	2393	2399					
2411	2417	2423	2437	2441	2447	2459	2467	2473	2477
2503	2521	2531	2539	2543	**2549**	**2551**	2557	2579	**2591**
2593									
2609	2617	2621	2633	2647	**2657**	**2659**	2663	2671	2677
2683	**2687**	**2689**	2693	2699					
2707	**2711**	**2713**	2719	**2729**	**2731**	2741	2749	2753	2767
2777	**2789**	**2791**	2797						
2801	**2803**	2819	2833	2837	2843	2851	2857	2861	2879
2887	2897								
2903	2909	2917	2927	2939	2953	2957	2963	**2969**	**2971**
2999									
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089								
3109	**3119**	**3121**	3137	3163	**3167**	**3169**	3181	3187	3191
3203	3209	3217	3221	3229	**3251**	**3253**	**3257**	**3259**	3271
3299									
3301	3307	3313	3319	3323	**3329**	**3331**	3343	3347	**3359**
3361	**3371**	**3373**	**3389**	**3391**					
3407	3413	3433	3449	3457	**3461**	**3463**	**3467**	**3469**	3491
3499									
3511	3517	**3527**	**3529**	3533	**3539**	**3541**	3547	**3557**	**3559**
3571	**3581**	**3583**	3593						
3607	3613	3617	3623	3631	3637	3643	3659	**3671**	**3673**
3677	3691	3697							
3701	3709	3719	3727	3733	3739	3761	**3767**	**3769**	3779
3793	3797								
3803	**3821**	**3823**	3833	3847	**3851**	**3853**	3863	3877	3881
3889									
3907	3911	**3917**	**3919**	3923	**3929**	**3931**	3943	3947	3967
3989									

Primzahldrillinge und -vierlinge in diesem Bereich sind

p	$p+2$	$p+6$	$p+8$
5	7	11	13
11	13	17	19
17	19	23	-
41	43	47	-
101	103	107	109
107	109	113	-
191	193	197	199
227	229	233	-
311	313	317	-
347	349	353	-
461	463	467	-
641	643	647	-
821	823	827	829
857	859	863	-
881	883	887	-
1091	1093	1097	-
1277	1279	1283	-
1301	1303	1307	-
1427	1429	1433	-
1481	1483	1487	1489
1487	1489	1493	-
1607	1609	1613	-
1871	1873	1877	1879
1997	1999	2003	-
2081	2083	2087	2089
2237	2239	2243	-
2267	2269	2273	-
2657	2659	2663	-
2687	2689	2693	-
3251	3253	3257	3259
3461	3463	3467	3469
3527	3529	3533	-
3671	3673	3677	-
3917	3919	3923	-

7.2 Germain-Primzahlen und verwandte Primzahlen bis 200

p	$q = 2p + 1$	$q = 4p + 1$	$q = 8p + 1$	$q = 16p + 1$
2	-	-	17	31
3	7	13	-	-
5	11	-	41	-
7	-	29	-	113
11	23	-	89	-
13	-	53	-	-
17	-	-	137	-
23	47	-	-	-
29	59	-	233	-
37	-	149	-	593
41	83	-	-	-
43	-	173	-	-
53	107	-	-	-
61	-	-	-	977
67	-	269	-	-
71	-	-	569	-
73	-	293	-	-
79	-	317	-	-
83	167	-	-	-
89	179	-	-	-
97	-	389	-	1553
101	-	-	809	-
107	-	-	857	-
113	227	-	-	-
127	-	509	-	-
131	263	-	1049	-
137	-	-	1097	-
139	-	557	-	-
149	-	-	1193	-
151	-	-	-	2417
163	-	653	-	2609
173	347	-	-	-
179	359	-	1433	-
181	-	-	-	2897
191	383	-	-	-
193	-	773	-	3089
199	-	797	-	-

7.3 Primzahlen der Form n!+1 oder n!-1

n	Stellen	Jahr	Entdecker
34790!-1	142891	2002	Marchal, Carmody, Kuosa
26951!+1	107701	2002	Davis, Kuosa
21480!-1	83727	2001	Davis, Kuosa
6917!-1	23560	1998	Caldwell
6380!+1	21507	1998	Caldwell
3610!-1	11277	1993	Caldwell
3507!-1	10912	1992	Caldwell
1963!-1	5614	1992	Dubner, Caldwell
1477!+1	4042	1984	Dubner
974!-1	2490	1992	Dubner, Caldwell
872!+1	2188	1983	Dubner
546!-1	1260	1992	Dubner
469!-1	1051	1981	Penk, Buhler& Crandall

7.4 Primzahlen der Form p!+1 oder p!-1

n	Stellen	Jahr	Entdecker
392113#+1	169966	2001	Heuer
366439#+1	158936	2001	Heuer
145823#+1	63142	2000	Anderson, Robinson
42209#+1	18241	1999	Caldwell
24029#+1	10387	1993	Caldwell
23801#+1	10273	1993	Caldwell
18523#+1	8002	1989	Dubner
15877#-1	6845	1992	Caldwell, Dubner
13649#+1	5862	1987	Dubner
13033#-1	5610	1992	Caldwell, Dubner
11549#+1	4951	1986	Dubner
6569#-1	2811	1992	Dubner
4787#+1	2038	1984	Dubner
4583#-1	1953	1992	Dubner
4547#+1	1939	1984	Dubner
4297#-1	1844	1992	Dubner
4093#-1	1750	1992	Caldwell, Dubner
3229#+1	1368	1984	Dubner
2657#+1	1115	1981	Penk, Buhler & Crandall
2377#-1	1007	1992	Dubner

7.5 Größte bekannte Germain-Primzahlen

n	Stellen	Jahr	Entdecker
$2618163402417 \cdot 2^{1290000} - 1$	388342	2016	Scott Brown
$18543637900515 \cdot 2^{666667} - 1$	200701	2012	Lee Blyth
$183027 \cdot 2^{265440} - 1$	79911	2010	Tom Wu
$648621027630345 \cdot 2^{253824} - 1$	76424	2009	Jarai et al.
$620366307356565 \cdot 2^{253824} - 1$	76424	2009	Jarai et al.
$99064503957 \cdot 2^{200008} - 1$	60220	2016	S. Urushihata
$607095 \cdot 2^{176311} - 1$	53081	2009	Tom Wu
$48047305725 \cdot 2^{172403} - 1$	51910	2007	Underbakke
$137211741292195 \cdot 2^{171960} - 1$	51780	2006	Jarai et al.
$33759183 \cdot 2^{123458} - 1$	37173	2009	Tornberg
$7068555 \cdot 2^{121301} - 1$	36523	2005	Minovic
$2540041185 \cdot 2^{114729} - 1$	34547	2003	Underbakke
$1124044292325 \cdot 2^{107999} - 1$	32523	2006	Underbakke
$112886032245 \cdot 2^{10800} - 1$	32523	2006	Underbakke
$38588805195 \cdot 2^{100002} - 1$	30115	2009	Urushi
$15744710163 \cdot 2^{100002} - 1$	30114	2009	Urushi
$35909079387 \cdot 2^{100000} - 1$	30114	2009	Urushi
$18912879 \cdot 2^{98395} - 1$	29628	2002	Angel, Joblin, Augustin
$3364553235 \cdot 2^{88888} - 1$	26768	2009	Tom Wu
$10495740081 \cdot 2^{83125} - 1$	25034	2006	Underbakke
$61078155 \cdot 2^{82002} - 1$	24693	2006	Underbakke
$1213822389 \cdot 2^{81131} - 1$	24432	2002	Angel, Joblin, Augustin
$64670473 \cdot 2^{74146} + 1$	22328	2009	Saridis
$232197 \cdot 2^{73457} - 1$	22119	2009	Tom Wu

7.6 Anzahl der Germain-Primzahlen unterhalb n

n	$S_{2,1}(n)$
10	2
10^2	9
10^3	37
10^4	190
10^5	1171
10^6	7746
10^7	56032
10^8	423140
10^9	3308859
10^{10}	26569515
10^{11}	218116524

7.7 Anzahl der Primzahlzwillinge unterhalb n

n	$\pi_2(n)$
10	2
10^2	8
10^3	35
10^4	205
10^5	1224
10^6	8169
10^7	58980
10^8	440312
10^9	3424506
10^{10}	27412679
10^{11}	224376048
10^{12}	1870585220
10^{13}	15834664872
10^{14}	135780321665
10^{15}	1177209242304

7.8 Primzahlzwillinge mit über 1000 Dezimalstellen

$n \pm 1$	Stellen	Jahr	Entdecker
$2996863034895 \cdot 2^{1290000} \pm 1$	388342	2016	?
$3756801695685 \cdot 2^{666669} \pm 1$	200700	2011	?
$65516468355 \cdot 2^{333333} \pm 1$	100355	2009	Kaiser & Klahn
$12770275971 \cdot 2^{222225} \pm 1$	66907	2017	?
$70965694293 \cdot 2^{200006} \pm 1$	60219	2016	?
$66444866235 \cdot 2^{200003} \pm 1$	60218	2016	?
$4884940623 \cdot 2^{198800} \pm 1$	59855	2015	?
$2003663613 \cdot 2^{195000} \pm 1$	58711	2007	Vautier et al.
$38529154785 \cdot 2^{173250} \pm 1$	52165	2014	?
$194772106074315 \cdot 2^{171960} \pm 1$	51780	2007	Jarai et al.
$100314512544015 \cdot 2^{171960} \pm 1$	51780	2006	Jarai et al.
$16869987339975 \cdot 2^{171960} \pm 1$	51779	2005	Jarai et al.
$33218925 \cdot 2^{169690} \pm 1$	51090	2002	Papp
$22835841624 \cdot 7^{54321} \pm 1$	45917	2010	?
$1679081223 \cdot 2^{151618} \pm 1$	45651	2012	?
$9606632571 \cdot 2^{151515} \pm 1$	45621	2014	?
$84966861 \cdot 2^{140219} \pm 1$	42219	2012	?
$12378188145 \cdot 2^{140002} \pm 1$	42155	2010	?
$23272426305 \cdot 2^{140001} \pm 1$	42155	2010	?
$8151728061 \cdot 2^{125987} \pm 1$	37936	2010	?
$307259241 \cdot 2^{115599} \pm 1$	34808	2009	Tornberg
$60194061 \cdot 2^{114689} \pm 1$	34533	2002	Underbakker
$108615 \cdot 2^{110342} \pm 1$	33222	2008	Chatfield
$1765199373 \cdot 2^{107520} \pm 1$	32376	2002	McElhatton
$318032361 \cdot 2^{107001} \pm 1$	32220	2001	Underbakker & Carmody
$4501763715 \cdot 2^{100006} \pm 1$	30115	2009	Urushi
$34776437961 \cdot 2^{100001} \pm 1$	30114	2009	Urushi
$156733989 \cdot 2^{100007} \pm 1$	30114	2009	Urushi
$1046619117 \cdot 2^{100000} \pm 1$	30113	2007	Barnes
$1807318575 \cdot 2^{98305} \pm 1$	29603	2001	Underbakker & Carmody
$744678855 \cdot 2^{95000} \pm 1$	28607	2009	Vogel
$23321624 \cdot 3^{53005} \pm 1$	25298	2009	Chatfield
$1035928263 \cdot 2^{83200} \pm 1$	25055	2009	Oakes
$7473214125 \cdot 2^{83125} \pm 1$	25033	2006	Underbakker
$11694962547 \cdot 2^{83124} \pm 1$	25033	2006	Underbakker
$58950603 \cdot 2^{83130} \pm 1$	25033	2006	Underbakker
$5583295473 \cdot 2^{80828} \pm 1$	24342	2006	Tornberg

$n \pm 1$	Stellen	Jahr	Entdecker
$134583 \cdot 2^{80828} \pm 1$	24337	2005	Underbakker
$665551035 \cdot 2^{80025} \pm 1$	24099	2000	Underbakker & Carmody
$1046886225 \cdot 2^{70000} \pm 1$	21082	2004	Minovic
$8544353655 \cdot 2^{66666} \pm 1$	20079	2005	Heuer
$8179665447 \cdot 2^{66666} \pm 1$	20079	2006	Heuer
$6968409117 \cdot 2^{66666} \pm 1$	20079	2005	Heuer
$242206083 \cdot 2^{38880} \pm 1$	11713	1995	Indlekofer & Jarai
$570918348 \cdot 10^{5120} \pm 1$	5129	1995	Dubner
$697053813 \cdot 2^{16352} \pm 1$	4932	1994	Indlekofer & Jarai
$6797727 \cdot 2^{15328} \pm 1$	4622	1995	Forbes
$1692923232 \cdot 10^{4020} \pm 1$	4030	1993	Dubner
$4655478828 \cdot 10^{3429} \pm 1$	3439	1993	Dubner
$1706595 \cdot 2^{11235} \pm 1$	3389	1989	Parady et al.
$459 \cdot 2^{8529} \pm 1$	2571	1993	Dubner
$1171452282 \cdot 10^{2490} \pm 1$	2500	1991	Dubner
$571305 \cdot 2^{7701} \pm 1$	2324	1989	Parady et al.
$75188117004 \cdot 10^{2298} \pm 1$	2309	1989	Dubner
$663777 \cdot 2^{7650} \pm 1$	2309	1989	Parady et al.
$107570463 \cdot 10^{2250} \pm 1$	2259	1985	Dubner
$2846!!!! \pm 1$	2151	1992	Dubner
$43690485351513 \cdot 10^{1995} \pm 1$	2009	1985	Dubner
$260497545 \cdot 2^{6625} \pm 1$	2003	1984	Atkin und Rickert
$(10^{720} + 41038783014) \cdot 10^{710} \pm 1$	1431	1990	Dubner
$519912 \cdot 10^{1420} \pm 1$	1426	1984	Dubner
$217695 \cdot 10^{1404} \pm 1$	1410	1984	Dubner
$219649815 \cdot 2^{4481} \pm 1$	1358	1983	Atkin und Rickert
$1639494 \cdot (2^{4423} - 1) \pm 1$	1338	1983	Keller
$2445810 \cdot (2^{4253} - 1) \pm 1$	1287	1983	Keller
$218313 \cdot 10^{1068} \pm 1$	1074	1985	Dubner
$499032 \cdot 10^{1040} \pm 1$	1046	1984	Dubner
$403089 \cdot 10^{1040} \pm 1$	1046	1984	Dubner
$(123737321 + 10^{524}) \cdot 10^{516} \pm 1$	1041	1990	Dubner
$256200945 \cdot 2^{3426} \pm 1$	1040	1980	Atkin & Rickert
$1579134 \cdot 10^{1017} \pm 1$	1024	1992	Dubner
$3257996742 \cdot 10^{1009} \pm 1$	1019	1993	Dubner
$1869766899 \cdot 10^{1009} \pm 1$	1019	1993	Dubner

Es ist $2846!!!! \pm 1 = (2846 - 4)(2846 - 8) \cdots 6 \cdot 2 \pm 1$.

7.9 Primfaktoren der ersten 60 Fibonacci-Zahlen

Diese Werte wurden von E. Lucas erstmals berechnet, mittlerweile sind die Faktorisierungen bis $n = 720$ vollständig bekannt.

n	ϕ_n	Primfaktoren
3	2	2
4	3	3
5	5	5
6	8	2^3
7	13	13
8	21	$3 \cdot 7$
9	34	$2 \cdot 17$
10	55	$5 \cdot 11$
11	89	89
12	144	$2^4 \cdot 3^2$
13	233	233
14	377	$13 \cdot 29$
15	610	$2 \cdot 5 \cdot 61$
16	987	$3 \cdot 7 \cdot 47$
17	1597	1597
18	2584	$2^3 \cdot 17 \cdot 19$
19	4181	$37 \cdot 113$
20	6765	$3 \cdot 5 \cdot 11 \cdot 41$
21	10946	$2 \cdot 13 \cdot 421$
22	17711	$89 \cdot 199$
23	28657	28657
24	46368	$2^5 \cdot 3^2 \cdot 7 \cdot 23$
25	75025	$5^2 \cdot 3001$
26	121393	$233 \cdot 521$
27	196418	$2 \cdot 17 \cdot 53 \cdot 109$
28	317811	$3 \cdot 13 \cdot 29 \cdot 281$
29	514229	514229
30	832040	$2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$

n	ϕ_n	Primfaktoren
31	1346269	$557 \cdot 2417$
32	2178309	$3 \cdot 7 \cdot 47 \cdot 2207$
33	3524578	$2 \cdot 89 \cdot 19801$
34	5702887	$1597 \cdot 3571$
35	9227465	$5 \cdot 13 \cdot 141961$
36	14930352	$2^4 \cdot 3^3 \cdot 17 \cdot 19 \cdot 107$
37	24157817	$73 \cdot 149 \cdot 2221$
38	39088169	$37 \cdot 113 \cdot 9349$
39	63245986	$2 \cdot 233 \cdot 135721$
40	102334155	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 41 \cdot 2161$
41	165580141	$2789 \cdot 59369$
42	267914296	$2^3 \cdot 13 \cdot 29 \cdot 211 \cdot 421$
43	433494437	433494437
44	701408733	$3 \cdot 43 \cdot 89 \cdot 199 \cdot 307$
45	1134903170	$2 \cdot 5 \cdot 17 \cdot 61 \cdot 109441$
46	1836311903	$139 \cdot 461 \cdot 28657$
47	2971215073	2971215073
48	4807526976	$2^6 \cdot 3^2 \cdot 7 \cdot 23 \cdot 47 \cdot 1103$
49	7778742049	$13 \cdot 97 \cdot 6168709$
50	12586269025	$5^2 \cdot 11 \cdot 101 \cdot 151 \cdot 3001$
51	20365011074	$2 \cdot 1597 \cdot 6376021$
52	32951280099	$3 \cdot 233 \cdot 521 \cdot 90481$
53	53316291173	$953 \cdot 55945741$
54	86267571272	$2^3 \cdot 17 \cdot 19 \cdot 53 \cdot 109 \cdot 5779$
55	139583862445	$5 \cdot 89 \cdot 661 \cdot 474541$
56	225851433717	$3 \cdot 7^2 \cdot 13 \cdot 29 \cdot 281 \cdot 14503$
57	365435296162	$2 \cdot 37 \cdot 113 \cdot 797 \cdot 54833$
58	591286729879	$59 \cdot 19489 \cdot 514229$
59	956722026041	$353 \cdot 2710260697$
60	1548008755920	$2^4 \cdot 3^2 \cdot 5 \cdot 11 \cdot 31 \cdot 41 \cdot 61 \cdot 2521$

7.10 Faktorisierungen der ersten dezimalen Repunits

n	R_n
1	1
2	prim
3	$3 \cdot 37$
4	$11 \cdot 101$
5	$41 \cdot 271$
6	$3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$
7	$239 \cdot 4649$
8	$11 \cdot 73 \cdot 101 \cdot 137$
9	$3^2 \cdot 37 \cdot 333667$
10	$11 \cdot 41 \cdot 271 \cdot 9091$
11	$21649 \cdot 513239$
12	$3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 101 \cdot 9901$
13	$53 \cdot 79 \cdot 265371653$
14	$11 \cdot 239 \cdot 4649 \cdot 909091$
15	$3 \cdot 31 \cdot 37 \cdot 41 \cdot 271 \cdot 2906161$
16	$11 \cdot 17 \cdot 73 \cdot 101 \cdot 137 \cdot 5882353$
17	$2071723 \cdot 5363222357$
18	$3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 37 \cdot 52579 \cdot 333667$
19	prim
20	$11 \cdot 41 \cdot 101 \cdot 271 \cdot 3541 \cdot 9091 \cdot 27961$
21	$3 \cdot 37 \cdot 43 \cdot 239 \cdot 1933 \cdot 4649 \cdot 10838689$
22	$11^2 \cdot 23 \cdot 4093 \cdot 8779 \cdot 21649 \cdot 513239$
23	prim
24	$3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot 73 \cdot 101 \cdot 9901 \cdot 9990001$
25	$41 \cdot 271 \cdot 21401 \cdot 25601 \cdot 182521213001$

7.11 Die bekannten Mersenneschen Primzahlen

n	p	Dezimalstellen	Jahr	Entdecker
1	2	1	-	-
2	3	1	-	-
3	5	2	-	-
4	7	3	-	-
5	13	4	1461	unbekannt
6	17	6	1588	P. A. Cataldi
7	19	6	1588	P. A. Cataldi
8	31	10	1750	L. Euler
9	61	19	1883	I. M. Pervushin
10	89	27	1911	R. E. Powers
11	107	33	1913	E. Fauquembergue
12	127	39	1876	E. Lucas
13	521	157	1952	R. M. Robinson
14	607	183	1952	R. M. Robinson
15	1279	386	1952	R. M. Robinson
16	2203	664	1952	R. M. Robinson
17	2281	687	1952	R. M. Robinson
18	3217	969	1957	H. Riesel
19	4253	1281	1961	A. Hurwitz
20	4423	1332	1961	A. Hurwitz
21	9689	2917	1963	D. B. Gillies
22	9941	2993	1963	D. B. Gillies
23	11213	3376	1963	D. B. Gillies
24	19937	6002	1971	B. Tuckerman
25	21701	6533	1978	C. Noll & L. Nickel
26	23209	6987	1979	C. Noll
27	44497	13395	1979	H. Nelson & D. Slowinski
28	86243	25962	1982	D. Slowinski
29	110503	33265	1988	W. N. Colquitt & L. Welsh
30	132049	39751	1983	D. Slowinski
31	216091	65050	1985	D. Slowinski
32	756839	227832	1992	D. Slowinski & P. Gage
33	859433	258716	1994	D. Slowinski & P. Gage

n	p	Dezimalstellen	Jahr	Entdecker
34	1257787	378632	1996	D. Slowinski & P. Gage
35	1398269	420921	1996	Woltman et al.
36	2976221	895932	1997	Woltman et al.
37	3021377	909526	1998	Woltman, Kurowski et al.
38	6972593	2098960	1999	Woltman, Kurowski et al.
39	13466917	4053946	2001	Woltman, Kurowski et al.
40	20996011	6320430	2003	Woltman, Kurowski et al.
41	24036583	7235733	2004	Woltman, Kurowski et al.
42	25964951	7816230	2005	Woltman, Kurowski et al.
43	30402457	9152052	2005	Woltman, Kurowski et al.
44	32582657	9808358	2006	Woltman, Kurowski et al.
45	37156867	11185272	2009	Woltman, Kurowski et al.
46	42643801	12837064	2008	Woltman, Kurowski et al.
47	43112609	12978189	2008	Woltman, Kurowski et al.
48*	57885161	17425170	2013	Woltman, Kurowski et al.
49*	74207281	22338618	2016	Woltman, Kurowski et al.
50*	77232917	23249425	2017	Woltman, Kurowski et al.
51*	82589933	24862048	2018	Woltman, Kurowski et al.

* bedeutet: Es sind noch nicht alle Primzahlen bis p getestet.

7.12 Große Prothsche Primzahlen

Primzahlen der Form $k \cdot 2^n + 1$ mit $k < 2^n$, vgl. [3], 5.3. Primfaktoren von Fermat-Zahlen sind hervorgehoben. Für kleine k sind noch wesentlich mehr n bekannt!

k	n								
3	2	5	6	8	12	18	30	36	**41**
	66	189	201	**209**	276	353	408	438	534
	2208	2816	3168	3189	3912	20909	34350	42294	42665
5	3	**7**	13	15	**25**	**39**	55	**75**	85
	127	**1947**	**3313**	4687	5947	13165	**23473**	26607	**125413**
7	4	5	**14**	20	26	50	52	92	**120**
	174	180	190	**290**	**320**	390	432	616	830
9	6	7	11	14	17	33	42	43	63
	65	**67**	81	134	162	206	211	366	663
11	5	7	19	21	43	81	125	127	209
13	8	10	**20**	28	82	188	308	316	1000
15	4	9	10	12	27	37	38	44	48
	78	112	168	**229**	297	339	517	522	654
17	15	27	51	**147**	243	267	347	471	**747**
19	6	10	46	366	1246	2038	4386	4438	**6838**
21	5	7	9	12	16	17	**41**	124	128
	129	187	209	**276**	313	397	899	1532	1613
23	9	13	29	41	49	69	73	341	381
25	6	10	20	22	52	64	78	184	232
	268	340	448	554	664	740	748	1280	1328
27	7	16	19	20	22	26	40	44	46
	47	50	56	59	64	92	175	215	275
29	5	11	27	43	**57**	75	77	93	103
	143	185	**231**	245	391	1053	1175	**2027**	3627
31	8	60	68	140	216	416	1808	1944	9096
33	6	13	18	21	22	25	28	66	93
	118	289	412	453	525	726	828	1420	1630
35	7	9	13	15	31	45	47	49	55
	147	245	327	355	663	1423	1443	2493	3627
37	8	10	12	**16**	22	26	68	82	84
	106	110	166	236	254	286	290	712	1240
39	7	10	11	**13**	14	18	21	22	31
	42	67	70	71	73	251	370	375	389
41	11	19	215	289	379	1991	7607	8411	12493
43	6	12	18	26	32	94	98	104	144
	158	252	778	1076	2974	3022	3528	4344	5322

k	n								
45	9	12	14	23	24	29	60	189	200
	333	372	43	464	801	1374	6146	6284	6359
47	583	1483	6115						
49	6	10	30	42	54	66	118	390	594
51	7	9	13	17	25	43	53	83	89
	119	175	187	257	263	267	321	333	695
53	17	21	61	85	93	105	133	485	857
55	8	16	22	32	94	220	244	262	286
57	7	8	10	16	18	19	40	48	55
	90	96	98	190	398	456	502	719	1312
59	11	27	35	291	1085	2685	9195	15995	22455
61	12	48	88	168	3328	172428	285652		
63	9	10	14	17	18	21	25	37	38
	44	60	65	94	133	153	228	280	314
	326	334	340	410	429	626	693	741	768
65	11	17	21	29	47	85	93	129	151
	205	239	257	271	307	351	397	479	553
67	14	20	44	66	74	102	134	214	236
69	10	14	19	26	50	55	145	515	842
71	9	19	23	27	57	59	65	119	299
73	14	24	30	32	42	44	60	110	212
75	7	10	12	34	43	51	57	60	63
	67	87	102	163	222	247	312	397	430
77	7	19	23	95	287	483	559	655	667
79	10	46	206	538	970	1330	1766	2162	20666
81	7	12	15	16	21	25	27	32	35
	36	39	48	89	104	121	125	148	152
83	5	157	181	233	373	2425	2773	3253	4129
85	10	30	34	36	38	74	88	94	148
87	8	18	26	56	78	86	104	134	207
89	7	9	21	37	61	589	711	1537	1921
91	8	168	260	696	5028	5536	6668	13388	14220
93	10	12	30	42	44	52	70	76	108
	122	164	170	226	298	398	686	1020	1110
95	7	13	17	21	53	57	**61**	83	89
	111	167	175	237	533	621	661	753	993
97	14	20	40	266	400	652	722	2026	2732
99	10	11	22	31	33	34	41	42	53
	58	65	82	126	143	162	170	186	189

k	n								
101	9	17	21	27	39	45	47	71	95
	117	123	143	173	387	389	513	633	827
103	16	18	30	40	58	138	250	616	622
105	7	8	12	14	23	27	33	38	49
	61	62	85	93	94	107	155	182	215
107	7	23	27	291	303	311	479	567	3087
109	14	58	62	318	1574	2034	26082	96838	103146
111	28	32	44	47	71	128	137	193	676
113	13	33	145	365	409	509	553	673	733
115	12	20	26	42	114	228	396	456	482
117	10	16	30	36	91	94	156	382	454
119	7	**13**	21	23	45	63	553	1115	2471
121	8	12	44	84	96	228	264	320	732
123	8	17	21	29	32	46	57	69	128
	141	268	333	476	742	832	1173	1677	5068
125	7	17	25	35	67	281	331	491	581
127	12	18	24	54	72	114	180	214	504
129	21	27	59	75	111	287	414	786	966
131	9	13	19	21	25	51	55	97	153
	165	199	261	285	361	373	465	475	529
133	10	16	30	124	174	192	336	600	720
135	10	15	18	20	30	31	35	38	39
	51	85	90	106	108	202	238	253	282
137	27	39	83	203	395	467	875	1979	6939
139	14	914	12614	335522	1567874				
141	8	12	15	20	31	33	37	41	61
	65	91	93	103	117	133	137	141	160
	291	303	343	488	535	555	556	640	756
143	53	77	293	333	393	809	825	20973	85349
145	16	28	70	76	250	276	312	562	636
147	8	11	15	18	19	26	44	60	84
	90	91	134	155	179	258	275	475	620
149	9	15	17	27	33	35	57	125	127
	137	191	513	819	827	921	931	1047	1147

7.13 Faktoren der kleineren Fermat-Zahlen

F_m bezeichnet die m-te Fermat-Zahl $2^{2^m}+1$, PN jeweils eine N-stellige Primzahl, CN eine N-stellige zusammengesetzte Zahl.

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65537$ sind prim.

m	F_m
5	$641 \cdot 6700417 = (5 \cdot 2^7 + 1) \cdot (3 \cdot 17449 \cdot 2^7 + 1)$
6	$274177 \cdot 67280421310721 =$ $(7 \cdot 9 \cdot 17 \cdot 2^8 + 1) \cdot (5 \cdot 47 \cdot 373 \cdot 2998279 \cdot 2^8 + 1)$
7	$59649589127497217 \cdot 5704689200685129054721 =$ $(116503103764643 \cdot 2^9 + 1) \cdot (3^5 \cdot 5 \cdot 12497 \cdot 733803839347 \cdot 2^9 + 1)$
8	$1238926361552897 (= 157 \cdot 3853149761 \cdot 2^{11} + 1) \cdot P62$
9	$2424833 (= 37 \cdot 2^{16} + 1) \cdot$ $7455602825647884208337395736200454918783366342657 \cdot P99$
10	$45592577 (= 11131 \cdot 2^{12} + 1) \cdot 6487031809 (= 3^2 \cdot 29 \cdot 37 \cdot 41 \cdot 2^{14} + 1) \cdot$ $4659775785220018543264560743076778192897 \cdot P252$
11	$319489 (= 3 \cdot 13 \cdot 2^{13} + 1) \cdot 974849 (= 7 \cdot 17 \cdot 2^{13} + 1) \cdot$ $167988556341760475137 \cdot 356084190644583392051 3 \cdot P564$
12	$114689 (= 7 \cdot 2^{14} + 1) \cdot 26017793 (= 397 \cdot 2^{16} + 1) \cdot$ $63766529 (= 7 \cdot 139 \cdot 2^{16} + 1) \cdot 190274191361 \cdot 1256132134125569 \cdot$ $56863064753535695516903341094086780483936074206081843 3 \cdot C1133$
13	$2710954639361 \cdot 2663848877152141313 \cdot$ $3603109844542291969 \cdot 319546020820551643220672513 \cdot C2391$
14	$1169280858730743698290359938345963713403867034233733 13 \cdot C4880$
15	$1214251009 (= 3 \cdot 193 \cdot 2^{21} + 1) \cdot 2327042503868417 \cdot$ $168768817029516972383024127016961 \cdot C9808$
16	$825753601 \cdot 188981757975021318420037633 \cdot C19694 =$ $(3^2 \cdot 5^2 \cdot 7 \cdot 2^{19} + 1) \cdot$ $(3^2 \cdot 31 \cdot 37 \cdot 13669 \cdot 1277254085461 \cdot 2^{20} + 1) \cdot C19694$
17	$31065037602817 (= 3 \cdot 7 \cdot 281517 \cdot 2^{19} + 1) \cdot$ $77510610998025225893589670583928869226935804231 69 \cdot C39395$
18	$13631489 \cdot 8127469070386051258777 \cdot C78884 =$ $(13 \cdot 2^{20} + 1) \cdot (29 \cdot 293 \cdot 1259 \cdot 905678539 \cdot 2^{23} + 1) \cdot C78884$
19	$70525124609 \cdot 646730219521 \cdot 37590055514133754286524446080499713$ $\cdot C157770 = (33629 \cdot 2^{21} + 1) \cdot (3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 89 \cdot 2^{21} + 1)$ $\cdot (896216762402862412608252670 3 \cdot 2^{22} + 1) \cdot C157770$
20	$C315653$
21	$4485296422913 (= 503 \cdot 1063 \cdot 2^{23} + 1) \cdot C631294$
22	$64658705994591851009055774868504577 \cdot C1262577$
23	$167772161 (= 5 \cdot 2^{25} + 1) \cdot C2525215$
24	$C5050446$

7.14 Bekannte Primfaktoren der größeren Fermat-Zahlen

Hier ist $p = k \cdot 2^{m+d} + 1$ Teiler von F_m.

m	k	d	m	k	d
25	48413	4	75	3447431	2
	1522849979	2	77	425	2
	16168301139	2		5940341195	2
26	143165	3	81	271	3
27	141015	3	83	1595863660157	4
	430816215	2	66	20018578522347	2
28	25709319373	8	88	119942751127	2
29	1120049	2	90	198922467387	2
30	149041	2	91	1421	2
	127589	3	93	92341	3
31	5463561471303	2	94	482524552001	3
32	1479	2	96	3334131633063	5
36	5	3	99	16233	5
	3759613	2	107	1289179925	4
37	1275438465	2	116	3433149787	4
38	3	3	117	7	3
	2653	2	122	5234775	2
39	21	2	125	5	2
	2864929972774011	2	133	88075576149	2
42	43485	3	142	8152599	3
	111318179143061	3	144	17	3
43	212675402445	2	146	37092477	2
48	2139543641769	2	147	3125	2
52	4119	2		124567335	2
	21626655	2	150	5439	4
	81909357657279	2		1575	7
55	29	2	164	1835601567	3
58	95	3	166	2674670937447	5
61	54985063	5	172	20569603303	2
62	697	2	178	313047661	2
63	9	4	184	117012935	3
64	17853639	3	201	4845	3
65	1210895760431083	3	205	232905	2
66	7551	3	207	3	2
71	683	2	215	32111	2
72	76432329	2	226	15	3
73	5	2	228	29	3

m	k	d	m	k	d
230	372236097	2	579	63856313	2
232	70899775	4	600	6213186413	5
250	403	2	620	10084141	4
251	85801657	3	635	4258979	10
255	629	2	637	11969	6
256	36986355	2	642	52943971	2
259	36654265	3	667	491628159	2
267	177	4	692	717	3
268	21	8	723	554815	7
275	22347	4	744	17	3
284	7	6	851	497531	8
	1061341513	2	885	16578999	2
286	78472588395	2	906	57063	2
287	5915	2	931	1985	2
297	72677552745	4	943	4785972759	11
298	247	4	971	541664191	5
299	272392805475	5	1069	137883	4
301	7183437	3	1082	82165	2
316	7	4	1114	11618577	2
329	1211	4	1123	25835	2
334	27609	7	1132	10111717305	4
338	27654487	4	1160	2018719057	2
343	4844391185	2	1201	837747239	2
353	18908555	2	1225	79707	6
370	573230511	3	1229	29139	4
375	733251	2	1394	62705223	2
376	810373	2	1451	13143	3
380	321116871	2	1551	291	2
398	120845	3	1598	10923781	2
416	8619	2	1710	351276975	9
	38039	3	1722	364182745	2
417	118086729	3	1849	98855	2
	303472680883	3	1945	5	2
431	5769285	3	1990	150863	3
452	27	3	2023	29	4
468	27114089	3	2059	591909	4
480	5673968845	4	2089	432	10
517	84977118993	3	2420	103257279	2
544	225	3	2456	85	2
547	77377	3	2606	238451805	2
556	127	2	3310	5	3
569	6616590375	6	3314	406860969	8

m	k	d
3335	43714055	2
3506	501	2
3703	262254673	3
3723	13308899	2
4250	173373	2
4258	1435	4
4265	72179955	4
4332	2466157	2
4652	143918649	2
4724	29	3
5320	21341	3
5531	1503975	2
5792	8872947	2
5957	421435	3
6208	763	2
6355	115185	3
6390	303	3
6537	17	2
6835	19	3
6909	6021	3
7181	168329	6
7309	145	3
8239	7473	3
8269	592131	2
8298	1054057	2
8555	645	2
9322	8247	2
9428	9	3
9447	5505161	2
9448	19	2
9549	1211	2
9691	260435	2
11695	203355	8
12185	81	4
12825	1814649	2
13250	351	2
13623	48265	3
14252	1173	2
14276	157	4
14528	17217	2
15161	55	3
17748	3860269	2
17906	135	3
18749	11	10
18757	33	9

m	k	d
18749	11	10
18757	33	9
19211	13323	9
22296	4777	2
23069	681	2
23288	19	2
23471	5	2
24651	99	2
25006	57	4
28281	81	4
30256	121531	4
35563	357	4
38967	177795	2
41894	4935	3
43665	2495	2
48624	28949	3
49093	165	2
49488	71007	2
50078	7619	3
60079	5731	5
63679	169	7
79221	6089	2
83861	99	2
90057	189	4
91213	585	2
94798	21	3
95328	7	2
104448	927	3
106432	30967	4
113547	39	2
114293	13	3
125410	5	3
138557	7333	3
142460	159	2
146221	57	2
157167	3	2
213321	3	2
221670	3771	6
226614	4479	4
270091	63	3
282717	51	2
287384	211	4
303088	3	5
338295	485	2
352279	7905	2

m	k	d
382447	3	2
410105	1207	3
461076	9	5
472097	89	2
476624	651	8
495728	243	4
567233	519	2
585042	151	2
617813	659	2
672005	27	2
906108	1705	2
960897	11	4
1246013	329	4
1494096	131	3
2141872	25	12
2145351	3	2
2167797	7	3
2478782	3	3
2543548	9	3

7.15 Pseudoprimzahlen

Basis										
2	341	561	645	1105	1387	1729	1905	2047	2465	2701
	2821	3277	4033	4369	4371	4681	5461	6601	7957	8321
3	91	121	286	671	703	949	1105	1541	1729	1891
4	15	85	91	341	435	551	561	645	703	1105
5	4	124	217	561	781	1541	1729	1891	2821	4123
6	35	185	217	301	481	1105	1111	1261	1333	1729
7	6	25	325	561	703	817	1105	1825	2101	2353
8	9	21	45	63	65	105	117	133	153	231
9	4	8	28	52	91	121	205	286	364	511

7.16 Starke Pseudoprimzahlen

Basis						
2	2047	3277	4033	4681	8321	
3	121	703	1891	3281	8401	8911
4	341	1387	2047	3277	4033	4371
5	781	1541	5461	5611	7813	
6	217	481	1111	1261	2701	
7	25	325	703	2101	2353	4525
8	9	65	481	511	1417	2047
9	91	121	671	703	1541	1729

7.17 Euler-Pseudoprimzahlen

Basis									
2	341	561	1105	1729	1905	2047	2465	4033	4681
3	121	703	1729	1891	2821	3281	7381		

7.18 Carmichael-Zahlen unterhalb 1000000

n	Primfaktoren
561	$3 \cdot 11 \cdot 17$
1105	$5 \cdot 13 \cdot 17$
1729	$7 \cdot 13 \cdot 19$
2465	$5 \cdot 17 \cdot 29$
2821	$7 \cdot 13 \cdot 31$
6601	$7 \cdot 23 \cdot 41$
8911	$7 \cdot 19 \cdot 67$
10585	$5 \cdot 29 \cdot 73$
15841	$7 \cdot 31 \cdot 73$
29341	$13 \cdot 37 \cdot 61$
41041	$7 \cdot 11 \cdot 13 \cdot 41$
46657	$13 \cdot 37 \cdot 97$
52633	$7 \cdot 73 \cdot 103$
62745	$3 \cdot 5 \cdot 47 \cdot 89$
63973	$7 \cdot 13 \cdot 19 \cdot 37$
75361	$11 \cdot 13 \cdot 17 \cdot 31$
101101	$7 \cdot 11 \cdot 13 \cdot 101$
115921	$13 \cdot 37 \cdot 241$
126217	$7 \cdot 13 \cdot 19 \cdot 73$
162401	$17 \cdot 41 \cdot 233$
172081	$7 \cdot 13 \cdot 31 \cdot 61$
188461	$7 \cdot 13 \cdot 19 \cdot 109$

n	Primfaktoren
252601	$41 \cdot 61 \cdot 101$
278545	$5 \cdot 17 \cdot 29 \cdot 113$
294409	$37 \cdot 73 \cdot 109$
314821	$13 \cdot 61 \cdot 397$
334153	$19 \cdot 43 \cdot 409$
340561	$13 \cdot 17 \cdot 23 \cdot 67$
399001	$31 \cdot 61 \cdot 211$
410041	$41 \cdot 73 \cdot 137$
449065	$5 \cdot 19 \cdot 29 \cdot 163$
488881	$37 \cdot 73 \cdot 181$
512461	$31 \cdot 61 \cdot 271$
530881	$13 \cdot 97 \cdot 421$
552721	$13 \cdot 17 \cdot 41 \cdot 61$
656601	$3 \cdot 11 \cdot 101 \cdot 197$
658801	$11 \cdot 13 \cdot 17 \cdot 271$
670033	$7 \cdot 13 \cdot 37 \cdot 199$
748657	$7 \cdot 13 \cdot 19 \cdot 433$
825265	$5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$
838201	$7 \cdot 13 \cdot 61 \cdot 151$
852841	$11 \cdot 31 \cdot 41 \cdot 61$
997633	$7 \cdot 13 \cdot 19 \cdot 577$

7.19 Anzahl der Primzahlen und Carmichael-Zahlen unterhalb n

n	$\pi(n)$	$C(n)$
10	4	0
10^2	25	0
10^3	168	1
10^4	1229	7
10^5	9592	16
10^6	78498	43
10^7	664579	105
10^8	5761455	255
10^9	50847534	646
10^{10}	455052511	1547
10^{11}	4118054813	3605
10^{12}	37607912018	8241
10^{13}	346065536839	19279
10^{14}	3204941750802	44706
10^{15}	29844570422669	105212
10^{16}	279238341033925	246683
10^{17}	2625557157654233	585355
10^{18}	24739954287740860	1401644
10^{19}	234057667276344607	3381806
10^{20}	2220819602560918840	8220777

7.20 Kleinste Primitivwurzeln modulo p bis 1200

Die kleinsten Primitivwurzeln modulo p, die nicht größer als $\sqrt[5]{p}$ sind, sind blau hervorgehoben (Satz von Burgess).

p	a	p	a	p	a	p	a	p	a
2	**1**	173	2	401	3	647	5	929	3
3	**2**	179	2	**409**	**21**	653	2	937	5
5	2	181	2	419	2	659	2	941	2
7	**3**	**191**	**19**	421	2	661	2	947	2
11	2	193	5	431	7	673	5	953	3
13	2	197	2	433	5	677	2	967	5
17	3	199	3	439	15	683	5	971	6
19	2	211	2	443	2	691	3	977	3
23	**5**	223	3	449	3	701	2	983	5
29	2	227	2	457	13	709	2	991	6
31	3	229	6	461	2	719	11	997	7
37	2	233	3	463	3	727	5	1009	11
41	**6**	239	7	467	2	733	6	1013	3
43	3	241	7	479	13	739	3	1019	2
47	5	251	6	487	3	743	5	1021	10
53	2	257	3	491	2	751	3	1031	14
59	2	263	5	499	7	757	2	1033	5
61	2	269	2	503	5	761	6	1039	3
67	2	271	6	509	2	769	11	1049	3
71	**7**	277	5	521	3	773	2	1051	7
73	5	281	3	523	2	787	2	1061	2
79	3	283	3	541	2	797	2	1063	3
83	2	293	2	547	2	809	3	1069	6
89	3	307	5	557	2	811	3	1087	3
97	5	311	17	563	2	821	2	1091	2
101	2	313	10	569	3	827	2	1093	5
103	5	317	2	571	3	829	2	1097	3
107	2	331	3	577	5	839	11	1103	5
109	6	337	10	587	2	853	2	1109	2
113	3	347	2	593	3	857	3	1117	2
127	3	349	2	599	7	859	2	1123	2
131	2	353	3	601	7	863	5	1129	11
137	3	359	7	607	3	877	2	1151	17
139	2	367	6	613	2	881	3	1153	5
149	2	373	6	617	3	883	2	1163	5
151	6	379	2	619	2	887	5	1171	2
157	5	383	5	631	3	907	2	1181	7
163	2	389	2	641	3	911	17	1187	2
167	5	397	5	643	11	919	7	1193	3

Literatur

[1] W. Borho, J. C. Jantzen, H. Kraft, et al. *Mathematische Miniaturen 1 - Lebendige Zahlen*. Birkhäuser Verlag, 1981.

[2] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp.*, 29:620 – 647, 1975.

[3] T. W. Cusick, C. Ding, and A. Renvall. *Stream Ciphers and Number Theory*. North-Holland Mathematical Library, 2004.

[4] L. Holzer. *Zahlentheorie I*. Teubner, 1958.

[5] L. Holzer. *Zahlentheorie II*. Teubner, 1959.

[6] L. Holzer. *Zahlentheorie III*. Teubner, 1965.

[7] G. Ifrah. *Universalgeschichte der Zahlen*. Campus Verlag, 1986.

[8] K. Kiyek and F. Schwarz. *Mathematik für Informatiker 1*. Teubner, 1989.

[9] U. Knauer. *Diskrete Strukturen - kurz gefasst*. Spektrum Akademischer Verlag, 2001.

[10] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag, 1994.

[11] F. Padberg. *Elementare Zahlentheorie*. Spektrum Verlag, 1996.

[12] A. Scholz and B. Schoeneberg. *Einführung in die Zahlentheorie*. de Gruyter, 1955.

[13] R. Schulze-Pillot. *Elementare Algebra und Zahlentheorie*. Springer, 2007.

[14] S. Wagon. *Mathematica in Aktion*. Spektrum Verlag, 1993.

[15] H. C. Williams. *Édouard Lucas and Primality Testing*. John Wiley & Sons, Inc, 1998.

[16] S. Y. Yan. *Perfect, Amicable and Sociable Numbers*. World Scientific, 1996.

Index