die Ziffern von $Z_0(n)$ in eine Liste `[1,2,3,...]` zu schreiben und darin jeweils die Streichungen vorzunehmen.

(2) Man finde einen Algorithmus, der Werte der Funktion

$$n \mapsto Z^*(n) \ : \ \mathbb{N} \to \{0,1,2,3,4,5,6,7,8,9\}$$

effizienter berechnet als das direkte Verfahren. Diese Aufgabe wurde einmal bei einer Mathematik-Olympiade gestellt, vgl. Redfern [88].

## 2 Primzahlen

**(2.1)** C. F. Gauß (1777 – 1855) schreibt in den "Disquisitiones arithmeticae", seinem großen Lehrbuch der Zahlentheorie aus dem Jahr 1801: "Problema, numeros primos a compositis dignoscendi, hosque in factores suos primos resolvendi, ad gravissima ac utilissima totius arithmeticae pertinere, et geometrarum tum veterum tum recentiorum industriam ac sagacitatem occupavisse, tam notum est, ut de hac re copiose loqui superfluum foret" (vgl. Gauß [37], Artikel 329; nach der Übersetzung von H. Maser (1889): "Daß die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten wie auch der neueren Mathematiker in Anspruch genommen hat, ist so bekannt, daß es überflüssig wäre, hierüber viele Worte zu verlieren"). Noch immer befassen sich Mathematiker mit dieser Aufgabe: Daß man sich für schnelle Primzahltests und für effiziente Algorithmen zur Faktorisierung natürlicher Zahlen interessiert, liegt heute auch an Anwendungen der Zahlentheorie in der Kryptologie, von denen in § 9 berichtet wird.

In diesem Paragraphen werden in erster Linie einige grundlegende Begriffe und Ergebnisse vorgestellt – Dinge, die durchaus der Schulmathematik angehören. Die Rechenverfahren, die dabei behandelt werden, haben mehr prinzipielle Bedeutung; sie liefern keine praktisch brauchbaren Algorithmen. Ein Primzahltest, der von großer praktischer Bedeutung ist, wird später in § 7 behandelt werden; von Faktorisierungverfahren, die über den üblicherweise in der Schule behandelten Stoff hinausgehen, wird in diesem Paragraphen in den Abschnitten (2.21) und (2.25) und in § 14 die Rede sein.

In diesem Buch kann nur ein kleiner Einblick in den Teil der Zahlentheorie gegeben werden, der sich mit Primzahlen beschäftigt. Wer sich näher für Primzahlen interessiert, sollte zu dem schönen Buch [89] von P. Ribenboim greifen: Es behandelt anregend und ausführlich viele Dinge, auf die hier nicht eingegangen werden kann, und erschließt auf den etwa hundert Seiten seines Literaturverzeichnisses die Originalliteratur bis zum Jahr 1988.

**(2.2) Definition:** Eine natürliche Zahl $p$ heißt eine Primzahl, wenn gilt: Es ist $p > 1$, und $1$, $-1$, $p$ und $-p$ sind die einzigen Teiler von $p$.

**(2.3) Bemerkung:** Es sei $a$ eine ganze Zahl mit $|a| > 1$. Dann ist

$$p := \min(\{d \in \mathbb{N} \mid d > 1;\ d \text{ teilt } a\})$$

ein Primteiler von $a$ (d.h. eine Primzahl, die $a$ teilt), und wenn $|a|$ keine Primzahl ist, so ist $p \leq \sqrt{|a|}$.
Beweis: Daß $p$ ein Primteiler von $a$ ist, ist klar. – Ist $|a|$ keine Primzahl, so ist $p < |a|$, somit ist $|a|/p$ eine natürliche Zahl $> 1$, die $|a|$ teilt, und daher gilt $|a|/p \geq p$, also $p \leq \sqrt{|a|}$.

**(2.4) MuPAD:** (1) Die folgende MuPAD-Funktion liefert für eine ganze Zahl $a$ die Ausgabe `TRUE`, falls $a$ eine Primzahl ist, und sonst die Ausgabe `FALSE`:

```
prim := proc(a)
  local d;
begin
  if testargs() then
    if args(0) <> 1 then
      error("prim requires one and only one argument")
    elif domtype(a) <> DOM_INT then
      error("the argument must be an integer")
    end_if
  end_if;
  if a <= 1 then
    return(FALSE)
  elif a > 2 and modp(a,2) = 0 then
    return(FALSE)
  else
    for d from 3 to floor(sqrt(a)) step 2 do
      if modp(a,d) = 0 then
        return(FALSE)
      end_if
    end_for;
    return(TRUE)
  end_if
end_proc:
```

(2) Es sei $a$ eine natürliche Zahl mit $a > 1$. Das in der Funktion `prim` aus (1) verwendete Verfahren ist denkbar einfach: Wird ein Teiler $d \in \mathbb{N}$ von $a$ mit

$2 \le d \le \sqrt{a}$ gefunden, so ist $a$ keine Primzahl; andernfalls ist $a$ eine Primzahl. Wie man sieht, ist der Aufwand von `prim` am größten, wenn $a$ eine Primzahl oder das Quadrat einer Primzahl ist; er ist dann (mindestens) proportional zu $\sqrt{a}$. Für größere Zahlen $a$ ist `prim` daher nicht geeignet. Man beachte aber, daß die Funktion `prim` mehr tut als nötig: Sie findet zu einer natürlichen Zahl $a > 1$ in jedem Fall einen Primteiler von $a$.

**(2.5) Satz:** *Es gibt unendlich viele Primzahlen.*

**Beweis** (Euklid): Es sei $n \in \mathbb{N}_0$, und es seien $p_1, p_2, \ldots, p_n$ paarweise verschiedene Primzahlen. Dann ist $a := 1 + p_1 p_2 \cdots p_n$ eine natürliche Zahl mit $a > 1$, und daher gibt es einen Primteiler $p$ von $a$. Für jedes $i \in \{1, 2, \ldots, n\}$ gilt $a \bmod p_i = 1$ und daher $p_i \nmid a$. Also ist $p \notin \{p_1, p_2, \ldots, p_n\}$.

**(2.6) Bemerkung:** Es sei $(p_i)_{i \ge 1}$ die Folge der Primzahlen in ihrer natürlichen Reihenfolge; es seien also $p_1 := 2$, $p_2 := 3, \ldots, p_{25} := 97$ und so fort.
(1) Es gilt: Zu jedem $a \in \mathbb{N}$ mit $a > 1$ gibt es eine Primzahl $p$ mit $a < p < 2a$. Dies wurde 1845 von J. L. F. Bertrand mit Hilfe der ihm zu Verfügung stehenden Primzahltafeln für jedes $a < 3\,000\,000$ nachgewiesen und 1854 von P. L. Tschebyscheff für jedes $a$ bewiesen. Ein Beweis dieses sogenannten "Bertrandschen Postulats" ist der Inhalt von Aufgabe 4 in (2.25).
(2) Es sei $m \in \mathbb{N}$ ungerade mit $m \ge 5$. $m$ ist dann und nur dann eine Primzahl, wenn es ein $k \ge 2$ mit $p_k < m$, mit $p_2 \nmid m, \ldots, p_k \nmid m$ und mit $\lfloor m/p_k \rfloor \le p_k$ gibt.
Beweis: (a) Es gelte: $m$ ist eine Primzahl. Dann gibt es ein $k \in \mathbb{N}$ mit $m = p_{k+1}$. Wegen $m \ge 5$ ist $k \ge 2$, und es gilt $p_k < m$ und $p_2 \nmid m, \ldots, p_k \nmid m$. Nach (1) gibt es eine Primzahl $p$ mit $p_k < p < 2p_k$. Es gilt

$$m \;=\; p_{k+1} \;\le\; p \;<\; 2p_k \;<\; p_k^2$$

und daher $\lfloor m/p_k \rfloor \le p_k$.
(b) Es gelte: Es gibt ein $k \ge 2$ mit $p_k < m$, mit $p_2 \nmid m, \ldots, p_k \nmid m$ und mit $\lfloor m/p_k \rfloor \le p_k$. Für jeden Primteiler $p$ von $m$ gilt $p \ge p_{k+1}$ und

$$m \;=\; p_k \cdot \left\lfloor \frac{m}{p_k} \right\rfloor + (m \bmod p_k) \;\le\; p_k^2 + (p_k - 1) \;<\; (p_k + 1)^2 \;<\; p_{k+1}^2$$

und daher $p \ge p_{k+1} > \sqrt{m}$. Also besitzt $m$ keinen Primteiler $\le \sqrt{m}$ und ist somit eine Primzahl.

**(2.7) MuPAD:** Die folgende MuPAD-Funktion berechnet zu einer natürlichen Zahl $n$ die Liste $[p_1, p_2, \ldots, p_n]$ der ersten $n$ Primzahlen. Man überlegt sich mit Hilfe von (2.6)(2) leicht, daß sie für jede Eingabe ein korrektes Ergebnis liefert.

```
listOfPrimes := proc(n)
  local p, m, i, j;
begin
  if args(0) <> 1 then
    error("listOfPrimes requires exactly one argument")
  elif domtype(n) <> DOM_INT then
    error("the argument must be a natural number")
  elif n < 1 then
    error("the argument must be a natural number")
  end_if;
  p[1] := 2;
  p[2] := 3;
  m := 3;
  i := 2;
  while i < n do
    j := 2;
    while j > 1 do
      if modp(m,p[j]) = 0 then
        m := m + 2;
        break
      elif m div p[j] <= p[j] then
        i := i + 1;
        p[i] := m;
        m := m + 2;
        break
      end_if;
      j := j+1
    end_while
  end_while;
  [p[i] $ hold(i) = 1..n]
end_proc:
```

**(2.8) Das Sieb des Eratosthenes:** Eine andere Methode, Tabellen von Primzahlen zu berechnen, wurde von dem griechischen Mathematiker Eratosthenes (um 230 v. Chr. Geb.) angegeben: Will man zu einer natürlichen Zahl $N$ alle Primzahlen $p \leq N$ berechnen, so schreibt man die Zahlen 2, 3, 4, ..., $N$ in eine Liste und streicht darin alle geraden Zahlen $> 2$. Die erste nichtgestrichene Zahl $> 2$, nämlich 3, ist dann eine Primzahl. Jetzt streicht man in der Tabelle alle durch 3 teilbaren Zahlen $> 3$. Die erste nichtgestrichene Zahl $> 3$, nämlich 5, ist wieder eine Primzahl; jetzt streicht man in der Liste alle durch 5

teilbaren Zahlen $> 5$. Dieses Verfahren wird fortgesetzt: Jedesmal, wenn man eine neue Primzahl $p$ gefunden hat, streicht man in der Liste alle Vielfachen $> p$ von $p$; die erste nichtgestrichene Zahl $> p$ hat keinen nichttrivialen Teiler, da sie sonst bereits gestrichen wäre, und ist daher eine Primzahl. Man hört auf, wenn man auf diese Weise eine Primzahl $p > \sqrt{N}$ gefunden hat. Dann sind die nichtgestrichenen Zahlen in der Tabelle genau die Primzahlen $\leq N$ (wegen (2.3)).

**(2.9) Mersenne-Zahlen:** Für jedes $n \in \mathbb{N}$ heißt $M(n) := 2^n - 1$ die $n$-te Mersenne-Zahl (nach M. Mersenne, 1588 - 1648).
(1) Ist $n \in \mathbb{N}$ keine Primzahl, so ist auch $M(n)$ keine Primzahl. Es ist nämlich $M(1) = 1$, und für natürliche Zahlen $r > 1$ und $s > 1$ gilt

$$M(rs) \;=\; (2^s - 1)\,(2^{(r-1)s} + 2^{(r-2)s} + \cdots + 2^s + 1).$$

(2) Nicht für jede Primzahl $p$ ist $M(p)$ eine Primzahl: Es ist $M(11) = 23 \cdot 89$.
(3) Die größte heute, am 18.2.1998, bekannte Primzahl ist die Mersenne-Zahl $M(3\,021\,377)$; sie wurde am 27.1.1998 gefunden. Seit dem Jahr 1588, in dem P. A. Cataldi (1548 - 1626) zeigte, daß $M(17) = 131\,071$ und $M(19) = 524\,287$ Primzahlen sind, war die größte jeweils bekannte Primzahl immer eine Mersenne-Zahl, mit Ausnahme der Zeit zwischen August 1989 und März 1992, in der $391\,581 \cdot 2^{216\,193} - 1$ den Rekord als größte Primzahl hielt.

Daß man gerade große Mersenne-Zahlen darauf untersucht, ob sie Primzahlen sind, liegt daran, daß es dafür einen einfachen Test gibt, nämlich den Test von E. Lucas (1878) und D. H. Lehmer (1930/35): Ist $(a_j)_{j\geq 1}$ die Folge mit

$$a_1 := 4 \quad \text{und} \quad a_{j+1} := a_j^2 - 2 \quad \text{für jedes } j \in \mathbb{N},$$

so ist für eine Primzahl $p \geq 3$ die Mersenne-Zahl $M(p)$ genau dann eine Primzahl, wenn $a_{p-1}$ durch $M(p)$ teilbar ist. Ein Beweis dafür steht erst in Abschnitt (11.22); eine Richtung dieses Beweises benötigt nämlich die in § 10 und § 11 behandelte Theorie der quadratischen Reste. Übrigens weiß man nicht, ob es unendlich viele Mersenne-Zahlen gibt, die Primzahlen sind.
(4) Die jeweils größte bekannte Primzahl und viele weitere Informationen über Primzahlen findet man (zur Zeit) unter der Adresse

`http://www.utm.edu/research/primes/largest.html`

im Internet.

**(2.10) MuPAD:** Der Aufruf `numlib::mersenne()` liefert die Liste der 37 heute bekannten Primzahlen $p$, für die die Mersenne-Zahl $M(p)$ eine Primzahl ist:

```
>> numlib::mersenne();
  [2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607,
   1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213,
   19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091,
   756839, 859433, 1257787, 1398269, 2976221, 3021377]
```

Die Definition dieser Funktion in der Bibliothek `numlib` läßt sich ohne Schwierigkeiten aktualisieren, sobald eine neue Primzahl $p$ gefunden ist, für die $M(p)$ eine Primzahl ist.

**(2.11) Die Primzahlfunktion:** (1) Über die Verteilung der Primzahlen innerhalb der natürlichen Zahlen gibt der sogenannte Primzahlsatz Auskunft, den C. F. Gauß 1792 vermutet hat und den J. Hadamard (1865 – 1963) und Ch. de la Vallée-Poussin (1866 – 1962) unabhängig voneinander 1896 bewiesen haben: Für die Primzahlfunktion

$$\pi : \mathbb{R} \to \mathbb{R} \quad \text{mit} \quad \pi(x) := \#(\{p \in \mathbb{P} \mid p \leq x\}) \quad \text{für jedes } x \in \mathbb{R}$$

gilt

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

Wie man diesen Satz mit funktionentheoretischen Methoden beweist, kann man in den Büchern von J. Brüdern ([17], Abschnitt 1.7) und von E. Freitag und R. Busam ([35], Kap. VII, § 4) nachlesen.

Es gibt Verfahren, mit denen man Werte der Primzahlfunktion $\pi$ genau ausrechnen kann und die natürlich nicht in der Berechnung großer Primzahltafeln bestehen. Die folgende Tabelle enthält einige Funktionswerte von $\pi$; sie sind umfangreicheren Tabellen in Riesel [90], S. 374–376, und in der Arbeit [24] von M. Deleglise und J. Rivat entnommen. In [24] findet sich neben der Beschreibung der bislang bekannten Methoden zur Berechnung von Werten der Funktion $\pi$ ein verbessertes Verfahren, mit dessen Hilfe $\pi(10^{17})$ und $\pi(10^{18})$ und später auch $\pi(10^{19})$ und $\pi(10^{20})$ berechnet wurden, wie man zur Zeit einer Notiz an der in (2.9)(4) angegebenen Internet-Adresse entnehmen kann. Dort findet man auch, daß Paul Zimmermann ausgerechnet hat, daß

$$\pi(4\,185\,296\,581\,467\,695\,669) = 100\,000\,000\,000\,000\,000$$

ist.

| $x$ | $\pi(x)$ | $x$ | $\pi(x)$ |
|---|---|---|---|
| $10^5$ | 9 592 | $10^{13}$ | 346 065 536 839 |
| $10^6$ | 78 498 | $10^{14}$ | 3 204 941 750 802 |
| $10^7$ | 664 579 | $10^{15}$ | 29 844 570 422 669 |
| $10^8$ | 5 761 455 | $10^{16}$ | 279 238 341 033 925 |
| $10^9$ | 50 847 534 | $10^{17}$ | 2 623 557 157 654 233 |
| $10^{10}$ | 455 052 511 | $10^{18}$ | 24 739 954 287 740 860 |
| $10^{11}$ | 4 118 054 813 | $10^{19}$ | 234 057 667 276 344 607 |
| $10^{12}$ | 37 607 912 018 | $10^{20}$ | 2 220 819 602 560 918 840 |

(2) Für jedes $\delta \in ]\,0,1\,[$ existiert das uneigentliche Integral

$$\int_0^{1-\delta} \frac{1}{\log t}\, dt,$$

und für jedes $x \in [\,2,\infty\,[$ gilt: Es existiert der Grenzwert

$$\int_0^x \frac{1}{\log t}\, dt \;:=\; \lim_{\delta\to 0+}\left(\int_0^{1-\delta} \frac{1}{\log t}\, dt + \int_{1+\delta}^x \frac{1}{\log t}\, dt\right).$$

(Das bei 1 uneigentliche Integral, das darin links vom Gleichheitszeichen steht, konvergiert nicht, aber es existiert der rechts stehende Grenzwert, der Cauchysche Hauptwert dieses Integrals). Die Funktion

$$\mathrm{Li} : [\,2,\infty\,[\ \to \mathbb{R} \quad \text{mit} \quad \mathrm{Li}(x) \;:=\; \int_0^x \frac{1}{\log t}\, dt \quad \text{für jedes } x \in [\,2,\infty\,[$$

heißt der Integrallogarithmus. Eine Anwendung der Regel von L'Hospital zeigt, daß

$$\lim_{x\to\infty}\left(\mathrm{Li}(x) \,/\, \frac{x}{\log x}\right) \;=\; 1$$

gilt. Daraus und aus der in (1) angegebenen Version des Primzahlsatzes folgt: Es gilt

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} \;=\; 1.$$

(In dieser Form wurde der Primzahlsatz von Hadamard und von de la Vallée-Poussin bewiesen). Die Funktion Li liefert bessere Näherungen für die Funktionswerte von $\pi$ als die Funktion $x \mapsto x/\log x : [2,\infty[ \to \mathbb{R}$. Für jedes $x \in [2,\infty[$ gilt: Es ist

$$\mathrm{Li}(x) \;=\; \gamma + \log\log x + \sum_{n=1}^{\infty} \frac{(\log x)^n}{n \cdot n!},$$

worin

$$\gamma \;:=\; \lim_{n\to\infty}\left(\sum_{j=1}^{n} \frac{1}{j} - \log n\right) \;=\; 0.57721\,75664\,90153\,28606\,06512\ldots$$

die Eulersche Konstante ist, und damit kann man mittels MuPAD $\mathrm{Li}(x)$ näherungsweise berechnen. MuPAD kennt die Eulersche Konstante unter dem Namen `EULER`.

(3) Eine weitere Funktion, mit deren Hilfe man Werte der Primzahlfunktion $\pi$ näherungsweise berechnen kann, ist die von B. Riemann (1826 – 1866) angegebene Funktion

$$\begin{cases} R : [2,\infty[ \;\to \mathbb{R} \quad \text{mit} \\ \\ R(x) \;:=\; \displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n}\, \mathrm{Li}\big(x^{1/n}\big) \quad \text{für jedes } x \in [2,\infty[\,. \end{cases}$$

Darin ist $\mu : \mathbb{N} \to \mathbb{Z}$ die Möbius-Funktion (A. F. Möbius, 1790 – 1868): Es ist

$$\mu(n) \;:=\; \begin{cases} (-1)^k, & \text{falls } n \text{ Produkt von } k \text{ verschiedenen Primzahlen ist,} \\ 0, & \text{falls } n \text{ durch das Quadrat einer Primzahl teilbar ist.} \end{cases}$$

Es gilt, was aber von Riemann noch nicht bewiesen wurde: Es ist

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

Zur Berechnung von Funktionswerten der Funktion $R$ ist ein Ergebnis nützlich, das von J. P. Gram 1884 angegeben wurde: Es ist

$$R(x) \;=\; 1 + \sum_{n=1}^{\infty} \frac{(\log x)^n}{n \cdot n! \cdot \zeta(n+1)} \quad \text{für jedes } x \in [2,\infty[\,.$$

Darin ist $\zeta$ die berühmte Riemannsche $\zeta$-Funktion: Es ist

$$\zeta(n+1) \;=\; \sum_{k=1}^{\infty} \frac{1}{k^{n+1}} \quad \text{für jedes } n \in \mathbb{N}.$$

Da MuPAD die $\zeta$-Funktion kennt (unter dem Namen `zeta`), kann man für $x \in [2, \infty[$ Näherungen für $\pi(x)$ gewinnen, indem man Partialsummen der Reihe

$$1 + \sum_{n=1}^{\infty} \frac{(\log x)^n}{n \cdot n! \cdot \zeta(n+1)}$$

mittels MuPAD berechnet. Diese Näherungen sind in dem Bereich, den die oben angegebene Tabelle von Werten der Primzahlfunktion $\pi$ abdeckt, deutlich besser als die vom Integrallogarithmus Li gelieferten Näherungen (vgl. dazu Aufgabe 8 in Abschnitt (2.25)).

(4) Die Riemannsche $\zeta$-Funktion $\zeta : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ ist in $\mathbb{C} \setminus \{1\}$ holomorph, hat in 1 einen einfachen Pol, und für jedes $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$ ist

$$\zeta(s) \;=\; \sum_{k=1}^{\infty} \frac{1}{k^s}.$$

Für jedes $m \in \mathbb{N}$ ist $\zeta(-2m) = 0$, und jede andere Nullstelle von $\zeta$ liegt in $\{s \in \mathbb{C} \mid 0 < \mathrm{Re}(s) < 1\}$. In dieser Menge hat $\zeta$ unendlich viele Nullstellen, und die berühmte Riemannsche Vermutung besagt, daß jede dieser Nullstellen den Realteil $1/2$ besitzt. Ein Beweis dieser Vermutung wäre für die Primzahltheorie von großer Bedeutung. So erhält man unter der Voraussetzung der Richtigkeit der Riemannschen Vermutung eine optimale Abschätzung des Fehlers im Primzahlsatz: Es gibt eine positive reelle Zahl $c$ mit

$$|\,\pi(x) - \mathrm{Li}(x)\,| \;\leq\; c\sqrt{x} \cdot \log x \quad \text{für jedes reelle } x \geq 2,$$

was mit Hilfe des Landau-Symbols abkürzend

$$\pi(x) \;=\; \mathrm{Li}(x) + O(\sqrt{x} \cdot \log x)$$

geschrieben wird. Eine ausführliche Darstellung der Bedeutung der $\zeta$-Funktion in der Primzahltheorie gibt H. M. Edwards in [29].

**(2.12) Bemerkung:** Das in (2.11) erwähnte Landau-Symbol $O$ ist nach dem Zahlentheoretiker E. Landau (1877 – 1938) benannt. Es ist folgendermaßen erklärt: Ist $X$ eine nach oben nicht beschränkte Teilmenge von $\mathbb{R}$, etwa ein Intervall der Form $[a, \infty[$ oder $\mathbb{N}$ oder die Menge $\mathbb{P}$ aller Primzahlen, und sind $f : X \to \mathbb{C}$, $g : X \to \mathbb{C}$ und $h : X \to \mathbb{C}$ Funktionen, so schreibt man

$$f(x) \;=\; g(x) + O\big(h(x)\big),$$

falls es eine positive reelle Zahl $c$ und ein $x_0 \in X$ gibt, für die gilt: Es ist

$$\big|\, f(x) - g(x) \,\big| \;\leq\; c \cdot \big|\, h(x) \,\big| \quad \text{für jedes } x \in X \text{ mit } x \geq x_0.$$

**(2.13)** Zum Abschluß der Bemerkungen über die Verteilung der Primzahlen in $\mathbb{N}$ soll ein noch offenes Problem erwähnt werden. Ist $p$ eine Primzahl und ist auch $p+2$ eine Primzahl, so heißen $p$ und $p+2$ Primzahlzwillinge. Man weiß nicht, ob es unendlich viele Paare von Primzahlzwillingen gibt. Die größten zur Zeit bekannten Primzahlzwillinge sind

$$2422\,06083 \cdot 2^{38\,880} - 1 \quad \text{und} \quad 2422\,06083 \cdot 2^{38\,880} + 1,$$

sie wurden im November 1995 von K.-H. Indlekofer und A. Járai gefunden (vgl. [49]).

**(2.14)** Im zweiten Teil dieses Paragraphen wird zuerst der sogenannte Hauptsatz der Elementaren Zahlentheorie bewiesen, der besagt, daß sich jede natürliche Zahl in eindeutig bestimmter Weise als Produkt von Primzahlpotenzen schreiben läßt (vgl. (2.16)). Bereits in der Schule lernt man ein Verfahren zur Herstellung solcher Primzerlegungen kennen, das aber sehr rechenaufwendig und daher für größere natürliche Zahlen nicht geeignet ist (vgl. (2.20)). Damit im Rest dieses Paragraphen auch etwas behandelt wird, das nicht jeder bereits aus der Schule kennt, wird zum Abschluß mit der rho-Methode von J. M. Pollard ein Faktorisierungverfahren vorgestellt, das auf einer geradezu genial einfachen Idee beruht und das keinerlei Theorie bedarf, aber doch noch in Fällen erfolgreich ist, in denen das Verfahren aus der Schule längst aufgegeben hat.

**(2.15) Bemerkung:** Es sei $n \in \mathbb{N}$, es seien $a_1, a_2, \ldots, a_n$ ganze Zahlen, und es sei $p$ eine Primzahl. Gilt $p \mid a_1 a_2 \cdots a_n$, so gibt es ein $i \in \{1, 2, \ldots, n\}$ mit $p \mid a_i$.
Beweis: Wenn die Primzahl $p$ keine der Zahlen $a_1, a_2, \ldots, a_n$ teilt, so gilt $\mathrm{ggT}(p, a_i) = 1$ für jedes $i \in \{1, 2, \ldots, n\}$ und daher $\mathrm{ggT}(p, a_1 a_2 \cdots a_n) = 1$ (vgl. (1.14)(2)), also $p \nmid a_1 a_2 \cdots a_n$.

**(2.16) Satz:** *Zu jedem $a \in \mathbb{N}$ gibt es ein eindeutig bestimmtes $r \in \mathbb{N}_0$, bis auf die Reihenfolge eindeutig bestimmte paarweise verschiedene Primzahlen $p_1, p_2, \ldots, p_r$ und eindeutig bestimmte natürliche Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_r$ mit*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

**Beweis:** (Existenz:) Für $a = 1$ ist nichts zu beweisen (hier ist $r = 0$). Es sei $a \in \mathbb{N}$ mit $a > 1$, und es sei bereits gezeigt: Jedes $b \in \mathbb{N}$ mit $b < a$ ist ein Produkt von Primzahlen. Nach (2.3) gibt es eine Primzahl $p$ mit $p \mid a$. Dann gilt $a/p \in \mathbb{N}$ und $a/p < a$, also gibt es nach Induktionsvoraussetzung ein $s \in \mathbb{N}_0$ und Primzahlen $q_1, q_2, \ldots, q_s$ mit $a/p = q_1 q_2 \cdots q_s$. Hiermit gilt $a = p q_1 q_2 \cdots q_s$.
(Einzigkeit:) Es seien $k, l \in \mathbb{N}_0$, es seien $p_1, p_2, \ldots, p_k$ und $q_1, q_2, \ldots, q_l$ Primzahlen, und es gelte $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$. Ist dabei $k = 0$, so ist auch

$l = 0$, denn sonst wäre $q_1 q_2 \cdots q_l > 1$. Ist $k \geq 1$, so gilt $p_1 \mid q_1 q_2 \cdots q_l$, und daraus folgt: Es ist $l \geq 1$, nach (2.15) gibt es ein $i \in \{1, 2, \ldots, l\}$ mit $p_1 \mid q_i$, also mit $p_1 = q_i$ (da $p_1$ und $q_i$ Primzahlen sind), und daher ist $p_2 p_3 \cdots p_k = q_1 \cdots q_{i-1} q_{i+1} \cdots q_l$. Durch Induktion nach $k$ ergibt sich auf diese Weise: Es gilt $k = l$, und es gibt eine Permutation $\sigma$ von $\{1, 2, \ldots, k\}$ mit $p_j = q_{\sigma(j)}$ für jedes $j \in \{1, 2, \ldots, k\}$.

**(2.17) Bezeichnungen:** Es sei $\mathbb{P}$ die Menge aller Primzahlen, und für jedes $p \in \mathbb{P}$ und jedes $a \in \mathbb{Z} \setminus \{0\}$ sei

$$v_p(a) \;:=\; \max\big(\{\alpha \in \mathbb{N}_0 \mid p^\alpha \text{ teilt } a\}\big).$$

**(2.18) Bemerkung:** Nach (2.16) besitzt jedes $a \in \mathbb{Z} \setminus \{0\}$ die eindeutig bestimmte *Primzerlegung*

$$a \;=\; \operatorname{sign}(a) \cdot \prod_{p \in \mathbb{P}} p^{v_p(a)},$$

worin gilt: Für jedes $p \in \mathbb{P}$ ist $v_p(a) \in \mathbb{N}_0$, und nur für endlich viele $p \in \mathbb{P}$ ist $v_p(a) > 0$.

**(2.19) Bemerkung:** Es seien $a$ und $b$ ganze Zahlen, und es seien

$$a \;=\; \operatorname{sign}(a) \cdot \prod_{p \in \mathbb{P}} p^{v_p(a)} \quad \text{und} \quad b \;=\; \operatorname{sign}(b) \cdot \prod_{p \in \mathbb{P}} p^{v_p(b)}$$

die Primzerlegungen von $a$ und $b$.
(1) Die Primzerlegung von $ab$ ist

$$ab \;=\; \operatorname{sign}(a)\operatorname{sign}(b) \cdot \prod_{p \in \mathbb{P}} p^{v_p(a)+v_p(b)},$$

d.h. für jedes $p \in \mathbb{P}$ ist $v_p(ab) = v_p(a) + v_p(b)$.
(2) $a$ ist ein Teiler von $b$, genau wenn gilt: Für jedes $p \in \mathbb{P}$ ist $v_p(a) \leq v_p(b)$.
(3) Es gilt

$$\operatorname{ggT}(a,b) \;=\; \prod_{p \in \mathbb{P}} p^{\min(\{v_p(a), v_p(b)\})} \quad \text{und} \quad \operatorname{kgV}(a,b) \;=\; \prod_{p \in \mathbb{P}} p^{\max(\{v_p(a), v_p(b)\})}.$$

(4) Es ist

$$\{d \in \mathbb{N} \mid d \text{ teilt } a\} \;=\; \Big\{ \prod_{p \in \mathbb{P}} p^{\delta_p} \;\Big|\; \text{für jedes } p \in \mathbb{P} \text{ ist } 0 \leq \delta_p \leq v_p(a) \Big\}.$$

Für die Summe $\sigma(a)$ und die Anzahl $\tau(a)$ aller Teiler $d \in \mathbb{N}$ von $a$ gilt daher

$$\sigma(a) = \sum_{d\in\mathbb{N},\, d\,|\,a} d = \prod_{p\in\mathbb{P},\, p\,|\,a} \left( \sum_{j=0}^{v_p(a)} p^j \right) = \prod_{p\in\mathbb{P},\, p\,|\,a} \frac{p^{v_p(a)+1}-1}{p-1}$$

und

$$\tau(a) = \#\big(\{d \in \mathbb{N} \mid d \text{ teilt } a\}\big) = \prod_{p\in\mathbb{P},\, p\,|\,a} \big(1 + v_p(a)\big).$$

**(2.20) Aufgabe 1:** (1) Es sei $(d_i)_{i\geq 1}$ eine Folge natürlicher Zahlen, in der alle Primzahlen vorkommen und für die gilt: Es ist $d_1 = 2$ und $d_i < d_{i+1}$ für jedes $i \in \mathbb{N}$. Der folgende Algorithmus liefert zu einer natürlichen Zahl $a$ Primzahlen $p_1, p_2, \ldots, p_n$ mit $p_1 \leq p_2 \leq \cdots \leq p_n$ und mit $a = p_1 p_2 \cdots p_n$.

**(PZ1)** Man setzt

$$n := 0, \quad i := 1, \quad b := a \quad \text{und} \quad d := d_1.$$

**(PZ2)** Ist $b = 1$, so gibt man $p_1, p_2, \ldots, p_n$ aus und bricht ab.

**(PZ3)** Man berechnet

$$q := b \operatorname{div} d \quad \text{und} \quad r := b \bmod d.$$

**(PZ4)** Wenn $r = 0$ ist, so setzt man

$$n := n+1, \quad p_n := d \quad \text{und} \quad b := q$$

und geht zu (PZ2).

**(PZ5)** Gilt $r \neq 0$ und $q > d$, so setzt man

$$i := i+1 \quad \text{und} \quad d := d_i$$

und geht zu (PZ3).

**(PZ6)** Gilt $r \neq 0$ und $q \leq d$, so setzt man

$$n := n+1 \quad \text{und} \quad p_n := b,$$

gibt $p_1, p_2, \ldots, p_n$ aus und bricht ab.

Man überlege sich, daß dieser Algorithmus das Verlangte leistet und daß es sich dabei um das im Schulunterricht übliche Verfahren zur Berechnung der Primzerlegung von $a$ handelt.

(2) Man schreibe eine MuPAD-Funktion, die mit dem in (1) beschriebenen Algorithmus zu jeder natürlichen Zahl $a$ die Primzerlegung von $a$ berechnet. Dabei verwende man die Folge $(d_i)_{i\geq 1}$ mit

$$d_1 = 2 \quad \text{und} \quad d_i = 2i - 1 \quad \text{für jedes } i \geq 2.$$

(3) Man setze $d_1 := 2$, $d_2 := 3$, $d_3 := 5$ und

$$d_{2i} := d_{2i-1} + 2 \quad \text{und} \quad d_{2i+1} := d_{2i} + 4 \quad \text{für jedes } i \geq 2.$$

In dieser Folge $(d_i)_{i\geq 1}$ kommen keine Vielfachen $> 3$ von 3 vor. Man schreibe eine MuPAD-Funktion, die mit dem in (1) angegebenen Algorithmus zu jeder natürlichen Zahl $a$ die Primzerlegung von $a$ berechnet und die diese Folge $(d_i)_{i\geq 1}$ verwendet. Man vergleiche mit der Funktion aus (2).

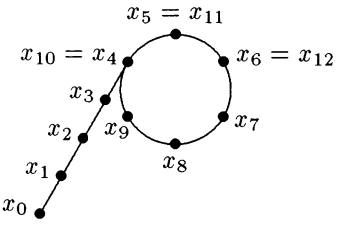
**(2.21) Die rho-Methode von J. M. Pollard:** (1) Die folgende MuPAD-Funktion `pollard` versucht zu einer natürlichen Zahl $m$ in $N$ Iterationen einen Teiler $d \in \mathbb{N}$ von $m$ mit $1 < d < m$ zu finden; wird sie nur mit dem einem Argument $m$ aufgerufen, so wird intern $N := 5000$ gesetzt.

```
pollard := proc()
  local m, N, x0, d, x, y, i;
begin
  m := args(1);
  if args(0) = 1 then
    N := 5000
  else
    N := args(2)
  end_if;
  x0 := modp(random(),m);
  x := x0; y := x0;
  for i from 1 to N do
    x := modp(x^2 + 2,m);
    y := modp(y^2 + 2,m);
    y := modp(y^2 + 2,m);
    d := igcd(y - x,m);
    if d > 1 and d < m then
      return(d)
    end_if
  end_for;
  FAIL
end_proc:
```

(2) Das Verfahren, das in der Funktion `pollard` implementiert ist, wählt zunächst (zufällig) einen Startwert $x_0 \in \{0,1,\ldots,m-1\}$ und berechnet damit mit Hilfe der Abbildung

$$\begin{cases} f : \{0,1,\ldots,m-1\} \to \{0,1,\ldots,m-1\} & \text{mit} \\ f(x) \;:=\; (x^2+2) \bmod m & \text{für jedes } x \in \{0,1,\ldots,m-1\} \end{cases}$$

die Terme der Folge $(x_i)_{i\geq 0}$ mit $x_i = f(x_{i-1})$ für jedes $i \in \mathbb{N}$ mit $i \leq N$. Für die Folge $(y_i)_{i\geq 0}$, deren Terme $y_i$ mit $i \leq N$ innerhalb der Funktion `pollard` berechnet werden, gilt $y_i = x_{2i}$ für jedes $i \in \mathbb{N}_0$. Wie man sieht, wird die Folge $(x_i)_{i\geq 0}$ – eventuell erst nach einer Vorperiode – periodisch: Es gibt also ein $i_0 \in \mathbb{N}_0$ und ein $l \in \mathbb{N}$ mit $x_{i+l} = x_i$ für jedes $i \in \mathbb{N}_0$ mit $i \geq i_0$. (Wenn man dieses Verhalten der Folge $(x_i)_{i\geq 0}$ graphisch darstellt, so ergibt sich eine Figur, die dem griechischen Buchstaben $\rho$ ähnlich ist; von daher hat das Verfahren seinen Namen). Ist $d \in \mathbb{N}$ ein Teiler von $m$ mit $d > 1$ und mit $d < m$, so gibt es somit Zahlen $i, j \in \mathbb{N}_0$ mit $i \neq j$ und mit $d \mid x_j - x_i$, und man darf daher wohl hoffen, daß es ein $i \in \{1,2,\ldots,N\}$ gibt, für das $x_{2i} - x_i = y_i - x_i$ durch $d$ teilbar ist und $x_{2i} \neq x_i$ gilt. (Es gibt ein $i \in \mathbb{N}$ mit $x_i = x_{2i}$, wie Aufgabe 11 in Abschnitt (2.25) zeigt). Das Verfahren sucht ein $i \in \mathbb{N}$ mit $i \leq N$, für das $x_{2i} - x_i$ einen Teiler $d \in \{2,3,\ldots,m-1\}$ mit $m$ gemeinsam hat. Es braucht, wie man sieht, nicht zu einem Erfolg zu führen: Es ist möglich, daß für jedes $i \in \{1,2,\ldots,N\}$ der größte gemeinsame Teiler der Zahlen $m$ und $x_{2i} - x_i$ gleich 1 oder gleich $m$ ist. In diesem Fall endet das Verfahren mit der Ausgabe `FAIL`.




Wenn das Verfahren nicht zum Erfolg führt, kann man einerseits die Maximalzahl $N$ der durchzuführenden Iterationen vergrößern, man kann aber auch eine andere Abbildung $f$ wählen, und dies ist interessanter als die Vergrößerung von $N$. Man kann etwa die Abbildung

$$x \mapsto f(x) \;:=\; (x^{32}+7) \bmod m \;:\; \{0,1,\ldots,m-1\} \to \{0,1,\ldots,m-1\}$$

oder die Abbildung

$$x \mapsto f(x) \;:=\; (x^{1024}+2) \bmod m \;:\; \{0,1,\ldots,m-1\} \to \{0,1,\ldots,m-1\}$$

verwenden. Mit der zuletzt genannten Abbildung fanden 1981 R. P. Brent und J. M. Pollard die Primzerlegung der Zahl $2^{2^8}+1$ (vgl. [13]).

(3) Das in diesem Abschnitt behandelte Faktorisierungsverfahren wurde 1975 von J. M. Pollard in [84] veröffentlicht. Zu einer genaueren Diskussion dieses Verfahrens vergleiche man neben [84] auch Knuth [55], Abschnitt 4.5.4, Koblitz [57], Kap. V, § 2, oder Riesel [90], Kap. VI, und insbesondere Bach [9].

**(2.22) Fermat-Zahlen:** Die Zahl, deren Primzerlegung Brent und Pollard mit Hilfe der rho-Methode gefunden haben, ist eine der Fermat-Zahlen. Für $n \in \mathbb{N}_0$ heißt

$$F(n) := 2^{2^n} + 1$$

die $n$-te Fermat-Zahl. Pierre de Fermat (1601 - 1665), der sich wohl als erster mit diesen Zahlen befaßt hat, war der Meinung, daß alle diese Zahlen Primzahlen sind. Dies ist nicht der Fall: $F(0) = 3$, $F(1) = 5$, $F(2) = 17$, $F(3) = 257$ und $F(4) = 65\,537$ sind Primzahlen, aber andere Primzahlen als diese sind unter den Fermat-Zahlen nicht bekannt. Man weiß, daß $F(5)$, $F(6), \ldots,$ $F(23)$ keine Primzahlen sind (vgl. [23]). Von einigen größeren Fermat-Zahlen kennt man kleine Primteiler: So besitzt zum Beispiel $F(23471)$ den Primteiler $1 + 5 \cdot 2^{23473}$ (vgl. dazu Riesel [90], Tabelle 4). Es gibt einen einfachen Primzahltest für Fermat-Zahlen, den T. Pepin 1877 angegeben hat: Für eine natürliche Zahl $n$ ist $F(n)$ dann und nur dann eine Primzahl, wenn

$$3^{(F(n)-1)/2} \equiv -1 \pmod{F(n)}$$

gilt. Ein Beweis dafür ist Inhalt der Aufgabe 3 in Abschnitt (11.24).

Fermat-Zahlen, die Primzahlen sind, spielen übrigens bei der Frage nach der Konstruierbarkeit von regelmäßigen Vielecken eine Rolle: Wie Gauß bewiesen hat, ist für eine ungerade Primzahl $p$ das einem Kreis vom Radius 1 einbeschriebene regelmäßige $p$-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn $p$ eine Fermat-Zahl ist (vgl. dazu Artin [7], Kap. XIII, § 4, oder Lorenz [65], § 11).

**(2.23) MuPAD:** Von den Funktionen zur Zahlentheorie, die MuPAD zu Verfügung stellt, sind hier die Funktionen `isprime`, `ithprime`, `ifactor`, `nextprime`, `prevprime`, `primedivisors`, `numprimedivisors`, `omega`, `divisors`, `numdivisors`, `sumdivisors` und `moebius` zu nennen:

- `isprime(a)` liefert für eine ganze Zahl $a$ die Ausgabe `TRUE`, falls $a$ eine Primzahl ist, und andernfalls die Ausgabe `FALSE`.
- `ithprime(i)` liefert zu einer natürlichen Zahl $i$ die $i$-te Primzahl.
- `ifactor(a)` liefert zu einer ganzen Zahl $a \neq 0$ die Primzerlegung von $a$, und zwar in der folgenden Gestalt: Ist $a = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ mit $\varepsilon :=$

$\mathrm{sign}(a) \in \{1, -1\}$, mit $r \in \mathbb{N}_0$, mit paarweise verschiedenen Primzahlen $p_1, p_2, \ldots, p_r$ und mit natürlichen Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_r$, so liefert die Anweisung `ifactor(a)` die Liste $[\varepsilon, p_1, \alpha_1, p_2, \alpha_2, \ldots, p_r, \alpha_r]$; `ifactor(0)` liefert die Ausgabe $[0]$.

- `nextprime(a)` liefert zu einer ganzen Zahl $a$ die kleinste Primzahl $\geq a$.
- `numlib::prevprime(a)` liefert zu einer ganzen Zahl $a \geq 2$ die größte Primzahl $\leq a$ und zu einer ganzen Zahl $a \leq 1$ die Ausgabe `FAIL`.
- `numlib::primedivisors(a)` liefert zu einer ganzen Zahl $a \neq 0$ die Liste der nach der Größe geordneten Primteiler von $a$.
- `numlib::numprimedivisors(a)` und `numlib::omega(a)` liefern zu einer ganzen Zahl $a \neq 0$ die Anzahl der Primteiler von $a$.
- `numlib::divisors(a)` liefert zu einer ganzen Zahl $a \neq 0$ die Liste der nach der Größe geordneten Teiler $d \in \mathbb{N}$ von $a$.
- `numlib::numdivisors(a)` und `numlib::tau(a)` liefern zu einer ganzen Zahl $a \neq 0$ die Anzahl $\tau(a)$ der Teiler $d \in \mathbb{N}$ von $a$.
- `numlib::sumdivisors(a)` und `numlib::sigma(a)` liefern zu einer ganzen Zahl $a \neq 0$ die Summe $\sigma(a)$ der Teiler $d \in \mathbb{N}$ von $a$.
- `numlib::moebius(a)` liefert zu einer natürlichen Zahl $a$ den Wert $\mu(a)$ der Möbius-Funktion $\mu$ (vgl. (2.11)(3)).

**(2.24) MuPAD:** (1) Der in `isprime` implementierte Primzahltest wird später in § 7 ausführlich besprochen. Es handelt sich dabei um einen stochastischen Primzahltest: Liefert `isprime(a)` für eine ganze Zahl $a$ die Ausgabe `TRUE`, so braucht $a$ keine Primzahl zu sein; aber die Wahrscheinlichkeit dafür ist vergleichsweise klein. Bei der Ausgabe `FALSE` ist $a$ wirklich keine Primzahl.

Man kann sich überlegen, daß `isprime` bei einmaliger Anwendung auf die Nichtprimzahl

$$a := 1253\,07596\,07784\,49601\,05845\,73923$$

mit der Wahrscheinlichkeit $(1/4)^{10}$ die falsche Ausgabe `TRUE` liefert (vgl. Aufgabe 5 in (7.9)). Bei einem Testlauf wurde `isprime` 5 000 000-mal auf $a$ angewandt, und dabei wurde 5-mal die Ausgabe `TRUE` beobachtet.
(2) `ithprime` verwendet eine Liste von Primzahlen und berechnet die nicht in der Liste stehenden mit Hilfe von `nextprime`. Diese Liste endet (in der

aktuellen Version von MuPAD) mit der 1 000 000-ten Primzahl 15 485 863. Für eine natürliche Zahl $i > 1\,000\,000$ rechnet `ithprime` von 15 485 863 aus mit Hilfe von `nextprime` solange, bis die $i$-te Primzahl erreicht ist. `ithprime` leistet mehr als die Primzahltafel [63] von D. N. Lehmer, die die 664 999 Primzahlen $\leq 10\,006\,721$ enthält und deren erste Auflage übrigens bereits 1914, also lange vor dem Beginn des Computer-Zeitalters, erschienen ist.
(3) Das Verfahren zur Berechnung von Primzerlegungen, das in `ifactor` implementiert ist, kann hier nicht erläutert werden. Die modernen Faktorisierungsverfahren für natürliche Zahlen gehören wohl zu den kompliziertesten Algorithmen der Zahlentheorie und erfordern wesentlich tieferliegende Methoden, als daß sie in diesem Buch besprochen werden können. Einen Eindruck davon kann man aus Bressoud [14], Koblitz [57] und Riesel [90] gewinnen. Das leistungsfähigste Faktorisierungsverfahren für natürliche Zahlen ist im Moment wohl das Zahlkörper-Sieb; darüber informieren die in [64] gesammelten Aufsätze.

**(2.25) Aufgaben:**

**Aufgabe 2:** Man schreibe eine MuPAD-Funktion, die mit Hilfe des Siebs des Eratosthenes (vgl. (2.8)) zu einer natürlichen Zahl $N$ die Liste aller Primzahlen $\leq N$ berechnet.

**Aufgabe 3:** Es sei $n \in \mathbb{N}$, und es sei $p$ eine Primzahl. Man beweise: Es gilt

$$v_p(n!) \;=\; \sum_{j=1}^{\lfloor \frac{\log n}{\log p} \rfloor} \left\lfloor \frac{n}{p^j} \right\rfloor \;=\; \sum_{j \geq 1} \left\lfloor \frac{n}{p^j} \right\rfloor .$$

**Aufgabe 4:** (Diese Aufgabe liefert einen Beweis für das Bertrandsche Postulat, vgl. (2.6)(1)). Für jedes $n \in \mathbb{N}$ sei

$$P(n) \;:=\; \prod_{n<p<2n} p$$

das Produkt aller Primzahlen $p$ mit $n < p < 2n$, und für jedes $x \in \mathbb{R}$ sei

$$Q(x) \;:=\; \prod_{p \leq x} p$$

das Produkt aller Primzahlen $p$ mit $p \leq x$.
(1) Man zeige: Für jedes $n \in \mathbb{N}$ gilt

$$P(n) \;\leq\; \binom{2n-1}{n} \;\leq\; 4^{n-1}.$$

(2) Man beweise durch Induktion: Für jedes $n \in \mathbb{N}$ gilt $Q(n) < 4^n$. Man folgere: Für jede reelle Zahl $x \geq 1$ gilt $Q(x) < 4^x$.

(3) Es sei $n \geq 3$, es sei $p$ eine Primzahl mit $2n/3 < p \leq n$. Man beweise: $p$ teilt $\binom{2n}{n}$ nicht.

(4) Man zeige durch Induktion: Für jede natürliche Zahl $n \geq 2$ gilt

$$\binom{2n}{n} > \frac{4^n}{2\sqrt{n}}.$$

(5) Man beweise: Für jede natürliche Zahl $n \geq 32$ gilt

$$\binom{2n}{n} \leq (2n)^{\pi(\sqrt{2n})} \cdot P(n) \cdot Q\left(\frac{2n}{3}\right).$$

Man folgere daraus: Für jede natürliche Zahl $n \geq 32$ gilt

$$\binom{2n}{n} \leq (2n)^{\sqrt{2n}/2} \cdot 4^{2n/3} \cdot P(n).$$

(6) Man beweise: Für jedes $n \in \mathbb{N}$ mit $4^{2n} > 8 \cdot (2n)^{3\cdot(1+\sqrt{2n})}$ gilt $P(n) > 1$.

(7) Man beweise: Zu jeder natürlichen Zahl $n \geq 72$ gibt es eine Primzahl $p$ mit $n < p < 2n$.

(8) Man beweise: Zu jeder natürlichen Zahl $n \geq 2$ gibt es eine Primzahl $p$ mit $n < p < 2n$.

**Aufgabe 5:** Man schreibe eine MuPAD-Funktion, die für eine natürliche Zahl $n$ die Ausgabe `TRUE` liefert, falls die Mersenne-Zahl $M(n)$ eine Primzahl ist, und sonst die Ausgabe `FALSE`. Bei der Anwendung auf eine ungerade Primzahl $p$ sollte diese Funktion das Kriterium von Lucas und Lehmer (vgl. (2.9)(3)) in der folgenden Form benützen: Ist $(a_j)_{j\geq 1}$ die Folge mit

$$a_1 := 4 \quad \text{und} \quad a_{j+1} := (a_j^2 - 2) \bmod M(p) \quad \text{für jedes } j \in \mathbb{N},$$

so ist $M(p)$ genau dann eine Primzahl, wenn $a_{p-1} = 0$ ist. Warum wird man diese Abänderung verwenden? Liefert sie das korrekte Ergebnis?

**Aufgabe 6:** Eine natürliche Zahl $m$ heißt vollkommen, wenn sie gleich der Summe aller ihrer Teiler $d \in \mathbb{N}$ mit $d < m$ ist.

Es sei $m$ eine *gerade* natürliche Zahl. Man beweise, daß die folgenden beiden Aussagen äquivalent sind:

(a) $m$ ist eine vollkommene Zahl.

(b) Es gibt ein $n \in \mathbb{N}$ mit: Die Mersenne-Zahl $M(n)$ ist eine Primzahl, und es gilt

$$m \;=\; 2^{n-1}M(n).$$

Bemerkung: Für vollkommene Zahlen und daher für Mersenne-Zahlen, die Primzahlen sind, interessierte man sich schon in der Antike. Die 37 heute bekannten Mersenne-Zahlen, die Primzahlen sind, liefern 37 gerade vollkommene Zahlen. Ob es ungerade vollkommene Zahlen gibt, weiß man nicht; man weiß aber, daß es keine ungerade vollkommene Zahl $\leq 10^{300}$ gibt und daß eine ungerade vollkommene Zahl mindestens acht verschiedene Primteiler besitzt. Es dürfte sich wohl nicht lohnen, mittels MuPAD nach solchen Zahlen zu suchen.

**Aufgabe 7:** Es sei $n \in \mathbb{N}$. Man beweise: Zu $a \in \mathbb{N}$ gibt es ein $b \in \mathbb{N}$ mit

$$\frac{1}{n} \;=\; \frac{1}{a} + \frac{1}{b},$$

genau wenn es einen Teiler $d \in \mathbb{N}$ von $n^2$ mit $a = n + d$ gibt. Man schreibe eine MuPAD-Funktion, die zu jeder natürlichen Zahl $n$ alle Paare $(a, b) \in \mathbb{N} \times \mathbb{N}$ mit

$$\frac{1}{n} \;=\; \frac{1}{a} + \frac{1}{b} \quad \text{und} \quad a \;\leq\; b$$

berechnet.

**Aufgabe 8:** Man gewinne mit Hilfe der in (2.11) angegebenen drei Funktionen

$$x \mapsto \frac{x}{\log x} : [\,2, \infty\,[ \to \mathbb{R}, \quad \mathrm{Li} : [\,2, \infty\,[ \to \mathbb{R} \quad \text{und} \quad R : [\,2, \infty\,[ \to \mathbb{R}$$

Näherungswerte für Werte der Primzahlfunktion $\pi$. Einige Werte dieser Funktion sind in der Tabelle in (2.11)(1) angegeben, weitere Werte findet man in Riesel [90], Tabelle 3, in der Arbeit [24] von M. Deleglise und J. Rivat und auch unter der in (2.9)(4) angegebenen Internet-Adresse.

**Aufgabe 9:** Diese Aufgabe handelt von einer auf Fermat zurückgehende Methode, nichttriviale Teiler einer natürlichen Zahl zu finden. Diese Methode erfordert einen vergleichsweise geringen Aufwand, wenn die zu faktorisierende Zahl das Produkt zweier nahezu gleich großer Faktoren ist.

(1) Es sei $m$ eine ungerade natürliche Zahl $> 1$, die keine Primzahl ist. Man zeige, daß es Zahlen $x$, $y \in \mathbb{N}_0$ gibt, für die gilt: Es ist

$$\lceil \sqrt{m} \rceil \;\leq\; x \;\leq\; \left\lfloor \frac{1}{2}\sqrt{m} + \frac{1}{6}\,m \right\rfloor \quad \text{und} \quad m \;=\; x^2 - y^2,$$

und $m = (x - y)(x + y)$ ist eine nichttriviale Faktorzerlegung von $m$.

(2) Man schreibe eine MuPAD-Funktion, die für eine natürliche Zahl $m > 1$ mit Hilfe der in (1) geschilderten Methode eine nichttriviale Faktorisierung von $m$ findet, bzw. feststellt, daß $m$ eine Primzahl ist.

**Aufgabe 10:** (1) Man vervollständige die in (2.21) gegebene Definition der MuPAD-Funktion `pollard`: Einerseits fehlen die Abfragen, die überprüfen, ob bei einem Aufruf der Funktion die übergebenen Parameter vom richtigen Typ sind, andererseits fehlt am Anfang von `pollard` die Abfrage, ob die zu faktorisierende Zahl $m$ eine Primzahl ist; ist $m$ eine Primzahl, so wird man das Verfahren sofort abbrechen.

(2) Man experimentiere mit der Funktion `pollard`; insbesondere ändere man die darin verwendete Funktion $f$ ab. (Funktionen wie die in (2.21)(2) angegebenen programmiert man in MuPAD übrigens mit Hilfe der Funktion `powermod`, vgl. dazu (4.24)). Man ändere die Definition von `pollard` so ab, daß neben einem gefundenem Teiler auch die Anzahl der zum Auffinden dieses Teilers benötigten Iterationen ausgegeben wird.

**Aufgabe 11:** Es sei $m \in \mathbb{N}$, es sei $f : \{0, 1, \ldots, m-1\} \to \{0, 1, \ldots, m-1\}$ eine Abbildung, und es sei $x_0 \in \{0, 1, \ldots, m-1\}$. Die Folge $(x_i)_{i \geq 0}$ mit $x_i := f(x_{i-1})$ für jedes $i \in \mathbb{N}$ ist nach einer Vorperiode periodisch; es seien $k$ die Länge der Vorperiode und $l$ die minimale Periodenlänge. Man beweise: Für $i := l \cdot (1 + \lfloor k/l \rfloor)$ ist $x_i = x_{2i}$.

**Aufgabe 12:** Man schreibe eine MuPAD-Funktion zum Test von Pepin aus Abschnitt (2.22) und wende sie auf einige Fermat-Zahlen an. Man versuche, mittels der in (2.21) beschriebenen rho-Methode von Pollard (und auch mit Hilfe der MuPAD-Funktion `ifactor`) nichttriviale Faktoren einiger Fermat-Zahlen $F(n)$ mit $n \geq 5$ zu finden (vgl. Riesel [90], Tabelle 4).

**Aufgabe 13:** Eine natürliche Zahl $n$ heißt teilerreich, wenn gilt: Für jede natürliche Zahl $k < n$ ist $\tau(k) < \tau(n)$. Man ermittle mittels MuPAD die ersten teilerreichen natürliche Zahlen, sehe sich ihre Primzerlegungen an, formuliere eine Vermutung und beweise sie oder lese dazu Kapitel 14 in Honsberger [46]. Mit teilerreichen Zahlen hat sich wohl zuerst der indische Zahlentheoretiker S. Ramanujan in [87] befaßt. In dieser Arbeit findet sich eine Tabelle von teilerreichen Zahlen; die größte darin ist 674 63283 88800.

# 3 Endliche abelsche Gruppen

**(3.1)** In diesem Paragraphen werden Gruppen $G$ betrachtet, deren Verknüpfung als "Multiplikation" $(a, b) \mapsto ab : G \times G \to G$ geschrieben ist. Ist $G$ eine solche Gruppe, so wird ihr neutrales Element mit $e_G$ bezeichnet, und für jedes $a \in G$ wird das zu $a$ inverse Element mit $a^{-1}$ bezeichnet.