Manuskript zur Vorlesung Elementare Zahlentheorie

gehalten von

PD Dr. K. HALUPCZOK

im

Sommersemester 2009

an der

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Dieses Manuskript wurde unter LaTeX gesetzt von
Dipl.–Math. S. FEILER

und basiert auf dem von M. GILG geTeXten
Manuskript zur Vorlesung Elementare Zahlentheorie SS 2005
von Prof. Dr. D. WOLKE.

Inhaltsverzeichnis

Einleitung

Über elementare Zahlentheorie

Die Vorlesung gibt eine Einführung in die elementare Zahlentheorie. Das Wort „elementar“ bedeutet dabei erstens, dass die Fragestellungen sich fast ausschließlich auf Eigenschaften der natürlichen und der ganzen Zahlen beziehen. Zweitens sollen außer Grundkenntnissen in Analysis und Algebra keine weiteren Hilfsmittel verwandt werden.

Die Zahlentheorie ist neben der Geometrie der älteste Teil der Mathematik. Aus Babylonien, dem alten Ägypten, und China sind erste theoretische Quellen überliefert (z.B. die Darstellung einer rationalen Zahl $a/q \in (0,1]$ als Summe $\frac{1}{n_1} + \cdots + \frac{1}{n_k}$ mit $n_j \in \mathbb{N}$ für alle $j \in \mathbb{N}$ mit $j \leq k$, $1 < n_1 < \ldots < n_k$ und $k \in \mathbb{N}$, „ägyptische Brüche“).

Die alten Griechen untersuchten Probleme, die teilweise noch heute aktuell sind, z.B. „diophantische Gleichungen“, d.h. die Suche nach ganzzahligen Lösungen von Gleichungen wie $x^2 + y^2 = z^2$ („pythagoräische Tripel“), oder das höchst rätselhafte Verhalten der Folge der Primzahlen.

Da einerseits die Bausteine, die Elemente von $\mathbb{Z}$, begrifflich leicht zugänglich sind, andererseits so viele höchst schwierige, zum Teil noch ungelöste Probleme bestehen, gehörte die Zahlentheorie stets zu dem bevorzugten Arbeitsgebiet der Mathematiker. Einige der bekanntesten Namen, wie Euler, Lagrange oder Gauss, werden im Folgenden mehrfach auftreten. Durch die Entwicklung schneller Rechner sind zahlentheoretische Methoden in den letzten Jahrzenten auch für Anwendungen, z.B. die Kryptografie, sehr wichtig geworden.

Mit dem Ausbau der Mathematik, vor allem seit Beginn des 19. Jahrhunderts, erweiterte sich die Zahlentheorie in Bezug auf Fragestellungen und Methoden erheblich. Die Untersuchung von algebraischen, transzendenten und p–adischen Zahlen, von Folgen ganzer Zahlen, unendlichen Reihen mit zahlentheoretisch interessanten Koeffizienten und vielem anderen gehört heute zu den Zweigen des uralten, aber immer noch rasch wach-

senden Baumes der Zahlentheorie. Dementsprechend werden Hilfsmittel aus nahezu allen Teilen der Mathematik verwandt, vor allem aus Algebra (algebraische Zahlentheorie) und komplexer Analysis (analytische Zahlentheorie).

In Freiburg werden regelmäßig Fortsetzungsveranstaltungen angeboten, insbesondere über transzendente Zahlen, algebraische und analytische Zahlentheorie. Hierfür ist der elementare Teil die verbindende Grundlage.

Literatur

Es gibt zahllose Einführungen in die Zahlentheorie.
Bei den folgenden Büchern handelt es sich um bewährte „Klassiker“.

- „*An Indroduction to the Theory of Numbers*“, G. H. Hardy and E. M. Wright, Clarendon Press (Oxford — 1979 (fifth edition))
- „*Introduction to number theory*“, Hua L. K., Springer–Verlag (Berlin, Heidelberg, New York — 1982)

Notation

$\mathbb{C}$ bezeichnet die Menge der komplexen Zahlen.
$\mathbb{R}$ bezeichnet die Menge der reellen Zahlen.
$\mathbb{R}^+$ bezeichnet die Menge der positiven reellen Zahlen (exklusive der 0).
$\mathbb{Q}$ bezeichnet die Menge der rationalen Zahlen.
$\mathbb{Z}$ bezeichnet die Menge der ganzen Zahlen.
$\mathbb{N}_0$ bezeichnet die Menge der natürlichen Zahlen (inklusive der 0).
$\mathbb{N}$ bezeichnet die Menge der natürlichen Zahlen (exklusive der 0).
$\mathbb{P}$ bezeichnet die Menge der Primzahlen.
Für eine Menge $\mathcal{A}$ bezeichnet $\#\mathcal{A} \in \mathbb{N}_0 \cup \{\infty\}$ die Anzahl der Elemente von $\mathcal{A}$.
Bei Gleitkommazahlen wird der ganzzahlige Anteil vom gebrochenen Anteil stets mit einem Punkt „ . “ getrennt.

Kapitel 1: Teilbarkeit

Während die Umkehrung der Addition, die Subtraktion, in $\mathbb{Z}$ unbeschränkt ausführbar ist, lässt sich die Division nicht immer durchführen. $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z} \setminus \{0\}$ und $\mathbb{Z}$ sind bezüglich der Multiplikation nur Halbgruppen. Der wesentliche Begriff hierzu ist der der **Teilbarkeit**.

Definition 1.1 (Teiler und Vielfache)

a) $a \in \mathbb{Z}$ **teilt** $b \in \mathbb{Z}$ (oder: a ist **Teiler** von b, b wird von a **geteilt**, b ist **Vielfaches** von a), falls es ein $c \in \mathbb{Z}$ mit $b = a \cdot c$ gibt.

c heißt dann **Gegenteiler** von a bezüglich b.

Kurz: $a|b \quad :\Longleftrightarrow \quad \exists\, c$ mit $b = ac$

Andernfalls $a \nmid b$ (a teilt b nicht)

b) $a \in \mathbb{Z}$ heißt **echter Teiler** von $b \in \mathbb{Z}$, falls $a|b$ und $|a| < |b|$ gelten.

Dann heißt b **echtes Vielfaches** von a.

Beispiel $1|5, \quad 5|5, \quad 2 \nmid 5, \quad 10|0, \quad -2|6, \quad 0|0, \quad 0 \nmid a \quad \forall\, a \neq 0.$

Folgerung 1.2
Für alle $a \in \mathbb{Z}$, alle $b \in \mathbb{Z}$ und alle $c \in \mathbb{Z}$ gilt

(1) $a|b \quad \Longrightarrow \ \forall\, z \in \mathbb{Z} : a|\,(bz)$

(2) $a|b \ \wedge \ b|c \Longrightarrow a|c$

(3) $a|b \ \wedge \ a|c \Longrightarrow \forall\ x, y \in \mathbb{Z} : \ a|\,(xb + yc)$

(4) $a|b \ \wedge \ b|a \Longrightarrow |a| = |b|$

(5) $a|b \ \wedge \ b \neq 0 \Longrightarrow |a| \leq |b|$

(6) $a|b \quad \Longrightarrow \ \forall\, z \in \mathbb{Z} : \ \ (za)\,|\,(zb)$

BEWEIS: (von Folgerung (4))
Es gibt ein $c_1 \in \mathbb{Z}$ und ein $c_2 \in \mathbb{Z}$ mit $b = c_1 a$ und $a = c_2 b$. Also ist $b = c_1 c_2 b$.
Im Fall $b = 0$ folgt $a = 0$. Im Fall $b \neq 0$ folgt $c_1 c_2 = 1$, also $c_1 \in \{-1, 1\}$ und $c_2 \in \{-1, 1\}$. □

Definition 1.3 (GAUSS–Klammer)
$\lfloor \cdot \rfloor : \left\{ \begin{array}{rcl} \mathbb{R} & \to & \mathbb{Z} \\ t & \mapsto & \lfloor t \rfloor := \max\{\, a \in \mathbb{Z}\,;\, a \leq t \} \end{array} \right\}$ heißt **GAUSS'sche Größte–Ganze–Funktion**. (Kurz: **GAUSS–Klammer**)
($\lfloor t \rfloor$ ist die **größte ganze Zahl kleiner oder gleich** $t \in \mathbb{R}$.
Kurz: Größtes Ganzes von t oder **GAUSS–Klammer** von t)

Hinweis
Häufig findet man auch die Schreibweise $[\,\cdot\,]$ für die GAUSS–Klammer.

Beispiel $\lfloor a \rfloor = a \quad \forall\, n \in \mathbb{Z}, \qquad \lfloor \pi \rfloor = 3, \qquad \lfloor -\pi \rfloor = -4.$

SATZ 1.4 (Division mit Rest)
BEHAUPTUNG:

$$\forall\, a \in \mathbb{Z}\ \forall\, n \in \mathbb{N}\ \exists\, r \in \mathbb{N}_0 \ \textit{mit } r < n \ \textit{und } a = \left\lfloor \frac{a}{n} \right\rfloor n + r.$$

In der Darstellung $a = bn + r$ mit $b \in \mathbb{Z}$, $r \in \mathbb{N}_0$ und $r < n$ sind b und r für alle $a \in \mathbb{Z}$ und alle $n \in \mathbb{N}$ eindeutig festgelegt.

BEWEIS:
Nach Definition von $\lfloor\cdot\rfloor$ ist $\left\lfloor\frac{a}{n}\right\rfloor \leq \frac{a}{n} < \left\lfloor\frac{a}{n}\right\rfloor + 1$, also $0 \leq a - \left\lfloor\frac{a}{n}\right\rfloor n < n$.
Dies ist die Ungleichung für r und es folgt die erste Behauptung.
Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Es existieren somit $b \in \mathbb{Z}$ und $r \in \mathbb{N}_0$ mit $a = bn + r$ und $r < n$.
Seien $b' \in \mathbb{Z}$ und $r' \in \mathbb{N}_0$ mit $a = b'n + r'$ und $r' < n$.
Dann ergibt sich $0 = (b - b') \cdot n + (r - r')$, wobei $-n < r - r' < n$.
Dies ist nur möglich mit $b = b'$ und $r = r'$. □

Das zu $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ eindeutig bestimmte $r \in \mathbb{N}_0$ heißt der **kleinste nichtnegative Rest** von a bei Division durch n.
Es kann r auch durch die Forderung $|r| \leq \frac{n}{2}$ (**absolut kleinster Rest**) festgelegt werden. Dann ist es nicht immer eindeutig festgelegt ($30 = 7 \cdot 4 + 2 = 8 \cdot 4 - 2$).

Definition 1.5 (Gemeinsame Teiler)
Für diese Definition seien $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $n \in \mathbb{N} \setminus \{1\}$ und $a_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}$ mit $j \leq n$.

a) $d \in \mathbb{N}$ heißt **gemeinsamer Teiler** von a und b, falls $d|a$ und $d|b$ gelten.

b) Ist $a^2 + b^2 \neq 0$, so heißt $\mathrm{ggT}\,(a, b) := \max\{\, c \in \mathbb{N}\,;\, c|a \text{ und } c|b\}$ **größter gemeinsamer Teiler** von a und b.

Kurz: $(a, b) := \mathrm{ggT}\,(a, b)$.

c) Ist $a \neq 0$, so sei $\mathrm{ggT}\,(a) := |a|$.

Sind $n \neq 2$ und $\sum_{j=1}^{n-1} a_j^2 \neq 0$, so seien

$$\mathrm{ggT}\,(a_1, \ldots, a_n) := ((a_1, \ldots, a_{n-1}), a_n)$$

und

$$\mathrm{ggT}\,(0, \ldots, 0, a_n) := |a_n|\,, \text{falls } a_n \neq 0 \text{ ist.}$$

Kurz: $(a_1, \ldots, a_n) := \mathrm{ggT}\,(a_1, \ldots, a_n)$

Sind $n \neq 2$ und $\sum_{j=1}^{n} a_j^2 \neq 0$, so heißt $\mathrm{ggT}\,(a_1, \ldots, a_n)$ **größter gemeinsamer Teiler** von $a_1, \ldots, a_n$.

d) a und b heißen **teilerfremd** oder **relativ prim**, wenn $(a, b) = 1$ und $a^2 + b^2 \neq 0$ sind.

$a_1, \ldots, a_n$ heißen **teilerfremd**, wenn $\mathrm{ggT}\,(a_1, \ldots, a_n) = 1$ und $\sum_{j=1}^{n} a_j^2 \neq 0$ sind.

$a_1, \ldots, a_n$ heißen **paarweise teilerfremd**, wenn $\#\{\, j \in \mathbb{N}\,;\, j \leq n \text{ und } a_j = 0\} \leq 1$ und

$$(a_j, a_k) = 1 \qquad \text{für alle } j \in \mathbb{N} \text{ und alle } k \in \mathbb{N} \text{ mit } j < k \leq n \text{ gilt.}$$

Aus der paarweisen Teilerfremdheit folgt die Teilerfremdheit.
Die Umkehrung braucht nicht zu gelten.

Beispiel Es ist $(6, 10, 15) = 1$, aber es sind $(6, 10) = 2$, $(6, 15) = 3$ und $(10, 15) = 5$.

Satz 1.6 (Minimaleigenschaft des ggT / Darstellung des ggT als $\mathbb{Z}$–Linearkombination)
Voraussetzungen:
Seien $n \in \mathbb{N}$ und $a_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}$ mit $j \leq n$ derart, dass $\sum_{j=1}^{n} a_j^2 \neq 0$ ist.

Behauptung: *Es ist*

$$(a_1, \ldots, a_n) = \min \{d \in \mathbb{N}; \exists\, z_1 \in \mathbb{Z} \ldots \exists\, z_n \in \mathbb{Z} \text{ mit } d = z_1 a_1 + \ldots + z_n a_n\}.$$

Dieser Satz wird später bewiesen.

Folgerung 1.7
Seien $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $d \in \mathbb{N}$, $n \in \mathbb{N}$, $a_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}$ mit $j \leq n$, $\mathcal{N} := \{m \in \mathbb{N}\,; m \leq n\}$ und $\sigma : \left\{ \begin{array}{ccc} \mathcal{N} & \to & \mathcal{N} \\ m & \mapsto & \sigma(m) \end{array} \right\}$ bijektiv derart, dass $a^2 + b^2 \neq 0$ und $\sum_{j=1}^{n} a_j^2 \neq 0$ sind. Dann gilt

(1) $d = (a, b) \iff d|a$ und $d|b$ und $\forall\, c \in \mathbb{N}$ gilt $(c|a \wedge c|b \Longrightarrow c|d)$

(2) $(ca, cb) = |c|\,(a, b) \quad \forall\, c \in \mathbb{Z} \setminus \{0\}$

(3) $(a_1, \ldots, a_n) = \left(a_{\sigma(1)}, \ldots, a_{\sigma(n)}\right)$

Beweis:

(i) Zu (1) „$\Longrightarrow$“
Es gelte $d = (a, b)$, so gilt $d|a$ und $d|b$ und nach Satz 1.6 gibt es ein $z_1 \in \mathbb{Z}$ und ein $z_2 \in \mathbb{Z}$ mit $d = z_1 a + z_2 b$.
Für alle $c \in \mathbb{Z}$ mit $c|a$ und $c|b$, gibt es ein $d_1 \in \mathbb{Z}$ mit $a = d_1 c$ und ein $d_2 \in \mathbb{Z}$ mit $b = d_2 c$, woraus folgt

$$d = z_1 a + z_2 b = z_1 d_1 c + z_2 d_2 c = (z_1 d_1 + z_2 d_2) \cdot c.$$

Also ist c auch ein Teiler von d für alle $c \in \mathbb{Z}$ mit $c|a$ und $c|b$.

(ii) Zu (1) „$\Longleftarrow$“
Es gelte $d|a$, $d|b$ und $c|d$ für alle $c \in \mathbb{Z}$ mit $c|a$ und $c|b$.
Sei $c' := \max\{c \in \mathbb{N}\,; c|a \text{ und } c|b\}$. Dann ist $c' = (a, b)$.
Nach Voraussetzung gilt $c'|d$.
Wegen $d|a$, $d|b$ und $d \in \mathbb{N}$ ist aber $d \leq c'$ nach Definition von c'.
Damit folgt also $d = c' = (a, b)$.

(iii) Zu (2)
Sei $c \in \mathbb{Z} \setminus \{0\}$. Es gelte $d = (a, b)$. Zu zeigen ist also $|c|\, d = (ac, bc)$.
Nach Satz 1.6 gibt es ein $z_1 \in \mathbb{Z}$ und ein $z_2 \in \mathbb{Z}$ mit $d = z_1 a + z_2 b$, $d|a$ und $d|b$. Nach Folgerung 1.2 (6) auf Seite 4 ist $|c|\, d$ ein Teiler von $a\,|c|$ und von $b\,|c|$.
Dann teilt $|c|\, d$ aber auch ac und bc.
Sei $e \in \mathbb{Z}$ mit $e|\,(ac)$ und $e|\,(bc)$. Dann teilt e auch

$$|c|\, d = |c| \cdot (z_1 a + z_2 b) = z_1 a\,|c| + z_2 b\,|c| = \operatorname{sign}(c)\, z_1\,(ac) + \operatorname{sign}(c)\, z_2\,(bc)\,.$$

Nach (1) ist $|c|\, d = (ac, bc)$.

(iv) Zu (3)
$(a_1, \ldots, a_n) = \left(a_{\sigma(1)}, \ldots, a_{\sigma(n)}\right)$ ist klar nach Satz 1.6. □

(1) kann auch folgendermaßen ausgedrückt werden:
Für alle $a \in \mathbb{Z}$ sei $\mathcal{T}(a)$ die Menge der Teiler von a. ($\mathcal{T}(0) = \mathbb{Z}$, $|\mathcal{T}(a)| < \infty$ für alle $a \in \mathbb{Z} \setminus \{0\}$)
Dann gilt für alle $a \in \mathbb{Z}$ und alle $b \in \mathbb{Z}$ mit $a^2 + b^2 \neq 0$

$$\mathcal{T}(a) \cap \mathcal{T}(b) = \mathcal{T}((a, b))\,.$$

(3) bedeutet, dass die Berechnung eines größten gemeinsamen Teilers von beliebig vielen Zahlen nicht auf die Reihenfolge der Zahlen ankommt.

Der Beweis zu Satz 1.6 beruht auf dem „Euklidischen Algorithmus“, dem ersten nicht auf der Hand liegenden algorithmischen Verfahren der Mathematik.

Algorithmus 1.8 (Euklidischer Algorithmus)
(Eukleides von Alexandria, um 300 vor Christus)
Zu gegebenen $n_1 \in \mathbb{N}$ und $n_2 \in \mathbb{N}$ finde man ein $k \in \mathbb{N}$ und für alle $j \in \mathbb{N}$ mit $j < k$ ein $a_j \in \mathbb{N}$ und ein $n_{j+2} \in \mathbb{N}$, so dass das folgende Schema von Divisionen mit Rest gilt:

$$\begin{aligned}
n_1 &= a_1 n_2 + n_3 && 0 < n_3 < n_2\\
n_2 &= a_2 n_3 + n_4 && 0 < n_4 < n_3\\
&\vdots\\
n_j &= a_j n_{j+1} + n_{j+2} && 0 < n_{j+2} < n_{j+1}\\
&\vdots\\
n_{k-2} &= a_{k-2} n_{k-1} + n_k && 0 < n_k < n_{k-1}\\
n_{k-1} &= a_{k-1} n_k
\end{aligned}$$

Behauptung: *Es ist* $n_k = (n_1, n_2)$.

BEWEIS:

(i) $n_k \geq (n_1, n_2)$
Sei $d \in \mathbb{N}$ ein gemeinsamer Teiler von n_1 und n_2.
Aus der ersten Zeile des Schemas folgt $d|n_3$, aus der zweiten $d|n_4$, also

$$d|n_1 \text{ und } d|n_2 \quad \Longrightarrow \quad d|n_k.$$

Also ist (n_1, n_2) ein Teiler von n_k und insbesondere gilt $(n_1, n_2) \leq n_k$.

(ii) n_k ist gemeinsamer Teiler von n_1 und n_2
Umgekehrt ergibt sich

$$n_k|n_{k-1}, \qquad n_k|n_{k-2}, \qquad \ldots, \qquad n_k|n_2 \qquad \text{und} \qquad n_k|n_1.$$

Also ist n_k ein gemeinsamer Teiler von n_1 und n_2.
Mit (i) folgt die Behauptung. □

Zusatzbemerkungen

1. Für die Praxis ist es wichtig, bei Paaren großer Zahlen rasch festzustellen, ob sie teilerfremd sind. Der EUKLIDische Algorithmus ist hierfür gut geeignet.

   Am Beweis sieht man, dass statt mit den kleinsten positiven Resten auch mit absolut kleinsten Resten gerechnet werden kann, d.h. in jedem Schritt erfolgt mindestens Halbierung, der Algorithmus stoppt nach $\leq C \cdot \ln(\min\{n_1, n_2\})$ Divisionen.

2. Auch bei den kleinsten positiven Resten stoppt er ähnlich schnell. Nach spätestens zwei Divisionen erfolgt Halbierung.

   Ist $n_2 < n_1$, dann ist $n_3 \leq \frac{1}{2} \cdot n_1$:

   Ist bereits $n_2 \leq \frac{1}{2} \cdot n_1$, dann ist es klar. Im Fall $n_2 > \frac{1}{2} \cdot n_1$ lautet die erste Zeile

   $$n_1 = n_2 + n_3 \quad \text{mit} \quad n_3 < \frac{1}{2} \cdot n_1.$$

   Ebenso bei den weiteren Divisionen.

Zur Erinnerung sei der noch zu beweisende Satz 1.6 hier noch einmal angegeben.

SATZ 1.6 (Minimaleigenschaft des ggT / Darstellung des ggT als $\mathbb{Z}$–Linearkombination)
VORAUSSETZUNGEN:
Seien $n \in \mathbb{N}$ und $a_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}$ mit $j \leq n$ derart, dass $\sum_{j=1}^{n} a_j^2 \neq 0$ ist.

BEHAUPTUNG: *Es ist*

$$(a_1, \ldots, a_n) = \min\{d \in \mathbb{N};\, \exists\, z_1 \in \mathbb{Z} \ldots \exists\, z_n \in \mathbb{Z} \text{ mit } d = z_1 a_1 + \ldots + z_n a_n\}.$$

BEWEIS:

(i) Anwenden des EUKLIDischen Algorithmus'
Seien $n_1 \in \mathbb{Z}$ und $n_2 \in \mathbb{Z}$ mit $n_1^2 + n_2^2 \neq 0$.
Aus dem EUKLIDischen Algorithmus 1.8 auf Seite 7 entnimmt man

$$\exists\, x_1 \in \mathbb{Z}\ \exists\, x_2 \in \mathbb{Z} \text{ mit } (n_1, n_2) = x_1 n_1 + x_2 n_2. \qquad (\diamondsuit)$$

(Denn nach der ersten Zeile läßt sich n_3 als ganzzahlige Linearkombination von n_1 und n_2 schreiben, nach der zweiten n_4, usw.)

(ii) „$n = 1$"
Der Beweis wird induktiv geführt.
Es ist $(a_1) = |a_1| = \min\{\, d \in \mathbb{N}\, ; \exists\, z_1 \in \mathbb{Z} \text{ mit } d = z_1 a_1\}$.
Sei nun also $n > 1$ vorausgesetzt.

(iii) Triviale Fälle
Ist $a_j = 0$ für alle $j \in \mathbb{N}$ mit $j < n$, so ist $a_n \neq 0$ und es folgt

$$(0, \ldots, 0, a_n) = |a_n| = \min\{\, d \in \mathbb{N}\, ; \exists\, z_1 \in \mathbb{Z} \ldots \exists\, z_n \in \mathbb{Z} \text{ mit } d = z_1 \cdot 0 + \ldots z_{n-1} \cdot 0 + z_n a_n\}.$$

Ist $a_n = 0$, so folgt $\sum_{j=0}^{n-1} a_j^2 \neq 0$ und die Induktionsvoraussetzung liefert

$$\begin{aligned}(a_1, \ldots, a_{n-1}, 0) &= (a_1, \ldots, a_{n-1}) \\ &= \min\{\, d \in \mathbb{N}\, ; \exists\, z_1 \in \mathbb{Z} \ldots \exists\, z_{n-1} \in \mathbb{Z} \text{ mit } d = z_1 a_1 + \ldots z_{n-1} a_{n-1}\} \\ &= \min\{\, d \in \mathbb{N}\, ; \exists\, z_1 \in \mathbb{Z} \ldots \exists\, z_n \in \mathbb{Z} \text{ mit } d = z_1 a_1 + \ldots z_{n-1} a_{n-1} + z_n \cdot 0\}.\end{aligned}$$

(iv) Nichttrivialer Fall
Es gelte nun $a_n \neq 0$ und $a_j \neq 0$ für ein $j \in \mathbb{N}$ mit $j < n$.
Seien dann

$$d_{n-1} := (a_1, \ldots, a_{n-1}) > 0 \quad \text{und} \quad d_n := (d_{n-1}, a_n) > 0.$$

Aus $(\diamondsuit)$ entnimmt man

$$\exists\, z' \in \mathbb{Z}\ \exists\, z_n \in \mathbb{Z} \text{ mit } d_n = z' d_{n-1} + z_n a_n.$$

Die Induktionsvoraussetzung für $a_1, \ldots, a_{n-1}$ liefert

$$\exists\, z_1 \in \mathbb{Z} \ldots \exists\, z_{n-1} \in \mathbb{Z} \text{ mit } d_n = z_1 a_1 + \ldots + z_n a_n.$$

Ist k das im Satz genannte Minimum, dann folgt $0 < k \leq d_n$.
Da umgekehrt $d_n | a_1, \ldots, d_n | a_n$ gilt, folgt $d_n | k$. Damit bleibt nur $d_n = k$. □

Lemma 1.9
VORAUSSETZUNGEN:
Seien $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ und $c \in \mathbb{Z}$ mit $b^2 + c^2 \neq 0$.
BEHAUPTUNG: **(1)** *Aus $(a, c) = (b, c) = 1$ folgt $(ab, c) = 1$, sofern $a^2 + c^2 \neq 0$ ist.*

(2) *Aus $c | (ab)$ und $(b, c) = 1$ folgt $c | a$.*

BEWEIS:

(i) Zu (2)
Es gilt $c|\,(ac)$. Gilt $c|\,(ab)$ und $(b,c)=1$, so teilt c auch $(ab,ac)=|a|\cdot(b,c)=|a|$, also $c|a$.

(ii) Zu (1)
Es gelte $a^2+c^2\neq 0$ und $(a,c)=(b,c)=1$. Sei $d:=(ab,c)$.
Mit Folgerung 1.7 (1) auf Seite 6 sieht man $d|\,(ab,ac)$ wegen $d|\,(ab)$ und $d|c$ bzw. $d|\,(ac)$.
Nach Folgerung 1.7 (2) ist $(ab,ac)=|a|\cdot(b,c)=|a|$ und somit ist d ein Teiler von a.
Mit $d|c$ und Folgerung 1.7 (1) folgt $d|\,(a,c)$. Wegen $(a,c)=1$ bleibt nur $d=1$. □

Definition 1.10 (Kleinstes gemeinsames Vielfaches)
Sind $n\in\mathbb{N}$ und $a_j\in\mathbb{Z}\setminus\{0\}$ für alle $j\in\mathbb{N}$ mit $j\leq n$, so heißt

$$\mathrm{kgV}\,(a_1,\ldots,a_n):=\min\{m\in\mathbb{N};\,\forall\, j\in\mathbb{N}\text{ mit }j\leq n\text{ gilt }a_j|m\}$$

kleinstes gemeinsames Vielfaches von $a_1,\ldots,a_n$.
Kurz: $[a_1,\ldots,a_n]:=\mathrm{kgV}\,(a_1,\ldots,a_n)$.

Hinweis
Wird die GAUSS–Klammer auch mit eckigen Klammern geschrieben, so darf im Fall $n=1$ das kleinste gemeinsame Vielfache nicht mit der GAUSS–Klammer verwechselt werden.
Für alle $a_1\in\mathbb{N}$ ist $\mathrm{kgV}\,(-a_1)=a_1$, aber $\lfloor -a_1\rfloor=-a_1$.

SATZ 1.11 (Satz über das kleinste gemeinsame Vielfache)
VORAUSSETZUNGEN:
Seien $n\in\mathbb{N}$, $a_j\in\mathbb{Z}\setminus\{0\}$ für alle $j\in\mathbb{N}$ mit $j\leq n$ und $b\in\mathbb{Z}$.
BEHAUPTUNG: **(1)** *b ist gemeinsames Vielfaches von $a_1,\ldots,a_n$ (d.h. $a_1|b,\ldots,a_n|b$) genau dann, wenn b Vielfaches von $[a_1,\ldots,a_n]$ ist.*

(2) *Es ist $[a_1,a_2]\cdot(a_1,a_2)=|a_1a_2|$, falls $n=2$ ist.*

Folgerung 1.7 (1) auf Seite 6 und Satz 1.11 entsprechen einander:

a) Die Menge der gemeinsamen Teiler von $a_1,\ldots,a_n$ ist gleich der Menge der Teiler von $(a_1,\ldots,a_n)$.

b) Die Menge der gemeinsamen Vielfachen von $a_1,\ldots,a_n$ ist gleich der Menge der Vielfachen von $[a_1,\ldots,a_n]$.

BEWEIS:

(i) zu (2)
Für diesen Beweispunkt gelte $n=2$.
Sei $m\in\mathbb{N}$ ein Vielfaches von a_1 und a_2.

Dann gibt es ein $b \in \mathbb{Z}$ mit $m = a_1 b$ und m ist zugleich Vielfaches von a_2. Damit folgt

$$k := \frac{m}{a_2} = \frac{a_1 b}{a_2} \in \mathbb{Z}.$$

Seien $d := (a_1, a_2)$, $c_1 := \frac{a_1}{d}$ und $c_2 := \frac{a_2}{d}$. Nach Folgerung 1.7 (2) auf Seite 6 ist $(c_1, c_2) = 1$.
Dies ergibt $k = \frac{a_1 b}{a_2} = \frac{c_1 b}{c_2}$, also $c_2 | c_1 b$.
Wegen $(c_2, c_1) = 1$ und Lemma 1.9 (2) auf Seite 9 folgt $c_2 | b$ und es gibt ein $c \in \mathbb{Z}$ mit $b = c_2 c$.
Es folgt

$$m = a_1 b = a_1 c_2 c = \frac{a_1 a_2}{d} \cdot c.$$

Also wird jedes gemeinsame Vielfache von a_1 und a_2 von $\frac{a_1 a_2}{(a_1, a_2)}$ geteilt.
Das kleinstmögliche gemeinsame Vielfache von a_1 und a_2 ist damit $\frac{|a_1 a_2|}{(a_1, a_2)}$.
Das ist Behauptung (2).

(ii) zu (1)
Die letzten Überlegungen beinhalten Aussage (1) für $n = 2$.
Im Fall $n = 1$ ist Aussage (1) trivial.
Die Erweiterung von (1) auf $n > 2$ erfolgt induktiv. Man erhält ähnlich wie beim ggT die Rekursion

$$[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n].$$ □

Bemerkung 1.12
Satz 1.11 (2) gilt i.a. nicht für $n \geq 3$.
Richtig ist dagegen:
$a_1, \ldots, a_n$ sind genau dann paarweise teilerfremd, wenn $[a_1, \ldots, a_n] = |a_1 \cdot \ldots \cdot a_n|$.

BEWEIS:

(i) „$\Longrightarrow$“
Der Beweis wird durch Induktion geführt. Der Induktionsanfang ($n = 2$) ist Satz 1.11 (2).
Mit der Induktionsvoraussetzung und Satz 1.11 (2) folgt für $n \geq 2$

$$\begin{aligned}[a_1, \ldots, a_{n+1}] &= [[a_1, \ldots, a_n], a_{n+1}] = [|a_1 \cdot \ldots \cdot a_n|, a_{n+1}] \\ &= \underbrace{\frac{1}{(|a_1 \cdot \ldots \cdot a_n|, a_{n+1})}}_{=1} \cdot ||a_1 \cdot \ldots \cdot a_n| \cdot a_{n+1}| = |a_1 \cdot \ldots \cdot a_{n+1}|.\end{aligned}$$

(ii) „$\Longleftarrow$“
Der Beweis wird durch Induktion geführt. Der Induktionsanfang ($n = 2$) ist Satz 1.11 (2).
Mit der Voraussetzung und Satz 1.11 (2) folgt für $n \geq 2$

$$|a_1 \cdot \ldots \cdot a_{n+1}| = [a_1, \ldots, a_{n+1}] = [[a_1, \ldots, a_n], a_{n+1}] = \frac{|[a_1, \ldots, a_n]| \cdot |a_{n+1}|}{([a_1, \ldots, a_n], a_{n+1})}.$$

Das heißt, $([a_1, \ldots, a_n], a_{n+1}) \cdot |a_1 \cdot \ldots \cdot a_n| = [a_1, \ldots, a_n]$.
Also ist $|a_1 \cdot \ldots \cdot a_n|$ ein Teiler von $[a_1, \ldots, a_n]$.
Da $|a_1 \cdot \ldots \cdot a_n|$ ein Vielfaches von a_j für alle $j \in \mathbb{N}$ mit $j \leq n$ ist, ist $|a_1 \cdot \ldots \cdot a_n| \geq [a_1, \ldots, a_n]$.
Es bleibt nur $|a_1 \cdot \ldots \cdot a_n| = [a_1, \ldots, a_n]$.
Damit folgt $([a_1, \ldots, a_n], a_{n+1}) = 1$.
Das heißt insbesondere $(a_j, a_{n+1}) = 1$ für alle $j \in \mathbb{N}$ mit $j \leq n$.
Nach Induktionsvoraussetzung folgt aus $|a_1 \cdot \ldots \cdot a_n| = [a_1, \ldots, a_n]$ außerdem

$$(a_j, a_k) = 1 \qquad \text{für alle } j \in \mathbb{N} \text{ und alle } k \in \mathbb{N} \text{ mit } j < k \leq n. \qquad \square$$

Die Primzahlen als multiplikative Bausteine der ganzen Zahlen bilden eine wichtige Teilmenge von $\mathbb{N}$ und haben von Beginn an die Aufmerksamkeit der Mathematiker auf sich gezogen.

Definition 1.13 (Primzahlen)

a) $p \in \mathbb{N}$ heißt **Primzahl** (oder **prim**), wenn $p > 1$ ist und nur die natürlichen Teiler 1 und p besitzt.

$\mathbb{P} := \{q \in \mathbb{N}; q \text{ ist Primzahl}\}$ ist die **Menge aller Primzahlen**.

b) $n \in \mathbb{N} \setminus \{1\}$ heißt **zusammengesetzt**, wenn n keine Primzahl ist.

Folgerung 1.14 (Lemma von Euklid)
Behauptung: $p \in \mathbb{N} \setminus \{1\}$ *ist genau dann eine Primzahl, wenn*

$$\forall\, a \in \mathbb{N}\ \forall\, b \in \mathbb{N} \text{ mit } p|\,(ab) \text{ folgt: } (p|a \text{ oder } p|b).$$

Beweis:

(i) „$\Longrightarrow$“
Seien $p \in \mathbb{P}$ eine Primzahl, $a \in \mathbb{N}$ und $b \in \mathbb{N}$ mit $p|\,(ab)$.
Ist $d := (p, a) > 1$, so muss $d = p$ sein. Dann folgt $p|a$.
Im Fall $(p, a) = 1$ folgt $p|b$ nach Lemma 1.9 (2) auf Seite 9.

(ii) „$\Longleftarrow$“
Die Umkehrung ist simpel.
Sei $n \in \mathbb{N} \setminus \{1\}$ zusammengesetzt.
Dann gibt es $n_1 \in \mathbb{N} \setminus \{1\}$ und $n_2 \in \mathbb{N} \setminus \{1\}$ mit $n = n_1 n_2$.
Insbesondere gilt $n|n_1 n_2$.
Wegen $n_1 > 1$ und $n_2 > 1$ ist $n > \max\{n_1, n_2\}$ und deshalb gilt weder $n|n_1$ noch $n|n_2$. $\square$

Satz 1.15 (Unendlichkeit der Primzahlmenge (Euklid))
Behauptung: *Es existieren unendlich viele Primzahlen.*

Beweis:

(i) Erster Beweis (nach Euklid)
Jedes $n \in \mathbb{N} \setminus \{1\}$ besitzt mindestens einen Primteiler (also Teiler, der Primzahl ist), beispielsweise den kleinsten Teiler d von n mit $1 < d \leq n$.
Seien $k \in \mathbb{N}$ und $p_j \in \mathbb{P}$ für alle $j \in \mathbb{N}$ mit $j \leq k$ verschiedene Primzahlen.
(Das heißt z.B., es ist $p_j < p_{j+1}$ für alle $j \in \mathbb{N}$ mit $j \leq k-1$.)
Dann ist jeder Primteiler von $n := 1 + \prod_{j=1}^{k} p_j > 1$ von $p_1, \ldots, p_k$ verschieden.
Denn aus $q \in \mathbb{P}$, $q|n$ und $q = p_j$ für ein $j \in \mathbb{N}$ mit $j \leq k$ folgte $q|1$, was nicht sein kann.
Auf diese Weise können unendlich viele Primzahlen gewonnen werden. □

(ii) Zweiter Beweis (nach Euler)
Angenommen es gibt ein $k \in \mathbb{N}$ und für alle $j \in \mathbb{N}$ mit $j \leq k$ ein $p_j \in \mathbb{P}$ mit

$$\mathbb{P} = \{ p_j \in \mathbb{P} \,;\, j \in \mathbb{N} \text{ mit } j \leq k \}\,.$$

Das heißt, $p_1, \ldots, p_k$ sind alle Primzahlen.
Dann ist das Produkt

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

konvergent, da es endlich ist. Mit dem Satz über die Eindeutigkeit der Primfaktorzerlegung 1.17 auf Seite 15 (zu dessen Beweis die Unendlichkeit der Primzahlmenge nicht benutzt wird) sieht man, dass das Produkt mit $\sum_{n=1}^{\infty} \frac{1}{n}$ übereinstimmt.
Die Divergenz der harmonischen Reihe ergibt einen Widerspruch. □

(iii) Dritter Beweis
Im Zusammenhang mit der Frage nach der Konstruierbarkeit des regulären n–Ecks ($n \in \mathbb{N}$) mit Zirkel und Lineal taucht das Problem auf, welche der Zahlen $2^m + 1$ mit $m \in \mathbb{N}$ prim sind. Weil für alle $k \in \mathbb{N}$ und alle (ungeraden) $\ell \in \mathbb{N}$ mit $2 \nmid \ell$

$$2^{k\ell} + 1 = \left(2^k + 1\right) \cdot \left(2^{k(\ell-1)} - 2^{k(\ell-2)} + - \cdots + 1\right)$$

ist, kann dies nur der Fall sein, wenn m selbst Zweierpotenz ist. Zu Ehren ihres ersten Untersuchers Pierre de Fermat (1601–1665) nennt man die Zahlen

$$F_n := 2^{2^n} + 1 \qquad \text{mit } n \in \mathbb{N}_0$$

Fermat–Zahlen. Diese Zahlen sind paarweise teilerfremd. Es gilt

$$(F_n, F_m) = 1 \quad \forall\, n \in \mathbb{N}\ \forall\, m \in \mathbb{N} \text{ mit } n \neq m$$

(Die Teilerfremdheit folgt mit $F_{n+k} = F_n \cdot \left(d^{2^k-1} - d^{2^k-2} + \cdots - 1\right) + 2$ für alle $n \in \mathbb{N}$ und alle $k \in \mathbb{N}$ mit $d := 2^{2^n}$.)
Jede unendliche Folge paarweise teilerfremder Zahlen liefert unendlich viele Primteiler. □

Die Tatsache, dass $F_1, \ldots, F_4$ prim sind, führte FERMAT zu der Vermutung, dass dies für alle F_n zutrifft. EULER widerlegte diese Vermutung durch das Beispiel

$$F_5 = 641 \cdot 6\,700\,417.$$

Ebenso sind F_6, F_7 und F_8 Produkte aus zwei Primzahlen. Bis heute kennt man kein weiteres primes F_n. Die Frage, ob es unter den F_n weitere, oder gar unendlich viele Primzahlen gibt, dürfte für lange Zeit noch unangreifbar sein.

Ein einfaches Verfahren zur Aufstellung von Primzahllisten ist

ALGORITHMUS 1.16 (Sieb des ERATOSTHENES)
(ERATOSTHENES, 276?–194? vor Christus)
Sei $N \in \mathbb{N} \setminus \{1\}$.

1) Man schreibe die Zahlen $2, \ldots, N$ auf.

2$_1$) Man streiche die echten Vielfachen von 2.

2$_2$) Man gehe zur nächsten nicht gestrichenen Zahl und streiche hiervon alle echten Vielfachen, usw.

3) Man höre auf, wenn die nächste ungestrichene Zahl größer als $\sqrt{N}$ ist.

BEHAUPTUNG: *Die nicht gestrichenen Zahlen sind die Primzahlen kleiner oder gleich N.*

BEWEIS:
Es geht keine Primzahl verloren, denn es werden nur echte Vielfache von Zahlen größer oder gleich 2 gestrichen.

Jedes zusammengesetzte $n \in \mathbb{N}$ mit $n \leq N$ wird gestrichen, denn es hat einen Primteiler $p \in \mathbb{P}$ mit $p \leq \sqrt{N}$.
Dieses p wird nicht gestrichen, n als echtes Vielfaches von p fällt weg. □

Zur Kenntnis der multiplikativen Struktur von $\mathbb{Z}$ ist der folgende Satz grundlegend. Obwohl er intuitiv wesentlich früher benutzt wurde, ist er erst von GAUSS in exakter Form angegeben worden.

Satz 1.17 (Satz von der eindeutigen Primfaktorzerlegung)
Behauptung: *Jedes $n > 1$ besitzt genau eine Darstellung („kanonische Zerlegung“)*

$$n = p_1^{k_1} \cdot \ldots \cdot p_\ell^{k_\ell}$$

mit $\ell \in \mathbb{N}$, $p_j \in \mathbb{P}$, $k_j \in \mathbb{N}$ für alle $j \in \mathbb{N}$ mit $j \leq k$ und $p_j < p_{j+1}$ für alle $j \in \mathbb{N}$ mit $j < k$.

Anders formuliert gibt es also genau eine Funktion $\alpha : \left\{ \begin{array}{ccc} \mathbb{P} \times \mathbb{N} & \to & \mathbb{N}_0 \\ (p,n)^T & \mapsto & \alpha_{p,n} \end{array} \right\}$ mit $n = \prod_{p \in \mathbb{P}} p^{\alpha_{p,n}}$ für alle $n \in \mathbb{N}$. ($(p,n)^T$ ist der Vektor aus $\mathbb{P} \times \mathbb{N}$ mit Einträgen p und n.)
Dabei ist das Produkt über alle Primzahlen erstreckt und $a_{p,n} \neq 0$ gilt für ein festes $n \in \mathbb{N}$ nur für endliche viele $p \in \mathbb{P}$. Es ist $\alpha_{p,1} = 0$ für alle $p \in \mathbb{P}$.

Beweis:

(i) Existenz
Der Beweis verläuft induktiv.
Falls $n \in \mathbb{N}$ nicht prim ist, zerfällt es in zwei Faktoren $n_1 \in \mathbb{N} \setminus \{1\}$ und $n_2 \in \mathbb{N} \setminus \{1\}$ mit $n = n_1 n_2$.
Wegen $\min\{n_1; n_2\} > 1$ und $n = n_1 n_2$ ist $\max\{n_1; n_2\} < n$.
Nach Induktionsvoraussetzung sind n_1 und n_2 Produkte von Potenzen von Primzahlen.
Also ist auch $n = n_1 n_2$ ein Produkt aus Potenzen von Primzahlen.

(ii) Eindeutigkeit
Es gebe Zahlen mit zwei Darstellungen. $n \in \mathbb{N} \setminus \{1\}$ sei unter diesen die Kleinste.
Seien $k \in \mathbb{N}$, $\ell \in \mathbb{N}$, $p_j \in \mathbb{P}$, $\alpha_j \in \mathbb{P}$ für alle $j \in \mathbb{N}$ mit $j \leq k$, $q_h \in \mathbb{P}$, $\beta_h \in \mathbb{P}$ für alle $h \in \mathbb{N}$ mit $h \leq \ell$ derart, dass $p_j < p_{j+1}$ für alle $j \in \mathbb{N}$ mit $j < k$ und $q_h < q_{h+1}$ für alle $h \in \mathbb{N}$ mit $h < \ell$ und

$$n = \prod_{j=1}^{k} p_j^{\alpha_j} = \prod_{h=1}^{\ell} q_h^{\beta_h} \qquad (\blacklozenge)$$

gilt.
Es ist $p_1 \neq q_h$ für alle $h \in \mathbb{N}$ mit $h \leq \ell$, da sonst durch p_1 dividiert werden könnte, und man ein kleineres $\tilde{n}$ mit zwei Darstellungen erhielte.
Also ist $(p_1, q_h) = 1$ (denn $(p_1, q_h) > 1$ bedingte $p_1 = q_h$) für alle $h \in \mathbb{N}$ mit $h \leq \ell$.
Aus ($\blacklozenge$) sieht man

$$p_1 \left| \left(q_1 \cdot q_1^{\beta_1 - 1} \cdot \prod_{h=2}^{\ell} q_h^{\beta_h} \right) \right. .$$

Sei $\tilde{n} := q_1^{\beta_1 - 1} \cdot \prod_{h=2}^{\ell} q_h^{\beta_h}$.
Lemma 1.9 (2) auf Seite 9 und $(p_1, q_1) = 1$ bewirken $p_1 | \tilde{n}$.
Die Fortsetzung dieses Verfahrens führt schließlich zu $p_1 | q_\ell$, was wegen $(p_1, q_\ell) = 1$ ausgeschlossen ist. □

Hinweis
Wird im Folgenden „$n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$“ oder „$n = \prod_{p \in \mathbb{P}} p^{a_p}$“ geschrieben, so ist stets die eindeutige Primfaktorzerlegung im Sinne von Satz 1.17 gemeint. Die Eigenschaften der Parameter k, p_j und a_j werden nicht mehr genauer definiert.

Für das Weitere ist eine einfache Feststellung wichtig.

Bemerkung 1.18
Für $n \in \mathbb{N}$ und $d \in \mathbb{N}$ mit

$$n = \prod_{p \in \mathbb{P}} p^{a_p}, \quad \text{und} \quad d = \prod_{p \in \mathbb{P}} p^{b_p}$$

gilt

$$d|n \qquad \Longleftrightarrow \qquad \forall\, p \text{ ist } b_p \leq a_p.$$

Beweis:
Die Richtung „$\Longleftarrow$“ ist klar.
Es gelte also $d|n$ und $b_p > a_p$ für (mindestens) ein $p \in \mathbb{P}$.
Seien $m := \dfrac{n}{d}$ und $c := \dfrac{d}{p^{b_p}}$. Es sind $m \in \mathbb{N}$ und $c \in \mathbb{N}$.
Damit folgt $n = md = mcp^{b_p}$ und somit $np^{-a_p} = cp^{b_p - a_p}m$.
Links steht ein $\tilde{n} \in \mathbb{N}$, in dessen Primfaktorzerlegung p nicht vorkommt, während es rechts mit einem Exponenten von mindestens $b_p - a_p > 0$ auftritt.
Dies widerspricht dem Satz von der eindeutigen Primfaktorzerlegung 1.17 auf der vorherigen Seite. □

Es gilt

$$\# \left\{ d \in \mathbb{N};\, d | \prod_{j=1}^{k} p_j^{a_j} \right\} = \prod_{j=1}^{k} (a_j + 1).$$

Mit Bemerkung 1.18 sieht man unmittelbar

Satz 1.19 (Primfaktorzerlegung von ggT und kgV)
Voraussetzungen:
Seien $k \in \mathbb{N}$ und $n_j = \prod_{p \in \mathbb{P}} p^{a_{p,j}} \in \mathbb{N}$ für alle $j \in \mathbb{N}$ mit $j \leq k$. Seien

$$A_p := \min_{j=1}^{k} (a_{p,j}) \quad \textit{und} \quad B_p := \max_{j=1}^{k} (a_{p,j}).$$

BEHAUPTUNG: *Dann gilt*

$$(n_1, \ldots, n_k) = \prod_{p \in \mathbb{P}} p^{A_p} \quad \textit{und} \quad [n_1, \ldots, n_k] = \prod_{p \in \mathbb{P}} p^{B_p}.$$

BEWEIS:

(i) $(n_1, \ldots, n_k)$

Bemerkung 1.18 auf der vorherigen Seite liefert, dass $\prod_{p \in \mathbb{P}} p^{A_p}$ für alle $j \in \mathbb{N}$ mit $j \leq k$ ein Teiler von n_j ist.
Ist $c = \prod_{p \in \mathbb{P}} p^{\alpha_{p,c}}$ nun ein gemeinsamer Teiler der n_j mit $j \in \mathbb{N}$ und $j \leq k$, so ist $\alpha_{p,c} \leq a_{p,j}$ für alle $j \in \mathbb{N}$ mit $j \leq k$ und alle $p \in \mathbb{P}$. Damit folgt für alle $p \in \mathbb{P}$

$$\alpha_{p,c} \leq A_p = \min_{j=1}^{k} (a_{p,j}).$$

Bemerkung 1.18 auf der vorherigen Seite zeigt $c | \prod_{p \in \mathbb{P}} p^{A_p}$ und mit Folgerung 1.7 (1) auf Seite 6 folgt

$$(n_1, \ldots, n_k) = \prod_{p \in \mathbb{P}} p^{A_p}.$$

(ii) $[n_1, \ldots, n_k]$

Bemerkung 1.18 auf der vorherigen Seite liefert, dass $\prod_{p \in \mathbb{P}} p^{B_p}$ für alle $j \in \mathbb{N}$ mit $j \leq k$ ein Vielfaches von n_j ist.
Ist $m = \prod_{p \in \mathbb{P}} p^{\alpha_{p,m}}$ nun ein gemeinsames Vielfaches der n_j mit $j \in \mathbb{N}$ und $j \leq k$, so ist $\alpha_{p,m} \geq a_{p,j}$ für alle $j \in \mathbb{N}$ mit $j \leq k$ und alle $p \in \mathbb{P}$. Damit folgt für alle $p \in \mathbb{P}$

$$\alpha_{p,m} \geq B_p = \max_{j=1}^{k} (a_{p,j}).$$

Dies zeigt $\prod_{p \in \mathbb{P}} p^{B_p} | m$ und es folgt

$$[n_1, \ldots, n_k] = \prod_{p \in \mathbb{P}} p^{B_p}.$$ □

Der Satz von der eindeutigen Primfaktorzerlegung besagt, dass jedes nicht–Null–Element des Ringes $\mathbb{Z}$ eindeutig als Produkt von unzerlegbaren Elementen $p \in \mathbb{P}$ und einer Einheit $e \in \{-1, 1\}$ geschrieben werden kann. Die nächsteinfachen Bereiche sind die Ringe

$$\mathbb{Z}\left[\sqrt{a}\right] := \left\{ b_1 + b_2\sqrt{a} \,;\, b_1 \in \mathbb{Z} \text{ und } b_2 \in \mathbb{Z} \right\}$$

für $a \in \mathbb{Z} \setminus \{ k^2 \in \mathbb{Z} \,;\, k \in \mathbb{Z} \}$. Hier können in naheliegender Weise Einheiten und Primelelemente definiert werden. Wie das Beispiel

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right) \quad \text{in} \quad \mathbb{Z}\left[\sqrt{-5}\right]$$

zeigt, kann die Eigenschaft der eindeutigen Zerlegbarkeit in Primfaktoren verloren gehen. Diese Probleme bilden den Ausgangspunkt zur algebraischen Zahlentheorie.

Kapitel 2: Kongruenzen und Restsysteme

Bei Division durch eine feste Zahl $m \in \mathbb{N}$ bilden die kleinsten nichtnegativen Reste eine m–periodische Folge. Für zahlreiche Fragen reicht es aus, das Verhalten innerhalb einer Periode zu studieren.

Definition 2.1 (kongruent modulo m)
Für $m \in \mathbb{N}$ heißen $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ **kongruent modulo m**, wenn $m \mid (b-a)$.
(D.h., wenn $b = a + gm$ für ein $g \in \mathbb{Z}$ ist.)
Kurz: $a \equiv b \bmod m$ oder $a \equiv b\,(m)$.
m heißt **Modul der Kongruenz**.

Folgerung 2.2
Seien $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, $a_1 \in \mathbb{Z}$, $b_1 \in \mathbb{Z}$, $a_2 \in \mathbb{Z}$ und $b_2 \in \mathbb{Z}$.
Seien $k \in \mathbb{N}$, $m \in \mathbb{N}$, $m_j \in \mathbb{N}$ für alle $j \in \mathbb{N}$ mit $j \le k$, $n \in \mathbb{Z}$ und $f \in \mathbb{Z}[x]$.
Dann gilt

(1) $a \equiv b\,(m) \iff$ a und b lassen bei Division durch m denselben kleinsten nichtnegativen Rest.

(2) $a \equiv b\,(m)$ und $b \equiv c\,(m) \implies a \equiv c\,(m)$.

(3) $a_1 \equiv b_1\,(m)$ und $a_2 \equiv b_2\,(m) \implies (a_1 + a_2) \equiv (b_1 + b_2)\,(m)$ und $a_1 a_2 \equiv b_1 b_2\,(m)$.

(4) $a \equiv b\,(m) \implies f(a) \equiv f(b)\,(m)$.

(5) $na \equiv nb\,(m) \implies a \equiv b\left(\frac{m}{(n,m)}\right)$. Insbesondere $a \equiv b\,(m)$, falls $(n,m) = 1$.

(6) $a \equiv b\,(m_j)$ für alle $j \in \mathbb{N}$ mit $j \le k \iff a \equiv b\,([m_1, \ldots, m_k])$.

(7) $a \equiv b\,(m) \implies (a,m) = (b,m)$.

Beweis:
Die Eigenschaften (1), (2) und (3) sind unmittelbar einzusehen.
(4) entsteht durch mehrfache Anwendung von (3).

Mit der Definition sieht man $\dfrac{m}{(n,m)} \Big| \dfrac{n}{(n,m)} \cdot (b-a)$.

Wegen $\left(\dfrac{m}{(m,n)}, \dfrac{n}{(m,n)}\right) = 1$ und Lemma 1.9 (2) auf Seite 9 gilt $\dfrac{m}{(m,n)} \Big| (b-a)$
Das ist Behauptung (5).

(6) ist klar.
(7) ergibt sich aus

$$a \equiv b\,(m) \implies (d|m \wedge d|a \iff d|m \wedge d|b)\,. \qquad \square$$

Die Relation „$\equiv \mod m$“ ist für alle $m \in \mathbb{N}$ offenbar eine Äquivalenzrelation auf $\mathbb{Z}$, zerlegt $\mathbb{Z}$ also in m paarweise disjunkte Äquivalenzklassen.

Definition 2.3 (Restklassen)
Für alle $m \in \mathbb{N}$ heißen die Äquivalenzklassen der Relation „$\equiv \mod m$“ auf $\mathbb{Z}$ **Restklassen modulo m**.

Folgerungen 2.4

(1) Für alle $m \in \mathbb{N}$ haben die Restklassen modulo m die Gestalt

$$x + m\mathbb{Z} := \{(x + ma) \in \mathbb{Z} \,;\, a \in \mathbb{Z}\} \qquad \text{mit } x \in \mathbb{Z}.$$

(Ist der Modul $m \in \mathbb{N}$ klar, so schreiben wir auch kurz $\underline{x} := x + m\mathbb{Z}$.)

Für alle $m \in \mathbb{N}$, alle $x \in \mathbb{Z}$ und alle $y \in \mathbb{Z}$ ist

$$x + m\mathbb{Z} = y + m\mathbb{Z} \qquad \Longleftrightarrow \qquad x \equiv y \bmod m.$$

(2) Für alle $m \in \mathbb{N}$ wird durch

$$(x_1 + m\mathbb{Z}) + (x_2 + m\mathbb{Z}) := (x_1 + x_2) + m\mathbb{Z}$$
$$\text{(Kurz: } \underline{x_1} + \underline{x_2} = \underline{x_1 + x_2}\text{)}$$

auf $\mathbb{Z}_m$, der Menge der Restklassen modulo m, eine Verknüpfung definiert, die $\mathbb{Z}_m$ zu einer Gruppe macht.

(3) Für alle $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +)$ zyklisch.

Für alle $m \in \mathbb{N}$ und alle $a \in \mathbb{Z}$ ist $a + m\mathbb{Z}$ genau dann ein erzeugendes Element von $(\mathbb{Z}_m, +)$, wenn $(a, m) = 1$ ist.

Beweis:
(1) ist klar. Sei $m \in \mathbb{N}$.
Die Definition der Addition in (2) ist unabhängig von den Repräsentanten.
Denn sind $x_1 \in \mathbb{Z}$, $x_1' \in \mathbb{Z}$, $x_2 \in \mathbb{Z}$ und $x_2' \in \mathbb{Z}$ mit

$$x_j' \in x_j + m\mathbb{Z}, \quad \text{also} \quad x_j' \equiv x_j \bmod m \qquad \text{für alle } j \in \{1, 2\},$$

dann folgt $x_1' + x_2' \equiv (x_1 + x_2) \bmod m$, also

$$(x_1' + m\mathbb{Z}) + (x_2' + m\mathbb{Z}) = (x_1 + x_2) + m\mathbb{Z}.$$

Assoziativität und Kommutativität der Verknüpfung gelten wie in $\mathbb{Z}$.
$0 + m\mathbb{Z}$ ist das neutrale Element, zu $x + m\mathbb{Z}$ mit $x \in \mathbb{Z}$ ist $(m - x) + m\mathbb{Z}$ das Inverse.
$1 + m\mathbb{Z}$ ist Erzeugendes der Gruppe.
Die letzte Bemerkung in (3) wird im Anschluss an die nächste Definition bewiesen. □

Definition 2.5 (vollständiges Restsystem)

a) Für alle $m \in \mathbb{N}$ heißt $(\mathbb{Z}_m, +)$ mit $\mathbb{Z}_m$ und $+$ wie in Folgerung 2.4 (2) **additive Restklassengruppe modulo m**.

b) $\{x_1, \ldots, x_m\} \subseteq \mathbb{Z}$ heißt **vollständiges Restsystem modulo $m \in \mathbb{N}$** wenn

$$x_j \not\equiv x_k \bmod m \qquad \text{für alle } j \in \mathbb{N} \text{ und alle } k \in \mathbb{N} \text{ mit } j < k \leq m$$

ist, bzw. jede Restklasse modulo m genau ein x_j mit $j \in \mathbb{N}$ und $j \leq m$ enthält.

Folgerung 2.6
Seien $m \in \mathbb{N}$, $\{x_1, \ldots, x_m\} \subseteq \mathbb{Z}$ ein vollständiges Restsystem modulo m, $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$
Dann ist $\{x_1 + a, \ldots, x_m + a\}$ ein vollständiges Restsystem modulo m.
$\{x_1 b, \ldots, x_m b\}$ ist genau dann ein vollständiges Restsystem mod m, wenn $(b, m) = 1$ ist.

Beweis:
Mit $x \in \mathbb{Z}$ und $y \in \mathbb{Z}$ sind auch $x + a$ und $y + a$ modulo m inkongruent.
Dasselbe gilt nach Folgerung 2.2 (5) auf Seite 18 für xb und yb, falls $(b, m) = 1$ ist.
Sei nun $d := (m, b) > 1$ vorausgesetzt. Dann ist $1 \leq \frac{m}{d} < m$ und $\frac{m}{d} \not\equiv 0\,(m)$.
Gilt oBdA $x_1 \equiv 0\,(m)$ und $x_2 \equiv \frac{m}{d}(m)$, dann folgt

$$x_1 b \equiv 0\,(m) \quad \text{und} \quad x_2 b \equiv \left(\frac{m}{d} \cdot b\right) \bmod m \equiv \left(\frac{b}{d} \cdot m\right) \bmod m \equiv 0\,(m)\,.$$

Also bildet $\{x_1 b, \ldots, x_m b\}$ kein vollständiges Restsystem modulo m. □

Dies beinhaltet Folgerung 2.4 (3) auf Seite 19, denn $x + m\mathbb{Z}$ erzeugt $(\mathbb{Z}_m, +)$ genau dann, wenn $\{x \cdot 0, x \cdot 1, \ldots, x \cdot (m-1)\}$ ein vollständiges Restsystem modulo m ist.

$(\mathbb{Z}_m, \cdot)$ mit $(x + m\mathbb{Z}) \cdot (y + m\mathbb{Z}) := xy + m\mathbb{Z}$ für alle $x \in \mathbb{Z}$ und alle $y \in \mathbb{Z}$ ist für alle $m \in \mathbb{N}$ assoziativ und kommutativ, $1 + m\mathbb{Z}$ wirkt als neutrales Element, aber nicht für alle $x + m\mathbb{Z}$ existiert ein multiplikatives Inverses, z.B. im Fall $m \neq 1$ für $0 + m\mathbb{Z}$.

Satz 2.7 (multiplikative Inverse)
Behauptung: *Zu $a + m\mathbb{Z}$ mit $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ existiert genau dann ein multiplikatives Inverses, also ein $a^* \in \mathbb{Z}$ mit*

$$(a + m\mathbb{Z}) \cdot (a^* + m\mathbb{Z}) = 1 + m\mathbb{Z},$$

wenn $(a, m) = 1$ ist.

Die maximale Teilmenge der Restklassen modulo m, auf der die Multiplikation zur Gruppen–Eigenschaft führt, ist somit die Menge der sogenannten „reduzierten“ Restklassen (siehe Definition 2.8).

BEWEIS:
Seien $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $(a, m) = 1$.
Nach Satz 1.6 auf Seite 6 existieren ein $a^* \in \mathbb{Z}$ und ein $z \in \mathbb{Z}$ mit $aa^* + mz = 1$.
Dies bedeutet $aa^* \equiv 1\,(m)$ oder $(a + m\mathbb{Z}) \cdot (a^* + m\mathbb{Z}) = 1 + m\mathbb{Z}$.
Gibt es ein $b \in \mathbb{Z}$ und ein $b^* \in \mathbb{Z}$ mit $(b + m\mathbb{Z}) \cdot (b^* + m\mathbb{Z}) = 1 + m\mathbb{Z}$, so gilt $bb^* \equiv 1\,(m)$.
Also gibt es ein $g \in \mathbb{Z}$ mit $bb^* = 1 + gm$ und aus $(b, m)\,|b$ und $(b, m)\,|m$ ergibt sich $(b, m)\,|1$.
Dies zeigt $(b, m) = 1$. □

Definition 2.8

a) $a + m\mathbb{Z}$ mit $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ heißt **reduzierte** oder **prime Restklasse modulo m**, wenn $(a, m) = 1$ ist.

(Nach Folgerung 2.2 (7) auf Seite 18 besteht die gesamte Restklasse aus zu m teilerfremden Zahlen, wenn dies für nur ein Element zutrifft.)

b) (Die Anzahl der reduzierten Restklassen modulo $m \in \mathbb{N}$ heißt $\varphi\,(m)$.)
$\varphi : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & \varphi\,(n) := \#\,\{\,a \in \mathbb{N}\,;\, a \leq n \text{ und } (a, n) = 1\} \end{array} \right\}$ wird als **EULER'sche φ–Funktion** oder kurz **EULER–Funktion** bezeichnet. (Leonhard EULER, 1707–1783).

c) Die Menge der $\varphi\,(m)$ reduzierten Restklassen modulo $m \in \mathbb{N}$ wird mit $\mathbb{Z}_m^*$ abgekürzt.

Die (nach Satz 2.7 auf der vorherigen Seite) abelsche Gruppe $(\mathbb{Z}_m^*, \cdot\,)$ heißt **multiplikative Restklassengruppe modulo m**.

d) Jedes Vertretersystem $\left\{x_1, \ldots, x_{\varphi(m)}\right\} \subseteq \mathbb{Z}$ der $\varphi\,(m)$ reduzierten Restklassen modulo $m \in \mathbb{N}$ heißt **reduziertes** oder **primes Restsystem modulo m**.

(„prim“ besagt hier nicht, dass die x_j Primzahlen sein sollen).

Folgerung 2.9
Sind $\left\{x_1, \ldots, x_{\varphi(m)}\right\} \subseteq \mathbb{Z}$ ein reduziertes Restsystem modulo $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $(a, m) = 1$, so ist auch $\left\{ax_1, \ldots, ax_{\varphi(m)}\right\}$ eines.

Der BEWEIS verläuft wie der zu Folgerung 2.6.

Für $m \in \mathbb{N} \setminus \{1\}$ sind die $m \in \mathbb{P}$ offenbar die einzigen Moduln, zu denen alle $a + m\mathbb{Z}$ mit $a \in \mathbb{Z} \setminus (0 + m\mathbb{Z})$ ein multiplikatives Inverses besitzen.

$$\mathbb{Z}_p\,(+, \cdot\,, 0 + p\mathbb{Z}, 1 + p\mathbb{Z}) \qquad \text{ist genau für alle } p \in \mathbb{P} \text{ ein Körper.}$$

Für kein anderes $m \in \mathbb{N} \setminus (\{1\} \cup \mathbb{P})$ hat $\mathbb{Z}_m\,(+, \cdot\,, 0 + m\mathbb{Z}, 1 + m\mathbb{Z})$ diese Eigenschaft. In der Algebra wird gezeigt, daß es exakt zu den $m \in \left\{p^k \in \mathbb{N}\,;\, p \in \mathbb{P} \text{ und } k \in \mathbb{N}\right\}$ einen Körper mit m Elementen gibt. Dieser ist bis auf Isomorphie eindeutig bestimmt und wird als $GF\left(p^k\right)$ (GALOIS–Feld; Evariste GALOIS, 1811–1832) bezeichnet. Für $k \in \mathbb{N} \setminus \{1\}$ und $p \in \mathbb{P}$ ist die Konstruktion der $GF\left(p^k\right)$ ein wenig verwickelter als für $k = 1$ und $p \in \mathbb{P}$.

Satz 2.10 (Werte von φ)
Voraussetzungen:
Seien $m \in \mathbb{N}$, $n \in \mathbb{N}$ mit $(n,m) = 1$, $\{x_1, \ldots, x_{\varphi(m)}\} \subseteq \mathbb{Z}$ ein reduziertes Restsystem modulo m und $\{y_1, \ldots, y_{\varphi(n)}\} \subseteq \mathbb{Z}$ ein reduziertes Restsystem modulo n.
Seien $p \in \mathbb{P}$, $k \in \mathbb{N}$, $\ell \in \mathbb{N}$, $p_j \in \mathbb{P}$ und $a_j \in \mathbb{N}$ für alle $j \in \mathbb{N}$ mit $j \leq \ell$ derart, dass $p_j < p_{j+1}$ für alle $j \in \mathbb{N}$ mit $j < \ell$ gilt.

Behauptung: **(1)** $\{(x_j n + y_h m) \in \mathbb{Z} \,;\, j \in \mathbb{N}$ *mit* $j \leq \varphi(m)$ *und* $h \in \mathbb{N}$ *mit* $h \leq \varphi(n)\}$ *ist ein reduziertes Restsystem modulo mn.*

(2) *Es gilt* $\varphi(mn) = \varphi(m) \cdot \varphi(n)$
(d.h. die zahlentheoretische Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ ist „multiplikativ“).

(3) *Es sind* $\varphi\left(p^k\right) = (p-1) \cdot p^{k-1}$ *und* $\varphi\left(\prod_{j=1}^{\ell} p_j^{a_j}\right) = \prod_{j=1}^{\ell} (p_j - 1) \cdot p_j^{a_j - 1}$.

Beweis:

(i) Zu (1) und (2)
Die $\varphi(m) \cdot \varphi(n)$ Zahlen aus der angegebenen Menge sind zu mn teilerfremd:
Seien $j \in \mathbb{N}$ mit $j \leq \varphi(n)$ und $h \in \mathbb{N}$ mit $h \leq \varphi(n)$.
Hat mn mit $z_{jh} := x_j n + y_h m$ einen Primteiler $p \in \mathbb{P}$ gemeinsam, dann gilt oBdA $p|n$, also $p|(y_h m) = z_{jh} - x_j n$.
Wegen $(y_h, n) = 1$ und Lemma 1.9 (2) auf Seite 9 folgt $p|m$, also $p|(m,n) = 1$, was nicht sein kann.

Die z_{jh} sind mod mn paarweise inkongruent:
Seien $j' \in \mathbb{N}$ und $h' \in \mathbb{N}$ mit $j' \leq \varphi(m)$, $h' \leq \varphi(n)$ und

$$x_j n + y_h m \equiv (x_{j'} n + y_{h'} m) \bmod mn.$$

Dann folgt

$$m \,|((x_j - x_{j'})\, n + (y_h - y_{h'})\, m)\,, \qquad \text{also} \qquad m \,|(x_j - x_{j'})\, n\,.$$

Mit $(m,n) = 1$ und Lemma 1.9 (2) ergibt sich $m|(x_j - x_{j'})$, bzw, $x_j \equiv x_{j'} \bmod m$.
Das heißt aber $j = j'$. Ebenso folgt $h = h'$.

Außerdem ist jedes $z \in \mathbb{Z}$ mit $(z, mn) = 1$ zu einem der z_{jh} modulo mn kongruent.
Denn nach Satz 1.6 auf Seite 6 existieren $x' \in \mathbb{Z}$ und $y' \in \mathbb{Z}$ mit $z = x'n + y'm$.
Hier muss $(x', m) = (y', n) = 1$ sein, da ansonsten $(z, mn) > 1$ wäre.
Es gibt also ein $\tilde{j} \in \mathbb{N}$ mit $\tilde{j} \leq \varphi(m)$ und ein $\tilde{h} \in \mathbb{N}$ mit $\tilde{h} \leq \varphi(n)$, so dass

$$x' \equiv x_{\tilde{j}}\,(m) \text{ und } y' \equiv y_{\tilde{h}}\,(n)\,, \quad \text{also} \quad z \equiv (x_{\tilde{j}} n + y_{\tilde{h}} m) \bmod mn$$

ist. Dies zeigt (1) und (2).

(ii) Zu (3)
Es ist

$$\begin{aligned}\varphi\left(p^k\right) &= \#\left\{a \in \mathbb{N}\,; a \leq p^k \text{ und } p \nmid a\right\} \\ &= \#\left\{a \in \mathbb{N}\,; a \leq p^k\right\} - \#\left\{a \in \mathbb{N}\,; a \leq p^k \text{ und } a \equiv 0\,(p)\right\} \\ &= p^k - p^{k-1}.\end{aligned}$$

Die letzte Formel entsteht durch mehrfaches Anwenden von (2) und dem Vorigen. □

Die nun folgende Kongruenz gehört zu den wichtigsten Aussagen der elementaren Zahlentheorie. Zum Anschluss an dieses Kapitel soll auf eine Anwendung in der Kryptografie (RSA–Verfahren) eingegangen werden.

Satz 2.11 (Eulersche Kongruenz)
Behauptung: *Für alle $a \in \mathbb{Z}$ und alle $m \in \mathbb{N}$ mit $(a, m) = 1$ gilt*

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

*Für alle $b \in \mathbb{Z}$ und alle $p \in \mathbb{P}$ gilt $b^p \equiv b \bmod p$ (**Fermat–Kongruenz**).*

Beweis:
Seien $m \in \mathbb{N}$, $\left\{x_1, \ldots, x_{\varphi(m)}\right\} \subseteq \mathbb{Z}$, $\left\{y_1, \ldots, y_{\varphi(m)}\right\} \subseteq \mathbb{Z}$ zwei reduzierte Restsysteme modulo m, $a \in \mathbb{Z}$ mit $(a, m) = 1$, $b \in \mathbb{Z}$ und $p \in \mathbb{P}$.
Dann folgt nach eventueller Umbenennung

$$x_j \equiv y_j\,(m) \qquad \text{für alle } j \in \mathbb{N} \text{ mit } j \leq \varphi\,(m)\,.$$

Mehrfache Anwendung von Folgerung 2.2 (3) auf Seite 18 ergibt

$$P := \prod_{j=1}^{\varphi(m)} x_j \equiv \prod_{j=1}^{\varphi(m)} y_j \bmod m. \qquad (\bigstar)$$

Außerdem ist $(P, m) = 1$, da $(x_j, m) = 1$ für alle $j \in \mathbb{N}$ mit $j \leq \varphi\,(m)$ ist.
Nach Folgerung 2.9 auf Seite 21 darf als $\left\{y_1, \ldots y_{\varphi(m)}\right\}$ das System $\left\{ax_1, \ldots, ax_{\varphi(m)}\right\}$ genommen werden. Dann wird aus $(\bigstar)$

$$P \equiv a^{\varphi(m)} \cdot P \bmod m.$$

Da $(P, m) = 1$, kann nach Folgerung 2.2 (5) P gekürzt werden.
Ist $(b, p) = 1$, so folgt $b^p \equiv b \bmod p$ aus $\varphi\,(p) = p - 1$ und dem Vorherigen.
Ist $(b, p) \neq 1$, so ist $b \equiv 0 \bmod p$ und deshalb auch $b^p \equiv 0 \bmod p$. □

Bemerkung
Die FERMAT–Kongruenz wird oft auch in der Form

$$b^{p-1} \equiv 1 \bmod p$$

für alle $b \in \mathbb{Z}$ und alle $p \in \mathbb{P}$ mit $p \nmid b$ angegeben.
Die EULERsche Kongruenz ist ein Spezialfall eines gruppentheoretischen Satzes:

BEHAUPTUNG: *Ist G eine Gruppe mit $n \in \mathbb{N}$ Elementen und dem neutralen Element $e \in G$, so gilt für jedes $g \in G$*

$$g^n = e.$$

Der Beweis beruht auf der gleichen Idee wie der eben ausgeführte Beweis.

Bemerkung (Die FERMAT–Kongruenz als „Glasperlenspiel“)
Es sollen Halsketten aus je $p \in \mathbb{P}$ Perlen gebastelt werden.
Dazu stehen Perlen in $a \in \mathbb{N} \setminus \{1\}$ verschiedenen Farben zur Verfügung ($p \nmid a$).

> Wieviele mögliche Halsketten gibt es, die aus Perlen
> mit verschiedenen Farben bestehen?

Es gibt a viele verschiedene einfarbige Ketten.
Insgesamt gibt es a^p viele Möglichkeiten, p Perlen hintereinander anzuordnen. Dies entpricht der Anzahl der möglichen Ketten, bevor die Enden verknotet werden.
Also gibt es $a^p - a$ viele verschiedene unverknotete bunte Ketten.
Durch Verknoten der Enden werden jeweils p solche Ketten miteinander identifiziert, weil man nun die Perlen auch über den Knoten schieben kann. Da die Ketten nicht einfarbig sind, sind dies tatsächlich p viele und nicht weniger. Hier geht entscheidend der Primzahlcharakter von p ein.
Also gibt es $\dfrac{a^p - a}{p}$ viele verschiedene Möglichkeiten, aus Perlen, die a verschiedene Farben haben, Halsketten, die aus p Perlen bestehen, zu basteln.
Insbesondere folgt

$$\frac{a^p - a}{p} \in \mathbb{Z} \qquad \text{bzw.} \qquad p \mid (a^p - a) \qquad \text{bzw.} \qquad a^p \equiv a \bmod p.$$

Während die Struktur der Gruppe $(\mathbb{Z}_m, +)$ auf der Hand liegt, ist $(\mathbb{Z}_m^*, \cdot\,)$ wesentlich mühsamer zu analysieren. Wie der nächste Satz — der erste in dieser Vorlesung mit einigem Tiefgang — zeigen wird, ist die Zyklizität der Gruppe eher die Ausnahme.

Definition 2.12 (Primitivwurzeln und Ordnung)

a) Für $m \in \mathbb{N}$ heißt ein $a \in \mathbb{Z}$ mit $(a, m) = 1$ **Primitivwurzel modulo m**, wenn $\{a^j \in \mathbb{N}\,;\, j \in \mathbb{N} \text{ mit } j \leq \varphi(m)\}$ ein reduziertes Restsystem modulo m bildet.

Mit anderen Worten: a ist erzeugendes Element der Gruppe $(\mathbb{Z}_m^*, \cdot\,)$.

b) Für alle $m \in \mathbb{N}$ und alle $a \in \mathbb{Z}$ mit $(a, m) = 1$ heißt

$$\operatorname{ord}_m(a) := \min\left\{ d \in \mathbb{N} \,;\, a^d \equiv 1 \bmod m \right\}$$

Ordnung von a modulo m.

Seien $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $(a, m) = 1$. Nach der EULER–Kongruenz 2.11 auf Seite 23 gibt es ein $d \in \{ j \in \mathbb{N} \,;\, j \leq \varphi(m) \}$ mit $a^d \equiv 1\,(m)$.

Das kleinste solche d ist die Ordnung von a modulo m.

Dies entspricht dem Begriff der Ordnung des Elements $a + m\mathbb{Z}$ in der Gruppe $(\mathbb{Z}_m^*, \cdot\,)$.

a ist demnach Primitivwurzel modulo m genau dann, wenn $\operatorname{ord}_m(a) = \varphi(m)$ ist.

Man beachte auch, dass $\operatorname{ord}_m(b)$ nur für $b \in \mathbb{Z}$ mit $(b, m) = 1$ definiert ist.

$(\mathbb{Z}_m^*, \cdot\,)$ ist genau dann zyklisch, wenn Primitivwurzeln modulo $m \in \mathbb{N}$ existieren.

SATZ 2.13 (Satz von EULER)
BEHAUPTUNG: *Zu $m \in \mathbb{N}$ existiert genau dann eine Primitivwurzel, wenn*

$$\begin{aligned} m \in \quad & \{1, 2, 4\} \\ & \cup \left\{ p^k \in \mathbb{N} \,;\, p \in \mathbb{P} \setminus \{2\}, k \in \mathbb{N} \right\} \\ & \cup \left\{ 2p^k \in \mathbb{N} \,;\, p \in \mathbb{P} \setminus \{2\}, k \in \mathbb{N} \right\} \quad \textit{ist.} \end{aligned}$$

Der Beweis des Satzes verwendet sowohl einige Überlegungen zum Ordnungs–Begriff, die auch außerhalb des Beweises interessant sind, als auch einen Satz von LAGRANGE. Diese werden zunächst aufgeführt, bevor der Satz von EULER dann bewiesen wird.

Lemma 2.14 (Zum Begriff der Ordnung)
VORAUSSETZUNGEN:

Seien $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $(a, m) = 1$

Seien $a_1 \in \mathbb{Z}$ mit $(a_1, m) = 1$, $a_2 \in \mathbb{Z}$ mit $(a_2, m) = 1$, $d_1 := \operatorname{ord}_m(a_1)$ und $d_2 := \operatorname{ord}_m(a_2)$.

BEHAUPTUNG: **(1)** *Für alle* $j \in \mathbb{N}_0$ *und alle* $k \in \mathbb{N}_0$ *mit* $j < k \leq \operatorname{ord}_m(a)$ *ist*

$$a^j \not\equiv a^k \bmod m.$$

(Die Zahlen $a^0, a^1, \ldots, a^{\operatorname{ord}_m(a)-1}$ *sind paarweise inkongruent modulo* m*.)*

(2) *Für alle* $\ell \in \mathbb{N}_0$ *und alle* $k \in \mathbb{N}_0$ *gilt*

$$a^\ell \equiv a^k \,(m) \qquad \Longleftrightarrow \qquad \ell \equiv k \,(\operatorname{ord}_m(a)).$$

Insbesondere gilt für alle $\ell \in \mathbb{N}_0$

$$a^\ell \equiv 1 \bmod m \qquad \Longleftrightarrow \qquad \operatorname{ord}_m(a) \,|\ell.$$

(3) $\operatorname{ord}_m(a) | \,\varphi(m)$

(4) *Sind* $n \in \mathbb{N}$ *und* $d \in \mathbb{N}$ *mit* $\operatorname{ord}_m(a) = nd$*, so gilt*

$$\operatorname{ord}_m(a^n) = d.$$

(5) *Ist* $(d_1, d_2) = 1$*, so gilt*

$$\operatorname{ord}_m(a_1 a_2) = d_1 d_2.$$

BEWEIS:

(i) Zu (1)
Für alle $j \in \mathbb{N}$ und alle $k \in \mathbb{N}$ mit $j < k \leq \operatorname{ord}_m(a)$ und $a^j \equiv a^k \bmod m$ folgt wegen $(a, m) = 1$ mit Folgerung 2.2 (5) auf Seite 18 $a^{k-j} \equiv 1 \bmod m$.
Dies ist (wegen $k - j < \operatorname{ord}_m(a)$) ein Widerspruch zur Minimalität von $\operatorname{ord}_m(a)$.

(ii) Zu (2)
Seien $k \in \mathbb{N}_0$ und $\ell \in \mathbb{N}_0$.
Nach Satz 1.4 auf Seite 4 gibt es ein $g_k \in \mathbb{Z}$, ein $r_k \in \mathbb{N}$, ein $g_\ell \in \mathbb{Z}$ und ein $r_\ell \in \mathbb{N}$ mit $r_k < \operatorname{ord}_m(a)$, $r_\ell < \operatorname{ord}_m(a)$,

$$k = g_k \cdot \operatorname{ord}_m(a) + r_k \qquad \text{und} \qquad \ell = g_\ell \cdot \operatorname{ord}_m(a) + r_\ell.$$

Mit Folgerung 2.2 (3) auf Seite 18 folgt

$$a^k = \left(a^{\operatorname{ord}_m(a)}\right)^{g_k} \cdot a^{r_k} \equiv 1^{g_k} \cdot a^{r_k} \,(m) \equiv a^{r_k} \,(m)$$

und

$$a^\ell = \left(a^{\operatorname{ord}_m(a)}\right)^{g_\ell} \cdot a^{r_\ell} \equiv 1^{g_\ell} \cdot a^{r_\ell} \,(m) \equiv a^{r_\ell} \,(m).$$

Ist nun $a^\ell \equiv a^k \bmod m$, so folgt $a^{r_\ell} \equiv a^{r_k} \bmod m$ und mit (1) ergibt sich $r_\ell = r_k$.
Aus $a^\ell \equiv a^k \bmod m$ folgt also $\ell \equiv k \bmod \operatorname{ord}_m(a)$.

Ist umgekehrt $\ell \equiv k \bmod \mathrm{ord}_m(a)$, so ist $r_\ell = r_k$ und es folgt

$$a^\ell \equiv a^{r_\ell} \bmod m \equiv a^{r_k} \bmod m \equiv a^k \bmod m.$$

(iii) Zu (3)
Nach der EULER'schen Kongruenz 2.11 auf Seite 23 ist $a^{\varphi(m)} \equiv 1\,(m) \equiv a^0\,(m)$.
Mit (2) folgt $\varphi(m) \equiv 0\,(\mathrm{ord}_m(a))$.

(iv) Zu (4)
Seien $n \in \mathbb{N}$ und $d \in \mathbb{N}$ mit $\mathrm{ord}_m(a) = nd$. Sei $d' := \mathrm{ord}_m(a^n)$. Dann gilt

$$a^{nd'} = (a^n)^{d'} \equiv 1 \bmod m \equiv a^0 \bmod m.$$

Mit (2) und $\mathrm{ord}_m(a) = nd$ folgt $nd' \equiv 0\,(nd)$, bzw. die Existenz eines $h \in \mathbb{Z}$ mit $nd' = ndh$.
Also ist $d' = hd$. Insbesondere ist $h > 0$, da $d' > 0$ und $d > 0$ sind.
Andererseits ist

$$(a^n)^d = a^{nd} = a^{\mathrm{ord}_m(a)} \equiv 1 \bmod m \equiv (a^n)^0 \bmod m$$

und mit (2) und $d' = \mathrm{ord}_m(a^n)$ folgt $d'|d$.
Also ist d ein Vielfaches von $d' = hd$, was nur für $h = 1$ möglich ist.
Das heißt aber $d = d' = \mathrm{ord}_m(a^n)$.

(v) Zu (5)
Sei $e := \mathrm{ord}_m(a_1a_2)$. Potenziert man die Kongruenz $(a_1a_2)^e \equiv 1\,(m)$ mit d_1, so ergibt sich

$$a_1^{ed_1} \cdot a_2^{ed_1} \equiv 1 \bmod m.$$

Wegen $a_1^{ed_1} = \left(a_1^{d_1}\right)^e \equiv 1^e\,(m)$ wird daraus $a_2^{ed_1} \equiv a_2^0 \bmod m$.
Nach (2) und Lemma 1.9 (2) auf Seite 9 folgt also mit $(d_1, d_2) = 1$

$$d_2|ed_1 \qquad \text{bzw.} \qquad d_2|e.$$

Analog ergibt sich $d_1|e$ und erneut wegen $(d_1, d_2) = 1$ folgt

$$d_1d_2|e.$$

Aus (2) und

$$(a_1a_2)^{d_1d_2} = \left(a_1^{d_1}\right)^{d_2} \cdot \left(a_2^{d_2}\right)^{d_1} \equiv 1^{d_2} \cdot 1^{d_1}\,(m) \equiv (a_1a_2)^0 \bmod m$$

folgt umgekehrt $e|d_1d_2$, woraus sich $e = d_1d_2$ ergibt. □

SATZ 3.5 (Satz von LAGRANGE)
VORAUSSETZUNGEN:
Seien $n \in \mathbb{N}$, $a_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}_0$ mit $j \le n$ und $p \in \mathbb{P}$ mit $(a_n, p) = 1$.

Sei $f : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & f(x) := \sum_{j=0}^{n} a_j x^j \end{array} \right\}$ *das Polynom mit Koeffizientenfolge $(a_j)_{j=0}^n \subseteq \mathbb{Z}$.*

Sei $\mathcal{R} \subseteq \mathbb{Z}$ ein vollständiges Restsystem modulo p.
BEHAUPTUNG: *Dann ist*

$$\#\left\{x \in \mathcal{R}\,;\, f(x) \equiv 0 \bmod p\right\} \leq n.$$

Es gibt also in jedem vollständigen Restsystem modulo $p \in \mathbb{P}$ (insbesondere in $\{0, \ldots, p-1\}$) höchstens $\deg(f)$ viele Lösungen der Kongruenz $f(x) \equiv 0 \bmod p$ ($f \in \mathbb{Z}[x]$).
Diese Aussage ist klar, wenn man bedenkt, dass „$\equiv \mod p$ in $\mathbb{Z}$“ dasselbe bedeutet wie „$=$ im Körper $\mathbb{Z}_p$“. Die Bedingung $p \nmid a_n$ besagt, dass f als Polynom über $\mathbb{Z}_p$ den Grad n hat. Nach einem allgemeinen Satz der Algebra — dessen Beweis im Folgenden im Prinzip gegeben wird — besitzt f über $\mathbb{Z}_p$ höchstens n Nullstellen, was der Behauptung entspricht.

BEWEIS:
Seien im Fall, dass es überhaupt Lösungen gibt, $x_1 \in \mathcal{R}$ mit $f(x_1) \equiv 0 \bmod p$. Polynomdivision ergibt

$$f(x) = (x - x_1) \cdot g(x) + b_1.$$

für alle $x \in \mathbb{Z}$ mit einem Polynom g vom Grad $n-1$, dessen Leitkoeffizient nicht von p geteilt wird. $x = x_1$ zeigt $b_1 \equiv 0 \bmod p$.
Für alle $x \in \mathcal{R} \setminus \{x_1\}$ mit $f(x) \equiv 0 \bmod p$ ist nun

$$(x - x_1) \cdot g(x) = f(x) \equiv 0 \bmod p.$$

Wegen $x - x_1 \not\equiv 0 \bmod p$ folgt also $g(x) \equiv 0 \bmod p$ für alle $x \in \mathcal{R} \setminus \{x_1\}$ mit $f(x) \equiv 0 \bmod p$.
Die Behauptung ergibt sich nun leicht induktiv.
Für $n = 0$ gibt es wegen $a_0 \not\equiv 0 \bmod p$ keine Lösung.
Für $n = 1$ werden $x \in \mathcal{R}$ mit

$$a_1 x + a_0 \equiv 0 \bmod p.$$

gesucht. Wegen $(a_1, p) = 1$ existiert ein a_1^* mit $a_1 a_1^* \equiv 1 \bmod p$, also werden $x \in \mathcal{R}$ mit

$$x + a_0 a_1^* \equiv 0 \bmod p,$$

gesucht.
Im Fall $n = 1$ gibt es modulo p also genau eine Lösung. □

Hinweis
Es darf hieraus nicht der Schluss gezogen werden, dass die Lösungsanzahl stets n ist.
Es kann z.B. sein, dass für $n \geq 2$ gar keine Lösungen existieren.

Nun kann auch Satz 2.13 bewiesen werden.

SATZ 2.13 (Satz von EULER)
BEHAUPTUNG: *Zu $m \in \mathbb{N}$ existiert genau dann eine Primitivwurzel, wenn*

$$\begin{aligned} m \in \quad & \{1, 2, 4\} \\ & \cup \left\{p^k \in \mathbb{N}\,;\, p \in \mathbb{P} \setminus \{2\}, k \in \mathbb{N}\right\} \\ & \cup \left\{2p^k \in \mathbb{N}\,;\, p \in \mathbb{P} \setminus \{2\}, k \in \mathbb{N}\right\} \quad \textit{ist.} \end{aligned}$$

BEWEIS:

(i) $m \in \mathbb{P} \setminus \{2\}$

1. Seien $p \in \mathbb{P} \setminus \{2\}$, $d_1, \ldots, d_k$ alle modulo p auftretenden Ordnungen und
$$d = [d_1, \ldots, d_k].$$
Es wird sich herausstellen, dass $d = \varphi(p) = p - 1$ ist und selbst als Ordnung angenommen wird, was der Behauptung entspricht.

2. Da alle d_j mit $j \in \mathbb{N}$ und $j \leq k$ nach Lemma 2.14 (3) auf Seite 25 $\varphi(p) = p - 1$ teilen, gilt
$$d | (p-1), \qquad \text{bzw.} \qquad d \leq p - 1.$$

3. Für jedes $a \in \mathbb{Z}_p^*$ ist $a^d \equiv 1 \bmod p$, da $\operatorname{ord}_p(a)$ die Zahl d teilt. Die Kongruenz
$$x^d - 1 \equiv 0 \bmod p$$
hat $p - 1$ Lösungen modulo p, nämlich alle $x \in \mathbb{Z}$ mit $p \nmid x$.
Nach dem Satz von LAGRANGE 3.5 auf Seite 45 muss $d \geq p - 1$ sein und mit 2. folgt
$$d = p - 1.$$
Wegen $p > 2$ ist damit auch $d > 1$.

4. Sei $d = q_1^{b_1} \cdot \ldots \cdot q_\ell^{b_\ell}$ die kanonische Zerlegung von d.
Sind $d_j = q_1^{b_{1,j}} \cdot \ldots \cdot q_\ell^{b_{\ell,j}}$ für alle $j \in \mathbb{N}$ mit $j \leq k$ die Primfaktorzerlegungen der modulo p auftretenden Ordnungen (einige der Exponenten können 0 sein), so gilt $b_h = \max\limits_{j=1}^{k} b_{h,j}$ nach Satz 1.19 auf Seite 16.
Also gibt es ein $c_1 \in \mathbb{Z}$ und ein $d_1' \in \mathbb{N}$ mit $(c_1, p) = 1$ und
$$\operatorname{ord}_p(c_1) = q_1^{b_1} \cdot d_1', \qquad \text{und} \qquad q_1 \nmid d_1'.$$
(Man nehme zum Beispiel ein $c_1 \in \mathbb{Z}$ mit $(c_1, p) = 1$ und $\operatorname{ord}_p(c_1) = d_\mu$, wobei $\mu \in \mathbb{N}$ mit $\mu \leq k$ so gewählt ist, dass $q_1^{b_1}$ ein Teiler von d_μ ist.)
Nach Lemma 2.14 (4) existiert $a_1 (= c_1^{d_1'})$ mit $\operatorname{ord}_p(a_1) = q_1^{b_1}$.
Analog erhält man $a_2, \ldots, a_\ell$.
Da die $q_j^{b_j}$ mit $j \in \mathbb{N}$ und $j \leq \ell$ paarweise teilerfremd sind, ergibt Lemma 2.14 (5)
$$\operatorname{ord}_p(a_1 \cdot \ldots \cdot a_\ell) = q_1^{b_1} \cdot \ldots \cdot q_\ell^{b_\ell} = d.$$
Mit 3. hat man $\operatorname{ord}_p(a_1 \cdot \ldots \cdot a_\ell) = p - 1$. Das ist die Behauptung.

(ii) Die Existenz von Primitivwurzeln modulo p^k bzw. $2p^k$ mit $k \in \mathbb{N}$

1. Es sei g eine Primitivwurzel modulo $p(>2)$. Es werden die Zahlen

$$c_\ell := (g + p\ell)^{p-1} \qquad \text{mit } \ell \in \mathbb{N}_0 \text{ und } \ell \leq p-1$$

betrachtet.

Es gibt ein $b_0 \in \mathbb{Z}$ mit $c_0 = g^{p-1} = 1 + pb_0$.

Für alle $\ell \in \mathbb{N}$ mit $\ell \leq p-1$ gibt es ein $y_\ell \in \mathbb{Z}$ mit

$$\begin{aligned} c_0 &= g^{p-1} \\ &= 1 + pb_0 \\ c_\ell &= (g + p\ell)^{p-1} \\ &= g^{p-1} + (p-1) \cdot g^{p-2} p\ell + p^2 y_\ell \\ &= 1 + p \cdot \big(b_0 - \ell g^{p-2} + p \cdot \big(y_\ell + g^{p-2}\ell\big)\big) \\ &= 1 + pb_\ell \end{aligned}$$

mit $b_\ell := b_0 - \ell g^{p-2} + p \cdot (y_\ell + g^{p-2}\ell)$ für alle $\ell \in \mathbb{N}$ mit $\ell \leq p-1$.

Wegen $(g, p) = 1$ durchlaufen mit ℓ auch die b_ℓ ein volles Restsystem modulo p. Insbesondere gibt es ein $\nu \in \{0, \ldots, p-1\}$ mit $p \nmid b_\nu$. Dieses ν werde im Folgenden benutzt.

2. Seien $k \in \mathbb{N}$ und $d := \operatorname{ord}_{p^k}(g + p\nu)$. Dann gilt $(g + p\nu)^d \equiv 1 \bmod p$, und deshalb ist $p-1$ ein Teiler von d, da mit g auch $g + p\nu$ Primitivwurzel modulo p ist.

3. Nach Lemma 2.14 (3) gilt $d \,\big|\, \varphi\big(p^k\big) = p^{k-1}(p-1)$, also gibt es mit 2. ein $n \in \mathbb{N}$ mit

$$d = p^{n-1}(p-1) \qquad \text{und} \qquad n \leq k.$$

4. Aus $(g + p\nu)^{p-1} = 1 + b_\nu p$ folgt schrittweise die Existenz von zu p teilerfremden $b_{\nu,j} \in \mathbb{Z}$ mit $j \in \mathbb{N}$, so dass

$$\begin{aligned} (g + p\nu)^{p^1(p-1)} &= 1 + p^2 \cdot b_{\nu,1}, \\ (g + p\nu)^{p^2(p-1)} &= 1 + p^3 \cdot b_{\nu,2}, \\ &\text{usw.} \end{aligned}$$

gelten, indem die vorangehende Gleichung mit p potenziert wird. Denn wegen $p > 2$ gilt für alle $j \in \mathbb{N}$

$$\big(1 + p^{j+1} \cdot b_{\nu,j}\big)^p = \sum_{h=1}^{p} \binom{p}{h} \cdot \big(p^{j+1} \cdot b_{\nu,j}\big)^h = 1 + p^{j+2} \cdot (b_{\nu,j} + p \cdot y_{\nu,j})$$

für ein $y_{\nu,j} \in \mathbb{Z}$. Mit $b_{\nu,0} := b_\nu$ setzt man für alle $j \in \mathbb{N}_0$ also $b_{\nu,j+1} := b_{\nu,j} + p \cdot y_{\nu,j}$, was für $(b_{\nu,j}, p) = 1$ auch wieder teilerfremd zu p ist.

Bemerkung
Man beachte, dass $p \neq 2$ bei „$y_{\nu,j} \in \mathbb{Z}$“ verwendet wird:

Für $p = 2$ ist $(1 + b_{\nu,j} \cdot 2)^2 = 1 + 2 \cdot 2b_{\nu,j} + (2b_{\nu,j})^2 = 1 + 2^2 \cdot \left(b_{\nu,j} + b_{\nu,j}^2\right)$ mit geradem $b_{\nu,j} + b_{\nu,j}^2$ für alle $j \in \mathbb{N}_0$ und alle $b_{\nu,j} \in \mathbb{Z}$.

Dieser problematische Fall tritt auf, wenn im letzten Summanden $\binom{p}{p} \cdot b_{\nu,j}^p \cdot p^{p\cdot(j+1)}$ der Exponent $p \cdot (j+1)$ mit $j+2$ übereinstimmt.

$$p \cdot (j+1) = j + 2 \qquad \Longleftrightarrow \qquad j \cdot (p-1) = 2 - p \qquad \Longleftrightarrow \qquad j = -\frac{p-2}{p-1}.$$

Dies ist nur für $j = 0$ und $p = 2$ möglich.

Aus der Kongruenz

$$(g + p\nu)^d = (g + p\nu)^{p^{n-1}(p-1)} \equiv 1 \bmod p^k$$

wird daher

$$1 + p^n \cdot b_{\nu,n-1} \equiv 1 \bmod p^k.$$

Wegen 3. ist also $n = k$ und $g + p\nu$ Primitivwurzel modulo p^k.

5. Ist h Primitivwurzel modulo p^k, so ist die ungerade unter den Zahlen h und $h + p^k$ Primitivwurzel modulo $2p^k$.

   Denn nach Satz 2.10 auf Seite 22 ist $\varphi\left(2p^k\right) = \varphi\left(p^k\right)$.

   Falls ein ungerades $x \in (1 + 2\mathbb{Z})$ die Kongruenz $x^j \equiv 1 \bmod p^k$ mit $j \in \mathbb{N}$ erfüllt, dann auch modulo $2p^k$, und umgekehrt. Für ungerade $x \in (1 + 2\mathbb{Z})$ ist also

$$\operatorname{ord}_{p^k}(x) = \operatorname{ord}_{2p^k}(x).$$

(iii) $m = 2^k$ besitzt Primitivwurzeln nur für $k = 1$ und $k = 2$
1 ist eine Primitivwurzel modulo 2, da $1 \equiv 1 \bmod 2$ ist.
3 ist eine Primitivwurzel modulo 4, da $3 \equiv 3 \bmod 4$ und $3^2 = 9 \equiv 1 \mod 4$ sind.
Es ist $\varphi\left(2^k\right) = 2^{k-1}$ nach Satz 2.10 auf Seite 22.
Ein ungerades $a \in (1 + 2\mathbb{Z})$ hat jedoch modulo 2^k höchstens die Ordnung 2^{k-2}, falls $k \geq 3$ ist.
Denn man sieht induktiv die Existenz von $a_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}$ mit

$$\begin{aligned} a^{2^1} &= 1 + 8 \cdot a_1, \\ a^{2^2} &= 1 + 16 \cdot a_2, \\ a^{2^{j-2}} &= 1 + 2^j \cdot a_{j-2} \equiv 1 \bmod 2^j. \end{aligned}$$

(Zu a_1: Es gibt ein $b \in \mathbb{Z}$ mit $a = 2b + 1$. Dann ist $a^2 = 4b^2 + 4b + 1 = 4 \cdot (b^2 + b) + 1$.
$z^2 + z$ ist aber für alle $z \in \mathbb{Z}$ gerade.)

Es sei bemerkt, dafür $k \geq 3$ die 2^{k-1} Zahlen

$$\pm 5^0, \pm 5^1, \ldots, \pm 5^{2^{k-2}-1}$$

ein reduziertes Restsystem mod 2^k bilden. Zum Beweis benutzt man

$$5^{2^{j-3}} \equiv 1 + 2^{j-1} \bmod 2^j \qquad \text{für alle } j \in \mathbb{N} \setminus \{1, 2\},$$

was $\operatorname{ord}_{2^k}(5) = 2^{k-2}$ zeigt.

(iv) Ausschließen der weiteren $m \in \mathbb{N}$
Seien $1 < m = q_1^{\alpha_1} \cdot \ldots \cdot q_\mu^{\alpha_\mu}$ in kanonischer Zerlegung gegeben und $c \in \mathbb{Z}$ mit $(c, m) = 1$. Für jedes $j \in \mathbb{N}$ mit $j \leq \mu$ gilt wegen der EULERschen Kongruenz 2.11 auf Seite 23

$$c^{\varphi\left(q_j^{\alpha_j}\right)} \equiv 1 \bmod q_j^{\alpha_j}.$$

Ist $f := \left[\varphi\left(q_1^{\alpha_1}\right), \ldots, \varphi\left(q_\mu^{\alpha_\mu}\right)\right]$, so folgt $c^f \equiv 1 \bmod q_j^{\alpha_j}$ für alle $j \in \mathbb{N}$ mit $j \leq \mu$, also ist

$$c^f \equiv 1 \bmod m.$$

Wegen $f | \varphi(m)$ existieren Primitivwurzeln modulo m also nur, wenn

$$\varphi\left(q_1^{\alpha_1}\right) \cdot \ldots \cdot \varphi\left(q_\mu^{\alpha_\mu}\right) = \varphi(m) = f = \left[\varphi\left(q_1^{\alpha_1}\right), \ldots, \varphi\left(q_\mu^{\alpha_\mu}\right)\right]$$

ist. Falls m mindestens zwei ungerade Primteiler besitzt, ist $f \leq \frac{\varphi(m)}{2}$. Im Fall $m = 2^{\alpha_1} \cdot q_2^{\alpha_2}$ mit $\alpha_1 \geq 2$ und $q_2 > 2$ gilt dies ebenfalls.
Also bleiben wegen (iii) nur die im Satz genannten m. □

Zusatzbemerkungen

1. Falls zu $m \in \mathbb{N}$ eine Primitivwurzel $g \in \mathbb{Z}$ existiert, bilden die Zahlen g^j mit $j \in \mathbb{N}$ und $j \leq \varphi(m)$ ein reduziertes Restsystem modulo m.

   Man überzeugt sich leicht, dass g^ℓ genau dann Primitivwurzel modulo m ist, wenn $(\varphi(m), \ell) = 1$ gilt. Somit gibt es zu den in Satz 2.13 genannten m genau $\varphi(\varphi(m))$ modulo m verschiedene Primitivwurzeln.

2. Die Struktur der abelschen Gruppe $\mathbb{Z}_m^*$ kann vollständig beschrieben werden.

   Ist $1 < m = q_1^{\alpha_1} \cdot \ldots \cdot q_\mu^{\alpha_\mu}$, dann zeigt Satz 2.10 auf Seite 22

   $$\mathbb{Z}_m^* = \mathbb{Z}_{q_1^{\alpha_1}}^* \times \ldots \times \mathbb{Z}_{q_\mu^{\alpha_\mu}}^*$$

   ($\times$ bedeutet das direkte Produkt). Für $q_j > 2$ ($j \in \mathbb{N}$, $j \leq \mu$) ist $\mathbb{Z}_{q_j^{\alpha_j}}^*$ isomorph zur zyklischen Gruppe $\left(\mathbb{Z}_{\varphi\left(q_j^{\alpha_j}\right)}, +\right)$. Für $q = 2$ und $k \geq 3$ ist nach der Bemerkung in (iii)

   $$\mathbb{Z}_{2^k}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$$

   (links mit der Multiplikation, rechts mit der Addition).

3. Die Konstruktion von Primitivwurzeln modulo $p \in \mathbb{P}$ erfolgt, wie in (i) 4. angegeben, sofern die Primfaktorzerlegung von $\varphi(p)$ vorliegt.

   Hat man eine Primitivwurzel modulo $p \in \mathbb{P}$ gefunden, kann man wie in (ii) beschrieben zu Primitivwurzeln modulo p^k und modulo $2p^k$ mit $k \in \mathbb{N}$ aufsteigen.

4. Eine bis heute unbewiesene Behauptung von ARTIN besagt, dass 2 für unendlich viele $p \in \mathbb{P}$ eine Primitivwurzel modulo p ist.

BEWEIS: (von 1. und 2.)

(i) Zu 1. „$\Longrightarrow$“
Seien $m \in \mathbb{N}$, $g \in \mathbb{N}$ eine Primitivwurzel modulo m und $\ell \in \mathbb{N}$.
Dann gilt

$$\left(g^{\ell}\right)^{\frac{\varphi(m)}{(\varphi(m),\ell)}} = \left(g^{\frac{\ell}{(\varphi(m),\ell)}}\right)^{\varphi(m)} \equiv 1 \bmod m$$

nach der EULER–Kongruenz 2.11 auf Seite 23.
Damit ist die Ordnung von g^{ℓ} höchstens $\frac{\varphi(m)}{(\varphi(m),\ell)}$.
Wenn g^{ℓ} eine Primitivwurzel modulo m ist, hat es Ordnung $\varphi(m)$, was nur mit $(\varphi(m), \ell) = 1$ möglich ist.

(ii) Zu 1. „$\Longleftarrow$“
Es gelte nun $(\varphi(m), \ell) = 1$. Dann gibt es ein $x \in \mathbb{Z}$ und ein $y \in \mathbb{Z}$ mit $1 = x\ell + y\varphi(m)$.
Mit der EULER–Kongruenz 2.11 auf Seite 23 folgt

$$g = g^1 = g^{x\ell + y\varphi(m)} = g^{x\ell} \cdot \left(g^{\varphi(m)}\right)^y \equiv g^{x\ell} \bmod m.$$

Ist $d := \operatorname{ord}_m\left(g^{\ell}\right)$, so gilt $g^{\ell d} = \left(g^d\right)^{\ell} \equiv 1 \bmod m$.
Erhebt man diese Kongruenz in die x–te Potenz, so zeigt sich mit $g \equiv g^{x\ell} \bmod m$

$$1 \equiv g^{x\ell d} \bmod m \equiv \left(g^{x\ell}\right)^d \bmod m \equiv g^d \bmod m.$$

Da g eine Primitivwurzel ist, folgt $\varphi(m) \mid d$ aus Lemma 2.14 (2) auf Seite 25. Mit Lemma 2.14 (3) ergibt sich $d \mid \varphi(m)$, was zu $d = \operatorname{ord}_m\left(p^{\ell}\right) = \varphi(m)$ führt.
Dies charakterisiert g^{ℓ} als Primitivwurzel modulo m.

(iii) Zu 2.
Seien $k \in \mathbb{N}$ und $n \in \mathbb{N}$ mit $(k, n) = 1$. Die Abbildung

$$\left\{ \begin{array}{rcl} \mathbb{Z}_{kn}^* & \to & \mathbb{Z}_k^* \times \mathbb{Z}_n^* \\ a + kn\mathbb{Z} & \mapsto & (a + k\mathbb{Z}, a + n\mathbb{Z})^T \end{array} \right\}$$

ist bijektiv.
Wegen Satz 2.10 (2) auf Seite 22 genügt es, die Injektivität zu zeigen, da beide Mengen endlich sind und gleich viele Elemente haben.
Ist $z \in \mathbb{Z}$ mit $z \equiv 1 \bmod k$ und $z \equiv 1 \bmod n$, so folgt aus $(k, n) = 1$ und Folgerung 2.2 (6) auf Seite 18 $z \equiv 1 \bmod mn$.
Damit ist die Abbildung injektiv und deshalb auch bijektiv.
Induktive Anwendung über die Anzahl der verschiedenen Primteiler des gegebenen Moduls liefert die Behauptung. □

Im folgenden Satz wird die Darstellbarkeit natürlicher Zahlen in Ziffernsystemen behandelt, im Anschluss daran die wohlbekannten Teilbarkeitsregeln im Zehnersystem.

Satz 2.15 (Ziffernsysteme)
Voraussetzung: *Sei* $g \in \mathbb{N} \setminus \{1\}$.

Behauptung: *Dann existieren zu jedem* $n \in \mathbb{N}$ *eindeutig ein* $k \in \mathbb{N}_0$ *(*$k+1$ *= Stellenzahl) und für alle* $j \in \mathbb{N}$ *mit* $j \le k$ *je ein* $a_j \in \mathbb{N}_0$ *mit* $a_j \le g-1$ *(Ziffern), so dass* $a_k \neq 0$ *und*

$$n = \sum_{j=0}^{k} a_j \cdot g^j \qquad \textit{sind.}$$

Beweis:

(i) Existenz
Zu jedem $n \in \mathbb{N}$ existiert genau ein $k \in \mathbb{N}_0$ mit

$$g^k \le n < g^{k+1}.$$

Der Existenzbeweis wird durch Induktion nach k geführt.
Für $k = 0$ ist nichts zu zeigen.
Seien $n \in \mathbb{N}$ und $k \in \mathbb{N}_0$ mit $g^{k+1} \le n < g^{k+2}$. Man setze

$$n' := n - \left\lfloor \frac{n}{g^{k+1}} \right\rfloor \cdot g^{k+1}.$$

Mit der Definition der Gauss–Klammer folgt $0 \le n' < g^{k+1}$, d.h. auf n' ist die Induktionsvoraussetzung anwendbar. Wegen $1 \le \frac{n}{g^{k+1}} < g$ ist $1 \le \left\lfloor \frac{n}{g^{k+1}} \right\rfloor < g$, d.h. $\left\lfloor \frac{n}{g^{k+1}} \right\rfloor$ ist als Ziffer $a_{k+1} \neq 0$ verwendbar.

(ii) Eindeutigkeit
Seien $m = \sum\limits_{j=0}^{k} a_j \cdot g^j$ und $m = \sum\limits_{j=0}^{r} b_j \cdot g^j$ zwei verschiedene Darstellungen von $m \in \mathbb{N}$.
Ist $k \neq r$, so seien $a_{k+1} := 0$ und $b_{r+1} := 0$
Sei $\ell := \max\{\, j \in \mathbb{N}_0 \,;\, j \le \max\{k, r\} \text{ und } a_j \neq b_j\}$ der größte Stelle, an der sich die Darstellungen unterscheiden. Dann folgt

$$(b_\ell - a_\ell) \cdot g^\ell = \sum_{j=0}^{\ell-1} (a_j - b_j) \cdot g^j.$$

Im Fall $\ell = 0$ ist dies offensichtlich widersprüchlich. Für $\ell \ge 1$ ist $\left|(b_\ell - a_\ell) \cdot g^\ell\right| \ge g^\ell$, während

$$\left| \sum_{j=0}^{\ell-1} (a_j - b_j) \cdot g^j \right| \le (g-1) \cdot \sum_{j=0}^{\ell-1} g^j = (g-1) \cdot \frac{g^\ell - 1}{g-1} < g^\ell$$

ist, was nicht zusammenpasst. □

Die wohlbekannten Teilbarkeitsregeln erweisen sich als Anwendung der Kongruenzrechnung.

Satz 2.16 (Teilbarkeitsregeln für 2, 3, 4, 5, 8, 9 und 11)
Voraussetzungen:

Seien $n \in \mathbb{N}_0$, $k \in \mathbb{N}_0$ *und* $a : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N}_0 \\ j & \mapsto & a_j \end{array} \right\}$ *mit* $a_j < 10$ *für alle* $j \in \mathbb{N}$ *derart, dass* $n = \sum_{j=0}^{k} a_j \cdot 10^j$ *ist*

Behauptung: *Dann gelten die folgenden Teilbarkeitsregeln.*

(1) $2|n \iff 2|a_0$,

(2) $4|n \iff 4|a_0 + 10\,a_1$,

(3) $8|n \iff 8|a_0 + 10\,a_1 + 100\,a_2$,

(4) $5|n \iff 5|a_0$,

(5) $3|n \iff 3 \left| \sum_{j=0}^{k} a_j \right.$,

(6) $9|n \iff 9 \left| \sum_{j=0}^{k} a_j \right.$,

(7) $11|n \iff 11 \left| \sum_{j=0}^{k} (-1)^j \cdot a_j \right.$.

Beweis: (von (7), der Rest geht analog)
Wegen $10 \equiv -1 \bmod 11$ ist $10^{2j} \equiv 1 \bmod 11$ und $10^{2j+1} \equiv -1 \bmod 11$ für alle $j \in \mathbb{N}$.
Also gilt

$$11|n \iff \sum_{j=0}^{k} a_j \cdot 10^j \equiv 0 \bmod 11 \iff \sum_{j=0}^{k} (-1)^j \cdot a_j \equiv 0 \bmod 11. \qquad \square$$

Etwas Algorithmische Zahlentheorie

Schnelles Potenzieren

Satz (Schnelles Potenzieren)
Behauptung: *Für alle $m \in \mathbb{N}$, alle $a \in \mathbb{Z}$ mit $(a,m) = 1$ und alle $d \in \mathbb{N}$ ist die Berechnung des Rests der (hohen) Potenz a^d modulo m mit sukzessiven Quadrieren („schnelles Potenzieren“ genannt) in wenigen Rechenschritten möglich; es genügen höchstens $2 \cdot \log_2(d)$ viele Multiplikationen.*

Hinweis:
Diese schnelle Berechnung von hohen Potenzen lässt sich auch in irgendwelchen Halbgruppen, also Mengen, auf der eine assoziative Verknüpfung definiert ist, durchführen, nicht nur in $\{a \in \mathbb{Z}\,;(a,m) = 1\}$ mit $m \in \mathbb{N}$.

Beweis:
1. Schritt: Mit höchstens $k := \lfloor \log_2(d) \rfloor$ vielen Multiplikationen (mit Reduktion modulo m) berechnet man sukzessive

$$a^2 \equiv a \cdot a\,(m)\,, \quad a^{2^2} \equiv a^2 \cdot a^2\,(m)\,, \quad a^{2^3} \equiv a^{2^2} \cdot a^{2^2}\,(m)\,, \quad \ldots, \quad a^{2^k} \equiv a^{2^{k-1}} \cdot a^{2^{k-1}}\,(m)\,.$$

2. Schritt: Nun lässt sich d binär (d. h. zur Basis $g = 2$) schreiben als

$$d = \sum_{j=0}^{k} b_j 2^j \qquad \text{mit } b_j \in \{0,1\}$$

für alle $j \in \mathbb{N}$ mit $j \le k$.
Wir können auch ohne Einschränkung annehmen, dass d bereits in der Binärdarstellung vorliegt.

3. Schritt: Dann ist

$$\begin{aligned} a^d = a^{\sum_{j=0}^{k} b_j 2^j} &= a^{b_0} \cdot a^{2b_1} \cdot a^{2^2 b_2} \cdot \ldots \cdot a^{2^k b_k} \\ &= a^{b_0} \cdot \left(a^2\right)^{b_1} \cdot \left(a^{2^2}\right)^{b_2} \cdot \ldots \cdot \left(a^{2^k}\right)^{b_k}, \end{aligned}$$

also ist der Rest von a^d modulo m mit nochmals höchstens k vielen Multiplikationen (mit Reduktion modulo m) berechenbar.
Somit erhalten wir einen Rechenaufwand von höchstens $2 \cdot \log_2(d)$ Multiplikationen. □

Beispiel Berechne 3^{18} modulo 10. Es ist $\lfloor \log_2(18) \rfloor = 4$.

Wir rechnen dann

$$3 \equiv 3\,(10)\,, \quad 3^{2^1} \equiv 9\,(10) \equiv -1\,(10)\,, \quad 3^{2^2} \equiv (-1)^2\,(10) \equiv 1\,(10)\,, \quad 3^{2^3} \equiv 3^{2^4}\,(10) \equiv 1\,(10)$$

und $18 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4$, also ist

$$3^{18} = 3^2 \cdot 3^{2^4} \equiv -1\,(10) \equiv 9\,(10)\,.$$

Damit schließen wir, dass 3^{18} die Endziffer 9 hat.

Der Rabin–Test, ein randomierter Primzahltest (1980)

Wir wollen testen, ob $N \in \mathbb{N} \setminus \{1,2\}$ (mit hoher Wahrscheinlichkeit) eine Primzahl ist.
Bisher hatten wir das Sieb des Eratosthenes als Primzahltest kennengelernt: Wir streichen dabei für alle $p \in \mathbb{P}$ mit $p \leq \sqrt{N}$ die $\frac{N}{p}$ Vielfachen von p, die kleiner oder gleich N sind.
Dies sind mindestens

$$\sum_{\substack{p \in \mathbb{P} \\ p \leq \sqrt{N}}} \frac{N}{p} \geq N \qquad (\text{für } N \geq 25)$$

viele Streichungen bzw. Rechenschritte. Das ist für große Zahlen N zu aufwendig! Man kann zwar mehrfache Streichungen vermeiden, aber selbst dann ist der Aufwand zu groß, wie man sich überlegen kann.
Wir stellen deshalb eine andere Methode vor, die so auch Anwendung in der Praxis findet.

Satz (Rabin)
Voraussetzungen:
Seien $N \in \mathbb{N} \setminus \{1,2\}$ ungerade, $t \in \mathbb{N}$ und $u \in \mathbb{N}$ ungerade mit $N - 1 = 2^t u$.
Behauptung: **(1)** *Gilt für jedes $a \in \mathbb{Z}$ mit $(a, N) = 1$*

$$a^u \equiv 1\,(N) \quad \text{oder} \quad \exists\ \ell \in \mathbb{N}_0 \text{ mit } \ell \leq t-1 \text{ und } a^{2^\ell u} \equiv -1\,(N)\,, \ (\star)$$

so ist $N \in \mathbb{P}$ eine Primzahl.

(2) *Ist $N \notin \mathbb{P}$ keine Primzahl, so gilt*

$$\#\,\{\,a \in \mathbb{N}\,;\, a \leq N, (a,N) = 1 \text{ und } (\star) \text{ gilt}\} \leq \frac{\varphi\,(N)}{4}.$$

(Ohne Beweis)

Definition (starke Pseudoprimzahlen)
Eine Zahl $N \in \mathbb{N} \setminus \{1,2\}$ heißt **starke Pseudoprimzahl zur Basis $a \in \mathbb{Z}$** mit $(a, N) = 1$, falls $(\star)$ für a gilt.

Folgerung
Ist $N \in \mathbb{N} \setminus \{1,2\}$ eine starke Pseudoprimzahl zu den $k \in \mathbb{N}$ mit $k \leq \varphi\,(N)$ paarweise modulo N verschiedenen Basen $a_j \in \mathbb{Z}$ mit $(a_j, N) = 1$, $j \in \mathbb{N}$ und $j \leq k$, so beträgt die Wahrscheinlichkeit, dass N *keine* Primzahl ist, höchstens $\left(\frac{1}{4}\right)^k$.

Somit können wir den Test der Bedingung (☆) für $a_1, \ldots, a_k$ als Algorithmus implementieren. Man nennt diesen Primzahltest dann auch „RABIN–Test“.

Laufzeit: Für jede Zahl a_j testet man (☆) mit höchstens $t+1 \leq \log_2(N)+1 \leq 2\cdot\log_2(N)$ vielen Kongruenzen, die alle wiederum höchstens $2\cdot\log_2(N)$ viele Multiplikationen brauchen (mit schnellem Potenzieren).
Der Aufwand ist damit insgesamt höchstens

$$4\cdot \underbrace{(\log_2(N))^2}_{\text{polynomial in } \log_2(N)} \cdot k.$$

Wir erhalten damit für $k \leq (\log_2 N)^A$ mit $A \in \mathbb{R}^+$, einen polynomiell schnellen Algorithmus.

Beispiel (RABIN) Seien $N := 2^{400} - 593$ und $k := 100$.
Dann ist N mit einer Wahrscheinlichkeit von weniger als $\left(\frac{1}{4}\right)^{100} < 10^{-60}$ *keine* Primzahl.
Später konnte man mit einem speziellen deterministischen Test $n \in \mathbb{P}$ zeigen.

Definition (Zeuge, kleinster Zeuge)
Für $N \in \mathbb{N}\setminus\{1,2\}$ heißt ein $a \in \mathbb{Z}$ mit $a < N$ und $(a,N)=1$, das (☆) nicht erfüllt, **Zeuge für N** (d. h. Zeuge für die Nicht–Primheit von N).
Sei W : $\left\{ \begin{array}{rcl} \mathbb{N}\setminus(\mathbb{P}\cup\{1\}) & \to & \mathbb{N} \\ N & \mapsto & W(N) := \min\{a \in \mathbb{N}\,;\, a \text{ ist Zeuge für } N\} \end{array} \right\}$.

SATZ (GRH und kleinste Zeugen)
BEHAUPTUNG: *Gilt die verallgemeinerte Riemannsche Vermutung (kurz GRH), so ist* $W(N) < 2\cdot\ln^2(N)$ *für alle zusammengesetzten Zahlen* $N \in \mathbb{N}\setminus(\mathbb{P}\cup\{1\})$.

(Ohne Beweis)

Folgerung
Man führe den RABIN–Test für $N \in \mathbb{N}\setminus\{1,2\}$ und alle natürlichen Zahlen $a \in \mathbb{N}$ mit $(a,N)=1$ und $a < 2\cdot\ln^2(N)$ als Basis aus, und wir nehmen an, dass dabei kein Zeuge für N gefunden wurde. Dies stellt einen polynomiell schnellen Algorithmus dar. Entscheidet dieser „Nein, N ist nicht prim“, so ist N nicht prim, und entscheidet dieser „Ja, N ist wahrscheinlich prim“, so ist N prim oder die GRH ist falsch.

Damit ist der RABIN–Test für die Praxis ausreichend!

Hinweis:
Im Jahr 2003 wurde ein deterministischer polynomieller Primzahltest von den indischen Mathematikern AGRAWAL, KAYAL, SAXENA („AKS“) entdeckt. Dieser ist für die Praxis allerdings (noch) nicht nutzbar. Man verwendet weiterhin randomisierte Tests wie etwa den RABIN–Test.

Erzeugung einer Primzahl mit vorgegebener Binärstellenanzahl

Zu gegebenen $n \in \mathbb{N}$ und $k \in \mathbb{N}$ wird ein $p \in \mathbb{N}$ mit $2^n \leq p < 2^{n+1}$ gesucht, das mit einer Wahrscheinlichkeit von mindestens $1 - \frac{1}{4^k}$ prim ist.

0) Setze $p_0 := 1$.

1) Wähle $p_1 \in \{0, 1\}$ beliebig.

$\vdots$

j) Wähle $p_j \in \{0, 1\}$ beliebig ($j \in \mathbb{N}$ mit $1 \leq j \leq n-1$).

$\vdots$

n) Setze $p_n := 1$.

n + 1) Teste mit dem RABIN–Primzahltest k mal, ob $\sum_{j=0}^{n} p_j \cdot 2^j$ wahrscheinlich prim ist.

Eine Wahrscheinlichkeitsanalyse zeigt, dass für $k \leq 3530$ und $n = 512$ Binärstellen (das ist ein typischer Wert für (kryptographische) Anwendungen) dieser Algorithmus nur wenige Minuten läuft.

Das RSA–Verfahren

Die Kryptographie beschäftigt sich mit der Verschlüsselung von Informationen oder geheimen Nachrichten und mit dem Schutz von Daten.
Die Kryptoanalyse dagegen beschreibt die Rückgewinnung von Informationen aus verschlüsselten Texten, der sogenannten Entschlüsselung.
Beide Gebiete werden in der Kryptologie zusammengefasst. Sie bedient sich einer gewissen Kodierung, also Vereinbarungen über eine Menge von Symbolen zum Informationsaustausch (Alphabete, ...).

Das RSA–Verfahren (R. L. RIVEST, A. SHAMIR, L. ADLEMAN, 1978) beruht darauf, dass die Zerlegung großer Zahlen in Primfaktoren (das „Faktorisieren“ großer Zahlen) rechnerisch kaum möglich ist.

Beschreibung des RSA–Verfahrens

A* → *B Alice (A) teilt Bob (B) mit, dass sie ihm eine geheime Nachricht schicken will.

B Bob wählt nun ein $p \in \mathbb{P}$ und ein $q \in \mathbb{P}$. Diese sollten sehr groß und etwa mit der gleichen Anzahl an Stellen gewählt sein.

Bob setzt $N := pq$, berechnet $\varphi(N) = (p-1) \cdot (q-1)$ und wählt einen „Schlüssel“ $s \in \mathbb{N}$ mit $(s, \varphi(N)) = 1$.

Zuguterletzt berechnet Bob noch ein $t \in \mathbb{N}$ mit $st \equiv 1 \bmod \varphi(n)$.

Die Daten p, q, $\varphi(N)$ und s hält Bob streng geheim.

$\boldsymbol{B \to A}$ Bob teilt Alice die Daten N und t mit.

$\boldsymbol{A}$ Alice verschlüsselt ihren Klartext $k \in \mathbb{N}$ mit $1 < k < \min\{p, q\}$ in $v(k) \in \mathbb{N}$, so dass $v(k) \equiv k^t \bmod N$ ist.

t fungiert hier als „Schließer“ des Klartextes.

$\boldsymbol{A \to B}$ Alice verrät Bob den verschlüsselten Text $v(k)$.

$\boldsymbol{B}$ Bob entschlüsselt $v(k)$ vermöge $(v(k))^s \equiv k \bmod N$.

s fungiert als „Öffner“.

Das funktioniert, da es ein $g \in \mathbb{Z}$ gibt, so dass

$$(v(k))^s \equiv k^{ts}(N) \equiv k^{1+g\cdot\varphi(N)}(N) \equiv k \bmod N \qquad \text{ist.}$$

Bemerkungen

1. Der große Vorteil des Verfahrens ist, dass nie geheime Daten, die zur Entschlüsselung dienen (p, q bzw. $\varphi(N)$, s) ausgetauscht werden.
2. Ein möglicher Angreifer, der nur $v(k)$, N und t kennt, kann daraus k nicht berechnen, wenn ihm die Faktorisierung von N nicht gelingt.
3. Alle Rechnungen sind schnell durchführbar:
   - Erzeugen großer Primzahlen mit RABIN–Test
   - Finden von s und t mit dem EUKLIDischen Algorithmus
   - Schnelles Potenzieren
4. Auch für $(k, N) > 1$, also in den seltenen Fällen $p|k$ oder $q|k$, arbeitet das Verfahren korrekt.

Beispiel
Seien $\mathcal{K} := \{n \in \mathbb{N}_0 \,;\, n \leq 26\}$ und $\mathcal{V} := \{n \in \mathbb{N}_0 \,;\, n \leq 28\}$.
Nun ordne man jedem Buchstaben außer A entsprechend der Stelle seines Vorgängers im Alphabet eine Zahl zu.
Die 0 ordne man dem A, die 26 dem Leerzeichen, die 27 dem Komma und die 28 dem Punkt zu. (In der Praxis nimmt man meist größere Alphabete.)
Die Verschlüsselung des Klartextes beginnt mit der Aufteilung des Textes in je drei Buchstaben bzw. Leerzeichen. (Gegebenenfalls wird am Ende des Textes mit ein oder zwei Leerzeichen aufgefüllt. Zum Beispiel wird „Klartext“ zu KLA RTE XT␣.
In jedem Dreierpäckchen ordne man einem Buchstaben seinen Korrespondenten aus $\mathcal{K}$ zu und trenne die Buchstaben dabei mit je einem Komma. Die Dreierpäckchen werden je mit einem Slash getrennt hintereinander geschrieben.

„Klartext“ $\rightsquigarrow$ KLA RTE XT␣ $\rightsquigarrow$ $10, 11, 0/17, 19, 4/23, 19, 26$

Zuletzt wird jedes Dreierpäckchen als Zahl im 27er–System interpretiert.

Sprich k_1, k_2, k_3 wird auf $k := 27^2 k_1 + 27 k_2 + k_3$ abgebildet.

„Klartext“ $\rightsquigarrow$ $10, 11, 0/17, 19, 4/23, 19, 26$ $\rightsquigarrow$ $7587/12910/17306$

Nun erfolgt die Verschlüsselung vermöge $v(k)$ mit $v(k) \equiv k^t \bmod N$.
Stellt man dann $v(k)$ im 29er–System dar, so erhält man pro verschlüsselter Zahl je ein $v_1 \in \mathcal{V}$, ein $v_2 \in \mathcal{V}$ und ein $v_3 \in \mathcal{V}$ mit $v(k) = 29^2 v_1 + 29 v_2 + v_3$.
Die erhaltene Reihe $v_{11}, v_{21}, v_{31}/v_{21}, v_{22}, v_{23}/\ldots$ wird wieder in Text übersetzt.
Ist N zwischen 27^3 und 29^3 gewählt, so werden Ver– und Entschlüsselung eindeutig.

Faktorisierung großer Zahlen

Die Faktorisierung großer Zahlen (etwa im Bereich von 512 oder mehr Binärstellen) ist in der Praxis nur sehr schwer möglich.
Die Firma „RSA Security“ führt seit 1991 Wettbewerbe durch, bei denen es darum geht, große Zahlen zu faktorisieren. Um den Rekord aus dem Jahre 2005 (RSA-640, eine Zahl mit 640 Binärstellen) zu faktorisieren, wäre ein Aufwand von 30 PC–Jahren notwendig. Durch Parallelisierung mehrerer PCs wurde die Faktorisierung innerhalb von 5 Monaten erreicht.

Bemerkungen

1. Die schnellsten bekannten Algorithmen zur Faktorisierung großer Zahlen sind subexponentiell.

   Genauer gibt es zu jedem $\varepsilon \in \mathbb{R}^+$ ein $C(\varepsilon) \in \mathbb{R}^+$, so dass die Berechnung der Faktorisierung einer Zahl $N \in \mathbb{N}$ mit einem Rechenaufwand von weniger als $C(\varepsilon) \cdot \exp \ln^{\frac{1}{2}+\varepsilon}(N)$ Schritten durchgeführt werden kann.

2. P. Shor zeigte 1999, dass am Quantencomputer die Faktorisierung großer Zahlen mit einer Laufzeit, die „nur sehr unwahrscheinlich länger als polynomiell“ ist, möglich ist.

   Aufgrund physikalischer Probleme ist die Entwicklung von Quantencomputern aber bisher technisch nicht bzw. kaum möglich.

Kapitel 3: Kongruenzen in einer Unbekannten

Definition 3.1
Für $f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & f(x) \end{array} \right\} \in \mathbb{Z}[x]$ (also ein Polynom mit ganzen Koeffizienten) und $m \in \mathbb{N}$ heißt die Anzahl

$$\rho(m) := \rho(m, f) := \#\{x \in \mathbb{N}_0 \,;\, x < m \text{ und } f(x) \equiv 0 \bmod m\}$$

der $x \in \mathbb{N}_0$ mit $x \leq m-1$ (bzw. der x aus irgendeinem vollständigen Restsystem modulo m) mit $f(x) \equiv 0\,(m)$ **Lösungszahl der Kongruenz $\boldsymbol{f(x) \equiv 0 \bmod m}$**.

Satz 3.2 (Lineare Kongruenzen)
Voraussetzungen:
Seien $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ und $m \in \mathbb{N}$.

Behauptung: *Die lineare Kongruenz*

$$ax + b \equiv 0\,(m)$$

ist genau dann lösbar, wenn (a, m) ein Teiler von b ist.
Im Falle $(a, m) \mid b$ gilt

$$\rho\,(m) = (a, m)\,.$$

Beweis:

(i) „$\Longrightarrow$“
Im Falle der Lösbarkeit existieren $x \in \mathbb{Z}$ und $g \in \mathbb{Z}$ mit $ax + b = gm$. Dann gilt $(a, m) \mid b$.

(ii) „$\Longleftarrow$“
Es sei $d := (a, m)$ und es werde $d|b$ vorausgesetzt. Gibt es ein $x \in \mathbb{Z}$ mit

$$ax + b \equiv 0 \bmod m,$$

so kann diese Kongruenz nach Definition der Kongruenzrechnung äquivalent zu

$$\frac{a}{d} \cdot x + \frac{b}{d} \equiv 0 \left(\frac{m}{d}\right) \qquad (\bigstar)$$

mit $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ umgeformt werden. Wie in Kapitel 2 sieht man mit dem Euklidischen Algorithmus 1.8 auf Seite 7 (oder mit Hilfe der Eulerschen Kongruenz 2.11 auf Seite 23), dass ein $a^* \in \mathbb{Z}$ mit $\frac{a}{d} \cdot a^* \equiv 1 \left(\frac{m}{d}\right)$ existiert. Dadurch wird $(\bigstar)$ äquivalent zu

$$x \equiv -\frac{b}{d} \cdot a^* \left(\frac{m}{d}\right), \qquad (\bigstar)$$

d.h. $(\bigstar)$ hat genau eine Lösung $x_0 := -\frac{b}{d} \cdot a^*$ modulo $\frac{m}{d}$. Die d Zahlen

$$x_0, \quad x_0 + \frac{m}{d}, \quad \ldots, \quad x_0 + (d-1) \cdot \frac{m}{d}$$

sind modulo m verschieden. Jedes x, das $(\bigstar)$ erfüllt, ist modulo m zu einer dieser Zahlen kongruent. Die einzige Lösung x_0 modulo $\frac{m}{d}$ induziert somit d Lösungen modulo m. □

Satz 3.3 (Chinesischer Restsatz (CRS))
Voraussetzungen:
Seien $k \in \mathbb{N}$ und $m_j \in \mathbb{N}$ für alle $j \in \mathbb{N}$ mit $j \leq k$ paarweise teilerfremd. Sei $m := \prod_{j=1}^{k} m_j$.

Behauptung: *Zu jedem k–Tupel $(x_1, \ldots, x_k)^T \in \mathbb{Z}^k$ gibt es modulo m genau ein $x_0 \in \mathbb{N}$, so dass für alle $x \in \mathbb{Z}$ gilt:*

$$x \equiv x_j \bmod m_j \qquad \forall\, j \in \mathbb{N} \text{ mit } j \leq k \qquad \Longleftrightarrow \qquad x \equiv x_0 \bmod m$$

Andere Formulierungen

Der Durchschnitt der Restklassen $\bigcap_{j=1}^{k} (x_j + m_j\mathbb{Z})$ ist gleich einer Restklasse $x_0 + m\mathbb{Z}$.

Es gibt einen Isomorphismus $C : \left\{ \begin{array}{rcl} \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k} & \to & \mathbb{Z}_m \\ \left(\underline{x_1}, \ldots, \underline{x_k}\right)^T & \mapsto & C\left(\underline{x_1}, \ldots, \underline{x_k}\right) := \underline{x_0} \end{array} \right\}$.

Bemerkungen

1. Die Namensgebung geht zurück auf chinesische Quellen um 1200. Das Prinzip des Satzes, Ersetzung eines Systems von Kongruenzen durch eine einzige, tritt unabhängig davon in zahlreichen früheren Schriften auf.
2. Die Bedingung der paarweisen Teilerfremdheit ist nötig. Man kann sich leicht überlegen, dass es andernfalls entweder keine oder mehr als eine Lösung modulo m gibt.

Beweis:

(i) Angabe eines x_0
Seien $x_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}$ mit $j \leq k$.
Das gesuchte $x_0 \in \mathbb{Z}$ kann explizit angegeben werden.
Seien $M_j := \dfrac{m}{m_j}$ für alle $j \in \mathbb{N}$ mit $j \leq k$.
Dann bewirkt die Voraussetzung $(M_j, m_j) = 1$ für alle $j \in \mathbb{N}$ mit $j \leq k$ und für alle $j \in \mathbb{N}$ mit $j \leq k$ existieren $M_j^* \in \mathbb{Z}$ mit

$$M_j \cdot M_j^* \equiv 1 \bmod m_j.$$

Es werde

$$x_0 := \sum_{j=1}^{k} M_j \cdot M_j^* \cdot x_j$$

gesetzt.

(ii) „$\Longleftarrow$“
Es sei $x \in \mathbb{Z}$ mit $x \equiv x_0\,(m)$.
Da für alle $j \in \mathbb{N}$ mit $j \leq k$ sowohl m als auch alle M_ℓ mit $\ell \in \mathbb{N}$, $\ell \leq k$ und $\ell \neq j$ von m_j geteilt werden, folgt

$$x \equiv \sum_{\ell=1}^{k} M_\ell \cdot M_\ell^* \cdot x_\ell\,(m_j) \equiv \left(M_j \cdot M_j^* \cdot x_j + 0\right)(m_j) \equiv 1 \cdot x_j\,(m_j) \equiv x_j\,(m_j)\,.$$

(iii) „$\Longrightarrow$“
Sei $y \in \mathbb{Z}$ mit

$$y \equiv x_j \bmod m_j \quad \text{für alle } j \in \mathbb{N} \text{ mit } j \leq k.$$

Nun gilt für alle $j \in \mathbb{N}$ mit $j \leq k$ und alle $\ell \in \mathbb{N}$ mit $\ell \leq k$ und $\ell \neq j$

$$M_j \cdot M_j^* \cdot x_j \equiv x_j \,(m_j) \qquad \text{und} \qquad M_\ell \cdot M_\ell^* \cdot x_\ell \equiv 0 \,(m_j)\,.$$

Damit folgt

$$y \equiv x_j \,(m_j) \equiv \sum_{\ell=1}^{k} M_\ell \cdot M_\ell^* \cdot x_\ell \,(m_j) \equiv x_0 \,(m_j) \qquad \text{für alle } j \in \mathbb{N} \text{ mit } j \leq k.$$

Wegen der paarweisen Teilerfremdheit ergibt sich daraus $y \equiv x_0 \,(m)$. □

Bemerkung
Die Beziehung zwischen Tupeln $(x_1, \ldots, x_k)^T$ und Lösungen x_0 ist eineindeutig.

- Zu x_0 existiert ein Tupel $(x_1, \ldots, x_k)^T$ mi $x_j \equiv x_0 \bmod m_j$ für alle $j \in \mathbb{N}$ mit $j \leq k$.
  Also ist die oben definierte Abbildung C surjektiv.
- Es ist klar, dass die Lösungen x_0 und x_0' zu Tupeln $(x_1, \ldots, x_k)^T$ und $(x_1', \ldots, x_k')^T$ modulo m genau dann verschieden sind, wenn die Tupel sich in mindestens einer Komponente modulo m_j ($j \in \mathbb{N}$ mit $j \leq k$) unterscheiden.
  Also ist C auch injektiv.

Satz 3.4 (ρ ist multiplikativ im Modul)
Behauptung: *Sind $m_1 \in \mathbb{N}$ und $m_2 \in \mathbb{N}$ mit $(m_1, m_2) = 1$, so folgt*

$$\rho\,(m_1 m_2) = \rho\,(m_1) \cdot \rho\,(m_2)$$

für alle $f \in \mathbb{Z}\,[x]$.
(D.h. die Lösungsanzahl $\rho\,(m, f)$ ist „multiplikativ“ im Modul).

Beweis:
Der Beweis ist eine einfache aussagenlogische Anwendung des chinesischen Restsatzes.
Seien $m_1 \in \mathbb{N}$, $m_2 \in \mathbb{N}$ mit $(m_1, m_2) = 1$, $f \in \mathbb{Z}\,[x]$, $k := \rho\,(m_1)$, $\ell := \rho\,(m_2)$, $x_1, \ldots, x_k$ Vertreter der Lösungsrestklassen modulo m_1 und $y_1, \ldots, y_\ell$ Vertreter der Lösungsrestklassen modulo m_2.
Wegen $(m_1, m_2) = 1$ ist

$$f\,(x) \equiv 0 \,(m_1 m_2) \qquad (\clubsuit)$$

für alle $x \in \mathbb{Z}$ äquivalent zu

$$f\,(x) \equiv 0 \,(m_1) \quad \wedge \quad f\,(x) \equiv 0 \,(m_2)\,.$$

Dies ist für alle $x \in \mathbb{Z}$ gleichbedeutend mit

$$\big(x \equiv x_1 \,(m_1) \vee \ldots \vee x \equiv x_1 \,(m_1)\big) \quad \wedge \quad \big(x \equiv y_1 \,(m_2) \vee \ldots \vee x \equiv y_1 \,(m_2)\big)$$

Dies wiederum lässt sich für alle $x \in \mathbb{Z}$ als Disjunktion von $k \cdot \ell$ Zweiersystemen schreiben:

$$\bigvee_{j=1}^{k} \bigvee_{h=1}^{\ell} \big(x \equiv x_j \,(m_1) \wedge x \equiv y_h \,(m_2)\big)$$

Jedes Zweiersystyem entspricht nach dem Chinesischen Restsatz 3.3 auf Seite 43 für alle $x \in \mathbb{Z}$ einer Kongruenz

$$x \equiv x_{j,h} \,(m_1 m_2)$$

mit $x_{j,h} \in \mathbb{Z}$ für alle $j \in \mathbb{N}$ mit $j \leq k$ und alle $h \in \mathbb{N}$ mit $h \leq \ell$.
Verschiedenen Paaren $(x_j, y_h)^T$ entsprechen modulo $m_1 m_2$ verschiedene $x_{j,h}$ ($j \in \mathbb{N}$ mit $j \leq k$ und $h \in \mathbb{N}$ mit $h \leq \ell$).
(✪) hat also $\rho\,(m_1) \cdot \rho\,(m_2)$ Lösungen. □

Der chinesische Restsatz 3.3 zeigt, wie aus den Lösungen modulo m_1 und modulo m_2 die Lösungen modulo $m_1 m_2$ konstruiert werden können.
Es reicht demnach für $f \in \mathbb{Z}\,[x]$ aus, Kongruenzen $f\,(x) \equiv 0 \,\big(p^k\big)$ mit $p \in \mathbb{P}$ und $k \in \mathbb{N}$ zu betrachten und durch mehrfache Anwendung von Satz 3.4 auf die Lösungen zu beliebigen $m \in \mathbb{N}$ aufzusteigen. Im Weiteren wird gezeigt, dass es im Prinzip ausreicht, Primzahlmoduln zu behandeln. Befriedigende Aussagen, was Lösbarkeit, Lösungsanzahl und die Gestalt der Lösungen angeht, sind nur im Fall linearer oder quadratischer Kongruenzen möglich.

Satz 3.5 (Satz von Lagrange)
Voraussetzungen:
Seien $f \in \mathbb{Z}\,[x]$ und $p \in \mathbb{P}$ derart, dass der Leitkoeffizient von f nicht von p geteilt wird.
Behauptung: *Dann ist*

$$\rho\,(p, f) \leq \deg\,(f)\,.$$

*(*deg *bezeichnet den Grad (englisch: degree) eines Polynoms.)*

Der Beweis wurde in Kapitel 2 gegeben.
Dass die Lösungsanzahl stark schwanken kann, zeigen folgende Beispiele.

Beispiel Für die Kongruenz

$$f\,(x) := x^3 + 2x - 7 \equiv 0 \bmod p$$

berechnet man

$$\rho\,(2) = 1, \quad \rho\,(3) = 0, \quad \rho\,(5) = 2, \quad \rho\,(7) = 1.$$

Die Kongruenz

$$g_p\,(x) := x^p - x \equiv 0 \bmod p$$

hat nach der Fermat–Kongruenz 2.11 auf Seite 23 genau p Lösungen.

Eine Anwendung, die allerdings für praktische Primzahltests ungeeignet ist, ist

Satz 3.6 (Satz von Wilson)
(M.B. Wilson, 1741–1793)
Behauptung: *Für alle* $n \in \mathbb{N} \setminus \{1\}$ *sind äquivalent*

(1) $n \in \mathbb{P}$ *ist Primzahl.*

(2) $(n-1)! \equiv -1 \bmod n$.

Beweis:

(i) (2) $\Longrightarrow$ (1)
Sei $n \in \mathbb{N}$ zusammengesetzt. Dann gibt es ein $q \in \mathbb{P}$ mit $q|n$ und $q < n$.
Also teilt q die Zahlen n und $(n-1)!$. Die Kongruenz (2) kann wegen $q \nmid -1$ nicht bestehen.

(ii) (1) $\Longrightarrow$ (2)
Es ist $(2-1)! = 1! = 1 \equiv -1 \bmod 2$.
Sei $p \in \mathbb{P} \setminus \{2\}$. Die Kongruenz

$$-\left(x^{p-1}-1\right) + \prod_{j=1}^{p-1}(x-j) = (x-1)\cdot(x-2)\cdot\ldots\cdot(x-(p-1)) - \left(x^{p-1}-1\right) \equiv 0 \bmod p$$

wird nach der Euler–Kongruenz 2.11 auf Seite 23 von den $p-1$ Zahlen $x = 1, \ldots, p-1$ gelöst.
Die linke Seite, als Polynom geschrieben, hat einen Grad von höchstens $p-2$. Ist einer der Koeffizienten $\not\equiv 0 \bmod p$, so ergibt sich ein Widerspruch zum Satz von Lagrange 3.5 auf der vorherigen Seite.
Insbesondere folgt durch Betrachtung des Absolutglieds

$$1 + \prod_{j=1}^{p-1}(-j) \equiv 0 \bmod p, \qquad \text{also} \qquad (p-1)! + 1 \equiv 0 \bmod p. \qquad \square$$

Im folgenden Satz wird beschrieben, wie man von den Lösungen der Kongruenz $f(x) \equiv 0 \bmod p$ mit $f \in \mathbb{Z}[x]$ und $p \in \mathbb{P}$ zu denen modulo p^k mit $k \in \mathbb{N} \setminus \{1\}$ aufsteigen kann.

Es ist klar, dass aus $f(x) \equiv 0 \left(p^k\right)$ die schwächere Bedingung $f(x) \equiv 0 \left(p^{k-1}\right)$ folgt. Eine Restklasse $x_0 + p^k\mathbb{Z}$ modulo p^k zerfällt in p Restklassen modulo p^{k+1}

$$\left(x_0 + bp^k\right) + p^{k+1}\mathbb{Z}$$

mit $b \in \mathbb{N}_0$ und $b < p$.

Ist also $x_0 + p^k\mathbb{Z}$ eine Lösungsrestklasse modulo p^k, so prüft man, welche der Restklassen $\left(x_0 + bp^k\right) + p^{k+1}\mathbb{Z}$ mit $b \in \mathbb{N}_0$ und $b < p$ Lösungen modulo p^{k+1} sind.
So kann man von allen Lösungen modulo p^k auf die modulo p^{k+1} schließen.

Satz 3.7 (Aufsteigesatz)
Voraussetzungen:
Seien $f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & f(x) \end{array} \right\} \in \mathbb{Z}[x]$, $k \in \mathbb{N}$, $x_0 \in \mathbb{Z}$ *mit* $f(x_0) \equiv 0 \bmod p^k$ *und*

$$g := g(x_0, k) := \#\left\{ b \in \mathbb{N}_0 \,;\, b < p \text{ und } f\left(x_0 + bp^k\right) \equiv 0 \bmod p^{k+1} \right\}$$

die Anzahl der Lösungen modulo p^{k+1}*, die aus* x_0 *entstehen.*
Behauptung: *Dann gilt*

(1) $g = 1$, *falls* $f'(x_0) \not\equiv 0 \bmod p$ *ist* $\left(b \equiv -f(x_0) \cdot p^{-k} \cdot (f'(x_0))^* \bmod p\right)$,

(2) $g = p$, *falls* $f'(x_0) \equiv 0 \bmod p$ *und* $f(x_0) \equiv 0 \bmod p^{k+1}$ *sind, bzw.*

(3) $g = 0$, *falls* $f'(x_0) \equiv 0 \bmod p$ *und* $f(x_0) \not\equiv 0 \bmod p^{k+1}$ *sind.*

Beweis:

(i) Die Taylor–Entwicklung von f
Durch Taylor–Entwicklung von f um x_0 erkennt man die Existenz eines $c \in \mathbb{Z}$, so dass für alle $b \in \mathbb{N}_0$ mit $b < p$

$$\begin{aligned} f\left(x_0 + bp^k\right) &= f(x_0) + bp^k \cdot f'(x_0) + cp^{k+1} \\ &\equiv f(x_0) + bp^k \cdot f'(x_0) \bmod p^{k+1} \end{aligned}$$

ist. Hierbei wurde benutzt, dass die Faktoren $\frac{f^{(\nu)}(x_0)}{\nu!}$ für alle $\nu \in \mathbb{N}_0$ ganzzahlig sind.
$x_0 + bp^k$ mit $b \in \mathbb{N}_0$ und $b < p$ ist somit genau dann Lösung modulo p^{k+1}, wenn

$$f(x_0)\, p^{-k} + bf'(x_0) \equiv 0 \bmod p \qquad (\bigstar)$$

ist.

(ii) 1. Fall: $f'(x_0) \not\equiv 0 \bmod p$
Ist $f'(x_0) \not\equiv 0 \bmod p$, also $(p, f'(x_0)) = 1$, so existiert nach Satz 3.2 auf Seite 42 genau ein $b \in \mathbb{N}_0$ mit $b < p$ und $(\bigstar)$. Damit folgt (1).

(iii) 2. Fall: $f'(x_0) \equiv 0 \bmod p$ und $f(x_0) \equiv 0 \bmod p^{k+1}$
Sind $f'(x_0) \equiv 0 \bmod p$ und $f(x_0) \equiv 0 \bmod p^{k+1}$, so wird $(\bigstar)$ von allen $b \in \mathbb{N}_0$ mit $b < p$ erfüllt und es ergibt sich (2).

(iv) 3. Fall: $f'(x_0) \equiv 0 \bmod p$ und $f(x_0) \not\equiv 0 \bmod p^{k+1}$
Sind $f'(x_0) \equiv 0 \bmod p$ und $f(x_0) \not\equiv 0 \bmod p^{k+1}$, so gilt zwar $p | f'(x_0)$, aber wegen $p \nmid f(x_0)\, p^{-k}$ wird $(\bigstar)$ von keinem $b \in \mathbb{Z}$ gelöst. Also gilt (3). □

Beispiel

(1) Seien $p := 3$ und $f(x) := x^4 + 7x + 4$.

Durch Einsetzen sieht man

$$f(0) = 4 \not\equiv 0 \bmod 3, \qquad f(1) = 1 + 7 + 4 = 12 \equiv 0 \bmod 3$$
$$\text{und} \qquad f(2) = 16 + 14 + 4 = 34 \not\equiv 1 \bmod 3.$$

Sei also $x_0 := 1$. Wegen $f'(x_0) = 4 \cdot 1^3 + 7 = 11 \equiv 2 \bmod 3$ tritt der erste Fall ein.

(✯) wird zu

$$\frac{12}{3} + 11b \equiv 0 \bmod 3, \quad \text{d.h.} \quad 4 + 2b \equiv 0 \bmod 3, \quad \text{d.h.} \quad b \equiv 1 \bmod 3.$$

Somit ist $x_0 + 1 \cdot 3 = 4$ die einzige Lösung modulo 9.

(2) Seien $q := 5$ und $g(y) := y^3 - 2y + 1$.

$y_0 := 1$ und $y_1 := 2$ sind die einzigen Lösungen von $g(y) \equiv 0 \bmod q$.

Wegen $g'(2) \equiv 0 \bmod 5$ und $g(2) = 5 \not\equiv 0 \bmod 5^2$ erzeugt y_1 keine Lösung modulo 25.

Da $g'(1) \equiv 1 \bmod 5$ ist, ist $0 \cdot 5^{-1} + 1 \cdot b \equiv 0 \bmod 5$ zu lösen. Damit folgt $b = 0$, was die einzige Lösung $y_0 + b \cdot 5 \equiv 1 \bmod 25$ erzeugt.

Die zweite Hälfte des Kapitels ist der von Euler und Gauss entwickelten Theorie der quadratischen Kongruenzen gewidmet. Diese stellt einen Höhepunkt der elementaren Zahlentheorie dar.

Bemerkung 3.8
Kennt man die Antwort auf die Frage nach der Lösbarkeit von Kongruenzen der Gestalt

$$x^2 \equiv a \bmod p \quad \text{mit } p \in \mathbb{P} \setminus \{2\}, a \in \mathbb{Z} \text{ und } p \nmid a,$$

so kennt man die Antwort auf die Frage nach der Lösbarkeit von Kongruenzen der Gestalt

$$a_2 \cdot y^2 + a_1 \cdot y + a_0 \equiv 0 \bmod m \quad \text{mit } a_0 \in \mathbb{Z}, a_1 \in \mathbb{Z}, a_2 \in \mathbb{Z} \text{ und } m \in \mathbb{N}.$$

Beweis:
Nach Satz 3.4 auf Seite 44 genügt es, die Lösbarkeit von Kongruenzen zu Primzahlpotenzen zu untersuchen. Der Übergang von der Lösbarkeit modulo einer Primzahl zu der Lösbarkeit modulo einer Potenz dieser Primzahl wird in Satz 3.15 auf Seite 62 diskutiert.
Wegen $z^2 \equiv z \bmod 2$ für alle $z \in \mathbb{Z}$ kann die Frage nach der Lösbarkeit quadratischer Kongruenzen modulo 2 auf den Fall der linearen Kongruenzen zurückgeführt werden.
Seien also $a_0 \in \mathbb{Z}$, $a_1 \in \mathbb{Z}$, $a_2 \in \mathbb{Z}$ und $p \in \mathbb{P} \setminus \{2\}$ mit $(a_2, p) = 1$.

Dann gilt für alle $y \in \mathbb{Z}$

$$a_2 \cdot y^2 + a_1 \cdot y + a_0 = \frac{(2a_2y + a_1)^2 - (a_1^2 - 4a_0a_2)}{4a_2}.$$

Wegen $(4a_2, p) = 1$ sind also

$$a_2 \cdot y^2 + a_1 \cdot y + a_0 \equiv 0 \bmod p \qquad \text{und} \qquad (2a_2y + a_1)^2 \equiv \left(a_1^2 - 4a_0a_2\right) \bmod p$$

für alle $y \in \mathbb{Z}$ äquivalent. Man löse zuerst

$$y^2 \equiv \left(a_1^2 - 4a_0a_2\right) \bmod p$$

nach $y \in \mathbb{Z}$ und sodann mit Satz 3.2 auf Seite 42 für jede Lösung $y \in \mathbb{Z}$ hiervon

$$2a_2x + a_1 \equiv y \bmod p.$$

□

Definition 3.9 (quadratische (Nicht–)Reste und LEGENDRE–Symbol)

a) Für alle $p \in \mathbb{P} \setminus \{2\}$ und alle $a \in \mathbb{Z}$ mit $(a, p) = 1$ heißt a **quadratischer Rest modulo p** (Kurz: qR mod p), falls es ein $x \in \mathbb{Z}$ gibt, das die Kongruenz $x^2 \equiv a \bmod p$ löst. Andernfalls heißt a **quadratischer Nicht–Rest modulo p** (Kurz: qNR mod p).

b) Für alle $p \in \mathbb{P} \setminus \{2\}$ heißt

$$\left(\frac{\cdot}{p}\right) : \left\{ \begin{array}{rcl} \{b \in \mathbb{Z}\,;(b,p) = 1\} & \to & \{-1, 1\} \\ a & \mapsto & \left(\frac{a}{p}\right) := \begin{cases} 1, & \text{falls } a \text{ qR mod } p \text{ ist} \\ -1, & \text{falls } a \text{ qNR mod } p \text{ ist} \end{cases} \end{array} \right\}$$

LEGENDRE–Symbol zu p. („a über p“, Adrien–Marie LEGENDRE, 1752–1833)

Man beachte, dass $\left(\frac{a}{p}\right)$ nur für $p \in \mathbb{P} \setminus \{2\}$ und $a \in \mathbb{Z}$ mit $p \nmid a$ definiert ist.

Folgerung 3.10
Seien $p \in \mathbb{P} \setminus \{2\}$, $a \in \mathbb{Z}$ mit $(a, p) = 1$ und $b \in \mathbb{Z}$ mit $(b, p) = 1$.

(1) Gilt $a \equiv b \bmod p$, so ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) Es ist $\left(\frac{a^2}{p}\right) = 1$.

(3) Unter den Zahlen $1, \ldots, p-1$ sind genau $\frac{p-1}{2}$ quadratische Reste modulo p und $\frac{p-1}{2}$ quadratische Nichtreste modulo p. Es ist also $\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0$.

(4) Im Fall $\left(\frac{a}{p}\right) = 1$ gibt es genau zwei $x \in \mathbb{N}$ mit $x < p$ und $x^2 \equiv a \bmod p$.

BEWEIS:
(1) und (2) sind unmittelbar klar.

(i) Zu (3)
Die Zahlen

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \qquad (\bigstar)$$

sind modulo p paarweise inkongruent. Denn $k^2 \equiv \ell^2 \bmod p$ mit $k \in \mathbb{N}$, $k \leq \frac{p-1}{2}$, $\ell \in \mathbb{N}$ und $\ell \leq \frac{p-1}{2}$ impliziert $(k-\ell)\cdot(k+\ell) \equiv 0 \bmod p$.
Wegen $2 \leq k+\ell \leq p-1$, bzw. $p \nmid (k+\ell)$ folgt $p \mid (k-\ell)$, also $k = \ell$, da $|k-\ell| < p$ ist.

Jede Zahl x^2 mit $x \in \mathbb{Z}$ und $p \nmid x$ ist zu einer der Zahlen aus $(\bigstar)$ modulo p kongruent.
Denn sind $x \in \mathbb{Z}$ mit $(x,p) = 1$, $y \in \mathbb{N}$ mit $y \leq p$, $x \equiv y \bmod p$ und $c := \frac{x-y}{p}$, so gilt

$$x^2 = (y+cp)^2 \equiv y^2 \bmod p.$$

Im Fall $\frac{p-1}{2} + 1 \leq y \leq p-1$ ist aber $1 \leq p-y \leq \frac{p-1}{2}$ und $y^2 \equiv (p-y)^2 \bmod p$.

Ein quadratischer Rest modulo p ist daher zu einem der $\frac{p-1}{2}$ quadratischen Reste, die aus den Zahlen in $(\bigstar)$ hervorgehen, kongruent.
D.h. es existieren je $\frac{p-1}{2}$ qR und qNR mod p in $\{b \in \mathbb{N}\,; b < p\}$.

(ii) Zu (4)
Die Kongruenzen $x^2 \equiv a \bmod p$, wobei $a \in \mathbb{Z}$ alle $\frac{p-1}{2}$ qR mod p durchläuft, haben zusammen $p-1$ Lösungen $x \in \mathbb{N}$ mit $x < p$. Jede Einzelne hat nach dem Satz von LAGRANGE 3.5 auf Seite 45 höchstens zwei Lösungen, also hat jede genau zwei Lösungen. □

SATZ 3.11 (EULER–Kriterium und Multiplikationssatz)
VORAUSSETZUNGEN:
Seien $p \in \mathbb{P} \setminus \{2\}$, $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ mit $(ab, p) = 1$.
BEHAUPTUNG: **(1)** *Es ist* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$ ***(EULER–Kriterium).***

(2) *Es gilt* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$ ***(Multiplikationssatz).***

BEWEIS:

(i) Zu (1)
Aus der EULERschen Kongruenz 2.11 auf Seite 23 ergibt sich

$$\left(a^{\frac{p-1}{2}} - 1\right)\cdot\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \bmod p. \qquad (\bigstar)$$

Nur einer der zwei Faktoren auf der linken Seite von (✯), wird von $p > 2$ geteilt, da die Differenz der beiden Faktoren 2 ist.
Ist $\left(\frac{a}{p}\right) = 1$, gibt es also ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \bmod p$, dann gilt nach der EULERschen Kongruenz 2.11

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

Der erste Faktor links in (✯) wird somit für die $\frac{p-1}{2}$ qR mod p von p geteilt. Nach dem Satz von LAGRANGE 3.5 auf Seite 45 gibt es keine weiteren Lösungen.
Also gilt im Falle $\left(\frac{a}{p}\right) = -1$

$$a^{\frac{p-1}{2}} + 1 \equiv 0 \bmod p, \qquad \text{d.h.} \qquad a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p.$$

(ii) Zu (2)
(1) bewirkt

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

Wegen $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \in \{-2, 0, 2\}$ und $p > 2$ folgt hieraus die Gleichheit. □

Lemma 3.12 (GAUSSsches Lemma)
VORAUSSETZUNGEN:
Seien $p \in \mathbb{P} \setminus \{2\}$ und $a \in \mathbb{Z}$ mit $(a, p) = 1$. Für alle $j \in \mathbb{N}$ mit $j \leq \frac{p-1}{2}$ sei $c_j := ja - \left\lfloor \frac{ja}{p} \right\rfloor \cdot p$ der kleinste positive Rest der Zahl $j \cdot a$ bei Division durch p.
Sei $\mu := \#\left\{ j \in \mathbb{N} \,;\, j \leq \frac{p-1}{2} \text{ und } c_j > \frac{p}{2} \right\}$.
BEHAUPTUNG: *Dann gilt*

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

BEWEIS:

(i) Definition von b_k und d_ℓ
Für alle $j \in \mathbb{N}$ mit $j \leq \frac{p-1}{2}$ sind

$$ja = \left\lfloor \frac{ja}{p} \right\rfloor \cdot p + c_j \quad \text{und} \quad 0 < c_j \leq p - 1.$$

Seien $\nu := \frac{p-1}{2} - \mu$,

$$b_1, \ldots, b_\mu \quad \text{die} \quad c_j \quad \text{mit} \quad \frac{p+1}{2} \leq c_j \leq p - 1$$

und

$$d_1, \ldots, d_\nu \quad \text{die} \quad c_j \quad \text{mit} \quad 1 \le c_j \le \frac{p-1}{2}.$$

Die c_j und somit die b_k und die d_ℓ sind paarweise inkongruent modulo p, da $\{ja \in \mathbb{N}_0 \,;\, j \in \mathbb{N} \text{ mit } j \le p-1\}$ ein vollständiges Restsystem modulo p ist.

(ii) $\boldsymbol{\bigcup\{d_\ell\} \cup \bigcup\{p - b_k\} = \left\{ j \in \mathbb{N} \,;\, j \le \frac{p-1}{2} \right\}}$
Für alle $k \in \mathbb{N}$ mit $k \le \mu$ und alle $\ell \in \mathbb{N}$ mit $\ell \le \nu$ gilt

$$p - b_k \not\equiv d_\ell \bmod p.$$

Denn aus der Richtigkeit einer solchen Kongruenz folgte $b_k + d_\ell \equiv 0 \bmod p$, also $(j_1 + j_2) \cdot a \equiv 0 \bmod p$ mit einem Paar $(j_1, j_2)^T \in \mathbb{N}$ mit $\max\{j_1, j_2\} \le \frac{p-1}{2}$ und $j_1 \ne j_2$. Dies kann wegen $p \nmid a$ und $0 < j_1 + j_2 \le p-1$ aber nicht sein.
Die Aussage kann auch so formuliert werden, dass die Mengen

$$\left\{1, \ldots, \frac{p-1}{2}\right\} \quad \text{und} \quad \{d_1, \ldots, d_\nu, p - b_1, \ldots, p - b_\mu\}$$

identisch sind.

(iii) Beweis der Behauptung
Nach (i) gilt mit dem EULER–Kriterium 3.11 (1) auf Seite 50

$$P := \prod_{k=1}^{\mu} b_k \cdot \prod_{\ell=1}^{\nu} d_\ell \equiv a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \bmod p \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{p-1}{2}\right)! \bmod p.$$

Mit (ii) folgt wegen $P = (-1)^\mu \cdot \prod_{k=1}^{\mu} (-b_k) \cdot \prod_{\ell=1}^{\nu} d_\ell \equiv (-1)^\mu \cdot \prod_{k=1}^{\mu} (p - b_k) \cdot \prod_{\ell=1}^{\nu} d_\ell \bmod p$

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

Wegen $\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$ darf dividiert werden:

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

Da beide Seiten im Betrag höchstens 1 sind, und $p > 2$ ist, folgt die Behauptung. □

Der nächste, wichtige Satz bringt für $p \in \mathbb{P} \setminus \{2\}$ und $q \in \mathbb{P} \setminus \{2, p\}$ die Lösbarkeit von „$x^2 \equiv q \bmod p$“ mit der von „$x^2 \equiv p \bmod q$“ in Verbindung.

Satz 3.13 (Quadratisches Reziprozitätsgesetz (QRG))
(Gauss, 1801)

Behauptung: *Für zwei verschiedene, ungerade Primzahlen $p \in \mathbb{P} \setminus \{2\}$ und $q \in \mathbb{P} \setminus \{2, p\}$ gilt*

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

Ergänzungsgesetze:
Für alle $p \in \mathbb{P} \setminus \{2\}$ sind

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

und

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

Die Aussagen können auch folgendermaßen formuliert werden:

$$\text{QRG}: \quad \left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \text{ ist} \\ -\left(\frac{q}{p}\right), & \text{falls } p \equiv 3 \bmod 4 \text{ und } q \equiv 3 \bmod 4 \text{ sind} \end{cases}$$

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

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

Mit Hilfe der früheren Ergebnisse und des Reziprozitätsgesetzes kann im Prinzip jedes Legendre–Symbol $\left(\frac{a}{p}\right)$ relativ rasch berechnet werden. Man verwendet Verschiebung des Zählers modulo p, multiplikative Zerlegung des Zählers und Invertierung nach dem QRG. Die rechnerisch aufwändige Faktorisierung kann, wie in Satz 3.17 auf Seite 64 gezeigt wird, mit Hilfe des „Jacobi–Symbols“ umgangen werden.

Beispiel Ist die Kongruenz $x^2 + 77 \equiv 0 \bmod 43$ mit $x \in \mathbb{Z}$ lösbar?
Da 43 prim ist, berechnet man

$$\begin{aligned}\left(\frac{-77}{43}\right) &= \left(\frac{-1}{43}\right) \cdot \left(\frac{7}{43}\right) \cdot \left(\frac{11}{43}\right) \\ &= (-1) \cdot \left(-\left(\frac{43}{7}\right)\right) \cdot \left(-\left(\frac{43}{11}\right)\right) \\ &= -\left(\frac{1}{7}\right) \cdot \left(\frac{10}{11}\right) = -1 \cdot \left(\frac{2}{11}\right) \cdot \left(\frac{5}{11}\right) \\ &= -(-1) \cdot \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1.\end{aligned}$$

Die Kongruenz ist somit lösbar.
Für die Bestimmung der Lösungen $x_0 \in \mathbb{Z}$ und $43 - x_0$ wird im Anschluss an den Beweis ein Verfahren vorgestellt.

BEWEIS:

(i) $\boldsymbol{\left(\frac{q}{p}\right) = (-1)^{S_1}}$
Seien $p \in \mathbb{P} \setminus \{2\}$ und $q \in \mathbb{P} \setminus \{2, p\}$.
Wie beim GAUSSschen Lemma 3.12 auf Seite 51 seien

$$\begin{aligned}&c_j := qj - \left\lfloor \frac{qj}{p} \right\rfloor \cdot p, && \text{für alle } j \in \mathbb{N} \text{ mit } j \le \tfrac{p-1}{2}, \\ &\mu := \#\left\{ j \in \mathbb{N}\,; j \le \frac{p-1}{2} \text{ und } c_j > \frac{p}{2} \right\}, && \nu := \frac{p-1}{2} - \mu, \\ &b_1, \ldots, b_\mu \quad \text{die} \quad c_j \in \left[\frac{p+1}{2}, p-1\right] \quad \text{und} && d_1, \ldots, d_\nu \quad \text{die} \quad c_j \in \left[1, \frac{p-1}{2}\right].\end{aligned}$$

Es werde

$$S_1 := \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor$$

gesetzt. Summation von qj über j von 1 bis $\frac{p-1}{2}$ ergibt

$$q \cdot \frac{(p-1)\cdot(p+1)}{8} = \sum_{j=1}^{\frac{p-1}{2}} qj = p \cdot S_1 + \sum_{j=1}^{\frac{p-1}{2}} c_j.$$

Wie in Beweisschritt (ii) zum GAUSSschen Lemma 3.12 sieht man

$$\begin{aligned}\sum_{j=1}^{\frac{p-1}{2}} c_j &= \sum_{k=1}^{\mu} b_k + \sum_{\ell=1}^{\nu} d_\ell \\ &= 2 \cdot \sum_{k=1}^{\mu} b_k + \sum_{k=1}^{\mu} (p - b_k) + \sum_{\ell=1}^{\nu} d_\ell - \mu p \\ &= 2 \cdot \sum_{k=1}^{\mu} b_k + \sum_{n=1}^{\frac{p-1}{2}} n - \mu p\end{aligned}$$

wegen

$$\left\{1, \ldots, \frac{p-1}{2}\right\} = \{d_1, \ldots, d_\nu, p - b_1, \ldots, p - b_\mu\}.$$

Also ist

$$\sum_{j=1}^{\frac{p-1}{2}} c_j = \frac{(p-1)\cdot(p+1)}{8} + 2 \cdot \sum_{k=1}^{\mu} b_k - \mu p.$$

Zusammenfassung ergibt

$$\mu p = p \cdot S_1 + \underbrace{(1-q)}_{\equiv 0 \bmod 2} \cdot \underbrace{\frac{(p-1)\cdot(p+1)}{8}}_{\in \mathbb{Z}} + 2 \cdot \sum_{k=1}^{\mu} b_k \equiv p \cdot S_1 \bmod 2,$$

also wegen $p \in \mathbb{P} \setminus \{2\}$

$$\mu \equiv S_1 \bmod 2,$$

und mit dem GAUSSschen Lemma 3.12

$$\left(\frac{q}{p}\right) = (-1)^{S_1}.$$

(ii) $\left(\frac{p}{q}\right) = (-1)^{S_2}$

In ähnlicher Weise sieht man

$$\left(\frac{p}{q}\right) = (-1)^{S_2} \qquad \text{mit } S_2 := \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor.$$

(iii) Beweis des QRG

Es wird sich

$$S_1 + S_2 = \frac{p-1}{2} \cdot \frac{q-1}{2} \qquad (\bigstar)$$

herausstellen, was nach (i) und (ii) die Behauptung des Satzes nach sich zieht.
Zum Beweis sei oBdA $p > q$. Bezeichnen $\mathcal{R}$ das abgeschlossene Rechteck

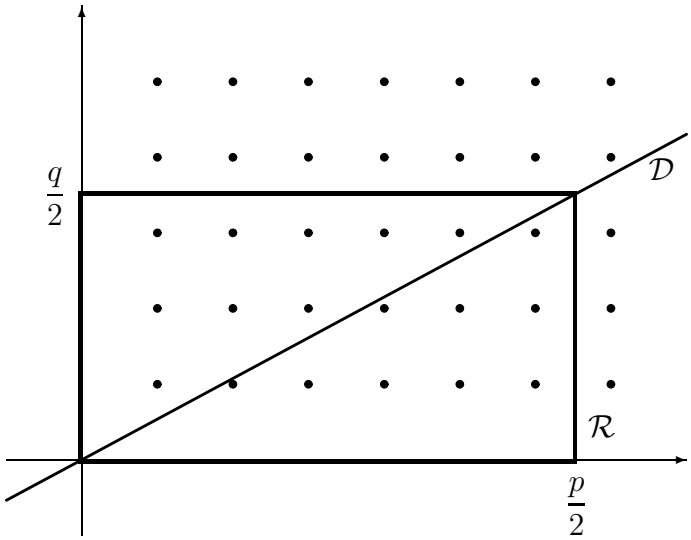
$$\mathcal{R} := \left[0, \frac{p}{2}\right] \times \left[0, \frac{q}{2}\right] \subseteq \mathbb{R}^2$$

und $G := \#\left(\mathbb{N}^2 \cap \mathcal{R}\right)$ die Anzahl der „Gitterpunkte“ in $\mathcal{R}$, so gilt offensichtlich

$$G = \frac{p-1}{2} \cdot \frac{q-1}{2}. \tag{$\star$}$$

Die Hauptdiagonale $\mathcal{D}$ von $\mathcal{R}$ lässt sich charakterisieren durch

$$\mathcal{D} := \left\{ \binom{n}{k} \in \mathbb{R}^2 \,; k = \frac{q}{p} \cdot n \right\}.$$



Auf $\mathcal{D}$ liegen keine Gitterpunkte $(n,k)^T \in \mathbb{N}^2 \cap \mathcal{R}$.
Denn $k = \frac{q}{p} \cdot n$ bewirkt $p|\,(qn)$, was für $1 \leq n \leq \frac{p-1}{2}$ und $(p,q) = 1$ nicht sein kann.
Für alle Gitterpunkte $(n,k)^T \in \mathbb{N}^2 \cap \mathcal{R}$ gilt

$$\frac{q}{p} \cdot n \leq \frac{q}{p} \cdot \frac{p-1}{2} = \frac{q}{2} - \frac{q}{2p} < \frac{q}{2}$$

und wegen $k \in \mathbb{N}$ folgt aus $k \leq \frac{q}{p} \cdot n$ also $k \leq \frac{q-1}{2}$.
Analog folgt $n \leq \frac{p-1}{2}$ aus $k > \frac{q}{p} \cdot n$ und $(n,k)^T \in \mathbb{N}^2 \cap \mathcal{R}$.
G kann nun berechnet werden durch Aufsummieren der Anzahl der $(n,k)^T \in \mathbb{N}^2 \cap \mathcal{R}$ unterhalb von $\mathcal{D}$, und der Anzahl der $(n,k)^T \in \mathbb{N}^2 \cap \mathcal{R}$ oberhalb von $\mathcal{D}$.

$$\begin{aligned} G &= \sum_{n=1}^{\frac{p-1}{2}} \sum_{\substack{k=1 \\ k \leq \frac{q}{p} n}}^{\frac{q-1}{2}} 1 + \sum_{k=1}^{\frac{q-1}{2}} \sum_{\substack{n=1 \\ n \leq \frac{p}{q} k}}^{\frac{p-1}{2}} 1 = \sum_{n=1}^{\frac{p-1}{2}} \sum_{k=1}^{\left\lfloor \frac{q}{p} n \right\rfloor} 1 + \sum_{k=1}^{\frac{q-1}{2}} \sum_{n=1}^{\left\lfloor \frac{p}{q} k \right\rfloor} 1 \\ &= \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{qn}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{pk}{q} \right\rfloor = S_1 + S_2. \end{aligned}$$

Mit ($\star$) ergibt dies ($\bigstar$), womit der Beweis des QRG geführt ist.

(iv) 1. Ergänzungsgesetz
Nach dem EULER–Kriterium 3.11 auf Seite 50 gilt

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

Mit $\left|\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}\right| \leq 2$ und $p > 2$ folgt die Behauptung.

(v) 2. Ergänzungsgesetz
Nach dem GAUSSschen Lemma 3.12 auf Seite 51 ist

$$\left(\frac{2}{p}\right) = (-1)^{\vartheta} \qquad \text{mit} \qquad \vartheta := \#\left\{ j \in \mathbb{N}\,;\, j \leq \frac{p-1}{2} \text{ und } 2j - \left\lfloor \frac{2j}{p} \right\rfloor \cdot p > \frac{p}{2} \right\}.$$

Sei $\mathcal{M} := \left\{ 2j \in \mathbb{N}\,;\, j \leq \frac{p-1}{2} \right\}$. Für alle $k \in \mathcal{M}$ ist $k \leq 2 \cdot \frac{p-1}{2} = p-1$. Wegen $\#\mathcal{M} = \frac{p-1}{2}$ besteht $\mathcal{M}$ also aus allen geraden natürlichen Zahlen, die kleiner als p sind. Insbesondere ist $\left\lfloor \frac{k}{p} \right\rfloor = 0$ für alle $k \in \mathcal{M}$ und damit folgt

$$\vartheta = \#\left\{ k \in \mathcal{M}\,;\, k > \frac{p}{2} \right\}.$$

Für alle $k \in \mathcal{M}$ mit $k \leq \frac{p}{2}$ gibt es ein $j \in \mathbb{N}$ mit $k = 2j$ und es folgt

$$2j \leq \frac{p}{2} \qquad \Longleftrightarrow \qquad j \leq \frac{p}{4}.$$

Also ist $\#\left\{ k \in \mathcal{M}\,;\, k \leq \frac{p}{2} \right\} = \left\lfloor \frac{p}{4} \right\rfloor$ und es folgt

$$\vartheta = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

Wegen $2 \nmid p$ gibt es ein $\ell \in \mathbb{N}$ und ein $r \in \{1,3,5,7\}$ mit $p = 8\ell + r$. Es folgt

$$\left(\frac{2}{p}\right) = (-1)^{\vartheta} \qquad \text{mit} \qquad \vartheta = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = 4\ell + \frac{r-1}{2} - \left\lfloor 2\ell + \frac{r}{4} \right\rfloor = 2\ell + \frac{r-1}{2} - \left\lfloor \frac{r}{4} \right\rfloor.$$

Für $r = 1$ ist $\frac{r-1}{2} - \left\lfloor \frac{r}{4} \right\rfloor = 0 - 0 = 0$ gerade, für $r = 3$ ist $\frac{r-1}{2} - \left\lfloor \frac{r}{4} \right\rfloor = 1 - 0 = 1$ ungerade, für $r = 5$ ist $\frac{r-1}{2} - \left\lfloor \frac{r}{4} \right\rfloor = 2 - 1 = 1$ ungerade und für $r = 7$ ist $\frac{r-1}{2} - \left\lfloor \frac{r}{4} \right\rfloor = 3 - 1 = 2$ gerade. □

ALGORITHMUS 3.14 (Bestimmung von Lösungen reinquadratischer Kongruenzen)
VORAUSSETZUNGEN:
Seien $p \in \mathbb{P}$ *und* $q \in \mathbb{P}$ *mit* $q \equiv 3 \bmod 4$.
Sei $a \in \mathbb{Z}$ *mit* $(a, pq) = 1$, $\left(\frac{a}{p}\right) = 1$ *und* $\left(\frac{a}{q}\right) = 1$.
Sei $b \in \mathbb{N}$ *mit* $b < p$, $(b^2 - a, p) = 1$ *und* $\left(\frac{b^2 - a}{p}\right) = -1$.

Sei $D \in \mathbb{N}$ *mit* $D < p$ *und* $D \equiv b^2 - a \bmod p$. *Sei*

$$\mathbb{Z}_p\left[\sqrt{D}\right] := \left\{ \underline{u} + \underline{v} \cdot \sqrt{D} \,;\, \underline{u} \in \mathbb{Z}_p \text{ und } \underline{v} \in \mathbb{Z}_p \right\}$$

versehen mit der offensichtlichen Addition und Multiplikation.

Seien $X := \left(\underline{b} + \underline{1} \cdot \sqrt{D}\right)^{\frac{p+1}{2}} \in \mathbb{Z}_p\left[\sqrt{D}\right]$ *und* $y := a^{\frac{q+1}{4}}$.

BEHAUPTUNG: *Es sind*

(1) $\#\left\{ d \in \mathbb{N} \,;\, d < p, \left(d^2 - a, p\right) = 1 \text{ und } \left(\dfrac{d^2 - a}{p}\right) = -1 \right\} \geq \dfrac{p-3}{2}$,

(2) $X \in \mathbb{Z}_p$, $x^2 \equiv a \bmod p$, $(p-x)^2 \equiv a \bmod p$ *für alle* $x \in X$,

(3) $y^2 \equiv a \bmod q$ *und* $(q-y)^2 \equiv a \bmod q$.

Bemerkung
Sowohl X als auch y können mit Hilfe des schnellen Potenzierens relativ schnell berechnet werden.
Nach Behauptung (1) liegt die Treffsicherheit beim Suchen eines b bei ungefähr 50%. Es sind also im Mittel etwa 2 Versuche nötig, um b zu finden.

Beispiel Seien $p := 17$ und $a := 8$. Finde alle $x \in \mathbb{N}$ mit $x < 17$ und $x^2 \equiv 8 \bmod 17$!
Es ist

$$\left(\frac{a}{p}\right) = \left(\frac{8}{17}\right) = \left(\frac{2^2}{17}\right) \cdot \left(\frac{2}{17}\right) = 1 \cdot (-1)^{\frac{17^2-1}{8}} = (-1)^{\frac{17-1}{8} \cdot (17+1)} = (-1)^{2 \cdot 18} = 1,$$

also gibt es ein $x \in \mathbb{Z}$ mit $x^2 \equiv 8 \bmod 17$.
Probiere $b := 1$. Es ist

$$\left(\frac{1^2 - 8}{17}\right) = \left(\frac{-1}{17}\right) \cdot \left(\frac{7}{17}\right) = (-1)^{\frac{17-1}{2}} \cdot \left(\frac{17}{7}\right) = 1 \cdot \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Seien also $D := 10 \equiv -7 \bmod 17 \equiv 1^2 - 8 \bmod 17$, $\mathcal{R} := \mathbb{Z}_{17}\left[\sqrt{10}\right]$ und

$$\xi := \underline{b} + \underline{1} \cdot \sqrt{D} = \underline{1} + \underline{1} \cdot \sqrt{10} \in \mathcal{R}.$$

Sei $X := \xi^{\frac{17+1}{2}} = \xi^9$. Mit schnellem Potenzieren folgt

$$\begin{aligned}
\xi^2 &= \left(\underline{1} + \underline{1} \cdot \sqrt{10}\right)^2 = \underline{1^2} + \underline{2 \cdot 1 \cdot 1} \cdot \sqrt{10} + \underline{1^2 \cdot 10} = \underline{1} + \underline{2} \cdot \sqrt{10} + \underline{10} \\
&= \underline{11} + \underline{2} \cdot \sqrt{10}, \\
\xi^4 &= \left(\underline{11} + \underline{12} \cdot \sqrt{10}\right)^2 = \underline{11^2} + \underline{2 \cdot 11 \cdot 2} \cdot \sqrt{10} + \underline{2^2 \cdot 10} = \underline{121} + \underline{44} \cdot \sqrt{10} + \underline{40} \\
&\overset{\text{in } \mathcal{R}}{=} \underline{8} + \underline{10} \cdot \sqrt{10}, \\
\xi^8 &= \left(\underline{8} + \underline{10} \cdot \sqrt{10}\right)^2 = \underline{8^2} + \underline{2 \cdot 8 \cdot 10} \cdot \sqrt{10} + \underline{10^2 \cdot 10} = \underline{64} + \underline{160} \cdot \sqrt{10} + \underline{1000} \\
&\overset{\text{in } \mathcal{R}}{=} \underline{10} + \underline{7} \cdot \sqrt{10}
\end{aligned}$$

und

$$\begin{aligned}\xi^9 &= \left(\underline{10} + \underline{7} \cdot \sqrt{10}\right) \cdot \left(\underline{1} + \underline{1} \cdot \sqrt{10}\right) = \underline{10 \cdot 1} + \underline{7 \cdot 1} \cdot \sqrt{10} + \underline{10 \cdot 1} \cdot \sqrt{10} + \underline{7 \cdot 1 \cdot 10} \\ &= \underline{10} + \underline{70} + \underline{(7+10)} \cdot \sqrt{10} \overset{\text{in } \mathcal{R}}{=} \underline{12} + \underline{0} \cdot \sqrt{10} = \underline{12}.\end{aligned}$$

Es sind also $12^2 = 144 \equiv 8 \bmod 17$ und $5^2 = 25 \equiv 8 \bmod 17$.

Beweis:

(i) Zu (3)
Nach dem Euler–Kriterium 3.11 auf Seite 50 und der binomischen Formel sind

$$y^2 = \left(a^{\frac{q+1}{4}}\right)^2 = a^{\frac{q+1}{2}} = a \cdot a^{\frac{q-1}{2}} \equiv a \cdot \left(\frac{a}{q}\right) \bmod q \equiv a \cdot 1 \bmod q \equiv a \bmod q$$

und

$$(q-y)^2 = q^2 - 2qy + y^2 \equiv y^2 \bmod q \equiv a \bmod q.$$

(ii) $\left(\mathbb{Z}_p\left[\sqrt{D}\right], \cdot, +\right)$ ist ein Körper
Sei $\mathcal{R} := \left(\mathbb{Z}_p\left[\sqrt{D}\right], \cdot, +\right)$. $\mathcal{R}$ ist ein Ring.
Sind $\underline{u} \in \mathbb{Z}_p$ und $\underline{v} \in \mathbb{Z}_p$ mit $\underline{u} + \underline{v} \cdot \sqrt{D} \neq 0$ in $\mathcal{R}$, so folgte aus $p \mid (u^2 - Dv^2)$, dass $u^2 \equiv Dv^2 \bmod p$ wäre.
Wegen $\left(\frac{Dv^2}{p}\right) = \left(\frac{D}{p}\right) \cdot \left(\frac{v^2}{p}\right) = \left(\frac{b^2-a}{p}\right) \cdot 1 = -1$ für alle $v \in \mathbb{Z}$ ist das aber nicht möglich.
Sei also $A : \left\{ \begin{array}{rcl} \mathbb{Z}_p\left[\sqrt{D}\right] \setminus \{0\} & \to & \mathbb{Z} \\ \underline{u} + \underline{v} \cdot \sqrt{D} & \mapsto & A^*(u,v) \end{array} \right\}$ derart, dass $A^*(u,v) \cdot (u^2 - Dv^2) \equiv 1 \bmod p$ für alle $\underline{u} + \underline{v} \cdot \sqrt{D} \in \mathbb{Z}_p\left[\sqrt{D}\right] \setminus \{0\}$ ist.
Dann gilt für alle $\underline{u} + \underline{v} \cdot \sqrt{D} \in \mathbb{Z}_p\left[\sqrt{D}\right] \setminus \{0\}$

$$\begin{aligned}&\left(\underline{u} + \underline{v} \cdot \sqrt{D}\right) \cdot \left(\underline{A^*(u,v) \cdot u} - \underline{A^*(u,v) \cdot v} \cdot \sqrt{D}\right) \\ &\quad = \underline{A^*(u,v) \cdot u^2} + \underline{v \cdot A^*(u,v) \cdot u} \cdot \sqrt{D} - \underline{u \cdot A^*(u,v) \cdot v} \cdot \sqrt{D} - \underline{A^*(u,v) \cdot v \cdot D} \\ &\quad = \underline{A^*(u,v) \cdot \left(u^2 - Dv^2\right)} + \underline{0} \cdot \sqrt{D} \\ &\quad = \underline{1}.\end{aligned}$$

Damit folgt, dass $\mathcal{R}$ sogar ein Körper ist.

(iii) Zu (2)
Für alle $\underline{u} \in \mathbb{Z}_p$ und alle $\underline{v} \in \mathbb{Z}_p$ ist

$$\begin{aligned}\left(\underline{u}+\underline{v}\cdot\sqrt{D}\right)^p &= \sum_{j=0}^{p}\underline{\binom{p}{j}}\cdot\underline{u}^j\cdot\left(\underline{v}\cdot\sqrt{D}\right)^{p-j}\\ &= \underline{u^p}+\underline{v^p}\cdot\sqrt{D}^p+\underbrace{\sum_{j=1}^{p-1}\underline{\binom{p}{j}}\cdot\underline{u^j}\cdot\left(\underline{v}\cdot\sqrt{D}\right)^{p-j}}_{=\underline{0},\text{ da } p\mid\binom{p}{j}\text{ für alle } j\in\mathbb{N}\text{ mit } j\le p-1}\\ &= \underline{u}+\underline{v\cdot D^{\frac{p-1}{2}}}\cdot\sqrt{D}=\underline{u}+\underline{-v}\cdot\sqrt{D},\end{aligned}$$

da nach der FERMATschen Kongruenz 2.11 auf Seite 23 $u^p \equiv u \bmod p$ und $v^p \equiv v \bmod p$ sind und nach dem EULER–Kriterium 3.11 auf Seite 50 $D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \bmod p \equiv -1 \bmod p$ ist.
Damit folgt

$$\begin{aligned}X^2 &= \left(\left(\underline{b}+\underline{1}\cdot\sqrt{D}\right)^{\frac{p+1}{2}}\right)^2=\left(\underline{b}+\underline{1}\cdot\sqrt{D}\right)^{p+1}\\ &= \left(\underline{b}+\underline{1}\cdot\sqrt{D}\right)^p\cdot\left(\underline{b}+\underline{1}\cdot\sqrt{D}\right)=\left(\underline{b}+\underline{-1}\cdot\sqrt{D}\right)\cdot\left(\underline{b}+\underline{1}\cdot\sqrt{D}\right)\\ &= \underline{b^2}+\underline{-b}\cdot\sqrt{D}+\underline{b}\cdot\sqrt{D}+\underline{-D}=\underline{b^2-D}=\underline{a}\end{aligned}$$

und

$$\left(\underline{p}-X\right)^2=\underline{p^2}-\underline{2p}\cdot X+X^2=X^2=\underline{a}.$$

Nach dem Satz von LAGRANGE 3.5 auf Seite 45 gibt es höchstens zwei Lösungen im Körper $\mathcal{R}$. Wegen $\left(\frac{a}{p}\right)=1$ gibt es bereits zwei Lösungen in $\mathbb{Z}_p$ nach Folgerung 3.10 (4) auf Seite 49. Wegen $\mathbb{Z}_p \subseteq \mathcal{R}$ sind Lösungen in $\mathcal{R}$ also bereits Elemente von $\mathbb{Z}_p$, da es sonst mehr als zwei Lösungen in $\mathcal{R}$ gäbe.
Also ist $X \in \mathbb{Z}_p$ und es folgt Behauptung (2).

(iv) Zu (1)
Sei $D' \in \mathbb{N}$ mit $D' < p$ und $\left(\frac{D'}{p}\right)=-1$. Analog (ii) folgt, dass $\left(\mathbb{Z}_p\left[\sqrt{D'}\right],\cdot,+\right)$ ein Körper ist. Definiere die sogenannte Norm–Abbildung

$$N:\left\{\begin{array}{ccc}\mathbb{Z}_p\left[\sqrt{D'}\right] & \to & \mathbb{Z}_p\\ \underline{u}+\underline{v}\cdot\sqrt{D'} & \mapsto & N\left(\underline{u}+\underline{v}\cdot\sqrt{D'}\right):=\underline{u^2-D'v^2}\end{array}\right\}.$$

Für alle $d \in \mathbb{Z}$ und alle $v \in \mathbb{Z}$ mit $p \nmid v$ und $N\left(\underline{d}+\underline{v}\cdot\sqrt{D'}\right)=\underline{a}$ gilt

$$\begin{aligned}\underline{v^2D'} &= \left(\underline{d}+\underline{v}\cdot\sqrt{D'}-\underline{d}\right)^2=\left(\underline{d}+\underline{v}\cdot\sqrt{D'}\right)^2-\underline{2d}\cdot\left(\underline{d}+\underline{v}\cdot\sqrt{D'}\right)+\underline{d^2}\\ &= \underline{d^2}+\underline{2dv}\cdot\sqrt{D'}+\underline{v^2D'}-\underline{2d^2}-\underline{2dv}\cdot\sqrt{D'}+\underline{d^2}\\ &= -\underline{\left(d^2-D'v^2\right)}+\underline{d^2}=\underline{d^2}-N\left(\underline{d}+\underline{v}\cdot\sqrt{D'}\right)=\underline{d^2}-\underline{a}=\underline{d^2-a}.\end{aligned}$$

Wegen $\left(\frac{D'v^2}{p}\right) = \left(\frac{D'}{p}\right) \cdot \left(\frac{v^2}{p}\right) = (-1) \cdot 1 = -1$ für alle $v \in \mathbb{Z}$ mit $p \nmid v$ ist $d^2 - a$ für alle $d \in \mathbb{Z}$ und alle $v \in \mathbb{Z}$ mit $p \nmid v$ und $N\left(\underline{d} + \underline{v} \cdot \sqrt{D'}\right) = \underline{a}$ ein qNR mod p.
Sei

$$\mathcal{M} := \left\{ \xi \in \mathbb{Z}_p\left[\sqrt{D'}\right] \setminus \{0\} \,;\, N(\xi) = \underline{a} \right\}.$$

Wegen $(a, p) = 1$ gibt es ein $a^* \in \mathbb{Z}$ mit $aa^* \equiv 1 \bmod p$.
Wie in (iii) folgt für alle $u \in \mathbb{Z}$ und alle $v \in \mathbb{Z}$

$$\begin{aligned}\left(\underline{u} + \underline{v} \cdot \sqrt{D'}\right)^{p+1} &= \left(\underline{u} + \underline{v} \cdot \sqrt{D'}\right)^{p} \cdot \left(\underline{u} + \underline{v} \cdot \sqrt{D'}\right) \\ &= \left(\underline{u} + \underline{-v} \cdot \sqrt{D'}\right) \cdot \left(\underline{u} + \underline{v} \cdot \sqrt{D'}\right) \\ &= \underline{u^2} + \underline{uv} \cdot \sqrt{D'} + \underline{-uv} \cdot \sqrt{D'} + \underline{v^2 D'} \\ &= \underline{u^2 - v^2 D'} = N\left(\underline{u} + \underline{v} \cdot \sqrt{D'}\right).\end{aligned}$$

Deshalb ist für alle $\xi \in \mathbb{Z}_p\left[\sqrt{D'}\right] \setminus \{0\}$

$$\xi \in \mathcal{M} \qquad \Longleftrightarrow \qquad N(\xi) = \underline{a} \qquad \Longleftrightarrow \qquad \underline{a^*} \cdot N(\xi) = \underline{1} \qquad \Longleftrightarrow \qquad \xi^{p+1} - \underline{a} = \underline{0}.$$

Damit ist

$$\mathcal{M} = \left\{ \xi \in \mathbb{Z}_p\left[\sqrt{D'}\right] \setminus \{0\} \,;\, \underline{a^*} \cdot N(\xi) = \underline{1} \right\} = \ker\left(\underline{a^*} \cdot N\right)$$

und, da die letzte Kongruenz nach dem Satz von Lagrange 3.5 auf Seite 45 höchstens $p+1$ Lösungen hat, folgt

$$\#\ker\left(\underline{a^*} \cdot N\right) \leq p + 1.$$

Weil $\underline{a^*} \cdot N(\xi)$ für alle $\xi \in \mathbb{Z}_p\left[\sqrt{D'}\right] \setminus \{0\}$ in $\mathbb{Z}_p \setminus \{\underline{0}\}$ landet, ist

$$\#\operatorname{im}\left(\underline{a^*} \cdot N\right) \leq \#\left(\mathbb{Z}_p \setminus \{\underline{0}\}\right) = p - 1.$$

Mit dem Homomorphiesatz aus der Algebra folgt

$$\begin{aligned}(p-1) \cdot (p+1) = p^2 - 1 &= \#\left(\mathbb{Z}_p\left[\sqrt{D'}\right] \setminus \{0\}\right) \\ &= \#\left(\left(\mathbb{Z}_p\left[\sqrt{D'}\right] \setminus \{0\}\right) / \ker\left(\underline{a^*} \cdot N\right)\right) \cdot \#\ker\left(\underline{a^*} \cdot N\right) \\ &= \#\operatorname{im}\left(\underline{a^*} \cdot N\right) \cdot \#\ker\left(\underline{a^*} \cdot N\right) \\ &\leq (p-1) \cdot (p+1).\end{aligned}$$

Damit folgt Gleichheit und mit dem Vorherigen ergibt sich

$$\#\ker\left(\underline{a^*} \cdot N\right) = p + 1 \qquad \text{und} \qquad \#\operatorname{im}\left(\underline{a^*} \cdot N\right) = p - 1.$$

Insbesondere ist

$$\#\mathcal{M} = p + 1.$$

Es ist

$$\#\left(\mathcal{M}\cap\mathbb{Z}_p\right)\leq 2,$$

denn für ein $\underline{x}\in\mathbb{Z}_p$ ist $N\left(\underline{x}\right)=\underline{x^2}$ und nach dem Satz von LAGRANGE 3.5 auf Seite 45 hat $\underline{y^2}-\underline{a}=\underline{0}$ im Körper $\mathbb{Z}_p$ höchstens zwei Lösungen.
Für alle $d\in\mathbb{Z}$, alle $v_1\in\mathbb{Z}$ und alle $v_2\in\mathbb{Z}$ ist

$$\begin{aligned} N\left(\underline{d}+\underline{v_1}\cdot\sqrt{D'}\right)=N\left(\underline{d}+\underline{v_2}\cdot\sqrt{D'}\right) \quad &\Longleftrightarrow \quad d^2-Dv_1^2=d^2-Dv_2^2\\ \Longleftrightarrow \quad v_1^2=v_2^2 \quad &\Longleftrightarrow \quad |v_1|=|v_2|\,. \end{aligned}$$

Also gibt es mindestens

$$\frac{\#\mathcal{M}}{2}-2=\frac{p+1}{2}-2=\frac{p-3}{2}$$

viele $\underline{d}\in\mathbb{Z}_p$, so dass es ein $v\in\mathbb{Z}$ mit $p\nmid v$ und $N\left(\underline{d}+\underline{v}\cdot\sqrt{D'}\right)=\underline{a}$ gibt, das heißt, für die $\left(\dfrac{d^2-a}{p}\right)=1$ ist. □

Für das spezielle Polynom $f\left(x\right)=x^2-a$ mit $a\in\mathbb{Z}$ ist das Lösungsverhalten modulo $p\in\mathbb{P}\setminus\{2\}$ und modulo p^k mit $k\in\mathbb{N}$ identisch, während das allgemeine Polynom zweiten Grades von Fall zu Fall nach dem Aufsteigesatz 3.7 auf Seite 47 untersucht werden muss. Der Vollständigkeit halber wird schließlich die Kongruenz $x^2\equiv a \bmod 2^\ell$ mit $\ell\in\mathbb{N}$ untersucht.

SATZ 3.15 (Lösungen modulo Primzahlpotenzen)
VORAUSSETZUNGEN:
Seien $p\in\mathbb{P}\setminus\{2\}$, $k\in\mathbb{N}$, $a\in\mathbb{Z}$ *mit* $(a,p)=1$, $b\in\mathbb{Z}$ *mit* $2\nmid b$ *und* $f:\left\{\begin{array}{ccc}\mathbb{R}&\to&\mathbb{R}\\ x&\mapsto&f\left(x\right):=x^2-b\end{array}\right\}$.

BEHAUPTUNG: **(1)** *Die Kongruenz* $x^2\equiv a \bmod p^k$ *hat genau* $1+\left(\dfrac{a}{p}\right)$ *Lösungen* $x\in\mathbb{Z}$.

(2) *Die Lösungszahl der Kongruenz* $f\left(x\right)\equiv 0 \bmod 2^k$ *ist*

$$\rho\left(2^k,f\right)=\begin{cases}1, & \text{falls } k=1 \text{ ist.}\\ 2, & \text{falls } k=2 \text{ und } b\equiv 1\,(4) \text{ sind.}\\ 0, & \text{falls } k=2 \text{ und } b\equiv 3\,(4) \text{ sind.}\\ 4, & \text{falls } k\geq 3 \text{ und } b\equiv 1\,(8) \text{ sind.}\\ 0, & \text{falls } k\geq 3 \text{ und } b\not\equiv 1\,(8) \text{ sind.}\end{cases}$$

BEWEIS:

(i) Zu (1)
Für $k = 1$ ist dies Folgerung 3.10 (4) auf Seite 49.
Ist $k \neq 1$, so wendet man den Aufsteigesatz 3.7 auf Seite 47 auf $h(x) = x^2 - a$ an.
Wegen $p \nmid (2a)$ gilt $h'(x_0) = 2x_0 \not\equiv 0\,(p)$ für jede Lösung $x_0 \in \mathbb{Z}$ mit $x_0^2 - a \equiv 0\,(p^k)$.
Es tritt also stets der erste Fall im Aufsteigesatz 3.7 ein und man erhält die Behauptung.

(ii) Zu (2)
Die Fälle $k = 1$ und $k = 2$ rechnet man ohne Schwierigkeiten nach.
Sei also nun $k \geq 3$ vorausgesetzt. Gibt es ein $x \in \mathbb{Z}$ mit

$$x^2 \equiv b \bmod 2^k, \tag{$\divideontimes$}$$

dann muss x wegen $2 \nmid b$ ungerade sein und es gibt ein $c \in \mathbb{Z}$ mit $x = 2c + 1$. Also gilt im Falle der Lösbarkeit

$$b \equiv (2c+1)^2 \bmod 2^k \equiv 4c \cdot (c+1) + 1 \bmod 2^k \equiv 8 \cdot \frac{c \cdot (c+1)}{2} + 1 \bmod 2^k \equiv 1 \bmod 8.$$

Für $b \equiv 1\,(8)$ hat ($\divideontimes$) bei $k = 3$ die vier Lösungen $x = 1$, $x = 3$, $x = 5$ und $x = 7$.
Dies diene als Induktionsanfang.
Für $k \geq 4$ sei $x \in \mathbb{Z}$ mit $x^2 \equiv b \bmod 2^{k-1}$.
Es gilt $2 \nmid x$ und deshalb gibt es ein $x^* \in \mathbb{Z}$ mit $x^* x \equiv 1\,(2^k)$. Es werde

$$d := x^* \cdot \frac{b - x^2}{2^{k-1}}$$

gesetzt. Damit gilt

$$\left(x + 2^{k-2}d\right)^2 \equiv x^2 + 2^{k-1}xd \bmod 2^k \equiv x^2 + b - x^2 \bmod 2^k \equiv b \bmod 2^k.$$

Es gibt also Lösungen von ($\divideontimes$) modulo 2^k.
Seien $x_1 \in \mathbb{Z}$ und $x_2 \in \mathbb{Z}$ zwei Lösungen von ($\divideontimes$) modulo 2^k. Dann gilt

$$x_1^2 - x_2^2 = (x_1 - x_2) \cdot (x_1 + x_2) \equiv 0 \bmod 2^k.$$

Da x_1 und x_2 beide ungerade sind, kann durch 4 dividiert werden:

$$\frac{x_1 - x_2}{2} \cdot \frac{x_1 + x_2}{2} \equiv 0 \bmod 2^{k-2}$$

$\frac{x_1 - x_2}{2}$ und $\frac{x_1 + x_2}{2}$ können nicht zugleich gerade oder ungerade sein, da sonst ihre Summe, nämlich x_1, gerade wäre.
Sei also im ersten Fall $\frac{x_1 - x_2}{2} \equiv 0\,(2^{k-2})$, das heißt $x_2 \equiv x_1 \bmod 2^{k-1}$. Dies induziert modulo 2^k die zwei Werte x_1 und $x_1 + 2^{k-1}$.
Ähnlich erhält man im Fall $\frac{x_1 + x_2}{2} \equiv 0\,(2^{k-2})$ die zwei Werte $-x_1$ und $-x_1 + 2^{k-1}$.
Man überzeugt sich, dass diese vier Zahlen modulo 2^k verschieden sind.
Alle vier lösen die Kongruenz ($\divideontimes$) (binomische Formel) und andere Lösungen kann es nicht geben. □

Zur raschen Berechnung des LEGENDRE–Symbols $\left(\frac{a}{p}\right)$ wurde 1846 durch Carl Gustav JACOBI (1804–1851) das später nach ihm benannte Symbol eingeführt.

Definition 3.16 (JACOBI–Symbol)
Für $b : \left\{ \begin{array}{ccc} \mathbb{P} & \to & \mathbb{N}_0 \\ p & \mapsto & b_p \end{array} \right\}$ mit $b_2 = 0$ und $0 < \#\{p \in \mathbb{P} \,; b_p \neq 0\} < \infty$, $m := \prod\limits_{p \in \mathbb{P}} p^{b_p}$ und $a \in \mathbb{Z}$ mit $(a, m) = 1$ wird das **JACOBI–Symbol** definiert durch

$$\left(\frac{a}{m}\right) := \prod_{\substack{p \in \mathbb{P} \\ (a,p)=1}} \left(\frac{a}{p}\right)^{b_p}.$$

Bemerkung
Für $m \in \mathbb{P} \setminus \{2\}$ stimmen LEGENDRE– und JACOBI–Symbol offenbar überein. Für zusammengesetztes $m \in \mathbb{N} \setminus \mathbb{P}$ mit $m \neq 1$ und $a \in \mathbb{Z}$ mit $(a, m) = 1$ bedeutet $\left(\frac{a}{m}\right) = 1$ nicht notwendig, dass die Kongruenz $x^2 \equiv a \bmod m$ lösbar ist.
Zum Beispiel ist $\left(\frac{2}{9}\right) = 1$, aber $x^2 \not\equiv 2 \bmod 9$ für alle $x \in \mathbb{Z}$.

Die Rechengesetze für das LEGENDRE–Symbol übertragen sich auf das JACOBI–Symbol.

SATZ 3.17 (Rechenregeln für das JACOBI–Symbol)
BEHAUPTUNG: *Für alle $m \in \mathbb{N} \setminus \{1\}$ mit $2 \nmid m$, alle $n \in \mathbb{N} \setminus \{1\}$ mit $2 \nmid n$, alle $a \in \mathbb{Z}$ mit $(a, mn) = 1$ und alle $b \in \mathbb{Z}$ mit $(b, m) = 1$ gilt*

(1) $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$, *falls* $a \equiv b \bmod m$ *ist,*

(2) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{b}{m}\right)$,

(3) $\left(\frac{a^2}{m}\right) = 1$,

(4) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{a}{n}\right)$,

(5) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$,

(6) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$ *und*

(7) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \cdot (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$, *falls* $(m, n) = 1$ *ist.*

Die Aussagen können alle ohne Mühe auf die entsprechenden Beziehungen für das Legendre–Symbol zurückgeführt werden. Es werde am Beispiel (7) ausgeführt.

BEWEIS: (von (7))
Seien $(n,m) = 1$, $m = \prod_{j=1}^{r} p_j$ und $n = \prod_{k=1}^{s} q_k$ mit ungeraden Primzahlen p_j und q_k. Dabei darf eine Primzahl in dem Produkt häufiger als einmal vorkommen. Dann ist $p_j \neq q_k$ für alle $j \in \mathbb{N}$ mit $j \leq r$ und alle $k \in \mathbb{N}$ mit $k \leq s$.
Nach Definition des JACOBI–Symbols, mit (2), (4) und mit dem quadratischen Reziprozitätsgesetz 3.13 auf Seite 53 für das LEGENDRE–Symbol ist dann

$$\begin{aligned}\left(\frac{m}{n}\right) &= \prod_{k=1}^{s}\prod_{j=1}^{r}\left(\frac{p_j}{q_k}\right)\\ &= \prod_{k=1}^{s}\prod_{j=1}^{r}\left(\frac{q_k}{p_j}\right)\cdot(-1)^{\frac{p_j-1}{2}\cdot\frac{q_k-1}{2}}\\ &= \left(\frac{n}{m}\right)\cdot(-1)^{\alpha} \qquad \text{mit}\\ \alpha &= \sum_{k=1}^{s}\sum_{j=1}^{r}\frac{p_j-1}{2}\cdot\frac{q_j-1}{2} = \left(\sum_{j=1}^{r}\frac{p_j-1}{2}\right)\cdot\left(\sum_{k=1}^{s}\frac{q_k-1}{2}\right).\end{aligned}$$

Man überprüft

$$\sum_{j=1}^{r}\frac{p_j-1}{2} \equiv \frac{m-1}{2} \bmod 2 \qquad \text{und} \qquad \sum_{k=1}^{s}\frac{q_k-1}{2} \equiv \frac{n-1}{2} \bmod 2$$

leicht durch Induktion nach r bzw. s, womit die Behauptung folgt. □

Satz 3.17 erlaubt es, $\left(\frac{a}{p}\right)$ für $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $p \nmid a$ ohne Faktorisieren des Zählers zu berechnen. Denn es sind folgende Operationen ausreichend.

a) Reduzieren des Zählers, so dass der Betrag des Zählers kleiner wird als die Hälfte des Nenners.

b) Herausziehen von Zweierpotenzen im Zähler.

c) Berechnen von $\left(\frac{-1}{m}\right)$ und $\left(\frac{2}{m}\right)$ für $m \in \mathbb{N} \setminus \{1\}$ mit $2 \nmid m$.

d) Anwenden des Reziprozitätsgesetzes 3.17 (7).

Beispiel Es soll die Lösbarkeit der Kongruenz $x^2 \equiv 383 \bmod 443$ untersucht werden. 443 ist eine Primzahl. Mit Satz 3.17 folgt

$$\begin{aligned}\left(\frac{383}{443}\right) &\overset{(7)}{=} -\left(\frac{443}{383}\right) \overset{(1)}{=} -\left(\frac{60}{383}\right) \overset{(2)}{=} -\left(\frac{2^2}{383}\right)\cdot\left(\frac{15}{383}\right)\\ &\overset{(3)}{=} -\left(\frac{15}{383}\right) \overset{(7)}{=} \left(\frac{383}{15}\right) \overset{(1)}{=} \left(\frac{8}{15}\right)\\ &\overset{(2)}{=} \left(\frac{2^2}{15}\right)\cdot\left(\frac{2}{15}\right) \overset{(3)}{=} \left(\frac{2}{15}\right) \overset{(6)}{=} 1.\end{aligned}$$

Die Kongruenz $x^2 \equiv 383 \bmod 443$ ist somit lösbar.

Kapitel 4: Summen aus Quadraten und höheren Potenzen

Definition 4.1 (Pythagoräische Tripel)
(Pythagoras, ca. 580–500 vor Christus)
Ein Tripel $(x,y,z)^T \in \mathbb{N}^3$ heißt **pythagoräisches Tripel**, wenn es die Gleichung $x^2+y^2=z^2$ erfüllt.
Ein pythagoräisches Tripel $(x,y,z)^T \in \mathbb{N}^3$ heißt **primitiv**, wenn $(x,y)=1$ und $2|x$ gelten.

Satz 4.2 (Indische Formeln)
Behauptung: *Es ist*

$$\begin{aligned}&\left\{(x,y,z)^T \in \mathbb{N}^3\,;(x,y)=1, 2|x \text{ und } x^2+y^2=z^2\right\}\\ &\qquad = \left\{\begin{pmatrix}2ab\\ a^2-b^2\\ a^2+b^2\end{pmatrix} \in \mathbb{N}^3\,;\ \begin{array}{l}a\in\mathbb{N}, b\in\mathbb{N} \text{ mit } a>b,\\ a+b\equiv 1 \bmod 2\\ \text{und } (a,b)=1\end{array}\right\}.\end{aligned}$$

Anders ausgedrückt erhält man alle primitiven pythagoräischen Tripel $(x,y,z)^T \in \mathbb{N}^3$ durch

$$a\in\mathbb{N}, \quad b\in\mathbb{N} \quad \text{mit} \quad (a,b)=1, \quad a>b \quad \text{und} \quad a+b\equiv 1 \bmod 2$$

und

$$x := 2ab, \quad y := a^2-b^2 \quad \text{und} \quad z := a^2+b^2.$$

Die Einschränkungen $(x,y)=1$ und $2|x$ sind unerheblich, denn

- Für $d\in\mathbb{N}$ mit $d|x$ und $d|y$ folgt $d^2|z^2$, also $d|z$.
- Sind x und y beide ungerade, so ist $x^2+y^2 \equiv 2\,(4)$ und kann somit kein Quadrat sein.

Es genügt daher, alle primitiven pythagoräischen Tripel zu bestimmen.

BEWEIS:

(i) „⊆“
Seien $x \in \mathbb{N}$, $y \in \mathbb{N}$ und $z \in \mathbb{N}$ mit $2|x$, $(x,y) = 1$ und

$$x^2 + y^2 = z^2.$$

Dann ist z ungerade, also sind $\frac{z-y}{2}$ und $\frac{z+y}{2}$ ganz und $\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$. Denn wenn ein $p \in \mathbb{P}$ beide Zahlen teilt, dann auch y (Differenz) und z (Summe) und somit x.
Aus $x^2 + y^2 = z^2$ folgt

$$\left(\frac{x}{2}\right)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2}.$$

Wegen der Teilerfremdheit sind nach Satz 1.17 auf Seite 15 beide Zahlen selbst Quadrate. Also gibt es ein $a \in \mathbb{N}$ und ein $b \in \mathbb{N}$ mit

$$\frac{z+y}{2} = a^2 \qquad \text{und} \qquad \frac{z-y}{2} = b^2.$$

Sofort folgen $z = a^2 + b^2$, $y = a^2 - b^2$, $a > b$ und $(a,b) = 1$.
Außerdem ergibt sich aus $x^2 + y^2 = z^2$, dass $x = 2ab$ sein muss.
Zuguterletzt ist

$$a + b \equiv a^2 + b^2 \bmod 2 \equiv z \bmod 2 \equiv 1 \bmod 2.$$

(ii) „⊇“
Seien umgekehrt $a' \in \mathbb{N}$ und $b' \in \mathbb{N}$ mit $a' > b'$, $a' + b' \equiv 1 \bmod 2$ und $(a', b') = 1$.
Seien $x' := 2a'b'$, $y' := a'^2 - b'^2$ und $z' := a'^2 + b'^2$.
Dann gilt $x' \in \mathbb{N}$, $y' \in \mathbb{N}$ wegen $a' > b'$, $z' \in \mathbb{N}$, $2|x'$ wegen $x' = 2a'b'$ und

$$\begin{aligned} x'^2 + y'^2 &= (2a'b')^2 + \left(a'^2 - b'^2\right)^2 = 4a'^2b'^2 + a'^4 - 2a'^2b'^2 + b'^4 \\ &= a'^4 + 2a'^2b'^2 + b'^4 = \left(a'^2 + b'^2\right)^2 = z'^2. \end{aligned}$$

Sei $d' := (x', y')$. Dann teilt d'^2 auch z'^2 und deshalb teilt d' auch z'. Wegen $d'|y'$ und $d'|z'$ teilt d' auch die Differenz und die Summe von y' und z'. Das heißt

$$d'|2a'^2 \qquad \text{und} \qquad d'|2b'^2.$$

Wegen $(a', b') = 1$ folgt $d'|2$, was $d' \in \{1, 2\}$ bewirkt. Nun folgt aus $a' + b' \equiv 1 \bmod 2$ aber $y' = a'^2 - b'^2 \equiv 1 \bmod 2$ und mit $d'|y'$ bleibt nur noch $d' = 1$. □

Die zulässigen Tripel $(x, y, z)^T \in \mathbb{N}^3$ und die Paare $(a, b)^T \in \mathbb{N}^2$ sind einander bijektiv zugeordnet.

Die ersten $(a,b)^T \in \mathbb{N}^2$ ergeben folgende primitiven phythagoräische Tripel

a	b	x	y	z
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25

Die „diophantische Gleichung“ $x^2 + y^2 = z^2$ hat demnach unendlich viele Lösungen in $\mathbb{N}^3$.

Zu den ganz großen Problemen der Mathematik gehörte hingegen die

FERMAT–Vermutung

(„großer FERMAT“, englisch: “FERMAT’s last theorem” — Pierre de FERMAT, 1601–1655)

BEHAUPTUNG: *Für alle* $n \in \mathbb{N} \setminus \{1,2\}$ *besitzt die Gleichung* $x^n + y^n = z^n$ *keine Lösung* $(x,y,z)^T \in \mathbb{N}^3$.

In den etwa 350 Jahren ihrer Geschichte haben sich fast alle namhaften Mathematiker ernsthaft um einen Beweis der FERMAT–Vermutung bemüht. Insbesondere die algebraische Zahlentheorie wurde durch die Arbeit am FERMATschen Problem entscheidend vorangetrieben. Erst 1995 gelang Andrew WILES der vollständige Beweis der Vermutung.

Falls die Unlösbarkeit der FERMATschen Gleichung für ein $n \in \mathbb{N} \setminus \{1,2\}$ bewiesen ist, dann folgt sie wegen $a^{mn} = (a^m)^n$ für alle $m \in \mathbb{N}$ und alle $a \in \mathbb{Z}$ auch für jedes Vielfache von n. Es ist somit für die Unlösbarkeit ausreichend, die Exponenten $n = 4$ und $n = p \in \mathbb{P} \setminus \{2\}$ zu untersuchen. Der Fall $n = 4$ ist nach FERMAT elementar zugänglich, während der Fall $n = p \in \mathbb{P} \setminus \{2\}$ algebraische Hilfsmittel erfordert. Ein Hinweis:
Sind $p \in \mathbb{P} \setminus \{2\}$ und $\xi := \exp\left(\frac{2\pi \mathrm{i}}{p}\right) = \cos\left(\frac{2\pi}{p}\right) + \mathrm{i} \cdot \sin\left(\frac{2\pi}{p}\right)$, so gilt für alle $x \in \mathbb{Z}$ und alle $y \in \mathbb{Z}$

$$x^p + y^p = (x+y) \cdot (x+\xi y) \cdot \left(x+\xi^2 y\right) \cdot \ldots \cdot \left(x+\xi^{p-1} y\right) = \prod_{j=0}^{p-1} \left(x+\xi^j y\right).$$

Es wird daher nützlich sein, den „Kreisteilungskörper“ $\mathbb{Q}(\xi)$ zu untersuchen.

SATZ 4.3 (Satz von FERMAT)
BEHAUPTUNG: *Die Gleichung* $x^4 + y^4 = z^4$ *besitzt keine Lösung* $(x,y,z)^T \in \mathbb{N}^3$.

BEWEIS:

(i) Definition von z_0
Es reicht, die Unlösbarkeit der Gleichung

$$x^4 + y^4 = z^2 \qquad (\ast)$$

mit $(x, y, z)^T \in \mathbb{N}^3$ zu zeigen.
Annahme: $(\ast)$ ist in $\mathbb{N}^3$ lösbar.
Sei $z_0 := \min\{\, z \in \mathbb{N} \,;\, \exists\, x \in \mathbb{N}, \exists\, y \in \mathbb{N} \text{ mit } x^4 + y^4 = z^2\}$ die kleinste Zahl, zu der es $x \in \mathbb{N}$ und $y \in \mathbb{N}$ mit $(\ast)$ gibt.
Seien $x \in \mathbb{N}$ und $y \in \mathbb{N}$ mit $x^4 + y^4 = z_0^2$. Es muss $(x, y) = 1$ gelten, da sonst in $(\ast)$ gekürzt werden könnte, was zu einem kleineren z führen würde. Insbesondere ist x oder y ungerade, also ist

$$z_0^2 = x^4 + y^4 \equiv 1 \bmod 4 \qquad \text{oder} \qquad z_0^2 = x^4 + y^4 \equiv 2 \bmod 4.$$

$z_0^2 \equiv 2\,(4)$ tritt nicht ein. Bleibt

$$z_0 \equiv 1\,(2) \qquad \text{und oBdA} \qquad x \equiv 0\,(2) \quad \wedge \quad y \equiv 1\,(2)\,.$$

(ii) Anwenden von Satz 4.2
Auf $(\ast)$ kann Satz 4.2 auf Seite 66 angewandt werden.
Es gibt ein $a \in \mathbb{N}$ und ein $b \in \mathbb{N}$ mit $a > b$, $(a, b) = 1$, $a + b \equiv 1\,(2)$,

$$x^2 = 2ab, \qquad y^2 = a^2 - b^2 \qquad \text{und} \qquad z_0 = a^2 + b^2.$$

Aus $a \equiv 0\,(2)$ und $b \equiv 1\,(2)$ folgte $y^2 \equiv 3\,(4)$, was nicht sein kann. Also gibt es ein $c \in \mathbb{N}$ mit

$$a \equiv 1\,(2) \qquad \text{und} \qquad b = 2c.$$

(iii) Konstruktion von z_1
Aus (ii) ergibt sich $\left(\frac{x}{2}\right)^2 = \frac{x^2}{4} = ac$ und $(a, c) = 1$, also gibt es ein $z_1 \in \mathbb{N}$ und ein $d \in \mathbb{N}$ mit

$$a = z_1^2, \qquad c = d^2, \qquad (z_1, d) = 1 \qquad \text{und} \qquad y^2 = a^2 - b^2 = z_1^4 - 4d^4.$$

Also ist

$$\left(2d^2\right)^2 + y^2 = \left(z_1^2\right)^2, \qquad (\text{✺})$$

wobei $2d^2$, y und z_1^2 paarweise teilerfremd sind.

(iv) Beweis von $z_1 < z_0$
Auf (✺) wird erneut Satz 4.2 angewandt und es gibt ein $a_1 \in \mathbb{N}$ und ein $b_1 \in \mathbb{N}$ mit $a_1 > b_1$, $(a_1, b_1) = 1$, $a_1 + b_1 \equiv 1\,(2)$,

$$2d^2 = 2a_1b_1, \qquad y = a_1^2 - b_1^2 \qquad \text{und} \qquad z_1^2 = a_1^2 + b_1^2.$$

Wegen $d^2 = a_1b_1$ und $(a_1, b_1) = 1$ gibt es ein $x_1 \in \mathbb{N}$ und ein $y_1 \in \mathbb{N}$ mit

$$a_1 = x_1^2, \qquad b_1 = y_1^2 \qquad \text{und} \qquad x_1^4 + y_1^4 = z_1^2.$$

Aber wegen $0 < z_1 \leq z_1^2 = a \leq a^2 < a^2 + b^2 = z_0$ ist somit eine kleinere Zahl als z_0 gefunden, die $(\ast)$ löst. Dies bedeutet einen Widerspruch. □

Die hier benutzte Methode, zu einer angenommenen Lösung eine kleinere zu konstruieren, geht auf FERMAT zurück und wird nach ihm „descendente infinie“ (Methode des „unendlichen Abstiegs“) genannt. Das Prinzip wird noch zweimal angewandt werden.

Als nächstes soll untersucht werden, welche Zahlen sich als Summe von zwei, drei oder mehr Quadraten schreiben lassen.

SATZ 4.4 (Satz von EULER über Summen von zwei Quadraten)
BEHAUPTUNG: *Für alle $n \in \mathbb{N}$ sind die folgenden Aussagen äquivalent*

(1) *Es gibt ein $x \in \mathbb{N}_0$ und ein $y \in \mathbb{N}_0$ mit $n = x^2 + y^2$.*

(2) *In der Primfaktorzerlegung von n treten alle Primteiler $p \in \mathbb{P}$ von n mit $p \equiv 3 \bmod 4$ in gerader Potenz auf.*

BEWEIS:

(i) $p|n$ und $p \equiv 3\,(4)$ $\implies$ $(x, y) \neq 1$
Sei $n \in \mathbb{N}$. Falls es ein $p \in \mathbb{P}$ mit $p \equiv 3\,(4)$ und $p|n$ gibt, gibt es kein $(x, y)^T \in \mathbb{Z}^2$ mit

$$n = x^2 + y^2 \quad \text{und} \quad (x, y) = 1.$$

Annahme: Es gibt ein $q \in \mathbb{P}$, ein $x \in \mathbb{Z}$ und ein $y \in \mathbb{Z}$ mit $q \equiv 3\,(4)$, $q|n$, $(x, y) = 1$ und $n = x^2 + y^2$.
Wegen $n \geq 3$ und $(x, y) = 1$ kann oBdA $x \geq 1$ und $y \geq 1$ angenommen werden. Wegen $q|n$ und $(x, y) = 1$ gelten $x \not\equiv 0\,(q)$ und $y \not\equiv 0\,(q)$.
Nach Satz 3.2 auf Seite 42 existiert ein $z \in \mathbb{Z}$ mit $y \equiv zx\,(q)$, also

$$x^2 \cdot \left(1 + z^2\right) \equiv x^2 + y^2\,(q) \equiv 0\,(q)$$

und somit $1 + z^2 \equiv 0\,(q)$. Damit ist $\left(\dfrac{-1}{q}\right) = 1$, also ist $q \equiv 1\,(4)$ nach dem ersten Ergänzungsgesetz 3.13 1. auf Seite 53, was einen Widerspruch bedeutet.

(ii) (1) $\implies$ (2)
Es gebe ein $x \in \mathbb{N}_0$ und ein $y \in \mathbb{N}_0$ mit $n = x^2 + y^2$.
Seien $d := (x, y)$, $x' := \frac{x}{d}$, $y' := \frac{y}{d}$ und $n' := x'^2 + y'^2$. Dann sind $(x', y') = 1$ und

$$n = d^2 \left(x'^2 + y'^2\right) = d^2 n'. \qquad (\bigstar)$$

n' besitzt also eine Darstellung $n' = x'^2 + y'^2$ mit $(x', y') = 1$.
Ist $q \in \mathbb{P}$ mit $q \equiv 3 \bmod 4$ ein Primteiler von n, so kann q nach (i) n' nicht teilen.
Sei a der Exponent von q in der kanonischen Zerlegung von d. Dann teilt q nach ($\bigstar$) die Zahl n in genau $2a$–ter Potenz.

(iii) Multiplikativität der Darstellbarkeit
Sind $n_1 \in \mathbb{N}$ und $n_2 \in \mathbb{N}$ darstellbar, so ist auch $n_1 n_2$ darstellbar, wie die für alle $(x_1, x_2, y_1, y_2)^T \in \mathbb{Z}^4$ gültige Identität

$$\left(x_1^2 + y_1^2\right) \cdot \left(x_2^2 + y_2^2\right) = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2$$

zeigt. Für die Richtung von (2) nach (1) reicht es danach aus, für jedes $p \in \mathbb{P}$ mit $p \equiv 1\,(4)$ die Lösbarkeit von $p = x^2 + y^2$ nachzuweisen.
Denn $2 = 1^2 + 1^2$ und für alle $p \in \mathbb{P}$ mit $p \equiv 3\,(4)$ ist $p^2 = 0 + p^2$.

(iv) (2) $\Longrightarrow$ (1)
Sei $p \in \mathbb{P}$ mit $p \equiv 1\,(4)$.

1. Es gibt ein $m \in \mathbb{N}$, ein $x' \in \mathbb{N}_0$ und ein $y' \in \mathbb{N}_0$ mit $m < p$, $p \nmid (x'y')$ und
$$x'^2 + y'^2 = mp.$$
Denn wegen $p \equiv 1\,(4)$ ist $\left(\frac{-1}{p}\right) = 1$, also existiert ein $z \in \mathbb{N}_0$ und ein $m \in \mathbb{Z}$ mit $z \leq \frac{p-1}{2}$ und $z^2 + 1 = mp$. Wegen $0 < 1 + z^2 < p^2$ ist $0 < m < p$.

2. Seien
$$\mathcal{M} := \left\{ n \in \mathbb{N}\,;\, n < p \text{ und } \exists\, x \in \mathbb{N}_0, \exists\, y \in \mathbb{N}_0 \text{ mit } x^2 + y^2 = np \right\}$$
und $m_0 := \min \mathcal{M}$.
Ist $m_0 = 1$, so folgt die Behauptung.
Nach der FERMATschen Idee wird im Fall $m_0 > 1$ ein kleineres $m_1 \in \mathcal{M}$ konstruiert.
Es werde also $m_0 > 1$ angenommen.
Wegen $m_0 \in \mathcal{M}$ gibt es ein $x \in \mathbb{N}_0$ und ein $y \in \mathbb{N}_0$ mit $x^2 + y^2 = m_0 p$.
Insbesondere folgt
$$m_0 \nmid x \qquad \text{oder} \qquad m_0 \nmid y.$$
Denn aus $m_0 | x$ und $m_0 | y$ folgte $m_0^2 | (x^2 + y^2) = m_0 p$. Das hieße $m_0 | p$, was wegen $1 < m_0 < p$ nicht eintreten kann.

3. Da $m_0 > 1$ ist, lassen sich ganze $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ finden, so dass für
$$x_1 := x - a m_0 \qquad \text{und} \qquad y_1 := y - b m_0$$
$\max\{|x_1|, |y_1|\} \leq \frac{m_0}{2}$ ist. (Man nehme die absolut kleinsten Reste von x und y modulo m_0.) Also sind
$$0 < x_1^2 + y_1^2 \leq 2\left(\frac{m_0}{2}\right)^2 < m_0^2 \qquad \text{und} \qquad x_1^2 + y_1^2 \equiv x^2 + y^2\,(m_0) \equiv 0\,(m_0)\,.$$
Insbesondere existiert ein $m_1 \in \mathbb{N}$ mit
$$x_1^2 + y_1^2 = m_1 m_0 \qquad \text{und} \qquad 0 < m_1 < m_0.$$

4. (iii), $m_0 p = x^2 + y^2$ und die letzte Gleichung ergeben

$$m_0^2 m_1 p = m_0 p \cdot m_1 m_0 = \left(x^2 + y^2\right) \cdot \left(x_1^2 + y_1^2\right) = \left(x x_1 + y y_1\right)^2 + \left(x y_1 - x_1 y\right)^2 .$$

Wegen

$$x x_1 + y y_1 = x \cdot (x - a m_0) + y \cdot (y - b m_0) = \underbrace{x^2 + y^2}_{= m_0 p} - m_0 \cdot (a x + b y)$$

und

$$x y_1 - x_1 y = x \cdot (y - b m_0) - y \cdot (x - a m_0) = \underbrace{x y - x y}_{= 0} - m_0 \cdot (b x - a y)$$

folgt daraus mit $x' := |p - a x - b y|$ und $y' := |a y - b x|$, dass

$$m_1 p = x'^2 + y'^2 \qquad \text{ist. Also ist} \qquad m_1 \in \mathcal{M}.$$

Wegen $0 < m_1 < m_0$ steht dies im Widerspruch zur Minimalität von m_0. □

Der Fall dreier Summanden ist wesentlich schwieriger und kann hier nur knapp diskutiert werden. Der Hauptgrund dafür ist, dass keine „Multiplikationsformel“ der Art

$$\left(x_1^2 + y_1^2 + z_1^2\right) \cdot \left(x_2^2 + y_2^2 + z_2^2\right) = L_1^2 \left(x_1, \ldots, z_2\right) + L_2^2 \left(x_1, \ldots, z_2\right) + L_3^2 \left(x_1, \ldots, z_2\right)$$

(L_1, L_2 und L_3 Polynome zweiten Grades in den sechs Variablen) existiert. Adolf HURWITZ (1859–1919) hat gezeigt, dass es solche Formeln nur für 1, 2, 4 oder 8 Summanden gibt.

SATZ 4.5 (Satz von LEGENDRE über Summen von drei Quadraten)
BEHAUPTUNG: *Für alle $n \in \mathbb{N}$ sind folgende Aussagen äquivalent*

(1) *Es gibt ein $(x, y, z)^T \in \mathbb{N}_0^3$ mit $n = x^2 + y^2 + z^2$.*

(2) $n \notin \left\{ 4^a \cdot (8b + 7) \in \mathbb{N} \,;\, a \in \mathbb{N}_0 \text{ und } b \in \mathbb{N}_0 \right\}$.

Die Richtung von (2) nach (1) erfordert einiges aus der Theorie der ternären quadratischen Formen

$$Q\left(x_1, x_2, x_3\right) = \sum_{j,k=1}^{3} a_{jk}\, x_j x_k \qquad \text{mit } a_{jk} \in \mathbb{Z}$$

sowie den Satz von DIRICHLET (1805–1859), dass in jeder reduzierten Restklasse $a + k\mathbb{Z}$ mit $k \in \mathbb{N}$, $a \in \mathbb{Z}$ und $(a, k) = 1$ unendlich viele Primzahlen liegen.

BEWEIS: (von **(1)** $\Longrightarrow$ **(2)**)
Die Richtung (1) $\Longrightarrow$ (2) ist einfach.
Annahme: Es gibt ein $n \in \mathbb{N}$, ein $(x_1, x_2, x_3)^T \in \mathbb{N}_0^3$, ein $a \in \mathbb{N}_0$ und ein $b \in \mathbb{N}_0$ mit

$$n = 4^a \cdot (8b + 7) = x_1^2 + x_2^2 + x_3^2. \qquad (\star)$$

Seien $(y_1, y_2, y_3)^T \in \mathbb{N}_0^3$ und $(a_1, a_2, a_3)^T \in \mathbb{N}_0^3$ mit

$$x_j = 2^{a_j} y_j \qquad \text{und} \qquad 2 \nmid y_j \qquad \text{für alle } j \in \{1, 2, 3\}. \qquad (\star\star)$$

OBdA gilt $a_1 \leq a_2 \leq a_3$.
Für jedes ungerade $y \in \mathbb{Z}$ gilt $y^2 \equiv 1\,(8)$, denn für alle $z \in \mathbb{Z}$ ist

$$(2z + 1)^2 = 4z^2 + 4z + 1 = 4z \cdot (z + 1) + 1 = 8 \cdot \frac{z \cdot (z + 1)}{2} + 1 \equiv 1 \bmod 8.$$

Also gilt $y_1^2 \equiv 1\,(8)$, $y_2^2 \equiv 1\,(8)$ und $y_3^2 \equiv 1\,(8)$. Dann folgt

$$0 \leq a = a_1 \leq a_2 \leq a_3. \qquad (\star\star\star)$$

Denn die Annahme $a_1 > a$ ergibt unmittelbar einen Widerspruch, da wegen $(\star)$ sonst $4^{a+1} | n$ gelten müsste und aus $a_1 < a$ ergäbe sich mit $(\star)$

$$\frac{n}{4^{a_1}} = 4^{a - a_1} \cdot (8b + 7) = y_1^2 + 2^{2 \cdot (a_2 - a_1)} y_2^2 + 2^{2 \cdot (a_3 - a_1)} y_3^2.$$

Die linke Seite wäre in $(0 + 8\mathbb{Z}) \cup (4 + 8\mathbb{Z})$. Der zweite und dritte Summand rechts sind kongruent zu 0, 1 oder 4 modulo 8, die rechte Seite wäre also kongruent zu 1, 2, 3, 5 oder 6 modulo 8, was nicht zusammenpasst.

Aus $(\star)$, $(\star\star)$ und $(\star\star\star)$ erhält man

$$n_1 := 8b + 7 = y_1^2 + 2^{b_2} y_2^2 + 2^{b_3} y_3^2$$

mit $b_2 := 2a_2 - 2a$, $b_3 := 2a_3 - 2a$, $2 \nmid y_j$ für alle $j \in \{1, 2, 3\}$ und $0 \leq b_2 \leq b_3$.
Man überzeugt sich durch Verfolgen aller Möglichkeiten (siehe oben), dass die rechte Seite nicht kongruent zu 7 modulo 8 sein kann. □

Am Beispiel

$$3 \cdot 5 = \left(1^2 + 1^2 + 1^2\right) \cdot \left(2^2 + 1^2 + 0^2\right) = 15 = 4^0 \cdot (8 \cdot 1 + 7)$$

sieht man, dass die Eigenschaft, Summe dreier Quadrate zu sein, nicht „multiplikativ“ ist.

Das Problem mit vier oder mehr Summanden hat eine einfache Lösung.

SATZ 4.6 (Vier–Quadrate–Satz von LAGRANGE)
BEHAUPTUNG: *Jedes $n \in \mathbb{N}$ besitzt eine Darstellung*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2 \qquad \textit{mit } (x_1, x_2, x_3, x_4)^T \in \mathbb{N}_0^4.$$

BEWEIS:

(i) Die LAGRANGEsche Identität
Die wichtige Multiplikationsformel lautet hier

$$\begin{aligned}&\left(x_1^2+x_2^2+x_3^2+x_4^2\right)\cdot\left(y_1^2+y_2^2+y_3^2+y_4^2\right)\\ &\quad= \quad (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\ &\qquad +(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2\,.\end{aligned}$$

für alle $(x_1,x_2,x_3,x_4)^T\in\mathbb{Z}^4$ und alle $(y_1,y_2,y_3,y_4)^T\in\mathbb{Z}^4$.
Wegen $2=1^2+1^2+0^2+0^2$ reicht es also aus, den Beweis für ungerade $p\in\mathbb{P}\setminus\{2\}$ zu führen.

(ii) Existenz und Definition von m_0
Sei $p\in\mathbb{P}\setminus\{2\}$. Dann sind die Zahlen

$$a^2 \qquad \text{mit } a\in\mathbb{Z} \text{ und } 0\le a\le\frac{p-1}{2}$$

und

$$-1-b^2 \qquad \text{mit } b\in\mathbb{Z} \text{ und } 0\le b\le\frac{p-1}{2}$$

jeweils paarweise inkongruent modulo p. Es muss also, da insgesamt $2\cdot\left(1+\frac{p-1}{2}\right)>p$ Zahlen zur Verfügung stehen, eine aus der ersten zu einer aus der zweiten Menge modulo p kongruent sein. (Schubfachschluss, auch „DIRICHLETsches Schubfachprinzip“ genannt, englisch “pigeonhole principle”!)
Es gibt also $a\in\mathbb{N}_0$, $b\in\mathbb{N}_0$ und $m\in\mathbb{N}_0$ mit

$$0^2+1^2+a^2+b^2=mp \qquad \text{und} \qquad 0<mp\le 1+2\cdot\left(\frac{p-1}{2}\right)^2<p^2,$$

also $0<m<p$. Demnach ist

$$\mathcal{M}:=\left\{n\in\mathbb{N}\,;n<p \text{ und } \exists\, x_1\in\mathbb{N}_0,\exists\, x_2\in\mathbb{N}_0,\exists\, x_3\in\mathbb{N}_0,\exists\, x_4\in\mathbb{N}_0 \text{ mit } \sum_{j=1}^{4}x_j^2=np\right\}$$

nicht leer und es gibt $m_0:=\min\mathcal{M}$, $x_1\in\mathbb{N}_0$, $x_2\in\mathbb{N}_0$ $x_3\in\mathbb{N}_0$ und $x_4\in\mathbb{N}_0$ mit

$$x_1^2+x_2^2+x_3^2+x_4^2=m_0p. \qquad (\maltese)$$

Ist $m_0=1$, so ist der Beweis geführt.
Es werde also $m_0>1$ angenommen.

(iii) $m_0 \neq 1$ ist ungerade
Angenommen, m_0 sei gerade. Dann wären

1. alle x_j gerade oder
2. oBdA x_1, x_2 gerade und x_3, x_4 ungerade oder
3. alle x_j ungerade.

Im 2. Fall wären

$$y_1 := x_1 + x_2, \quad y_2 := x_1 - x_2, \quad y_3 := x_3 + x_4 \quad \text{und} \quad y_4 := x_3 - x_4$$

sämtlich gerade, ebenso wie im 1. und im 3. Fall.
Aus (✺) folgte

$$\frac{m_0}{2} \cdot p = \left(\frac{y_1}{2}\right)^2 + \left(\frac{y_2}{2}\right)^2 + \left(\frac{y_3}{2}\right)^2 + \left(\frac{y_4}{2}\right)^2$$

im Widerspruch zur Minimalität von m_0. Also ist $m_0 \geq 3$ ungerade.

(iv) Konstruktion von m_1, $1 < m_1 < m_0$
Es gibt ein $j_0 \in \{1, 2, 3, 4\}$, für das x_{j_0} nicht durch m_0 teilbar ist, denn andernfalls folgte aus (✺) $m_0 | p$. Zur Konstruktion eines kleineren $m_1 \in \mathcal{M}$ werde wie im Beweis zu Satz 4.4 auf Seite 70 für alle $j \in \{1, 2, 3, 4\}$

$$y_j = x_j - a_j m_0 \qquad \text{mit } |y_j| < \frac{m_0}{2}$$

und $a_j \in \mathbb{Z}$ gesetzt (das strenge $<$ ist wegen $m_0 \equiv 1\,(2)$ möglich). Dann gilt

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4 \cdot \left(\frac{m_0}{2}\right)^2 = m_0^2.$$

Aus (✺) ergibt sich

$$\begin{aligned} y_1^2 + y_2^2 + y_3^2 + y_4^2 = {} & x_1^2 - 2a_1x_1m_0 + a_1^2m_0 + x_2^2 - 2a_2x_2m_0 + a_2^2m_0 \\ & + x_3^2 - 2a_3x_3m_0 + a_3^2m_0 + x_4^2 - 2a_4x_4m_0 + a_4^2m_0 \\ = {} & m_0 \cdot \left(p + \sum_{j=1}^{4} \left(a_j^2 - 2a_jx_j\right)\right) \\ = {} & m_0 \cdot m_1 \end{aligned}$$

mit $m_1 := p + \sum_{j=1}^{4} \left(a_j^2 - 2a_jx_j\right) > 0$, wegen $y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0$ und $m_0 > 0$.
Insbesondere gilt $0 < m_0 \cdot m_1 = y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2$, was zu $0 < m_1 < m_0$ führt.

(v) $m_1 \in \mathcal{M}$
Multiplikation von (✺) und der letzten Gleichung gemäß (i) zeigt die Existenz von $z_1 \in \mathbb{Z}$, $z_2 \in \mathbb{Z}$, $z_3 \in \mathbb{Z}$ und $z_4 \in \mathbb{Z}$ mit

$$m_0^2 m_1 p = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

wobei die z_j für alle $j \in \{1,2,3,4\}$ wie in (i) angegeben aus den x_k und den y_ℓ mit $k \in \{1,2,3,4\}$ und $\ell \in \{1,2,3,4\}$ berechnet werden. Zum Beispiel ist

$$z_1 = \sum_{1\le j\le 4} x_j y_j = \sum_{1\le j\le 4} x_j \cdot (x_j - a_j m_0) \equiv \sum_{1\le j\le 4} x_j^2 \bmod m_0 \equiv 0 \bmod m_0.$$

Ebenso ergeben sich $z_2 \equiv 0\,(m_0)$, $z_3 \equiv 0\,(m_0)$ und $z_4 \equiv 0\,(m_0)$.
Also gibt für alle $j \in \{1,2,3,4\}$ ein $c_j \in \mathbb{N}_0$ mit

$$|z_j| = m_0 \cdot c_j.$$

In $m_0^2 m_1 p = z_1^2 + z_2^2 + z_3^2 + z_4^2$ eingesetzt, ergibt das

$$m_1 p = c_1^2 + c_2^2 + c_3^2 + c_4^2,$$

also $m_1 \in \mathcal{M}$ mit $m_1 < m_0$, was der Minimalität von m_0 widerspricht. □

Der Vier–Quadrate–Satz von LAGRANGE kann als Spezialfall eines allgemeineren Problems aufgefasst werden.

WARINGsches Problem

(Edward WARING, 1734–1798)

Existiert zu jedem $k \in \mathbb{N}$ ein $g\,(k) \in \mathbb{N}$, so dass jedes $n \in \mathbb{N}$ als Summe $\sum\limits_{j=1}^{g(k)} x_j^k$ von $g\,(k)$ vielen k–ten Potenzen mit $x_j \in \mathbb{N}_0$ für alle $j \in \mathbb{N}$ mit $j \le g\,(k)$ dargestellt werden kann?

Der erste allgemeine Beweis für die Existenz eines $g\,(k)$s für alle $k \in \mathbb{N}$ wurde 1909 von David HILBERT (1862–1943) gegeben. Unter den verschiedenen, sämtlich nicht elementaren Lösungswegen hat sich Folgender als am ergiebigsten erwiesen. Sei für $k \in \mathbb{N}$ und $\alpha \in \mathbb{R}$

$$S_k\,(\alpha) := \sum_{m=1}^{\lfloor n^{1/k} \rfloor} \exp\left(2\pi \mathrm{i} \cdot \alpha m^k\right).$$

Dann gilt für alle $\ell \in \mathbb{N}$ und alle $n \in \mathbb{N}$

$$\begin{aligned} R_{\ell,k}(n) &:= \#\left\{ (x_1,\ldots,x_\ell)^T \in \mathbb{N}^\ell \,;\, \sum_{j=1}^{\ell} x_j^k = n \right\} \\ &= \int_0^1 \left(S_k\,(\alpha)\right)^\ell \cdot \exp\left(-2\pi \mathrm{i} \cdot \alpha n\right) \mathrm{d}\alpha. \end{aligned}$$

Eine genaue Analyse des Integrals führt für hinreichend großes $\ell \in \mathbb{N}$ mit $\ell \ge \ell_0\,(k) \in \mathbb{N}$ zu einer Näherungsformel für $R_{\ell,k}(n)$ und damit zur Lösung des WARINGschen Problems.

Kapitel 5: Zahlentheoretische Funktionen

Definition 5.1 (Zahlentheoretische Funktionen)

a) Eine Abbildung $f : \mathbb{N} \to \mathbb{C}$ heißt **zahlentheoretische Funktion.** (Kurz: zF)
Die **Menge aller zahlentheoretischen Funktionen** wird mit $\mathcal{F}$ bezeichnet.

b) Eine zF $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ heißt **multiplikativ**, wenn

(i) $f(1) = 1$ und

(ii) $f(mn) = f(m) \cdot f(n)$ für alle $m \in \mathbb{N}$ und alle $n \in \mathbb{N}$ mit $(n, m) = 1$ sind.

f heißt **vollständig multiplikativ**, wenn $f(1) = 1$ und $f(mn) = f(m) \cdot f(n)$ für alle $m \in \mathbb{N}$ und alle $n \in \mathbb{N}$ sind.

c) Eine zF $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ heißt **additiv**, wenn $f(mn) = f(m) + f(n)$ für alle $m \in \mathbb{N}$ und alle $n \in \mathbb{N}$ mit $(n, m) = 1$ ist.

f heißt **vollständig additiv**, wenn $f(mn) = f(m) + f(n)$ für alle $m \in \mathbb{N}$ und alle $n \in \mathbb{N}$ gilt.

Bemerkungen

(1) Die erste Bedingung für die Multiplikativität einer zF $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ kann auch durch

$$\text{„}\exists\, n_0 \in \mathbb{N} \text{ mit } f(n_0) \neq 0\text{“}$$

ersetzt werden. Denn mit der zweiten Bedingung folgt daraus

$$f(n_0) = f(n_0 \cdot 1) = f(n_0) \cdot f(1),$$

also $f(1) = 1$.

(2) Während es sich bei der Multiplikativität als günstig erweist, die Null–Funktion auszuschließen, ist dies bei der Additivität nicht nötig.

(3) Multiplikative Funktionen $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ sind wegen

$$f(p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}) = f(p_1^{a_1}) \cdot \ldots \cdot f(p_k^{a_k})$$

für $k \in \mathbb{N}$, beliebige $a_j \in \mathbb{N}_0$ und paarweise verschiedene $p_j \in \mathbb{P}$ mit $j \in \mathbb{N}$ und $j \leq k$ durch ihre Werte auf den Primzahlpotenzen vollständig bestimmt, vollständig multiplikative durch ihre Werte an den Primzahlen.

(4) Ist $g : \mathbb{N} \to \mathbb{C}$ additiv, dann ist $f := \exp \circ g$ multiplikativ.

Definition 5.2 (σ_α, σ, τ, ω, Ω, $\mathbb{1}$ und ε)

a) Für $\mathcal{D}: \left\{ \begin{array}{ccl} \mathbb{N} & \to & \{\mathcal{C}\,; \mathcal{C} \subseteq \mathbb{N}\} \\ n & \mapsto & \mathcal{D}(n) := \{d \in \mathbb{N}\,; d|n\} \end{array} \right\}$ und eine zF $f: \left\{ \begin{array}{ccl} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ wird

$$\sum_{d|n} f(d) := \sum_{d \in \mathcal{D}(n)} f(d)$$

gesetzt.

b) Für alle $\alpha \in \mathbb{R}$ wird

$$\sigma_\alpha: \left\{ \begin{array}{ccl} \mathbb{N} & \to & \mathbb{R} \\ n & \mapsto & \sigma_\alpha(n) := \displaystyle\sum_{d|n} d^\alpha \end{array} \right\}$$

als **Teilersummen–Funktion zum Exponent α** bezeichnet. Insbesondere heißen

$\sigma := \sigma_1$ **Teilersummen–Funktion** und
$\tau := \sigma_0$ **Teileranzahl–Funktion**.

c) Seien

$$\omega: \left\{ \begin{array}{ccl} \mathbb{N} & \to & \mathbb{N}_0 \\ n & \mapsto & \omega(n) := \#\{p \in \mathbb{P}\,; p|n\} \end{array} \right\}$$

die **Primteileranzahl–Funktion** und

$$\Omega: \left\{ \begin{array}{ccl} \mathbb{N} & \to & \mathbb{N}_0 \\ n & \mapsto & \Omega(n) := \#\left\{(p,j)^T \in \mathbb{P} \times \mathbb{N}\,; p^j \middle| n\right\} \end{array} \right\}$$

die **Primfaktorenanzahl–Funktion**.

d) Seien

$$\mathbb{1}: \left\{ \begin{array}{ccl} \mathbb{N} & \to & \mathbb{N}_0 \\ n & \mapsto & \mathbb{1}(n) := 1 \end{array} \right\}$$

die **Konstante 1–Funktion** und

$$\varepsilon: \left\{ \begin{array}{ccl} \mathbb{N} & \to & \mathbb{N}_0 \\ n & \mapsto & \varepsilon(n) := \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & \text{falls } n = 1 \\ 0, & \text{falls } n \neq 1 \end{cases} \end{array} \right\}$$

die **1–Erkennungs–Funktion**.

Folgerung 5.3
Für alle $\alpha \in \mathbb{R}$ ist σ_α multiplikativ, aber nicht vollständig multiplikativ.
ω ist additiv, aber nicht vollständig additiv. Ω ist vollständig additiv.
$\mathbb{1}$ und ε sind vollständig multiplikativ.

Ist $n \in \mathbb{N}$ mit der Primfaktorzerlegung $n = \prod_{j=1}^{r} p_j^{\alpha_j}$, so gilt

$$\omega(n) = r \qquad \text{und} \qquad \Omega(n) = \sum_{j=1}^{r} \alpha_j.$$

Die erste Aussage ergibt sich unmittelbar aus dem späteren Satz 5.9 auf Seite 83. Zur Übung werde der Beweis hier ausgeführt. Die anderen Aussagen sieht man unmittelbar ein.

BEWEIS: (für σ_α mit $\alpha \in \mathbb{N}$)
Seien $\alpha \in \mathbb{R}$, $m \in \mathbb{N}$ und $n \in \mathbb{N}$ mit $(m,n) = 1$. Dann sind die Paare $(d,k)^T \in \mathbb{N}^2$ mit $d|m$ und $k|n$ den Teilern $\ell := dk$ von mn bijektiv zugeordnet und es gilt

$$\begin{aligned}\sigma_\alpha(mn) &= \sum_{\ell|mn} \ell^\alpha = \sum_{d|m} \sum_{k|n} (dk)^\alpha \\ &= \sum_{d|m} d^\alpha \cdot \sum_{k|n} k^\alpha = \sigma_\alpha(m) \cdot \sigma_\alpha(n).\end{aligned}$$

Für alle $p \in \mathbb{P}$ und alle $k \in \mathbb{N}_0$ ist

$$\sigma_\alpha\left(p^k\right) = \sum_{j=1}^{k} \left(p^k\right)^\alpha = 1 + p^\alpha + p^{2\alpha} + \ldots + p^{k\alpha} \neq 0.$$

Wegen

$$\begin{aligned}\sigma_\alpha\left(p^2\right) &= 1 + p^\alpha + p^{2\alpha} \qquad \text{und} \\ \sigma_\alpha(p) \cdot \sigma_\alpha(p) &= (1+p^\alpha) \cdot (1+p^\alpha) = 1 + 2p^\alpha + p^{2\alpha}\end{aligned}$$

für alle $p \in \mathbb{P}$ sieht man, dass σ_α nicht vollständig multiplikativ ist. □

Die folgenden zwei Bezeichnungen gehen auf die alten Griechen zurück. Die dritte Bezeichnung erschließt sich aus dem auf die Definition folgenden Satz.

Definition 5.4 (Vollkommene und befreundete Zahlen, MERSENNE–Zahlen)

a) Eine natürliche Zahl $n \in \mathbb{N}$ heißt **vollkommen** (oder **perfekt**), wenn

$$\sigma(n) = \sum_{d|n} d = 2n \qquad \text{ist.}$$

b) Zwei verschiedene natürliche Zahlen $n \in \mathbb{N}$ und $m \in \mathbb{N} \setminus \{n\}$ heißen **befreundet**, wenn

$$\sigma(n) - n = m \qquad \text{und} \qquad \sigma(m) - m = n \qquad \text{sind.}$$

c) Die Zahlen $M_p := 2^p - 1$ mit $p \in \mathbb{P}$ heißen **MERSENNE–Zahlen**.

Satz 5.5 (Geradene vollkommene Zahlen und Mersenne–Primzahlen)
Behauptung: **(1)** *(Euklid–Euler)*

Eine natürliche Zahl $n \in \mathbb{N}$ ist genau dann gerade und vollkommen, wenn es ein $k \in \mathbb{N}$ mit $n = 2^k \cdot \left(2^{k+1} - 1\right)$ und $2^{k+1} - 1 \in \mathbb{P}$ gibt.

(2) *(Marin Mersenne, 1588–1648)*

Ist $m \in \mathbb{N}$ mit $2^m - 1 \in \mathbb{P}$, so ist $m \in \mathbb{P}$ prim.

Bemerkung
Für alle $p \in \{2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127\}$ sind die M_p prim, für die übrigen $p \in \mathbb{P}$ mit $p < 500$ ist M_p zusammengesetzt. Seit 12. Juni 2009 sind siebenundvierzig prime Mersenne–Zahlen bekannt. Das am 12. Juni 2009 größte solche M_p gehört zu $p = 43\,112\,609$, hat 12 978 189 Dezimalstellen und ist zugleich die größte damals berechnete Primzahl. Man vermutet, dass es unendlich viele prime und unendlich viele zusammengesetzte Mersenne–Zahlen gibt.
Ob ungerade vollkommene Zahlen existieren, ist ein offenes Problem. Falls es welche gibt, müssen sie größer als 10^{150} sein.
Ebenso ist unbekannt, ob es unendlich viele Paare befreundeter Zahlen gibt.

Beweis:

(i) Zu (1), „$\Longleftarrow$“
Ist $k \in \mathbb{N}$ mit $p := 2^{k+1} - 1 \in \mathbb{P}$, so sieht man

$$\begin{aligned}\sigma\left(2^k \cdot \left(2^{k+1} - 1\right)\right) &= 1 + 2 + \ldots + 2^k + \left(1 + 2 + \ldots + 2^k\right) \cdot p \\ &= \left(2^{k+1} - 1\right) \cdot (p + 1) = \left(2^{k+1} - 1\right) \cdot 2^{k+1} = 2 \cdot 2^k \cdot \left(2^{k+1} - 1\right).\end{aligned}$$

Dies ist die Euklidsche Feststellung.

(ii) Zu (1), „$\Longrightarrow$“
Eine Zweierpotenz 2^k mit $k \in \mathbb{N}$ ist wegen $\sigma\left(2^k\right) = 1 + \ldots + 2^k = 2^{k+1} - 1 \neq 2 \cdot 2^k$ nicht vollkommen.
Seien also $n \in \mathbb{N}$, $k \in \mathbb{N}$ und $u \in \mathbb{N}$ mit

$$n = 2^k u \quad \text{ist vollkommen,} \qquad u \geq 3 \qquad \text{und} \qquad 2 \nmid u.$$

Dann folgt mit der Multiplikativität von σ

$$2^{k+1}u = 2n = \sigma(n) = \sigma\left(2^k\right) \cdot \sigma(u) = \left(2^{k+1} - 1\right) \cdot \sigma(u),$$

also

$$\sigma(u) = 2^{k+1}u \cdot \left(2^{k+1} - 1\right)^{-1} = u + \frac{u}{2^{k+1} - 1}. \qquad (*)$$

Da u und $\sigma(u)$ ganz sind, ist es auch $\frac{u}{2^{k+1}-1}$. Das heißt $2^{k+1} - 1$ und $\frac{u}{2^{k+1}-1}$ sind Teiler von u. Aus der Identität $(*)$ entnimmt man, dass u und $\frac{u}{2^{k+1}-1}$ die einzigen Teiler von u sind. Also ist $u \in \mathbb{P}$ Primzahl und $\frac{u}{2^{k+1}-1} = 1$.

(iii) Zu (2)
Seien $h \in \mathbb{N} \setminus \{1\}$ und $\ell \in \mathbb{N} \setminus \{1\}$. Dann ist

$$2^{h\ell} - 1 = \left(2^h - 1\right) \cdot \left(2^{h\cdot(\ell-1)} + 2^{h\cdot(\ell-2)} + \ldots + 2^h + 1\right)$$

zusammengesetzt. □

Definition 5.6 (MÖBIUS–Funktion und VON MANGOLDT–Funktion)

a) Die Funktion

$$\mu : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{Z} \\ n & \mapsto & \mu(n) := \begin{cases} (-1)^{\omega(n)}, & \text{falls } p^2 \nmid n \text{ für alle } p \in \mathbb{P} \text{ gilt} \\ 0, & \text{falls es ein } p \in \mathbb{P} \text{ mit } p^2 | n \text{ gibt} \end{cases} \end{array} \right\}$$

heißt **MÖBIUS–Funktion** (August Ferdinand MÖBIUS, 1790–1868).

b) Ganze Zahlen, in deren Primfaktorzerlegung keine Primzahlen in zweiter oder höherer Potenz auftreten, heißen **quadratfrei** (squarefree).

Alle anderen ganzen Zahlen heißen **quadrathaltig** (squareful, nonsquarefree).

c) Die Funktion

$$\Lambda : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{R} \\ n & \mapsto & \Lambda(n) := \begin{cases} \ln p, & \text{falls es ein } (p,k)^T \in \mathbb{P} \times \mathbb{N} \text{ mit } n = p^k \text{ gibt} \\ 0, & \text{sonst.} \end{cases} \end{array} \right\}$$

heißt **VON MANGOLDT–Funktion** (Hans Karl Friedrich VON MANGOLDT, 1854–1925).

Die fundamentale Bedeutung der etwas merkwürdig anmutenden MÖBIUS–Funktion wird bald klar.
Die VON MANGOLDT–Funktion ist zwar weder multiplikativ noch additiv, spielt jedoch in der Primzahltheorie eine sehr wichtige Rolle.

Folgerungen 5.7

(1) Die MÖBIUS–Funktion ist multiplikativ, aber nicht vollständig multiplikativ.

(2) Für alle $n \in \mathbb{N}$ gilt

$$\begin{array}{rcl} n \text{ ist quadratfrei} & \iff & |\mu(n)| = \mu^2(n) = 1. \\ n \text{ ist quadrathaltig (d.h. } \exists\, p \in \mathbb{P} \text{ mit } p^2 | n) & \iff & \mu(n) = 0. \end{array}$$

(3) Es ist $\displaystyle\sum_{d|n} \Lambda(d) = \ln(n)$ für alle $n \in \mathbb{N}$.

BEWEIS:
(2) ist mit (1) sofort klar.

(i) Zu (1)
Sei $p \in \mathbb{P}$. Seien $n \in \mathbb{N}$ und $m \in \mathbb{N}$ mit $(n,m) = 1$.
Falls beide quadratfrei mit den Primfaktorenzerlegungen $n = p_1 \cdot \ldots \cdot p_r$ und $m = q_1 \cdot \ldots \cdot q_s$ sind, so ist es wegen $(n,m) = 1$ auch nm und es gilt

$$\mu(nm) = \mu(p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(n) \cdot \mu(m).$$

Falls nm quadrathaltig ist, dann wegen der Teilerfremdheit auch n oder m, also

$$0 = \mu(nm) = \mu(n) \cdot \mu(m).$$

Wegen $\mu(p^2) = 0$, aber $\mu(p) \cdot \mu(p) = (-1)^2 = 1$ liegt keine vollständige Multiplikativität vor.

(ii) Zu (3)
Es ist $\ln(1) = 0 = \Lambda(1) = \sum_{d|1} \Lambda(d)$. Sei also $\ell \in \mathbb{N} \setminus \{1\}$ mit der Primfaktorzerlegung $\ell = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$. Nach Definition von Λ tragen zur Teilersumme nur die $d \in \mathbb{N}$ mit $d|\ell$ etwas bei, die die Gestalt p_j^b mit $b \in \mathbb{N}$, $b \leq a_j$, $j \in \mathbb{N}$ und $j \leq k$ haben. Also ist

$$\begin{aligned}\sum_{d|n} \Lambda(d) &= \sum_{j=1}^{k} \sum_{b=1}^{a_j} \ln(p_j) \\ &= \sum_{j=1}^{k} \ln\left(p_j^{a_j}\right) = \ln\left(p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}\right) = \ln(\ell).\end{aligned}$$

□

Definition 5.8 (Falt–Produkt zweier zahlentheoretischer Funktionen)
Für zwei zF $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ und $g : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & g(n) \end{array} \right\}$ wird durch

$$f * g : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & (f*g)(n) := \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right) \end{array} \right\}$$

das **Falt–Produkt von f und g** definiert.

Satz 5.9 (Multiplikativität des Falt–Produkts zweier multiplikativer Funktionen)
Behauptung: *Falls* $f : \mathbb{N} \to \mathbb{C}$ *und* $g : \mathbb{N} \to \mathbb{C}$ *multiplikativ sind, ist auch* $f * g$ *multiplikativ.*

Bemerkung
Die vollständige Multiplikativität bleibt bei der Faltung nicht immer erhalten, wie das Beispiel

$$\tau = \mathbb{1} * \mathbb{1}$$

in Verbindung mit Folgerung 5.3 auf Seite 78 zeigt.

Beweis:
Seien $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ und $g : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & g(n) \end{array} \right\}$ multiplikativ.
Seien $n_1 \in \mathbb{N}$ und $n_2 \in \mathbb{N}$ mit $(n_1, n_2) = 1$.
Durchlaufen $d_1 \in \mathbb{N}$ und $d_2 \in \mathbb{N}$ unabhängig voneinander alle Teiler von n_1 und n_2, so durchläuft $d_1 d_2$ alle Teiler von $n_1 n_2$.
Umgekehrt lässt sich jeder Teiler $d \in \mathbb{N}$ von $n_1 n_2$ eindeutig als $d_1 d_2$ mit $d_1 \in \mathbb{N}$, $d_1 | n_1$, $d_2 \in \mathbb{N}$ und $d_2 | n_2$ schreiben. Für $d_1 \in \mathbb{N}$ und $d_2 \in \mathbb{N}$ mit $d_1 | n_1$ und $d_2 | n_2$ ist wegen $(n_1, n_2) = 1$ auch $(d_1, d_2) = \left(\frac{n_1}{d_1}, \frac{n_2}{d_2} \right) = 1$.
Also folgt

$$\begin{aligned}
(f * g)(n_1 n_2) &= \sum_{d | n_1 n_2} f(d) \cdot g\left(\frac{n_1 n_2}{d} \right) \\
&= \sum_{d_1 | n_1} \sum_{d_2 | n_2} f(d_1 d_2) \cdot g\left(\frac{n_1}{d_1} \cdot \frac{n_2}{d_2} \right) \\
&= \sum_{d_1 | n_1} f(d_1) \cdot g\left(\frac{n_1}{d_1} \right) \cdot \sum_{d_2 | n_2} f(d_2) \cdot g\left(\frac{n_2}{d_2} \right) \\
&= (f * g)(n_1) \cdot (f * g)(n_2).
\end{aligned}$$

□

Die erste Aussage von Folgerung 5.3 auf Seite 78 ist hierin wegen

$$\sigma_\alpha = P_\alpha * \mathbb{1} \qquad \text{mit } P_\alpha(n) := n^\alpha \text{ für alle } n \in \mathbb{N}$$

für alle $\alpha \in \mathbb{R}$ offenbar enthalten.

Satz 5.10 (Gruppeneigenschaft der zahlentheoretischen Funktionen)
Behauptung: **(1)** *Die Menge $\mathcal{F}$ der zahlentheoretischen Funktionen bildet mit $*$ als Verknüpfung eine abelsche Halbgruppe mit Einselement.*

(2) *Die Menge*

$$\mathcal{Z} := \left\{ f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\} ; f(1) \neq 0 \right\}$$

der zahlentheoretischen Funktionen, die an der Stelle 1 nicht verschwinden, bildet mit $*$ als Verknüpfung eine abelsche Gruppe.

(3) *ε ist in $(\mathcal{Z}, *)$ das neutrale Element.* $\left(\varepsilon(n) = \left\lfloor \frac{1}{n} \right\rfloor \text{ für alle } n \in \mathbb{N}\right)$

(4) *Die* Möbius*–Funktion ist das Faltungs–Inverse der Funktion $\mathbb{1}$, das heißt, es ist*

$$\boxed{\mu * \mathbb{1} = \mathbb{1} * \mu = \varepsilon.}$$

(5) *Die Menge der multiplikativen Funktionen bildet eine Untergruppe von $(\mathcal{Z}, *)$.*

Beweis:

(i) $*$ ist eine Verknüpfung auf $\mathcal{F}$ und Anwenden von Satz 5.9
Dass $*$ auf $\mathcal{F}$ eine Verknüpfung bildet, ist klar.
Dass $*$ nicht aus $\mathcal{M} := \{ f \in \mathcal{Z} ; f \text{ ist multiplikativ} \}$ hinausführt, wurde in Satz 5.9 auf der vorherigen Seite gezeigt.

(ii) Kommutativität
Durchläuft $d \in \mathbb{N}$ alle Teiler von $n \in \mathbb{N}$, so durchläuft auch $\frac{n}{d}$ alle Teiler von n. Damit folgt für alle $n \in \mathbb{N}$, alle $f \in \mathcal{F}$ und alle $g \in \mathcal{F}$

$$(f * g)(n) = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{\frac{n}{d}}\right) \cdot g\left(\frac{n}{d}\right) = \sum_{d'|n} g(d') \cdot f\left(\frac{n}{d'}\right) = (g * f)(n).$$

Also ist $*$ kommutativ auf $\mathcal{F}$ und insbesondere auch auf $\mathcal{Z} \subseteq \mathcal{F}$.

(iii) Assoziativität
Es kann $(f * g)(n)$ für alle $n \in \mathbb{N}$, alle $f \in \mathcal{F}$ und alle $g \in \mathcal{F}$ auch als $\sum_{\substack{d_1|n \text{ und } d_2|n \\ d_1 d_2 = n}} f(d_1) \cdot g(d_2)$ geschrieben werden.

Für alle $n \in \mathbb{N}$, alle $f_1 \in \mathcal{F}$, alle $f_2 \in \mathcal{F}$ und alle $f_3 \in \mathcal{F}$ folgt

$$\begin{aligned}
&(f_1 * (f_2 * f_3))(n) \\
&\quad = \sum_{\substack{d_1 \mid n \text{ und } d' \mid n \\ d_1 d' = n}} f(d_1) \cdot (f_2 * f_3)(d') = \sum_{\substack{d_1 \mid n \text{ und } d' \mid n \\ d_1 d' = n}} f(d_1) \cdot \sum_{\substack{d_2 \mid d' \text{ und } d_3 \mid d' \\ d_2 d_3 = d'}} f_2(d_2) \cdot f_3(d_3) \\
&\quad = \sum_{\substack{(d_1,d_2,d_3)^T \in \mathbb{N}^3 \\ d_1 d_2 d_3 = n}} f_1(d_1) \cdot f_2(d_2) \cdot f_3(d_3) = \sum_{\substack{d' \mid n \text{ und } d_3 \mid n \\ d' d_3 = n}} \sum_{\substack{d_1 \mid d' \text{ und } d_2 \mid d' \\ d_1 d_2 = d'}} f_1(d_1) \cdot f_2(d_2) \cdot f_3(d_3) \\
&\quad = \sum_{\substack{d' \mid n \text{ und } d_3 \mid n \\ d' d_3 = n}} (f_1 * f_2)(d') \cdot f_3(d_3) = ((f_1 * f_2) * f_3)(n).
\end{aligned}$$

Also ist $*$ assoziativ auf $\mathcal{F}$ und insbesondere auch auf $\mathcal{Z} \subseteq \mathcal{F}$.

(iv) Zu (3)
Es gilt für beliebiges $f \in \mathcal{F}$ und alle $n \in \mathbb{N}$

$$(f * \varepsilon)(n) = (\varepsilon * f)(n) = \sum_{d \mid n} \varepsilon(d) \cdot f\left(\frac{n}{d}\right) = 1 \cdot f\left(\frac{n}{1}\right) + \sum_{\substack{d \mid n \\ d \neq 1}} 0 \cdot f\left(\frac{n}{d}\right) = f(n).$$

(v) Zu (4)
Mit $\mathbb{1}$ und μ ist auch $\mathbb{1} * \mu$ multiplikativ. Insbesondere ist $(\mathbb{1} * \mu)(1) = 1$.
Für Primzahlpotenzen, also alle $p \in \mathbb{P}$ und alle $k \in \mathbb{N}$ gilt jedoch

$$(\mathbb{1} * \mu)\left(p^k\right) = (\mu * \mathbb{1})\left(p^k\right) = \sum_{d \mid p^k} \mu(d) \cdot \mathbb{1}\left(\frac{p^k}{d}\right) = \sum_{d \mid p^k} \mu(d) = \mu(1) + \mu(p) = 0.$$

Also ist $(\mathbb{1} * \mu)(n) = 0$ für alle $n \in \mathbb{N} \setminus \{1\}$.

(vi) Invertierbarkeit in $(\mathcal{Z}, *)$
Zum Nachweis des Inversen $g \in \mathcal{Z}$ zu $f \in \mathcal{Z}$ bezüglich $*$ wird die Gleichung

$$g * f = \varepsilon \qquad (\circledast)$$

rekursiv nach g aufgelöst.
Induktionsanfang:
Für $n = 1$ lautet $(\circledast)$ $g(1) \cdot f(1) = 1$. Sei also $g(1) := (f(1))^{-1}$.
Das Inverse von $f(1)$ existert in $\mathbb{C} \setminus \{0\}$, weil $f(1) \neq 0$ wegen $f \in \mathcal{Z}$ ist.
Induktionsvoraussetzung:
Es gibt ein $n \in \mathbb{N}$ und für alle $m \in \mathbb{N}$ mit $m \leq n$ gibt es ein $g(m) \in \mathbb{C}$, so dass $(\circledast)$ für m erfüllt ist, also $(g * f)(m) = \varepsilon(m)$ gilt.
Induktionsschluss:
Die Gültigkeit von $(\circledast)$ für $n+1$ besagt dann

$$0 = \varepsilon(n+1) = g(n+1) \cdot f(1) + \sum_{\substack{d \mid (n+1) \\ d \neq n+1}} g(d) \cdot f\left(\frac{n+1}{d}\right).$$

Diese Gleichung ist mit $g(n+1) := -\sum_{\substack{d|(n+1)\\ d\neq n+1}} g(d)\cdot f\left(\frac{n+1}{d}\right)\cdot (f(1))^{-1}$ erfüllt.

(vii) $\mathcal{M}$ bildet eine Untergruppe
Nach (i) ist zur Untergruppen–Eigenschaft von $\mathcal{M}$ noch zu zeigen, dass mit $f\in\mathcal{M}$ auch das durch $g*f=\varepsilon$ eindeutig festgelegte, in (vi) konstruierte $g\in\mathcal{Z}$ multiplikativ ist.
Induktionsanfang:
Es ist $g(1)=\frac{1}{f(1)}=\frac{1}{1}=1=1\cdot 1=g(1)\cdot g(1)$.
Induktionsvoraussetzung:
Für ein $n\in\mathbb{N}\setminus\{1\}$ sei schon gezeigt, dass $g(d_1d_2)=g(d_1)\cdot g(d_2)$ für alle $d_1\in\mathbb{N}$ und alle $d_2\in\mathbb{N}$ mit $(d_1,d_2)=1$ und $d_1d_2<n$ erfüllt ist.
Induktionsschluss:
Nach (*) ist wegen $f(1)=1$ und $n\geq 2$

$$g(n)=-\sum_{\substack{d|n\\ d\neq n}} g(d)\cdot f\left(\frac{n}{d}\right).$$

Wegen $g(1)=1$ ist $g(1\cdot n)=g(n)=1\cdot g(n)=g(1)\cdot g(n)$.
Gibt es $n_1\in\mathbb{N}\setminus\{1\}$ und $n_2\in\mathbb{N}\setminus\{1\}$ mit $n=n_1n_2$ und $(n_1,n_2)=1$, so ergibt sich mit der Induktionsvoraussetzung

$$\begin{aligned}
g(n_1n_2) &= -\sum_{\substack{d|n_1n_2\\ d\neq n_1n_2}} g(d)\cdot f\left(\frac{n_1n_2}{d}\right)\\
&= -\sum_{\substack{(d_1,d_2)^T\in\mathbb{N}^2\\ d_1|n_1 \text{ und } d_2|n_2\\ d_1<n_1 \text{ oder } d_2<n_2}} g(d_1d_2)\cdot f\left(\frac{n_1}{d_1}\cdot\frac{n_2}{d_2}\right)\\
&= -\sum_{\substack{(d_1,d_2)^T\in\mathbb{N}^2\\ d_1|n_1 \text{ und } d_2|n_2\\ d_1<n_1 \text{ oder } d_2<n_2}} g(d_1)\cdot g(d_2)\cdot f\left(\frac{n_1}{d_1}\right)\cdot f\left(\frac{n_2}{d_2}\right)\\
&= -\sum_{d_1|n_1}\sum_{d_2|n_2} g(d_1)\cdot g(d_2)\cdot f\left(\frac{n_1}{d_1}\right)\cdot f\left(\frac{n_2}{d_2}\right)+g(n_1)\cdot g(n_2)\cdot f(1)\cdot f(1)\\
&= g(n_1)\cdot g(n_2)-(g*f)(n_1)\cdot(g*f)(n_2)\\
&= g(n_1)\cdot g(n_2)-\varepsilon(n_1)\cdot\varepsilon(n_2)\\
&= g(n_1)\cdot g(n_2).
\end{aligned}$$

□

Satz 5.11 (Möbiussche Umkehrformel)
Behauptung: *Für zwei zahlentheoretische Funktionen $f:\mathbb{N}\to\mathbb{C}$ und $F:\mathbb{N}\to\mathbb{C}$ gilt*

$$F=f*\mathbb{1} \qquad\Longleftrightarrow\qquad f=F*\mu.$$

Das bedeutet für alle $f: \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ und alle $F: \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & F(n) \end{array} \right\}$

$$F(n) = \sum_{d|n} f(d) \qquad \text{für alle } n \in \mathbb{N}$$

$$\iff \qquad f(n) = \sum_{d|n} F(d) \cdot \mu\left(\frac{n}{d}\right) \qquad \text{für alle } n \in \mathbb{N}.$$

Die Umkehrformel erlaubt es also, eine Teilersummen–Identität „$F(n) = \sum_{d|n} f(d)$ für alle $n \in \mathbb{N}$“ nach f hin aufzulösen.

Beweis:
Ergibt sich sofort aus den Punkten (1) und (4) von Satz 5.10 auf Seite 84. □

Lemma 5.12 (1. Beispiel zur Möbiusschen Umkehrformel 5.11)
Behauptung: **(1)** *Es ist* $\varphi * \mathbb{1} = \mathrm{id}$*, also gilt für alle* $n \in \mathbb{N}$

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

(2) *Es ist* $\varphi = \mu * \mathrm{id}$*, also gilt für alle* $n \in \mathbb{N}$

$$\varphi(n) = n \cdot \sum_{d|n} \frac{\mu(d)}{d}.$$

Beweis:

(i) Zu (1)
Sei $n \in \mathbb{N}$. Mit $d \in \mathbb{N}$ durchläuft auch $\frac{n}{d}$ alle Teiler von n. Sei

$$\mathcal{K}: \left\{ \begin{array}{ccc} \{d \in \mathbb{N}\,;d|n\} & \to & \{\mathcal{D}\,;\mathcal{D} \subseteq \mathbb{N}\} \\ d & \mapsto & \mathcal{K}_d := \left\{a \in \mathbb{N}\,;a \le n \text{ und } (a,n) = \frac{n}{d}\right\} \end{array} \right\}.$$

Durch $\mathcal{K}$ wird die n–elementige Menge $\{1, 2, \ldots, n\}$ in disjunkte Klassen eingeteilt und insbesondere ist

$$n = \sum_{d|n} \#\mathcal{K}_d.$$

Wegen

$$\begin{aligned} \mathcal{K}_d &= \left\{b \in \mathbb{N}\,;b \cdot \frac{n}{d} \le n \text{ und } \left(b \cdot \frac{n}{d}, n\right) = \frac{n}{d}\right\} \\ &= \{b \in \mathbb{N}\,;b \le d \text{ und } (b,d) = 1\} \end{aligned}$$

gilt $\#\mathcal{K}_d = \varphi(d)$ für alle $d \in \mathbb{N}$ mit $d|n$. Damit folgt die Behauptung.

(ii) Zu (2)
(2) folgt aus (1) mit der MÖBIUSschen Umkehrformel 5.11 auf Seite 86. □

Damit ist erneut die Multiplikativität von φ gezeigt.
(2) ergibt wegen der Multiplikativität von μ und id obendrein für alle $n \in \mathbb{N}$ mit der Primfaktorzerlegung $n = p_1^{a_1} \cdots p_k^{a_k}$

$$\begin{aligned}\frac{\varphi(n)}{n} &= \sum_{d|n} \frac{\mu(d)}{d} = \left(1 + \frac{\mu(p_1)}{p_1} + \ldots + \frac{\mu(p_1^{a_1})}{p_1^{a_1}}\right) \cdot \ldots \cdot \left(1 + \frac{\mu(p_k)}{p_k} + \ldots + \frac{\mu(p_k^{a_k})}{p_k^{a_k}}\right) \\ &= \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) = \prod_{p|n} \left(1 - \frac{1}{p}\right).\end{aligned}$$

Lemma 5.13 (2. Beispiel zur MÖBIUSschen Umkehrformel 5.11)
BEHAUPTUNG: *Für alle $n \in \mathbb{N}$ ist*

$$\Lambda(n) = \sum_{d|n} \mu(d) \cdot \ln\left(\frac{n}{d}\right) = -\sum_{d|n} \mu(d) \cdot \ln(d).$$

BEWEIS:
Die erste Aussage entsteht durch Umkehrung von Folgerung 5.7 (3) auf Seite 81.
Aus der ersten Aussage und Punkt (4) von Satz 5.10 auf Seite 84 folgt

$$\begin{aligned}\Lambda(n) &= \ln(n) \cdot \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \ln(d) \\ &= \ln(n) \cdot \varepsilon(n) - \sum_{d|n} \mu(d) \ln(d) = -\sum_{d|n} \mu(d) \ln(d).\end{aligned}$$ □

SATZ 5.14 (LEGENDREsche Formel)
VORAUSSETZUNGEN:
Seien $\mathcal{A} \subseteq \mathbb{N}$ mit $\#\mathcal{A} < \infty$, $k \in \mathbb{N}$ und $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ eine zahlentheoretische Funktion.
BEHAUPTUNG: *Dann gilt*

$$\sum_{\substack{n \in \mathcal{A} \\ (n,k)=1}} f(n) = \sum_{d|k} \mu(d) \cdot \sum_{\substack{n \in \mathcal{A} \\ n \equiv 0 \bmod d}} f(n).$$

BEWEIS:
Die Aussage ist klar, wenn man bedenkt, dass die Summationsbedingung $(n,k) = 1$ für alle $n \in \mathcal{A}$ durch den Faktor $\varepsilon((n,k)) = \sum_{\substack{d|n \\ d|k}} \mu(d)$ in der Summe ersetzt werden kann. (Diese Ersetzung wird auch „**MÖBIUS–Trick**“ genannt.) □

Satz 5.14 entspricht dem **Inklusion–Exklusion–Prinzip** in der Kombinatorik:
Seien $\mathcal{M}$ eine endliche Menge, $\ell \in \mathbb{N}$ und $E_1, \ldots, E_\ell$ Eigenschaften oder Merkmale, die Elemente von $\mathcal{M}$ besitzen können.
Für alle $r \in \mathbb{N}$ mit $r \leq \ell$ und alle $(j_1, \ldots, j_r)^T \in \mathbb{N}^r$ mit $j_h < j_{h+1} \leq \ell$ für alle $h \in \mathbb{N}$ mit $h < r$ sei $\mathcal{M}_{j_1,\ldots,j_r}$ die Teilmenge derjenigen Elemente von $\mathcal{M}$, die die Eigenschaften $E_{j_1}, \ldots, E_{j_r}$ haben.
Bezeichne $\mathcal{M}'$ die Menge aller Elemente von $\mathcal{M}$, die keine der Eigenschaften E_j mit $j \in \mathbb{N}$ und $j \leq \ell$ haben. Dann gilt

$$\#\mathcal{M}' = \#\mathcal{M} - \sum_{j_1=1}^{\ell} \#M_{j_1} + \sum_{\substack{(j_1,j_2)^T \in \mathbb{N}^2 \\ j_1 < j_2 \leq \ell}} \sum \#\mathcal{M}_{j_1 j_2} \mp \ldots + (-1)^\ell \cdot \#M_{1,\ldots,\ell}. \tag{IEP}$$

Im Hinblick auf Satz 5.14 sei also

$$f := \mathbb{1}, \qquad k = p_1^{a_1} \cdot \ldots \cdot p_\ell^{a_\ell} \neq 1 \qquad \text{und} \qquad \mathcal{A} := \mathcal{M}.$$

E_j bedeute $p_j | n$ für alle $j \in \mathbb{N}$ mit $j \leq \ell$.
Dann ergibt (IEP)

$$\begin{aligned}
\sum_{\substack{n \in \mathcal{A} \\ (n,k)=1}} 1 &= \#\mathcal{M}' \\
&= \#\mathcal{A} - \sum_{j_1=1}^{\ell} \#\left\{n \in \mathcal{A} \,;\, n \equiv 0 \,(p_{j_1})\right\} \\
&\qquad + \sum_{\substack{(j_1,j_2)^T \in \mathbb{N}^2 \\ j_1 < j_2 \leq \ell}} \sum \#\left\{n \in \mathcal{A} \,;\, n \equiv 0 \,(p_{j_1}) \text{ und } n \equiv 0 \,(p_{j_2})\right\} \mp \ldots \\
&= \sum_{d|k} \mu(d) \cdot \#\left\{n \in \mathcal{A} \,;\, n \equiv 0 \bmod d\right\}.
\end{aligned}$$

Die gängigen zahlentheoretischen Funktionen wie σ_α mit $\alpha \in \mathbb{R}$, φ oder μ weisen ein sehr sprunghaftes Verhalten auf. Insbesondere ist es unmöglich, sie durch vertraute stetige Funktionen zu approximieren, so wie es beispielsweise in der STIRLINGschen Formel mit der Fakultätsfunktion geschieht.
Betrachtet man für $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ hingegen die Summenfunktion

$$F : \left\{ \begin{array}{ccc} \{y \in \mathbb{R} \,;\, y \geq 1\} & \to & \mathbb{C} \\ x & \mapsto & F(x) := \displaystyle\sum_{n=1}^{\lfloor x \rfloor} f(n) \end{array} \right\},$$

so lässt sich in vielen Fällen ein Verhalten der Art

$$F = H + R$$

feststellen. Dabei bedeutet H („Hauptterm“) eine „glatte“ Funktion, während das im Allgemeinen nicht genau angebbare R („Restglied“) von geringerer Größenordnung ist als H. Hierzu hat sich eine — nicht auf die Zahlentheorie beschränkte — Schreibweise als sehr nützlich erwiesen.

Definition 5.15 (Bachmann–Landau–Symbolik)
(Paul Bachmann, 1837–1920; Edmund Landau, 1877–1938)
Für diese Definition seien $x_0 \in \mathbb{R}$, $\mathbb{R}_{\geq x_0} := \{w \in \mathbb{R}\,;w \geq x_0\}$, $f : \left\{ \begin{array}{rcl} \mathbb{R}_{\geq x_0} & \to & \mathbb{C} \\ x & \mapsto & f(x) \end{array} \right\}$,
$h : \left\{ \begin{array}{rcl} \mathbb{R}_{\geq x_0} & \to & \mathbb{C} \\ x & \mapsto & h(x) \end{array} \right\}$ und $g : \left\{ \begin{array}{rcl} \mathbb{R}_{\geq x_0} & \to & \{w \in \mathbb{R}\,;w \geq 0\} \\ x & \mapsto & g(x) \end{array} \right\}$.

a) f heißt **höchstens von der Ordnung g**, wenn es ein $C \in \mathbb{R}$ mit $C > 0$ und

$$|f(x)| \leq C \cdot g(x) \qquad \text{für alle } x \in \mathbb{R} \text{ mit } x \geq x_0$$

gibt. (Kurz: $f = O(g)$, $f(x) = O(g(x))$, $f \ll g$ oder $f(x) \ll g(x)$, „f ist groß–O von g“ — die Schreibweise mit $\ll$ heißt „Виноградов[§]“–Schreibweise)

Für $f - h = O(g)$ schreibt man auch kurz $f = h + O(g)$.

b) f heißt **von kleinerer Ordnung als g**, falls

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} \text{ existiert mit } \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

(Kurz: $f = o(g)$ oder $f(x) = o(g(x))$, „f ist klein–o von g“)

Für $f - h = o(g)$ schreibt man auch kurz $f = h + o(g)$.

Beispiele und Bemerkungen

(1) $\ln(x) = O(x^{\varepsilon})$ für jedes $\varepsilon \in \mathbb{R}$ mit $\varepsilon > 0$
(wobei die „O–Konstante“ $C \in \mathbb{R}$ mit $C > 0$ von ε abhängt).

(2) x ist nicht groß–O von $\ln(x)$, kurz: $x \neq O(\ln(x))$.

(3) $\sin(x) = O(1)$, aber $\sin(x) \neq o(1)$.

(4) $f(x) = O(1)$ besagt nicht, dass f konstant ist, sondern nur, dass f beschränkt ist.

(5) Eine „asymptotische Formel“ $F = H + O(R)$ macht nur Sinn, wenn R von kleinerer Ordnung als H ist.
Z.B. ist $F(x) = x + O(x^2)$ nicht aussagekräftiger als $F(x) = O(x^2)$.

(6) Bei konkurrierenden O–Termen reicht es, den größten zu behalten:

$$O(x) + O\left(x^2\right) + O(\exp(x)) = O(\exp(x)).$$

[§]sprich: „Vinogradov“

(7) Ist $f = o(g)$, so existiert ein $\delta : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & \delta(x) \end{array} \right\}$ mit

$$f(x) = \delta(x) \cdot g(x) \qquad \text{und} \qquad \lim_{x \to \infty} \delta(x) = 0.$$

(8) Aus $f(x) = o(x)$ folgt $f(x) = O(x)$. Die Umkehrung gilt im Allgemeinen nicht.

(9) $\lfloor x \rfloor = x + O(1)$, aber $\lfloor x \rfloor \neq x + o(1)$.

(10) $\tau(n) = O(n^{\varepsilon})$ für jedes $\varepsilon \in \mathbb{R}$ mit $\varepsilon > 0$ aber $\tau(n) \neq o(\ln(n))$, da für alle $k \in \mathbb{N}$

$$\tau\left(2^k\right) = k + 1 > k = \frac{\ln\left(2^k\right)}{\ln(2)} \text{ ist.}$$

(11) $\varphi(n) = O(n)$, aber $\varphi(n) \neq o(n)$, da $\varphi(p) = p - 1 \geq \frac{p}{2}$ für alle $p \in \mathbb{P}$ ist.

Lemma 5.16 (Partielle oder abelsche Summation)
(Niels Henrik Abel, 1802–1829)
Voraussetzungen:
Seien $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$, $\mathcal{A} \subseteq \mathbb{R}$ *mit* $x \in \mathcal{A}$ *für alle* $x \geq 1$,

$$F : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ & & \\ x & \mapsto & F(x) := \displaystyle\sum_{n=1}^{\lfloor x \rfloor} f(n) \end{array} \right\} \textit{ und}$$

$$g : \left\{ \begin{array}{ccc} \mathcal{A} & \to & \mathbb{C} \\ x & \mapsto & g(x) \end{array} \right\} \textit{ stetig differenzierbar.}$$

Behauptung: *Dann gilt für alle* $x \in \mathbb{R}$ *mit* $x \geq 1$

$$\sum_{n=1}^{\lfloor x \rfloor} f(n) \cdot g(n) = F(x) \cdot g(x) - \int_1^x F(t) \cdot g'(t)\,\mathrm{d}t.$$

Beweis:
Mit $s : \left\{ \begin{array}{ccc} \mathbb{Z} \times \mathbb{R} & \to & \mathbb{R} \\ & & \\ (n,t)^T & \mapsto & s_n(t) := \begin{cases} 1, & \text{falls } t \geq n \\ 0, & \text{falls } t < n \end{cases} \end{array} \right\}$ folgt

$$\begin{aligned} \int_1^x F(t) \cdot g'(t)\,\mathrm{d}t &= \int_1^x \sum_{n=1}^{\lfloor t \rfloor} f(n) \cdot g'(t)\,\mathrm{d}t = \int_1^x \left(\sum_{n=1}^{\lfloor x \rfloor} f(n) \cdot s_n(t) \right) \cdot g'(t)\,\mathrm{d}t \\ &= \sum_{n=1}^{\lfloor x \rfloor} f(n) \cdot \int_1^x s_n(t) \cdot g'(t)\,\mathrm{d}t = \sum_{n=1}^{\lfloor x \rfloor} f(n) \cdot \int_n^x g'(t)\,\mathrm{d}t \\ &= F(x) \cdot g(x) - \sum_{n=1}^{\lfloor x \rfloor} f(n) \cdot g(n). \end{aligned}$$

□

Lemma 5.17 (Endliche harmonische Reihe und Logarithmussumme)
BEHAUPTUNG: **(1)** *Es gibt ein* $\gamma \in \mathbb{R}$ *mit* $\gamma > 0$ *und*

$$\sum_{n=1}^{\lfloor x \rfloor} \frac{1}{n} = \ln(x) + \gamma + O\left(\frac{1}{x}\right).$$

(2) *Es ist*

$$\sum_{n=1}^{\lfloor x \rfloor} \ln(n) = x \ln(x) + O(x).$$

Bemerkung
$\gamma = 0.5772\ldots$ heißt EULER–Konstante oder EULER–MASCHERONI–Konstante. Es gilt

$$\gamma = \lim_{n\to\infty}\left(-\ln(n) + \sum_{k=1}^{n}\frac{1}{k}\right) = \int_1^\infty \left(\frac{1}{\lfloor x \rfloor} - \frac{1}{x}\right) \mathrm{d}x = \lim_{x\to\infty}\left(x - \Gamma\left(\frac{1}{x}\right)\right) = -\Gamma'(1),$$

wobei Γ die Gamma–Funktion bezeichnet.

BEWEIS:

(i) Zu (1)
Es wird partielle Summation 5.16 auf der vorherigen Seite auf $f := \mathbb{1}$ und $g: \left\{ \begin{array}{rcl} R \setminus \{0\} & \to & \mathbb{R} \\ t & \mapsto & g(t) := \frac{1}{t} \end{array} \right\}$ angewandt.
Seien also $F := \lfloor \cdot \rfloor$ und $\langle \cdot \rangle : \left\{ \begin{array}{rcl} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \langle x \rangle := x - \lfloor x \rfloor \end{array} \right\}$.
Dann ist $\sum_{n=1}^{\lfloor x \rfloor} f(n) = F(x) = \lfloor x \rfloor = x - \langle x \rangle = x + O(1)$ für alle $x \in \mathbb{R}$ mit $x \geq 1$. Also gilt

$$\begin{aligned} \sum_{n=1}^{\lfloor x \rfloor} \frac{1}{n} &= \frac{x - \langle x \rangle}{x} + \int_1^x (t - \langle t \rangle) \cdot t^{-2}\, \mathrm{d}t \\ &= 1 + O\left(\frac{1}{x}\right) + \ln(x) - \int_1^x \frac{\langle t \rangle}{t^2}\, \mathrm{d}t. \end{aligned}$$

$\int_1^\infty \frac{\langle t \rangle}{t^2}\, \mathrm{d}t$ konvergiert nach dem Majorantenkriterium.

Für alle $x \in \mathbb{R}$ mit $x \geq 1$ lässt sich $\int\limits_x^\infty \frac{\langle t \rangle}{t^2}\,\mathrm{d}t$ im Betrag abschätzen durch

$$\int\limits_x^\infty \frac{1}{t^2}\,\mathrm{d}t = \frac{1}{x}.$$

Setzt man $\gamma := 1 - \int\limits_1^\infty \frac{\langle t \rangle}{t^2}\,\mathrm{d}t$, so ergibt sich Behauptung (1).

(ii) Zu (2)
Da ln monoton wächst, gilt für alle $x \in \mathbb{R}$ und alle $n \in \mathbb{N}$ mit $2 \leq n \leq x$ die Ungleichung

$$\ln\left(\frac{x}{n}\right) \leq \int\limits_{n-1}^{n} \ln\left(\frac{x}{t}\right)\mathrm{d}t.$$

Also gilt für alle $x \in \mathbb{R}$ mit $x \geq 2$

$$\begin{aligned}\sum_{n=2}^{\lfloor x \rfloor} \ln\left(\frac{x}{n}\right) &\leq \int\limits_1^{\lfloor x \rfloor} \ln\left(\frac{x}{t}\right)\mathrm{d}t \leq \int\limits_1^{x} \ln\left(\frac{x}{t}\right)\mathrm{d}t \\ &= x \cdot \int\limits_1^x \frac{\ln(v)}{v^2}\,\mathrm{d}v < x \cdot \int\limits_1^\infty \frac{\ln(v)}{v^2}\,\mathrm{d}v = O(x).\end{aligned}$$

Damit folgt für alle $x \in \mathbb{R}$ mit $x \geq 2$

$$\sum_{n=1}^{\lfloor x \rfloor} \ln\left(\frac{x}{n}\right) = O(x)$$

Dies gilt offensichtlich auch für alle $x \in \mathbb{R}$ mit $1 \leq x < 2$.
Hiermit ist Behauptung (2) sofort einzusehen:

$$\sum_{n=1}^{\lfloor x \rfloor} \ln(n) = \sum_{n=1}^{\lfloor x \rfloor} \ln(x) - \sum_{n=1}^{\lfloor x \rfloor} \ln\left(\frac{x}{n}\right) = (x + O(1)) \cdot \ln(x) + O(x) = x \cdot \ln(x) + O(x). \qquad \square$$

Den Abschluss des Kapitels bilden einige Beispiele asymptotischen Formeln für Summen über multiplikative Funktionen.

Satz 5.18 (Satz von Dirichlet über die Teileranzahl–Summenfunktion)
Behauptung: *Bezeichnet $\gamma \in \mathbb{R}$ mit $\gamma > \frac{1}{2}$ die* Euler*–Konstante aus Lemma 5.17 (1) auf Seite 92, so gilt*

$$\sum_{n=1}^{\lfloor x \rfloor} \tau(n) = x \cdot \ln(x) + (2\gamma - 1) \cdot x + O\left(x^{\frac{1}{2}}\right).$$

Bemerkung
Eine schwächere Aussage kann direkt mit Lemma 5.17 (1) hergeleitet werden:

$$\begin{aligned}\sum_{n=1}^{\lfloor x\rfloor}\tau(n) &= \sum_{\substack{d\in\mathbb{N}\text{ und }k\in\mathbb{N}\\ dk\le x}}\sum 1 = \sum_{d=1}^{\lfloor x\rfloor}\sum_{k=1}^{\left\lfloor\frac{x}{d}\right\rfloor}1\\ &= \sum_{d=1}^{\lfloor x\rfloor}\left\lfloor\frac{x}{d}\right\rfloor = x\cdot\sum_{d=1}^{\lfloor x\rfloor}\frac{1}{d}+O\left(\sum_{d=1}^{\lfloor x\rfloor}1\right)\\ &= x\cdot\left(\ln(x)+\gamma+O\left(x^{-1}\right)\right)+O\left(\lfloor x\rfloor\right) = x\cdot\ln(x)+O(x).\end{aligned}$$

Beweis:
Ist $n\in\mathbb{N}$ keine Quadratzahl, so ist für $d\in\mathbb{N}$ mit $d|n$ eine der Zahlen d und $\frac{n}{d}$ kleiner als $n^{\frac{1}{2}}$ und die andere größer, also ist

$$\tau(n) = 2\cdot\sum_{\substack{d|n\\ d<\sqrt{n}}}1+\begin{cases}0, & \text{falls } n\neq m^2 \text{ für alle } m\in\mathbb{N} \text{ ist}\\ O(1), & \text{sonst.}\end{cases}$$

für alle $n\in\mathbb{N}$. Somit folgt aus Lemma 5.17 (1) auf Seite 92

$$\begin{aligned}\sum_{n=1}^{\lfloor x\rfloor}\tau(n) &= 2\cdot\sum_{n=1}^{\lfloor x\rfloor}\sum_{\substack{d|n\\ d<\sqrt{n}}}1+O\left(x^{\frac{1}{2}}\right) = 2\cdot\sum_{\substack{d=1\\ d\neq\sqrt{x}}}^{\lfloor\sqrt{x}\rfloor}\sum_{\substack{n=d^2+1\\ n\equiv 0(d)}}^{\lfloor x\rfloor}1+O\left(x^{\frac{1}{2}}\right)\\ &= 2\cdot\sum_{\substack{d=1\\ d\neq\sqrt{x}}}^{\lfloor\sqrt{x}\rfloor}\sum_{m=d+1}^{\left\lfloor\frac{x}{d}\right\rfloor}1+O\left(x^{\frac{1}{2}}\right) = 2\cdot\sum_{\substack{d=1\\ d\neq\sqrt{x}}}^{\lfloor\sqrt{x}\rfloor}\left(\left\lfloor\frac{x}{d}\right\rfloor-d\right)+O\left(x^{\frac{1}{2}}\right)\\ &= 2x\cdot\sum_{\substack{d=1\\ d\neq\sqrt{x}}}^{\lfloor\sqrt{x}\rfloor}\frac{1}{d}+O\left(x^{\frac{1}{2}}\right)-2\cdot\sum_{\substack{d=1\\ d\neq\sqrt{x}}}^{\lfloor\sqrt{x}\rfloor}d+O\left(x^{\frac{1}{2}}\right)\\ &= 2x\cdot\left(\ln\left(x^{\frac{1}{2}}\right)+\gamma+O\left(x^{-\frac{1}{2}}\right)\right)-2\cdot\frac{\lfloor\sqrt{x}\rfloor\cdot(\lfloor\sqrt{x}\rfloor+1)}{2}+O\left(x^{\frac{1}{2}}\right)\\ &= x\cdot(\ln(x)+2\gamma-1)+O\left(x^{\frac{1}{2}}\right).\end{aligned}$$

□

Satz 5.19 (Quadratfreie und teilerfremde Zahlen)
Behauptung: *Es sind*

$$\textbf{(1)} \qquad \sum_{n=1}^{\lfloor x \rfloor} \mu^2(n) = \frac{6x}{\pi^2} + O\left(x^{\frac{1}{2}}\right)$$

und

$$\textbf{(2)} \qquad \sum_{n=1}^{\lfloor x \rfloor} \varphi(n) = \frac{3x^2}{\pi^2} + O\left(x \cdot \ln(x) + 1\right).$$

Bemerkungen

1. Da mit Hilfe von μ^2 die quadratfreien Zahlen gezählt werden, kann (1) auch so gelesen werden: Für $x := N \in \mathbb{N}$ wird

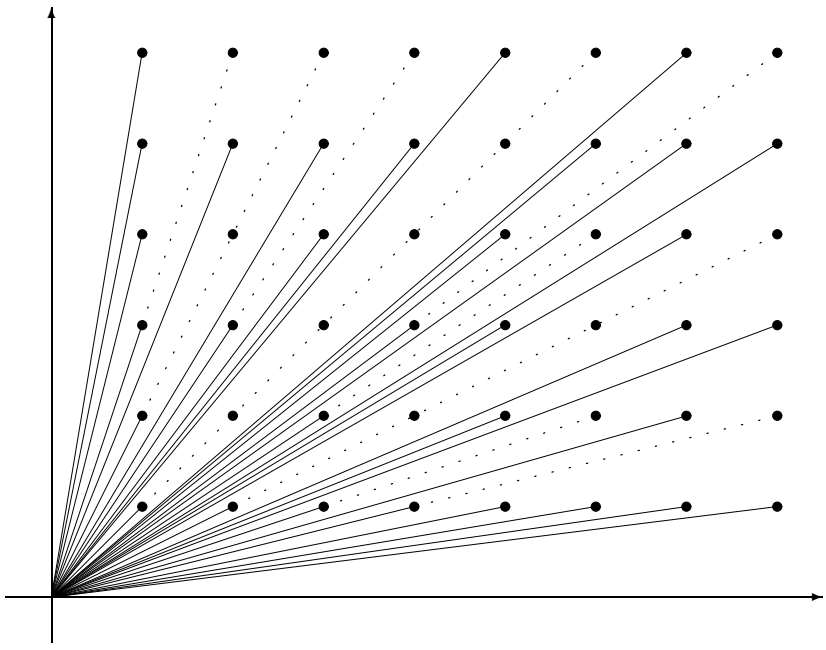
$$\frac{1}{N} \cdot \#\left\{n \in \mathbb{N}\,; n \leq N \text{ und } n \text{ quadratfrei}\right\} = \frac{6}{\pi^2} + O\left(\frac{1}{\sqrt{N}}\right) \overset{N\to\infty}{\longrightarrow} \frac{6}{\pi^2}.$$

   Das heißt, dass die relative Häufigkeit der quadratfreien unter den natürlichen Zahlen bis zu N mit $N \to \infty$ gegen $\frac{6}{\pi^2}$ strebt.

   Grob: Etwa zwei Drittel aller natürlichen Zahlen sind quadratfrei.

2. (2) lässt sich in der folgenden Weise geometrisch interpretieren:

   Nennt man einen Gitterpunkt $(m,n)^T \in \mathbb{Z}^2$ **sichtbar**, wenn auf der Strecke zwischen $(0,0)^T$ und $(m,n)^T$ kein weiterer Gitterpunkt liegt, wenn er also vom Koordinatenursprung aus sichtbar ist, ohne von einem weiteren Gitterpunkt verdeckt zu werden, so ist $(m,n)^T \in \mathbb{Z}^2$ genau dann sichtbar, wenn m und n teilerfremd sind.



Die Dichte der sichtbaren Punkte wird definiert durch

$$\lim_{x\to\infty}\frac{T(x)}{(2x)^2},$$

wobei

$$T(x) := \#\left\{(m,n)^T \in \mathbb{Z}^2\,;(m,n)^T \text{ sichtbar}, |n| \le x \text{ und } |m| \le x\right\}$$

für alle $x \in \mathbb{R}$ mit $x \ge 0$ bezeichnet. Klar ist

$$\begin{aligned} T(x) &= 8\cdot\#\left\{(m,n)\in\mathbb{N}^2\,;(m,n)^T \text{ sichtbar und } 1\le m\le n\le x\right\}+O(1)\\ &= 8\cdot\#\left\{(m,n)^T\in\mathbb{N}^2\,;1\le m\le n\le x \text{ und } (m,n)=1\right\}+O(1)\end{aligned}$$

für alle $x \in \mathbb{R}$ mit $x \ge 1$. Ferner ist

$$\begin{aligned}\sum_{n=1}^{\lfloor x\rfloor}\varphi(n) &= \sum_{n=1}^{\lfloor x\rfloor}\sum_{\substack{m=1\\(m,n)=1}}^{n}1\\ &= \#\left\{(m,n)^T\in\mathbb{N}^2\,;(m,n)^T \text{ sichtbar und } 1\le m\le n\le x\right\},\end{aligned}$$

also

$$T(x) = 8\cdot\sum_{n=1}^{\lfloor x\rfloor}\varphi(n)+O(1) = \frac{6}{\pi^2}\cdot(2x)^2+O(x\cdot\ln(x)+1)$$

für alle $x \in \mathbb{R}$ mit $x \ge 1$ nach (2).

Damit haben sichtbare Punkte also die Dichte $\frac{6}{\pi^2}$, oder anders ausgedrückt:

Bei zufälliger Wahl zweier ganzer Zahlen sind diese mit einer Wahrscheinlichkeit von $\frac{6}{\pi^2}\approx 60.8\%$ teilerfremd.

BEWEIS:

(i) Die Identität (✻)
Für alle $n \in \mathbb{N}$ besteht die Identität

$$\mu^2(n) = \sum_{\substack{d=1\\d^2|n}}^{n}\mu(d). \qquad (✻)$$

Die rechte Seite von (✻) ist multiplikativ: Seien $n_1 \in \mathbb{N}$ und $n_2 \in \mathbb{N}$ mit $(n_1,n_2)=1$.
Jeder Teiler $d \in \mathbb{N}$ von n_1n_2 lässt sich eindeutig als d_1d_2 mit $d_1 \in \mathbb{N}$, $d_1|n_1$, $d_2 \in \mathbb{N}$ und $d_2|n_2$ schreiben. Für $d_1 \in \mathbb{N}$ und $d_2 \in \mathbb{N}$ mit $d_1|n_1$ und $d_2|n_2$ ist wegen $(n_1,n_2)=1$ auch $(d_1,d_2)=1$. Für $d_1 \in \mathbb{N}$ und $d_2 \in \mathbb{N}$ ist $d_1|n_1$, $d_2|n_2$ und $d_1^2d_2^2|n_1n_2$ äquivalent zu $d_1^2|n_1$ und $d_2^2|n_2$.

Also folgt

$$\sum_{\substack{d=1\\ d^2\mid n_1n_2}}^{n_1n_2}\mu(d)=\sum_{\substack{(d_1,d_2)^T\in\mathbb{N}^2\\ d_1\mid n_1 \text{ und } d_2\mid n_2\\ d_1^2d_2^2\mid n_1n_2}}\mu(d_1d_2)=\sum_{\substack{d_1=1\\ d_1^2\mid n_1}}^{n_1}\ \sum_{\substack{d_2=1\\ d_2^2\mid n_2}}^{n_2}\mu(d_1)\cdot\mu(d_2)=\sum_{\substack{d_1=1\\ d_1^2\mid n_1}}^{n_1}\mu(d_1)\cdot\sum_{\substack{d_2=1\\ d_2^2\mid n_2}}^{n_2}\mu(d_2).$$

Wegen der Multiplikativität von μ und μ^2 sind in (✻) beide Seiten multiplikativ.

Es ist $\mu^2(p^a)=\begin{cases}1, & \text{falls } a=1\\ 0, & \text{falls } a\neq 1\end{cases}$ für alle $p\in\mathbb{P}$ und alle $a\in\mathbb{N}$.

Es ist $\sum\limits_{\substack{d=1\\ d^2\mid p^a}}^{p^a}\mu(d)=\underbrace{\mu(1)}_{=1}+\begin{cases}0, & \text{falls } a=1\\ -1+0, & \text{falls } a\neq 1\end{cases}$ für alle $p\in\mathbb{P}$ und alle $a\in\mathbb{N}$.

(ii) Zu (1)

Mit (✻) folgt für alle $x\in\mathbb{R}$ mit $x\geq 1$

$$\begin{aligned}\sum_{n=1}^{\lfloor x\rfloor}\mu^2(n)&=\sum_{n=1}^{\lfloor x\rfloor}\sum_{\substack{d=1\\ d^2\mid n}}^{\lfloor\sqrt{x}\rfloor}\mu(d)=\sum_{d=1}^{\lfloor\sqrt{x}\rfloor}\mu(d)\cdot\sum_{\substack{n=1\\ n\equiv 0\left(d^2\right)}}^{\lfloor x\rfloor}1\\ &=\sum_{d=1}^{\lfloor\sqrt{x}\rfloor}\mu(d)\cdot\left(\frac{x}{d^2}+O(1)\right)\\ &=x\cdot\sum_{d\in\mathbb{N}}\frac{\mu(d)}{d^2}-x\cdot\sum_{\substack{d\in\mathbb{N}\\ d>\sqrt{x}}}\frac{\mu(d)}{d^2}+O\left(\sqrt{x}\right)\\ &=x\cdot\sum_{d\in\mathbb{N}}\frac{\mu(d)}{d^2}+O\left(\sqrt{x}\right).\end{aligned}\qquad(❁)$$

Die letzte Gleichheit ergibt sich aus der Theorie der RIEMANNschen Untersummen durch die für alle $x\in\mathbb{R}$ mit $x\geq 4$ gültige Abschätzung

$$\begin{aligned}\left|-x\cdot\sum_{\substack{d\in\mathbb{N}\\ d>\sqrt{x}}}\frac{\mu(d)}{d^2}\right|&\leq x\cdot\sum_{\substack{d\in\mathbb{N}\\ d\geq\lfloor\sqrt{x}\rfloor+1}}\frac{1}{d^2}\leq x\cdot\int_{\lfloor\sqrt{x}\rfloor}^{\infty}\frac{1}{t^2}\,\mathrm{d}t=x\cdot\left[-\frac{1}{t}\right]_{t=\lfloor\sqrt{x}\rfloor}^{t=\infty}\\ &=x\cdot\frac{1}{\lfloor\sqrt{x}\rfloor}\leq\frac{x}{\sqrt{x}-1}\leq\frac{x}{\frac{\sqrt{x}}{2}}=2\cdot\sqrt{x}.\end{aligned}$$

Zur Berechnung von $\sum\limits_{d\in\mathbb{N}}\frac{\mu(d)}{d^2}$ benutzt man die EULERsche Formel $\sum\limits_{k\in\mathbb{N}}\frac{1}{k^2}=\frac{\pi^2}{6}$.

Da beide Reihen absolut konvergieren, kann ausmultipliziert und beliebig angeordnet werden.

$$\begin{aligned}\frac{\pi^2}{6}\cdot\sum_{d\in\mathbb{N}}\frac{\mu(d)}{d^2} &= \sum_{k\in\mathbb{N}}\frac{1}{k^2}\cdot\sum_{d\in\mathbb{N}}\frac{\mu(d)}{d^2} = \sum_{k\in\mathbb{N}}\sum_{d\in\mathbb{N}}\frac{\mu(d)}{(dk)^2}\\ &= \sum_{n\in\mathbb{N}}\frac{1}{n^2}\cdot\sum_{d\mid n}\mu(d) = \sum_{n\in\mathbb{N}}\frac{(\mu*\mathbb{1})(n)}{n^2} = \sum_{n\in\mathbb{N}}\frac{\varepsilon(n)}{n^2} = 1.\end{aligned}$$

das heißt, die Reihe in der letzten Zeile von (❀) hat den Wert $\frac{6}{\pi^2}$.

(iii) Zu (2)
Mit Lemma 5.12 (2) auf Seite 87, Lemma 5.17 (1) auf Seite 92 und dem in (ii) Gezeigten sieht man für alle $x\in\mathbb{R}$ mit $x\geq 1$

$$\begin{aligned}\sum_{n=1}^{\lfloor x\rfloor}\varphi(n) &= \sum_{n=1}^{\lfloor x\rfloor} n\cdot\sum_{d\mid n}\frac{\mu(d)}{d} = \sum_{d=1}^{\lfloor x\rfloor}\frac{\mu(d)}{d}\cdot\sum_{\substack{n=1\\ n\equiv 0(d)}}^{\lfloor x\rfloor} n\\ &= \sum_{d=1}^{\lfloor x\rfloor}\frac{\mu(d)}{d}\cdot\sum_{m=1}^{\left\lfloor\frac{x}{d}\right\rfloor} md = \sum_{d=1}^{\lfloor x\rfloor}\mu(d)\cdot\frac{1}{2}\cdot\left\lfloor\frac{x}{d}\right\rfloor\cdot\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right)\\ &= \frac{1}{2}\cdot\sum_{d=1}^{\lfloor x\rfloor}\mu(d)\cdot\left(\frac{x^2}{d^2}+O\left(\frac{x}{d}\right)\right) = \frac{x^2}{2}\cdot\sum_{d=1}^{\lfloor x\rfloor}\frac{\mu(d)}{d^2}+O\left(x\cdot\sum_{d=1}^{\lfloor x\rfloor}\frac{1}{d}\right)\\ &= \frac{x^2}{2}\cdot\sum_{d\in\mathbb{N}}\frac{\mu(d)}{d^2}+O(x\cdot\ln(x)) = \frac{3}{\pi^2}\cdot x^2+O(x\cdot\ln(x)),\end{aligned}$$

wobei der Reihenrest für alle $x\in\mathbb{R}$ mit $x\geq 2$ wie oben abgeschätzt werden kann durch

$$\begin{aligned}\left|-\frac{x^2}{2}\cdot\sum_{\substack{d\in\mathbb{N}\\ d>x}}\frac{\mu(d)}{d^2}\right| &\leq \frac{x^2}{2}\cdot\sum_{\substack{d\in\mathbb{N}\\ d\geq\lfloor x\rfloor+1}}\frac{1}{d^2}\leq\frac{x^2}{2}\cdot\int_{\lfloor x\rfloor}^{\infty}\frac{1}{t^2}\,\mathrm{d}t = \frac{x^2}{2}\cdot\left[-\frac{1}{t}\right]_{t=\lfloor x\rfloor}^{t=\infty}\\ &= \frac{x^2}{2}\cdot\frac{1}{\lfloor x\rfloor}\leq\frac{x^2}{2\cdot(x-1)}\leq\frac{x^2}{2\cdot\frac{x}{2}} = x.\end{aligned}$$

□

Das Verhalten der Summe $\sum_{n=1}^{\lfloor x\rfloor}\mu(x)$ für $x\in\mathbb{R}$ mit $x\geq 1$, also insbesondere die Häufigkeit quadratfreier Zahlen mit geradzahlig bzw. ungeradzahlig vielen Primfaktoren, ist wesentlich schwieriger zu studieren. Jedenfalls ist das hier mehrfach benutzte Prinzip, eine zahlentheoretische Funktion f als Faltung zu schreiben, und in der entstehenden Doppelsumme die Reihenfolge richtig zu wählen, bei μ nicht ohne Weiteres anwendbar.

Kapitel 6: Elementare Primzahltheorie

In diesem Kapitel soll die Verteilung der Primzahlen, insbesondere ihre Häufigkeit innerhalb der natürlichen Zahlen, näher untersucht werden.

Definition 6.1

a) Die **Primzahlzählfunktion** heißt

$$\pi : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{N}_0 \\ x & \mapsto & \pi(x) := \#\{p \in \mathbb{P} \,;\, p \leq x\} \end{array} \right\}$$

b) Die **erste** Чебышёв[‡]**–Funktion** wird definiert durch

$$\vartheta : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \vartheta(x) := \sum\limits_{\substack{p \in \mathbb{P} \\ p \leq x}} \ln(p) \end{array} \right\}$$

c) Die **zweite** Чебышёв**–Funktion** wird definiert durch

$$\psi : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \psi(x) := \sum\limits_{n=1}^{\lfloor x \rfloor} \Lambda(n) \end{array} \right\}$$

Lemma 6.2 (Primfaktorzerlegung von $n!$ mit $n \in \mathbb{N}_0$)
VORAUSSETZUNG: *Sei* $a : \left\{ \begin{array}{ccc} \mathbb{P} \times \mathbb{N}_0 & \to & \mathbb{N}_0 \\ (p,n)^T & \mapsto & a_{p,n} \end{array} \right\}$ *mit* $n! = \prod\limits_{p \in \mathbb{P}} p^{a_{p,n}}$ *für alle* $n \in \mathbb{N}_0$.

BEHAUPTUNG: *Dann gilt für alle* $n \in \mathbb{N}$ *und alle* $p \in \mathbb{P}$

$$a_{p,n} = \sum_{\ell \in \mathbb{N}} \left\lfloor \frac{n}{p^\ell} \right\rfloor .$$

Bemerkung
Die Summe wird nur formal bis unendlich erstreckt, da für $p \in \mathbb{P}$, $n \in \mathbb{N}_0$ und $\ell \in \mathbb{N}$ mit $p^\ell > n$ der ℓ–te Summand verschwindet.

[‡]sprich: „CHEBYSHEV“

Beweis:
Seien $n \in \mathbb{N}_0$, $p \in \mathbb{P}$ und $j \in \mathbb{N}_0$.
Ein $r \in \mathbb{N}_0$ mit $r \leq n$, das p in genau j–ter Potenz enthält, liefert zu $a_{p,n}$ den Beitrag j.
Also ist

$$\begin{aligned} a_{p,n} &= \sum_{\ell \in \mathbb{N}_0} \ell \cdot \# \left\{ r \in \mathbb{N}_0 \, ; r \leq n, p^\ell | r \text{ und } p^{\ell+1} \not| \, r \right\} \\ &= \sum_{\ell \in \mathbb{N}_0} \ell \cdot \left(\# \left\{ r \in \mathbb{N}_0 \, ; r \leq n \text{ und } p^\ell | r \right\} - \# \left\{ r \in \mathbb{N}_0 \, ; r \leq n \text{ und } p^{\ell+1} | r \right\} \right) \\ &= \sum_{\ell \in \mathbb{N}_0} \ell \cdot \left(\left\lfloor \frac{n}{p^\ell} \right\rfloor - \left\lfloor \frac{n}{p^{\ell+1}} \right\rfloor \right) = \sum_{\ell \in \mathbb{N}_0} \ell \cdot \left\lfloor \frac{n}{p^\ell} \right\rfloor - \sum_{\ell \in \mathbb{N}} (\ell - 1) \cdot \left\lfloor \frac{n}{p^\ell} \right\rfloor \\ &= \sum_{\ell \in \mathbb{N}} \left\lfloor \frac{n}{p^\ell} \right\rfloor. \end{aligned}$$

□

Numerische Untersuchungen brachten Mathematiker wie Euler, Legendre und Gauss zu der Vermutung, dass π sich näherungsweise wie $x \cdot \ln(x)$ verhält. Das erste in diese Richtung führende Ergebnis ist

Satz 6.3 (Satz von Чебышёв)
(1850, Пафну́тий Льво́вич Чебышёв[‡‡], 1821–1894)

Behauptung: *Für alle $j \in \{1, 2, 3, 4, 5, 6\}$ existieren $C_j \in \mathbb{R}$ mit $C_j > 0$, so dass für alle $x \in \mathbb{R}$ mit $x \geq 2$ gilt:*

(1) $$C_1 \cdot \frac{x}{\ln(x)} \leq \pi(x) \leq C_2 \cdot \frac{x}{\ln(x)},$$

(2) $$C_3 \cdot x \leq \psi(x) \leq C_4 \cdot x$$

und

(3) $$C_5 \cdot x \leq \vartheta(x) \leq C_6 \cdot x.$$

Bemerkungen

1. Diese drei Aussagen sind äquivalent.

2. Auf die Werte der Konstanten wird hier nicht geachtet.

   Der angegebene Beweis führt beispielsweise zu $C_1 = \frac{1}{8}$ und $C_2 = 12$.

[‡‡]sprich: „Pafnuty Lvovich Chebyshev“

BEWEIS:

(i) Von ϑ zu π und ψ
Es wird sich als günstig erweisen, (3) zu beweisen.
Aus (3) folgt (1). Denn mit der oberen Abschätzung in (3) ergibt sich für alle $x \in \mathbb{R}$ mit $x \geq 2$

$$\begin{aligned}\pi(x) &= \pi\left(\frac{x}{\ln(x)}\right) + \sum_{\substack{p\in\mathbb{P}\\ \frac{x}{\ln(x)}<p\leq x}} \frac{\ln(p)}{\ln(p)} \\ &\leq \frac{x}{\ln(x)} + \frac{1}{\ln\left(\frac{x}{\ln(x)}\right)} \cdot \sum_{\substack{p\in\mathbb{P}\\ \frac{x}{\ln(x)}<p\leq x}} \ln(p) \\ &\leq \frac{x}{\ln(x)} + \frac{C_7}{\ln(x)} \cdot \vartheta(x) \leq (1 + C_6C_7) \cdot \frac{x}{\ln(x)}\end{aligned}$$

mit einem $C_7 \in \mathbb{R}$ mit $C_7 > 0$.
Umgekehrt folgt aus (3) für alle $x \in \mathbb{R}$ mit $x \geq 2$

$$\pi(x) = \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \frac{\ln(p)}{\ln(p)} \geq \frac{\vartheta(x)}{\ln(x)} \geq C_5 \cdot \frac{x}{\ln(x)}.$$

Analog folgt (2) aus (3) wegen $\psi(x) \geq \vartheta(x) \geq C_5 \cdot x$ und

$$\psi(x) = \vartheta(x) + \sum_{\substack{(p,k)^T\in\mathbb{P}\times\mathbb{N}\\ k\geq 2 \text{ und } p^k\leq x}} \ln(p).$$

für alle $x \in \mathbb{R}$ mit $x \geq 2$. In der Doppelsumme treten nur $p \in \mathbb{P}$ mit $p \leq \sqrt{x}$ auf ($x \in \mathbb{R}$ mit $x \geq 2$), also gilt für alle $x \in \mathbb{R}$ mit $x \geq 2$

$$\begin{aligned}\sum_{\substack{(p,k)^T\in\mathbb{P}\times\mathbb{N}\\ k\geq 2 \text{ und } p^k\leq x}} \ln(p) &\leq \sum_{\substack{p\in\mathbb{P}\\ p\leq\sqrt{x}}} \ln(p) \cdot \sum_{k=2}^{\left\lfloor\frac{\ln(x)}{\ln(p)}\right\rfloor} 1 \\ &\leq \sum_{p\leq x^{\frac{1}{2}}} \ln(x) \leq x^{\frac{1}{2}} \cdot \ln(x) \leq C_8 \cdot x\end{aligned}$$

mit einem $C_8 \in \mathbb{R}$ mit $C_8 > 0$ und somit

$$\psi(x) \leq (C_6 + C_8) \cdot x.$$

(ii) Einführung und Abschätzung der B_n
Die entscheidende Idee zum hier geschilderten Beweis von (3) wurde 1932 vom damals 19–jährigen Paul ERDŐS (1913–1997) gefunden.
Es werde für alle $n \in \mathbb{N}$

$$B_n := \binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

betrachtet. B_n genügt für alle $n \in \mathbb{N}$ den Ungleichungen

$$B_n < \sum_{j=0}^{2n} \binom{2n}{j} \cdot 1^j \cdot 1^{2n-j} = (1+1)^{2n} = 4^n,$$

und

$$B_n = \frac{n+1}{1} \cdot \frac{n+2}{2} \cdot \ldots \cdot \frac{2n}{n} \geq 2^n.$$

Also gilt für alle $n \in \mathbb{N}$

$$2^n \leq B_n < 4^n. \qquad (❄)$$

(iii) Obere Abschätzung für ϑ
Sei $P_n := \prod_{\substack{p \in \mathbb{P} \\ n < p \leq 2n}} p$ für alle $n \in \mathbb{N}$.
Für alle $n \in \mathbb{N}$ und alle $p \in \mathbb{P}$ mit $n < p \leq 2n$ teilt p den Zähler $(2n)!$ von B_n, aber nicht den Nenner $(n!)^2$. Also gilt für alle $n \in \mathbb{N}$

$$P_n | B_n \qquad \text{und insbesondere} \qquad P_n \leq B_n.$$

Wegen der für alle $n \in \mathbb{N}$ gültigen Identität

$$P_n = \exp\left(\sum_{\substack{p \in \mathbb{P} \\ n < p \leq 2n}} \ln(p) \right) = \exp\left(\vartheta(2n) - \vartheta(n) \right)$$

ergibt sich daraus für alle $n \in \mathbb{N}$ mit (❄)

$$\vartheta(2n) - \vartheta(n) \leq \ln(B_n) < n \cdot \ln(4).$$

Seien nun $x \in \mathbb{R}$ und $k \in \mathbb{N}$ mit $2 \leq x < 2^k \leq 2x$.
Die Anwendung der letzten Abschätzung auf die Zweierpotenzen unterhalb von $2x$ liefert

$$\begin{aligned} \vartheta(x) &\leq \vartheta\left(2^k\right) \\ &= \left(\vartheta\left(2^k\right) - \vartheta\left(2^{k-1}\right)\right) + \left(\vartheta\left(2^{k-1}\right) - \vartheta\left(2^{k-2}\right)\right) + \ldots + \left(\vartheta\left(2^1\right) - \vartheta\left(2^0\right)\right) + \vartheta(1) \\ &= \sum_{j=0}^{k-1} \left(\vartheta\left(2^{j+1}\right) - \vartheta\left(2^j\right)\right) < \ln(4) \cdot \sum_{j=0}^{k-1} 2^j \leq \ln(4) \cdot 2^k \leq \ln(16) \cdot x. \end{aligned}$$

(iv) Untere Abschätzung von ϑ

Bei der linken Ungleichung in (3) muss man etwas sorgfältiger vorgehen.

Sei $a: \left\{ \begin{array}{ccc} \mathbb{P}\times\mathbb{N}_0 & \to & \mathbb{N}_0 \\ (p,n)^T & \mapsto & a_{p,n} \end{array} \right\}$ mit $B_n = \prod_{p\in\mathbb{P}} p^{a_{p,n}}$ für alle $n\in\mathbb{N}_0$.

Lemma 6.2 auf Seite 99 ergibt für alle $n\in\mathbb{N}$ und alle $p\in\mathbb{P}$

$$0 \le a_{p,n} = \sum_{\ell\in\mathbb{N}} \left(\left\lfloor \frac{2n}{p^\ell} \right\rfloor - 2\cdot \left\lfloor \frac{n}{p^\ell} \right\rfloor \right).$$

In der Summe brauchen für alle $n\in\mathbb{N}$ und alle $p\in\mathbb{P}$ nur die $\ell\in\mathbb{N}$ mit $\ell \le \frac{\ln(2n)}{\ln(p)}$ berücksichtigt zu werden.

Für alle $n\in\mathbb{N}$, alle $p\in\mathbb{P}$ und alle $\ell\in\mathbb{N}$ sei $\xi_{n,p,\ell} := \frac{n}{p^\ell} - \left\lfloor \frac{n}{p^\ell} \right\rfloor$.

Für alle $n\in\mathbb{N}$, alle $p\in\mathbb{P}$ und alle $\ell\in\mathbb{N}$ folgen $0\le\xi_{n,p,\ell}<1$, $0\le\xi_{2n,p,\ell}<1$ und

$$\begin{aligned} \left\lfloor \frac{2n}{p^\ell} \right\rfloor - 2\cdot \left\lfloor \frac{n}{p^\ell} \right\rfloor &= \left(\frac{2n}{p^\ell} - \xi_{2n,p,\ell} \right) - 2\cdot \left(\frac{n}{p^\ell} - \xi_{n,p,\ell} \right) \\ &= 2\xi_{n,p,\ell} - \xi_{2n,p,\ell} \in \{0,1\}, \end{aligned}$$

da der Wert links ganzzahlig ist.

Somit erhält man $0\le a_{p,n} \le \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor$ für alle $n\in\mathbb{N}$ und alle $p\in\mathbb{P}$. Dies liefert für alle $n\in\mathbb{N}$

$$\begin{aligned} \ln(B_n) = \ln\left(\prod_{p\in\mathbb{P}} p^{a_{p,n}} \right) &\le \sum_{\substack{p\in\mathbb{P}\\ p\le 2n}} \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor \cdot \ln(p) \\ &= \sum_{\substack{p\in\mathbb{P}\\ p\le 2n}} \ln(p) \cdot \sum_{\substack{a\in\mathbb{N}\\ p^a\le 2n}} 1 = \sum_{m=1}^{2n} \Lambda(m) = \psi(2n). \end{aligned}$$

Mit (❄) führt das zu

$$\psi(2n) \ge \ln(2)\cdot n$$

für alle $n\in\mathbb{N}$. Wie in (i) sieht man hiermit $\vartheta(2n)\ge C_9\cdot n$ für alle $n\in\mathbb{N}$ und ein $C_9\in\mathbb{R}$ mit $C_9>0$. Daher ist

$$\vartheta(x) \ge C_5\cdot x. \qquad \square$$

Satz 6.4 (Mertens–Formeln)
Behauptung: *Es gibt ein* $C \in \mathbb{R}$ *mit* $\frac{523}{2000} < C < \frac{327}{1250}$ $(C = 0.2615\ldots)$,

$$\textbf{(1)} \qquad \sum_{n=1}^{\lfloor x \rfloor} \frac{\Lambda(n)}{n} = \ln(x) + O(1),$$

$$\textbf{(2)} \qquad \sum_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{\ln(p)}{p} = \ln(x) + O(1)$$

und

$$\textbf{(3)} \qquad \sum_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{1}{p} = \ln(\ln(x)) + C + O\left(\frac{1}{\ln(x)}\right).$$

Beweis:

(i) Zu (1)
Mit Folgerung 5.7 (3) auf Seite 81 sieht man

$$\sum_{n=1}^{\lfloor x \rfloor} \ln(n) = \sum_{n=1}^{\lfloor x \rfloor} \sum_{d \mid n} \Lambda(d) = \sum_{d=1}^{\lfloor x \rfloor} \Lambda(d) \cdot \sum_{\substack{n=1 \\ n \equiv 0 (d)}}^{\lfloor x \rfloor} 1 = \sum_{d=1}^{\lfloor x \rfloor} \Lambda(d) \cdot \left\lfloor \frac{x}{d} \right\rfloor$$

$$= x \cdot \sum_{d=1}^{\lfloor x \rfloor} \frac{\Lambda(d)}{d} + O(\psi(x)).$$

Satz 6.3 (2) auf Seite 100 und Hilfsatz 5.17 (2) auf Seite 92 ergeben Behauptung (1).

(ii) Zu (2)
Es ist

$$0 \le \sum_{n=1}^{\lfloor x \rfloor} \frac{\Lambda(n)}{n} - \sum_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{\ln(p)}{p} = \sum_{\substack{(p,k)^T \in \mathbb{P} \times \mathbb{N} \\ k \ge 2 \text{ und } p^k \le x}} \frac{\ln(p)}{p^k} \le \sum_{\substack{p \in \mathbb{P} \\ p \le \sqrt{x}}} \ln(p) \cdot \sum_{k \in \mathbb{N} \setminus \{1\}} \frac{1}{p^k}$$

$$\le \sum_{\substack{p \in \mathbb{P} \\ p \le \sqrt{x}}} \ln(p) \cdot \frac{1}{p^2} \cdot \frac{1}{1 - \frac{1}{p}} = \sum_{\substack{p \in \mathbb{P} \\ p \le \sqrt{x}}} \frac{\ln(p)}{p \cdot (p-1)} = O(1).$$

Mit (1) ergibt das Aussage (2).

(iii) Zu (3)
(3) folgt aus (2) mit partieller Summation 5.16 auf Seite 91. Man nimmt

$$f: \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{R} \\ n & \mapsto & f(n) := \begin{cases} \frac{\ln(n)}{n}, & \text{für } n \in \mathbb{P} \\ 0, & \text{sonst} \end{cases} \end{array} \right\} \text{ und}$$

$$g: \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & g(x) \end{array} \right\} \text{ stetig differenzierbar mit } g(t) = \frac{1}{\ln(t)} \text{ für alle } t \in \mathbb{R} \text{ mit } t \ge 2.$$

Nach (2) gibt es ein $R: \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & R(x) \end{array} \right\}$ mit $R(x) = O(1)$ und

$$\sum_{n=1}^{\lfloor x \rfloor} f(n) = \begin{cases} 0, & \text{falls } 1 \leq x < 2 \\ \ln(x) + R(x), & \text{falls } x \geq 2 \end{cases}$$

für alle $x \in \mathbb{R}$ mit $x \geq 1$. Mit partieller Summation folgt für alle $x \in \mathbb{R}$ mit $x \geq 2$

$$\begin{aligned} \sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{p} &= \sum_{n=1}^{\lfloor x \rfloor} f(n) \cdot g(n) \\ &= (\ln(x) + R(x)) \cdot \frac{1}{\ln(x)} + \int_2^x (\ln(t) + R(t)) \cdot \frac{1}{t \cdot \ln^2(t)} \, \mathrm{d}t \\ &= 1 + \frac{R(x)}{\ln(x)} + \int_2^x \frac{1}{t \cdot \ln(t)} \, \mathrm{d}t + \int_2^x \frac{R(t)}{t \cdot \ln^2(t)} \, \mathrm{d}t. \end{aligned}$$

Da wegen $R(t) = O(1)$ das letzte Integral konvergiert, gibt es ein $C' \in \mathbb{R}$ mit

$$\int_2^x \frac{R(t)}{t \cdot \ln^2(t)} \, \mathrm{d}t = C' + O\left(\frac{1}{\ln(x)}\right).$$

Also gibt es ein $C \in \mathbb{R}$ mit $\displaystyle\sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{p} = \ln(\ln(x)) + C + O\left(\frac{1}{\ln(x)}\right)$. □

Hinweis
Die Divergenz der Reihe $\displaystyle\sum_{p \in \mathbb{P}} \frac{1}{p}$ erfolgt außerordentlich langsam.
Zum Beispiel wird der Wert 4 erst etwa beim $\pi(1.79 \cdot 10^{18})$–ten Summanden erreicht.

Satz 6.5 (Summenabschätzungen für ω und Ω)
Behauptung: *Es gibt ein $C \in \mathbb{R}$ und ein $D \in \mathbb{R}$, so dass für alle $x \in \mathbb{R}$ mit $x \geq 3$ gilt:*

(1) $$\sum_{n=1}^{\lfloor x \rfloor} \omega(n) = x \cdot (\ln(\ln(x)) + C) + O\left(\frac{x}{\ln(x)}\right),$$

(2) $$\sum_{n=1}^{\lfloor x \rfloor} \Omega(n) = x \cdot (\ln(\ln(x)) + D) + O\left(\frac{x}{\ln(x)}\right)$$

und

(3) $$\sum_{n=1}^{\lfloor x \rfloor} |\omega(n) - \ln(\ln(x))|^2 = O(x \cdot \ln(\ln(x))).$$

Bemerkung
(1) und (2) besagen, dass die $n \in \mathbb{N}$ mit $n \leq x$ und $x \in \mathbb{R}$ mit $x \geq 3$ im Mittel etwa $\ln(\ln(x))$ Primteiler bzw. Primfaktoren besitzen. Wegen des langsamen Wachstums des iterierten Logarithmus ist dies eine überraschend niedrige Anzahl. Ein Mittelwert kann dadurch erreicht werden, dass viele Werte wesentlich darunter und viele wesentlich darüber liegen. So ist es bei multiplikativen Funktionen oft der Fall. Bei additiven Funktionen ist vielfach eine Versammlung der Werte nahe des Mittelwerts zu beobachten. (3) kann als Varianz–Abschätzung gedeutet werden. Aus (3) folgt insbesondere für jedes $\delta \in \mathbb{R}$ mit $\delta > 0$

$$\begin{aligned}
&\#\left\{n \in \mathbb{N}\,;n \leq x \text{ und } |\omega(n) - \ln(\ln(x))| > \delta \cdot \ln(\ln(x))\right\} \\
&\leq (\delta \cdot \ln(\ln(x)))^{-2} \cdot \sum_{n=1}^{\lfloor x \rfloor} |\omega(n) - \ln(\ln(x))|^2 \\
&= o(x)
\end{aligned}$$

für alle $x \in \mathbb{R}$ mit $x \geq 3$. Das heißt, „für die meisten“ $n \in \mathbb{N}$ mit $n \leq x$ liegt $\omega(x)$ sehr dicht beim Mittelwert $\ln(\ln(x))$. Mit Methoden der analytischen Zahlentheorie und der Stochastik zeigten Erdős und Kac 1940, dass ω dem „zentralen Grenzwertsatz“ genügt:

$$\frac{1}{x} \cdot \#\left\{n \in \mathbb{N}\,;n \leq x \text{ und } \frac{\omega(n) - \ln(\ln(x))}{\sqrt{\ln(\ln(x))}} \leq t\right\} \overset{x\to\infty}{\longrightarrow} \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{t} \exp\left(-\frac{y^2}{2}\right) \mathrm{d}y$$

für jedes $t \in \mathbb{R}$.

Ein so regelmäßiges Verhalten zeigen multiplikative Funktionen im Allgemeinen nicht.

Beweis:

(i) Zu (1)
Nach Satz 6.4 (3) auf Seite 104 und dem Satz von Чебышёв 6.3 (1) auf Seite 100 gibt es ein $C \in \mathbb{R}$ mit

$$\begin{aligned}
\sum_{n=1}^{\lfloor x \rfloor} \omega(n) &= \sum_{n=1}^{\lfloor x \rfloor} \sum_{\substack{p \in \mathbb{P} \\ p|n}} 1 = \sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \left\lfloor \frac{x}{p} \right\rfloor = x \cdot \sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{p} + O(\pi(x)) \\
&= x \cdot \left(\ln(\ln(x)) + C + O\left(\frac{1}{\ln(x)}\right)\right) + O\left(\frac{x}{\ln(x)}\right)
\end{aligned}$$

für alle $x \in \mathbb{R}$ mit $x \geq 3$.

(ii) Zu (2)
(2) ergibt sich analog mit

$$\begin{aligned}
0 \leq \sum_{n=1}^{\lfloor x \rfloor} \Omega(n) &= \sum_{\substack{(p,k)^T \in \mathbb{P} \times \mathbb{N} \\ p^k \leq x}} \left\lfloor \frac{x}{p^k} \right\rfloor \\
&\leq x \cdot \sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{p} + O(\pi(x)) + x \cdot \sum_{\substack{(p,k)^T \in \mathbb{P} \times \mathbb{N} \\ k \geq 2 \text{ und } p^k \leq x}} \frac{1}{p^k} + \sum_{\substack{(p,k)^T \in \mathbb{P} \times \mathbb{N} \\ k \geq 2 \text{ und } p^k \leq x}} O(1)
\end{aligned}$$

für alle $x \in \mathbb{R}$.
Der Beitrag der p^k mit $p \in \mathbb{P}$ und $k \in \mathbb{N} \setminus \{1\}$ erweist sich als

$$\begin{aligned}
x \cdot \sum_{\substack{(p,k)^T \in \mathbb{P}\times\mathbb{N} \\ k\geq 2 \text{ und } p^k \leq x}} \frac{1}{p^k} + \sum_{\substack{(p,k)^T \in \mathbb{P}\times\mathbb{N} \\ k\geq 2 \text{ und } p^k \leq x}} O(1) &\leq x \cdot \sum_{\substack{p\in\mathbb{P} \\ p\leq x}} \sum_{k\in\mathbb{N}\setminus\{1\}} \left(\frac{1}{p}\right)^k + \sum_{\substack{p\in\mathbb{P} \\ p\leq x}} \sum_{k=2}^{\left\lfloor \frac{\ln(x)}{\ln(p)} \right\rfloor} O(1) \\
&= x \cdot \sum_{\substack{p\in\mathbb{P} \\ p\leq x}} \left(\frac{1}{1-\frac{1}{p}} - \frac{1}{p^1} - \frac{1}{p^0}\right) + \sum_{\substack{p\in\mathbb{P} \\ p\leq x}} O\left(\left\lfloor \frac{\ln(x)}{\ln(p)} \right\rfloor - 1\right) \\
&\leq x \cdot \sum_{n\in\mathbb{N}\setminus\{1\}} \left(\frac{n}{n-1} - \frac{n+1}{n}\right) + \sum_{\substack{p\in\mathbb{P} \\ p\leq x}} O\left(\frac{\ln(x)}{\ln(p)}\right) \\
&\leq x \cdot \sum_{n\in\mathbb{N}\setminus\{1\}} \frac{1}{n\cdot(n-1)} + O\left(\ln(x) \cdot \sum_{\substack{p\in\mathbb{P} \\ p\leq x}} \frac{1}{p}\right) \\
&\leq x \cdot \sum_{n\in\mathbb{N}} \frac{1}{n^2} + O(\ln(x) \cdot \ln(\ln(x))) \\
&= O(x)
\end{aligned}$$

wegen der Konvergenz der verbliebenen Reihe und Satz 6.4 (3) auf Seite 104.

(iii) Zu (3)
Seien $x \in \mathbb{R}$ mit $x \geq 3$, $y := x^{\frac{1}{4}}$ und

$$\tilde{\omega} : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N}_0 \\ n & \mapsto & \tilde{\omega}(n) := \#\left\{ p \in \mathbb{P} \,;\, p|n \text{ und } p \leq x^{\frac{1}{4}} \right\} \end{array} \right\}.$$

Dann gilt für alle $n \in \mathbb{N}$ mit $n \leq x$

$$0 \leq \omega(n) - \tilde{\omega}(n) \leq 3$$

da n höchstens drei Primteiler zwischen $x^{\frac{1}{4}}$ und x besitzt.
Mit $\ln(\ln(x)) - \ln(\ln(y)) = \ln(4)$ und der für alle $a \in \mathbb{R}$ und alle $b \in \mathbb{R}$ gültigen Ungleichung $(a+b)^2 \leq 2\cdot(a^2+b^2)$ sieht man

$$\begin{aligned}
S(x) := \sum_{n=1}^{\lfloor x \rfloor} |\omega(n) - \ln(\ln(x))|^2 &= \sum_{n=1}^{\lfloor x \rfloor} (\tilde{\omega}(n) - \ln(\ln(y)) + O(1))^2 \\
&\leq 2 \cdot \sum_{n=1}^{\lfloor x \rfloor} (\tilde{\omega}(n) - \ln(\ln(y)))^2 + O(x) \\
&= 2 \cdot \left(\sum_{n=1}^{\lfloor x \rfloor} \tilde{\omega}^2(n) - 2 \cdot \ln(\ln(y)) \cdot \sum_{n=1}^{\lfloor x \rfloor} \tilde{\omega}(n) + (\ln(\ln(y)))^2 \cdot x \right) + O(x). \qquad (\maltese)
\end{aligned}$$

Wegen Satz 6.4 (3) auf Seite 104 ist

$$\begin{aligned}\sum_{n=1}^{\lfloor x\rfloor}\tilde{\omega}^2(n) &= \sum_{\substack{p\in\mathbb{P}\\ p\le y}}\sum_{\substack{q\in\mathbb{P}\\ q\le y}} \#\{n\in\mathbb{N}\,; n\le x, p|n \text{ und } q|n\}\\ &= \sum_{\substack{p\in\mathbb{P}\\ p\le y}}\sum_{\substack{q\in\mathbb{P}\setminus\{p\}\\ q\le y}}\left\lfloor\frac{x}{pq}\right\rfloor + \sum_{\substack{p\in\mathbb{P}\\ p\le y}}\left\lfloor\frac{x}{p}\right\rfloor\\ &= \sum_{\substack{p\in\mathbb{P}\\ p\le y}}\sum_{\substack{q\in\mathbb{P}\\ q\le y}}\left\lfloor\frac{x}{pq}\right\rfloor - \sum_{\substack{p\in\mathbb{P}\\ p\le y}}\left\lfloor\frac{x}{p^2}\right\rfloor + \sum_{\substack{p\in\mathbb{P}\\ p\le y}}\left\lfloor\frac{x}{p}\right\rfloor\\ &= x\cdot\sum_{\substack{p\in\mathbb{P}\\ p\le y}}\frac{1}{p}\cdot\sum_{\substack{p\in\mathbb{P}\\ p\le y}}\frac{1}{p} + O\left(y^2\right) - x\cdot\sum_{\substack{p\in\mathbb{P}\\ p\le y}}\frac{1}{p^2} + O(y) + x\cdot\sum_{\substack{p\in\mathbb{P}\\ p\le y}}\frac{1}{p} + O(y)\\ &= x\cdot(\ln(\ln(y)))^2 + O(x\cdot\ln(\ln(y)))\,.\end{aligned}$$

Aus (1) ergibt sich

$$\sum_{n\le x}\tilde{\omega}(n) = x\cdot\ln(\ln(y)) + O(x)\,.$$

Damit wird aus (❄)

$$\begin{aligned}S(x) &\le 2\cdot\left(\sum_{n=1}^{\lfloor x\rfloor}\tilde{\omega}^2(n) - 2\cdot\ln(\ln(y))\cdot\sum_{n=1}^{\lfloor x\rfloor}\tilde{\omega}(n) + (\ln(\ln(y)))^2\cdot x\right) + O(x)\\ &= 2\cdot\big(\quad x\cdot(\ln(\ln(y)))^2 + O(x\cdot\ln(\ln(y)))\\ &\qquad - 2\cdot\ln(\ln(y))\cdot(x\cdot\ln(\ln(y)) + O(x))\\ &\qquad + (\ln(\ln(y)))^2\cdot x\big) + O(x)\\ &= O(x\cdot\ln(\ln(y)))\,,\end{aligned}$$

also wegen $S(x) = \sum_{n=1}^{\lfloor x\rfloor}|\omega(n) - \ln(\ln(x))|^2 \ge 0$

$$\sum_{n=1}^{\lfloor x\rfloor}|\omega(n) - \ln(\ln(x))|^2 = O(x\ln(\ln(x)))\,. \qquad \square$$

Mit zusätzlichem Aufwand kann man

$$\sum_{n=1}^{\lfloor x\rfloor}|\omega(n) - \ln(\ln(x))|^2 = x\ln(\ln(x)) + O(x)$$

für alle $x\in\mathbb{R}$ mit $x\ge 3$ zeigen.

Der numerische Vergleich von $\pi(x)$ und $\dfrac{x}{\ln(x)}$ legt die Vermutung nahe, dass $\pi(x)\cdot\left(\dfrac{x}{\ln(x)}\right)^{-1}$ für $x \to \infty$ gegen 1 konvergiert. Dies ist der Inhalt des berühmten Primzahlsatzes. Das Problem besteht hier darin, die Existenz des Limes zu zeigen.

Satz 6.6 (Im Konvergenzfall ist $\lim\limits_{x\to\infty} \pi(x)\cdot\left(\frac{x}{\ln(x)}\right)^{-1} = 1$)
(Чебышёв)

Behauptung: *Falls* $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{\frac{x}{\ln(x)}}$ *existiert, hat er den Wert* 1.

Beweis:

(i) Partielle Summation
Es existiere $A := \lim\limits_{x\to\infty} \dfrac{\pi(x)}{\frac{x}{\ln(x)}}$. Dann gibt es ein $\delta : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \delta(x) \end{array} \right\}$ mit $\lim\limits_{x\to\infty} \delta(x) = 0$ und

$$\pi(x) = A\cdot\frac{x}{\ln(x)} + \delta(x)\cdot\frac{x}{\ln(x)}.$$

für alle $x \in \mathbb{R}$. Partielle Summation 5.16 auf Seite 91 mit

$$f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{R} \\ n & \mapsto & f(n) := \begin{cases} 1, & \text{falls } n \in \mathbb{P} \\ 0, & \text{falls } n \notin \mathbb{P} \end{cases} \end{array} \right\},$$

$\sum\limits_{n=1}^{\lfloor x\rfloor} f(n) = \pi(n)$ und $g : \left\{ \begin{array}{ccc} \mathbb{R}\setminus\{0\} & \to & \mathbb{R} \\ t & \mapsto & g(t) := \frac{1}{t} \end{array} \right\}$ ergibt für alle $x \in \mathbb{R}$ mit $x \geq 3$

$$\begin{aligned} \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \frac{1}{p} &= \sum_{n=1}^{\lfloor x\rfloor} f(n)\cdot g(n) = \frac{\pi(x)}{x} + \int_2^x \frac{\pi(t)}{t^2}\,\mathrm{d}t \\ &= O\left(\frac{1}{\ln(x)}\right) + A\cdot\int_2^x \frac{1}{t\cdot\ln(t)}\,\mathrm{d}t + \int_2^x \frac{\delta(t)}{t\cdot\ln(t)}\,\mathrm{d}t. \qquad (❁) \end{aligned}$$

(ii) Abschätzung des hinteren Integrals
Sei $\eta \in \mathbb{R}$ mit $\eta > 0$. Es gibt ein $x_0(\eta) \in \mathbb{R}$ und ein $C_1(\eta) \in \mathbb{R}$ mit $x_0(\eta) \geq 3$, $C_1(\eta) > 0$, $|\delta(x)| \leq \eta$ für alle $x \in \mathbb{R}$ mit $x \geq x_0(\eta)$ und $|\delta(x)| \leq C_1(\eta)$ für alle $x \in \mathbb{R}$ mit $2 \leq x \leq x_0(\eta)$. Für alle $x \in \mathbb{R}$ mit $x \geq x_0(\eta)$ ist

$$\begin{aligned} \left|\int_2^x \frac{\delta(t)}{t\cdot\ln(t)}\,\mathrm{d}t\right| &\leq C_1(\eta)\cdot\int_2^{x_0(\eta)} \frac{1}{t\cdot\ln(t)}\,\mathrm{d}t + \eta\cdot\int_{x_0(\eta)}^x \frac{1}{t\cdot\ln(t)}\,\mathrm{d}t \\ &\leq C_1(\eta)\cdot\ln(\ln(x_0(\eta))) + \eta\cdot\ln(\ln(x)). \end{aligned}$$

Also gibt es ein $x_1(\eta) \in \mathbb{R}$ mit $x_1(\eta) \geq 3$ und

$$\left| \int_2^x \frac{\delta(t)}{t \cdot \ln(t)} \, \mathrm{d}t \right| \leq 2\eta \cdot \ln(\ln(x))$$

für alle $x \in \mathbb{R}$ mit $x \geq x_1(\eta)$. Aus (❄) erhält man daher

$$\sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{p} = A \cdot \ln(\ln(x)) + o(\ln(\ln(x))),$$

was nach Satz 6.4 (3) auf Seite 104 nur für $A = 1$ richtig sein kann. □

Den entscheidenden Anstoß zum Beweis des Primzahlsatzes gab 1859 Bernhard Riemann (1826–1866) durch das Studium der nach ihm benannten „**Riemannschen Zeta–Funktion**“

$$\zeta : \left\{ \begin{array}{rcl} \{z \in \mathbb{C} \,;\, \mathrm{Re}(z) > 1\} & \to & \mathbb{C} \\ s & \mapsto & \zeta(s) := \displaystyle\sum_{n \in \mathbb{N}} \frac{1}{n^s} \end{array} \right\}.$$

Ihre Bedeutung für die Primzahlverteilung wird sichtbar durch die im gleichen Bereich, also für alle $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$ gültigen Formeln

$$\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \qquad \text{und} \qquad -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n \in \mathbb{N}} \frac{\Lambda(n)}{n^s}.$$

Nach der von Riemann vorgeschlagenen Methode konnten 1896 erstmals Jaques Hadamard (1866–1963) und Charles de la Vallée–Poussin (1866–1962) den Primzahlsatz beweisen. Einen elementaren Zugang, der ganz ohne komplexe Funktionentheorie auskommt, fanden 1948 Paul Erdős und Atle Selberg.

Primzahlsatz

Behauptung: *Es gelten die asymptotischen Formeln*

(1) $\pi(x) = \dfrac{x}{\ln(x)} + o\left(\dfrac{x}{\ln(x)}\right)$, *also* $\dfrac{\pi(x)}{\frac{x}{\ln(x)}} \overset{x \to \infty}{\longrightarrow} 1$,

(2) $\psi(x) = x + o(x)$, *also* $\dfrac{\psi(x)}{x} \overset{x \to \infty}{\longrightarrow} 1$

und

(3) $\displaystyle\sum_{n=1}^{\lfloor x \rfloor} \mu(n) = o(x)$, *also* $\displaystyle\sum_{n=1}^{\lfloor x \rfloor} \frac{\mu(n)}{x} \overset{x \to \infty}{\longrightarrow} 0.$

Ein analytischer Beweis zu (1) und (2) — deren Äquivalenz leicht einzusehen ist — wird in jeder Vorlesung zur analytischen Zahlentheorie gegeben.

Der elementare Beweis erfordert zwar keine weitgehenden Hilfsmittel, ist aber extrem verwickelt. Als Beispiel für kunstvolle elementare Umformungen, insbesondere mit Hilfe der MÖBIUS–Funktion, soll hier die Implikation „(2) $\Longrightarrow$ (3)“ gezeigt werden:

Lemma 6.7 („(2) $\Longrightarrow$ (3)“ im Primzahlsatz)

VORAUSSETZUNG: *Es sei* $M:\ \left\{\begin{array}{ccc}\mathbb{R} & \to & \mathbb{Z}\\ x & \mapsto & M(x):=\displaystyle\sum_{n=1}^{\lfloor x\rfloor}\mu(n)\end{array}\right\}$.

BEHAUPTUNG: *Aus* $\lim\limits_{x\to\infty}\dfrac{\psi(x)}{x}=1$ *folgt* $\lim\limits_{x\to\infty}\dfrac{M(x)}{x}=0$.

BEWEIS:

(i) Einführung von δ

Es gelte $\lim\limits_{x\to\infty}\dfrac{\psi(x)}{x}=1$. Dann gibt es ein $\delta:\ \left\{\begin{array}{ccc}\mathbb{R} & \to & \mathbb{R}\\ x & \mapsto & \delta(x)\end{array}\right\}$ mit

$$\psi(x)=\sum_{n=1}^{\lfloor x\rfloor}\Lambda(n)=x+\delta(x)\cdot x \qquad \text{und} \qquad \lim_{t\to\infty}\delta(t)=0 \tag{❋}$$

für alle $x\in\mathbb{R}$ mit $x\geq 0$. Sei $x\in\mathbb{R}$ mit $x\geq 0$.

(ii) $M(x)\cdot\ln(x)=\sum\mu(n)\cdot\ln(n)+O(x)$

Mit Lemma 5.17 (2) auf Seite 92 sieht man

$$\begin{aligned}M(x)\cdot\ln(x)&=\sum_{n=1}^{\lfloor x\rfloor}\mu(n)\cdot\ln\left(\frac{x}{n}\right)+\sum_{n=1}^{\lfloor x\rfloor}\mu(n)\cdot\ln(n)\\&=\sum_{n=1}^{\lfloor x\rfloor}\mu(n)\cdot\ln(n)+O\left(\sum_{n=1}^{\lfloor x\rfloor}\ln\left(\frac{x}{n}\right)\right)\\&=\sum_{n=1}^{\lfloor x\rfloor}\mu(n)\cdot\ln(n)+O(x).\end{aligned}$$

(iii) Aufsplitten der Summe in (ii) in zwei Teilsummen nach (❋)
Mit der nach Lemma 5.13 auf Seite 88 für alle $n \in \mathbb{N}$ gültigen Formel

$$\begin{aligned}(\Lambda * \mu)(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot \Lambda(d) &= -\sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot \sum_{k|d} \mu(k) \cdot \ln(k) \\ &= -\sum_{k|n} \mu(k) \cdot \ln(k) \cdot \sum_{\substack{d|n \\ d \equiv 0(k)}} \mu\left(\frac{n}{d}\right) \\ &= -\sum_{k|n} \mu(k) \cdot \ln(k) \cdot \sum_{\ell|\frac{n}{k}} \mathbb{1}(\ell) \cdot \mu\left(\frac{\frac{n}{k}}{\ell}\right) \\ &= -\sum_{k|n} \mu(k) \cdot \ln(k) \cdot \varepsilon\left(\frac{n}{k}\right) \\ &= -\mu(n) \cdot \ln(n)\end{aligned}$$

erhält man mit (❋)

$$\begin{aligned}-\sum_{n=1}^{\lfloor x \rfloor} \mu(n) \cdot \ln(n) = \sum_{n=1}^{\lfloor x \rfloor} \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot \Lambda(d) &= \sum_{\substack{(d,k)^T \in \mathbb{N}^2 \\ dk \le x}} \mu(k) \cdot \Lambda(d) \\ &= \sum_{k=1}^{\lfloor x \rfloor} \mu(k) \cdot \sum_{d=1}^{\lfloor \frac{x}{k} \rfloor} \Lambda(d) = \sum_{k=1}^{\lfloor x \rfloor} \mu(k) \cdot \psi\left(\frac{x}{k}\right) \\ &= x \cdot \sum_{k=1}^{\lfloor x \rfloor} \frac{\mu(k)}{k} + x \cdot \sum_{k=1}^{\lfloor x \rfloor} \frac{\mu(k)}{k} \cdot \delta\left(\frac{x}{k}\right) \qquad (\text{❇})\end{aligned}$$

(iv) Abschätzen der ersten Summe aus (❇)
Es gilt

$$\begin{aligned}x \cdot \sum_{k=1}^{\lfloor x \rfloor} \frac{\mu(k)}{k} &= \sum_{k=1}^{\lfloor x \rfloor} \mu(k) \cdot \left(\left\lfloor \frac{x}{k} \right\rfloor + O(1)\right) = \sum_{k=1}^{\lfloor x \rfloor} \mu(k) \cdot \sum_{d=1}^{\lfloor \frac{x}{k} \rfloor} 1 + O(x) \\ &= \sum_{\substack{(d,k)^T \in \mathbb{N}^2 \\ dk \le x}} \mu(k) + O(x) = \sum_{n=1}^{\lfloor x \rfloor} \sum_{k|n} \mu(k) \cdot \mathbb{1}\left(\frac{n}{k}\right) + O(x) \\ &= \sum_{n=1}^{\lfloor x \rfloor} \varepsilon(n) + O(x) = 1 + O(x) = O(x).\end{aligned}$$

(v) Abschätzen der zweiten Summe aus (❇)
Sei $\eta \in \mathbb{R}$ mit $\eta > 0$. Nach (❋) existiert ein $x_0(\eta) \in \mathbb{R}$ mit $x_0(\eta) \geq 1$, so dass $|\delta(t)| \leq \eta$ für alle $t \in \mathbb{R}$ mit $t \geq x_0(\eta)$ erfüllt ist. Ferner gibt es ein $C_1(\eta)$ mit $C_1(\eta) \geq 0$ und $|\delta(t)| \leq C_1(\eta)$ für alle $t \in \mathbb{R}$ mit $0 \leq t \leq x_0(\eta)$. Damit ergibt sich im Falle $x \geq x_0(\eta)$

$$\left| x \cdot \sum_{k=1}^{\lfloor x \rfloor} \frac{\mu(k)}{k} \cdot \delta\left(\frac{x}{k}\right) \right| \leq x \cdot \sum_{k=1}^{\left\lfloor \frac{x}{x_0(\eta)} \right\rfloor} \frac{\eta}{k} + x \cdot \sum_{k=\left\lfloor \frac{x}{x_0(\eta)} \right\rfloor + 1}^{\lfloor x \rfloor} \frac{C_1(\eta)}{k}.$$

Anwendung von Lemma 5.17 (1) auf Seite 92 führt zu

$$\begin{aligned} \left| x \cdot \sum_{k=1}^{\lfloor x \rfloor} \frac{\mu(k)}{k} \cdot \delta\left(\frac{x}{k}\right) \right| &\leq \eta \cdot x \cdot \sum_{k=1}^{\lfloor x \rfloor} \frac{1}{k} + C_1(\eta) \cdot x \cdot \left(\ln(x) - \ln\left(\frac{x}{x_0}\right) + O(1) \right) \\ &\leq \eta \cdot x \cdot \ln(x) + C_2(\eta) \cdot x \end{aligned}$$

mit einem $C_2(\eta) \in \mathbb{R}$.

(vi) Zusammenführung
Fasst man das Vorige zusammen, dann ergibt sich im Falle $x \geq x_0(\eta)$ die Existenz eines $C_3 \in \mathbb{R}$ mit $C_3 > 0$ und eines $C_4(\eta)$ mit $C_4(\eta) > 0$ und

$$|M(x)| \leq \frac{1}{\ln(x)} \cdot \left| \sum_{n=1}^{\lfloor x \rfloor} \mu(n) \cdot \ln(n) \right| + C_3 \cdot \frac{x}{\ln(x)} \leq \eta \cdot x + C_4(\eta) \cdot \frac{x}{\ln(x)}.$$

Also existiert ein $x_1(\eta) \in \mathbb{R}$ mit $x_1(\eta) \geq x_0(\eta)$, so dass im Falle $x \geq x_1(\eta)$

$$|M(x)| \leq 2\eta \cdot x$$

gilt. Dies besagt aber $M(x) = o(x)$. □

In ähnlicher Weise kann auch die Umkehrung „(3) $\Longrightarrow$ (2)“ gezeigt werden. Insofern ist es gleichgültig, ob man (1), (2) oder (3) ansteuert. Dementsprechend gibt es elementare Beweise von vergleichbarem Schwierigkeitsgrad zu (2) oder (3). (1) wird seltener direkt gezeigt, da die Indikatorfunktion zur Menge der Primzahlen nicht so günstige Summationseigenschaften hat wie die VON MANGOLDT–Funktion Λ.

Index

[‡]sprich: „Chebyshev“

‡sprich: „CHEBYSHEV“