Einführung in die Zahlentheorie

Prof. J. Sander
Universität Hannover
WS 2000/01

LaTeX 2_ε-Umsetzung von Miriam Westerfrölke und Marco Pries

Inhaltsverzeichnis

0 Grundlagen

$$\mathbb{N} = \{1, 2, \ldots\}$$

erfüllt die Peano-Axiome. Die wesentlichen Eigenschaften für uns sind:

Satz 0.1

Sei $M \subseteq \mathbb{N}$

(i) Ist $1 \in M$ und gilt für alle $n \in M$, dass auch $n + 1 \in M$, so ist $M = \mathbb{N}$.

(ii) Ist $M \neq \emptyset$, so enthält M genau ein kleinstes Element.

Auf $\mathbb{N}$ lassen sich Addition und Multiplikation erklären. Diese sind kommutativ, assoziativ und distributiv. $\mathbb{N}$ lässt sich so anordnen, dass für alle $m, n \in \mathbb{N}$ gilt: $m = n$ oder $m < n$ oder $m > n$. Aus $\mathbb{N}$ erhalten wir leicht
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ und $\mathbb{Q} = \{a/b : a \in \mathbb{Z}, b \in \mathbb{N}\}$.

Weiterhin verwenden wir die Menge $\mathbb{R}$ der reellen Zahlen und die Menge $\mathbb{C}$ der komplexen Zahlen. Aus Satz 0.1 folgt leicht

Satz 0.2

Sei $M \subseteq \mathbb{Z}$

(i) Ist $a \in M$ und gilt für alle $n \in M$ mit $n \geq a$, dass auch $n + 1 \in M$, so ist

$$\{n \geq a : n \in M\} = \{n \geq a : n \in \mathbb{Z}\}.$$

(ii) Sei $M \neq \emptyset$. Ist M nach unten beschränkt, so enthält M genau ein kleinstes Element. Ist M nach oben beschränkt, so enthält M genau ein größtes Element.

1 Teilbarkeit

Definition:

Seien $a, b \in \mathbb{N}$. Wir sagen a *teilt* b, geschrieben $a \mid b$, falls ein $c \in \mathbb{N}$ existiert derart, dass $b = c \cdot a$. Dann heißt a *Teiler* oder *Faktor* von b, b heißt *Vielfaches* von a, c heißt *Komplementärteiler* von b bezüglich a. Aus der Definition folgt sofort

Satz 1.1

Seien $a, b, c \in \mathbb{N}$.

(i) Die Relation $a \mid b$ ist reflexiv ($a \mid a$) und transitiv ($a \mid b$ und $b \mid c \Longrightarrow a \mid c$).

(ii) Die Relation $a \mid b$ ist nicht symmetrisch, es gilt sogar: $a \mid b$ und $b \mid a \Longrightarrow a = b$.

(iii) Aus $a \mid b$ folgt $a \leq b$. Insbesondere hat jede natürliche Zahl nur endlich viele Teiler.

Definition:

Seien $a, b \in \mathbb{Z}$, $a \neq 0$. Wir sagen $a \mid b$, falls es ein $c \in \mathbb{Z}$ gibt mit $b = c \cdot a$.

Bemerkung:

Satz 1.1 gilt analog in $\mathbb{Z}$. Zu ändern sind nur

(ii) $a \mid b$ und $b \mid a \Longrightarrow |a| = |b|$.

(iii) $a \mid b \Longrightarrow |a| \leq |b|$.

Satz 1.2 (Divisionsalgorithmus mit Rest)

Seien $a, b \in \mathbb{Z}$, $b > 0$. Dann existieren q, $r \in \mathbb{Z}$ mit $a = q \cdot b + r$ und $0 \leq r < b$.

Beweis:

Wähle q maximal mit der Eigenschaft, dass $b \cdot q \leq a$ (Satz 0.2(ii)). Selbstverständlich folgt $r := a - q \cdot b \geq 0$. Nach Konstruktion ist $b \cdot (q+1) > a$, also
$r = a - q \cdot b = a - (q+1) \cdot b + b < a - a + b = b$.

□

Bemerkung:

Satz 1.2 gilt analog für jedes $b \in \mathbb{Z}, b \neq 0$, dann allerdings mit $0 \leq r < |b|$.

Hilfssatz 1.3 (Existenz des größten gemeinsamen Teilers)

Seien $a, b \in \mathbb{N}$. Dann gibt es ein eindeutiges $d \in \mathbb{N}$ derart, dass

(i) $d \mid a$ und $d \mid b$ (d ist gemeinsamer Teiler).

(ii) Für jeden gemeinsamen Teiler t von a und b gilt $t \mid d$.

Beweis:

Existenz: Wir betrachten die Menge $M = \{a \cdot x + b \cdot y : x, y \in \mathbb{Z}\}$ und bilden $M' := M \cap \mathbb{N}$. Offenbar ist $M' \neq \emptyset$ (z.B. $a \in M'(x = 1, y = 0)$). Nach Satz 0.1(ii) enthält M' ein kleinstes Element d. Nach Konstruktion gibt es Zahlen $x_0, y_0 \in \mathbb{Z}$ mit $d = a \cdot x_0 + b \cdot y_0$. Ist t ein Teiler von a und b, so folgt $t \mid a \cdot x_0$ und $t \mid b \cdot y_0$, also $t \mid (a \cdot x_0 + b \cdot y_0) = d$. Damit ist (ii) gezeigt.
Nach Satz 1.2 existieren $q, r \in \mathbb{Z}$ mit $0 \leq r < d$ und $a = q \cdot d + r$. Es folgt
$r = a - q \cdot d = a - (ax_0 + by_0) \cdot q = ax' + by'$, wobei $x' = 1 - qx_0$, $y' = -qy_0$. Wegen der Minimalität von d bleibt nur $r = 0$, d.h. $a = q \cdot d$, also $d \mid a$. Analog folgt $d \mid b$. Damit ist auch (i) gezeigt.
Eindeutigkeit: Wir nehmen an, es gäbe ein d' mit (i) und (ii). Mit (ii) folgt $d' \mid d$ und umgekehrt $d \mid d'$, also $d = d'$ (Satz 1.1(ii)).

□

Definition:

Seien $a, b \in \mathbb{N}$. Die nach Hilfssatz 1.3 eindeutige Zahl d heißt *größter gemeinsamer Teiler* von a und b, geschrieben $\mathrm{ggT}(a, b)$ oder kurz (a, b). Ist $(a, b) = 1$, so heißen a und b *teilerfremd*.

Bemerkungen:

(i) Hilfssatz 1.3 läßt sich auf Zahlen $a_1, a_2, \ldots, a_n \in \mathbb{N}$ übertragen. Die eindeutige Zahl $d = (a_1, \ldots, a_n)$ heißt dann analog ggT von $a_1, \ldots a_n$. Ist $d = 1$, so heißen $a_1, \ldots a_n$ teilerfremd. Gilt paarweise $(a_i, a_j) = 1$ $(i \neq j)$, so heißen $a_1, \ldots a_n$ *paarweise teilerfremd*.

(ii) Die Definition des ggT läßt sich sofort auf $\mathbb{Z}$ verallgemeinern:
Für $a_1, \ldots a_n \in \mathbb{Z} \setminus \{0\}$ setzen wir $(a_1, \ldots, a_n) := (|a_1|, |a_2|, \ldots, |a_n|)$.
Da 0 durch jede natürliche Zahl teilbar ist, liegt folgende Definition nahe:
$(a_1, \ldots, a_n, 0) := (a_1, \ldots, a_n)$, sofern nicht alle $a_i = 0$ sind. Sind alle $a_i = 0$, so setzen wir $(a_1, \ldots, a_n) := 0$.

In der Zahlentheorie geht es häufig um das Lösen von Gleichungen in ganzen Zahlen. Sind nur ganzzahlige Lösungen zugelassen, so heißt die entsprechende Gleichung *Diophantisch*.

Satz 1.4 (Lösbarkeit linearer Diophantischer Gleichungen)

Seien $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}, b \in \mathbb{Z}$. Die Diophantische Gleichung
$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ ist genau dann lösbar, wenn $(a_1, \ldots, a_n) \mid b$.

Beweis:

„$\Longrightarrow$“

Sei $d = (a_1, \ldots, a_n) \nmid b$.

$\Longrightarrow d \mid a_1, \ldots, d \mid a_n$. Es folgt $d \mid a_1x_1, \ldots, d \mid a_nx_n$ für beliebige $x_i \in \mathbb{Z}$.

$\Longrightarrow d \mid (a_1x_1 + \cdots + a_nx_n) = b$. Widerspruch!

„$\Longleftarrow$“

Sei $d = (a_1, \ldots, a_n)$. Nach Definition des ggT existieren $x_1, \ldots, x_n \in \mathbb{Z}$ mit $d = a_1x_1 + \cdots + a_nx_n$. Wegen $d \mid b$ existiert $c \in \mathbb{Z}$ mit $b = c \cdot d$.

Also $a_1(c \cdot x_1) + \cdots + a_n(c \cdot x_n) = c \cdot d = b$.

□

Ein außerordentlich elegantes Verfahren zur Bestimmung des ggT zweier Zahlen geht auf Euklid zurück und besteht in der mehrfachen Anwendung der Division mit Rest.

Euklidischer Algorithmus

Gegeben $a, b \in \mathbb{N}$, gesucht ist (a, b).

Nach Division mit Rest (Satz 1.2) existieren $q_1, r_1 \in \mathbb{Z}$ mit $a = q_1 \cdot b + r_1$ und $0 \leq r_1 < b$. Ist $r_1 \neq 0$, so gibt es nach Division mit Rest $q_2, r_2 \in \mathbb{Z}$ mit $b = q_2 \cdot r_1 + r_2$ und $0 \leq r_2 < r_1$. Ist $r_2 \neq 0$, so existieren $q_3, r_3 \in \mathbb{Z}$ mit $r_1 = q_3 \cdot r_2 + r_3$ und $0 \leq r_3 < r_2$. Der Algorithmus bricht ab, sobald $r_j = 0$ auftritt. Dies geschieht spätestens nach b Schritten, denn $b > r_1 > r_2 > \ldots > r_j \geq 0$.

Satz 1.5

Mit den obigen Bezeichnungen gilt: Ist $k + 1$ der kleinste Index mit $r_{k+1} = 0$, so haben wir $r_k = (a, b)$.

Beweis:

Wegen

$$\begin{aligned} a &= q_1 \cdot b + r_1 \\ b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k \cdot r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} \cdot r_k \end{aligned}$$

ist klar, dass $d := (a, b) \mid r_1$ (1.Glg). $\Longrightarrow d \mid r_2$ (2.Glg) $\Longrightarrow \ldots \Longrightarrow d \mid r_k$. Umgekehrt haben wir $r_k \mid r_{k-1}$ (letzte Glg.). $\Longrightarrow r_k \mid r_{k-2}$ (vorletzte Glg.) $\Longrightarrow \ldots \Longrightarrow r_k \mid b$ $\Longrightarrow r_k \mid a$. Nach Definition des ggT folgt $r_k \mid d$, also nach Satz 1.1 $r_k = d$.

□

Durch Umkehrung des euklidischen Algorithmus erhalten wir außerdem eine Darstellung $(a, b) = a \cdot x + b \cdot y$ für gewisse $x, y \in \mathbb{Z}$ (vergleiche Satz 1.4).

Definition:

Eine natürliche Zahl $n > 1$ heißt *Primzahl*, falls n nur die *trivialen Teiler* 1 und n besitzt. Die Menge aller Primzahlen bezeichnen wir mit $\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$.

Satz 1.6 (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis:

Der kleinste Faktor $d > 1$ einer natürlichen Zahl $n > 1$ ist eine Primzahl, denn sonst wäre $d = d_1 \cdot d_2$ mit $1 < d_1 < d$ und $1 < d_2 < d$ und daher nicht minimal. Wäre $\mathbb{P} = \{p_1, \ldots, p_k\}$ endlich, so enthielte $n := p_1 \cdot \ldots \cdot p_k + 1 > 1$ einen Primteiler p. $\Longrightarrow p = p_j$ für ein $j \in \{1, \ldots, k\}$. Wegen $p \mid n$ folgt $p \mid 1$. Widerspruch!

□

Satz 1.7 (Fundamentalsatz der Zahlentheorie)

Jede natürliche Zahl $n > 1$ besitzt eine bis auf die Reihenfolge der Faktoren eindeutige Darstellung als Produkt von Primzahlen.

Beweis:

Existenz: Wegen $n > 1$ hat n einen Primfaktor p_1. Ist $n = p_1$, so ist alles gezeigt. Sonst wiederholen wir das Argument für die Zahl $n/p_1 < n$. Induktiv ergibt sich $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$. Das Verfahren bricht nach endlich vielen Schritten ab, da $n > n/p_1 > n/p_1p_2 > \ldots \geq 1$.

Eindeutigkeit: Wir zeigen zunächst: Ist $p \in \mathbb{P}$ mit $p \mid mn$ für gewisse $m, n \in \mathbb{N}$, so folgt $p \mid m$ oder $p \mid n$. Dazu nehmen wir an, dass $p \nmid m$, also $(p, m) = 1$. Nach Satz 1.4 existieren $x, y \in \mathbb{Z}$ mit $px + my = 1$. Also gilt $pnx + mny = n$. Wegen $p \mid mn$ folgt $p \mid n$. Allgemeiner gilt also: $p \mid n_1 n_2 \cdots n_k \Longrightarrow p \mid n_j$ für ein j mit $1 \leq j \leq k$. Wir nehmen nun an, es sei $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ mit $p_i, q_j \in \mathbb{P}$. Induktion liefert:

$n = 2$: Offenbar gilt $p_1 = q_1 = 2$.

$n - 1 \to n$: Nach obigem Argument folgt $p_1 \mid q_j$ für ein $j \in \{1, \ldots, l\}$, o.B.d.A. $p_1 \mid q_i$. Da $q_1 \in \mathbb{P}$, folgt $p_1 = q_1$. $\Longrightarrow n' = p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_l < n$. Daraus folgt die Behauptung.

□

Definition:

Sei $n > 1$ eine natürliche Zahl. Die nach Satz 1.7 eindeutige Darstellung

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

mit Primzahlen $p_1 < p_2 < \ldots < p_k$ und $e_j \in \mathbb{N}$ heißt *kanonische Primfaktorzerlegung* von n. Wir schreiben $e_j =: e_{p_j}(n) \in \mathbb{N}_0$, wobei $e_{p_j}(n) := 0$, falls $p \nmid n$. Also formal

$$n = \prod_{p \in \mathbb{P}} p^{e_p(n)}$$

Dabei heißt $e_p(n)$ die *Ordnung* von p in n.

Satz 1.8

Seien $a_1, \ldots, a_n \in \mathbb{Z}$, nicht alle gleich 0. Dann gilt mit $e_p(0) := \infty$

$$(a_1, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{\min\ e_p(a_i)}.$$

Beweis:

Das Produkt erfüllt offensichtlich die Bedingungen (i), (ii) aus Hilfssatz 1.3 (in der entsprechenden Verallgemeinerung), d.h. es ist genau $(a_1, \ldots, a_n)$.

□

Dual zum ggT ist das kgV.

Definition:

Seien $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. Die natürliche Zahl

$$[a_1, \ldots, a_n] := \prod_{p \in \mathbb{P}} p^{\max\ e_p(a_i)}$$

heißt *kleinstes gemeinsames Vielfaches* von $a_1, \ldots, a_n$. Ist eines der $a_i = 0$, so sei $[a_1, \ldots, a_n] := 0$. Aus Satz 1.8 und den Definitionen folgt direkt

Satz 1.9

Für $a_1, \ldots, a_n, t \in \mathbb{Z}$ gilt

(i) $(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$; $[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$;

(ii) $(ta_1, \ldots, ta_n) = |t| \cdot (a_1, \ldots, a_n)$; $[ta_1, \ldots, ta_n] = |t| \cdot [a_1, \ldots, a_n]$;

(iii) $(a_1, \ldots, a_n) \mid (a_1, \ldots, a_{n-1})$; $[a_1, \ldots, a_{n-1}] \mid [a_1, \ldots, a_n]$;

(iv) $(a_1, a_2) \cdot [a_1, a_2] = |a_1 \cdot a_2|$.

Im Beweis zu Satz 1.7 hatten wir gesehen, dass die Implikation $p \mid mn,\ p \nmid m \Longrightarrow p \mid n$ für alle Primzahlen p gilt. Allgemeiner ist das folgende Ergebnis, das in zahlreichen Situationen zur Anwendung kommt.

Hilfssatz 1.10

Seien $a, b \in \mathbb{Z}$ mit $a \mid bc$ und $(a, b) = 1$. Dann gilt $a \mid c$.

Beweis:

Wegen $(a, b) = 1$ ist nach Satz 1.9(ii) $(ac, bc) = |c| \cdot (a, b) = |c|$. Wegen $a \mid bc$ existiert ein $g \in \mathbb{Z}$ mit $bc = ag$. Also $|c| = (ac, bc) = (ac, ag) = |a| \cdot (c, g) \Longrightarrow a \mid c$.

□

Nach Satz 1.4 wissen wir, dass $ax + by = c$ genau dann lösbar ist, wenn $(a, b) \mid c$. Wir wollen nun alle Lösungen dieser Gleichung angeben.

Satz 1.11

Die Diophantische Gleichung $ax + by = c$ besitze die Lösung $x_0, y_0 \in \mathbb{Z}$ (z.B. mit eukl. Alg.). Die Gesamtheit der Lösungen ist dann gegeben durch

$$x = x_0 - \frac{b}{(a,b)} \cdot t \qquad , \qquad y = y_0 + \frac{a}{(a,b)} \cdot t \qquad (t \in \mathbb{Z}).$$

Beweis:

Die angegebenen x, y sind Lösungen, denn

$$a \cdot \left(x_0 - \frac{b}{(a,b)} \cdot t \right) + b \cdot \left(y_0 + \frac{a}{(a,b)} \cdot t \right) = ax_0 + by_0 = c.$$

Sei x_1, y_1 eine weitere Lösung, d.h. $ax_0 + by_0 = c = ax_1 + by_1 \Longrightarrow a(x_0 - x_1) = b(y_1 - y_0)$. Sei $d := (a, b)$. Dann folgt $a = d \cdot a'$, $b = d \cdot b'$ mit $(a', b') = 1$

$$\Longrightarrow a'(x_0 - x_1) = b'(y_1 - y_0). \qquad (*)$$

Insbesondere folgt $a' \mid b'(y_1 - y_0)$. Mit Hilfssatz 1.10 erhält man $a' \mid (y_1 - y_0)$, d.h. $y_1 - y_0 = a' \cdot t$ für ein $t \in \mathbb{Z}$. Einsetzen in $(*)$ liefert $x_0 - x_1 = b' \cdot t$. Es folgt

$$x_1 = x_0 - \frac{b}{(a,b)} \cdot t \qquad \text{und} \qquad y_1 = y_0 + \frac{b}{(a,b)} \cdot t.$$

□

2 Zahlentheoretische Funktionen

Für jede reelle Zahl x bezeichne

$$[x] := \max\{n \in \mathbb{Z} : n \leq x\}.$$

Namen: *Gauß-Klammer*, *Größtes Ganzes*, *Ganzteil* (von x). Weiterhin heißt

$\{x\} := x - [x]$ *Bruchteil von* x.

Hilfssatz 2.1

Seien $x, y \in \mathbb{R}$. Dann gilt:

(i) $x - 1 < [x] \leq x \quad , \quad 0 \leq \{x\} < 1;$

(ii) für $n \in \mathbb{Z}$ ist $[x + n] = [x] + n;$

(iii) $[x] + [y] \leq [x + y] \quad , \quad \{x + y\} \leq \{x\} + \{y\};$

(iv) für $n \in \mathbb{N}$ ist $[x/n] = \big[[x]/n\big]$.

Satz 2.2

Sei $n \in \mathbb{N}$, $p \in \mathbb{P}$. Mit $n! = 1 \cdot 2 \cdot \ldots \cdot n$ gilt

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

Beweis:

Für beliebiges $n \in \mathbb{N}$ sind genau $[n/m]$ Zahlen aus der Menge $\{1, 2, \ldots, n\}$ durch m teilbar, nämlich $n \cdot t$ mit $1 \leq t \leq [n/m]$. Also sind unter den Zahlen $1, \ldots, n$ genau $[n/p^j]$ teilbar durch p^j.

Also gilt

$$\begin{aligned} e_p(n!) &= \sum_{k=1}^{n} e_p(k) = \sum_{k=1}^{n} \sum_{\substack{j=1 \\ p^j \mid k}}^{\infty} 1 \\ &= \sum_{j=1}^{\infty} \sum_{\substack{k=1 \\ p^j \mid k}}^{n} 1 = \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right]. \end{aligned}$$

□

Korollar 2.3

(i) $e_p(n!) \leq \left[\dfrac{n}{p-1} \right]$ für $n \in \mathbb{N}$ und $p \in \mathbb{P}$;

(ii) $\binom{m}{n} := \dfrac{m!}{n!(m-n)!} \in \mathbb{N}$ für $1 \leq n \leq m$.

Beweis:

(i) $e_p(n!) = \displaystyle\sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right] \leq \sum_{j=1}^{\infty} \frac{n}{p^j} = n \cdot \sum_{j=1}^{\infty} \frac{1}{p^j} = n \cdot \left(\frac{1}{1-1/p} - 1 \right) = \frac{n}{p-1} \Longrightarrow$ Beh.

(ii) Für jedes $p \in \mathbb{P}$ gilt mit Hilfssatz 2.1 (iii)

$$\begin{aligned} e_p\left(\binom{m}{n} \right) &= e_p\left(\frac{m!}{n!(m-n)!} \right) = e_p(m!) - e_p(n!) - e_p\left((m-n)!\right) \\ &= \sum_{j=1}^{\infty} \left(\left[\frac{m}{p^j} \right] - \left[\frac{n}{p^j} \right] - \left[\frac{m-n}{p^j} \right] \right) \geq 0. \end{aligned}$$

□

Unter einer *zahlentheoretischen Funktion* (auch *arithmetische Funktion*) verstehen wir eine Funktion von $\mathbb{N}$ nach $\mathbb{R}$ oder $\mathbb{C}$, d.h. eine reelle oder komplexe Folge.

Definition:

Eine zahlentheoretische Funktion f heißt *multiplikativ*, falls für alle $m, n \in \mathbb{N}$ mit $(m, n) = 1$ gilt $f(m \cdot n) = f(m) \cdot (n)$.

Hilfssatz 2.4

Sei f multiplikativ und nicht die Nullfunktion. Dann gilt:

(i) $f(1) = 1$;

(ii) $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} \Longrightarrow f(n) = f\left(p_1^{e_1}\right) \cdot \ldots \cdot f\left(p_k^{e_k}\right)$.

Beweis:

(i) $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$

1. Fall: $f(1) \neq 0 \Longrightarrow f(1) = 1$ (durch $f(1)$ teilen)

2. Fall: $f(1) = 0 \Longrightarrow f(n) = f(n \cdot 1) = f(n) \cdot f(1) = 0$ für jedes $n \in \mathbb{N}$. Widerspruch!

(ii) Wegen $p_i \neq p_j$ $(i \neq j)$ folgt $f(n) = f\left(p_1^{e_1} \cdot (p_2^{e_2} \cdot \ldots \cdot p_k^{e_k})\right)$
$= f(p_1^{e_1}) \cdot f(p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}) = \ldots = f\left(p_1^{e_1}\right) \cdot \ldots \cdot f\left(p_k^{e_k}\right)$.

□

Ist f zahlentheoretische Funktion, so heißt

$$g(n) = \sum_{d|n} f(d)$$

die zugehörige *summatorische Funktion*. Hier wie in Zukunft bedeutet die Summationsbedingung $d \mid n$, dass über alle positiven Teiler von n summiert wird.

Hilfssatz 2.5

Mit f ist auch die summatorische Funktion von f multiplikativ.

Beweis:

Seien $(m,n)=1$. Zu zeigen: $g(m\cdot n)=g(m)\cdot g(n)$.

$$\begin{aligned} g(m\cdot n) &= \sum_{d\mid mn} f(d) = \sum_{d_1\mid m}\cdot\sum_{d_2\mid n} f(d_1d_2) = \sum_{d_1\mid m}\cdot\sum_{d_2\mid n} f(d_1)f(d_2) \\ &= \sum_{d_1\mid m} f(d_1)\cdot\sum_{d_2\mid n} f(d_2) = g(m)\cdot g(n), \end{aligned}$$

wobei jeder Teiler $d \mid n$ aufgespalten wurde in $d=d_1d_2$ folgendermaßen:
Sei $m=p_1^{e_1}\cdots p_r^{e_r}$ und $n=q_1^{f_1}\cdots q_s^{f_s}$. Ist $d=p_1^{a_1}\cdots p_r^{a_r}q_1^{b_1}\cdots q_s^{b_s}$, so folgt $d_1=p_1^{a_1}\cdots p_r^{a_r}$ und $d_2=q_1^{b_1}\cdots q_s^{b_s}$.

□

Wir behandeln im Folgenden einige wichtige zahlentheoretische Funktionen. Zuerst untersuchen wir die *Eulersche φ-Funktion*, definiert durch

$$\varphi(n) := \sum_{\substack{m=1\\(m,n)=1}}^{n} 1 \qquad (n\in\mathbb{N}).$$

Hilfssatz 2.6

Für $p\in\mathbb{P}$ und $j\in\mathbb{N}$ gilt

$$\varphi(p^j) = p^j - p^{j-1} = p^j\,(1-1/p)\,.$$

Beweis:

Nach Definition von φ ist

$$\varphi(p^j) = \sum_{\substack{m=1\\(m,p^j)=1}}^{p^j} 1 = \sum_{m=1}^{p^j} 1 - \sum_{\substack{m=1\\(m,p^j)>1}}^{p^j} 1 = p^j - \sum_{\substack{m=1\\p\mid m}}^{p^j} 1 = p^j - \left[\frac{p^j}{p}\right] = p^j - p^{j-1}.$$

Wunschdenken: Wäre $\varphi(n)$ multiplikativ, so folgte nach Hilfssatz 2.4.(ii)

für $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$:

$\varphi(n) = \varphi(p_1^{e_1}) \cdot \ldots \cdot \varphi(p_r^{e_r}) = p_1^{e_1}(1 - 1/p_1) \cdot \ldots \cdot p_r^{e_r}(1 - 1/p_r) = n \cdot \prod_{p|n}(1 - 1/p).$

Wir aber machen es umgekehrt:

Satz 2.7

Für $n \in \mathbb{N}$ gilt

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Beweis:

Seien $p_1, p_2, \ldots, p_k$ die verschiedenen Primfaktoren von n . Durch Ausmultiplizieren des Produkts erhält man

$$\begin{aligned} n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) \\ &= n - \sum_{r=1}^{k} \frac{n}{p_r} + \sum\sum_{1 \le s < r \le k} \frac{n}{p_r p_s} - \sum\sum\sum_{1 \le t < s < r \le k} \frac{n}{p_r p_s p_t} + \cdots \end{aligned}$$

$[n/p_r] = n/p_r$ ist die Anzahl derjenigen Zahlen $m \le n$, die durch p_r teilbar sind. Entsprechend ist $n/p_r p_s = [n/p_r p_s]$ die Anzahl der $m \le n$ mit $p_r p_s \mid m$ und so weiter. Also folgt nach Vertauschen der Summen

$$\begin{aligned} n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) &= \sum_{m=1}^{n} 1 - \sum_{r=1}^{k} \sum_{\substack{m=1 \\ p_r | m}}^{n} 1 + \sum\sum_{1 \le s < r \le k} \sum_{\substack{m=1 \\ p_r p_s | m}}^{n} 1 - \cdots \\ &= \sum_{m=1}^{n} \left(1 - \sum_{\substack{r=1 \\ p_r | m}}^{k} 1 + \sum\sum_{\substack{1 \le s < r \le k \\ p_r p_s | m}} 1 - \cdots\right) \\ &= \sum_{m=1}^{n} \left(1 - \binom{l(m)}{1} + \binom{l(m)}{2} - \binom{l(m)}{3} + \cdots\right), \end{aligned}$$

wobei $l(m)$ die Anzahl der Primzahlen $p_1, \ldots, p_k$ ist, die m teilen. Ist $l(m) \neq 0$, so ist der letzte Klammerausdruck nach dem Binomischen Lehrsatz gleich $(1-1)^{l(m)} = 0$.

Für $l(m) = 0$ ergibt die Klammer den Wert 1. Also haben wir

$$n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) = \sum_{\substack{m=1 \\ l(m)=0}}^{n} 1.$$

Es bedeutet aber $l(m) = 0$, dass m von keiner der Primzahlen $p_1, \ldots, p_k$ geteilt wird, d.h. zu n teilerfremd ist. Damit ist das Gewünschte gezeigt.

□

Korollar 2.8

(i) φ ist multiplikativ.

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

Beweis:

(i) Sei $(m, n) = 1$. Daraus folgt mit Satz 2.7

$$\begin{aligned} \varphi(m \cdot n) &= mn \prod_{p|mn} \left(1 - \frac{1}{p}\right) = mn \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right) \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ &= m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right) \cdot n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) = \varphi(m) \cdot \varphi(n). \end{aligned}$$

(ii) Nach (i) und Hilfssatz 2.5 ist $\sum_{d|n} \varphi(n)$ als summatorische Funktion von φ multiplikativ. Wegen Hilfssatz 2.4 brauchen wir die gewünschte Identität daher nur für Primzahlpotenzen $n = p^k$ nachzuweisen. In der Tat ist

$$\begin{aligned} \sum_{d|p^k} \varphi(d) &= \varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^k) \\ &= 1 + p(1 - 1/p) + p^2(1 - 1/p) + \cdots + p^k(1 - 1/p) \\ &= 1 + (p - 1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) = p^k \end{aligned}$$

mit Hilfssatz 2.6.

□

Wir kommen nun zur Definition der *Möbius-Funktion* $\mu(n)$. Eine natürliche Zahl n heißt *quadratfrei*, wenn $p^2 \nmid n$ für alle $p \in \mathbb{P}$. Damit definieren wir $\mu(n)$ wie folgt: $\mu(1) := 1$; für $n > 1$ und quadratfrei, d.h. $n = p_1 \cdot \ldots \cdot p_k$ mit $p_i \neq p_j$ für $i \neq j$, sei $\mu(n) = (-1)^k$; für n nicht quadratfrei sei $\mu(n) = 0$.

Satz 2.9

(i) μ ist multiplikativ.

(ii) Die summatorische Funktion $\varepsilon(n) := \sum_{d|n} \mu(d)$ erfüllt

$$\varepsilon(n) = \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{sonst.} \end{cases}$$

Beweis:

(i) Sei $(m, n) = 1$. Hat m oder n einen quadratischen Primfaktor, so auch $m \cdot n$. Dann gilt $\mu(m) = 0$ oder $\mu(n) = 0$ und $\mu(m \cdot n) = 0$. Also $\mu(m) \cdot \mu(n) = 0 = \mu(m \cdot n)$. Für m und n quadratfrei gilt $m = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ und $n = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ mit $p_i \neq p_j$ und $q_i \neq q_j$ für $i \neq j$. Wegen $(m, n) = 1$ ist außerdem $p_i \neq q_j$ für alle i, j. Daher ist $\mu(m \cdot n) = \mu(p_1 \cdot p_2 \cdot \ldots \cdot p_k \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_l) = (-1)^{k+l} = (-1)^k \cdot (-1)^l = \mu(m) \cdot \mu(n)$.

(ii) Nach (i) und Hilfssatz 2.5 ist $\varepsilon(n)$ multiplikativ, d.h. wir müssen nur zeigen $\varepsilon(p^k) = 0$ für alle $p \in \mathbb{P}$ und $k \in \mathbb{N}$. In der Tat gilt
$\varepsilon(p^k) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) = \mu(1) + \mu(p) = 1 - 1 = 0$.

□

Mit Hilfe der μ-Funktion lässt sich aus einer summatorischen Funktion die ursprüngliche Funktion zurückgewinnen.

Satz 2.10 (1. Möbius-Umkehrung)

Sei f eine zahlentheoretische Funktion und $g(n) := \sum_{d|n} f(d)$ die zugehörige summatorische Funktion. Dann gilt

$$f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right).$$

Ist umgekehrt f durch diese Identität gegeben bei vorgegebenem g, so folgt $g(n) = \sum_{d|n} f(d)$.

Beweis:

Sei $g(n) = \sum_{d|n} f(d)$. Nach Satz 2.9(ii) gilt dann

$$\begin{aligned}\sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \cdot \sum_{d'|n/d} f(d') = \sum_{d'|n} f(d') \cdot \sum_{d|n/d'} \mu(d) \\ &= \sum_{d'|n} f(d') \cdot \varepsilon\left(\frac{n}{d'}\right) = f(n).\end{aligned}$$

Die umgekehrte Implikation ergibt sich so:

$$f(n) = \sum_{d'|n} \mu(d') \cdot g(\frac{n}{d'}) = \sum_{d'|n} \mu\left(\frac{n}{d'}\right) \cdot g(d'),$$

also wieder mit Satz 2.9(ii)

$$\begin{aligned}\sum_{d|n} f(d) &= \sum_{d|n} f\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{d'|n/d} \mu\left(\frac{n}{dd'}\right) \cdot g(d') \\ &= \sum_{d'|n} g(d') \cdot \sum_{d|n/d'} \mu\left(\frac{n/d'}{d}\right) = \sum_{d'|n} g(d') \cdot \sum_{d|n/d'} \mu(d) \\ &= \sum_{d'|n} g(d') \cdot \varepsilon\left(\frac{n}{d'}\right) = g(n).\end{aligned}$$

□

Satz 2.11

Für alle $n \in \mathbb{N}$ gilt

$$\varphi(n) = n \cdot \sum_{d|n} \frac{\mu(d)}{d}.$$

Beweis:

Nach Korollar 2.8 ist $\sum_{d|n} \varphi(d) = n$. Mit $f(n) = \varphi(n)$ und $\sum_{d|n} \varphi(d) = n$ folgt daraus nach 1. Möbius-Umkehrung

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n \cdot \sum_{d|n} \frac{\mu(d)}{d}.$$

□

Bemerkung:

Satz 2.11 folgt auch ohne Möbius-Umkehrung aus Satz 2.7.

Satz 2.12 (2. Möbius-Umkehrung)

Seien f und g reelle Funktionen mit $g(x) = \sum_{n \le x} f(x/n)$, wobei nur über natürliche Zahlen summiert wird. Dann ist

$$f(x) = \sum_{n \le x} \mu(n) \cdot g\left(\frac{x}{n}\right),$$

und die Umkehrung gilt ebenfalls.

Beweis:

$$\begin{aligned}
\sum_{n \le x} \mu(n) \cdot g\left(\frac{x}{n}\right) &= \sum_{n \le x} \mu(n) \cdot \sum_{m \le x/n} f\left(\frac{x}{m \cdot n}\right) = \sum_{m \cdot n \le x} \sum \mu(n) \cdot f\left(\frac{x}{m \cdot n}\right) \\
&\overset{l := mn}{=} \sum_{l \le x} \sum_{n|l} \mu(n) \cdot f\left(\frac{x}{l}\right) = \sum_{l \le x} f\left(\frac{x}{l}\right) \sum_{n|l} \mu(n) \\
&= \sum_{l \le x} f\left(\frac{x}{l}\right) \cdot \varepsilon(l) = f(x)
\end{aligned}$$

mit Satz 2.9(ii). Die Umkehrung folgt entsprechend.

□

Weitere zahlentheoretische Funktionen sind die *Teileranzahl* $\tau(n)$ und die *Teilersumme* $\sigma(n)$, d.h.

$$\tau(n) := \sum_{d|n} 1 \qquad , \qquad \sigma(n) := \sum_{d|n} d.$$

Satz 2.13

τ und σ sind multiplikativ, und es gilt für alle $n \in \mathbb{N}$

(i) $$\tau(n) = \prod_{p|n} (e_p(n) + 1);$$

(ii) $$\sigma(n) = \prod_{p|n} \frac{p^{e_p(n)+1} - 1}{p - 1}.$$

Beweis:

Die Funktionen $f_1(n) = 1$ bzw. $f_2(n) = n$ $(n \in \mathbb{N})$ sind offensichtlich (streng) multiplikativ. Nach Hilfssatz 2.5 sind deren summatorische Funktionen τ bzw. σ ebenfalls multiplikativ. Wir berechnen für $p \in \mathbb{P}$ und $k \in \mathbb{N}$

(i) $$\tau\left(p^k\right) = \sum_{d|p^k} 1 = k + 1 = e_p(p^k) + 1 \qquad \text{und}$$

(ii) $$\sigma\left(p^k\right) = \sum_{d|p^k} d = 1 + p + p^2 + \cdots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

Mit Multiplikativität folgt die Behauptung.

□

Die Griechen der Antike nannten eine natürliche Zahl n vollkommen (perfekt), sofern n die Summe seiner Teiler (ohne n selbst) ist, d.h. $\sigma(n) = 2n$. Solche Zahlen

gibt es, nämlich $6, 28, 496, 8128, \ldots$ Bis heute offen: Gibt es unendlich viele vollkommene Zahlen? Vermutlich viel einfacher sollte sein: Gibt es ungerade vollkommene Zahlen? Wir beweisen ein Kriterium für *gerade* vollkommene Zahlen.

Satz 2.14 (von Euklid und Euler)

Eine gerade natürliche Zahl n ist genau dann vollkommen, wenn

$$n = 2^{p-1}(2^p - 1)$$

mit $p \in \mathbb{P}$ und $2^p - 1 \in \mathbb{P}$ (d.h. 2^{p-1} ist sogenannte *Mersenne-Primzahl*).

Beweis:

„$\Longrightarrow$“

Sei $\sigma(n) = 2n$ für ein gerades n. Dann gilt $n = 2^k \cdot m$ für $k, m \in \mathbb{N}$ mit $2 \nmid m$. Wegen der Multiplikativität von σ nach Satz 2.13 folgt $\sigma(n) = \sigma\left(2^k \cdot m\right) = \sigma\left(2^k\right) \cdot \sigma(m)$ $= (2^{k+1}-1) \cdot \sigma(m)$, mit $\sigma(n) = 2n = 2^{k+1} \cdot m$ ergibt sich also $(2^{k+1}-1)\sigma(m) = 2^{k+1} \cdot m$. Wegen $(2^{k+1} - 1, 2^{k+1}) = 1$ liefert Hilfssatz 1.10 $\sigma(m) = 2^{k+1} \cdot l$ und $m = (2^{k+1} - 1) \cdot l$ für ein geeignetes $l \in \mathbb{N}$.

Behauptung: $l = 1$

Für $l > 1$ hätte m die verschiedenen Teiler $1, l, m$, also

$\sigma(m) \geq 1 + l + m = 1 + l + (2^{k+1} - 1) \cdot l = 2^{k+1} \cdot l + 1 = \sigma(m) + 1$. Widerspruch!

Somit ist $\sigma(m) = 2^{k+1} = m + 1 \Longrightarrow m \in \mathbb{P}$. Bekanntlich ist eine natürliche Zahl $m = 2^{k+1} - 1$ Primzahl nur dann, wenn $k+1$ selbst Primzahl ist; d.h. $k+1 = p \in \mathbb{P}$. Das liefert genau die gesuchte Darstellung.

„$\Longleftarrow$“

Sei $n = 2^{p-1}(2^p - 1)$ für ein $p \in \mathbb{P}$, wobei auch $2^p - 1 =: q \in \mathbb{P}$. Dann gilt mit Satz 2.13

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

□

Weitere klassische Begriffe im Zusammenhang mit $\sigma(n)$ sind:

$$n \in \mathbb{N} \text{ heißt } \textit{defizient} \iff \sigma(n) < 2n;$$

$$n \in \mathbb{N} \text{ heißt } \textit{abundant} \iff \sigma(n) > 2n.$$

Es ist nicht schwer zu zeigen, dass unendlich viele defiziente bzw. abundante Zahlen existieren. Weiterhin heißen zwei natürliche Zahlen $m \neq n$ *befreundet*, falls $\sigma(m) = \sigma(n) = m + n$. Zum Beispiel sind 220 und 284 befreundet. Es ist unbekannt, ob unendlich viele Paare befreundeter Zahlen existieren.

Die meisten interessanten zahlentheoretischen Funktionen verhalten sich in der Folge ihrer Werte sehr unregelmäßig. Zum Beispiel ist $\varphi(n) = n - 1$ unendlich oft, nämlich für jedes $n \in \mathbb{P}$, andererseits kann φ erheblich kleinere Werte annehmen, nämlich für Zahlen mit vielen Primteilern. Entsprechend ist $\tau(n) = 2$ für alle $n \in \mathbb{P}$ und erheblich größer für Zahlen mit vielen Primfaktoren. Wir wollen trotzdem versuchen, für die definierten Funktionen einige Abschätzungen herzuleiten.

Satz 2.15

(i) $2 \leq \tau(n) \leq C(\varepsilon) \cdot n^{\varepsilon}$ für jedes $\varepsilon > 0$ und eine Konstante $C(\varepsilon)$, die nur von ε abhängt.

(ii) $n+1 \leq \sigma(n) \leq n(1+\log n)$, wobei log den natürlichen Logarithmus bezeichnet.

(iii) $\dfrac{1}{4} \cdot \dfrac{n}{\log n} \leq \varphi(n) \leq n - 1$ für alle $n > 1$.

Beweis:

(i) Sei $\varepsilon > 0$ fest. Die Funktion $f(n) := \tau(n)/n^{\varepsilon}$ ist multiplikativ als Quotient zweier multiplikativer Funktionen. Zu ε existiert ein $K(\varepsilon)$ derart, dass $p^{\varepsilon} \geq 2$ für

alle $p \geq K(\varepsilon)$. Wegen $k+1 \leq 2^k$ für $k \in \mathbb{N}$ (Induktion) ist $(k+1)/p^{\varepsilon k} \leq (2/p^{\varepsilon})^k \leq 1^k = 1$ für $p \geq K(\varepsilon)$. Für jede Primzahl $p < K(\varepsilon)$ gibt es höchstens endlich viele Werte $k \in \mathbb{N}$ derart, dass $(k+1)/p^{\varepsilon k} > 1$ (wegen $\lim\limits_{k\to\infty}(k+1)/p^{\varepsilon k} = 0$). Somit gilt $(k+1)/p^{\varepsilon k} \leq 1$ für alle Paare $p \in \mathbb{P}$, $k \in \mathbb{N}$ mit höchstens endlich vielen Ausnahmen $p_i, k_i (i = 1, 2, \ldots, I(\varepsilon))$.

Mit Satz 2.13 folgt

$$\begin{aligned} f(n) &= \prod_{p|n} f(p^{e_p(n)}) = \prod_{p|n} \frac{\tau(p^{e_p(n)})}{p^{\varepsilon \cdot e_p(n)}} = \prod_{p|n} \frac{e_p(n)+1}{p^{\varepsilon \cdot e_p(n)}} \\ &\leq \prod_{i=1}^{I(\varepsilon)} \frac{k_i+1}{p_i^{\varepsilon k_i}} =: C(\varepsilon). \end{aligned}$$

(ii) Mit der Formel für die harmonische Reihe ergibt sich

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} = n \cdot \sum_{d|n} \frac{1}{d} \leq n \cdot \sum_{d \leq n} \frac{1}{d} \leq n \cdot (1 + \log n).$$

(iii) $f(n) := \big(\sigma(n) \cdot \varphi(n)\big)/n^2$ ist multiplikativ. Nach Satz 2.13 und Hilfssatz 2.6 gilt

$$f(p^k) = \frac{\sigma(p^k)\varphi(p^k)}{p^{2k}} = \frac{1}{p^{2k}} \cdot \frac{p^{k+1}-1}{p-1} \cdot (p^k - p^{k-1}) = 1 - \frac{1}{p^{k+1}} \geq 1 - \frac{1}{p^2},$$

also

$$f(n) = \prod_{p|n} f\left(p^{e_p(n)}\right) \geq \prod_{p|n} \left(1 - \frac{1}{p^2}\right) \geq \prod_{m=2}^{\infty} \left(1 - \frac{1}{m^2}\right) = \frac{1}{2},$$

denn

$$\begin{aligned} \prod_{m=2}^{M} \left(1 - \frac{1}{m^2}\right) &= \prod_{m=2}^{M} \left(1 - \frac{1}{m}\right)\left(1 + \frac{1}{m}\right) \\ &= \left(\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdot \ldots \cdot \frac{M-1}{M}\right)\left(\frac{3}{2} \cdot \frac{4}{3} \cdot \frac{5}{4} \cdot \ldots \cdot \frac{M+1}{M}\right) \\ &= \frac{1}{M} \cdot \frac{M+1}{2} \to \frac{1}{2} \quad \text{für } M \to \infty. \end{aligned}$$

Mit (ii) folgt für $n \geq 3$

$$\varphi(n) = \frac{n^2 \cdot f(n)}{\sigma(n)} \geq \frac{n^2/2}{n(1+\log n)} = \frac{n}{2(1+\log n)} \geq \frac{1}{4} \cdot \frac{n}{\log n}.$$

Für $n = 2$ gilt (iii) trivialerweise.

□

Alternativ zu Abschätzungen bietet sich bei unregelmäßigen Funktionen die Berechnung eines Mittelwertes an; d.h.

$$\frac{1}{x}\sum_{n\le x} f(x) = H(x) + F(x),$$

wobei $H(x)$ der Hauptterm und $F(x)$ ein möglichst kleiner Fehlerterm ist. Zur Behandlung von Fehlertermen führen wir die sogenannten *Landau-Symbole* $O(\ )$ bzw. $o(\ )$ ein. Seien $f(x)$ und $g(x)$ reelle Funktionen. Dann bezeichnet $f(x) = O\left(g(x)\right)$ bzw. $f(x) \ll g(x)$ die Aussage: $|f(x)| \le C \cdot g(x)$ für eine Konstante C und alle $x \in \mathbb{R}$ in einem festgelegten Bereich (häufig für „große“ x , $x \to \infty$).
$f(x) = o\left(g(x)\right)$ bedeutet $\lim\limits_{x\to x_0} f(x)/g(x) = 0$ für ein gegebenes x_0 (häufig: $x_0 = \infty$).

Satz 2.16

Für $x \to \infty$ gilt

(i) $$\sum_{n\le x} \tau(n) = x\log x + O(x);$$

(ii) $$\sum_{n\le x} \sigma(n) = \frac{\pi^2}{12}x^2 + O(x\log x);$$

(iii) $$\sum_{n\le x} \varphi(n) = \frac{3}{\pi^2}x^2 + O(x\log x).$$

Beweis:

(i) Mit Hilfssatz 2.1(i) erhalten wir

$$\begin{aligned}\sum_{n\le x}\tau(n) &= \sum_{n\le x}\sum_{d|n} 1 = \sum_{d\le x}\sum_{\substack{n\le x\\ d|n}} 1 = \sum_{d\le x}\left[\frac{x}{d}\right]\\ &= \sum_{d\le x}\Big(\frac{x}{d} + O(1)\Big) = x\sum_{d\le x}\frac{1}{d} + O\left(\sum_{d\le x} 1\right)\\ &= x\cdot\big(\log x + O(1)\big) + O(x) = x\log x + O(x)\end{aligned}$$

unter Verwendung der Formel für die harmonische Reihe.

(ii) Es gilt

$$\begin{aligned}\sum_{n\le x}\sigma(n) &= \sum_{n\le x}\sum_{d|n} d = \sum_{n\le x}\sum_{d|n}\frac{n}{d} = \sum_{d\le x}\sum_{\substack{n\le x\\ d|n}}\frac{n}{d} = \sum_{d\le x}\sum_{dm\le x} m = \sum_{d\le x}\sum_{m\le x/d} m\\ &= \sum_{d\le x}\frac{1}{2}\left[\frac{x}{d}\right]\left(\left[\frac{x}{d}\right]+1\right) = \sum_{d\le x}\frac{1}{2}\left(\frac{x}{d}+O(1)\right)\left(\frac{x}{d}+O(1)\right)\\ &= \frac{1}{2}\sum_{d\le x}\left(\frac{x^2}{d^2}+O\left(\frac{x}{d}\right)\right) = \frac{x^2}{2}\sum_{d\le x}\frac{1}{d^2}+O\left(x\sum_{d\le x}\frac{1}{d}\right)\\ &= \frac{x^2}{2}\sum_{d\le x}\frac{1}{d^2}+O(x\log x).\end{aligned}$$

Dabei gilt

$$\sum_{d\le x}\frac{1}{d^2} = \sum_{d=1}^{\infty}\frac{1}{d^2} - \sum_{d>x}\frac{1}{d^2} \quad \text{und}$$

$$\sum_{d>x}\frac{1}{d^2} \le \int_{x-1}^{\infty}\frac{dt}{t^2} = \frac{1}{x-1} = O\left(\frac{1}{x}\right) \quad \text{für } x\to\infty.$$

Also zusammen

$$\sum_{n\le x}\sigma(n) = \frac{x^2}{2}\sum_{d=1}^{\infty}\frac{1}{d^2}+O(x)+O(x\log x) = \frac{\pi^2}{12}x^2+O(x\log x).$$

Dabei haben wir $\sum\limits_{d=1}^{\infty} 1/d^2 = \pi^2/6$ verwendet, was sich leicht mit Hilfe von Fourierreihen zeigen lässt.

(iii) Zunächst gilt mit Satz 2.11 analog zu (ii)

$$\begin{aligned}\sum_{n\le x}\varphi(n) &= \sum_{n\le x} n\cdot\sum_{d|n}\frac{\mu(d)}{d} = \sum_{d\le x}\mu(d)\cdot\sum_{\substack{n\le x\\ d|n}}\frac{n}{d} = \sum_{d\le x}\mu(d)\sum_{m\le x/d} m\\ &= \sum_{d\le x}\mu(d)\cdot\left(\frac{1}{2}\left(\left[\frac{x}{d}\right]+1\right)\left[\frac{x}{d}\right]\right) = \frac{1}{2}\sum_{d\le x}\mu(d)\left(\left(\frac{x}{d}\right)^2+O\left(\frac{x}{d}\right)\right)\\ &= \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2}+O\left(x\cdot\sum_{d\le x}\frac{\mu(d)}{d}\right).\end{aligned}$$

Wegen $|\mu(d)| \leq 1$ erhalten wir als Fehlerterm

$$x \cdot \sum_{d \leq x} \frac{\mu(d)}{d} = O\left(x \cdot \sum_{d \leq x} \frac{1}{d}\right) = O\left(x \log x\right).$$

Der Hauptterm liefert wie in (ii)

$$\frac{1}{2} \sum_{d \leq x} \frac{\mu(d)}{d^2} x^2 = \frac{x^2}{2} \left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O\left(\frac{1}{x}\right)\right) = \frac{x^2}{2} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O(x).$$

Zwecks expliziter Berechnung der Konstanten im Hauptterm berechnen wir das Produkt der beiden absolut konvergenten Reihen:

$$\left(\sum_{d_1=1}^{\infty} \frac{\mu(d_1)}{d_1^2} \right) \left(\sum_{d_2=1}^{\infty} \frac{1}{d_2^2} \right) = \sum_{d_1=1}^{\infty} \sum_{d_2=1}^{\infty} \frac{\mu(d_1)}{(d_1 d_2)^2} = \sum_{n=1}^{\infty} \sum_{d_1 | n} \frac{\mu(d_1)}{n^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} \cdot \varepsilon(n) = 1$$

mit Satz 2.9 (ii). Wegen $\sum\limits_{d_2=1}^{\infty} 1/d^2 = \pi^2/6$ folgt

$$\sum_{n \leq x} \varphi(n) = \frac{3}{\pi^2} \cdot x^2 + O(x \log x).$$

□

Korollar 2.17

Die Wahrscheinlichkeit dafür, dass zwei zufällig gewählte natürliche Zahlen teilerfremd sind, ist $6/\pi^2$.

Beweis:

Naiv ist die Wahrscheinlichkeit

$$\frac{\text{Anzahl der günstigen Fälle}}{\text{Anzahl der möglichen Fälle}} =: \frac{G}{M}.$$

Offenbar ist

$$M = \sum_{m \leq x} \sum_{n \leq m} 1 = \sum_{m \leq x} m = \frac{1}{2}(x^2 + x).$$

$$G = \sum_{\substack{m \le x \\ (m,n)=1}} \sum_{n \le m} 1 = \sum_{m \le x} \sum_{\substack{n \le m \\ (n,m)=1}} 1 = \sum_{m \le x} \varphi(m) = \frac{3}{\pi^2} x^2 + O(x \log x).$$

$$\Longrightarrow \frac{G}{M} = \frac{\frac{3}{\pi^2} x^2 + O(x \log x)}{\frac{1}{2}(x^2 + x)} = \frac{6}{\pi^2} + O\left(\frac{\log x}{x}\right) \longrightarrow \frac{6}{\pi^2} \qquad (\text{für } x \to \infty).$$

□

3 Kongruenzen

Definition:

Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$. Wir sagen: a ist *kongruent zu* b *modulo* m, geschrieben: $a \equiv b \bmod m$, falls $m \mid (b-a)$. Ist $0 \leq b \leq m-1$ so heißt b *Rest von* a mod m. Offenbar ist „$\equiv \bmod m$“ eine Äquivalenzrelation auf $\mathbb{Z}$. Die Äquivalenzklassen heißen

Restklassen mod m. Es sind dies die Mengen

$$\begin{aligned} [0]_m &:= \{km = k \in \mathbb{Z}\}, \\ [1]_m &:= \{km+1 : k \in \mathbb{Z}\}, \\ &\vdots \\ [m-1]_m &:= \{km+(m-1) : k \in \mathbb{Z}\}. \end{aligned}$$

Wir schreiben dafür häufig $0 \bmod m, 1 \bmod m, \ldots, m-1 \bmod m$ oder kürzer $0, 1, \ldots, m-1$. Unter einem *vollen Restsystem mod* m verstehen wir eine Menge von m ganzen Zahlen mit jeweils einer aus jeder Restklasse.

Satz 3.1

Sei $m \in \mathbb{N}$. Die Menge der Restklassen mod m bildet mit den Verknüpfungen

$$[a]_m \pm [b]_m := [a \pm b]_m \qquad , \qquad [a]_m \cdot [b]_m := [a \cdot b]_m$$

einen Ring, den sogenannten *Restklassenring* mod m.

Beweis:

Die Ringeigenschaften ergeben sich direkt aus den Ringeigenschaften von $\mathbb{Z}$. Einziges Problem ist die Wohldefiniertheit von „$\pm$“ und „$\cdot$“.

Seien $[a]_m = [a']_m$ und $[b]_m = [b']_m$, d.h. $m \mid (a-a')$, $m \mid (b-b')$.

Es folgt $m \mid \big((a-a') \pm (b-b')\big) = \big((a \pm b) - (a' \pm b')\big) \Longleftrightarrow [a \pm b]_m = [a' \pm b']_m$.

Es folgt auch $m \mid \big((a-a')b + a'(b-b')\big) = (ab - a'b') \Longleftrightarrow [ab]_m = [a'b']_m$.

□

Korollar 3.2

Ist $f(x) \in \mathbb{Z}[x]$, so folgt aus $a \equiv a' \bmod m$, dass auch $f(a) \equiv f(a') \bmod m$.

Beweis:

$f(x)$ läßt sich mit den Operationen $+, -, \cdot$ aus x und den Koeffizienten von f aufbauen. Nach Beweis zu Satz 3.1 folgt die Behauptung.

□

Hilfssatz 3.3

Seien $m, k \in \mathbb{N}, a, a', a_1, \ldots, a_m \in \mathbb{Z}$. Dann gilt:

(i) $a \equiv a' \bmod \frac{m}{(k,m)} \iff ka \equiv ka' \bmod m$.

(ii) Für $(k,m) = 1$ ist $a \equiv a' \bmod m \iff ka \equiv ka' \bmod m$.

(iii) Für $(k,m) = 1$ ist mit $a_1, \ldots, a_m$ auch $ka_1, \ldots, ka_m$ ein volles Restsystem mod m.

Beweis:

(i) „$\Longrightarrow$“

Sei $a \equiv a' \bmod \frac{m}{(k,m)} \Longrightarrow \frac{m}{(k,m)} \mid (a - a')$. Wegen $(k,m) \mid k$ folgt

$(k,m) \cdot \frac{m}{(k,m)} \mid k \cdot (a - a') \Longrightarrow m \mid k \cdot (a - a') \Longrightarrow ka \equiv ka' \bmod m$.

„$\Longleftarrow$“

Sei $ka \equiv ka' \bmod m \Longrightarrow m \mid k \cdot (a - a') \Longrightarrow \frac{m}{(k,m)} \mid \frac{k}{(k,m)}(a - a') \Longrightarrow \frac{m}{(k,m)} \mid (a - a') \Longrightarrow a \equiv a' \bmod \frac{m}{(k,m)}$.

(ii) folgt sofort aus (i).

(iii) Nach Voraussetzung gilt für alle $i \neq j$, dass $a_i \not\equiv a_j \bmod m$. Mit (ii) folgt für alle $i \neq j$, dass auch $ka_i \not\equiv ka_j \bmod m$. Also bilden die m Zahlen $ka_1, \ldots, ka_m$

zwangsläufig ein volles Restsystem mod m.

□

Satz 3.4

Seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Die lineare Kongruenz $ax \equiv b \bmod m$ ist genau dann lösbar ($x \in \mathbb{Z}$), wenn $(a, m) \mid b$,. In diesem Fall existieren genau (a, m) verschiedene Lösungen mod m.

Beweis:

Wir dürfen O.B.d.A. annehmen, dass $a \in \mathbb{N}$ ist, denn sonst betrachten wir die Kongruenz $-ax \equiv -b \bmod m$.

„$\Longrightarrow$“

Sei $ax \equiv b \bmod m$ lösbar, d.h. $m \mid (ax - b)$ für ein $x \in \mathbb{Z}$, d.h. $ax - b = c \cdot m$ für ein $c \in \mathbb{Z}$. Wegen $(a, m) \mid a$ und $(a, m) \mid m$ folgt $(a, m) \mid b$.

„$\Longleftarrow$“

Sei $d := (a, m) \mid b$. Wir setzen $a' := a/d$, $b' := b/d$, $m' := m/d$. Die zu lösende Kongruenz, d.h. die zu lösende Gleichung $ax - b = cm$ ist äquivalent zu $a'x - b' = cm'$, d.h. zu

$a'x \equiv b' \bmod m'$. Wegen $(a', m') = 1$ durchläuft $a'x$ mit x ein volles Restsystem mod m', d.h. es gibt ein eindeutiges x_0 mod m', das die Kongruenz löst. Wir wissen bereits, dass die reduzierte Kongruenz $a'x \equiv b' \bmod m'$ genau eine Lösung x_0 mod m' besitzt (sofern $(a, m) \mid b$). Damit kommen als weitere Lösungen nur Zahlen der Form $x_0 + km', k \in \mathbb{Z}$ in Frage. Dies sind verschiedene Lösungen mod m, sofern $0 \leq x_0 + km' < m$, d.h. $0 \leq k < m/m' = d = (a, m)$.

□

Satz 3.5 (Chinesischer Restsatz)

Seien $m_1, \ldots, m_k \in \mathbb{N}$ paarweise teilerfremd. Sind $c_1, \ldots, c_k \in \mathbb{Z}$ beliebig, so besitzt das Kongruenzsystem:

$$\begin{aligned} x &\equiv c_1 \bmod m_1 \\ x &\equiv c_2 \bmod m_2 \\ &\vdots \\ x &\equiv c_k \bmod m_k \end{aligned}$$

eine eindeutige Lösung mod m mit $m = m_1 \cdot \ldots \cdot m_k$.

Beweis:

Existenz: Wir setzen $m'_j := m/m_j$ $(1 \leq j \leq k)$. Wegen $(m_i, m_j) = 1$ für $i \neq j$ ist $(m'_j, m_j) = (m_1 \cdot \ldots \cdot m_{j-1} \cdot m_{j+1} \cdot \ldots \cdot m_k, m_j) = 1$. Nach Satz 3.4 existieren Zahlen $x_j \in \mathbb{Z}$ mit $m'_j x_j \equiv c_j \bmod m_j$. Wir setzen: $x := m'_1 x_1 + \cdots + m'_k x_k$ und erhalten $x \equiv m'_1 x_1 + m'_2 x_2 + \cdots + m'_k x_k \equiv m'_j x_j \equiv c_j \bmod m_j$ $(j = 1, \ldots, k)$.

Eindeutigkeit: Seien x und y zwei Lösungen des Kongruenzsystems, d.h.

$x \equiv c_j \equiv y \bmod m_j$ $(1 \leq j \leq k)$. Also: $m_j \mid (x - y) \Longrightarrow m = m_1 \cdot \ldots \cdot m_k \mid (x - y)$

$\Longleftrightarrow x \equiv y \bmod m$.

□

Korollar 3.6

Seien $m_1, \ldots, m_k \in \mathbb{N}$ paarweise teilerfremd, $a_j, b_j \in \mathbb{Z}$ beliebig $(1 \leq j \leq k)$.
Das Kongruenzsystem

$$\begin{aligned} a_1 x &\equiv b_1 \bmod m_1 \\ &\vdots \\ a_k x &\equiv b_k \bmod m_k \end{aligned}$$

ist genau dann lösbar, wenn gilt: $(a_j, m_j) \mid b_j$ $(1 \leq j \leq k)$.

Beweis:

„$\Longrightarrow$“

Sei das System lösbar. Nach Satz 3.4 ist jede einzelne Kongruenz nur lösbar, sofern $(a_j, m_j) \mid b_j$.

„$\Longleftarrow$“

Seien $(a_j, m_j) \mid b_j$ für $1 \leq j \leq k$. Nach Satz 3.4 existiert zu jedem j ein c_j mit $a_j c_j \equiv b_j \bmod m_j$. Nach Satz 3.5 gibt es dazu ein x mit $x \equiv c_j \bmod m_j$ $(1 \leq j \leq k)$. Dies leistet das Gewünschte $(a_j x \equiv a_j c_j \equiv b_j \bmod m_j)$.

□

Neben einem vollen Restsystem mod m gibt es die sogenannten *primen Restsysteme* mod m. Dies ist eine Menge von $\varphi(m)$ Zahlen $a_1, \ldots, a_{\varphi(m)}$ derart, dass $(a_j, m) = 1$ für $1 \leq j \leq \varphi(m)$ und $a_i \not\equiv a_j \bmod m$ $(i \neq j)$. Insbesondere bildet die Menge $\{1 \leq a \leq m : (a, m) = 1\}$ ein primes Restsystem mod m.

Hilfssatz 3.7

Seien $(m, n) = 1$. Durchlaufen a und b jeweils ein primes Restsystem mod m bzw. mod n, so durchläuft $an + bm$ ein primes Restsystem mod $m \cdot n$, und zwar genau einmal.

Beweis:

Wegen $(m, n) = (a, m) = (b, n) = 1$ ist $(an + bm, m) = (an, m) = 1$ und $(an + bm, n) = (bm, n) = 1$, also $(an + bm, mn) = 1$. Außerdem ist $an + bm \equiv a'n + b'm \bmod mn$ nur für $a \equiv a' \bmod m$ und $b \equiv b' \bmod n$, denn wegen $mn \mid \big((a - a')\, n + (b - b')\, m\big)$ folgt $m \mid (a - a')\, n$ und $n \mid (b - b')\, m$, also mit $(m, n) = 1$ das Behauptete. Das heißt, die enstehenden Ausdrücke $an + bm$ sind paarweise inkongruent mod mn. Es bleibt also nur zu zeigen, dass tatsächlich jede prime Restklasse d mod mn

als ein Wert $an+bm$ angenommen wird. Da $(m,n)=1$, gibt es nach Satz 1.4 Zahlen x,y mit $mx+ny=1$. Dabei ist offenbar $(x,n)=y,m)=1$. Mit $(d,m)=(d,n)=1$ folgt $(xd,n)=(yd,m)=1$. Also können wir als Lösung a,b wählen: $a\equiv dy \bmod m$ und $b\equiv dx \bmod n$. In der Tat gilt $an+bm\equiv dyn+dxm=d(mx+ny)\equiv d \bmod mn$.

□

Bemerkung:

Hilfssatz 3.7 liefert einen neuen Beweis für die Multiplikativität von $\varphi(n)$.

Der folgende Satz wurde von Fermat für $m=p\in\mathbb{P}$ formuliert und in allgemeiner Form von Euler bewiesen.

Satz 3.8 (Kleiner Satz von Fermat)

Sei $m\in\mathbb{N}$ und $a\in\mathbb{Z}$ mit $(a,m)=1$. Dann gilt

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

Beweis:

Durchläuft x ein primes Restsystem mod m, so auch ax, denn aus$(x,m)=1$ folgt $(ax,m)=1$ und aus $ax_1\equiv ax_2 \bmod m$ sofort $m\mid a(x_1-x_2)$, also nach Hilfssatz 1.10, dass $m\mid(x_1-x_2)$, d.h. $x_1\equiv x_2 \bmod m$. Also gilt

$$\prod_{\substack{x \bmod m\\(x,m)=1}} ax \equiv \prod_{\substack{x \bmod m\\(x,m)=1}} x \bmod m.$$

Es folgt

$$0\equiv \prod_{\substack{x \bmod m\\(x,m)=1}} ax - \prod_{\substack{x \bmod m\\(x,m)=1}} x \equiv \left(\prod_{\substack{x \bmod m\\(x,m)=1}} a-1\right) \prod_{\substack{x \bmod m\\(x,m)=1}} x \bmod m.$$

Also teilt m die rechte Seite der Kongruenz. Wegen $(x, m) = 1$ für alle vorkommenden x ist, erneut mit Hilfssatz 1.10, m ein Teiler von

$$\prod_{\substack{x \bmod m \\ (x,m)=1}} a - 1 \equiv a^{\varphi(m)} - 1 \bmod m,$$

woraus sofort das Gewünschte folgt.

□

Der nun folgende Satz wurde von Waring formuliert, von Lagrange bewiesen und nach einem ganz anderen Mathematiker benannt.

Satz 3.9 (Satz von Wilson)

Für eine natürliche Zahl $n > 1$ gilt:

$$n \in \mathbb{P} \Longleftrightarrow (n-1)! \equiv -1 \bmod n.$$

Beweis:

„$\Longrightarrow$“

Sei $n = p \in \mathbb{P}$. Für $p = 2$ ist die Behauptung richtig. Wir dürfen also annehmen, dass $2 \nmid p$.

Behauptung: Zu jedem a mit $0 < a < p$ existiert genau ein $\overline{a}$, $0 < \overline{a} < p$, mit $a\overline{a} \equiv 1 \bmod p$; $\overline{a}$ heißt auch *multiplikatives Inverses* von a mod p. Die Existenz von $\overline{a}$ folgt sofort aus Satz 3.4, denn $(a, p) = 1$. Die Eindeutigkeit folgt ebenfalls sofort mit dem Argument zu Beginn des Beweises von Satz 3.8. Ist $a = a'$, so folgt $a^2 \equiv a\overline{a} \equiv 1 \bmod p$, d.h. $p \mid (a^2 - 1) = (a-1)(a+1)$, also nur für die Fälle $a = 1$ und $a = p - 1$. Dennoch können wir die Zahlen $2, 3, \ldots, p-2$ zu genau $(p-3)/2$ Paaren $a_i, \overline{a_i}$ mit $a_i\overline{a_i} \equiv 1 \bmod p$ $(1 \leq i \leq (p-3)/2)$ ordnen. Wir erhalten

$$(p-1)! \equiv 1 \cdot (p-1) \cdot \prod_{i=1}^{(p-3)/2} a_i \cdot \overline{a_i} \equiv p - 1 \equiv -1 \bmod p.$$

„$\Longleftarrow$“

Annahme: $n \notin \mathbb{P}$, d.h. $n = 1$ oder $n = m \cdot k$ mit $1 \leq m \leq n-1$. Nach Voraussetzung ist $n \neq 1$; daher folgt offenbar $m \mid (n-1)!$. Daraus folgt aber $m \nmid \big((n-1)! + 1\big)$, d.h. $(n-1)! \not\equiv -1 \bmod m$. Erst recht ist $(n-1)! \not\equiv -1 \bmod n$.

□

Korollar 3.10

Sei $p \in \mathbb{P}_{>2}$. Dann ist die Kongruenz $x^2 \equiv -1 \bmod p$ genau dann lösbar, wenn $p \equiv 1 \bmod 4$, und zwar mit $x \equiv \pm \big(\frac{p-1}{2}\big)! \bmod p$.

Beweis:

„$\Longrightarrow$“

Wir setzen $r := (p-1)/2$. Ist $p \not\equiv 1 \bmod 4$, d.h. $p \equiv 3 \bmod 4$, so folgt aus derLösbarkeit der Kongruenz $x^{p-1} \equiv (x^2)^r \equiv (-1)^r \equiv -1 \bmod p$, da r ungerade ist. Andererseits ist nach kleinem Fermat $x^{p-1} \equiv 1 \bmod p$ für alle x mit $p \nmid x$. Die Folgerung $1 \equiv -1 \bmod p$ bedeutet $p \mid 2$. Widerspruch!

„$\Longleftarrow$“

Nach Satz 3.9 gilt mit $r := (p-1)/2$ wegen $2 \mid r$

$$\begin{aligned} -1 \equiv (p-1)! &\equiv 1 \cdot 2 \cdot \ldots \cdot r(r+1)(r+2) \cdot \ldots \cdot (r+r) \bmod p \\ &\equiv r!(-r)(-r+1)(-r+2) \cdot \ldots \cdot (-1) \equiv (-1)^r (r!)^2 = (r!)^2 \bmod p. \end{aligned}$$

Also sind $r!$ und $-r!$ Lösungen der Kongruenz.

□

Satz 3.11 (von Lagrange)

Sei $p \in \mathbb{P}$ und sei $f(x) \in \mathbb{Z}[x]$ mit führendem Koeffizienten, der nicht durch p teilbar ist. Ist grad $f = n$, so hat die Kongruenz $f(x) \equiv 0 \bmod p$ höchstens n verschiedene Lösungen mod p.

Beweis: (Induktion über n)

$n = 1$:

Sei $f(x) = ax + b$ mit $p \nmid a$. Nach Satz 3.4 besitzt die Kongruenz $ax \equiv -b \bmod p$, genau $(a, p) = 1$ Lösungen mod p.

$n - 1 \to n$:

Für jedes $a \in \mathbb{Z}$ gilt $f(x) - f(a) = (x - a) \cdot g(x)$, wobei $g(x) \in \mathbb{Z}[x]$ den Grad $n - 1$ und denselben führenden Koeffizienten wie f besitzt. Ist a eine Nullstelle von f mod p, dann folgt $f(x) \equiv 0 \bmod p \iff x \equiv a \bmod p$ oder $g(x) \equiv 0 \bmod p$. Nach Induktionsvoraussetzung folgt die Behauptung.

□

Bemerkung:

Satz 3.11 ist im allgemeinen falsch für zusammengesetzte Moduln. Besitzt z.B. $f \in \mathbb{Z}[x]$ für paarweise teilerfremde Moduln $m_1, \ldots, m_k$ jeweils $s_1, \ldots, s_k$ Lösungen bezüglich der Kongruenzen $f(x) \equiv 0 \bmod m_i$ $(1 \leq i \leq k)$, so hat $f(x) \equiv 0 \bmod m_1 \cdot \ldots \cdot m_k$ nach dem Chinesischen Restsatz $s_1 \cdot \ldots \cdot s_k$ Lösungen mod $m_1 \cdot \ldots \cdot m_k$. Sogar für Primzahlpotenzmoduln ist Satz 3.11 im Allgemeinen falsch: $x^2 \equiv 1 \bmod 8$ hat die Lösungen $x \equiv 1, 3, 5, 7 \bmod 8$.

Der Restklassenring mod p bildet einen Körper (vgl. Beweis Wilson), geschrieben $\mathbb{Z}_p$ oder $\mathbb{F}_p$ (engl. Field = Körper). Statt $x^d \equiv 1 \bmod p$ schreiben wir auch $x^d = 1$, zu lösen über $\mathbb{Z}_p$.

Korollar 3.12

Sei $p \in \mathbb{P}$ und sei $d \mid (p - 1)$. Dann hat die Kongruenz $x^d \equiv 1 \bmod p$ genau d Lösungen mod p.

Beweis:

Nach dem Satz von Lagrange ist nur zu zeigen, dass die Kongruenz mindestens d Lösungen hat. Die spezielle Kongruenz $x^{p-1} \equiv 1 \bmod p$ hat die Lösungen $1, 2, 3, \ldots, p-1$, d.h. genau $p-1$ Lösungen (nach dem kleinem Satz von Fermat). Wegen $d \mid (p-1)$ ist

$$x^{p-1} - 1 = \left(x^d - 1\right)\left(x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1\right) =: \left(x^d - 1\right) g(x).$$

Nach Satz 3.11 hat $g(x) \equiv 0 \bmod p$ höchstens $p - 1 - d$ Lösungen mod p, woraus die Behauptung folgt.

□

Definition:

Sind $a, m \in \mathbb{N}$ mit $(a, m) = 1$, so heißt $\mathrm{ord}_m(a) := \min\{d \in \mathbb{N} : a^d \equiv 1 \bmod m\}$ *Ordnung von* a mod m. Nach dem kleinem Satz von Fermat ist $a^{\varphi(m)} \equiv 1 \bmod m$, d.h. $\mathrm{ord}_m(a)$ existiert und ist höchstens gleich $\varphi(m)$.

Hilfssatz 3.13

Ist $k \in \mathbb{N}$ mit $a^k \equiv 1 \bmod m$ für $a, m \in \mathbb{N}$, $(a, m) = 1$, so gilt $\mathrm{ord}_m(a) \mid k$. Insbesondere ist $\mathrm{ord}_m(a) \mid \varphi(m)$.

Beweis:

Nach Division mit Rest existieren $q, r \in \mathbb{Z}$ mit $0 \leq r \leq \mathrm{ord}_m(a)$ derart, dass $k = \mathrm{ord}_m(a) \cdot q + r$. Es folgt $a^r \equiv a^r \left(a^{ord_m(a)}\right)^q = a^k \equiv 1 \bmod m$. Wegen der Minimalität von $\mathrm{ord}_m(a)$ bleibt nur $r = 0$ (sonst wäre r ein Subminimum). Die 2. Behauptung gilt nach dem kleinem Satz von Fermat.

□

Definition:

Sei $m \in \mathbb{N}$. Eine natürliche Zahl a heißt *Primitivwurzel* mod m, falls $\mathrm{ord}_m(a) = \varphi(m)$.

Satz 3.14

Sei $p \in \mathbb{P}_{>2}$. Dann gibt es genau $\varphi(p-1)$ Primitivwurzeln mod p.

Beweis:

Jede der Zahlen $1, 2, \ldots, p-1$ besitzt eine Ordnung mod p, die nach Hilfssatz 3.13 ein Teiler von $\varphi(p) = p-1$ ist. Sei

$$\psi(d) := \sharp\{a : 1 \leq a \leq p-1, \mathrm{ord}_p(a) = d\}$$

für alle $d \mid (p-1)$. Es folgt $\sum_{d|(p-1)} \psi(d) = p-1$.

Behauptung: $\psi(d) \neq 0 \Longrightarrow \psi(d) = \varphi(d)$.

Sei $\psi(d) \neq 0$, d.h. es existiert ein a mit $\mathrm{ord}_p(a) = d$. Die Zahlen $a, a^2, \ldots, a^d$ sind sämtlich Lösungen der Kongruenz $x^d \equiv 1 \bmod p$. Außerdem gilt $a^i \not\equiv a^j \bmod p$ für $1 \leq i < j \leq d$, denn sonst wäre $a^{j-i} \equiv 1 \bmod p$ mit $1 \leq j-i \leq d-1$. Widerspruch! Also haben wir genau die d Lösungen $a, a^2, \ldots, a^d$ der Kongruenz $x^d \equiv 1 \bmod p$ gefunden (Korollar 3.12). Darunter befinden sich also alle b mit $\mathrm{ord}_p(b) = d$. Wir wollen zeigen, dass $b = a^m$ für ein m, $1 \leq m \leq d$ genau dann gilt, wenn $(m, d) = 1$. Einerseits haben solche $b = a^m$, $(m, d) = 1$ die Ordnung d, denn: Sei $1 \equiv b^{d'} \equiv a^{m \cdot d'} \bmod p$. Wegen $\mathrm{ord}_p(a) = d$ folgt, dass $d \mid md' \Longrightarrow d \mid d' \Longrightarrow b$ hat in der Tat die Ordnung d. Hat umgekehrt b die Ordnung d, so ist nach obiger Vorüberlegung $b \equiv a^m \bmod p$ für ein $1 \leq m \leq d$. Daraus folgt $(m, d) = 1$, denn sonst wäre $b^{d/(m,d)} \equiv a^{md/(m,d)} \equiv (a^d)^{d/(m,d)} \equiv 1 \bmod p$. Dies ist ein Widerspruch, da b dann eine kleinere Ordnung als d hätte. Also gibt es genau $\varphi(d)$ Zahlen der Ordnung d (nämlich die a^m mit $(m, d) = 1$), d.h. $\psi(d) = \varphi(d)$. Insbesondere ist $\psi(p-1) = \varphi(p-1)$,

sofern es mindestens eine Primitivwurzel gibt. Nach Korollar 2.8(ii) ist

$$\sum_{d|(p-1)} \varphi(d) = p - 1 = \sum_{d|(p-1)} \psi(d),$$

also mit unserer Zwischenbehauptung

$$0 = \sum_{d|(p-1)} (\varphi(d) - \psi(d)) = \sum_{\substack{d|(p-1) \\ \psi(d)=0}} \varphi(d).$$

Wegen $\varphi(d) \geq 1$ für alle $d \in \mathbb{N}$ folgt $\psi(d) \neq 0$ für alle $d \mid (p-1)$, also insbesondere $\psi(p-1) = \varphi(p-1)$.

□

Bemerkungen:

(i) Der Beweis zeigt, dass $\psi(d) = \varphi(d)$ für alle $d \mid (p-1)$.

(ii) Der Beweis zeigt auch: Ist a mod p Primitivwurzel, so finden wir alle Primitivwurzeln mod p mit der Form a^m mod p mit $1 \leq m \leq p-1$ und $(m, p-1) = 1$.

Satz 3.15

Sei $p \in \mathbb{P}_{>2}$, $k \in \mathbb{N}$. Dann existiert eine Primitivwurzel mod p^k.

Beweis:

Sei g eine Primitivwurzel mod p (existiert nach Satz 3.14). Wir wollen zeigen, dass es ein geeignetes $x \in \mathbb{N}$ gibt derart, dass $g_x := g + p \cdot x$ Primitivwurzel mod p^k für alle $k \in \mathbb{N}$ ist. Zunächst ist $g^{p-1} \equiv 1 \bmod p$, also $g^{p-1} = 1 + py$ für ein $y \in \mathbb{N}$. Nach dem binomischen Lehrsatz folgt

$$\begin{aligned} g_x^{p-1} = (g+px)^{p-1} &= g^{p-1} + (p-1)g^{p-2} \cdot px + \binom{p-1}{2} g^{p-3} \cdot p^2x^2 + \cdots \\ &\equiv 1 + \big(y + (p-1)g^{p-2}x\big)\, p \bmod p^2, \end{aligned}$$

d.h. $g_x^{p-1} = 1 + pz$, wobei $z \equiv y + (p-1)g^{p-2}x \bmod p$. Wegen $p \nmid (p-1)g^{p-2}$ durchläuft mit x auch $(p-1)g^{p-2}x$ ein volles Restsystem mod p. Insbesondere kann

x so gewählt werden, dass $(p-1)g^{p-2}x \not\equiv -y \bmod p$, d.h. $p \nmid z$. Wir tun dies und behaupten, dass so ein g_x Primitivwurzel mod p^k für jedes $k \in \mathbb{N}$ ist. Setze $d := \mathrm{ord}_{p^k}(g_x)$. Nach Hilfssatz 3.13 gilt $d \mid \varphi(p^k) = p^{k-1}(p-1)$. Wegen $g_x \equiv g \bmod p$ ist g_x nach Voraussetzung Primitivwurzel mod p, also $\mathrm{ord}_p(g_x) = p-1$; Daher gilt $(p-1) \mid d$, d.h. $d = (p-1)p^j$ für ein $j < k$. Nach dem binomischen Lehrsatz und Korollar 2.3(i) gilt

$$\begin{aligned}(1+pz)^{p^j} &= 1 + \binom{p^j}{1}pz + \sum_{t=2}^{p^j}\binom{p^j}{t}(pz)^t \\ &= 1 + p^{j+1}\cdot z + \sum_{t=2}^{p^j}\frac{p^j(p^j-1)\cdot\ldots\cdot(p^j-t+1)}{t!}\cdot(pz)^t \\ &= 1 + p^{j+1}\cdot z_j\end{aligned}$$

für ein z_j mit $p \nmid z_j$ wegen $p \nmid z$ nach Konstruktion. Nach Definition von d ist $g_x^d \equiv 1 \bmod p^k$, d.h.

$$1 \equiv g_x^d \equiv g_x^{(p-1)p^j} \equiv (1+pz)^{p^j} \equiv 1 + p^{j+1}z_j \bmod p^k,$$

also $j+1 \geq k$, da $p \nmid z_j$. Wegen $j < k$ folgt $j = k-1$, d.h. $d = \varphi\left(p^k\right)$ wie gewünscht.

□

Korollar 3.16

Sei $m \in \mathbb{N}$. Es gibt Primitivwurzeln mod m genau dann, wenn $m = 1, 2, 4$ oder $m = p^k$ oder $m = 2p^k$ mit $p \in \mathbb{P}_{>2}$ und $k \in \mathbb{N}$.

Beweis:

„$\Longleftarrow$“

Der Fall $m = p^k$ ist genau Satz 3.15. Zum Fall $m = 2p^k$: Sei g Primitivwurzel mod p^k (Satz 3.15). Sei g' das ungerade Element aus $\{g, g+p^k\}$. Dann ist g' Primitivwurzel mod $2p^k$, denn: $\varphi(2p^k) = \varphi(2)\cdot\varphi(p^k) = \varphi(p^k)$, und aus $g'^d \equiv 1 \bmod 2p^k$ folgt $g'^d \equiv 1 \bmod p^k$; also $d \geq \varphi(p^k) = \varphi(2p^k)$, da g' Primitivwurzel mod $2p^k$ ist.

„$\Longrightarrow$“

1.Fall: $n = n_1 \cdot n_2$ mit $(n_1, n_2) = 1$ und $n_1 \geq 3$, $n_2 \geq 3$.

Dann enthält jedes n_i einen ungeraden Primfaktor p_0 oder einen Faktor 2^{m_0} mit $m_0 \geq 2$. Wegen $\varphi(p_0^{k_o}) = p_0^{k_0} - p_0^{k_0-1}$ bzw. $\varphi(2^{m_0}) = 2^{m_0-1}$ folgt $2 \mid \varphi(n_1)$ und $2 \mid \varphi(n_2)$. Also gilt für jedes a mit $(a, n) = 1$

$$a^{\frac{1}{2}\varphi(n)} = \left(a^{\varphi(n_1)}\right)^{\frac{1}{2}\varphi(n_2)} \equiv 1 \bmod n_1$$

und analog $a^{\frac{1}{2}\varphi(n)} \equiv 1 \bmod n_2$, also $a^{\frac{1}{2}\varphi(n)} \equiv 1 \bmod n$. Das bedeutet: es existiert keine Primitivwurzel.

2.Fall: $n = 2^k, k \geq 3$.

Wir zeigen mit Induktion: $a^{2^{k-2}} \equiv 1 \bmod 2^k$ für alle ungeraden a, d.h. es gibt keine Primitivwurzeln mod 2^k, $k \geq 3$.

$k = 3$: $a^2 \equiv 1 \bmod 8$ für ein ungerades a.

$k \to k+1$: $a^{2^{k-1}} - 1 = \left(a^{2^{k-2}}\right)^2 - 1 = \left(a^{2^{k-2}} - 1\right)\left(a^{2^{k-2}} + 1\right)$. Nach Induktionsvoraussetzung ist der erste Faktor durch 2^k teilbar und der zweite ist gerade. Daraus folgt $2^{k+1} \mid \left(a^{2^{k-1}} - 1\right)$. Nach kurzem Nachdenken sind wir überzeugt, dass damit alle möglichen Fälle erschlagen wurden.

□

4 Quadratische Reste

Nach Behandlung linearer Kongruenzen ($ax + b \equiv 0 \bmod m$) wenden wir uns jetzt der Lösung quadratischer Kongruenzen in einer Variablen $ax^2 + bx + c \equiv 0 \bmod m$ zu. Mit $y := 2ax + b$ und $d := b^2 - 4ac$ ist dies äquivalent zu $y^2 \equiv d \bmod 4am$, wie sich nach Multiplikation der Ausgangskongruenz mit $4a$ und anschließender quadratischer Ergänzung sofort ergibt. Es genügt also, reinquadratische Kongruenzen zu untersuchen.

Definition:
Sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $(a, m) = 1$. Dann heißt a *quadratischer Rest* mod m, falls die Kongruenz $x^2 \equiv a \bmod m$ lösbar ist, andernfalls *quadratischer Nichtrest* mod m. Für Primzahlmoduln $m = p$ und ein beliebiges $a \in \mathbb{Z}$ heißt

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{für } p \,|\, a, \\ 1 & \text{falls a quadratischer Rest } \bmod p \text{ ist}, \\ -1 & \text{falls a quadratischer Nichtrest } \bmod p \text{ ist}, \end{cases}$$

Legendre-Symbol.

Hilfssatz 4.1

Sei $p \in \mathbb{P}$. Dann gilt:

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

(ii) Es gibt genau $(p-1)/2$ quadratische Reste und $(p-1)/2$ quadratische Nichtreste mod p.

Beweis:

(i) Klar.

(ii) Wir setzen $r := (p-1)/2$. Offenbar sind $1^2, 2^2, \ldots, r^2$ quadratische Reste mod p

(sogar Quadratzahlen) und paarweise inkongruent mod p, denn: Seien $1 \leq i < j \leq r$ mit $i^2 \equiv j^2 \bmod p$. $\Longrightarrow 0 \equiv j^2 - i^2 \bmod p \equiv (i+j)(i-j) \bmod p$, also $j - i \equiv 0 \bmod p$ oder $j + i \equiv 0 \bmod p$. Widerspruch! Wegen $(p-j)^2 \equiv p^2 - 2pj + j^2 \equiv j^2 \bmod p$ liefern die Quadrate $(r+1)^2, (r+2)^2, \ldots, (p-1)^2$ dieselben quadratischen Reste wie oben. Daher existieren genau $r = (p-1)/2$ quadratische Reste mod p, also auch genau r Nichtreste mod p (0 ist weder Rest noch Nichtrest).

□

Satz 4.2 (Eulers Kriterium)

Seien $p \in \mathbb{P}_{>2}$, $a \in \mathbb{Z}$. Dann gilt

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

Beweis:

Sei wieder $r := (p-1)/2$. Für $p \mid a$ ist alles klar.

1.Fall: a ist quadratischer Rest mod p. Dann existiert ein $x \in \mathbb{N}$ mit $x^2 \equiv a \bmod p$. Mit dem kleinen Satz von Fermat folgt

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

2.Fall: a ist quadratischer Nichtrest. Nach Satz 3.11 von Lagrange hat die Kongruenz $x^r \equiv 1 \bmod p$ höchstens r Lösungen. Nach Hilfssatz 4.1(ii) sind dies genau die r quadratischen Reste $j^2 = 1^2, 2^2, \ldots, r^2 \bmod p$, denn $(y^2)^r \equiv y^{p-1} \equiv 1 \bmod p$ nach dem kleinen Satz von Fermat. Also lösen die quadratischen Nichtreste die Kongruenz

nicht. Nach dem kleinen Satz von Fermat gilt jedoch $a^{2r} = a^{p-1} \equiv 1 \bmod p$, d.h. $(a^r - 1)(a^r + 1) \equiv 0 \bmod p$. Es bleibt nur

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

nach Definition des Legendre-Symbols.

□

Bemerkung:

Anstelle des Satzes von Lagrange könnten wir auch die Existenz von Primitivwurzeln verwenden.

Korollar 4.3

Für $p \in \mathbb{P}$ und $a, b \in \mathbb{Z}$ gilt

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

Beweis:

Für $p = 2$ ist die Aussage trivial. Sei also $p \geq 3$. Nach Eulers Kriterium gilt

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

Wegen $p \geq 3$ und $\left(\frac{\cdot}{p}\right) \in \{0, 1, -1\}$ folgt aus der Kongruenz sogar die Gleichheit beider Seiten.

□

Satz 4.4 (1. Ergänzungsgesetz)

Für $p \in \mathbb{P}$, $p \neq 2$ gilt

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

Beweis:

Nach Eulers Kriterium gilt $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$. Daraus folgt die Behauptung.

□

Bemerkung:

Das 1. Ergänzungsgesetz besagt, dass -1 quadratischer Rest mod p ist, genau dann, wenn $p \equiv 1 \bmod 4$, d.h. -1 ist quadratischer Nichtrest mod p für alle $p \equiv 3 \bmod 4$. Also ist für $p \equiv 1 \bmod 4$ die Kongruenz $x^2 \equiv -1 \bmod p$ lösbar. Nach Korollar 3.10 sind die beiden Lösungen gegeben durch $x = \pm\left(\frac{p-1}{2}\right)!$.

Definition:

Sei $n \in \mathbb{N}_{>1}$ und $a \in \mathbb{Z}$. Wir definieren den *betragskleinsten Rest* a' mod n als diejenige Zahl $a' \in \mathbb{Z}$, für die gilt $a' \equiv a \bmod n$ und $-n/2 < a' \leq n/2$.

Hilfssatz 4.5 (Lemma von Gauß)

Sei $p \in \mathbb{P}_{>2}$, sei $a \in \mathbb{Z}, p \nmid a$. Es bezeichne $l_p(a)$ die Anzahl der betragskleinsten Reste $(ak)' \bmod p, 1 \leq k \leq \frac{p-1}{2}$, mit $(ak)' < 0$. Dann gilt

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

Beweis:

Wir setzen $r := (p-1)/2$ und $a_k := (ak)'$.

Behauptung: $\{|a_k| : 1 \leq k \leq r\} = \{1, 2, \ldots, r\}$.

Wegen $p \nmid a$ ist für alle k offensichtlich $1 \leq |a_k| \leq r$. Es bleibt zu zeigen, dass die $|a_k|$ paarweise verschieden sind. Aus $a_i = a_j$ folgt $(ai)' = (aj)'$, d.h. $a_i \equiv a_j \bmod p$, also $i \equiv j \bmod p$, d.h. $i = j$. Aus $a_i = -a_j$ ergäbe sich $a(i+j) \equiv 0 \bmod p \mid (i+j)$, es gilt aber $1 \leq i + j \leq 2r = p - 1$. Widerspruch! Damit gilt die Zwischenbehauptung. Es folgt

$$\begin{aligned} a^r \cdot r! \equiv \prod_{k=1}^{r}(ak) &\equiv a_1 \cdot \ldots \cdot a_r \equiv |a_1| \cdot \ldots \cdot |a_r| \cdot (-1)^{l_p(a)} \\ &\equiv r! \cdot (-1)^{l_p(a)} \bmod p, \end{aligned}$$

d.h. $a^r \equiv (-1)^{l_p(a)} \bmod p$. Mit Eulers Kriterium (Satz 4.2) folgt auch hier die Behauptung.

□

Korollar 4.6

Für $p \in \mathbb{P}_{>2}$ gilt

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

Beweis:

Mit der Terminologie der betragskleinsten Reste haben wir $(2k)' = 2k$ für $1 \leq k \leq [p/4]$ und $(2k)' = 2k - p$ für $[p/4] < k \leq (p-1)/2$. Also ist mit dem Lemma von Gauß $l_p(2) = (p-1)/2 - [p/4]$. Danach bleibt nur zu zeigen: $(p-1)/2 - [p/4] \equiv (p^2-1)/8 \bmod 2$. Wir unterscheiden $p = 4n + r$ mit $r \in \{1, 3\}$. Dann ist

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] = 2n + \frac{r-1}{2} - n = n + \frac{r-1}{2} \qquad \text{und}$$

$$\frac{p^2-1}{8} = \frac{1}{8}(16n^2 + 8nr + r^2 - 1) = 2n^2 + nr + \frac{r^2-1}{8} \equiv n + \frac{r^2-1}{8} \bmod 2.$$

In den beiden Fällen $r = 1, 3$ stimmen die Ausdrücke mod 2 überein.

□

Bemerkung:

Das 2. Ergänzungsgesetz besagt, dass 2 quadratischer Rest mod p ist für alle $p \equiv \pm 1 \bmod 8$ und quadratischer Nichtrest mod p für alle $p \equiv \pm 3 \bmod 8$.

Das folgende Ergebnis wurde von Euler, Legendre und Gauß unabhängig voneinander entdeckt, jedoch erst von Gauß bewiesen.

Satz 4.7 (Quadratisches Reziprozitätsgesetz)

Seien $p, q \in \mathbb{P}_{>2}, p \neq q$. Dann gilt

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

d.h. für $p \equiv q \equiv 3 \bmod 4$ gilt $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, sonst $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

Beweis:

Nach dem Lemma von Gauß (Hilfssatz 4.5) ist $\left(\frac{p}{q}\right) = (-1)^{l_q(p)}$, wobei $l_q(p)$ die Anzahl der betragskleinsten Reste $(px)' \bmod q$ mit $1 \leq x \leq (q-1)/2$ und $-q/2 < (px)' < 0$ ist. Wegen $(px)' \equiv px \bmod q$, d.h. $(px)' = px - qy$ für ein eindeutiges $y \in \mathbb{Z}$ ist

$$l_q(p) = \sharp\left\{(x,y) \in \mathbb{Z}^2 : 1 \leq x \leq \frac{q-1}{2}, -\frac{q}{2} < px - qy < 0\right\}.$$

Dabei haben wir offensichtlich:

$$1 \leq y \leq \frac{px}{q} + \frac{1}{2} < \frac{p}{2} + \frac{1}{2} = \frac{p+1}{2},$$

also $1 \leq y \leq (p-1)/2$. Demnach ist

$$l_q(p) = \sharp\left\{(x,y) \in \mathbb{Z}^2 : 0 < x < \frac{q}{2}, 0 < y < \frac{p}{2}, -\frac{q}{2} < px - qy < 0\right\}.$$

Analog erhalten wir $\left(\frac{q}{p}\right) = (-1)^{l_p(q)}$, wobei aus Symmetriegründen

$$l_p(q) = \sharp\left\{(x,y) \in \mathbb{Z}^2 : 0 < x < \frac{q}{2}, 0 < y < \frac{p}{2}, -\frac{p}{2} < qy - px < 0\right\}.$$

Es bleibt zu zeigen

$$l_q(p) + l_p(q) \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \bmod 2,$$

d.h.

$$L(p,q) := \frac{p-1}{2} \cdot \frac{q-1}{2} - \big(l_q(p) + l_p(q)\big) \equiv 0 \bmod 2.$$

Offenbar ist $\frac{p-1}{2} \cdot \frac{q-1}{2}$ genau die Anzahl der Gitterpunkte $(x,y) \in \mathbb{Z}^2$ im Rechteck $0 < x < q/2$, $0 < y < p/2$. Also ist $L(p,q)$ gerade die Anzahl der Gitterpunkte dieses Rechtecks mit $px - qy \leq -q/2$ oder $qy - px \leq -p/2$. Wir bezeichnen

$$\triangle_1 = \left\{(x,y) \in \mathbb{Z}^2 : 0 < x < \frac{q}{2}, 0 < y < \frac{p}{2}, px - qy \leq -\frac{q}{2}\right\},$$

$$\triangle_2 = \left\{(x,y) \in \mathbb{Z}^2 : 0 < x < \frac{q}{2}, 0 < y < \frac{p}{2}, qy - px \leq -\frac{p}{2}\right\},$$

also $L(p,q) = |\triangle_1 \cup \triangle_2|$. Offenbar gilt $\triangle_1 \cap \triangle_2 = \emptyset$, und wir haben eine Bijektion zwischen den Gitterpunkten in $\triangle_1$ und denen in $\triangle_2$, nämlich

$$(x,y) \longmapsto \left(\frac{q+1}{2} - x, \frac{p+1}{2} - y\right).$$

Es folgt $L(p,q) = |\triangle_1| + |\triangle_2| = 2 \cdot |\triangle_1|$, also wie gewünscht, ist $L(p,q)$ gerade.

□

Beispiel:

Ist $x^2 \equiv -15 \bmod 71$ lösbar? Wir berechnen

$$\begin{aligned}\left(\frac{-15}{71}\right) &= \left(\frac{-1}{71}\right) \cdot \left(\frac{3}{71}\right) \cdot \left(\frac{5}{71}\right) = (-1)^{35} \cdot \left(\frac{71}{3}\right) \cdot (-1)^{35 \cdot 1} \cdot \left(\frac{71}{5}\right) \cdot (-1)^{35 \cdot 2} \\ &= \left(\frac{71}{3}\right) \cdot \left(\frac{71}{5}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{1}{5}\right) = (-1)^1 \cdot 1 = -1;\end{aligned}$$

daher ist die obige Kongruenz unlösbar.

Das Legendre-Symbol lässt sich ohne weiteres auf zusammengesetzte Moduln verallgemeinern.

Definition:

Sei $n \in \mathbb{N}, \quad 2 \nmid n$, so dass $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ mit ungeraden, nicht notwendig verschiedenen Primzahlen p_i. Ist $a \in \mathbb{Z}$, so heißt

$$\left(\frac{a}{n}\right) := \begin{cases} \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_k}\right) & \text{für } (a,n) = 1, \quad n > 1, \\ 1 & \text{für } \quad n = 1, \\ 0 & \text{für } \quad (a,n) > 1 \end{cases}$$

Jacobi-Symbol.

Satz 4.8

Seien $n \in \mathbb{N}$, $2 \nmid n$ und $(a, n) = 1$. Dann ist a quadratischer Rest mod n genau dann, wenn a quadratischer Rest mod p für alle $p \in \mathbb{P}$ mit $p \nmid n$ ist. Insbesondere gilt

$$\left(\frac{a}{n}\right) = 1 \not\Longleftrightarrow_{i.A.} \quad a \text{ ist quadratischer Rest mod } n,$$

aber

$$\left(\frac{a}{n}\right) = -1 \Longrightarrow \quad a \text{ ist quadratischer Nichtrest mod } n.$$

Beweis:

„$\Longrightarrow$“

Sei $n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$ die Primfaktorzerlegung von n. Ist a quadratischer Rest mod n, so existiert ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \bmod n \Longrightarrow x^2 \equiv a \bmod p_i$ für alle $1 \leq i \leq k$.

„$\Longleftarrow$“

Nach Voraussetzung existieren $x_i \in \mathbb{Z}, (1 \leq i \leq k)$ derart, dass $x_i^2 \equiv \bmod p_i$. Wir zeigen zunächst mittels Induktion für $p \mid n$ die Behauptung:

$x^2 \equiv a \bmod p$ lösbar $\Longrightarrow a \bmod p^r (r \in \mathbb{N})$ lösbar.

$r = 1$: Klar.

$r \to r + 1$: Sei $x_0^2 \equiv a \bmod p^r$. Wegen $(a, n) = 1$ und $p \neq 2$ ist $(2x_0, p) = 1$. Also besitzt die Kongruenz $2x_0 \cdot y + (x_0^2 - a)/p^r \equiv 0 \bmod p$ eine Lösung y. Wir setzen $x := x_0 + p^r y$ und erhalten

$$\begin{aligned} x^2 = x_0^2 + 2x_0 y p^r + p^{2r} y^2 &\equiv x_0^2 + 2x_0 y p^r \\ &\equiv x_0^2 - (x_0^2 - a) \equiv a \bmod p^{r+1}. \end{aligned}$$

Damit ist unsere Zwischenbehauptung gezeigt. Demnach existieren $y_i \in \mathbb{Z}\,(1 \leq i \leq k)$ derart, dass $y_i^2 \equiv \bmod p_i^{e_i}$. Mit dem Chinesischem Restsatz konstruieren wir ein $y \equiv y_i \bmod p_i^{e_i}$ für alle $1 \leq i \leq k$. Dies erfüllt offenbar $y^2 \equiv a \bmod p_i^{e_i}$, also $y^2 \equiv \bmod n$.

Die Zusatzbehauptungen folgen leicht:

Ist etwa $n = p_1 \cdot p_2$, $p_1, p_2 \in \mathbb{P}$ verschieden, und a quadratischer Nichtrest mod p_1

und mod p_2 (z.B. ist 2 quadratischer Nichtrest mod 3 und mod 5), so gilt zwar

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) = (-1)\cdot(-1) = 1,$$

aber nach obigem Ergebnis ist a trotzdem kein quadratischer Rest mod n. Gilt allerdings $\left(\frac{a}{n}\right) = -1$, so existiert mindestens ein $p \mid n$ mit $\left(\frac{a}{p}\right) = -1$, d.h. a ist quadratischer Nichtrest mod n.

□

Sämtliche von uns bewiesenen Resultate über das Legendre-Symbol gelten entsprechend für das Jacobi-Symbol und lassen sich vollkommen analog herleiten. Dabei wird lediglich zusätzlich verwendet, dass für ungerades $n = n_1 n_2$ gilt

$$\begin{aligned} 0 \equiv \frac{1}{2}(n_1-1)(n_2-1) &\equiv \frac{1}{2}n_1n_2 - \frac{1}{2}n_1 - \frac{1}{2}n_2 + \frac{1}{2} \\ &\equiv \frac{1}{2}(n-1) - \frac{1}{2}(n_1-1) - \frac{1}{2}(n_2-1) \bmod 2, \end{aligned}$$

also

$$\frac{1}{2}(n-1) \equiv \frac{1}{2}(n_1-1) + \frac{1}{2}(n_2-1) \bmod 2,$$

und entsprechend

$$\frac{1}{8}(n^2-1) \equiv \frac{1}{8}(n_1^2-1) + \frac{1}{8}(n_2^2-1) \bmod 2.$$

Satz 4.9

Seien $m, n \in \mathbb{N}$ ungerade und $a, a', b \in \mathbb{Z}$.

(i) $a \equiv a' \bmod n \Longrightarrow \left(\frac{a}{n}\right) = \left(\frac{a'}{n}\right)$;

(ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\cdot\left(\frac{b}{n}\right)$ (Multiplikativität);

(iii) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\cdot\left(\frac{a}{n}\right)$ (Multiplikativität);

(iv) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ (1. Ergänzungsgesetz);

(v) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ (2. Ergänzungsgesetz);

(vi) sind $(m, n) = 1$, so gilt $\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$ (Reziprozitätsgesetz).

5 Quadratische Formen

Wir betrachten quadratische Formen über $\mathbb{Z}$ in zwei Variablen, also

$$f(x,y) = ax^2 + bxy + cy^2$$

mit $a, b, c \in \mathbb{Z}$. Die Größe $d_f := b^2 - 4ac$ heißt *Diskriminante* von f und ist offenbar $\equiv 0 \bmod 4$ für gerades b sowie $\equiv 1 \bmod 4$ für ungerades b.

Hilfssatz 5.1

Für $d_f < 0$ nimmt $f(x,y)$ nur Werte ≥ 0 ($a \geq 0$) bzw. nur Werte ≤ 0 ($a \leq 0$) an; f heißt dann *positiv* bzw. *negativ definit*. Für $d_f > 0$ nimmt f positive und negative Werte an und heißt *indefinit*.

Beweis:

Es gilt

$$4af(x,y) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 - d_f y^2,$$

woran sich alle Behauptungen ablesen lassen.

□

Für die folgenden Begriffe bietet sich die Matrixschreibweise quadratischer Formen an, obwohl diese verzichtbar wäre. Setzen wir

$$F = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \quad , \quad \vec{x} = \begin{pmatrix} x \\ y \end{pmatrix} \quad , \quad \text{also } \vec{x}^t = (x,y),$$

so ist offensichtlich

$$\vec{x}^t F \vec{x} = f(x,y).$$

Eine (2×2)-Matrix T mit ganzzahligen Koeffizienten heißt *unimodular*, falls $\det T = 1$. Die entsprechende Variablensubstitution $\vec{x} \mapsto T\vec{x}$ nennen wir ebenfalls unimodular.

Definition:

Zwei quadratische Formen f und g heißen *äquivalent*, falls die zugehörigen Matrizen F und G durch eine unimodulare Transformation T auseinander hervorgehen, d.h.

$$\vec{x}^t G\vec{x} = (T\vec{x})^t F\,(T\vec{x}) = \vec{x}^t \left(T^t FT\right)\vec{x}.$$

Offensichtlich ist diese Relation eine Äquivalenzrelation auf den quadratischen Formen über $\mathbb{Z}$.

Hilfssatz 5.2

Seien f und g äquivalente quadratische Formen. Dann gilt:

(i) f und g haben dieselbe Wertemenge für $x, y \in \mathbb{Z}$.

(ii) f und g haben dieselbe Wertemenge für $x, y \in \mathbb{Z}$ mit $(x, y) = 1$.

(iii) f und g haben dieselbe Diskriminante.

Beweis:

Sei T die unimodulare Transformation zwischen f und g. Wegen $\det T = 1$ ist T invertierbar und $\det T^{-1} = 1/\det T = 1$. Genauer gilt

$$T = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \quad \Longrightarrow \quad T^{-1} = \frac{1}{\det T} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix},$$

also hat auch T^{-1} ganzzahlige Koeffizienten.

(i) Ist $n = g(x, y) = \vec{x}^t G \vec{x}$, so gilt nach Definition von T

$$f\left(T(x, y)\right) = \left(T\vec{x}\right)^t F \left(T\vec{x}\right) = n.$$

(ii) Seien $(x, y) = 1$. Es genügt zu zeigen, dass auch

$$T(x, y) = (px + qy, rx + sy) = 1.$$

Sei also $(px + qy, rx + sy) = m$, d.h. $prx + qry = mrm_1$, $prx + psy = mp \cdot m_2$. Es folgt $y = (ps - qr)y = m(pm_2 - rm_1)$, also $m \mid y$. Analog ergibt sich $m \mid x$, also $m \mid (x, y) = 1$.

(iii) Sind F bzw. G die zu f und g gehörigen Matrizen, so ist

$$\begin{aligned} d_g = -4 \det G &= -4 \cdot \det\left(T^t F T\right) = -4 \left(\det T^t\right) (\det F) (\det T) \\ &= -4 \cdot \det F = d_f. \end{aligned}$$

□

Wir wollen im Folgenden nur noch positiv definite quadratische Formen behandeln. Mit Hilfssatz 5.1 nehmen wir also ab jetzt stets $d_f < 0$ und $a > 0$ an. Demnach ist auch $c > 0$.

Satz 5.3 (Reduktionssatz)

Jede positiv definite Form f ist äquivalent zu einer Form $f_0(x, y) = a_0x^2+b_0xy+c_0y^2$ mit $-a_0 < b_0 \leq a_0 < c_0$ oder $0 \leq b_0 \leq a_0 = c_0$.

Beweis:

Wir wenden die drei folgenden unimodularen Transformationen an:

$$T_0 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad , \quad T_\pm := \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}.$$

Ist $f(x, y) = ax^2 + bxy + cy^2$, so erhalten wir unter Anwendung der drei Transformationen

$$\begin{aligned} f\left(T_0\vec{x}\right) &= \vec{x}^t T_0^t \cdot \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \cdot T_0\vec{x} = \\ &= \vec{x}^t \cdot \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix} \cdot \vec{x} = cx^2 - bxy + ay^2, \end{aligned}$$

d.h. T_0 vertauscht a und c bei unverändertem $|b|$, und

$$f\left(T_+\vec{x}\right) = ax^2 + (b + 2a)xy + (a + b + c)y^2$$

sowie

$$f\left(T_-\vec{x}\right) = ax^2 + (b - 2a)xy + (a - b + c)y^2,$$

d.h. wir können b durch $b \pm 2a$ ersetzen, also b mod $2a$ abändern, ohne dass a geändert wird. Demnach können wir durch mehrfache Anwendung von T_+ bzw. T_-

den Koeffizienten b bei festem a zu b' mit $|b'| \leq a$ abändern. Zusammen mit T_0 können wir eine zu f äquivalente Form mit Koeffizienten $|b'| \leq a' \leq c'$ erreichen. Dies geschieht nach endlich vielen Schritten, da jede Anwendung von T_0 (nur für den Fall $a > c$) den Wert von a verkleinert.
Erhalten wir auf diese Weise $-a' < b' \leq a' < c'$, so ist das Gewünschte erreicht. Es bleiben also die Fälle $-a' = b'$ und $a' = c'$. In der ersten Situation wenden wir erneut T_+ an und es entsteht $b'' = a''$ mit unverändertem c'. Für den Fall $a' = c'$ liefert T_0 bei negativem b' noch $b'' = -b' \geq 0$.

□

Eine Form, deren Koeffizienten eine der beiden Relationsbedingungen aus Satz 5.3 erfüllen, heißt *reduziert*.

Beispiel:
Wir wollen $f(x, y) = 2x^2 + 9xy + 11y^2$ reduzieren.

$$\begin{aligned} 2x^2 + 9xy + 11y^2 &\overset{T_-}{\longmapsto} 2x^2 + 5xy + 4y^2 \overset{T_-}{\longmapsto} 2x^2 + xy + y^2 \\ &\overset{T_0}{\longmapsto} x^2 - xy + 2y^2 \overset{T_+}{\longmapsto} x^2 + xy + 2y^2 =: f_0(x, y). \end{aligned}$$

Probe: $d_f = 9^2 - 4 \cdot 2 \cdot 11 = -7 = 1^2 - 4 \cdot 1 \cdot 2 = d_{f_0}$

Hilfssatz 5.4

Sei $d < 0$ gegeben. Ist $f(x, y) = ax^2 + bxy + cy^2$ positiv definit und reduziert mit $d_f = d$, so gilt

$$-\frac{d}{4} \leq ac \leq -\frac{d}{3}$$

und damit $0 < a \leq -d/3$, $|b| \leq -d/3$, $0 < c \leq -d/3$. Insbesondere gibt es nur endlich viele positiv definite, reduzierte quadratische Formen mit Diskriminante d.

Beweis:

Nach Definition von d_f ist $-d = 4ac - b^2$. Da f reduziert ist, gilt $b^2 \leq a^2 \leq ac$, also

$$3ac \leq 4ac - b^2 = -d \leq 4ac.$$

Insbesondere ist

$$0 \leq |b| \leq a \leq c \leq -\frac{d}{3a} \leq -\frac{d}{3}.$$

□

Definition:

Sei $d < 0$. Die nach Hilfssatz 5.4 endliche Anzahl von positiv definiten, reduzierten quadratischen Formen mit Diskriminante d heißt *Klassenzahl* von d und wird mit $h(d)$ bezeichnet.

Beispiel:

Wir berechnen $h(-4)$. Nach Hilfssatz 5.4 gilt $1 \leq ac \leq 4/3$, also $a = c = 1$. Wegen $0 \leq b \leq a = 1$ bleibt nur $b = 0$, da für $b = 1$ gilt $b^2 - 4ac \neq -4$. D.h. $x^2 + y^2$ ist die einzige reduzierte Form mit Diskriminante -4, also $h(-4) = 1$.

Satz 5.5

Zwei verschiedene positiv definite, reduzierte quadratische Formen sind nicht äquivalent. Also ist $h(d)$ die Anzahl der Klassen nicht äquivalenter Formen mit Diskriminante d.

Beweis:

Sei $f(x, y) = ax^2 + bxy + cy^2$ positiv definit und reduziert, also insbesondere $a > 0, c > 0$. Sind $x, y \in \mathbb{Z} \setminus \{0\}$ mit $|x| \geq |y|$, so folgt

$$\begin{aligned} f(x,y) &\geq a|x|^2 - |b||x||y| + c|y|^2 = |x|\,(a|x| - |b||y|) + c|y|^2 \\ &\geq |x|\,(a|x| - |b||x|) + c|y|^2 = |x|^2\,(a - |b|) + c|y|^2 \\ &\geq a - |b| + c. \end{aligned}$$

Dasselbe folgt für $|x| \leq |y|$. Wir betrachten nun die kleinsten Werte, die $f(x,y)$ für $(x,y) = 1$ annehmen kann. Für $x, y \neq 0$ ist dies nach obiger Abschätzung offenbar der Wert $a - |b| + c$ für $x = 1, y = \pm 1$. Für $x = 1, y = 0$ bzw. $x = 0, y = 1$ nimmt f die Werte a bzw. c an. Die kleinsten von f angenommenen Werte für teilerfremde x, y sind also $a \leq c \leq a - |b| + c$. Ist $f'(x,y) = a'x^2 + b'xy + c'y^2$ nun eine zu f äquivalente, positiv definite, reduzierte quadratische Form, so nimmt f' nach Hilfssatz 5.2(ii) für $(x,y) = 1$ dieselben Werte wie f an, allerdings unter Umständen in anderer Reihenfolge. Die kleinsten dieser Werte sind aber $a' \leq c' \leq a' - |b'| + c'$. Damit folgt zwangsläufig $a = a', c = c'$ und $|b| = |b'|$, d.h. $b = \pm b'$. Es genügt nun zu zeigen, dass im Falle $b = -b'$ folgt, dass $b = 0$. Da f reduziert ist, wissen wir $-a < b \leq a < c$ oder $0 \leq b \leq a = c$. Entsprechend gilt für f', dass

$$-a' = -a < b' = -b \leq a' = a < c' = c$$

oder

$$0 \leq b' = -b \leq a' = a = c' = c.$$

Es folgt hieraus $a < c$, denn für $a = c$ ergibt sich sofort $b \geq 0$ und $-b \geq 0$, also $b = 0$. Damit ergibt sich $b < a$, also zusammen $-a < b < a < c$. Nach obigen Vorüberlegungen gilt dann für alle $x, y \neq 0$

$$f(x,y) \geq a - |b| + c > c > a,$$

d.h. $f(x,y) = a$ nur für $x = \pm 1, y = 0$.

Sei nun $T = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ die unimodulare Transformationsmatrix zwischen f und f', also

$$f'(x,y) = f\left(T\begin{pmatrix} x \\ y \end{pmatrix}\right).$$

Es folgt

$$a = f'(1,0) = f(p,r) \quad \Longrightarrow \quad p = \pm 1, r = 0,$$

also wegen $ps - qr = 1$ sofort $s = \pm 1$. Weiterhin ist

$$c = f'(1,0) = f(q,s) = f(q,\pm 1) \quad \Longrightarrow \quad q = 0.$$

Also haben wir $T = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. Sind F und F' die zu f und f' gehörigen Matrizen so ergibt sich

$$F' = T^t F T = F,$$

d.h. $b = -b = 0$.

□

Wir sagen, dass eine Zahl n von einer binären Form $f(x,y)$ *eigentlich dargestellt* wird, falls für gewisse $(x,y) = 1$ gilt $f(x,y) = n$.

Satz 5.6

Seien $d \in \mathbb{Z}$ und $n \in \mathbb{Z}$ gegeben. Es gibt eine binäre quadratische Form mit Diskriminante d, die n eigentlich darstellt, genau dann, wenn $x^2 \equiv d \bmod 4n$ lösbar ist.

Beweis:

„$\Longrightarrow$“

Sei f quadratische Form mit $d_f = d$ und $n = f(p,r)$ für $p, r \in \mathbb{Z}$ mit $(p,r) = 1$. Dann existieren $q, s \in \mathbb{Z}$ derart, dass $ps - qr = 1$. Wir setzen $T = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ und

erhalten

$$T^t \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} T = \begin{pmatrix} ap^2 + bpr + cr^2 & * \\ * & * \end{pmatrix} = \begin{pmatrix} f(p,r) & * \\ * & * \end{pmatrix},$$

d.h. f ist äquivalent zu $f'(x,y) = f(p,r)x^2 + b'xy + c'y^2$. Nach Hilfssatz 5.2(iii) haben f und f' dieselbe Diskriminante, also $d = b'^2 - 4nc'$, d.h. $b'^2 \equiv d \bmod 4n$.

„$\Longleftarrow$“

Sei $b^2 \equiv d \bmod 4n$. Wir setzen $a := n$ und $c := (b^2 - d)/4n$. Dann hat $f(x,y) := ax^2 + bxy + cy^2$ die Diskriminante d und stellt n eigentlich dar, nämlich $f(1,0) = n$.

□

Korollar 5.7

Sei $h(d) = 1$ für ein $d < 0$, sei f eine beliebige positiv definite quadratische Form mit $d_f = d$. Ein $n \in \mathbb{N}$ wird von f genau dann eigentlich dargestellt, wenn $x^2 \equiv d \bmod 4n$ lösbar ist.

Beweis:

Wegen $h(d) = 1$ sind alle Formen der Diskriminante d äquivalent, d.h. sie stellen nach Hilfssatz 5.2(ii) dieselben Zahlen eigentlich dar. Die Behauptung folgt mit Satz 5.6.

□

Das folgende Resultat geht im Wesentlichen auf Fermat und Euler zurück.

Satz 5.8 (Zwei-Quadrate-Satz)

Sei $n \in \mathbb{N}$. Dann ist n Summe von zwei Quadraten, d.h. $n = x^2 + y^2$ mit $x, y \in \mathbb{Z}$ genau dann, wenn $e_p(n)$ gerade ist für alle $p \mid n$, $p \equiv 3 \bmod 4$. Insbesondere gilt für $p \in \mathbb{P}$

$$p = x^2 + y^2 \quad \Longleftrightarrow \quad p = 2 \text{ oder } p \equiv 1 \bmod 4.$$

Beweis:

Die Aussage für Primzahlen folgt direkt aus der Äquivalenz für allgemeines n, die wir nun zeigen wollen.

„$\Longrightarrow$“

Sei $p \mid n$, $p \equiv 3 \bmod 4$. Wegen $n = x^2 + y^2$ ist $x^2 \equiv -y^2 \bmod p$, aber $\left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right) = -1$ für $p \nmid y$ nach 1. Ergänzungsgesetz 4.4. Also bleibt nur $p \mid x$, $p \mid y$, mithin

$$\left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2 = \frac{n}{p^2} \in \mathbb{Z},$$

d.h. $p^2 \mid n$. Gilt $p \mid n/p^2$, so erhalten wir induktiv $2 \mid e_p(n)$.

„$\Longleftarrow$“

Sei $n = m^2 \cdot k$ mit k quadratfrei. Ist $k = x'^2 + y'^2$, so auch $n = (x'm)^2 + (y'm)^2$. Sei also o.B.d.A. n quadratfrei. Nach Voraussetzung ist daher $n = p_1 \cdot \ldots \cdot p_s$ mit $p_i = 2$ oder $p_i \equiv 1 \bmod 4$ paarweise verschieden. Die quadratische Form $x^2 + y^2$ hat Diskriminante -4, und nach früherem Beispiel ist $h(-4) = 1$. Also ist nach Korollar 5.7 ausreichend zu zeigen, dass die Kongruenz $x^2 \equiv -4 \bmod 4n$ lösbar ist, d.h. mit $x = 2x'$ die Kongruenz $x'^2 \equiv -1 \bmod n$ lösbar ist. Die Kongruenzen $x_i^2 \equiv -1 \bmod p_i$ sind für $p_i = 2$ trivialerweise und für $p_i \equiv 1 \bmod 4$ nach 1. Ergänzungsgesetz 4.4 lösbar. Der Chinesische Restsatz (Satz 3.5) garantiert die Lösung $x' \bmod n$.

□

Bemerkungen:

(i) Wegen der Identität

$$(x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2$$

ist offenbar das Produkt zweier Zahlen, die sich als Summe zweier Quadrate darstellen lassen, wieder Summe zweier Quadrate. Damit ließe sich Satz 5.8 für allgemeines $n \in \mathbb{N}$ aus der Kenntnis $p = x^2 + y^2 \Leftrightarrow p = 2$ oder $p \equiv 1 \bmod 4$ ohne Verwendung des Chinesischen Restsatzes herleiten.

(ii) Der Beweis zu Satz 5.8 liefert kein Verfahren zur Konstruktion der Zahlen $x, y \in \mathbb{Z}$ mit $x^2 + y^2 = n$. Ein entsprechender Beweis existiert jedoch und wird beim nachfolgenden Vier-Quadrate-Satz verwendet. Er basiert wesentlich auf einer zu (i) analogen Identität für vier Quadrate.

Die folgende Aussage wurde zuerst von Bachet behauptet und von Lagrange bewiesen.

Satz 5.9 (Vier-Quadrate-Satz)

Jede natürliche Zahl n lässt sich als Summe von vier Quadraten darstellen, d.h. es gibt $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ mit $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

Beweis: (Fermats Methode des Abstiegs)
Wir zeigen die Behauptung zunächst für $n = p \in \mathbb{P}$. Wegen $2 = 1^2 + 1^2 + 0^2 + 0^2$ können wir $p > 2$ annehmen. Nach Hilfssatz 4.1 sind die Zahlen x_1^2 für $0 \leq x_1 \leq (p-1)/2$ paarweise inkongruent mod p, und dasselbe gilt damit auch für $-1-x_2^2$, $0 \leq x_2 \leq (p-1)/2$. Da aber nur p Reste mod p existieren, ist unter jenen mindestens ein Paar x_1, x_2 mit $x_1^2 \equiv -1 - x_2^2 \bmod p$, d.h. $x_1^2 + x_2^2 + 1 = mp$ für ein $m \in \mathbb{N}$ und

$$1 \leq x_1^2 + x_2^2 + 1 \leq 2 \cdot \left(\frac{p-1}{2}\right)^2 + 1 < \frac{p^2}{2} + 1 < p^2.$$

Es folgt $1 \leq m < p$. Wir setzen

$$l_p := \min\{l \in \mathbb{N} : lp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \text{ mit } x_i \in \mathbb{Z}\}.$$

Also ist $l_p \leq m < p$. Wir können außerdem voraussetzen, dass l_p ungerade ist, denn: Wäre l_p gerade, so wären auch $0, 2$ oder 4 der entsprechenden Zahlen x_1, x_2, x_3, x_4 ungerade. Nach eventuellem Umsortieren können wir annehmen, dass $x_1 + x_2, x_1 - x_2, x_3 + x_4, x_3 - x_4$ alle gerade sind. Wegen

$$\left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2 = \frac{x_1^2}{2} + \frac{x_2^2}{2} + \frac{x_3^2}{2} + \frac{x_4^2}{2} = \frac{1}{2} \cdot l_p \cdot p$$

wäre dann l_p nicht minimal. Widerspruch!

Wir wollen nun zeigen, dass in der Tat $l_p = 1$.

Annahme: $l_p > 1$.

Sei also $l_p \cdot p = x_1^2 + x_2^2 + x_3^2 + x_4^2$, und seien x_1', x_2', x_3', x_4' die betragskleinsten Reste von x_1, x_2, x_3, x_4 mod l_p. Wir setzen

$$n = x_1'^2 + x_2'^2 + x_3'^2 + x_4'^2.$$

Offenbar ist $n \equiv 0 \bmod l_p$, und trivialerweise $n > 0$, da sonst l_p ein Teiler von x_1, x_2, x_3 und x_4 wäre, also $l_p \cdot p = l_p^2 \cdot r$ und somit $l_p \mid p$, was wegen $1 \leq l_p < p$ ausgeschlossen ist. Da l_p ungerade ist, haben wir $1 \leq n < 4 \cdot \left(\frac{l_p}{2}\right)^2 = l_p^2$. Mit $l_p \mid n$ folgt, dass $n = l_p \cdot k$ für ein $k, 1 \leq k < l_p$. Aufgrund der Identität

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(x_1'^2 + x_2'^2 + x_3'^2 + x_4'^2) = (x_1x_1' + x_2x_2' + x_3x_3' + x_4x_4')^2 +$$

$$(x_1x_2' - x_1'x_2 + x_3'x_4' - x_3x_4')^2 + (x_1x_3' - x_1'x_3 + x_2x_4' - x_2'x_4)^2 + (x_1x_4' - x_1'x_4 + x_2'x_3 - x_2x_3')^2$$

erhalten wir $(l_p \cdot p)n = l_p^2 \cdot k \cdot p$ als Summe von vier Quadraten. Wegen

$$x_1x_1' + x_2x_2' + x_3x_3' + x_4x_4' \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod l_p$$

und $x_ix_j' - x_i'x_j \equiv x_ix_j - x_ix_j \equiv 0 \bmod l_p$ für alle i, j ist jede dieser vier Quadratzahlen durch l_p^2 teilbar, d.h. kp ist Summe von vier Quadraten, was wegen $1 \leq k < l_p$ der Minimalität von l_p widerspricht. Also bleibt nur $l_p = 1$.

Ist nun $n \in \mathbb{N}$ eine zusammengesetzte Zahl, so lässt sich jeder Primteiler $p \mid n$ als Summe von vier Quadraten darstellen. Mit Hilfe der obigen Identität lässt sich daraus die gewünschte Darstellung von n berechnen.

□

Beispiel:

Wir wollen 34 als Summe von vier Quadraten darstellen. Es ist $34 = 2 \cdot 17$, wobei $2 = 1^2 + 1^2 + 0^2 + 0^2$. Betreffs 17 haben wir z.B.

$$3 \cdot 17 = 51 = 7^2 + 1^2 + 1^2 + 0^2$$

Reduktion mod 3 liefert

$$1^2 + 1^2 + 1^2 + 0^2 = 3 = n$$

Es folgt

$$\begin{aligned}(3 \cdot 17) \cdot n &= (7+1+1+0)^2 + (7-1+0-0)^2 + (7-1+0-0)^2 + (0-0+1-1)^2 \\ &= 9^2 + 6^2 + 6^2 + 0^2,\end{aligned}$$

also

$$17 = \left(\frac{9}{3}\right)^2 + \left(\frac{6}{3}\right)^2 + \left(\frac{6}{3}\right)^2 + \left(\frac{0}{3}\right)^2 = 3^2 + 2^2 + 2^2 + 0^2.$$

Zusammen

$$34 = (1^2 + 1^2 + 0^2 + 0^2)(3^2 + 2^2 + 2^2 + 0^2) = 5^2 + 1^2 + 2^2 + 2^2.$$

Wir haben aber auch

$$34 = 5^2 + 3^2 + 0^2 + 0^2 = 4^2 + 4^2 + 1^2 + 1^2 = 4^2 + 3^2 + 3^2.$$

Bemerkungen:

(i) Wie das Beispiel schon zeigt, ist die Darstellung einer Zahl als Summe von vier (wie auch von zwei) Quadraten im Allgemeinen nicht eindeutig.

(ii) Der Vier-Quadrate-Satz ist bestmöglich, d.h. drei Quadrate reichen im Allgemeinen nicht aus; es gilt: Alle Zahlen der Form $n \equiv 7 \bmod 8$ lassen sich nicht als Summe von drei Quadraten darstellen, denn:

$$x^2 \equiv 0, 1, 4 \bmod 8 \quad \Longrightarrow \quad x^2 + y^2 + z^2 \not\equiv 7 \bmod 8.$$

6 Primzahlverteilung

Der zentrale Gegenstand der Primzahltheorie ist die Primzahlzählfunktion

$$\pi(x) := \sum_{\substack{p \le x \\ p \in \mathbb{P}}} 1.$$

Um 1800 vermuteten Legendre und Gauß, dass $\pi(x) \sim x/\log x$, d.h.

$$\frac{\pi(x)}{x/\log x} \to 1$$

für $x \to \infty$. Dies wurde 1896 von Hadamard und de la Vallée-Poussin mit Methoden der komplexen Analysis bewiesen und heißt *Primzahlsatz*. Wir werden mit elementaren Argumenten gute Abschätzungen für $\pi(x)$ herleiten.

Es hat sich herausgestellt, dass es günstiger ist, anstelle von $\pi(x)$ die Funktion

$$\vartheta(x) := \sum_{p \le x} \log p = \log \left(\prod_{p \le x} p \right)$$

zu betrachten (hier wie im Folgenden stehe p stets für Primzahlen, d.h.

$p \le x :\Longleftrightarrow p \le x$ und $p \in \mathbb{P}$.) Den engen Zusammenhang zwischen $\pi(x)$ und $\vartheta(x)$ zeigt

Hilfssatz 6.1

Sei $0 < \varepsilon < 1$. Dann gilt für alle $x \ge 2$

$$\frac{\vartheta}{\log x} \le \pi(x) \le \frac{1}{1-\varepsilon} \cdot \frac{\vartheta(x)}{\log x} + x^{1-\varepsilon}.$$

Beweis:

Klar ist

$$\vartheta(x) = \sum_{p \le x} \log p \le \log x \cdot \sum_{p \le x} 1 = \pi(x) \cdot \log x,$$

womit die linke Ungleichung schon gezeigt ist. Außerdem gilt

$$\begin{aligned}\vartheta(x) \geq \sum_{x^{1-\varepsilon}<p\leq x} \log p \geq \log(x^{1-\varepsilon}) \cdot \sum_{x^{1-\varepsilon}<p\leq x} 1 &= (1-\varepsilon)\log x(\pi(x)-\pi(x^{1-\varepsilon})) \\ &\geq (1-\varepsilon)\log x\left(\pi(x)-x^{1-\varepsilon}\right),\end{aligned}$$

also die rechte Ungleichung.

□

Hilfssatz 6.2 (Schwache Stirling-Formel)

Für $n \in \mathbb{N}_{>1}$ gilt

$$n\log n - n + 1 < \log n! < n\log n.$$

Beweis:

Wegen der strengen Monotonie des Logarithmus gilt für jedes $j \in \mathbb{N}$

$$\int_j^{j+1} \log x\, dx < \log(j+1),$$

also

$$\int_1^n \log x\, dx = \sum_{j=1}^{n-1} \left(\int_j^{j+1} \log x\, dx \right) < \sum_{j=1}^{n-1} \log(j+1) = \log n!.$$

Partielle Integration liefert $\int_1^n \log x\, dx = \left[x\log x - x\right]_1^n = n\log n - n + 1$, also die Unterschranke unserer Behauptung. Die obere Ungleichung ergibt sich sofort aus

$$\log n! = \sum_{j=1}^{n} \log j < \log n \cdot \sum_{n=1}^{n} 1 = n\log n.$$

□

Hilfssatz 6.3

Für $n \in \mathbb{N}_{>1}$ gilt

$$P_n := \prod_{p \leq n} p < 4^n.$$

Beweis: (nach Erdös)

Für $n = 2$ ist die Behauptung offenbar richtig. Wir nehmen nun an, sie gelte für alle $k \leq n$. Ist $n+1$ gerade, so ist $n+1 \notin \mathbb{P}$, also

$$\prod_{p \leq n+1} p = \prod_{p \leq n} p < 4^n < 4^{n+1}.$$

Sei also $n+1$ ungerade, etwa $n+1 = 2m+1$. Wir erhalten damit

$$P_{n+1} = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p \leq 2m+1} p = P_{m+1} \cdot \prod_{m+1 < p \leq 2m+1} p.$$

Offensichtlich teilt jedes p, $m+1 < p \leq 2m+1$, den Zähler von

$$\binom{2m+1}{m} = \frac{(2m+1) \cdot 2m \cdot \ldots \cdot (m+2)}{m!},$$

aber nicht den Nenner. Also haben wir

$$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m},$$

und damit nach Induktionsvoraussetzung

$$P_{n+1} \leq P_{m+1} \cdot \binom{2m+1}{m} < 4^{m+1} \cdot \binom{2m+1}{m}.$$

Wegen $\binom{3}{1} = 3 < 4$ und für $m > 1$

$$\binom{2m+1}{m} : \binom{2m-1}{m-1} = \frac{2m(2m+1)}{m(m+1)} < 4$$

erhalten wir induktiv $\binom{2m+1}{m} < 4^m$, also insgesamt

$$P_{n+1} < 4^{m+1} \cdot 4^m = 4^{2m+1} = 4^{n+1}.$$

□

Das folgende Ergebnis stellte einen wichtigen Zwischenschritt auf dem Wege zum Primzahlsatz dar und wurde um 1850 bewiesen.

Satz 6.4 (Chebyshev)

Es gibt zwei positive Konstanten $C_1 < C_2$ derart, dass für alle $x \geq 2$ gilt

$$C_1 \cdot \frac{x}{\log x} \leq \pi(x) \leq C_2 \cdot \frac{x}{\log x}.$$

Beweis: (nach Erdös und Shapiro)
Wir werden zeigen, dass für geeignete positive Konstanten $B_1 < B_2$

$$B_1 x \leq \vartheta(x) \leq B_2(x)$$

gilt. Dies ist hinreichend, denn mit Hilfssatz 6.1 folgt daraus

$$B_1 \frac{x}{\log x} \leq \frac{\vartheta(x)}{\log x} \leq \pi(x) \leq \frac{1}{1-\varepsilon} \cdot \frac{B_2 x}{\log x} + x^{1-\varepsilon} \leq 2B_2 \cdot \frac{x}{\log x} + \frac{x}{\log x}$$

für $\varepsilon = 1/2$, da $\log x \leq \sqrt{x}$ für $x \geq 2$ (z.B. wegen $f(x) := \sqrt{x} - \log x$ erfüllt $f(2) > 0$ und $f'(x) > 0$ für $x \geq 2$). Mit $C_1 := B_1$ und $C_2 := 2B_2 + 1$ ergibt sich der Satz. Zum Beweis der Ungleichung für $\vartheta(x)$ dürfen wir o.B.d.A. annehmen, dass $x = n \in \mathbb{N}$ ist, da für $n \leq x < n+1$ mit $x \geq 2$ gilt

$$\frac{1}{2} B_1 x \leq B_1 x - 1 < B_1 n \leq \vartheta(n) = \vartheta(x) \leq B_2 n \leq B_2 x.$$

Wegen $\vartheta(n) = \log P_n$ liefert Hilfssatz 6.3 sofort die obere Abschätzung $\vartheta(n) < (\log 4) \cdot n$. Es bleibt nur noch die untere Ungleichung zu zeigen. Mit Satz 2.2 gilt

$$\begin{aligned} \log n! &= \log \left(\prod_{p \leq n} p^{e_p(n!)} \right) = \sum_{p \leq n} e_p(n!) \cdot \log p = \\ &= \sum_{p \leq n} \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right] \log p = \sum_{p \leq n} \left[\frac{n}{p} \right] \log p + O\left(n \sum_{p \leq n} \sum_{j=2}^{\infty} \frac{\log p}{p^j} \right). \end{aligned}$$

Wegen

$$\sum_{j=2}^{\infty} \frac{1}{p^j} = \frac{1}{1 - 1/p} - 1 - \frac{1}{p} = \frac{1}{p(p-1)} < \frac{2}{p^2}$$

ist der Fehlerterm höchstens

$$2n \cdot \sum_{p \le n} \frac{\log p}{p^2} < 2n \sum_{k=1}^{\infty} \frac{\log k}{k^2} = O(n).$$

Nach Hilfssatz 6.2 ist $\log n! = n \log n + O(n)$, also insgesamt

$$\sum_{p \le n} \left[\frac{n}{p} \right] \log p = n \log n + O(n).$$

Mit Hilfe der bereits bewiesenen oberen Abschätzung für $\vartheta(n)$ erhalten wir

$$\begin{aligned} n \cdot \sum_{p \le n} \frac{\log p}{p} &= \sum_{p \le n} \left(\left[\frac{n}{p} \right] + \left\{ \frac{n}{p} \right\} \right) \log p \\ &= n \log n + O(n) + O\left(\vartheta(n)\right) = n \log n + O(n), \end{aligned}$$

also

$$\sum_{p \le n} \frac{\log p}{p} = \log n + O(1).$$

Ist eine reelle Zahl a, $0 < a < 1$, gegeben, so folgt für $n \ge 2$

$$\begin{aligned} \sum_{an < p \le n} \frac{\log p}{p} &= \log n - \log an + O(1) = \log \frac{1}{a} + O(1) \\ &\ge \log \frac{1}{a} - C \end{aligned}$$

für eine absolute Konstante $C > 0$. Trivialerweise haben wir

$$\sum_{an < p \le n} \frac{\log p}{p} \le \sum_{an < p \le n} \frac{\log p}{an} \le \frac{1}{an} \sum_{p \le n} \log p = \frac{\vartheta(n)}{an}.$$

Mit $B_2 := a := e^{-C-1}$ erhalten wir schließlich

$$\vartheta(n) \ge an(\log(e^{C+1}) - C) = B_2 n.$$

□

Im Laufe des vorstehenden Beweises haben wir unter anderem gezeigt

Satz 6.5 (von Mertens)

Für $x \geq 2$ gilt

$$\sum_{p \leq n} \frac{\log p}{p} = \log x + O(1).$$

Das folgende diskrete Pendant zur partiellen Integration ist ein oft verwendetes Hilfsmittel zur Umformung von zahlentheoretischen Summen.

Hilfssatz 6.6 (Abelsche Teilsummation)

Sei $\lambda_1 < \lambda_2 < \lambda_3 < \ldots$ eine reelle Folge mit $\lim\limits_{n \to \infty} \lambda_n = \infty$. Seien $a_n \in \mathbb{C}\,(n \in \mathbb{N})$ und $x \in \mathbb{R}$, $x \geq \lambda_1$. Wir setzen $A(x) := \sum\limits_{\lambda_n \leq x} a_n$. Sei $f(t)$, $t \geq \lambda_1$, eine komplexwertige, stetig differenzierbare Funktion. Dann gilt

$$\sum_{\lambda_n \leq x} a_n f(\lambda_n) = A(x)f(x) - \int_{\lambda_1}^{x} A(t)f'(t)dt.$$

Beweis:

Wegen $\lim\limits_{n \to \infty} \lambda_n = \infty$ sind die auftretenden Summen alle endlich. Es gilt

$$\begin{aligned} A(x)f(x) - \sum_{\lambda_n \leq x} a_n f(\lambda_n) &= \sum_{\lambda_n \leq x} a_n (f(x) - f(\lambda_n)) \\ &= \sum_{\lambda_n \leq x} \int_{\lambda_n}^{x} a_n f'(t)dt, \end{aligned}$$

also wegen $\lambda_1 \leq \lambda_n \leq t \leq x$ durch Vertauschung von $\sum$ und $\int$

$$A(x)f(x) - \sum_{\lambda_n \leq x} a_n f(\lambda_n) = \int_{\lambda_1}^{x} \sum_{\lambda_n \leq t} a_n \cdot f'(t)dt = \int_{\lambda_1}^{x} A(t)f'(t)dt.$$

□

Satz 6.7

Es existiert eine Konstante $C_3 \in \mathbb{R}$ derart, dass für $x \geq 2$ gilt

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + C_3 + O\left(\frac{1}{\log x}\right).$$

Beweis:

Bezeichnet $p^{(n)}$, $n \in \mathbb{N}$, die n-te Primzahl, also $p^{(1)} = 2, p^{(2)} = 3, \ldots$, so ist

$$\sum_{p \leq x} \frac{1}{p} = \sum_{p^{(n)} \leq x} \frac{\log p^{(n)}}{p^{(n)}} \cdot \frac{1}{\log p^{(n)}}.$$

Wir setzen $\lambda_n := p^{(n)}$, $a_n := \log p^{(n)}/p^{(n)}$, $f(t) := 1/\log t$. Nach Satz 6.5 gilt damit

$$A(x) = \sum_{p^{(n)} \leq x} \frac{\log p^{(n)}}{p^{(n)}} = \log x + r(x),$$

wobei $r(x) = O(1)$ stückweise stetig ist. Hilfssatz 6.6 liefert

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= \frac{\log x + r(x)}{\log x} + \int_2^x (\log t + r(t)) \cdot \frac{dt}{t(\log t)^2} \\ &= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{dt}{t \log t} + \int_2^x \frac{r(t)}{t(\log t)^2} dt. \end{aligned}$$

Die Substitution $v := \log t$, also $dv = dt/t$, im 2. Integral gibt

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= 1 + O\left(\frac{1}{\log x}\right) + \left[\log\log t\right]_2^x + \int_{\log 2}^{\log x} \frac{r(e^v)}{v^2} dv \\ &= \log\log x + 1 - \log\log 2 + \int_{\log 2}^{\infty} \frac{r(e^v)}{v^2} dv - \int_{\log x}^{\infty} \frac{r(e^v)}{v^2} dv + O\left(\frac{1}{\log x}\right). \end{aligned}$$

Wegen

$$\left| \int_{\log 2}^{\infty} \frac{r(e^v)}{v^2} dv \right| \leq \int_{\log 2}^{\infty} \frac{C}{v^2} dv = C \cdot \left[\frac{-1}{v}\right]_{\log 2}^{\infty} = \frac{C}{\log 2} \qquad \text{(für ein geeignetes C)}$$

existiert $B_3 := \displaystyle\int_{\log 2}^{\infty} r(e^v)/v^2 dv$. Außerdem ist analog $\left| \displaystyle\int_{\log x}^{\infty} r(e^v)/v^2 dv \right| \leq C/\log x$.
Also folgt die Behauptung mit $C_3 := 1 - \log\log 2 + B_3$.

□

Korollar 6.8

Es existiert eine Konstante $C_4 > 0$ derart, dass für $x \geq 2$ gilt

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = C_4 \log x + O(1).$$

Beweis:

Es ist mit $T(x) := \prod_{p \leq x} (1 - 1/p)^{-1}$ und der Potenzreihe von log

$$\log T(x) = \sum_{p \leq x} -\log(1 - \frac{1}{p}) = \sum_{p \leq x} \sum_{j=1}^{\infty} \frac{1}{j \cdot p^j} = \sum_{p \leq x} \frac{1}{p} + \sum_{p \leq x} \sum_{j=2}^{\infty} \frac{1}{j \cdot p^j}.$$

Trivialerweise gilt

$$0 < B_4 := \sum_{p \in \mathbb{P}} \sum_{j=2}^{\infty} \frac{1}{j \cdot p^j} < \sum_{n=2}^{\infty} \frac{1}{2n(n-1)} = \frac{1}{2} \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n}\right) = \frac{1}{2},$$

also ist B_4 wohldefiniert. Außerdem haben wir

$$\begin{aligned} 0 < \sum_{p > x} \sum_{j=2}^{\infty} \frac{1}{j \cdot p^j} &< \sum_{n > x} \frac{1}{2n(n-1)} \\ &= \frac{1}{2} \sum_{n \geq [x]+1} \left(\frac{1}{n-1} - \frac{1}{n}\right) = \frac{1}{2[x]} = O\left(\frac{1}{x}\right). \end{aligned}$$

Wegen $1/x = O\left(1/\log x\right)$ folgt mit Satz 6.7

$$\log T(x) = \log \log x + C_3 + B_4 + O\left(\frac{1}{\log x}\right),$$

also wegen $e^y = 1 + y + y^2/2 + \cdots$ mit $C_4 := e^{C_3 + B_4}$

$$T(x) = C_4 \log x \cdot e^{O(1/\log x)} = C_4 \log x \left(1 + O\left(\frac{1}{\log x}\right)\right) = C_4 \log x + O(1).$$

□

In einer weiteren Anwendung von Satz 6.7 behandeln wir die zahlentheoretische Funktion

$$\omega(n) := \sum_{\substack{p \mid n \\ p \in \mathbb{P}}} 1,$$

die also die verschiedenen Primteiler einer gegebenen Zahl $n \in \mathbb{N}$ zählt. Wie sich sofort nachweisen lässt, ist $\omega(n)$ *additiv*, d.h. für $(m, n) = 1$ gilt stets $\omega(m \cdot n) = \omega(m) + \omega(n)$.

Korollar 6.9

Mit der Konstanten C_3 aus Satz 6.7 gilt für $x \geq 2$

$$\sum_{n \leq x} \omega(n) = x \log\log x + C_3 x + O\left(\frac{x}{\log x}\right).$$

Beweis:

Wir haben

$$\begin{aligned}\sum_{n\leq x} \omega(n) &= \sum_{n\leq x} \sum_{p|n} 1 = \sum_{p\leq x} \sum_{\substack{n\leq x \\ p|n}} 1 = \sum_{p\leq x} \left[\frac{x}{p}\right] \\ &= \sum_{p\leq x} \left(\frac{x}{p} + O(1)\right) = x \cdot \sum_{p\leq x} \frac{1}{p} + O\big(\pi(x)\big) = x\log\log x + C_3 x + O\left(\frac{x}{\log x}\right)\end{aligned}$$

nach Satz 6.7 und Satz 6.4.

□

7 Kettenbrüche und Diophantische Approximation

Die Diophantische Approximation beschäftigt sich mit der Lösbarkeit von Diophantischen Ungleichungen, d.h. Ungleichungen in ganzzahligen Variablen bzw. Unbekannten. Ein grundlegendes Resultat dieses Gebiets stammt von Dirichlet (1842).

Satz 7.1

Seien α und $Q > 1$ reelle Zahlen. Dann gibt es $p, q \in \mathbb{Z}$ mit $(p, q) = 1$ und $0 < q < Q$ derart, dass

$$|\alpha q - p| \leq \frac{1}{Q} \quad \text{bzw.} \quad \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}.$$

Beweis:

Ist die gewünschte Ungleichung überhaupt lösbar, so können wir o.B.d.A. $(p, q) = 1$ annehmen, denn sonst würde sogar eine schärfere Abschätzung gelten.
Wir setzen zunächst voraus, dass $Q \in \mathbb{N}$. Wir betrachten die $Q + 1$ Zahlen
$0, \{\alpha\}, \{2\alpha\}, \ldots, \{(Q-1)\alpha\}, 1$, die nach Definition des Bruchteils $\{.\}$ alle im Intervall $[0, 1]$ liegen.

Wir teilen nun $[0, 1]$ in Q disjunkte Teilintervalle $\left[\frac{i}{Q}, \frac{i+1}{Q}\right)$ für $0 \leq i \leq Q - 2$ und $\left[\frac{Q-1}{Q}, q\right]$ ein. Nach dem Schubfachschluss liegen in mindestens einem dieser Intervalle zwei der obigen $Q+1$ Zahlen. Die Differenz dieser beiden Zahlen (in der richtigen Reihenfolge) hat offenbar die Form $q\alpha - p$ für ein $0 < q < Q$ und ein geeignetes p, da $\{j\alpha\} = j\alpha - [j\alpha]$, und erfüllt außerdem $|q\alpha - p| \leq 1/Q$ wegen der Lage der beiden Subtrahenden im selben Teilintervall. Auf diese Weise folgt die Behauptung.

□

Für $Q \in \mathbb{R}$ ergibt sich das Gewünschte aus Obigem mit $[Q]+1$ anstelle von Q, denn $q < [Q]+1 \Longrightarrow q < Q$ und $|\alpha q - p| \leq 1/([Q]+1) < 1/Q$.
Als Korollar ergibt sich

Satz 7.2 (Dirichlet'scher Approximationssatz)

Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Dann gibt es unendlich viele $p/q \in \mathbb{Q}, q > 0, (p,q) = 1$ mit

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Beweis:

Sei $Q > 1$ beliebig. Nach Satz 7.1 existieren $(p,q) = 1$, $0 < q < Q$ mit

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ} < \frac{1}{q^2}.$$

Wegen $\alpha \notin \mathbb{Q}$ ist $|\alpha q - p| \neq 0$. Wähle $Q_1 > |\alpha q - p|^{-1}$. Nach Satz 7.1 existieren $(p_1, q_1) = 1$, $0 < q_1 < Q_1$ mit

$$\left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{q_1 Q_1} < \left|\alpha - \frac{p}{q}\right|,$$

also $p_1/q_1 \neq p/q$. Induktiv erhalten wir das Gewünschte.

□

Bemerkungen:

(i) Der Dirichlet'sche Approximationssatz garantiert Näherungen an eine gegebene Zahl α, die viel genauer sind als wir es z.B. von Dezimalzahlnäherungen erwarten können; z.B.

$$\left|\pi - \frac{3141}{1000}\right| = \left|3,1415\ldots - \frac{3141}{1000}\right| \approx \frac{5}{10000} = \frac{1}{2000}.$$

Nach Dirichlet existiert ein Näherungsbruch von π mit Nenner unterhalb 1000 derart, dass der Fehler höchstens 10^{-6} ist.

(ii) Für $\alpha \in \mathbb{Q}$ gilt Satz 7.2 nicht; wir haben sogar:

$\alpha \in \mathbb{Q} \Longrightarrow$ es gibt nur endlich viele Brüche $p/q \neq \alpha$ mit

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2};$$

denn: Sei $\alpha = a/b$. Für $p/q \neq \alpha$ folgt

$$0 < \left|\alpha - \frac{p}{q}\right| = \left|\frac{aq - bp}{bq}\right|, \text{also } \left|\alpha - \frac{p}{q}\right| \geq \frac{1}{bq} \geq \frac{1}{q^2}$$

für $q \geq b$. Für $q < b$ existieren aber nur endlich viele geeignete Zähler p.

Der Dirichtlet'sche Approximationssatz garantiert zwar für irrationale Zahlen sehr gute rationale Näherungen, sagt aber nichts darüber aus, wie wir diese finden können. Das liegt letztlich daran, dass der im Beweis von Satz 7.1 verwendete Schubfachschluss ineffektiv, d.h. nicht konstruktiv ist. Ein Mittel, um diesem Missstand abzuhelfen, sind sogenannte Kettenbrüche.

Definition:

Unter einem *endlichen Kettenbruch* verstehen wir einen Ausdruck der Form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \\ a_{n-1} + \cfrac{1}{a_n}}}}$$

mit $a_0 \in \mathbb{Z}$ und $a_j \in \mathbb{N} (1 \leq j \leq n)$. Ist $a_n \neq 1$, so heißt der Kettenbruch *normiert*. Schreibweise für Kettenbrüche: $\langle a_0; a_1, \ldots, a_n \rangle$. Dabei heißt a_j *j-ter Teilnenner*.

Satz 7.3

Jeder endliche Kettenbruch stellt eine rationale Zahl dar. Umgekehrt wird jede rationale Zahl von genau einem normierten endlichen Kettenbruch dargestellt: Ist $a/b \in \mathbb{Q}$, $b > 0$, so liefert der Euklidische Algorithmus (vgl. §1) in der Form

$$\begin{aligned} a &= b \cdot a_0 + r_1 \quad , \quad 0 < r_1 < b \\ b &= r_1 \cdot a_1 + r_2 \quad , \quad 0 < r_2 < r_1 \\ &\vdots \qquad\qquad\qquad\quad \vdots \\ r_{n-1} &= r_n a_n \end{aligned}$$

die Darstellung $a/b = \langle a_0; a_1, \ldots, a_n \rangle$.

Beweis:

Die erste Aussage des Satzes ist klar. Sei also jetzt $\alpha := a/b$ gegeben. Dann gilt nach dem Euklidischen Algorithmus

$$\begin{aligned} \frac{a}{b} &= a_0 + \frac{r_1}{b} = a_0 + \frac{1}{b/r_1} = a_0 + \frac{1}{a_1 + r_2/r_1} \\ &= a_0 + \frac{1}{a_1 + \dfrac{1}{r_1/r_2}} = \cdots = \langle a_0; a_1, \ldots, a_n \rangle \, . \end{aligned}$$

Die Eindeutigkeit der normierten Kettenbruchdarstellung folgt sofort:

Sei $\alpha = \langle a_0; a_1, \ldots, a_n \rangle = \langle b_0; b_1, \ldots, b_m \rangle$. Ist $a_0 \neq b_0$, so folgt wegen

$[\langle a_0; a_1, \ldots, a_n \rangle] = a_0$, $[\langle b_0; b_1, \ldots, b_m \rangle] = b_0$ ein Widerspruch. Für $a_0 = b_0$ ist wegen

$$a_0 + \frac{1}{\langle a_1; a_2, \ldots, a_n \rangle} = \langle a_0; a_1, \ldots, a_n \rangle = \langle b_0; b_1, \ldots, b_m \rangle = b_0 + \frac{1}{\langle b_1; b_2, \ldots, b_m \rangle}$$

dann $\langle a_1; a_2, \ldots, a_n \rangle = \langle b_1; b_2, \ldots, b_m \rangle$. Induktiv erhalten wir schließlich für $n \leq m$, etwa,

$$a_n = \langle a_n \rangle = \langle b_n; b_{n+1}, \ldots, b_m \rangle \, ,$$

also $a_n = b_n, n = m$ oder $a_n = b_n + 1$, d.h. $n = m - 1, b_m = 1$; aber letzteres ist bei normierten Kettenbrüchen nicht möglich.

□

Wir wollen nun auch *unendliche Kettenbrüche* zur Darstellung irrationaler Zahlen konstruieren. Dabei müssen wir natürlich die notwendige Kongruenz sichern. Als Vorbereitung zeigen wir zunächst

Hilfssatz 7.4

Sei $a_0 \in \mathbb{Z}, (a_n)_{n\in\mathbb{N}}$ eine Folge natürlicher Zahlen. Setzen wir für $n \geq 0$

$$\langle a_0; a_1, \ldots, a_n\rangle = \frac{p_n}{q_n},\ (p_n, q_n) = 1,$$

so gelten mit $p_{-1} := 1,\ p_0 := a_0,\ q_{-1} := 0,\ q_0 := 1$ die Rekursionsformeln

$$p_n = a_n p_{n-1} + p_{n-2} \quad , \quad q_n = a_n q_{n-1} + q_{n-2} \quad (n \geq 1).$$

Beweis: (Induktion über n)
$n = 1$: klar;
$n - 1 \to n$: Wir setzen $\langle a_1; a_2, \ldots, a_{j+1}\rangle =: p'_j/q'_j$ mit $(p'_j, q'_j) = 1$ für $j \geq 0$. Nach Induktionsvoraussetzung gilt

$$p'_{n-1} = a_n p'_{n-2} + p'_{n-3} \quad , \quad q'_{n-1} = a_n q'_{n-2} + q'_{n-3}.$$

Offenbar gilt aber $p_j/q_j = a_0 + q'_{j-1}/p'_{j-1}$, also wegen $(p_j, q_j) = 1$ nach Voraussetzung

$$p_j = a_0 p'_{j-1} + q'_{j-1} \quad , \quad q_j = p'_{j-1}.$$

Für $j = n$ ergibt sich

$$\begin{aligned} p_n &= a_0(a_n p'_{n-2} + p'_{n-3}) + (a_n q'_{n-2} + q'_{n-3}) = a_n(a_0 p'_{n-2} + q'_{n-2}) + (a_0 p'_{n-3} + q'_{n-3}) \\ q_n &= a_n p'_{n-2} + p'_{n-3}, \end{aligned}$$

und für $j = n - 1$ bzw. $j = n - 2$ kommt

$$\begin{aligned} p_{n-1} &= a_0 p'_{n-2} + q'_{n-2} \quad , \quad p_{n-2} = a_0 p'_{n-3} + q'_{n-3}, \\ q_{n-1} &= p'_{n-2} \quad , \quad q_{n-2} = p'_{n-3}. \end{aligned}$$

Durch Einsetzen folgt die Behauptung.

□

Korollar 7.5

Für $n \geq 0$ gilt

(i) $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$;

(ii) $(p_n, q_n) = 1$.

Beweis:

(i) Für $n = 0$ ist in der Tat $a_0 \cdot 0 - 1 \cdot 1 = (-1)^1$. Induktiv folgt mit Hilfssatz 7.4

$$\begin{aligned} p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\ &= -(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = -(-1)^n = (-1)^{n+1}. \end{aligned}$$

(ii) Dies ist klar nach Hilfssatz 7.4. Die Rekursionsformeln liefern automatisch die gekürzten Brüche p_n/q_n.

□

Definition:

Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Wir setzen $\vartheta_0 := \alpha$ und definieren rekursiv zwei Folgen $(a_n)_{n \in \mathbb{N}_0}$ über $\mathbb{N}$ (bis auf $a_0 \in \mathbb{Z}$) bzw. $(\vartheta_n)_{n \in \mathbb{N}_0}$ über $\mathbb{R}_{>1}$ (bis auf $\vartheta_0 \in \mathbb{R}$) durch

$$a_n = [\vartheta_n] \quad \text{und} \quad \vartheta_n = a_n + \frac{1}{\vartheta_{n+1}} \quad (n \geq 0).$$

Dann heißt $\langle a_0; a_1, a_2, \ldots \rangle$ (*unendlicher*) *Kettenbruch* von α.

Bemerkung:

Für $\alpha \in \mathbb{Q}$ bricht der obige Algorithmus irgendwann dadurch ab, dass für ein $n \in \mathbb{N}$ gilt $a_n = \vartheta_n$. Dann erhalten wir genau den endlichen Kettenbruch $\langle a_0; a_1, \ldots, a_n \rangle$ von α (vgl. Satz 7.3).

Satz 7.6

Sei $\langle a_0; a_1, a_2, \ldots\rangle$ der (endliche oder unendliche) Kettenbruch einer Zahl $\alpha \in \mathbb{R}$. Für $p_n/q_n := \langle a_0; a_1, \ldots, a_n\rangle$ $(n \geq 0)$ gilt dann:

(i) $\quad \dfrac{p_n}{q_n} \leq \alpha \leq \dfrac{p_{n+1}}{q_{n+1}}$ oder $\dfrac{p_{n+1}}{q_{n+1}} \leq \alpha \leq \dfrac{p_n}{q_n}$ $(n \geq 0)$;

(ii) $\quad \left|\alpha - \dfrac{p_n}{q_n}\right| \leq \dfrac{1}{q_n q_{n+1}}$ $(n \geq 0)$;

(iii) $\quad \lim\limits_{n\to\infty} \dfrac{p_n}{q_n} = \alpha$, d.h. $\alpha = \langle a_0; a_1, a_2, \ldots\rangle$.

Beweis:

(i) Wir haben nach Definition der ϑ_n

$\alpha = \vartheta_0 = \langle a_0; \vartheta_1\rangle = \langle a_0; a_1, \vartheta_2\rangle = \cdots = \langle a_0; a_1, \ldots, a_n, \vartheta_{n+1}\rangle$,

wobei $0 < 1/\vartheta_{n+1} \leq 1/a_{n+1}$. Also gilt

$p_n/q_n = \langle a_0; a_1, \ldots, a_n\rangle \leq \langle a_0; a_1, \ldots, a_n + 1/\vartheta_{n+1}\rangle = \alpha \leq \langle a_0; a_1, \ldots, a_n + 1/a_{n+1}\rangle$

$= p_{n+1}/q_{n+1}$ oder

$p_{n+1}/q_{n+1} = \langle a_0; a_1, \ldots, a_n + 1/a_{n+1}\rangle \leq \langle a_0; a_1, \ldots, a_n + 1/\vartheta_{n+1}\rangle$

$= \alpha \leq \langle a_0; a_1, \ldots, a_n\rangle = p_n/q_n$.

(ii) Mit Korollar 7.5(i) gilt wegen $q_n > 0$ für $n \geq 0$

$$\left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{|p_n q_{n+1} - p_{n+1} q_n|}{q_n q_{n+1}} = \frac{1}{q_n q_{n+1}}.$$

Nach (i) folgt die Behauptung.

(iii) Wir zeigen mit Induktion zunächst, dass $q_n \geq 2^{(n-1)/2}$ für $n \geq 0$: Nach Hilfssatz 7.4 gilt $q_0 = 1 \geq 2^{-1/2}$, $q_1 \geq 1 = 2^0$, $q_2 \geq q_1 + q_0 \geq 2 \geq 2^{1/2}$ und für $n \geq 3$ nach Induktionsvoraussetzung $q_n \geq q_{n-1} + q_{n-2} \geq 2^{(n-2)/2} + 2^{(n-3)/2} \geq 2 \cdot 2^{(n-3)/2} = 2^{(n-1)/2}$. Also insbesondere ist $\lim\limits_{n\to\infty} q_n = \infty$. Damit ergibt (ii) das Gewünschte.

□

Satz 7.6(ii) rechtfertigt die nachfolgende

Definition:

Sei $\alpha = \langle a_0; a_1, a_2, \ldots \rangle$. Dann heißt $p_n/q_n := \langle a_0; a_1, a_2, \ldots, a_n \rangle$ *n-ter Näherungsbruch* von α.

Korollar 7.7

Sei $\alpha \in \mathbb{R}$. Jeder Näherungsbruch p/q von α erfüllt

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Beweis:

Dies ergibt sich sofort aus Satz 7.6(ii) wegen

$$q_{n+1} = a_{n+1} q_n + q_{n-1} \geq q_n + q_{n-1} > q_n \quad (n \geq 1)$$

nach Hilfssatz 7.4.

□

Bemerkungen:

(i) Mit der Methode aus dem Beweis von Satz 7.3 lässt sich sofort zeigen, dass die Darstellung einer irrationalen Zahl durch einen Kettenbruch eindeutig ist. Wir haben also mit Satz 7.3 insgesamt eine Bijektion zwischen $\mathbb{R}$ und der Menge aller normierten Kettenbrüche.

(ii) Korollar 7.7 besagt, wie die im Dirichlet'schen Approximationssatz garantierten Näherungen konstruiert werden können.

Mit Hilfe der Theorie der Kettenbrüche lässt sich der Dirichlet'sche Approximationssatz verschärfen.

Satz 7.8 (Hurwitz'scher Approximationssatz)

Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Dann gibt es unendlich viele $p/q \in \mathbb{Q},\ q > 0,\ (p,q) = 1$ mit

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Beweis:

Seien p_n/q_n, p_{n+1}/q_{n+1}, p_{n+2}/q_{n+2} drei aufeinanderfolgende Näherungsbrüche von α. Dann genügt es zu zeigen, dass mindestens einer von ihnen die gewünschte Ungleichung erfüllt.

Annahme:

$$\left|\alpha - \frac{p_j}{q_j}\right| \geq \frac{1}{\sqrt{5}q_j^2} \quad \text{für} \quad j = n, n+1, n+2.$$

Nach Satz 7.6(i) haben $\alpha - p_n/q_n$ und $\alpha - p_{n+1}/q_{n+1}$ verschiedene Vorzeichen; also mit Korollar 7.5(i) und der Annahme

$$\frac{1}{\sqrt{5}q_n^2} + \frac{1}{\sqrt{5}q_{n+1}^2} \leq \left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{1}{q_n q_{n+1}}.$$

Es folgt

$$\frac{q_{n+1}}{q_n} + \frac{q_n}{q_{n+1}} \leq \sqrt{5},$$

also für $\lambda := q_{n+1}/q_n$ die Ungleichung $\lambda + 1/\lambda \leq \sqrt{5}$. Wegen $\lambda \in \mathbb{Q}$ gilt sogar $\lambda + 1/\lambda < \sqrt{5}$. Lösen der quadratischen Ungleichung liefert

$$\lambda < \frac{1+\sqrt{5}}{2}.$$

Setzen wir $\mu := q_{n+2}/q_{n+1}$, so ergibt die vollkommen analoge Argumentation

$$\mu < \frac{1+\sqrt{5}}{2}.$$

Nach Hilfssatz 7.4 haben wir $q_{n+2} = a_{n+2} \cdot q_{n+1} + q_n$, also

$$\mu = \frac{q_{n+2}}{q_{n+1}} = a_{n+2} + \frac{q_n}{q_{n+1}} \geq 1 + \frac{q_n}{q_{n+1}} = 1 + \frac{1}{\lambda}.$$

Daher

$$\frac{1+\sqrt{5}}{2} > \mu \geq 1 + \frac{1}{\lambda} > 1 + \frac{2}{1+\sqrt{5}} = \frac{1+\sqrt{5}}{2}.$$

Widerspruch!

□

Bemerkung:

Wir werden später noch sehen anhand der Zahl

$$\alpha = \frac{1}{2}(1+\sqrt{5}) = \langle 1; 1, 1, 1, \ldots \rangle ,$$

dass die Konstante $\sqrt{5}$ in Satz 7.8 bestmöglich ist.

Wir wollen nun nachweisen, dass die Näherungsbrüche die besten Approximationen an eine Zahl $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ sind in dem Sinne, dass $|\alpha - p/q|$ für alle Brüche p/q mit $0 < q < q_{n+1}$ minimal ist für $p/q = p_n/q_n$.

Satz 7.9

Für $\alpha = \langle a_0; a_1, a_2, \ldots \rangle$ gilt

(i) $$\alpha = \frac{p_n \vartheta_{n+1} + p_{n-1}}{q_n \vartheta_{n+1} + q_{n-1}} \quad (n \geq 0);$$

(ii) $$|\alpha q_n - p_n| = \frac{1}{q_n \vartheta_{n+1} + q_{n-1}} \quad (n \geq 0);$$

(iii) $$\frac{1}{(a_{n+2}+2)q_n^2} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{a_{n+1}q_n^2} \quad (n \geq 0).$$

(iv) Für alle p, q mit $0 < q < q_{n+1}$ gilt $|\alpha q - p| \geq |\alpha q_n - p_n|$.

Beweis:

(i) Nach Definition der ϑ_n gilt

$$\begin{aligned}\alpha = \vartheta_0 &= a_0 + \frac{1}{\vartheta_1} = \frac{a_0\vartheta_1 + 1}{\vartheta_1} = \frac{p_0\vartheta_1 + p_{-1}}{q_0\vartheta_1 + q_{-1}} \\ &= \frac{p_0(a_1 + 1/\vartheta_2) + p_{-1}}{q_0(a_1 + 1/\vartheta_2) + q_{-1}} = \frac{(a_1p_0 + p_{-1})\vartheta_2 + p_0}{(a_1q_0 + q_{-1})\vartheta_2 + q_0} = \frac{p_1\vartheta_2 + p_0}{q_1\vartheta_2 + q_0} = \cdots\end{aligned}$$

mit Hilfssatz 7.4.

(ii) Aus (i) folgt mit Korollar 7.5(i)

$$\begin{aligned}|\alpha q_n - p_n| &= \left|\frac{q_np_n\vartheta_{n+1} + q_np_{n-1}}{q_n\vartheta_{n+1} + q_{n-1}} - \frac{p_nq_n\vartheta_{n+1} + p_nq_{n-1}}{q_n\vartheta_{n+1} + q_{n-1}}\right| \\ &= \frac{|q_np_{n-1} - p_nq_{n-1}|}{q_n\vartheta_{n+1} + q_{n-1}} = \frac{1}{q_n\vartheta_{n+1} + q_{n-1}}.\end{aligned}$$

(iii) Nach Definition von ϑ_n haben wir wegen $\vartheta_n > 1 \quad (n \geq 1)$

$$a_{n+1}q_n < \vartheta_{n+1}q_n + q_{n-1} < (a_{n+1} + 1)q_n + q_n = (a_{n+1} + 2)q_n.$$

Mit (ii) folgt das Gewünschte.

(iv) Wir setzen für ein gegebenes p/q

$$u = \frac{pq_{n+1} - qp_{n+1}}{p_nq_{n+1} - q_np_{n+1}} \quad , \quad v = \frac{pq_n - qp_n}{q_np_{n+1} - p_nq_{n+1}},$$

wobei $u, v \in \mathbb{Z}$ nach Korollar 7.5(i). Wegen $(p_{n+1}, q_{n+1}) = 1$ nach Korollar 7.5(ii) und $0 < q < q_{n+1}$ nach Voraussetzung ist $u \neq 0$. Wir erhalten

$$up_n + vp_{n+1} = p \quad \text{und} \quad uq_n + vq_{n+1} = q.$$

Aus der letzten Gleichung ergibt sich wegen $0 < q < q_{n+1}$, dass für $v \neq 0$ die Zahlen u und v entgegengesetzte Vorzeichen haben. Da nach Satz 7.6(i) auch $\alpha q_n - p_n$ und $\alpha q_{n+1} - p_{n+1}$ verschiedene Vorzeichen haben, ergibt sich

$$\begin{aligned}|\alpha q - p| &= |\alpha(uq_n + vq_{n+1}) - (up_n + vp_{n+1})| \\ &= |u(\alpha q_n - p_n) + v(\alpha q_{n+1} - p_{n+1})| \geq |\alpha q_n - p_n|.\end{aligned}$$

□

Korollar 7.10

Sei $\alpha \in \mathbb{R}$ und $p/q \in \mathbb{Q}$. Ist

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2},$$

so ist p/q ein Näherungsbruch von α.

Beweis:

Wir wählen denjenigen Näherungsbruch p_n/q_n von α mit $q_n \leq q < q_{n+1}$. Dann gilt

$$\begin{aligned}\left|\frac{p}{q} - \frac{p_n}{q_n}\right| &= \left|\left(\frac{p}{q} - \alpha\right) + \left(\alpha - \frac{p_n}{q_n}\right)\right| \leq \left|\alpha - \frac{p}{q}\right| + \left|\alpha - \frac{p_n}{q_n}\right| \\ &= \frac{1}{q} \cdot |\alpha q - p| + \frac{1}{q_n} \cdot |\alpha q_n - p_n| \leq \left(\frac{1}{q} + \frac{1}{q_n}\right) |\alpha q - p|\end{aligned}$$

nach Satz 7.9(iv). Nach Voraussetzung und wegen $q \geq q_n$ erhalten wir

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| < \frac{2}{q_n} \cdot \frac{1}{2q} = \frac{1}{q \cdot q_n}.$$

Also bleibt nur $p/q = p_n/q_n$.

□

Seit Lagrange ist bekannt, dass ein unendlicher Kettenbruch genau dann periodisch (unter Umständen mit einer Vorperiode) ist, wenn die durch ihn dargestellte Zahl quadratisch irrational ist. Wir zeigen nur

Satz 7.11

Wird $\alpha \in \mathbb{R}$ von einem periodischen Kettenbruch dargestellt, d.h.

$$\alpha = \langle a_0; a_1, \ldots, a_{n-1}, \overline{a_k, \ldots, a_{k+m-1}} \rangle,$$

wobei der Oberstrich die Periode andeutet, so ist α eine quadratische Irrationalzahl.

Beweis:

Nach Satz 7.9(i) gilt für $\beta := \langle \overline{a_k; \ldots, a_{k+m-1}} \rangle$

$$\alpha = \frac{p_{k-1}\vartheta_k + p_{k-2}}{q_{k-1}\vartheta_k + q_{k-2}} = \frac{p_{k-1}\beta + p_{k-2}}{q_{k-1}\beta + q_{k-2}},$$

und wegen der Periodizität von β auch

$$\beta = \frac{p'_{m-1}\beta + p'_{m-2}}{q'_{m-1}\beta + q'_{m-2}},$$

wobei hier p'_n/q'_n die Näherungsbrüche von β bezeichnet. Es folgt sofort, dass β eine quadratische Gleichung über $\mathbb{Z}$ erfüllt, also auch α. Die Unendlichkeit des Kettenbruches von α impliziert schließlich dessen Irrationalität.

□

Bemerkung (ii) zu Satz 7.2 bedeutet, dass es zu jedem $\alpha \in \mathbb{Q}$ eine positive Konstante $c = c(\alpha)$ gibt derart, dass für alle $p/q \in \mathbb{Q},\ q > 0$, gilt

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^2}.$$

Wir werden dies nun auf beliebige *algebraische Zahlen* verallgemeinern, wobei wir diesen Begriff zuvor definieren wollen.

Definition:

Eine reelle (oder komplexe) Zahl α heißt *algebraisch vom Grad n*, falls es ein Polynom

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad \in \mathbb{Z}[x] \setminus \{0\},$$

aber kein solches Polynom geringeren Grades gibt mit $P(\alpha) = 0$. Setzen wir voraus, dass $a_n > 0$ und $(a_0, a_1, \ldots, a_n) = 1$, so ist $P(x)$ eindeutig bestimmt und heißt *Minimalpolynom* von α. Ist α nicht algebraisch, so nennen wir α *transzendent*.

Bemerkung:

Der Nachweis der Transzendenz gewisser bekannter Zahlen wie e, π ist schwierig.

Um 1844 bewies Liouville das folgende Ergebnis, das erstmalig die Existenz transzendenter Zahlen zeigte.

Satz 7.12 (von Liouville)

Sei α algebraisch vom Grad $n \geq 2$ (d.h. irrational). Dann existiert eine positive Konstante $c = c(\alpha)$ derart, dass für alle $p/q \in \mathbb{Q},\ q > 0$, gilt

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}.$$

Beweis:

Für $\alpha \in \mathbb{C}$, d.h. $\alpha = \text{Re } \alpha + i \cdot \text{Im } \alpha$ gilt offenbar nach Dreiecksungleichung

$$\left|\alpha - \frac{p}{q}\right| \geq \left|\text{Re } \alpha - \frac{p}{q}\right|.$$

Also können wir von vornherein $\alpha \in \mathbb{R}$ annehmen. Sei nun $P(x)$ das Minimalpolynom von α. Nach dem Mittelwertsatz gibt es für jedes p/q ein $\xi \in \mathbb{R}$ zwischen α und p/q derart, dass

$$\frac{P(\alpha) - P(p/q)}{\alpha - p/q} = P'(\xi),$$

wobei $P'(x)$ die Ableitung von $P(x)$ bezeichnet. Da α mindestens quadratisch ist, gilt $P\,(p/q) \neq 0$, denn sonst ließe sich von $P(x)$ ein Faktor $(x - p/q)$ abspalten, und der Grad von $P(x)$ wäre nicht minimal mit $P(\alpha) = 0$. Offenbar ist

$$q^n \cdot P\left(\frac{p}{q}\right) = q^n \cdot \left(a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_0\right) \quad \in \mathbb{Z} \quad ,$$

also $|q^n \cdot P\,(p/q)| \geq 1$. Mit der obigen Identität erhalten wir wegen $P(\alpha) = 0$

$$\left|\left(\alpha - \frac{p}{q}\right) \cdot P'(\xi)\right| = \left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}.$$

Ist $|\alpha - p/q| \geq 1$, so gilt der Satz trivialerweise. Wir düren also o.B.d.A. $|\alpha - p/q| < 1$ voraussetzen. Da ξ zwischen α und p/q liegt, folgt daraus $|\xi| < |\alpha| + 1$,

also mit $A := \max\limits_{1\le j\le n} |a_j|$

$$\begin{aligned} |P'(\xi)| &= |n\cdot a_n\xi^{n-1} + (n-1)a_{n-1}\xi^{n-2} + \ldots + a_1| \\ &< n\cdot(n\cdot A)\left(|\alpha|+1\right)^{n-1} =: \frac{1}{c(\alpha)}. \end{aligned}$$

Wir erhalten wie gewünscht

$$\left|\alpha - \frac{p}{q}\right| \ge \frac{1}{q^n\cdot|P'(\xi)|} > \frac{c(\alpha)}{q^n}.$$

□

Bemerkung:

Der vorstehende Beweis ermöglicht die Angabe einer expliziten Konstanten $c(\alpha)$. Wir wollen dies für die Zahl $\alpha_0 = \left(1+\sqrt{5}\right)/2$ ausnutzen, um zu zeigen, dass Satz 7.8 von Hurwitz bestmöglich ist.

Das Minimalpolynom von $\left(1+\sqrt{5}\right)/2$ ist $P_0(x) = x^2 - x - 1$, also $P_0'(x) = 2x - 1$. Wir setzen für $p/q \in \mathbb{Q},\ q > 0$, die Größe $\delta := |\alpha_0 - p/q|$. Nach dem Mittelwertsatz existiert ein ξ zwischen α_0 und p/q mit $|P_0\left(p/q\right)| = \delta\cdot|P_0'(\xi)|$. Wegen

$$|\xi| = |\alpha_0 + (\xi-\alpha_0)| \le \alpha_0 + |\xi-\alpha_0| \le \alpha_0 + \left|\frac{p}{q} - \alpha_0\right| = \alpha_0 + \delta$$

folgt

$$|P_0'(\xi)| \le 2(\alpha_0+\delta) - 1 = 2\delta + \sqrt{5}.$$

Wie im vorigen Beweis erhalten wir

$$\left|\alpha_0 - \frac{p}{q}\right| \ge \frac{1}{q^2\left|P_0'(\xi)\right|} \ge \frac{1}{\left(2\delta+\sqrt{5}\right)q^2} > \frac{1}{\left(\sqrt{5}+\varepsilon\right)q^2}$$

für jedes $\varepsilon > 0$, sofern q hinreichend groß ist, denn

$$\delta = \left|\alpha_0 - \frac{p}{q}\right| < \frac{1}{q^2} < \frac{\varepsilon}{2}$$

für alle Näherungsbrüche p/q mit hinreichend großem Nenner q nach Korollar 7.7, und $|\alpha_0 - p'/q'| \ge |\alpha_0 - p/q|$ für beliebige $p'/q' \in \mathbb{Q}$ mit $q' \le q$ nach Satz 7.9(iv).

Der Satz von Liouville besagt, dass sich algebraische Zahlen nicht „beliebig gut“ rational approximieren lassen. Dies kann zur Konstruktion gewisser transzendenter Zahlen verwendet werden.

Korollar 7.13

Die Zahl

$$\alpha := \sum_{k=1}^{\infty} 10^{-k!} = 0,11000100\ldots0100\ldots$$

ist transzendent.

Beweis:

Wir setzen

$$p_n := 10^{n!} \cdot \sum_{k=1}^{n} 10^{-k!} \in \mathbb{Z} \quad , \quad q_n := 10^{n!} \in \mathbb{Z}.$$

Offenbar gilt

$$\begin{aligned} \left|\alpha - \frac{p_n}{q_n}\right| &= \sum_{k=n+1}^{n} 10^{-k!} = 10^{-(n+1)!}\left(1 + 10^{(n+1)!-(n+2)!} + 10^{(n+1)!-(n+3)!} + \cdots\right) \\ &< 10^{-(n+1)!}\left(1 + 10^{-1} + 10^{-2} + \cdots\right) = \frac{10}{9} \cdot 10^{-(n+1)!} < 10^{-(n+1)!+1}, \end{aligned}$$

also wegen $(n+1)! - 1 = (n+1)n! - 1 \geq n \cdot n!$

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^n}.$$

Nach Satz 7.12 kann dann α nicht algebraisch von irgendeinem Grad sein. Daher ist α transzendent.

□

Bemerkung:

Der vorangegangene Beweis führt allgemeiner immer dann zur Transzendenz einer gegebenen Zahl α, sofern eine Folge verschiedener Zahlen $p_n/q_n \in \mathbb{Q}$ existiert derart, dass

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{\omega_n}} \quad \text{mit} \quad \lim_{n\to\infty} \omega_n = \infty.$$

Dies geht beispielsweise auch für andere Basen als 10, sofern in der entsprechenden g-adischen Entwicklung von α nur hinreichend lange Blöcke von Nullen auftreten. Entsprechend ist die Behandlung von Kettenbrüchen möglich, deren Teilnenner hinreichend schnell wachsen.

8 Diophantische Gleichungen

Die Lösbarkeit linearer Diophantischer Gleichungen (in mehreren Veränderlichen) wurde in §1 erschöpfend behandelt (Satz 1.4). Wir wenden uns nun Gleichungen höheren Grades zu, zunächst der sogenannten *Pell'schen Gleichung*

$$x^2 - Dy^2 = 1,$$

wobei $D \in \mathbb{N}$ keine Quadratzahl sei (für $D = d^2$ haben wir offenbar $x^2 - Dy^2 = (x - dy)(x + dy)$, also nur die trivialen Lösungen $x = \pm 1, y = 0$). Das folgende Resultat wurde von Fermat vermutet und von Lagrange bewiesen.

Satz 8.1

Ist $D \in \mathbb{N}$ und $\sqrt{D} \notin \mathbb{N}$, so hat die Gleichung $x^2 - Dy^2 = 1$ unendlich viele Lösungen $x, y \in \mathbb{N}$.

Beweis:

Wegen $\sqrt{D} \notin \mathbb{N}$ ist sogar $\sqrt{D} \notin \mathbb{Q}$, denn aus $\sqrt{D} = a/b,\ (a, b) = 1$, folgte $b^2 D = a^2$, also $a^2 \mid D$ und damit $b = 1$. Widerspruch!

Nach dem Dirichlet'schen Approximationssatz 7.2 existieren unendlich viele Paare $x_i, y_i \in \mathbb{N},\ i = 1, 2, \ldots,$ mit

$$0 < \left| \frac{x_i}{y_i} - \sqrt{D} \right| < \frac{1}{y_i^2}.$$

Wegen

$$0 < \left| \frac{x_i}{y_i} + \sqrt{D} \right| = \left| \frac{x_i}{y_i} - \sqrt{D} + 2\sqrt{D} \right| \leq \left| \frac{x_i}{y_i} - \sqrt{D} \right| + 2\sqrt{D} < \frac{1}{y_i^2} + 2\sqrt{D}$$

erhalten wir

$$0 < \left| x_i^2 - Dy_i^2 \right| = \left| x_i - \sqrt{D} y_i \right| \cdot \left| x_i + \sqrt{D} y_i \right| < \frac{1}{y_i} \left(\frac{1}{y_i} + 2\sqrt{D} y_i \right) \leq 2\sqrt{D} + 1$$

für alle Paare $x_i y_i$.

Wir wenden im Folgenden mehrfach den *unendlichen Schubfachschluss* an, der besagt: Werden unendlich viele Objekte auf endlich viele Schubladen verteilt, so befinden sich in mindestens einer Schublade unendlich viele Objekte. Nach den obigen Vorüberlegungen gibt es also eine ganze Zahl $k,\ 0 < |k| \leq 2\sqrt{D} + 1$, derart, dass

$$x_i^2 - Dy_i^2 = k$$

unendlich viele Lösungen $x_i, y_i \in \mathbb{N}$ besitzt. Durch erneute Anwendung des Schubfachschlusses finden wir darunter unendlich viele x_i, y_i mit $x_i \equiv x_j \bmod |k|$ und $y_i \equiv y_j \bmod |k|$ für alle i, j. Selbstverständlich haben wir darunter zwei Paare x_1, y_1 und x_2, y_2 (neue Numerierung) mit $x_1 \neq x_2$, also auch $y_1 \neq y_2$, die all die obigen Bedingungen erfüllen, d.h.

$$x_1^2 - Dy_1^2 = x_2^2 - Dy_2^2 = k, \quad x_1 \equiv x_2 \bmod |k|, \quad y_1 \equiv y_2 \bmod |k|.$$

Es folgt

$$x_1x_2 - y_1y_2D \equiv x_1^2 - Dy_1^2 \equiv 0 \bmod |k|,$$

also

$$x_1x_2 - y_1y_2D = ku,$$

bzw.

$$x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \bmod |k|,$$

also

$$x_1y_2 - x_2y_1 = kv$$

mit geeigneten $u, v \in \mathbb{Z}$. Also kommt

$$\left(x_1 - \sqrt{D}y_1\right)\left(x_2 + \sqrt{D}y_2\right) = x_1x_2 - y_1y_2D + (x_1y_2 - x_2y_1)\sqrt{D} = k\left(u + \sqrt{D}v\right)$$

und

$$\left(x_1 + \sqrt{D}y_1\right)\left(x_2 - \sqrt{D}y_2\right) = x_1x_2 - y_1y_2D - (x_1y_2 - x_2y_1)\sqrt{D} = k\left(u - \sqrt{D}v\right).$$

Multiplikation der beiden Terme liefert

$$k^2 = \left(x_1^2 - Dy_1^2\right)\left(x_2^2 - Dy_2^2\right) = k\left(u + \sqrt{D}v\right) \cdot k\left(u - \sqrt{D}v\right) = k^2\left(u^2 - Dv^2\right),$$

also $u^2 - Dv^2 = 1$. Hierbei ist $v \neq 0$, denn sonst wäre $u = \pm 1$ und damit

$$\begin{aligned}\left(x_1 - \sqrt{D}y_1\right) \cdot k &= \left(x_1 - \sqrt{D}y_1\right)\left(x_2 + \sqrt{D}y_2\right)\left(x_2 - \sqrt{D}y_2\right) \\ &= ku \cdot \left(x_2 - \sqrt{D}y_2\right) = \pm k\left(x_2 - \sqrt{D}y_2\right),\end{aligned}$$

also $x_1 - \sqrt{D}y_1 = \pm\left(x_2 - \sqrt{D}y_2\right)$. Wegen $\sqrt{D} \notin \mathbb{Q}$ folgt $x_1 = \pm x_2$, $y_1 = \pm y_2$, mit $x_1, x_2, y_1, y_2 \in \mathbb{N}$ daher $x_1 = x_2$ und $y_1 = y_2$. Widerspruch!

Wir haben also *eine* Lösung $u, v \in \mathbb{Z} \setminus \{0\}$ der Pell'schen Gleichung gefunden, wobei o.B.d.A. $u, v \in \mathbb{N}$.

Jeder Lösung $x, y \in \mathbb{N}$ der Pell'schen Gleichung ordnen wir die Irrationalzahl $x + \sqrt{D}y$, eine sogenannte *Pell'sche Einheit* zu. Wir definieren natürliche Zahlen x_n, y_n, $n = 1, 2, \ldots$, durch

$$x_n + \sqrt{D}y_n = \left(x + \sqrt{D}y\right)^n.$$

Nach dem Binomischen Lehrsatz gilt dann

$$\left(x - \sqrt{D}y\right)^n = \sum_{i=0}^{n} \binom{n}{i} \left(-\sqrt{D}y\right)^i x^{n-i} = \sum_{\substack{i=0 \\ 2|i}}^{n} \binom{n}{i} \left(\sqrt{D}y\right)^i x^{n-i} - \sum_{\substack{i=0 \\ 2\nmid i}}^{n} \binom{n}{i} \left(\sqrt{D}y\right)^i x^{n-i}$$

und

$$\left(x + \sqrt{D}y\right)^n = \sum_{\substack{i=0 \\ 2|i}}^{n} \binom{n}{i} \left(\sqrt{D}y\right)^i x^{n-i} + \sum_{\substack{i=0 \\ 2\nmid i}}^{n} \binom{n}{i} \left(\sqrt{D}y\right)^i x^{n-i},$$

also $\left(x - \sqrt{D}y\right)^n = x_n - \sqrt{D}y_n$. Es folgt

$$x_n^2 - Dy_n^2 = \left(x_n - \sqrt{D}y_n\right)\left(x_n + \sqrt{D}y_n\right) = \left(x - \sqrt{D}y\right)^n \cdot \left(x + \sqrt{D}y\right)^n = \left(x^2 - Dy^2\right)^n = 1,$$

d.h. alle $x_n + \sqrt{D}y_n$ sind Pell'sche Einheiten. Wegen

$$u + \sqrt{D}v > 1$$

sind die Potenzen $\left(u+\sqrt{D}v\right)^n$ paarweise verschieden, womit die Paare u_n, v_n unendlich viele Lösungen der Pell-Gleichung sind.

□

Nach Satz 8.1 besitzt jede Pell'sche Gleichung $x^2 - Dy^2 = 1$ Lösungen $x, y \in \mathbb{Z}$. Die kleinste unter ihnen, d.h. diejenige mit minimalem x und daher minimalem y, bezeichnen wir mit x_1, y_1. Sie heißt *Grundlösung* und die zugehörige Pell'sche Einheit $x_1 + \sqrt{D}y_1$ *Grundeinheit*.

Satz 8.2

Die Pell'schen Einheiten sind genau die Potenzen der Grundeinheit; mit anderen Worten: Alle Lösungen einer Pell'schen Gleichung ergeben sich als $\pm x_n, \pm y_n$ mit

$$x_n + \sqrt{D}y_n = (x_1 + \sqrt{D}y_1)^n \quad , \quad n \geq 1,$$

sowie der trivialen Lösung $x_0 = \pm 1, y_0 = 0$.

Beweis:

Sei $x+\sqrt{D}y$ eine Pell'sche Einheit, die keine Potenz von $x_1+\sqrt{D}y_1$ ist. Also existiert ein $n \in \mathbb{N}$ mit

$$\left(x_1 + \sqrt{D}y_1\right)^n < x + \sqrt{D}y < \left(x_1 + \sqrt{D}y_1\right)^{n+1}.$$

Wir multiplizieren mit $\left(x_1 - \sqrt{D}y_1\right)^n$ und erhalten

$$1 = \left(x_1^2 - \sqrt{D}y_1^2\right)^n < \left(x + \sqrt{D}y\right)\left(x_1 - \sqrt{D}y_1\right)^n < x_1 + \sqrt{D}y_1.$$

Setzen wir $\left(x_1 - \sqrt{D}y_1\right)^n = a + \sqrt{D}b$, so bekommen wir wie im vorigen Beweis $\left(x_1 + \sqrt{D}y_1\right)^n = a - \sqrt{D}b$. Es folgt mit

$$c + \sqrt{D}d := \left(x + \sqrt{D}y\right)\left(x_1 - \sqrt{D}y_1\right)^n = ax + Dby + \sqrt{D}\left(ay + bx\right),$$

dass

$$c - \sqrt{D}d = \left(x - \sqrt{D}y\right)\left(a - \sqrt{D}b\right) = \left(x - \sqrt{D}y\right)\left(x_1 + \sqrt{D}y_1\right)^n.$$

Damit kommt

$$c^2 - Dd^2 = \left(x^2 - Dy^2\right)\left(x_1^2 - Dy_1^2\right)^n = 1 \cdot 1^n = 1,$$

d.h. $\left(x + \sqrt{D}y\right)\left(x_1 - \sqrt{D}y_1\right)^n = c + \sqrt{D}d$ ist auch Pell'sche Einheit, sofern $c, d \in \mathbb{N}$. Wir wissen, dass $1 < c + \sqrt{D}d < x_1 + \sqrt{D}y_1$. Daher haben wir wegen $c - \sqrt{D}d = \left(c + \sqrt{D}d\right)^{-1}$ sofort $0 < c - \sqrt{D}d < 1$.
Es ergibt sich

$$c = \frac{1}{2}\left(c + \sqrt{D}d\right) + \frac{1}{2}\left(c - \sqrt{D}d\right) > \frac{1}{2}c \geq \frac{1}{2}$$

und

$$\sqrt{D}d = \frac{1}{2}\left(c + \sqrt{D}d\right) - \frac{1}{2}\left(c - \sqrt{D}d\right) > \frac{1}{2}c - \frac{1}{2} \geq 0,$$

d.h. $c, d \in \mathbb{N}$. Dies steht im Widerspruch zur Minimalität der Grundlösung x_1, y_1.

□

Bemerkungen:

(i) Der Beweis von Satz 8.1 impliziert, dass als Lösungen der Pell'schen Gleichung $x^2 - Dy^2 = 1$ die Näherungsbrüche p_n/q_n von $\sqrt{D}$ in der Form $x = p_n, y = q_n$ in Frage kommen. In der Tat ergibt eine genauere Analyse des Kettenbruchs von $\sqrt{D}$, dass dieser immer die Gestalt

$$\sqrt{D} = \langle a_0; \overline{a_1, \ldots, a_l} \rangle$$

besitzt. Die Periodenlänge l erweist sich als markante Größe, denn als Grundlösung stellt sich gerade das Paar
$x_1 = p_{l-1}, y_1 = q_{l-1}$ $(2 \mid l)$ bzw. $x_1 = p_{2l-1}, y_1 = q_{2l-1}$ $(2 \nmid l)$ heraus. Alle Lösungen sind

$$x_n = p_{nl-1}, y_n = q_{nl-1} \ (n \in \mathbb{N} \text{ für } 2 \mid l, \ n = 2, 4, 6, \ldots \text{ für } 2 \nmid l).$$

(ii) Nahe verwandt mit der Pell'schen Gleichung ist

$$x^2 - Dy^2 = -1.$$

Wie in (i) hängt das Lösungsverhalten eng mit der Kettenbruchentwicklung von $\sqrt{D}$ zusammen: Bei gerader Periodenlänge l existiert überhaupt keine Lösung, bei ungeradem l sind die positiven Lösungen

$$x_n = p_{nl-1}, y_n = q_{nl-1} \quad (n = 1, 3, 5, \ldots).$$

Die vielleicht berühmteste Diophantische Gleichung ist die *Fermat-Gleichung*

$$x^n + y^n = z^n$$

für $n \in \mathbb{N}, n \geq 2$. Der Spezialfall $n = 2$ geht auf die Griechen der Antike zurück, die entsprechenden Lösungen $x, y \in \mathbb{N}$ heißen *Pythagoräische Tripel*. Wegen der Homogenität der Fermat-Gleichung können wir o.B.d.A. stets $(x, y, z) = 1$ voraussetzen.

Satz 8.3

Die Lösungen von $x^2 + y^2 = z^2$ mit $(x, y, z) = 1$ sind genau gegeben durch

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2$$

(bzw. $x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2$) mit $a, b \in \mathbb{N},\ (a, b) = 1,\ 2 \mid ab$.

Beweis:

Offenbar sind die gegebenen Tripel Lösungen, denn

$$x^2 + y^2 = (a^4 - 2a^2b^2 + b^4) + 4a^2b^2 = a^4 + 2a^2b^2 + b^4 = z^2.$$

Sei nun umgekehrt x, y, z ein Pythagoräisches Tripel mit $(x, y, z) = 1$. O.B.d.A. sei y gerade, denn für $x \equiv y \equiv 1 \bmod 2$ wäre $x^2 + y^2 \equiv 2 \bmod 4$, aber $z^2 \equiv 0, 1 \bmod 4$. Es folgt $2 \nmid x, 2 \nmid z$. Wir schreiben die Ausgangsgleichung in der Form

$$y^2 = z^2 - x^2 = (z + x)(z - x).$$

Wegen $(z+x, z-x) = (z+x, 2z) = 2$ erhalten wir

$$z + x = 2a^2, \quad z - x = 2b^2, \quad y = 2ab$$

für gewisse a, b mit $(a, b) = 1$. Wegen $z \equiv 1, 3 \bmod 4$ und $x \equiv 1, 3 \bmod 4$ folgt $z + x \equiv 2 \bmod 4$, $z - x \equiv 0 \bmod 4$ oder $z + x \equiv 0 \bmod 4$, $\quad z - x \equiv 2 \bmod 4$, also ist eine der Zahlen a, b gerade, d.h. $2 \mid ab$.

□

Bekanntlich besagt die *Fermat'sche Vermutung*, die kürzlich von Wiles und Taylor in erheblich größerer Allgemeinheit bewiesen wurde, dass die Fermat'sche Gleichung für $n \geq 3$ keine Lösung $x, y, z \in \mathbb{N}$ besitzt. Der einfachste Fall ist $n = 4$, der bereits von Fermat selbst geklärt wurde.

Satz 8.4

Die Gleichung $x^4 + y^4 = z^2$ besitzt keine Lösung $x, y, z \in \mathbb{N}$.

Beweis: (Fermat'scher Abstieg)
Wir nehmen an, es gäbe eine Lösung $x, y, z \in \mathbb{N}$, wobei z minimal sei. Dann gilt selbstverständlich $(x, y, z) = 1$. Außerdem ist - wie bei $x^2 + y^2 = z^2$ - eine der Zahlen x, y gerade, o.B.d.A. sei $2 \mid y$. Damit ist x^2, y^2, z^2 ein Pythagoräisches Tripel, d.h. nach Satz 8.3 existieren $a, b \in \mathbb{N}$ mit

$$x^2 = a^2 - b^2, \quad y^2 = 2ab, \quad z = a^2 + b^2$$

und $(a, b) = 1$, $2 \mid ab$. Wäre $2 \mid a$, $2 \nmid b$, so hätten wir $x^2 \equiv 4 - 1 \equiv 3 \bmod 4$, was unmöglich ist; also $2 \mid b$, $2 \nmid a$. Mit $x^2 + b^2 = a^2$ ist weiterhin auch x, b, a ein Pythagoräisches Tripel. Daher existieren nach Satz 8.3 Zahlen $c, d \in \mathbb{N}$, $(c, d) = 1$ mit

$$x = c^2 - d^2, \quad b = 2cd, \quad a = c^2 + d^2.$$

Es folgt

$$y^2 = 2ab = 4cd(c^2 + d^2).$$

Wegen $(c, d) = 1$ ist $(c, c^2 + d^2) = (d, c^2 + d^2) = 1$, d.h.

$$c = e^2, \quad d = f^2, \quad c^2 + d^2 = g^2$$

für gewisse $e, f, g \in \mathbb{N}$. Damit ist

$$e^4 + f^4 = g^2,$$

wir haben also eine weitere Lösung unserer Ausgangsgleichung konstruiert. Dabei ist aber

$$g \leq g^2 = c^2 + d^2 = a \leq a^2 < a^2 + b^2 = z$$

im Widerspruch zur Annahme der Minimalität von z.

□

Korollar 8.5

Die Gleichung $x^4 + y^4 = z^4$ besitzt keine Lösung $x, y, z \in \mathbb{N}$.

Wir wollen noch ein anderes Beispiel einer Gleichung vierten Grades angeben, das ebenfalls auf Fermat zurückgeht.

Satz 8.6

Die Gleichung

$$x^4 - x^2y^2 + y^4 = z^2 \quad , \quad (x, y) = 1,$$

hat nur die Lösungen $x^2 = 1, y = 0$ und $x = 0, y^2 = 1$ und $x^2 = y^2 = 1$.

Beweis:

O.B.d.A. seien $x, y, z \in \mathbb{N}$. Wir schreiben die Gleichung als

$$(x^2 - y^2)^2 + (xy)^2 = z^2.$$

Fall 1: $2 \mid xy$.

Es folgt $2 \nmid (x^2 - y^2)$, also nach Satz 8.3

$$x^2 - y^2 = a^2 - b^2 \quad , \quad xy = 2ab$$

für gewisse $(a, b) = 1$. Wir setzen $d_1 := (x, b),\ d_2 := (y, a)$ und $x =: d_1 X,\ b =: d_1 B$, $y =: d_2 Y,\ a =: d_2 A$, also $XY = 2AB$. Selbstverständlich ist $(X, B) = (Y, A) = 1$ und daher $X \mid 2A,\ A \mid X$ und $Y \mid 2B,\ B \mid Y$. Es folgt $X = 2A,\ Y = B$, oder $X = A,\ Y = 2B$.

Fall 1.1: $X = 2A,\ Y = B$.

Es ergibt sich

$$x = 2Ad_1, \quad b = d_1 B, \quad y = d_2 B, \quad a = d_2 A.$$

Einsetzen in $x^2 - y^2 = a^2 - b^2$ liefert

$$4A^2 d_1^2 - d_2^2 B^2 = d_2^2 A^2 - d_1^2 B^2,$$

also

$$d_1^2(4A^2 + B^2) = d_2^2(A^2 + B^2).$$

Es ist $(A^2 + B^2, 4A^2 + B^2) = (A^2 + B^2, 3A^2) = (A^2 + B^2, A^2)$, denn wegen $(a, b) = 1$ ist auch $(A, B) = 1$ und somit $A^2 + B^2 \not\equiv 0 \bmod 3$. Also haben wir

$$(A^2 + B^2, 4A^2 + B^2) = (B^2, A^2) = 1.$$

Damit folgt für gewisse C und D

$$A^2 + B^2 = C^2 \quad \text{und} \quad 4A^2 + B^2 = D^2.$$

O.B.d.A. sei B ungerade, denn für $2 \mid B$ ergäbe sich ein entsprechendes Paar von Gleichungen mit vertauschten Variablen. Die zweite der Gleichungen $(2A)^2 + B^2 = D^2$ hat nach Satz 8.3 eine Lösung mit $B = p^2 - q^2$ und $A = pq$ für gewisse $(p, q) = 1$ mit $2 \mid pq$.

Einsetzen in die erste Gleichung liefert

$$p^4 - p^2q^2 + q^4 = C^2.$$

Wegen $pq = A \leq a \leq xy/2$ lässt sich die Methode des Fermat'schen Abstiegs anwenden, zumal $p^2 = q^2 = 1$ wegen $B \neq 0$ auch nicht eintreten kann. Die Ausgangsgleichung ist in diesem Fall unlösbar.

Fall 1.2: $X = A,\ Y = 2B$.

Es folgt analog zu Fall 1.1

$$d_1^2(A^2 + B^2) = d_2^2(A^2 + 4B^2),$$

und die obige Argumentation lässt erneut einen Fermat'schen Abstieg zu, und auch hier existiert keine Lösung.

Fall 2: $2 \nmid xy$.

Mit Satz 8.3 folgt sofort

$$xy = a^2 - b^2 \quad , \quad x^2 - y^2 = 2ab$$

für gewisse $(a, b) = 1$, weshalb $2 \mid ab$. Wir haben daher

$$a^4 - a^2b^2 + b^4 = (xy)^2 + \left(\frac{x^2 - y^2}{2}\right)^2 = \left(\frac{x^2 + y^2}{2}\right)^2.$$

Nach Fall 1 lässt dies nur die triviale Lösung $ab = 0$ zu, d.h. wegen $(x, y) = 1$ bleibt nur $x^2 = y^2 = 1$.

□

Korollar 8.7

Es gibt keine vier Quadrate in arithmetischer Progression, d.h. Quadrate $x_1^2, x_2^2, x_3^2, x_4^2$ mit $x_{i+1}^2 - x_i^2 = \text{const} \quad (1 \leq i \leq 3)$.

Beweis:

Wir nehmen an, es gäbe eine Konstante $c \in \mathbb{N}$ mit $x_{i+1}^2 - x_i^2 = c$ für $i = 1, 2, 3$. Es folgt

$$x_1^2 + x_3^2 = (x_1^2 + c) + (x_3^2 - c) = 2x_2^2$$

und

$$x_2^2 + x_4^2 = 2x_3^2.$$

Also ergibt sich

$$x_1^2(2x_3^2 - x_2^2) = x_1^2 x_4^2 = x_4^2(2x_2^2 - x_3^2)$$

und daraus

$$2(x_1^2 x_3^2 - x_2^2 x_4^2) = x_1^2 x_2^2 - x_3^2 x_4^2.$$

Wir setzen $a := x_1 x_3, \quad b := x_2 x_4, \quad c := \frac{1}{2}(x_1 x_2 + x_3 x_4), \quad d := \frac{1}{2}(x_1 x_2 - x_3 x_4)$. Offenbar sind $x_1 \equiv x_3 \bmod 2$ und $x_2 \equiv x_4 \bmod 2$, also c,d ganz. Damit kommt neben $ab = c^2 - d^2$ aus obiger Identität

$$a^2 - b^2 = 2cd$$

und daraus

$$a^4 - a^2 b^2 + b^4 = 4c^2 d^2 + (c^2 - d^2)^2 = (c^2 + d^2)^2.$$

Nach Satz 8.6 bleiben nur $a = 0$ oder $b = 0$, d.h. eines der $x_i = 0$, oder $a^2 = b^2$, d.h. $(x_1 x_3)^2 = (x_2 x_4)^2$. Beides ist offensichtlich unmöglich.

□

Bemerkung:

Drei Quadrate in arithmetischer Progression existieren, z.B. $1^2 = 1, \quad 5^2 = 25$ und $7^2 = 49$ und daraus allgemein

$$x_1 = k, \quad x_2 = 5k, \quad x_3 = 7k \quad (k \in \mathbb{N}),$$

denn $x_2^2 - x_1^2 = 24k^2 = x_3^2 - x_2^2$.

Wir kommen nun auf eine Diophantische Gleichung zu sprechen, die - anders als die bisher behandelten - nicht polynomial ist, nämlich die sogenannte *Catalan'sche Gleichung*

$$x^n - y^m = 1.$$

Hierbei sind x, y, n, m als Variablen aufzufassen, und wir sprechen deshalb von einer *Diophantischen Exponential-Gleichung*. Catalan vermutete 1844, dass für $x, y, n, m \in \mathbb{N} \setminus \{1\}$ die einzige Lösung gegeben ist durch $x = 3,\ y = 2,\ n = 2,\ m = 3$. Nach Tijdeman (1976) ist bekannt, dass die Catalan'sche Gleichung nur endlich viele Lösungen besitzt, und diese lassen sich effektiv beschränken. Wir behandeln ganz elementar einen Spezialfall.

Satz 8.8

Die Gleichung $3^n - 2^m = 1$ hat über $\mathbb{N}$ nur die Lösungen $n = m = 1$ und $n = 2, m = 3$.

Beweis:

1. Fall: $n = 2k + 1,\ k \in \mathbb{N}_0$.

Es ist $3^n \equiv 3^{2k+1} \equiv 9^k \cdot 3 \equiv 1^k \cdot 3 \equiv 3 \bmod 4$, also haben wir $3^n - 1 \equiv \bmod 4$. Für $m \geq 2$ gilt $4 \mid 2^m$, also ist $3^n - 1 = 2^m$ nur für $m = 1$, daher $n = 1$ möglich.

2. Fall: $n = 2k, \quad k \in \mathbb{N}$.

Wir haben $3^n - 1 = (3^k - 1)(3^k + 1) = 2^m$, also $3^k - 1 = 2^s, \quad 3^k + 1 = 2^t$ für gewisse $s, t \in \mathbb{N}_0$. Es kommt $2^s + 1 = 3^k = 2^t - 1$, d.h. $2^t - 2^s = 2$, mit anderen Worten $t = 2, \quad s = 1$, also $k = 1$. Es ergibt sich $n = 2k = 2$ und daraus $m = 3$.

□

9 p-adische Zahlen

Der gewöhnliche Absolutbetrag $|x|$ für $x \in \mathbb{Q}$ ist eine Norm auf $\mathbb{Q}$ und induziert die Metrik $d(x,y) := |x-y|$ für $x, y \in \mathbb{Q}$. Wir werden andere Normen und Metriken auf $\mathbb{Q}$ kennenlernen.

Für $p \in \mathbb{P}$ und $x = \pm a/b \in \mathbb{Q}$ definieren wir (in Erweiterung der Ordnung $e_p(n)$ für $n \in \mathbb{N}$)

$$e_p(x) = \begin{cases} e_p(a) - e_p(b) & \text{für} \quad x \neq 0, \\ 0 & \text{für} \quad x = 0. \end{cases}$$

Dabei hängt $e_p(x)$ nicht von der speziellen Bruchdarstellung von x ab, denn

$$e_p\left(\frac{ac}{bc}\right) = e_p(ac) - e_p(bc) = e_p(a) + e_p(c) - e_p(b) - e_p(c) = e_p\left(\frac{a}{b}\right).$$

Lemma 9.1

Sei $p \in \mathbb{P}$. Die Abbildung $|\quad|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ definiert durch

$$|x|_p = \begin{cases} p^{-e_p(x)} & \text{für} \quad x \neq 0, \\ 0 & \text{für} \quad x = 0, \end{cases}$$

ist eine Norm auf $\mathbb{Q}$; d.h.

(1) $|x|_p = 0 \Longleftrightarrow x = 0$,

(2) $|x \cdot y|_p = |x|_p \cdot |y|_p$

(3) $|x + y|_p \leq |x|_p + |y|_p$

für alle $x, y \in \mathbb{Q}$. Anstelle der Dreiecksungleichung (3) gilt sogar die schärfere Ungleichung $|x + y|_p \leq \max(|x|_p, |y|_p)$, wobei „<“ nur für $|x|_p = |y|_p$ auftreten kann.

Beweis:

(1) ist klar.

Für $xy = 0$ ist auch (2) klar. Für $xy \neq 0$ haben wir

$$|xy|_p = p^{-e_p(xy)} = p^{-e_p(x)} \cdot p^{-e_p(y)} = |x|_p \cdot |y|_p.$$

Für $x = 0, y = 0$ oder $x + y = 0$ ist die verschärfte Dreiecksungleichung klar. Sei also $xy \neq 0$ und $x + y \neq 0$. Mit gekürzten Brüchen $x = a/b,\ y = c/d$ haben wir

$$\begin{aligned} e_p(x+y) &= e_p\left(\frac{ad+bc}{bd}\right) = e_p(ad+bc) - e_p(b) - e_p(d) \\ &\geq \min(e_p(ad), e_p(bc)) - e_p(b) - e_p(d) \\ &= \min(e_p(a) + e_p(d), e_p(b) + e_p(c)) - e_p(b) - e_p(d) \\ &= \min(e_p(a) - e_p(b), e_p(c) - e_p(d)) = \min(e_p(x), e_p(y)). \end{aligned}$$

Also

$$|x+y|_p = p^{-e_p(x+y)} \leq \max\left(p^{-e_p(x)}, p^{-e_p(y)}\right) = \max(|x|_p, |y|_p).$$

□

Definition:

Eine Norm heißt *nicht-archimedisch*, falls stets $|x + y| \leq \max(|x|, |y|)$ gilt. Eine Metrik heißt nicht-archimedisch, falls $d(x, y) \leq \max(d(x, z), d(z, y))$ für alle x, y, z. Gewöhnliche Normen und Metriken heißen *archimedisch*.

Bemerkung:

Nach Lemma 9.1 ist jedes $|.|_p$ eine nicht-archimedische Norm auf $\mathbb{Q}$. Nicht-archimedische Normen induzieren nicht-archimedische Metriken, denn

$$d(x, y) := |x - y| = |(x - z) + (z - y)| \leq \max(|x - z|, |z - y|) = \max(d(x, z), d(z, y)).$$

Der gewöhnliche Absolutbetrag ist eine archimedische Norm auf $\mathbb{Q}$, z.B.

$$|1 + 1| > \max(|1|, |1|).$$

Bezüglich des gewöhnlichen Absolutbetrages bzw. der davon induzierten Metrik ist $\mathbb{Q}$ nicht vollständig, d.h es gibt rationale Cauchy-Folgen, die in $\mathbb{Q}$ keinen Grenzwert besitzen. Durch Vervollständigung entsteht $\mathbb{R}$. Das folgende Beispiel zeigt, dass $\mathbb{Q}$ auch bzgl. $|\quad|_p$ (jedenfalls für ein hinreichend großes p) nicht vollständig ist.

Beispiel 9.2

Sei $p \neq 2$ und r quadratischer Rest mod p. Wir definieren rekursiv eine Folge $(a_n)_{n\in\mathbb{N}}$ über $\mathbb{Z}$ mit der Bedingung

$$a_n^2 \equiv r \bmod p^n \quad (n \in \mathbb{N}).$$

Dies ist möglich (und nicht eindeutig), denn:
$a_1^2 \equiv r \bmod p$ ist lösbar, wobei $p \nmid a_1$. Wir setzen $a_2 = a_1 + kp$ mit k derart, dass

$$a_2^2 = (a_1 + kp)^2 \equiv a_1^2 + 2a_1k \overset{!}{\equiv} r \bmod p^2$$

(lösbar wegen $p = (2a_1p, p^2) \mid (r - a_1^2)$). Allgemein setzen wir $a_{n+1} := a_n + k_n \cdot p^n$ mit $a_{n+1}^2 \equiv r \bmod p^{n+1}$. Die Folge $(a_n)_{n\in\mathbb{N}}$ ist Cauchy-Folge bezüglich $|.|_p$, denn für $n > m$ gilt

$$\begin{aligned} a_n - a_m &= (a_n - a_{n-1}) + (a_{n-1} - a_{n-2}) + \cdots + (a_{m+1} - a_m) \\ &= k_{n-1}p^{n-1} + k_{n-2}p^{n-2} + \cdots + k_mp^m, \end{aligned}$$

also $|a_n - a_m| \leq p^{-m}$.
Annahme: $(a_n)_{n\in\mathbb{N}}$ besitzt den Grenzwert $a \in \mathbb{Q}$.
Wir nehmen zunächst außerdem an, dass $a^2 \neq r$. Dann sei $|a^2 - r|_p =: p^{-e_0}$. Wegen $\lim\limits_{n\to\infty} a_n = a$ ist $|a_n - a|_p < p^{-(e_0+1)}$ für alle großen $n \in \mathbb{N}$. Mit $a = c/d,\ (c, d) = 1$, ist $a_n - a = (a_nd - c)/d$, wobei $p \nmid d$ (sonst $p \mid c$ wegen $p^{e_0+1} \mid (a_n - a)$). Es folgt

$$|a_n + a|_p = \left|\frac{a_nd + c}{d}\right| \leq 1.$$

Also

$$|a_n^2 - a^2|_p = |a_n - a|_p \cdot |a_n + a|_p < p^{-(e_0+1)}.$$

Wir erhalten

$$\begin{aligned} |a^2 - r|_p &= |(a^2 - a_n^2) + (a_n^2 - r)|_p \leq \max(|a^2 - a_n^2|_p, |a_n^2 - r|_p) \\ &< \max(p^{-(e_0+1)}, p^{-n}) = p^{-(e_0+1)} \quad \text{für} \quad n \geq e_0 + 1. \end{aligned}$$

Widerspruch!

Es bleibt nur die Möglichkeit $r = a^2$, d.h. r ist Quadratzahl in $\mathbb{Z}$. Zwischen 0 und p gibt es $(p-1)/2$ quadratische Reste, aber nur $\left[\sqrt{p}\right]$ Quadratzahlen. Wegen $\sqrt{p} < (p-1)/2$ für $p \geq 7$ können wir also einen quadratischen Rest r mod p wählen, der keine Quadratzahl ist. Die damit konstruierte Folge $(a_n)_{n\in\mathbb{N}}$ ist Cauchy-Folge ohne Grenzwert in $\mathbb{Q}$.

Vervollständigung von $\mathbb{Q}$ bzgl. $|.|_p$

Wir nennen zwei Cauchy-Folgen $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ bezüglich $|.|_p$ *äquivalent*, falls $|a_n - b_n|_p \to 0$ für $n \to \infty$. Wir definieren $\mathbb{Q}_p$ als die Menge der Äquivalenzklassen von Cauchy-Folgen über $\mathbb{Q}$. Für $x \in \mathbb{Q}$ bezeichne (x) die konstante Cauchy-Folge $(x, x, x, \ldots)$. Offenbar gilt

$$(x) \sim (x') \Longleftrightarrow x = x'.$$

Die Norm eines Elements $a \in \mathbb{Q}_p$ (d.h. einer Äquivalenzklasse) sei erklärt durch

$$|a|_p := \lim_{n\to\infty} |a_n|_p,$$

wobei $(a_n)_{n\in\mathbb{N}}$ ein beliebiger Repräsentant von a sei (wir schreiben: $a = \overline{(a_n)}$).

Lemma 9.3

Für $a \in \mathbb{Q}_p$ ist $|a|_p$ existent und wohldefiniert.

Beweis:

Existenz: Falls $a \sim (0)$, so gilt nach Definition der Äquivalenz $|a_n|_p = |a_n - 0|_p \to 0$. Sei also $a \not\sim (0)$. Dann gilt

$$\begin{array}{ccc} \exists & \forall & \exists \\ \varepsilon > 0 & N \in \mathbb{N} & n_0 > N \end{array} \quad |a_{n_0}|_p > \varepsilon.$$

Wir wählen N so groß, dass $|a_n - a_{n'}|_p < \varepsilon$ für alle $n, n' > N$. Insbesondere haben wir $|a_n - a_{n_0}|_p < \varepsilon$ für alle $n, n' > N$. Außerdem gilt

$$|a_n - a_{n_0}|_p \leq \max(|a_n|_p, |a_{n_0}|_p),$$

wobei $|a_{n_0}|_p > \varepsilon$. Nach Lemma 9.1 bleibt nur die Möglichkeit $|a_n|_p = |a_{n_0}|_p$ für alle $n > N$, also

$$\lim_{n\to\infty} |a_n|_p = |a_{n_0}|_p.$$

Wohldefiniertheit: Für $a \sim b \sim (0)$ folgt wieder aus der Definition der Äquivalenz $|a_n|_p \to 0$ und $|b_n|_p \to 0$. Für $a \sim b \not\sim (0)$ erhalten wir aufgrund des Arguments im ersten Teil des Beweises, dass $|a|_p = p^\alpha$ und $|b|_p = p^\beta$ für gewisse $\alpha, \beta \in \mathbb{Z}$. Die Annahme $\alpha \neq \beta$ stände im Widerspruch zu $|a_n - b_n|_p \to 0$.

□

Bemerkung:

Das vorstehende Lemma zeigt, dass

$$\{|a|_p : a \in \mathbb{Q}_p\} = \{|r|_p : r \in \mathbb{Q}\} = \{0\} \cup \{p^t : t \in \mathbb{Z}\},$$

d.h. der Wertebereich der Norm bleibt bei der Vervollständigung von $\mathbb{Q}$ nach $\mathbb{Q}_p$ unverändert. Im Gegensatz dazu erweitert sich beim Übergang von $\mathbb{Q}$ zu $\mathbb{R}$ der Normwertebereich von $\mathbb{Q}_{\geq 0}$ zu $\mathbb{Q}_{\geq 0}$.

Satz 9.4

Jedes $\mathbb{Q}_p$ ist ein vollständiger Körper bzgl. $|.|_p$ mit Unterkörper $\mathbb{Q}$ (also char $\mathbb{Q}_p = 0$).

Beweis:

Seien $(a = \overline{(a_n)} = \overline{(a'_n)}, \quad b = \overline{(b_n)} = \overline{(b'_n)} \in \mathbb{Q}_p$. Wir setzen

$$a + b := \overline{(a_n + b_n)}, \quad a \cdot b := \overline{(a_n \cdot b_n)}.$$

Die Wohldefiniertheit folgt aus

$$\begin{aligned} |(a_n + b_n) - (a'_n + b'_n)|_p &= |(a_n - a'_n) + (b_n - b'_n)|_p \\ &\leq \max(|a_n - a'_n|_p, |b_n - b'_n|_p) \to 0 \end{aligned}$$

bzw.

$$\begin{aligned} |a_n b_n - a'_n b'_n|_p &= |a_n(b_n - b'_n) + b'_n(a_n - a'_n)|_p \\ &\leq \max(|a_n|_p \cdot |b_n - b'_n|_p, |b'_n|_p \cdot |a_n - a'_n|_p) \to 0. \end{aligned}$$

Additive Inverse werden in offensichtlicher Weise erklärt. Bei multiplikativen Inversen berücksichtigen wir, dass jede Cauchy-Folge (a_n) äquivalent ist zu $(\tilde{a}_n)$ mit

$$\tilde{a}_n = \begin{cases} a_n & \text{für} \quad a_n \neq 0, \\ p^n & \text{für} \quad a_n = 0. \end{cases}$$

Damit ist auch $(a_n)^{-1} := 1/\tilde{a}_n$ eine Cauchy-Folge außer für $|\tilde{a}_n|_p \to 0$, d.h. $\overline{(a_n)} = 0$. Die Rechengesetze für Körper folgen für $\mathbb{Q}_p$ direkt aus denen für $\mathbb{Q}$. Wegen $\mathbb{Q} \simeq \{\overline{(r)} : r \in \mathbb{Q}\} \subseteq \mathbb{Q}_p$ haben wir gezeigt, dass $\mathbb{Q}_p$ ein Oberkörper von $\mathbb{Q}$ ist. Zu zeigen bleibt die Vollständigkeit von $\mathbb{Q}_p$. Sei also $(\alpha_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge über $\mathbb{Q}_p$, d.h. für $\varepsilon > 0$ gilt $|\alpha_i - \alpha_j|_p < \varepsilon$, sofern $i, j > N(\varepsilon)$.

Wir zeigen zunächst, dass zu jedem α_i ein $a_i \in \mathbb{Q}$ existiert mit $|\alpha_i - a_i|_p < 2^i$: Sei etwa $\alpha_i = \overline{(\alpha_{ij})}_{j\in\mathbb{N}}$. Dann gilt $|\alpha_{ij} - \alpha_{ij'}|_p < 2^{-i}$ für hinreichend große j, j'. Mit $a_i := \alpha_{ij'}$ haben wir gemäß Definition der Norm auf $\mathbb{Q}_p$

$$|\alpha_i - a_i|_p = \lim_{j\to\infty} |\alpha_{ij} - \alpha_{ij'}|_p < 2^{-i}.$$

Die Folge $(a_n)_{n\in\mathbb{N}}$ ist eine Cauchy-Folge (über $\mathbb{Q}$), denn für hinreichend große i, j gilt

$$\begin{aligned} |a_i - a_j|_p &= |(a_i - \alpha_i) + (\alpha_i - \alpha_j) + (\alpha_j - a_j)|_p \\ &\leq |a_i - \alpha_i|_p + |\alpha_i - \alpha_j|_p + |\alpha_j - a_j|_p < 2^{-i} + \varepsilon + 2^{-j} < 2\varepsilon. \end{aligned}$$

Wir setzen $\alpha := \overline{(a_n)}_{n\in\mathbb{N}}$ und haben für ein hinreichend großes i

$$\begin{aligned} |\alpha_i - \alpha|_p = \lim_{j\to\infty} |\alpha_i - a_j|_p &\leq \lim_{j\to\infty} (|\alpha_i - a_i|_p + |a_i - a_j|_p) \\ &\leq 2^{-i} + 2\varepsilon < 3\varepsilon; \end{aligned}$$

d.h. $(\alpha_n)_{n\in\mathbb{N}}$ konvergiert gegen α.

□

Bemerkung:

Der oben durchgeführte Vervollständigungsprozess kann ganz allgemein benutzt werden bei beliebigen Körpern, auf denen eine Norm erklärt ist.

Satz 9.5

Für $p_1 \neq p_2$ sind die Körper $\mathbb{Q}_{p_1}$ und $\mathbb{Q}_{p_2}$ nicht isomorph.

Beweis:

Es gibt eine natürliche Zahl r, die quadratischer Rest mod p_1 und quadratischer Nichtrest mod p_2 ist, denn:

Seien a_0 quadratischer Rest mod p_1 und b_0 quadratischer Nichtrest mod p_2. Damit ist $a_0 + p_1 s \quad (s \in \mathbb{Z})$ quadratischer Rest mod p_1 und $b_0 + p_2 t \quad (t \in \mathbb{Z})$ quadratischer Nichtrest mod p_2. Die Diophantische Gleichung

$$p_1 s - p_2 t = b_0 - a_0$$

ist wegen $(p_1, p_2) = 1$ lösbar und liefert das gewünschte r.

In Beispiel 9.2 hatten wir gezeigt, dass für den quadratischen Rest $r \bmod p_1$, die dort konstruierte Cauchy-Folge den Grenzwert a mit $a^2 = r$ besitzt. Wegen der Vollständigkeit von $\mathbb{Q}_{p_1}$ ist $a \in \mathbb{Q}_{p_1}$, d.h. $x^2 = r$ ist lösbar über $\mathbb{Q}_{p_1}$. Da r quadratischer Nichtrest mod p_2 ist, kann $x^2 = r$ über $\mathbb{Q}_{p_2}$ nicht lösbar sein, da nicht einmal $x^2 \equiv r \bmod p_2$ lösbar ist. Daher können $\mathbb{Q}_{p_1}$ und $\mathbb{Q}_{p_2}$ nicht isomorph sein.

□

Bemerkung:

Nach einem Satz von Ostrowski sind der gewöhnliche Absolutbetrag $|.|$ und die p-adischen Beträge $|.|_p$ ($p \in \mathbb{P}$) „bis auf Äquivalenz“ alle möglichen Normen auf $\mathbb{Q}$. Da äquivalente Normen zu isomorphen Vervollständigungen führen, sind somit $\mathbb{R}$ und die p-adischen Körper $\mathbb{Q}_p$ ($p \in \mathbb{P}$) bis auf Isomorphie alle möglichen Vervollständigungskörper von $\mathbb{Q}$.

Die reellen Zahlen lassen sich (statt als Äquivalenzklassen von Cauchy-Folgen) konkret als Dezimalzahlen schreiben. Eine ähnlich konkrete Darstellung existiert auch für p-adische Zahlen.

Wir definieren den Ring der *ganzen p-adischen Zahlen*

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Offenbar ist $\mathbb{Z} \subseteq \mathbb{Z}_p$; es gilt sogar

$$\left\{\frac{a}{b} : (a,b) = 1, p \nmid b\right\} \subseteq \mathbb{Z}_p.$$

Damit lässt sich $\mathbb{Q}_p$ auch auffassen als Quotientenkörper von $\mathbb{Z}_p$ (so wie $\mathbb{Q}$ als Quotientenkörper von $\mathbb{Z}$.

Lemma 9.6

$\mathbb{Z}$ liegt dicht in $\mathbb{Z}_p$.

Beweis:

Sei $\alpha \in \mathbb{Z}_p$. Gemäß Beweis zu Satz 9.4 existiert zu jedem $i \in \mathbb{N}$ ein $r_i \in \mathbb{Q}$ mit $|\alpha - r_i|_p \leq p^{-i}$. Wegen $|\alpha|_p \leq 1$ folgt $|r_i|_p \leq 1$ (sonst $|\alpha - r_i|_p = \max(|\alpha|_p, |r_i|_p) > 1$ Widerspruch!). Also ist $r_i = a_i/b_i$ für gewisse $(a_i, b_i) = 1$ mit $p \nmid b_i$. Gesucht ist ein $n_i \in \mathbb{Z}$ mit $|r_i - n_i|_p \leq p^{-i}$. Wir haben

$$\left|n_i - \frac{a_i}{b_i}\right|_p \leq p^{-i} \iff |b_i n_i - a_i|_p = |b_i n_i - a_i|_p \cdot \frac{1}{|b_i|_p} \leq p^{-i} \quad (\text{da} \quad p \nmid b_i)$$
$$\iff b_i n_i \equiv a_i \bmod p^i.$$

Wegen $(b_i, p^i) = 1$ ist die Kongruenz lösbar, und es folgt

$$|\alpha - n_i|_p = |(\alpha - r_i) + (r_i - n_i)|_p \leq |\alpha - r_i|_p + |r_i - n_i|_p \leq 2p^{-i}.$$

□

Satz 9.7

Sei $\alpha \in \mathbb{Z}_p$. Dann existiert eine eindeutige Cauchy-Folge $(a_n)_{n\in\mathbb{N}}$ mit $\overline{(a_n)}_{n\in\mathbb{N}} = \alpha$ derart, dass

$$a_n \in \mathbb{Z}, \quad 0 \leq a_n < p^n, \quad a_{n+1} \equiv a_n \bmod p^n \quad (n \in \mathbb{N}).$$

Beweis:

Nach Lemma 9.6 existiert $a_n \in \mathbb{Z}$ mit $|\alpha - a_n|_p \leq p^{-n}$. Wegen

$$|\alpha - (a_n + tp^n)|_p \leq \max(|\alpha - a_n|_p, |t \cdot p^n|_p) \leq \max(p^{-n}, p^{-n}) = p^{-n}$$

können wir o.B.d.A. $0 \leq a_n < p^n$ voraussetzen. Aus

$$|a_{n+1} - a_n|_p \leq \max(|a_{n+1} - \alpha|_p, |a_n - \alpha|_p) \leq p^{-n}$$

folgt $a_{n+1} \equiv a_n \bmod p^n$. Insbesondere ist $(a_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge mit $\overline{(a_n)}_{n\in\mathbb{N}} = \alpha$. Zum Beweis der Eindeutigkeit sei eine Folge $(a'_m)_{m\in\mathbb{N}}$ mit denselben Eigenschaften gegeben. Wir haben

$$|a'_m - \alpha|_p \leq p^{-n} \text{ für } m \geq m_0(n) \geq n.$$

Nach Voraussetzung gilt

$$a'_m \equiv a'_{m-1} \equiv \cdots \equiv a'_n \bmod p^n,$$

also

$$|a'_m - a'_n|_p \leq \max(|a'_m - a'_{m-1}|_p, \ldots, |a'_{n+1} - a'_n|_p) \leq p^{-n}.$$

Mit $|a_n - \alpha|_p \leq p^{-n}$ folgt

$$|a'_n - a_n|_p \leq \max(|a'_n - a'_m|_p, |a'_m - \alpha|_p, |\alpha - a_n|_p) \leq p^{-n},$$

d.h. $a_n \equiv a'_n \bmod p^n$. Wegen $0 \leq a_n,\ a'_n < p^n$ folgt $a_n = a'_n$.

□

Satz 9.8

Für $p \in \mathbb{P}$ ist

$$\mathbb{Q}_p \cong \left\{ \frac{b_{-k}}{p^k} + \frac{b_{-k+1}}{p^{k-1}} + \cdots + \frac{b_{-1}}{p} + b_0 + b_1 p + b_2 p^2 + \cdots :\ k \in \mathbb{Z},\ b_{-k} \neq 0,\ 0 \leq b_i < p \right\}$$

(d.h. jede p-adische Zahl wird durch eine Laurent-Reihe dargstellt), wobei ganz kanonisch mit Überträgen gerechnet wird.

Beweis:

Sei zunächst $\alpha \in \mathbb{Z}_p$, und sei $(a_n)_{n\in\mathbb{N}}$ die eindeutige Folge aus Satz 9.7. Wir setzen

$$a_1 =: b_0, \quad a_2 = a_1 + pb_1, \quad a_3 = a_2 + p^2 b_2, \ldots,$$

also $0 \leq b_n < p$ für alle $n \geq 0$. Einsetzen liefert

$$a_1 = b_0, \quad a_2 = b_0 + b_1 p, \quad a_3 = b_0 + b_1 p + b_2 p^2, \ldots,$$

also

$$\alpha = \lim_{n\to\infty} a_n = b_0 + b_1 p + b_2 p^2 + \cdots$$

Sei nun $\alpha \in \mathbb{Q}_p, \quad \alpha \neq 0$. Dann existiert ein $k \in \mathbb{Z}$ mit $|\alpha|_p = p^k$. Es folgt

$$\left|\alpha \cdot p^k\right|_p = |\alpha|_p \cdot \left|p^k\right|_p = p^k \cdot p^{-k} = 1,$$

d.h. $\alpha \cdot p^k \in \mathbb{Z}_p$ und

$$\alpha \cdot p^k = b_{-k} + b_{-k+1} p + b_{-k+2} p^2 + \cdots,$$

wobei $b_{-k} \neq 0$ (sonst $\left|\alpha \cdot p^k\right| < 1$). Es ergibt sich

$$\alpha = \frac{b_{-k}}{p^k} + \frac{b_{-k+1}}{p^{k-1}} + \cdots + b_0 + b_1 p + \cdots$$

Die Richtigkeit des Rechnens mit Überträgen ergibt sich leicht, indem zuerst Teilsummen dieser unendlichen Reihen verwendet werden und anschließend Grenzwerte bezüglich $|.|_p$ gebildet werden.

□

Beispiel: (vgl. Beispiel 9.2)
Wir berechnen näherungsweise $\sqrt{6}$ in $\mathbb{Q}_5$, d.h. wir lösen $x^2 = 6$ in $\mathbb{Q}_5$. Gesucht werden $a_0, a_1, a_2, \ldots \quad (0 \leq a_i \leq 4)$ mit $(a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots)^2 = 6 = 1 + 1 \cdot 5$.
Koeffizientenvergleich mod 5, mod 5^2, mod $5^3, \ldots$ liefert

$$a_0 = 1, a_1 = 3, a_2 = 0, a_3 = 4, \ldots \quad \text{oder} \quad a_0 = 4, a_1 = 1, a_2 = 4, a_3 = 0, \ldots.$$

Die Gleichung $x^2 = 6$ hat also in $\mathbb{Q}_5$ die beiden Lösungen

$$a = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + \cdots$$

und

$$-a = 4 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + \cdots$$

Ein Beispiel für die ungewohnten Konsequenzen des nicht-archimedischen Absolutbetrages gibt

Satz 9.9

Sei $(c_n)_{n \in \mathbb{N}_0}$ eine Folge über $\mathbb{Q}_p$. Dann gilt

$$\sum_{n=0}^{\infty} c_n \quad \text{ist konvergent} \iff \lim_{n \to \infty} c_n = 0.$$

Beweis:

„$\Longrightarrow$“
Sei $S_N := \sum_{n=0}^{N} c_n$, also existiert $\lim_{N\to\infty} S_N$. Es folgt

$$\lim_{n\to\infty} c_n = \lim_{n\to\infty} (S_n - S_{n-1}) = \lim_{n\to\infty} S_n - \lim_{n\to\infty} S_n = 0.$$

„$\Longleftarrow$“
Sei $m > n$. Dann ist

$$|S_m - S_n|_p = |c_{n+1} + c_{n+2} + \ldots + c_m|_p \leq \max(|c_{n+1}|_p, \ldots, |c_m|_p) \to 0$$

für $n \to \infty$. Also ist $(S_n)_{n\in\mathbb{N}}$ Cauchy-Folge und somit konvergent in $\mathbb{Q}_p$.

□