Elementare Zahlentheorie

Inoffizielles Skript
zur Vorlesung von Prof. Henk, WS 2016/17

Henning Seidler
henning.seidler@mailbox.tu-berlin.de

Inhaltsverzeichnis

1 Grundlagen **2**

2 Kongruenzen **10**

3 Kettenbrüche **23**

4 Summen von Quadraten **33**
4.1 Pythagoreische Tripel 36

5 Zahlentheoretische Funktionen **39**

6 Geometrie der Zahlen **46**

Wir beginnen mit einfachen Themen, wie dem Euklidischen Algorithmus, Primzahlen. Dann betrachten wir zahlentheoretische Funktionen, wie zum Beispiel die Anzahl oder die Summe der Teiler
Später wird es etwas mehr analytisch. Dort beschäftigen wir uns mit Grenzwertverhalten. Das heißt, wir suchen die Allgemeine Komplexität (im Sinne von Landau-Notation).
Dabei bleiben wir die meiste Zeit im Bereich der natürlichen Zahlen.
Zahlentheorie ist eine der ältesten Wissenschaften, bekannt schon in der Antike.
Eine Eigenschaft ist, dass viele Probleme sehr einfach zu formulieren sind, aber schwer zu lösen.

Beispiel (Ramanujan/Hardy). 1729 ist die kleinste Zahl, die sich auf zwei verschiedene Arten als Summe von dritten Potenzen schreiben lässt.

$$1729 = 12^3 + 1^3 = 10^3 + 9^3$$

Beispiel (Fermat). Die Gleichung $a^n + b^n = c^n$ hat für $n \geq 3$ keine nicht-triviale natürliche Lösung. Aufgestellt wurde es 1637 von Pierre de Fermat. Bewiesen wurde es erst 1997 von Andrew Wiles.

Beispiel (Summen von Quadraten). Wir können jede Zahl als Summe von Quadraten schreiben. Trivialerweise gilt $n = 1^2 + \ldots + 1^2$. Aber im Falle von Quadraten geht es besser: Wir können jede Zahl als Summe von 4 Quadraten schreiben. Bei höheren Potenzen wir es schwieriger. Es geht mit 9 dritten Potenzen und 19 vierten Potenzen. Bei höheren Potenzen kennt man nur Schranken.

Beispiel.
- Gibt es unendlich viele Primzahlzwillinge?
- Goldbach-Vermutung: Jede gerade Zahl ≥ 4 ist Summe von zwei Primzahlen.

1 Grundlagen

1.1 Notation. Bei uns gilt $0 \notin \mathbb{N}$, dafür haben wir $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Ansonsten haben wir $\mathbb{Z}, \mathbb{R}$ und $\mathbb{C}$ wie üblich.
Für Induktion verwenden wir folgende Axiomatik von Peano: Jedes $A \subseteq \mathbb{N}_0$ hat ein kleinstes Element.

1.2 Satz. *Sei $a \in \mathbb{N}$ und $b \in \mathbb{Z}$. Dann gibt es eindeutige $q, r \in \mathbb{Z}$ mit $b = qa + r$ und $0 \leq r < a$.*

Beweis. Existenz: Sei $D := \{b - ua \in \mathbb{N}_0 : u \in \mathbb{Z}\}$. Für $u = -b$ erhalten wir eine nicht-negative Zahl, also ist $D \neq \emptyset$. Also gibt es ein kleinstes Element $r = b - qa \in D$. Wäre $r \geq a$, so wäre $b - (q+1)a = r - a \geq 0$, also $b - (q+y)a \in D$, was ein Widerspruch zur Wahl von r ist.
Eindeutigkeit: Sei $b = q'a + r' = qa + r$ mit $0 \leq r, r' < a$. Dann ist $\{-a+1, \ldots, a-1\} \ni r - r' = (q' - q)a$ ein Vielfaches von a. Das kann nur $r - r' = (q' - q)a = 0$ sein, also $r = r'$ und $q = q'$. $\square$

1.3 Satz (b-adische Darstellung). *Sei $b \in \mathbb{N}$, $b \geq 2$. Dann hat jede natürliche Zahl $a \in \mathbb{N}_0$ eine eindeutige Darstellung der Form $a = \sum_{i=0}^{n} a_i b^i$ mit $0 \leq a_i < b$ und $a_n > 0$.*

Beweis. Existenz: Induktion nach a, für $a < b$ klar. Sei nun $b^n \leq a < b^{n+1}$. Nach Satz 1.2 gibt es $a_n, r \in \mathbb{Z}$ mit $a = a_n b^n + r$ und $0 \leq r < b^n$. Nach Induktionsvoraussetzung können wir nun r weiter zerlegen.
Eindeutigkeit: Angenommen, wir haben zwei verschiedene Darstellungen.

$$a = \sum_{i=0}^{n} a_i b^i = \sum_{j=0}^{m} a'_j b^j$$

Sei s der größte Index, an welchem die beiden verschieden sind. Dann gilt

$$0 = \sum_{i=0}^{n} a_i b^i - \sum_{j=0}^{m} a'_i b^i = \sum_{l=0}^{s} e_l b^l$$

Nun machen wir Induktion über s. Ist $s = 0$, so folgt $e_0 = 0$, also $a_i = a'_i$ ein Widerspruch. Sei $s \geq 1$. Dann ist

$$b^s \leq |e_s b^s| = \left| \sum_{l=0}^{s-1} e_l b^l \right| \leq \sum_{l=0}^{s-1} |e_s| b^l = \sum_{l=0}^{s-1} |a_l - a'_l| b^l \leq \sum_{l=0} s - 1(b-1)b^l = b^s - 1$$

womit wir auch in diesem Fall einen Widerspruch haben. $\square$

1.4 Definition. Seien $a, b \in \mathbb{Z}$, $a \neq 0$. Dann sagen wir "a ist Teiler von b", falls ein $c \in \mathbb{Z}$ existiert mit $ac = b$. Kurz $a \mid b$ (und wenn nicht, dann $a \nmid b$).

1.5 Bemerkung. (i) Wenn $a \mid b$, so $a \mid (bz)$ für alle $z \in \mathbb{Z}$.

(ii) $a \mid b$ und $b \mid c$ impliziert $a \mid c$.

(iii) $a \mid b$ und $a \mid c$ impliziert $a \mid (bx + cy)$ für alle $x, y \in \mathbb{Z}$.

(iv) Ist $a \mid b$ und $b \leq 0$, so $|a| \leq |b|$.

(v) Wenn $a \mid b$ und $b \mid a$, dann $|a| = |b|$.

1.6 Satz. *Seien $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$. Dann existiert eine eindeutige positive Zahl b mit $d \mid a$ und $d \mid b$ und d ist maximal mit dieser Eigenschaft. Das heißt, wenn $e \mid a$ und $e \mid b$, dann $e \mid d$. Dieses d heißt "größter gemeinsamer Teiler von a und b", kurz $d = \mathrm{ggT}(a, b)$.*
Ist $\mathrm{ggT}(a, b) = 1$, so heißen a und b teilerfremd.

Beweis. Konstruktiv mit wiederholter Anwendung von Satz 1.2. OBdA seien $a \geq b > 0$. Für $a = b$ ist $d = a = b$ und wir sind fertig, also nehmen wir an $a > b$.
Zur einheitlichen Notation setze $r_0 := a$ und $r_1 := b$. Nach Satz 1.2 gibt es eindeutige q_1, r_2 mit $a = q_1 r_1 + r_2$ und $0 \leq r_2 < b$. Für $r_2 = 0$ gilt $b \mid a$, also $d = b$ und wir sind fertig mit Bemerkung 1.5.
Andernfalls fahren wir fort mit r_1 und r_2. Dies liefert eine Folge von q_i, r_i mit $r_{i+1} < r_i$. Damit bricht dieses Verfahren irgendwann ab. Wir haben einen letzten Rest $r_k \neq 0$ und $r_{k+1} = 0$, also $r_{k-1} = q_k r_k$. Setze nun $d = r_k$.
Nun wissen wir $r_k \mid r_{k-1}$. Mit Bemerkung 1.5 teilt es die Linearkombination $r_{k-2} = q_{k-1} r_{k-1} + r_k$. Induktiv folgt $r_k \mid a$ und $r_k \mid b$.
Für die andere Richtung nehmen wir an $e \mid a$ und $e \mid b$. Dann folgt $e \mid (a - q_1 b) = r_2$. Induktiv folgt $e \mid r_i$ für alle i. Insbesondere gilt $e \mid r_k = d$. Daraus folgt mit Bemerkung 1.5 auch die Eindeutigkeit von d, da der ggT positiv ist. $\square$

1.7 Satz. *Seien $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$.*

(i) $\mathrm{ggT}(a, b) = \min\{ax + by :\in \mathbb{N} : x, y \in \mathbb{Z}\}$. *Insbesondere ist* $\{ax + by : x, y \in \mathbb{Z}\} = \mathrm{ggT(a, b)}\,\mathbb{Z}$.

(ii) Ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, c) = 1$, *so ist* $\mathrm{ggT}(a, bc) = 1$.

(iii) Gilt $a \mid bc$ und $\mathrm{ggT}(a, b) = 1$, *so folgt $a \mid c$.*

Beweis. (i) Sei $s = \min\{ax + by \in \mathbb{N} : x, y \in \mathbb{Z}\}$. Wir zeigen, dass s die beiden Eigenschaften aus Satz 1.6 erfüllt.
Sei $d_1 \mid a$ und $d_1 \mid b$, dann $d_1 \mid ax + by$ für alle x, y, also $d_1 \mid s$.
Angenommen $s \nmid a$. Mit Satz 1.2 erhalten wir $a = qs + r$ und $0 < r < s$. Sei nun $s = a\bar{x} + b\bar{y}$. Dann ist $r = a - sq = a - (a\bar{x} + b\bar{y})q = a(1 - \bar{x}q) + b(-\bar{y}q)$ eine kleinere Linearkombination.

$\supseteq$: Aus $\mathrm{ggT}(a,b) \mid a$ und $\mathrm{ggT}(a,b) \mid b$) folgt $\mathrm{ggT}(a,b) \mid ax+by$ für alle $x,y \in \mathbb{Z}$.
$\subseteq$: Sei $\mathrm{ggT}(a,b) = a\bar{x} + b\bar{y}$. Dann ist $\mathrm{ggT}(a,b)m = a(\bar{x}m) + b(\bar{y}m)$.

(ii) Sei $\mathrm{ggT}(a,b) = \mathrm{ggT}(a,c) = 1$. Dann existieren Koeffizienten mit $1 = ax_1 + by_1 = ax_2 + cy_2$. Multipliziert haben wir

$$1 = a(ax_1x_2 + cx_1y_2 + by_1x_2) + bc(y_1y_2)$$

Diese Linearkombination muss das Minimum sein, also der ggT.

(iii) Sei $a \mid bc$ und $\mathrm{ggT}(a,b) = 1$, also $1 = ax + by$. Dann ist $c = a \cdot (cx) + bc \cdot y$ und die rechte Seite ist durch a teilbar. □

Wir haben somit die ganzzahligen Linearkombinationen charakterisiert. Interessanter ist das Problem der natürlichen Kombinationen, für mehr als zwei Zahlen ist es immer noch nicht exakt gelöst. Die größte nicht-darstellbare Zahl aus einer gegebenen Menge heißt Frobenius-Zahl.
Wir können den ggT auch geometrisch interpretieren. Die Gleichung $ax + by = 0$ ist die Normalform einer Geraden in der Ebene. Nun schränken wir uns auf die Gitterpunkte ein, dann ist der ggT die minimale Verschiebung so, dass diese Gerade wieder durch einen Gitterpunkt geht.

1.8 Bemerkung. Man kann den ggT auf beliebig viele Argumente erweitern.

1.9 Notation. Eine positive Zahl $a \in \mathbb{N}$ mit $a \geq 2$ heißt Primzahl, falls sie nur die trivialen Teiler 1 und a hat. Die Menge der Primzahlen wird mit $\mathbb{P}$ bezeichnet.

1.10 Lemma. *(i) Jede ganze Zahl $a > 1$ lässt sich als Produkt von Primzahlen darstellen.*

(ii) Seien $p_1, \ldots, p_n \in \mathbb{P}$ und $p \mid \prod_{i=1}^n p_i$. Dann gilt $p = p_j$ für ein $j \in \{1, \ldots, n\}$.

Beweis. (i) Induktion über a; IA mit $a = 2$ ist klar.
Sei $a \geq 4$ keine Primzahl. Dann hat a einen nicht-trivialen Teiler b mit $1 < b < a$, also $a = bc$. Nach IV sind b und c Produkte von Primzahlen, also auch a.

(ii) Sei $p \neq p_1, \ldots, p_n$. Es gilt $\mathrm{ggT}(p, p_i) = 1$ für $i = 1, \ldots, n-1$. Nach Satz 1.7.((ii)) ist dann auch $\mathrm{ggT}\left(p, \prod_{i=1}^{n-1} p_i\right) = 1$. Mit Satz 1.7.((iii)) gilt also $p \mid p_n$, und somit $p = p_n$. □

1.11 Satz. *Jede Zahl $a \geq 2$ lässt sich eindeutig (bis auf Reihenfolge) darstellen als Produkt von Primzahlen.*

Beweis. Sei $a \geq 4$ die kleinste Zahl mit zwei verschiedenen Darstellungen

$$a = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} p'_j$$

Dann darf wegen der Minimalität keine Primzahl auf beiden Seiten vorkommen. Andererseits ist $p_1 \mid \prod p'_j$, also muss nach Lemma 1.10 es ein s geben mit $p_1 = p'_s$ und wir haben einen Widerspruch. □

1.12 Proposition. *Seien $a, b \in \mathbb{N}$ mit*

$$a = \prod_{p \in \mathbb{P}} p^{\alpha_p} \qquad b = \prod_{p \in \mathbb{P}} p^{\beta_p} \qquad \text{mit } \alpha_p, \beta_p \in \mathbb{N}_0$$

(i) Es ist $b \mid a$ genau dann, wenn $\beta_p \leq \alpha_p$ für alle $p \in \mathbb{P}$.

(ii) Es gilt $\mathrm{ggT}(a, b) = \prod p^{\min(\alpha_p, \beta_p)}$.

(iii) Die Anzahl der Teiler ist

$$\tau(a) := \#\{d \in \mathbb{N} : d \mid a\} = \prod (\alpha_p + 1)$$

(iv) Die Summe der Teiler ist

$$\sigma(a) := \sum_{d \mid a} d = \prod_{p \in \mathbb{P}} \frac{p^{\alpha_p + 1} - 1}{p - 1}$$

Beweis. (i) Rückrichtung klar, sei also $\beta_{p'} > \alpha_{p'}$ und $a = bc$. Dann ist $a \cdot p'^{-\alpha_{p'}} = bc \cdot p'^{-\alpha_{p'}}$. Der Faktor p' kommt nun rechts vor, aber nicht links, was der Eindeutigkeit widerspricht.

(ii) Sei $\mathrm{ggT}(a, b) = \prod p^{\gamma_p}$. Nach (i) folgt $\gamma_p \leq \alpha_p, \beta_p$. Aber das Minimum liefert einen Teiler.

(iii) Kombinatorik, wir haben je Teiler $\alpha_p + 1$ Möglichkeiten. Nach Eindeutigkeit der Primfaktorzerlegung liefert jede Möglichkeit auch eine neue Zahl.

(iv) Sei $a = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ die Zerlegung. Dann ist

$$\sigma(a) = \sum_{\gamma_1 = 0}^{\alpha_1} \dots \sum_{\gamma_m = 0}^{\alpha_m} \prod_{i=1}^{m} p_i^{\gamma_i} = \left(\sum_{\gamma_1 = 0}^{\alpha_1} p_1^{\gamma_1} \right) \cdot \left(\sum_{\gamma_m = 0}^{\alpha_m} p_m^{\gamma_m} \right) = \prod_{p \in \mathbb{P}} \frac{p^{\alpha_p + 1} - 1}{p - 1}. \qquad \square$$

1.13 Satz. *Es gibt unendlich viele Primzahlen der Form $4k - 1$.*

Beweis. Angenommen wir haben nur endlich viele Primzahlen $q_1, \dots, q_n$ dieser Form. Setze $N := 4(q_1 \cdot \ldots \cdot q_n) - 1$. Dann ist N ungerade, also jeder Primfaktor von der Form $4k \pm 1$. Wegen $N \bmod 4 = 3$ muss mindestens einer der Faktoren die Form $4k - 1$ haben, also eines der q_j sein. Dann folgt mit $q_j \mid -1$ der Widerspruch. $\square$

Wenn man nur unendlich viele haben möchte:

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p \in \mathbb{P}} \left(\sum_{l=0}^{\infty} \left(\frac{1}{p} \right)^l \right) = \prod_{p \in \mathbb{P}} \frac{1}{1 - 1\frac{1}{p}} < \infty \quad \lightning$$

Man kann Satz 1.13 verallgemeinern. Seien a, b teilerfremd. Dann enthält die arithmetische Folge $am + b$ für $m \in \mathbb{Z}$ unendlich viele Primzahlen (bewiesen durch Dirichlet).

1.14 Satz. *Seien $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$. Dann gibt es eine eindeutige Zahl $m \in \mathbb{N}$ mit*

(i) $a \mid m$ *und* $b \mid m$

(ii) Wenn $a \mid \bar{m}$ *und* $b \mid \bar{m}$*, dann* $m \mid \bar{m}$*.*

Diese Zahl heißt kleinstes gemeinsames Vielfaches $\mathrm{kgV}(a, b)$.
Haben wir die Primfaktorzerlegungen $a = \prod_{p \in \mathbb{P}} p^{\alpha_p}$ *und* $b = \prod_{p \in \mathbb{P}} p^{\beta_p}$*, so gilt* $\mathrm{kgV}(a, b) = \prod p^{\max(\alpha_p, \beta_p)}$.

1.15 Korollar. *(i) Seien $a, b \in \mathbb{Z}$ mit $ab \neq 0$. Dann gilt $|ab| = \mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b)$, denn*

$$\prod p^{\alpha_p + \beta_p} = \prod p^{\min(\alpha_p, \beta_p)} \cdot \prod p^{\max(\alpha_p, \beta_p)}$$

(ii) Sei $a \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$ mit $m_1 \mid a$ und $m_2 \mid a$. Dann gilt $\mathrm{kgV}(m_1, m_2) \mid a$.

1.16 Bemerkung. Für mehrere Argumente kann $\mathrm{kgV}(a_1, \ldots, a_n)$ rekursiv definiert werden. Aber dann gilt Korollar 1.15.(i) nicht mehr.

Bemerkung. Diese Konzepte können wir auch nutzen, wenn wir uns für ganzzahlige Lösungen von Gleichungen interessieren. Betrachte $ax + by = c$ mit $a, b, c \in \mathbb{Z}$. Dies hat eine Lösung genau dann, wenn $\mathrm{ggT}(a, b) \mid c$; sei also $\mathrm{ggT}(a, b) \cdot k = c$.
Eine Lösung erhalten wir mit erweitertem Euklidischem Algorithmus. Dies liefert $a\bar{x} + b\bar{y} = k$, also die Lösung $(k\bar{x}, k\bar{y})$. Für die Menge aller Lösungen betrachten wir den Kern. Erst einmal liegt $(-b, a)$ im Kern, aber wir suchen den kleinsten ganzzahligen Vektor im Kern. Diesen erhalten wir, indem wir durch den ggT teilen.

1.17 Definition. Sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann heißen a und b *kongruent modulo m*, falls $m \mid a - b$. Geschrieben $a \equiv b \mod m$.

1.18 Proposition. *(i) Es gilt $a \equiv b \mod m$ genau dann, wenn a und b bei Division durch m den selben Rest lassen.*

(ii) Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann $a \equiv c \mod m$.

(iii) Wenn $a_i \equiv b_i \mod m$, dann ist $(a_1 \pm a_2) \equiv (b_1 \pm b_2) \mod m$ und $a_1 a_2 \equiv b_1 b_2 \mod m$.

(iv) Wenn $a \equiv b \mod m$, dann $ka \equiv kb \mod m$.

(v) Sei $ka \equiv kb \mod m$. Dann ist $a \equiv b \mod \frac{m}{\mathrm{ggT}(k,m)}$.

(vi) Sei $a \equiv b \mod m_i$ für $1 \leq i \leq n$. Dann ist $a \equiv b \mod \mathrm{kgV}(m_1, \ldots, m_n)$.

(vii) Wenn $a \equiv b \mod m$, dann $\mathrm{ggT}(a, m) = \mathrm{ggT}(b, m)$.

Beweis. (i) Sei $a = lm + r$ und $b = \bar{l}m + \bar{r}$ mir $0 < r, \bar{r} < m$. Dann ist $a - b = (l - \bar{l})m + (r - \bar{r})$ durch m teilbar. Also gilt $m \mid (r - \bar{r}) \in (-m, m)$, also $r - \bar{r} = 0$.

(ii) Folgt sofort mit (i).

(iii) Folgt sofort mit (i).

(iv) Induktion über k mittels (iii).

(v) Sei $ka - kb = lm$ und $d = \mathrm{ggT}(m, k)$. Dann ist $l \cdot \frac{m}{d} = (a - b) \cdot \frac{k}{d}$. Nun aber ist $\mathrm{ggT}\left(\frac{m}{d}, \frac{k}{d}\right) = 1$, also folgt mit Definition 1.17, dass $\frac{m}{d} \mid (a - b)$.

(vi) klar

(vii) Sei $a - b = lm$. Dann gilt $d \mid a \wedge d \mid m \Leftrightarrow d \mid b \wedge d \mid m$. □

Polynome in einer Variablen können wir charakterisieren mit $f(x) = \sum\limits_{k=0}^{n} a_k x^k$. Bei mehreren Variablen haben wir

$$f(x_1, \ldots, x_n) = \sum_{\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n} a_\alpha x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$$

und wieder einmal interessieren wir uns nur für ganzzahlige Koeffizienten.

1.19 Satz. *Sei $f \in \mathbb{Z}[x_1, \ldots, x_n]$ ein Polynom (in $x_1, \ldots, x_n$ mit ganzzahligen Koeffizienten). Seien $a_i, b_i \in \mathbb{Z}$ mit $a_i \equiv b_i \mod m$. Dann gilt $f(a_1, \ldots, a_n) \equiv f(b_1, \ldots, b_n) \mod m$.*

Beweis. induktiv, über wiederholte Anwendung von Proposition 1.18.(iii) □

1.20 Korollar. *$a \in \mathbb{N}$ ist durch 9 (3) teilbar genau dann, wenn die Quersumme durch 9 (3) teilbar ist. $a \in \mathbb{N}$ ist durch 11 teilbar genau dann, wenn die alternierende Quersumme durch 11 teilbar ist.*

Beweis. Sei $a = \sum c_i \cdot 10^i$. Setze $f(x) := \sum c_i x^i$. Dann ist $f(10) = a$ und $f(1)$ die Quersumme von a und $f(-1)$ die alternierende Quersumme. Nach Satz 1.19 ist $f(10) \equiv f(1) \mod 9$ und $f(10) \equiv f(-1) \mod 11$. □

1.21 Bemerkung. Die Relation $(\cdot \equiv \cdot \mod m$ ist eine Kongruenz auf $(\mathbb{Z}, +, -(\cdot), \cdot)$. Die Äquivalenzklassen heißen Restklassen und lassen sich darstellen als $a + m\mathbb{Z}$. Es gilt $a + m\mathbb{Z} = c + m\mathbb{Z} \Leftrightarrow a \equiv c \mod m$.

1.22 Notation. Wenn m im Kontext klar ist, schreibe $\overline{a} := a + m\mathbb{Z}$ und $\mathbb{Z}_m := \{\overline{a} : a \in \mathbb{Z}\}$.

1.23 Definition. Sei $m \in \mathbb{Z}$. Eine Menge $\{a_1, \ldots, a_m\}$ heißt vollständiges Restesystem, falls $\mathbb{Z}_m = \{\overline{a_i} : i = 1, \ldots, m\}$. Äquivalent dazu ist $a_i \not\equiv a_j \mod m$ für alle $i \neq j$.

1.24 Satz. *Sei $m \in \mathbb{N}$ und sei $\{a_1, \ldots, a_m\}$ ein vollständiges Restesystem. Seien $a, k \in \mathbb{Z}$.*

(i) *$\{a_i + a : i = 1, \ldots, m\}$ ist ein vollständiges Restesystem.*

(ii) *$\{ka_i : i = 1, \ldots, m\}$ ist ein vollständiges Restesystem genau dann, wenn $\mathrm{ggT}(k, m) = 1$.*

Beweis. (i) folgt mit Proposition 1.18.(iii). (ii) folgt mit Proposition 1.18.(v). □ mehr?

1.25 Bemerkung. Sei $m \in \mathbb{N}$. Zusammen mit den Verknüpfungen $\overline{a} + \overline{b} \mapsto \overline{a+b}$ und $\overline{a} \cdot \overline{b} \mapsto \overline{ab}$ ist $\mathbb{Z}_m$ ein kommutativer Ring mit Eins. Für Wohldefiniertheit siehe Lineare Algebra.

1.26 Satz. *Sei $m \in \mathbb{N}$, $\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$. Dann existiert genau ein $b \in \mathbb{Z}_m$ mit $a \cdot b = 1$ genau dann, wenn* $\mathrm{ggT}(a, m) = 1$.

Beweis. Es ist $ab = 1 \Leftrightarrow \exists l \in \mathbb{Z}.ab - lm = 1 \Leftrightarrow \mathrm{ggT}(a, m) = 1$ mit Satz 1.7. Für die Eindeutigkeit nehmen wir an $ab = 1 = ac$. Dann ist $a(b - c) = 0$ und da a und m teilerfremd sind,folgt $b - c = 0$, also $b = c$. □ overline

1.27 Bemerkung. Sei $m \in \mathbb{N}$. Dann ist $(\mathbb{Z}_m, +, \cdot)$ ein Körper genau dann, wenn m eine Primzahl ist. Wir brauchen nämlich nur noch Invertierbarkeit und die erhalten wir mit Bemerkung 1.27. Falls m echte Teiler hat, so hat $\mathbb{Z}_m$ Nullteiler.

1.28 Definition. Sei $m \in \mathbb{N}, m \geq 2$. Die Menge $\{a_1, \ldots, a_k\} \subseteq \mathbb{Z}$ heißt reduziertes Restesystem von $\mathbb{Z}_m$, falls

$$\mathbb{Z}_m^* := \{\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\} : \exists b \in \mathbb{Z}_m.\overline{a} \cdot \overline{b} = \overline{1}\} = \{\overline{a_i} : i = 1, \ldots, k\}$$

und $\overline{a_i} \neq \overline{a_j}$. $(\mathbb{Z}_m^*, \cdot)$ ist die Gruppe der Einheiten.

1.29 Bemerkung. Sei $m \in \mathbb{N}, \geq 2$.

(i) $a \in \mathbb{Z}_m^* \Leftrightarrow \mathrm{ggT}(a, m) = 1$

(ii) $\{a \in \{1, \ldots, -1\} : \mathrm{ggT}(a, m) = 1\}$ ist ein reduziertes Restesystem.

1.30 Definition. Die Funktion $\phi : \mathbb{N} \to \mathbb{N}$ mit $\phi(m) = \#\{a \in \mathbb{Z}_m : \mathrm{ggT}(a, m) = 1\}$ heißt (Eulersche) ϕ-Funktion.

1.31 Satz. *Sei $m \in \mathbb{N}, m \geq 2$ und sei $\{a_1, \ldots, a_k\}$ ein reduziertes Restesystem von $\mathbb{Z}_m$, sei $l \in \mathbb{Z}$. Dann ist $\{la_1, \ldots, la_k\}$ ein reduziertes Restesystem genau dann, wenn* $\mathrm{ggT}(l, m) = 1$.

Beweis. Falls $\mathrm{ggT}(l, m) > 1$, so ist auch $\mathrm{ggT}(la_1, m) > 1$, also ist la_1 nicht invertierbar. Wenn $\mathrm{ggT}(a_i, m) = 1 = \mathrm{ggT}(l, m)$, dann ist $\mathrm{ggT}(la_i, m) = 1$, also invertierbar. Mit Proposition 1.18.(v) ist $la_i \not\equiv la_j \mod m$ für$i \neq j$. □

1.32 Bemerkung. (i) $\phi(p) = p - 1$, falls p eine Primzahl

(ii) $\phi(m) = |\mathbb{Z}_m^*|$

1.33 Theorem. *Sei $m \in \mathbb{N}, a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$. Dann ist $a^{\phi(m)} \equiv 1 \mod m$. Der Spezialfall für Primzahlen ist $a^{p-1} \equiv 1 \mod p$ ist der* Kleine Satz von Fermat.

Beweis. Sei $a_1, \ldots, a_{\phi(m)}$ ein reduziertes Restesystem von $\mathbb{Z}_m$. Wegen $\mathrm{ggT}(a, m) = 1$ ist auch $\{a \cdot a_i : i = 1, \ldots, \phi(m)\}$ ein reduziertes Restesystem. Bis auf Reihenfolge stehen

dort die gleichen Reste. Das heißt, für jedes $i \leq \phi(m)$ existiert ein $j \leq \phi(m)$ mit $aa_i \equiv a_j \mod m$. Dann ist

$$\prod a_i \equiv \prod (aa_i) \equiv a^{\phi(m)} \cdot \prod a_i \mod m$$
$$\Rightarrow 1 \equiv a^{\phi(m)} \mod m \qquad \text{nach Proposition 1.18.(v)} \qquad \square$$

1.34 Bemerkung (Fermats (Nicht-)Primzahltest). Gegeben eine Zahl $n \in \mathbb{N}$. Wähle ein $a \in \{2, \ldots, n-1\}$. Wenn $\mathrm{ggT}(a, n) \neq 1$, dann ist n keine Primzahl. Ist $a^{n-1} \not\equiv 1 \mod n$, so ist n keine Primzahl. Andernfalls haben wir keine Information.
Zahlen mit a^{n-1} für alle $a \in \mathbb{Z}_n^*$ heißen Carmichael-Zahlen. Davon gibt es unendlich viele, sodass sich der Test nicht ohne Weiteres retten lässt.

1.35 Definition. Eine Funktion $f : \mathbb{N} \to \mathbb{C}$ heißt multiplikativ, falls $f(mn) = f(m) \cdot f(n)$ falls $\mathrm{ggT}(n, m) = 1$.

1.36 Satz. *Die ϕ-Funktion ist multiplikativ.*

Beweis. Es ist $\phi(1) = 1$. Seien also $m, n \geq 2$ teilerfremd. Wir wissen $\mathrm{ggT}(a, mn) = 1 \Leftrightarrow \mathrm{ggT}(a, m) = \mathrm{ggT}(a, n) = 1$ nach Satz 1.7. Wir sind also an Zahlen $a \in \{1, \ldots, mn-1\}$ interessiert, die teilerfremd sind mit m und n. Wir betrachten dazu die $n \times m$-Matrix A mit $a_{ij} = (i-1)m + j - 1$. Jede Spalte hat bezüglich m einen einheitlichen Rest, sogar noch stärker, sie haben einen einheitlichen ggT nach Proposition 1.18. Es gibt also $\phi(m)$ Spalten, mit Einträgen, die teilerfremd zu m sind. Diese enthalten nun alle Zahlen $a \in \{0, \ldots, nm-1\}$ mit $\mathrm{ggT}(a, m) = 1$. Wegen $\mathrm{ggT}(n, m) = 1$ ist aber auch jede Spalte ein vollständiges Restesystem modulo n, nach Satz 1.24. Davon sind jeweils $\phi(n)$ Einträge teilerfremd zu n. Damit haben wir $\phi(m) \cdot \phi(n)$ Einträge, die zu m und n teilerfremd sind, also teilerfremd zu $m \cdot n$. $\square$

1.37 Korollar.

$$m = \prod p^{m_p} \implies \phi(m) = \prod \phi\left(p^{m_p}\right) = \prod_{p|m} (p-1)p^{m_p - 1} = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

Beweis. Für Primzahlpotenzen gilt: $\phi(p^k) = p^k - p^{k-1}$, denn wir entfernen alle Vielfachen von p, also p^{k-1} viele Elemente. $\square$

1.38 Satz. *Für $n \in \mathbb{N}$ gilt $\sum_{d|n} \phi(d) = n$.*

Beweis. Seien $d_1, \ldots, d_k$ alle Teiler von n. Für $1 \leq i \leq k$ betrachte die Mengen $M_i := \{m \in \{1, \ldots, n\} : \mathrm{ggT}(m, n) = d_i\}$. Die Mengen sind paarweise disjunkt, und decken alles ab; das heißt die bilden eine Partition. Daraus folgt $n = \sum |M_i|$. Weiterhin gilt $\mathrm{ggT}(m, n) = d_i \Leftrightarrow \mathrm{ggT}\left(\frac{m}{d_i}, \frac{n}{d_i}\right) = 1$. Also ist

$$|M_i| = \#\left\{1 \leq k \leq \frac{n}{d_i} : \mathrm{ggT}\left(k, \frac{n}{d_i}\right) = 1\right\} = \phi\left(\frac{n}{d_i}\right)$$

Damit gilt

$$n = \sum |M_i| = \sum_{l=1}^{k} \phi\left(\frac{n}{d_i}\right) = \sum_{l=1}^{k} \phi(d_i) \qquad \square$$

2 Kongruenzen

2.1 Satz. *Sei $m \in \mathbb{N}$.*

(i) Seien $a, b \in \mathbb{Z}$. Dann ist $ax \equiv b \mod m$ lösbar genau dann, wenn $\mathrm{ggT}(a, m) \mid b$. In diesem Fall gibt es $\mathrm{ggT}(a, m)$ viele Lösungen, die verschieden modulo m sind.

(ii) Seien $a_1, \ldots, a_n, b \in \mathbb{Z}$. Dann ist $\sum a_i x_i \equiv b \mod m$ lösbar genau dann, wenn $\mathrm{ggT}(a_1, \ldots, a_n, m) \mid b$. Dann gibt es $\mathrm{ggT}(a_1, \ldots, a_n, m) \cdot m^{n-1}$ viele Lösungen, die verschieden modulo m sind.

Beweis. (i) Die Kongruenz $ax \equiv b \mod b$ ist lösbar, genau dann, wenn es $x, y \in \mathbb{Z}$ gibt mit $ax - my = b$. Nach Satz 1.7.(i) ist dies äquivalent zu $\mathrm{ggT}(a, m) \mid b$.

Setze $d := \mathrm{ggT}(a, m)$. Haben wir eine Lösung x, so ist auch $\frac{a}{d} \cdot x \equiv \frac{b}{d} \mod \frac{m}{d}$, was wir schreiben als $a'x \equiv b' \mod m'$ mit $\mathrm{ggT}(a', m') = 1$. Jetzt betrachten wir $a', 2a', \ldots, m'a'$. Dabei gilt $ia' \not\equiv ja' \mod m'$ für $i \neq j$, nach Proposition 1.18. Damit muss in dieser Reihe jeder Rest modulo m' genau einmal vorkommen. Also gibt es ein eindeutiges $l \in \{1, \ldots, m\}$ mit $a'l \equiv b' \mod m'$. Also hat $a'x \equiv b' \mod m'$ genau eine Lösung modulo m', nämlich

$$l + m'\mathbb{Z} = \bigcup_{i=0}^{d-1} (l + im' + m\mathbb{Z})$$

(ii) Dass Lösbarkeit äquivalent ist zu $\mathrm{ggT}(a_1, \ldots, a_n, m) \mid b$ folgt nach Übungsblatt 1. Für die Anzahl der Lösungen machen wir Induktion nach n. Den Fall $n = 1$ haben wir bereits in (i).

Erneut setze $d := \mathrm{ggT}(a_1, \ldots, a_n, m)$ und $a'_i := \frac{a_i}{d}$, sowie $b' := \frac{b}{d}$ und $m' := \frac{m}{d}$. Dann betrachten wir

$$a'_1 x_1 + \ldots + a'_n x_n \equiv b' \mod m' \tag{1}$$

Sei nun $d' := \mathrm{ggT}(a'_1, \ldots, a'_{n-1}, m)$ (ohne a'_n). Eine Lösung $x_1, \ldots, a_n$ von (1) erfüllt

$$\sum_{i=1}^{n-1} a'_i x_i + a_n * x_n \equiv b' \mod d'$$

da $d' \mid m'$. Weil d' die Summe teilt, folgt

$$a'_n x_n \equiv b' \mod d' \tag{2}$$

Wegen $\mathrm{ggT}(a'_1, \ldots, a'_n, m) = 1$ folgt $\mathrm{ggT}(a'_n, d') = 1$. Nach (i) hat (2) eine eindeutig Lösung modulo d' und genau $\frac{m'}{d'}$ verschiedene Lösungen modulo m'. Einsetzen dieser Lösungen in (1) ergibt eine lineare Kongruenz in $n - 1$ Variablen. Dieses System hat nach Induktion genau $d'(m')^{n-2}$ Lösungen modulo m'. Das heißt (1) hat genau $\frac{m'}{d'} \cdot d'(m')^{n-2} = m'^{n-1}$ viele verschiedene Lösungen.

Für jede Lösung $x_1, \ldots, x_n$ von (1) sind auch $(x_i + k_i m')_{i=1,\ldots,n}$ Lösungen, welche für $0 \leq k_i \leq d - 1$ modulo m verschieden sind. Damit ist die Anzahl der Lösungen $d^n \cdot m'^{n-1} = d \cdot m^{n-1}$. □

Beispiel. Betrachte $43x \equiv 60 \mod 98$. Dabei gilt $\mathrm{ggT}(34, 98) = 2 \mid 60$. Daraus folgt, es gibt 2 Lösungen modulo 98. Um diese zu erhalten, lösen wir $17x \equiv 30 \mod 49$, was die (eindeutige) Lösung $x = -4 \equiv 45$ hat. Somit hat unser ursprüngliches System die Lösungen $x = 45$ und $x = 94$.

Bemerkung. Wir haben gezeigt, wie man konkrete Lösungen finden kann. Aber eine andere Fragestellung ist eine effiziente Darstellung aller Lösungen. Wenn wir allein die Kongruenz $\sum a_i x_i \equiv 0 \mod m$ betrachten, dann suchen wir eine ganzzahlige Basis, deren Größe polynomiell in m beschränkt ist.

Als nächstes interessieren wir uns dafür, mehrere Kongruenzen simultan zu lösen. Dazu betrachten wir $a_i x \equiv b_i \mod m_i$ für $i = 1, \ldots, n$.

2.2 Satz (Chinesischer Restsatz). *Seien $m_1, \ldots, m_n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{Z}$.*

(i) Ist $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i \neq j$, dann hat das System der linearen Kongruenzen $X \equiv c_i \mod m_i$ genau eine Lösung modulo $\prod m_i$.

(ii) $x \equiv c_i \mod m_i$ ist lösbar genau dann, wenn $\mathrm{ggT}(m_i, m_j) \mid (c_i - c_j)$ für alle $i \neq j$. In diesem Fall ist die Lösung eindeutig modulo $\mathrm{kgV}(m_1, \ldots, m_n)$.

Beweis. Seien $x, \bar{x}$ Lösungen dieses Systems. Dann ist $x - \bar{x} \equiv 0 \mod m_i$ für alle i und somit $x \equiv \bar{x} \mod \mathrm{kgV}(m_1, \ldots, m_n)$. Damit haben wir die Eindeutigkeit der Lösung, falls sie existiert.
Beachte $\mathrm{kgV}(m_1, \ldots, m_n) = \prod m_i$ falls $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i \neq j$.

(i) Induktion über n, wobei $n = 1$ klar ist.
Nach Induktionsvoraussetzung sind die ersten $n - 1$ Kongruenzen eindeutig modulo $M := \prod_{i=1}^{n-1} m_i$ lösbar. Also muss eine Lösung die zwei Kongruenzen $x \equiv c_n \mod m_n$ und $x \equiv c \mod M$ erfüllen. Das heißt, es existiert ein y mit $x \equiv c_n + m_n y \equiv c \mod M$ sein. Dies reduziert sich wiederum auf die einfache Gleichung $m_n y \equiv c - c_n \mod M$. Nach Satz 2.1.(i) und Voraussetzung $\mathrm{ggT}(m_n, M) = 1$ folgt, dass dies eine eindeutige Lösung modulo M hat. Sei dies $y = \bar{c} + M\mathbb{Z}$. Daraus folgt $x = c_n + m_n \bar{c} + m_n M\mathbb{Z} = \tilde{c} + (m_1 \cdot \ldots \cdot m_n)\mathbb{Z}$ ist die Restklasse aller Lösungen.

(ii) Zurückführen auf (i).
$\Rightarrow$: Sei $x \equiv c_i \mod m_i$, dann existieren y_i mit $x = c_i + y_i m_i$ für $1 \leq i \leq n$. Es muss also gelten $c_i + y_i m_i = c_j + m_j y_j$ für alle $i \neq j$. Damit haben wir $m_i y_i = (c_j - c_i) + m_j y_j$. Dies liefert die Kongruenz $m_i x \equiv c_j - c_i \mod m_j$ und nach (i) ist dies lösbar genau dann, wenn $\mathrm{ggT}(m_i, m_j) \mid (c_j - c_i)$.
$\Leftarrow$: Seien $m_i = \prod p^{\alpha_{p,i}}$ die Primfaktorzerlegungen der m_i. Insbesondere ist

$$\mathrm{kgV}(m_1, \ldots, m_n) = \prod_{p \in \mathbb{P}} p^{\max\{\alpha_{p,i} : 1 \leq i \leq n\}}$$

Es gilt $x \equiv c_i \mod m_i$ genau dann, wenn $x \equiv c_i \mod p^{\alpha_{p,i}}$ für alle $p \in \mathbb{P}$ und $\alpha_{p,i} \geq 1$. Sei $p \in \mathbb{P}$ und $\alpha_{p,i} \geq p\alpha_{p,j} \geq 1$. Dann haben wir die beiden Kongruenzen $x \equiv c_i \mod p^{\alpha_{p,i}}$ und $x \equiv c_j \mod p^{\alpha_{p,j}}$. Nach Annahme ist $p^{\alpha,j} \mid \mathrm{ggT}(m_i, m_j) \mid (c_j - c_i)$. Daraus folgt $c_i \equiv c_j \mod p^{\alpha_{p,j}}$. Da auch $x \equiv c_i \mod p^{\alpha_{p,j}}$ gilt, folgt $x \equiv c_j$

mod $p^{\alpha_{p,j}}$. Das heißt, eine Lösung von $x \equiv c_i \mod p^{\alpha_{p,i}}$ ist auch eine Lösung von $x \equiv c_j \mod p^{\alpha_{p,j}}$ für $\alpha_{p,j} \leq \alpha_{p,i}$. (***) Sei also P die Menge aller Primzahlen, die in einem der m_i vorkommen und sei $i_p \in \{1, \ldots, n\}$ für $p \in P$ ein Index mit $\alpha_{p,i_p} = \max\{\alpha_{p,i} : 1 \leq i \leq n\}$. Wegen (***) reich es, das System $x \equiv c_{i,p} \mod p^{\alpha_{p,i_p}}$ für $p \in P$ zu betrachten. Nach (i) hat dieses System genau eine Lösung modulo $\prod_{p \in P} p^{\alpha_{p,i_p}} = \mathrm{kgV}(m_1, \ldots, m_n)$. □

Beispiel. Betrachte das System

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 5 \mod 8 \\ x &\equiv 11 \mod 17 \end{aligned}$$

Aus den ersten beiden folgt $x = 3t + 1 \equiv 5 \mod 8$, mit der Lösung $t = 4$, also $x \in 13 + 24\mathbb{Z}$. Weiter geht es mit $x = 13 + 24u \equiv 11 \mod 17$ mit der Lösung $u = 7$. Somit erhalten wir $x = 13 + 24 \cdot 7 = 181$ modulo 408.

2.3 Notation. Seien $f, g \in \mathbb{Z}[x]$ mit $f = \sum a_i x^i$ und $g = \sum b_i x^i$, sowie $m \in \mathbb{N}$. Wir schreiben $f \equiv g \mod n$, falls $a_i \equiv b_i$ für alle i gilt.

Beispiel. Es gilt $(x + a)^2 \equiv x^2 + a^2 \mod 2$. Andererseits gilt $a^3 \equiv a \mod 3$ für alle $a \in \mathbb{Z}$ (kleiner Fermat), aber dies gilt nicht als Polynom: $x^3 \not\equiv x \mod 3$.

- $a^7 + a^4 + a \equiv 0 \mod 3 \Leftrightarrow a + a^2 + a \equiv 0 \mod 3$, da wir alle Potenzen ≥ 3 verringern können.
- $x^2 - x \mod 6$ hat die Nullstellen $\bar{0}, \bar{1}, \bar{3}$ und $\bar{4}$. wozu?

2.4 Bemerkung. Sei $f \in \mathbb{Z}[x]$, $m \in \mathbb{N}, a \in \mathbb{Z}$ mit $f(a) \equiv 0 \mod m$.

(i) Es gilt $f(a + km) \equiv 0 \mod m$ für alle $k \in \mathbb{Z}$. (siehe Satz 1.19)

(ii) Sei $g \in \mathbb{Z}[x]$ mit $f \equiv g \mod m$. Dann ist $g(a) \equiv 0 \mod m$.

2.5 Satz. *Sei $f \in \mathbb{Z}[x]$, $m \in \mathbb{N}$ und sei a eine Lösung von $f(x) \equiv 0 \mod m$, das heißt $f(a) \equiv 0 \mod m$. Dann gibt es ien $g \in \mathbb{Z}[x]$ mit $f(x) \equiv (x - a)g(x) \mod m$.*

Beweis. Wir teilen f mit Rest durch $(x - a)$. Dies liefert $g \in \mathbb{Z}[x]$ und $r \in \mathbb{Z}$ mit $f = (x - a)g + r$. Insbesondere gilt diese Gleichheit modulo m. Einsetzen von a liefert die Bedingung $0 \equiv f(a) \equiv (a - a)g(a) + r \mod m$, und damit $r \equiv 0 \mod m$. Damit ist $f(x) \equiv (x - a)g(x) \mod m$. □

2.6 Satz. *sei $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, $p \in \mathbb{P}$ und sei $\mathrm{ggT}(a_n, p) = 1$. Dann hat die Kongruenz $f(x) \equiv 0 \mod p$ höchstens n verschiedene Lösungen modulo p.*

Beweis. Induktion über n: Der Fall $n = 1$ folgt aus Satz 2.1.(i).
IS: Sei $n \geq 2$ und $f(a) \equiv 0 \mod p$. Nach Satz 2.5 existiert ein $g \in \mathbb{Z}[x]$ mit $f(x) \equiv (x - a)g(x) \mod p$. Für jede andere Lösung $f(c) \equiv 0 \mod p$ mit $c \not\equiv a \mod p$ gilt nun $(c - a)g(c) \equiv 0 \mod p$, also $p \mid g(c)$. Wegen $\deg g = \deg f - 1$ kann es nach IV nur maximal $n - 1$ solcher Werte geben. □

2.7 Satz. *Sei $p \in \mathbb{P}$. Dann gilt $(p-1)! \equiv -1 \mod p$.*

Beweis. Für $p = 2$ ist es klar. Sei also $p \geq 3$.
Betrachte das Polynom

$$f(x) := \prod_{j=1}^{p-1}(x-j) - \left(x^{p-1} - 1\right)$$

Es ist $\deg f \leq p-2$. Andererseits gilt $f(a) \equiv 0 \mod p$ für $a = 1, \ldots, p-1$ (beachte $a^{p-1} \equiv 1 \mod p$). Nach Lagrange (Satz 2.6) sind alle Koeffizienten von f durch p teilbar. Der konstante Term aber ist gegeben durch $(-1)^{p-1}(p-1)! + 1 = (p-1)! + 1$, da p ungerade. Damit gilt $(p-1)! + 1 \equiv 0 \mod p$. □

Bemerkung. Die Umkehrung gilt auch: Falls $m \in \mathbb{N} \setminus \mathbb{P}$, so ist $(m-1)! + 1 \equiv 1 \not\equiv 0 \mod m$. Damit haben wir eine Identität für Primzahlen.

2.8 Satz. *Sei $f \in \mathbb{Z}[x]$, $k \in \mathbb{N}$ und sei $\rho(f,k) := |\{\bar{a} \in \mathbb{Z}_k : f(\bar{a}) \equiv 0 \mod k\}|$. Dann ist $rho(f, m_1 \cdot m_2) = \rho(f, m_1) \cdot \rho(f, m_2)$ für $\mathrm{ggT}(m_1, m_2) = 1$.*

Beweis. Setze $m := m_1 \cdot m_2$ mit $\mathrm{ggT}(m_1, m_2) = 1$. Dann gilt

$$f(a) \equiv 0 \mod m \Leftrightarrow f(a) \equiv 0 \mod m_1 \wedge f(a) \equiv 0 \mod m_2 \tag{3}$$

Jedes dieser beiden Systeme wird individuell gelöst mit Lösungen $a_1, \ldots, a_l \mod m_1$ und $b_1, \ldots, b_s \mod m_2$. Wir erhalten somit $l \cdot s$ mögliche Systeme von linearen Kongruenzen $x \equiv a_i \mod m_1 \wedge x \equiv b_j \mod m_2$, welche nach Satz 2.2.(i) eindeutig modulo m lösbar sind und dies sind alle Lösungen. □

2.9 Satz. *Sei $f \in \mathbb{Z}[x]$, $p \in \mathbb{P}$ und $l \in \mathbb{N}$.*

(i) Wenn $f(z) \equiv 0 \mod p^{k+1}$, dann $f(z) \equiv 0 \mod p^k$. Wählen wir $0 \leq z < p^{k+1}$ mit der Darstellung $z = x_0 + rp^k$, dann ist $f(x_0) \equiv 0 \mod p^k$.

(ii) Sei $x_0 \in \{0, \ldots, p^k - 1\}$ mit $f(x_0) \equiv 0 \mod p^k$. Definiere $S(x_0, k) := \{r \in \{0, \ldots, p-1\} : f(x_0 + rp^k) \equiv 0 \mod p^{k+1}\}$. Dann gilt

$$\#S(x_0,k) = \begin{cases} 1 & : f'(x_0) \not\equiv 0 \mod p \\ p & : f'(x_0) \equiv 0 \mod p, f(x_0) \equiv 0 \mod p^{k+1} \\ 0 & : f'(x_0) \equiv 0 \mod p, f(x_0) \not\equiv 0 \mod p^{k+1} \end{cases}$$

Beweis. Sei $f(x) = \sum_{i=0}^{n} c_i x^i$. Taylorentwicklung bei Stelle x_0 liefert

$$f(x) = \sum_{l=0}^{n} \frac{f^{(l)}(x_0)}{l!}(x - x_0)^l$$

$$\frac{f^{(l)}(x_0)}{l!} = \sum_{i=l}^{n} \underbrace{\frac{i(i-1)\ldots(i-l+1)}{l!}}_{=\binom{i}{l}} c_i x_0^{i-l} \in \mathbb{Z}$$

Wenn wir in die Taylorentwicklung nun $x_0 + rp^k$ einsetzen, erhalten wir

$$f(x_0 + rp^k) = f(x_0) + f'(x_0)rp^k + C \cdot p^{k+1}$$

für ein $C \in \mathbb{Z}$, und damit $f(x_0+rp^k) \equiv f(x_0)+f'(x_0)rp^k \mod p^{k+1}$. Das heißt x_0+rp^k ist Lösung genau dann, wenn $f(x_0)p^{-k}+r \cdot f'(x_0)$. Dies betrachten wir als lineare Kongruenz in r. Nun betrachten wir die einzelnen Fälle. Für $p \nmid f'(x_0)$, können wir es invertieren und nach Satz 2.1 erhalten wir die eindeutige Lösung $r \equiv f(x_0)p^{k-1} \cdot f'(x_0)^{-1} \mod p$. Die übrigen beiden Fälle sind klar. □

Beispiel. Betrachte $(x) = x^4 + 7x + 4$. Wir suchen eine Nullstelle modulo 9. Zunächst rechne modulo 3: $f(0) \equiv 4 \equiv 1 \mod 3$, $f(1) = 12 \equiv 0 \mod 3$ und $f(2)34 \equiv 1 \mod 3$. Nun sei $x_0 \equiv 1 \mod 3$. Dabei gilt $f' = 4x^3 + 7$ und $f'(1) = 11 \equiv 2 \mod 3$ mit dem Inversen $f'(1)^{-1} \equiv -1 \mod 3$. Damit haben wir die eindeutige Lösung $r = 1 \mod 3$. Das heißt die einzige Lösung modulo 9 ist $x_1 = x_0 + 1 \cdot 3 = 4$.

2.10 Satz (Chevalley). *Sei $p \in \mathbb{P}$ und $f \in \mathbb{Z}_p[x_1, \ldots, x_n]$ mit $\deg f < n$ und $f(\vec{0}) = 0$ (f hat keinen konstanten Term). Dann existiert eine nicht-triviale Lösung von $f(x) \equiv 0 \mod p$.*

Beweis. Wir nehmen an, dass $f(x) = 0$ nur die triviale Lösung $x = \vec{0} \mod p$ hat. Dann betrachten wir die neue Kongruenz

$$(*)1 - f(x)^{p-1} \equiv \prod_{i=1}^{n} \left(1 - x_i^{p-1}\right)$$

Nach kleinem Fermat ist jedes x eine Lösung dieser Kongruenz. Aber nach Annahme ist $\deg 1 - f(x)^{p-1} < n(p-1) = \deg \prod_{i=1}^{n}(1 - x_i^{p-1})$. Die rechte Seite lässt sich jedoch darstellen als $\prod x_i^{p-1} + g(x)$ für ein $g \in \mathbb{Z}_p[x]$ mit $\deg g < n(p-1)$. Nach Theorem 1.33 ist $a^p \equiv a \mod p$ und somit können wir annehmen, dass jedes x_i in $f(x)^{p-1}$ maximal in Potenz $p-1$ vorkommt.

check/fix

Wir betrachten die Differenz der Terme, nennen es (**). Dies fassen wir auf als Polynom in X_n und schreiben es als

$$x_n^{p-1}\left(\prod_{i=1}^{n-1} x_i^{p-1} - h_{n-1}(x_1, \ldots, x_{n-1}\right) + \ldots + x_n h_1(x_1, \ldots, x_{n-1}) + h_0(x_1, \ldots, x_{n-1}) \equiv 0 \mod p$$

mit $\deg g_i(x_1, \ldots, x_{n-1}) < i(p-1)$. Nach Satz 2.6 hat dieses Polynom in x_n für jede Wahl von $x_1, \ldots, x_{n-1}$ maximal $p-1$ Nullstellen modulo p, es sei denn, alle Koeffizienten sind 0. Daraus folgt $\prod_{i=1}^{n-1} x_i^{p-1} - h_{n-1}(x_1, \ldots, x_{n-1}) = 0$. Dies führen wir fort, und erhalten zum Schluss $x_1^{p-1} - g_1(x_1) = 0$, was p Lösungen haben muss, aber $\deg g_1 < p-1$, was einen Widerspruch liefert. □

2.11 Bemerkung. Für die Lösbarkeit von $a_2x^2+a_1x+a_0 \equiv 0 \mod n$ mit $n \in \mathbb{N}, a_i \in \mathbb{Z}$ zu untersuchen, reicht es Kongruenzen der Form $x^2 \equiv a \mod p$ für $p \in \mathbb{P}_{>2}$ zu betrachten, sofern wir eine Faktorisierung von n haben.

Den Fall $p = 2$ schließen wir aus, das $a^2 \equiv a \mod 2$; wir hätten also eine lineare Kongruenz.
Sei $\mathrm{ggT}(a_2, p) = 1$. Nun ist $4a_2(a_2x^2 + a_1x + a_0) = (2a_2x + a_1)^2 - (a_1^2 - 4a_1a_0)$. Wegen $\mathrm{ggT}(4a_2, p) = 1$ gilt

$$a_2x^2 + a_1x + a_0 \equiv 0 \mod p \Leftrightarrow (2a_2x + a_1)^2 \equiv (a_1^2 - 4a_1a_0) \mod p$$

Nun löst man $y^2 \equiv (a_1^2 - 4a_1a_0) \mod p$ und aus y lässt sich dann x berechnen.

Wir interessieren uns nun für quadratische Reste. Das heißt, wir suchen nach Lösungen der Kongruenz $x^2 \equiv a \mod p$, wobei wir verlangen, dass $p \in \mathbb{P}_{>2}$ und $\mathrm{ggT}(a, p) = 1$.

2.12 Definition. Sei $p \in \mathbb{P}_{>2}$, $a \in \mathbb{Z}$, $\mathrm{ggT}(a, p) = 1$. Dann heißt a quadratischer Rest modulo p, falls es ein $x \in \mathbb{Z}$ gibt mit $x^2 \equiv a \mod p$. Sonst heißt a quadratischer Nicht-Rest. Die Funktion

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & : a \text{ ist qR} \\ -1 & : a \text{ ist qNR} \\ 0 & : p \mid a \end{cases}$$

heißt Legendre-Symbol.

Beispiel. Wir betrachten alle Quadrate modulo 13.

x	1	2	3	4	5	6	7	8	9	10	11	12
x^2	1	4	9	3	12	10	10	12	3	9	4	1

Das heißt, die quadratischen Reste sind $\{1, 3, 4, 9, 10, 12\}$. Die Nicht-Reste sind $\{2, 5, 6, 7, 8, 11\}$.

2.13 Bemerkung. (i) Es gibt genau $\frac{p-1}{2}$ quadratische Reste (und damit $\frac{p-1}{2}$ quadratische Nicht-Reste). Wählen wir Repräsentanten $\{-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}\}$, und nutzen $x^2 = (-x)^2$. Falls jedoch $k^2 \equiv l^2 \mod p$ gilt, haben wir $p \mid k^2 - l^2 = (k + l)(k - l)$. Für die Repräsentanten gilt jedoch $-p < k - l, k + l < p$ und damit muss $k = \pm l$ gelten. Also haben alle positiven Repräsentanten verschiedene Quadrate.

(ii) Ist $a \equiv b \mod p$, so gilt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(iii) $\left(\frac{a^2}{p}\right) = 1$

(iv) Ist $\left(\frac{a}{p}\right) = 1$, so gibt es genau zwei Lösungen der Kongruenz $x^2 \equiv a \mod p$ (hier brauchen wir $p > 2$).

2.14 Satz. *Sei $p \in \mathbb{P}_{>2}$ und $a \in \mathbb{Z}$. Dann ist $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$.*

Beweis. Für$p \mid a$ ist es klar. Ansonsten gilt $x^{p-1} \equiv \mod p$, was wir schreiben als

$$\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p$$

Ist $\left(\frac{a}{p}\right) = 1$,so existiert ein x mit $x^2 \equiv a \mod p$. Damit gilt $1 \equiv x^{p-1} \equiv a^{\frac{p-1}{2}} \mod p$. Jedes Element ist Nullstelle von x^{p-1}. Nach Lagrange hat aber der linke Faktor maximal $\frac{p-1}{2}$ Nullstellen. Aber alle quadratischen Reste sind Nullstellen davon. Somit muss jeder Nicht-Rest eine Nullstelle von $x^{\frac{p-1}{2}+1}$ sein. □

2.15 Korollar. *Sei $p \in \mathbb{P}_{>2}$, $a, b \in \mathbb{Z}$. Dann gilt $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Beweis.

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

Aber da wir nur im Bereich $-1, 1$ sind (und $p > 2$), ist diese Kongruenz wirklich eine Gleichheit. □

2.16 Proposition. *Sei $p \in \mathbb{P}_{>2}$. Dann ist*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & : p \equiv 1 \mod 4 \\ -1 & : p \equiv -1 \mod 4 \end{cases}$$

Beweis. Folgt direkt aus Korollar 2.15. □

2.17 Lemma (Lemma von Gauss). *Sei $p \in \mathbb{P}_{>2}$ und $a \in \mathbb{Z}$, $p \nmid a$. Wir setzen*

$$\mu := \#\left\{j : 1 \leq j < \frac{p}{2}, ja \bmod p > \frac{p}{2}\right\}$$

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

Beweis. Sei $M := \left\{j : 1 \leq j < \frac{p}{2}, ja \bmod p > \frac{p}{2}\right\}$ und $\overline{M} := \left\{j : 1 \leq j < \frac{p}{2}, ja \bmod p > \frac{p}{2}\right\}$. Setze

$$U(M) := \{(-ja) \bmod p : j \in M\} = \{(p - ja) : j \in M\} \subset \{1, \ldots, \frac{p-1}{2}\}$$

und analog $U(\overline{M})$. Zuerst stellen wir fest, dass ja für $j = 1, \ldots, p-1$ ein vollständiges Restesystem ist. Daraus folgt $\#M = \#U(M)$, sowie $\#\overline{M} = \#U(\overline{M})$. Seien $j_1 \in M$ und $j_2 \in \overline{M}$, so folgt $-j_1 a \not\equiv j_2 a \bmod p$ (sonst wäre $(j_1 + j_2)a \equiv 0 \bmod p$ für $j_1 + j_2 \in \{1, \ldots, p-1\}$, was nicht möglich ist). Also gilt $U(M) \cup U(\overline{M}) = \left\{1, \ldots, \frac{p-1}{2}\right\}$. Nun haben wir

$$\left(\frac{p-1}{2}\right)! = \prod_{j \in M} (-ja \bmod p) \cdot \prod_{j \in \overline{M}} (ja \bmod p) \equiv (-1)^{\#M} \left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \mod p$$

$$\xRightarrow{p \nmid \left(\frac{p-1}{2}\right)!} 1 \equiv (-1)^\mu a^{\frac{p-1}{2}} \mod p \Rightarrow (-1)^\mu \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p$$

und wegen $p > 2$ folgt Gleichheit. □

Beispiel. Wähle $a = 3$ und $p = 31$.

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$ja \bmod p$	3	6	9	12	15	18	21	24	27	30	2	5	8	11	14

Davon sind $\mu = 5$ Zahlen $> \frac{p}{2}$. Damit ist $\left(\frac{5}{31}\right) = (-1)^5 = -1$.

Für $a = 2$ lässt sich eine allgemeine Regel für p aufstellen.

2.18 Proposition. *Es gilt*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & : p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases} = (-1)\frac{p^2-1}{8}$$

Beweis. Wir nutzen Lemma 2.17. Dabei gilt

$$\mu = \#$$

finish

□

2.19 Satz (Quadratische Reziprozitätsgesetz). *Sei $q, p \in \mathbb{P}_{>2}$, $p \neq q$. Dann gilt*

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

Das heißt, wir können zwischen beiden Legendre-Symbolen wechseln und erhalten dabei einen berechenbaren eventuellen Vorzeichenwechsel.

Beweis. Nach Lemma 2.17 ist $\left(\frac{q}{p}\right) = (-1)^\mu$ mit

$$\mu = \#\{x \in \mathbb{N} : 1 \leq x \leq \frac{p-1}{2}, qx \mod p > \frac{p}{2}\}$$

Für qx gibt es ein eindeutiges $y \in \mathbb{Z}$ mit $qx = py + r$, $r \in \left\{-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}\right\}$. Insbesondere ist $y \geq 0$ und

$$\mu = \#\left\{x \in \mathbb{N} : x \leq \frac{p-1}{2}, \exists y \in \mathbb{N}_0. -\frac{p}{2} < qx - py < 0\right\}$$

Wir können annehmen, dass $y \geq 1$. Weiterhin ist

$$py < \frac{p}{2}qx < \frac{p}{2} + q\left(\frac{p-1}{2}\right) < \frac{p}{2}(q+1)$$

Somit können wir μ zählen als

$$\mu = \#\left\{(x,y) \in \left\{1, \ldots, \frac{p-1}{2}\right\} \times \left\{1, \ldots, \frac{q-1}{2}\right\} : -\frac{p}{2} < qx - py < 0\right\}$$

Dies können wir auffassen als Geradengleichung und suchen davon Punkte mit ganzzahligen Koordinaten.
Wenn wir p und q vertauschen, und dann auch noch x und y, so ändern sich nur die Ungleichungen. Sei also $\left(\frac{p}{q}\right) = (-1)^\rho$. Analog erhalten wir

$$\rho = \#\left\{(x,y) \in \left\{1,\dots,\frac{p-1}{2}\right\} \times \left\{1,\dots,\frac{q-1}{2}\right\} : -\frac{q}{2} < py - qx < 0\right\}$$

Wenn wir die Ungleichung am Ende umschreiben, erhalten wir $0 < qx - py < \frac{q}{2}$. Dies interpretieren wir nun geometrisch also Gitter im Rechteck von $(1,1)$ bis $\left(\frac{p-1}{2}, \frac{q-1}{2}\right)$. Grafik
Unsere Bedigungen liefern uns zwei Streifen, von denen wir wissen wollen, wie viele Punkte darin liegen. Auf der entsprechenden Gerade durch den Nullpunkt liegen keine Punkte, da dazu $x \geq p$ und $y \geq q$ sein müssten. Damit ergibt sich für die Summe

$$\mu + \rho = \#\left\{(x,y) \in \left\{1,\dots,\frac{p-1}{2}\right\} \times \left\{1,\dots,\frac{q-1}{2}\right\} : -\frac{p}{2} < qx - py < \frac{q}{2}\right\}$$

Wir müssen nur heraus bekommen, dass diese Summe gerade ist, denn

$$(-1)^{\mu+\rho} = -1^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \Leftrightarrow \mu + \rho\frac{p-1}{2}\cdot\frac{q-1}{2} \mod 2$$

Besser lässt sich aber das Komplement zählen. Im ganzen Rechteck haben wir $\frac{p-1}{2}\cdot\frac{q-1}{2}$. Sei

$$\lambda_1 := \#\left\{(x,y) \in \left\{1,\dots,\frac{p-1}{2}\right\} \times \left\{1,\dots,\frac{q-1}{2}\right\} : py - qx > \frac{p}{2}\right\}$$
$$\lambda_2 := \#\left\{(x,y) \in \left\{1,\dots,\frac{p-1}{2}\right\} \times \left\{1,\dots,\frac{q-1}{2}\right\} : py - qx < -\frac{q}{2}\right\}$$

und wir wissen $\mu + \rho + \lambda_1 + \lambda_2 = \frac{p-1}{2}\cdot\frac{q-1}{2}$, was eine gerade Zahl ist. Unser Ziel ist nun zu zeigen $\lambda_1 + \lambda_2 \equiv 0 \mod 2$. Seien $x, y \in \left\{1,\dots,\frac{p-1}{2}\right\} \times \left\{1,\dots,\frac{q-1}{2}\right\}$ mit $py - qx > \frac{p}{2}$. Sei $y' := \frac{q+1}{2} - y$ und $x' := \frac{p+1}{2} - x$. Dann gilt $py' - qx' = \frac{p}{2} - \frac{q}{2} - py + qx < -\frac{q}{2}$. Die Idee ist, dass wir eine Punktspiegelung (Drehung) am Mittelpunkt des Rechtecks durchführen und damit eine selbstinverse Abbildung zwischen beiden Teilen erhalten. Damit ist $\lambda_1 = \lambda_2$ und die Summe ist gerade. $\square$

Beispiel.

$$\begin{aligned}\left(\frac{2819}{4177}\right) &= \left(\frac{4177}{2819}\right) = \left(\frac{1358}{2819}\right) = \left(\frac{2}{2819}\right)\cdot\left(\frac{7}{2819}\right)\cdot\left(\frac{97}{2819}\right)\\ &= (-1)\cdot -\left(\frac{2819}{7}\right)\cdot\left(\frac{2819}{97}\right) = \left(\frac{5}{7}\right)\cdot\left(\frac{6}{97}\right) = \left(\frac{7}{5}\right)\left(\frac{2}{97}\right)\left(\frac{3}{97}\right)\\ &= \left(\frac{2}{5}\right)\cdot 1\cdot\left(\frac{1}{3}\right) = (-1)\cdot 1\cdot 1 = -1\end{aligned}$$

2.20 Satz. *Seien $p, q \in \mathbb{P}_{>2}$ und wir schreiben p eindeutig als $p = 4qk \pm a$, wobei $a, k \in \mathbb{Z}$, $a \equiv 1 \mod 4$ und $1 \leq a < 4q$. Dann gilt $\left(\frac{q}{p}\right) = \left(\frac{a}{q}\right)$.*

Beweis. Wir schreiben $p = 4qk + a$ mit $k \in \mathbb{Z}$ und $1 \leq a < 4q$. Da p eine Primzahl ist (insbesondere ungerade), gilt $a \equiv \pm 1 \mod 4$. Im Fall $a \equiv 1 \mod 4$ haben wir die gesuchte Form. Dann ist $p \equiv 1 \mod 4$, also $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{a}{q}\right)$.
Im Fall $a \equiv -1 \mod 4$ setze $k' := k + 1$ und $p = 4qk' - a'$, dann muss $a' \equiv 1 \mod 4$ sein, denn $a' + a = 4q$. In diesem Fall ist $p \equiv -1 \mod 4$. Dann betrachten wir den Rest von $q \mod 4$.

$q \equiv -1 \mod 4$**:** Dann gilt nach Reziprozitätsgesetz

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{-a}{q}\right)$$

$q \equiv 1 \mod 4$**:** Dann gilt nach Reziprozitätsgesetz

finish

□

2.21 Bemerkung. Sei $q \in \mathbb{P}$. Für $p \in \mathbb{P}_{>2}$ gilt $\left(\frac{q}{p}\right) = 1$ genau dann, wenn p die Form $p = 4qk \pm a$ hat mit $1 \leq a < 4q$, $a \equiv 1 \mod 4$ und $\left(\frac{a}{q}\right) = 1$. Die möglichen Werte für a erhält man, indem man alle $(2l+1)^2 \mod 4q$ für $l = 0, \ldots, \frac{q-3}{2}$ ausrechnet.

Beispiel. Betrachte $q = 3$. Dann ist die einzige Möglichkeit $a = 1$. Daraus ergibt sich $\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \mod 12$.
Für $q = 17$ sieht es weniger schön aus. Wir erhalten $\left(\frac{17}{p}\right) = 1$ genau dann, wenn p von der Form $68k \pm a$ mit $a \in \{1, 9, 25, 49, 13, 53, 33, 21\}$.

2.22 Definition (Jacobi-Symbol). Sei $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ ungerade. Weiter sei $b = p_1 \cdot \ldots \cdot p_m$ für $p_i \in \mathbb{P}$. Dann heißt

$$\left(\frac{a}{b}\right) := \prod_{i=1}^{m} \left(\frac{a}{p_i}\right)$$

das *Jacobi-Symbol*. Dabei gilt $\left(\frac{a}{1}\right) = 1$ (da leeres Produkt).

2.23 Bemerkung. Ist a quadratischer Rest modulo b, so ist es insbesondere quadratischer Rest modulo jedes Primteilers. Also gilt $\left(\frac{a}{b}\right) = 1$. Die Rückrichtung gilt jedoch nicht. Als Gegenbeispiel haben wir

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

Aber 2 ist kein quadratischer Rest modulo 15.

2.24 Lemma. *Sei $a, a_1, a_2 \in \mathbb{Z}$ und $b, b_1, b_2 \in \mathbb{N}$ ungerade. Dann gilt*

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right) \tag{4}$$

$$\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right) \tag{5}$$

$$a_1 \equiv a_2 \mod b \implies \left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right) \tag{6}$$

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} \tag{7}$$

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{2}} \tag{8}$$

$$2 \nmid 2, \mathrm{ggT}(a,b) = 1 \implies \left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}\left(\frac{b}{a}\right) \tag{9}$$

2.25 Satz. *Sei $a \in \mathbb{Z}$. Dann ist $x^2 \equiv a \mod p$ ist lösbar für alle Primzahlen genau dann, wenn a ein Quadrat ist, das heißt $a = b^2$ für $b \in \mathbb{N}$.*

Beweis. Falls $a = b^2$ ist offenbar $x = b$ eine Lösung.
Sei also a kein Quadrat und wir betrachten die Primfaktorenzerlegung $a = \pm 2^{r_0} p_1^{r_1} \cdot \ldots \cdot p_m^{r_m}$. Wir unterscheiden drei Fälle:

r_0 **ungerade:** Schreibe $a = \pm 2^k \cdot b$ mit k, b ungerade. Nach Satz 2.2 gibt es eine Zahl u mit $u \equiv 5 \mod 8$ und $u \equiv 1 \mod b$. Insbesondere ist dann $u \equiv 1 \mod 4$. Nach Lemma 2.24.(6) gilt $\left(\frac{b}{u}\right) = \left(\frac{u}{b}\right) = \left(\frac{1}{b}\right) = 1$. Nach Lemma 2.24.(7) gilt $\left(\frac{-1}{u}\right) = 1$ und Lemma 2.24.(8) ergibt $\left(\frac{2}{u}\right) = -1$. Damit ist insgesamt $\left(\frac{a}{u}\right) = -1$.

r_0 **gerade, ein anderes r_i ungerade:** Schreibe $a = \pm 2^{2l} q^k \cdot b$ mit $q \in \mathbb{P}$, k, b ungerade, $q \nmid b$. Sei n ein quadratischer Nicht-Rest modulo q. Mit Satz 2.2 gibt es ein $u \in \mathbb{N}$ mit $u \equiv 1 \mod 4b$ und $u \equiv n \mod q$. Dann ist $g \equiv 1 \mod 4$ und damit $\left(\frac{-1}{u}\right) = 1$ nach Lemma 2.24. Ebenso gilt $\left(\frac{b}{u}\right) = \left(\frac{u}{b}\right) = \left(\frac{1}{b}\right) = 1$. Der Faktor 2^{2l} spielt keine Rolle, da es gerade Potenz hat. Es bleibt $\left(\frac{q}{u}\right) = \left(\frac{u}{q}\right) = \left(\frac{n}{q}\right) = -1$. Damit gilt insgesamt $\left(\frac{a}{q}\right) = -1$, da k ungerade.

alle r_i gerade, also $a = -b^2$: Sei $u \in \mathbb{P}$ mit $u \equiv -1 \mod 4$ und $u \nmid b$. Eine solche Primzahl existiert, da unendlich viele in dieser Kongruenzklasse existieren, also wählen wir eine Zahl $u > b$. Dann ist $\left(\frac{a}{u}\right) = \left(\frac{-b^2}{u}\right) = \left(\frac{-1}{u}\right) = -1$.

In allen drei Fällen finden wir eine ungerade Zahl u mit $\left(\frac{a}{u}\right) = -1$. Dann muss es aber ein $p \mid u$ geben mit $\left(\frac{a}{p}\right) = -1$, also ist a kein Quadrat modulo dieser Primzahl. □

Bemerkung. Wir interessieren uns nun noch für die Verteilung der Quadrate. Wir wissen, insgesamt ist die Hälfte aller Elemente quadratischer Rest. Aber es gilt noch mehr. Wenn wir uns ein beliebiges Intervall der Länge k nehmen, so ist auch dort etwa die Hälfte der Elemente quadratischer Rest.

2.26 Satz. *Sei $p \in \mathbb{P}_{>2}$. Setze*

$$RR := \#\left\{(i, i+1) : 1 \leq i \leq p-2, \left(\frac{i}{p}\right) = \left(\frac{i+1}{p}\right) = 1\right\}$$
$$RN := \#\left\{(i, i+1) : 1 \leq i \leq p-2, \left(\frac{i}{p}\right) = 1, \left(\frac{i+1}{p}\right) - = 1\right\}$$

und analog NR und NN. Dann liegen alle diese Zahlen zwischen $\frac{1}{4}(p-5)$ und $\frac{1}{4}(p+1)$.

Beweis. $RR + RN$ liefert die Anzahl der quadratischen Reste zwischen 1 und $p-2$. Das gleiche machen wir mit weiteren Kombinationen. Das liefert

$$RR + RN = \frac{p-2-\left(\frac{-1}{p}\right)}{2} \qquad NR + NN = \frac{p-2+\left(\frac{-1}{p}\right)}{2}$$
$$RR + NR = \frac{p-1}{2} - 1 \qquad RN + NN = \frac{p-1}{2}$$

Die dieses LGS linear abhängig ist, betrachten wir dazu noch das Produkt

$$\left(\frac{i}{p}\right) \cdot \left(\frac{i+1}{p}\right) = \begin{cases} 1 & : i, i+1 \text{ ist qR oder } i, i+1 \text{ ist qNR} \\ -1 & : i \text{ ist qR, } i+1 \text{ ist qNR oder } i \text{ ist qNR und } i+1 \text{ is qR} \end{cases}$$
$$\Longrightarrow \sum_{i=1}^{p-2} \left(\frac{i}{p}\right)\left(\frac{i+1}{p}\right) = RR + NN - RN - NR$$

Sei j_i das multiplikative Inverse zu i modulo p. Dann lässt sich obige Summe schreiben als

$$\sum_{i=1}^{p-2} \left(\frac{i}{p}\right)\left(\frac{i+1}{p}\right) = \sum_{i=1}^{p-2} \left(\frac{i(i+1)}{p}\right) = \sum_{i=1}^{p-2} \left(\frac{i(i+i\cdot j_i)}{p}\right) = \sum_{i=1}^{p-2} \left(\frac{i^2(1+j_i)}{p}\right)$$
$$= \sum_{i=1}^{p-2} \left(\frac{1+j_i}{p}\right) = \sum_{i=2}^{p-1} \left(\frac{j_i}{p}\right) = \sum_{i=2}^{p-1} \left(\frac{i}{p}\right) = -1$$

Da $p-1$ sein eigenes Inverses ist, durchlaufen die j_i der Summe alle Werte von 1 bis $p-2$. Zusammen mit den obigen Gleichungen liefert dies die Aussage. □

2.27 Lemma (Thue). *Seien $l, m, , v \in \mathbb{Z}$ mit $0 < u, v \leq m < uv$ mit $\mathrm{ggT}(l, m) = 1$. Dann existieren $x, y \in \mathbb{N}$ mit $1 \leq x < u$ und $1 \leq y < v$ sowie $ly \equiv x \mid m$ oder $ly \equiv -x \mod m$. Insbesondere ist $(ly)^2 = x^2 \mod m$.*

Beweis. Wir betrachten $r + ls \mod m$ mit $0 \leq r < u$ und $0 \leq s < v$. Nach Schubfachprinzip haben wir verschiedene r_1, r_2, s_1, s_2 mit $r_1 + ls_1 = r_2 + ls_2 \mod m$ und somit $l(s_2 - s_1) \equiv r_1 - r_2 \mod m$. OBdA sein $s_1 < s_2$. Dann setze $y := s_2 - s_1$ und $x := |r_1 - r_2|$. Damit ist $ly \equiv x \mod m$ oder $ly \equiv -x \mod m$. Außerdem gilt $y < v$ und $x < m$. Falls $y = 0$, ist $s_1 = s_2$ und damit $r_1 \equiv r_2 \mod m$, also $r_1 = r_2$. Ist $x = 0$, so folgt $r_1 = r_2$ und damit $m \mid l(s_2 - s_1)$. Wegen $\mathrm{ggT}(l, m) = 1$ folgt $m \mid s_2 - s_1$, also $s_1 = s_2$. □

2.28 Lemma. *Sei $p \in \mathbb{P}$ mit $p \equiv 1 \mod 4$. Dann existieren $x, y \in \mathbb{N}$ mit $p = x^2 + y^2$.*

Beweis. Nach Proposition 2.16 existiert ein $l \in \mathbb{Z}$ mit $l^2 \equiv -1 \mod p$. Dabei gilt $\mathrm{ggT}(l,p) = 1$. Nun wenden wir Lemma 2.27 an mit $m = p$ und $u = v = \lfloor\sqrt{p}\rfloor + 1$. Damit haben wir $x, y \in \mathbb{N}$ mit $x, y \leq \lfloor\sqrt{p}\rfloor$ mit $l^2y^2 \equiv x^2 \mod p$. Das heißt $x^2 + y^2 \equiv 0 \mod p$. Wegen $0 < x^2 + y^2 < 2p$ folgt $x^2 + y^2 = p$. □

2.29 Satz. *Für $p \in \mathbb{P}_{>2}$ gilt $p \equiv 1 \mod 4$ genau dann, wenn p Summe von zwei Quadrate ist und die Darstellung ist eindeutig.*

Beweis. Angenommen $p = x^2 + y^2$. Es gilt $x^2, y^2 \mod 4 \in \{0,1\}$, also $p \mod 4 \in \{0,1,2\}$. Insbesondere ist $p \not\equiv 3 \mod 4$, also bleibt $p \equiv 1 \mod$.
Sei $p \equiv 1 \mod 4$. Dass die Darstellung existiert, liefert Lemma 2.28. Es bleibt die Eindeutigkeit. Angenommen $p = x^2 + y^2 = u^2 + v^2$ mit $0 < x < y$ und $0 < u < v$. Dann gilt $x, y, u, v \leq \sqrt{p}$. Ferner ist

$$\begin{aligned} x^2v^2 - y^2u^2 &= (p - y^2)v^2 - y^2 - u^2 = p(v^2 - y^2) \\ \implies p \mid (x^2v^2 - y^2u^2) &= (xv - yu)(xv + yu) \end{aligned}$$

Fall $p \mid xv + yu$**:** Es gilt $1 \leq xv + yu < 2p$, also $p = xv + yu$. Nun schreiben wir $p^2 = (x^2 + y^2)(u^2 + v^2) = (xv + yu)^2 + (xu + yv)^2 = p^2 + (xu - yv)^2$. Also gilt $xu = yv$, was ein Widerspruch ist ($x < y$ und $u < v$).

Fall $p \mid xv - yu$**:** Wegen $-p < xv - yu < p$ folgt $xv = yu$. Da x, y und u, v teilerfremd sind, folgt $x \mid u$ und $v \mid y$, aber auch umgekehrt, also $x = u$ und $y = v$. □

3 Kettenbrüche

Wir beginnen mit einem Beispiel und rechnen den Euklidischen Algorithmus mit $a = 67$ und $b = 24$.

$$\begin{aligned} 67 &= 2 \cdot 24 + 19 \\ 24 &= 1 \cdot 19 + 5 \\ 19 &= 3 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \end{aligned}$$

Damit haben wir an Brüchen dir folgende Darstellung.

$$\frac{67}{24} = 2 + \frac{19}{24} = 2 + \frac{1}{\frac{24}{19}} = 2 + \frac{1}{1 + \frac{5}{19}} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{4}{5}}} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}} =: [2; 1, 3, 1, 4]$$

eigene Notation, einfacher in LaTeX

Falls der Bruch negativ ist, dann erhalten wir ein negatives erstes Glied; der Rest läuft wie im positiven Fall.
Da wir nun auch über irrationale Zahlen sprechen wollen, definieren wir die Abrundung $\lfloor x \rfloor := \max\{z \in \mathbb{Z} : z \leq x\}$. Beachte $x = \lfloor x \rfloor + (x - \lfloor x \rfloor)$, wobei der zweite Summand in $[0, 1)$ liegt. Setze $x_0 := x$ und $x_{i+1} := \frac{1}{x_i - \lfloor x_i \rfloor}$. Dann können wir Kettenbrüche für $x \in \mathbb{R}$ schreiben mittels

$$x = \lfloor x \rfloor + \frac{1}{\lfloor x_1 \rfloor + \frac{1}{x_2}} = \dots$$

Das letzte Glied ist dann eventuell eine irrationale Zahl.
Als Beispiel für konkrete Zahlen haben wir

$$\begin{aligned} \varphi &= [1; 1, 1, 1, 1, \dots] && \text{goldener Schnitt} \\ \pi &= [3; 7, 15, 1, 292, \dots] \end{aligned}$$

3.1 Definition. Sei $x \in \mathbb{R}$. Setze $x_0 := 0$ und $a_i = \lfloor x_i \rfloor$, sowie $x_{i+1} := \frac{1}{x_i - a_i}$ für $i \geq 0$, solange $x_i \notin \mathbb{Z}$. Wir erhalten die folgende kanonische Darstellung von x als

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \frac{1}{a_{k-1} + \frac{1}{x_k}}}} =: [a_0; a_1, a_2, \dots, a_{k-1}; x_k]$$

Dabei gilt $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$ für $i \geq 1$ und $x_k \in \mathbb{R}$.

3.2 Definition. (i) Ein Ausdruck der Form $[z_0; z_1, \dots, z_k]$ mit $z_i \in \mathbb{R}$, $z_i > 0$ für $1 \leq i < k$ heißt endlicher Kettenbruch. Ist $z_0 \in \mathbb{Z}$ und $z_i \in \mathbb{N}$ für $i \leq i \leq k$, dann heißt der Ausdruck einfacher endlicher Kettenbruch.

(ii) Für $0 \leq n \leq k$ heißt die Zahl $[z_0; z_1, \dots, z_m]$ die n-te Konvergente.

Beispiel. Kommen wir zurück zu $\pi = [3; 7, 15, 1, 292, \dots]$. Dann ist

- 0-te Konvergente: 3
- 1-te Konvergente: $\frac{22}{7}$
- 2-te Konvergente: $\frac{333}{106}$
- 3-te Konvergente: $\frac{355}{113}$
- 4-te Konvergente: $\frac{103993}{33102}$

3.3 Bemerkung. Die kanonische Darstellung einer rationalen Zahl ist ein einfacher kanonischer Kettenbruch.

3.4 Notation. Im folgenden sei p_n und q_n der Zähler und Nenner der n-ten Konvergente, die wir erhalten, wenn wir $[z_0; z_1, \ldots, z_k]$ als formalen bruch schreiben. Das heißt $p_0 = z_0$ und $q_0 = 1$; $p_1 = z_0 z_1 + 1$ und $q_1 = z_1$ und so weiter.

3.5 Lemma. *Sei $\frac{p_n}{q_n}$ die n-te Konvergente des endlichen Kettenbruchs $x = [z_0; z_1, \ldots, z_k]$.*

(i) Dann gilt $p_n = p_{n+1} z_n + p_{n-2}$ und $q_n = q_{n-1} z_n + q_{n-2}$ für $2 \leq n \leq k$. Insbesondere ist $x = \frac{p_{k-1} z_k + p_{k-2}}{q_{k-1} z_k + q_{k-2}}$.

(ii) $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}$ für $1 \leq n \leq k$.

(iii) $p_n q_{n-2} - q_n p_{n-2} = (-1)^n z_n$ für $2 \leq n \leq k$.

(iv) Wir haben die Abschätzung

$$\frac{p_{2i}}{q_{2i}} < \frac{p_{2(i+1)}}{q_{2(i+1)}} \leq x \leq \frac{p_{2(i+1)+1}}{q_{2(i+1)+1}} < \frac{p_{2i+1}}{q_{2i+1}}$$

Beweis. Beweise mittels Induktion über n

(i) Der Anfang für $n = 2$ ist klar. Weiter gilt

$$\begin{aligned}\frac{p_{n+1}}{q_{n+q}} &= [z_0; z_1, \ldots, z_n, z_{n+1}] = \left[z_0; z_1, \ldots, z_n + \frac{1}{z_{n+1}}\right] \overset{\text{IV}}{=} \frac{p_{n-1}\left(z_n + \frac{1}{z_{n+1}}\right) + p_{n-2}}{q_{n-1}\left(z_n + \frac{1}{z_{n+1}}\right) + q_{n-2}} \\ &= \frac{p_{n-1} z_n + p_{n-2} + \frac{p_{n-1}}{z_{n+1}}}{q_{n-1} z_n + q_{n-2} + \frac{q_{n-1}}{z_{n+1}}} \overset{\text{IV}}{=} \frac{p_n + \frac{p_{n-1}}{z_{n+1}}}{q_n + \frac{q_{n-1}}{z_{n+1}}}\end{aligned}$$

(ii) Für $n = 1$ gilt $p_1 q_0 - p_0 q_1 = (z_0 z_1 + 1) \cdot 1 - z_0 z_1 = 1$. Weiter ist

$$\begin{aligned}p_{n+1} q_n - p_n q_{n+1} &\overset{\text{(i)}}{=} (p_n z_{n+1} + p_{n-1})\, q_n - p_n (q_n z_{n+1} + q_{n-1}) = p_{n-1} q_n - p_n q_{n-1} \\ &= (-1) \cdot (-1)^{n+1} = (-1)^{n+2}\end{aligned}$$

(iii) folgt analog

(iv) Wenn $z_i > 0$ für $i \geq 1$, dann folgt $q_i > 0$ für alle $i \geq 1$.

$$\frac{p_n}{q_n} - \frac{p_{n+2}}{q_{n+2}} = \frac{p_n q_{n+2} - p_{n+2} q_n}{q_{n+2} q_n} = \frac{(-1)^n z_n}{q_n q_{n+2}}$$

Damit erhalten wir, dass die geraden Glieder streng steigen und die ungeraden Glieder streng fallen. Aus (ii) folgt

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n+1}}{q_n q_{n-1}}$$

Damit sind die geraden Glieder immer kleiner als die ungeraden. Da x selbst eine Konvergente ist, muss es dazwischen liegen. □

3.6 Satz. *Jede rationale Zahl $x \in \mathbb{Q} \setminus \mathbb{Z}$ hat eine eindeutige Darstellung als einfacher endlicher Kettenbruch $[a_0; a_1, \ldots, a_k]$ mit $a_k \geq 2$. Die einzige andere Darstellung ist $[a_0; a_1, \ldots, a_k - 1, 1]$.*

Beweis. Sei $x = \frac{a}{b} = [a_0; a_1, \ldots, a_k] = [b_0; b_1, \ldots, b_l]$. In beiden Fällen in der gebrochene Anteil $[0; a_1, \ldots, a_k], [0; b_1, \ldots, b_l] \in (0, 1)$, da $a_k, b_l \geq 2$. Also ist $a_0 = b_0 = \lfloor x \rfloor$. Wenn wir auf die nächste Stufe gehen, dann erhalten wir $[a_1; \ldots, a_k] = [b_1; \ldots, b_l]$. Induktiv folgt $k = l$ und $a_i = b_i$ für $1 \leq i \leq k$.
Die einzig mögliche Abweichung ist dann $l = k + 1$ und $b_l = 1$, ansonsten verläuft die Argumentation analog. □

Wir haben auch eine geometrischen Interpretation. Wir tragen $\frac{a}{b}$ als Punkt (a, b) ins Koordinatensystem. Dann sind die geraden Kettenbrüche Punkte unterhalb der Linie, die ungeraden liegen drüber.

Beispiel. Als Beispiel für den Spielraum bei der Darstellung haben wir $\frac{4}{11} = [0; 2, 1, 3] = [0; 2, 1, 2, 1]$.

3.7 Korollar. *Seien $a, b \in \mathbb{Z}$ mit $b > 0$,$\mathrm{ggT}(a, b) = 1$ und sei $\frac{a}{b} = [a_0; a_1, \ldots, a_k]$ mit k ungerade (möglich nach Satz 3.6). Dann gilt $aq_{k-1} - bp_{k-1} = 1$.*

Beweis. Es gilt $\frac{a}{b} = \frac{p_k}{q_k}$ und wegen $\mathrm{ggT}(a, b) = 1$ heißt das $a = p_k$ und $b = q_k$. Mit Lemma 3.5.item (ii) folgt

$$1 = (-1)^{k-1} = p_k q_{k-1} - q_k p_{k-1} = aq_{k-1} - bp_{k-1}$$

□

3.8 Definition. Ein Ausdruck der Form $[a_0; a_1, a_2, \ldots]$ mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i \in \mathbb{N}$ heißt einfacher unendlicher Kettenbruch.

3.9 Bemerkung. Aufgrund der kanonischen Darstellung (siehe Definition 3.1) kann jeder irrationalen Zahl ein einfacher unendlicher Kettenbruch zugeordnet werden. Diese Darstellung heißt kanonischer unendlicher Kettenbruch.

Beispiel. Betrachte den goldenen Schnitt $\varphi = \frac{1}{2}(\sqrt{5}+1)$. Dieser ist Lösung der Gleichung $x = 1 + \frac{1}{x}$ was den Kettenbruch $[1; 1, 1, \ldots]$ liefert. Die n-te Konvergente liefert $\frac{f_{n+1}}{f_n}$ (Fibonacci-Zahlen).

3.10 Satz. *(i) Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ mit kanonischen unendlichen Kettenbruch $[a_0; a_1, \ldots]$ und Konvergenten $\frac{p_n}{q_n}$. Dann gilt $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$. Insbesondere gilt $\frac{p_n}{q_n} \xrightarrow{n\to\infty} \alpha$.*

(ii) Sei $[a_0; a_1, \ldots]$ ein unendlicher Kettenbruch Konvergenten $\frac{p_n}{q_n}$. Dann existiert der Grenzwert $\alpha := \lim_{n\to\infty} \frac{p_n}{q_n}$, $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ und der Kettenbruch stimmt überein mit dem kanonischen Kettenbruch von α.

Beweis. (i) Wir können den Kettenbruch abbrechen mittels $\alpha = [a_0; a_1, \ldots, a_n, z_{n+1}]$ mit $z_{n+1} \geq 1$. Mit Lemma 3.5.item (i) folgt

$$\alpha - \frac{p_n}{q_n} = \frac{p_n z_{n+1} + p_{n-1}}{q_n z_{n+1} + q_{n-1}} - \frac{p_n}{q_n} = \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(q_n z_{n+1} + q_{n-1})} = \frac{(-1)^{n-1}}{q_n(q_n z_{n+1} + q_{n-1}} \overset{|\cdot|}{\leq} \frac{1}{q_n^2}$$

(ii) Nach Lemma 3.5.item (iv) wissen wir, die geraden Konvergenten bilden eine streng monoton wachsende Folge mit $\frac{p_{2i}}{q_{2i}} \leq \frac{p_1}{q_1}$. Damit konvergiert diese Folge gegen einen Wert α_1. Analog konvergieren die ungeraden Folgenglieder gegen einen Wert α_2. Unter Ausnutzung der Rekursion erhalten wir aber auch $\left|\frac{p_{2i}}{q_{2i}} - \frac{p_{2i+1}}{q_{2i+1}}\right| \leq \frac{1}{q_{2i}q_{2i+1}}$. Aber die Nenner werden immer größer. Daraus folgt $\alpha_1 = \alpha_2 =: \alpha$.

Nun zeigen wir $\alpha \notin \mathbb{Q}$. Dazu sei $x_n := \lim_{n\to\infty}[a_n; a_{n+1}, \ldots, a_{n+k}] \geq 1$. Daraus folgt $\alpha = [a_0; a_1, \ldots, a_n, x_n]$ und somit

$$|q_n\alpha - p_n| \overset{Lemma\ 3.5}{=} \frac{1}{q_n x_{n+1} + q_{n-1}} < \frac{1}{q_n}$$

Angenommen $\alpha = \frac{p}{q} \in \mathbb{Q}$. dann gibt es unendlich viele Konvergenten $\frac{p_n}{q_n} \neq \frac{p}{q}$, nämlich für $q_n > q$. Für solch eine Konvergente ist $q_n\alpha - p_n| \geq \frac{1}{q} > \frac{1}{q_n}$, was ein Widerspruch ist.

Nun ist $\alpha = a_0 + \frac{1}{x_1}$ nd damit $\lfloor\alpha\rfloor = a_0$. Mit $x_1 = a_1 + \frac{1}{x_2}$ fahren wir nun fort und erhalten, dass $[a_0; a_1, \ldots]$ die kanonische Darstellung von α ist.

□

In der geometrischen Interpretation nehmen wir die Gerade mit Anstieg α und suchen ganzzahlige Punkte (p_n, q_n), die in der Nähe liegen. Der Abstand ist einfach das Skalarprodukt $\langle(\alpha, 1), (p_n, q_n)\rangle$. Der Abstand ist dann kleiner als $\frac{1}{q_n}$. Wenn wir das noch durch q_n dividieren, erhalten wir ebenfalls die erste Aussage.

3.11 Definition. Eine Zahl $\alpha \in \mathbb{R}$ heißt algebraische Zahl vom Grad n falls es ein Polynom $f \in \mathbb{Z}[X]$ vom Grad $\deg f = n$ gibt mit $f(\alpha) = 0$ und $g(\alpha) \neq 0$ für alle $g \in \mathbb{Z}[x] \setminus \{0\}$ mit $\deg g < n$.
Im Fall $n = 2$ heißt α quadratisch irrational. Eine solche hat die Form $x + y\sqrt{d}$ mit $x, y \in \mathbb{Q}$ und $d \in \mathbb{N}$ ist kein Quadrat.

Beispiel. Betrachte $\alpha = \sqrt{7}$. Dann ist der Kettenbruch $[2; 1, 1, 1, 4, 1, 1, 1, 4, \ldots]$ und periodisch so weiter.

3.12 Satz. *(i) Ein periodischer, einfacher, unendlicher Kettenbruch konvergiert gegen eine quadratische irrationale Zahl.*

(ii) Der einfache unendliche Kettenbruch einer quadratisch irrationalen Zahl ist periodisch.

Beweis. (i) Sei h unsere Periode. Dann schreibe $x = [a_0, a_1, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+h-1}}]$. Sei x_n der Kettenbruch ab dem n-ten Glied. Damit gilt

$$\begin{aligned} x &= \frac{p_{n-1}x_n + p_{n-2}}{q_{n-1}x_n + q_{n-2}} \\ x &= \frac{p_{n+h-1}x_{n+h} + p_{n+h-2}}{q_{n+h-1}x_{n+h} + q_{n+h-2}} = \frac{p_{n+h-1}x_n + p_{n+h-2}}{q_{n+h-1}x_n + q_{n+h-2}} \end{aligned}$$

Gleichsetzen liefert eine quadratische Gleichung für x_n. Denn wir dies wieder einsetzen ist auch x Nullstelle einer quadratischen Gleichung. Da der Kettenbruch unendlich ist, geht kein kleinerer Grad, also ist x quadratisch irrational.

(ii) Sei $0 = f(\alpha) = A\alpha^2 + B\alpha + C$ mit $A, B, c \in \mathbb{Z}$ und $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Schreibe $\alpha = [a_0; a_1, \ldots, a_{k-1}, \alpha_k]$. Damit erhalten wir

$$\begin{aligned} \alpha &= \frac{p_{k-1}\alpha_k + p_{k-2}}{q_{k-1}\alpha_k + q_{k-2}} \\ \implies 0 &= A(p_{k-1}\alpha_k + p_{k-2})^2 + B(p_{k-2}\alpha_k + p_{k-2})(q_{k-1}\alpha_k + q_{k-2}) + C(q_{-1}\alpha_k + q_{k-2})^2 \\ \implies 0 &= A_k\alpha_k^2 + B_k\alpha_k + C_k && \text{für ganzzahlige Koeffizienten } A_k, B_k, C_k \\ A_k &= Ap_{k-1}^2 + Bp_{k-1}q_{k-1} + Cq_{k-1} && B_k, C_k \text{ analog} \\ &= q_{k-1}^2 f\left(\frac{p_{k-1}}{q_{k-1}}\right) \\ &= q_{k-1}^2 \cdot \sum_{i=0}^{\infty} \frac{1}{i!} \cdot f^{(i)}(\alpha) \cdot \left(\frac{p_{k-1}}{q_{k-1}} - \alpha\right)^i \\ \implies |A_k| &\overset{\text{Lemma 3.5}}{<} |f'(\alpha)| + \frac{|f''(\alpha)|}{2q_{k-1}^2} \end{aligned}$$

Analog verfährt man mit C_k. Es lässt sich auch zeigen, dass $B_k^2 - 4A_kC_k = B^2 - 4AC$. Da A_k und C_k beschränkt sind, ist somit auch B_k beschränkt.

Nach Schubfachprinzip gibt es $n_1, n_2, n_3 \in \mathbb{N}$ mit $A_{n_1} = A_{n_2} = A_{n_3}$, $B_{n_1} = B_{n_2} = B_{n_3}$ und $C_{n_1} = C_{n_2} = C_{n_3}$. Da aber das Polynom $A_{n_i}\alpha^2 + B_{n_i}\alpha + c_{n_i}$ nur zwei Nullstellen hat, kommt eine Nullstelle doppelt vor. OBdA sei $\alpha_{n_1} = \alpha_{n_2}$ zu $h := n_2 - n_1$. Aufgrund der Eindeutigkeit der Kettenbruchzerlegung wiederholen sich nun alle folgenden Glieder, sodass wir periodisch mit Periode h sind. □

3.13 Satz. *Sei $\alpha = [a_0; a_1, \ldots, a_n, x_{n+1}]$ ein Kettenbruch mit Konvergenten $\frac{p_n}{q_n}$. Dann ist $|q_n\alpha - p_n| < |q_{n-1}\alpha - p_{n-1}|$. Insbesondere ist $|\alpha - \frac{p_n}{q_n}| < |\alpha - \frac{p_{n-1}}{q_{n-1}}|$.*

Beweis. Ist $\alpha = \frac{p_n}{q_n}$, so ist alles klar. Ansonsten sei $x_{n+1} \geq 1$. Dann ist $|q_n\alpha - p_n| \overset{\text{Lemma 3.5}}{=} \frac{1}{q_n x_{n+1} + q_{n+1}}$. Nun ist der Nenner an den Seiten beschränkt durch

$$\begin{aligned} & q_{n+1} = q_n a_{n+1} q_{n-1} \leq q_n x_{n+1} q_{n-1} < q_n(a_{n+1} + 1) + q_{n-1} = q_n + q_{n+1} \leq q_{n+2} \\ \implies & \frac{1}{q_{+1}} < |q_{n+1}\alpha - p_n| \leq \frac{1}{q_{n+1}} \end{aligned}$$

□

3.14 Satz. *Sei* $\alpha = [a_0; a_1, \ldots, a_n, x_{n+1}]$ *mit Konvergenten* $\frac{p_n}{q_n}$. *Sei* $n \geq 2$ *und zu* $1 \leq q \leq q_n$ *und* $p \in \mathbb{Z}$ *mit* $\frac{p}{q} \neq \frac{p_n}{q_n}$. *Dann gilt* $|q_n\alpha - p_n| < |q\alpha - p|$. *Insbesondere ist* $\left|\alpha - \frac{p_n}{q_n}\right| < \left|\alpha - \frac{p}{q}\right|$, *das heißt Kettenbrüche sind die besten Approximationen bis hin zu diesem Nenner.*

Beweis. Im Fall $q = q_n$ gilt $\left|\frac{p_n}{q_n} - \frac{p}{q}\right| \geq \frac{1}{q_n}$. Andererseits ist $\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{2q_n}$. Mit Dreiecksungleichung folgt

$$\left|\alpha - \frac{p}{q}\right| \geq \left|\frac{p_n}{q_n} - \frac{p}{q}\right| - \left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{2q_n} > \left|\alpha - \frac{p_n}{q_n}\right|$$

Sei also $q < q_n$ und sei $q_{n-1} < q < q_n$ (nach Satz 3.13 folgt es dann für alle q). Weiterhin sei $\mathrm{ggT}(p, q) = 1$. Nun gilt

$$\det \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \pm 1 \implies \exists r, s \in \mathbb{Z}. rp_n + sp_{n-1} = p, rq_n + sq_{n-1} = q$$

Aus der Teilerfremdheit folgt $r, s \neq 0$. Wegen $q < q_n$ müssen beiden Koeffizienten nun unterschiedliches Vorzeichen haben, also $rs < 0$. Es ist

$$(q_k\alpha - p_k)(q_{n-1}\alpha - p_{n-1}) < 0 \implies r(q_k\alpha - p_k) \cdot s(q_{n-1}\alpha - p_{n-1}) > 0$$

Das heißt, diese beiden Faktoren haben gleiches Vorzeichen. Damit können wir im folgenden die Beträge vereinfachen zu

$$\begin{aligned} |q\alpha - p| &= |(rq_n + sq_{n-1})\alpha - (rp_n + sp_{n-1})| = |r(q_n\alpha - p_n) - s(q_{n-1}\alpha - p_{n-1})| \\ &= |r(q_n\alpha - p_n)| + |s(q_{n-1}\alpha - p_{n-1})| > |q_{n-1}\alpha - p_{n-1}| > |q_n\alpha - p_n| \end{aligned}$$

□

3.15 Satz. *Sei* $\alpha \in \mathbb{R}$ *und* $\frac{p}{q} \in \mathbb{Q}$ *mit* $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$. *Dann ist* $\frac{p}{q}$ *Konvergente von* α.

Beweis. Ist q bereits Nenner einer Konvergenten q_n, so wissen wir bereits, dass $p = p_n$ (siehe Beweis von Satz 3.14).
Sei also q kein Nenner einer Konvergenten.

Fall $q_{k-1} < q < q_k$**:** Wie im Beweis von Satz 3.14 folgt

$$\begin{aligned} &|q_{k-1}\alpha - p_{k-1}| < |q\alpha - p| < \frac{1}{2q} \implies \left|\alpha - \frac{p_{k-1}}{q_{k-1}}\right| < \frac{1}{2qq_{k-1}} \wedge \left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2} < \frac{1}{2qq_{k-1}} \\ &\implies \frac{1}{qq_{k-1}} > \left|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right| \geq \frac{1}{qq_{k-1}} \quad \lightning \end{aligned}$$

Fall $\alpha = \frac{p_n}{q_n}$ **und** $q > q_n$**:** Dann ist $\frac{p}{q} \neq \frac{p_n}{q_n}$, wegen Teilerfremdheit und damit

$$\frac{1}{q^2} \leq \frac{1}{qq_n} \leq \left|\frac{p}{q} - \frac{p_n}{q_n}\right| < \frac{1}{2q^2} \quad \lightning$$

□

3.16 Satz. *Sei* $\alpha \in \mathbb{R}$.

(i) Eine von zwei aufeinander folgenden Konvergenten $\frac{p_n}{q_n}$ und $\frac{p_{n+1}}{q_{n+1}}$ für $n \geq 1$ erfüllt $\left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{2q_i^2}$.

(ii) Eine von zwei aufeinander folgenden Konvergenten $\frac{p_n}{q_n}$ und $\frac{p_{n+1}}{q_{n+1}}$ für $n \geq 1$ erfüllt $\left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{\sqrt{5}\cdot q_i^2}$. Diese Schranke ist scharf.

Beweis nur für (i). Angenommen, dies ist nicht der Fall. Nun gilt

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

$$\implies \left(\frac{1}{q_n} - \frac{1}{q_{n+1}}\right)^2 = 0 \implies q_n = q_{n+1} \quad \lightning$$

□

3.17 Proposition. *(i) Sei $x \in \mathbb{R}$. Dann existieren unendlich viele $\frac{p}{q} \in \mathbb{Q}$ mit $|x - \frac{p}{q}| \leq \frac{1}{2q}$.*

(ii) Ist $x = \frac{s}{t}$, dann gilt $|x - \frac{p}{q}| \geq \frac{1}{tq}$ für alle $\frac{p}{q} \neq \frac{s}{t}$.

(iii) Ist $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, dann existieren unendlich viele $\frac{p}{q} \in \mathbb{Q}$ mit $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.

3.18 Proposition. *Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ mit $\alpha = [a_0; a_1, a_2, \ldots]$ und sei $|a_i| \leq A$ für alle $i \in \mathbb{N}$. Dann $|\alpha - \frac{p}{q}| > (A+2)^{-2}\frac{1}{q^2}$. Insbesondere haben wir für festes A einen mindestens quadratischen Fehler.*
Wenn wir eine obere Fehlerschranke $\frac{1}{q^{2+\varepsilon}}$ wollen, dann ergibt sich daraus eine Ungleichung der Form $q < C$ für eine Konstante. Damit gibt es nur endlich viele Brüche, die diese Schranke erfüllen.

Beweis. Sei $\frac{p}{q}$ mit $q_{i-1} \leq q < q_i$ und sei $\alpha = [a_0; a_1, \ldots, a_i, \alpha i + 1]$. Dann haben wir mit Satz 3.14 die Abschätzung

$$|q\alpha - p| > |q_i\alpha - p_i| = \frac{1}{q_i\alpha_{i+1} + qi - 1} > \frac{1}{q_i(a_{i+1}+1) + q_{i-1}} > \frac{1}{q_i(a_{i+1}+2)} > \frac{1}{q_i(A+2)}$$

Nun ist $q_i = q_{i-1}a_i q_{i-2} < q_{i-1}(A+2) \leq q(A+2)$. Daraus erhalten wir

$$|q\alpha - p| > \frac{1}{q(A+2)^2} \implies \left|\alpha - \frac{p}{q}\right| > \frac{1}{q^2(A+2)^2}$$

□

3.19 Satz. *Sei $\alpha \in \mathbb{R}$ algebraisch vom Grad $n \geq 2$. Dann existiert eine Konstante $0 < C(\alpha) < 1$ (die nur von α abhängt) so, dass für $q > 0$ gilt $\left|\alpha - \frac{p}{q}\right| > \frac{C(\alpha)}{q^n}$. Analog zu den rationalen Zahlen folgt, dass es nur endlich viele Brüche mit Fehler $< \frac{1}{q^{n+\varepsilon}}$ gibt.*

Beweis. Sei $f \in \mathbb{Z}[x]$ das Minimalpolynom zu α und sei $\frac{p}{q} \in \mathbb{Q}$ mit $|\alpha - \frac{p}{q}| \leq 1$. Nach Definition von n ist $\alpha \notin \mathbb{Q}$ und $f\left(\frac{p}{q}\right) \neq 0$. Damit ist $|q^n \cdot f(\frac{p}{q})| \geq 1$. Nach dem Mittelwertsatz ist

$$f\left(\frac{p}{q}\right) = f\left(\frac{p}{q}\right) - f(\alpha) = \left(\frac{p}{q} - \alpha\right) \cdot f'(C)$$

für ein $C \in [-1+\alpha, 1+\alpha]$. Also Konstante $C(\alpha)$ wähle $\max\{|f'(x)| : x \in [-1, \alpha, 1+\alpha]\}$. Damit ergibt sich

$$\left|\alpha - \frac{p}{q}\right| = \frac{q^n \left|f\left(\frac{p}{q}\right)\right|}{q^n |f'(C)|} \geq \frac{1}{q^n} \cdot \frac{1}{|f'(C)|} \geq \frac{C_1(\alpha)^{-1}}{q^n}$$

Mit $C(\alpha) := \frac{1}{2} \cdot \min\{1, C_1(\alpha)\}$ erhalten wir die Aussage. □

3.20 Korollar. *Sei $a \in \mathbb{N}_{\geq 2}$. Dann ist $\alpha := \sum_{n=1}^{\infty} a^{-n!}$ transzendent.*

Beweis. Für $k \in \mathbb{N}$ sei $p_k := a^{k!} \sum_{n=1}^{k} a^{-n!}$ und $q_k := a^{k!}$. Dann sind $p_k, q_k \in \mathbb{Z}$. Dann gilt

$$\left|\alpha - \frac{p_k}{q_k}\right| = \sum_{n=k+1}^{\infty} a^{-n!} = \frac{1}{a^{(k+1)!}} \sum_{n=k+1}^{\infty} \frac{a^{(k+1)!}}{a^{n!}} = \frac{1}{a^{(k+1)!}} \sum_{n=1}^{\infty} a^{-n} = \frac{C}{a^{(k+1)!}} = \frac{C}{q_k^{k+1}}$$

Wir finden also unendlich viele Abschätzungen beliebig hohen Grades. Damit kann diese Zahl nicht algebraisch sein. □

3.21 Lemma. *Sei $\alpha \in \mathbb{R}$ eine quadratisch irrationale Zahl mit Minimalpolynom $f = ax^2 + bx + c \in \mathbb{Z}[x]$, $a > 0$ und sei $A > \sqrt{b^2 - 4a} =: D$. Dann gibt es nur endlich viele $\frac{p}{q} \in \mathbb{Q}$ mit $|\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$.*

Beweis. Sei β die zweite Nullstelle von f. Dann ist

$$f = a(x-\alpha)(x-\beta) = ax^2 - a(\alpha+\beta)x + a\alpha\beta$$

Dann ist $D = a^2(\alpha+\beta)^2 - 4a^2\alpha\beta = a^2(\alpha-\beta)^2$. Sei $|\alpha - \frac{p}{q}| < \frac{1}{Aq^2}$. Dann folgt

$$\begin{aligned}
\frac{1}{q^2} &\leq \left|f\left(\frac{p}{q}\right)\right| = a\left|\alpha - \frac{p}{q}\right| \cdot \left|\beta - \frac{p}{q}\right| < \frac{a}{Aq^2}\left|\beta - \frac{p}{q}\right| < \frac{a}{Aq^2}\left(\left|\alpha - \frac{p}{q}\right| + |\beta - \alpha|\right) \\
&< \frac{a}{Aq^2}\left(\frac{1}{Aq^2} + \frac{\sqrt{D}}{a}\right) \\
\implies \frac{1}{q^2}\left(1 - \frac{\sqrt{D}}{A}\right) &< \frac{a}{A^2q^4} \\
\implies q^2 &< \frac{a}{A(A-\sqrt{D})} \\
\implies q \leq q &< \sqrt{\frac{a}{A(A-\sqrt{D})}}
\end{aligned}$$

Damit können nur endlich viele q die Ungleichung erfüllen. □

Beispiel.

3.22 Bemerkung. (i) Die Schranke aus Lemma 3.21 ist scharf.
Betrachte $\alpha = \varphi = \frac{1}{2}(1+\sqrt{5})$ mit $f = x^2 - x - 1$. Dann ist $b^2 - 4a = 5$. Für jedes $\varepsilon > 0$ hat $|\alpha - \frac{p}{q}| < \frac{1}{(\sqrt{5}+\varepsilon)q^2}$ nur endlich viele Lösungen.

(ii) Sei α algebraisch vom Grad n. Nach Satz 3.19 gibt es nur endlich viele rationale Zahlen mit $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\mu}$ für $\mu > n$.

(iii) Es wurde von Roth gezeigt, dass dies bereits korrekt ist für $\mu > 2$ (Fields-Medaille).

3.23 Satz (Dirichlet). *Seien $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. Dann existieren $p_i, q \in \mathbb{Z}$, mit $q \geq 1$ und $\left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{n}}}$. Ist wenigstens ein $\alpha_i \in \mathbb{R} \setminus \mathbb{Q}$, dann gibt es unendlich viele $\frac{p}{q}$, welche die Ungleichung erfüllen.*

Beweis. OBdA sei $0 < \alpha_i < 1$ (rechne Brüche modulo q). Der halboffene Würfel $[0,1)^n$ kann in Q^n Würfel der Form $[0, \frac{1}{Q})^n$ unterteilt werden. Wir betrachten die Punkte $(m\alpha_i - \lfloor m\alpha_i \rfloor)_{i=1,\ldots,n}$, für $m = 0, \ldots, Q^n$. Diese liegen alle in $[0,1)^n$. Nach Schubfachprinzip gibt es einen Teilwürfel mit 2 Punkten; seien die Parameter $m_1 > m_2$. Damit ist

$$|m_1\alpha_i - \lfloor m_1\alpha_i \rfloor - (m_2\alpha_i - \lfloor m_2\alpha_i \rfloor)| < \frac{1}{Q} \qquad \text{für } i = 1, \ldots, n$$

Sei nun $q := m_1 - m_2$ und $p_i := \lfloor m_2\alpha_i \rfloor - \lfloor m_1\alpha_i \rfloor$. Daraus folgt $q \leq Q^n$. Dann erhalten wir $|q\alpha_i - p_i| < \frac{1}{Q} \leq q^{-\frac{1}{n}}$.
Falls $\alpha_1 \notin \mathbb{Q}$, dann ist $|q\alpha_1 - p_1| > 0$. Sei also $|q\alpha_1 - p_1| > \frac{1}{M}$ für ein $M \in \mathbb{N}$. Dann führen wir obige Konstruktion erneut mit M statt Q durch. Die neue Differenz ist kleiner als $\frac{1}{M}$, also haben wir einen neuen Bruch. $\square$

Bemerkung. Geometrisch liefert Satz 3.23 die Ungleichung $|(q\alpha_1 - p_1, \ldots, q\alpha_n - p_n)|_\infty < q^{-\frac{1}{n}}$. Das heißt in der Maximumsnorm kommen wir beliebig nah an ganzzahlige Punkte heran.

Bemerkung. Es gibt eine inhomogene Variaante von Satz 3.23, die auf Kronecker zurück geht. Seien $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ und $\beta \in \mathbb{R}$. Dann hat $|q\alpha - p - \beta| < \varepsilon$ eine Lösung und auch dies können wir auf Systeme erweitern.
Eine wichtige Beobachtung dabei ist, dass wegen der Irrationalität die Elemente $q\alpha - \lfloor q\alpha \rfloor$ gleichverteilt sind, wenn wir q iterieren.
Beweisidee: OBdA sei $\beta \in [0,1)$. Wir nutzen Satz 3.23 und erhalten $q\alpha - \lfloor q\alpha \rfloor < \varepsilon$. Dann iterieren wir $k \cdot q\alpha - \lfloor k \cdot q\alpha \rfloor$ und erhalten ein Netz mit Abstand $\leq \varepsilon$. Damit erreichen wir irgendwann Abstand β.

3.24 Definition. Eine Diophantische Gleichung der Form $x^2 - dy^2 = N$ für $d, N \in \mathbb{Z}$ mit d quadratfrei heißt Pellsche Gleichung. Zum Teil meint man damit explizit den Fall $N = 1$.

3.25 Bemerkung. (i) Die allgemeine binäre quadratische Gleichung hat die Form $ax^2 + bxy + cy^2 + dx + ey + f = 0$ mit $a, \ldots, f \in \mathbb{Z}$. Dies kann man auffassen als Polynom in x via $ax^2 + x(by + d) + (cy^2 + ey + f)$. Dabei stellt man fest, dass für die Diskriminante gelten muss

$$\exists z \in \mathbb{N}. z^2 = (by + d)^2 - 4a(cy^2 + ey + f) = (b^2 - 4ac)y^2 + (2bd - 4ae)y + (d^2 - 4af)$$

Setzen wir $p := b^2 - 4ac$, $q := 2bd - 4ae$ und $r := d^2 - 4af$, so müssen wir nun $py^2 + qy + r - z^2$ lösen. Wieder erhalten wir für die Diskriminante die Bedingung

$\exists w \in \mathbb{N}.q^2 - 4p(r - z^2) = w^2$. Umgestellt erhalten wir die Pellsche Gleichung $w^2 - 4pz^2 = q^2 - 4pr$.

(ii) Es reicht, den Fall $d \geq 2$ zu untersuchen. Für $d = 1$ muss $(x+y)(x-y) = N$ gelten, also teste alle Teiler. Für $d < 0$ haben wir positive Summen von Quadraten, also nur endlich viele Möglichkeiten.

3.26 Satz. *Sei $d \in \mathbb{N}_{>2}$ kein Quadrat zu $N \in \mathbb{Z}$ mit $|N| < \sqrt{d}$. Seien ferner $p, q \in \mathbb{N}$ mit $p^2 - dq^2 = N$. Dann ist $\frac{p}{q}$ eine Konvergente von $\sqrt{d}$.*

Beweis. Sei $x, y \in \mathbb{N}$ eine Lösung.

Fall $N > 0$**:** Dann gilt

$$0 < x - y\sqrt{d} = \frac{N}{x + y\sqrt{d}} < \frac{\sqrt{d}}{x + y\sqrt{d}} = \frac{1}{y\left(\frac{x}{y\sqrt{d}} + 1\right)}$$

$$\implies 0 < \frac{x}{y} - \sqrt{d} < \frac{1}{y^2\left(\frac{x}{y\sqrt{d}} + 1\right)} \leq \frac{1}{2y^2}$$

Nach Satz 3.15 ist $\frac{x}{y}$ Konvergente von $\sqrt{d}$.

Fall $N < 0$**:** Umstellen liefert $y^2 - \frac{1}{d} \cdot x^2 = \frac{N}{d}$. Weiterhin ist $\left|\frac{N}{d}\right| < \sqrt{\frac{1}{d}}$. Da wir im ersten Fall nicht benötigt haben, dass $N \in \mathbb{Z}$, können wir es anwenden und erhalten, dass $\frac{y}{x}$ eine Konvergente von $\sqrt{\frac{1}{d}}$ ist. Wenn $\sqrt{d} = [a_0; a_1, \ldots]$, dann ist $\frac{1}{\sqrt{d}} = [0; a_0, a_1, \ldots]$, also ist $\frac{x}{y}$ eine Konvergente von $\sqrt{d}$. □

Beispiel. Betrachte $x^2 + 7y^2$. Dabei gilt $7 = [2; \overline{1, 1, 1, 4}]$.

p_k	2	3	5	8	37	45	82
q_k	1	1	2	3	14	17	31

Dann gilt $p_k^2 - 7q_k^2 = -3, 2, -3, 1, -3, 2, -3, \ldots$

3.27 Lemma. *Sei $\sqrt{d} \in \mathbb{R} \setminus \mathbb{Q}$ und sei $\frac{p_n}{q_n}$ eine Konvergente zu $\sqrt{d}$. Dann gilt $|p_n^2 - dq_n^2| < 1 + 2\sqrt{d}$.*

Beweis. Nach Satz 3.10 ist $\left|\frac{p_n}{q_n} - \sqrt{d}\right| < \frac{1}{q_n^2}$ und damit $\frac{p_n}{q_n} < \frac{1}{q_n^2} + \sqrt{d}$ und $|p_n - q_n\sqrt{d}| < \frac{1}{q_n}$. Daraus folgt

$$|p_n^2 - dq_n^2| = |p_n - q_n\sqrt{d}| \cdot |p_n + q_n\sqrt{d}| < \frac{|p_n + q_n\sqrt{d}|}{q_n} = \frac{p_n}{q_n} + \sqrt{d} < \frac{1}{q_n^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}$$

□

3.28 Satz. *Sei $d \in \mathbb{N}_{>2}$ kein Quadrat. Dann gibt es unendlich viele $x, y \in \mathbb{N}$ mit $x^2 - dy^2 = 1$.*

Beweis. Nach Lemma 3.27 existiert ein $k \in \mathbb{Z}$ mit $|k| < 1 + 2\sqrt{d}$ und $x^2 + dy^2 = k$ hat unendlich viele Lösungen $(\overline{x}_i, \overline{y}_i)$ mit $i \in \mathbb{N}$. Wenn wir dies Lösungen modulo k

betrachten, gibt es nur $|k|^2$ viele Restklassen, also enthält eine davon unendlich viele Lösungen $(x_i, y_i)_{i\in\mathbb{N}}$. Das heißt $x_i \equiv x_1 \mod k$ und $y_i \equiv y_1 \mod k$. Sei $\alpha_i := x_i + y_i\sqrt{d}$ mit dem Konjugierten $\overline{\alpha_i} = x_i - y_i\sqrt{d}$. Setze nun

$$\beta_i := \frac{\alpha_1\overline{\alpha_i}}{k} = \frac{x_1x_i - y_1y_id}{k} + \sqrt{d}\cdot\underbrace{\frac{y_1x_i - x_1y_i}{k}}_{\in\mathbb{Z}}$$

Weiterhin ist

$$x_1x_i - y_1y_id = x_i(x_1 - x_i) + y_id(y_1 - y_i) + x_i^2 - dy_i^2 \equiv 0 \mod k$$

Damit ist $\beta_i = a_i + b_i\sqrt{d}$ mit $a_i, b_i \in \mathbb{Z}$. Nun gilt aber

$$\beta_i\overline{\beta_i} = \frac{\alpha_1\overline{\alpha_i}}{k}\cdot\frac{\overline{\alpha_1}\alpha_i}{k} = \frac{\alpha_1\overline{\alpha_1}}{k}\cdot\frac{\overline{\alpha_i}\alpha_i}{k} = 1$$

Beweis abschließen mit paar Worten

□

4 Summen von Quadraten

4.1 Satz. *Sei $n \in \mathbb{N}$, schreibe als Primfaktorzerlegung*

$$n = \prod_{p\equiv 3 \mod 4} p^{\alpha_p} \cdot \prod_{p\not\equiv 3 \mod 4} p^{\beta_p}$$

Dann ist n eine Summe von zwei Quadraten genau dann, wenn alle α_p gerade sind.

Beweis. Beobachtung: $(u^2 + v^2)(r^2 + s^2) = (ur - sv)^2 + (us + rv)^2$, nachrechnen oder durch Rechnen in $\mathbb{Z}[i]$.
$\Leftarrow$: Sei $d := \prod_{p\equiv 3 \mod 4} p^{\frac{\alpha_p}{2}}$. Mit obiger Beobachtung und Satz 2.29 ist $\frac{n}{d^2} = x^2 + y^2$ für geeignete $x, y \in \mathbb{N}$. Damit ist $n = (dx)^2 + (dy)^2$.
$\Rightarrow$: Sei $n = x^2+y^2$ und $d := \mathrm{ggT}(x, y)$. Dann genügt zu zeigen $p \mid \left(\frac{n}{d^2}\right) \implies p \not\equiv 3 \mod 4$. Sei also $p \mid \frac{n}{d^2}$ und $x_1 := \frac{x}{d}$ und $y_1 := \frac{y}{d}$. Nach Definition von d gilt $\mathrm{ggT}(x_1, y_1) = 1$. Dann gilt $x_1^2 + y_1^2 \equiv 0 \mod p$, aber p kann nicht beide teilen. Sei also $p \nmid y_1$. Damit existiert ein $\overline{y_1} \in \mathbb{N}$ mir $y_1\overline{y_1} \equiv 1 \mod p$. Daraus folgt

$$x_1^2\overline{y_1}^2 + y_1^2\overline{y_1}^2 \equiv x_1^2\overline{y_1}^2 + 1 \mod p \implies (x_1\overline{y_1})^2 \equiv -1 \mod p$$

Damit ist -1 ein quadratischer Rest, also $p = 2$ oder $p \equiv 1 \mod 4$. □

Setze $S(n) := \{n \in \mathbb{N} : \exists x, y. n = x^2 + y^2\}$. Dann ist $\#S(x) \approx \frac{x}{\sqrt{\ln x}}$.

4.2 Satz (Legendre). *Eine Zahl $n \in \mathbb{N}$ ist Summe von 3 Quadraten genau dann, wenn n nicht von der Form $n = 4^m \cdot l$ mit $l \equiv 7 \mod 8$ ist.*

Beweis. $\Rightarrow$: Sei $n = 4^m l$. Es gilt $x^2 \mod 8 \in \{0, 1, 4\}$. Damit ist $x^2 + y^2 + z^2 \not\equiv 7 \mod 8$. Also ist der Fall $m = 0$ erledigt.
Sei nun $m \geq 1$ ein minimales Gegenbeispiel und $n = x^2 + y^2 + z^2 \equiv 0 \mod 4$. Dann sind x, y, z gerade. Also ist $\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2 = 4^{m-1} l$ eine Summe von drei Quadraten, was der Minimalität von m widerspricht.
Die andere Richtung ist deutlich schwieriger, benötigt Satz von Dirichlet und anderes. □

4.3 Lemma. *Sei $p \in \mathbb{P}$.*

(i) Es existieren $x, y \leq \frac{p}{2}$ mit $x^2 + y^2 + 1 \equiv 0 \mod p$.

(ii) Sei p ungerade. Dann gibt es $x_1 \leq \frac{p-1}{2}$ und $1 \leq h \leq p-1$ mit $x_1^2 + x_2^2 + x_3^2 + x_4^2 = hp$.

Beweis. Für$p = 2$ ist es klar.

(i) Die beiden Mengen $\{0^2, -1^2, -2^2, \ldots, -(\frac{1}{2}(p-1))^2\}$ und $\{1, 1^2+1, 2^2+1, \ldots, (\frac{1}{2}(p-1))^2 + 1\}$ enthalten jeweils $\frac{1}{2}(p+1)$ Elemente. Damit haben existieren darin k, l mit $k^2 + 1 \equiv -l^2 \mod p$ und somit $k^2 + l^2 + 1 \equiv 0 \mod p$.

(ii) Nach (i) existieren $x, y \leq \frac{p-1}{2}$ mit $x^2 + y^2 + 1 \equiv 0 \mod p$. Dann ist $0 < x^2 + y^2 + 1^2 + 0^2 < 4(\frac{1}{2}p)^2 = p^2$. Da es ein Vielfaches von p ist, folgt die Existenz eines solchen h. □

4.4 Satz (Lagrange). *Jede natürliche Zahl ist Summe von 4 Quadraten.*

Beweis. Für die Multiplikativität beobachte

$$\left(\sum_{i=1}^{4} x_i^2\right) \cdot \left(\sum_{i=1}^{4} y_i^2\right) = \left(\sum_{i=1}^{4} x_i y_i\right)^2 + (-x_1y_2 + x_2y_1 - x_3y_4 + x_4y_3)^2 \tag{10}$$

$$+ (-x_1y_3 + x_3y_1 - x_4y_2 + x_2y_4)^2 + (-x_1y_4 + x_4y_1 - x_2y_3 + y_3x_2)^2 \tag{11}$$

Erkennbar ist dies aus der Norm von Quaternionen. Damit genügt es, die Aussage für Primzahlen zu zeigen. $p = 2$ ist klar.
Sei p ungerade und sei $1 \leq h_0 \leq p$ minimal so, dass es $x_1^2 + x_2^2 + x_3^2 + x_4^2 = h_0 p$ gibt. Ist h_0 gerade, so sind alle oder keines der x_i ungerade. OBdA sei $x_1 - x_2$ und $x_3 - x_4$ gerade. Dann sind auch $x_1 + x_2$ und $x_3 + x_4$ gerade. Dann aber ist

$$\left(\frac{1}{2}(x_1 + x_2)\right)^2 + \left(\frac{1}{2}(x_3 + x_4)\right)^2 + \left(\frac{1}{2}(x_1 - x_2)\right)^2 + \left(\frac{1}{2}(x_3 - x_4)\right)^2 = \frac{h_0}{2} p$$

was der Minimalität von h_0 widerspricht. Also ist h_0 ungerade.
Angenommen $h_0 \geq 3$. Sei $-\frac{1}{2}h_0 < y_i < \frac{1}{2}h_0$ mit $x_i \equiv y_i \mod h_0$. Nicht alle y_i können 0 sein, da wir sonst alle x_i durch h_0 teilbar. Also ist $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < (\frac{1}{2}h_0)^2 = h_0^2$. Weiterhin gilt aber auch $\sum y_i^2 \equiv \sum x_i^2 \equiv 0 \mod h_0$. Also ist $\sum y_i^2 = h_1 h_0$ mit $h_1 < h_0$. Wegen $x_i \equiv y_i \mod h_0$, sind die letzten drei Summanden in (10) durch h_0 teilbar. Weiterhin ist aber $\sum x_i y_i = \sum x_i^2 \equiv 0 \mod h_0$. Wir können also h_0^2 aus jedem Summanden heraus ziehen. Das liefert

$$h_0 \cdot p \cdot h_0 h_1 = h_0^2(m_1^2 + m_2^2 + m_3^2 + m_4^2) \implies h_1 p = m_1^2 + m_2^2 + m_3^2 + m_4^2$$

mit $h_1 < h_0$, was der Minimalität widerspricht. Also folgt $h_0 = 1$. □

4.5 Definition. (i) Für $g \in \mathbb{N}_{\geq 2}$ sei $r_g(n) = \#\{(m_1, \ldots, m_g) \in \mathbb{Z}^g : n = m_1^2 + \ldots + m_g^2\}$ die Anzahl der Darstellungen von n als Summe von g Quadraten (mit Berücksichtigung der Reihenfolge).

(ii) Wir setzen

$$\sigma_u(n) := \sum_{d|n, 2\nmid d} d \qquad\qquad \delta(n) := \sum_{d|n, 2\nmid d} (-1)^{\frac{d-1}{2}}$$

Beispiel. Es ist $2 = (\pm 1)^2 + (\pm 1)^2$, also ist $r_2(2) = 4$. Außerdem ist $4 = 0^2 + (\pm 2)^2 = (\pm 2)^2 + 0^2$, also auch $r_2(4) = 4$. Allgemein ist $r_2(2^k) = 4$.

4.6 Lemma. *σ_u und δ sind multiplikativ.*

für δ. Seien $n_1, n_2 \in \mathbb{N}$ teilerfremd. Sei $d \mid n_1 n_2$, dann lässt sich d schreiben als $d = d_1 d_2$ mit $d_i \mid n_i$ und für d ungerade, sind d_1 und d_2 ungerade. Für ungerade Zahlen l, m gilt $lm - 1 + (l-1) + (m-1) = (l-1)(m-1)$. Daraus folgt $\frac{1}{2}(lm-1) \equiv \frac{1}{2}(l-1) + \frac{1}{2}(m-1) \mod 2$. Nun gilt

$$\begin{aligned}\delta(n_1 n_2) &= \sum_{d|n_1 n_2, 2\nmid d} (-1)^{\frac{d-1}{2}} = \sum_{d_1|n_1, d_2|n_2, 2\nmid d_i} (-1)^{\frac{d_1 d_2 - 1}{2}} = \sum_{d_1|n_1, d_2|n_2, 2\nmid d_i} (-1)^{\frac{d_1-1}{2}} (-1)^{\frac{d_2-1}{2}} \\ &= \sum_{d_1|n_1, 2\nmid d_1} (-1)^{\frac{d_1-1}{2}} \cdot \sum_{d_2|n_2, 2\nmid d_2} (-1)^{\frac{d_2-1}{2}} = \delta(n_1)\delta(n_2)\end{aligned}$$

Für σ_u: Übungsaufgabe □

Um das Problem nun zu lösen betrachten wir erzeugende Funktionen. Für die Potenzreihe gilt

$$\sum_{n=0}^{\infty} r_g(n) z^n = \left(\sum_{n=0}^{\infty} z^{m^2} \right)^g$$

4.7 Satz. *Sei $\Theta(z) := \sum_{m \in \mathbb{Z}} z^{m^2}$ für $z \in \mathbb{C}, |z| < 1$.*

$$\Theta(z)^2 = 1 + 4 \sum_{l=0}^{\infty} (-1)^l \frac{z^{2l+1}}{1 - z^{2l+1}} \qquad\qquad \Theta(z)^4 = 1 + 8 \sum_{l=0}^{\infty} \frac{l z^l}{1 + (-z)^l}$$

4.8 Satz. *Sei $n = 2^k \cdot \prod p^{\alpha_p}$ die Primfaktorzerlegung. Dann ist*

$$r_2(n) = 4\delta(n) = \begin{cases} 0 & : 2 \nmid \alpha_p \text{ für alle } p \equiv 3 \mod 4 \\ 4 \prod_{p \equiv 1 mod 4} \alpha_p & : sonst \end{cases}$$

Beweis. Mit Satz 4.7 haben wir

$$\begin{aligned}\sum_{n=0}^{\infty} r_2(n) z^n = \Theta(z)^2 &= 1 + 4 \sum_{l=0}^{\infty} (-1)^l \frac{z^{2l+1}}{1 - z^{2l+1}} = 1 + 4 \sum_{l=0}^{\infty} \sum_{m=1}^{\infty} (-1)^l z^{(2l+1)m} \\ &= 1 + 4 \sum_{n=1}^{\infty} \delta(n) z^n\end{aligned}$$

da wir für jeden ungeraden Teiler $2l+1 \mid n$ einen Term erhalten. Nach Lemma 4.6 genügt es, $\delta(n)$ auf Primzahlpotenzen zu untersuchen. Dabei gilt $\delta(2^k) = 1$, da 1 der einzige ungerade Teiler ist. Für ungerades $p \in \mathbb{P}$ gilt

$$\delta(p^k) = \sum_{m=0}^{k} (-1)^{\frac{p^m-1}{2}} = \begin{cases} 1+k & : p \equiv 1 \mod 4 \\ 1 & : p \equiv 3 \mod 4, k \text{ gerade} \\ 0 & : p \equiv 3 \mod 4, k \text{ ungerade} \end{cases}$$

Schlussbemerkung

□

4.9 Satz. *Es gilt* $r_4(n) = 8 \cdot (2 + (-1)^n)\sigma_u(n)$.

Beweis. Ähnlich zu Satz 2.8 haben wir

$$\begin{aligned} \sum_{m=0}^{\infty} r_4(n) z^n = \Theta(z)^4 = 1 + 8 \sum_{l=1}^{\infty} \frac{lz^l}{1-(-z)^l} &= 1 + 8 \sum_{l=1}^{\infty} lz^l \sum_{m=0}^{\infty} (-(-z)^l)^m \\ &= 1 + 8 \sum_{l=1}^{\infty} \sum_{m=0}^{\infty} (-1)^{(l+1)m} lz^{(m+1)l} = 1 + 8 \sum_{l=1}^{\infty} \sum_{m=1}^{\infty} (-1)^{(l+1)(m+1)} lz^{ml} \\ &= 1 + 8 \sum_{n=1}^{\infty} \Delta(n) z^n \end{aligned}$$

mit $\Delta(n) = \sum_{l \mid n} (-1)^{(l+1)(\frac{n}{l}+1)} l$. Wenn n ungerade, dann sind alle diese l ungerade und somit $(-1)^{(l+1)*} = 1$, also ist $\Delta(n) = \sum_{l \mid n} l = \sigma_u(n)$. Sei nun $n = 2^i k$ mit $i > 0$ und k ungerade. Ist $l \mid n$, so hat l die Form $l = 2^j v$ mit $j \leq i$ und $v \mid k$ ungerade. Dann ist

$$\begin{aligned} \Delta(n) &= \sum_{j=0}^{i} \sum_{v \mid k} (-1)^{(2^j v+1)(2^{i-j}\frac{k}{v}+1)} 2^j v = \sum_{j=0}^{i} \sum_{v \mid k} (-1)^{(2^j+1)(2^{i-j}+1)} 2^j v \\ &= \sum_{j=0}^{i} (-1)^{(2^j+1)(2^{i-j}+1)} 2^j \cdot \sum_{v \mid k} v = \sum_{j=0}^{i} (-1)^{(2^j+1)(2^{i-j}+1)} 2^j \cdot \sigma_u(n) \end{aligned}$$

In dieser Summe erhalten wir immer -1 außer in den Fällen $j = i$ oder $j = 0$. Damit ist es $1 - \sum_{j=1}^{i-1} 2^j + 2^i = 3$. Damit haben wir das gewünschte Ergebnis für gerades n. □

4.1 Pythagoreische Tripel

Definition. Ein Pythagoreisches Tripel ist ein Tripel $(x, y, z) \in \mathbb{Z}^3$ mit $x^2 + y^2 = z^2$ und $xyz \neq 0$. Es heißt *primitiv*, wenn $\mathrm{ggT}(x, y, z) = 1$ (damit sind sie auch paarweise teilerfremd). Für solch eine Lösung ist entweder x oder y eine gerade Zahl.

Bemerkung. Bereits Euklid wusste, dass es unendliche viele Pythagoreische Tripel gibt, nämlich von der Form $(2k+1, 2k^2+2k, 2k^2+2k+1)$.

4.10 Lemma. *Seien* $g, h, n, m \in \mathbb{N}$ *mit* $\mathrm{ggT}(g, h) = 1$ *und* $m^n = g \cdot h$. *Dann existieren* $g_1, h_1 \in \mathbb{N}$ *mit* $g = g_1^n$ *und* $h = h_1^n$ *und* $\mathrm{ggT}(g_1, h_1) = 1$.

Beweis. Induktion über m^n: Sei $p \in \mathbb{P}$ mit $p \mid m^n$, damit auch $p^n \mid m^n$. Dann folgt oBdA $p \mid g$. Da g und h teilerfremd, folgt $p \nmid h$, damit muss der komplette p-Anteil in g liegen. Es gilt also $g = p^n g'$ für ein $g' \in \mathbb{N}$. Nun ist $\left(\frac{m}{p}\right)^n = g'h$, also existieren nach IH teilerfremde g_1' und h' mit $g' = g_1'^n$ und $h = h_1^n$. Also ist auch $g = (pg_1')^n$ eine n-te Potenz. □

4.11 Satz. *Alle primitiven Pythagoreischen Tripel $(x, y, z) \in \mathbb{N}^3$ sind gegeben durch*

$$x = a^2 - b^2 \qquad y = 2ab \qquad z = a^2 + b^2$$

mit $a, b \in \mathbb{N}$, $a > b$, $\mathrm{ggT}(a, b) = 1$ und $a - b$ ist ungerade.

Beweis. $\Leftarrow$: Nachrechnen ergibt, dass dies tatsächlich Lösungen sind. Angenommen $p \mid x, y, z$. Wegen $x = (a - b)(a - b + 2b)$ ungerade, also $p \neq 2$. Weiter gilt $p \mid x + z = 2a^2$, also $p \mid a$ und aus $p \mid x - z = 2b^2$ folgt $p \mid b$. Damit $p \mid a, b$, also $p = 1$. Damit sind diese Lösungen primitiv.
$\Rightarrow$: Sei (x, y, z) eine primitive Lösung. Dann ist oBdA y gerade und x, z ungerade. Damit sind $x + z, x - z$ gerade. Sei also $m = \frac{1}{2}y$, $g = \frac{x+z}{2}$ und $h = \frac{x-z}{2}$. Dann gilt $m^2 = gh$. Angenommen $p \mid g, h$, dann folgt $p \mid g + h = z$ und $p \mid g - h = x$. Da die Lösung primitiv ist, folgt $p = 1$, also $\mathrm{ggT}(g, h) = 1$. Nach Lemma 4.10 gibt es teilerfremde $a, b \in \mathbb{N}$ mit $g = a^2$ und $h = b^2$. Damit ist $x = a^2 - b^2$, $z = a^2 + b^2$ und somit $y = 2ab$. Da nach Annahme x ungerade und natürlich, folgt $a > b$ und $a - b$ ungerade. □

4.12 Bemerkung. Für den Großen Satz von Fermat ($x^m + y^m = z^m$ hat für $m \geq 3$ keine Lösung in $\mathbb{N}^3$) genügt es, die Fälle $m = 4$ und $m \in \mathbb{P}_{>2}$ zu betrachten.

4.13 Satz. *Die Gleichung $x^4 + y^4 = z^4$ hat keine Lösung in $\mathbb{N}^3$.*

Beweis. Wegen $z^4 = (z^2)^2$ genügt es zu zeigen, dass $x^4 + y^4 = z^2$ keine Lösung in $\mathbb{N}^3$ hat. Sei (x, y, z) eine Lösung davon mit minimalem z, insbesondere $\mathrm{ggT}(x, y, z) = 1$. Betrachtung modulo 4 ergibt oBdA y gerade und x ungerade. Mit Bemerkung 4.12 existieren teilerfremde $a, b \in \mathbb{N}$ mit $x^2 = a^2 - b^2$, $z = a^2 + b^2$ und $y^2 = 2ab$, $a > b$ und $a - b$ ungerade. Wenn a gerade, ist b ungerade und damit $x^2 = a^2 - b^2 \equiv -1 \mod 4$, was ein Widerspruch ist. Also ist a ungerade und b gerade. Nun ist $x^2 + b^2 = a^2$ und die Zahlen sind teilerfremd. Mit Bemerkung 4.12 gibt es teielrfremde p, q mit $x = p^2 - q^2$, $b = 2pq$ und $a = p^2 + q^2$ mit $p > q$ und $p - q$ ungerade. Damit haben wir $y^2 = 2ab = 4pq(p^2 + q^2)$, bzw. $\left(\frac{y}{2}\right)^2 = pq(p^2 + q^2)$. Da p, q teilerfremd, sind $p, q, p^2 + q^2$ paarweise teilerfremd. Wir wenden Satz 4.11 dreimal an, mit $g = p$ und mit $g = q$. Also sind beides Quadratzahlen, sagen wir $p = r^2$ und $q = s^2$, sowie $p^2 + q^2 = t^2$. Damit gilt $r^4 + s^4 = t^2$, aber $z = a^2 + b^2 = (p^2 + q^2)^2 + 4p^2q^2 > t^4$, was der Minimalität widerspricht. □

4.14 Definition. Sei $f(x, y) = c_{00} + 2c0, 1x + 2x_{0,2}y + c_{1,1}x^2 + 2c_{1,2}xy + c_{2,2}y^2 \in \mathbb{Q}[x, y]$.

$$f = (1, x, y) \cdot C \cdot (1, x, y)^T \qquad C := \begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} \\ c_{0,1} & c_{1,1} & c_{1,2} \\ c_{0,2} & c_{1,2} & c_{2,2} \end{pmatrix}$$

Sei $\det C \neq 0$ und sei f irreduzibel. Dann heißt f eine algebraische Kurve vom Grad 2.

Beispiel. Betrachte

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} \implies f = 1 + x^2 + y^2 + 4xy \qquad \text{Hyperbel}$$

$$C = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \implies f = 1 + x^2 + y^2 \qquad \text{Kreis}$$

4.15 Satz. *Sei f eine algebraische Kurve vom Grad 2 und sei $(x_0, y_0) \in \mathbb{Q}^2$ mit $f(x_0, y_0) = 0$. Dann besitzt f unendlich viele rationale Nullstellen. Bis auf eine Ausnahme ergeben sich alle Lösungen als Werte einer rationalen Funktion in einer Unbekannten. Die rationalen Koeffizienten der Funktion hängen nur von f, x_0, y_0 ab.*

Beweis. Wir betrachten das Taylorprolynom von $f(x, y)$ an der Stelle (x_0, y_0). Dafür ist

$$f(x,y) = \underbrace{f(x_0,y_0)}_{=0} + \nabla f(x_0,y_0)(x_0,y_0)^T \begin{pmatrix} x - x_0 \\ y - y_0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} x - x_0 \\ y - y_0 \end{pmatrix}^T H_f(x_0,y_0) \begin{pmatrix} x - x_0 \\ y - y_0 \end{pmatrix} = 2d_1(x - x_0) +$$

mit $d_1 = c_{0,1} + c_{1,1}x_0 + c_{1,2}y_0$ und $d_2 = c_{0,2} + c_{1,2}x_0 + c_{2,2}y_0$. Höhere Ableitungen tauchen nicht auf, da $\deg f = 2$.
Nun stellen wir fest, dass der Gradient nicht verschwinden kann, also $d_1^2 + d_2^2 \neq 0$: Angenommen $d_1 = d_2 = 0$. Wegen $f(x_0, y_0) = 0$ wäre dann $(1, x_0, y_0) \in \overline{ker}C$, was $\det C \neq 0$ widerspricht.

ausführlicher?

Sei nun $k \in \mathbb{Q}$ mit $c_{1,1}k^2 + 2c_{1,2}k + c_{1,2} \neq 0$ (das schließt max. 2 Werte aus) und sei

$$\begin{aligned} t(k) &:= \frac{2(d_1k + d_2)}{c_{1,1}k^2 + 2c_{1,2}k + c_{2,2}} \\ x(k) &:= x_0 + t(k) \cdot k \\ y &:= y_0 + t(k)\} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + t(k) \begin{pmatrix} k \\ 1 \end{pmatrix} \end{aligned}$$

Wenn wir dies ins Taylorpolynom einsetzen, erhalten wir

$$f(x(k), y(k)) = 2d_1kt(k) + 2d_2t(k) + c_{1,1}k^2t(k)^2 + 2c_{1,2}kt(k)^2 + c_{2,2}t(k)^2 = t(k)\left(2d_1k + 2d_2 + c_{1,1}k^2t(k)\right.$$

Nun ist zu zeigen, dass alle diese Lösungen verschieden sind. Dies folgt durch

$$\begin{aligned} x(k) = x(k') \wedge y(k) = y(k') &\Leftrightarrow t(k)k = t(k')k' \wedge t(k) = t(k') \\ &\xRightarrow{t(k)\neq 0} k = k' \\ &\xRightarrow{t(k)=0} \end{aligned}$$

Zuletzt zeigen wir, dass dies alle Lösungen sind. Angenommen, wir haben eine weitere finish

Lösungen $(\overline{x}, \overline{y})$. Sei $\overline{y} \neq y_0$ und $t := \overline{y} - y_0$ und $k = \frac{\overline{x}-x_0}{t}$. Wieder nutzen wir das Taylorpolynom

$$0 = f(\overline{x}, \overline{y}) = 2d_1(\overline{x} - x_0) + 2d_2(\overline{y} - y_0) + c_{1,1}(\overline{x} - x_0)^2 + c_{1,2}(\overline{x} - x_0)(\overline{y} - y_0) + c_{2,2}(\overline{y} - y_0) = 2d_1tk + 2$$

Wäre nun $c_{1,1}k^2 + 2c_{1,2}k + c_{2,2} = 0$, dann wäre $2d_1k + 2d_2 = 0$, also $(x_0, y_0) + t(k, 1)$ eine Lösung für alle $t \in \mathbb{R}$. Dies widerspricht aber der Annahme f irreduzibel. Daraus folgt $t = -\frac{2(d_1k+d_2)}{c_{1,1}k^2+2c_{1,2}k+c_{2,2}}$ hängt nicht von x, y ab.
Im zweiten Fall sei $\overline{y} = y_0$, aber $\overline{x} \neq x_0$. Dann ist wieder

$$0 = f(\overline{x}, y_0) = 2d_1(\overline{x} - x_0) + c_{1,1}(\overline{x} - x_0)^2 \Leftrightarrow 0 = 2d_1 + c_{1,1}(\overline{x} - x_0)$$

Wie zuvor würde diese eine Gerade an Lösungen liefern, was der Irreduzibilität widerspricht. □

Beispiel. Sei wieder $f = x^2 + y^2 - 1$ mit Startlösung $x_0 = 0$ und $y_0 = 1$. Dann erhalten wir $y(k) = t(k) = \frac{2k}{k^2+1}$ und $x(k) = -1 + t(k) \cdot k = \frac{k^2-1}{k^2+1}$. Wenn wir $k = \frac{a}{b}$ schreiben, dann passt es zu obiger Analyse der pythagoreischen Tripel. cref

4.16 Definition. Für $k \geq 2$ setze $g(k) := \inf \left\{ g \in \mathbb{N} : \forall n ß \mathbb{N}. \exists m_1, \ldots, m_g. n = \sum m_i^k \right\}$.

4.17 Satz. *Für $k \geq 2$ gilt $g(k) \geq 2 + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$.*

Beweis. Betrachte $n_k := 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 < 3^k$. Sei nun $n_k = m_1^k + \ldots + m_g^k$ eine minimale Darstellung mit k-ten Potenzen. Dann gilt $m_i \in \{1, 2\}$ für alle i. Setze $\alpha_j := \#\{i : m_i = j\}$. Damit ist $n_k = \alpha_1 + \alpha_2 \cdot 2^k$. Ferner gilt

$$\begin{aligned} g(k) \geq g = \alpha_1 + \alpha_2 = n_k - \alpha_2(2^k - 1) &\geq n_k - \left(\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 \right) (2^k - 1) \\ &= 2 + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2 \end{aligned}$$

□

Bemerkung. Es wird vermutet, dass diese untere Schranke zugleich auch die Lösung ist, also Gleichheit gilt.

5 Zahlentheoretische Funktionen

Häufig verwendet man "zahlentheoretische Funktionen" und "multiplikative" Funktionen als Synonyme. Beispiele, für die man sich interessiert, sind

- $\tau(n) = \sum_{d|n} 1$
- $\sigma(n) = \sum_{d|n} d$

- $\varphi(n)$

5.1 Satz. *Sei $f : \mathbb{N} \to \mathbb{C}$ multiplikativ. Dann ist $F(n) := \sum_{d|n} f(d)$ ebenfalls multiplikativ.*

Beweis. Seien n, m teilerfremd. Jedes $d \mid nm$ lässt sich eindeutig schreiben als $d = d_1 d_2$ mit $d_1 \mid m$ und $d_2 \mid n$. Damit ergibt sich

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2) = \sum_{d_1|m, d_2|n} f(d_1) f(d_2) = F(m) \cdot F(n)$$

□

Damit erhalten wir sofort, dass τ, σ multiplikativ sind, durch $f(n) = 1$ und $f(n) = n$.

5.2 Definition. (i) Eine Zahl $n \in \mathbb{N}$ heißt vollkommen, wenn $\sigma(n) = 2n$.

(ii) $M_n = 2^n - 1$ heißen Mersenne-Zahlen. Diese sind insbesondere interessant, weil sich auf diese Art häufig Primzahlen finden lassen. Wenn $M_n \in \mathbb{P}$, dann ist $n \in \mathbb{P}$.

5.3 Satz. *$n \in \mathbb{N}$ ist eine gerade, vollkommene Zahl genau dann, wenn es ein $k \in \mathbb{N}$ gibt mit $n = 2^k(2^{k+1} - 1)$ und $2^{k+1} - 1$ ist eine Primzahl. Insbesondere ist dieser Exponent prim.*

Beweis. $\Leftarrow$: Mit der Multiplikativität von σ ist

$$\sigma(n) = \sigma(2^k) \cdot \sigma(2^{k+1} - 1) = \sum_{i=0}^{k} 2^i \cdot 2k + 1 = \left(2^{k+1} - 1\right) \cdot 2 \cdot 2^k = 2n$$

$\Rightarrow$: Schreibe $n = 2^k n'$ mit $2 \nmid n'$ und $k \geq 1$.

$$2^{k+1} n' = \sigma(n) = \sigma(2^k)\sigma(n') = \left(2^{k+1} - 1\right) \sigma(n')$$
$$\implies 2^{k+1} - 1 \mid n' \implies n' = \left(2^{k+1} - 1\right) \cdot n'' \implies \sigma(n') = 2^{k+1} n'' \implies n' + n'' = 2^{k+1} n'' = \sigma(n')$$

Damit kann n' keinen weiteren Teiler mehr haben, sonst passt die Summe nicht mehr. Und damit ist $n'' = 1$ und n' ist prim. □

5.4 Bemerkung. kommt noch

5.5 Definition. Die Möbius-Funktion $\mu : \mathbb{N} \to \{-1, 0, 1\}$ ist definiert als

$$\mu(n) = \begin{cases} 1 & : n = 1 \\ 0 & : \exists a. a^2 \mid n \\ (-1)^r & : n = p_1 \cdot \ldots \cdot p_r, p_i \in \mathbb{P} \end{cases}$$

5.6 Lemma. *μ ist multiplikativ und es ist $\sum_{d|n} \mu(d) = \begin{cases} 1 & : n = 1 \\ 0 & : sonst \end{cases}$ (ebenfalls multiplikativ).*

Beweis. Multiplikativität von μ ist klar (Fallunterscheidung). Damit ist $M(n) := \sum_{d|n} \mu(d)$ ebenfalls multiplikativ nach Satz 5.1. Sei $p \in \mathbb{P}$, $n \in \mathbb{N}$. Dann ist $M(p^n) = 1-1+0+\ldots = 0$ und $M(p^0) = 1$. □

5.7 Satz. *Sei $f : \mathbb{N} \to \mathbb{C}$ und $F(n) := \sum_{d|n} f(d)$. Dann ist*

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

Beweis. Es gilt

$$\begin{aligned}\sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) &= \sum_{d_1 d_2 = n} \mu(d_1)F(d_2) = \sum_{d_1 d_2 = n} \mu(d_1) F\left(\sum_{d|d_2} f(d)\right) = \sum_{d_1 d|n} \mu(d_1) f(d) \\ &= \sum_{d|n} f(d) \cdot \sum_{d_1 | \frac{n}{d}} \mu(d_1) \overset{Lemma\ 5.6}{=} f(n)\end{aligned}$$

□

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

Beweis. Nach Satz 1.38 ist $F(n) = \sum_{d|n} \varphi(d) = n$. Eingesetzt in Satz 5.7 in der zweiten Form ergibt die Behauptung. □

5.9 Satz. *Seien $F, f : \mathbb{N} \to \mathbb{C}$ und $F(n) := \sum_{d|n} f(d)$.*

(i) Wenn F multiplikativ ist, dann ist auch f multiplikativ.

(ii) $\sum_{k=1}^{n} F(k) = \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor f(k)$.

Beweis. (i) Die Multiplikativität folgt wie üblich, mittels Satz 5.7

$$\begin{aligned}f(mn) &= \sum_{d_1|m, d_2|n} F(d_1 d_2)\mu\left(\frac{m}{d_1}\frac{n}{d_2}\right) = \sum_{d_1|m, d_2|n} F(d_1)F(d_2)\mu\left(\frac{m}{d_1}\right)\mu\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} F(d_1)F\mu\left(\frac{m}{d_1}\right) \cdot \sum_{d_2|n} F(d_2)\mu\left(\frac{n}{d_2}\right) = f(m)f(n)\end{aligned}$$

(ii) Es gilt durch Umsortierung der Summanden

$$\sum_{k=1}^{n} F(k) = \sum_{k=1}^{n} \sum_{d|k} f(d) = \sum_{d=1}^{n} \sum_{k=1}^{\left\lfloor \frac{n}{d} \right\rfloor} f(d) = \sum_{d=1}^{n} \left\lfloor \frac{n}{d} \right\rfloor f(d)$$

□

5.10 Definition (Landau-Notation). Für die Größenordnung definieren wir

$$\begin{aligned}\mathcal{O}(g) &= \left\{ f : \mathbb{N} \to \mathbb{N} : \limsup_{n\to\infty} \frac{f(n)}{g(n)} < \infty \right\} \\ o(g) &= \left\{ f : \mathbb{N} \to \mathbb{N} : \limsup_{n\to\infty} \frac{f(n)}{g(n)} = 0 \right\} \\ \Theta(g) &= \{ f \in \mathcal{O}(g) : g \in \mathcal{O}(f) \}\end{aligned}$$

Wie üblich schreiben wir $\mathcal{O}(n^2)$ statt $\mathcal{O}(\lambda n.n^2)$.

Beispiel. $\ln(x) \in o(x^\varepsilon)$ für alle $\varepsilon > 0$.

5.11 Lemma. *Sei f multiplikativ und sei $\lim_{p^m \to \infty} f(p^n) = 0$ für alle Folgen von Primzahlpotenzen (kein festes p!). Dann ist $\lim_{n\to\infty} f(n) = 0$.*

Beweis. Nach Voraussetzung existiert ein $A > 0$ mit $|f(p^m)| \leq A$ für alle p^m. Weiter existiert ein $B \geq 1$ mit $f(p^m)| \leq 1$ für alle $p^m \geq B$ und für jedes $\varepsilon > 0$ existiert ein $c = c(\varepsilon) \in \mathbb{N}$ mit $|f(p^m)| \leq \frac{\varepsilon}{A^B}$ für $p^{\geq} c$. Schreibe nun n als $n = \prod_{p\in\mathbb{P}} p^{\alpha_p} > c^c$. Dann existiert ein Faktor mit $p^{\alpha_p} > c$. Wegen der Multiplikativität ist

$$|f(n)| = \prod_{p\in\mathbb{P}} |f(p^{\alpha_p})| = \prod_{p^{\alpha_p}\leq B} |f(p^{\alpha_p})| \cdot \prod_{B<p^{\alpha_p}\leq c} |f(p^{\alpha_p})| \cdot \prod_{c<p^{\alpha_p}} |f(p^{\alpha_p})| \leq A^b \cdot \frac{\varepsilon}{A^B} = \varepsilon$$

□

5.12 Proposition. *(i) Für die Anzahl der Teiler gilt $\tau(n) \in o(n^\varepsilon)$ für alle $\varepsilon > 0$, aber $\limsup_{n\to\infty} \frac{\tau(n)}{\ln(n)^k} > 0$.*

(ii) $\varphi(n) \in \mathcal{O}(n)$, und $n^{1-\varepsilon} \in o(\varphi(n))$. $\sigma(n) \in \mathcal{O}(n \log n)$ und $n \in \mathcal{O}(\sigma(n))$.

Beweis. (i) Beachte $f(n) := \frac{\tau(n)}{n^\varepsilon}$ ist multiplikativ und für $p \in \mathbb{P}$ gilt

$$f(p^m) = \frac{\tau(p^m)}{p^{\varepsilon m}} = \frac{m+1}{p^{\varepsilon m}} \leq \frac{2m}{p^{\varepsilon m}} = \frac{2\log p^m}{\varphi^{\varepsilon m}\log p} \leq \frac{2}{\log 2} \cdot \frac{\log p^m}{(p^m)^\varepsilon} \xrightarrow{n\to\infty} 0$$

Für $m \in \mathbb{N}$ sei $n := (2 \cdot 3 \cdot \ldots \cdot p_k)^m$, vom Produkt der ersten k Primzahlen. Dann ist

$$\tau(n) = (m+1)^k \sim m^k = \left(\frac{\log n}{\log(2\cdot 3\cdot \ldots \cdot p_k)}\right)^k \geq c_k \cdot (\log n)^k$$

da wir das Produkt der ersten k Primzahlen durch eine Funktion in k abschätzen können.

(ii) $\varphi(n) \leq n$ ist klar. Sei nun $f(n) = \frac{n^{1-\varepsilon}}{\varphi(n)}$, dies ist multiplikativ. Für $p \in \mathbb{P}$ ist

$$f(p^m) = \frac{p^{m(1-\varepsilon)}}{(p-1)p^{m-1}} = \frac{1}{p^{m\varepsilon}} \cdot \frac{p}{p-1} \leq \frac{2}{p^{m\varepsilon}}$$

(iii) Wir wissen $\sigma(n) \geq n+1 > n$. Damit ist $n \in \mathcal{O}(\sigma(n))$. Nun ist

$$\sigma(n) = \sum_{d|n} \frac{n}{d} = n \cdot \sum_{d|n} \frac{1}{d} \leq n \cdot \sum_{d=1}^{n} \frac{1}{d} \leq n(1+\ln n) \in \mathcal{O}(n\log n)$$ □

Wir wollen als nächstes zwei Resultate über die Kehrwerte von Primzahlen zeigen.

$$\sum_{p\leq x} \frac{1}{p} \approx \ln\ln x \qquad\qquad \sum_{p,p+2\in\mathbb{P}} \frac{1}{p} + \frac{1}{p+2} < \infty$$

5.13 Satz. *(i) Es gibt eine Konstante $\gamma \approx 0.57721\ldots$ (Euler-Mascheroni) so, dass $\sum_{k=1}^{n} \frac{1}{k} \in \ln n + \gamma + \mathcal{O}(\frac{1}{n})$.*

(ii) Es gilt $\sum_{k=1}^{n} \ln n \in n \ln n + \mathcal{O}(n)$.

Beweis. (i) Bild, Integral 1/x vs Summe

Setze $\alpha_k = \ln k - \ln(k-1) - \frac{1}{k}$ für $k \geq 2$. Dann ist α_k der Fehler im Intervall $[k-1, k]$, den man macht, wenn man den Summanden durch das Integral abschätzt. Der Fehler, bei Summation bis n sei $\gamma_n = \sum_{k=1}^{n} \frac{1}{k} - \ln n$. Daraus ergibt sich die Teleskopsumme

$$\sum_{k=2}^{n} \alpha_k = \ln n - \sum_{k=2}^{n} \frac{1}{k} = 1 - \gamma_n$$

Zu jedem α_k nehmen wir das die Fläche umschließende Rechteck. Indem wir alle Rechtecke nach links an die y-Achse schieben, erhalten wir, dass die Summe ihrer Flächeninhalte 1 ist. Da $\frac{1}{x}$ konvex ist, liegt jede dieser α_k-Flächen in der unteren Hälfte, also $\sum \alpha_k < \frac{1}{2}$. Damit gilt $0 < 1 - \gamma_n < \frac{1}{2}$ und $1 - \gamma_{n+1} > 1 - \gamma_n$. Setze nun $1 - \gamma = \lim_{n\to\infty} 1 - \gamma_n$. Daraus folgt

$$\gamma_n - \gamma = (1-\gamma) - (1-\gamma_n) = \sum_{k=n+1}^{\infty} \alpha_k < \frac{1}{n}$$

$$\implies \sum_{k=1}^{n} \frac{1}{k} = \ln n + \gamma_n \in \ln n + \gamma + \mathcal{O}\left(\frac{1}{n}\right)$$

(ii) Wir nutzen die Stirling-Formel $n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n$. Logarithmieren ergibt

$$\sum_{k=1}^{n} \ln k = \ln(n!) \in n \ln n - n + (O \ln n) \subseteq n \ln n + \mathcal{O}(n) \qquad \square$$

5.14 Satz. *Es gilt*

$$\sum_{k=1}^{n} \tau(k) \in n \ln n + (2\gamma - 1)n + \mathcal{O}(\sqrt{n})$$

Beweis. Aus Satz 5.9 (oder scharfes Hinsehen) erhalten wir

$$\begin{aligned}
\sum_{k=1}^{n} \tau(k) &= \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor = \#\{(x,y) \in \mathbb{N}^2 : xy \leq n\} \\
&= 2\#\{(x,y) \in \mathbb{N}^2 : xy < n, y > x\} + \#\{(x,x) \in \mathbb{N}^2 : x^2 \leq n\} \\
&= 2 \sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \left(\left\lfloor \frac{n}{k} \right\rfloor - k \right) + \lfloor\sqrt{n}\rfloor \\
&= 2 \sum_{k=1}^{\lfloor\sqrt{n}\rfloor} \left(\frac{1}{k} \right) + \mathcal{O}(\sqrt{n}) + \frac{\lfloor\sqrt{n}\rfloor(\lfloor\sqrt{n}\rfloor + 1)}{2} + \lfloor\sqrt{n}\rfloor \\
&= 2n \left(\ln\lfloor\sqrt{n}\rfloor + \gamma + \mathcal{O}\left(\frac{1}{\lfloor\sqrt{n}\rfloor} \right) \right) - n + \mathcal{O}(\lfloor\sqrt{n}\rfloor) \\
&= n \ln n - (2\gamma - 1)n + \mathcal{O}(\lfloor\sqrt{n}\rfloor)
\end{aligned}$$

Die zweite Summe fassen wir auf als alle Gitterpunkte, die unterhalb der Funktion $y = \frac{n}{x}$ liegen. Diese Funktion ist symmetrisch an der ersten Winkelhalbierenden. □

5.15 Definition. Die Riemannsche Zeta-Funktion $\zeta : \mathbb{C} \setminus \{1\} \to \mathbb{C}$ ist die analytische Fortsetzung der Dirichlet-Summe $\sum_{n=1}^{\infty} \frac{1}{n^s}$, die konvergent ist für alle $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$.

5.16 Bemerkung. (i) $\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \cdot \zeta(1-s)$. Daraus ergeben sich die trivialen Nullstellen $s = -2m$ für $m \in \mathbb{N}$, weil dann der Sinus 0 wird. Im positiven geht das nicht, da dann $\Gamma(1-s)$ einen Pol hat. Die Riemannsche Vermutung sagt nun, dass für jede weitere Nullstelle gilt $\mathrm{re}(s) = \frac{1}{2}$.

(ii) $\zeta(2) = \sum_{\frac{1}{n^2}} = \frac{\pi^2}{6}$

5.17 Satz. *Sei* $\mathrm{Re}(s) > 1$. *Dann gilt*

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

Beweis.

$$\zeta(s) \cdot \sum \frac{\mu(n)}{n^s} = \left(\sum \frac{1}{n^s} \right) \cdot \left(\sum \frac{\mu(n)}{n^s} \right) = \sum_{m,n=1}^{\infty} \frac{\mu(n)}{(mn)^s} = \sum_{k=1}^{\infty} \frac{1}{k^s} \cdot \sum_{n|k} \mu(n) \overset{5.6}{=} 1 \qquad \square$$

5.18 Satz. *Für sie Summe der Phi-Funktion gilt*

$$\sum_{k=1}^{n} \varphi(k) \in \frac{3}{\pi^2} n^2 + \mathcal{O}(n \ln n)$$

Beweis. Für Quadrate gilt $\lfloor x \rfloor^2 \in x^2 + \mathcal{O}(x)$. Damit erhalten wir

$$\begin{aligned}
\sum_{k=1}^{n} \varphi(k) &\overset{5.8}{=} \sum_{m=1}^{n} m \sum_{d|m} \frac{\mu(d)}{d} = \sum_{m=1}^{n} \sum_{dd'=m} d'\mu(d) = \sum_{dd' \le n} d'\mu(d) \\
&= \sum_{d=1}^{n} \mu(d) \left(\sum_{d'=1}^{\lfloor \frac{n}{d} \rfloor} d' \right) = \sum_{d=1}^{n} \mu(d) \cdot \frac{\lfloor \frac{n}{d} \rfloor^2 + \lfloor \frac{n}{d} \rfloor}{2} \\
&= \frac{1}{2} \sum_{d=1}^{n} \mu(d) \cdot \left\lfloor \frac{n}{d} \right\rfloor^2 + \mathcal{O}\left(\sum_{d=1}^{n} a \frac{n}{d} \right) = \frac{n^2}{2} \left(\sum_{d=1}^{n} \frac{\mu(d)}{d^2} + \sum_{d|mn} \infty \frac{\mu(d)}{d^s} \right) + \mathcal{O}(n \ln n) \\
&= \frac{n^2}{2} \cdot \frac{1}{\zeta(2)} + \mathcal{O}\left(n^2 \cdot \sum_{d=n+1}^{\infty} \frac{1}{d^2} \right) + \mathcal{O}(n \ln n) = \frac{3}{\pi^2} n^2 + \mathcal{O}(n) + \mathcal{O}(n \ln n) \qquad \square
\end{aligned}$$

5.19 Korollar. *Wir betrachten die vom Nullpunkt sichtbaren Gitterpunkte*

$$\alpha := \lim_{n \to \infty} \frac{1}{N} \#\{(a,b) \in \mathbb{N}^2 : a, b \le N, \mathrm{ggT}(a,b) = 1\}$$

Dann ist $\alpha = \frac{6}{\pi^2}$

Beweis. Übung $\square$

5.20 Satz.

$$\sum_{k=1}^{n} \sigma(k) = \frac{\pi^2}{12} n^2 + \mathcal{O}(n \ln n)$$

Beweis. Übung $\square$

3 Vorlesungen fehlen

5.32 Lemma. *Setze* $P(x) = x \left(\frac{\ln \ln x}{\ln x} \right)^2$. *Sei* $x \ge 3$ *und* $y \le \sqrt{x}$.

Beweis. Wir haben $A(x,y) = \{(n, n+2) : 1 \le n \le x, \text{es ex. kein } p \in \mathbb{P}_{\le y} \text{ mit } p \mid n(n+2)\}$. Zu zeigen: $\#A(x,y) \in \mathcal{O}(P(x))$ für ein $y = y(x)$ mit $\pi(y) \in \mathcal{O}(P(x))$.

$$R := \prod_{p \in \mathbb{P}_{\le y}} p$$

$$\#A(x,y) \le C \left(x \cdot \prod_{p|R, p>2} \left(1 - \frac{p}{2}\right) + \pi(y)^{2k} + x\omega_3 \right)$$

$$\text{und } \omega_3 = \sum_{p_1 \dots p_{2k+1} | R, p_1 < \dots < p_{2k+1}} \frac{\tau'(p_1 \dots p_{2k+1})}{p_1 \dots p_{2k+1}}$$

Dann schätzen wir ab mit

$$\sum_{p_1\dots p_{2k+1}|R, p_1<\dots<p_l} \frac{\tau'(p_1\dots p_l)}{p_1\dots p_l} \leq \sum_{p_1\dots p_{2k+1}|R, p_1<\dots<p_l} \frac{2^l}{p_1\dots p_l} \leq \frac{1}{l!}\cdot\left(\sum_{p\in\mathbb{P}_{\leq y}} \frac{2}{p}\right)^l$$

„Multinom“

Mit **??** und $l! \geq \frac{l^l}{e^l}$ (Stirling) erhalten wir

$$\begin{aligned}\omega_3 &< \sum_{2k<l\leq\pi(y)} \frac{1}{l!}\left(\sum_{pin\mathbb{P}_{\leq y}} \frac{2}{p}\right)^l \overset{??}{<} \sum_{2k<l\leq\pi(y)} \frac{1}{l!}(2\ln\ln y + C)^l < \sum_{2k<l\leq\pi(y)} \left(\frac{(2\ln\ln y + C)e}{l}\right)^l \\ &< \sum_{2k<l} \left(\frac{k}{l}\right)^l < \sum_{2k<l} \left(\frac{1}{2}\right)^l = \left(\frac{1}{2}\right)^{2l} = 2^{\lfloor -6\ln\ln y\rfloor} y \leq 2^{-10\ln\ln y} \leq (|\ln y|)^{-6}\end{aligned}$$

Nun schätzen wir noch das Produkt ab.

$$\prod_{p\in\mathbb{P}_{\leq y}} \left(1-\frac{2}{p}\right) \leq \prod_{p\in\mathbb{P}_{\leq y}} \left(\left(1-\frac{1}{p}\right)^2 - \frac{1}{p^2}\right) < \prod_{p\in\mathbb{P}_{\leq y}} \left(1-\frac{1}{p}\right)^2 < \left(\frac{1}{\ln y}\right)^2$$

Das liefert uns

$$\begin{aligned}\#A(x,y) &\leq C\left(\frac{x}{(\ln y)^2} + \pi(y)^{2k} + \frac{x}{(\ln y)^6}\right) \leq \overline{C}\left(\frac{x}{(\ln y)^2} + \pi(y)^{2k}\right) \\ \Longrightarrow \pi_2(x) &\leq \widetilde{C}\left(\frac{x}{(\ln y)^2} + \pi(y)^{2k}\right) \overset{??}{\leq} \widetilde{C}\left(\frac{x}{(\ln y)^2} + \left(\frac{C_2 y}{\ln y}\right)^{2\lfloor 6\ln\ln y\rfloor}\right)\end{aligned}$$

Mit der Wahl $y = x^{\frac{1}{12\ln\ln x}}$, also $\ln y = \frac{\ln x}{12\ln\ln x}$ erhalten wir

$$\leq C_3 x\left(\frac{\ln x}{\ln\ln x}\right)^2 + c_5\left(x^{\frac{1}{12\ln\ln x}}\cdot\frac{\ln\ln x}{\ln x}\right)^{12\ln\ln x} \in \mathcal{O}(P(x)) \qquad \square$$

6 Geometrie der Zahlen

6.1 Definition. (i) Eine Menge $C \subseteq \mathbb{R}^n$ heißt konvex, wenn $\forall x, y \in C. \forall \lambda \in [0,1]. \lambda x + (1-\lambda)y \in C$. Die Menge aller kompakten, konvexen Mengen wird bezeichnet mit $\mathcal{K}^n$.

(ii) Für $X, Y \subseteq \mathbb{R}^n, \mu \in \mathbb{R}$ setze

$$X + Y = \{x + y : x \in X, y \in Y\} \qquad \mu X = \{\mu x : x \in X\}$$

(iii) $X \subseteq \mathbb{R}^n$ heißt 0-symmetrisch, falls $X = -X$. Setze $\mathcal{K}_0^n := \{K \in \mathcal{K}^n : K = -K\}$.

(iv) Für $X \subseteq \mathbb{R}^n$ sei $\mathrm{vol}(X)$ das Volumen (Riemann/Lebesgue/...).

(v) Für $S \subseteq \mathbb{R}^n$ setzen wir

$$\operatorname{lin}_{\mathbb{Z}} S := \operatorname{span}_{\mathbb{Z}}(S) = \left\{ \sum_{i=1}^{m} z_i s_i : z_i \in \mathbb{Z}, s_i \in S, m \in \mathbb{N} \right\}$$

Beispiel. Beispiele für 0-symmetrische Mengen sind $B_n = \{x \in \mathbb{R}^n : |x| \leq 1\}$, $W_n := [-1,1]^n$ und $B_{1,n} := \{x \in \mathbb{R}^n : \sum |x_i| = 1\}$. Generell gehen alle Einheitskugeln bezüglich einer beliebigen Norm.
Diese haben Volumen $\operatorname{vol}(W_n) = 2^n$, $\operatorname{vol}(B_{1,n} = \frac{2^n}{n!}$ und $\operatorname{vol}(B_n) = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)}$.

Lemma. *Für das Volumen haben wir die Rechenregeln*

- $\operatorname{vol}(\mu X) = \mu^n \cdot \operatorname{vol}(X)$
- $\operatorname{vol}(A \cdot X) = |\det A| \cdot \operatorname{vol}(X)$ *für eine lineare Abbildung* A.

6.2 Definition. Seien $b_1, \ldots, b_n \in \mathbb{R}^n$ linear unabhängig. Die Menge $\Lambda = \operatorname{lin}_{\mathbb{Z}}\{b_1, \ldots, b_n\}$ heißt *Gitter*, die Elemente heißt *Gitterpunkt*. Die Menge $\{b_1, \ldots, b_n\}$, bzw. die Matrix $B = (b_1, \ldots, b_n)$ heißt *Basis von* Λ. Dann Gitter lässt sich dann schreiben als $\Lambda = B\mathbb{Z}^n$.

6.3 Bemerkung. (i) $e_1, \ldots, e_n$ bilden eine Basis von $\mathbb{Z}^n$.

(ii) Λ ist eine (additive) Untergruppe von $\mathbb{R}^n$.

(iii) Die Basis ist nicht eindeutig, siehe das folgende Beispiel.

Beispiel. Nehmen wir $B = \begin{pmatrix} 25 & 64 \\ 16 & 41 \end{pmatrix}$, dann ist $\Lambda := B\mathbb{Z}^2 = \mathbb{Z}^2$. Der Grund dafür ist, dass $\det B = 1$, also ist B über $\mathbb{Z}^2$ invertierbar.

6.4 Definition. Eine ganzzahlige Matrix $U \in \mathbb{Z}^{n \times n}$ heißt *unimodular* falls $|\det U| = 1$. Die *lineare Gruppe* ist

$$\overline{GL}(n, \mathbb{Z}) = \left\{ U \in \mathbb{Z}^{n \times n} : |\det U| = 1 \right\}$$

6.5 Proposition. $\operatorname{GL}(n, \mathbb{Z}) = \{U \in \mathbb{R}^{n \times n} : U\mathbb{Z}^n = \mathbb{Z}^n\}$.

Beweis. Wir haben die Kette

$$\begin{aligned} U \in \operatorname{GL}(n, \mathbb{Z}) &\Leftrightarrow U, U^{-1} \in \mathbb{Z}^n \Leftrightarrow U\mathbb{Z}^n \subseteq \mathbb{Z}^n \wedge U^{-1}\mathbb{Z}^n \subseteq \mathbb{Z}^n \\ &\Leftrightarrow U\mathbb{Z}^n \subseteq \mathbb{Z}^n \wedge \mathbb{Z}^n \subseteq U\mathbb{Z}^n \Leftrightarrow U\mathbb{Z}^n = \mathbb{Z}^n \end{aligned}$$ □

6.6 Lemma. *Sei* $\Lambda = B\mathbb{Z}^n$ *mit* $\det B \neq 0$. *A ist eine Basis von Λ genau dann, wenn ein* $U \in \operatorname{GL}(n, \mathbb{Z})$ *existiert mit* $A = BU$.

Beweis. Wenn A eine Basis ist, dann gilt $A\mathbb{Z}^n = B\mathbb{Z}^n$, also $B^{-1}A\mathbb{Z}^n = \mathbb{Z}^n$. Damit ist $B^{-1}A \in \operatorname{GL}(n, \mathbb{Z})$. Umgekehrt analog. □

6.7 Definition. Sei $\Lambda = B\mathbb{Z}^n$, $\det B \neq 0$.

(i) Wir setzen $\det \Lambda := |\det B|$, die *Determinante des Gitters* (wohldefiniert nach Lemma 6.6).

(ii) Setze $P_B := \{p_1 b_1 + \ldots + p_n b_n : 0 \leq p_i < 1\} = B[0,1)^n$, die *fundamentale Zelle* des Gitters, siehe Abbildung 1.

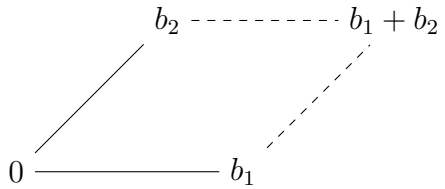

Abbildung 1: Fundamentale Zelle

6.8 Bemerkung. (i) $\det \Lambda$ ist unabhängig von der Wahl der Basis.

(ii) $\det \Lambda = \mathrm{vol}(P_B)$

(iii) $\det \Lambda \leq |b_1| \cdot \ldots \cdot |b_n|$, mit Gleichheit genau dann, wenn die b_i orthogonal.

(iv) $P_B \cap \Lambda = \{0\}$; folgt aus der Eindeutigkeit der Darstellung in Vektorräumen. Auch für $P_B - P_B = B(-1,1)^n$ gilt $(P_B - P_B) \cap \Lambda = \{0\}$.

6.9 Notation. seien $a_1, \ldots, a_n \in \mathbb{R}^n$ linear unabhängig, $A = (a_1, \ldots, a_n)$. Sei $x \in \mathbb{R}^n$ mit $x = \sum \rho_i a_i$ mit $\rho_i \in \mathbb{R}$. Dann setzen wir $\lfloor x \rfloor_A := \sum \lfloor \rho_i \rfloor a_i$. Damit ist $\lfloor x \rfloor \in A\mathbb{Z}^n$ und $x - \lfloor x \rfloor \in P_A$.

Definition. Setze $V(\Lambda) := \{x \in \mathbb{R}^n : \forall b \in \Lambda . |x| \leq |x - b|\}$ die *Voronoi-Zelle*. Das sind alle Punkte, die näher am Nullpunkt liegen, als an jedem anderen Punkt des Gitters.

Es wird vermutet, dass jeder Raumteiler ein Voronoi-Diagramm eines geeigneten Gitters ist; offen seit ca. 130 Jahren.

6.10 Proposition. *Sei* $\Lambda = B\mathbb{Z}^n$, $\det B \neq 0$. *Dann gilt*

$$\mathbb{R}^n = \bigoplus_{b \in \Lambda} (b + P_B)$$

Beweis. sei $x \in \mathbb{R}^n$, dann ist $x = \lfloor x \rfloor_B - (x - \lfloor x \rfloor_B) \in \Lambda + P_B$. Umgekehrt angenommen $x \in (b + P_B) \cap (b' + P_B)$, dann ist $b - b' \in (P_B - P_B) \cap \Lambda = \{0\}$, also $b = b'$. □

6.11 Definition. Eine Menge $S \subseteq \mathbb{R}^n$ heißt *diskret*, falls es ein $\varepsilon > 0$ gibt so, dass $|s_1 - s_2| \geq \varepsilon$ für alle $s_1 \neq s_2$.

6.12 Satz. *Eine Teilmenge* $S \subseteq \mathbb{R}^n$ *ist ein Gitter genau dann, wenn* S *eine diskrete Untergruppe von* $\mathbb{R}^n$ *ist, die* n *linear unabhängige Punkte enthält.*

Beweis. Ein Gitter ist klar eine Untergruppe. Sei $S = B\mathbb{Z}^n$. Wir setzen $\varepsilon = \min\{|Bx| : |x| = 1\}$. Dann ist $|Bz| \geq \varepsilon |z|$ für alle $z \in \mathbb{Z}^n \setminus \{0\}$. Damit ist ε eine untere Schranke für den Abstand.

Seien anders herum $s_1, \ldots, s_n \in S$ linear unabhängig. Induktiv zeigen wir die Existenz von $b_1, \ldots, b_n$ mit

$$\mathrm{lin}_{\mathbb{R}}\{s_1, \ldots, s_n\} \cap S = \mathrm{lin}_{\mathbb{Z}}\{b_1, \ldots, b_n\}$$

$k = 1$: Wähle als b_1 den kürzesten Vektor der Menge $(0, s_1] \cap S$. Ein solcher existiert, weil S diskret ist. Dann gilt $\mathrm{lin}_{\mathbb{Z}}\{b_1\} \subseteq S \cap \langle s_1 \rangle$. Sei also $s \in S \cap \langle s_1 \rangle$. Dann ist $s = \lambda b_1$für ein $\lambda \in \mathbb{R}$. Dann ist

$$S \ni s - \lfloor \lambda \rfloor b_1 = (\lambda - \lfloor \lambda \rfloor) b_1 \in [0, b_1)$$

und nach Wahl von b_1 folgt $\lambda = \lfloor \lambda \rfloor$, also $\lambda \in \mathbb{Z}$.
$k \to k+1$: Hierzu betrachten wir das Parallelepiped

$$P_k = \left\{ \sum_{i=1}^{k} \alpha_i b_i + a_{k+1} s_{k+1} : 0 \leq \alpha_i \leq 1 \right\}$$

Sei $b_{k+1} \in P_k \cap S$ mit minimalem, positivem Abstand zu $\mathrm{lin}_{\mathbb{Z}}\{b_1, \ldots, b_k\}$. Schreibe

$$b_{k+1} = \sum_{i=1}^{k} \overline{\alpha}_i b_i + \overline{\alpha}_{k+1} b_{k+1}$$

mit $\overline{\alpha}_{k+1} > 0$ minimal unter allen Punkten in $P_k \cap S$. Über $\mathbb{R}$ haben wir zunächst $\langle s_1, \ldots, s_{k+1} \rangle = \langle b_1, \ldots, b_{k+1} \rangle$. Weiterhin gilt $\mathrm{lin}_{\mathbb{Z}}\{b_1, \ldots, b_{k+1}\} \subseteq \langle s_1, \ldots, s_{k+1} \rangle \cap S$. Sei andererseits $s \in \langle s_1, \ldots, s_{k+1} \rangle \cap S$ mit $s = \sum_{i=1}^{k+1} \beta_i b_i$ (mit $\beta_i \in \mathbb{R}$). Dann gilt

$$\begin{aligned} S \ni s - \sum_{i=1}^{k+1} \lfloor \beta_i \rfloor b_i &= \sum_{i=1}^{k+1} (\beta_i - \lfloor \beta_i \rfloor) b_i \\ &= \left(\sum_{i=1}^{k} \underbrace{(\beta_i - \lfloor \beta_i \rfloor) + \overline{\alpha}_i (\beta_{k+1} - \lfloor \beta_{k+1} \rfloor)}_{=:\mu_i} \right) b_i + \underbrace{\overline{\alpha}_{k+1} (\beta_{k+1} - \lfloor \beta_{k+1} \rfloor)}_{=:\mu_{k+1}} s_{k+1} \end{aligned}$$

Dann gilt $\mu_{k+1} < \overline{\alpha}_{k+1}$. Wenn dieser Punkt in P_{k+1} liegt, dann muss wegen der Minimalität von $\overline{\alpha}_{k+1}$ gelten, dass $\beta_{k+1} \in \mathbb{Z}$. Dazu betrachte

$$S - \sum_{i=1}^{k+1} \lfloor \beta_i \rfloor b_i - \sum_{i=1}^{k} \lfloor \mu_i \rfloor b_i = \sum_{i=1}^{k} (\underbrace{\mu_i - \lfloor \mu_i \rfloor}_{\in [0,1)}) b_i + \underbrace{\overline{\alpha}_{k+1} (\beta_{k+1} - \lfloor \beta_{k+1} \rfloor)}_{\in [0, \overline{\alpha}_{k+1})} s_{k+1} \in S \cap P_k$$

Da $\overline{\alpha}_{k+1}$ minimal, folgt $\beta_{k+1} = \lfloor \beta_{k+1} \rfloor \in \mathbb{Z}$. Damit ist

$$S - \beta_{k+1} b_{k+1} = \sum_{i=1}^{k} \beta_i b_i \in \langle s_1, \ldots, s_k \rangle \cap S = \mathrm{lin}_{\mathbb{Z}}\{b_1, \ldots, b_k\} \qquad \square$$

6.13 Korollar. *Seien $a_1, \ldots, a_n \in \Lambda$ linear unabhängig. Dann gibt es eine Basis $b_1, \ldots, b_n \in \Lambda$ mit $a_k \in \mathrm{lin}_{\mathbb{Z}}\{b_1, \ldots, b_k\}$. Das heißt, $\vec{a} = \vec{b} \cdot M$ mit einer oberen Dreiecksmatrix.*

Beweis. Folgt aus der Konstruktion in Satz 6.12. □

6.14 Definition. Sei Λ ein Gitter und $a_1, \ldots, a_n \in \Lambda$ linear unabhängig. Die Menge $\Lambda_0 := \mathrm{lin}_{\mathbb{Z}}\{a_1, \ldots, a_n\}$ heißt *Untergitter* mit Basis $\{a_1, \ldots, a_n\}$. Die Anzahl der Nebenklassen von Λ_0 heißt der *Index von* Λ_0, notiert mit $|\Lambda : \Lambda_0|$.

Beispiel. Sei $\lambda = \mathbb{Z}^2$, sowie $a_1 = (2, 0)$ und $a_2 = (0, 3)$. Dann hat Λ_0 den Index 6, was die Anzahl der Punkte von Λ in der Fundamentalzelle von Λ_0 ist. Ebenso ist es der Quotient der Determinanten.

6.15 Lemma. *Sei $\Lambda_0 \leq \Lambda$. Dann gilt*

(i) $|\Lambda : \Lambda_0| = \#(P_A \cap \Lambda)$ *für jede Basis A von Λ_0.*

(ii) $|\Lambda : \Lambda_0| = \frac{\det \Lambda_0}{\det \Lambda}$.

Beweis. (i) Wir zeigen

$$\Lambda = \bigoplus_{c \in P_A \cap \Lambda} (c + \Lambda_0)$$

Sei $b \in \Lambda$,dann gilt $\lfloor b \rfloor_A \in \Lambda_0 \subseteq \Lambda$. Daraus folgt $(b - \lfloor b \rfloor_A) \in P_A \cap \Lambda$, also $b = (b - \lfloor b \rfloor_A) + \lfloor b \rfloor_A \in (P_A \cap \Lambda) + \Lambda_0$. Damit haben wir die Vereinigung. Da Nebenklassen von Gruppen disjunkt oder gleich sind, sind wir fertig.

(ii) Wir stellen fest

$$mP_A = \bigoplus_{0 \leq m_i < m} \left(\left(\sum_{i=1}^{n} m_i a_i \right) + P_A \right)$$

Weiter gilt, wenn man um einen Punkt aus Λ verschiebt, so bleibt die Anzahl der Punkte in der Fundamentalzelle gleich. Das heißt für $a \in \Lambda$ gilt $\#((a + P_A) \cap \Lambda) = \#(P_A \cap \Lambda)$. Daraus folgt $\#(mP_A \cap \Lambda) = m^n \#(P_A \cap \Lambda) \overset{(i)}{=} m^n |\Lambda : \Lambda_0|$. Somit erhalten wir

$$\begin{aligned} \det \Lambda_0 = \mathrm{vol}(P_A) &= \lim_{m \to \infty} \# \left(P_A \cap \frac{1}{m} \Lambda \right) \cdot \frac{\det \Lambda}{m^n} = \det \Lambda \cdot \lim_{m \to \infty} \frac{\#(mP_A \cap \Lambda)}{m^n} \\ &= \det \Lambda \cdot \lim_{m \to \infty} \frac{m^n |\Lambda : \Lambda_0|}{m^n} = \det \Lambda \cdot |\Lambda : \Lambda_0| \end{aligned}$$ □

6.16 Korollar. *Seien $z_1, \ldots, z_n \in \mathbb{Z}^n$ linear unabhängig. Dann ist*

$$\# \left(\left\{ \sum_{i=1}^{n} p_i z_i : 0 \leq p_i < 1 \right\} \cap \mathbb{Z}^n \right) = \det(z_1, \ldots, z_n)$$

Beweis. Folgt mit Lemma 6.15, da $\det \mathbb{Z}^n = 1$. □

6.17 Bemerkung. Sei $\Lambda_0 = A\mathbb{Z}^n \leq \Lambda$. Dann sind äquivalent

- A ist eine Basis von Λ.

- $|\Lambda : \Lambda_0| = 1$
- $\Lambda \cap P_A = \{0\}$
- $\Lambda \cap A[0,1]^n = A\{0,1\}^n$

6.18 Lemma. *Sei $\Lambda \leq \mathbb{R}^2$ ein Gitter und seien $a_1, a_2 \in \Lambda$ linear unabhängig. Dann ist a_1, a_2 Basis von Λ genau dann, wenn das von $0, a_1, a_2$ aufgespannte Dreieck $\Delta(0, a_1, a_2)$ nur diese Punkte enthält, das heißt $\Delta(0, a_1, a_2) \cap \Lambda = \{0, a_1, a_2\}$.*

Beweis. $\Rightarrow$: klar
$\Leftarrow$: Sei $P_A = \{p_1 a_1 + p_2 a_2 : 0 \leq p_i < 1\}$. Es ist zu zeigen, dass $P_A \cap \Lambda = \{0\}$. Hierzu sei $b \in P_A \cap \Lambda$. Wenn $b \in \Delta(0, a_1, a_2)$, so folgt $b = 0$ und wir sind fertig. Andernfalls schreibe $b = p_1 a_1 + p_2 a_2$ mit $0 < p_i < 1$ und $p_1 + p_2 > 1$. Dann aber ist

$$a_1 + a_2 - b = (1 - p_1)a_1 + (1 - p_2)a_2 \in \Delta(0, a_1, a_2) \cap \Lambda = \{0, a_1, a_2\}$$

und alle drei Möglichkeiten liefern sofort einen Widerspruch. □

6.19 Bemerkung. Ab Dimension 3 gilt die Aussage nicht mehr. Betrachte hierzu den Tetraeder, der aufgespannt wird von $(0,0,0), b_1 = (1,0,0), b_2 = (0,1,0)$ und $b_3 = (0,0,n)$. Dieser enthält keine weiteren ganzzahligen Punkte, hat aber das Volumen $\frac{n}{6}$, und ist für $n \neq \pm 1$ keine Basis.

6.20 Lemma. *Seien $u_1, \ldots, u_m \in \mathbb{Z}^n$ und $k_i \in \mathbb{N}$. Dann ist $\Lambda := \{z \in \mathbb{Z}^n : \langle u_i, z\rangle \equiv 0 \mod k_i\}$ ein Gitter mit $\det \Lambda \leq k_1 \ldots k_m$.*

Beweis. λ ist eine diskrete Untergruppe von $\mathbb{Z}^n$ und enthält $k_1 \ldots k_m \cdot e_i$ für $i = 1, \ldots, n$.

$$|\mathbb{Z}^n : \Lambda| = \frac{\det \Lambda}{\det \mathbb{Z}^n} = \det \Lambda$$

und nach Satz 6.12 ist Λ somit ein Gitter. Definiere die Abbildung $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$ mit $\varphi(z)_i = (\langle u_i, z\rangle \bmod k_i) \in \{0, \ldots, k_i - 1\}$. Damit ist $\#\varphi(\mathbb{Z}^n) \leq k_1 \ldots k_m$: Gehören z und $\bar{z}$ zu verschiedenen Nebenklassen bezüglich $\mathbb{Z}^n$ und Λ, dann ist $z - \bar{z} \notin \Lambda$, also $\varphi(z) \neq \varphi(\bar{z})$. □

6.21 Lemma. *Sei $X \subseteq \mathbb{R}^n$ beschränkt und messbar.*

(i) Wenn $(z + X) \cap (\bar{z} + X) = \emptyset$ für alle $z \neq \bar{z} \in \mathbb{Z}^n$, dann ist $\mathrm{vol}(X) \leq 1$.

(ii) Wenn $\mathbb{Z}^n + X = \mathbb{R}^n$, dann $\mathrm{vol}(V) \geq 1$.

Die Grenze 1 ist scharf, was man sieht, wenn man für X die Fundamentalzelle wählt.

Beweis. Sei $P = [0,1)^n$ und sei $M = \{z \in \mathbb{Z}^n : (z + P) \cap X \neq \emptyset\}$. Dann ist M endlich, da X beschränkt ist. Beachte ferner $\mathbb{R}^n = \mathbb{Z}^n + P$. Für das Volumen gilt nun

$$\mathrm{vol}(X) = \mathrm{vol}((\mathbb{Z}^n + P) \cap X) = \sum_{z \in M} \mathrm{vol}((z + P) \cap X)$$

Weiter ist $(z + P) \cap X = (P \cap (X - z)) + z$ und somit $\mathrm{vol}(X) = \sum_{z \in M} \mathrm{vol}(P \cap (X - z))$ da das Volumen translationsinvariant ist.

(i) Wenn nun $(P \cap (X - z)) \cap (P \cap (X - \bar{z})) = \emptyset$ für alle $z \neq \bar{z} \in \mathbb{Z}^n$, dann ist

$$\sum_{z \in M} \mathrm{vol}(P \cap (X - z)) \leq \mathrm{vol}(P) = 1$$

da nur disjunkte Teile der Fundamentalzelle ausgeschnitten werden.

(ii) Hier gilt zusätzlich $M = \{z \in \mathbb{Z} : P \cap (X - z) \neq \emptyset\}$. Da $\mathbb{R}^n = X + \mathbb{Z}^n$, folgt $\bigcup_{z \in M} P \cap (X - z) = P$. Damit ist

$$\sum_{z \in M} \mathrm{vol}(P + (X - z)) \geq \bigcup_{z \in M} \mathrm{vol}(P + (X - z)) = \mathrm{vol}(P) = 1$$

□

6.22 Korollar. *Sei $X \subseteq \mathbb{R}^n$ mit $\mathrm{vol}(X) > 1$. Dann existieren $x_1, x_2 \in X$ mit $x_1 - x_2 \in \mathbb{Z}^n \setminus \{0\}$, bzw. $(X - X) \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset$.*

Beweis. OBdA sei X beschränkt (sonst mit hinreichend großer Kugel schneiden). Nach Lemma 6.21 gibt es $z \neq \bar{z} \in \mathbb{Z}^n$ mit $(z + X) \cap (\bar{z} + X) \neq \emptyset$. Und damit gilt $z - \bar{z} \in (X - X) \cap \mathbb{Z}^n \setminus \{0\}$. □

6.23 Satz (Minkowski,1896). *Sei $K \in \mathcal{K}_o^n$ mit $\mathrm{vol}(K) \geq 2^n$, dann ist $K \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset$. Die Schranke ist optimal, was man durch den Grenzfall $(0,1)^n$ sieht.*

Beweis. Falls $\mathrm{vol}(K) > 2^n$ gilt, so haben wir $\mathrm{vol}(\frac{1}{2}K) > 1$. Mit Korollar 6.22 haben wir $\left(\frac{1}{2}K - \frac{1}{2}K\right) \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset$, aber durch die Symmetrie ist $K = \frac{1}{2}K - \frac{1}{2}K$.
Sei nun $\mathrm{vol}(K) = 2^n$ und sei $K \cap \mathbb{Z}^n \setminus \{0\} = \emptyset$. Da K kompakt (also abgeschlossen) ist und $\mathbb{Z}^n$ diskret, existiert ein $\lambda > 1$ mit $\lambda K \cap \mathbb{Z}^n = K \cap \mathbb{Z}^n = \{0\}$. Nun aber ist $\mathrm{vol}(\lambda K) > 2^n$, was dem ersten Teil widerspricht. □

6.24 Korollar. *Sei $\Lambda \subseteq \mathbb{R}^n$ ein Gitter und $K \in \mathcal{K}_o^n$ mit $\mathrm{vol}(K) \geq 2^n \det \Lambda$. Dann ist $K \cap \Lambda \neq \{0\}$.*

Beweis. Sei B eine Basis von Λ, also $\Lambda = B\mathbb{Z}^n$. Dann gilt

$$K \cap \Lambda \neq \{0\} \Leftrightarrow B^{-1}(K \cap \Lambda) \neq \{0\} \Leftrightarrow B^{-1}K \cap \mathbb{Z}^n \neq \{0\}$$

Nach Voraussetzung ist $\mathrm{vol}(B^{-1}K) = \frac{\mathrm{vol}(K)}{\det B} \geq 2^n$. Damit sind wir fertig nach Satz 6.23. □

Bemerkung. Als nächstes schauen wir uns das Problem von quadratischen Formen an. Gegeben Matrix $A \in \mathbb{R}^n$ und $\gamma \in \mathbb{R}$. Die Frage ist, ob ein x existiert mit $g(x) := x^T A^T A x \leq \gamma$. Dieses Problem ist nahe verwandt mit dem Problem der Kugelpackungen, und das ist erst gelöst für Dimension ≤ 8 und für 24.

6.25 Satz. *Seien $a_i \in \mathbb{R}^n$ eine Basis, setze $A := (a_1, \ldots, a_n)^T$. Weiter seien $\tau_i > 0$ mit $\prod \tau_i \geq |\det A|$. Dann existiert ein $z \in \mathbb{Z}^n \setminus \{0\}$ mit $|\langle a_i, z \rangle| \leq \tau_i$ für alle i.*
Bemerkung: Dieser Satz ist ein hinreichendes Kriterium für die Lösbarkeit eines bestimmten ILP (ganzzahligen linearen Programms).

Beweis. Sei $P = \{x \in \mathbb{R}^n : \forall i. |\langle a_i, x\rangle \leq \tau_i\}$. Dann ist

$$P = A^{-1}\{x \in \mathbb{R}^n : \forall i. |\langle e_i, x\rangle \leq \tau_i\} \implies \operatorname{vol}(P) = \frac{2^n \prod \tau_i}{|\det A|} \geq 2^n$$

damit haben wir $P \cap \mathbb{Z}^n \neq \{0\}$ und wir sind fertig. □

6.26 Korollar (vgl. Satz 3.23). *Seien $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ und sei $0 < \varepsilon < 1$. dann existieren $p_1, \ldots, p_n, q \in \mathbb{Z}$ mit $1 \leq q \leq \varepsilon^{-n}$ mit $|\alpha_i - \frac{p_i}{q}| < \frac{\varepsilon}{q}$.*

Beweis. Sei $a_i = -e_i + \alpha_i e_{n+1}$ für $i \leq n$ und $a_{n+1} = e_{n+1}$. Nach Satz 6.25 gibt es für jedes $\tau > 0$ ein Punkt $(p_1, \ldots, p_n, q) \in \mathbb{Z}^{n+1} \setminus \{0\}$ mit $|\langle a_i, z\rangle| = |\alpha_i q - p_i| \leq \tau^{-\frac{1}{n}}$ und $|\langle a_{n+1}, z\rangle| = |q| \leq \tau$. Sei nun $\tau > \varepsilon^{-n}$ und $\lfloor \tau \rfloor \leq \varepsilon^{-n}$. Daraus folgt $|\alpha_i q - p_i| < \varepsilon$ und $|q| \leq \lfloor \tau \rfloor \leq \varepsilon^{-n}$. Wäre nun $q = 0$, dann folgt $p_i = 0$ für alle i, was ein Widerspruch ist. Also ist oBdA $q \geq 1$ und wir können dadurch dividieren. □

6.27 Theorem (Lagrange). *Jedes $m \in \mathbb{N}$ lässt sich schreiben als Summe von 4 Quadraten.*

Beweis. Wir betrachten die vierdimensionale Kugel $B_4 = \{x \in \mathbb{R} : x_1^2 + x_2^2 + x_3^2 + x_4^2 \leq 1\}$. Zu zeigen, dass $\partial(\sqrt{m}B_4)$ einen ganzzahligen Gitterpunkt enthält.
Sei oBdA m quadratfrei, also $m = p_1 \cdot \ldots \cdot p_k$ mit p_i prim, verschieden. Mit Lemma 4.3 gibt es $a_i, b_i \in \mathbb{N}$ mit $a_i^2 + b_i^2 + 1 \equiv 0 \mod p_i$. Sei

$$\Lambda = \left\{z \in \mathbb{Z}^4 : z_1 \equiv (a_i z_3 + b_i z_4) \mod p_i, z_1 \equiv (b_i z_3 - a_i z_4) \mod p_i, i = 1, \ldots, k\right\}$$

Nach Lemma 6.20 ist Λ ein Gitter mit $\det \Lambda \leq p_1^2 \cdot \ldots \cdot p_k^2 = m^2$. Damit ist

$$\operatorname{vol}\left(\sqrt{2m}B_4\right) = (2m)^2 \operatorname{vol}(B_4) = (2m)^2 \frac{\pi^2}{2} > 2^4 m^2 \geq 2^4 \det \Lambda$$

Nach Korollar 6.24 existiert $z \in \Lambda \setminus \{0\}$ im *Inneren* von $\sqrt{2m}B_4$ (da wir ein $>$ haben). Also gilt $0 < z_1^2 + \ldots + z_4^2 < 2m$. Nach Wahl von Λ gilt

$$\begin{aligned} z_1^2 + z_2^2 + z_3^2 + z_4^2 &\equiv (a_i z_3 + b_i z_4)^2 + (b_i z_3 - a_i z_4)^2 + z_3^2 + z_4^2 \mod p_i \\ &\equiv z_3^2(a_i^2 + b_i^2 + 1) + z_4^2(a_i^2 + b_i^2 + 1) \equiv 0 \mod p_i \qquad \text{für } i = 1, \ldots, k \end{aligned}$$

Daraus folgt $m = p_1 \ldots p_k \mid z_1^2 + \ldots + z_4^2$, also $z_1^2 + z_2^2 + z_3^2 + z_4^2 = m$. □

6.28 Theorem. *Sei $k \in \mathbb{N}$ und sei $X \subset \mathbb{R}^n$ eine Jordan-messbare Menge mit $\operatorname{vol}(X) > k$. Dann existieren $x_1, \ldots, x_{k+1} \in X$ mit $x_i - x_j \in \mathbb{Z}^n \setminus \{0\}$ für $i \neq j$.*

Beweis. Es gilt

$$\begin{aligned} k < \operatorname{vol}(X) &= \lim_{m \to \infty} \# \left(X \cap \frac{1}{m}\mathbb{Z}^n\right) \cdot \frac{1}{m^2} \\ \implies \exists m \in \mathbb{N}. \# \left(X \cap \frac{1}{m}\mathbb{Z}^n\right) &> k \cdot m^n \end{aligned}$$

$\mathbb{Z}^n$ ist Untergitter von $\frac{1}{m}\mathbb{Z}^n$ vom Index m^n. Nach Schubfachprinzip gibt es $x_1, \ldots, x_{k+1}$, die in der gleichen Nebenklasse liegen und damit liegen ihre Differenzen in $\mathbb{Z}^n$. □

6.29 Korollar. *Sei $\Lambda \subset \mathbb{R}^n$ ein Gitter, $K \in \mathcal{K}_o^n$. Wenn $\mathrm{vol}(K) \geq k2^n \det \Lambda$, dann ist $\#(L \cap \Lambda) \geq 2k+1$.*

Beweis. OBdA (siehe Beweis Korollar 6.24) sei $\Lambda = \mathbb{Z}^n$ und $\mathrm{vol}(K) > k2^n$ (siehe Beweis Satz 6.23). Nach Theorem 6.28 existieren $k+1$ verschiedene Punkte $x_1, \ldots, x_{k+1} \in \frac{1}{2}K$ mit $x_i - x_j \in \mathbb{Z}^n \cap K$. Sei x_1 ein Pnkt mit maximaler Euklischer Norm. Setze $z_i := x_{i+1} - x_1$ für $i = 1, \ldots, k$. Es ist $z_i \neq z_j$ für $i \neq j$, sowie $z_i \in K \cap \mathbb{Z}^n \setminus \{0\}$. Weiterhin gilt $\langle x_1, z_i \rangle < 0$ für $i \leq k$. Beachte $\langle x_1, x_{i+1} \rangle \leq |x_1| \cdot |x_{i+1}|$ und Gleichheit kann nur gelten, wenn sie kolinear sind.
Sei H die Hyperebene orthogonal zu x_1. Dann liegen alle z_i unterhalb dieser Ebene. Folglich liegen alle $-z_i$ oberhalb. Damit sind $\pm z_i, 0$ zusammen $2k+1$ verschiedene Punkte von $K \cap \Lambda$. □

Satz (Kronecker). *Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\beta \in \mathbb{R}$, $N \in \mathbb{N}$ und $\varepsilon > 0$. Dann existieren $n, p \in \mathbb{N}$ mit $n > N$ und $|n\alpha - p - \beta| < \varepsilon$.*

Beweis. Nach Satz 3.23(mit $n = 1$) gibt es $r, s \in \mathbb{Z}$ mit $|s\alpha - r| < \frac{1}{s}$. Da $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ gibt es unendlich viele Lösungen, also können wir weiter annehmen, dass $s > \max\{N, \frac{1}{\varepsilon}\}$. Damit ist $|s\alpha - r| < \varepsilon$. Folglich gilt $\{s\alpha\} := s\alpha - \lfloor s\alpha \rfloor < \varepsilon$ oder $1 - \{s\alpha\} < \varepsilon$. Das heißt für $k = 1, 2, 3$ gibt $\{k \cot s\alpha\}$ Punkte in $[0, 1]$ mit Abstand $< \varepsilon$. Damit existiert ein $m \in \mathbb{N}$ mit

$$|\{ms\alpha\} - \{\beta\}| = |(ms)\alpha - \lfloor ms\alpha \rfloor - \beta + \lfloor \beta \rfloor|$$

□

Satz. *Seien $\alpha_1, \ldots, \alpha_n, 1$ linear unabhängig über $\mathbb{Q}$ und seien $\beta_1, \ldots, \beta_n \in \mathbb{Q}$, $N \in \mathbb{N}$ und $\varepsilon > 0$. Dann existieren $q, p_1, \ldots, p_n \in \mathbb{Z}$ mit $|q\alpha_i - p_i - \beta_i| < \varepsilon$ für alle i.*

Beweisidee. Dieser Satz ist die Verallgemeinerung, wo die Ungleichungen zugleich erfüllt werden. Nutze den vorigen Satz, um induktiv vorzugehen.
Wieder ist die Bedingung „linear unabhängig“ notwendig. Wäre $\sum m_i \alpha_i + m_{n+1} = 0$, dann wäre $\sum m_i (q\alpha_i - p_i) \in \mathbb{Z}$. Damit hätten wir eine diskrete Schar von Hyperebenen und da könnte ein β_i dazwischen liegen. □

Definition. Eine Folge $(a_i)_{i \in \mathbb{N}} \subset [0, 1]$ heißt *gleichverteilt* in $[0, 1]$, falls für jedes Teil-Intervall $[a, b) \subset [0, 1]$ gilt:

$$\lim_{n \to \infty} \left(\frac{1}{n} \cdot \#\{a_i \in [a, b) : i \leq n\} \right) = b - a$$

Bemerkung. Folgende Aussagen sind äquivalent für eine Folge $(a_i)_{i \in \mathbb{N}}$:

- Die Folge ist gleichverteilt.
- Für jede Riemann-integrierbare Funktion $f : [0, 1] \to \mathbb{R}$ gilt

$$\lim_{n \to \infty} \left(\frac{1}{n} \sum_{i=1}^{n} f(a_i) \right) = \int_0^1 f(x) \, \mathrm{d}\, x$$

- Für $0 \neq k \in \mathbb{Z}$ gilt

$$\lim_{n\to\infty}\left(\frac{1}{n}\sum_{i=1}^{n} e^{2\pi i k a_i}\right) = \int_0^1 e^{2\pi i k x}\,\mathrm{d}\,x = 0$$

Das Konzept "gleichverteilt" können wir ebenso in höhere Dimension übertragen.

Satz. *Sei $\alpha \in \mathbb{R}\setminus\mathbb{Q}$. Dann ist die Folge $a_n := \{n\alpha\} = n\alpha - \lfloor n\alpha \rfloor$ gleichverteilt.*

Beweis. Wir nutzen das dritte Kriterium. Es ist $e^{2\pi i k\{n\alpha\}} = e^{2\pi i k n\alpha}$. Sei $A_k := e^{2\pi i k\alpha}$. Dann ist $e^{2\pi i k\{n\alpha\}} = A_k^n$. Damit können wir wie folgt umschreiben

$$\sum_{j=1}^{n} e^{2\pi i k\{j\alpha\}} = \sum_{j=1}^{n} A_k^n = \frac{A_k^{n+1} - A_k}{A_k - 1}$$

Nun ist $|A_k| = 1$, aber da $\alpha \notin \mathbb{Q}$, ist $k\alpha \not\equiv 0 \mod 1$, also $A_k \neq 1$. Die rechte Seite schätzen wir nun ab mittels

$$\left|\frac{A_k^{n+1} - A_k}{A_k - 1}\right| \leq \frac{2}{|A_k - 1|} \implies \lim_{n\to\infty}\left(\frac{1}{n}\sum_{j=1}^{n} e^{2\pi i k\{j\alpha\}}\right) = 0 \qquad \square$$