B. Arithmetische Funktionen

B.1. Definition. Unter einer zahlentheoretischen (oder arithmetischen) Funktion versteht man eine Abbildung $f : \mathbb{N}_1 \to \mathbb{C}$.
Die Funktion $f : \mathbb{N}_1 \to \mathbb{C}$ heißt *multiplikativ*, wenn $f(1) = 1$ und

$$f(mn) = f(m)f(n) \quad \text{für alle } m, n \in \mathbb{N}_1 \text{ mit } \gcd(m, n) = 1.$$

Eine multiplikative Funktion $f : \mathbb{N}_1 \to \mathbb{C}$ heißt *vollständig multiplikativ*, wenn $f(mn) = f(m)f(n)$ ohne Einschränkung gilt.

Bemerkung. Eine multiplikative zahlentheoretische Funktion $f : \mathbb{N}_1 \to \mathbb{C}$ ist durch ihre Werte auf den Primzahlpotenzen eindeutig bestimmt. Denn aus $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ folgt

$$f(n) = f(p_1^{k_1}) \cdot \ldots \cdot f(p_r^{k_r}).$$

Ist f vollständig multiplikativ, so genügt es schon, die Werte auf den Primzahlen zu kennen, denn $f(p^k) = f(p)^k$.

B.2. Beispiele

Für viele zahlentheoretische Funktionen liegen die Werte bereits in $\mathbb{Z}$ oder in $\mathbb{R}$.

a) Die Funktion

$$\mathtt{1} : \mathbb{N}_1 \to \mathbb{Z}, \quad \mathtt{1}(n) := 1 \quad \text{für alle } n \in \mathbb{N}_1$$

ist offenbar vollständig multiplikativ.

b) Die Abbildung

$$\iota : \mathbb{N}_1 \to \mathbb{Z}, \quad \iota(n) := n \quad \text{für alle } n \in \mathbb{N}_1$$

ist ebenfalls vollständig multiplikativ.

c) Die sog. Mangoldtsche Funktion $\Lambda : \mathbb{N}_1 \to \mathbb{R}$ ist definiert durch

$$\Lambda(n) := \begin{cases} \log p, & \text{falls } n = p^k \text{ eine Primzahlpotenz ist,} \\ 0 & \text{sonst.} \end{cases}$$

Diese Funktion ist nicht multiplikativ.

d) Ein Beispiel einer multiplikativen, aber nicht vollständig multiplikativen Funktion wird durch die Eulersche Phi-Funktion gegeben.

B.3. Satz. *Die Eulersche Phi-Funktion $\varphi : \mathbb{N}_1 \to \mathbb{Z}$ ist multiplikativ, aber nicht vollständig multiplikativ.*

Beweis. Nach Definition gilt $\varphi(m) = \#(\mathbb{Z}/m)^*$. Ist $m = m_1 m_2$ mit teilerfremden m_1, m_2, so hat man nach dem Chinesischen Restsatz die Isomorphie

$$(\mathbb{Z}/m)^* \xrightarrow{\sim} (\mathbb{Z}/m_1)^* \times (\mathbb{Z}/m_2)^*,$$

woraus folgt $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.

Dass φ nicht vollständig multiplikativ ist, sieht man an folgendem Beispiel: Es ist $\varphi(2) = 1$ und $\varphi(4) = 2$, denn

$$(\mathbb{Z}/2)^* = \{\overline{1}\}, \qquad (\mathbb{Z}/4)^* = \{\overline{1}, \overline{3}\}.$$

Also ist $\varphi(2 \cdot 2) \neq \varphi(2)\varphi(2)$, q.e.d.

Mit Satz B.3 kann man eine Formel für $\varphi(m)$ mithilfe der Primfaktor-Zerlegung von n aufstellen. Für eine Primzahlpotenz p^k ist $\varphi(p^k)$ die Anzahl der Zahlen aus $M := \{1, 2, \ldots, p^k\}$, die zu p^k teilerfremd, d.h. nicht durch p teilbar sind. Es sind aber genau $p^k/p = p^{k-1}$ Elemente aus M durch p teilbar, also

$$\varphi(p^k) = p^k - p^{k-1} = p^k\Big(1 - \frac{1}{p}\Big).$$

Hat n die Primfaktor-Zerlegung $n = \prod_{j=1}^{r} p_j^{k_j}$, so folgt

$$\varphi(n) = \prod_j \varphi(p_j^{k_j}) = \prod_j p_j^{k_j}\Big(1 - \frac{1}{p_j}\Big) = n \prod_j \Big(1 - \frac{1}{p_j}\Big),$$

also

$$\varphi(n) = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big),$$

wobei p alle Primteiler von n durchläuft.

B.4. Summatorische Funktion. Ist $f : \mathbb{N}_1 \to \mathbb{C}$ eine zahlentheoretische Funktion, so definiert man die *summatorische Funktion* $F : \mathbb{N}_1 \to \mathbb{C}$ von f durch

$$F(n) := \sum_{d|n} f(d).$$

Dabei wird über alle positiven Teiler d von n summiert, einschließlich 1 und n.

Z.B. ist

$$F(6) = f(1) + f(2) + f(3) + f(6).$$

Für jede Primzahl p gilt

$$F(p) = f(1) + f(p).$$

B.5. Satz (Summatorische Funktion der Eulerschen Phi-Funktion). *Für alle $n \in \mathbb{N}_1$ gilt*

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

Dies lässt sich auch so ausdrücken: Die summatorische Funktion von φ ist die Funktion ι aus Beispiel B.2b).

Beweis. Sei $M_n := \{1, 2, \ldots, n\}$. Für einen Teiler $d \mid n$ setzen wir

$$A_n(d) := \{k \in M_n : \gcd(k, n) = d\}.$$

Offenbar gilt

$$M_n = \bigcup_{d|n}^{\cdot} A_n(d) \qquad \text{(disjunkte Vereinigung)},$$

$\varphi(n) := \#A_n(1)$ und $\#A_n(d) = \#A_{n/d}(1) = \varphi(n/d)$, denn die

$$A_n(d) \longrightarrow A_{n/d}(1), \quad k \mapsto n/d,$$

ist bijektiv. Also folgt

$$n = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d),$$

denn durchläuft d alle Teiler von n, so durchläuft auch n/d alle Teiler von n. Damit ist Satz B.5 bewiesen.

B.6. Satz. *Sei $f : \mathbb{N}_1 \to \mathbb{C}$ eine multiplikative zahlentheoretische Funktion und $F : \mathbb{N}_1 \to \mathbb{C}$ ihre summatorische Funktion. Dann ist auch F multiplikativ.*

Beweis. Seien $m_1, m_2 \in \mathbb{N}_1$. Dann lässt sich jeder Teiler $d \mid m_1 m_2$ eindeutig zerlegen als $d = d_1 d_2$ mit $d_1 \mid m_1$ und $d_2 \mid m_2$. Damit folgt

$$\begin{aligned} F(m_1 m_2) &= \sum_{d|m_1 m_2} f(m_1 m_2) \\ &= \sum_{d_1|m_1} \sum_{d_2|m_2} f(m_1 m_2) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(m_1) f(m_2) \\ &= \sum_{d_1|m_1} f(m_1) \sum_{d_2|m_2} f(m_2) = F(m_1) F(m_2), \quad \text{q.e.d.} \end{aligned}$$

B.7. Teileranzahl und Teilersumme. Für eine natürliche Zahl $n \in \mathbb{N}_1$ bezeichne $\tau(n)$ die Anzahl der positiven Teiler von n (einschließlich 1 und n). Dies lässt sich auch so ausdrücken:

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

Das bedeutet, dass τ die summatorische Funktion der Funktion $\mathtt{1}(n) = 1$ für alle n aus Beispiel B.2a) ist. Da $\mathtt{1}$ multiplikativ ist, ist nach Satz B.6 auch τ multiplikativ.

Mit $\sigma(n)$ sei die Summe aller Teiler von n bezeichnet, d.h.

$$\sigma(n) := \sum_{d|n} d.$$

Also ist σ die summatorische Funktion der Funktion $\iota(n) = n$ für alle n aus Beispiel B.2b). Da ι multiplikativ ist, ist auch σ multiplikativ.

Aus der Multiplikativität lassen sich einfach Formeln für $\tau(n)$ und $\sigma(n)$ herleiten. Eine Primzahlpotenz p^k hat genau $k+1$ Teiler, nämlich $1, p, \ldots, p^k$. Daraus folgt

$$\tau(p^k) = k + 1$$

und

$$\sigma(p^k) = \sum_{i=0}^{k} p^i = \frac{p^{k+1} - 1}{p - 1}.$$

Daraus folgt für $n = \prod_{j=1}^{r} p_j^{k_j}$

$$\tau(n) = \prod_{j=1}^{r} (k_j + 1) \quad \text{und} \quad \sigma(n) = \prod_{j=1}^{r} \frac{p_j^{k_j+1} - 1}{p_j - 1}.$$

B.8. Mersennesche Primzahlen, vollkommene Zahlen

Es ist leicht zu sehen, dass eine Zahl der Gestalt $M = 2^n - 1$ höchstens dann prim ist, wenn der Exponent n prim ist, denn $2^{k\ell} - 1$ ist durch $2^k - 1$ teilbar. Die Zahlen

$$M_p := 2^p - 1, \quad p \text{ prim},$$

heißen *Mersennesche Zahlen*. Sie sind nicht alle prim. Die ersten Mersenneschen Primzahlen sind

$$\begin{aligned}
M_2 &= 2^2 - 1 = 3,\\
M_3 &= 2^3 - 1 = 7,\\
M_5 &= 2^5 - 1 = 31,\\
M_7 &= 2^7 - 1 = 127,\\
M_{13} &= 2^{13} - 1 = 8191,\\
M_{17} &= 2^{17} - 1 = 131071,\\
M_{19} &= 2^{19} - 1 = 524287,\\
M_{31} &= 2^{31} - 1 = 2147483647.
\end{aligned}$$

Dagegen sind

$$\begin{aligned} M_{11} &= 2^{11} - 1 = 2047 = 23 \cdot 89, \\ M_{23} &= 2^{23} - 1 = 8388607 = 47 \cdot 178481, \\ M_{29} &= 2^{29} - 1 = 536870911 = 233 \cdot 1103 \cdot 2089 \end{aligned}$$

zusammengesetzt.

Eine Zahl $n \in \mathbb{N}_1$ heißt *vollkommen*, falls $\sigma(n) = 2n$. Dies lässt sich auch so ausdrücken: Bezeichnet

$$\sigma'(n) := \sum_{\substack{d|n \\ d<n}} d = \sigma(n) - n$$

die Summe der *echten* Teiler von n, so ist eine vollkommene Zahl n dadurch charakterisiert, dass $\sigma'(n) = n$. Die kleinsten vollkommenen Zahlen sind

$$\begin{aligned} 6 &= 2 \cdot 3 = 1 + 2 + 3, \\ 28 &= 2^2 \cdot 7 = 1 + 2 + 4 + 7 + 14, \\ 496 &= 2^4 \cdot 31 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248. \end{aligned}$$

Die vollkommenen Zahlen hängen eng mit den Mersenneschen Primzahlen zusammen, wie folgender Satz zeigt:

B.9. Satz. a) (Euklid) *Ist $M_p = 2^p - 1$ eine Primzahl, so ist*

$$N := 2^{p-1}(2^p - 1)$$

eine vollkommene Zahl.

b) (Euler) *Umgekehrt lässt sich jede gerade vollkommene Zahl als $2^{p-1}(2^p - 1)$ mit einer Mersenneschen Primzahl $2^p - 1$ schreiben.*

Beweis. a) Wegen der Multiplikativität von σ gilt

$$\sigma(N) = \sigma(2^{p-1})\sigma(2^p - 1).$$

Nun ist $\sigma(2^{p-1}) = 2^p - 1$ und, da $2^p - 1$ nach Voraussetzung prim ist, $\sigma(2^p - 1) = 2$, also insgesamt $\sigma(N) = 2N$.

b) Sei N eine gerade vollkommene Zahl. Sie lässt sich scheiben als

$$N = 2^s n \qquad \text{mit } s \geqslant 1 \text{ und } n \text{ ungerade.}$$

Nun ist

$$2N = \sigma(N) = \sigma(2^s)\sigma(n) = (2^{s+1} - 1)\sigma(n).$$

Da $2N = 2^{s+1}n$, folgt daraus

$$\sigma(n) = \frac{2^{s+1}}{2^{s+1}-1}\,n = n + \frac{n}{2^{s+1}-1} = n + d$$

mit $d := n/(2^{s+1}-1) \in \mathbb{N}_1$. Da d ein Teiler von n ist, folgt aus der Gleichung $\sigma(n) = n+d$, dass n und d die einzigen Teiler von n sind; also muss $d = 1$ und n eine Primzahl sein. Aus $d = 1$ folgt weiter $n = 2^{s+1} - 1$, also ist n eine Mersennesche Primzahl, insbesondere ist $p := s + 1$ prim (vgl. B.8). Daraus folgt Teil b) des Satzes.

Bemerkung. Die vollkommenen Zahlen 6, 28 und 496 gehören zu den Mersenneschen Primzahlen $M_2 = 3$, $M_3 = 7$ und $M_5 = 31$. Die nächsten Beispiele vollkommener Zahlen sind also $2^6(2^7 - 1) = 8128$ und $2^{12}(2^{13} - 1) = 33550336$. Es ist unbekannt, ob es ungerade vollkommenene Zahlen gibt.

B.10. Die Möbius-Funktion

Eine Zahl $n \in \mathbb{N}_1$ heißt *quadratfrei*, wenn n von keiner Quadratzahl > 1 geteilt wird, d.h. wenn es keine Primzahl p mit $p^2 \mid n$ gibt. Die Möbius-Funktion $\mu : \mathbb{N}_1 \to \mathbb{Z}$ wird nun definiert durch

$$\mu(n) := \begin{cases} 0, & \text{falls } n \text{ nicht quadratfrei,} \\ (-1)^r, & \text{falls } n \text{ quadratfrei und } r \text{ verschiedene Primteiler hat.} \end{cases}$$

Für $n \leqslant 14$ ergeben sich folgende Werte

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1	−1	0	−1	1

Es folgt unmittelbar aus der Definition, dass μ multiplikativ ist.

B.11. Satz (Summatorische Funktion der Möbius-Funktion).

$$\sum_{d|n} \mu(n) = \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{sonst.} \end{cases}$$

Dies lässt sich auch so ausdrücken: Die summatorische Funktion von μ ist die Funktion $\delta_1 : \mathbb{N}_1 \to \mathbb{Z}$ mit

$$\delta_1(n) := \delta_{1n} := \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{sonst.} \end{cases}$$

Beweis. Wir setzen $S(n) := \sum_{d|n} \mu(n)$. Es ist also zu zeigen, dass die Funktionen S und δ_1 übereinstimmen. δ_1 ist offensichtlich multiplikativ, ebenso S als summatorische Funktion der multiplikativen Funktion μ. Daher genügt es,

$$S(p^k) = \delta_1(p^k) \quad \text{für Primzahlpotenzen } p^k$$

zu beweisen. Der Fall $k = 0$ ist trivial. Für $k \geqslant 1$ ist

$$S(p^k) = \sum_{i=0}^{k} \mu(p^i) = \mu(1) + \mu(p) = 1 - 1 = 0 = \delta_1(p^k), \quad \text{q.e.d.}$$

Eine interessante Anwendung der Möbiusschen μ-Funktion wird durch folgenden Satz gegeben.

B.12. Satz (Möbiusscher Umkehrsatz). *Sei $f : \mathbb{N}_1 \to \mathbb{C}$ eine zahlentheoretische Funktion und*

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

ihre summatorische Funktion. Dann gilt für alle $n \in \mathbb{N}_1$

$$f(n) = \sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) F(d).$$

Beweis. Dass die beiden Summen in der letzten Formel gleich sind, folgt wieder aus der Tatsache, dass wenn d alle Teiler von n durchläuft, auch n/d alle Teiler von n durchläuft. Wir berechnen nun die Summe

$$\begin{aligned}\sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) &= \sum_{d|n} \mu(d) \sum_{\ell|\frac{n}{d}} f(\ell) = \sum_{\substack{d,\ell \\ d\ell|n}} \mu(d) f(\ell) \\ &= \sum_{\ell|n} f(\ell) \sum_{d|\frac{n}{\ell}} \mu(d) = \sum_{\ell|n} f(\ell) \delta_1\Big(\frac{n}{\ell}\Big) = f(n), \quad \text{q.e.d.}\end{aligned}$$

Beispiele. a) Die Teileranzahl-Funktion $\tau(n) = \sum_{d|n} 1$ ist summatorische Funktion der konstanten Funktion $\mathtt{1}(n) = 1$. Also gilt

$$\sum_{d|n} \mu\Big(\frac{n}{d}\Big) \tau(d) = 1.$$

b) Die Teilersummen-Funktion $\sigma(n) = \sum_{d|n} d$ ist summatorische Funktion der Funktion $\iota(n) = n$. Daraus folgt

$$\sum_{d|n} \mu\Big(\frac{n}{d}\Big) \sigma(d) = n.$$

c) Für die Eulersche Phi-Funktion haben wir in Satz B.5 bewiesen

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

Daraus folgt

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

Dies lässt sich so umformen:

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

Vergleich mit der in B.5 bewiesenen Formel $\varphi(n) = n\prod_{p|n}(1-1/p)$ ergibt

$$\prod_{p|n}\Big(1-\frac{1}{p}\Big) = \sum_{d|n}\frac{\mu(d)}{d},$$

wobei auf der linken Seite das Produkt über alle Primteiler von n zu nehmen ist, während auf der rechten Seite über alle Teiler von n summiert wird.

B.13. Dirichlet-Faltung. Sind $f, g : \mathbb{N}_1 \to \mathbb{C}$ zwei zahlentheoretische Funktionen, so definiert man ihre Dirichlet-Faltung $f * g : \mathbb{N}_1 \to \mathbb{C}$ durch

$$(f*g)(n) = \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big) = \sum_{d|n} f\Big(\frac{n}{d}\Big)g(d) = \sum_{\substack{k,\ell\\ k\ell=n}} f(k)g(\ell).$$

Beispiele. Ist $f : \mathbb{N}_1 \to \mathbb{C}$ eine zahlentheoretische Funktion, so kann man ihre summatorische Funktion

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

als Faltung von f mit der konstanten Funktion $\mathtt{1}(n) = 1$ für alle $n \in \mathbb{N}_1$ auffassen,

$$F = f * \mathtt{1}.$$

Insbesondere ergibt sich für die Teileranzahl-Funktion $\tau(n) = \sum_{d|n} 1$ die Darstellung

$$\tau = \mathtt{1} * \mathtt{1}.$$

Die Formel des Möbiusschen Umkehrsatzes

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

lässt sich mit der Dirichlet-Faltung einfach schreiben als

$$f = \mu * F.$$

B.14. Satz. *Die Dirichlet-Faltung ist eine kommutative und assoziative Verknüpfung auf der Menge aller zahlentheoretischen Funktionen $f : \mathbb{N}_1 \to \mathbb{C}$. Die Funktion $\delta_1 : \mathbb{N}_1 \to \mathbb{C}$,*

$$\delta_1(n) := \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{sonst.} \end{cases}$$

ist ein Eins-Element für die Dirichlet-Faltung.

Beweis. a) Die Kommutativität $f * g = g * f$ ist klar.

b) Zur Assoziativität: Seien $f, g, h : \mathbb{N}_1 \to \mathbb{C}$ drei zahlentheoretische Funktionen. Dann ist

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{\substack{k,\ell \\ k\ell=n}} (f * g)(k)h(\ell) = \sum_{\substack{k,\ell \\ k\ell=n}} \sum_{\substack{i,j \\ ij=k}} f(i)g(j)h(\ell) \\ &= \sum_{\substack{i,j,\ell \\ ij\ell=n}} f(i)g(j)h(\ell). \end{aligned}$$

Andrerseits gilt

$$\begin{aligned} (f * (g * h))(n) &= ((g * h) * f)(n) = \sum_{\substack{i,j,\ell \\ ij\ell=n}} g(i)h(j)f(\ell) \\ &= \sum_{\substack{i,j,\ell \\ ij\ell=n}} g(j)h(\ell)f(i) = ((f * g) * h)(n), \quad \text{q.e.d.} \end{aligned}$$

c) Einselement:

$$(\delta_1 * f)(n) = \sum_{d|n} \delta_1(d) f\Big(\frac{n}{d}\Big) = \delta_1(1) f\Big(\frac{n}{1}\Big) = f(n),$$

d.h. $\delta_1 * f = f$. Damit ist Satz B.14 bewiesen.

Anwendung. Mit der Dirichlet-Faltung erhalten wir einen neuen Beweis des Möbiusschen Umkehrsatzes: Sei f eine zahlentheoretische Funktion mit summatorischer Funktion $F = f * \mathtt{1}$. Multiplizieren wir diese Gleichung (bzgl. der Dirichlet-Faltung) mit der Möbius-Funktion μ, erhalten wir wegen $\mu * \mathtt{1} = \delta_1$ (Satz B.11)

$$F * \mu = (f * \mathtt{1}) * \mu = f * (\mathtt{1} * \mu) = f * \delta_1 = f,$$

d.h. den Umkehrsatz $f = F * \mu$.

Aus $f = F * \mu$ lässt sich umgekehrt durch Multiplikation mit der Funktion $\mathtt{1}$ wieder $F = f * \mathtt{1}$ herleiten.

B.15. Dirichlet-Reihen. Jeder zahlentheoretischen Funktion $a : \mathbb{N}_1 \to \mathbb{C}$ kann eine sog. Dirichlet-Reihe

$$F(s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

zugeordnet werden. Dies ist zunächst nur eine formale Reihe. Falls aber die Koeffizienten $a(n)$ einer Abschätzung der Form

$$|a(n)| \leqslant Cn^\alpha \quad \text{für alle } n \in \mathbb{N}_1$$

mit Konstanten $C \in \mathbb{R}_+$, $\alpha \in \mathbb{R}$, genügen, konvergiert die Reihe $F(s)$ absolut für alle reellen $s > \sigma_0 := \alpha + 1$, denn mit $\varepsilon := s - \sigma_0 > 0$ gilt

$$\Big|\frac{a(n)}{n^s}\Big| \leqslant C\frac{n^\alpha}{n^s} = \frac{C}{n^{1+\varepsilon}},$$

und bekanntlich konvergiert die Reihe $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^{1+\varepsilon}}$.
Ein ähnliches Argument zeigt, dass die Reihe sogar für jedes $\sigma_1 > \sigma_0$ auf dem Intervall $[\sigma_1, \infty[\subset \mathbb{R}$ gleichmäßig konvergiert, also eine auf dem Intervall $]\sigma_0, \infty[$ stetige Funktion darstellt.

Beispiel. Für die konstante Funktion $\mathtt{1}(n) = 1$ entsteht die Zetafunktion

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

Die Reihe konvergiert für alle $s > 1$.

Bemerkung. In der analytischen Zahlentheorie betrachtet man die Zetafunktion auch für komplexe Argumente s. Hier beschränken wir uns jedoch auf reelle Argumente.

B.16. Dirichlet-Reihen und Dirichlet-Faltung. Seien $a, b : \mathbb{N}_1 \to \mathbb{C}$ zwei zahlentheoretische Funktionen und

$$F(s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s}, \qquad G(s) := \sum_{n=1}^{\infty} \frac{b(n)}{n^s}$$

ihre zugeordneten Dirichlet-Riehen. Wir setzen voraus, dass beide Reihen für $s > \sigma_0$ absolut konvergieren. Wegen der absoluten Konvergenz darf man beide Reihen gliedweise multiplizieren.

$$F(s)G(s) = \sum_k \frac{a(k)}{k^s} \sum_\ell \frac{b(\ell)}{\ell^s} = \sum_{k,\ell} \frac{a(k)b(\ell)}{(k\ell)^s} = \sum_{n=1}^{\infty} \Big(\sum_{k\ell=n} a(k)b(\ell) \Big) \frac{1}{n^s}.$$

Es folgt also

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{(a * b)(n)}{n^s}.$$

Das Produkt der a und b zugeordneten Dirichlet-Reihen gehört also zum Faltungs-Produkt von a und b.

Beispiele. a) Wir haben gesehen, dass sich die Teileranzahl-Funktion τ als Faltung der konstanten Funktion $\mathtt{1}(n) = 1$ mit sich selbst schreiben lässt, $\tau = \mathtt{1} * \mathtt{1}$. Daraus folgt

$$\zeta(s)^2 = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} \qquad \text{für } s > 1.$$

b) Aus der Gleichung $\mathtt{1} * \mu = \delta_1$ folgt

$$\zeta(s)\Big(\sum_n \frac{\mu(n)}{n^s}\Big) = \sum_n \frac{\delta_1(n)}{n^s} = 1,$$

also

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \qquad \text{für } s > 1.$$

C. Verteilung der Primzahlen. Bertrandsches Postulat

C.1. Satz (Euklid). *Es gibt unendlich viele Primzahlen.*

Beweis. Wir zeigen, dass es zu jeder endlichen Menge $p_1, p_2, \ldots, p_n$ von Primzahlen immer noch eine weitere Primzahl q gibt, die von allen p_j, $(1 \leqslant j \leqslant n)$, verschieden ist. Dazu betrachten wir die Zahl

$$Q := p_1 p_2 \cdot \ldots \cdot p_n + 1.$$

Dann ist Q entweder selbst eine Primzahl oder besitzt einen Primfaktor $q \mid Q$. Dieser ist von allen p_j verschieden, da $p_j \nmid Q$ für alle j.

C.2. Anzahl der Primzahlen. Für eine reelle Zahl $x \geqslant 0$ bezeichnet man mit $\pi(x)$ die Anzahl aller Primzahlen $p \leqslant x$. (Dieses $\pi(x)$ ist natürlich nicht zu verwechseln mit der Kreiszahl $\pi = 3.14159\ldots$.) Z.B. ist $\pi(1) = 0$, $\pi(\sqrt{5}) = 1$, $\pi(3.14) = 2$. Einige weitere Werte sind

x	10	100	1000	10^4	10^5	10^6	10^7	10^8
$\pi(x)$	4	25	168	1229	9592	78498	664579	5761455

Nach Satz C.1 gilt jedenfalls

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

Von Legendre und Gauß wurde vermutet, dass sich $\pi(x)$ für $x \to \infty$ asymptotisch wie $x/\log x$ verhält, in Zeichen

$$\pi(x) \sim \frac{x}{\log x}.$$

Dabei bedeutet das Zeichen $\sim$ *asymptotisch gleich*, d.h. der Quotient der rechten und linken Seite konvergiert für $x \to \infty$ gegen 1 . Diese Vermutung wurde 1896 unabhängig von Hadamard und de la Vallée Poussin bewiesen. In diesem Kapitel werden wir nur eine abgeschwächte Form des Primzahlsatzes beweisen, nämlich

$$c_1 \frac{x}{\log x} \leqslant \pi(x) \leqslant c_2 \frac{x}{\log x} \quad \text{für } x \geqslant x_0$$

mit gewissen Konstanten $0 < c_1 < 1 < c_2$. Solche Abschätzungen wurden zuerst von Tschebyscheff um 1850 bewiesen.

Wir benötigen einige Vorbereitungen.

C.3. Lemma (Legendre). *Sei n eine natürliche Zahl. Dann gilt für die Primfaktor-Zerlegung von $n!$*

$$n! = \prod_{p\leqslant n} p^{\alpha(p,n)},$$

wobei $\quad \alpha(p,n) := v_p(n!) = \sum_{k\geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor .$

Bemerkung. Die Summe ist natürlich endlich, denn $\lfloor n/p^k \rfloor = 0$ für $p^k > n$.

Beweis. Die Anzahl der Zahlen aus $\{1, 2, \ldots, n\}$, die durch p teibar sind, ist gleich $\lfloor n/p \rfloor$. Davon sind $\lfloor n/p^2 \rfloor$ sogar durch p^2 teilbar, $\lfloor n/p^3 \rfloor$ durch p^3, usw. Daraus folgt die Behauptung.

Beispiel. Für $n = 10$ hat $10!$ die Primfaktoren $2, 3, 5, 7$ mit den Vielfachheiten

$$\begin{aligned} v_2(10!) &= \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{4} \right\rfloor + \left\lfloor \frac{10}{8} \right\rfloor = 5 + 2 + 1 = 8, \\ v_3(10!) &= \left\lfloor \frac{10}{3} \right\rfloor + \left\lfloor \frac{10}{9} \right\rfloor = 3 + 1 = 4, \\ v_5(10!) &= \left\lfloor \frac{10}{5} \right\rfloor = 2, \\ v_7(10!) &= \left\lfloor \frac{10}{7} \right\rfloor = 1, \end{aligned}$$

also $\quad 10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 = 3\,628\,800.$

C.4. Lemma. *Sei $n \geqslant 1$ eine natürliche Zahl. Für den Binomial-Koeffizienten $\binom{2n}{n}$ gelten die folgenden Aussagen:*

a) $2 \,\Big|\, \binom{2n}{n}$ *und* $p \,\Big|\, \binom{2n}{n}$ *für alle Primzahlen p mit $n < p \leqslant 2n$.*

b) *Ist $p \geqslant 3$ eine Primzahl mit $2n/3 < p \leqslant n$, so folgt $p \nmid \binom{2n}{n}$.*

c) *Falls $p^r \,\Big|\, \binom{2n}{n}$ für eine Primzahlpotenz p^r, so folgt $p^r \leqslant 2n$.*

d) $\dfrac{2^{2n-1}}{n} \leqslant \binom{2n}{n} \leqslant 2^{2n-1}.$

Beweis. a) Es gilt

$$\binom{2n}{n} = \binom{2n-1}{n-1} + \binom{2n-1}{n} = 2\binom{2n-1}{n-1} \quad \Longrightarrow \quad 2 \,\Big|\, \binom{2n}{n}$$

und

$$\binom{2n}{n} = \frac{2n \cdot (2n-1) \cdot \ldots \cdot (n+1)}{1 \cdot 2 \cdot \ldots \cdot n}.$$

Eine Primzahl $n < p \leqslant 2n$ im Zähler kann sich deshalb nicht wegkürzen.

b) Da $p^2 > 2n$ gilt nach Lemma C.3

$$v_p\binom{2n}{n} = v_p\Big(\frac{(2n)!}{(n!)^2}\Big) = \left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor = 2 - 2 = 0,$$

d.h. $p \nmid \binom{2n}{n}$.

c) In der Formel

$$v_p\binom{2n}{n} = \sum_{k\geqslant 1}\left\{\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right\}$$

ist jeder Summand entweder 0 oder 1, denn für jede reelle Zahl x gilt $\lfloor 2x\rfloor - 2\lfloor x\rfloor \in \{0,1\}$. Da $\lfloor 2n/p^k\rfloor = 0$ für

$$k > r_p := \left\lfloor\frac{\log 2n}{\log p}\right\rfloor$$

folgt $v_p\binom{2n}{n} \leqslant r_p$, also $p^r \leqslant p^{r_p} \leqslant 2n$.

d) Aus $(1+1)^{2n-1} = 2^{2n-1}$ folgt mit dem binomischen Lehrsatz

$$(*) \qquad 1 + \binom{2n-1}{1} + \ldots + \binom{2n-1}{n-1} + \binom{2n-1}{n} + \ldots + \binom{2n-1}{2n-2} + 1 = 2^{2n-1}$$

Daraus folgt einerseits

$$\binom{2n}{n} = \binom{2n-1}{n-1} + \binom{2n-1}{n} \leqslant 2^{2n-1}$$

und andrerseits, da $\binom{2n-1}{n-1} = \binom{2n-1}{n}$ die größten der $2n$ Summanden der linken Seite von $(*)$ sind,

$$\binom{2n-1}{n-1} = \binom{2n-1}{n} \geqslant \frac{2^{2n-1}}{2n},$$

also

$$\binom{2n}{n} \geqslant \frac{2^{2n-1}}{n}.$$

C.5. Satz. *Für alle $n \geqslant 3$ gilt*

$$\frac{1}{2}\cdot\frac{n}{\log n} \leqslant \pi(n) \leqslant 2\cdot\frac{n}{\log n}.$$

Beweis

A. Abschätzung nach oben

Wir bezeichnen mit

$$P(m,2m) = \prod_{m<p\leqslant 2m} p$$

das Produkt aller Primzahlen p mit $m < p \leqslant 2m$. Da die Anzahl der Faktoren gleich $\pi(2m) - \pi(m)$ ist, folgt

$$P(m, 2m) > m^{\pi(2m)-\pi(m)}.$$

Nach Lemma C.4 gilt für $m \geqslant 2$

$$2P(m, 2m) \leqslant \binom{2m}{m} \leqslant 2^{2m-1},$$

also folgt

$$m^{\pi(2m)-\pi(m)} < 2^{2m-2},$$

und nach Logarithmieren

$$\pi(2m) - \pi(m) < \frac{(2m-2)\log 2}{\log m}. \tag{1}$$

Wir beweisen jetzt die Abschätzung nach oben durch Induktion nach n. Durch direktes Nachprüfen überzeugt man sich, dass die Abschätzung für $3 \leqslant n \leqslant 2^7 = 128$ richtig ist.

Induktionsschritt. Sei zunächst $n = 2m-1 > 2^7$ ungerade. Es gilt $\pi(2m-1) = \pi(2m)$. Aus (1) folgt unter Benutzung der Induktionsvoraussetzung für $\pi(m)$

$$\begin{aligned}
\pi(2m-1) &\leqslant \pi(m) + \frac{(2m-2)\log 2}{\log m} \\
&\leqslant \frac{2m + (2m-2)\log 2}{\log m} \\
&= \frac{2m(1+\log 2) - 2\log 2}{\log m} \\
&\overset{!}{\leqslant} 2 \cdot \frac{2m-1}{\log(2m-1)}.
\end{aligned}$$

Die Abschätzung an der Stelle $\overset{!}{\leqslant}$ ist äquivalent mit

$$2m(1+\log 2) - 2\log 2 \;\leqslant\; (4m-2) \cdot \frac{\log m}{\log(2m-1)}$$

und dies wiederum ist gleichbedeutend mit

$$(1+\log 2) - \frac{\log 2}{m} \;\leqslant\; \Big(2 - \frac{1}{m}\Big) \cdot \frac{\log m}{\log(2m-1)}.$$

Diese Ungleichung folgt aber aus

$$1 + \log 2 \leqslant \Big(2 - \frac{1}{m}\Big) \cdot \frac{\log m}{\log(2m)} = \Big(2 - \frac{1}{m}\Big)\Big(1 - \frac{\log 2}{\log(2m)}\Big) \tag{2}$$

Die Gültigkeit von (2) folgt für $2m \geqslant 2^7$ daraus, dass

$$\Big(2 - \frac{1}{2^6}\Big)\Big(1 - \frac{\log 2}{\log(2^7)}\Big) = \Big(2 - \frac{1}{64}\Big)\Big(1 - \frac{1}{7}\Big) = 1.7008928\ldots$$

und $1 + \log 2 = 1.693147\ldots$.

Für gerade $n = 2m$ folgt die Abschätzung nach oben aus

$$\pi(2m) = \pi(2m-1) \leqslant 2 \cdot \frac{2m-1}{\log(2m-1)} < 2 \cdot \frac{2m}{\log(2m)},$$

denn die Funktion $x \mapsto x/\log x$ ist streng monoton wachsend.

B. Abschätzung nach unten

Nach Lemma C.4 c) gilt

$$\binom{2m}{m} = \prod_{p \leqslant 2m} p^{k_p} \quad \text{mit } p^{k_p} \leqslant 2m,$$

also

$$\binom{2m}{m} \leqslant (2m)^{\pi(2m)}.$$

Daraus folgt

$$(2m)^{\pi(2m)} \geqslant \frac{2^{2m}}{2m}$$

und durch Logarithmieren

$$\pi(2m) \geqslant \frac{2m \log 2}{\log 2m} - 1 = \frac{2m}{\log 2m}\Big(\log 2 - \frac{\log 2m}{2m}\Big).$$

Für $2m \geqslant 16$ ist

$$\Big(\log 2 - \frac{\log 2m}{2m}\Big) \geqslant \Big(\log 2 - \frac{\log 16}{16}\Big) = 0.519860\ldots > \frac{1}{2},$$

Damit ist die Abschätzung nach unten für gerade $n \geqslant 16$ bewiesen, für $3 < n < 16$ prüft man sie direkt nach.

Für ungerade $n = 2m - 1$ folgt die Abschätzung aus

$$\pi(2m-1) = \pi(2m) \geqslant \frac{1}{2} \cdot \frac{2m}{\log 2m} > \frac{1}{2} \cdot \frac{2m-1}{\log(2m-1)}.$$

C.6. Satz. *Für jede ganze Zahl $n \geqslant 1$ gilt*

$$\prod_{p \leqslant n} p < 4^n.$$

Dabei ist das Produkt über alle Primzahlen $p \leqslant n$ zu nehmen.

Beweis. Sei $P(n) := \prod_{p \leqslant n} p$. Es ist also zu zeigen, dass $P(n) < 4^n$ für alle $n \geqslant 1$. Dies beweisen wir durch Induktion nach n.

Die Behauptung ist offensichtlich wahr für $n = 1, 2$.

Für den *Induktionsschritt* nehmen wir an, dass $n \geqslant 3$ und $P(k) < 4^k$ für alle $k < n$ und schließen daraus $P(n) < 4^n$. Dies ist trivial, falls n gerade, denn $P(2m) = P(2m-1)$. Sei also n ungerade, $n = 2m - 1$. Nach Lemma C.4a) und C.4d) gilt

$$2\Big(\prod_{m<p\leqslant 2m-1} p\Big) \,\Big|\, \binom{2m}{m} \quad\Longrightarrow\quad \prod_{m<p\leqslant 2m-1} p \;\leqslant 2^{2m-2} = 4^{m-1}.$$

Da nach Induktionsvoraussetzung $P(m) < 4^m$, folgt

$$P(2m-1) = P(m) \prod_{m<p\leqslant 2m-1} p \;<\; 4^m \cdot 4^{m-1} = 4^{2m-1}, \quad \text{q.e.d.}$$

C.7. Satz (Bertrandsches Postulat). *Zu jeder natürlichen Zahl $n \geqslant 1$ gibt es wenigstens eine Primzahl p mit $n < p \leqslant 2n$.*

Beweis. Wir benutzen die Primfaktor-Zerlegung von

$$N := \binom{2n}{n}.$$

Ist $n \geqslant 3$, so kommen nach Lemma C.4a) und C.4b) in N nur Primfaktoren p mit $p \leqslant 2n/3$ und $n < p \leqslant 2n$ vor. Nach C.4c) ist die Vielfachheit jedes Primfaktors $p \mid N$ mit $p > \sqrt{2n}$ gleich 1. Wir führen folgende Abkürzungen ein:

$$P(2n/3) := \prod_{p\leqslant 2n/3} p, \qquad P(n, 2n) := \prod_{n<p\leqslant 2n} p$$

und

$$Q := \prod_{p\leqslant\sqrt{2n}} p^{\upsilon_p(N)-1}.$$

Damit gilt

$$\binom{2n}{n} \leqslant Q \cdot P(2n/3) \cdot P(n, 2n)$$

Um Q abzuschätzen, beachten wir, dass nach C.4c)

$$p^{\upsilon_p(N)} \leqslant 2n \quad\Longrightarrow\quad p^{\upsilon_p(N)-1} \leqslant n.$$

Die Anzahl der Primzahlen $p \leqslant \sqrt{2n}$ ist $\leqslant \sqrt{2n} - 1$, also

$$Q \leqslant n^{\sqrt{2n}-1}.$$

Nach Lemma C.6 ist $P(2n/3) < 4^{2n/3} = 2^{4n/3}$. Mit Lemma C.4d) zusammen ergibt sich

$$\frac{2^{2n-1}}{n} \leqslant \binom{2n}{n} < n^{\sqrt{2n}-1}\, 2^{4n/3}\, P(n, 2n),$$

woraus folgt

$$P(n, 2n) > \frac{2^{2n/3-1}}{n^{\sqrt{2n}}}.$$

Der Zähler wächst für $n \to \infty$ schneller gegen ∞, als der Nenner; daher gibt es ein n_0 mit $P(n, 2n) > 1$ für $n \geqslant n_0$. Man kann $n_0 = 2^9 = 512$ wählen, denn für $n = 2^\alpha$ ist

$$\log\Big(\frac{2^{2n/3-1}}{n^{\sqrt{2n}}}\Big) = \Big(\frac{2n}{3} - 1\Big)\log 2 - \sqrt{2n}\log n = \Big(\frac{2^{\alpha+1}}{3} - 1 - 2^{(\alpha+1)/2}\alpha\Big)\log 2.$$

Dies ist positiv für $\alpha \geqslant 9$. Also gilt $P(n, 2n) > 1$ für $n \geqslant 512$, d.h. das Bertrandsche Postulat ist richtig für $n \geqslant 512$. Für kleinere n gilt es ebenfalls, wie die Reihe der Primzahlen

$$2, 3, 5, 7, 13, 23, 41, 71, 139, 263, 521$$

zeigt, von denen jede kleiner als das Doppelte der vorhergehenden ist.

D. Primitivwurzeln

D.1. Satz. *Sei G eine zyklische Gruppe der Ordnung m und $g \in G$ ein erzeugendes Element. Das Element $a := g^k$, $k \in \mathbb{Z}$, ist genau dann ein erzeugendes Element von G, wenn k zu m teilerfremd ist, d.h.* $\gcd(k, m) = 1$.

Bemerkung. Es folgt, dass eine zyklische Gruppe der Ordnung m genau $\varphi(m)$ erzeugende Elemente besitzt.

Beweis. a) Sei zunächst vorausgesetzt, dass $\gcd(k, m) = 1$. Dann gibt es ganze Zahlen λ, μ mit $\lambda k + \mu m = 1$. Daraus folgt

$$g = g^{\lambda k + \mu m} = (g^k)^\lambda (g^m)^\mu = a^\lambda e^\mu = a^\lambda.$$

Dies bedeutet, dass g in der von a erzeugten Untergruppe $\langle a \rangle \subset G$ liegt. Dann liegen aber auch alle Potenzen von g in $\langle a \rangle$, d.h. $\langle a \rangle = G$.

b) Sei a erzeugendes Element von G. Dann lässt sich insbesondere g als Potenz von a schreiben, es gibt also $\lambda \in \mathbb{Z}$ mit

$$g = a^\lambda = g^{k\lambda} \quad \Longrightarrow \quad g^{k\lambda - 1} = e \quad \Longrightarrow \quad k\lambda - 1 \equiv 0 \bmod m.$$

Es gibt also eine ganze Zahl μ mit $k\lambda - 1 = \mu m$, d.h. $\lambda k + \mu m = 1$. Daraus folgt aber $\gcd(k, m) = 1$, q.e.d.

D.2. Definition. Sei m eine positive ganze Zahl. Eine zu m teilerfremde ganze Zahl g heißt *Primitivwurzel* modulo m, wenn die Restklasse von g in $(\mathbb{Z}/m)^*$ ein erzeugendes Element dieser Gruppe ist.

Wir werden unter anderem zeigen:

a) Zu jeder Primzahl p gibt es eine Primitivwurzel modulo p.

b) Ist p eine ungerade Primzahl, so gibt es zu jeder Primzahlpotenz p^k, $(k \geqslant 1)$, eine Primitivwurzel modulo p^k.

Zunächst rechnen wir einige numerische Beispiele.

(1) $m = p = 7$.
Wir berechnen die Ordnungen aller Elemente von $(\mathbb{Z}/7)^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.

x	x^2	x^3	x^4	x^5	x^6	$\mathrm{ord}(x)$
1						1
2	4	1				3
3	2	6	4	5	1	6
4	2	1				3
5	4	6	2	3	1	6
6	1					2

Dabei entsteht z.B. die Zeile für $x = 5$ folgendermaßen:

$$x^2 \equiv 5 \cdot 5 \equiv 21 + 4 \equiv 4, \quad x^3 \equiv 4 \cdot 5 \equiv 14 + 6 \equiv 6,$$
$$x^4 \equiv 6 \cdot 5 \equiv 28 + 2 \equiv 2, \quad x^5 \equiv 2 \cdot 5 \equiv 7 + 3 \equiv 3,$$
$$x^6 \equiv 3 \cdot 5 \equiv 14 + 1 \equiv 1.$$

Aus der Tabelle entnimmt man, dass 3 und 5 Primitivwurzeln modulo 7 sind.
Man sieht auch, dass es zu jedem Teiler d der Gruppenordnung 6 ein Element gibt, das die Ordnung d hat.

(2) $m = 8 = 2^3$.

Hier ist $(\mathbb{Z}/8)^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

x	x^2	ord(x)
1		1
3	1	2
5	1	2
7	1	2

Es gibt also keine Primitivwurzel modulo 8.
Bemerkenswert ist auch, dass im Ring $\mathbb{Z}/8$ das quadratische Polynom $X^2 - 1$ insgesamt 4 Nullstellen hat und zwar alle invertierbaren Elemente von $\mathbb{Z}/8$. (In einem Körper hat ein Polynom vom Grad n höchstens n Nullstellen.)

D.3. Satz. *Sei G eine endliche Untergruppe der multiplikativen Gruppe $K^* = K \setminus \{0\}$ eines Körpers K. Dann ist G zyklisch.*

Wendet man den Satz auf die multiplikative Gruppe $(\mathbb{Z}/p)^*$ des Körpers $\mathbb{F}_p = \mathbb{Z}/p$ an, erhält man:

Folgerung. *Zu jeder Primzahl p gibt es eine Primitivwurzel g modulo p.*

Nach Satz D.1 gibt es dann insgesamt $\varphi(p-1)$ Primitivwurzeln modulo p.

Beweis. Es sei n die Ordnung der Gruppe G. Es ist zu zeigen, dass es in G ein Element der Ordnung n gibt. Wir benützen dazu die in Satz B.5 bewiesene Gleichung

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

Sei $x \in G$ ein beliebiges Element. Die Ordnung $d := \text{ord}(x)$ ist jedenfalls ein Teiler von n. Die von x erzeugte Untergruppe $H := \langle x \rangle \subset G$ ist zyklisch von der Ordnung d. Jedes Element von H ist Nullstelle des Polynoms $X^d - 1$. Da dieses Polynom über dem Körper K höchstens d Nullstellen hat, hat $X^d - 1$ auch keine anderen Nullstellen als die Elemente von H. Daraus folgt, dass jedes Element $y \in G$ der Ordnung d bereits in der zyklischen Gruppe H enthalten ist. Nach Satz D.1 gibt es somit $\varphi(d)$ Elemente

der Ordnung d in G. Für die Gesamtzahl m der Elemente aus G, deren Ordnung $< n$ ist, gilt deshalb

$$m \leqslant \sum_{\substack{d|n \\ d<n}} \varphi(d) = n - \varphi(n) < n.$$

Deshalb gibt es mindestens ein Element der Ordnung n, q.e.d.

D.4. Satz. *Ein Element a einer Gruppe G hat genau dann die Ordnung $r \in \mathbb{N}_1$, wenn folgende beiden Bedingungen erfüllt sind:*

(1) $a^r = e$,

(2) $a^{r/q} \neq e$ *für alle Primteiler $q \mid r$.*

Beweis. a) Beide Bedingungen sind offenbar notwendig.

b) Seien jetzt (1) und (2) vorausgesetzt und sei $s := \mathrm{ord}(a)$. Aus (1) folgt, dass $s \mid r$. Wäre $s \neq r$, gäbe es einen mindestens einen Primteiler $q \mid r$, so dass $s \mid (r/q)$. Daraus würde aber folgen, dass $a^{r/q} = e$, was im Widerspruch zu (2) steht. Also muss doch $s = r$ gelten, q.e.d.

D.5. Corollar. *Sei p eine Primzahl. Eine ganze Zahl $g \not\equiv 0 \bmod p$ ist genau dann eine Primitivwurzel modulo p, wenn*

$$g^{(p-1)/q} \not\equiv 1 \bmod p \quad \textit{für alle Primteiler } q \mid p-1.$$

Beweis. Dies folgt unmittelbar aus dem Satz D.4 mit $r = p - 1$, da nach dem kleinen Satz von Fermat die Bedingung (1) automatisch erfüllt ist.

Bemerkungen. 1) Für eine ungerade Primzahl p ist stets 2 ein Teiler von $p - 1$. Für eine Primitivwurzel g modulo p gilt also $g^{(p-1)/2} \not\equiv 1$. Genauer gilt sogar

$$g^{(p-1)/2} \equiv -1 \bmod p,$$

denn das Quadrat von $g^{(p-1)/2} \bmod p$ ist gleich 1, und in einem Körper (hier $\mathbb{F}_p = \mathbb{Z}/p$) hat die Gleichung $x^2 = 1$ genau zwei Lösungen, nämlich $+1$ und -1.

2) Falls die Primfaktorzerlegung von $p - 1$ bekannt ist, liefert das Corollar D.5 ein effizientes Verfahren, um eine Primitivwurzel modulo p zu finden. Man testet der Reihe nach für $g = 2, 3, \ldots$, ob das Kriterium des Corollars erfüllt ist (die Potenzen können mittels des schnellen Potenzierungs-Algorithmus berechnet werden). Da es insgesamt $\varphi(p-1) = (p-1)\prod_{q|(p-1)}(1-\frac{1}{q})$ Primitivwurzeln gibt, stößt man im allgemeinen schnell auf eine Primitivwurzel. Häufig ist bereits 2 eine Primitivwurzel. Nach einer noch unbewiesenen Vermutung von Artin ist 2 Primitivwurzel für unendlich viele Primzahlen p.

Übrigens kann man bem Testen die Quadratzahlen auslassen, denn eine Quadratzahl $a = b^2$ kann niemals Primitivwurzel einer Primzahl $p \geqslant 3$ sein, denn $a^{(p-1)/2} = b^{p-1} \equiv 1 \bmod p$, also ist die Ordnung von $a \bmod p$ ein Teiler von $(p-1)/2$.

D.6. Satz. *Sei p eine ungerade Primzahl.*
a) *Eine ganze Zahl g ist genau dann Primitivwurzel modulo p^2, wenn folgende beiden Bedingungen erfüllt sind:*

(1) *g ist Primitivwurzel modulo p*

(2) $g^{p-1} \not\equiv 1 \bmod p^2$.

b) *Ist g Primitivwurzel modulo p, aber nicht Primitivwurzel modulo p^2, so ist $\tilde{g} := g+p$ Primitivwurzel modulo p^2.*

Beweis. a) Natürlich sind die beiden Bedingungen notwendig. Sei umgekehrt vorausgesetzt, dass (1) und (2) gilt und sei x eine beliebige nicht durch p teilbare ganze Zahl. Wir müssen zeigen, dass eine natürliche Zahl n existiert mit $x \equiv g^n \bmod p^2$. Wegen (1) gibt es ein k mit

$$x \equiv g^k \bmod p.$$

Modulo p^2 ist dann

$$x \equiv (g^k + \alpha p) \bmod p^2$$

mit einer gewissen ganzen Zahl α. Da g^k modulo p invertierbar ist, gibt es eine ganze Zahl β mit $g^k\beta \equiv \alpha \bmod p$. Damit gilt dann

$$x \equiv g^k\,(1 + \beta p) \bmod p^2 \qquad (*)$$

Nach Voraussetzung (2) ist

$$g^{p-1} \equiv 1 + \gamma p \bmod p^2 \quad \text{mit } \gamma \not\equiv 0 \bmod p,$$

Daraus folgt mit dem binomischen Lehrsatz für alle $\ell \geqslant 1$

$$g^{(p-1)\ell} \equiv (1 + \gamma p)^\ell \equiv 1 + \ell\gamma p \bmod p^2.$$

Da γ invertierbar modulo p, kann man ℓ so wählen, dass $\ell\gamma \equiv \beta \bmod p$. Dann ist

$$g^{(p-1)\ell} \equiv (1 + \beta p) \bmod p^2.$$

Setzt man dies in $(*)$ ein, erhält man

$$x \equiv g^k g^{(p-1)\ell} \equiv g^{k+(p-1)\ell} \bmod p^2, \quad \text{q.e.d.}$$

b) Ist g Primitivwurzel modulo p, aber nicht modulo p^2, so ist nach Teil a)

$$g^{p-1} \equiv 1 \bmod p^2.$$

Für $\tilde{g} = g + p$ folgt dann wieder mit dem binomischen Lehrsatz

$$\tilde{g}^{p-1} \equiv (g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \not\equiv 1 \bmod p^2.$$

Also ist nach a) $\tilde{g}$ eine Primitivwurzel modulo p^2, q.e.d.

Beispiel. Die Zahl 2 ist Primitivwurzel modulo 3, da $(\mathbb{Z}/3)^* = \{\overline{1}, \overline{2}\}$. Wegen

$$2^2 \equiv 4 \not\equiv 1 \bmod 9$$

ist 2 auch Primitivwurzel modulo 9.

D.7. Satz. *Sei p eine ungerade Primzahl und g eine Primitivwurzel modulo p^2. Dann ist g auch Primitivwurzel modulo allen Potenzen p^k, $k \geqslant 2$.*

Bemerkung. Zusammen mit Satz D.6 ergibt sich daraus, das für alle Primzahlpotenzen p^k, $p \geqslant 3$, Primitivwurzeln existieren.

Beweis. Wir beweisen durch Induktion über $k \geqslant 2$: Ist x Primitivwurzel modulo p^k, so auch modulo p^{k+1}. Dazu genügt es zu zeigen (vgl. den Beweis von D.6): Für eine Primitivwurzel x modulo p^k gilt

$$x^{p^{k-1}(p-1)} \not\equiv 1 \bmod p^{k+1}.$$

(Es ist $p^{k-1}(p-1) = \#((\mathbb{Z}/p^k\mathbb{Z})^*)$.) Dies sieht man so: Da $x \bmod p^k$ die Ordnung $p^{k-1}(p-1)$ hat, ist

$$x^{p^{k-2}(p-1)} \not\equiv 1 \bmod p^k,$$

aber $x^{p^{k-2}(p-1)} \equiv 1 \bmod p^{k-1}$, d.h. $x^{p^{k-2}(p-1)} = 1 + ap^{k-1}$ mit $p \nmid a$. Daraus folgt

$$x^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p \equiv 1 + ap^k \mod p^{k+1}.$$

Daraus folgt die Behauptung.

Wir wenden uns jetzt den Potenzen der Primzahl 2 zu. Trivialerweise sind

$$(\mathbb{Z}/2)^* = \{\overline{1}\} \quad \text{und} \quad (\mathbb{Z}/4)^* = \{\overline{1}, \overline{3}\}$$

zyklisch. Dies gilt nicht mehr für höhere Potenzen, wie wir schon für $(\mathbb{Z}/8)^*$ gesehen haben.

D.8. Satz. *Die Gruppe $(\mathbb{Z}/2^k)^*$ ist für $k \geqslant 3$ nicht zyklisch. Die Elemente der Form*

$$x \equiv 1 \bmod 4$$

bilden eine zyklische Untergruppe der Ordnung 2^{k-2}, die von der Restklasse $5 \bmod 2^k$ erzeugt wird. Man hat einen Gruppen-Isomorphismus

$$\begin{aligned} (\mathbb{Z}/2, +) \times (\mathbb{Z}/2^{k-2}, +) &\longrightarrow (\mathbb{Z}/2^k)^*, \\ (\mu \bmod 2 \ , \ \nu \bmod 2^{k-2}) &\mapsto (-1)^\mu 5^\nu \bmod 2^k. \end{aligned}$$

Beweis. ...

F. Quadratische Reste. Reziprozitätsgesetz

F.1. Definition. Sei m eine natürliche Zahl $\geqslant 2$. Eine ganze Zahl a heißt *quadratischer Rest* modulo m (Abkürzung QR), falls die Kongruenz

$$x^2 \equiv a \bmod m$$

eine Lösung $x \in \mathbb{Z}$ besitzt. Andernfalls heißt a *quadratischer Nichtrest* modulo m (Abkürzung NR).

Dies lässt sich auch so ausdrücken: a ist genau dann quadratischer Rest modulo m, wenn die Klasse von a im Ring $\mathbb{Z}/m$ ein Quadrat ist. Wegen des Chinesischen Restsatzes kann man den allgemeinen Fall darauf zurückführen, dass der Modul m eine Primzahlpotenz ist, $m = p^k$. Wir beschäftigen uns in dieser Vorlesung hauptsächlich mit dem Fall $k = 1$, d.h. quadratischen Resten modulo einer Primzahl p. Der Fall $p = 2$ ist trivial (jede ganze Zahl ist Quadrat modulo 2). Sei daher jetzt p eine ungerade Primzahl. Die Frage nach den quadratischen Resten modulo p ist dann gleichbedeutend mit der Frage nach den Quadraten im Körper $\mathbb{Z}/p$. Da 0 stets ein Quadrat ist, kann man sich auf $(\mathbb{Z}/p)^*$ beschränken.

Betrachten wir zunächst ein Beispiel $p = 11$.

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

mod 11

Es sind also die Restklassen von 1,3,4,5,9 Quadrate in $(\mathbb{Z}/11)^*$, die Restklassen von 2,6,7,8,11 sind Nicht-Quadrate. Es sind also genau die Hälfte der Elemente von $(\mathbb{Z}/11)^*$ Quadrate. Wir werden sehen, dass dies auch für beliebige ungerade Primzahlen p gilt.

Dies gilt nicht mehr für zusammengesetzte Moduln. Z.B. haben wir für für $m = 15$ folgende Quadrate-Tafel für $(\mathbb{Z}/15)^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

x	1	2	4	7	8	11	13	14
x^2	1	4	1	4	4	1	4	1

mod 15

Hier gibt es also nur zwei Quadrate. Dies lässt sich so erklären: Nach dem Chinesischen Restsatz gilt $(\mathbb{Z}/15)^* \cong (\mathbb{Z}/3)^* \times (\mathbb{Z}/5)^*$. In $(\mathbb{Z}/3)^*$ gibt es nur ein Quadrat und in $(\mathbb{Z}/5)^*$ zwei Quadrate, also im Produkt auch nur zwei Quadrate.

F.2. Definition (Legendre-Symbol). Sei $a \in \mathbb{Z}$ und p eine ungerade Primzahl. Dann wird das *Legendre-Symbol* $\left(\frac{a}{p}\right)$ wie folgt definiert:

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{falls } p \mid a, \\ +1, & \text{falls } p \nmid a \text{ und } a \text{ ist QR mod } p, \\ -1, & \text{falls } p \nmid a \text{ und } a \text{ ist NR mod } p. \end{cases}$$

Die Gleichung $x^2 \equiv a \bmod p$ ist also genau dann lösbar, wenn $(\frac{a}{p}) \geqslant 0$. Offenbar gilt

$$a \equiv b \bmod p \quad \Longrightarrow \quad \Big(\frac{a}{p}\Big) = \Big(\frac{b}{p}\Big).$$

F.3. Satz (Euler-Kriterium). *Sei p eine ungerade Primzahl. Dann gilt für jede ganze Zahl a*

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

Beweis. Falls $p \mid a$, sind beide Seiten $\equiv 0 \bmod p$. Wir können also im folgenden voraussetzen, dass $p \nmid a$.

1. Fall: a ist quadratischer Rest modulo p. Dann gibt es eine ganze Zahl b mit $a \equiv b^2 \bmod p$. Natürlich gilt auch $p \nmid b$. Daher folgt aus dem kleinen Satz von Fermat

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \equiv \Big(\frac{a}{b}\Big) \bmod p.$$

2. Fall: a ist quadratischer Nichtrest. Sei g eine Primitivwurzel modulo p. Dann ist $a \equiv g^m$ mit einer ungeraden Zahl $m = 2k+1$. Damit folgt

$$a^{(p-1)/2} \equiv g^{(2k+1)(p-1)/2} \equiv g^{k(p-1)} g^{(p-1)/2} \equiv g^{(p-1)/2} \equiv -1 \equiv \Big(\frac{a}{b}\Big) \bmod p.$$

Bemerkung. Wegen des schnellen Potenzierungs-Algorithmus liefert Satz F.3 eine effiziente Methode, das Legendre-Symbol zu berechnen. Wir werden aber später sehen, dass man mittels des quadratischen Reziprozitätsgesetzes das Legendre-Symbol noch schneller berechnen kann.

F.4. Corollar. *Für jede ungerade Primzahl p und alle ganzen Zahlen a, b gilt*

$$\Big(\frac{a}{p}\Big)\Big(\frac{b}{p}\Big) = \Big(\frac{ab}{p}\Big).$$

Aus der Multiplikativität des Legendre-Symbols folgt z.B. dass das Produkt zweier quadratischer Nichtreste ein quadratischer Rest ist.

Das Corollar bedeutet, dass die Abbildung

$$\Big(\frac{-}{p}\Big) : (\mathbb{Z}/p)^* \longrightarrow \{\pm 1\}, \quad x \mapsto \Big(\frac{x}{p}\Big)$$

ein Gruppen-Homomorphismus ist. Dieser Homomorphismus ist surjektiv, da eine Primitivwurzel g modulo p sicher ein quadratischer Nichtrest ist. Der Kern dieser Abbildung ist die Menge der Quadrate in $(\mathbb{Z}/p)^*$. Dies ist eine Untergruppe vom Index 2. Es gibt also ebenso viele Quadrate wie Nichtquadrate in $(\mathbb{Z}/p)^*$.

F.5. Quadratisches Reziprozitätsgesetz

Das quadratische Reziprozitätsgesetz macht eine Aussage darüber, wie sich die Legendresymbole $(\frac{p}{q})$ und $(\frac{q}{p})$ zueinander verhalten, wobei $p \neq q$ zwei ungerade Primzahlen sind. Es stellt sich heraus, dass beide Symbole denselben Wert haben, falls wenigstens eine der beiden Primzahlen $\equiv 1 \bmod 4$ ist; dagegen sind die Symbole entgegengesetzt gleich, falls $p \equiv q \equiv 3 \bmod 4$. Das Reziprozitätsgesetz wurde zuerst von Gauß bewiesen, nachdem sich vorher schon u.a. Legendre und Euler vergeblich darum bemüht hatten. Gauß selbst hat 8 Beweise gegeben und bis heute wurden rund 200 Beweise veröffentlicht, wenn auch die meisten nur Varianten von vorherigen sind. Wir bringen hier einen elementaren, auf Gauß zurückgehenden Beweis. Dazu brauchen wir einige Vorbereitungen.

Sei p eine ungerade Primzahl. Wir bezeichnen mit $H(p)$ das 'Halbsystem' modulo p,

$$H(p) := \Big\{1, 2, \ldots, \frac{p-1}{2}\Big\}.$$

Für jede ganze Zahl n, die nicht durch p teilbar ist, lässt sich ihre Restklasse modulo p eindeutig schreiben als

$$n \equiv \varepsilon \cdot u \bmod p \quad \text{mit } \varepsilon \in \{\pm 1\} \text{ und } u \in H(p).$$

Man nennt εu den *absolut kleinsten Rest* von n modulo p.

Sei nun eine Zahl $a \in \mathbb{Z}$ mit $p \nmid a$ vorgegeben. Für $x \in H(p)$ definieren definieren wir $\varepsilon_a(x) \in \{\pm 1\}$ und $\sigma_a(x) \in H(p)$ durch die Bedingung

$$ax \equiv \varepsilon_a(x)\sigma_a(x) \bmod p.$$

Es ist leicht zu sehen, dass die Abbildung $\sigma_a : H(p) \to H(p)$ bijektiv, d.h. eine Permutation von $H(p)$ ist.

F.6. Satz (Gaußsches Lemma). *Sei p eine ungerade Primzahl und a eine zu p teilerfremde ganze Zahl. Dann gilt*

$$\Big(\frac{a}{p}\Big) = \prod_{x \in H(p)} \varepsilon_a(x).$$

Dies ist äquivalent mit folgender Aussage: Sei m die Anzahl der Elemente von

$$\Big\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\Big\},$$

deren absolut kleinster Rest modulo p negativ ist. Dann ist $(\frac{a}{p}) = 1$, wenn m gerade, und $(\frac{a}{p}) = -1$, wenn m ungerade ist.

Beweis. Es gilt

$$\prod_{x \in H(p)} (ax) \equiv \prod_{x \in H(p)} \varepsilon_a(x) \prod_{x \in H(p)} \sigma_a(x) \equiv \prod_{x \in H(p)} \varepsilon_a(x) \prod_{x \in H(p)} x,$$

denn durchläuft x alle Elemente von $H(p)$, so durchläuft auch $\sigma_a(x)$ alle Elemente von $H(p)$. Andrerseits ist

$$\prod_{x\in H(p)} (ax) = a^{(p-1)/2} \prod_{x\in H(p)} x,$$

also folgt mit dem Euler-Kriterium

$$\prod_{x\in H(p)} \varepsilon_a(x) \equiv a^{(p-1)/2} \equiv \Big(\frac{a}{p}\Big), \quad \text{q.e.d.}$$

Beispiel. Sei $p = 7$. Dann ist $H(p) = \{1, 2, 3\}$. Für $a = 2$ haben wir

$$2 \cdot 1 = 2, \quad 2 \cdot 2 = 4 \equiv -3, \quad 2 \cdot 3 = 6 \equiv -1,$$

also $\varepsilon_2(1) = 1$, $\varepsilon_2(2) = -1$, $\varepsilon_2(3) = -1$, woraus folgt $(\frac{2}{7}) = 1$, d.h. 2 ist quadratischer Rest modulo 7. In der Tat ist $3^2 \equiv 2 \bmod 7$.

Für die Anwendung des Gaußschen Lemmas ist eine Umformulierung nützlich. Sei weiter p eine ungerade Primzahl und a eine positive, zu p teilerfremde ganze Zahl. Für $\nu = 1, \ldots, a$ betrachten wir die Intervalle

$$I_\nu := \Big\{ x \in \mathbb{R} : (\nu - 1)\,\frac{p}{2} < x < \nu\,\frac{p}{2} \Big\}.$$

Offenbar ist für $k \in H(p) = \{1, \ldots, (p-1)/2\}$ der absolut kleinste Rest von ka modulo p genau dann negativ, d.h. $\varepsilon_a(k) = -1$, wenn ka in einem Intervall I_ν mit geradem Index ν liegt. Wir bezeichnen mit r_ν die Anzahl der ka, $k \in H$, die in I_ν liegen. Da kein ka auf einem Randpunkt eines der I_ν liegt, folgt

$$r_\nu = \Big\lfloor \nu\,\frac{p}{2a} \Big\rfloor - \Big\lfloor (\nu - 1)\,\frac{p}{2a} \Big\rfloor,$$

wobei $\lfloor x \rfloor$ für eine reelle Zahl x die größte ganze Zahl $\leqslant x$ bezeichnet. Nach dem Gaußschen Lemma ist $(\frac{a}{p}) = (-1)^m$ mit

$$m = \sum_{0<2\nu\leqslant a} r_{2\nu}.$$

Somit folgt

F.7. Corollar. *Sei p eine ungerade Primzahl und a eine positive, zu p teilerfremde ganze Zahl. Dann gilt*

$$\Big(\frac{a}{p}\Big) = (-1)^m \quad \text{mit} \quad m = \sum_{k=1}^{\lfloor a/2 \rfloor} \Big(\Big\lfloor k\,\frac{p}{a} \Big\rfloor - \Big\lfloor (k - \tfrac{1}{2})\,\frac{p}{a} \Big\rfloor \Big).$$

Als erste Anwendung beweisen wir die sog. Ergänzungssätze zum Reziprozitätsgesetz.

F.8. Satz. *Sei p eine ungerade Primzahl. Dann gilt:*

i) (1. Ergänzungssatz)

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \text{für } p \equiv 1 \bmod 4, \\ -1 & \text{für } p \equiv 3 \bmod 4. \end{cases}$$

ii) (2. Ergänzungssatz)

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \text{für } p \equiv \pm 1 \bmod 8, \\ -1 & \text{für } p \equiv \pm 3 \bmod 8. \end{cases}$$

Beweis. i) Dies folgt aus dem Gaußschen Lemma, da $\varepsilon_{-1}(x) = -1$ für alle $x \in H(p)$. Die Behauptung ist aber auch eine direkte Anwendung des Euler-Kriteriums F.3.

ii) Für $a = 2$ ergibt die Formel des Corollars F.7

$$\left(\frac{2}{p}\right) = (-1)^m \quad \text{mit} \quad m = \lfloor p/2 \rfloor - \lfloor p/4 \rfloor.$$

Wir werten dies durch Fallunterscheidung aus

p	$\lfloor p/2 \rfloor$	$\lfloor p/4 \rfloor$	m	$(-1)^m$
$8k+1$	$4k$	$2k$	$2k$	$+1$
$8k-1$	$4k-1$	$2k-1$	$2k$	$+1$
$8k+3$	$4k+1$	$2k$	$2k+1$	-1
$8k-3$	$4k-2$	$2k-1$	$2k-1$	-1

Daraus folgt die Behauptung.

F.9. Satz. *Sei p eine ungerade Primzahl und a eine positive, zu p teilerfremde ganze Zahl. Sei q eine weitere Primzahl mit $q \equiv \pm p \bmod 4a$. Dann folgt*

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

Beweis. Nach dem Corollar F.7 gilt $\left(\frac{a}{p}\right) = (-1)^m$ mit

$$m = \sum_{\nu=1}^{\lfloor a/2 \rfloor} (s_{2\nu} - s_{2\nu-1}), \quad \text{wobei} \quad s_k = \left\lfloor k \frac{p}{2a} \right\rfloor$$

und entsprechend $\left(\frac{a}{q}\right) = (-1)^{m'}$ mit

$$m' = \sum_{\nu=1}^{\lfloor a/2 \rfloor} (s'_{2\nu} - s'_{2\nu-1}), \quad \text{wobei} \quad s'_k = \left\lfloor k \frac{q}{2a} \right\rfloor.$$

i) Wir behandeln zunächst den Fall $q \equiv p \bmod 4a$. Dann ist $q = p + 4at$ mit einer ganzen Zahl t. Es folgt

$$s'_k = \left\lfloor k\,\frac{p+4at}{2a} \right\rfloor = \left\lfloor k\frac{p}{2a} + 2kt \right\rfloor = \left\lfloor k\frac{p}{2a} \right\rfloor + 2kt = s_k + 2kt.$$

Also gilt $m' \equiv m \bmod 2$, woraus die Behauptung folgt.

ii) Sei jetzt $q \equiv -p \bmod 4a$, d.h. $q = 4at - p$ mit einer ganzen Zahl t. Dann ist

$$s'_k + s_k = \left\lfloor k\,\frac{4at-p}{2a} \right\rfloor + \left\lfloor k\frac{p}{2a} \right\rfloor = 2kt + \left\lfloor -k\frac{p}{2a} \right\rfloor + \left\lfloor k\frac{p}{2a} \right\rfloor = 2kt - 1$$

für $1 \leqslant k \leqslant a$, da dann $\frac{kp}{2a}$ keine ganze Zahl ist. Es folgt

$$(s'_{2\nu} - s'_{2\nu-1}) + (s_{2\nu} - s_{2\nu-1}) \equiv 0 \bmod 2 \quad \text{für } 1 \leqslant \nu \leqslant \lfloor a/2 \rfloor,$$

also $m' \equiv m \bmod 2$, q.e.d.

F.10. Satz (Quadratisches Reziprozitätsgesetz). *Seien $p \neq q$ zwei ungerade Primzahlen. Dann gilt*

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

Dies lässt sich auch so aussprechen: Ist wenigstens eine der Primzahlen $\equiv 1 \bmod 4$, so gilt $(\frac{p}{q}) = (\frac{q}{p})$; falls aber $p \equiv q \equiv 3 \bmod 4$, so folgt $(\frac{p}{q}) = -(\frac{q}{p})$.

Beweis. i) Wir behandeln zuerst den Fall $p \equiv q \bmod 4$. Dann ist $p = q + 4r$ mit einer ganzen Zahl r, die wir als positiv annehmen können (sonst vertausche man die Rollen von p und q). Außerdem gilt $q \nmid r$. Nach Satz F.9 ist

$$\left(\frac{r}{q}\right) = \left(\frac{r}{p}\right).$$

Andrerseits ist

$$\left(\frac{r}{q}\right) = \left(\frac{4r}{q}\right) = \left(\frac{4r+q}{q}\right) = \left(\frac{p}{q}\right)$$

und unter Benutzung des 1. Ergänzungssatzes

$$\left(\frac{r}{p}\right) = \left(\frac{4r}{p}\right) = \left(\frac{p-q}{p}\right) = \left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right),$$

also $(\frac{p}{q}) = (\frac{q}{p})$, falls $p \equiv q \equiv 1 \bmod 4$ und $(\frac{p}{q}) = -(\frac{q}{p})$, falls $p \equiv q \equiv 3 \bmod 4$.

ii) Falls $p \not\equiv q \bmod 4$, gilt $p \equiv -q \bmod 4$, also $p + q = 4r$ mit einer ganzen Zahl r. Wieder gilt nach Satz F.9

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

und

$$\Big(\frac{r}{q}\Big) = \Big(\frac{4r}{q}\Big) = \Big(\frac{4r-q}{q}\Big) = \Big(\frac{p}{q}\Big)$$

sowie

$$\Big(\frac{r}{p}\Big) = \Big(\frac{4r}{p}\Big) = \Big(\frac{4r-p}{p}\Big) = \Big(\frac{q}{p}\Big),$$

also $(\frac{p}{q}) = (\frac{q}{p})$. Damit ist das quadratische Reziprozitätsgesetz vollständig bewiesen.

Bemerkung. Wir haben hier das Reziprozitätsgesetz aus Satz F.9 abgeleitet. Umgekehrt lässt sich Satz F.9 auch leicht mithilfe des Reziprozitätsgesetzes beweisen (Übung).

Als Anwendung der Ergänzungssätze zum quadratischen Reziprozitätsgesetz beweisen wir jetzt die Existenz von unendlich vielen Primzahlen in arithmetischen Progressionen zum Modul 8.

F.11. Satz. *In jeder der arithmetischen Progressionen*

$$8k+1, \quad 8k+3, \quad 8k+5, \quad 8k+7, \quad (k \in \mathbb{N}),$$

gibt es unendlich viele Primzahlen.

Beweis. Sei $B > 0$ eine vorgegebene Schranke und U das Produkt aller ungeraden natürlichen Zahlen $\leqslant B$. Wir definieren

$$\begin{aligned} N_1 &:= (2U)^4 + 1, \\ N_3 &:= U^2 + 2, \\ N_5 &:= U^2 + 4, \\ N_7 &:= 8U^2 - 1. \end{aligned}$$

Da ein Quadrat einer ungeraden Zahl stets $\equiv 1 \bmod 8$ ist, folgt $U^2 \equiv 1 \bmod 8$ und

$$N_k \equiv k \bmod 8 \quad \text{für } k = 1, 3, 5, 7.$$

Außerdem besitzt N_k keinen Primteiler $q \leqslant B$. Denn ein solcher Primteiler ist ungerade und teilt U. Also kann q nicht N_k ohne Rest teilen.

Unser Satz wird deshalb bewiesen sein, wenn wir zeigen, dass N_k einen Primteiler $q \mid N_k$ mit $q \equiv k \bmod 8$ besitzt.

i) Sei q ein Primteiler von $N_1 = (2U)^4 + 1$. Dann gilt $(2U)^4 + 1 \equiv 0 \bmod q$, d.h.

$$x^4 \equiv -1 \bmod q \quad \text{mit } x := 2U.$$

Daraus folgt, dass das Element x in $(\mathbb{Z}/q)^*$ die Ordnung 8 besitzt. Daher ist 8 ein Teiler von $\#(\mathbb{Z}/q)^* = q - 1$, d.h. $q \equiv 1 \bmod 8$, q.e.d.

ii) Sei q ein Primteiler von $N_3 = U^2 + 2$. Dann folgt

$$U^2 \equiv -2 \bmod q \quad \Longrightarrow \quad \Big(\frac{-2}{q}\Big) = 1.$$

Aus den Ergänzungssätzen zum quadratischen Reziprozitäts-Gesetz folgt dann $q \equiv 1 \bmod 8$ oder $q \equiv 3 \bmod 8$. Es können aber nicht alle Primteiler von N_3 kongruent $1 \bmod 8$ sein, denn dann wäre $N_3 \equiv 1 \bmod 8$. Es gibt also mindestens einen Primteiler $q \mid N_3$ mit $q \equiv 3 \bmod 8$.

iii) Sei q ein Primteiler von $N_5 = U^2 + 4$. Dann folgt

$$U^2 \equiv -4 \bmod q \quad \Longrightarrow \quad \Big(\frac{-1}{q}\Big) = 1.$$

Daraus folgt $q \equiv 1 \bmod 4$, d.h. $q \equiv 1 \bmod 8$ oder $q \equiv 5 \bmod 8$. Es können aber nicht alle Primteiler von N_5 kongruent $1 \bmod 8$ sein, denn dann wäre $N_5 \equiv 1 \bmod 8$. Es gibt also mindestens einen Primteiler $q \mid N_5$ mit $q \equiv 5 \bmod 8$.

iv) Sei q ein Primteiler von $N_7 = 8U^2 - 1$. Dann folgt $8U^2 - 1 \equiv 0 \bmod q$, also nach Multiplikation mit 2

$$(4U)^2 \equiv 2 \bmod q \quad \Longrightarrow \quad \Big(\frac{2}{q}\Big) = 1.$$

Nach dem 2. Ergänzungssatz zum quadratischen Reziprozitäts-Gesetz ist daher $q \equiv \pm 1 \bmod 8$. Es können aber nicht alle Primteiler von N_7 kongruent $1 \bmod 8$ sein, denn dann wäre $N_7 \equiv 1 \bmod 8$. Es gibt also mindestens einen Primteiler $q \mid N_7$ mit $q \equiv -1 \equiv 7 \bmod 8$, q.e.d.

F.12. Das Jacobi-Symbol. Es ist für manche Zwecke nützlich, das Legendre-Symbol $(\frac{a}{p})$ auf den Fall zu verallgemeinern, dass der 'Nenner' keine Primzahl mehr ist.

Sei $m \geqslant 3$ eine ungerade Zahl und

$$m = p_1 p_2 \cdot \ldots \cdot p_r$$

die Primfaktor-Zerlegung von m (die p_j sind nicht notwendig paarweise verschieden). Dann definiert man für eine ganze Zahl a das *Jacobi-Symbol* $(\frac{a}{m})$ durch

$$\Big(\frac{a}{m}\Big) := \prod_{j=1}^{r} \Big(\frac{a}{p_j}\Big).$$

Das Jacobi-Symbol genügt folgenden Rechenregeln:

1) $\Big(\frac{a}{m}\Big) = \Big(\frac{b}{m}\Big)$, falls $a \equiv b \bmod m$,

2) $\Big(\frac{ab}{m}\Big) = \Big(\frac{a}{m}\Big)\Big(\frac{b}{m}\Big)$,

3) $\left(\frac{a}{mk}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{k}\right)$ für ungerade $m, k \geqslant 3$,

4) $\left(\frac{a}{m}\right) = 0 \iff \gcd(a, m) \neq 1$.

Diese Regeln folgen unmittelbar aus der Definition und den entsprechenden Regeln für das Legendre-Symbol.

Man beachte jedoch folgenden Unterschied zum Legendre-Symbol: Ist a quadratischer Rest modulo m und $\gcd(a, m) = 1$, so folgt zwar $(\frac{a}{m}) = 1$, aber umgekehrt kann man aus $(\frac{a}{m}) = 1$ nicht schließen, dass a quadratischer Rest modulo m ist. Z.B. ist 2 weder quadratischer Rest mod 3 noch mod 5, also auch nicht quadratischer Rest mod 15, aber

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

F.13. Satz (Quadratisches Reziprozitätsgesetz für das Jacobi-Symbol).
Sei $m \geqslant 3$ eine ungerade Zahl.

(1) 1. Ergänzungssatz:

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2} = \begin{cases} +1 & \text{für } m \equiv 1 \bmod 4, \\ -1 & \text{für } m \equiv 3 \bmod 4. \end{cases}$$

(2) 2. Ergänzungssatz:

$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8} = \begin{cases} +1 & \text{für } m \equiv \pm 1 \bmod 8, \\ -1 & \text{für } m \equiv \pm 3 \bmod 8. \end{cases}$$

(3) *Ist $k \geqslant 3$ eine weitere, zu m teilerfremde ungerade Zahl, so gilt*

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

d.h. $\left(\frac{k}{m}\right) = \left(\frac{m}{k}\right)$, *falls* $m \equiv 1 \bmod 4$ *oder* $k \equiv 1 \bmod 4$

und $\left(\frac{k}{m}\right) = -\left(\frac{m}{k}\right)$, *falls* $m \equiv k \equiv 3 \bmod 4$.

Beweis. (Zurückführung auf die entsprechenden Aussagen für das Legendre-Symbol)

F.14. Effiziente Berechnung des Jacobi-Symbols. Mit dem Reziprozitätsgesetz kann man einen effizienten Algorithmus zur Berechnung des Jacobi-Symbols herleiten: Es sei $(\frac{a}{m})$, $a, m \in \mathbb{Z}$, $m \geqslant 3$ ungerade, zu berechnen.

(1) Zunächst reduziere man a mod m, d.h. man bestimme ein a' mit $a \equiv a' \bmod m$ und $0 \leqslant a' < m$. Natürlich ist

$$\Big(\frac{a}{m}\Big) = \Big(\frac{a'}{m}\Big).$$

Falls $a' = 0$ oder $a' = 1$ ist man fertig.

(2) Falls a' gerade, schreibe man $a' = 2^\nu b$ mit b ungerade. (Falls a' ungerade, ist $b = a'$ und $\nu = 0$.) Dann ist

$$\Big(\frac{a'}{m}\Big) = \Big(\frac{2}{m}\Big)^\nu \Big(\frac{b}{m}\Big),$$

und $(\frac{2}{m}) = \pm 1$ kann nach dem zweiten Ergänzungssatz berechnet werden. Falls $b = 1$, ist man fertig.

(3) Auf $(\frac{b}{m})$ kann jetzt das Reziprozitätsgesetz angewendet werden:

$$\Big(\frac{b}{m}\Big) = (-1)^{\frac{b-1}{2}\frac{m-1}{2}} \Big(\frac{m}{b}\Big).$$

Dies gilt auch, wenn b und m nicht teilerfremd sind, denn dann sind beide Seiten $= 0$.

Auf $(\frac{m}{b})$ kann man jetzt wieder (1) anwenden. Da die 'Nenner' des Jacobi-Symbols immer kleiner werden, ist man nach endlich vielen Schritten fertig. Die Anzahl der Schritte ist vergleichbar mit den beim Euklidischen Algorithmus für die Berechnung von $\gcd(a, m)$ nötigen Schritte, wächst also nur linear mit der Stellenzahl von m.

Man beachte: Selbst wenn man nur ein Legendre-Symbol $(\frac{a}{p})$ mit einer Primzahl p mit dieser Methode ausrechnet, kann man zwischenzeitlich auf die allgemeineren Jacobi-Symbole stoßen.

Beispiel.

$$\begin{aligned}\Big(\frac{170}{211}\Big) &= \Big(\frac{2}{211}\Big)\Big(\frac{85}{211}\Big) = -\Big(\frac{85}{211}\Big) = -\Big(\frac{211}{85}\Big) = -\Big(\frac{41}{85}\Big) = \\ &= -\Big(\frac{85}{41}\Big) = -\Big(\frac{3}{41}\Big) = -\Big(\frac{41}{3}\Big) = -\Big(\frac{2}{3}\Big) = 1.\end{aligned}$$

L. Der Drei-Quadrate-Satz von Gauß

Bekanntlich ist eine ungerade Primzahl p genau dann Summe zweier Quadratzahlen, wenn $p \equiv 1 \bmod 4$. Daraus folgt, dass eine positive ganze Zahl n genau dann Summe zweier Quadratzahlen ist, wenn in der Primfaktor-Zerlegung von n alle Primfaktoren mit $p \equiv 3 \bmod 4$ mit gerader Vielfachheit vorkommen. Relativ einfach zu beweisen ist auch der Satz von Lagrange, dass jede natürliche Zahl Summe von vier Quadratzahlen ist. Schwieriger ist der Fall von Summen dreier Quadrate.

L.1. Satz (Drei-Quadrate-Satz von Gauß). *Eine positive ganze Zahl n ist genau dann Summe dreier Quadratzahlen,*

$$(*) \qquad n = x_1^2 + x_2^2 + x_3^2, \qquad x_i \in \mathbb{Z},$$

wenn $n = 4^k m$ mit $4 \nmid m$ und $m \not\equiv 7 \bmod 8$.

Wir zeigen jetzt kurz die Notwendigkeit der Bedingungen. Das Quadrat einer ganzen Zahl nimmt modulo 8 nur die Werte 0,1,4 an. Daraus folgt, dass eine natürliche Zahl $n \equiv 7 \bmod 8$ nicht die Summe dreier Quadratzahlen sein kann. Es ist also nur noch zu zeigen: Ist $4n$ eine Summe von drei Quadraten, so auch n. Dies sieht man so: Ist $4n = x_1^2 + x_2^2 + x_3^2$, so müssen alle x_i gerade sein, und n ist Summe der Quadratzahlen $(x_i/2)^2$.

Dass die Bedingungen auch hinreichend sind, können wir erst nach einigen Vorbereitungen beweisen.

Der folgende Satz zeigt, dass es genügt, eine Abschwächung der Gleichung $(*)$ zu lösen.

L.2. Satz (L. Aubry). *Sei n eine natürliche Zahl. Genau dann besitzt die Gleichung*

$$n = x_1^2 + x_2^2 + x_3^2$$

eine ganzzahlige Lösung $(x_1, x_2, x_2) \in \mathbb{Z}^3$, wenn die Gleichung

$$nt^2 = x_1^2 + x_2^2 + x_3^2$$

eine nicht-tiviale Lösung $(t, x_1, x_2, x_2) \in \mathbb{Z}^4$ besitzt.

Beweis. Wir benutzen die Abkürzungen

$$\|x\|^2 := \sum_{i=1}^{3} x_i^2 \quad \text{und} \quad \langle x, y\rangle := \sum_{i=1}^{3} x_i y_i$$

für $(x_1, x_2, x_3), (y_1, y_2, y_3) \in \mathbb{Z}^3$. Sei

$$nt^2 = \|x\|^2, \quad (t, x) \in \mathbb{Z} \times \mathbb{Z}^3, \quad t \neq 0.$$

Wir können $t > 0$ annehmen. Falls $t = 1$, sind wir fertig. Sei also $t > 1$. Es genügt offenbar, ein $t' \in \mathbb{Z}$ und ein $x' \in \mathbb{Z}^3$ zu finden mit $1 \leqslant t' < t$ und $nt'^2 = \|x'\|^2$.

Wir teilen x_ν durch t mit absolut kleinstem Rest:

$$x_\nu = ty_\nu + z_\nu, \quad y_\nu, z_\nu \in \mathbb{Z}, \quad |z_\nu| \leqslant \tfrac{1}{2}\, t.$$

Für die Vektoren $y = (y_1, y_2, y_3), z = (z_1, z_2, z_3) \in \mathbb{Z}^3$ gilt dann

$$x = ty + z, \quad \|z\|^2 \leqslant \tfrac{3}{4}\, t^2.$$

Falls $z = 0$, sind wir fertig, denn dann ist $n = \|y\|^2$. Sei nun $z \neq 0$. Es ist

$$nt^2 = \|x\|^2 = t^2\|y\|^2 + 2t\langle y, z\rangle + \|z\|^2.$$

Daraus folgt, dass $\|z\|^2$ durch t teilbar ist,

$$\|z\|^2 = tt' \quad \text{mit } t' \in \mathbb{Z}, \quad 0 < t' \leqslant \tfrac{3}{4}\, t.$$

Setzen wir dies in die vorige Gleichung ein, so erhalten wir nach Kürzung durch t

$$t\,(n - \|y\|^2) = 2\langle y, z\rangle + t'.$$

Mit der Abkürzung $\delta := n - \|y\|^2$ haben wir

$$2\langle y, z\rangle = t\delta - t'.$$

Behauptung. Für den Vektor $x' := t'y - \delta z$ gilt

$$nt'^2 = \|x'\|^2.$$

Beweis hierfür.

$$\begin{aligned} \|x'\|^2 &= t'^2\|y\|^2 - 2t'\delta\langle y, z\rangle + \delta^2\|z\|^2 \\ &= t'^2\|y\|^2 - t'\delta(t\delta - t') + \delta^2 tt' \\ &= t'^2\|y\|^2 + t'^2\delta = nt'^2, \quad \text{q.e.d.} \end{aligned}$$

Damit ist Satz 2 bewiesen.

Legendresche Gleichung

Unter der Legendre-Gleichung versteht man die Diophantische Gleichung

$$ax^2 + by^2 + cz^2 = 0 \tag{1}$$

Dabei seien a, b, c von 0 verschiedene ganze Zahlen. Unter einer Lösung von (1) verstehen wir stets eine ganzzahlige Lösung $(x, y, z) \in \mathbb{Z}^3$ mit $(x, y, z) \neq (0, 0, 0)$. Es ist klar, dass genau dann eine ganzzahlige Lösung existiert, wenn es eine rationale Lösung $(x, y, z) \in \mathbb{Q}^3 \setminus \{(0, 0, 0)\}$ gibt. Bei der Behandlung der Legendre-Gleichung kann man sich auf den Fall beschränken, dass die Koeffizienten quadratfrei sind, denn mit $a = a_1\alpha^2,\ b = b_1\beta^2,\ c = c_1\gamma^2$ ist

$$ax^2 + by^2 + cz^2 = a_1(\alpha x)^2 + b_1(\beta y)^2 + c_1(\gamma z)^2$$

Für den Beweis des Drei-Quadrate-Satzes brauchen wir nur folgenden Spezialfall.

L.3. Satz (Legendre). *Seien $a, b \in \mathbb{Z} \setminus \{0\}$ quadratfreie, teilerfremde ganze Zahlen, die nicht beide negativ sind. Genau dann besitzt die Gleichung*

$$ax^2 + by^2 = z^2 \tag{2}$$

eine Lösung $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$, wenn folgende Bedingungen erfüllt sind:

(i) *a ist ein Quadrat modulo b,*

(ii) *b ist ein Quadrat modulo a.*

Beweis.

a) Zur Notwendigkeit der Bedingungen. In diesem Teil des Beweises wird nicht benutzt, dass a und b teilerfremd sind.

Sei (x, y, z) eine primitive Lösung, d.h. x, y, z haben keinen gemeinsamen Primeiler. Wir zeigen, dass dann x und b teilerfremd sind. Denn ein gemeinsamer Primteiler p von x und b wäre auch ein Teiler von z. Aus (2) folgt dann $p^2 \mid by^2$, und weil b quadratfrei ist, $p \mid y$, im Widerspruch zur Primitivität der Lösung.

Aus (2) folgt

$$ax^2 \equiv z^2 \bmod b.$$

Da x invertierbar modulo b ist, bedeutet dies, dass a ein Quadrat modulo b ist. Ebenso zeigt man, dass b ein Quadrat modulo a ist.

b) Seien jetzt umgekehrt die Bedingungen (i) und (ii) vorausgesetzt, d.h. es gebe ganze Zahlen u_0, v_0 mit

$$u_0^2 \equiv a \bmod b \quad \text{und} \quad v_0^2 \equiv b \bmod a.$$

Da a und b teilerfremd sind, gibt es ganze Zahlen λ, μ mit $\lambda a + \mu b = 1$. Wir setzen

$$u := \lambda a u_0 = u_0 - \mu b u_0, \qquad v := \mu b v_0 = v_0 - \lambda a v_0.$$

Damit ist

$$u \equiv u_0 \bmod b,\ u \equiv 0 \bmod a \quad \text{und} \quad v \equiv v_0 \bmod a,\ v \equiv 0 \bmod b,$$

also

$$u^2 \equiv a \bmod ab, \quad uv \equiv 0 \bmod ab, \quad v^2 \equiv b \bmod ab.$$

Mit ganzzahligen Variablen x, y gilt deshalb

$$(ux + vy)^2 \equiv (ax^2 + by^2) \bmod ab.$$

Es folgt

$$(3) \qquad (ux + vy - z)(ux + vy + z) \equiv (ax^2 + by^2 - z^2) \bmod ab.$$

Wir bestimmen jetzt eine "kleine" Lösung der Kongruenz

$$(4) \qquad ux + vy - z \equiv 0 \bmod ab.$$

Dazu betrachten wir die Menge

$$S := \{(x, y, z) \in \mathbb{Z}^3 : 0 \leqslant x < \sqrt{|b|},\ 0 \leqslant y < \sqrt{|a|},\ 0 \leqslant z < \sqrt{|ab|}\}.$$

Wir können annehmen, dass $a \neq 1$ und $b \neq 1$ (da für $a = 1$ oder $b = 1$ die Lösbarkeit von (2) trivial ist). Dann ist $|ab| > 1$ keine Quadratzahl, also $\sqrt{|ab|}$ keine ganze Zahl. Daraus folgt, dass S mehr als $|ab|$ Gitterpunkte enthält. Nach dem Dirichletschen Schubfachprinzip gibt es daher zwei verschiedene Vektoren $(x_i, y_i, z_i) \in S$ mit

$$ux_1 + vy_1 - z_1 \equiv ux_2 + vy_2 - z_2 \bmod ab.$$

Die Differenz $(x, y, z) := (x_1 - x_2, y_1 - y_2, z_1 - z_2) \neq (0, 0, 0)$ erfüllt dann (4) und es gilt

$$(5) \qquad |a|x^2 < |ab|, \quad |b|y^2 < |ab|, \quad z^2 < |ab|.$$

Aus (3) und (4) folgt jetzt

$$ax^2 + by^2 - z^2 \equiv 0 \bmod ab,$$

und wegen (5) ist

$$|ax^2 + by^2 - z^2| < 2|ab|.$$

Aufgrund der möglichen Vorzeichen von a und b überlegt man sich, dass nur die beiden Fälle

$$(6)_2^1 \qquad ax^2 + by^2 - z^2 = \begin{cases} 0 \\ ab \end{cases}$$

auftreten können. Im ersten Fall sind wir fertig. Im zweiten Fall schließen wir so weiter: Aus $(6)_2$ ergibt sich

(7) $$ax^2 - ab = a(x^2 - b) = z^2 - by^2.$$

Mit der Normfunktion

$$\mathbb{N}(s + t\sqrt{b}) := (s + t\sqrt{b})(s - t\sqrt{b}) = s^2 - bt^2$$

im Zahlring $\mathbb{Z}[\sqrt{b}]$ lässt sich (7) auch so schreiben:

$$a\mathbb{N}(x + \sqrt{b}) = \mathbb{N}(z + y\sqrt{b}).$$

Multipliziert man dies mit $x_1 := \mathbb{N}(x + \sqrt{b})$, so erhält man wegen der Multiplikativität der Norm

$$ax_1^2 = \mathbb{N}\left((z + y\sqrt{b})(x + \sqrt{b})\right) = \mathbb{N}\Big((zx + by) + (z + xy)\sqrt{b})\Big) = z_1^2 - by_1^2,$$

wobei $z_1 := zx + by$, $y_1 := z + xy$. Wir haben damit eine Lösung der Gleichung (2) gefunden, q.e.d.

Aus Satz 3 können wir nun das entscheidende Hilfsmittel zum Beweis des Drei-Quadrate-Satzes herleiten.

L.4. Lemma. *Sei n eine quadratfreie natürliche Zahl.*

a) *Falls $n \equiv 1 \bmod 4$ oder $n \equiv 2 \bmod 4$, gibt es eine Primzahl $p \equiv 1 \bmod 4$, so dass die Legendresche Gleichung*

(8) $$nx^2 - py^2 = z^2$$

lösbar ist.

b) *Falls $n \equiv 3 \bmod 8$, gibt es eine Primzahl $p \equiv 1 \bmod 4$, so dass die Legendresche Gleichung*

(9) $$nx^2 - 2py^2 = z^2$$

lösbar ist.

Beweis. Der Beweis benutzt den Dirichletschen Primzahlsatz: Sind k, m teilerfremde natürliche Zahlen, so gibt es unendlich viele Primzahlen p mit

$$p \equiv k \bmod m.$$

a1) Wir behandeln zuerst den Fall, dass $n \equiv 1 \bmod 4$.

Nach dem Dirichletschen Primzahlsatz gibt es eine Primzahl p mit

$$p \equiv 2n - 1 \bmod 4n$$

Damit ist $p \equiv 1 \bmod 4$ und p zu n teilerfremd. Nach Satz 3 ist deshalb nur noch zu zeigen:

(i) n ist ein Quadrat modulo p.
(ii) $-p$ ist ein Quadrat modulo n.

Zu (i) Da $p \equiv -1 \bmod n$, ist

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

Dabei wurde das quadratische Reziprozitätsgesetz benutzt.

Zu (ii) Da $-p \equiv 1 \equiv 1^2 \bmod n$, ist $-p$ ein trivialerweise ein Quadrat modulo n.

a2) Sei jetzt $n \equiv 2 \bmod 4$. Wir wählen eine Primzahl p mit

$$p \equiv n - 1 \bmod 4n$$

Wieder ist $p \equiv 1 \bmod 4$ und p zu n teilerfremd. Außerdem gilt $p \equiv -1 \bmod n$. Wir setzen $n = 2m$. Dann ist m ungerade. Es gilt

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

Wir unterscheiden jetzt zwei Fälle:
Falls $m \equiv 1 \bmod 4$, folgt $n \equiv 2 \bmod 8$, also $p \equiv 1 \bmod 8$. Dann ist $(\frac{-1}{m}) = 1$ und $(\frac{2}{p}) = 1$ (nach dem 2. Ergänzungssatz zum Reziprozitätsgesetz). Daraus folgt $(\frac{n}{p}) = 1$, d.h. die Bedingung (i) ist erfüllt.

Falls $m \equiv 3 \bmod 4$, folgt $n \equiv 6 \bmod 8$, also $p \equiv 5 \bmod 8$. Dann ist $(\frac{-1}{m}) = -1$ und $(\frac{2}{p}) = -1$, also $(\frac{n}{p}) = 1$, d.h. die Bedingung (i) ist ebenfalls erfüllt.

Wegen $-p \equiv 1 \bmod n$ ist $-p$ ein Quadrat modulo n. Nach Satz 3 ist deshalb (8) lösbar.

b) Falls $n \equiv 3 \bmod 8$, ist $n - 2$ zu $4n$ teilerfremd, es gibt deshalb eine Primzahl p mit

$$p \equiv n - 2 \bmod 4n.$$

Wieder ist $p \equiv 1 \bmod 4$ und p zu n teilerfremd. Es gilt

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

Daraus folgt: n ist Quadrat modulo p, also auch modulo $2p$.

Da $p \equiv -2 \bmod n$, folgt $-2p \equiv 4 \bmod n$, also ist $-2p$ ein Quadrat modulo n.

Daher ist nach Satz 3 die Gleichung (9) lösbar.

Beweis des Drei-Quadrate-Satzes

Es genügt, den Satz für quadratfreies n zu beweisen. Denn aus $n = mk^2$ mit einer ungeraden Zahl k folgt $n \equiv m \bmod 8$.

Sei also n eine natürliche Zahl mit $n \not\equiv 0, 4, 7 \bmod 8$.

Falls $n \equiv 1, 2, 5, 6 \bmod 8$, können wir nach Lemma 4 eine Primzahl $p \equiv 1 \bmod 4$ finden, so dass die Gleichung

$$nx^2 - py^2 = z^2$$

eine nicht-triviale ganzzahlige Lösung besitzt. Da $p \equiv 1 \bmod 4$, ist p Summe zweier Quadratzahlen, $p = u^2 + v^2$, $u, v \in \mathbb{Z}$. Es folgt

$$nx^2 = z^2 + (uy)^2 + (vy)^2.$$

Aus Satz 2 folgt nun, dass n Summe dreier Quadratzahlen ist.

Im verbleibenden Fall $n \equiv 3 \bmod 8$ gibt es nach Lemma 4 eine Primzahl $p \equiv 1 \bmod 4$, so dass die Gleichung

$$nx^2 - 2py^2 = z^2$$

eine nicht-triviale ganzzahlige Lösung besitzt. Auch $2p$ ist Summe zweier Quadratzahlen, denn aus $p = u^2 + v^2$ folgt $2p = (u + v)^2 + (u - v)^2$. Also kann man weiter wie oben schließen.

Damit ist der Drei-Quadrate-Satz bewiesen.

Übrigens ist der Vier-Quadrate-Satz von Lagrange eine einfache Folgerung aus dem Drei-Quadrate-Satz. Denn entweder ist eine natürliche Zahl n schon Summe von drei Quadraten oder von der Form $n = 4^k m$ mit $m \equiv 7 \bmod 8$. Dann ist aber $n - (2^k)^2 = 4^k(m - 1)$ Summe von drei Quadraten und deshalb n Summe von vier Quadraten.

Dreieckszahlen. Unter einer Dreieckszahl versteht man eine natürliche Zahl der Gestalt

$$\Delta_m := \sum_{k=1}^{m} k = \frac{m(m+1)}{2}.$$

L.5. Corollar. *Jede natürliche Zahl n ist Summe von drei Dreieckszahlen.*

Beweis. Die Zahl $N := 8n + 3$ ist nach Satz 1 Summe von drei Quadratzahlen, die notwendig alle ungerade sind:

$$N = 8n + 3 = \sum_{i=1}^{3} (2m_i + 1)^2 = \sum_{i=1}^{3} (4m_i^2 + 4m_i + 1) = 8 \sum_{i=1}^{3} \frac{m_i(m_i+1)}{2} + 3,$$

also

$$n = \Delta_{m_1} + \Delta_{m_2} + \Delta_{m_3}, \qquad \text{q.e.d.}$$