§ 6. Die Primfaktorzerlegung

(6.1) Der HAUPTSATZ der elementaren Zahlentheorie

Jede natürliche Zahl $n \geq 2$ läßt sich als ein Produkt von endlich vielen Primzahlen darstellen.

Diese Produktdarstellung ist eindeutig bis auf die Reihenfolge der Faktoren.

(6.2) KOROLLAR: Jede natürliche Zahl $n \geq 2$ läßt sich auf genau eine Weise darstellen in der Form

$$(\star) \qquad n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} = \prod_{i=1}^{r} p_i^{k_i}$$

mit $r \in \mathbb{N}$, $p_i \in \mathbb{P}$ und $k_i \in \mathbb{N}$ für alle $i = 1, 2, \ldots, r$ und $p_1 < p_2 < \ldots < p_r$.

$(\star)$ heißt die **kanonische PFZ von** n .

(6.3) BEM: **a)** Für $n \in \mathbb{N}$ bezeichne

$$T_{\mathbb{P}}(n) := T(n) \cap \mathbb{P}$$

die **Menge aller Primteiler von** n .

b) Besitzt $n \in \mathbb{N}$ die kanonische PFZ $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$, so gilt

$$T_{\mathbb{P}}(n) = \{p_1, p_2, \ldots, p_r\} .$$

c) In manchen Fällen ist es günstiger, auch den Exponenten 0 in der PFZ einer Zahl zuzulassen:

$$25 = 2^0 \cdot 5^2 \cdot 7^0$$

Dies ist aber nicht mehr die kanonische PFZ von 25 , da $2 \nmid 25$ und $7 \nmid 25$.

Die positiven Teiler einer natürlichen Zahl

Beispiel: Die positiven Teiler von $72 = 2^3 \cdot 3^2$

k	l	$2^k \cdot 3^l$	t
0	0	$2^0 \cdot 3^0$	1
1	0	$2^1 \cdot 3^0$	2
2	0	$2^2 \cdot 3^0$	4
3	0	$2^3 \cdot 3^0$	8
0	1	$2^0 \cdot 3^1$	3
1	1	$2^1 \cdot 3^1$	6
2	1	$2^2 \cdot 3^1$	12
3	1	$2^3 \cdot 3^1$	24
0	2	$2^0 \cdot 3^2$	9
1	2	$2^1 \cdot 3^2$	18
2	2	$2^2 \cdot 3^2$	36
3	2	$2^3 \cdot 3^2$	72

(6.4) SATZ: Besitzt die natürliche Zahl $n \in \mathbb{N}$ eine Darstellung der Form

$$n \;=\; p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$$

mit paarweise verschiedenen Primzahlen $p_1, p_2, \ldots, p_s$ und Exponenten $k_i \geq 0$, so sind für $t \in \mathbb{N}$ folgende Aussagen quivalent:

a) $t \,|\, n$

b) Es gibt Zahlen $l_i \in \mathbb{N}_0$ mit $0 \leq l_i \leq k_i$ für alle $i = 1, 2, \ldots, s$ und

$$t \;=\; p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_s^{l_s}$$

(6.5) KOROLLAR: Besitzt die natürliche Zahl $n \in \mathbb{N}$ eine Darstellung der Form

$$n \;=\; \prod_{i=1}^{s} p_i^{k_i}$$

mit paarweise verschiedenen Primzahlen $p_1, p_2, \ldots, p_s$ und Exponenten $k_i \geq 0$, so gilt

$$\tau(n) \;=\; \prod_{i=1}^{s} (k_i + 1)$$

BEM: Die Anzahl der Teiler einer natürlichen Zahl n hängt nicht von der Größe dieser Zahl ab, sondern von der Häufigkeit der Primteiler. So haben z.B. die Zahlen

$$72 = 2^3 \cdot 3^2 \quad \text{und} \quad 1\,048\,929\,872\,381 \;=\; 101^3 \cdot 1009^2 \quad \text{(13 Stellen)}$$

diegleiche Anzahl positiver Teiler, nämlich 12 .

(6.6) SATZ: Für die **Teileranzahlfunktion** $\tau : \mathbb{N} \longrightarrow \mathbb{N}$ gilt:

a) $\tau(1) = 1$ **b)** $\tau(p^k) = k + 1$ für alle $p \in \mathbb{P}, k \in \mathbb{N}$

c) Für teilerfremde natürliche Zahlen m und n gilt $\tau(m \cdot n) \;=\; \tau(m) \cdot \tau(n)$. (Diese Bedingung bedeutet, daß τ **multiplikativ** ist.)

BEM: Durch die drei Eigenschaften aus (6.6) ist die Teileranzahlfunktion τ vollständig bestimmt.

Berechnungsmethode für ggT und kgV

(6.7) SATZ: Seien $m, n \in \mathbb{N}$. Dann gibt es paarweise verschiedene Primzahlen $p_1, p_2, \ldots, p_t$ und Zahlen $k_1, k_2, \ldots, k_t, l_1, l_2, \ldots, l_t \in \mathbb{N}_0$ mit folgenden Eigenschaften:

a) $m \;=\; \prod_{i=1}^{t} p_i^{k_i} \quad , \quad n \;=\; \prod_{i=1}^{t} p_i^{l_i}$

b) $\operatorname{ggT}(m, n) \;=\; \prod_{i=1}^{t} p_i^{\min(k_i, l_i)}$ **c)** $\operatorname{kgV}(m, n) \;=\; \prod_{i=1}^{t} p_i^{\max(k_i, l_i)}$

(6.8) KOROLLAR: Für alle $m, n \in \mathbb{N}$ gilt $\mathrm{ggT}(m,n) \cdot \mathrm{kgV}(m,n) = m \cdot n$.

Berechnung der PFZ einer natürlichen Zahl

Problem 1 : Wie läßt sich die PFZ einer natürlichen Zahl $n \geq 2$ bestimmen ?

Problem 2 : Wie kann man einen nichttrivialen Teiler einer ungeraden Zahl $n \geq 3$ finden ?

(6.9) Methode der sukzessiven Divisionen

Sei $n \geq 3$ eine ungerade natürliche Zahl. $(u_k)_{k \in \mathbb{N}}$ sei eine streng monoton wachsende Folge ungerader natürlicher Zahlen ≥ 3, die alle ungeraden Primzahlen enthält. Teile n der Reihe nach durch alle Zahlen $u_1, u_2, u_3, \ldots$, die $\leq \lfloor\sqrt{n}\rfloor$ sind. Man findet dann entweder einen echten Teiler von n oder stellt fest, daß n eine Primzahl ist.

(6.10) BEM: **a)** Beispiele für die Folge $(u_k)_{k \in \mathbb{N}}$ findet man in (5.25).

b) Diese Methode ist günstig, wenn n kleine Teiler besitzt, wird aber sehr aufwendig,wenn n Teiler bei $\lfloor\sqrt{n}\rfloor$ besitzt, oder sogar prim ist. Um Teiler in der Nähe von $\lfloor\sqrt{n}\rfloor$ zu finden, kann man u.U. das **Verfahren von Fermat** anwenden, das auf dem folgenden Satz basiert:

(6.11) SATZ: Sei $n \in \mathbb{N}$ eine ungerade Zahl. Ferner seien

$$T := \{\, (a,b) \mid a,b \in \mathbb{N}\,,\ n = a \cdot b\,,\ a \geq b > 0 \,\} \quad , \quad D := \{\, (x,y) \mid x,y \in \mathbb{N}_0\,,\ n = x^2 - y^2 \,\}\,.$$

Dann ist die Abbildung $f : T \longrightarrow D\,,\ (a,b) \longmapsto \left(\dfrac{a+b}{2}\,, \dfrac{a-b}{2}\right)$ bijektiv.

(6.12) Das Verfahren von Fermat:

Sei $n \geq 3$ eine ungerade natürliche Zahl.

Setze $x := \lfloor\sqrt{n}\rfloor$

Teste, ob $x^2 - n$ Quadrat einer natürlichen Zahl y

Wenn ja, gilt $n = x^2 - y^2 = (x+y) \cdot (x-y)$, und es ist ein Teiler von n gefunden.

Wenn nein, setze das Verfahren mit $x := \lfloor\sqrt{n}\rfloor + 1$ fort, usw.

Brich das Verfahren ab, wenn $x^2 - n$ eine Qudratzahl ist.

Beispiel: Finde einen Teiler von $n = 200\,819$:

x	$x^2 - n$	Quadratzahl	Grund
$\lfloor\sqrt{n}\rfloor = 448$	-115	nein	$-115 \notin \mathbb{N}_0$
$\lfloor\sqrt{n}\rfloor + 1 = 449$	782	nein	$27^2 = 729$ und $28^2 = 784$
$\lfloor\sqrt{n}\rfloor + 2 = 450$	$1\,681$	ja	$1\,681 = 41^2$

Mit $y := 41$ gilt also $x^2 - n = y^2$, und damit

$$n \;=\; x^2 - y^2 \;=\; (x+y) \cdot (x-y) \;=\; (450+41) \cdot (450-41) \;=\; 491 \cdot 409$$

Da 409 und 491 Primzahlen sind, hat man sogar schon die PFZ von n gefunden, insbesondere ist n keine Primzahl.

Die Euler'sche φ–Funktion

(6.13) DEF: Für $n \in \mathbb{N}$ bezeichne $\boldsymbol{\varphi(n)}$ die Anzahl der Zahlen aus $\{1, 2, 3, \ldots, n\}$, die zu n teilerfremd sind.
Die Funktion $\boldsymbol{\varphi : \mathbb{N} \longrightarrow \mathbb{N}\,,\ n \longmapsto \varphi(n)}$, heißt **Euler'sche Funktion**.

(6.14) BEM: **a)** Für $n \in \mathbb{N}$ bezeichne R'_n die Menge

$$R'_n := \{\, l \mid l \in \mathbb{N}, 1 \le l \le n, \mathrm{ggT}(l, n) = 1 \,\}$$

der Zahlen aus $\{1, 2, 3, \ldots, n\}$, die zu n teilerfremd sind. Damit gilt $\varphi(n) = |R'_n|$.

b) $\varphi(1) = 1$.

c) Für eine Primzahl p gilt $\varphi(p) = p - 1$.

(6.15) SATZ: Für $p \in \mathbb{P}$ und $k \in \mathbb{N}$ gilt $\varphi(p^k) = p^k - p^{k-1}$.

(6.16) SATZ: Für <u>teilerfremde</u> natürliche Zahlen m und n gilt:

a) $R'_{mn} \;=\; \{\, (lm + kn) \bmod (mn) \mid l \in R'_n\,,\ k \in R'_m \,\}$

b) $\varphi(m \cdot n) \;=\; \varphi(m) \cdot \varphi(n)$, d.h. φ ist **multiplikativ**.

(6.17) KOROLLAR: Sind $m_1, m_2, \ldots, m_r$ $(r \ge 2)$ paarweise teilerfremde natürliche Zahlen, so gilt

$$\varphi(m_1 \cdot m_2 \cdot \ldots \cdot m_r) \;=\; \varphi(m_1) \cdot \varphi(m_2) \cdot \ldots \cdot \varphi(m_r)$$

(6.18) SATZ: Die natürliche Zahl $n \ge 2$ besitze die kanonische Primfaktorzerlegung

$$n \;=\; \prod_{i=1}^{r} p_i^{k_i}\,.$$

Dann gilt **a)** $\displaystyle \varphi(n) \;=\; \prod_{i=1}^{r} \left(p_i^{k_i} - p_i^{k_i - 1}\right)$ **b)** $\displaystyle \varphi(n) \;=\; n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

(6.19) BEM: **a)** $\displaystyle \varphi(n) \;=\; n \cdot \prod_{p \in T_{\mathbb{P}}(n)} \left(1 - \frac{1}{p}\right)$

b) Die φ–Funktion besitzt entsprechende Eigenschaften wie die Teilerfunktion τ (vgl. (6.6)).

c) Sei $n = 43\,560$. Berechne $\varphi(n)$:

Bestimme die Primfaktorzerlegung: $n = 2^3 \cdot 3^2 \cdot 5 \cdot 11^2$. Wende (6.18) an:

$\varphi(n) \;=\; (2^3 - 2^2)(3^2 - 3)(5 - 1)(11^2 - 11) \;=\; 4 \cdot 6 \cdot 4 \cdot 110 \;=\; 10\,560$.

oder

$\varphi(n) \;=\; n \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{11}\right) \;=\; n \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{10}{11} \;=\; n \cdot \frac{8}{33} \;=\; 10\,560$