(9.23) DEF: Eine natürliche Zahl p heißt **Primzahl**, wenn gilt:

i) $p \geq 2$ **ii)** 1 und p sind die einzigen positiven Teiler von p.
Es bezeichne $\mathbb{P}$ die Menge aller Primzahlen.

$1 \notin \mathbb{P}$, $4 \notin \mathbb{P}$, $6 \notin \mathbb{P}$, $\{2,3,5,7,11,13,17,19,23,29,31\} \subseteq \mathbb{P}$
2 ist die einzige gerade Primzahl.

(9.24) SATZ: **Eindeutige Primfaktorzerlegung**

Jede natürliche Zahl $n \geq 2$ läßt sich als Produkt von Primzahlen darstellen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.

Beweis: s. (6.8) Beispiel: $24 = 2 \cdot 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2 \cdot 2 = 2 \cdot 2 \cdot 2 \cdot 3$

(9.25) FOLG: Zu jeder natürlichen Zahl $n \geq 2$ gibt es eindeutig bestimmte Primzahlen $p_1, \ldots, p_r$ ($r \in \mathbb{N}$) und natürliche Zahlen $k_1, \ldots, k_r \in \mathbb{N}$ mit $p_1 < p_2 < \ldots < p_r$ und

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$$

Dies ist die sog. **kanonische Primfaktorzerlegung von** n.

$72 = 2^3 \cdot 3^2$

(9.26) FOLG: Sei $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ die kanonische Primfaktorzerlegung der natürlichen Zahl $n \geq 2$. Eine Zahl $t \in \mathbb{N}$ ist genau dann ein Teiler von n, wenn es Zahlen $l_1, \ldots, l_r \in \mathbb{N}_0$ gibt mit $0 \leq l_i \leq k_i$ für alle $i = 1, \ldots, r$ gibt und

$$t = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_r^{l_r}$$

Bezeichnet $\tau(n)$ die Anzahl der positiven Teiler von n, so gilt

$$\tau(n) = (k_1 + 1) \cdot (k_2 + 1) \cdot \ldots \cdot (k_r + 1).$$

Beispiel: $\tau(72) = \tau(2^3 \cdot 3^2) = (3+1) \cdot (2+1) = 12$

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

(9.27) FOLG: **a)** Jede natürliche Zahl $n \geq 2$ besitzt mindestens einen Primteiler.

b) Teilt eine Primzahl p ein Produkt zweier natürlicher Zahlen, so teilt p mindestens eine dieser Zahlen.

(9.28) SATZ: $p_1, \ldots, p_r$ seien paarweise verschiedene Primzahlen, und es gelte $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ und $n = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_r^{l_r}$ mit $k_i, l_i \in \mathbb{N}_0$. Dann gilt:

a) $\mathrm{ggT}(m,n) = p_1^{\min(k_1,l_1)} \cdot \ldots \cdot p_r^{\min(k_r,l_r)}$

b) $\mathrm{kgV}(m,n) = p_1^{\max(k_1,l_1)} \cdot \ldots \cdot p_r^{\max(k_r,l_r)}$

c) $\mathrm{ggT}(m,n) \cdot \mathrm{kgV}(m,n) \; = \; m \cdot n$

Beispiel: ggT$(72, 20)$=?

$$\begin{aligned} 72 &= 2^3 \cdot 3^2 &&= 2^3 \cdot 3^2 \cdot 5^0 \\ 20 &= 2^2 \cdot 5 &&= 2^2 \cdot 3^0 \cdot 5^1 \end{aligned}$$

$$\begin{aligned} \mathrm{ggT}(72,20) &= 2^{\min(3,2)} \cdot 3^{\min(2,0)} \cdot 5^{\min(0,1)} = 2^2 \cdot 3^0 \cdot 5^0 = 4 \\ \mathrm{kgV}(72,20) &= 2^{\max(3,2)} \cdot 3^{\max(2,0)} \cdot 5^{\max(0,1)} = 2^3 \cdot 3^2 \cdot 5^1 = 360 \end{aligned}$$

$\mathrm{ggT}(72,20) \cdot \mathrm{kgV}(72,20) = 4 \cdot 360 = 1440 = 72 \cdot 20$

(9.29) SATZ: **(Euklid , ca. 300 v.Chr.)** Es gibt unendlich viele Primzahlen.

Verteilung der Primzahlen

Die Verteilung der Primzahlen innerhalb der natürlichen Zahlen ist völlig regellos. Zwischen je zwei aufeinanderfolgenden ungeraden Primzahlen liegt mindestens eine gerade Zahl, es gibt aber aufeinanderfolgende Primzahlen mit dem Abstand 2: $(3,5), (5,7), (11,13), (17,19), (29,31)$. Solche Paare nennt man **Primzahlzwillinge**. Im Gegensatz zu (9.29) ist bis heute unbekannt, ob es unendlich viele Primzahlzwillinge gibt. Es sind Primzahlzwillinge mit mehr als 18 000 Dezimalstellen bekannt.

Der Abstand zwischen zwei aufeinanderfolgenden Primzahlen kann aber auch beliebig groß werden: Zu jeder natürlichen Zahl n gibt es stets n aufeinanderfolgende zusammengesetzte Zahlen (also Nicht–Primzahlen):

$$(n+1)! + 2 \; , \; (n+1)! + 2 \; , \; (n+1)! + 4 \, , \ldots , \; (n+1)! + n \; , \; (n+1)! + (n+1)$$

Für $x \in \mathbb{R}$ bezeichne $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Der **Primzahlsatz** besagt:

$$\pi(x) \;\sim\; \frac{x}{\ln(x)}$$

Dabei bedeutet $\sim$ asymptotische Annäherung, d.h. immer besser werdende Übereinstimmung bei immer größer werdendem x.

Dieser Primzahlsatz wurde 1792 von Carl Friedrich Gauß vermutet und erst mehr als 100 Jahre später von Hadamard und de la Valleé–Poussin 1896 bewiesen.