

Setze $\tilde{m} = nq - \hat{m}^1$ $\tilde{n} = mq - \hat{n}^1$

$\Rightarrow m(\hat{m} + \tilde{m}) = m \cdot n \cdot q = n(\hat{n} + \tilde{n})$

Definition: $m, n \in \mathbb{N}$ heißen teilerfremd, wenn gilt $(m, n) = 1$.

Dann gibt es $\tilde{m}, \tilde{n}$ mit $m \cdot \tilde{m} - n \cdot \tilde{n} = 1$

Satz: $m, n \in \mathbb{N}$, $m_d = m : (m, n)$, $n_d = n : (m, n)$
 $\Rightarrow m_d, n_d$ teilerfremd.

Satz: $k \mid m \cdot n$, k, m teilerfremd $\Rightarrow k \mid n$

Beweis: k, m teilerfremd $\Rightarrow$ Wir finden $\tilde{k}, \tilde{m}$ mit $k\tilde{k} - m\tilde{m} = 1$
 $\Rightarrow n \cdot k \cdot \tilde{k} - n \cdot m \cdot \tilde{m} = n$
 $k \mid n \cdot k \cdot \tilde{k}$ $k \mid n \cdot m \cdot \tilde{m}$ $\Rightarrow k \mid n$

Vielfachenmenge von $n \in \mathbb{N}$: $V_n = \{v \in \mathbb{N} : n \mid v\}$

7.11.05

$m, n \in \mathbb{N}$ $V_m \cap V_n \ni m \cdot n \Rightarrow V_m \cap V_n \neq \emptyset$
 $\Rightarrow \exists v_* = \text{kgV}(m, n) = \min(V_m \cap V_n)$

Satz: $k, m, n \in \mathbb{N}$, $k \in V_m \cap V_n \Rightarrow v_* = \text{kgV}(m, n) \mid k$

Beweis durch Widerspruch:

Annahme:

O.B.d.A $k \neq v_* \Rightarrow v_* < k$

$v_* \nmid k$ Division mit Rest $k = v_* \cdot q + r$, $r < v_*$

$m \mid k$, $m \mid v_* \cdot q \Rightarrow m \mid r \Rightarrow r \in V_m$

$n \mid k$, $n \mid v_* \cdot q \Rightarrow n \mid r \Rightarrow r \in V_n$

$\Rightarrow r \in V_m \cap V_n \Rightarrow v_* \leq r$ $\nmid$ Widerspruch

Folgerung:

$m, n \in \mathbb{N} \Rightarrow V_m \cap V_n = V_{\text{kgV}(m, n)}$

Satz:

$$m, n \in \mathbb{N} \quad \tilde{m} = m : d, \quad \tilde{n} = n : d$$

$$\Rightarrow v_* = \text{kgV}(m, n) = d \cdot \tilde{m} \cdot \tilde{n}$$

Beweis:

$$d|m, m/v_* \Rightarrow d|v_* \text{ setze } \tilde{v} = v_* : d, m_1 = v_* : m$$

$$n_1 = v_* : n; \quad v_* = d \cdot \tilde{v} = m \cdot m_1 = d \cdot \tilde{m} \cdot m_1$$

$$\Rightarrow \tilde{v} = \tilde{m} \cdot m_1, v_* = d \cdot \tilde{v} = m \cdot n_1 = d \cdot \tilde{n} \cdot n_1$$

$$\Rightarrow \tilde{v} = \tilde{n} \cdot n_1$$

$$\Rightarrow \left. \begin{array}{l} \tilde{m} / \tilde{v}, \tilde{n} / \tilde{v} \\ \tilde{m}, \tilde{n} \text{ teilerfremd} \end{array} \right\} \Rightarrow \tilde{m} \cdot \tilde{n} / \tilde{v} \text{ setze } v_1 = \tilde{v} : (\tilde{m} \cdot \tilde{n})$$

$$v_* = d \cdot \tilde{v} = d \cdot \tilde{m} \cdot \tilde{n} \cdot v_1 \Rightarrow d \cdot \tilde{m} \cdot \tilde{n} / v_* \Rightarrow d \cdot \tilde{m} \cdot \tilde{n} \leq v_*$$

$$\left. \begin{array}{l} d \cdot \tilde{m} \cdot \tilde{n} = m \cdot \tilde{n} \in V_m \\ d \cdot \tilde{m} \cdot \tilde{n} = n \cdot \tilde{m} \in V_n \end{array} \right\} \Rightarrow d \cdot \tilde{m} \cdot \tilde{n} \in V_m \cap V_n$$

$$\Rightarrow d \cdot \tilde{m} \cdot \tilde{n} = v_*$$

Folgerung:

$$m, n \in \mathbb{N} \quad \Rightarrow \text{ggT}(m, n) \cdot \text{kgV}(m, n) = m \cdot n$$

Potenzen (zu Basis $m \in \mathbb{N}$)

definiert:

$$\begin{array}{ccc} 1 & \mathbb{N} & \xleftarrow{s} \mathbb{N} \\ \downarrow & \uparrow m & \downarrow m \\ m & \mathbb{N} & \xleftarrow{m \cdot} \mathbb{N} \end{array} \quad m_n^{\uparrow} = m^n$$

Grundgleichungen der Rekursion: $m^1 = m, \quad m^{s(n)} = m^{n+1} = m^n \cdot m$

$$\uparrow \mathbb{N} : \mathbb{N} \rightarrow \mathbb{N}(m, n) \rightarrow m^n$$

Die Potenzierung $\uparrow$ ist im allgemeinen weder kommutativ noch assoziativ

$$8 = 2^3 \neq 3^2 = 9$$

Catalan-Vermutung: 8 und 9 sind beiden einzigen aufeinanderfolgenden Potenzen.

Fermat-Vermutung:

Die Gleichung $x^n + y^n = z^n$ hat natürliche Zahlen n, x, y, z als Lösungen nur für $n=2$
 $3^2 + 4^2 = 5^2$ Andrew Wiles

$$729 = 9^3 = (3^2)^3 \neq 3^{(2^3)} = 3^8 = 6561$$

Ausnahmen:

$$2^4 = 16 = 4^2$$

$$(2^2)^2 = 4^2 = 16 = 2^4 = 2^{(2^2)}$$

Potenzgesetze:

$$1^n = 1$$

$$*) (m^n) \cdot (m^p) = m^{n+p}$$

$$(m^n)^p = m^{n \cdot p}$$

$$(m \cdot n)^p = m^p \cdot n^p$$

Beweis von (*) durch Induktion nach p

$$\text{J.A. } (m^n) \cdot (m^1) = (m^n) \cdot m = m^{n+1}$$

$$\begin{aligned} \text{J.S. } (m^n) \cdot (m^{s(p)}) &= (m^n) \cdot (m^{p+1}) = (m^n) \cdot (m^p) \cdot m \\ &\stackrel{\text{J.V.}}{=} m^{n+p} \cdot m = m^{n+p+1} = m^{n+s(p)} \end{aligned}$$

Konvention:

Potenz bindet stärker als Produkt:

$$m^{n+1} = m^n + m, \quad m^n \cdot m^p = m^{n+p}$$

Monotonieigenschaften der Potenzierung:

$$k < m \iff k^n < m^n$$

$$n \leq p \implies m^n \leq m^p$$

$$m > 1 \quad n < p \iff m^n < m^p$$

Beweis als Übungsaufgabe (Blatt 3)

Erste Zahlenbereichserweiterung

Satz:

Jede kommutative Halbgruppe mit Kürzungsregel lässt sich durch Hinzunahme genau eines Elements zu einem kommutativen Monoid mit Kürzungsregel ergänzen.

Beweis am Beispiel $(\mathbb{N}, +)$:

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} \quad 0 \notin \mathbb{N}$$

$$n \in \mathbb{N}_0 \quad 0 + n = n + 0 = n \quad (\text{Kommutativität})$$

$$(0 + n) + m = n + m = 0 + (n + m) \quad (\text{Assoziativität})$$

$$m + n = m + p \Rightarrow n = p \quad (\text{Kürzungsregel})$$

$$0 + n = 0 + p \Rightarrow n = p$$

$$m + 0 = m + p \Rightarrow m = m + p \Rightarrow p = 0$$

Fortsetzung der Multiplikation auf $\mathbb{N}_0$ (bei Erhaltung des Distributivgesetzes)

$$0 \cdot n + 0 \cdot n = (0 + 0) \cdot n = 0 \cdot n = 0 \cdot n + 0 \xRightarrow[\text{Regel}]{\text{Kürz.}} 0 \cdot n = 0$$

$$\text{assoziativ: } (0 \cdot m) \cdot n = 0 \cdot n = 0 = 0 \cdot (m \cdot n) \dots$$

$$1 \text{ neutral: } 1 \cdot 0 = 0 = 0 \cdot 1$$

Kürzungsregel gilt nicht mehr!

$$\text{Anordnung: } m < n \iff \exists d \in \mathbb{N} : m + d = n \quad \text{auch } \mathbb{N}_0$$

$$\Rightarrow 0 < n \quad \text{für alle } n \in \mathbb{N} \quad n - 0 = n$$

$$m \leq n \iff \exists d \in \mathbb{N}_0 : m + d = n$$

Monotonie der Addition gilt weiter:

$$m < n \Rightarrow k + m < k + n$$

$$m < n \Rightarrow m \cdot k \leq n \cdot k$$

Teilbarkeit:

$0 \cdot m = 0$ für alle $m \Rightarrow m \mid 0$ für alle m $0 \cdot m = 0$
 $m \cdot 0 = n$ nur lösbar für $n=0$, dann aber nicht
eindeutig $\Rightarrow n:0$ nicht definiert.

Potenzierung unter Erhaltung von $(*)$

$$m^{n+p} = m^n \cdot m^p$$

$$p=0: m^n \cdot 1 = m^n = m^{n+0} = m^n \cdot m^0$$

führt zu $m^0 = 1$ für alle $m \in \mathbb{N}$.

$$0^1 = 0, \quad 0^{n+1} = 0^n \cdot 0 = 0 \quad 0^n = 0 \text{ für alle } n \in \mathbb{N}$$

$\Rightarrow$ Konvention: $0^0 = 1$

Division mit Rest: $\mathbb{N}_0 \times \mathbb{N} \rightarrow \mathbb{N}_0 \times \mathbb{N}_0: (n, m) \mapsto (q, r)$

$$n = m \cdot q + r$$

$$m \mid n: r = 0$$

$$m > n: q = 0$$

$$m = n: q = 1, r = 0$$