1.37 Satz: $x \sim y \Leftrightarrow x \mid y$ ist Ordnungsrelation auf $\mathbb{N}$.

Bew Übung.

1.38 Hilfssatz: Seien $k, l, n, m \in \mathbb{Z}$, und $d \in \mathbb{N}$. Dann

$d \mid n \wedge d \mid m \Rightarrow d \mid (k \cdot n + l \cdot m)$

Bew $d \mid n \wedge d \mid m \overset{\text{def}}{\Leftrightarrow} \exists k_1, k_2 \in \mathbb{Z}: n = k_1 d \wedge m = k_2 d$

Weiter gilt

$k \cdot n + l \cdot m = k k_1 d + l k_2 d = \underbrace{(k k_1 + l k_2)}_{\in \mathbb{Z}} d$. □

1.39 Teilen mit Rest (ohne Beweis)

Seien $n, m \in \mathbb{N}$ mit $n \leq m$. Dann

$\exists! q \in \mathbb{N}, r \in \mathbb{N}_0: m = qn + r \wedge 0 \leq r \leq n-1$

1.40 Satz: 1.39 erfüllt den ggT

Sei also $n = qm + r$ wie oben, dann gilt

$ggT(n,m) = ggT(m,r)$.

Bew Idee Zeige $D(n) \cap D(m) = D(m) \cap D(r)$

"$\subseteq$" Sei $d \in D(n) \cap D(m) \Rightarrow r = n - qm$ ist teilb. durch d

$\overset{\text{def}}{\Rightarrow} d \in D(r)$

$\Rightarrow d \in D(m) \cap D(r)$

"$\supseteq$" $d \in D(m) \cap D(r) \to d \mid n$

$\Rightarrow d \in D(n) \cap D(m)$

□

Bsp $m = 30, n = 24 \overset{1.39}{\Rightarrow} m = 1 \cdot 24 + 6$, $m = q \cdot n + r$

Also $ggT(30,24) = ggT(24,6) = 6$.

1.41 Euklidischer Algorithmus

Seien $n, m \in \mathbb{N}$, $n < m$, dann

$\exists!\ k, q_1, q_2, \dots, q_{k+1} \in \mathbb{N}$

$r_1, \dots, r_k \in \mathbb{N}_0$:

$m = q_1 n + r_1 \quad 0 \le r_1 \le n-1$

$n = q_2 r_1 + r_2 \quad 0 \le r_2 \le r_1 - 1$

$r_1 = q_3 r_2 + r_3 \quad 0 \le r_3 \le r_2 - 1$ } (*)

$\vdots$

$r_{k-2} = q_k \cdot r_{k-1} + r_k \quad 0 \le r_k \le r_{k-1} - 1$

$r_{k-1} = q_{k+1} \cdot r_k + 0$

und es gilt $ggT(n,m) = r_k$

Bew 1) Eindeutigkeit und Existenz der q_j, r_j folgt aus 1.3.9

2) Wegen (*) ist

$0 \le r_1 \le n-1$

$0 \le r_2 \le r_1 - 1 \le n-1-1 = n-2$

$0 \le r_3 \le r_2 - 1 \le n-2-1 = n-3$

$\vdots$

und das Verfahren bricht nach höchstens n Schritten ab.

3) Nach Satz 1.40 ist

$ggT(n,m) = ggT(n,r_1) = ggT(r_1,r_2)$

$= \dots = ggT(r_{k-1},r_k) = r_k.$ □

2) $ggT(132,11) = 11$ $\quad 132 = 12 \cdot 11 + 0$

Bsp 1) $ggT(210,25) = 5$

$210 = 8 \cdot 25 + 10$

$25 = 2 \cdot 10 + 5$

$10 = 2 \cdot 5$

Drei Folgerungen aus dem E.A.

1.43 Hilfssatz:

Seien $k,m,n \in \mathbb{N}$, dann gilt

$ggT(k \cdot m, k \cdot n) = k \cdot ggT(m,n)$

Beu

$km = k q_1 n + k r_1$

$kn = k q_2 r_1 + k r_2$

$\vdots$

$k r_{k-1} = k q_{k+1} r_k + 0$

E.A. ↓ $ggT(km,kn) = k r_k$

$= k \cdot ggT(m,n)$ □

1.44 Folgerung.

Seien $k,m,n \in \mathbb{N}$, dann

$$k \mid m \wedge k \mid n \Rightarrow k \mid ggT(m,n)$$

Bew $k \mid m \wedge k \mid n \overset{def}{\iff} \exists u,v \in \mathbb{Z}: uk = m \wedge vk = n$

$\Rightarrow ggT(m,n) = ggT(uk, vk) \overset{1.43}{=} k \cdot ggT(u,v)$

$\Rightarrow k \mid ggT(m,n)$ $\square$ ($ggT(u,v) \in \mathbb{N}$)

1.45 Satz.

Seien $n,m \in \mathbb{N}$ fest und $M(n,m) = \{xn + xm : x,y \in \mathbb{Z}\}$.

Dann gilt $M(n,m) = \{z \cdot ggT(m,n) : z \in \mathbb{Z}\} = ggT(n,m)\mathbb{Z}$

Bew "$\subseteq$" Zeige: $\exists z \in \mathbb{Z}: mx + ny = z \, ggT(n,m)$

Da $ggT(n,m) \mid m \wedge ggT(n,m) \mid n$ folgt mit 1.38

$$ggT(n,m) \mid (xm + ny) \overset{def}{\iff} \exists z \in \mathbb{Z}: z\,ggT(n,m) = xm + yn.$$

"$\supseteq$" Es genügt $ggT(n,m) \overset{(*)}{\in} M(n,m)$ zu zeigen, durch Skalierung folgt dann die Beh.

Für $l_1, l_2 \in \mathbb{Z}$ ist

$$k_1, k_2 \in M(n,m) \overset{def}{\iff} k_1 = x_1 n + y_1 m \wedge k_2 = x_2 n + y_2 m \quad \left(\begin{matrix} x_1, x_2, y_1, y_2 \\ \in \mathbb{Z} \end{matrix}\right)$$

$$\Rightarrow l_1 k_1 + l_2 k_2 = l_1(x_1 n + y_1 m) + l_2(x_2 n + y_2 m) \in$$

$\in$ $n\underbrace{(l_1x_1+l_2x_2)}_{=:x\in\mathbb{Z}}+m\underbrace{(l_1y_1+l_2y_2)}_{=:y\in\mathbb{Z}}=nx+my\in M(n,m)$ (4)

(*) EA. $m=q_1n+r_1 \Rightarrow r_1=m-q_1n \overset{(1)}{\in} M(n,m)$

$n=q_2r_1+r_2 \Rightarrow r_2=n-q_2r_1 \overset{(2)}{\in} M(n,m)$

$\vdots$

$r_{k-2}=q_kr_{k-1}+0 \overset{(1)}{\Rightarrow} r_k=r_{k-2}-q_kr_{k-1}\overset{(4)}{\in} M(n,m)$

$\|$ ggT(n,m) $\lightning$

1.7 Primzahlen

1.46 Def: Eine Zahl $p\in\mathbb{N}$ heißt Primzahl, falls $D(p)=\{p,1\}$.

1.47 Eukl. Hilfssatz:
Sei p prim und $m,n\in\mathbb{N}$, dann gilt
$p\mid(m\cdot n) \Rightarrow p\mid m \vee p\mid n$

Bew: Fall 1 $p\mid m$ $\rightsquigarrow$ fertig

Fall 2 $\neg(p\mid m)$:

Aus $p\mid m\cdot n \wedge p\mid np$ folgt

$p\mid ggT(mn,np)=n\cdot\underbrace{ggT(m,p)}_{=1,\text{ da } p \text{ prim}}=n$

$\Rightarrow p\mid n$ $\square$

Anmerkung Induktiv lässt sich damit zeigen, dass

$p \mid (n_1 \cdot \ldots \cdot n_k) \Rightarrow \exists_{j \in \{1,\ldots,k\}} \; p \mid n_j$.

1.48 **Fundamentalsatz der Arithmetik**

Sei $n \geq 2$. Dann lässt sich n als (bis auf Reihenfolge) eindeutiges Produkt aus Primzahlen darstellen,

$n \geq 2 \Rightarrow \exists\, p_1, \ldots, p_k \text{ prim} : \; n = \prod_{j=1}^{k} p_j$

Bew Zeige, dass jede Zahl in der Menge $M = \{2, \ldots, n\}$ die Auss. erfüllen

(IA) $n = 2 \Rightarrow n = p_1 = 2$ wahr.

(IS) **Fall 1** $n+1$ ist prim $\rightsquigarrow$ fertig

Fall 2 $n+1$ nicht prim

$\Rightarrow \exists\, d \in D(n+1) \setminus \{n+1\} \neq \{1\}$ ($n+1 \to$ prim)

$\Rightarrow \exists\, k \in \mathbb{N} : \; n+1 = k \cdot d$ mit $k, d \in M$

(IV) $\Rightarrow \exists\, \hat{p}_1, \dots, \hat{p}_j, \check{p}_1, \dots, \check{p}_i$ prim :

$$n+1 = k \cdot d = \underbrace{\left(\prod_{\ell=1}^{j} \hat{p}_\ell\right)}_{k \in M} \underbrace{\left(\prod_{q=1}^{i} \check{p}_q\right)}_{d \in M}$$

Dann ist $q_1 \in P$, denn sonst

$$q_1 \Big| \left(\prod_{j=1}^{n} p_j\right) \Rightarrow q_1 \Big| \left(m - \prod_{j=1}^{n} p_j\right) \Leftrightarrow q_1 \Big| 1 \quad \lightning$$

□

1.49 Satz: Es gibt unendl. viele Primzahlen.

Bew Gegenannahme: Angenommen es ex. nur endl. viele Primzahlen

$$P = \{p_1, \dots, p_n\}.$$

Dann lässt sich

$$m = 1 + \prod_{j=1}^{n} p_j \overset{1.48}{=} \prod_{j=1}^{k} q_j$$

1.50 Satz

$$\pi(n) := \#\{p \text{ prim} \mid p \le n\},$$

dann $\lim\limits_{n \to \infty} \dfrac{\pi(n)}{\frac{n}{\log n}} = 1 \quad \left(\pi(n) \sim \dfrac{n}{\log n}\right)$