16. Vorlesung 17.11.2020

Notiztitel 17.11.2020

Aus der 15. Vorlesung

- $b \in \mathbb{Z}$, Teilermenge von b: $\tilde{T}(b) = \{a \in \mathbb{Z} \mid b = k \cdot a \text{ für ein } k \in \mathbb{Z}\}$
- $a \in \tilde{T}(b) \Rightarrow -a \in \tilde{T}(b)$ ← „Symmetrie" der Teilermenge $\tilde{T}(b)$
- Für alle $a \in \tilde{T}(b)$ gilt: $-|b| \leq a \leq |b| \Rightarrow \tilde{T}(b)$ ist eine endliche Menge.
- $\tilde{T}(b) = \tilde{T}(-b)$ denn: $b = k \cdot a \Rightarrow -b = (-k) \cdot a$

→ es reicht aus bei Fragen zur Teilbarkeit in $\mathbb{Z}$ die positiven Zahlen zu betrachten also Teilbarkeit in $\mathbb{N}$ zu diskutieren!

$$T(b) = \{a \in \mathbb{N} \mid b = k \cdot a\} \subseteq \mathbb{N}$$

↑ $b \in \mathbb{N}$

$p \in \mathbb{N}$ ist Primzahl $\Leftrightarrow T(p) = \{1, p\}$

Gegeben $a, b \in \mathbb{N}$: $T(a,b) = T(a) \cap T(b)$

↑ Menge der gemeinsamen Teiler von a und b

$T(a,b)$ ist eine endliche Menge, da $T(a)$ und $T(b)$ endliche Mengen sind. In einer endlichen Menge von Zahlen gibt es immer ein größtes (maximales) Element.

Definition:

Der größte gemeinsame Teiler $ggT(a,b)$ ist definiert als

$$ggT(a,b) = \max\{x \mid x \in T(a,b)\}$$

Zur Berechnung des ggT dient der euklidische Algorithmus basierend auf (ganzzahliger) Division mit Rest.

Gegeben sind $a, b \in \mathbb{Z}$, $a \neq 0$, dann existieren $k \in \mathbb{Z}$ und $r \in \mathbb{N}_0$ mit $b = k \cdot a + r$; $0 \leq r < |a|$. r ist der Rest beim (ganzzahligen) Dividieren von b durch a!

Euklidischer Algorithmus als Anwendung des Satzes über Division mit Rest:

Für $a, b \in \mathbb{Z}$ mit $b = k \cdot a + r$ nach Division mit Rest gilt: $\underline{ggT(a,b) = ggT(a,r)}$

zum Beweis zeigen wir, dass die Teilermengen $T(a,b)$ und $T(a,r)$ gleich sind, dann sind auch die größten Elemente dieser Mengen gleich!

$t \in T(a,b) \Rightarrow t \mid a \wedge t \mid b \Rightarrow a = n \cdot t,\ b = \tilde{n} \cdot t$ für $n, \tilde{n} \in \mathbb{Z}$.

Mit $b = k \cdot a + r$ folgt $r = b - k \cdot a = \tilde{n} \cdot t - k \cdot n \cdot t = \underbrace{(\tilde{n} - k \cdot n)}_{\in \mathbb{Z}} \cdot t$

$\Rightarrow t \mid r \wedge t \mid a \Rightarrow t \in T(a,r)$

$\rightarrow$ damit: $T(a,b) \subseteq T(a,r)$

$t \in T(a,r) \Rightarrow t \mid a \wedge t \mid r \Rightarrow a = m \cdot t \wedge r = \tilde{m} \cdot t$ für $m, \tilde{m} \in \mathbb{Z}$.

Mit $b = k \cdot a + r$ folgt $b = k \cdot m \cdot t + \tilde{m} \cdot t = \underbrace{(k \cdot m + \tilde{m})}_{\in \mathbb{Z}} \cdot t$

$\Rightarrow t \mid b \wedge t \mid a \Rightarrow t \in T(a,b)$

$\rightarrow$ damit: $T(a,r) \subseteq T(a,b)$

insgesamt: $T(a,r) = T(a,b)$

Gesucht $ggT(a,b)$, dann: Führe Division mit Rest aus

$a \leq b$

$$b = k \cdot a + r$$

$$\Rightarrow \boxed{ggT(a,b) = ggT(a,r)}$$

und wiederhole diesen Schritt bis $r = 0$ ist; der letzte von 0 verschiedene Rest in der Schrittfolge ist der gesuchte $ggT(a,b)$!

Beispiel: 1) $ggT(426,54)$

$426 = \overbrace{7\cdot 54}^{378} + 48$ ← $ggT(426,54) = ggT(54,48)$

$54 = 1\cdot 48 + 6$ ← $ggT(54,48) = ggT(48,6)$

$48 = 8\cdot 6 + 0$ ← Rest $r=0$ Algorithmus endet

(letzter von 0 verschiedener Rest:) $6 = ggT(426,54)$

2) $ggT(1312,251)$

$1312 = \overbrace{5\cdot 251}^{1255} + 57$ ← $ggT(1312,251) = ggT(251,57)$

$251 = \overbrace{4\cdot 57}^{228} + 23$ ← $ggT(251,57) = ggT(57,23)$

$57 = \overbrace{2\cdot 23}^{46} + 11$ ← $ggT(57,23) = ggT(23,11)$

$23 = 2\cdot 11 + 1$ ← $ggT(23,11) = ggT(11,1)$

$11 = 11\cdot 1 + 0$ ← Rest $r=0$ Algorithmus endet

(letzter von 0 verschiedener Rest) $1 = ggT(1312,251)$

Definition: Zwei Zahlen $a,b \in \mathbb{Z}$ heißen teilerfremd, falls gilt $ggT(a,b) = 1$, d.h. $T(a,b) = \{1\}$

Beispiel: 1312 und 251 sind teilerfremd!

Beweis zum Teilen mit Rest

Gegeben sind $a,b \in \mathbb{Z}$, $a \neq 0$, dann existieren $k \in \mathbb{Z}$ und $r \in \mathbb{N}_0$ mit $b = k\cdot a + r$; $0 \leq r < |a|$. r ist der Rest beim (ganzzahligen) Dividieren von b durch a!

1) Wegen $T(b) = T(-b)$ reicht es aus, den Satz für $a,b \in \mathbb{N}$ zu beweisen!

2) Es reicht aus $a < b$ anzunehmen, denn für $a = b$ hat man $b = 1\cdot b + 0 = 1\cdot a + 0 = k\cdot a + r$ mit $k=1$, $r=0<a$ ($b = a$)

3) Es reicht aus $a \geq 2$ zu betrachten, denn

für $a = 1$ gilt $b = b \cdot 1 + 0 = b \cdot a + 0 = k \cdot a + r$ mit $k = b, r = 0 < a = 1$

($a = 1$)

4) Zu beweisen bleibt: Für $a, b \in \mathbb{N}$ mit $b \geq a \geq 2$ gilt:

Es existieren $k, r \in \mathbb{N}_0$ mit $b = k \cdot a + r$, $0 \leq r < a$

Beweis durch vollständige Induktion bezogen auf $b \in \mathbb{N}$

Induktionsanfang $b = 2$: $2 = 1 \cdot 2 + 0$

($a = 2$, $r = 0$, $0 \leq r < a$)

Induktionsschritt:

Induktionsvoraussetzung: Aussage ist wahr für $b = u$ also

$u = k \cdot a + r$ für ein $k \in \mathbb{N}$, $0 \leq r < a$

Induktionsbehauptung: Aussage ist auch wahr für $u+1$ also

$u + 1 = \tilde{k} \cdot a + \tilde{r}$ für ein $\tilde{k} \in \mathbb{N}$, $0 \leq \tilde{r} < a$

Beweis: $u + 1 = (k \cdot a + r) + 1$, $k \in \mathbb{N}$, $0 \leq r < a$

(Induktionsvor.)

$r < a$, $r \in \mathbb{N}$, $a \in \mathbb{N}$ also $r \leq a - 1$

$= k \cdot a + (r + 1)$

1. Fall: $r + 1 < a \Rightarrow \tilde{k} = k$, $\tilde{r} = r + 1$: $u + 1 = \tilde{k} \cdot a + \tilde{r}$ mit $\tilde{k} \in \mathbb{Z}$, $0 \leq \tilde{r} < a$

2. Fall $r + 1 = a \Rightarrow u + 1 = k \cdot a + \underbrace{(r+1)}_{a}$

$= k \cdot a + a$

$= \underbrace{(k+1)}_{\tilde{k}} \cdot a = \tilde{k} \cdot a + \tilde{r}$ mit $\tilde{k} = k + 1$ und $\tilde{r} = 0$

($0 \leq \tilde{r} < a$)

Beispiel: $ggT(125, 13) = 1$ denn 13 ist Primzahl also $T(13) = \{1, 13\}$ und $13 \nmid 125$

Der euklidische Algorithmus liefert

$125 = \overbrace{9 \cdot 13}^{117} + 8$

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$ggT(125, 13) = 1$ letzter von 0 verschiedener Rest

$2 = 2 \cdot 1 + 0$ ← Rest 0, Algorithmus endet

„Umkehrung ≙ Rückwärtsrechnung" in diesem Algorithmus

$$1 = ggT(125,13) = 3 - 1 \cdot 2$$
$$= 3 - 1 \cdot (5 - 1 \cdot 3) = (-1) \cdot 5 + 2 \cdot 3$$
$$= (-1) \cdot 5 + 2 \cdot (8 - 1 \cdot 5) = 2 \cdot 8 - 3 \cdot 5$$
$$= 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8) = (-3) \cdot 13 + 5 \cdot 8$$
$$= (-3) \cdot 13 + 5 \cdot (125 - 9 \cdot 13)$$
$$= \underbrace{5}_{s} \cdot 125 \underbrace{- 48}_{t} \cdot 13 = s \cdot 125 + t \cdot 13$$

d.h. es gibt $s \in \mathbb{Z}$ (hier $s = 5$) und $t \in \mathbb{Z}$ (hier $t = -48$) mit
$ggT(125,13) = s \cdot 125 + t \cdot 13$

Lemma von Bézout:

Gegeben sind $a, b \in \mathbb{Z}$; dann existieren Zahlen $s, t \in \mathbb{Z}$ mit

$$ggT(a,b) = s \cdot a + t \cdot b$$

Beweisidee: euklidischen Algorithmus „umkehren ≙ rückwärts rechnen"
mathematisch exakt ist Beweis mit vollständiger Induktion (siehe Skript)

Beispiel: $ggT(378, 45)$

$$378 = \underbrace{8 \cdot 45}_{360} + 18$$
$$45 = \underbrace{2 \cdot 18}_{36} + 9$$
$$18 = 2 \cdot 9 + 0$$

$\Rightarrow ggT(378,45) = 9$

$$9 = 45 - 2 \cdot 18$$
$$= 45 - 2 \cdot (378 - 8 \cdot 45)$$
$$= (-2) \cdot 378 + 17 \cdot 45 = s \cdot 378 + t \cdot 45 \text{ mit } s = -2 \text{ und } t = 17.$$