Zahlentheorie ggT, kgV, erweiterter Euklidischer Algorithmus

Prof. Dr. Dörte Haftendorn, www.uni-lueneburg.de/mathe-lehramt Mai 05

Definitionen:

Teilermenge $T_n = \textit{Menge der Teiler von } n = \{t \mid \exists\, k \in N \;\; mit \;\; t \cdot k = n\}$

Vielfachenmenge $V_n = \{v \mid \exists\, k \in N \;\; mit \;\; k \cdot n = v\}$

Größter gemeinsamer Teiler $ggT(a,b) = \max\left(T_a \cap T_b\right)$ englisch gcd(a,b)

Kleinstes gemeinsames Vielfaches $kgV(a,b) = \min\left(V_a \cap V_b\right)$ =lcm(a,b)

Ist ggT(a,b)=1, dann sagt man “a ist teilerfremd zu b” oder “a ist relativ prim zu b”.

TI: gcd(45,63) oder ggte(45,63) ergibt {9,3,-2,}

Algorithmen zur Bestimmung des ggT:

Wechselwegnahme

$45 \mid 63$ $45 \mid 18$ $27 \mid 18$ $9 \mid 18$	ggT(45,63)=? Man schreibt die beiden Zahlen in eine Tabelle und zieht solange immer die kleinere von der größeren ab, bis die kleinere die größere teilt. Dann ist diese letzte kleinere Zahl der ggT. ggT(45,63)=9	$15 \mid 22$ $15 \mid 7$ $8 \mid 7$ $1 \mid 7$	Das klappt, weil jeder gemeinsame Teiler jede Differenz teilt.

Dass man dabei nicht auf einen kleineren gemeinsamen Teiler kommen kann, merkt man, wenn man weiter abzieht.

Euklidischer Algorithmus

$63 = 1 \cdot 45 + 18$ $45 = 2 \cdot 18 + \boxed{9}$ $18 = 2 \cdot 9 + 0$ $ggT(63,45) = 9$	$220 = 2 \cdot 75 + 70$ $75 = 1 \cdot 70 + \boxed{5}$ $70 = 12 \cdot 5 + 0$ $ggT(220,75) = 5$	ggT(a,b)=? Sei a>b. Man teilt a durch b mit Rest r_1. Man teilt b durch r_1 mit Rest r_2. Man teilt r_1 durch r_2 mit Rest r_3. und so fort.... bis ein Rest 0 ist. Der vorige Rest ist dann der ggT(a,b).

Ersichtlich ist der Euklidische Algorithmus eine Abkürzung der Wechselweg-nahme. Gemeinsame Teiler werden auf die Reste “durchgereicht”.

Erweiterter Euklidischer Algorithmus zur Erzeugung der **Vielfachsummendarstellung** des ggT, d.h.

$\exists s,t \in Z \;\; mit \;\; ggT(a,b) = s \cdot \boxed{a} + t \cdot \boxed{b}$, **Linearkombination** von a und b

$ggT(63,45) = 9$ $9 = 45 - 2 \cdot 18$ $9 = 45 - 2 \cdot (63 - 1 \cdot 45)$ $\boxed{9} = -2 \cdot \boxed{63} + 3 \cdot \boxed{45}$	Man verfolgt die Zeilen des Euklidischen Algorithmus termmäßig ohne auszurechnen rückwärts. Günstig ist es, stets den größeren Rest links zu schreiben. Ersichtlich entstehen so die gesuchten Linearfaktoren s und t. Die Existenz dieser Darstellung heißt auch “Lemma von Bezoût”.