

Proseminar Theoretische Informatik
Elmar Eder, Universität Salzburg
Blatt 1, Aufgaben für 10.3.2021

Aufgabe 1 Zeigen Sie, dass der euklidische Algorithmus zur Berechnung von $\text{ggT}(a, b)$ korrekt ist, d.h. für alle natürlichen Zahlen (also nichtnegativen ganzen Zahlen) a und b nach endlich vielen Schritten ein Ergebnis liefert und dass dieses Ergebnis tatsächlich der größte gemeinsame Teiler von a und b ist.

Bemerkung: In der Mathematik definiert man den größten gemeinsamen Teiler von 0 und 0 als 0. In der Teilbarkeitstheorie verwendet man das Wort “größter” nicht im Sinne von “am größten bezüglich der $<$ -Relation”, sondern im Sinne von “am größten bezüglich der Teilbarkeitsrelation” (da ist 0 die “größte” natürliche Zahl). Für den größten gemeinsamen Teiler von a und b kommt das aber auf dasselbe hinaus, eben außer wenn a und b beide Null sind.

Hinweise zur Lösung:

- Zum Beweis der Terminierung, also dass der Algorithmus tatsächlich nach endlich vielen Schritten stoppt, können Sie entweder das *Prinzip der starken Induktion* oder die *Wohlordnungseigenschaft der Menge der natürlichen Zahlen* benutzen.
- Zum Beweis, dass das vom Algorithmus gelieferte Ergebnis tatsächlich der größte gemeinsame Teiler von a und b ist, können Sie eine *Schleifeninvariante* definieren.

Starke Induktion Sei P eine Eigenschaft von natürlichen Zahlen derart, dass immer wenn $P(x)$ für alle $x < y$ gilt, dann auch $P(y)$ gilt. Dann gilt $P(x)$ für alle natürlichen Zahlen.

Wohlordnungseigenschaft Jede nichtleere Menge von natürlichen Zahlen hat ein kleinstes Element.

Schleifeninvariante ist eine Größe, deren Wert sich beim Durchlaufen einer Schleife eines Computerprogramms nicht verändert.

Aufgabe 2 Schätzen Sie ungefähr ab, wieviele Schritte der euklidische Algorithmus im schlimmsten Fall braucht, wenn er mit zwei Eingabezahlen a und b aufgerufen wird, und wieviel Zeit und Speicherplatz der Computer dafür braucht!