

9. Übungsblatt

Ausgabe: 19.06.18**Abgabe:** 19.06.18

9.1 Größer gemeinsamer Teiler

Eine Zahl $a \in \mathbb{Z}$ teilt eine Zahl $b \in \mathbb{Z}$, geschrieben $a \mid b$, genau dann wenn es ein $r \in \mathbb{Z}$ gibt so dass $r \cdot a = b$.

Gegeben zwei Zahlen $x, y \in \mathbb{Z}$, dann ist der *größte gemeinsame Teiler* von x und y , geschrieben $\gcd(x, y)$, die Zahl $z \in \mathbb{Z}$, so dass z sowohl x als auch y teilt und für jede Zahl $u \in \mathbb{Z}$, die x und y teilt, gilt, dass $u \leq z$.

Für den größten gemeinsamen Teiler gelten folgende Gleichungen:

$$\gcd(a, a) = a \quad (1)$$

$$0 < a, 0 < b, a \leq b \implies \gcd(a, b) = \gcd(b - a, a) \quad (2)$$

$$0 < a, 0 < b, b \leq a \implies \gcd(a, b) = \gcd(b, a - b) \quad (3)$$

$$\gcd(a, b) = \gcd(b, a) \quad (4)$$

Folgendes C0-Programm soll den größten gemeinsamen Teiler berechnen:

```
1  int ggt(int a, int b)
2  /** pre ?
3     post ?
4  */
5  {
6      while (1) /** inv ? */ {
7          if (a == b) {
8              return a;
9          }
10         else
11             {}
12         /** { ? } */
13         if (a <= b) {
14             b = b - a;
15         }
16         else {
17             a = a - b;
18         }
19     }
20 }
```

- (i) Formalisieren Sie die Korrektheit, indem Sie die Vorbedingung ggf. ergänzen und eine Nachbedingung formulieren.
- (ii) Finden Sie eine Invariante.
- (iii) Beweisen Sie die Korrektheit, indem Sie die Verifikationsbedingungen mit der schwächste Vorbedingung berechnen.

Hinweise:

- 1. In Zeile 12 können Sie gegenfalls eine Zusicherung einfügen, die den Beweis vereinfacht.
- 2. Die Invariante ist denkbar einfach: der größte gemeinsame Teiler von a und b bleibt immer gleich.