

9. Übungsblatt

Ausgabe: 14.06.18**Abgabe:** 21.06.18

9.1 Größer gemeinsamer Teiler: die Formalisierung

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:

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

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

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

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

Formalisieren Sie die Definition von $\gcd$ in Prädikatenlogik. Sie brauchen die Gleichungen *nicht* zu beweisen, benötigen sie aber in der nächsten Aufgabe.

9.2 Größer gemeinsamer Teiler: die Berechnung

Folgendes C0-Programm soll den größten gemeinsamen Teiler berechnen:

```
1 // {0 ≤ a, 0 ≤ b}
2 while (b != a) /** inv ? */ {
3     if (a <= b) {
4         b = b - a;
5     }
6     else {
7         a = a - b;
8     }
9 }
```

- (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 stärksten Nachbedingung berechnen. Dabei ist es hilfreich, diese direkt nach der Generierung soweit wie möglich zu vereinfachen, bevor damit weitergerechnet wird.

Hinweise:

- 1. Grob gesprochen ist die Spezifikation: a (oder b) ist der größte gemeinsame Teiler von dem ursprünglichen Wert von a und b .
- 2. Zu Beweis und Vereinfachung benötigen Sie möglicherweise die Gleichungen (1)- (4) oben.
- 3. Die Invariante ist denkbar einfach: der größte gemeinsame Teiler von a und b bleibt immer gleich.