

# 7. Übungsblatt

**Ausgabe:** 10.06.21

**Abgabe:** 15.06.21 10:00

Dieses Übungsblatt ist ein PDF-Formular. Bitte in einem PDF-Viewer Ihrer Wahl ausfüllen, abspeichern und in Ihrem Gitlab-Abgabe-Repository committen. Alternativ können Sie die Lösungen in der Markdown-Datei `uebung-XX.md` eintragen und diese committen.

Gruppe:

Name:

Matrikelnummer:

Name:

Matrikelnummer:

Name:

Matrikelnummer:

## 7.1 Größter Gemeinsamer Teiler

Dieses Programm berechnet den größten gemeinsamen Teiler (ggT) zweier ganzer Zahlen:

```
1 // {0 < a ∧ 0 < b ∧ a = A ∧ b = B}
2 while (b != 0) /** inv ??? */
3 {
4     if (a <= b) {
5         b = b - a;
6     }
7     else {
8         a = a - b;
9     }
10 }
11 // {a = ggT(A, B)}
```

(1) Was ist die Invariante?

*Hinweis:* Betrachten Sie dazu den ggT von  $a$  und  $b$ , und den ggT von  $A$  und  $B$ .

(2) Berechnen Sie ausgehend von der Invariante die vereinfachten Verifikationsbedingungen, und damit einhergehend die schwächsten Vorbedingungen, wie in der Vorlesung eingehend vorgestellt. Es kann dabei sinnvoll sein, explizite Zusicherungen einzufügen.

Programm mit den annotierten schwächsten Vorbedingungen:

Vereinfachte Verifikationsbedingungen:

(3) Beweisen Sie alle vereinfachten Verifikationsbedingungen, die nicht trivial bewiesen werden:

Dabei können Sie auf folgende Eigenschaften des ggT zurückgreifen:

$$\begin{aligned}\forall x y. 0 < y \leq x &\implies \text{ggT}(x, y) = \text{ggT}(x - y, y) \\ \forall x y. \text{ggT}(x, y) &= \text{ggT}(y, x) \\ \forall x. \text{ggT}(x, 0) &= x\end{aligned}$$

**Änderungen:**

- *Version 1.1* Erste Eigenschaft des ggT berichtigt,  $y \leq x$  statt  $y < x$  in der Vorbedingung.