Erweiterter Euklid'scher Algorithmus

1 Die Problemstellung

Wir wollen den Erweiterten Euklid'schen Algorithmus *für ganze Zahlen* betrachten. Die Problembeschreibung dafür lautet:

> Gegeben: a, b
> sodass: $a, b \in \mathbb{Z}$.
> Gesucht: d, x, y
> sodass: $d \in \mathbb{N} \wedge x, y \in \mathbb{Z} \wedge \text{ist-ggT}[d, a, b] \wedge d = a\,x + b\,y$.

Bekanntlich beruht die Lösung dieser Problemstellung auf der Zurückführung des Problems auf ein einfacheres Problem, nämlich auf jenes mit natürlichen Zahlen als Eingabe, d.h.

> Gegeben: a, b
> sodass: $a, b \in \mathbb{N}$.
> Gesucht: d, x, y
> sodass: $d \in \mathbb{N} \wedge x, y \in \mathbb{Z} \wedge \text{ist-ggT}[d, a, b] \wedge d = a\,x + b\,y$.

In den Algorithmischen Methoden haben wir gelernt (siehe Skriptum), dass die Korrektheit der Reduktion durch Transformation durch mathematisches Wissen der Form

$$\textbf{wenn}\ \overline{P}_{\text{pre}[x],y}\ \textbf{dann}\ P_{x,\text{post}[y]} \tag{1}$$

bewiesen werden kann. Dazu aus dem Skriptum Algorithmische Methoden:

- Wir schreiben $P_{x,y}$ für ein Problem mit Eingabegrößen x und Ausgabegrößen y, d.h. wenn x die Eingabebedingung des Problems P erfüllt, dann erfüllen x und y die Ausgabebedingung des Problems P, d.h. y ist eine Lösung des Problems P mit Eingabegrößen x.

2 Aufgabe

- Wie lauten “pre” und “post” in diesem konkreten Beispiel.
- Wie lautet Formel (1) in diesem konkreten Beispiel. Achten Sie auf korrekte Formulierung in der Prädikatenlogik und darauf, dass alle notwendigen Quantoren gesetzt sind.
- Beweisen Sie Formel (1) für dieses konkrete Beispiel. Achten Sie darauf, welches mathematische Zusatzwissen Sie im Beweis verwenden und führen Sie es entsprechend an.
- Schreiben Sie einen Technical Report zu diesem Thema.