Opgave 39 Variationer over Euklid

Betragt algoritmen Udvidet Euklid fra afsnit 6.4.1 i [H&S].

a) Vis, at algoritmen også er korrekt såfremt løkkens krop erstattes af

$$
\begin{array}{l}
\textsf{if } p > q \textsf{ then} \\
\qquad S^{\text{then}}; \\
\qquad p \leftarrow p - x * q; \quad s \leftarrow s + x * t \\
\textsf{else} \\
\qquad S^{\text{else}}; \\
\qquad q \leftarrow q - x * p; \quad t \leftarrow t + x * s
\end{array}
$$

– hvor x er en hjælpevariabel, og S^{then} og S^{else} ikke ændrer på p og q, men tilfredsstiller bevisbyrderne

$$\{0 < q < p\} S^{\text{then}} \{0 < x * q < p\} \qquad \{0 < p < q\} S^{\text{else}} \{0 < x * p < q\}.$$

b) En vigtig sætning i talteorien siger, at der for vilkårlige positive heltal m og n findes ikke-negative heltal a og b, således at $\text{sfd}(m,n) = am - bn$. Skriv en version af Euklids algoritme, der givet m og n beregner a og b. Følgende skitse til en algoritme kan være nyttig.

Algoritme: Euklid(m,n)
Inputbetingelse : $m, n \geq 0$
Outputkrav : $\text{sfd}(m,n) = am - bn$
Metode :

$$
\begin{array}{l}
S^{\text{init}}; \\
\{I\}\textsf{while } p \neq q \textsf{ do} \\
\qquad \textsf{if } p > q \textsf{ then} \\
\qquad\qquad S^{\text{then}} \\
\qquad \textsf{else} \\
\qquad\qquad S^{\text{else}}
\end{array}
$$

– hvor I er udsagnet

$$(\text{sfd}(p,q) = \text{sfd}(m,n)) \wedge (p = am - bn) \wedge (q = cn - dm) \wedge (p,q \geq 1) \wedge (a,b,c,d \geq 0).$$