Opgave 39 Betragt den udvidede Euklids algoritme i afsnit 2.4.1 i noten om transitionssystemer.

a) Vis, at algoritmen også er korrekt såfremt "indmaden" erstattes af

if $m > n$ **then**
  $\mathrm{S}^{\mathrm{then}}$;
  $m \leftarrow m - x * n;\ p \leftarrow p + x * q$
else
  $\mathrm{S}^{\mathrm{else}}$;
  $n \leftarrow n - x * m;\ q \leftarrow q + x * p$

hvor x er en hjælpevariabel og $\mathrm{S}^{\mathrm{then}}$ og $\mathrm{S}^{\mathrm{else}}$ tilfredsstiller bevisbyrderne

$$[0 < n < m]\mathrm{S}^{\mathrm{then}}[0 < x * n < m]$$

$$[0 < m < n]\mathrm{S}^{\mathrm{else}}[0 < x * m < n]$$

b) En vigtig sætning i talteorien siger, at der for vilkårlige positive heltal m og n findes ikke-negative tal a og b, således at $\mathrm{sfd}(m,n) = a * m - b * n$. 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: sfd(m,n) $= a * m - b * n$
Metode: S^{init}
  $\{(sfd(p,q) = sfd(m,n)) \wedge$
  $(p = a * m - b * n) \wedge (q = c * n - d * m) \wedge$
  $(p,q \geq 1) \wedge (a,b,c,d \geq 0)\}$
  while $p \neq q$ **do**
    if $p > q$ **then**
      S^{then}
    else
      S^{else}