Opgave 14 — ExtendedEuclid

Betragt algoritmen ExtendedEuclid i afsnit 2.4.1 i [HS].

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

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

- hvor x er en hjælpevariabel, og $\mathcal{S}^{\text{then}}$ og $\mathcal{S}^{\text{else}}$ ikke ændrer på n, m, p og q, men tilfredsstiller bevisbyrderne

$$\{0 < n < m\}\mathcal{S}^{\text{then}}\{0 < x * n < m\}$$

$$\{0 < m < n\}\mathcal{S}^{\text{else}}\{0 < x * m < n\}\ .$$

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 den største fælles divisor $\text{sfd}(m, n) = a * m - b * n$. 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 : $m, n \geq 1$
Outputkrav : $\text{sfd}(m, n) = a * m - b * n$
Metode : $\mathcal{S}^{\text{init}}$;
    $\{I\}$**while** $p \neq q$ **do**
        if $p > q$ **then**
            $\mathcal{S}^{\text{then}}$
        else
            $\mathcal{S}^{\text{else}}$

– hvor I er udsagnet

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