Feladat: Határozzuk meg az x és az y természetes számok legnagyobb közös osztóját!

Specifikáció:
$A = \underset{x}{\mathbb{N}} \times \underset{y}{\mathbb{N}} \times \underset{a}{\mathbb{N}} \times \underset{b}{\mathbb{N}}$
$B = \underset{x'}{\mathbb{N}} \times \underset{y'}{\mathbb{N}}$
$Q = (x = x' \wedge y = y')$
$R = (Q \wedge a = b = \text{lnko}(x,y))$

A specifikációból kiolvasható, hogy az eredményt az állapottér két változója (a és b) is szolgáltatja.

Megoldás:
Most keressük meg a specifikációnak megfelelő megoldó programot! A megoldást úgy sejtjük, hogy egy ciklussal találhatjuk meg. Nos, mi legyen ennek a ciklusnak az invariánsa?

$P = (Q \wedge a \in [1..x] \wedge b \in [1..y] \wedge \text{lnko}(a,b) = \text{lnko}(x,y))$

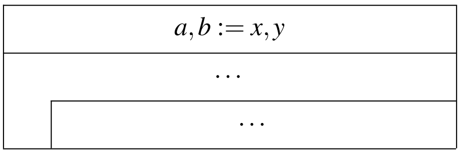
Ellenőrízzük le a ciklus feltételeit:
1. $\boxed{Q \Rightarrow P}$

Jól láthatóan nem teljesül, sőt fordítva igaz. Ezért megpróbálunk egy olyan közbülső állapotot felírni, ami a Q-ból könnyedén (egy értékadással) elérhető és ugyanakkor ez a kívánt feltétel teljesül rá. Amennyiben ez sikerül, akkor már csak egy szekvencia közbülső feltételeként kell pillantani erre az új Q' feltételre és máris felírható lesz a kívánt program egy értékadás és egy ciklus szekvenciájaként.

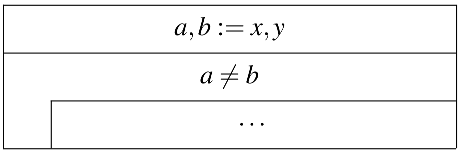
$Q' = (Q \wedge a = x \wedge b = y)$

Látható, hogy $Q' \Rightarrow P$ és $Q \Rightarrow \text{lf}(a,b := x,y,Q') = (Q \wedge x = x \wedge y = y) = Q\surd$.

Tehát a program valahogy így néz ki:

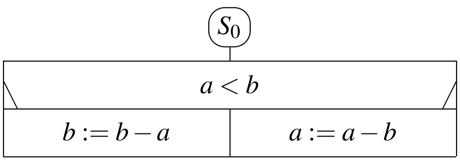


2. $\boxed{P \wedge \neg\pi \Rightarrow R}$
Ez a feltétel kezünkbe adja a ciklusfeltételt, hiszen P és R összehosonlításából $\neg\pi$-re $a = b$ adódik (hiszen az $a = b = lnko(a,b)$ csak így teljesülhet). Tehát $\pi = (a \neq b)$.



3. $\boxed{P \wedge \pi \Rightarrow t > 0}$
Jelen esetben ez: $Q \wedge a \in [1..x] \wedge b \in [1..y] \wedge \text{lnko}(a,b) = \text{lnko}(x,y) \Rightarrow t > 0$. Tehát $t := a+b$ egy megfelelő terminálófüggvény.

5. $\boxed{P \wedge \pi \wedge t = t_0 \Rightarrow \text{lf}(S_0, t < t_0)}$
Ellenőrízzük, hogy a következő program biztosítja ezt a tulajdonságot:



5/1. $\boxed{P \wedge \pi \wedge t = t_0 \Rightarrow \left(\bigvee_{i=1}^{n} \pi_i\right)}$ Ez nyilván teljesül (sőt az is igaz, hogy a teljes állapotteret leírjuk).

5/2. $\boxed{\forall i \in [1..n] : P \wedge \pi \wedge t = t_0 \wedge \pi_i \Rightarrow \mathrm{lf}(S_i, t < t_0)}$

1. $a < b$: $P \wedge \pi \wedge a + b = t_0 \overset{?}{\Rightarrow} \mathrm{lf}(b := b - a, t < t_0) = a + b - a = b < t_0 \surd$(hiszen $a > 0$)
2. $a \geq b$: $P \wedge \pi \wedge a + b = t_0 \overset{?}{\Rightarrow} \mathrm{lf}(a := a - b, t < t_0) = a - b + b = a < t_0 \surd$(hiszen $b > 0$)

4. $\boxed{P \wedge \pi \Rightarrow \mathrm{lf}(S_0, P)}$

A mi esetünkben:
$(Q \wedge a \in [1..x] \wedge b \in [1..y] \wedge \mathrm{lnko}(a,b) = \mathrm{lnko}(x,y) \wedge a \neq b) \overset{?}{\Rightarrow} \mathrm{lf}(S_0, P)$

4/1. $\boxed{P \wedge \pi \Rightarrow \left(\bigvee_{i=1}^{n} \pi_i\right)}$ Ez nyilván teljesül (sőt az is igaz, hogy a teljes állapotteret leírjuk).

4/2. $\boxed{\forall i \in [1..n] : P \wedge \pi \wedge \pi_i \Rightarrow \mathrm{lf}(S_i, P)}$

1. $a < b$: $P \wedge \pi \wedge a < b \overset{?}{\Rightarrow} \mathrm{lf}(b := b - a, P)$
   $(Q \wedge a \in [1..x] \wedge b \in [1..y] \wedge \mathrm{lnko}(a,b) = \mathrm{lnko}(x,y) \wedge a < b)$
   $\overset{?}{\Rightarrow}$
   $\mathrm{lf}(b := b - a, P) = (Q \wedge a \in [1..x] \wedge b - a \in [1..y] \wedge \mathrm{lnko}(a, b - a) = \mathrm{lnko}(x,y)) \surd$
2. $a \geq b$: $P \wedge \pi \wedge a > b \overset{?}{\Rightarrow} \mathrm{lf}(a := a - b, P)$
   $(Q \wedge a \in [1..x] \wedge b \in [1..y] \wedge \mathrm{lnko}(a,b) = \mathrm{lnko}(x,y) \wedge a > b)$
   $\overset{?}{\Rightarrow}$
   $\mathrm{lf}(a := a - b, P) = (Q \wedge a - b \in [1..x] \wedge b \in [1..y] \wedge \mathrm{lnko}(a - b, b) = \mathrm{lnko}(x,y)) \surd$

Ezen következések felismeréséhez szükséges az alábbi tétel:
$\mathrm{lnko}(a,b) = \mathrm{lnko}(a - b, b)$ (ha $a > b$)
Bizonyítás:
Ha egy szám osztója a-nak és b-nek is, akkor $a - b$-nek is, illetve, ha osztója $a - b$-nek és b-nek, akkor a-nak is, ui.:

1. $\forall x \in \mathbb{N} : (\exists c, d \in \mathbb{N} : cx = a \wedge dx = b) \overset{a>b}{\Rightarrow} (c - d)x = a - b$
2. $\forall x \in \mathbb{N} : (\exists c, d \in \mathbb{N} : cx = a - b \wedge dx = b) \Rightarrow (c + d)x = a$

Ha a közös osztók halmaza pontosan egyenlő (és véges), akkor a maximális elem (az lnko) is egyezik. Ezzel a tételt megmutattuk.