Legnagyobb közös osztó meghatározása

A feladat specifikációja:

$$A = \underset{a}{\mathbb{N}} \times \underset{b}{\mathbb{N}} \times \underset{d}{\mathbb{N}}$$

$$B = \underset{a'}{\mathbb{N}} \times \underset{b'}{\mathbb{N}}$$

$$Q : \big(a = a' \land b = b'\big)$$

$$R : \big(d = \mathrm{lnko}(a', b')\big)$$

Keressük a megoldást adó programot **ciklus** formában, ahol

$$P : \big(\mathrm{lnko}(a', b') = \mathrm{lnko}(a, d)\big)$$

1. $Q \not\Rightarrow P$, de $Q \Rightarrow P^{d \leftarrow b}$.
   Innen adódik, hogy
   $Q \Rightarrow \mathrm{lf}(d := b,\ P)$
2. A ciklus levezetési szabálya második feltétele:
   $P \land \neg\pi \Rightarrow R$
   teljesül, ha $\neg\pi :\ (a = d)$, mivel
   $\mathrm{lnko}(a', b') = \mathrm{lnko}(a, d) \land a = d\ \Rightarrow d = \mathrm{lnko}(a', b')$.
   Ezért $\pi :\ (a \neq d)$ alkalmas választás.
3. A ciklus levezetési szabálya harmadik feltétele:
   $P \land \pi \Rightarrow t > 0$
   teljesül, ha $t :\ a + d$
   a π választása miatt.
5. A ciklus levezetési szabálya ötödik feltétele:
   $P \land \pi \land t \leq t_0 + 1 \Rightarrow \mathrm{lf}(S_0, t \leq t_0)$ minden $t_0 \in \mathbb{Z}$-re.
   Könnyen látható, hogy
   $P \land \pi \land a > d \land a + d \leq t_0 + 1 \Rightarrow (a - d) + d \leq t_0 \Leftrightarrow (t \leq t_0)^{a \leftarrow a - d} \Leftrightarrow$
   $\Leftrightarrow \mathrm{lf}(a := a - d, t \leq t_0)$,
   valamint $P \land \pi \land a < d \land a + d \leq t_0 + 1 \Rightarrow a + (d - a) \leq t_0 \Leftrightarrow (t \leq t_0)^{d \leftarrow d - a} \Leftrightarrow$
   $\Leftrightarrow \mathrm{lf}(d := d - a, t \leq t_0)$.
   Alkalmazva az elágazás levezetési szabályát, kapjuk
   $P \land \pi \land (a < d \lor a > d) \land t \leq t_0 + 1 \Rightarrow$
   $\Rightarrow \mathrm{lf}(IF(a > d : a := a - d, a < d : d := d - a), t \leq t_0)$.
   Vegyük észre, hogy
   $\pi \land (a < d \lor a > d) \Leftrightarrow \pi$,
   ezért
   $P \land \pi \land t \leq t_0 + 1 \Rightarrow \mathrm{lf}(IF(a > d : a := a - d, a < d : d := d - a), t \leq t_0)$.

4. Belátható, hogy a ciklus levezetési szabályának negyedik feltétele is teljesül, ha
   $S_0 : IF(a > d : a := a - d, a < d : d := d - a)$.
   Vegyük észre, hogy
   $P \wedge \pi \wedge a > d \Rightarrow (\mathrm{lnko}(a', b') = \mathrm{lnko}(a, d) = \mathrm{lnko}(a - d, d)) \Rightarrow$
   $\Rightarrow (\mathrm{lnko}(a', b') = \mathrm{lnko}(a - d, d)) \Leftrightarrow P^{a \leftarrow a-d} \Leftrightarrow \mathrm{lf}(a := a - d, P)$.
   Tehát
   $P \wedge \pi \wedge a > d \Rightarrow \mathrm{lf}(a := a - d, P)$. Ugyanígy belátható, hogy
   $P \wedge \pi \wedge a < d \Rightarrow \mathrm{lf}(d := d - a, P)$.
   Alkalmazva az elágazás levezetési szabályát, kapjuk, hogy
   $P \wedge \pi \Rightarrow \mathrm{lf}(IF(a > d : a := a - d, a < d : d := d - a), P)$,
   tehát a ciklus levezetési szabályának negyedik feltétele is teljesül az S_0 fenti választása esetén.
   Mivel $P \Rightarrow P$ nyilván teljesül, ezért
   $P \Rightarrow \mathrm{lf}(DO(a \neq d, IF(a > d : a := a - d, a < d : d := d - a)), R)$.

Alkalmazva a szekvencia levezetési szabályat, kapjuk, hogy
$Q \Rightarrow \mathrm{lf}((d := b, DO(a \neq d, IF(a > d : a := a - d, a < d : d := d - a))), R)$.
A **specifikáció** tételének alkalmazásával adódik, hogy egy lehetséges megoldás a

$$(d := b, DO(a \neq d, IF(a > d : a := a - d, a < d : d := d - a)))$$

program, amely struktogrammja:

$d := b$	
$a \neq d$	
$a > d$	$a < d$
$a := a - d$	$d := d - a$