Prím tulajdonság meghatározása

$A = \underset{n}{\mathbb{N}} \times \underset{l}{\mathbb{L}}$

$B = \underset{n'}{\mathbb{N}}$

$Q : \big(n = n'\big)$

$R : \big(Q \land (\neg l \leftrightarrow (n = 1 \lor \exists k \in [2..n-1] : n \bmod k = 0))\big)$

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

$P : \big(Q \land i \in [1..n] \land (\neg l \leftrightarrow (n = 1 \lor \exists k \in [2..i] : n \bmod k = 0))\big)$

1. A ciklus levezetési szabálya második feltétele:
   $P \land \neg\pi \Rightarrow R$
   teljesül, ha $\neg\pi :\ \neg l \lor i \geq n-1$.
   Tehát $\pi :\ l \land i < n-1$ alkalmas választás.
2. A ciklus levezetési szabálya harmadik feltétele:
   $P \land \pi \Rightarrow t > 0$
   teljesül, ha $t : n - 1 - i$
   a π választása miatt.
3. Célszerű a ciklusmagot
   $S_0 : (S_1; S_2)$
   szekvencia fomában keresni, ahol
   $S_2 = (i := i + 1)$
   abból a meggondolásból, hogy a ciklus levezetési szabályának 5. feltétele is teljesüljön. Alkalmazva a szekvencia leggyengébb előfeltételére ismert tételt,
   $P \land \pi \Rightarrow \mathrm{lf}(S_0,\ P) \Leftrightarrow \mathrm{lf}(S_1,\ lf(S_2,\ P))$
   teljesül, ha
   $P \land \pi \Rightarrow \mathrm{lf}(S_1, P^{i \leftarrow i+1})$,
   mivel
   $\mathrm{lf}(i := i+1,\ P) \Leftrightarrow P^{i \leftarrow i+1}$.
   $P^{i \leftarrow i+1} : \big(Q \land i+1 \in [1..n] \land (\neg l \leftrightarrow (n = 1 \lor \exists k \in [2..i+1] : n \bmod k = 0))\big)$,
   ugyanakkor
   $P \land \pi \Rightarrow$
   $Q \land i+1 \in [1..n] \land (\neg n \bmod i+1 \neq 0 \leftrightarrow (n = 1 \lor \exists k \in [2..i+1] : n \bmod k = 0))$,
   ahonnan
   $P \land \pi \Rightarrow {P^{i \leftarrow i+1}}^{l \leftarrow n \bmod i+1 \neq 0}$.
   Ezért Tehát
   $S_0 = (l := n \bmod i + 1 \neq 0; i := i + 1)$
   alkalmas választás a ciklus levezetési szabálya negyedik feltétele teljesüléséhez.
4. 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.

Mivel
$\mathrm{lf}(S_0, t \leq t_0) \Leftrightarrow (t \leq t_0)^{i \leftarrow i+1}{}^{l \leftarrow n \bmod i+1 \neq 0} \Leftrightarrow n - 1 - i \leq t_0 + 1 \Leftrightarrow t \leq t_0 + 1$
tetszőleges $t_0 \in \mathbb{Z}$-re,
ezért a ciklus levezetési szabályának ötödik feltétele is teljesül.

5. Könnyen ellenőrizhető, hogy
$Q \Rightarrow P$
nem teljesül. Ugyanakkor látható, hogy
$Q \Rightarrow P^{i,l \leftarrow 1, n \neq 1}$
fennáll, mivel
$P^{i,l \leftarrow 1, n \neq 1} : \big(Q \wedge 1 \in [1..n] \wedge (\neg n \neq 1 \leftrightarrow (n = 1 \vee \exists k \in [2..1] : n \bmod k = 0))\big)$
és
$\big(1 \in [1..n] \wedge (\neg n \neq 1 \leftrightarrow (n = 1 \vee \exists k \in [2..1] : n \bmod k = 0))\big) \Leftrightarrow \mathit{true}$.
Tehát
$Q \Rightarrow \mathrm{lf}(i, l := 1, n \neq 1,\ P)$.
Ugyanakkor a ciklus levezetési szabálya első feltétele:
$P \Rightarrow P$
nyilván teljesül, ezért
$P \Rightarrow \mathrm{lf}(DO,\ R)$
is igaz, ahol $DO = (l \wedge i < n - 1, S_0)$.
Alkalmazva a szekvenciával kapcsolatos levezetési szabályt, kapjuk:
$Q \Rightarrow \mathrm{lf}((i, l := 1, n \neq 1; DO),\ R)$

Tehát a keresett program:

$i, l := 1, n \neq 1$
$l \wedge i < n - 1$
$l := n \bmod i + 1 \neq 0$
$i := i + 1$