271 (least common multiple) Given two positive integers, write a program to find their least common multiple.

After trying the question, scroll down to the solution.

§ Let L be the least common multiple of a and b, defined as

$$L\text{: } a\times(nat+1) \text{ ‘ } b\times(nat+1) \ \land\ \forall m\text{: } a\times(nat+1) \text{ ‘ } b\times(nat+1)\cdot\ L\le m$$

Let x and y be positive integer variables whose final value will be L. Let t be time. Define

$$Q \ = \quad x\text{: } a\times(nat+1) \ \land\ x\le L \ \land\ y\text{: } b\times(nat+1) \ \land\ y\le L$$
$$\Rightarrow\ x'=y'=L \ \land\ t' = t + (L-x)/a + (L-y)/b$$

Then the refinements are

$$x'=y'=L \ \land\ t' = t + L/a + L/b - 2 \ \Leftarrow\ x\text{:= } a.\ y\text{:= } b.\ Q$$

$Q \ \Leftarrow\ $ **if** $x=y$ **then** ok
else if $x<y$ **then** $x\text{:= } x+a.\ t\text{:= } t+1.\ Q$
else $y\text{:= } y+b.\ t\text{:= } t+1.\ Q$ **fi fi**

Proof of first refinement, starting with its right side.

$x\text{:= } a.\ y\text{:= } b.\ Q$ — expand Q, then Substitution Law twice

$=\quad a\text{: } a\times(nat+1) \ \land\ a\le L \ \land\ b\text{: } b\times(nat+1) \ \land\ b\le L$
$\Rightarrow\ x'=y'=L \ \land\ t' = t + (L-a)/a + (L-b)/b$

$=\quad x'=y'=L \ \land\ t' = t + L/a + L/b - 2$

Proof of last refinement, first case.

$x=y \land ok \ \Rightarrow\ Q$ — expand Q and ok

$=\quad x=y \land x'=x \land y'=y \land t'=t$
$\Rightarrow\ (\quad x\text{: } a\times(nat+1) \ \land\ x\le L \ \land\ y\text{: } b\times(nat+1) \ \land\ y\le L$
$\Rightarrow\ x'=y'=L \ \land\ t' = t + (L-x)/a + (L-y)/b \ )$ — portation

$=\quad x=y=x'=y' \ \land\ t'=t \ \land\ x\text{: } a\times(nat+1) \ \land\ x\le L \ \land\ y\text{: } b\times(nat+1) \ \land\ y\le L$
$\Rightarrow\ x'=y'=L \ \land\ t' = t + (L-x)/a + (L-y)/b$ — use context

$=\quad x=y=x'=y' \ \land\ t'=t \ \land\ x\text{: } a\times(nat+1) \ \land\ x\le L \ \land\ x\text{: } b\times(nat+1) \ \land\ x\le L$
$\Rightarrow\ x=x=L \ \land\ t = t + (L-x)/a + (L-x)/b$ — the antecedent and definition of L imply $x=L$

$=\quad x=y=x'=y' \ \land\ t'=t \ \land\ x\text{: } a\times(nat+1) \ \land\ x\le L \ \land\ x\text{: } b\times(nat+1) \ \land\ x\le L$
$\Rightarrow\ x=x=x \ \land\ t = t + (x-x)/a + (x-x)/b$

$=\quad \top$

Proof of last refinement, middle case.

$x<y \land (x\text{:= } x+a.\ t\text{:= } t+1.\ Q)$ — expand Q and Substitution Law twice

$=\quad x<y \land (x+a\text{: } a\times(nat+1) \ \land\ x+a\le L \ \land\ y\text{: } b\times(nat+1) \ \land\ y\le L$
$\Rightarrow\ x'=y'=L \ \land\ t' = t + 1 + (L-x-a)/a + (L-y)/b)$ — subtract a from both sides of $x+a\text{: } a\times(nat+1)$, and "+1" cancels "$-a/a$"

$=\quad x<y \land (x\text{: } a\times nat \ \land\ x+a\le L \ \land\ y\text{: } b\times(nat+1) \ \land\ y\le L$
$\Rightarrow\ x'=y'=L \ \land\ t' = t + (L-x)/a + (L-y)/b)$ — use $nat+1\text{: } nat$ to decrease $a\times nat$, and so strengthen the inclusion, and so strengthen the antecedent, and so weaken the implication and the whole expression

$\Rightarrow\quad x<y \land (x\text{: } a\times(nat+1) \ \land\ x+a\le L \ \land\ y\text{: } b\times(nat+1) \ \land\ y\le L$
$\Rightarrow\ x'=y'=L \ \land\ t' = t + (L-x)/a + (L-y)/b)$ — I guess I lose some marks here because I don't know which laws to invoke. I'm working on $x+a\le L$ in the context $x<y \ \land\ x\text{: } a\times(nat+1) \ \land\ y\le L$. So $x<L$. Both x and L are multiples of a, but x is a smaller multiple. The next multiple up from x is $x+a$, so $x+a\le L$. In its context, we can replace $x+a\le L$ with $\top$.

$=\quad x<y \land (x\text{: } a\times(nat+1) \ \land\ \top \ \land\ y\text{: } b\times(nat+1) \ \land\ y\le L$
$\Rightarrow\ x'=y'=L \ \land\ t' = t + (L-x)/a + (L-y)/b)$ — strengthen antecedent and so weaken the whole expression

$\Rightarrow\quad x<y \land (x\text{: } a\times(nat+1) \ \land\ x\le L \ \land\ y\text{: } b\times(nat+1) \ \land\ y\le L$
$\Rightarrow\ x'=y'=L \ \land\ t' = t + (L-x)/a + (L-y)/b)$ — specialization

$\Rightarrow\quad Q$

Proof of last refinement, last case.

$x>y \land (y\text{:= } y+b.\ t\text{:= } t+1.\ Q)$ — exactly like the previous case

$\Longrightarrow \quad Q$

Using $lcm\ a\ b \times gcd\ a\ b \ = \ a \times b$, where lcm is least common multiple and gcd is greatest common divisor, we can instead find gcd as in Exercise 270. Then

$m' = lcm\ a\ b \ \land \ t' \le t + a{\uparrow}b \ \Longleftarrow$
$x{:=}\ a.\ \ y{:=}\ b.$
$(\textbf{frame}\ a, b\cdot \ a' = b' = gcd\ a\ b \ \land \ t' \le t + a{\uparrow}b).$
$m{:=}\ x{\times}y/a$

Here is a program to compute lcm at the same time as gcd , rather than afterward. I'll leave out the time, which is the same as before.

$m' = lcm\ a\ b \ \Longleftarrow$
$x{:=}\ a.\ \ y{:=}\ b.\ \ a' = b' = gcd\ a\ b \ \land \ a'{\times}y'{+}b'{\times}x' = a{\times}y{+}b{\times}x.\ \ m{:=}\ (x{+}y)/2$
$a' = b' = gcd\ a\ b \ \land \ a'{\times}y'{+}b'{\times}x' = a{\times}y{+}b{\times}x \ \Longleftarrow$
$\textbf{if}\ a{>}b\ \textbf{then}\ a{:=}\ a{-}b.\ \ x = x{+}y.\ \ a' = b' = gcd\ a\ b \ \land \ a'{\times}y'{+}b'{\times}x' = a{\times}y{+}b{\times}x$
$\textbf{else if}\ a{<}b\ \textbf{then}\ b{:=}\ b{-}a.\ y{:=}\ y{+}x.\ a'{=}b'{=}gcd\ a\ b \land a'{\times}y'{+}b'{\times}x' = a{\times}y{+}b{\times}x$
$\textbf{else}\ ok\ \textbf{fi fi}$