220 (remainder) Write a program to find the remainder after natural division (Exercise 219), using only comparison, addition, and subtraction (not multiplication, division, *div*, *mod*).

After trying the question, scroll down to the solution.

§ Let n be a natural state variable whose initial value is the numerator and whose final value is the remainder. Let d: $nat{+}1$ be the divisor (a constant). Let t be time. The problem is P defined as

$$P \;=\; n'{<}d \;\wedge\; (\exists m{:}\; nat{\cdot}\; n = m{\times}d + n') \;\wedge\; t' \le t + n/d$$

or if you prefer

$$P \;=\; n'{:}\; 0,..d \;\wedge\; n{:}\; nat{\times}d + n' \;\wedge\; t' \le t + n/d$$

And my solution is

$$P \;\Leftarrow\; \textbf{if } n{<}d \textbf{ then } ok \textbf{ else } n{:=}\, n{-}d.\;\; t{:=}\, t{+}1.\;\; P \textbf{ fi}$$

The proof is by parts and cases. I have to prove the following 6 refinements.

$$n'{<}d \;\Leftarrow\; n{<}d \;\wedge\; ok$$
$$n'{<}d \;\Leftarrow\; n{\ge}d \;\wedge\; (n{:=}\, n{-}d.\;\; t{:=}\, t{+}1.\;\; n'{<}d)$$
$$\exists m{:}\; nat{\cdot}\; n = m{\times}d + n' \;\Leftarrow\; n{<}d \;\wedge\; ok$$
$$\exists m{:}\; nat{\cdot}\; n = m{\times}d + n' \;\Leftarrow\; n{\ge}d \;\wedge\; (n{:=}\, n{-}d.\;\; t{:=}\, t{+}1.\;\; \exists m{:}\; nat{\cdot}\; n = m{\times}d + n')$$
$$t' \le t + n/d \;\Leftarrow\; n{<}d \;\wedge\; ok$$
$$t' \le t + n/d \;\Leftarrow\; n{\ge}d \;\wedge\; (n{:=}\, n{-}d.\;\; t{:=}\, t{+}1.\;\; t' \le t + n/d)$$

First, turning it around:

	$n{<}d \wedge ok \;\Rightarrow\; n'{<}d$	expand ok
$=$	$n{<}d \wedge n'{=}n \wedge t'{=}t \;\Rightarrow\; n'{<}d$	context
$=$	$n{<}d \wedge n'{=}n \wedge t'{=}t \;\Rightarrow\; n{<}d$	specialization
$=$	$\top$	

Next, turning it around:

	$n{\ge}d \;\wedge\; (n{:=}\, n{-}d.\;\; t{:=}\, t{+}1.\;\; n'{<}d) \;\Rightarrow\; n'{<}d$	substitution twice
$=$	$n{\ge}d \;\wedge\; n'{<}d \;\Rightarrow\; n'{<}d$	specialization
$=$	$\top$	

Next, turning it around:

	$n{<}d \;\wedge\; ok \;\Rightarrow\; \exists m{:}\; nat{\cdot}\; n = m{\times}d + n'$	expand ok
$=$	$n{<}d \;\wedge\; n'{=}n \wedge t'{=}t \;\Rightarrow\; \exists m{:}\; nat{\cdot}\; n = m{\times}d + n'$	context
$=$	$n{<}d \;\wedge\; n'{=}n \wedge t'{=}t \;\Rightarrow\; \exists m{:}\; nat{\cdot}\; n = m{\times}d + n$	generalization: 0 for m
$\Leftarrow$	$n{<}d \;\wedge\; n'{=}n \wedge t'{=}t \;\Rightarrow\; n = 0{\times}d + n$	arithmetic
$=$	$n{<}d \;\wedge\; n'{=}n \wedge t'{=}t \;\Rightarrow\; \top$	base
$=$	$\top$	

Next, starting with its right side:

	$n{\ge}d \;\wedge\; (n{:=}\, n{-}d.\;\; t{:=}\, t{+}1.\;\; \exists m{:}\; nat{\cdot}\; n = m{\times}d + n')$	substitution twice
$=$	$n{\ge}d \;\wedge\; \exists m{:}\; nat{\cdot}\; n{-}d = m{\times}d + n'$	specialize and arithmetic
$\Rightarrow$	$\exists m{:}\; nat{\cdot}\; n = (m{+}1){\times}d + n'$	change local variable
$=$	$\exists p{:}\; nat{+}1{\cdot}\; n = p{\times}d + n'$	widen domain
$\Rightarrow$	$\exists p{:}\; nat{\cdot}\; n = p{\times}d + n'$	change local variable back to m
$=$	$\exists m{:}\; nat{\cdot}\; n = m{\times}d + n'$	

Next, turning it around:

	$n{<}d \;\wedge\; ok \;\Rightarrow\; t' \le t + n/d$	expand ok
$=$	$n{<}d \;\wedge\; n'{=}n \wedge t'{=}t \;\Rightarrow\; t' \le t + n/d$	context
$=$	$n{<}d \;\wedge\; n'{=}n \wedge t'{=}t \;\Rightarrow\; t \le t + n/d$	arithmetic
$=$	$n{<}d \;\wedge\; n'{=}n \wedge t'{=}t \;\Rightarrow\; 0 \le n/d$	n: nat and d: $nat{+}1$
$=$	$n{<}d \;\wedge\; n'{=}n \wedge t'{=}t \;\Rightarrow\; \top$	base
$=$	$\top$	

Last, turning it around:

	$n{\ge}d \;\wedge\; (n{:=}\, n{-}d.\;\; t{:=}\, t{+}1.\;\; t' \le t + n/d) \;\Rightarrow\; t' \le t + n/d$	substitution twice
$=$	$n{\ge}d \;\wedge\; t' \le t + 1 + (n{-}d)/d \;\Rightarrow\; t' \le t + n/d$	arithmetic
$=$	$n{\ge}d \;\wedge\; t' \le t + n/d \;\Rightarrow\; t' \le t + n/d$	specialization
$=$	$\top$	