144 Let x be an integer variable. Prove the refinement

$$P \Leftarrow \textbf{if } x{=}0 \textbf{ then } ok \textbf{ else } x{:=}\, x{-}1.\ \ t{:=}\, t{+}1.\ \ P \textbf{ fi}$$

where $P \;=\; x'{=}0 \;\wedge\; \textbf{if } x{\geq}0 \textbf{ then } t' = t{+}x \textbf{ else } t'{=}\infty \textbf{ fi}$

After trying the question, scroll down to the solution.

§ By parts. First part:

$x'=0 \;\Leftarrow\; \textbf{if } x=0 \textbf{ then } ok \textbf{ else } x:= x-1.\ t:= t+1.\ x'=0 \textbf{ fi}$

§ By Cases. First case:

	$x=0 \wedge ok \Rightarrow x'=0$	expand *ok*
$=$	$x=0 \wedge x'=x \wedge t'=t \Rightarrow x'=0$	context
$=$	$x=0 \wedge x'=x \wedge t'=t \Rightarrow x=x$	reflexive
$=$	$x=0 \wedge x'=x \wedge t'=t \Rightarrow \top$	base
$=$	$\top$	

Last case:

	$x\neq 0 \wedge (x:= x-1.\ t:= t+1.\ x'=0)$	substitution twice
$=$	$x\neq 0 \wedge x'=0$	specialization
$\Longrightarrow$	$x'=0$	

Last part:

$Q \;\Leftarrow\; \textbf{if } x=0 \textbf{ then } ok \textbf{ else } x:= x-1.\ t:= t+1.\ Q \textbf{ fi}$

where $Q \;=\; \textbf{if } x\geq 0 \textbf{ then } t' = t+x \textbf{ else } t'=\infty \textbf{ fi}$

And we prove it by Cases. First case:

	$x=0 \wedge ok \Rightarrow \textbf{if } x\geq 0 \textbf{ then } t' = t+x \textbf{ else } t'=\infty \textbf{ fi}$	expand *ok*
$=$	$x=0 \wedge x'=x \wedge t'=t \Rightarrow \textbf{if } x\geq 0 \textbf{ then } t' = t+x \textbf{ else } t'=\infty \textbf{ fi}$	context
$=$	$x=0 \wedge x'=x \wedge t'=t \Rightarrow \textbf{if } 0\geq 0 \textbf{ then } t = t+0 \textbf{ else } t'=\infty \textbf{ fi}$	reflexive, case base
$=$	$x=0 \wedge x'=x \wedge t'=t \Rightarrow t=t$	reflexive
$=$	$x=0 \wedge x'=x \wedge t'=t \Rightarrow \top$	base
$=$	$\top$	

Last case:

	$x\neq 0 \wedge (x:= x-1.\ t:= t+1.\ \textbf{if } x\geq 0 \textbf{ then } t' = t+x \textbf{ else } t'=\infty \textbf{ fi})$	substitution twice
$=$	$x\neq 0 \wedge \textbf{if } x-1\geq 0 \textbf{ then } t' = t+1+x-1 \textbf{ else } t'=\infty \textbf{ fi}$	simplify
$=$	$x\neq 0 \wedge \textbf{if } x>0 \textbf{ then } t' = t+x \textbf{ else } t'=\infty \textbf{ fi}$	context: $x\neq 0 \Rightarrow (x>0 = x\geq 0)$
$=$	$x\neq 0 \wedge \textbf{if } x\geq 0 \textbf{ then } t' = t+x \textbf{ else } t'=\infty \textbf{ fi}$	specialization
$\Longrightarrow$	$\textbf{if } x\geq 0 \textbf{ then } t' = t+x \textbf{ else } t'=\infty \textbf{ fi}$	