142 (square) Let s and n be natural variables. Find a specification P such that both the following refinements can be proven:

$s' = n^2 \quad \Leftarrow \quad s{:=}\ n.\ \ P$

$P \quad \Leftarrow \quad$ **if** $n{=}0$ **then** ok **else** $n{:=}\ n{-}1.\ \ s{:=}\ s{+}n{+}n.\ \ P$ **fi**

This program squares using only addition, subtraction, and test for zero.

After trying the question, scroll down to the solution.

§ Looking at the last refinement, I see that it's a loop, and n gets decreased each iteration, until it is 0 . Also, s gets increased each iteration. So P should have the form

$$s' = s + \text{something}$$

In other words, P says that the final value of s is the current value plus something more. When I am proving the first refinement,

$$s' = n^2 \;\Leftarrow\; s:= n.\;\; s' = s + \text{something}$$

I will use the Substitution Law, making it

$$s' = n^2 \;\Leftarrow\; s' = n + \text{something}$$

Now I see that "something" has to get rid of n and supply n^2 . So I'll try

$$P \;=\; s' = s + n^2 - n$$

Proof of first refinement, starting with its right side:

$$
\begin{array}{lll}
 & s:= n.\;\; P & \text{replace } P \\
= & s:= n.\;\; s' = s + n^2 - n & \text{substitution law} \\
= & s' = n + n^2 - n & \text{arithmetic} \\
= & s' = n^2 &
\end{array}
$$

Proof of last refinement, starting with its right side:

$$
\begin{array}{lll}
 & \textbf{if } n=0 \textbf{ then } ok \textbf{ else } n:= n-1.\;\; s:= s+n+n.\;\; P \textbf{ fi} & \text{replace } P \text{ and } ok \\
= & \textbf{if } n=0 \textbf{ then } s'=s \wedge n'=n \textbf{ else } n:= n-1.\;\; s:= s+n+n.\;\; s' = s + n^2 - n \textbf{ fi} & \text{substitution law} \\
= & \textbf{if } n=0 \textbf{ then } s'=s \wedge n'=n \textbf{ else } n:= n-1.\;\; s' = s + n^2 + n \textbf{ fi} & \text{substitution law} \\
= & \textbf{if } n=0 \textbf{ then } s'=s \wedge n'=n \textbf{ else } s' = s + (n-1)^2 + n - 1 \textbf{ fi} & \text{arithmetic} \\
= & \textbf{if } n=0 \textbf{ then } s'=s \wedge n'=n \textbf{ else } s' = s + n^2 - n \textbf{ fi} & \text{context in } \textbf{then}\text{-part} \\
= & \textbf{if } n=0 \textbf{ then } s' = s + n^2 - n \wedge n'=n \textbf{ else } s' = s + n^2 - n \textbf{ fi} & \text{specialize } \textbf{then}\text{-part and} \\
 & & \text{monotonicity} \\
\Longrightarrow & \textbf{if } n=0 \textbf{ then } s' = s + n^2 - n \textbf{ else } s' = s + n^2 - n \textbf{ fi} & \text{generic case idempotent} \\
= & s' = s + n^2 - n & \\
= & P &
\end{array}
$$

I could have used Refinement by Cases to prove the last refinement.