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

$s' = n^2 \iff s := n \cdot P$

$P \iff \text{if } n = 0 \text{ then } \text{ok } \text{ else } n := n - 1. \ s := s + n + n. \ P \text{ fi}$

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,
\[ s' = n^2 \iff s := n. \quad s' = s + \text{something} \]
I will use the Substitution Law, making it
\[ s' = n^2 \iff s' = n + \text{something} \]
Now I see that “something” has to get rid of \( n \) and supply \( n^2 \). So I'll try
\[ P \iff s' = s + n^2 - n \]

Proof of first refinement, starting with its right side:
\[
\begin{align*}
s := n. & \quad P \\
\equiv & \quad s := n. \quad s' = s + n^2 - n \\
\equiv & \quad s' = n + n^2 - n \\
\equiv & \quad s' = n^2
\end{align*}
\]

Proof of last refinement, starting with its right side:
\[
\begin{align*}
\text{if } n=0 & \text{ then ok else } n := n-1. \quad s := s + n + n. \quad P \quad & \text{replace } P \text{ and } ok \\
\equiv & \quad \text{if } n=0 \text{ then } s' := s \land n' := n \text{ else } n := n-1. \quad s := s + n + n. \quad s' = s + n^2 - n \quad & \text{substitution law} \\
\equiv & \quad \text{if } n=0 \text{ then } s' := s \land n' := n \text{ else } n := n-1. \quad s' = s + n^2 + n \quad & \text{substitution law} \\
\equiv & \quad \text{if } n=0 \text{ then } s' := s \land n' := n \text{ else } s' = s + (n-1)^2 + n - 1 \quad & \text{arithmetic} \\
\equiv & \quad \text{if } n=0 \text{ then } s' := s \land n' := n \text{ else } s' = s + n^2 - n \quad & \text{context in then-part} \\
\Rightarrow & \quad s' = s + n^2 - n \\
\equiv & \quad P
\end{align*}
\]

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