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

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

$P \Leftarrow$ **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.

§ 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

$s' = s +$ 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,

$s' = n^2 \Leftarrow s := n.\ s' = s +$ something

I will use the Substitution Law, making it

$s' = n^2 \Leftarrow s' = n +$ 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:

	$s := n.\ P$	replace P
$=$	$s := n.\ s' = s + n^2 - n$	substitution law
$=$	$s' = n + n^2 - n$	arithmetic
$=$	$s' = n^2$	

Proof of last refinement, starting with its right side:

	if $n=0$ **then** *ok* **else** $n := n-1.\ s := s+n+n.\ P$ **fi**	replace P and *ok*
$=$	**if** $n=0$ **then** $s'=s \wedge n'=n$ **else** $n := n-1.\ s := s+n+n.\ s' = s + n^2 - n$ **fi**	substitution law
$=$	**if** $n=0$ **then** $s'=s \wedge n'=n$ **else** $n := n-1.\ s' = s + n^2 + n$ **fi**	substitution law
$=$	**if** $n=0$ **then** $s'=s \wedge n'=n$ **else** $s' = s + (n-1)^2 + n - 1$ **fi**	arithmetic
$=$	**if** $n=0$ **then** $s'=s \wedge n'=n$ **else** $s' = s + n^2 - n$ **fi**	context in **then**-part
$\Longrightarrow$	$s' = s + n^2 - n$	
$=$	P	

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