165 (*mod* 4) Let n be a natural variable. Here is a refinement.

$$n' = mod\ n\ 4 \quad \Leftarrow \quad \textbf{if } n<4 \textbf{ then } ok \textbf{ else } n := n-4.\ \ n' = mod\ n\ 4 \textbf{ fi}$$

(a) Prove it.

(b) Insert time increments according to the recursive time measure, and write a timing specification.

(c) Prove the timing refinement.

After trying the question, scroll down to the solution.

(a) Prove it.

§ Proof uses refinement by cases.

$n' = mod\ n\ 4 \Leftarrow n<4 \wedge ok$ expand *ok*

$= \quad n' = mod\ n\ 4 \Leftarrow n<4 \wedge n'=n$ context and arithmetic

$= \quad n'=n \Leftarrow n<4 \wedge n'=n$ specialization

$= \quad \top$

$n' = mod\ n\ 4 \Leftarrow n\geq 4 \wedge (n := n-4.\ n' = mod\ n\ 4)$ substitution law

$= \quad n' = mod\ n\ 4 \Leftarrow n\geq 4 \wedge n' = mod\ (n-4)\ 4$ context and arithmetic

$= \quad n' = mod\ n\ 4 \Leftarrow n\geq 4 \wedge n' = mod\ n\ 4$ specialization

$= \quad \top$

(b) Insert time increments according to the recursive time measure, and write a timing specification.

§ $t' = t + div\ n\ 4 \Leftarrow$ **if** $n<4$ **then** *ok* **else** $n := n-4.\ t := t+1.\ t' = t + div\ n\ 4$ **fi**

(c) Prove the timing refinement.

§ Proof uses refinement by cases.

$t' = t + div\ n\ 4 \Leftarrow n<4 \wedge ok$ expand *ok*

$= \quad t' = t + div\ n\ 4 \Leftarrow n<4 \wedge n'=n \wedge t'=t$ context and arithmetic

$= \quad t'=t + 0 \Leftarrow n<4 \wedge n'=n \wedge t'=t$ simplify and specialize

$= \quad \top$

$t' = t + div\ n\ 4 \Leftarrow n\geq 4 \wedge (n := n-4.\ t := t+1.\ t' = t + div\ n\ 4)$ substitution law twice

$= \quad t' = t + div\ n\ 4 \Leftarrow n\geq 4 \wedge t' = t + 1 + div\ (n-4)\ 4$ arithmetic

$= \quad t' = t + div\ n\ 4 \Leftarrow n\geq 4 \wedge t' = t + div\ n\ 4$ specialization

$= \quad \top$