168 (fast *mod* 2) Let n and p be natural variables. The problem to reduce n modulo 2 can be solved as follows:

$n' = mod\ n\ 2 \ \Leftarrow\ $ **if** $n<2$ **then** *ok* **else** $even\ n' = even\ n.\ \ n' = mod\ n\ 2$ **fi**

$even\ n' = even\ n \ \Leftarrow\ p:= 2.\ \ even\ p \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ n$

$even\ p \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ n \ \Leftarrow$

$n:= n-p.\ \ p:= p+p.$

if $n<p$ **then** *ok* **else** $even\ p \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ n$ **fi**

(a) Prove these refinements.

(b) Using the recursive time measure, find and prove a sublinear upper time bound.

After trying the question, scroll down to the solution.

(a) Prove these refinements.

§ I assume the property

$$mod\ n\ 2 \ = \ \textbf{if } even\ n \textbf{ then } 0 \textbf{ else } 1 \textbf{ fi}$$

is known. First refinement, by cases; first case, starting with the right side:

$n{<}2 \land ok$ — expand ok

$= \ n{<}2 \land n'{=}n \land p'{=}p$ — specialization and property of mod

$\Rightarrow \ n' = mod\ n\ 2$

First refinement, second case, starting with the right side:

$n{\ge}2 \land (even\ n' = even\ n.\ \ n' = mod\ n\ 2)$ — sequential composition

$= \ n{\ge}2 \land \exists n'', p''\cdot\ even\ n'' = even\ n \ \land\ n' = mod\ n''\ 2$ — property of mod

$= \ n{\ge}2 \land \exists n'', p''\cdot\ even\ n'' = even\ n \ \land\ n' = \textbf{if } even\ n'' \textbf{ then } 0 \textbf{ else } 1 \textbf{ fi}$ — context

$= \ n{\ge}2 \land \exists n'', p''\cdot\ even\ n'' = even\ n \ \land\ n' = \textbf{if } even\ n \textbf{ then } 0 \textbf{ else } 1 \textbf{ fi}$ — property of mod

$= \ n{\ge}2 \land \exists n'', p''\cdot\ even\ n'' = even\ n \ \land\ n' = mod\ n\ 2$ — distribution

$= \ n{\ge}2 \land (\exists n'', p''\cdot\ even\ n'' = even\ n) \ \land\ n' = mod\ n\ 2$ — specialization

$\Rightarrow \ n' = mod\ n\ 2$

Second refinement, starting with the right side:

$p{:=}\ 2.\ \ even\ p \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ n$ — substitution

$= \ even\ 2 \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ n$ — simplify and specialize

$\Rightarrow \ even\ n' = even\ n$

Last refinement,

$(\quad even\ p \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ n$

$\Leftarrow \ n{:=}\ n{-}p.\ \ p{:=}\ p{+}p.\ \ \textbf{if } n{<}p \textbf{ then } ok \textbf{ else } even\ p \ \Rightarrow\ even\ p' \land even\ n' = even\ n \textbf{ fi})$

expand ok and then two substitutions

$= \ (\quad even\ p \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ n$

$\Leftarrow \ \textbf{if } n{-}p{<}p{+}p \textbf{ then } n'{=}n{-}p \land p'{=}p{+}p$

$\textbf{else } even\ (p{+}p) \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ (n{-}p) \textbf{ fi}\ )$ — portation

$= \quad even\ p$

$\land\ \textbf{if } n{-}p{<}p{+}p \textbf{ then } n'{=}n{-}p \land p'{=}p{+}p$

$\textbf{else } even\ (p{+}p) \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ (n{-}p) \textbf{ fi}$

$\Rightarrow \ even\ p' \ \land\ even\ n' = even\ n$ — use $even\ p$ as context

$= \ even\ p \ \land\ \textbf{if } n{-}p{<}p{+}p \textbf{ then } n'{=}n{-}p \land p'{=}p{+}p \textbf{ else } even\ p' \ \land\ even\ n' = even\ n \textbf{ fi}$

$\Rightarrow \ even\ p' \ \land\ even\ n' = even\ n$ — case analysis, then distribution

$= \ (even\ p \land n{-}p{<}p{+}p \land n'{=}n{-}p \land p'{=}p{+}p \ \Rightarrow\ even\ p' \ \land\ even\ n' = even\ n)$

$\land\ (even\ p \land n{-}p{\ge}p{+}p \land even\ p' \ \land\ even\ n' = even\ n \ \Rightarrow\ even\ p' \land even\ n' = even\ n)$

the first implication uses properties of $even$, and the second is just specialization

$= \ \top$

(b) Using the recursive time measure, find and prove a sublinear upper time bound.

§ Adding recursive time, we have

$$X \ \Leftarrow\ \textbf{if } n{<}2 \textbf{ then } ok \textbf{ else } Y.\ \ t{:=}\ t{+}1.\ \ X \textbf{ fi}$$
$$Y \ \Leftarrow\ p{:=}\ 2.\ \ Z$$
$$Z \ \Leftarrow\ n{:=}\ n{-}p.\ \ p{:=}\ p{+}p.\ \ \textbf{if } n{<}p \textbf{ then } ok \textbf{ else } t{:=}\ t{+}1.\ \ Z \textbf{ fi}$$

Defining X, Y, and Z appropriately is really, really hard. I used recursive construction (Chapter 6) plus a guess to get Z. Then Y was easy from Z by looking at the refinement for Y. But I still don't fully know X. I'll write $f\ n$ for a not-yet-known function of n.

$$X \ =\ \textbf{if } n{<}2 \textbf{ then } t'{=}t \textbf{ else } t' = t + f\ n \textbf{ fi}$$
$$Y \ =\ n{\ge}2 \ \Rightarrow\ t' = t + floor\ log\ (n{+}2) - 2 \ \land\ n' = n - 2^{floor\ log\ (n+2)} + 2$$
$$Z \ =\ n{\ge}p{\ge}2 \ \Rightarrow\ t' = t + floor\ log\ (n/p + 1) - 1 \ \land\ n' = n - p{\times}2^{floor\ log\ (n/p\ +\ 1)} + p$$

Proof of the Z refinement:

$$(Z \Leftarrow n{:=}\ n-p.\ \ p{:=}\ p+p.\ \ \textbf{if}\ n<p\ \textbf{then}\ ok\ \textbf{else}\ t{:=}\ t+1.\ \ Z\ \textbf{fi})$$

replace ok and rightmost Z and substitution law

$$\begin{aligned}=\ \ &(Z \Leftarrow n{:=}\ n-p.\ \ p{:=}\ p+p.\\ &\quad \textbf{if}\ n<p\ \textbf{then}\ \ n'=n \wedge p'=p \wedge t'=t\\ &\quad \textbf{else}\ n\ge p\ge 2 \Rightarrow \ \ t' = t+1+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\\ &\qquad\qquad \wedge\ \ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1)\ \textbf{fi})\end{aligned}$$

substitution law twice more

$$\begin{aligned}=\ \ &(Z \Leftarrow \textbf{if}\ n-p < p+p\ \textbf{then}\ \ n'=n-p \wedge p'=p+p \wedge t'=t\\ &\quad \textbf{else}\ n-p\ge p+p\ge 2 \Rightarrow \ \ t' = t+1+\mathit{floor}\ \mathit{log}\ ((n-p)/(p+p)+1)-1\\ &\qquad\qquad \wedge\ \ n' = n-p-(p+p)\times(2^{\mathit{floor}\ \mathit{log}\ ((n-p)/(p+p)+1)}-1)\ \textbf{fi})\end{aligned}$$

simplify

$$\begin{aligned}=\ \ &(Z \Leftarrow \textbf{if}\ n < 3\times p\ \textbf{then}\ \ n'=n-p \wedge p'=2\times p \wedge t'=t\\ &\quad \textbf{else}\ n\ge 3\times p \wedge p\ge 1 \Rightarrow \ \ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\\ &\qquad\qquad \wedge\ \ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1)\ \textbf{fi})\end{aligned}$$

replace Z and portation

$$\begin{aligned}=\ \ &\quad n\ge p\ge 2 \wedge \textbf{if}\ n < 3\times p\ \textbf{then}\ \ n'=n-p \wedge p'=2\times p \wedge t'=t\\ &\qquad \textbf{else}\ n\ge 3\times p \wedge p\ge 1 \Rightarrow \ \ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\\ &\qquad\qquad \wedge\ \ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1)\ \textbf{fi}\\ &\Rightarrow\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\ \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1)\end{aligned}$$

case analysis and distribution

$$\begin{aligned}=\ \ &\qquad n\ge p\ge 2 \wedge n<3\times p \wedge n'=n-p \wedge p'=2\times p \wedge t'=t\\ &\quad \vee\ \ n\ge p\ge 2 \wedge (n\ge 3\times p \wedge p\ge 1 \Rightarrow \ \ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\\ &\qquad\qquad \wedge\ \ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\\ &\Rightarrow\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\ \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1)\end{aligned}$$

antidistribution

$$\begin{aligned}=\ \ &\quad (\ \ 2\le p\le n<3\times p \wedge n'=n-p \wedge p'=2\times p \wedge t'=t\\ &\quad \Rightarrow\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\ \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\\ &\wedge\ (\ \ n\ge p\ge 2 \wedge n\ge 3\times p \wedge (n\ge 3\times p \wedge p\ge 1 \Rightarrow \ \ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\\ &\qquad\qquad \wedge\ \ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\\ &\quad \Rightarrow\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\ \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\end{aligned}$$

In the bottom conjunct, discharge

$$\begin{aligned}=\ \ &\quad (\ \ 2\le p\le n<3\times p \wedge n'=n-p \wedge p'=2\times p \wedge t'=t\\ &\quad \Rightarrow\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\ \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\\ &\wedge\ (\qquad n\ge p\ge 2 \wedge n\ge 3\times p \wedge\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\\ &\qquad \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\\ &\quad \Rightarrow\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\ \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\end{aligned}$$

In the top conjunct, $2\le p\le n<3\times p\ \Rightarrow\ 2 \le (n/p+1) < 4$
so $\mathit{floor}\ \mathit{log}\ (n/p+1) = 1$

$$\begin{aligned}=\ \ &\quad (\ \ 2\le p\le n<3\times p \wedge n'=n-p \wedge p'=2\times p \wedge t'=t\\ &\quad \Rightarrow\ t' = t+1-1\ \wedge\ n' = n - p\times(2^{1}-1))\\ &\wedge\ (\qquad n\ge p\ge 2 \wedge n\ge 3\times p \wedge\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\\ &\qquad \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\\ &\quad \Rightarrow\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\ \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\end{aligned}$$

simplify second line, then specialize, then identity

$$\begin{aligned}=\ \ &\qquad n\ge p\ge 2 \wedge n\ge 3\times p \wedge\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\\ &\quad \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1))\\ &\Rightarrow\ t' = t+\mathit{floor}\ \mathit{log}\ (n/p+1)-1\ \wedge\ n' = n - p\times(2^{\mathit{floor}\ \mathit{log}\ (n/p+1)}-1)\end{aligned}$$

specialize

$$=\ \ \top$$

Proof of the Y refinement is one use of the substitution law.

Proof of the X refinement:

$$
\begin{array}{lll}
& (X \Leftarrow \textbf{if } n<2 \textbf{ then } ok \textbf{ else } Y.\ t:= t+1.\ X \textbf{ fi}) & \text{replace first } X \\
= & (\quad \textbf{if } n<2 \textbf{ then } t'=t \textbf{ else } t' = t + f\,n \textbf{ fi} & \\
& \Leftarrow \textbf{if } n<2 \textbf{ then } ok \textbf{ else } Y.\ t:= t+1.\ X \textbf{ fi}) & \text{monotonicity} \\
\Leftarrow & n\ge2 \wedge (Y.\ t:= t+1.\ \textbf{if } n<2 \textbf{ then } t'=t \textbf{ else } t' = t + f\,n \textbf{ fi}) \Rightarrow t' = t + f\,n & \text{substitution law} \\
= & n\ge2 \wedge (Y.\ \textbf{if } n<2 \textbf{ then } t'=t+1 \textbf{ else } t' = t + 1 + f\,n \textbf{ fi}) \Rightarrow t' = t + f\,n &
\end{array}
$$

Now I want to focus on the sequential composition

$$
\begin{array}{lll}
& Y.\ \textbf{if } n<2 \textbf{ then } t'=t+1 \textbf{ else } t' = t + 1 + f\,n \textbf{ fi} & \text{replace } Y \\
= & n\ge2 \Rightarrow t' = t + floor\ log\ (n+2) - 2 \wedge n' = n - 2^{floor\ log\ (n+2)} + 2. & \\
& \textbf{if } n<2 \textbf{ then } t'=t+1 \textbf{ else } t' = t + 1 + f\,n \textbf{ fi} & \text{condition law} \\
\Rightarrow & n\ge2 \Rightarrow (\ t' = t + floor\ log\ (n+2) - 2 \wedge n' = n - 2^{floor\ log\ (n+2)} + 2. & \\
& \quad \textbf{if } n<2 \textbf{ then } t'=t+1 \textbf{ else } t' = t + 1 + f\,n \textbf{ fi}\ ) & \text{sequential composition} \\
= & n\ge2 \Rightarrow \exists n'', p'', t''\cdot\ t'' = t + floor\ log\ (n+2) - 2 \wedge n'' = n - 2^{floor\ log\ (n+2)} + 2 & \\
& \quad \wedge\ \textbf{if } n''<2 \textbf{ then } t'=t''+1 \textbf{ else } t' = t'' + 1 + f\,n'' \textbf{ fi} & \\
& & \text{one-point twice, and } p'' \text{ is unused} \\
= & n\ge2 \Rightarrow \textbf{if } n - 2^{floor\ log\ (n+2)} + 2 < 2 & \\
& \quad \textbf{then } t'= t + floor\ log\ (n+2) - 2 + 1 & \\
& \quad \textbf{else } t' = t + floor\ log\ (n+2) - 2 + 1 + f\,(n - 2^{floor\ log\ (n+2)} + 2) \textbf{ fi} & \\
& & \text{simplify} \\
= & n\ge2 \Rightarrow \textbf{if } n < 2^{floor\ log\ (n+2)} & \\
& \quad \textbf{then } t'= t + floor\ log\ (n+2) - 1 & \\
& \quad \textbf{else } t' = t + floor\ log\ (n+2) - 1 + f\,(n - 2^{floor\ log\ (n+2)} + 2) \textbf{ fi} &
\end{array}
$$

Popping out from the focus, resuming the earlier calculation,

$$
\begin{array}{lll}
\Leftarrow & \quad n\ge2 \wedge (n\ge2 \Rightarrow \textbf{if } n < 2^{floor\ log\ (n+2)} & \\
& \qquad \textbf{then } t'= t + floor\ log\ (n+2) - 1 & \\
& \qquad \textbf{else } t' = t + floor\ log\ (n+2) - 1 + f\,(n - 2^{floor\ log\ (n+2)} + 2) \textbf{ fi}) & \\
& \Rightarrow t' = t + f\,n & \text{discharge} \\
= & \quad n\ge2 \wedge \textbf{if } n < 2^{floor\ log\ (n+2)} & \\
& \qquad \textbf{then } t'= t + floor\ log\ (n+2) - 1 & \\
& \qquad \textbf{else } t' = t + floor\ log\ (n+2) - 1 + f\,(n - 2^{floor\ log\ (n+2)} + 2) \textbf{ fi} & \\
& \Rightarrow t' = t + f\,n & \text{case analysis and antidistribution} \\
= & \quad (n\ge2 \wedge n < 2^{floor\ log\ (n+2)} \wedge t'= t + floor\ log\ (n+2) - 1 \Rightarrow t' = t + f\,n) & \\
& \wedge\ (\quad n\ge2 \wedge n \ge 2^{floor\ log\ (n+2)} & \\
& \qquad \wedge\ t' = t + floor\ log\ (n+2) - 1 + f\,(n - 2^{floor\ log\ (n+2)} + 2) & \\
& \quad \Rightarrow t' = t + f\,n) & \\
\Leftarrow & \quad (2 \le n < 2^{floor\ log\ (n+2)} \Rightarrow f\,n = floor\ log\ (n+2) - 1) & \\
& \wedge\ (\quad n\ge2 \wedge n \ge 2^{floor\ log\ (n+2)} & \\
& \quad \Rightarrow f\,n = floor\ log\ (n+2) - 1 + f\,(n - 2^{floor\ log\ (n+2)} + 2)) &
\end{array}
$$

And that's the definition of f that we needed. We can write it as a recursive function as follows:

$$f \;=\; \langle n\colon nat\cdot \;\; \textbf{if}\ n<2\ \textbf{then}\ 0$$
$$\textbf{else if}\ n\colon 2^{nat+2} - (1, 2)\ \textbf{then}\ \mathit{floor}\ \mathit{log}\ (n+2) - 1$$
$$\textbf{else}\ \mathit{floor}\ \mathit{log}\ (n+2) - 1 + f\,(n - 2^{\mathit{floor}\ \mathit{log}\ (n+2)} + 2)\ \textbf{fi fi}\rangle$$

That is the sublinear time exactly.