MODULE *TLASAFETYY*

EXTENDS *Integers*, *Naturals*, *TLC*, *TLAPS*

CONSTANTS n

ASSUME $n \in Nat$

VARIABLES $x,\ y$

$a \triangleq x \geq 0 \quad \land x' = x + 1 \land \ y' = y$

$bplus \triangleq y < n \land y' = y + 1 \land x' = x$

$bminus \triangleq 0 < y \land y' = y - 1 \land x' = x$

$Init \triangleq x = -1 \land y = 0$

$Next \triangleq a \lor bplus \lor bminus$

$Spec \triangleq Init \land \Box[Next]_{\langle x,\, y \rangle}$

$Typing \triangleq x \in Int \land y \in Int$

$Safe1 \triangleq x = -1$

$Safe2 \triangleq x \leq 0$

$$Safe3 \triangleq \begin{array}{l} \land\, 0 \leq y \\ \land\, y \leq n \end{array}$$

$InductiveInvariant \triangleq Safe1 \land Safe3$

ASSUME $Assumption \triangleq n \in Nat$

THEOREM $InitProperty \triangleq Init \Rightarrow InductiveInvariant$

THEOREM $Invariance \triangleq Spec \Rightarrow \Box InductiveInvariant$

THEOREM $Correctness \triangleq Spec \Rightarrow \Box Safe2$
