MODULE *inmalgtd1ex5*

EXTENDS *Integers*, *TLC*

CONSTANTS *mini*, *maxi*, *und*, *bund* constants for undefinedness, bounds of domain

requires
CONSTANTS x x is the input
ASSUME $x \in Nat$

VARIABLES y, z, pc

$Init \triangleq y = und \land z = bund \land pc =$ "start"

$L1 \triangleq pc =$ "start" $\land\, y' = 2 \land pc' =$ "loop" $\land$ UNCHANGED $\langle z \rangle$
$L2 \triangleq pc =$ "loop" $\land\, y \geq x \land z' =$ TRUE $\land\, pc' =$ "halt" $\land$ UNCHANGED $\langle y \rangle$
$L3 \triangleq pc =$ "loop" $\land\, y < x \land x \% y = 0 \land z' =$ FALSE $\land\, pc' =$ "halt" $\land$ UNCHANGED $\langle y \rangle$
$L4 \triangleq pc =$ "loop" $\land\, y < x \land x \% y \neq 0 \land y' = y + 1 \land$ UNCHANGED $\langle pc, z \rangle$
$skip \triangleq$ UNCHANGED $\langle pc, z, y \rangle$

$Next \triangleq L1 \lor L2 \lor L3 \lor L4 \lor skip$

auxiliary definitions
$prime(u) \triangleq \forall\, v \in 2 \,..\, u - 1 : u \% v \neq 0$ define that x is a prime number
$Dint \triangleq mini \,..\, maxi$ domain for integer variables
$Dbool \triangleq \{$FALSE, TRUE$\}$
$DDint(v) \triangleq v \neq und \Rightarrow v \in Dint$
$DDbool(v) \triangleq v \neq bund \Rightarrow v \in Dbool$

$Q1 \triangleq pc =$ "halt" $\Rightarrow z = prime(x)$ is the algorithm partially correct?
$SafePC \triangleq pc =$ "halt" $\Rightarrow z = prime(x)$ the algorithm is partially correct
$Q2 \triangleq pc \neq$ "halt"
$Q3 \triangleq DDint(y) \land DDbool(z)$ is the algorithm runtime errors free?
$SafeRTE \triangleq DDint(y) \land DDbool(z)$ the algorithm is runtime errors free.
$Safe \triangleq SafePC \land SafeRTE$