MODULE *malgtd1ex5*

EXTENDS *Integers*, *TLC*

contract

variables x,y,z

requires $x0 \in Nat \land y0 \in Nat \land Z$ \IN $BOOL$

ensures $zf = prime(x0)$

CONSTANTS $mini, \; maxi, \; und, \; bund$ constants for undefinedness, bounds of domain

requires

CONSTANTS $x0$ $x0$ is the input

precondition

ASSUME $x0 \in Nat$

VARIABLES $x, \; y, \; z, \; pc$

$Init \triangleq \; x = x0 \land y = und \; \land z = bund \land pc = \text{“start”}$

$L1 \triangleq pc = \text{“start”} \land y' = 2 \land pc' = \text{“loop”} \land \text{UNCHANGED} \; \langle x, \; z \rangle$

$L2 \triangleq pc = \text{“loop”} \land y \geq \; x \land z' = \text{TRUE} \land pc' = \text{“halt”} \land \text{UNCHANGED} \; \langle x, \; y \rangle$

$L3 \triangleq pc = \text{“loop”} \land y < x \land x\%y = 0 \land z' = \text{FALSE} \land pc' = \text{“halt”} \land \text{UNCHANGED} \; \langle x, \; y \rangle$

$L4 \triangleq pc = \text{“loop”} \land y < x \land x\%y \neq 0 \; \land y' = y + 1 \land \text{UNCHANGED} \; \langle pc, \; x, \; z \rangle$

$skip \triangleq \text{UNCHANGED} \; \langle pc, \; x, \; z, \; y \; \rangle$

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

auxiliary definitions

$prime(u) \triangleq \forall \, v \in 2 \mathrel{..} u - 1 : u\%v \neq 0$ define that u is a prime number

$Dbool \triangleq \{\text{FALSE}, \; \text{TRUE}\}$

$Dint \triangleq mini \mathrel{..} maxi$ domain for integer variables

$DDint(v) \triangleq \; v \neq und \Rightarrow v \in Dint$

$DDbool(v) \triangleq \; v \neq bund \Rightarrow v \in Dbool$

properties to check

$SafePC \triangleq pc = \text{“halt”} \Rightarrow z = prime(x0) \land PrintT(z)$ the algorithm is partially correct

$SafeRTE \triangleq DDint(y) \land DDbool(z)$ the algorithm is runtime errors free.

$Safe \triangleq SafePC \land SafeRTE$