MODULE *pluscal_squareroot*

EXTENDS *Integers*, *TLC*

CONSTANTS x x is the input

-wfNext

```
--algorithm squareroot{
variables y1, y2, y3, z ;
{
l0: y1 := 0 ; y2 := 1 ; y3 := 1 ;
l1: while ( y2 ≤ x ) {
    l2: y1 := y1 + 1 ; y2 := y2 + y3 + 2 ; y3 := y3 + 2 ;
      } ;
l3:  z := y1 ;
l4: print ⟨x, z, y1, y2, y3⟩ ;
      }
  }
```

BEGIN TRANSLATION

CONSTANT *defaultInitValue*

VARIABLES $y1$, $y2$, $y3$, z, pc

$vars \triangleq \langle y1, y2, y3, z, pc \rangle$

$Init \triangleq$ Global variables
$\land y1 = defaultInitValue$
$\land y2 = defaultInitValue$
$\land y3 = defaultInitValue$
$\land z = defaultInitValue$
$\land pc = \text{“l0”}$

$l0 \triangleq \land pc = \text{“l0”}$
$\land y1' = 0$
$\land y2' = 1$
$\land y3' = 1$
$\land pc' = \text{“l1”}$
$\land z' = z$

$l1 \triangleq \land pc = \text{“l1”}$
$\land$ IF $y2 \leq x$
THEN $\land pc' = \text{“l2”}$
ELSE $\land pc' = \text{“l3”}$
$\land$ UNCHANGED $\langle y1, y2, y3, z \rangle$

$l2 \triangleq \land pc = \text{“l2”}$
$\land y1' = y1 + 1$
$\land y2' = y2 + y3 + 2$
$\land y3' = y3 + 2$

$\land\ pc' = \text{“l1”}$
$\land\ z' = z$

$l3 \triangleq \land\ pc = \text{“l3”}$
$\land\ z' = y1$
$\land\ pc' = \text{“l4”}$
$\land\ \text{UNCHANGED}\ \langle y1,\ y2,\ y3\rangle$

$l4 \triangleq \land\ pc = \text{“l4”}$
$\land\ PrintT(\langle x,\ z,\ y1,\ y2,\ y3\rangle)$
$\land\ pc' = \text{“Done”}$
$\land\ \text{UNCHANGED}\ \langle y1,\ y2,\ y3,\ z\rangle$

$Next \triangleq\ l0 \lor l1 \lor l2 \lor l3 \lor l4$
$\lor$ Disjunct to prevent deadlock on termination
$(pc = \text{“Done”} \land \text{UNCHANGED}\ vars)$

$Spec \triangleq\ Init \land \Box[Next]_{vars}$

$Termination \triangleq\ \Diamond(pc = \text{“Done”})$

END TRANSLATION

$MAX \triangleq\ 32768$ 16 bits
$D \triangleq\ 0\ldots 32768$
$x \leq 32760$

$Safety\_absence \triangleq\ \ (y1 \in D)\ \land (y2 \in D) \land (y3\ \in D) \land (z \in D)$

$i \triangleq$
$\land\ pc = \text{“l0”} \Rightarrow y1 \in D\ \land\ y2 \in D \land\ y3 \in D \land\ z \in D$
$\land\ pc = \text{“l1”} \Rightarrow y2 = (y1+1) * (y1+1) \land y3 = 2 * y1 + 1\ \land\ y1 * y1 \leq x \land Safety\_absence$
$\land\ pc = \text{“l2”} \Rightarrow y2 = (y1+1) * (y1+1) \land y3 = 2 * y1 + 1\ \land\ y1 * y1 \leq x \land y2 \leq x\ \land Safety\_absence$
$\land\ pc = \text{“l3”} \Rightarrow y2 = (y1+1) * (y1+1) \land y3 = 2 * y1 + 1\ \land\ y1 * y1 \leq x \land Safety\_absence$
$\land\ pc = \text{“l4”} \Rightarrow y2 = (y1+1) * (y1+1) \land y3 = 2 * y1 + 1\ \land\ y1 * y1 \leq x \land x < y2 \land Safety\_absence$
$\land\ pc = \text{“l5”} \Rightarrow y2 = (y1+1) * (y1+1) \land y3 = 2 * y1 + 1\ \land\ z * z \leq x \land x < (z+1) * (z+1) \land Safety\_$

$Safety\_partialcorrectness \triangleq\ pc = \text{“l5”} \Rightarrow \land\ y2\ \ \ = (y1\ \ \ + 1) * (y1 + 1)$
$\land\ y3 = 2 * y1 + 1$
$\land\ \ z * z \leq x \land x < (z+1) * (z+1)$