

THEOREM $\wedge Init \Rightarrow Inv$

$\wedge Inv \wedge Next \Rightarrow Inv'$

$\wedge Inv \Rightarrow Safe$

$\langle 1 \rangle 1. Init \Rightarrow Inv$

BY *MNPosInt* DEF *Init, Inv, TypeOK, GCDInv*

$\langle 1 \rangle 2. Inv \wedge Next \Rightarrow Inv'$

$\langle 2 \rangle 1. \text{SUFFICES ASSUME } Inv, Next$

PROVE Inv'

OBVIOUS

$\langle 2 \rangle 2. \text{CASE } y > x$

$\langle 3 \rangle 1. (y - x \in Nat \setminus \{0\}) \wedge \neg(x > y)$

BY $\langle 2 \rangle 1, \langle 2 \rangle 2, \text{SimpleArithmetic}$ DEF *Inv, TypeOK*

$\langle 3 \rangle 2. \text{QED}$

BY $\langle 2 \rangle 1, \langle 3 \rangle 1, \text{GCD3}$ DEF *Inv, TypeOK, GCDInv, Next*

$\langle 2 \rangle 3. \text{CASE } x > y$

$\langle 3 \rangle 1. (x - y \in Nat \setminus \{0\}) \wedge \neg(y > x)$

BY $\langle 2 \rangle 1, \langle 2 \rangle 3, \text{SimpleArithmetic}$ DEF *Inv, TypeOK*

$\langle 3 \rangle 2. \text{GCD}(y, x - y) = \text{GCD}(y, x)$

BY $\langle 2 \rangle 1, \langle 3 \rangle 1, \text{GCD3}$ DEF *Inv, TypeOK, Next*

$\langle 3 \rangle 3. \text{QED}$

BY $\langle 2 \rangle 1, \langle 3 \rangle 1, \langle 3 \rangle 2, \text{GCD2}$ DEF *Inv, TypeOK, GCDInv, Next*

$\langle 2 \rangle 4. \text{QED}$

BY $\langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3$ DEF *Next*

$\langle 1 \rangle 3. Inv \Rightarrow Safe$

BY *GCD1* DEF *Inv, Safe, TypeOK, GCDInv*

$\langle 1 \rangle 4. \text{QED}$

BY $\langle 1 \rangle 1, \langle 1 \rangle 2, \langle 1 \rangle 3$