THEOREM $\land\, Init \Rightarrow Inv$
$\land\, Inv \land Next \Rightarrow Inv'$
$\land\, Inv \Rightarrow Safe$

$\langle 1 \rangle 1$. $Init \Rightarrow Inv$
BY $MNPosInt$ DEF $Init$, Inv, $TypeOK$, $GCDInv$

$\langle 1 \rangle 2$. $Inv \land Next \Rightarrow Inv'$
$\langle 2 \rangle 1$. SUFFICES ASSUME Inv, $Next$
PROVE Inv'
OBVIOUS

$\langle 2 \rangle 2$. CASE $y > x$
$\langle 3 \rangle 1$. $(y - x \in Nat \setminus \{0\}) \;\land\; \neg(x > y)$
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $SimpleArithmetic$ DEF Inv, $TypeOK$
$\langle 3 \rangle 2$. QED
BY $\langle 2 \rangle 1$, $\langle 3 \rangle 1$, $GCD3$ DEF Inv, $TypeOK$, $GCDInv$, $Next$

$\langle 2 \rangle 3$. CASE $x > y$
$\langle 3 \rangle 1$. $(x - y \in Nat \setminus \{0\}) \;\land\; \neg(y > x)$
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 3$, $SimpleArithmetic$ DEF Inv, $TypeOK$
$\langle 3 \rangle 2$. $GCD(y, x - y) = GCD(y, x)$
BY $\langle 2 \rangle 1$, $\langle 3 \rangle 1$, $GCD3$ DEF Inv, $TypeOK$, $Next$
$\langle 3 \rangle 3$. QED
BY $\langle 2 \rangle 1$, $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $GCD2$ DEF Inv, $TypeOK$, $GCDInv$, $Next$

$\langle 2 \rangle 4$. 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, $Safe$, $TypeOK$, $GCDInv$

$\langle 1 \rangle 4$. QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$

CLOSE