

THEOREM *Induction* \triangleq $Inv \wedge Next \Rightarrow Inv'$

$\langle 1 \rangle 1$. SUFFICES ASSUME: 1. Inv
2. $Next$

PROVE: Inv'

PROOF: Obvious.

$\langle 1 \rangle 2$. CASE: $\wedge x > y$
 $\wedge x' = x - y$
 $\wedge y' = y$

$\langle 2 \rangle 1$. *TypeOK'*

PROOF: $\langle 1 \rangle 1.1$ and the definitions of Inv and $TypeOK$ imply that x and y are in $Nat \setminus \{0\}$. By case assumption $\langle 1 \rangle 2$, this implies that x' and y' are in $Nat \setminus \{0\}$, proving $\langle 2 \rangle 1$.

$\langle 2 \rangle 2$. *GCDInv'*

$\langle 3 \rangle 1$. $GCD(y', x') = GCD(y, x)$

PROOF: $\langle 1 \rangle 1.1$ and the definitions of Inv and $TypeOK$ imply that x and y are in $Nat \setminus \{0\}$, so $\langle 3 \rangle 1$ follows from case assumption $\langle 1 \rangle 2$ and GCD3 (substituting y for m and x for n).

$\langle 3 \rangle 2$. $GCD(x', y') = GCD(x, y)$

PROOF: $\langle 1 \rangle 1.1$, the definitions of Inv and $TypeOK$, and $\langle 2 \rangle 1$ imply that x , y , x' , and y' are in $Nat \setminus \{0\}$, so $\langle 3 \rangle 2$ follows from $\langle 3 \rangle 1$ and GCD2.

$\langle 3 \rangle 3$. Q.E.D.

PROOF: $\langle 3 \rangle 2$, $\langle 1 \rangle 1.1$, and the definitions of Inv and $GCDInv$ imply $\langle 2 \rangle 2$.

$\langle 2 \rangle 3$. Q.E.D.

PROOF: By $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, and definition of Inv .

$\langle 1 \rangle 3$. CASE: $\wedge y > x$
 $\wedge y' = y - x$
 $\wedge x' = x$

$\langle 2 \rangle 1$. *TypeOK'*

PROOF: $\langle 1 \rangle 1.1$ and the definitions of Inv and $TypeOK$ imply that x and y are in $Nat \setminus \{0\}$. By case assumption $\langle 1 \rangle 3$, this implies that x' and y' are in $Nat \setminus \{0\}$, proving $\langle 2 \rangle 1$.

$\langle 2 \rangle 2$. *GCDInv'*

$\langle 3 \rangle 1$. $GCD(x', y') = GCD(x, y)$

PROOF: $\langle 1 \rangle 1.1$ and the definitions of Inv and $TypeOK$ imply that x and y are in $Nat \setminus \{0\}$, so $\langle 3 \rangle 1$ follows from case assumption $\langle 1 \rangle 3$ and GCD3 (substituting x for m and y for n).

$\langle 3 \rangle 2$. Q.E.D.

PROOF: $\langle 3 \rangle 1$, $\langle 1 \rangle 1.1$, and the definitions of Inv and $GCDInv$ imply $\langle 2 \rangle 2$.

$\langle 2 \rangle 3$. Q.E.D.

PROOF: By $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, and definition of Inv .

$\langle 1 \rangle 4$. Q.E.D.

PROOF: By $\langle 1 \rangle 1.2$ and the definition of $Next$, the cases $\langle 1 \rangle 2$ and $\langle 1 \rangle 3$ are exhaustive.

[CLOSE](#)