MODULE *GCD*

EXTENDS *Integers*

$Divides(p, n) \triangleq \exists\, q \in Int : n = p * q$

$DivisorsOf(n) \triangleq \{p \in Int : Divides(p, n)\}$

$SetMax(S) \triangleq$ CHOOSE $i \in S : \forall\, j \in S : i \geq j$

$GCD(m, n) \triangleq SetMax(DivisorsOf(m) \cap DivisorsOf(n))$

THEOREM $GCD1 \triangleq \forall\, m \in Nat \setminus \{0\} : GCD(m, m) = m$

$\langle 1 \rangle$ SUFFICES ASSUME NEW $m \in Nat \setminus \{0\}$
PROVE $GCD(m, m) = m$
OBVIOUS

$\langle 1 \rangle 1.$ $Divides(m, m)$
BY DEF *Divides*

$\langle 1 \rangle 2.$ $\forall\, i \in Nat : Divides(i, m) \Rightarrow (i \leq m)$
BY DEF *Divides*

$\langle 1 \rangle 3.$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$ DEF *GCD*, *SetMax*, *DivisorsOf*

THEOREM $GCD2 \triangleq \forall\, m, n \in Nat \setminus \{0\} : GCD(m, n) = GCD(n, m)$
BY DEF *GCD*

THEOREM $GCD3 \triangleq \forall\, m, n \in Nat \setminus \{0\} :$
$(n > m) \Rightarrow (GCD(m, n) = GCD(m, n - m))$

$\langle 1 \rangle$ SUFFICES ASSUME NEW $m \in Nat \setminus \{0\}$, NEW $n \in Nat \setminus \{0\}$,
$n > m$
PROVE $GCD(m, n) = GCD(m, n - m)$
OBVIOUS

$\langle 1 \rangle$ $\forall\, i \in Int :$
$Divides(i, m) \land Divides(i, n) \equiv Divides(i, m) \land Divides(i, n - m)$
BY DEF *Divides*

$\langle 1 \rangle$ QED
BY DEF *GCD*, *SetMax*, *DivisorsOf*
