MODULE *gcd*

EXTENDS *Integers*, *TLAPS*

$Number \triangleq Nat \setminus \{0\}$

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

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

$SetMax(S) \triangleq \text{CHOOSE } i \in S : \forall j \in S : i \geq j$

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

LEMMA $Div \triangleq \forall m, n \in Number :$
$\quad \exists d \in Number :$
$\quad Divides(d, m)^{Divides}(d, n) \Rightarrow Divides(d, m + n)$

$\langle 1 \rangle$ SUFFICES ASSUME NEW $m \in Number$,
NEW $n \in Number$,
NEW $d \in Int$,
$Divides(d, m)$,
$Divides(d, n)$
PROVE $Divides(d, m)^{Divides}(d, n) \Rightarrow Divides(d, m + n)$

$\langle 1 \rangle 1.$ PICK $q \in Number : m = q * d$
BY DEF *Divides*

$\langle 1 \rangle$ QED

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*

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

THEOREM $GCD2 \triangleq \forall m, n \in Number : GCD(m, n) = GCD(n, m)$
BY DEF *GCD*, *SetMax*, *DivisorsOf*, *Divides*

THEOREM $GCD3 \triangleq \forall m, n \in Number : (n > m) \Rightarrow (GCD(m, n) = GCD(m, n - m))$

$\langle 1 \rangle$ SUFFICES ASSUME NEW $m \in Number$, NEW $n \in Number$,
$n > m$
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, $SetMax$, $DivisorsOf$, $Divides$

* Modification History

* Last modified Thu Nov 06 14:37:26 PST 2014 by $Chris.Nott$

* Created Thu Nov 06 12:18:54 PST 2014 by $Chris.Nott$