MODULE GCD

EXTENDS $Integers$

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

For integers p and n, equals TRUE iff p divides n – which I think is really neat; don't you?

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

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

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

$SetGCD(T) \triangleq SetMax(\{d \in Int : \forall t \in T : Divides(d, t)\})$

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

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

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

\ * Modification History
\ * Last modified *Wed Jun* 04 10:21:15 *CST* 2014 by *yaojingguo*
\ * Last modified *Tue Jun* 03 18:18:13 *CST* 2014 by *yaojingguo*
\ * Last modified Sat May 31 15:55:06 *CST* 2014 by *jing*
\ * Created Sat May 31 09:50:23 *CST* 2014 by *jing*