Module GCD

MODULE *GCD*

EXTENDS *Integers*, *FiniteSets*, *TLAPS*, *NaturalsInduction*

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

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

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

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

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

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

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

CLOSE