MODULE *Euclid*

EXTENDS *Integers*
CONSTANTS $M,\ N$

ASSUME $\land M \in Nat \setminus \{0\}$
$\land N \in Nat \setminus \{0\}$

VARIABLES $x,\ y$

$TypeOK \triangleq x \in Nat \setminus \{0\} \ \land \ y \in Nat \setminus \{0\}$

$Init \triangleq (x = M) \ \land \ (y = N)$

$$
\begin{array}{lll}
Next \triangleq & \lor & \land\, x > y \\
& & \land\, x' = x - y \\
& & \land\, y' = y \\
& \lor & \land\, y > x \\
& & \land\, y' = y - x \\
& & \land\, x' = x
\end{array}
$$

$Divides(p,\ n) \triangleq \exists\, q \in 0 \,..\, n : n = q * p$

$DivisorsOf(n) \triangleq \{p \in 0 \,..\, n : Divides(p,\ n)\}$

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

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

$GCDInv \triangleq GCD(x,\ y) = GCD(M,\ N)$

$Inv \triangleq TypeOK \land GCDInv$

CLOSE