─────────── MODULE *Euclid* ───────────

EXTENDS *Integers*
CONSTANTS M, N

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

VARIABLES x, y

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

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

$Next \triangleq \ \vee \ \wedge x > y$
$\wedge x' = x - y$
$\wedge y' = y$
$\vee \ \wedge y > x$
$\wedge y' = y - x$
$\wedge x' = x$

─────────────────────────────

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

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

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

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

─────────────────────────────

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

$Inv \triangleq TypeOK \wedge GCDInv$

─────────────────────────────