# Euclid's Algorithm

MODULE *Euclid*

EXTENDS *Integers*, *GCD*

CONSTANT $M$, $N$

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

```
**************************************************************************
--algorithm Euclid{
  variables x = M, y = N ;
  {  while ( x ≠ y ) { if ( x < y ) { y := y − x }
                       else         { x := x − y }
                     }
   }
 }
**************************************************************************
```

$PartialCorrectness \triangleq$
$(pc = \text{“Done”}) \Rightarrow (x = y) \land (x = GCD(M, N))$

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

$Inv \triangleq \land TypeOK$
$\land GCD(x, y) = GCD(M, N)$
$\land (pc = \text{“Done”}) \Rightarrow (x = y)$

CLOSE