

# Euclid's Algorithm

MODULE *Euclid*

EXTENDS *Integers*, *GCD*

CONSTANT  $M, N$

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

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

$\text{PartialCorrectness} \triangleq$   
 $(pc = \text{"Done"}) \Rightarrow (x = y) \wedge (x = \text{GCD}(M, N))$

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

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