```
1  ---------- MODULE Euclid ----------
2  EXTENDS Integers, TLAPS
3  ----------------------------------
4  p | q ≜ ∃ d ∈ 1 .. q : q = p * d
5  Divisors(q) ≜ {d ∈ 1 .. q : d | q}
6  Maximum(S) ≜ CHOOSE x ∈ S : ∀ y ∈ S : x ≥ y
7  GCD(p, q) ≜ Maximum(Divisors(p) ∩ Divisors(q))
8  Number ≜ Nat \ {0}
9  ----------------------------------
10 CONSTANTS M, N
11 VARIABLES x, y
12
13 ASSUME NumberAssumption ≜ M ∈ Number ∧ N ∈ Number
14 ----------------------------------
15 Init ≜ (x = M) ∧ (y = N)
16
17 Next ≜ ∨ ∧ x < y
18        ∧ y' = y - x
19        ∧ x' = x
20      ∨ ∧ y < x
21        ∧ x' = x - y
22        ∧ y' = y
23
24 Spec ≜ Init ∧ □[Next]⟨x, y⟩
25 ----------------------------------
26 ResultCorrect ≜ (x = y) ⇒ x = GCD(M, N)
27
28 InductiveInvariant ≜
29    ∧ x ∈ Number
30    ∧ y ∈ Number
31    ∧ GCD(x, y) = GCD(M, N)
32 ----------------------------------
33 USE DEF Number
34
35 THEOREM InitProperty ≜ Init ⇒ InductiveInvariant
36   BY NumberAssumption DEF Init, InductiveInvariant
37 ----------------------------------
38 AXIOM GCDProperty1 ≜ ∀ p ∈ Number : GCD(p, p) = p
39 AXIOM GCDProperty2 ≜ ∀ p, q ∈ Number : GCD(p, q) = GCD(q, p)
40 AXIOM GCDProperty3 ≜ ∀ p, q ∈ Number : (p < q) ⇒ GCD(p, q) = GCD(p, q - p)
41 ----------------------------------
42 THEOREM NextProperty ≜ InductiveInvariant ∧ Next ⇒ InductiveInvariant'
43 ⟨1⟩ SUFFICES ASSUME InductiveInvariant, Next
44              PROVE InductiveInvariant'
45   OBVIOUS
46 ⟨1⟩ USE DEF InductiveInvariant, Next
```

47 $\langle 1\rangle 1.\ (x < y) \lor (y < x)$
48 OBVIOUS
49 $\langle 1\rangle$a.CASE $x < y$
50 $\langle 2\rangle 1.\ (y - x \in \mathit{Number}) \land \neg(y < x)$
51 BY $\langle 1\rangle$a, *SMT* DEF *Number*
52 $\langle 2\rangle 2.$ QED
53 BY $\langle 1\rangle$a, $\langle 2\rangle 1$, *GCDProperty*3
54 $\langle 1\rangle$b.CASE $y < x$
55 $\langle 2\rangle 1.\ (x - y \in \mathit{Number}) \land \neg(x < y)$
56 BY $\langle 1\rangle$b, *SMT* DEF *Number*
57 $\langle 2\rangle 2.\ \mathit{GCD}(y', x') = \mathit{GCD}(y, x)$
58 BY $\langle 1\rangle$b, $\langle 2\rangle 1$, *GCDProperty*3
59 $\langle 2\rangle 4.$ QED
60 BY $\langle 1\rangle$b, $\langle 2\rangle 1$, $\langle 2\rangle 2$, *GCDProperty*2
61 $\langle 1\rangle$ QED
62 BY $\langle 1\rangle 1$, $\langle 1\rangle$a, $\langle 1\rangle$b
63 ├──┤
64 THEOREM $\mathit{Correctness} \triangleq \mathit{Spec} \Rightarrow \Box\mathit{ResultCorrect}$
65 $\langle 1\rangle 1\ \mathit{InductiveInvariant} \land$ UNCHANGED $\langle x, y\rangle \Rightarrow \mathit{InductiveInvariant}'$
66 BY DEF *InductiveInvariant*
67 $\langle 1\rangle 2\ \mathit{Spec} \Rightarrow \Box\mathit{InductiveInvariant}$
68 BY *PTL*, *InitProperty*, *NextProperty*, $\langle 1\rangle 1$ DEF *Spec*
69 $\langle 1\rangle 3\ \mathit{InductiveInvariant} \Rightarrow \mathit{ResultCorrect}$
70 BY *GCDProperty*1 DEF *InductiveInvariant*, *ResultCorrect*
71 $\langle 1\rangle$ QED
72 BY *PTL*, $\langle 1\rangle 2$, $\langle 1\rangle 3$
73 └──┘