Problem 1 (10 Points)

We use the $gcd$ algorithm from your last homework to demonstrate the use of axiomatic semantics.

Algorithm 1

Input: Two integers $M$ and $N$

Output: An integer $r$ such that $r = gcd(M, N)$

1. $a \leftarrow M$
2. $b \leftarrow N$
3. $t \leftarrow 0$
4. while $a \mod b \neq 0$ do
   5. \hspace{1em} $t \leftarrow a$
   6. \hspace{1em} $a \leftarrow b$
   7. \hspace{1em} $b \leftarrow t \mod b$
5. end while
6. $r \leftarrow b$

a) Find a loop invariant that is strong enough to prove the correctness of the program.

b) Use Hoare logic to prove $\{true\} \ P \{r = gcd(N,M)\}$