Exercise: Function exp() is defined as
exp(*M*,0) = 1,
exp(*M*,*N*) = *Mexp(*M*, *N*-1).**
Write a program to compute exp(*M*,*N*) according to the definition.
Prove that the program computes M^N, if *M*, *N* are natural numbers

To solve the exercise you have to

- write a program
- formalize the specification as a pre- and post-condition
- find the loop invariant and annotate the program
- apply the rules to show that the program meets specification
- prove the verification conditions using predicate calculus and arithmetic

Program:

```
{N>0 ∧ N=n}                        % ≡ Pre
Z:=1  { Pre ∧ Z=1}                 % annotation
WHILE N>0 DO
  {N ≥ 0 ∧ Z * M^N = M^n}          % ≡ Inv
  BEGIN
    Z := Z * M;
    N := N - 1;
  END;
{Z= M^n}                           % ≡ Post
```

C1 C2 C3

Proof:

$$\dfrac{\dfrac{\dfrac{④}{N>0 \land Inv \Rightarrow N-1 \geq 0 \land Z * M * M^{N-1} = M^n}}{\{N>0 \land Inv\}\ Z:=Z*M\ \{N-1 \geq 0 \land Z * M^{N-1} = M^n\}}\ (:=)}{\{N>0 \land Inv\}\ Z := Z * M;\ N := N-1\ \{Inv\}}\ (:=\ ;\ :=)$$

$$\dfrac{\{N>0 \land Inv\}\ Z := Z * M;\ N := N-1\ \{Inv\}}{\{N>0 \land Inv\}\ C3\ \{Inv\}}\ (bl)$$

$$\dfrac{\dfrac{①}{Pre \Rightarrow Pre \land 1=1}}{\{Pre\}\ Z:=1\ \{Pre \land Z=1\}}\ (:=)$$

$$\dfrac{\dfrac{②}{Pre \land Z=1 \Rightarrow Inv} \qquad \{N>0 \land Inv\}\ C3\ \{Inv\} \qquad \dfrac{③}{Inv \land \neg(N>0) \Rightarrow Post}}{\{Pre \land z=1\}\ C2\ \{Post\}}\ (while)$$

$$\dfrac{\{Pre\}\ Z:=1\ \{Pre \land Z=1\} \qquad \{Pre \land z=1\}\ C2\ \{Post\}}{\{Pre\}\ C1\ \{Post\}}\ (;)$$

Prove ①-④ using predicate calculus and arithmetic:

① is trivially true

② $Pre \land Z=1 \Rightarrow Inv$

$N>0 \land N=n \land Z=1 \Rightarrow N \geq 0 \land Z * M^N = M^n$	[rewrite *Pre*, *Inv*]
$N>0 \Rightarrow N \geq 0$	[arithm]
$N=n \land Z=1 \Rightarrow 1 * M^n = M^n$	[rewrite Z, N; arithm]

③

$N \geq 0 \land Z * M^N = M^n \land \neg(N>0) \Rightarrow Z= M^n$	[rewrite *Inv*, *Post*]
$N \geq 0 \land \neg(N>0) \Rightarrow N = 0$	[arithm]
$Z * M^0 = M^n \Rightarrow Z= M^n$	[rewrite N=0; arithm]

④

$N>0 \Rightarrow N-1 \geq 0$	[arithm]
$Z * M^N = M^n \Rightarrow Z * M * M^{N-1} = M^n$	[rewrite *Inv*, simplify]
$Z * M^N = M^n \Rightarrow Z * M^N = M^n$	[arithm]