

Exercise: Function $\text{exp}()$ is defined as

$$\text{exp}(M, 0) = 1,$$

$$\text{exp}(M, N) = M * \text{exp}(M, N-1).$$

Write a program to compute $\text{exp}(M, N)$ 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

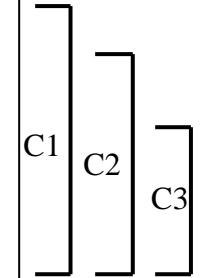
Proof:

Program:

```

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

```



④

$$N > 0 \wedge \text{Inv} \Rightarrow N - 1 \geq 0 \wedge Z * M * M^{N-1} = M^n$$

$$\frac{}{\{N > 0 \wedge \text{Inv}\} Z := Z * M \{N - 1 \geq 0 \wedge Z * M^{N-1} = M^n\}} \quad (:=)$$

$$\frac{}{\{N > 0 \wedge \text{Inv}\} Z := Z * M; N := N - 1 \{ \text{Inv} \}} \quad (:= ; :=)$$

③

$$\frac{}{\text{Inv} \wedge \neg(N > 0) \Rightarrow \text{Post}} \quad (\text{bl})$$

$$\frac{}{\{Pre \wedge z=1\} C2 \{ \text{Post} \}} \quad (\text{while})$$

(;)

$$\{Pre\} C1 \{ \text{Post} \}$$

Prove ①-④ using predicate calculus and arithmetic:

① is trivially true

② $Pre \wedge Z=1 \Rightarrow \text{Inv}$

$$N > 0 \wedge N=n \wedge Z=1 \Rightarrow N \geq 0 \wedge Z * M^N = M^n$$

$$N > 0 \Rightarrow N \geq 0$$

$$N=n \wedge Z=1 \Rightarrow 1 * M^n = M^n$$

[rewrite Pre, Inv]

[arithm]

[rewrite Z, N ; arithm]

③

$$N \geq 0 \wedge Z * M^N = M^n \wedge \neg(N > 0) \Rightarrow Z = M^n$$

$$N \geq 0 \wedge \neg(N > 0) \Rightarrow N = 0$$

$$Z * M^0 = M^n \Rightarrow Z = M^n$$

[rewrite Inv, Post]

[arithm]

[rewrite $N=0$; arithm]

④

$$N > 0 \Rightarrow N - 1 \geq 0$$

$$Z * M^N = M^n \Rightarrow Z * M * M^{N-1} = M^n$$

$$Z * M^N = M^n \Rightarrow Z * M^N = M^n$$

[arithm]

[rewrite Inv , simplify]

[arithm]