a,b) $\{m \in Z \wedge n \in Z\}$ -> precondition

$K := m$

$P := n$

$Y := 1$

$\{K = m, P = n, Y = 1\}$ -> annotation 1

while $K > 0$ do

$\{Y P^K = x^m, K \geq 0\}$ -> annotation 2.

If $k \bmod 2 = 0$ then

$P := P \times P$

$K := K/2$

Else:

$Y := Y \times P$

$K := K - 1$

FI

od

$\{Y = x^m\}$ ->Postcondition

c) now for the verification condition

$$\{P\} \quad V := E \quad \{Q\}$$

$$P \rightarrow \quad Q[E/V]$$

it implies:

$$\{ m \in Z, n \in Z \} \qquad \{ k = n, P = x, y = 1 \}$$

thus:

$$\boxed{\{ m \in Z, x \in Z \} \rightarrow \{ n = n, x = x, 1 = 1 \}} \quad 1$$

For the while condition now

$P \rightarrow R$ where

$$\{P\} = \{ k = n, p = x, y = 1 \}$$

$$\{R\} = \{ y * p^k = x^n, k \geq 0 \}$$

thus:

$$\boxed{\{ k = n, P = x, y = 1 \} \rightarrow \{ 1 \times x^n = x^n, n \geq 0 \}} \quad 2$$

$(R \wedge \neg S) \rightarrow Q$ where

$\{R\} = \{y \times p^k = x^m, k \geq 0\}$

$\{S\} = k > 0$

$$\boxed{\{y \times p^k = x^m, k \geq 0, k \leq 0\} \rightarrow \{y = x^m\}}$$ 3

add condition for

$\{R \wedge S\}\ C\ \{R\}$

Here C is the if Else statement from line 5 - 11

$\{R \wedge S\} = \{y \times p^k = x^m, k \geq 0, k > 0\} \rightarrow P$

Poscondition:

$\{y \times p^k = x^m, k \geq 0\} \rightarrow Q$

→ now we encouter another if condition:

→ the first one:

$\{x \times p^k = x^m, k \geq 0, k > 0, (k \bmod 2 = 0)\}$

$$\boxed{\rightarrow \{k/2 \geq 0 ; y \times (p \times p)^{k/2} = x^m\}}$$ 4

Second statement:

$\{ y * p^k = x^n,\ k \geq 0,\ k > 0 \wedge k \bmod 2 = 1 \}$

$\rightarrow \boxed{\{ k-1 \geq 0,\ (y * p) * (p)^{(k-1)} = x^n \}}$ 5

d.) now we need to prove the conditions $1 \rightarrow 5$

1). $\{ n \in \mathbb{Z},\ x \in \mathbb{Z} \} \rightarrow \{ n = n,\ x = x,\ 1 = 1 \}$

this is clearly true because $n, x \in \mathbb{Z}$
and the outcome is also true.

2.) $\{ k = n,\ p = x,\ y = 1 \} \rightarrow \{ 1 \times x^n = x^n,\ n \geq 0$

$\rightarrow\ 1 \times x^n = x^n$

$x^n = x^n$

$\rightarrow$ n is derived from k and $k \geq 0$ so

$n \geq 0$

proved.

3.) $\{ y \times p^k = x^n,\ k \geq 0,\ k \leq 0 \} \rightarrow \{ y = x^n \}$

$k \leq 0$ and $k \geq 0 \Rightarrow k = 0$ so

$y \times p^k = x^n$

$y = x^n$ proved

4) $\{k \geq 0,\ y \times p^k = x^n,\ k>0,\ (k \bmod 2 = 0)\}$

$\rightarrow$

$\{k/2 \geq 0,\ y \times (p \times p)^{k/2} = x^n\}$

$\rightarrow$ $k \geq 0$ divisble by 2 on boths

$k/2 \geq 0$

$\rightarrow$ $y \times (p \times p)^{k/2} = x^n$

$y \times p^k = x^n$ proved

5)

$k>0,\ k \geq 0$ $k \bmod 2 = 1$

so $k = 1$,

$1 - 1 = 0$

$0 \geq 0$ true

$y \times p^k = x^n$

$y \times p^{k-1} \times p^1 = x^n$ proved e.) for total correctness we don't have to do anything for assignment and if - else condition statements; the partial correctness is sufficient

For the while loop we however need to add that it terminates:

E [k] added in the beggining of file

[k] added after the loop

ALL other conditions are set b followed through from partial correctness.