Problem Sheet 3

Problem 3.1

Solution:

a,b)

```
Precondition: {X = x AND N = n AND N >= 0}
    K:=N
    P:=X
    Y:=1
    WHILE K > 0 DO
        IF (K%2) = 0 THEN
            P:=P*P
            K:=K/2
        ELSE
            Y:=Y*P
            K:=K-1
        FI
    OD
Postcondition: {Y = x^n}
```

c)

```
Precondition: {X = x AND N = n AND N >= 0}
    K:=N
    P:=X
    Y:=1
    {K = N AND P = X AND Y = 1}
    WHILE K > 0 DO
    {Y*P^K = x^n}
        IF (K%2) = 0 THEN
            P:=P*P
            K:=K/2
        ELSE
            Y:=Y*P
            K:=K-1
        FI
    OD
Postcondition: {Y = x^n}
```

d)

```
1st condition:
{X = x AND N = n AND N >= 0}K:=N;P:=X;Y:=1;{K = N AND P = X AND Y = 1}
{X = x AND N = n AND N >= 0}K:=N;P:=X;{K = N AND P = X AND 1 = 1}
{X = x AND N = n AND N >= 0}K:=N;{K = N AND X = X AND 1 = 1}
{X = x AND N = n AND N >= 0}{N = N AND X = X AND 1 = 1}

while loop:
{K = N AND X = X AND Y = 1}->{Y*P^K = x^n}
{Y*P^K = x^n AND NOT (K > 0)}->{Y = x^n}

{Y*P^K = x^n AND (K > 0)}IF (K%2) = 0 THEN P:=P*P;K:=K/2; ELSE Y:=Y*P;K:=K-1;FI {Y*P^K = x

Decompose IF
{Y*P^K = x^n AND (K > 0) AND (K%2) = 0}P:=P*P;K:=K/2;{Y*P^K = x^n}
{Y*P^K = x^n AND (K > 0) AND (K%2) != 0}Y:=Y*P;K:=K-1;{Y*P^K = x^n}
```

```
Simplify Then branch
{Y*P^K = x^n AND (K > 0) AND (K%2) = 0}P:=P*P;K:=K/2;{Y*P^K = x^n}
{Y*P^K = x^n AND (K > 0) AND (K%2) = 0}P:=P*P;{Y*P^(K/2) = x^n}
=
{Y*P^K = x^n AND (K > 0) AND (K%2) = 0}->{Y*(P*P)^(K/2) = x^n}

Simplify Else branch
{Y*P^K = x^n AND (K > 0) AND (K%2) != 0}Y:=Y*P;K:=K-1;{Y*P^K = x^n}
=
{Y*P^K = x^n AND (K > 0) AND (K%2) != 0}{Y*P*P^(K-1) = x^n}
```

e)

```
{X = x AND N = n AND N >= 0}{N = N AND X = X AND 1 = 1} => (tautology)
{X = x AND N = n AND N >= 0}{1}Proved.

{K = N AND P = X AND Y = 1}->{Y*P^K = x^n} => (Since Y=1)
{K = N AND P = X AND Y = 1}->{P^K = x^n} => (Since K=N, P=X)
{K = N AND X = X AND Y = 1}->{X^N = x^n}=> (Since X=x, N=n)
{K = N AND X = X AND Y = 1}->{X^N = X^N} Proved.

{Y*P^K = x^n AND NOT (K > 0)}->{Y = x^n} => (If NOT K > 0, then k = 0, since only two chan
{Y*P^0 = x^n AND NOT (0 > 0)}->{Y = x^n} => (NOT (0>0) evaluates to 1, P^0 = 1)
=>
{Y*1 = x^n}->{Y = x^n} Proved.

{Y*P^K = x^n AND (K > 0) AND (K%2) = 0}->{Y*(P*P)^(K/2) = x^n} =>
Y*P^K = Y*P*P^(K/2) (prove this, since everything else is not contradicting or in question
P^K = P*P^(K/2) => P^K = (P^2)^(K/2) => P^K = (P)^(2*K/2) => P^K = P^K. Proved.

{Y*P^K = x^n AND (K > 0) AND (K%2) != 0}{Y*P*P^(K-1) = x^n}
Y*P^K = Y*P*P^(K-1) => P^K = P*P^(K-1) = > P^K = P^K Proved.
```

f)

```
Precondition: {X = x AND N = n AND N >= 0}
    K:=N
    P:=X
    Y:=1
    {K = N AND P = X AND Y = 1}
    WHILE K > 0 DO
    {Y*P^K = x^n}
    [K]
        IF (K%2) = 0 THEN
            P:=P*P
            K:=K/2
        ELSE
            Y:=Y*P
            K:=K-1
        FI
    OD
Postcondition: {Y = x^n}
```

g)

```
Conditions from before:
    {X = x AND N = n AND N >= 0}{N = N AND X = X AND 1 = 1}

    while loop:
    {K = N AND X = X AND Y = 1}->{Y*P^K = x^n}
    {Y*P^K = x^n AND NOT (K > 0)}->{Y = x^n}


We need to add new rules for while loop:
{Y*P^K = x^n AND (K > 0)}->K>=0
```

```
{Y*P^K = x^n AND (K > 0) AND (K = n2)}IF (K%2) = 0 THEN P:=P*P;K:=K/2; ELSE Y:=Y*P;K:=K-1;

Decompose IF
{Y*P^K = x^n AND (K > 0) AND (K = n2) AND (K%2) = 0}P:=P*P;K:=K/2;{Y*P^K = x^n AND (K<n2)}
{Y*P^K = x^n AND (K > 0) AND (K = n2) AND (K%2) != 0}Y:=Y*P;K:=K-1;{Y*P^K = x^n AND (K<n2)

Simplify Then branch
{Y*P^K = x^n AND (K > 0) AND (K%2) = 0 AND (K = n2)}P:=P*P;K:=K/2;{Y*P^K = x^n AND (K<n2)}
{Y*P^K = x^n AND (K > 0) AND (K%2) = 0 AND (K = n2)}P:=P*P;{Y*P^(K/2) = x^n AND (K/2<n2)}
=
{Y*P^K = x^n AND (K > 0) AND (K%2) = 0 AND (K = n2)}->{Y*(P*P)^(K/2) = x^n AND (K/2<n2)}

Simplify Else branch
{Y*P^K = x^n AND (K > 0) AND (K%2) != 0  AND (K = n2)}Y:=Y*P;K:=K-1;{Y*P^K = x^n}
=
{Y*P^K = x^n AND (K > 0) AND (K%2) != 0  AND (K = n2)}{Y*P*P^(K-1) = x^n AND (K-1<n2)}
```

h)

```
Proofs for first 3 conditions are same as before.

{Y*P^K = x^n AND (K > 0)}->K>=0 - If K>0 then K>=0. Proved

{Y*P^K = x^n AND (K > 0) AND (K%2) = 0 AND (K = n2)}->{Y*(P*P)^(K/2) = x^n AND (K/2<n2)}.
Prove only (K = n2) -> (K/2<n2) since other parts are already proven.
(K = n2 ) -> (n2/2<n2) -> 1/2 <2. Proved.

{Y*P^K = x^n AND (K > 0) AND (K%2) != 0  AND (K = n2)}{Y*P*P^(K-1) = x^n AND (K-1<n2)}
Prove only (K = n2) -> (K-1<n2) since other parts are already proven.
(K = n2 ) -> (n2-1<n2) -> -1 <0. Proved.
```