SHEET 12

a) Precondition → $\{n \in Z \wedge x \in Z\}$

Postcondition → $\{Y = x^n\}$

b) Precondition : $\{n \in Z \wedge x \in Z\}$

```
K := n
P := x
Y := 1
```

$\{K = n,\ P = x,\ Y = 1\}$ → Annotation 1

```
while K > 0 do
```

$\{Y \times P^K = x^n,\ K \geq 0\}$ → Annotation 2

```
    if K mod 2 = 0 then
            P := P × P
            K : K/2
    else
            Y := Y × P
            K := K - 1
    fi
od
```

Postcondition : $\{ Y = x^n \}$

c) Verification conditions

For assignments

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

$P \Rightarrow Q \{E/V\}$

this implies to:

$\{n \in Z \wedge x \in Z\}$

$K := n$

$P := x$

$Y := 1$

$\{k = n, \; P = x, \; Y = 1\}$

which results to

$\{n \in Z \wedge x \in Z\} \quad \{n = n, x = x, 1 = 1\}$

For the while loop condition

P R where

$\{P\} = \{K = n, P = x, Y = 1\}$

$\{R\} = \{Y \times P^K = x^n, K \geq 0\}$

this results to:

$$\{K = n \;,\; P = x \;,\; Y = 1\} \rightarrow \{1 \times x^n = x^n,\; n \geq 0\}$$

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

$\{R\} = \{Y \times P^K = x^n,\; K \geq 0\}$

$\{S\} = K > 0$

this results to:

$$\{Y \times P^K = x^n,\; K \geq 0,\; K \leq 0\} \rightarrow \{Y = x^n\}$$

Add conditions from $\{R \wedge S\}\; C\{R\}$

C is the if-else statement

So:

$$\{R \wedge S\} = \{Y \times P^K = x^n,\; K \geq 0,\; K > 0\}$$

↳ P

→ This is a precondition now

$$\{R\} = \{Y \times P^K = x^n,\; K \geq 0\}$$

↳ Q

→ This is a postcondition now

We bump into another if condition now

- $\{P \wedge S\}\ C_1\ \{Q\}$

$\{Y \times P^K = X^n,\ K \geq 0,\ K > 0,\ (K \bmod 2 = 0)\}$

$P := P \times P$

$K := K/2$

Do the assignment too:

$\{Y \times P^K = X^n,\ K \geq 0,\ K > 0,\ (K \bmod 2 = 0)\}$

$\{\frac{K}{2} \geq 0,\ Y \times (P \times P)^{K/2} = X^n\}$

- $\{P \wedge \neg S\}\ C_2\ \{Q\}$

$\{Y \times P^K = X^n,\ K \geq 0,\ K > 0,\ K \bmod 2 = 1\}$

$Y := Y \times P$

$K := K - 1$

$\{K - 1 \geq 0,\ Y \times P \times P^{K-1} = X^n\}$

d) Proving the partial correctness verification conditions

- $\{n \in Z \wedge x \in Z\} \rightarrow \{n = n, x = x, 1 = 1\}$

This is true as n and x are both integers and the outcome is also true

- $\{K = n, P = x, y = 1\} \rightarrow \{1 \times x^n = x^n, n \geq 0\}$

We have : $1 \times x^n = x^n$

so : $x^n = x^n$

$n \geq 0 \rightarrow n$ is derived from K, as $K > 0$, n also satisfies this

- $\{y \times P^K = x^n, k \geq 0, k \leq 0\} \rightarrow \{y = x^n\}$

We have : $k \geq 0$ and $K \leq 0$

so $K = 0$ is the only thing that satisfies this

$$y \times P^K = x^n$$

$$y \times P^0 = x^n$$

$$y = x^n$$

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

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

$k \geq 0 \xrightarrow{\text{divide by 2}} \frac{k}{2} \geq 0$

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

$y \times p^{k/2 + k/2} = x^n$

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

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

$\{k - 1 \geq 0,\ y \times p \times p^{k-1} = x^n\}$

We have: $k \geq 0$

$k > 0$

$k \bmod 2 = 1$

so we can say $k = 1$

$k - 1 \geq 0$

$1 - 1 \geq 0$

$0 \geq 0$ → this is true

Also:

$$y \times p \times p^{k-1} = x^n$$

$$y \times p^{1+k-1} = x^n$$

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

e) We need to put an additional annotation to show that the while loop is terminating

K is the variable of the loop:

$E = [K]$ → put in the beginning

$[K]$ → put after the loop

f) Updating verification conditions

$P \rightarrow R$ (shown before)

$R \wedge \neg S \rightarrow Q$ (shown before)

$R \wedge S \quad E \geq 0$

$\{ y \times p^k = x^n, K \geq 0, K > 0 \} \rightarrow E \geq 0$

$\rightarrow K \geq 0$

The precondition and the postcondition change for the if-else statement:

$$\{R \wedge S \wedge (E = m)\} = y \times p^k = x^n$$

$$k \geq 0,\ k > 0,\ k = m\}$$

$$\downarrow$$

precondition

$$\{R \wedge (E < m)\} = \{y \times p^k = x^n,\ k \geq 0,\ k < m\}$$

$$\downarrow$$

postcondition

- $\{P \wedge S\}\ C_1\ \{Q\}$

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

$$p := p \times p$$

$$k := k/2$$

$$\left\{\frac{k}{2} \geq 0,\ y \times (p \times p)^{k/2} = x^n,\ \frac{k}{2} < m\right\}$$