Mahiem Agrawal
Sheet 12.

a, b) $\{n \in Z \wedge x \in Z\}$ → Pre condition

```
1   k := n
2   P := x
3   y := 1
4   {k = n, P = x, y = 1} → Annotation 1.
4   while k > 0 do
6     {y * P^k = x^n, k ≥ 0} → Annotation 2
5     If k MOD 2 = 0 then
6       P := P x P
7       k := k/2
8     ELSE
9       y := y x P
10      k := k - 1
11    fi
12  od.
```

$\{y = x^n\}$ → Post condition.

c) Now for the verification condition.

For assignments.

Formula

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

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

This implies to.

$\{n \in \mathbb{Z}, x \in \mathbb{Z}\}$ lines 1,2,3 $\{K=n, P=x, y=1\}$

which results to

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

For the while condition now.

$P \rightarrow R$ where.

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

$\{R\} = \{Y * p^K = x^n, K \geq 0\}$

which resol

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

→ (2)

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

$\{R\} = \{Y * p^K = x^n, K \geq 0\}$

$\{S\} = K > 0$

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

→ (3)

Add conditions from

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

∴ ~~no~~

Here C is the if-else statement from line 5-11.

So,

R ~~would be that of prev~~

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

$\{R\} =$ ~~$\{R\}$~~

This is precondition now.

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

This is post condition. → Q //

Now we encounter another if condition.

← First one

$\{P \wedge S\}\ C_1\ \{Q\}$ so,

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

~~Lines~~

$P = P * P$

$K = K/2$

~~$\{Y \times (P \times P)^{K/2}, K/2 = 0\}$~~

~~which is~~

Doing the assignment as well

$\{K \geq 0, Y * P^K = n, K > 0, (K \text{ MOD } 2 = 0)$

$\longrightarrow$

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

(4)

Second statement

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

$\{Y * P^K = x^n, K \geq 0, K > 0 \wedge K \text{ MOD } 2 = 1\}$

$Y = Y * P$

$K = K - 1$

Now the out come would be

$\{K - 1 \geq 0, (Y * P) * (P)^{K-1} = x^n\}$

(5)

∴ Theese are all conditions needed for partial correctness

a) Now we need to prove our condition so

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

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

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

$1 * x^n = x^n$

$x^n = x^n$ // proved.

$n \geq 0$

and as n is derived from k and $k \geq 0$ n also satisfies this.

proved //

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

We know from condition $k \geq 0$ and $k \leq 0$ and only thing satisfied this is when $k = 0$ so.

$y * p^k = x^n$

$= x * p^0$ $y * p^0 = x^n$

$y = x^n$ // proved.

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

$\longrightarrow$

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

$k \geq 0$ now dividing by 2 in both sides

$k/2 \geq 0$ // proved

Other than that $k > 0, k \geq 0$ and $k \bmod 2 = 0$ which can be ~~easily prove~~ seen as our answer to also satisfy.

$y * (p * p)^{k/2} = x^n$

$y * p^{2 * k/2} = x^n$

$y * p^k = x^n$ // proved.

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

$\longrightarrow$

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

~~Even when k=0~~

~~k=~~ ~~From this~~

From this we can know
$k > 0$ & $k \geq 0$ and $k \bmod 2 = 1$

So we can ~~or nan~~ odd numbers greater than 1.

So, $k = 1$.

$1 - 1 \geq 0$

$0 \geq 0$ (True).

$Y * p^k = x^n$

$Y * p^{k-1+1} = x^n$

$Y * p^{k-1} * p^1 = x^n$ // proved.

c) For total correctness we dont have to anything for assignment and if-else condition statements the partial correctness is sufficient.
The
Now for the while loop we however need to add ~~an~~ that it is terminating so.

we know by this K is the looping variant so,

E=[K] added in the beggining of file.

and.

[k] added after the while loop.

All other conditions are set be followed through from partial correctness.

f) Updating verification condition for while condition as that only changes.

P → R (already placed)

R ∧ ¬S → Q (already proved)

R ∧ S → E ≥ 0 now

↓

(K ≥ 0), (∀ x P^K = x^n), (K > 0) → E ≥ 0

→ K ≥ 0 //

→ (6)

Now we also need to add condition for

Again, for the if condition the precondition and post-condition changes.

$\{R \wedge S \wedge (E=m)\}$

$= \{(K \geq 0), Y * P^K = x^n, K > 0, K = m\}$

→ precondition.

$\{R \wedge (E < m\}$ → post condition.

$= \{K \geq 0, Y * P^K = x^n, K < m\}$.

Now we go to the while loop.

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

$\{K \geq 0, Y * P^K = x^n, K > 0, K = m, K \bmod 2 = 0\}$

$P = P \times P$

$K = K/2$

which resolves in.

$\{K/2 \geq 0, Y * (P*P)^{K/2} = x^n; K/2 < m\}$

→ (7)

$\{P \wedge 7\}\ C_2\ \{\Theta\}$.

So,

$\{(K \geq 0,\ X * P^K = x^n,\ K > 0,\ K = m\}$

$Y = Y * P$

$K = K - 1$,

which leads to

$\underline{(X * P \times P^{K-1} = x^n,\ (K-1) < m\}}$

(8)

g) Now proving all of them.

6) $\{(K \geq 0),\ X * P^K = x^n,\ K > 0) \rightarrow K \geq 0$

This is very simple as the conditions on the left satisfy them of the right.

7) $\{K \geq 0,\ X * P^K = x^n,\ K > 0,\ K = m,\ K \bmod 2 = 0\}$

$\rightarrow$

$\{K/2 \geq 0,\ Y * (P * P)^{K/2} = x^n,\ K/2 < m\}$

We have already proved for

$k/2 \geq 0$ and $x*(p*p)^{k/2} = x^n$ in

partial correctness. So for

$k/2 < m$

replacing $k = m$.

$\frac{m}{2} < m$ which ~~has to be~~ is true logically

$m/2 < m$ // proved.

8) ~~$\{x*p*p^{k-1} = x^n, (k-1) < m$~~

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

$\longrightarrow (y*p*p^{k-1} = x^n, (k-1) < m\}$

we have already proved
$y*p*p^{k-1} = x^n$ so,

$k-1 < m$ replacing k by m

$m-1 < m$ logically true so

$m-1 < m$ // proved. Finally done //