Ejercicios Practico 6

1)

a)

$$wp.(x := x + y).(x = 6 \wedge y = 5)$$
$$\equiv \{\text{Def de wp para ":="}\}$$
$$(x = 6 \wedge y = 5)(x \leftarrow x + y)$$
$$\equiv \{\text{Reemplazamos}\}$$
$$(x + y = 6 \wedge y = 5)$$
$$\equiv \{\text{Leibniz}\}$$
$$(x + 5 = 6 \wedge y = 5)$$
$$\equiv \{\text{Aritmetica}\}$$
$$(x = 6 - 5 \wedge y = 5)$$
$$\equiv \{\text{Aritmetica}\}$$
$$(x = 1 \wedge y = 5)$$

b)

$$wp.(x := 8).(x := 8)$$
$$\equiv \{\text{Def de wp para la asignacion}\}$$
$$(x := 8)(x \leftarrow 8)$$
$$\equiv \{\text{Reemplazamos}\}$$
$$8 := 8$$
$$\equiv \{\text{Logica}\}$$
$$True$$

c)

$$wp.(x := 8).(x = 7)$$
$$\equiv \{\text{Def de wp ":="}\}$$
$$(x = 7)(x \leftarrow 8)$$
$$\equiv \{\text{Reemplazamos}\}$$
$$(8 = 7)$$
$$\equiv \{\text{Logica}\}$$
$$False$$

d)

$$wp.(x, y := y, x).(x = B \wedge y = A)$$
$$\equiv \{\text{Def de wp asignacion}\}$$
$$(x = B \wedge y = A)(x \leftarrow y, y \leftarrow x)$$
$$\equiv \{\text{Reemplazamos}\}$$
$$(y = B \wedge x = A)$$

e)

$$wp.(a, x := x, y; y := a).(x = B \wedge y = A)$$
$$\equiv \{\text{Def wp ";"}\}$$
$$wp.(a, x := x, y).(\underline{wp.(y := a).(x = B \wedge y = A)})$$
$$\equiv \{\text{Def wp asignacion}\}$$
$$wp.(a, x := x, y).((x = B \wedge y = A)(y \leftarrow a))$$
$$\equiv \{\text{Reemplazamos}\}$$
$$wp.(a, x := x, y).(x = B \wedge a = A)$$
$$\equiv \{\text{Def de wp asignacion}\}$$
$$(x = B \wedge a = A)(a \leftarrow x, x \leftarrow y)$$
$$\equiv \{\text{Reemplazamos}\}$$
$$(y = B \wedge x = A)$$

f)

$$(x \geq y \vee x \leq y)$$
$$\wedge(x \geq y \Rightarrow wp.(x := 0).((x = 0 \vee x = 2) \wedge y = 1))$$
$$\wedge(x \leq y \Rightarrow wp.(x := 2).((x = 0 \vee x = 2) \wedge y = 1))$$
$$\equiv \{\text{Def wp asignacion y logica}\}$$
$$(True)$$
$$\wedge(x \geq y \Rightarrow ((x = 0 \vee x = 2) \wedge y = 1)(x \leftarrow 0))$$
$$\wedge(x \leq y \Rightarrow ((x = 0 \vee x = 2) \wedge y = 1)(x \leftarrow 2)$$
$$\equiv \{\text{Neutro conjuncion y reemplazamos}\}$$
$$(x \geq y \Rightarrow ((0 = 0 \vee 0 = 2) \wedge y = 1))$$
$$\wedge(x \leq y \Rightarrow ((2 = 0 \vee 2 = 2) \wedge y = 1)$$
$$\equiv \{\text{Logica}\}$$
$$(x \geq y \Rightarrow ((True \vee 0 = 2) \wedge y = 1))$$
$$\wedge(x \leq y \Rightarrow ((2 = 0 \vee True) \wedge y = 1)$$

$$
\begin{gathered}
\equiv \{\text{Logica}\} \\
(x \geq y \Rightarrow (True \wedge y = 1)) \\
\wedge(x \leq y \Rightarrow (True \wedge y = 1) \\
\equiv \{\text{Neutro conjuncion}\} \\
(x \geq y \Rightarrow y = 1) \\
\wedge(x \leq y \Rightarrow y = 1) \\
\equiv \{\text{Logica}\} \\
(x \geq y \vee x \leq y \Rightarrow y = 1) \\
\equiv \{\text{Logica}\} \\
(True \Rightarrow y = 1) \\
\equiv \{\text{Logica}\} \\
(y = 1)
\end{gathered}
$$

Resultado final:

$$
\begin{array}{l}
\{y = 1\} \\
if\ x \geq y \rightarrow \\
\quad \{y = 1\} \\
\quad x := 0 \\
\quad \{(x = 0 \vee x = 2) \wedge y = 1\} \\
[]x \leq y \rightarrow \\
\quad \{y = 1\} \\
\quad x := 2 \\
\quad \{(x = 0 \vee x = 2) \wedge y = 1\} \\
\{(x = 0 \vee x = 2) \wedge y = 1\}
\end{array}
$$

2) a)

$$
\begin{aligned}
& wp.(if..fi).(x \neq 1) \\
& \equiv \{\text{Def wp if}\} \\
& (x \geq 1 \vee x \leq 1) \\
& \wedge (x \geq 1 \Rightarrow wp.(x := x + 1).(x \neq 1)) \\
& \wedge (x \leq 1 \Rightarrow wp.(x := x - 1).(x \neq 1)) \\
& \equiv \{\text{Logica}\} \\
& True \\
& \wedge (x \geq 1 \Rightarrow wp.(x := x + 1).(x \neq 1)) \\
& \wedge (x \leq 1 \Rightarrow wp.(x := x - 1).(x \neq 1)) \\
& \equiv \{\text{Def wp asignacion y neutro conjuncion}\} \\
& (x \geq 1 \Rightarrow (x \neq 1)(x \leftarrow x + 1) \\
& \wedge (x \leq 1 \Rightarrow (x \neq 1)(x \leftarrow x - 1) \\
& \equiv \{\text{Reemplazamos}\} \\
& (x \geq 1 \Rightarrow (x + 1 \neq 1) \\
& \wedge (x \leq 1 \Rightarrow (x - 1 \neq 1) \\
& \equiv \{\text{logica}\} \\
& True \wedge True \\
& \equiv \{\text{logica}\} \\
& True
\end{aligned}
$$

$wp.(if..fi).(x > y)$
$\equiv$ {Reemplazo P y def de wp if}
$(x > y \vee x < y) \wedge$
$\wedge (x > y \Rightarrow wp.(skip).(x > y))$
$\wedge (x < y \Rightarrow wp.(x, y := y, x).(x > y))$
$\equiv$ {Def wp skip}
$(x > y \vee x < y) \wedge$
$\wedge (x > y \Rightarrow x > y)$
$\wedge (x < y \Rightarrow wp.(x, y := y, x).(x > y))$
$\equiv \{P \Rightarrow P \equiv True\}$
$(x > y \vee x < y) \wedge$
$\wedge True$
$\wedge (x < y \Rightarrow wp.(x, y := y, x).(x > y))$
$\equiv$ {Neutro conjuncion y wp asignacion}
$(x > y \vee x < y) \wedge$
$\wedge (x < y \Rightarrow (x > y)(x \leftarrow y, y \leftarrow x)$
$\equiv$ {Reemplazamos}
$(x > y \vee x < y) \wedge$
$\wedge (x < y \Rightarrow (y > x)$
$\equiv$ {Logica}
$(x > y \vee x < y) \wedge$
$\wedge True$
$\equiv$ {Neutro conjuncion}
$(x > y \vee x < y)$

Ahora veamos si se cumple $P \Rightarrow wp.(if..fi).(x > y)$

$P \Rightarrow wp.(if..fi).(x > y)$
$\equiv$ {Reemplazamos P y la wp del if}
$x \neq y \Rightarrow (x > y \vee x < y)$
$\equiv$ {Logica}
$True$

c) $wp.(x, y := y * y, x * x).(wp.(if..fi).(x \geq 0 \wedge y \geq 0))$

Trabajemos primero sobre la wp del if:

$wp.(if..fi).(x \geq 0 \wedge y \geq 0)$
$\equiv \{\text{Def wp if}\}$
$(x \geq y \vee x \leq y) \wedge$
$\wedge (x \geq y \Rightarrow wp.(x := x - y).(x \geq 0 \wedge y \geq 0))$
$\wedge (x \leq y \Rightarrow wp.(y := y - x).(x \geq 0 \wedge y \geq 0))$
$\equiv \{\text{Logica}\}$
$(True) \wedge$
$\wedge (x \geq y \Rightarrow wp.(x := x - y).(x \geq 0 \wedge y \geq 0))$
$\wedge (x \leq y \Rightarrow wp.(y := y - x).(x \geq 0 \wedge y \geq 0))$
$\equiv \{\text{Elem neutro conjuncion}\}$
$(x \geq y \Rightarrow wp.(x := x - y).(x \geq 0 \wedge y \geq 0))$
$\wedge (x \leq y \Rightarrow wp.(y := y - x).(x \geq 0 \wedge y \geq 0))$
$\equiv \{\text{Def wp asignacion}\}$
$(x \geq y \Rightarrow (x \geq 0 \wedge y \geq 0)(x \leftarrow x - y))$
$\wedge (x \leq y \Rightarrow (x \geq 0 \wedge y \geq 0)(y \leftarrow y - x))$
$\equiv \{\text{Reemplazo}\}$
$(x \geq y \Rightarrow (x - y \geq 0 \wedge y \geq 0)(x \leftarrow x - y))$
$\wedge (x \leq y \Rightarrow (x \geq 0 \wedge y - x \geq 0)(y \leftarrow y - x))$
$\equiv \{\text{Aritmetica}\}$
$(x \geq y \Rightarrow (x \geq y \wedge y \geq 0))$
$\wedge (x \leq y \Rightarrow (x \geq 0 \wedge y \geq x))$
$\equiv \{\text{Aritmetica}\}$
$(x \geq y \Rightarrow (x \geq y \wedge y \geq 0))$
$\wedge (x \leq y \Rightarrow (x \geq 0 \wedge x \leq y))$
$\equiv \{P \Rightarrow P \wedge Q \equiv P \Rightarrow Q\}$
$(x \geq y \Rightarrow y \geq 0) \wedge (x \leq y \Rightarrow x \geq 0)$
$\equiv \{\text{Transitividad}\}$
$(x \geq y \Rightarrow (x \geq 0 \wedge y \geq 0)) \wedge (x \leq y \Rightarrow (x \geq 0 \wedge y \geq 0))$
$\equiv \{\text{Distributividad izquierda implicacion disyuncion}\}$
$(x \geq y \vee x \leq y \Rightarrow (x \geq 0 \wedge y \geq 0))$
$\equiv \{\text{Logica}\}$
$(True \Rightarrow (x \geq 0 \wedge y \geq 0))$
$\equiv \{\text{Logica}\}$
$(x \geq 0 \wedge y \geq 0)$

Por lo cual nos queda lo siguiente:

$$
\begin{aligned}
& wp.(x,y := y*y, x*x).(wp.(if..fi).(x \geq 0 \wedge y \geq 0)) \\
& \equiv \{\text{wp if calculado previamente}\} \\
& wp.(x,y := y*y, x*x).(x \geq 0 \wedge y \geq 0) \\
& \equiv \{\text{Def wp asignacion}\} \\
& (x \geq 0 \wedge y \geq 0)(x \leftarrow y*y, y \leftarrow x*x) \\
& \equiv \{\text{Reemplazamos}\} \\
& (y*y \geq 0 \wedge x*x \geq 0) \\
& \equiv \{\text{Logica}\} \\
& True
\end{aligned}
$$

Finalmente:

$$
\begin{aligned}
& P \Rightarrow wp.(x,y := y*y, x*x).(wp.(if..fi).(x \geq 0 \wedge y \geq 0)) \\
& \equiv \{\text{Reemplazamos por los resultados obtenidos previamente}\} \\
& P \Rightarrow wp.(x,y := y*y, x*x).(x \geq 0 \wedge y \geq 0) \\
& \equiv \{\text{Reemplazamos por los resultados obtenidos previamente}\} \\
& P \Rightarrow True \\
& \equiv \{\text{Reemplazamos P}\} \\
& True \Rightarrow True \\
& \equiv \{\text{Logica}\} \\
& True
\end{aligned}
$$

d)

$$wp.(if..fi).(a \vee b)$$
$$\equiv \{\text{Def wp if}\}$$
$$(\neg a \vee b \vee a \vee \neg b) \wedge$$
$$\wedge\ (\neg a \vee b \Rightarrow wp.(a := \neg a).(a \vee b))$$
$$\wedge\ (a \vee \neg b \Rightarrow wp.(b := \neg b).(a \vee b))$$
$$\equiv \{\text{Tercero excluido, elem absorbente disyuncion, elem neutro conjuncion}\}$$
$$(\neg a \vee b \Rightarrow wp.(a := \neg a).(a \vee b))$$
$$\wedge\ (a \vee \neg b \Rightarrow wp.(b := \neg b).(a \vee b))$$
$$\equiv \{\text{Def wp asignacion}\}$$
$$(\neg a \vee b \Rightarrow (\neg a \vee b))$$
$$\wedge\ (a \vee \neg b \Rightarrow (a \vee \neg b))$$
$$\equiv \{\text{Logica}\}$$
$$True$$

e) Primero veamos si se cumple la siguiente terna $\{N \geq 0\}\ x := 0\ \{x \leq N\}$:

$$N \geq 0 \Rightarrow wp.(x := 0).(x \leq N)$$
$$\equiv \{\text{Def wp asignacion}\}$$
$$N \geq 0 \Rightarrow (0 \leq N)$$
$$\equiv \{\text{Aritmetica}\}$$
$$N \geq 0 \Rightarrow (N \geq 0)$$
$$\equiv \{\text{Logica}\}$$
$$True$$

Por ende, el invariante se cumple antes de comenzar el cuerpo del bucle.

Ahora demostremos que el invariante se cumple al finalizar el bucle:

$$x \leq N \wedge \neg(x \neq N) \Rightarrow x = N$$
$$\equiv \{\text{Logica}\}$$
$$x \leq N \wedge (x = N) \Rightarrow x = N$$
$$\equiv \{\text{Debilitamiento para } \wedge\}$$
$$True$$

Ahora procedamos a verificar $\{x \leq N \wedge (x \neq N)\}x := x + 1\{x \leq N\}$, para ello supongamos $x \leq N \wedge (x \neq N)$ y demostremos la wp:

$$
\begin{aligned}
& wp.(x := x + 1).(x \leq N) \\
& \equiv \{\text{Def de wp asignacion}\} \\
& x + 1 \leq N \\
& \equiv \{\text{Logica}\} \\
& x + 1 < N \vee (x + 1 = N) \\
& \equiv \{\text{Logica}\} \\
& x \leq N \vee (x + 1 = N) \\
& \equiv \{\text{Por suposicion } x \leq N \equiv True\} \\
& True \vee (x + 1 = N) \\
& \equiv \{\text{elemento absorvente disyuncion}\} \\
& True
\end{aligned}
$$

f)

$$
\begin{aligned}
& True \Rightarrow r \leq |N| \\
& \wedge\, r \leq |N| \wedge \neg(r \neq 0) \Rightarrow r = 0 \\
& \wedge\, \{r \leq |N| \wedge r \neq 0\} if..fi \{r \leq |N|\}
\end{aligned}
$$

Primero veamos si el invariante se cumple antes de iniciar el bucle, para ello demostremos la terna $\{True\}\ r := N\ \{r \leq N\}$:

$$
\begin{aligned}
& True \Rightarrow wp.(r := N).(r \leq N) \\
& \equiv \{\text{Def de wp asignacion}\} \\
& True \Rightarrow (N \leq N) \\
& \equiv \{\text{Logica}\} \\
& True \Rightarrow True \\
& \equiv \{\text{Logica}\} \\
& True
\end{aligned}
$$

Ahora demostremos que la postcondicion se cumple al finalizar el bucle:

$$
\begin{aligned}
&I \wedge \neg B \Rightarrow Q \\
&\equiv \{\text{Reemplazamos}\} \\
&r \leq |N| \wedge \neg(r \neq 0) \Rightarrow r = 0 \\
&\equiv \{\text{Logica}\} \\
&r \leq |N| \wedge (r = 0) \Rightarrow r = 0 \\
&\equiv \{\text{Debilitamiento para } \wedge\} \\
&True
\end{aligned}
$$

Ahora demostremos que el invariante se cumple adentro del cuerpo del bucle, para ello verifiquemos la terna $\{r \leq |N| \wedge r \neq 0\}\ if..fi\ \{r \leq |N|\}$:

$$
\begin{aligned}
& r \leq |N| \wedge r \neq 0 \Rightarrow wp.(if..fi).(r \leq |N|) \\
& \equiv \{\text{Supongamos } r \leq |N| \wedge r \neq 0 \text{ y demostremos la wp}\} \\
& wp.(if..fi).(r \leq |N|) \\
& \equiv \{\text{Def de wp if}\} \\
& (r < 0 \vee r > 0) \wedge \\
& \wedge (r < 0 \Rightarrow wp.(r := r+1).(r \leq |N|) \\
& \wedge (r > 0 \Rightarrow wp.(r := r-1).(r \leq |N|) \\
& \equiv \{\text{Por suposicion como } r \neq 0 \text{ entonces } r < 0 \wedge r > 0 \equiv True\ \} \\
& (r < 0 \Rightarrow wp.(r := r+1).(r \leq |N|) \\
& \wedge (r > 0 \Rightarrow wp.(r := r-1).(r \leq |N|) \\
& \equiv \{\text{Def wp asignacion}\} \\
& (r < 0 \Rightarrow (r+1 \leq |N|) \\
& \wedge (r > 0 \Rightarrow (r-1 \leq |N|) \\
& \equiv \{\text{Aritmetica}\} \\
& (r < 0 \Rightarrow (|N| \geq r+1) \\
& \wedge (r > 0 \Rightarrow (|N| \geq r-1) \\
& \equiv \{\text{Aritmetica desigualdad y valor absoluto}\} \\
& (r < 0 \Rightarrow (N \leq -(r+1) \vee N \geq r+1) \\
& \wedge (r > 0 \Rightarrow (N \leq -(r-1) \vee N \geq r-1) \\
& \equiv \{\text{Aritmetica}\} \\
& (r < 0 \Rightarrow (N+1 \leq -r \vee N-1 \geq r) \\
& \wedge (r > 0 \Rightarrow (N-1 \leq -r \vee N+1 \geq r) \\
& \equiv \{N \leq -r \vee N \geq r\} \\
\equiv \{\text{Macumba}\} & (r < 0 \Rightarrow (N \leq -r \vee (N+1 = -r) \vee N-1 \geq r) \\
& \wedge (r > 0 \Rightarrow (N-1 \leq -r \vee N+1 \geq r)
\end{aligned}
$$

3)a) Asumimos P y vemos la wp de la asignacion:

$$
\begin{aligned}
&wp.(x, y := x + 1, E).(y = x + 1)\\
&\equiv \{\text{Def wp asignacion}\}\\
&(y = x + 1)(x \leftarrow x + 1, y \leftarrow E)\\
&\equiv \{\text{Reemplazamos}\}\\
&E = x + 1 + 1\\
&\equiv \{\text{Aritmetica}\}\\
&E = x + 2\\
&\equiv \{E \leftarrow x + 2\}\\
&x + 2 = x + 2\\
&\equiv \{\text{Logica}\}\\
&True
\end{aligned}
$$

Resultado final:

$$
\begin{aligned}
&\{True\}\\
&x, y := x + 1, x + 2\\
&\{y = x + 1\}
\end{aligned}
$$

b) Asumimos $q = a * c \wedge w = c^2$ y realizamos la wp de la asignacion

$$
\begin{aligned}
&wp.(a, q := a + c, E).(q = a * c)\\
&\equiv \{\text{Def de wp asignacion}\}\\
&E = (a + c) * c\\
&\equiv \{\text{Aritmetica}\}\\
&E = a * c + c^2\\
&\equiv \{\text{Suposicion}\}\\
&E = q + w\\
&\equiv \{E \leftarrow q + w\}\\
&q + w = q + w\\
&\equiv \{\text{Logica}\}\\
&True
\end{aligned}
$$

Resultado final:

$$\{q = a * c \wedge w = c^2\}$$
$$a, q := a + c, q + w$$
$$\{q = a * c\}$$

c) Supongamos la premisa $A = q * B + r$ y veamos la wp:

$wp.(q := E; r := r - B).(A = q * B + r)$
$\equiv$ {Def wp composicion}
$wp.(q := E).(wp.(r := r - B).(A = q * B + r))$
$\equiv$ {Def wp asignacion}
$wp.(q := E).(A = q * B + (r - B))$
$\equiv$ {Def wp asignacion}
$A = E * B + r - B$
$\equiv$ {Aritmetica}
$A = E * B + r - B$
$\equiv$ {Suposicion}
$q * B + r = E * B + r - B$
$\equiv$ {Aritmetica}
$q * B = E * B - B$
$\equiv$ {Aritmetica}
$q * B = (E - 1) * B$
$\equiv$ {Reemplazo E (No sabemos si B es igual a 0 o no)}
$(q + 1) * B = (q + 1) * B$
$\equiv$ {logica}
$True$

Resultado final:

$$\{A = q * B + r\}$$
$$q := q + 1; r := r - B$$
$$\{A = q * B + r\}$$

d) Supongamos la premisa $x * y + p * q = N$ y veamos la wp:

$$
\begin{aligned}
& wp.(x := x - p).(wp.(q := F).(x * y + p * q = N)) \\
& \equiv \{\text{Def wp asignacion}\} \\
& wp.(x := x - p).(x * y + p * F = N) \\
& \equiv \{\text{Def wp asignacion}\} \\
& (x - p) * y + p * F = N \\
& \equiv \{\text{Suposicion}\} \\
& (x - p) * y + p * F = x * y + p * q \\
& \equiv \{\text{Aritmetica}\} \\
& (x * y) - (p * y) + p * F = x * y + p * q \\
& \equiv \{\text{Aritmetica}\} \\
& -(p * y) + p * F = p * q \\
& \equiv \{\text{Aritmetica}\} \\
& p * F = p * q + (p * y) \\
& \equiv \{\text{Aritmetica}\} \\
& p * F = p * (q + y) \\
& \equiv \{\text{Reemplazo F}\} \\
& p * (q + y) = p * (q + y) \\
& \equiv \{\text{Logica}\} \\
& True
\end{aligned}
$$

Resultado final:

$$
\begin{aligned}
& \{x * y + p * q = N\} \\
& x := x - p; \\
& q := q + y \\
& \{x * y + p * q = N\}
\end{aligned}
$$

4) Calcular el minimo de dos valores:

$$
\begin{aligned}
& \{x = X \wedge y = Y\} \\
& if\ x \leq y \rightarrow r := x \\
& []\ x > y \rightarrow r := y \\
& fi \\
& \{r = min.x.y\}
\end{aligned}
$$

Ahora verifiquemos esta terna de hoare. Supongamos P y demostremos la wp del if

$wp.(if..fi).(r = min.x.y)$
$\equiv$ {Def wp if}
$(x \leq y \vee x > y)$
$\wedge (x \leq y \Rightarrow wp.(r := x).(r = min.x.y))$
$\wedge (x > y \Rightarrow wp.(r := y).(r = min.x.y))$
$\equiv$ {Logica y elemento neutro conjuncion}
$(x \leq y \Rightarrow wp.(r := x).(r = min.x.y))$
$\wedge (x > y \Rightarrow wp.(r := y).(r = min.x.y))$
$\equiv$ {Def wp asignacion}
$(x \leq y \Rightarrow (x = min.x.y))$
$\wedge (x > y \Rightarrow (y = min.x.y))$
$\equiv$ {Supongamos $x \leq y$ y demostremos $x = min.x.y$}
$(x = min.x.y)$
$\wedge (x > y \Rightarrow (y = min.x.y))$
$\equiv$ {Por suposicion $x \leq y$, entonces $min.x.y = x$}
$True \wedge (x > y \Rightarrow (y = min.x.y))$
$\equiv$ {Supongamos el precedente y demostremos el consecuente}
$True \wedge (y = min.x.y)$
$\equiv$ {Por suposicion como $x > y$ entonces $min.x.y = y$}
$True \wedge True$
$\equiv$ {Logica}
$True$

b) Calcular el valor absoluto de un numero:

$\{x = X\}$
$if\ x \geq 0 \rightarrow skip$
$[]\ x < 0 \rightarrow x := -x$
fi
$\{x = |X|\}$

Ahora procedamos a verificar el programa suponiendo P y demostrando la wp del if:

$wp.(if..fi).(x = |X|)$
$\equiv$ {Def wp if}
$(x \geq 0 \vee x < 0)$
$\wedge\,(x \geq 0 \Rightarrow wp.(skip).(x = |X|))$
$\wedge\,(x < 0 \Rightarrow wp.(x := -x).(x = |X|))$
$\equiv$ {Logica y elemento neutro conjuncion}
$(x \geq 0 \Rightarrow wp.(skip).(x = |X|))$
$\wedge\,(x < 0 \Rightarrow wp.(x := -x).(x = |X|))$
$\equiv$ {Def wp skip y asignacion}
$(x \geq 0 \Rightarrow (x = |X|))$
$\wedge\,(x < 0 \Rightarrow (-x = |X|))$
$\equiv$ {Suponemos $x \geq 0$ y demostramos el consecuente}
$(x = |X|)$
$\wedge\,(x < 0 \Rightarrow (-x = |X|))$
$\equiv$ {Por suposicion como $x \geq 0 \wedge x = X$ y por def de valor absoluto}
$True \wedge (x < 0 \Rightarrow (-x = |X|))$
$\equiv$ {Suponemos el antecedente y demostramos el consecuente}
$True \wedge (-x = |X|)$
$\equiv$ {Por suposicion como $x < 0 \wedge x = X$ y por def de valor absoluto}
$True \wedge True$
$\equiv$ {Logica}
$True$

$P \Rightarrow (B_0 \vee B_1)$
$\wedge (B_0 \Rightarrow wp.(S0).Q)$
$\wedge (B_1 \Rightarrow wp.(S1).Q)$
$\Rightarrow$
$P \Rightarrow (B_0 \vee \neg B_0)$
$\wedge (B_0 \Rightarrow wp.(S0).Q)$
$\wedge (\neg B_0 \Rightarrow wp.(S1).Q)$
$\equiv$ {Supongamos el antecedente y demostremos el consecuente}
$P \Rightarrow (B_0 \vee \neg B_0)$
$\wedge (B_0 \Rightarrow wp.(S0).Q)$
$\wedge (\neg B_0 \Rightarrow wp.(S1).Q)$
$\equiv$ {Distributividad derecha implicacion}
$(P \Rightarrow B_0 \vee \neg B_0)$
$\wedge (P \Rightarrow B_0 \Rightarrow wp.(S0).Q)$
$\wedge (P \Rightarrow \neg B_0 \Rightarrow wp.(S1).Q)$
$\equiv$ {Tercero excluido y Logica}
$True$
$\wedge (P \Rightarrow B_0 \Rightarrow wp.(S0).Q)$
$\wedge (P \Rightarrow \neg B_0 \Rightarrow wp.(S1).Q)$
$\equiv$ {Elemento neutro conjuncion y currificacion}
$(P \wedge B_0 \Rightarrow wp.(S0).Q)$
$\wedge (P \wedge \neg B_0 \Rightarrow wp.(S1).Q)$
$\equiv$ {Supongamos los precedentes y demostremos los consecuentes}
$wp.(S0).Q \wedge wp.(S1).Q$
$\equiv$ {Por primera suposicion ambos wp son equivalen a True}
$True \wedge True$
$\equiv$ {Logica}
$True$

6)

a) Postcondicion: Suma de todos los elementos del array A. El programa no es valido ya que nunca se incrementa el valor de i, por ende siempre se estaria sumando A.0.

b) Postcondicion: Suma de todos los elementos del array A. El programa no es valido, ya que no toma al elemento de A en el indice 0 y además se va de rango.

c) Postcondicion: Suma de todos los elementos del array A. El programa no es valido porque se va de rango.

d) Postcondicion: Si existe un elemento en A que sea igual a E, este se encuentra en la posicion i de A El programa no es valido ya que el i resultante siempre va a ser mayor por 1 que la posicion de E en el array A.

7)

a) No es valido ya que no cumple con que $P \Rightarrow 1 \leq i$, ya que i comienza en 0.

b) No es valido, ya que no sirve para demostrar $I \wedge \neg(B) \Rightarrow Q$

c) No es valido, ya que no sirve para demostrar $I \wedge \neg(B) \Rightarrow Q$

d) No es valido ya que siempre suma k-veces el elemento en la posicion i. Por ende no se cumple que $P \Rightarrow I$

e) No es valido ya que siempre suma k-veces el elemento en la posicion i. Por ende no se cumple que $P \Rightarrow I$

8)

$$\begin{aligned}
&\{x = X \wedge y = Y\} \\
&x, y := y, x \\
&\{x = Y \wedge y = X\}
\end{aligned}$$

Ahora procedamos a realizar la verificacion:

$$\begin{aligned}
&x = X \wedge y = Y \Rightarrow wp.(x, y := y, x).(x = Y \wedge y = X) \\
&\equiv \{\text{Def wp asignacion}\} \\
&x = X \wedge y = Y \Rightarrow (y = Y \wedge x = X) \\
&\equiv \{\text{Logica}\} \\
&True
\end{aligned}$$

$$\begin{aligned}
&\{x = X \wedge y = Y\} \\
&x := x - y; \\
&y := x + y; \\
&x := y - x \\
&\{x = Y \wedge y = X\}
\end{aligned}$$

Ahora procedamos a realizar la verificacion:

$x = X \wedge y = Y \Rightarrow wp.(x := x - y; y := x + y; x := y - x).(x = Y \wedge y = X)$
$\equiv$ {Supongamos el antecedente y demostremos el consecuente}
$wp.(x := x - y; y := x + y; x := y - x).(x = Y \wedge y = X)$
$\equiv$ {Def de wp composicion}
$wp.(x := x - y; y := x + y).(wp.(x := y - x).(x = Y \wedge y = X))$
$\equiv$ {Def wp asingacion}
$wp.(x := x - y; y := x + y).(y - x = Y \wedge y = X)$
$\equiv$ {Def de wp composicion}
$wp.(x := x - y).(wp.(y := x + y).(y - x = Y \wedge y = X))$
$\equiv$ {Def wp asingacion}
$wp.(x := x - y).((x + y) - x = Y \wedge x + y = X)$
$\equiv$ {Def wp asingacion}
$((x - y) + y) - (x - y) = Y \wedge (x - y) + y = X)$
$\equiv$ {Aritmetica}
$x - y + y - x + y = Y \wedge x - y + y = X$
$\equiv$ {Aritmetica}
$y = Y \wedge x = X$
$\equiv$ {Por suposicion}
$True$

9)

$\{X > 0 \wedge Y > 0 \wedge x = X \wedge y = Y\}$
$do\ B \rightarrow$
$\quad \{I \wedge B\}$
$\quad S$
$\quad \{I\}$
od
$\{x = mcd.X.Y\}$

Intentemos descubrir S, para ello tengamos en cuenta que $I \wedge \neg B \Rightarrow Q$

$I \wedge \neg B \Rightarrow$
$\equiv$ {Reemplazo}
$x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y \wedge \neg B \Rightarrow x = mcd.X.Y$
$\equiv$ {Reemplazo B por $x \neq y$ y aplico negacion}
$x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y \wedge x = y \Rightarrow x = mcd.X.Y$
$\equiv$ {Supongo antecedente y demuestro precedente}
$x = mcd.X.Y$
$\equiv$ {Por suposicion $y = x$, entonces $mcd.x.y = x$}
$mcd.x.y = mcd.X.Y$
$\equiv$ {Por suposicion mcd.x.y = mcd.X.Y}
$True$

Podemos reemplazar S por un if con las propiedades del mcd:

$\{X > 0 \wedge Y > 0 \wedge x = X \wedge y = Y\}$
$do\ x \neq y \rightarrow$
  $\{I \wedge B\}$
  $if\ x > y \rightarrow x, y := x - y, y$
  $[]\ y > x \rightarrow x, y := x, y - x$
  fi
  $\{I\}$
od
$\{x = mcd.X.Y\}$

Ahora procedamos a verificar el programa que obtuvimos:

$$I : x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y$$

Veamos si el invariante se cumple antes de iniciar el bucle:

$P \Rightarrow I$
$\equiv$ {Reemplazo}
$(X > 0 \wedge Y > 0 \wedge x = X \wedge y = Y) \Rightarrow (x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y)$
$\equiv$ {Suponemos precedente y demostramos antecedente}
$x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y$
$\equiv$ {Por suposicion $x = X \wedge y = Y$}
$X > 0 \wedge Y > 0 \wedge mcd.X.Y = mcd.X.Y$
$\equiv$ {Por suposicion $X > 0 \wedge Y > 0$}
$True \wedge True \wedge mcd.X.Y = mcd.X.Y$
$\equiv$ {Logica}
$True \wedge True \wedge True$
$\equiv$ {Elemento neutro conjuncion}
$True$

Ahora veamos si el invariante se cumple al finalizar el bucle:

$I \wedge \neg(B) \Rightarrow Q$
$\equiv$ {Reemplazo}
$(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y) \wedge \neg(x \neq y) \Rightarrow (x = mcd.X.Y)$
$\equiv$ {Logica}
$(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y) \wedge (x = y) \Rightarrow (x = mcd.X.Y)$
$\equiv$ {Supongo precedente y demuestro antecedente}
$x = mcd.X.Y$
$\equiv$ {Por suposicion $x = y$, entonces $mcd.x.y = mcd.x.x = x$}
$mcd.x.y = mcd.X.Y$
$\equiv$ {Por suposicion, $mcd.x.y = mcd.X.Y$}
$True$

Ahora veamos si el invariante se cumple durante la ejecucion del bucle:

$\{(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y) \wedge x \neq y\} if..fi \{(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y)\}$

$\equiv$ {Verificacion para el if}

$((x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y) \wedge x \neq y) \Rightarrow wp.(if..fi).(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y)$

$\equiv$ {Supongo antecedente y demustro precedente}

$wp.(if..fi).(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y)$

$\equiv$ {Def wp if}

$(x > y \vee y > x)$

$\wedge (x > y \Rightarrow wp.(x, y := x - y, y).(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y))$

$\wedge (y > x \Rightarrow wp.(x, y := x, y - x).(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y))$

$\equiv$ {Por suposicion $x \neq y$ y logica}

$True$

$\wedge (x > y \Rightarrow wp.(x, y := x - y, y).(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y))$

$\wedge (y > x \Rightarrow wp.(x, y := x, y - x).(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y))$

$\equiv$ {Def wp asignacion y elemento neutro conjuncion}

$(x > y \Rightarrow ((x - y) > 0 \wedge y > 0 \wedge mcd.(x - y).y = mcd.X.Y))$

$\wedge (y > x \Rightarrow (x > 0 \wedge (y - x) > 0 \wedge mcd.x.(y - x) = mcd.X.Y))$

$\equiv$ {Aritmetica}

$(x > y \Rightarrow (x > y \wedge y > 0 \wedge mcd.(x - y).y = mcd.X.Y))$

$\wedge (y > x \Rightarrow (x > 0 \wedge y > x \wedge mcd.x.(y - x) = mcd.X.Y))$

$\equiv$ {Supongo antecedente y demustro precedente}

$(x > y \wedge y > 0 \wedge mcd.(x - y).y = mcd.X.Y)$

$\wedge (y > x \Rightarrow (x > 0 \wedge y > x \wedge mcd.x.(y - x) = mcd.X.Y))$

$\equiv$ {Por suposicion $x > y$ y por (c)}

$(True \wedge y > 0 \wedge mcd.x.y = mcd.X.Y)$

$\wedge (y > x \Rightarrow (x > 0 \wedge y > x \wedge mcd.x.(y - x) = mcd.X.Y))$

$\equiv$ {Por suposicion $y > 0$ y $\quad mcd.x.y = mcd.X.Y$}

$(True \wedge True \wedge True)$

$\wedge (y > x \Rightarrow (x > 0 \wedge y > x \wedge mcd.x.(y - x) = mcd.X.Y))$

$\equiv$ {Logica}

$(y > x \Rightarrow (x > 0 \wedge y > x \wedge mcd.x.(y - x) = mcd.X.Y))$

$\equiv$ {Supongo precedente y demustro antecedente}

$(x > 0 \wedge y > x \wedge mcd.x.(y - x) = mcd.X.Y)$

$\equiv$ {Por suposicion $x > 0$ y $y > x$}

$(True \wedge True \wedge mcd.x.(y - x) = mcd.X.Y)$

$\equiv$ {Como $y > x$ aplicamos propiedad (d)}

$(True \wedge True \wedge mcd.x.y = mcd.X.Y)$

$\equiv$ {Por suposicion $mcd.x.y = mcd.X.Y$}

$(True \wedge True \wedge True)$

$\equiv$ {Logica}

$True$

Cota candidata: $max.x.y - min.x.y$

$(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y) \wedge x \neq y \Rightarrow (max.x.y - min.x.y) \geq 0$
$\equiv$ {Supongo precedente y demuestro consecuente}
$(max.x.y - min.x.y) \geq 0$
$\equiv$ {Aritmetica}
$max.x.y \geq min.x.y$
$\equiv$ {Por suposicion como $x \neq y$ sabemos que $max.x.y \geq min.x.y$}
$True$

Ahora veamos si el bucle finaliza:

$\{(x > 0 \wedge y > 0 \wedge mcd.x.y = mcd.X.Y) \wedge x \neq y \wedge (max.x.y - min.x.y) = T\}$
$if..fi$
$\{(max.x.y - min.x.y) < T\}$
$\equiv$ {Supongamos la precondicion y veamos la wp}
$wp.(if..fi).((max.x.y - min.x.y) < T)$
$\equiv$ {Def wp if}
$(x > y \vee y > x)$
$\wedge (x > y \Rightarrow wp.(x, y := x - y, y).((max.x.y - min.x.y) < T))$
$\wedge (y > x \Rightarrow wp.(x, y := x, y - x).((max.x.y - min.x.y) < T))$
$\equiv$ {Por suposicion $x \neq y$ y tercero excluido}
$(x > y \Rightarrow wp.(x, y := x - y, y).((max.x.y - min.x.y) < T))$
$\wedge (y > x \Rightarrow wp.(x, y := x, y - x).((max.x.y - min.x.y) < T))$
$\equiv$ {Def wp asignacion}
$(x > y \Rightarrow ((max.(x - y).y - min.(x - y).y) < T))$
$\wedge (y > x \Rightarrow ((max.x.(y - x) - min.x.(y - x)) < T))$
$\equiv$ {Supongo antecedentes y demuestro consecuentes}
$((max.(x - y).y - min.(x - y).y) < T))$
$\wedge ((max.x.(y - x) - min.x.(y - x)) < T)$
$\equiv$ {Por suposicion de T}
$((max.(x - y).y - min.(x - y).y) < max.x.y - min.x.y))$
$\wedge ((max.x.(y - x) - min.x.(y - x)) < max.x.y - min.x.y)$
$\equiv$ {Suponsiciones $x > y$ y $y > x$ y def de max y min}
$((max.(x - y).y - min.(x - y).y) < x - y))$
$\wedge ((max.x.(y - x) - min.x.(y - x)) < y - x)$

10) Estructura del programa:

$$\{x = X \wedge y = Y \wedge x \geq 0 \wedge y \geq 0\}$$
$$S_0$$
$$\{I : y \geq 0 \wedge r * x^y = X^Y\}$$
$$do\ B \rightarrow$$
$$\{I \wedge B\}$$
$$S_1$$
$$\{I\}$$
$$od$$
$$\{r = X^Y\}$$

Veamos S_0:

$$\{x = X \wedge y = Y \wedge x \geq 0 \wedge y \geq 0\}$$
$$S_0$$
$$\{I : y \geq 0 \wedge r * x^y = X^Y\}$$

Como r no aparece en P, S_0 no puede ser skip.

Supongamos la precondicion, veamos si r puede ser de la forma $r := E$ y hagamos la wp:

$$wp.(r := E).(y \geq 0 \wedge r * x^y = X^Y)$$
$$\equiv \{\text{Def wp asignacion}\}$$
$$y \geq 0 \wedge E * x^y = X^Y$$
$$\equiv \{\text{Por suposicion } y \geq 0\}$$
$$E * x^y = X^Y$$
$$\equiv \{\text{Por suposicion } x = X \wedge y = Y\}$$
$$E * x^y = x^y$$
$$\equiv \{\text{Elijo } E = 1\}$$
$$1 * x^y = x^y$$
$$\equiv \{\text{Aritmetica}\}$$
$$x^y = x^y$$
$$\equiv \{\text{Logica}\}$$
$$True$$

Por ende, tenemos que $r := 1$.

Ahora veamos la guarda del ciclo, teniendo en cuenta que se tiene que cumplir que $I \wedge \neg B \Rightarrow Q$:

$$(y \geq 0 \wedge r * x^y = X^Y \wedge \neg B) \Rightarrow r = X^Y$$

Para que se de que $r = X^Y$ nos sirve que $x^y = 1$, para ello podemos hacer que $B = y \geq 0$:

$$
\begin{aligned}
&(y \geq 0 \wedge r * x^y = X^Y \wedge \neg(y \geq 0)) \Rightarrow r = X^Y \\
&\equiv \{\text{Logica}\} \\
&(y \geq 0 \wedge r * x^y = X^Y \wedge y \leq 0) \Rightarrow r = X^Y \\
&\equiv \{y \geq 0 \wedge y \leq 0 \equiv y = 0\} \\
&(y = 0 \wedge r * x^y = X^Y) \Rightarrow r = X^Y \\
&\equiv \{\text{Supongo antecedente y demustro consecuente}\} \\
&r = X^Y \\
&\equiv \{\text{Por suposicion } X^Y = r * x^y\} \\
&r = r * x^y \\
&\equiv \{\text{Por suposicion como } y = 0\text{, entonces } x^y = 1\} \\
&r = r * 1 \\
&\equiv \{\text{Aritmetica}\} \\
&r = r \\
&\equiv \{\text{Logica}\} \\
&True
\end{aligned}
$$

Por ende, tenemos que $B = y \geq 0$.

Ahora que conocemos B, procedamos a derivar el cuerpo del bucle:

$$
\begin{aligned}
&\{y \geq 0 \wedge r * x^y = X^Y \wedge y \neq 0\} \\
&S_1 \\
&\{y \geq 0 \wedge r * x^y = X^Y\}
\end{aligned}
$$

Podemos probar con una asignacion de la forma $r, x, y = E, F, G$.

Supongamos la precondicion y realicemos la wp.

$wp.(r, x, y = E, F, G).(y \geq 0 \wedge r * x^y = X^Y)$

$\equiv$ {Def wp asignacion}

$G \geq 0 \wedge E * F^G = X^Y$

$\equiv$ {Por suposicion $X^Y = r * x^y$}

$G \geq 0 \wedge E * F^G = r * x^y$

$\equiv$ {Como por suposicion $y \neq 0$ Usamos definicion de exponenciacion (a)}

$G \geq 0 \wedge E * F^G = r * (x * x^{(y-1)})$

$\equiv$ {Asociatividad}

$G \geq 0 \wedge E * F^G = (r * x) * x^{(y-1)})$

$\equiv$ {Elijo $G = y - 1$}

$(y - 1) \geq 0 \wedge E * F^{(y-1)} = (r * x) * x^{(y-1)})$

$\equiv$ {Aritmetica}

$y \geq 1 \wedge E * F^{(y-1)} = (r * x) * x^{(y-1)})$

$\equiv$ {Por suposicion como $y \geq 0 \wedge y \neq 0$}

$E * F^{(y-1)} = (r * x) * x^{(y-1)}$

$\equiv$ {Elijo $E = (r * x), F = x$}

$(r * x) * x^{(y-1)} = (r * x) * x^{(y-1)}$

$\equiv$ {Logica}

$True$

Por ende tenemos que $S_1 \equiv r, y := r * x, y - 1$

Resultado final:

$\{x = X \wedge y = Y \wedge x \geq 0 \wedge y \geq 0\}$
$r := 1$
$\{I : y \geq 0 \wedge r * x^y = X^Y\}$
$do\ y \geq 0 \rightarrow$
  $\{I \wedge B\}$
  $r, y := r * x, y - 1$
  $\{I\}$
od
$\{r = X^Y\}$