Ejercicio 3

a)

```
i:= 0;
result:= 1;
while(i < n) do
    result := result * m;
    i := i + 1
endwhile
```

Teorema del invariante

- $P_c \longrightarrow I$
- $(I \wedge \neg B) \longrightarrow Q_c$
- $\{I \wedge B\}$ ciclo $\{I\}$
- $\{I \wedge B \wedge (v_0 = f_v)\}$ ciclo $\{f_v < v_0\}$
- $(I \wedge f_v \leq 0) \longrightarrow \neg B$

Demostración

Datos

- $P_c \equiv n \geq 0 \wedge (m \neq 0 \vee n \neq 0) \wedge i = 0 \wedge result = 1$
- $Q_c \equiv result = m^n$
- $I \equiv 0 \leq i \leq n \wedge result = m^i$
- $B \equiv i < n$
- $S1 \equiv result := result * m$
- $S2 \equiv i := i + 1$
- $ciclo \equiv S1; S2;$
- $f_v \equiv n - i$

$P_c \longrightarrow I$

$P_c \longrightarrow I \equiv$
$n \geq 0 \wedge (m \neq 0 \vee n \neq 0) \wedge i = 0 \wedge result = 1 \longrightarrow 0 \leq i \leq n \wedge result = m^i$

- $n \geq 0 \wedge (m \neq 0 \vee n \neq 0) \wedge i = 0 \wedge result = 1 \longrightarrow 0 \leq i \leq n \equiv \text{true}$
- $n \geq 0 \wedge (m \neq 0 \vee n \neq 0) \wedge i = 0 \wedge result = 1 \longrightarrow result = m^i \equiv \text{true}$

$(I \wedge \neg B) \longrightarrow Q_c$

$(I \wedge \neg B) \longrightarrow Q_c \equiv$
$0 \leq i \leq n \wedge result = m^i \wedge i \geq n \longrightarrow result = m^n$

$\{I \wedge B\}$ **ciclo** $\{I\}$

$wp(S1; S2, I) \overset{Ax3}{\equiv}$
$wp(S1, wp(S2, I))$

- $wp(S2; I) \equiv$

  $wp(i := i+1, 0 \leq i \leq n \wedge result = m^i) \overset{Ax1}{\equiv}$

  $\{def(i+1) \wedge_L 0 \leq i+1 \leq n \wedge result = m^{i+1}\} \equiv$

  $\{0 \leq i+1 \leq n \wedge result = m^{i+1}\} \equiv$

- $wp(S1, wp(S2, I)) \equiv$

  $wp(result := result * m, 0 \leq i+1 \leq n \wedge result = m^{i+1}) \overset{Ax1}{\equiv}$

  $\{def(result * m) \wedge_L 0 \leq i+1 \leq n \wedge result * m = m^{i+1}\}$

  $\{0 \leq i+1 \leq n \wedge result * m = m^{i+1}\}$

Qvq $I \wedge B \longrightarrow wp(S1; S2, I)$

- $I \wedge B \equiv$

  $0 \leq i \leq n \wedge result = m^i \wedge i < n \equiv$

  $0 \leq i \leq n \wedge result = m^i$

- $I \wedge B \longrightarrow wp(S1; S2, I) \equiv$

  $0 \leq i \leq n \wedge result = m^i \longrightarrow 0 \leq i+1 \leq n \wedge result * m = m^{i+1} \equiv \text{true}$

$\{I \wedge B \wedge (v_0 = f_v)\}$ **ciclo** $\{f_v < v_0\}$

$wp(S1; S2, n - i < v_0) \overset{Ax3}{\equiv}$
$wp(S1, wp(S2, n - i < v_0)) \overset{Ax3}{\equiv}$

- $wp(S2, n - i < v_0) \equiv$

  $wp(i := i+1, n - i < v_0) \overset{Ax1}{\equiv}$

  $\{n - i - 1 < v_0)\}$

- $wp(S1, wp(S2, f_v < v_0)) \equiv$

  $wp(result := result * m, n - i - 1 < v_0)) \overset{Ax1}{\equiv}$

  $n - i - 1 < v_0$

Qvq $(I \wedge B \wedge (v_0 = f_v)) \longrightarrow wp(S1; S2, f_v < v_0)$
$(I \wedge B \wedge (v_0 = f_v)) \longrightarrow wp(S1; S2, f_v < v_0) \equiv$
$0 \leq i \leq n \wedge result = m^i \wedge v_0 = n - i \longrightarrow n - i - 1 < v_0 \equiv True$

$(I \wedge f_v \leq 0) \longrightarrow \neg B$

$(I \wedge f_v \leq 0) \longrightarrow \neg B \equiv$
$0 \leq i \leq n \wedge result = m^i \wedge n - i \leq 0 \longrightarrow i \geq n \equiv \text{true}$

b)

```
i:= 0;
result:= 0;
while(i < m) do
    result := result * n;
    i := i + 1
endwhile
```

Datos

- $P_c \equiv n \geq 0 \wedge (m \neq 0 \vee n \neq 0) \wedge i = 0 \wedge result = 0$
- $Q_c \equiv result = m^n$
- $I \equiv 0 \leq i \leq n \wedge result = m^i$
- $B \equiv i < m$
- $S1 \equiv result := result * n$
- $S2 \equiv i := i + 1$
- $ciclo \equiv S1; S2;$
- $f_v \equiv m - i$

$P_c \longrightarrow I$

$n \geq 0 \wedge (m \neq 0 \vee n \neq 0) \wedge i = 0 \wedge result = 0 \longrightarrow 0 \leq i \leq n \wedge result = m^i$

- $n \geq 0 \wedge (m \neq 0 \vee n \neq 0) \wedge i = 0 \wedge result = 0 \longrightarrow 0 \leq i \leq n$
- $n \geq 0 \wedge (m \neq 0 \vee n \neq 0) \wedge i = 0 \wedge result = 0 \longrightarrow result = m^i$

Si $i = 0 \wedge m \neq 0$, $m^i = 0 \neq result = 0$, la demostración falla

c)

```
i:= 0;
result:= 1;
while(i < n) do
    i := i + 1
    result := result * m;
endwhile
```

Datos

- $P_c \equiv n \geq 0 \wedge (m \neq 0 \vee n \neq 0) \wedge i = 0 \wedge result = 1$
- $Q_c \equiv result = m^n$
- $I \equiv 0 \leq i \leq n \wedge result = m^i$
- $B \equiv i < m$
- $S1 \equiv i := i + 1$
- $S2 \equiv result := result * m$
- $ciclo \equiv S1; S2;$
- $f_v \equiv m - i$

$\{I \wedge B\}$ **ciclo** $\{I\}$

$wp(S1; S2, I) \overset{Ax3}{\equiv}$
$wp(S1, wp(S2, I))$

- $wp(S2; I) \equiv$

  $wp(result := result * m, 0 \leq i \leq n \wedge result = m^i) \overset{Ax1}{\equiv}$
  $\{0 \leq i \leq n \wedge result * m = m^i\}$

- $wp(S1, wp(S2, I)) \equiv$

  $wp(i := i + 1, 0 \leq i \leq n \land result * m = m^i) \stackrel{Ax1}{\equiv}$
  $\{0 \leq i + 1 \leq n \land result * m = m^{i+1}\}$

Qvq $I \land B \longrightarrow wp(S1; S2, I)$

- $I \land B \equiv$

  $0 \leq i \leq n \land result = m^i \land i < n \equiv$

  $0 \leq i < n \land result = m^i$

- $I \land B \longrightarrow wp(S1; S2, I) \equiv$

  $0 \leq i < n \land result = m^i \longrightarrow 0 \leq i + 1 \leq n \land result * m = m^{i+1} \equiv \text{true}$

$\{I \land B \land (v_0 = f_v)\}$ **ciclo** $\{f_v < v_0\}$

$wp(S1; S2, n - i < v_0) \stackrel{Ax3}{\equiv}$
$wp(S1, wp(S2, n - i < v_0)) \stackrel{Ax3}{\equiv}$

- $wp(S2, n - i < v_0) \equiv$

  $wp(result := result * m, n - i < v_0) \stackrel{Ax1}{\equiv}$
  $\{n - i < v_0)\}$

- $wp(S1, wp(S2, f_v < v_0)) \equiv$

  $wp(i := i + 1, n - i - 1 < v_0)) \stackrel{Ax1}{\equiv}$
  $n - i - 1 < v_0$s

Qvq $(I \land B \land (v_0 = f_v)) \longrightarrow wp(S1; S2, f_v < v_0)$
$(I \land B \land (v_0 = f_v)) \longrightarrow wp(S1; S2, f_v < v_0) \equiv$
$0 \leq i < n \land result = m^i \land v_0 = n - i \longrightarrow n - i - 1 < v_0 \equiv True$
Es valido

d)

```
i:= 2;
result:= m*m;
while(i < n) do
    result := result * m;
    i := i + 1
endwhile
```

Datos

- $P_c \equiv n \geq 0 \land (m \neq 0 \lor n \neq 0) \land i = 2 \land result = m * m$
- $Q_c \equiv result = m^n$
- $I \equiv 0 \leq i \leq n \land result = m^i$
- $B \equiv i < m$
- $S1 \equiv i := i + 1$
- $S2 \equiv result := result * m$
- $ciclo \equiv S1; S2;$
- $f_v \equiv m - i$

Es valido