Exercici 1: Especificacio i O(n)

1. Precondicion: $(x == \underline{X} \wedge n == \underline{N} \wedge x \geq 0 \wedge n > 0)$

Pos Ccondicion: $(p = \underline{X}^{\overline{N}})$

Invariamté: $(x > 0 \wedge n \geq 0 \wedge \underline{X}^{\overline{N}} == p^{*} x^{n})$

$T : n$

2. $O(\log_2 n)$ és $\log_2(n)$ ja que a cada iteració del bucle n és redueix a la meitat.

Exercici 1: Verificació formal

```
private int p;
public void power(int x, int n) {
    if (x != 0) {          // B
        p = 1              // S1
        while (n != 0) {   // C
            If (n % 2 != 0) p *= x;   // D, S3
            n /= 2; x *= x;
        }
    } else p = 0; }        // S2
```

Verificació

1.1) $P \Rightarrow dom(B)$ imt

1.2) $P \wedge B \Rightarrow wp(S_1, R)$

$P \wedge x != \emptyset \Rightarrow wp(S_1, R)$

1.2.1) $Q \Rightarrow P$

$wp(p=1, P) = \{x > \emptyset \wedge m \geq \emptyset \wedge \underline{x}^{\bar{N}} == 1 \cdot x^m\}$

1.2.2) $P \wedge C \Rightarrow wp(S_3, P)$

1.2.2.1) $U \equiv wp(m /= 2; x^2 = \underline{X}, P) \rightarrow \underline{X}^{\bar{N}} == p \cdot (x^{\cancel{2}})^{\frac{m}{\cancel{2}}} \wedge x^2 > 0 \wedge \frac{m}{2} \geq \emptyset$

1.2.2.2) $P \wedge m != \emptyset \Rightarrow wp(If, U)$

1.2.2.2.1) $U \Rightarrow dom(c)$ imt

1.2.2.2.2) $P \wedge C \wedge D \Rightarrow wp(p \cdot = x, U)$

$wp(p \cdot = x, \underline{X}^{\bar{N}} == p(x^2)^{\frac{m}{2}} \wedge x^2 > \emptyset \wedge \frac{m}{2} \geq \emptyset)$

$\underline{X}^{\bar{N}} == (p x x^m \wedge x^2 > \emptyset \wedge \frac{m}{2} < \emptyset \wedge x^2 != 0 \wedge \frac{m}{2} \% 2 == 0) \Rightarrow$

$(\underline{X}^{\bar{N}} == p x^2 (\frac{m-1}{2}) \wedge x^2 > \emptyset \wedge \frac{m-1}{2} \geq \emptyset \wedge x^2 != 0 \wedge \frac{m}{2} / 2 == 0) \Rightarrow$

$\underline{X}^{\bar{N}} == p x^m \wedge x^2 > \emptyset \wedge m \geq \emptyset$

1.2.2.2.3) $P \wedge C \wedge \neg D \Rightarrow wp(null, U)$

$wp(null, U) == \underline{X}^{\bar{N}} == p \cdot x^m \wedge x^2 > \emptyset \wedge \frac{m}{2} \geq \emptyset$

1.2.2.3) $P \land \neg C \to R = p = \underline{\bar{X}}^{\bar{N}}$

$\underline{\bar{X}}^{\bar{N}} == p \cdot x^{m} \land x > \emptyset \land m \geq \emptyset \land m == \emptyset \Rightarrow$

$\underline{\bar{X}}^{\bar{N}} = p$

1.2.2.4) $P \land C \to r > \emptyset \quad (r = m)$

$\underline{\bar{X}}^{\bar{N}} == p \cdot x^{m} \land X > \emptyset \land m \geq \emptyset \land m \leq m \,!\!\neq \emptyset$

$m > \emptyset \Rightarrow r > \emptyset$

1.2.2.5) $P \land C \land m \leq r+1 \Rightarrow wp(S_3, m \leq r)$

$\underline{\bar{X}}^{\bar{N}} == p x^{m} \land x > \emptyset \land m \geq \emptyset \land m \leq r+1 \Rightarrow$

$m > \emptyset \land m \leq r+1$

$\Rightarrow \frac{m}{2} < m \land m \leq r+1$

$\Rightarrow \frac{m}{2} < r+1 \Rightarrow \frac{m}{2} \leq r$

1.3) $P \land \neg B$

$P \land x == \emptyset \Rightarrow wp(S_3, R)$

$p = \underline{\bar{X}}^{\bar{N}} == \emptyset \to \emptyset^{m} == 0$