PRÀCTICA (15% no recuperable)

- Exercici 1: Especificació formal, verificació formal i ordre de complexitat

```
private int p;
//Q ≡ { x == X  ∧  n == N  ∧  x ≥ 0  ∧  n > 0 }
public void power (int x, int n){
    if ((x!=0)){ →B1
        p=1;
        while ((n!=0)){ →B2
            if ((n%2!=0)) p*=x; } S1.1
            n/=2; x *= x; } S1.2
        }
    } else p=0; } S2
}
//R ≡ { p == X^N }
```

S1

El bucle while se ejecuta mientras $n != 0$. En cada iteracion se realiza esto:

1. Si n es impar, => p*x
2. Luego, n / 2
3. x se eleva al cuadrado

este proceso continua hasta q llega a 0 el bucle se ejecuta tantas veces como sea necesario para q n llege a cero y en cada iteración n se divide por 2 Por lo tanto, el orden de complejidad: $O(\log n)$

INVARIANT $P \equiv \{ x \geq 0 \wedge n > 0 \wedge X^N == p * x^n \}$

$t \equiv n$

Hay tres casos en los cuales aplicamos dos teoremas:

Caso 1 ⇒ $\begin{matrix}\{Q\} \\ IF \\ \{R\}\end{matrix}$

1. $Q \rightarrow dom(B)$, se auto verifica gracias a la precondicion

2. $Q \wedge B_1 \Rightarrow wp(S1, R)$

$\{x == X \wedge n == N \wedge x \geq 0 \wedge n > 0 \wedge x != 0\}$

$\{x == X \wedge n == N \wedge x > 0 \wedge n \geq 0\}$

3. $Q \wedge \neg B_1 \Rightarrow wp(S2, R)$

$\{x == X \wedge n == N \wedge x \geq 0 \wedge n > 0 \wedge x == 0\}$

$\{x == X \wedge n == N \wedge x == 0 \wedge n > 0\}$

- proof (B=true)

$Q \Rightarrow \equiv dom(B_1) \wedge ((B \wedge wp(S1,R)) \vee (\neg B \wedge wp(S2,R)))$

$\equiv dom(B_1) \wedge ((true \wedge wp(S1,R)) \vee (false \wedge wp(S2,R)))$

$\equiv dom(B_1) \wedge \underbrace{wp(S1, R)}$

situado en el while
por lo que lo realizaremos
en el caso 2

Coso 2 $\Rightarrow$ $\begin{matrix}\{Q\}\\ \text{loop}\\ \{R\}\end{matrix}$

1. $Q \Rightarrow P$

$\swarrow$

$wp(p=1, P) \equiv \{x \geq 0 \wedge n > 0 \wedge \mathbb{X}^{\mathbb{N}} == p * x^n\}$

$\{$ Tenemos en cuenta $n == \mathbb{N}$ y $x == \mathbb{X}$, por lo que $\mathbb{X}^{\mathbb{N}} = x^n$

Tambien $p = 1$, entonces $p * x^n = x^n$

$\equiv \{x \geq 0 \wedge n > 0 \wedge x^n\}$

2. $P \wedge B_2 \Rightarrow wp(S1.1, P)$

$U \equiv wp\ (n /= 2 ; x *= x\ , P)$

$\underbrace{(x^2)^{n/2} == x^{\frac{2n}{2}} == x^n}$

$P \wedge (n != 0) \Rightarrow wp(IF, U)$

$U \equiv wp(n/=2; x*=x, P) \equiv \mathbb{X}^{\mathbb{N}} == (x \cdot x)^{(\frac{n}{2})} * p \wedge (\frac{n}{2}) > 0 \wedge x^2 \geq 0$

$\equiv \mathbb{X}^{\mathbb{N}} == x^n * p \wedge (\frac{n}{2}) > 0 \wedge x^2 \geq 0$

Aplicamos el teorema

2.1. $P \Rightarrow (\text{dom } B_2)$

2.2. $P \wedge \underbrace{n != 0}_{B2} \wedge \underbrace{n \% 2 !}_{IF} = 0 \Rightarrow wp(p *= x, U) \equiv$

$\equiv \mathbb{X}^{\mathbb{N}} == x^n * (p * x) \wedge (\frac{n}{2}) > 0 \wedge x^2 \geq 0$

senar $\rightarrow$ $\mathbb{X}^{\mathbb{N}} == p * x^n \wedge n > 0 \wedge x \geq 0 \wedge \cancel{n != 0} \wedge n \% 2 != 0$

primer $\rightarrow$ $\mathbb{X}^{\mathbb{N}} == p * x^{(n-1)} \wedge n > 1 \wedge x \geq 0 \wedge (n-1) \% 2 != 0$

$\hookrightarrow$ $\mathbb{X}^{\mathbb{N}} == (p * x)\, x^{(n-1)} \wedge n > 1 \wedge x \geq 0 \wedge (n-1) \% 2 != 0$

$\mathbb{X}^{\mathbb{N}} == (p * x)\, x^n \wedge x^2 \geq 0 \wedge \frac{n}{2} > 0$

2.3. $P \wedge n != 0 \wedge n \% 2 == 0 \Rightarrow wp(null, U) \equiv$

$\equiv \mathbb{X}^{\mathbb{N}} == (p * x)\, x^n \wedge \frac{n}{2} > 0 \wedge x^2 \geq 0$

3. $P \wedge \neg B \Rightarrow R \equiv p == \mathbb{X}^{\mathbb{N}}$

$\mathbb{X}^{\mathbb{N}} == p * x^n \wedge x \geq 0 \wedge \cancel{n > 0} \wedge n == 0 \Rightarrow \mathbb{X}^{\mathbb{N}} == p * x^n \wedge x \geq 0 \wedge n == 0$

$\Rightarrow \mathbb{X}^{\mathbb{N}} == p$

4. $P \wedge B \Rightarrow t > 0 \equiv x > 0$

$\mathbb{X}^{\mathbb{N}} == p * x^n \wedge x \geq 0 \wedge n > 0 \wedge n != 0 \Rightarrow n > 0$

5. $P \wedge B \wedge n \leq T + 1 \Rightarrow wp(S, x <= T) \equiv \frac{n}{2} \leq T$

$\mathbb{X}^{\mathbb{N}} == p * x^n \wedge x \geq 0 \wedge n > 0 \wedge n != 0 \wedge n \leq T + 1 \Rightarrow n > 0 \wedge n \leq T + 1 \Rightarrow$

$\Rightarrow \frac{n}{2} < n \wedge n \leq T + 1 \Rightarrow \frac{n}{2} < T + 1 \Rightarrow \frac{n}{2} \leq T$