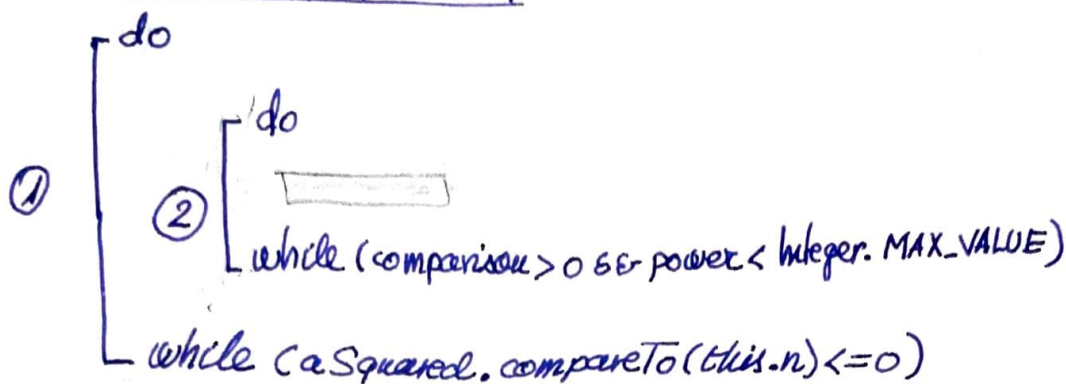


①

## Estudio Analítico. Cuestiones básicas.

Técnicas 1 y 2

¿Es  $n$  una potencia perfecta?



Cuestión 1. ¿Cuántas veces se ejecuta ①?

Téngase en cuenta que nos mantenemos en el bucle

$$\text{si } B^2 \leq n \Rightarrow B \leq \sqrt{n}$$

$B$ : base

$$B^2 = aSquared$$

Cuestión 2. ¿Cuántas veces se ejecuta ②?

Intento resolver

$$b^{\frac{\log n}{\log b} - 1 + k} > n$$

para determinar  $k$ .

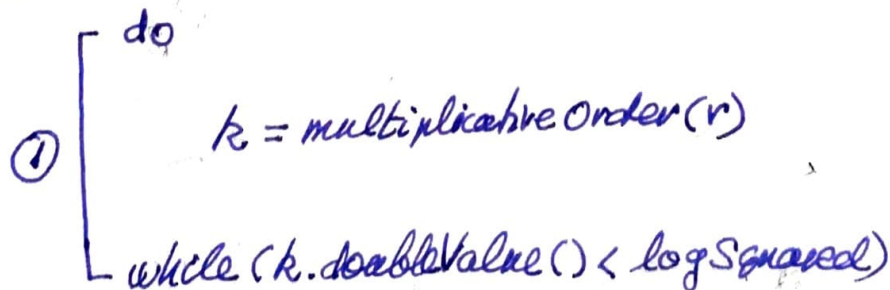
$b$  es la base una vez dentro del bucle interno.

Cuestión 3

Determinare la complejidad de la ejecución en ② (Cuerpo del bucle)

¿Es  $1 < \text{mcd}(a, n) < n$  para algún  $a \leq r$ ?

Cuestión 4. (Sobre la determinación de  $r$ )



¿Cuántas veces se ejecuta ①?

Búscase en literatura cuál es el  $r$  máximo tal que  $or(n) > \log^2 n$

②

Cuestión 5 ¿Cuál es el máximo de iteraciones en multiplicative Order?

Hágase un pequeño estudio empírico con varios valores de  $n$ , p.ej. 8, 9.

Véase la relación entre  $r$  y  $k$ .

Cuestión 6 ¿Cuál es la complejidad del cálculo del mcd?

Basémonos en la complejidad del cálculo de  $r$  y en la complejidad del cálculo del mcd (v. ejercicios introductorios)

¿Es  $n \leq r$ ?

Véase cuál es la complejidad del cálculo.