Estudio Analítico. Cuestiones básicas. Heurísticas 1 y 2

¿Es n una potencia perfecta?

```
do
  ① do
      ②
    while (comparison > 0 && power < Integer.MAX_VALUE)
  while (aSquared.compareTo(this.n) <= 0)
```

Cuestión 1. ¿Cuántas veces se ejecuta ①

Téngase en cuenta que nos mantenemos en el bucle si $B^2 \leq n \Rightarrow B \leq \sqrt{n}$

B: base $\quad B^2 = aSquared$

Cuestión 2. ¿Cuántas veces se ejecuta ②?

Intentar 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

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

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

Cuestión 4 (Sobre la determinación de r)

```
do
  ①  k = multiplicativeOrder(r)
while (k.doubleValue() < logSquared)
```

¿Cuántas veces se ejecuta ①?

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

(2)

Cuestión 5 ¿Cuál es el máximo de iteraciones en multiplicativeOrder?

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.