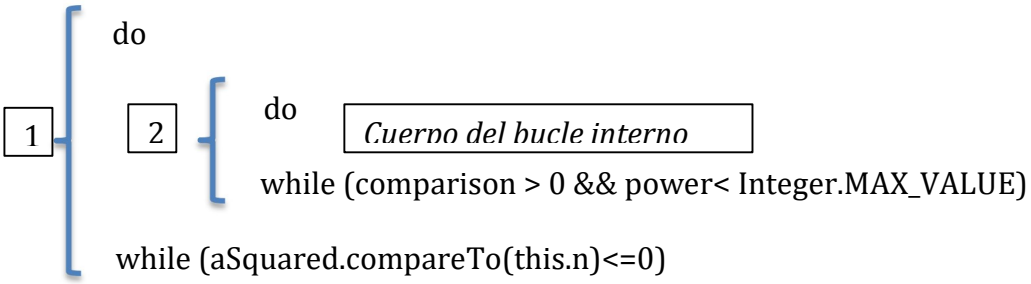
Cuestiones básicas de AKS (heurísticas)

¿Es *n* una potencia perfecta?



Cuestión 1. ¿Cuántas veces se ejecuta [1]?

Téngase en cuenta que nos mantenemos en el bucle si:

$$B^2 \leq n \quad \text{(while aSquared.compareTo(this.n)} \leq 0)$$

B: base B^2*: aSquared*

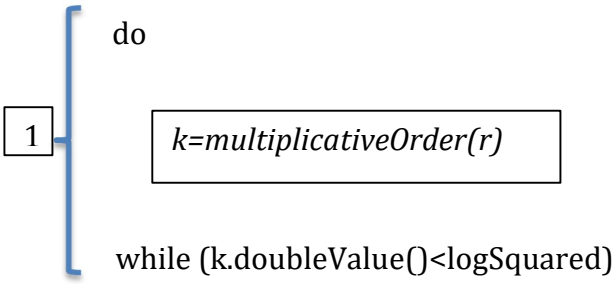
Cuestion 2. ¿Cuántas veces se ejecuta [2]?

Sea b: base, k: testigo de número de iteraciones. (log es $\log_2$).
Resuélvase para determinar *k*. (*b* es la base una vez dentro del bucle interno).

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

Cuestion 3. ¿Complejidad de la ejecución en [2]?

Cuestion 4. ¿Cuántas veces se ejecuta [1]?



Búsquese en la literatura sobre AKS cuál es el *r* máximo tal que $O_r(n) > log_2{}^2 n$

Cuestión 5. ¿Cuál es el máximo de iteraciones en *multiplicativeOrder*?
Hágase un pequeño estudio empírico con varios valores de *n*, p. ej. 8 y 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 prácticos introductorios).

Cuestiones básicas sobre la complejidad de AKS (Condición suficiente)

Primero fijamos un límite para el bucle (1) $\sqrt{\phi(r)}\log(n)$ (*limit* en el código)

Luego ejecutamos el bucle. Es el análisis de la condición suficiente.

Estudio de la complejidad.

Calculamos la complejidad de (1). Para ello analizamos la complejidad de calcular $\phi(r)$ (*Totient*)
Totient tiene un for externo y un while interno.

Cuestión 7
¿Cuántas veces se ejecuta el for externo?

Cuestión 8
¿Cuántas veces se ejecuta el while interno?
¿Cuál es la complejidad del cálculo de *totient?*

Calculamos el límite. Nos dará el máximo de ejecuciones.

Cuestión 9 ¿Cuál es el máximo $\phi(r)$?

(No confundamos el máximo $\phi(r)$ con el coste de calcular $\phi(r)$)

Cuestión 10 ¿Cuál es el máximo $\phi(r)$ en términos de n?

Calculamos la complejidad de la ejecución en el interior del bucle

Es la parte de la división polinómica.
El test de nulidad requiere $O(\log n)$ multiplicaciones de polinomios de grado *r* con coeficientes no mayores que $O(\log n)$. ¿Cuántas operaciones se requieren?