3. Algoritmo

Algoritmo 1 AKS

Entrada: $n \in Z^+$

PASO 1:
si $n = a^b$ **con** $a \in N \wedge b > 1$ **entonces**
devolver `COMPUESTO`
fin si

PASO 2:
Encontrar $min(r) \in N : O_r(n) > log^2 n$ **con** $r < n$

PASO 3
si $1 < mcd(a, n) < n$ **para algún** $a \leq r$ **entonces**
devolver `COMPUESTO`
fin si

PASO 4
si $n \leq r$ **entonces**
devolver `PRIMO`
fin si

PASO 5
$a = 1$
mientras $a < \lfloor \sqrt{\phi(r)} \rfloor * log_2(n)$ **hacer**
si $(X + a)^n \not\equiv X^n + a \ mod \ (mod \ X^r - 1, n)$ **entonces**
devolver `COMPUESTO`
fin si
fin mientras
devolver `PRIMO`