NOTAS SOBRE ALGORITMO AKS

- ANÁLISIS DE LA CONDICIÓN SUFICIENTE -

Lema

Sea $a < n$, $mcd(a,n) = 1$, n es primo (sii)

$$(X+a)^n \equiv (X^n + a) \pmod n$$

Ej 1 $a=1$ $n=3$

el resto de $\dfrac{(X+1)^3 - (X^3+1)}{3}$ es $0 \Rightarrow 3$ es primo

Ej 2 $a=3$ $n=5$

el resto de $\dfrac{(X+3)^5 - (X^5+3)}{5}$ es $0 \Rightarrow 5$ es primo

Mejora

$$(X+a)^n \equiv (X^n + a) \pmod{X^r - 1}$$ en el anillo de los enteros módulo n *

Ejemplo 3 $a=3$ $n=5$

$$(X+3)^5 \equiv X^5 + 3 \pmod{X^4 - 1}$$

- resto de dividir el resto de $(X+3)^5 : (X^4-1)$ por 5 es igual al resto de dividir el resto de $(X^5+3) : (X^4-1)$ por 5
- También podemos decir que el resto de dividir el resto de $\left[(X+3)^5 - (X^5+3)\right] : (X^4-1)$ por 5 es 0

Para (r) tomamos el menor r tal que $Or(n) > \log_2^2 n$.

$Or(n)$ es el orden de n módulo r y representa el menor k tal que $n^k \equiv 1 \pmod r$. Ejemplo

---

* Pero algunos números compuestos cumplen esto. Sin embargo haciendo la prueba de la mejora para unos cuantos números se garantiza la primalidad

$O_3(5) = 2$, ya que en

$5^h \equiv 1 \pmod 3$ $(5^2 - 1) : 3$ de resto 0, y 2 es el número más pequeño que lo cumple.

-ooo-

Para a examinarnos en rango de enteros $[1, 2\sqrt{r}\log_2 n)$ * si en todos los casos se cumple la congruencia, n es primo.

* Hay una mejora: en lugar de $\sqrt{r}$, hacer $\sqrt{\varphi(r)}$

$\varphi(r)$ es el número de enteros positivos menores o iguales que r, y coprimos con r (su mcd es 1)

Ej: $\varphi(9) = 6$

Estudio de Totient

$\varphi(n)$ es el número de naturales menores o iguales que n tales que n es coprimo con ellos

$$\varphi(n) = |\{m \in \mathbb{N} \mid m \leq n \wedge \text{mcd}(n,m) = 1\}|$$

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

p son los distintos primos que dividen a n

Ej: $\varphi(18) = 18 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 6$

Se calcula totient(n)