$$N = P \cdot Q$$

$$\phi(N) = (P-1)\cdot(Q-1)$$

$$m \in \{0, \ldots, N-1\}$$

$$\boxed{(e, N)} \qquad (d, N)$$

$$(m^e \bmod N)^d \bmod N = m$$

$$m^{e \cdot d} \bmod N = m$$

$$\boxed{m^{e \cdot d} \equiv m \mod N}$$

$$e \cdot d \equiv 1 \mod \phi(N)$$

$$\phi(N) \mid e \cdot d - 1$$

$$\alpha \cdot \phi(N) = e \cdot d - 1$$

$$\therefore \boxed{e \cdot d = \alpha \phi(N) + 1}$$

$$\boxed{m^{\alpha\phi(N)+1} \equiv m \mod N}$$

$m \in \{0, \ldots, N-1\}$ $\boxed{N = P \cdot Q}$

$\mathrm{MCD}(m, P) = 1$

$$m^{P-1} \mod P = 1$$

$$m^{P-1} \equiv 1 \mod P$$

$$\boxed{(m^{P-1})^{q-1} \equiv 1^{q-1}} \mod P$$

$$m^{\alpha\phi(N)} \equiv 1 \mod P$$

$$\boxed{m^{\alpha\phi(N)+1} \equiv m \mod P}$$

$\mathrm{MCD}(P, m) > 1$ $\boxed{m \equiv 0 \mod P}$

$$\boxed{m^{\alpha\phi(N)+1} \equiv m \mod P}$$

① $m^{\alpha\phi(N)+1} \equiv m \mod P$

$m \in \{0, \ldots, N-1\}$

② $\boxed{m^{\alpha\phi(N)+1} \equiv m \mod Q}$

① $P \mid m^{\alpha\phi(N)+1} - m$

$\beta \cdot P = m^{\alpha\phi(N)+1} - m$ ①

② $\gamma \cdot Q = m^{\alpha\phi(N)+1} - m$ ②

$\boxed{\beta \cdot P} = \boxed{\gamma \cdot Q}$ $\quad \therefore \gamma = P \cdot \gamma'$

$\therefore P \mid \boxed{\gamma \cdot Q}$

② $\gamma' \underbrace{P \cdot Q}_{N} = m^{\alpha\phi(N)+1} - m$

$\therefore m^{\alpha\phi(N)+1} \equiv m \mod N$

$P \longrightarrow BPP$

$$\boxed{FACT = \{ (n, k) \ / \ \text{existe } \ell \text{ tal que } \ell \mid n \text{ y } 2 \leq \ell \leq k \}}$$

n k 2 n

$(n, 2)$

$(n, 3)$

$O\left(\frac{n}{2}\right)$

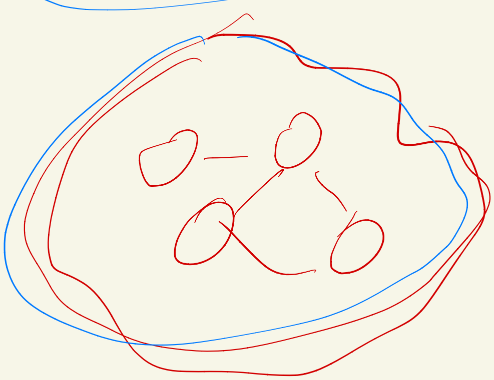
$\log_2 n$ $O\left(\frac{2^{(\log_2 n)}}{2}\right)$

$\left(n, \left\lfloor \frac{n}{2} \right\rfloor\right) \in FACT$ $\xrightarrow{NO}$ n es primo

$\xrightarrow{sí}$

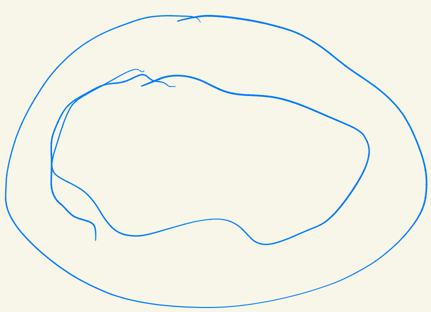
$\log_2 n \, (\log_2 n)^2$

FACT $\in$ NP



$(n,k) \in \mathrm{FACT}$

$\ell \qquad \underline{\ell \mid n} \qquad 2 \leq \ell \leq k$



p primo

$$a^{p-1} \bmod p = 1$$

$$a \in \{1, \dots, p-1\}$$

---

n compuesto

$$a^{n-1} \bmod n \neq 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

existe $a \in \{1, \dots, n-1\}$

$a | n$

$a > 1$ $\qquad a^{n-1} \not\equiv 1 \mod n$

$$a \cdot a^{n-2} \cancel{\not\equiv} 1 \mod n$$

$\mathrm{MCD}(a, n) > 1$

n

sacar al azar $a \in \{1, \dots, n-1\}$

$$a^{n-1} \bmod n \begin{cases} \xrightarrow{1} \text{primo} & \frac{1}{2} \\ \xrightarrow{\neq 1} \text{Compuesto} & \checkmark \end{cases}$$

$$\frac{1}{2} \longrightarrow \left(\frac{1}{2}\right)^{100}$$

n compuesto

$$\Pr_{a \leftarrow \{1,\dots,n-1\}} \left(a^{n-1} \equiv 1 \bmod n \right) \leq \frac{1}{2}$$

$$= \frac{|\{a \,/\, a^{n-1} \equiv 1 \bmod n\}|}{n-1}$$

$$|\{a \,/\, a^{n-1} \equiv 1 \bmod n\}| \leq \frac{n-1}{2}$$

n es compuesto

$$\mathrm{MCD}(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

$$\{a \,/\, a^{n-1} \equiv 1 \mod n\}$$

$$= \{a \,/\, \mathrm{MCD}(a, \underline{n}) = 1\}$$

$$a^{n-1} \mod n$$

$$a^{n-1} \mod n$$

$$a^{\frac{n-1}{2}} \mod n$$

n es primo

$(x-1)(x+1)$

x^2-1

$$a^{n-1} \equiv 1 \mod n$$

$$a^{\frac{n-1}{2}} \equiv 1 \mod n$$

$$a^{\frac{n-1}{2}} \equiv -1 \mod n$$

$$a^{n-1} - 1 \equiv 0 \mod n$$

$$\underbrace{\left(a^{\frac{n-1}{2}} - 1\right)}_{0}\underbrace{\left(a^{\frac{n-1}{2}} + 1\right)}_{0} \equiv 0 \mod n$$

$$a^{\frac{n-1}{2}} + 1 \equiv 0 \mod n$$

n es primo

$a \in \{1, \ldots, n-1\}$

$a^{\frac{n-1}{2}} \equiv 1 \mod n$

o

$a^{\frac{n-1}{2}} \equiv n-1 \mod n$

$$\underbrace{\hspace{6em}}_{}$$

100

$1 \text{ ——— } 1$

$\frac{1}{2}$

$n - 1 = 2^r \cdot d$

d es impar

$$\boxed{n = 2^r \cdot d + 1}$$

n es primo

$a^{n-1} \bmod n = 1$ ✓

$a^{2^r \cdot d} \bmod n = 1$

$a^{2^{r-1} \cdot d} \bmod n = a^{\frac{n-1}{2}} \bmod n$

$\boxed{1}$ ✓ $\quad -1$ ✓

$a^{2^{r-2} \cdot d} \bmod n$

$a^{\left(\frac{\frac{(n-1)}{2}}{2}\right)} \equiv 1 \bmod n$ → -1 ✓, → 1

$\equiv -1$