**Corolario:** Sea $n \in \mathbb{Z}^+$

1) Si $n$ tiene descomposición factorial $n = p_1^{e_1} \dots p_k^{e_k}$ con los $p_i$ primos distintos
$\Rightarrow \varphi(n) = (p_1^{e_1} - p_1^{e_1-1}) \dots (p_k^{e_k} - p_k^{e_k-1})$

2) $\varphi(n) = n \prod_{\substack{p \text{ primo} \\ p \mid n}} (1 - 1/p)$

**Corolario:** Sean $a, n$ dos enteros coprimos

1) Si $m \in \mathbb{Z}$ y $m = \varphi(n).q + r \Rightarrow a^m \equiv a^r \pmod n$

2) Si $m \equiv k \pmod{\varphi(n)} \Rightarrow a^m \equiv a^k \pmod n$

## Exponenciación Rapida

Este metodo se usa cuando queremos calcular $s^m \bmod n$ con $0 \le s < n$ y $0 \le m < \varphi(n)$

Llamamos $s_k = s^{2^k}$

- $s_1 = s^2$
- $s_2 = s^{2^2} = s_1^2$
- $s_3 = s^{2^2 \cdot 2} = s_2^2$
- $\vdots$
- $s_k = s^{2^k} = s^{2^{k-1} \cdot 2} = (s^{2^{k-1}})^2 = (s_{k-1})^2$

$$\boxed{s_k = (s_{k-1})^2}$$

Escribimos $m$ en su Representación binaria

$m = \sum_{i=0}^{r} a_i . 2^i$ con $a_i \in \{0, 1\}$ $\quad k \le \log_2(m) = r$

$$\Rightarrow s^m = s^{\sum a_i . 2^i} = \prod_{i=0}^{r} s^{a_i . 2^i} = \prod_{i=0}^{r} (s^{2^i})^{a_i} = \prod_{i=0}^{r} (s_i)^{a_i}$$

## ¿Como hacer los ej. de potencia?

Tenemos que encontrar $0 \le r < n$:
$a^k \equiv r \bmod n$ $\quad a \in \mathbb{Z}$ y $k, n \in \mathbb{Z}^+$

1) Reducir el modulo, es decir buscar $0 \le s < n$ / $a \equiv s \bmod n$
$\Rightarrow a^k \equiv s^k \bmod n$.

2) Si $\mcd(s, n) = 1 \Rightarrow s^{\varphi(n)} \equiv 1 \bmod n$,
Divido $k$ entre $\varphi(n) \Rightarrow k = \varphi(n).q + t$
con $0 \le t \le \varphi(n)$
$\Rightarrow s^k \equiv s^{\varphi(n).q+t} \equiv s^t \bmod(n)$

3) Usar TCR: $n = p_1^{e_1} \dots p_n^{e_n}$,
puedo cambiar el problema $s^t \equiv r \bmod n$ a
$$\begin{cases} s^t \equiv r \bmod p_1^{e_1} \\ \vdots \\ s^t \equiv r \bmod p_n^{e_n} \end{cases}$$
y vuelvo a aplicar (1) y (2) para cada $s^t \equiv r \bmod p_i^{e_i}$ $\forall i = 1, \dots, n$

4) Aplicar exponenciación rapida

## + Propiedades Practico:

- Si $p$ y $q$ son primos distintos:
$a^p \equiv a \pmod q$ y $a^q \equiv a \pmod p$
$\Rightarrow a^{pq} \equiv a \pmod{pq}$
- $\varphi(mn) = \dfrac{\varphi(m)\varphi(n).d}{\varphi(d)}$ con $d = \mcd(m, n)$