$$\frac{(p-1)(q-1)}{\gcd((p-1),(q-1))}$$

Fermat

$$a^{(p-1)} \equiv 1 \bmod p$$

$$a^{k(p-1)} \equiv 1 \bmod p$$

$$priv * pub = 1 \bmod [\varphi(p), \varphi(q)]$$

$$priv * pub - 1 = n \cdot [\varphi(p) \cdot \varphi(q)] = n \cdot k (p-1)(q-1)$$

$\downarrow$ $\varphi(p) \cdot \varphi(q)$

$$a^{k(p-1)\varphi(q)} - 1 = n \cdot p$$

$$2^{n \cdot k \varphi(p)\varphi(q)} - 1 = n \cdot p$$

$$2^{n \cdot k \varphi(p)\varphi(q)} - 1 = n q$$

$$2^{n \cdot k \varphi(p)\varphi(q)} - 1 = n \cdot p \cdot q$$

$$\gcd(2^{n \cdot k \varphi(p) \cdot \varphi(q)} - 1, p^2 q)$$

$\rightarrow pq$