Euler theorem: if a and n are coprime: $a^{\varphi(n)} \equiv 1 \pmod{n}$

$\varphi(n) = n - 1$ if n is prime

$n = a * b$; a, b coprime: $\varphi(n) = \varphi(a) * \varphi(b)$

Problem: $a^b \% 1337$

if: $a \% 1337 = 0 \Rightarrow 0$

if $a \not\vdots 7$ and $a \not\vdots 9 \Rightarrow a$ and 1337 are co-prime.

$\Rightarrow a^{\varphi(1337)} \equiv 1 \pmod{n}$

let $b = k\varphi(1337) + q$

$\Rightarrow a^b \% 1337 = a^{k\varphi(1337)+q} \% n = a^q \% n$

if $a \vdots 7$ or $a \vdots 9$.

$\Rightarrow$ similar $a \vdots 9$

let assume: $a \vdots 7$

$\Rightarrow a = 7^k x$

$\Rightarrow a^b = 7^{bk} \times x^b$

$\Rightarrow a^b \% n = (7^{bk} x^b) \% n = ((7^{bk} \% 1337) \times (x^b \% 1337)) \% 1337$

$= ((7^{1140pk+qk} \% 1337) \times (x^{1140p+q} \% 1337)) \% 1337$

$= (7(7^{1140pk+qk-1})) \% 1337 \times (x^{1140p+q} \% 1337) \% 1337$

$= (7^{1140pk+qk-1} \% 191) \times (x^{1140p+q} \% 1337) \% 1337$

$= (7^{qk-1} \% 191) \times (x^{1140p+q} \% 1337) \% 1337$

$= ((7^{qk} \% 1337) \times (x^{1140p+q} \% 1337)) \% 1337$

$= (7^{qk} \% 1337) \times (x^q \% 1337) = (7^k x)^q \% 1337$

Sol 2: Fermat + Chinese remain theorem

* Fermat nhỏ: p is prime , $n \in \mathbb{N}$, $(n,p) = 1$

$$\Rightarrow \begin{cases} n^{p-1} \equiv 1 \pmod p \\ \phi(p) = p-1 \end{cases}$$

* Euler : $a, m \in \mathbb{N}$; $(a,m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \pmod m$

* Inverted modulo: $x^{-1} \pmod M$; M is prime

$$x^{-1} \equiv x^{M-2} \pmod M$$

* Chiness remaind theorem (CRT)

Given $2n$ $\{a_i\}$; $\{m_i\} \in \mathbb{N}$; $\forall i,j\ (m_i, m_j) = 1$.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

The solution set: $x \equiv \sum_{i=1}^{n} P_i P_i^{-1} a_i \pmod M$

When $M = \prod_{i=1}^{n} m_i$; $P_i = \frac{M}{m_i}$; P_i^{-1} is inverse modulo m_i of P_i

Back to problem: $a^b \bmod 1337$

$1337 = 7 \times 191$ (not prime) $\Rightarrow$ apply CRT.

let : $u = a^b \% 7$; $v = a^b \% 191$.
we can calculat u, v by Fermat small

So:

$m_1 = 7$ $\quad P_1 = \frac{1337}{7} = 191$; $[P_1^{-1}]_{m_1} = [191^{-1}]_7 = 4$

$m_2 = 191$ $\quad P_2 = \frac{1337}{191} = 7$; $[P_2^{-1}]_{m_2} = [7^{-1}]_{191} = 82$

$$\Rightarrow \quad a^b \equiv 191 \times 4 \times u + 7 \times 82 \times v \pmod{1337}$$

$$\Rightarrow \quad a^b \equiv 764 \times u + 574 \times v \pmod{1337}$$