

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: $a^b \pmod{1337}$

$$\text{if } a \pmod{1337} = 0 \Rightarrow 0$$

if $a \not\equiv 0$ and $a \not\equiv 9 \Rightarrow a$ and 1337 are co-prime
 $\Rightarrow a^{\varphi(1337)} \equiv 1 \pmod{n}$

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

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

if $a \not\equiv 7$ or $a \not\equiv 9$

let assume: $a \not\equiv 7 \Rightarrow$ similar $a \not\equiv 9$

$$\Rightarrow a = 7^k x$$

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

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

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

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

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

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

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

$$= (7^{qk} \pmod{1337}) \times (x^q \pmod{1337}) = (7^k \pmod{191})^q \pmod{1337}$$