定理 2.4 $(a, m) = 1$，证：$a^{\varphi(m)} \equiv 1 \pmod{m}$.

设 $r_1, \ldots, r_{\varphi(m)}$ 为模 m 的最小正简化剩余系，则 $(a, m) = 1$ 时，

$ar_1, \ldots, ar_{\varphi(m)}$ 遍历该简化剩余系.

$\Rightarrow r_1 \cdots r_{\varphi(m)} \equiv (ar_1) \cdots (ar_{\varphi(m)})$ ~~mod (m)~~ $\pmod{m}$

$\Rightarrow (a^{\varphi(m)} - 1)(r_1 r_2 \cdots r_{\varphi(m)}) \equiv 0 \pmod{m}$

由 $(r_i, m) = 1 \Rightarrow a^{\varphi(m)} - 1 \equiv 0 \pmod{m} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

$2^{20210322} \equiv 2^6 \equiv 1 \pmod{7}$

1. (1) $2^{20210322} \bmod 7$.

$2^3 \equiv 1 \pmod{7}$

(2) ~~20210322~~ $2^4 = 16 \equiv -1 \pmod{17}$.

$20210322 = 1263145 \times 16 + 2$

$2^{20210322} \equiv (\ldots)^{1263145} \cdot 2^2 \equiv (-1) \cdot 4 \equiv -4$ ~~mo~~ $\equiv 13$ (mod