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

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

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

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

$\Rightarrow (a^{\varphi(m)}-1)(r_1r_2\cdots r_{\varphi(m)})\equiv 0 \pmod m$

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

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

$2^3\equiv 1 \pmod 7$ $\qquad 2^{20210322}\equiv 2^6\equiv 1 \pmod 7$

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

~~$20210322 = 1263145\times 16$~~ $+2$

~~$\Rightarrow 2^{20210322}\equiv(-1)^{1263145}\cdot 2^2 \equiv (-1)\cdot 4\equiv -4$~~ ~~mo~~ $\equiv 13 \pmod{17}$.

$(2,17)=1 \Rightarrow 2^{16}\equiv 1 \pmod{17}$.

$2^{20210322}\equiv 2^2\equiv 4 \pmod{17}$.

(3) $\varphi(7\cdot 17)=7\cdot 17\times\frac{6}{7}\times\frac{16}{17}=96$.

$(2,7\times 17)=1$. $\quad 2^{96}\equiv 1 \pmod{119} \Rightarrow$ ~~2^{18}~~ $2^{20210322}\equiv 2^{18} \pmod{119}$.

$2^9=512$, $\quad 512\equiv 36 \pmod{119}$

$\Rightarrow 2^{18}=2^9\cdot 2^9\equiv 36\cdot 36$ ~~(mod 119)~~ $\equiv 1296\equiv 106 \pmod{119}$.

2\. $a\in\{1,2,3,4,5,6,0\}$ $\qquad p=7$.

$a^6\equiv 1 \pmod p$. $\Leftrightarrow a^6\equiv 1 \pmod 7$.

a^{202103} ~~mod~~ $\equiv a^5 \pmod 7$.

~~$x^{20210322}$~~ $a^{20210322}\equiv 1 \pmod 7$.

$a^{2021}\equiv a^5 \pmod 7$ $\qquad a^{322}\equiv a^4 \pmod 7$.

$\Rightarrow f(a)\equiv 2a^5+a^4+2 \pmod 7$.

$f(0)\equiv 1$

$f(1)\equiv 5$

$f(2)\equiv 5$

$f(3)\equiv 2$

$f(4)\equiv 3$

$f(5)\equiv 3$

$f(6)\equiv 1$

(ii) $a^{2^{17}} \equiv a^2 \pmod 7$ $\quad a^7 \equiv a \pmod 7$ $\quad a^6 \equiv 1 \pmod 7$.

$a^{2^4} \equiv a^4 \pmod 7$

$f(a) \equiv 2a^4 + a^2 + a + 1 \pmod 7$.

$f(0) \equiv 1$ $\quad f(4) \equiv 1$

$f(1) \equiv 5$ $\quad f(5) \equiv 0$

$f(2) \equiv 4$ $\quad f(6) \equiv 3$

$f(3) \equiv 0$

3. 当 n 是素数：

当 $n=2$，显然.

当 $n \geq 3$：对每个整数 $1 \leq a \leq n-1$，存在唯一的整数 a' 使 $(1 \leq a' \leq n-1)$

$a \cdot a' \equiv 1 \pmod n$.

若 $a = a'$，则 $a^2 \equiv 1 \pmod n$，反之亦然.

"$\Rightarrow$"：显然

"$\Leftarrow$" $a^2 \equiv 1$，$a \cdot a' \equiv 1 \Rightarrow a(a-a') \equiv 0 \pmod n$ 由 $(a,n)=1$.

$\Rightarrow a - a' \equiv 0$ 由 $1 \leq a, a' \leq n-1 \Rightarrow a = a'$.

$1 \cdot 2 \cdot \cdots (p-2)(p-1)$. 将 ~~2，p~~ 2 至 $p-2$ 的整数配对 $\Rightarrow$.

$1 \cdot (p-1) \prod_a a' a \equiv p-1 \equiv -1 \pmod p$. 证毕.

若 p 不是素数，$p = ab$，$a \neq 1$ 且 $b \neq 1$.

当 k 从 1 遍历至 $p-1$ 时，必有 $k = (a-1)b$ 与 $k = a(b-1)$.

累乘，$(p-1)!$ 中含 a 与 b. 则 $(p-1)! = K \cdot a \cdot b \equiv 0 \pmod p$.

矛盾！ $\Rightarrow p$ 为素数 .