拓展：证明：存在一个由正整数组成的单增数列 $\{a_n\}$，使得对任意 $k\in N^+$ 数列 $\{k+a_n\}$ 中都至多有有限项为素数

proof：用 $p_1, p_2 \cdots$ 表示所有素数由小到大排列

令 $a_1=2$，现设 $a_1 \cdots a_n$ 确定，若 a_{n+1} 满足

$$\begin{cases} x\equiv 0 \pmod{p_1} \\ x\equiv -1 \pmod{p_2} \\ \vdots \\ x\equiv -n \pmod{p_{n+1}} \end{cases}$$

存在 a_{n+1}

取 a_{n+1} 满足且大于 a_n → $\{a_n\}$ 递增

对 $\forall k\in N^+$ $n\geq k+1$ 时 $k+a_n\equiv 0 \pmod{p_{k+1}}$，且从 $k+2$ 项起

有项都是 p_{k+1} 倍数 → $\{k+a_n\}$ 中至多有 $k+1$ 项为素数

---

1) 证明：$n \mid \varphi(a^n-1)$ $a>1$ $\in N^+$

$a^n\equiv 1 \pmod{a^n-1}$ 且 n 最小（因为 $1\leq k<n$ $a^k\not\equiv 1 \pmod{a^n-1}$）

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

$n \mid \varphi(a^n-1)$

$\delta_m(a^k) = \frac{\delta_m(a)}{(\delta_m(a), k)}$ a 模 m 的阶为 $\delta_m(a)$

$(a^k)^{\delta_m(a^k)} \equiv 1 \pmod{n}$

$\delta_m(a) \mid k\,\delta_m(a^k)$

$\rightarrow \frac{\delta_m(a)}{(\delta_m(a), k)} \mid k\,\delta_m(a^k)$

$a^{\delta_m(a)} \equiv 1 \pmod{m}$

$(a^k)^{\frac{\delta_m(a)}{(\delta_m(a),k)}} = (a^{\delta_m(a)})^{\frac{k}{(\delta_m(a),k)}} \equiv 1 \pmod{m}$

$\delta_m(a^k) \mid \frac{\delta_m(a)}{(\delta_m(a), k)}$

$a^b \bmod c = \begin{cases} a^b \bmod c & b < \phi(c) \\ a^{b \bmod \phi(c) + \phi(c)} \bmod c & b \geq \phi(c) \end{cases}$

作用：快速求幂

$b \geq \phi(c)$ 时：对 c 素因子分解 $c = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

即证 $a^b \equiv a^{b \bmod \phi(c) + \phi(c)} \pmod{p_i^{e_i}}$

1) $p_i \nmid a$ $\quad a^{\phi(c)} \equiv 1 \pmod{p_i^{e_i}}$

$a^b \equiv a^{\left[\frac{b}{\phi(c)}\right]\phi(c) + b \bmod \phi(c)}$

$\equiv a^{b \bmod \phi(c)} \equiv a^{b \bmod \phi(c) + \phi(c)} \pmod{p_i^{e_i}}$

2) $p_i \mid a$ $\quad b \geq \phi(c) \geq \phi(p_i^{e_i}) \geq e_i$

~~$p_i \mid (a^b)$~~ $\quad p_i^{e_i} \mid a^b$

$p_i^{e_i} \mid a^{\phi(c)}$

威尔逊定理：$(p-1)! \equiv -1 \pmod p$ p为素数

proof：$\forall a \in [p]$ $\exists$ 唯一 b $ab \equiv 1 \pmod p$

除1和自己 $1 \cdot 1 \equiv 1 \pmod p$

$(p-1)^2 \equiv 1 \pmod p$

$\rightarrow (p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod p$

$V_p(n)$：n中p的幂，即 $p^{V_p(n)} \mid n$ 且 $p^{V_p(n)+1} \nmid n$

$V_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$

$a^2 \equiv 0, 1 \pmod 3$ $a^2 \equiv 0, 1 \pmod 4$

多项式意义下整除：$(x-1) \mid (x+1)(x-2) = x^2 - 3x + 2$

多项式意义下中国剩余：

$$\begin{cases} f(x) \equiv 1 \pmod{(x-1)} \\ ! \\ f(x) \equiv n \pmod{(x-n)} \end{cases}$$

要证明 左式 = 右式

可考虑 左式 $\mid$ 右式 且 右式 $\mid$ 左式