



江苏省前黄高级中学
Jiangsu Qianhuang Senior Middle School



2024.7 杭州

科目: 数论

班级: _____

姓名: 曹宇航

* 整除理论

1. 带余法定理: 设 $a, b \in \mathbb{Z}$ 且 $b > 0$, 则存在唯一的 $q, r \in \mathbb{Z}$, 使 $a = bq + r$

其中 $0 \leq r < b$

(1) $\frac{a}{b} = q + \frac{r}{b}$, 其中 $0 \leq \frac{r}{b} < 1$, 因此 $q = [\frac{a}{b}]$

(2) 设 $a, b \in \mathbb{N}^*$, 则 $1, 2, \dots, a$ 中能被 b 整除的数的个数为 $[\frac{a}{b}]$

2. 裴蜀定理: 设 $a, b \in \mathbb{Z}$, 不全为 0, 则存在 $s, t \in \mathbb{Z}$, 使得 $as + bt = (a, b)$

(1) $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$

(2) 若 $d|a, d|b$, 则 $d|(a, b)$

3. 算术基本定理

设正整数 $n > 1$, 则 $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, 其中 $p_1 < p_2 < \dots < p_k$ 为素数, $\alpha_i \geq 1, i=1, \dots, k$

(1) 设 $n \in \mathbb{N}^*$, 则 $n = 2^{\alpha} \cdot b$ 其中 $2 \nmid b, \alpha \geq 0$

(2) 设 $n \in \mathbb{N}^*$, 则 $n = a^2 \cdot b$, 其中 $a, b \in \mathbb{N}^*$, b 为平方因子

4. 恒等式 $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$

推论 $a^m - 1 | a^n - 1 \Leftrightarrow m | n$

5. 抽屉原理

设 $m \in \mathbb{N}^*, m > 1, (a, m) = 1$, 则 $\exists t \in \mathbb{N}^*, 1 \leq t < m$, 使 $m | at - 1$

题:

1. (1) 分析: 设 $n \in \mathbb{N}^*, p \nmid n$, 如果 n 不为好数, 那么存在正整数 $m \neq n$ 使 $\{\frac{p^n}{n^p}\} = \{\frac{p^m}{m^p}\}$

不妨设 $m = p^{\alpha} \cdot m_1$, 其中 $p \nmid m_1, \alpha \geq 0$. 因此有 $\{\frac{p^{m_1}}{m_1^p}\} = \{\frac{p^n}{n^p}\}$, 从而 $\frac{p^{m_1}}{m_1^p} - \frac{p^n}{n^p} = L$ 其中 $L \in \mathbb{Z}$. 因此有 $n^p p^{m_1} - m_1^p n^p = m_1^p \cdot n^p \cdot L$

因此 $m_1^p | n^p \cdot p^{m_1}$ 且

$m_1^p | n^p$ 且 $n^p | m_1^p$ 从而 $m_1 = n$, 因此 $m = p^{\alpha} n$ 其中 $\alpha \geq 1$. 代入 (*)

有 $\{\frac{p^{m_1}}{n^p}\} = \{\frac{p^n}{n^p}\}$ 从而 $n^p | p^{m_1} - p^n = p^n (p^{m_1-n} - 1)$

因此 $n^p | p^{m_1-n} - 1 = p^{\alpha \cdot n - n - p\alpha} - 1 = p^{(p^{\alpha}-1)n - p\alpha} - 1$

总结: 若 n 为正整数, $p \nmid n$, 且 n 不是好数, 则存在正整数 k , 使得

$$n^p | p^{(p^{\alpha}-1)n - p\alpha} - 1$$

(2) 构造: $n_g = \frac{p^{pg}-1}{p^g-1}$ 其中 g 为大于 p 的素数

1° 先证 n_g 为合数且 $p \nmid n_g$

$$p^g-1 \mid p^{pg}-1, \text{ 因此 } \frac{p^g-1}{p-1} \mid \frac{p^{pg}-1}{p-1} = \frac{p^{pg}-1}{p^g-1} \cdot \frac{p^g-1}{p-1}$$

$$\text{又 } (p^g-1, p^p-1) = p^{(p,g)}-1 = p-1 \text{ 因此 } \left(\frac{p^g-1}{p-1}, \frac{p^p-1}{p-1}\right) = 1$$

$$\frac{p^{pg}-1}{p-1} \mid \frac{p^{pg}-1}{p^g-1} \cdot \frac{p^g-1}{p-1}, \therefore 1 < \frac{p^g-1}{p-1} < \frac{p^{pg}-1}{p^g-1} = n_g$$

$$\text{从而 } n_g \text{ 为合数, 又 } n_g = \frac{p^{pg}-1}{p^g-1}, \text{ 那么 } (p^p-1)n_g = p^{pg}-1$$

$$\text{因此 } p \nmid n_g$$

2° 若 $g \neq r$ 均大于 p 的素数, 则 $(n_g, n_r) = 1$

$$\text{观察: } (p^{pg}-1, p^{pr}-1) = p^p-1, \text{ 因此 } \left(\frac{p^{pg}-1}{p^g-1}, \frac{p^{pr}-1}{p^r-1}\right) = 1$$

$$\text{从而 } (n_g, n_r) = 1$$

3° $n = n_g = \frac{p^{pg}-1}{p^g-1}$ 为合数

反证法: 假设 n 不是合数, 又 $p \nmid n$, 利用 (1), 存在正整数 $\alpha \geq 1$, 使

$$n^p \mid p^{(p^p-1)n-p^\alpha}-1, \text{ 从而 } n \mid p^{(p^p-1)n-p^\alpha}-1$$

$$\text{又 } (p^p-1)n = p^{pg}-1, \text{ 从而 } n \mid p^{(p^p-1)n-p^\alpha}-1$$

$$\text{因此 } n \mid (p^{(p^p-1)n-p^\alpha}-1, p^{pg}-1) = p^{((p^p-1)n-p^\alpha, pg)}-1 = p^\alpha-1$$

$$\text{其中 } d = ((p^p-1)n-p^\alpha, pg) = ((p^p-1)n-p^\alpha, g) \mid g \text{ 即 } d \mid g, \text{ 从而}$$

$$p^d-1 \mid p^g-1, \text{ 又 } n \mid p^d-1, \text{ 从而 } n \mid p^g-1, \text{ 因此 } n \leq p^g-1$$

$$\text{但是 } n = \frac{p^{pg}-1}{p^g-1} > p^g-1, \text{ 矛盾 } \#$$

2. 略

3. 分析: 引理: 设 a, m 均为正整数, 则数列 $\{a^n\}_{n=1}^{+\infty}$ 模 m 的数列是准周期的
 具体地说, $\exists n, T \in \mathbb{N}^+$, 均不大于 m , 满足条件对 $\forall n \geq n_0$ 均有 $a^{n+T} \equiv a^n \pmod{m}$

证明: 考虑以下的 $m+1$ 个数 $a^1, a^2, a^3, \dots, a^{m+1}$

利用抽屉原理, 存在 $1 \leq i < j \leq m+1$, 使 $a^i \equiv a^j \pmod{m}$

取 $n_0 = i$, $T = j - i$, 则 $n_0 \leq m$, $T \leq m$ 且 $a^{n_0+T} \equiv a^{n_0} \pmod{m}$?

因此 $a^{n_0+T} \equiv a^{n_0+1} \pmod{m}$

$a^{n_0+2T} \equiv a^{n_0+2} \pmod{m}$

$\vdots$
 $a^{n+T} \equiv a^n \pmod{m} \quad \forall n \geq n_0$

回到原题, 对 b 利用数学归纳法

1° $b=1$ 时, 结论成立

2° 假设 $b < m$ 结论成立, 其中 $(b, c) = (m, c) = 1$, 则 $b=m$ 时:

$\{d \cdot a^n\}_{n=1}^{+\infty}$ 模 m 是准周期的, 因此存在 $n_0, T \in \mathbb{N}^+$, 使得对 $\forall n \geq n_0$ 都有 $d \cdot a^{n+T} \equiv d \cdot a^n \pmod{m}$, 可以要求 T 是最小的, 由于 $T \leq m$, 那么分情况讨论 ① 若 $T=m$, 则 $\exists n \geq n_0$ 使 $m \mid d \cdot a^n$

因此对 $\forall n \geq n_0$, 均有 $m \mid d \cdot a^n$, 从而 $T=1$

因此 $m=1$, 结论成立

② 若 $T < m$, 令 $s = (T, m)$. 显然 $s < m$, 而且 $(s, c) = 1$

对 s , 利用假设, 存在无穷多正整数 s , 使

$$d \cdot a^n - cx \equiv e \pmod{s}$$

取一个适当大的正整数解 $x = x_0$ 使 $d \cdot a^{x_0} - cx_0 \equiv e \pmod{s}$

$$\text{即 } d \cdot a^{x_0} - cx_0 = e + sL \quad \text{其中 } L \in \mathbb{Z}$$

$$\text{考虑 } d \cdot a^{x_0+Ty} - c(x_0+Ty) \equiv e \pmod{s}$$

$$d \cdot a^{x_0} - c(x_0+Ty) \equiv e \pmod{s}$$

$$d \cdot a^{x_0} - c(x_0+Ty) = e + m\lambda$$

$$\text{又 } d \cdot a^{x_0} - cx_0 = e + sL \quad \text{从而 } sL = cTy + m\lambda$$

$$\text{因此 } c \cdot \frac{T}{s} \cdot y + \frac{m}{s} \lambda = L, \text{ 此时 } (c \cdot \frac{T}{s}, \frac{m}{s}) = 1$$

利用裴蜀定理, 上述不定方程有无穷多整数解 (y, z) ,

并且 $y > 0$, 任取一组解 (y_0, z_0) , $y_0 > 0$

取 $x_1 = x_0 + Ty_0$

则 $d \cdot a^{x_1} - cx_1 \equiv e \pmod{m}$

由于 $y_0 \rightarrow +\infty$, 那么 x_1 有无穷多

4. 分析: (1) $\varphi(n)$ 的性质: $1^\circ \varphi(1) = 1$

$2^\circ \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

3° 一般的 $n > 1$, 令 n 的标准分解式为 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

那么 $\varphi(n) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$

$= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1})$

4° 若 $n|m$, 则 $\varphi(n)|\varphi(m)$

$5^\circ \varphi(n) = 1$, 则 $n = 1$ 或 2 ; 若 $n \geq 3$, 则 $2|\varphi(n)$

(2) 回到原题, 对 m 分情况讨论

1° 若 $2|m$, 则取 $p = 3$, 因此 $\varphi(n) = 3m$ 无解

2° 若 $2 \nmid m$, 不妨设 m 的所有正因子分别引 $= d_1 < d_2 < \cdots < d_k = m$

再取 k 个互不相同的均大于 m 的素数 $q_1 < q_2 < \cdots < q_k$

考虑同余方程

$$\begin{cases} d_1 x \equiv -1 \pmod{q_1} \\ d_2 x \equiv -1 \pmod{q_2} \\ \vdots \\ d_k x \equiv -1 \pmod{q_k} \end{cases} \quad \text{即} \quad \begin{cases} x \equiv -d_1^{q_1-2} \pmod{q_1} \\ x \equiv -d_2^{q_2-2} \pmod{q_2} \\ \vdots \\ x \equiv -d_k^{q_k-2} \pmod{q_k} \end{cases}$$

因此, 利用中国剩余定理, 上述方程有整数解 $x = x_0$.

而且它的所有整数解为 $(x_0, q_1 q_2 \cdots q_k) = 1$

上述同余方程有一无穷多素数解 (Dirichlet 定理)

取一个素数解 $x = p$, 充分大, $p > q_1 \cdots q_k$

因此 $\varphi(m) = pm$ 无正整数解, 理由如下

反证法: 假设 $\varphi(m) = pm$ 有正整数解

分情况讨论: ① 若 $p|n_0$, 则 $\varphi(p)|\varphi(n_0)$ 因此 $p-1|pm$

又 $(p-1, p)=1$, 从而 $p-1|m$, 因此 $p-1 \leq m$, 与 p 充分大矛盾

② 若 $p \nmid n_0$, 由于 $p|\varphi(n_0)$, 那么存在 $q|n_0$ 使 $p|q-1$, 又 $\varphi(q)|\varphi(n_0)=pm$, 从而 $q-1|pm$

$\frac{q-1}{p}|m$

从而 $\frac{q-1}{p}=d_i, \exists i$. 因此 $d_i p+1=q$

而 $d_i p \equiv -1 \pmod{q_i}$, 从而 $q_i | d_i p+1=q$

因此 $q=q_i$ 从而 $d_i p+1=q_i$ 即 $p < q_i$, 与 p 充分大矛盾

5. 显然 d 不是完全平方数, 要求 $d \neq 0, 1 \pmod{4}$ 可以要求 $d \equiv 3 \pmod{4}$

$$n \lfloor d \rfloor \cdot \{n \lfloor d \rfloor\} = n \lfloor d \rfloor (n \lfloor d \rfloor - \lfloor n \lfloor d \rfloor \rfloor) = n \lfloor d \rfloor \frac{(n \lfloor d \rfloor)^2 - \lfloor n \lfloor d \rfloor \rfloor^2}{n \lfloor d \rfloor + \lfloor n \lfloor d \rfloor \rfloor} > n \lfloor d \rfloor \frac{n^2 d - \lfloor n \lfloor d \rfloor \rfloor^2}{2n \lfloor d \rfloor} = \frac{n^2 d - \lfloor n \lfloor d \rfloor \rfloor^2}{2}$$

只要满足 $n^2 d - \lfloor n \lfloor d \rfloor \rfloor^2 \geq 5$

取 $d \in \{a+1, \dots, a+20\}$ 满足 $d \equiv 15 \pmod{20}$

因此 d 不是平方数, 考虑方程 $x^2 - dy^2 = k, k=0, -1, -2, -3, -4, -5, \dots$

① 由于 d 不是平方数, 那么 $x^2 - dy^2 = k$ 无解

② 又 $d \equiv 3 \pmod{4}$, 那么 $x^2 - dy^2 = -1, x^2 - dy^2 = -4$ 均无解

③ 又 $5|d$ 那么 $x^2 - dy^2 = -2, -3$ 均无解

从而 $n^2 d - \lfloor n \lfloor d \rfloor \rfloor^2 \geq 5$ #

6. (1) Dirichlet 原理

① 若 α 为无理数, 则存在无穷有理数 $\frac{p}{q}$, 其中 $(p, q)=1, q>0$, 使 $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$

证明: 熟知 $\alpha = \lfloor \alpha \rfloor + \{ \alpha \}$ 其中 $0 < \{ \alpha \} < 1$, 因此 $|\alpha - \frac{0}{1}| < \frac{1}{1^2}$

想证“无穷”: 反证法: 如果只有有限个有理数符合条件, 不妨记为 $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_r}{q_r}$

因此 $|\alpha - \frac{p_i}{q_i}| < \frac{1}{q_i^2}, (p_i, q_i)=1, q_i>0, i=1, 2, \dots, r$

令 $\delta = \min \{ |\alpha - \frac{p_1}{q_1}|, \dots, |\alpha - \frac{p_r}{q_r}| \}$, 则 $0 < \delta < 1$

取正整数 $N > \frac{1}{\delta}$ 由于 α 为无理数, 利用 Dirichlet 原理

整数 h, k 使得 $|k\alpha - h| < \frac{1}{N}$, 其中 $1 \leq k \leq N$

因此 $|\alpha - \frac{h}{k}| < \frac{1}{kN} \leq \frac{1}{k^2}$, 又 $|\alpha - \frac{h}{k}| < \frac{1}{kN} \leq \frac{1}{N} < \delta$

令 $d=(h, k), h=dh_1, k=dk_1, (h_1, k_1)=1, 1 \leq k_1 \leq k$

因此, $\frac{h_1}{k_1} = \frac{p}{k}$, 从而 $\frac{h_1}{k_1} \notin \{\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_k}{q_k}\}$

而且 $|\alpha - \frac{h_1}{k_1}| = |\alpha - \frac{p}{k}| < \frac{1}{k} \leq \frac{1}{k_0}$, 矛盾.

(3) 本题 (Kronecker 定理)

1° 由于 α 为无理数, 那么存在无穷多个互素的整数对

使得 $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$ 其中 $q > 0$

因此 $\alpha = \frac{p}{q} + \frac{\lambda}{q^2}$, 其中 $|\lambda| < 1$

2° 由于 β 为实数, 对上述的 (p, q) , 存在整数 t , 使得 $|q\beta - t| \leq \frac{1}{2}$

因此 $|\beta - \frac{t}{q}| \leq \frac{1}{2q}$, 从而 $\beta = \frac{t}{q} + \frac{z}{2q}$, 其中 $|z| \leq 1$

3° $\alpha x - y - \beta = (\frac{p}{q} + \frac{\lambda}{q^2})x - y - (\frac{t}{q} + \frac{z}{2q}) = \frac{px - qy - t}{q} + \frac{\lambda x}{q^2} - \frac{z}{2q}$ (*)

由于 $(p, q) = 1$, 利用裴蜀定理, 存在 $x, y \in \mathbb{Z}$, 使得 $px - qy = t$

其中 $\frac{q}{2} \leq x < \frac{3}{2}q$, 代入 (*) 有 $|\alpha x - y - \beta| = |\frac{\lambda x}{q^2} - \frac{z}{2q}| < \frac{x}{q^2} + \frac{1}{2q}$

由于 $\frac{q}{2} \leq x < \frac{3}{2}q$, 那么 $q = \frac{2}{3}x$ 因此

$$\frac{x}{q^2} + \frac{1}{2q} < \frac{x}{(\frac{2}{3}x)^2} + \frac{1}{2 \cdot \frac{2}{3}x} = \frac{9}{4x} + \frac{3}{4x} = \frac{3}{x}$$

因此 $|\alpha x - y - \beta| < \frac{3}{x}$

又 $\frac{q}{2} \leq x, q \rightarrow +\infty$

那么 $x \rightarrow +\infty$, 从而 (x, y) 有无穷多组 #

7. 原式可改写为 $2024 \times 10^m \leq 2^n < 2025 \times 10^m$

$$\ln 2024 \leq n \lg 2 < \ln 2025$$

$$\text{即 } \lg 2024 \leq n \lg 2 < \lg 2025 \quad (*)$$

$$\text{取 } \alpha = \lg 2, \beta = \frac{\lg 2024 + \lg 2025}{2}; \text{ 则 } (*) \text{ 改写为 } \lg 2024 - \beta < n\alpha - m\beta < \lg 2025 - \beta$$

$$\text{即 } |n\alpha - m\beta| < \frac{\lg 2025 - \lg 2024}{2} = \frac{\lg 2025 - \lg 2024}{2}$$

利用 Kronecker 定理 $|\alpha x - y - \beta| < \frac{3}{x} < \frac{\lg 2025 - \lg 2024}{2}$, 取 $n = x, m = y$ 即可. #

8. 反证法: 假设 β 为有理数, 存在 $n_0, T \in \mathbb{N}^*$, 使 $\forall n \geq n_0$ 均有 $a_{n+T} = a_n$.

$$\text{因此 } [a(n+T)] \equiv [a_n] \pmod{10} \quad \forall n \geq n_0$$

$$\alpha(n+T) - \{a(n+T)\} \equiv \alpha n - \{a_n\} \pmod{10}$$

$$\alpha T - \{\alpha(n+T)\} + \{a_n\} \equiv 0 \pmod{10}$$

$$\alpha T - \{\alpha n\} + \{a_n\} \equiv 0 \pmod{10}$$

$$\text{因此 } [\alpha T] + (\{\alpha T\} + \{\alpha n\}) - \{\{\alpha n\} + \{\alpha T\}\} \equiv 0 \pmod{10}$$

此时 α, T 均是固定的, $n \geq n_0$

下面分情况讨论

(1) 如果 $[\alpha T] \equiv 0 \pmod{10}$, 由于 α 为无理数, 那么

$\{\alpha n\}$, $n \geq n_0$, 在 $(0, 1)$ 上是稠密的, 取一个 n , 要求 $\{\alpha n\} > 1 - \{\alpha T\}$ 代入 (*)

有 $0 + 1 \equiv 0 \pmod{10}$, 矛盾

(2) 如果 $[\alpha T] \not\equiv 0 \pmod{10}$, 取一个 n , 要求

$\{\alpha n\} < 1 - \{\alpha T\}$, 代入 (*) 有 $[\alpha T] \equiv 0 \pmod{10}$ 矛盾 #

9. (1) 升幂定理: 设 p 为素数, $p \nmid a-1$, $a > 1$, $n \geq 1$, 那么 $V_p(a^n - 1) = V_p(a - 1) + V_p(n)$

其中 $V_p(m) = t$ 表示 $p^t \mid m$ 且 $p^{t+1} \nmid m$, $t \geq 0$

(2) Legendre 公式, $V_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right] = \frac{n - S(n)}{p-1}$

(3) 回到原题: $n=1$, 无解, 以下 $a > 1$, 考虑方程 $n! = a^b - a^c$, 想证 n, b, c 均有界

设 p 为大于 a 的奇素数, 则 $(p, a) = 1$, 而 $n! = a^c(a^{b-c} - 1)$

因此 $V_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right] \geq \left[\frac{n}{p} \right] > \frac{n}{p} - 1$

$$V_p(a^{b-c} - 1) \leq V_p(a^{(b-1)(p-1)} - 1) = V_p((a^{p-1})^{b-c} - 1)$$

$$= V_p(a^{p-1} - 1) + V_p(b-c), \text{ 那么 } \frac{n}{p} - 1 < V_p(a^{p-1} - 1) + V_p(b-c)$$

不妨设 $V_p(a^{p-1} - 1) = \alpha$, 因此 $V_p(b-c) > \frac{n}{p} - 1 - \alpha$,

从而 $n^n > n! = a^c(a^{b-c} - 1) > a^{b-c} > a^{p^{n/p-1-\alpha}}$ 因此 $\log_p n \log_p n > \frac{n}{p} - 1 - \alpha$

因此 n 有界

又 $b-c < \log_p n!$, $c < \log_p n!$, 从而 b, c 有界.

10. 不妨设 $\begin{cases} x^{p^1} + y = p^\alpha \\ x + y^{p^1} = p^\beta \end{cases}$ 其中 $x \geq y, \alpha \geq \beta$.

首先 $x \neq y$, 否则 $p^\alpha = x^{p^1} + x = x(x^{p^2} + 1)$, 矛盾.

其次 $p \nmid xy$, 理由: 由于 $x^{p^1} + y = p^\alpha$, 那么 $V_p(x^{p^1}) = V_p(y)$

且 $(p-1)V_p(x) = V_p(y)$, 又 $x + y^{p^1} = p^\beta$ 那么 $V_p(x) = V_p(y^{p^1})$

即 $V_p(x) = (p-1)V_p(y)$, 因此 $V_p(x) = V_p(y) = 0$, 从而 $p \nmid xy$

因此 $\begin{cases} x^{p^1} + y = p^\alpha \\ x + y^{p^1} = p^\beta \end{cases} \quad x > y \geq 1, \alpha > \beta \geq 1, p \nmid xy$

利用FLT, 有 $x^{p-1} \equiv y^{p-1} \equiv 1 \pmod{p}$, 代回去, 有 $1+y \equiv x+1 \equiv 0 \pmod{p}$

因此 $x \equiv y \equiv -1 \pmod{p}$

回忆升幂定理, 设 p 为奇素数, $p \nmid xy$, $x \not\equiv \pm y$, $p \nmid x \mp y$, $n \geq 1$,

则 $V_p(x^n \mp y^n) = V_p(x \mp y) + V_p(n)$

因此 $x^p - y^p = (x^p + xy) - (y^p + xy)$

$$= x(x^{p-1} + y) - y(y^{p-1} + x) = xp^{p-1} - yp^{p-1}$$

利用LTE, 有 $V_p(x^p - y^p) = V_p(x - y) + 1$

又 $V_p(xp^{p-1} - yp^{p-1}) = \beta$ 因此 $V_p(x - y) + 1 = \beta$,

从而 $V_p(x - y) = \beta - 1$, 令 $x - y = k \cdot p^{\beta-1}$, 其中 $p \nmid k$ 代入

$$x + y^{p-1} = p^{\beta}$$

有 $k \cdot p^{\beta-1} + y + y^{p-1} = p^{\beta}$, 从而 $y(1 + y^{p-2}) = p^{\beta-1}(p - k)$ 此时 $(y, p) = 1$

从而 $y \mid p - k$, 又 $p \nmid y + 1$, 因此 $k = 1$, $y = p - 1$ 代入(*)

$$有 p^{\beta-1} + p - 1 + (p - 1)^{p-1} = p^{\beta}$$

$$从而 (p - 1) + (p - 1)^{p-1} = p^{\beta} - p^{\beta-1} = p^{\beta-1}(p - 1)$$

$$因此 1 + (p - 1)^{p-2} = p^{\beta-1}, 1 + (p - 1)^{p-2} = p^1 \Rightarrow p = 3$$

$$\beta - 1 = V_p(p^{\beta-1}) = V_p(1 + (p - 1)^{p-2}) = V_p(1 + (p - 1)) + V_p(p - 2) = 1, \beta = 2$$

$$又 x + y^{p-1} = p^{\beta}, 从而 x = p^{\beta} - y^{p-1} = p^2 - (p - 1)^{p-1} = 3^2 - 2^2 = 5$$

$$从而 (p, x, y) = (3, 5, 2) 或 (3, 2, 5) \#$$

11. 注记, 给定正整数 $k \geq 2$, 求所有的正整数 n , 满足条件: 存在正整数 $a_1, \dots, a_k$, 满足

$$(n + a_1)(n + a_2) \cdots (n + a_k) = a_1^2 + a_2^2 + \cdots + a_k^2$$

分析 (1) $n = 1$, 不符合条件, 反证法: 假设 $n = 1$ 符合条件

因此, 存在正整数 a, b , 使得 $(a+1)(b+1) \mid a^2 + b^2$

$$即 (a+1)(b+1)k = a^2 + b^2, k \in \mathbb{N}^*$$

$$设 S_k = \{(u, v) \mid u, v \in \mathbb{N}^*, u^2 + v^2 = (u+1)(v+1)k\}$$

因此 $S_k \neq \emptyset$. 取 $(a, b) \in S_k$

若 $(u, v) \in S_k$, 则 $(v, u) \in S_k$, 且 $u \neq v$

否则若 $u = v$, 则 $2u^2 = (u+1)^2 k$

从而 $(u+1)^2 \mid 2u^2$, 又 $(u+1)^2, u^2 = 1$, 因此 $(u+1)^2 \mid 2$, 矛盾.

不妨设 $(u, v) \in S_k$, 那么, $u^2 + v^2 = (u+1)(v+1)k$

因此 $u^2 - (v+1)ku + v^2 - (v+1)k = 0$

从而 $x=u$ 为方程 $x^2 - (v+1)kx + v^2 - (v+1)k = 0$ 的一个根

从而有另一个根 $x=w$, 因此 $\begin{cases} u+w = (v+1)k \\ u+w = v^2 - (v+1)k \end{cases}$

从而 $w \in \mathbb{Z}$ 且 $w < v$

由于 $x=w$ 也是方程的根, 那么 $w^2 - (v+1)kw + v^2 - (v+1)k = 0$

因此 $w^2 + v^2 = (w+1)(v+1)k$, 从而 $w > -1$, 因此 $w \geq 0$

①. 如果 $w=0$, 那么 $v^2 = (v+1)k$, 从而 $v+1 \mid v^2$ 矛盾

②. 如果 $w \geq 1$, 那么 $(w, v) \in S_k$ 且 $w+v < u+v$, 与 (u, v) 的选取矛盾

(2) 如果 $n \geq 2$ 那么 n 符合条件, 即存在正整数 a, b 使得 $(a+n)(b+n) \mid a^2 + b^2$. (*)

下面构造 (a, b)

(*) $\Leftrightarrow b+n \mid a^2 + b^2$ 且 $a+n \mid \frac{a^2 + b^2}{b+n}$

观察 $b+n \mid a^2 + b^2 = a^2 + n^2 + b^2 - n^2$, 因此 $b+n \mid a^2 + n^2$

要求 $b+n = a^2 + n^2$, 则 $b = a^2 + n^2 - n$

$$a+n \mid \frac{a^2 + b^2}{b+n} = \frac{a^2 + n^2 + b^2 - n^2}{b+n} = \frac{a^2 + n^2}{b+n} + b - n = 1 + b - n$$

$$= 1 + a^2 + n^2 - n - n$$

$$= a^2 + n^2 - 2n = a^2 - n^2 + 2n^2 - 2n + 1$$

因此 $a+n \mid 2n^2 - 2n + 1$, 要求 $a+n = 2n^2 - 2n + 1$

从而 $\begin{cases} a = 2n^2 - 3n + 1, n \geq 1 \\ b = a^2 + n^2 - n = (2n^2 - 3n + 1)^2 + n^2 - n \end{cases}$

$\#$

12 (1) 阶 1° 欧拉定理

2° 若 $(a, m) = 1$, 则存在最小的正整数 t , 使得 $a^t \equiv 1 \pmod{m}$

则称 t 为 a 模 m 的阶, 记为 $t = \text{ord}_m(a)$

3° 若 $\text{ord}_m(a) = t$, 且 $a^r \equiv 1 \pmod{m}$, 则 $t \mid r$

特别, 有 $t \mid \varphi(m)$

(2) 回到原題, 对正整数 n , 分情况讨论

1° 如果 $p|n$, 那么 n 不是好数, 理由如下

构造一个正整数 $m \neq n$, 使得 $\left\{\frac{p^m}{n^p}\right\} = \left\{\frac{p^n}{n^p}\right\}$ (*)

由于 $p|n$, 不妨设 $n = p^\alpha \cdot n_1$, 其中 $\alpha \geq 1, p \nmid n_1$.

取 $m = p^\beta \cdot n$, 其中 $\beta \geq 1$, 代入 (*)

$$\text{有 } \left\{\frac{p^{m+\beta}}{n^{p+\beta}}\right\} = \left\{\frac{p^n}{n^p}\right\}$$

$$\text{因此 } n^p | p^{m+\beta} - p^n = p^n (p^{m-n-\beta} - 1) \quad (**)$$

$$\text{由于 } n^p = (p^\alpha n_1)^p = p^{\alpha p} \cdot n_1^p, \quad p^{\alpha p} | p^n \quad p\alpha \leq n$$

$$\text{将 } (**) \text{ 改写为 } n_1^p | p^{m-n-\beta} - 1 = p^{\beta \cdot n - n - \beta} - 1$$

要求 $\beta = n \cdot x$, 其中 x 待定, 代回去, 有

$$p^\beta \cdot n - n - p\beta = p^{\alpha-1} n_1 \cdot n - n - nx = n (p^{\alpha-1} n_1 x - x - 1)$$

$$\text{取 } a = p^{\alpha-1} n_1, \quad b = p(n_1, p), \quad c = 1, \quad e = 1, \quad d = 1, \text{ 则 } (b, c) = 1$$

利用第1题, 存在无穷多个

取一个正整数解 x_0 . $\varphi(n, p) |$

$$\text{由欧拉定理, } n_1^p | p^{a x_0 - x_0 - 1}, \text{ 从而 } n_1^p | p^{n(a x_0 - x_0 - 1)} - 1$$

$$\text{取 } m = p^\beta \cdot n = p^{\alpha-1} n_1 x_0 n \text{ 则 } \left\{\frac{p^{m+\beta}}{n^{p+\beta}}\right\} = \left\{\frac{p^n}{n^p}\right\}$$

因此 n 不是好数 #

2° 若 $p \nmid n$ 且 $p \nmid \text{ord}_p(p)$, 则 n 不是好数

本质上, 构造正整数 $m \neq n$, 使得 $\left\{\frac{p^m}{n^p}\right\} = \left\{\frac{p^n}{n^p}\right\}$ (*)

不妨设 $z = \text{ord}_p(p)$, 即 z 为最小的正整数满足 $p^z \equiv 1 \pmod{p^p}$

令 $m = p^\alpha \cdot n$, 其中 α 待定, 要求 (*) 成立, 因此 $\left\{\frac{p^{m+\alpha}}{n^{p+\alpha}}\right\} = \left\{\frac{p^n}{n^p}\right\}$

$$\text{从而 } n^p | p^{m+\alpha} - p^n = p^n (p^{m-n-\alpha} - 1) = p^n (p^{(p^\alpha-1)n-\alpha} - 1)$$

$$\text{因此 } (*) \Leftrightarrow n^p | p^{(p^\alpha-1)n-\alpha} - 1 \quad (**)$$

再令 $d = nx$, 其中 x 待定

$$\text{则 } (**) \Leftrightarrow n^p | p^{(p^\alpha-1)n-pnx} - 1 = p^{n(p^\alpha-px-1)} - 1 \quad (***)$$

$$z = \text{ord}_p(p) \text{ 取 } a = p^n, \quad b = z, \quad c = p, \quad d = 1, \quad e = 1$$

利用第3题, 方程 $a^x - px \equiv 1 \pmod{z}$ 有无穷多正整数解 x .

取一个正整数解 $x=x_0$, 则 $z \mid p^{nx_0} - p^{x_0} - 1$
 因此 $p^{p^{nx_0} - p^{x_0} - 1} \equiv 1 \pmod{p^n}$, 从而 $p^{n(p^{nx_0} - p^{x_0} - 1)} \equiv 1 \pmod{p^n}$
 从而 $n \mid p^{n(p^{nx_0} - p^{x_0} - 1)} - 1$, 从而 $\left\{ \frac{p^m}{m^p} \right\} = \left\{ \frac{p^n}{n^p} \right\}$
 其中 $m = p^a \cdot n = p^{nx_0} \cdot n \neq n$

3. 若 $p \nmid n$ 且 $p \mid \text{ord}_n(p)$, 则 n 为好数

反证法, 假如 n 不是好数, 又 $p \nmid n$, 利用第1题, 存在正整数 a , 使 $p \mid (p^a - 1)n - pa$
 不妨设 $z = \text{ord}_p(p)$ 即 z 为最小的正整数满足 $p^z \equiv 1 \pmod{p}$
 因此 $z \mid (p^a - 1)n - pa$, 又 $p \nmid n$, 那么 $p \nmid (p^a - 1)n - pa$, 从而 $p \nmid z$, 与 $p \mid z$ 矛盾

13. (1) $n \leq 225$, 均可以举例说明

(2) 下证 $n \geq 25$ 时, $(n, 2n)$ 中至少有5个不同的素数

考虑 $M = C_{2n}^n = \frac{2n(2n-1)\cdots(n+1)}{n!}$, 设 M 的标准分解式 $M = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$

估计 α_i 大小: $\alpha_i = V_{p_i} \left(\frac{2n!}{n!n!} \right) = V_{p_i}(2n!) - 2V_{p_i}(n!)$

$$= \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p_i^k} \right\rfloor - 2 \left\lfloor \frac{n}{p_i^k} \right\rfloor \right)$$

不妨设 $p_i^{\beta} \leq 2n < p_i^{\beta+1}$, 那么 $\alpha_i = \sum_{k=1}^{\beta} \left(\left\lfloor \frac{2n}{p_i^k} \right\rfloor - 2 \left\lfloor \frac{n}{p_i^k} \right\rfloor \right)$

回忆 $\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 0, & 0 \leq \{x\} < \frac{1}{2} \\ 1, & \frac{1}{2} \leq \{x\} < 1 \end{cases}$

因此 $\alpha_i \leq \beta$, 从而 $p_i^{\alpha_i} \leq p_i^{\beta} \leq 2n$, $\forall i=1, 2, \dots, t$

令 $M = \prod_{p \leq 2n} p^{\alpha} \cdot \prod_{\substack{p \leq 2n \\ p \nmid M}} p^{\alpha} \cdot \prod_{\substack{p \leq 2n \\ \frac{2n}{3} < p \leq n}} p^{\alpha} \cdot \prod_{n < p \leq 2n} p^{\alpha}$

① $\prod_{p \leq \frac{2n}{3}} p^{\alpha} \leq (2n)^{\pi(\frac{2n}{3})}$, 其中 $\pi(x)$ 表示不大于 x 的素数个数

② 现在 $\sqrt{2n} < p \leq \frac{2n}{3}$, 那么 $p^2 > 2n$, 因此

$\alpha = V_p(m) = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) = \left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor \leq 1$

因此 $\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\alpha} < \prod_{p \leq \frac{2n}{3}} p < 4^{\frac{2n}{3}-1}$, 理由如下

引理, 设实数 $x \geq 2$, 则 $\prod_{p \leq x} p < 4^{x-1}$

证明: 令 $n = \lfloor x \rfloor$, 只需证 $\prod_{p \leq n} p < 4^{n-1}$

归纳法, 1° $n=2$ 时, $\prod_{p \leq 2} p = 2 < 4^{2-1}$ ✓

2° 假设 $n \leq m$, 结论成立

3° 考虑 $n = m+1$ 的情况, 想证 $\prod_{p \leq m+1} p < 4^{m+1} < 4^m$

对 $m+1$ 分情况讨论

1° 若 $m+1=2k$, 则 $\prod_{p \leq m+1} p = \prod_{p \leq 2k} p < 4^{m-1} < 4^m$

2° 若 $m+1=2k+1$, 则

$$\prod_{p \leq m+1} p = \prod_{p \leq 2k+1} p = \prod_{p \leq k+1} p \cdot \prod_{k+1 < p \leq 2k+1} p < 4^k \cdot (2k+1) < 4^k \cdot 2^{2k} = 4^{2k}$$

③ 现在 $\frac{2}{3}n < p \leq n$, 有 $\frac{2}{3}n < p \leq n < \frac{3}{2}p < 2p \leq 2n < 3p$

$$\text{观察 } C_{2n}^n = \frac{2n(2n-1)\cdots(n+1)}{n!} \quad \text{因此 } V_p(C_{2n}^n) = 0$$

$$\text{因此 } \prod_{\frac{2}{3}n < p \leq n} p^\alpha = 1. \text{ 因此 } M = C_{2n}^n = \prod_{p \leq \sqrt{2n}} p^\alpha \cdot \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^\alpha \cdot \prod_{\frac{2n}{3} < p \leq 2n} p^\alpha, \text{ 其中 } \alpha \leq 1$$

$$\text{即 } C_{2n}^n < (2n)^{\pi(\sqrt{2n})} \cdot 4^{\frac{2n}{3}-1} \cdot p$$

$$\therefore C_{2n}^0 + C_{2n}^1 + \cdots + C_{2n}^{2n} = 2^{2n}$$

$$\text{因此 } C_{2n}^n > \frac{2^{2n}}{2n} \text{ 代回去, } \frac{2^{2n}}{2n} < (2n)^{\pi(\sqrt{2n})} \cdot 4^{\frac{2n}{3}-1} \cdot p \quad (*)$$

想证在 $(n, 2n)$ 之间至少有 5 个不同的素数, 其中 $n \geq 225$

反证法, 至多 4 个

$$p \leq (2n-1)(2n-3)(2n-5)(2n-7) < (2n)^4, \text{ 代入 } (*)$$

$$\text{有 } \frac{4^n}{n} < (2n)^{\pi(\sqrt{2n})} \cdot 4^{\frac{2n}{3}-1} \cdot (2n)^4, \text{ 其中 } n \geq 225$$

$$\text{即 } 4^{\frac{n}{3}+1} < (2n)^{\pi(\sqrt{2n})+5}, \text{ 其中 } n \geq 225$$

令 $k = \lfloor \sqrt{2n} \rfloor$ 由于 $n \geq 225$, 那么 $k \geq 20$ $\pi(k)$ 表示 $1, 2, \dots, k$ 中素数的个数

观察: $1, 9, 15, 4, 6, 8, \dots, 2\lfloor \frac{k}{2} \rfloor$ 均不是素数

$$\text{因此 } \pi(k) \leq k - \lfloor \frac{k}{2} \rfloor + 2 = k - \lfloor \frac{k}{2} \rfloor + 1 \leq k - 1 - \frac{k}{2}$$

$$= \frac{k}{2} - 1 \leq \frac{1}{2}\sqrt{2n} - 1 = \sqrt{\frac{n}{2}} - 1, \text{ 代回去, 有:}$$

$$4^{\frac{n}{3}} < 4^{\frac{n}{3}+1} < (2n)^{\pi(\sqrt{2n})+5} < (2n)^{\sqrt{\frac{n}{2}}-1+5} = (2n)^{\sqrt{\frac{n}{2}}+4}, \text{ 由 } n \geq 225, \text{ 那么 } \sqrt{\frac{n}{2}}+4 < \sqrt{n}, \text{ 因此}$$

$$\sqrt{\frac{n}{2}}+4 < \sqrt{n} \Leftrightarrow \frac{n}{2}+16+8\sqrt{\frac{n}{2}} < n \Leftrightarrow 16+8\sqrt{\frac{n}{2}} < \frac{n}{2} \Leftrightarrow (\text{令 } \sqrt{\frac{n}{2}}=x, \text{ 则 } x \geq \sqrt{\frac{225}{2}} > 10) 16+8x < x^2$$

$$\Leftrightarrow (x-4)^2 > 32 \Leftrightarrow x > 4+\sqrt{32} \# , \text{ 代回去有 } (4^{\frac{n}{3}})^{\sqrt{n}} = 4^{\frac{n}{3}\sqrt{n}} < (2n)^{\sqrt{n}}, \text{ 其中 } n \geq 225$$

$$\text{再令 } l = \lfloor \frac{\sqrt{n}}{3} \rfloor, \text{ 则 } l \leq \frac{\sqrt{n}}{3} < l+1 \Rightarrow \sqrt{n} < 3(l+1)$$

$$\text{已知 } 4^l < 2n, \text{ 从而 } 2^l < \sqrt{2n} < \sqrt{2} \cdot 3(l+1) < 5 \cdot (l+1)$$

$$\text{即 } 2^l < 5 \cdot (l+1), \text{ 其中 } l = \lfloor \frac{\sqrt{n}}{3} \rfloor \geq 5$$

$$\text{但是 } 2^l < 5(l+1) \Rightarrow l < 5$$

矛盾 #

14. (1) $a=1$ 时, 结论成立

(2) $n=1$ 时, 结论成立

(3) 以下 a, n 均为大于 1 的整数且 $a^n \equiv 1 \pmod{n}$

反证法, 假设存在 $1 \leq i < j \leq n$ 使 $a^i + i \equiv a^j + j \pmod{n}$ (*)

可以要求 n 是最小的, 由于 $a^n \equiv 1 \pmod{n}$, 那么 $(a, n) = 1$, 不妨设 $\text{ord}_n(a) = d$

即 d 为最小的正整数满足 $a^d \equiv 1 \pmod{n}$, 因此 $d | n$, 又 $a^{\varphi(n)} \equiv 1 \pmod{n}$

因此 $d | \varphi(n)$, 由于 $n > 1$, 那么 $1 \leq d \leq \varphi(n) < n$

显然 $d \neq 1$, 否则 $a \equiv 1 \pmod{n}$ 那么 $a^i + i \equiv 1 + j \pmod{n}$, $i=1, 2, \dots, n$

从而 $a^i + i$, $i=1, \dots, n$ 均成模 n 的完全剩余系,

从而 $1 < d < n$, $d | n$

由于 $a^d \equiv 1 \pmod{n}$, 那么 $a^d \equiv 1 \pmod{d}$, 利用 n 的最小性

可知 $a^1 + 1, a^2 + 2, \dots, a^d + d$ 模 d 互不同余

由 (*) 可知 $a^i + i \equiv a^j + j \pmod{d}$

不妨设 $i = dq_1 + r_1$, $j = dq_2 + r_2$ 其中 $1 \leq r_1, r_2 \leq d$

代回去, 有 $a^{dq_1+r_1} + r_1 \equiv a^{dq_2+r_2} + r_2 \pmod{d}$

因此 $r_1 = r_2 = r$, 从而 $a^{dq_1+r} + r \equiv a^{dq_2+r} + r \pmod{d}$

又 $a^d \equiv 1 \pmod{n}$, 则上式改写为 $a^r + i \equiv a^r + j \pmod{n}$

即 $i \equiv j \pmod{n}$ 与 $1 \leq i < j \leq n$ 矛盾

15. (1) 回忆: 1° 若 $d | a, d | b$ 则 $d | (a, b)$

2° 若 $a | m, b | m$, 则 $[a, b] | m$

(2) 令 $\frac{a_{i+1}}{a_i} = \frac{x_i}{y_i}$ 其中 $x_i, y_i \in \mathbb{N}^*$, $(x_i, y_i) = 1$

因此 $y_i | a_i$, $x_i | a_{i+1}$, 从而 $a_{i+1} < (a_i, a_{i+1}) = (a_i, \frac{x_i}{y_i} \cdot a_i) = \frac{a_i}{y_i} (y_i, x_i) = \frac{a_i}{y_i}$

因此 $\forall i \geq 1, \frac{a_i}{y_i} > y_i$

又 $\frac{a_i}{y_i} = \frac{x_{i-1}}{y_{i-1}}$, 从而 $\frac{x_{i-1}}{y_{i-1}} > y_i$ 其中 $i \geq 1$

因此 $\frac{x_{i-1}}{y_{i-1}} \geq y_i + \frac{1}{y_{i-1}} \geq 2\sqrt{y_i \cdot \frac{1}{y_{i-1}}} = 2\sqrt{\frac{y_i}{y_{i-1}}} \quad \forall i \geq 1$

又 $\frac{a_1}{y_0} = \frac{x_0}{y_0}$, $y_0 | a_0$, 从而 $a_0 \geq y_0$

想证 $a_n \geq 2^n$, $\forall n \geq 0$

$$a_n = \frac{a_n}{a_{n-1}} \cdot \frac{a_{n-1}}{a_{n-2}} \cdots \frac{a_2}{a_1} \cdot \frac{a_1}{a_0} \cdot a_0 = \frac{a_{n-1}}{a_{n-2}} \cdots \frac{a_1}{a_0} \cdot a_0$$

$$\geq 2 \sqrt{\frac{a_{n-1}}{a_{n-2}}} \cdots 2 \sqrt{\frac{a_1}{a_0}} \cdot a_0 = 2 \sqrt{a_0} \geq 2$$

16. (1) $\sigma(n)$ 为 n 的所有不同正因子之和

性质: 1° $\sigma(1) = 1$

$$2^\circ \sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1} \quad (p \text{ 为素数})$$

3° 一般地 $n > 1$, 不妨设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 为标号分解式

$$\text{那么 } \sigma(n) = \sigma(p_1^{\alpha_1}) \cdot \sigma(p_2^{\alpha_2}) \cdots \sigma(p_k^{\alpha_k})$$

$$= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

$$4^\circ \text{ 若 } (m, n) = 1, \text{ 则 } \sigma(mn) = \sigma(m) \cdot \sigma(n)$$

(2) 回到原题: 一定存在 $m \in \mathbb{N}^*$, 使 $2^m - 1$ 至少有 k 个不同的素因子.

理由如下: 取 $m = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$

其中 $p_1, p_2, \dots, p_k$ 为前 k 个奇素数, 即 $3, 5, 7, \dots$

$$\text{则 } p_i \mid 2^m - 1, \forall i = 1, \dots, k. \quad \#$$

$$\text{令 } n_0 = 2^m - 1, \text{ 则 } \sigma(n_0) = 2^m - 1 = p_1^{\alpha_1} \cdots p_t^{\alpha_t}, \quad i_1 < \cdots < i_t$$

$$\text{因此 } B_{n_0} = \{2\} \quad A_{n_0} = \{p_{i_1}, \dots, p_{i_t}\}$$

这组 p_i 表示第 i 个奇素数, 按照大小顺序.

因此 $t \geq k$

2° 若 $t = k$, 则结论成立

3° 若 $t > k$, 不妨设 $t - k = r$, 其中 $r \in \mathbb{N}^*$

$$\text{令 } n_1 = n_0 \cdot p_1 p_2 \cdots p_{i_{k+1}} \cdots p_{i_r} = 2^m \cdot p_1 p_2 \cdots p_r$$

$$\text{因此 } \sigma(n_1) = (2^m - 1) \cdot (p_1 + 1)(p_2 + 1) \cdots (p_r + 1)$$

$$= p_1^{\alpha_1} \cdots p_r^{\alpha_r} (p_1 + 1)(p_2 + 1) \cdots (p_r + 1)$$

$$\text{此时 } B_{n_1} = \{2, p_1, \dots, p_r\}, \quad |B_{n_1}| = t + r$$

因此 $A_{n_1} \setminus B_{n_1}$ 表示 A_{n_1} 中大于 p_r 的素数构成的集合

$$A_{n_1} \setminus B_{n_1} = \{p_{i_{k+1}}, \dots, p_{i_r}\}$$

$$|A_{n_1} \setminus B_{n_1}| = t - r = k$$

17. (1) 来源: 设 a 为大于 1 的正整数, 证明存在无穷正整数 k , 使 $\left[\frac{a^k}{k}\right]$ 为素数

(2) 回到原题, 取 $k = t \cdot a^x$, 其中 t, x 待定, 因此 $\left[\frac{a^k}{k}\right] = \left[\frac{a^{t \cdot a^x}}{t \cdot a^x}\right] = \left[\frac{a^{ta^x-x}}{t}\right]$
 $= \left[\frac{a^{ta^x-x} - a^e}{t}\right] = \left[\frac{a^e(a^{ta^x-x-e} - 1)}{t}\right] + \left[\frac{a^e}{t}\right]$

可以要求 $(t, a) = 1$, 如果 $\varphi(tb) \mid ta^x - x - e$ 那么 $tb \mid (a^{ta^x-x-e} - 1)a^e$
 再要求 $\left[\frac{a^e}{t}\right] = c$ #

由于 a, c 均为正整数, 那么取一个充分大的正整数 e , 使得 $\left(\frac{a^e}{c}, \frac{a^e}{c}\right)$
 中存在一个正整数 t , 满足 $(t, a) = 1$

事实上, 只需 $\frac{a^e}{c} - \frac{a^e}{c+1} > a$ 即可

令 $k = ta^x$ 其中 x 待定, 因此 $\frac{a^k}{k} = \frac{a^{ta^x}}{ta^x} = \frac{a^{ta^x-x}}{t}$

熟知 $ta^x - x \equiv e \pmod{\varphi(tb)}$ 有无穷多正整数解

取一个充分大的正整数解 $x = x_0$, 因此 $k = t \cdot a^{x_0}$, 则 $ta^{x_0} - x_0 \equiv e \pmod{\varphi(tb)}$

因此 $tb \mid a^{ta^{x_0}-x_0} - a^e$

从而 $\left[\frac{a^k}{k}\right] = \left[\frac{a^{ta^{x_0}-x_0}}{t}\right] = \frac{a^{ta^{x_0}-x_0} - a^e}{t} + \left[\frac{a^e}{t}\right]$

$\equiv \left[\frac{a^e}{t}\right] \pmod{b}$

又 $\frac{a^e}{c+1} < t < \frac{a^e}{c}$, 即 $c < \frac{a^e}{t} < c+1$, 因此 $\left[\frac{a^e}{t}\right] = c$, 从而 $\left[\frac{a^k}{k}\right] \equiv c \pmod{b}$

18. 反证法: 假设存在正整数 m 使 $\frac{b^2}{a^2+ab-1} \leq m < \frac{b^2}{a^2+ab}$

因此, $ma^2 + mab - m = m(a^2 + ab - 1) < b^2 \leq m(a^2 + ab) = ma^2 + mab$

从而 $b^2 = ma^2 + mab - r$ 其中 $0 \leq r < m$

可以要求 $a+b$ 是最小的

显然, $b > a$, 而且 $b^2 - mab - (ma^2 - r) = 0$

换句话说, $x=b$ 为方程 $x^2 - max - (ma^2 - r) = 0$ 的一个根

因此 $\Delta = (ma)^2 + 4(ma^2 - r)$ 为平方数

观察 $\Delta = (ma)^2 + 4ma^2 - 4r = a^2(m^2 + 4m) - 4r = (a(m+2))^2 - 4(rta^2)$

$= (a(m+2)^2 - t)^2$, 其中 $t \in \mathbb{N}^*$ 待定

既知 $2 \mid t$, 不妨设 $t = 2k, k \in \mathbb{N}^*$.

如果 $2a \leq 2k \leq 2a(m+2)$, 那么 $(a(m+2) - t)^2 \leq (am)^2$

但是 $(a(m+2))^2 - 4(rta^2) = (am)^2 + 4(a^2m - r)$, 又 $0 \leq r < m$

从而 $\Delta > (am)^2$, 因此 $0 < k < a$

$$\text{因此, } \Delta \text{ 为平方数} \Leftrightarrow (a(mt+2))^2 - 4(rta^2) = (a(mt+2) - 2k)^2$$

$$\Leftrightarrow 4(rta^2) = 4ka(mt+2) - 4k^2$$

$$\Leftrightarrow rta^2 = ka(mt+2) - k^2$$

$$\Leftrightarrow (a-k)^2 + r - akm = 0 \quad \text{此时 } 0 < k < a$$

$$\text{令 } a-k=l, \text{ 则 } l \in \mathbb{N}^*, \text{ 而且 } l^2 + r - (l+k)km = 0$$

$$\text{即 } l^2 - kml - (k^2m - r) = 0 \quad \text{此时 } k+l = n < a+b, \text{ 矛盾!}$$

19. (1) 引理: 设 p 为奇素数, $k=1, 2, \dots, p-2$,

$$\text{那么 } 1^k + 2^k + \dots + (p-1)^k \equiv 0 \pmod{p}$$

证明: 令 $S_k = 1^k + 2^k + \dots + (p-1)^k$, 想证 $p \mid S_k$ 其中 $k=1, \dots, p-2$

对 k , 利用归纳法

$$1^\circ k=1 \text{ 时, 有 } S_1 = 1+2+\dots+(p-1) = \frac{p(p-1)}{2} \equiv 0 \pmod{p} \quad \checkmark$$

2° 假设 $k \leq m$ 时结论成立, 此时 $m \leq p-3$

3° 考虑 $k=m+1$ 中的情形, 想证 $p \mid S_{m+1}$

$$\text{观察 } (1+x)^{m+2} - x^{m+2} = 1 + C_{m+2}^1 x + \dots + C_{m+2}^{m+1} x^{m+1}$$

在上式两边同时对 $x=1, 2, \dots, p-1$ 求和, 因此

$$\sum_{i=1}^{p-1} ((1+x)^{m+2} - x^{m+2}) = (p-1) + C_{m+2}^1 S_1 + \dots + C_{m+2}^{m+1} S_{m+1}$$

$$\text{因此 } k^{m+2} - 1 = p-1 + C_{m+2}^1 S_1 + \dots + C_{m+2}^m S_m + (m+2) S_{m+1}$$

利用假设, 并且两边同时模 p , 有 $-1 \equiv -1 + (m+2) S_{m+1} \pmod{p}$

因此 $p \mid (m+2) S_{m+1}$, 由于 $m \leq p-3$, 那么 $m+2 \leq p-1$

因此 $p \nmid m+2$, 从而 $p \mid S_{m+1}$ 并

推论: 设 p 为奇素数, $k \in \mathbb{Z}$, 则 $1^k + 2^k + \dots + (p-1)^k \equiv \begin{cases} 0 \pmod{p}, & \text{其中 } p \nmid k \\ -1 \pmod{p}, & \text{其中 } p \mid k \end{cases}$

(2) 回到原题: 1° 由题知 $p \geq 5$, 而且 $2p < 3n < 3p$ 且 $3p-3n < p$

2° 现在 $0 \leq j \leq n < p$, 我们知道 $C_n^j = \frac{n(n-1)(n-2)\dots(n-j+1)}{j!}$

$$\text{因此 } j! C_n^j \equiv n(n-1)\dots(n-j+1) \pmod{p}$$

$$\equiv (-1)^j \cdot (n)(-n+1)\dots(-(n-j+1)) \pmod{p}$$

$$\equiv (-1)^j (p-n)(p-n+1)\dots(p-n+j-1) \pmod{p}$$

$$\text{从而 } C_n^j \equiv (-1)^j \frac{(p-n)(p-n+1)\dots(p-n+j-1)}{j!} \pmod{p}$$

3° 想证 $p \mid \sum_{j=0}^n (-1)^j (C_n^j)^3$ 即证 $\sum_{j=0}^n (-1)^j (C_n^j)^3 \equiv 0 \pmod{p}$

只需证 $\sum_{j=0}^n (C_{p-n+j-1}^j)^3 \equiv 0 \pmod{p}$ (*)

如果 $n+1 \leq j \leq p-1$, 那么 $p \mid C_{p-n+j-1}^j$ 因此 (*) 可改写为 $\sum_{j=0}^{p-1} (C_{p-n+j-1}^j)^3 \equiv 0 \pmod{p}$

$$\Delta M = \sum_{j=0}^{p-1} (C_{p-n+j-1}^j)^3$$

$$\text{因此 } M = \sum_{j=0}^{p-1} (C_{p-n+j-1}^{p-n-1})^3 = \sum_{j=0}^{p-1} \left(\frac{(j+p-n-1)(j+p-n-2)\cdots(j+1)}{(p-n-1)!} \right)^3$$

$$\text{从而 } ((p-n-1)!)^3 \cdot M = \sum_{j=0}^{p-1} ((j+p-n-1)\cdots(j+1))^3 = \sum_{j=0}^{p-1} f(j)$$

$$\text{其中 } f(x) = ((x+p-n-1)(x+p-n-2)\cdots(x+1))^3$$

$$= x^t + a_{t-1}x^{t-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$$

此时 $t = 3(p-n-1) = 3p-3n-3 < p-3$, 代回去, 有

$$((p-n-1)!)^3 \cdot M = \sum_{j=0}^{p-1} (j^t + a_{t-1}j^{t-1} + \cdots + a_1j + a_0)$$

$$= S_t + a_{t-1}S_{t-1} + \cdots + a_1S_1 + a_0p$$

$$\equiv 0 \pmod{p}$$

从而 $p \mid M$ #

20. 分析: 反证法, 假设对任意 $i \neq j$, 均存在 k 使 $a_i + a_j \mid 3a_k$

不妨设 $(a_1, a_2, \dots, a_n) = 1$ 且 $a_1 < a_2 < \cdots < a_n$

(1) 取 $j=n$, 因此对每个 $i < n$, 均存在 k , 使 $a_i + a_n \mid 3a_k$

因此 $3 \mid a_i + a_n$, 理由如下: 反证法, 否则 $3 \nmid a_i + a_n$

因此 $(3, a_i + a_n) = 1$, 因此 $a_i + a_n \mid a_k$

从而 $a_i + a_n \leq a_k$, 矛盾.

从而 $a_i \equiv -a_n \pmod{3}$, $\forall i=1, 2, \dots, n-1$

具体地说 $a_1 \equiv a_2 \equiv \cdots \equiv a_{n-1} \equiv -a_n \pmod{3}$

又 $(a_1, a_2, \dots, a_n) = 1$, 因此 $3 \nmid a_n$

(2) 取 $i=n-2$, $j=n-1$, 则存在 k , 使 $a_{n-2} + a_{n-1} \mid 3a_k$

由于 $a_{n-2} + a_{n-1} \equiv -2 \not\equiv 0 \pmod{3}$, 那么 $a_{n-2} + a_{n-1} \mid a_k$

从而 $k=n$, 因此 $a_{n-2} + a_{n-1} \mid a_n$, 从而 $a_n = (a_{n-1} + a_{n-2}) \cdot L$, 其中 $L \in \mathbb{N}^*$ ✓

(3) 取 $i=n-1$, $j=n$, 则存在 k , 使得 $a_{n-1} + a_n \mid 3a_k$

因此 $3a_k = (a_{n-1} + a_n)q$, 其中 q 为正整数, 从而 $q=1$ 或 2 .

①若 $q=1$, 则 $3a_k = a_{n-1} + a_n \geq a_{n-1} + (a_{n-1} + a_{n-2}) = 2a_{n-1} + a_{n-2} > 3a_{n-2}$

因此 $k=n-1$ 或 n

如果 $k=n-1$, 那么 $3a_{n-1} = a_{n-1} + a_n$ 即 $a_n = 2a_{n-1}$

从而 $2a_{n-1} = a_n = (a_{n-1} + a_{n-2}) \cdot L$, 矛盾

如果 $k=n$ 则 $3a_n = a_{n-1} + a_n$, 矛盾

②若 $q=2$, 则 $3a_k = (a_{n-1} + a_n) \cdot 2$, 从而 $k=n$

因此 $a_n = 2a_{n-1}$, 从而 $2a_{n-1} = a_n = (a_{n-1} + a_{n-2}) \cdot L$, 矛盾 $\#$

21. (1) 引理: 设 $a \in \mathbb{Z}$ 且 $(a, p) = 1$, 则 $a^{p-1} \equiv 1 \pmod{p}$ (费马小定理)

因此 $a^{-1} \equiv a^{p-2} \pmod{p}$

对 $\forall n \in \mathbb{Z}$, 令 $n = (p-1)q + r$ 则 $a^n \equiv a^r \pmod{p}$

(2) 引理: 设 p 为素数, 那么 $\sum_{k=1}^{p(p-1)} k^{p(p-1)+k} \equiv -1 \pmod{p}$

即 $1^{p(p-1)} + 2^{p(p-1)+1} + 3^{p(p-1)+2} + \dots + (p(p-1))^{p(p-1)+p(p-1)} \equiv -1 \pmod{p}$

证明 $\sum_{k=1}^{p(p-1)} k^{p(p-1)+k} \equiv \sum_{\substack{k=pi+j \\ 1 \leq j \leq p-1 \\ 0 \leq i \leq p-2}} (pi+j)^{p(p-1)+pi+j} \pmod{p}$

$$\equiv \sum_{i=0}^{p-2} \sum_{j=1}^{p-1} (pi+j)^{p(p-1)+pi+j} \pmod{p}$$

$$\equiv \sum_{i=0}^{p-2} \sum_{j=1}^{p-1} j^{p(p-1)+1-pi-j} \pmod{p}$$

$$\equiv \sum_{i=0}^{p-2} \sum_{j=1}^{p-1} j^{1-i-j} \pmod{p}$$

$$\equiv \sum_{j=1}^{p-1} j^{-j} \left(\sum_{i=0}^{p-2} j^{1-i} \right) \pmod{p}$$

我们知道 $\sum_{i=0}^{p-2} j^{1-i} \equiv \begin{cases} 0 \pmod{p} & j \not\equiv 1 \pmod{p} \\ 1 \pmod{p} & j \equiv 1 \pmod{p} \end{cases}$

代回去, 有 $\sum_{k=1}^{p(p-1)} k^{p(p-1)+k} \equiv -1 \pmod{p}$

(3) 构造 n : 令 $n = tp(p-1)$ 其中 $t \in \mathbb{N}^*$, 待定

$$\sum_{k=1}^n k^{n+k} \equiv \sum_{k=tp(p-1)+i}^{tp(p-1)+tp(p-1)} k^{n+k} \pmod{p}$$

$$\equiv \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} (p(p-1)i+j)^{tp(p-1)+1-(p(p-1)i+j)} \pmod{p}$$

$$\equiv \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} j^{tp(p-1)+1-p(p-1)i-j} \pmod{p}$$

$$\equiv \sum_{i=0}^{t-1} \sum_{j=1}^{p-1} j^{tp(p-1)+1-j} \pmod{p}$$

$$\equiv \sum_{i=0}^{t-1} \sum_{j=1}^{p-1} j^{p(p-1)+1-j} \pmod{p}$$

$$\equiv \sum_{i=0}^{t-1} (-1) \pmod{p} \equiv -t \pmod{p}$$

取 $-t \equiv 2024 \pmod{p}$ 即可 #

思考题: 设 p 为素数, 证明: 存在正整数 n , 使得

$$1^n + 2^{n-1} + 3^{n-2} + \dots + n^1 \equiv 2024 \pmod{p^2}$$

23 分析: 令 $b = \lfloor \sqrt{a} \rfloor$, 则 (*) 改写为 $a! + (a+2)! \mid (a+2b)!$

$$\text{即 } 1(a+2)(a+4) \mid (a+2b)(a+2b+1) \dots (a+2b) \quad (**)$$

事实上 $1(a+2)(a+4) = a^2 + 3a + 2$, 此时 $b = \lfloor \sqrt{a} \rfloor$

取 $a = c^2 - 1$, 其中 $c \in \mathbb{N}^*$, 待定, 那么 $b = c - 1$

$$\text{因此 } (**) \text{ 改写为 } c^4 + c^2 + 1 \mid (c^2 + 2c - 3)(c^2 + 2c - 4) \dots c^2 \quad (***)$$

要证存在无穷多正整数 c 使 (***) 成立

$$\text{熟知: } c^4 + c^2 + 1 = (c^2 - c + 1)(c^2 + c + 1)$$

$$\text{且 } (c^2 - c + 1, c^2 + c + 1) = (c^2 - c + 1, 2c) = 1$$

由于 c 适当大, 那么 $c^2 + c + 1 \mid (c^2 + 2c - 3) \dots c^2$

只需构造正整数 c , 充分大, 使得 $c^2 - c + 1 \mid (c^2 + 2c - 3) \dots c^2$

$$\text{令 } c^2 - c + 1 = 3y^2, \text{ 则 } 4c^2 - 4c + 4 = 12y^2, \text{ 即 } (2c - 1)^2 - 12y^2 = -3$$

熟知: $x^2 - 12y^2 = -3$, 有无穷多正整数解 (x, y)

且 $2 \nmid x$, 任取一组正整数解 (x_0, y_0) , x_0 充分大, 则 $x_0 = 2c - 1$

$$(2c - 1)^2 - 12y_0^2 = -3, (2c - 1)^2 = 12y_0^2 - 3, \text{ 因此 } 2c - 1 > \sqrt{12} y_0 - 1$$

从而 $2c - 3 > \sqrt{12} y_0 - 3 > (2y_0)!$, 因此 $(2y_0)! \mid (c^2 + 2c - 3)(c^2 + 2c - 4) \dots c^2$

$$\text{又 } c^2 - c + 1 = 3y_0^2 \mid (2y_0)! \text{ 从而 } c^2 - c + 1 \mid (c^2 + 2c - 3) \dots c^2 \quad \#$$

24 分析: 对 n 分情况讨论

(1) $n = 1$ 时, $a \mid (a-1)!$. 显然, a 不为素数, $a \neq 4$, 其余正整数 $a > 1$ 均符合.

(2) 以下 $n \geq 2$, 求所有正整数 $a \geq 2$ 满足条件 $a^n \mid n(n+1) \dots (a^n - 1)$

1° 若 a 为素数, 即 $a = p$ 为素数, 则 a 不符合条件, 理由如下.

反证法, 如果符合条件, 那么 $p^n | n(n+1) \cdots (pn-1) = \frac{(pn-1)!}{(n-1)!}$
 从而 $p^{n+1} | \frac{(pn)!}{n!}$, 但是 $V_p\left(\frac{(pn)!}{n!}\right) = V_p((pn)!) - V_p(n!) =$

(Q42: Legendre公式)

$$\text{因此 } V_p((pn)!) - V_p(n!) = \frac{n - S(pn)}{p-1} - \frac{n - S(n)}{p-1} = \frac{pn - S(n)}{p-1} - \frac{n - S(n)}{p-1} = n \text{ 即 } p^n || \frac{(pn)!}{n!} \text{ 矛盾}$$

2° 如果 $a \geq 2$, 奇数, 那么结论成立

对 n , 利用数学归纳法

①, $n=2$ 时, 想证 $a^2 | 2 \cdot 3 \cdots (2a-1) = (2a-1)!$

由于 n 为奇数, 不妨设 a 的最小素因子为 p , 则 $p|a$

令 $a = pb, p \leq b$

(I) 若 $p < b$, 则 $a^2 = p^2 \cdot b^2 = pbpb$

$1 < p < b < pb < 2a-1$, 从而 $a^2 | (2a-1)!$

(II) 若 $p = b$, 则 $a = p^2, p \geq 2$, 想证 $p^4 | (2p^2-1)!$

(A) 若 $p \geq 3$, 则 $p < 2p < p^2 < 2a-1$ 且 $p^2 | (2a-1)!$

(B) 若 $p = 2$, 则 $2^4 | (2^3-1)! = 7! = 7 \times 720 = 5040 \nmid$

②. 假设对 n , 结论成立, 考虑 $n+1$ 的情形, 此时 n 为奇数

想证 $a^{n+1} | (n+1)(n+2) \cdots (a(n+1)-1)$

$(n+1)(n+2) \cdots (a(n+1)-1)$

$= (n+1)(n+2) \cdots (na-1)na(na+1) \cdots (a(n+1)-1)$

$= (n+1)(n+2) \cdots (na-1) \cdot a(na+1) \cdots (a(n+1)-1)$

利用假设 $0 \pmod{a^{n+1}}$ 若 $a^{n+1} | (n+1)(n+2) \cdots (a(n+1)-1) \nmid$

2.5 (1) 取 $n = p^2$, 其中 p 为奇素数, 则 n 符合条件, 证明如下

观察: $p=2$ 时, $C_4^4, C_8^4, C_{12}^4, C_{16}^4$ 是模 n 的完全剩余系 (计算略)

想证 $C_n^n, C_{2n}^n, C_{3n}^n, \dots, C_{n^2}^n$ 模 n 互不同余

事实上, 对 $k=1, 2, \dots, p^2$, 想证 $C_{kp^2}^{p^2} \equiv k \pmod{p^2}$, 即证 $C_{kp^2-1}^{p^2-1} \equiv 1 \pmod{p^2}$

$$C_{kp^2-1}^{p^2-1} = \frac{(kp^2-1)(kp^2-2) \cdots ((k-1)p^2+1)}{(p^2-1)!}$$

$$= \frac{(kp^2-1) \cdots (kp^2-p)}{(p^2-1) \cdots (p^2-p)} \cdot \frac{kp^2-p}{p^2-2p}$$

$$\begin{aligned}
 & \dots \frac{k^2 - (p^2 - p)}{p^2 - (p^2 - p)} \frac{(k^2 - (p^2 - p) - 1) \dots (k^2 - (p^2 - p) - (p-1))}{(p-1)!} \\
 &= \frac{(k^2 - p)(k^2 - 2p) \dots (k^2 - (p^2 - p))}{(p^2 - p)(p^2 - 2p) \dots (p^2 - (p^2 - p))} \cdot A_0 \cdot A_1 \dots A_p \\
 &= \frac{(kp-1)(kp-2) \dots (kp-(p-1))}{(p-1)(p-2) \dots 1} \cdot A_0 \cdot A_1 \dots A_p \\
 &= \beta \cdot A_0 A_1 \dots A_p
 \end{aligned}$$

$$B = (1 - \frac{k}{p^2})(1 - \frac{k}{p^2}) \dots (1 - \frac{k}{p^2}) \equiv 1 - kp(1 + \frac{1}{p} + \dots + \frac{1}{p-1}) \equiv 1 \pmod{p^2}$$

$$\begin{aligned}
 A_i &= \frac{(k^2 - ip-1)(k^2 - ip-2) \dots (k^2 - ip-(p-1))}{(p^2 - ip-1)(p^2 - ip-2) \dots (p^2 - ip-(p-1))}, i=0, 1, \dots, p-1 \\
 &= \frac{k^2 - p^2 + p^2 - ip-1}{p^2 - ip-1} \cdot \frac{k^2 - p^2 + p^2 - ip-2}{p^2 - ip-2} \dots \frac{k^2 - p^2 + p^2 - ip-(p-1)}{p^2 - ip-(p-1)} \\
 &= (1 + \frac{(p-1)p^2}{p^2 - ip-1})(1 + \frac{(p-2)p^2}{p^2 - ip-2}) \dots (1 + \frac{(k-1)p^2}{p^2 - ip-(p-1)}) \\
 &\equiv 1 \pmod{p^2}, \forall i=0, 1, \dots, p-1
 \end{aligned}$$

因此 $C_{k^2}^{p^2} \equiv k \pmod{p^2} \quad \forall k=1, 2, \dots, p^2$

(2) 取 $n=2p$, p 为奇素数, 则 n 符合条件, 证明如下

$$\begin{aligned}
 \text{对每个 } 1 \leq k \leq 2p, \text{ 有 } C_{kn}^n &= C_{2kp}^{2p} = k C_{2kp-1}^{2p-1} \\
 &= k \cdot \frac{(2kp-1)(2kp-2) \dots (2kp-(p-1))}{(2p-1)(2p-2) \dots (2p-(p-1))} \cdot \frac{2kp}{2p} \cdot \frac{(2kp-1) \dots (2kp-p)}{(k-1)!} \\
 &= k(2k-1) \cdot A_0 \cdot A_1 \\
 &\equiv k(2k-1) \frac{(-1)(-2) \dots (-(p-1))}{(-1)(-2) \dots (-(p-1))} \cdot \frac{(-1)(-2) \dots (-(p-1))}{(p-1)!} \pmod{p} \\
 &\equiv k(2k-1) \pmod{p}
 \end{aligned}$$

取 $k=p, 2p, \frac{p+1}{2}$, 则 $C_{kn}^n \equiv 0 \pmod{p}$

因此 $C_1^n, C_{2n}^n, C_{3n}^n, \dots, C_n^n$ 中至少有 3 个能被 p 整除 $\#$

26. 假设只有有限个 i 符合条件, 则存在正整数 N , 当 $i \geq N$ 时, 均有 $(a_i, a_{i+1}) > \frac{3}{4}i$ (*)

观察, 当 $i \geq N$ 时, 有 $a_i \geq (a_i, a_{i+1}) > \frac{3}{4}i \geq 3N$, 换句话说 $\{1, 2, \dots, 3N\} \subseteq \{a_1, a_2, \dots, a_{i+1}\}$

又 $|\{1, 2, \dots, 3N\} \cap \{a_{2N}, a_{2N+1}, \dots, a_{4N-1}\}| \geq 3N - (2N-1) = N+1$

因此, 存在 $j, 2N \leq j \leq 4N-2$, 使得 $a_j, a_{j+1} \in \{1, 2, \dots, 3N\}$

从而 $a_j \leq 3N, a_{j+1} \leq 3N$, 因此 $(a_j, a_{j+1}) \leq \frac{1}{2} \max\{a_j, a_{j+1}\} \leq \frac{3}{2}N \leq \frac{3}{4}j, j \geq 2N$, 矛盾 $\#$

27 (1) 分析 Fermat 数 $F_n = 2^{2^n} + 1$ ($n=0, 1, 2, \dots$) F_1, F_2, F_3, F_4, F_5 为素数, $641 | F_5$

(2) 回到原题, 构造等差数列 $\{a_n\}_{n=1}^{\infty}$, 令 $m = a_n$

要求 $m \neq 2^\alpha + p$, $\forall \alpha \geq 1$, $\forall$ 素数 p .

即 $m - 2^\alpha \neq p$, $\forall \alpha \geq 1$, $\forall$ 素数 p .

由于 α 为正整数, 不妨设 $\alpha = 2^a \cdot b$, 其中 $2 \nmid b$, $a \geq 0$

① 如果 $0 \leq n \leq 4$, 那么要求 $F_n | m - 2^\alpha$, 即

$$0 \equiv m - 2^\alpha \pmod{641}$$

$$\equiv m - 2^{2^a \cdot b} \pmod{641}$$

$$\equiv m - (-1)^b \pmod{641} \equiv m + 1 \pmod{641}$$

$$\text{因此 } m \equiv -1 \pmod{641}$$

② 如果 $a \geq b$, 那么要求 $q | m - 2^\alpha$, 因此

$$0 \equiv m - 2^\alpha \pmod{q}$$

$$\equiv m - 2^{2^a \cdot b} \pmod{q}$$

$$\equiv m - (2^{2^5} + 1)^{2^{a-5} \cdot b} \pmod{q} \equiv m - 1 \pmod{q}$$

$$\text{从而 } m \equiv 1 \pmod{q}$$

$$\text{构造同余方程组 } \begin{cases} m \equiv -1 \pmod{F_0} \\ m \equiv -1 \pmod{F_1} \\ m \equiv -1 \pmod{F_2} \end{cases} \begin{cases} m \equiv -1 \pmod{F_3} \\ m \equiv -1 \pmod{F_4} \\ m \equiv -1 \pmod{641} \end{cases} \begin{cases} m \equiv -1 \pmod{q} \\ m \equiv -1 \pmod{2} \\ m \equiv -1 \pmod{31} \end{cases} (*)$$

利用 CRT, (*) 存在无穷多正整数解构成等差数列

不妨记为 $\{a_n\}_{n=1}^{\infty}$ 因此对 $\forall n \geq 1$, 均有 $a_n \neq 2^\alpha + p$, 其中 $\alpha \geq 1$, p 为素数

理由如下. 反证法, 假设存在 n , 使 a_n 可以写成 $2^\alpha + p$ 的形式, 不妨设 $m = a_n = 2^\alpha + p$

下面找出矛盾, 显然 $m - 2^\alpha = p$

由于 α 为正整数, 不妨设 $\alpha = 2^a \cdot b$, 其中 $2 \nmid b$, $a \geq 0$, 如果 $0 \leq n \leq 4$, 那么

$$m \equiv -1 - (-1)^b \equiv 0 \pmod{F_n}, \text{ 因此 } p = F_n$$

② 如果 $a \geq 5$, 那么 $m \equiv -1 \pmod{641}$, 因此

$$p = m - 2^\alpha \equiv -1 - 2^\alpha \equiv -1 - 2^{2^a \cdot b} \equiv -1 - (-1)^b \equiv 0 \pmod{641} \dots$$

因此 $p = q$

信息, 若 $m = a_{n_0} = 2^x + p$, 则 $p \in \{F_0, F_1, F_2, F_3, F_4, 8, 641\}$

另一方面, $p = m - 2^x$, $m \equiv 1 \pmod{31}$, 那么

$$p \equiv 1 - 2^x \equiv 1 - 2^1, 1 - 2^2, 1 - 2^3, 1 - 2^4, 1 - 2^5 \equiv -1, -3, -7, -15, 0 \equiv 0, 16, 24, 28, 30 \pmod{31}$$

下面计算 Fermat 数模 31 的余数

$$F_0 \equiv 3 \pmod{31}, F_1 \equiv 5 \pmod{31}, F_2 \equiv 17 \pmod{31},$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 \equiv 2^3 + 1 \equiv 9 \pmod{31}$$

$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 \equiv 2^1 + 1 \equiv 3 \pmod{31}$$

$$641 \equiv 21 \pmod{31} \quad 8 \equiv ? \pmod{31}$$

我们知道 $F_5 = 641 \cdot 8$

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 \equiv 2^2 + 1 \equiv 5 \pmod{31}$$

$$\text{因此 } 641 \cdot 8 \equiv 5 \pmod{31}$$

$$\text{从而 } 21 \cdot 8 \equiv 5 \pmod{31}$$

$$63 \cdot 8 \equiv 15 \pmod{31}$$

$$\text{即 } 8 \equiv 15 \pmod{31} \quad \text{矛盾} \quad \#$$

28. (1) 观察: $u_p = pu_1 + u_0$

$$u_{2p} = pu_{p+1} + u_p = p(pu_2 + u_1) + (pu_1 + u_0)$$

$$= p^2 u_2 + 2pu_1 + u_0$$

$$u_{3p} = pu_{2p+1} + u_{2p} = p(pu_{p+2} + u_{p+1}) + u_{2p}$$

$$= p^2(pu_3 + u_2) + p(pu_2 + u_1) + p^2 u_2 + 2pu_1 + u_0$$

$$= p^3 u_3 + 3p^2 u_2 + 3pu_1 + u_0$$

$$\text{猜想 } u_{4p} = p^4 u_4 + 4p^3 u_3 + 6p^2 u_2 + 4pu_1 + u_0$$

$$\text{因此 } u_{np} = \sum_{k=0}^n C_n^k p^k \cdot u_k \quad \checkmark$$

$$\text{推广 } u_{npt+i} = \sum_{k=0}^n C_n^k p^k \cdot u_{kt+i}, \text{ 对 } n, i \text{ 归纳证明 } \checkmark$$

(2) 想证 $V_p(u_n) = V_p(n)$

$$\text{若 } 1 \leq i \leq p-1, \text{ 则 } V_p(u_{npt+i}) = 0 = V_p(npt+i)$$

$$\text{若 } i=0, \text{ 则 } V_p(u_{np}) = V_p\left(\sum_{k=0}^n C_n^k p^k u_k\right)$$

$$\text{我们知道 } \sum_{k=0}^n C_n^k p^k u_k = \sum_{k=1}^n C_n^k p^k u_k = np + C_n^2 p^2 \cdot 2 + C_n^3 p^3 \cdot 3 + \cdots + C_n^n p^n \cdot u_n$$

如果 $p \geq 3$, 那么

$$V_p(C_n^k \cdot p^k u_k) = V_p(C_n^k) + k + V_p(u_k) \\ \geq V_p(n) - V_p(k) + k + V_p(u_k) > V_p(n) + 1 = V_p(np)$$

从而 $V_p(u_{np}) = V_p(np)$

如果 $p=2$, 那么 $u_{2n} = \sum_{k=1}^n C_n^k \cdot 2^k \cdot u_k$

$$= 2n + C_n^2 \cdot 2^2 \cdot 2 + C_n^3 \cdot 2^3 \cdot u_3 + \dots + C_n^n \cdot 2^n \cdot u_n$$

$$V_2(C_n^2 \cdot 2^2 \cdot 2) = 3 + V_2(C_n^2) = 2 + V_2(n) + V_2(n-1) > V_2(n) + 1 = V_2(2n)$$

对 $\forall k \geq 3$

$$V_2(C_n^k \cdot 2^k \cdot u_k) \geq k + V_2(C_n^k) \geq k + V_2(n) + V_2(n-1) + V_2(n-2) - V_2(k!) > V_2(n) + 1$$

我们知道 $V_2(k!) = k - S(k) \leq k-1$, 因此

$$V_2(C_n^k \cdot 2^k \cdot u_k) \geq 1 + V_2(n) + V_2(n-1) + V_2(n-2) > 1 + V_2(n) = V_2(2n)$$

因此 $V_2(u_{2n}) = V_2(2n)$ #

29. (1) $m=1$, 显然

(2) 以下, $m>1$, 不妨设 m 的标准分解式为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$

不妨设 $n \equiv r_i \pmod{p_i}$, $i=1, 2, \dots, t$, 其中 $0 \leq r_i \leq p_i-1$

① 如果 $r_i=0$, 那么取 $a_i=1$, $b_i=p_i-1$, 则 $2r_i \equiv a_i + b_i \pmod{p_i}$

② 如果 $r_i \neq 0$, 即 $1 \leq r_i \leq p_i$. 取 $a_i=b_i=r_i$, 则 $2r_i \equiv a_i + b_i \pmod{p_i}$

构造同方程组

$$\begin{cases} x \equiv a_1 \pmod{p_1} \\ \dots \\ x \equiv a_t \pmod{p_t} \end{cases} \quad (*)$$

利用 CRT, (*) 有解 $x = x_0$.
因此 $2n = x_0 + (2n - x_0)$

从而 $x_0 \equiv a_i \pmod{p_i}$ $\forall i=1, \dots, t$

$2n - x_0 \equiv 2r_i = a_i \equiv b_i \pmod{p_i}$, $\forall i=1, \dots, t$

从而 $(x_0, m)=1$, $(2n-x_0, m)=1$

因此 $2n = x_0 + (2n-x_0)$ 符合条件 #

30. 不妨设 S 符合条件, 令 $|S|=n$, $S = \{s_1, s_2, \dots, s_n\}$

对 $\forall s \in S$, 不妨设 s 的不同正因子分解 $d_1, d_2, \dots, d_{\tau(s)}$

利用条件, 分别存在唯一的 $t_1, t_2, \dots, t_{\tau(s)} \in S$, 使得

$$\begin{cases} (t_1, s) = d_1 \\ (t_2, s) = d_2 \\ \dots \\ (t_{\tau(s)}, s) = d_{\tau(s)} \end{cases}$$

因此 $t_1, t_2, \dots, t_{\tau(S)}$ 互不相同, 从而 $|S| = m \geq \tau(S)$

另一方面 $(S, S), (S_2, S), \dots, (S_m, S)$ 均为 S 的正因子

互不相同, 从而 $m \leq \tau(S)$, 因此 $|S| = m \leq \tau(S)$, $\forall i \in S$

换句话说, 如果 S 符合条件, 那么 S 中的元素个数等于 S 中每一个元素的所有不同的正因子的个数.

因此 $|S|$ 只能为 2 的幂, 即 $|S| = 2^k$, $k = 0, 1, 2, \dots$

现在 S 符合条件, 想证 $|S| = 2^k$, 只需证 S 中每一个元素为无平方因子

素数 p , $\forall s \in S$, 均有 $v_p(s) \leq 1$

反证法, 假设 $v_p(s) \geq 2$, 令 $s = p^\alpha s_1$, $p \nmid s_1$, $\alpha \geq 2$

由于 $\frac{s}{p} = p^{\alpha-1} s_1 = (u, S)$, $\exists u \in S$

因此 $p^{\alpha-1} s_1 \mid u$, $\exists v \in S$, 使得 $(v, S) = 1$

因此 $(v, u) \neq 1$, 且 $\tau(u) = \tau(v) = \tau(S) = |S|$

从而存在素数 $q \mid u$ 且 $q \nmid v$, 从而 $q \nmid S$

从 $q \cdot p^{\alpha-1} s_1 \mid u$

因此 $m = \tau(u) \geq \tau(q \cdot p^{\alpha-1} s_1) = 2\alpha \tau(s_1) > (\alpha+1) \tau(s_1) = \tau(s) = m$, 矛盾

最后, 对每个 2^k , $k = 0, 1, 2, \dots$, S 均存在

① $k=0$ 时, 取 $S = \{1\}$ 即可

② $k \geq 1$ 时, 取 2^k 个互不相同的素数

$p_1, p_2, \dots, p_k; q_1, q_2, \dots, q_k$

令 $S = \{r_1, r_2, \dots, r_k \mid r_i \in \{p_i, q_i\}, i = 1, 2, \dots, k\}$

则 $|S| = 2^k$

容易验证: S 符合条件.

31. 令 $f(m)$ 表示 $m+1, m+2, \dots, m+n^2$ 中好数的个数

想证, 存在无穷多的正整数 m , 使得 $f(m) = n+1$

1° 显然 $|f(m+1) - f(m)| \leq 1$

理由: 观察以下的两组数 $m+1, m+2, \dots, m+n^2$

$m+2, \dots, m+n^2, m+1+n^2$

2° 再证, 存在无穷多正整数 m , 使 $f(m) \geq n+1$

对 n , 分情况讨论

① 若 $n \geq 3$, 那么观察以下的数: $k^6+1, k^6+2, \dots, k^6+n^2$, 即 $m=k^6$

我们知道 $k^6+1^2, k^6+2^2, k^6+3^2, \dots, k^6+n^2, k^6+2^3$ 均为好数

从而 $f(k^6) \geq n+1$

② 若 $n=2$, 观察以下的数: $k^3+1, k^3+2, k^3+3, k^3+2^2$, k 待定

我们知道 k^3+1^2, k^3+2^2 均为好数

现在要求正整数 k 满足条件: $k^3+2=y^3+z^2$, 其中 $y, z \in \mathbb{N}^*$

再要求 $y=k-1$, 因此, 上式改写为

$$k^3+2=(k-1)^3+z^2, \text{ 因此我们有}$$

$$k^3-(k-1)^3+2=z^2$$

$$\text{从而 } 3k^2-3k+3=z^2, \text{ 令 } z=3z_1, \text{ 从而}$$

$$k^2-k+1=3z_1^2$$

$$\text{即 } 4k^2-4k+4=12z_1^2, \quad (2k-1)^2-12z_1^2=-3$$

我们知道 $x^2-12y^2=-3$ 有无穷多正整数解 (x, y) 且 $2 \nmid x$

3° 最后, 再证: 存在无穷多正整数 m , 使得 $f(m) \leq n+1$

反证法: 假设只有有限个正整数 m 使得 $f(m) \leq n+1$

因此存在正整数 M , 使 $m \geq M$ 时, 有 $f(m) \geq n+2$, 下面构造矛盾

考虑集合 $S = \{1, 2, 3, 4, \dots, T^6\}$, 其中 T 为正整数, 充分大

对 $\forall i \in S$, 若 $i = x^2 + y^3$, 其中 $x, y \in \mathbb{N}^*$, 则

$$x^2 < T^6 \text{ 且 } y^3 < T^6 \text{ 从而 } 1 \leq x < T^3, 1 \leq y < T^2$$

因此 S 中好数的个数 $\leq (T^3-1)(T^2-1) < T^6$

由于 T 充分大, n 给定, 考虑以下的数

$M+1, M+2, \dots, M+n^2$ 中至少有 $n+2$ 个好数

$(M+n^2)+1, (M+n^2)+2, \dots, (M+n^2)+n^2$ 中至少有 $n+1$ 个好数

一直做下去, 我们知道: S 中至少有 $\left\lfloor \frac{T^6-M}{n^2} \right\rfloor (n+2)$ 个好数

$$\text{从而 } T^6 > \left\lfloor \frac{T^6-M}{n^2} \right\rfloor (n+2) > \left(\frac{T^6-M}{n^2} - 1 \right) (n+2)$$

即 $\frac{T^5}{n+2} + 1 + \frac{m}{n} > \frac{T^6}{n}$, $T \rightarrow \infty$, 矛盾 $\#$

32. 分析: (1) $n=1$, 不行

(2) 以下, $n > 1$, 对 n 分情况讨论

1° 如果 n 为奇数, 显然 $n^m + 1$ 为偶数, 取 $p=2$, 因此 $q-2 \mid m$, $q \mid n^m + 1$, $q > 2$
因此 $(n, q) = 1$, 考虑同余方程组

$$\begin{cases} m \equiv 0 \pmod{q-2} \\ m \equiv 2 \pmod{q-1} \end{cases} \quad (*)$$

利用 CRT, (*) 有无穷多正整数解, 任取一个正整数解 m

那么 $q-2 \mid m$ 且 $m \equiv 2 \pmod{q-1}$, 因此 $m = 2 + (q-1)L$

从而 $n^m + 1 \equiv n^{2+(q-1)L} + 1 \equiv n^2 + 1 \equiv 0 \pmod{p}$

即 $q \mid n^m + 1$ $\times$

2° 以下 $n > 1$ 且 $2 \mid n$, 想证, n 不符合条件

反证法, 假设 n 符合条件, 因此存在素数 p, q , 正整数 m ,

使得 $p < q$, $p \mid n^m + 1$, $q \mid n^m + 1$, 且 $q-p \mid m$

由于 n 为偶数, 那么 $n^m + 1$ 为奇数, 因此 p, q 为奇素数

从而 $3 \leq p < q$, 因此 $2 \mid q-p$, 从而 m 为偶数. 下面推出矛盾.

引理: 设 p 为奇素数, a, n 均为正整数, 如果 $p \mid a^{2^n} + 1$ 那么 $2^{n+1} \mid p-1$

证明: 由于 $p \mid a^{2^n} + 1$, 又 $a^{2^n} + 1 \mid (a^{2^n} + 1)(a^{2^n} - 1) = a^{2^{n+1}} - 1$

因此 $p \mid a^{2^{n+1}} - 1$ 显然 $(a, p) = 1$ 利用 FLT, 有 $p \mid a^{p-1} - 1$

因此 $p \mid (a^{2^{n+1}} - 1, a^{p-1} - 1) = a^{(2^{n+1}, p-1)} - 1 = a^d - 1$

其中 $d = (2^{n+1}, p-1)$, 因此 $d \mid 2^{n+1}$ 且 $d \mid p-1$, 由 $d \mid 2^{n+1}$ 那么 $d \mid 2^t$

其中 $1 \leq t \leq n+1$, 想证 $t = n+1$, 即 $d = 2^{n+1}$, 又 $d \mid p-1$

从而 $2^{n+1} \mid p-1$ $\#$

现在 m 为偶数, 不妨设 $m = 2^\alpha \cdot m_1$, 其中 $2 \nmid m_1$, $\alpha \geq 1$

由于 $p \mid n^m + 1 = n^{2^\alpha \cdot m_1} + 1 = (n^{m_1})^{2^\alpha} + 1$, 利用引理, 有 $2^{\alpha+1} \mid p-1$

同理 $q \mid n^m + 1$, 那么 $2^{\alpha+1} \mid q-1$, 因此 $2^{\alpha+1} \mid (q-1) - (p-1) = q-p$, 又 $q-p \mid m$

从而 $2^{\alpha+1} \mid m = 2^\alpha \cdot m_1$, 矛盾 $\#$

34. (1) 同证: 若 $a, b \in \mathbb{N}^*$, 则 $ab = (a, b) \cdot [a, b]$

(2) 回到原题

不妨设 $1 \leq a_1 < a_2 < \dots < a_n < N$, 由于 $m = (a_1, a_2, \dots, a_n)$

那么令 $a_i = mb_i$, $i = 1, 2, \dots, n$

因此 $b_1 < b_2 < \dots < b_n$ 且 $(b_1, b_2, \dots, b_n) = 1$

我们知道 $M = [a_1, a_2, \dots, a_n] = [mb_1, mb_2, \dots, mb_n] = m[b_1, b_2, \dots, b_n]$

由于 $M | m^2$, 那么 $m \cdot [b_1, b_2, \dots, b_n] | m^2$

因此 $[b_1, b_2, \dots, b_n] | m$, 从而 $b_i | m$, $\forall i = 1, 2, \dots, n$

由于 $b_1 < b_2 < \dots < b_n$, 那么 $b_1, b_2, \dots, b_n$ 是 n 个互不相同的正因子

引理: 设 n 为正整数, 则 $\tau(n) \leq 2\sqrt{n}$, 其中 $\tau(n)$ 表示 n 的所有不同的正因子个数

理由: 不妨设 $1 = d_1 < d_2 < \dots < d_k = n$ 为所有不同正因子

因此 $d_i \cdot d_k = d_2 \cdot d_{k-1} = \dots = d_k \cdot d_1 = n$

① 如果 k 为偶数, 则 $d_1 < d_2 < \dots < d_{\frac{k}{2}} \leq \sqrt{n}$

因此 $\frac{k}{2} \leq d_{\frac{k}{2}} \leq \sqrt{n}$, 从而 $k \leq 2\sqrt{n}$

② 如果 k 为奇数, 则 n 为平方数, 因此, 令 $k = 2l + 1$

$d_1 < d_2 < \dots < d_l < d_{l+1} = \sqrt{n}$

因此 $l + 1 \leq d_{l+1} \leq \sqrt{n}$, 从而 $k = 2l + 1 < 2(l + 1) \leq 2\sqrt{n}$ #

利用引理, 有 $n \leq 2\sqrt{m}$, 因此 $n^2 \leq 4m$

又 $N > a_n = m \cdot b_n \geq mn$ 从而 $n^3 \leq n^2 \cdot n \leq 4m \cdot n < 4N$. #

35. (1) 令 $S_k(n) = 1^k + 2^k + \dots + n^k$

① 已知 $S_1(n) = 1 + 2 + \dots + n = \frac{n(n+1)}{2}$

$S_1(n) = y^2 \Leftrightarrow \frac{n(n+1)}{2} = y^2$

$\Leftrightarrow (2n+1)^2 = 8y^2 + 1$

$\Leftrightarrow (2n+1)^2 - 8y^2 = 1$

② $S_2(n) = 1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$

$S_2(n) = y^2 \Leftrightarrow \frac{n(n+1)(2n+1)}{6} = y^2$

$\Leftrightarrow n = 1$ 和 $n = 144$

(证明很复杂, 略)

$$\textcircled{3}. S_3(n) = 1^3 + 2^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

(2) 回到原题

求所有的正整数 m , 满足条件, 存在正整数 n_0 , 对 $\forall n \geq n_0$ 均有 $f(n) = 1^m + 2^m + \dots + n^m$ 均为平方数

想证: $m=3$

理由如下

① $m=3$, 符合条件

② 下证 $m \neq 3$ 时, 不符合条件

1° 若 $2 \mid m$, 则 m 不符合条件, 取 $n = 9l + 2$, 因此

$$f(n) = f(9l+2) = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + 7^2 + 8^2 + 9^2 + \dots + (9l+1)^2 + (9l+2)^2 \\ \equiv 2 \pmod{3}$$

从而 $f(n)$ 不是平方数, m 不符合条件.

2° 若 $2 \nmid m$ 且 $m \neq 3$, 则 m 不符合条件, 理由如下:

反证法, 假设存在正整数 n_0 , 使 $n \geq n_0$ 时, $f(n)$ 为平方数

取 $n = 2k \cdot (1 + 2^m)^2 - 3 = 2kt^2 - 3$, 其中 $t = 1^m + 2^m$, $k \in \mathbb{N}^+$, 待定.

因此 $y^2 = f(n) = 1^m + 2^m + \dots + n^m$

$$= (1^m + 2^m) + (3^m + (2kt^2 - 3)^m) + (4^m + (2kt^2 - 3)^m) + \dots + \\ ((kt^2 - 1)^m + (kt^2 + 1)^m) + kt^2$$

$$\equiv 1 + 2^m \equiv t \pmod{t^2}$$

$y^2 = f(n) = t + t^2 a = t(1 + ta)$, 由于 $(t, 1 + ta) = 1$, t 为平方数, 令 $t = b^2$, $b \geq 1$

$$\text{因此 } 1 + 2^m = b^2$$

$$\text{从而 } 2^m = b^2 - 1 = (b-1)(b+1)$$

$$2^{m-2} = \frac{b-1}{2} \cdot \frac{b+1}{2}, \text{ 其中 } \left(\frac{b-1}{2}, \frac{b+1}{2}\right) = 1$$

$$\text{因此 } \begin{cases} \frac{b-1}{2} = 1 \\ \frac{b+1}{2} = 2^{m-2} \end{cases} \Rightarrow \begin{cases} b = 3 \\ m = 3 \end{cases} \text{ 矛盾} \quad \#$$

37. (1) 熟知 $n+1 \mid C_n^n$, $\forall n \geq 1$, 因此 $f(1) = 1$

(2) $m=2$ 时, 我们知道 $(n+1)(n+2) \mid f(2) \cdot C_n^n$, $\forall n \geq 1$

观察一下: $2 \cdot 3 \mid f(2) \cdot C_2^1$, $3 \cdot 4 \mid f(2) \cdot C_4^2$, $4 \cdot 5 \mid f(2) \cdot C_6^3$, $5 \cdot 6 \mid f(2) \cdot C_8^4$, ...

因此 $6 \mid f(2)$, 从而 $f(2) \geq 6$, 猜想 $f(2) = 6$, 换句话说 $(n+1)(n+2) \mid 6C_{2n}^n, \forall n \geq 1$
(不会证)

(3) $m=3$ 时, 我们知道 $(n+1)(n+2)(n+3) \mid f(3) \cdot C_{2n}^n, \forall n \geq 1$

观察一下: $4! \mid f(3) \cdot C_2^1$, $3 \cdot 4 \cdot 5 \mid f(3) \cdot C_4^2$, $4 \cdot 5 \cdot 6 \mid f(3) \cdot C_6^3$, ...

从而 $60 \mid f(3)$, 从而 $f(3) \geq 60$, 猜想 $f(3) = 60$

(4) $m=4$ 时, 我们知道 $(n+1)(n+2)(n+3)(n+4) \mid f(4) \cdot C_{2n}^n, \forall n \geq 1$

$60 \mid f(4)$, $3 \cdot 4 \cdot 5 \cdot 6 \mid f(4) \cdot C_4^2$, $4 \cdot 5 \cdot 6 \cdot 7 \mid f(4) \cdot C_6^3$, ...

(5) 猜想: $f(m) = m! \cdot C_{2m-1}^{m-1}, \forall m \geq 1$ (杨辉三角)

1° 先证: $(n+1)(n+2) \cdots (n+m) \mid m! \cdot C_{2m-1}^{m-1} \cdot C_{2n}^n, \forall n \geq 1$

令 $A(m, n) = \frac{m! \cdot C_{2m-1}^{m-1} \cdot C_{2n}^n}{(n+1)(n+2) \cdots (n+m)}$, 猜想 $A \in \mathbb{Z}$

对 m 利用归纳法

① $m=1$ 时, 有 $A(1, n) = \frac{1}{n+1} C_{2n}^n \in \mathbb{Z}, \forall n \geq 1$

② 假设对 $\forall n \geq 1$, 均有 $A(m-1, n) \in \mathbb{Z}$

观察 $A(m, n) + A(m-1, n+1)$

$$\begin{aligned} \text{我们观察 } A(m, n) &= \frac{m! \cdot C_{2m-1}^{m-1} \cdot C_{2n}^n}{(n+1)(n+2) \cdots (n+m)} = \frac{m! \cdot C_{2m}^m \cdot C_{2n}^n}{2(n+2) \cdots (n+m)} \\ &= \frac{m! \cdot \frac{(2m)!}{m!m!} \cdot \frac{(2n)!}{n!n!}}{2(n+1) \cdots (n+m)} = \frac{(2m)! \cdot (2n)!}{2 \cdot m! \cdot n! \cdot (n+m)!} \end{aligned}$$

因此 $A(m, n) + A(m-1, n+1) = \cdots = 4A(m-1, n) \in \mathbb{Z}$
(过于复杂)

因此 $A(m, n) \in \mathbb{Z} \#$

2° 再证最小性, 记 $f(m) \mid m! \cdot C_{2m-1}^{m-1}$

由于 $f(m) \mid m! \cdot C_{2m-1}^{m-1}$ 即 $f(m) \mid \frac{(2m)!}{2 \cdot m!}$, 猜想 $f(m) = \frac{(2m)!}{2 \cdot m!}$

反证法, 假设 $f(m) \neq \frac{(2m)!}{2 \cdot m!}$, 那么 $f(m) < \frac{(2m)!}{2 \cdot m!}$

令素数 $p \mid \frac{(2m)!}{f(m) \cdot 2 \cdot m!}$ 因此, 利用 $A(m, n) = \frac{\frac{(2m)!}{2 \cdot m!} \cdot C_{2n}^n}{(n+1) \cdots (n+m)} = \frac{\frac{(2m)!}{2 \cdot m!} \cdot \frac{(2n)!}{n!n!}}{f(m)} = \frac{f(m) \cdot C_{2n}^n}{(n+1) \cdots (n+m)}$

从而 $p \mid A(m, n)$

因此, 对 $\forall m' \geq m$ 均有 $p \mid A(m', n)$, $\forall n \geq 1$

(对 $m' \nmid \exists$ 成立)

取 $m' = n = p^k$, k 充分大, 使得 $p^k > m$

$$p \mid A(p^k, p^k) = \frac{C_{p^k}^{p^k}}{2} = \binom{p^k}{2} \not\equiv 0 \pmod{p}$$

矛盾 $\#$