

初

降

数

记

四

记

春

内

Ex 19. 设 p 为素数, n 为正整数, 且 $n < p < \frac{3}{2}n$, 证明:

$$p \mid \sum_{j=1}^n (-1)^j \cdot (C_n^j)^3.$$

分析:

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

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

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 , 用归纳法.

(i) $k=1$ 时, 有 $S_1 = 1+2+\dots+(p-1) = \frac{p(p-1)}{2} \equiv 0 \pmod{p}$. ✓

(ii) 假设 $k \leq m$, 结论成立. 此时 $m \leq p-3$.

(iii) 考虑 $k=m+1$ 的情况, 想证: $p \mid S_{m+1}$.

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. (i) 也

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

(ii) 也

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

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 $m \leq p-3$, 则 $p \nmid m+2 \leq p-1$. 因此,
 $p \nmid m+2$, 从而 $p \mid S_{m+1}$. ~~*~~

推论: 设 p 为奇素数, $k \in \mathbb{Z}$, 则

$$1^k + 2^k + \dots + (p-1)^k \equiv \begin{cases} 0 \pmod{p}, & \text{若 } p-1 \nmid k; \\ -1 \pmod{p}, & \text{若 } p-1 \mid k. \end{cases}$$

(2) 回到原问题.

∴ 现在 p 为素数, n 为正整数, 且 $n < p < \frac{3}{2}n$. 则

$$\frac{2}{3}p < n < p.$$

因此 $p \geq 5$. 而且 $2p < 3n < 3p$. 则 $3p - 3n < p$.

(ii) 现在 $0 \leq j \leq n < p$, 我们知道

$$C_n^j = \frac{n(n-1) \cdots (n-j+1)}{j!}.$$

(*) 比,

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

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

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

从而

$$C_n^j \equiv (-1)^j \cdot \frac{(p-n)(p-n+1) \cdots (p-n+j-1)}{j!} \pmod{p}$$

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

(iii) ~~由~~ $\sum_{j=0}^n (-1)^j (C_n^j)^3$, 证:

$$\sum_{j=0}^n (-1)^j (C_n^j)^3 \equiv 0 \pmod{p}.$$

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

如果 $n+1 \leq j \leq p-1$, 则 $p \mid C_{p-n+j-1}^j$. 因此 (*) 恒成立

现证为 $\sum_{j=0}^{p-1} (C_{p-n+j-1}^j)^3 \equiv 0 \pmod{p}. \quad (**)$

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

因此

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

从 $\mathbb{P}_p$

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

其中

$$\begin{aligned} f(x) &= ((x+p-n-1)(x+p-n-2) \cdots (x+1))^3 \\ &= x^t + a_{t-1}x^{t-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]. \end{aligned}$$

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

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

$$= S_t + a_{t-1} S_{t-1} + \dots + a_1 S_1 + a_0 p.$$

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

从而 $p \mid M$. ~~#~~

Ex 20. 设正整数 $n \geq 3$, $a_1, a_2, \dots, a_n$ 是 n 个不同的正整数.

证明: 存在 $i \neq j$, 使得 $a_i + a_j$ 不整除 $3a_1, 3a_2, \dots, 3a_n$ 中的任何一项.

分析: 反证法, 如果结论不对, 那么对 $\forall i \neq j$, 均存在 k , 使得

$$a_i + a_j \mid 3a_k.$$

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

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

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: $a_1 \equiv a_2 \equiv \dots \equiv a_{n-1} \equiv -a_n \pmod{3}$.

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 , 使得 $\frac{a_i}{3}$:

$$a_{n-2} + a_{n-1} \mid 3a_k.$$

由 $a_{n+2} + a_{n-1} \equiv -2a_n \not\equiv 0 \pmod{3}$, 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

$$\underline{a_n = (a_{n-1} + a_{n-2}) \cdot L, \text{ 其中 } L \in \mathbb{Z}_{\geq 1}.$$

(3) 取 $i=n-1$, $j=n$. 则存在 k , 使得

$$a_{n-1} + a_n \mid 3a_k.$$

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

从而 $q=1$ 或 2 .

$$\begin{aligned} \text{① 若 } q=1, \text{ 则 } 3a_k = a_{n-1} + a_n &\geq a_{n-1} + (a_{n-1} + a_{n-2}) \\ &= 2a_{n-1} + a_{n-2} > 3a_{n-2}. \end{aligned}$$

同也 $k=n-1$ 或 n .

• 如果 $k=n-1$, 则 $\exists a_{n-1} = a_{n-1} + a_n$. 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 $\exists a_n = a_{n-1} + a_n$ 矛盾.

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

同也 $a_n = 2a_{n-1}$. 从而

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

Ex 21. 设 p 为素数, 则存在正整数 n , 使得:

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

分析:

(1) 引理, 设 $a \in \mathbb{Z}$ 且 $(a, p) = 1$, 则 $a^{p-1} \equiv 1 \pmod{p}$. 因此

$$\frac{1}{a} \equiv a^{p-2} \pmod{p}.$$

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

$$a^n \equiv a^r \pmod{p}.$$

(2) 引理 设 p 为素数, 那么

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

$$\mathbb{Z}_p \quad 1^{p(p-1)} + 2^{p(p-1)-1} + 3^{p(p-1)-2} + \dots + (p(p-1))^1 \equiv -1 \pmod{p}.$$

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

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

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

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

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

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

我們知道:

$$\sum_{i=0}^{p-2} j^{1-i} \equiv \begin{cases} 0 \pmod{p}, & j \not\equiv 1 \pmod{p}; \\ -1 \pmod{p}, & j \equiv 1 \pmod{p}. \end{cases} \quad (\text{思考})$$

代回去, 有

$$\sum_{k=1}^{p(p-1)} k^{p(p-1)+1-k} \equiv -1 \pmod{p}. \quad \#$$

(3) 构造 n :

令 $n = t p(p-1)$, 其中 $t \in \mathbb{Z}_1$, 待定.

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

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

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

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

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

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

$$\overline{F}_2 \quad -t \equiv 2024 \pmod{p}, \quad 2024! \quad \#$$

思考题: 设 p 为素数, 证明: 存在正整数 n , 使得

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

Ex 23. 证明: 存在无穷多正整数 a , 满足条件:

$$a! + (a+2)! \mid (a+2[\sqrt{a}])! \quad (*)$$

分析: 令 $b = [\sqrt{a}]$, 则 (*) 改写为:

$$a! + (a+2)! \mid (a+2b)!$$

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

$$\text{事实上 } 1 + (a+2)(a+1) = a^2 + 3a + 3. \text{ 当 } b = [\sqrt{a}] \text{ 时}$$

$$\text{取 } a = c^2 - 1, \text{ 其中 } c \in \mathbb{Z}_{>1}, \text{ 给定, 那么 } b = c - 1.$$

因此 (**) 改写为:

$$c^4 + c^2 + 1 \mid (c^2 + 2c - 3)(c^2 + 2c - 4) \cdots c^2 \quad (***)$$

问题: 想: 是否存在无穷正整数 c , 使得:

$$c^4 + c^2 + 1 \mid (c^2 + 2c - 3)(c^2 + 2c - 4) \cdots c^2. \quad (****)$$

我们知:

$$c^4 + c^2 + 1 = (c^2 - c + 1)(c^2 + c + 1).$$

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

由于 c 足够大, 即, $c^2 + c + 1 \mid (c^2 + 2c - 3) \cdots c^2$.

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

令 $c^2 - c + 1 = 3y^2$. 则 $4c^2 - 4c + 4 = 12y^2$. 即

$$(2c-1)^2 - 12y^2 = -3.$$

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

且 $2 \nmid x$.

任取一组正整数解 (x_0, y_0) ^{x_0 是奇数} 则 $x_0 = 2c-1$.

$$(2c-1)^2 - 12y_0^2 = -3.$$

从而

$$(2c-1)^2 = 12y_0^2 - 3.$$

从而

$$2c-1 > \sqrt{12} y_0 - 1$$

从而

$$2c-3 > \sqrt{12} y_0 - 3 > 2y_0 !$$

$$(\dagger) y_0, (2y_0)! \mid (c^2+2c-3)(c^2+2c-4)\cdots c^2.$$

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

Ex 24. 固定正整数 n , 求所有大于1的正整数 a , 满足条件:

$$a^n \mid n(n+1)(n+2)\cdots(a-1).$$

分析: 对 n , 分情况讨论:

(1) $n=1$ 时, 求所有的大于1的正整数 a , 满足条件:

$$a \mid (a-1)!$$

显然 $a=p$ 为素数, 不满足条件. $a=4$ 也不满足条件. 其余的正整数 $a \geq 1$, 均满足条件. (课后思考)

(2) 以下 $n \geq 2$, 求所有的正整数 $a \geq 2$. 满足条件:

$$a^n \mid n(n+1) \dots (n-1).$$

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

$$p^n \mid n(n+1) \dots (p-1) = \frac{(p-1)!}{(n-1)!}.$$

从而 $p^{n+1} \mid \frac{(p-1)!}{n!}.$

但是 $v_p \left(\frac{(p-1)!}{n!} \right) = v_p((p-1)!) - v_p(n!).$

② 1.2: Legendre's v_p :

$$v_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right] = \frac{n-s(n)}{p-1}. \quad (\text{思考}).$$

$$\begin{aligned} (i) \leadsto v_p((pn)!) - v_p(n!) &= \frac{pn-s(pn)}{p-1} - \frac{n-s(n)}{p-1} \\ &= \frac{pn-s(n)}{p-1} - \frac{n-s(n)}{p-1} = n. \quad \text{即 } p^n \parallel \frac{(pn)!}{n!}, \text{ 证毕. } \# \end{aligned}$$

(ii) 如果 $a \geq 2$, 为合数. 即 $\exists \frac{1}{a} \in \mathbb{N} \times \frac{1}{a}$. 即
对 $\forall n \geq 2$, 均有 $a^n \mid n(n+1) \cdots (a^n-1)$.

对 n , 用同数学归纳法

① $n=2$ 时. 相 $\leadsto a^2 \mid 2 \cdot 3 \cdots (2a-1) = (2a-1)!$

由于 a 为合数. 不妨设 a 的最小因子为 p . 则 $p \mid a$.

$$\wedge a = pb, \quad p \leq b.$$

$$(I) \text{ 若 } p < b, \text{ 则 } a^2 = p^2 \cdot b^2 = p \cdot b \cdot pb$$

$$p < p < b < pb < 2a-1, \quad \text{且 } a^2 \mid (2a-1)!$$

$$(II) \text{ 若 } p = b, \text{ 则 } a = p^2, \quad p \geq 2. \quad \text{想证: } p^4 \mid (2p^2-1)!$$

$$(A) \text{ 若 } p \geq 3, \text{ 则 } p < 2p < p^2 < 2a-1 \text{ 则 } p^4 \mid (2a-1)!$$

$$(B) \text{ 若 } p=2, \text{ 则 } 2^4 \mid (2^2-1)! = 7! = 7 \times 720 = 5040. \quad \#$$

$$(2) \text{ 作 } 2 \text{ 个 } 2 \text{ 个 } n, \text{ 记 } i \in n, j \in n.$$

$$(3) \text{ 若 } n+1 \text{ 为素数, 此时 } a \text{ 为合数, 想证:}$$

$$a^{n+1} \mid (n+1)(n+2) \cdots (a(n+1)-1).$$

我们证之:

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

$$= (n+1)(n+2) \dots (na-1) \cdot \underline{na} \cdot (na+1) \dots (a(n+1)-1)$$

$$= \underline{n(n+1)(n+2) \dots (na-1)} \cdot a \cdot (na+1) \dots (a(n+1)-1)$$

$$\begin{array}{l} \text{证法一} \\ \equiv \\ \text{证法二} \end{array} \quad 0 \pmod{a^{n+1}} \quad \text{由 } a^{n+1} \mid (n+1)(n+2) \dots (a(n+1)-1) \quad \#$$