

初

等

数

论

(三)

记

看

内

Ex 12. n 为好数当且仅当 $p \nmid n$ 且 $\text{ord}_{n^p}(p) \equiv 0 \pmod{p}$.

分析:

(1) 若 $p \mid n$, 则 n 不是好数.

(2) 若 $p \nmid n$ 且 $p \nmid \text{ord}_{n^p}(p)$, 则 n 也不是好数.

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

不妨设 $\delta = \text{ord}_{n^p}(p)$, 即 δ 为最小的正整数满足 $p^\delta \equiv 1 \pmod{n^p}$.

令 $m = p^\alpha \cdot n$, 其中 α 待定, 要求 (*) 成立. 因此

$$\left\{ \frac{p^{m-\alpha p}}{n^p} \right\} = \left\{ \frac{p^n}{n^p} \right\}$$

$$\text{H.R.} \quad n^p \mid p^{m-\alpha p} - p^n = p^n \cdot (p^{m-n-\alpha p} - 1) = p^n \cdot (p^{(p^\alpha-1) \cdot n - p^\alpha} - 1).$$

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

再令 $\alpha = nx$, 其中 x 待定.

$$\text{则 } (**) \Leftrightarrow n^p \mid p^{(p^{nx}-1) \cdot n - p^{nx}} - 1 = p^n (p^{nx} - p^{x-1}) - 1. \quad (***)$$

我們知道: $\delta = \text{ord}_{n^p}(p)$.

$$\text{取 } a = p^n, \quad b = \delta, \quad c = p, \quad d = 1, \quad e = 1.$$

利用 Ex3, T-3.1 可知: $a^x - px \equiv 1 \pmod{\delta}$ 有无穷多正整数 x .

取一个正整数解 $x = x_0$. 则 $\delta \mid p^{nx_0} - px_0 - 1$. 因此

$$p^{p^{nx_0} - px_0 - 1} \equiv 1 \pmod{n^p}. \quad \text{从而 } p^n (p^{nx_0} - p^{x_0-1}) \equiv 1 \pmod{n^p}.$$

$$\text{从而 } n^p \mid p^n (p^{nx_0} - p^{x_0-1}) - 1. \quad \text{从而 } \left\{ \frac{p^m}{n^p} \right\} = \left\{ \frac{p^n}{n^p} \right\}.$$

其中 $m = p^2 \cdot n = p^{n \times 0} \cdot n$. #

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

反证法, 如果结论不对, 那么 n 不是好数, 又 $p \nmid n$, 利用 Ex1, 存在正整数 α , 使得: $n^p \mid p^{(p^2-1) \cdot n - p^2} - 1$.

不妨设 $\delta = \text{ord}_{n^p}(p)$. 即 δ 为最小的正整数 (满足 $p^\delta \equiv 1 \pmod{n^p}$).

因此 $\delta \mid (p^2-1) \cdot n - p^2$. 又 $p \nmid n$, 即 $p \nmid (p^2-1) \cdot n - p^2$. 从而 $p \nmid \delta$.

与 $p \mid \delta$ 矛盾. #

Ex 13, 设 $n \geq 21$, 则开区间 $(n, 2n)$ 中至少有 5 个不同的素数.

分析:

(1) 先看例子.

$n=21, 22$: $23, 29, 31, 37, 41$;

$n=23, \dots, 28$: $29, 31, 37, 41, 43$;

$n=29, \dots, 36$: $37, 41, 43, 47, 53$;

$\vdots$

$n \leq 225$. 均可以举例子说明.

(2) 以下 $n \geq 225$, 则开区间 $(n, 2n)$ 中至少有 5 个不同的素数.

考虑:

$$M = C_{2n}^n = \frac{2n \cdot (2n-1) \cdots (n+1)}{n!}$$

不妨设 M 的标准分解式:

$$M = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}, \quad \text{其中 } 2 = p_1 < p_2 < \cdots < p_t < 2n.$$

其中 $\alpha_i \geq 1, i=1, 2, \dots, t$. 估计 α_i 的大小?

我們知道:

$$\begin{aligned} \alpha_i &= v_{p_i}(M) = v_{p_i}\left(\frac{(2n)!}{n! \cdot n!}\right) = v_{p_i}((2n)!) - 2v_{p_i}(n!) \\ &= \sum_{k=1}^{+\infty} \left(\left\lfloor \frac{2n}{p_i^k} \right\rfloor - 2 \left\lfloor \frac{n}{p_i^k} \right\rfloor \right) \end{aligned}$$

注意到 $p_i^\beta \leq 2n < p_i^{\beta+1}$, $\forall p_i$

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

例 1.2:
$$\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 0, & 0 \leq \{x\} < \frac{1}{2}; \\ 1, & \frac{1}{2} \leq \{x\} < 1. \end{cases}$$

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

$$\hat{M} = C_{2n}^n = \prod_{p \leq \sqrt{2n}} p^{\alpha} \cdot \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\alpha} \cdot \prod_{\frac{2n}{3} < p \leq n} p^{\alpha} \cdot \prod_{n < p < 2n} p^{\alpha}.$$

① $\prod_{p \leq \sqrt{2n}} p^{\alpha} \leq (2n)^{\pi(\sqrt{2n})}$, 其中 $\pi(x)$ 表示不大于 x 的素数的个数.

② 现在 $\sqrt{2n} < p \leq \frac{2n}{3}$, 则 $p \nmid p^2 > 2n$. 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 $n = [x]$. 只需证: $\prod_{p \leq n} p < 4^{n-1}$ 即可! 对 n , 用归纳法.

(i) $n=2$ 时, $\prod_{p \leq 2} p = 2 < 4^{2-1}$. $\checkmark$

(ii) 假设 $n \leq m$, 结论成立.

(iii) 对于 $n = m+1$ 的情况. 想证: $\prod_{p \leq m+1} p < 4^m$.

对 $m+1$ 分情况讨论:

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

② 若 $m+1=2k+1$, 则

$$\prod_{p \leq m+1} p = \prod_{p \leq 2k+1} p = \prod_{p \leq k+1} p \cdot \prod_{k+1 < p \leq 2k+1} p$$

$$< 4^k \cdot C_{2k+1}^{k+1} < 4^k \cdot 2^{2k} = 4^{2k}.$$

③ 现在 $\frac{2n}{3} < p \leq n$, 我们有

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

又由 $\hat{\sigma}_p$:

$$C_{2n}^n = \frac{2n \cdot (2n-1) \cdots (n+1)}{n!} \quad \text{且} \quad v_p(C_{2n}^n) = 0.$$

且

$$\prod_{\frac{2n}{3} < p \leq n} p^2 = 1. \quad \text{且}$$

$$M = C_{2n}^n = \prod_{p \leq \sqrt{2n}} p^2 \cdot \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^2 \cdot \prod_{n < p \leq 2n} p^2, \quad \#p \mid 2, 3.$$

$$C_{2n}^n < (2n)^{\pi(\sqrt{2n})} \cdot 4^{\frac{2n}{3}-1} \cdot P.$$

我们知道:

$$C_{2n}^0 + \dots + C_{2n}^n + \dots + C_{2n}^{2n} = 2^{2n}.$$

因此 $C_{2n}^n > \frac{2^{2n}}{2n}$ 代入②式.

$$\frac{2^{2n}}{2n} < (2n)^{\pi(\sqrt{2n})} \cdot 4^{\frac{2n}{3}-1} \cdot P. \quad (*)$$

证明: 在 $(n, 2n)$ 之间的数有 5 个不同的数, 即 $n \geq 225$.

反证法. 如果只有 4 个, 那么数只有 4 个. 因此

$$P \leq (2n-1)(2n-3)(2n-5)(2n-7) < (2n)^4. \quad \text{代入 } (*). \text{ 有}$$

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

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

令 $k = \lfloor \sqrt{2n} \rfloor$, 由于 $n \geq 225$, 所以 $k \geq 20$. 我们知道 $\pi(k)$ 表示 $1, 2, \dots, k$ 中的素数的个数.

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

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

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

$$4^{\frac{n}{3}} < 4^{\frac{n}{3}+1} < (2n)^{\pi(\sqrt{2n})+5} < (2n)^{\sqrt{\frac{n}{2}}-1+5} = (2n)^{\sqrt{\frac{n}{2}}+4}.$$

其中 $n \geq 225$.

由于 $n \geq 225$, 则有 $\sqrt{\frac{n}{2}} + 4 < \sqrt{n}$. 理由如下:

$$\sqrt{\frac{n}{2}} + 4 < \sqrt{n} \Leftrightarrow \frac{n}{2} + 16 + 8\sqrt{\frac{n}{2}} < n$$

$$\Leftrightarrow 16 + 8\sqrt{\frac{n}{2}} < \frac{n}{2}. \quad \text{令 } \sqrt{\frac{n}{2}} = x$$

$$\Leftrightarrow 16 + 8x < x^2$$

$$\text{则 } x \geq \sqrt{\frac{225}{2}} > 10.$$

$$\Leftrightarrow (x-4)^2 > 32$$

$$\Leftrightarrow x > 4 + \sqrt{32}. \quad \text{代回去, 我们有}$$

$$\left(4^{\frac{\sqrt{n}}{3}}\right)^{\sqrt{n}} = 4^{\frac{n}{3}} < (2n)^{\sqrt{n}}, \quad \text{其中 } n \geq 225.$$

$$\text{因此 } 4^{\frac{\sqrt{n}}{3}} < 2n. \quad \text{其中 } n \geq 225.$$

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

我们已知: $4^l < 2n$. 从而 $2^l < \sqrt{2n} < \sqrt{2} \cdot 3 \cdot (l+1) < 5 \cdot (l+1)$.

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

但是 $2^l < 5 \cdot (l+1) \Rightarrow l < 5$. 矛盾. #

Ex 14. 设 n, a 均为正整数, 满足条件: $a^n \equiv 1 \pmod{n}$. 因此,

$a^1+1, a^2+2, a^3+3, \dots, a^n+n$
模 n 余数两两不同.

分析:

(1) $a=1$ 时, 结论成立.

(2) $n=1$ 时, 结论也成立.

(3) 以下 a, n 均为大于1的正数且 $a^n \equiv 1 \pmod{n}$. 想证:

$a^1+1, a^2+2, a^3+3, \dots, a^n+n$
构成模 n 的一个完全剩余系.

反证法, 如果不对, 那么存在 $1 \leq i < j \leq n$, 使得

$$a^i+i \equiv a^j+j \pmod{n}. \quad (*)$$

可以要求 n 是最小的.

由于 $a^n \equiv 1 \pmod{n}$, 所以 $(a, n)=1$. 不妨设 $\text{ord}_n(a)=d$. 则 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 $n>1$, 所以
 $1 \leq d \leq \varphi(n) < n$.

显然, $d \neq 1$. 否则 $a \equiv 1 \pmod{n}$, 所以

$$a^i + i \equiv 1 + i \pmod{n}, \quad i=1, 2, \dots, n$$

从而 $a^i + i, i=1, \dots, n$ 构成模 n 的完全系, 矛盾.

$$\text{从而 } 1 \leq d < n, \quad d | n$$

由 $a^d \equiv 1 \pmod{n}$, 得 $\underline{a^d \equiv 1 \pmod{d}}$. 从而 n 的倍数.

已知: $a^1 + 1, a^2 + 2, \dots, a^d + d$ 模 d 两两同余.

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

不妨设 $i = d \cdot q_1 + r_1, \quad j = d \cdot q_2 + r_2$. 其中 $1 \leq r_1, r_2 \leq d$.

$$\text{代入, 有 } a^{r_1} + r_1 \equiv a^{r_2} + r_2 \pmod{d}.$$

因此 $r_1 = r_2 = r$ 代入 (*), 有

$$\text{L2.7} \quad a^{d q_1 + r} + i \equiv a^{d q_2 + r} + j \pmod{n}.$$

又 $a^d \equiv 1 \pmod{n}$, 则上式可化为

$$a^r + i \equiv a^r + j \pmod{n}$$

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

Ex 15. 设正整数数列 $\{a_n\}_{n=0}^{\infty}$ 满足条件: $(a_{i+1}, a_i) > a_{i-1}$, $\forall i \geq 1$,

证明: 对 $\forall n \geq 0$, 均有 $a_n \geq 2^n$.

分析:

(1) 回忆: 若 $d|a, d|b$, 则 $d|(a, b)$.

(ii) 若 $a|m, b|m$, 则 $[a, b]|m$.

(2) 回到原问题:

$$\wedge_i \quad \underbrace{\frac{a_{i+1}}{a_i}} = \frac{x_i}{y_i}, \text{ 其中 } x_i, y_i \in \mathbb{Z}_{\geq 1}, \text{ 且 } (x_i, y_i) = 1.$$

$$\text{因此 } y_i | a_i, x_i | a_{i+1}.$$

从而

$$a_{i-1} < (a_i, a_{i+1}) = (a_i, \frac{x_i}{y_i} \cdot a_i) = \frac{a_i}{y_i} \cdot (y_i, x_i) = \frac{a_i}{y_i}.$$

$$\text{因此 } \frac{a_i}{a_{i-1}} > y_i, \quad \forall i \geq 1.$$

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

$$(\#) \text{ 也, } \frac{x_{i-1}}{y_{i-1}} \geq y_i + \frac{1}{y_{i-1}} \geq 2 \sqrt{y_i \cdot \frac{1}{y_{i-1}}} = 2 \sqrt{\frac{y_i}{y_{i-1}}}, \quad \forall i \geq 1.$$

$$\text{又 } \frac{a_1}{a_0} = \frac{x_0}{y_0}, \quad y_0 | a_0. \text{ 由 } \# \text{ 得 } a_0 \geq y_0.$$

$$\text{归纳得: } a_n \geq 2^n, \quad \forall n \geq 0.$$

我們知道:

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

$$= \frac{x_{n-1}}{y_{n-1}} \cdot \frac{x_{n-2}}{y_{n-2}} \cdots \frac{x_0}{y_0} \cdot a_0$$

$$\geq 2 \sqrt{\frac{y_n}{y_{n-1}}} \cdot 2 \sqrt{\frac{y_{n-1}}{y_{n-2}}} \cdots 2 \sqrt{\frac{y_1}{y_0}} \cdot y_0$$

$$= 2^n \cdot \sqrt{y_n y_0} \geq 2^n. \quad \#$$

Ex 16. 设 n 为正整数, A_n 表示 $\sigma(n)$ 的所有不同的素因子构成的集合.

这里 $\sigma(n)$ 表示 n 的所有不同的正因子之和. B_n 表示 n 的所有不同的素因子构成的集合. 证明: 对任意的正整数 k , 一定存在正整数 m , 使得:

$$|A_m \setminus B_m| = k.$$

分析:

(1) $\sigma(n)$ 的性质.

(i) $\sigma(1) = 1$.

(ii) $\sigma(p^2) = 1 + p + p^2 + \dots + p^2 = \frac{p^{2+1} - 1}{p - 1}$.

(iii) 一般的 $n > 1$, 不妨设

$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$
为标准分解式, 那么

“积性函数”

$$\sigma(n) = \sigma(p_1^{\alpha_1}) \cdot \sigma(p_2^{\alpha_2}) \dots \sigma(p_t^{\alpha_t})$$

$$= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_t^{\alpha_t+1} - 1}{p_t - 1}$$

(100) 若 $(m, n) = 1$, 则 $\sigma(mn) = \sigma(m) \cdot \sigma(n)$. #

(2) 回到问题: 现在 k 为正整数, 想问: 存在正整数 n 使得

$$|A_n \setminus B_n| = k.$$

(i) 一定存在正整数 m , 使得 $2^m - 1$ 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. 则 $p_i \mid 2^m - 1, \forall i = 1, \dots, k$. #

$$\triangleq \quad \underbrace{n_0 = 2^m - 1}, \quad \text{则} \quad \sigma(n_0) = 2^m - 1 = p_{i_1}^{a_1} \cdots p_{i_t}^{a_t}, \quad i_1 < \cdots < i_t$$

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

这里 p_j 表示第 j 个奇素数, 按照大小顺序.

因此, $t \geq k$.

(ii) 如果 $t = k$, 那么 $|A_{n_0} \setminus B_{n_0}| = k$.

(iii) 如果 $t > k$, 不妨设 $t - k = r$, 其中 r 为已素数.

$\triangleq$

$$n_1 = n_0 \cdot p_1 p_2 \cdots p_{i_r-1} \cdot \underbrace{p_{i_r}}_m = 2^{m-1} \cdot p_1 p_2 \cdots p_{i_r}$$

$$(\dagger) \leadsto \sigma(n_1) = (2^m - 1) \cdot (p_1 + 1)(p_2 + 1) \cdots (p_{i_r} + 1).$$

$$= p_{i_1}^{d_1} \cdots p_{i_t}^{d_t} \cdot (p_1 + 1)(p_2 + 1) \cdots (p_{i_r} + 1).$$

$$\hookrightarrow \text{此时 } B_{n_1} = \{2, p_1, \dots, p_{i_r}\}, \quad |B_{n_1}| = 1 + i_r.$$

(\dagger) \leadsto A_{n_1} \setminus B_{n_1} 表示 A_{n_1} 中大于 p_{i_r} 的 素数 构成的集合 非空

$$\hookrightarrow A_{n_1} \setminus B_{n_1} = \{p_{i_r+1}, \dots, p_{i_t}\}$$

$$(\dagger) \leadsto |A_{n_1} \setminus B_{n_1}| = t - r = k. \quad \#$$

Ex 17. 设 a, b 均为大于1的正整数, c 是正整数, 证明: 存在无穷多正整数 k , 使得:

$$\left[\frac{a^k}{k} \right] \equiv c \pmod{b}.$$

分析:

(1) 来证: 设 a 为大于1的正整数, 证明: 存在无穷多正整数 k , 使得 $\left[\frac{a^k}{k} \right]$ 为奇数.

(2) 回到原题:

分析: 取 $k = t \cdot a^x$, 其中 t, x 待定. 则

$$\left[\frac{a^k}{k} \right] = \left[\frac{a^{t \cdot a^x}}{t \cdot a^x} \right] = \left[\frac{a^{\overbrace{t \cdot a^x}^x}}{t} \right] = \left[\frac{a^{t \cdot a^x - x} - a^x + a^x}{t} \right]$$

$$= \left[\frac{a^e \cdot (a^{t \cdot a^x - x - e} - 1)}{t} + \frac{a^e}{t} \right]$$

可以要求 $(t, a) = 1$. 如果 $g(tb) \mid t \cdot a^x - x - e$, 即,

$$tb \mid (a^{t \cdot a^x - x - e} - 1) \cdot a^e, \quad \text{再要求 } \left[\frac{a^e}{t} \right] = c. \quad \#$$

由于 a, c 均为正整数, 即, 取一个充分大的正整数 e , 使得

并证 $\left(\frac{a^e}{c+1}, \frac{a^e}{c} \right)$ 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 $k = t \cdot a^x$, 其中 x 待定. 因此

$$\frac{a^k}{k} = \frac{a^{t \cdot ax}}{t \cdot a^x} = \frac{a^{t \cdot a^x - x}}{t}.$$

取 k_0 : $t \cdot a^x - x \equiv e \pmod{\varphi(tb)}$ 有无穷正整数解.

取一个充分大的正整数 $x = x_0$, 因此 $k = t \cdot a^{x_0}$, 则

$$t \cdot a^{x_0} - x_0 \equiv e \pmod{\varphi(tb)}.$$

因此, $tb \mid a^{t \cdot a^{x_0} - x_0} - a^e$. (思考)??

$$\text{从而 } \left\lfloor \frac{a^k}{k} \right\rfloor = \left\lfloor \frac{a^{t \cdot a^{x_0} - x_0}}{t} \right\rfloor = \frac{a^{t \cdot a^{x_0} - x_0} - a^e}{t} + \left\lfloor \frac{a^e}{t} \right\rfloor$$

$$\equiv \left\lfloor \frac{a^e}{t} \right\rfloor \pmod{b}.$$

$$\text{又 } \frac{a^e}{c+1} < t < \frac{a^e}{c}, \quad \text{即 } c < \frac{a^e}{t} < c+1. \quad \text{因此}$$

$$\left\lfloor \frac{a^e}{t} \right\rfloor = c. \quad \text{从而 } \left\lfloor \frac{a^k}{k} \right\rfloor \equiv c \pmod{b}. \quad \#$$

Ex 18. 设 a, b 均是正整数, 证明: 仅当 $\left(\frac{b^2}{a^2+ab}, \frac{b^2}{a^2+ab-1} \right) \perp$
不存在正整数.

分析: 反证法, 如果结论不对, 那么存在正整数 m , 使得

$$\frac{b^2}{a^2+ab} \leq m < \frac{b^2}{a^2+ab-1}.$$

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

从而

$$b^2 = ma^2 + mab - r, \text{ 其中 } 0 \leq r < m.$$

可以要求 $a+b$ 是最小的。

显然, $b > a$, 而且

$$b^2 - ma \cdot b - (ma^2 - r) = 0.$$

换句话说, $x=b$ 为方程

$$x^2 - ma \cdot x - (ma^2 - r) = 0$$

的一个根。因此

$$\Delta = (ma)^2 + 4(ma^2 - r) \text{ 为平方数.}$$

观察:

$$\Delta = (ma)^2 + 4ma^2 - 4r$$

$$= a^2 \cdot (m^2 + 4m) - 4r$$

$$= \underline{(a(m+2))^2} - 4(r + a^2)$$

$$= (a(m+2)^2 - t)^2, \text{ 其中 } t \in \mathbb{Z}_{>0} \text{ 待定.}$$

我們知道: $2|t$. 不妨設 $t=2k$, 其中 $k \in \mathbb{Z}_{\geq 1}$.

$$\text{如果 } 2a \leq 2k \leq 2a(m+2), \text{ 即 } a \leq k \leq a(m+2)$$

$$(a(m+2) - t)^2 \leq (am)^2.$$

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

$$\text{故 } \Delta > (am)^2. \text{ 因此 } 0 < k < a.$$

$$\text{因此 } \Delta \text{ 为平方数} \Leftrightarrow (a(m+2))^2 - 4(r+a^2) = (a(m+2) - 2k)^2.$$

$$\Leftrightarrow 4(r+a^2) = 4ka(m+2) - 4k^2$$

$$\Leftrightarrow r+a^2 = ka(m+2) - k^2$$

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

② $a-k=l$, 则 $l \in \mathbb{Z}_1$. 而且

$$l^2 + r - (l+k)km = 0.$$

③

$$l^2 - km \cdot l - (k^2m - r) = 0$$

④ 此时 $k+l=a < a+b$. $\frac{3}{4}$ 有.