初等数论

（二）

教育

Ex7. 证明：对于无穷多正整数 n，使得

$$2^n = 2024\cdots\cdots \qquad (*)$$

分析：我们知道，$(*)$ 改写为

$$2024\times 10^m < 2^n < 2025\times 10^m.$$

即 $$\lg 2024 + m < n\lg 2 < \lg 2025 + m.$$

即 $$\lg 2024 < n\lg 2 - m < \lg 2025. \qquad (**)$$

取 $\alpha = \lg 2$，$\beta = \dfrac{\lg 2025 + \lg 2024}{2}$. 则 $(**)$ 改写为

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

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

利用 Kronecker 定理. 存在无穷多数对 (x, y), 使得

$$|\alpha x - y - \beta| < \frac{1}{x} < \frac{\lg 2025 - \lg 2024}{2}.$$

取 $n = x$, $m = y$ 即可. #

Ex8. 设 α 为正无理数, 令 a_n 表示 $[\alpha n]$ 的个位数, $n = 1, 2, \cdots$.

再令 $$\beta = 0.a_1 a_2 a_3 \cdots\cdots$$

证明: β 为无理数.

分析: 反证法, 如果 β 不是无理数, 那么 β 为有理数. 因此, 存在

正整数 n_0, T，对 $\forall n \geq n_0$，均有

$$a_{n+T} = a_n.$$

因此 $[\alpha(n+T)] \equiv [\alpha n] \pmod{10}, \forall n \geq n_0$

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

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

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

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. #

Ex9. 设 a 为正整数, 证明: 方程 $n! = a^b - a^c$ 只有有限组正整数解 (n, b, c).

分析：

(1) 升幂定理. 设 p 为奇素数，$p \mid a-1$，$a>1$，$n \geq 1$，则

$$v_p(a^n-1) = v_p(a-1) + v_p(n).$$

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：$a=1$，无解. 以下 $a>1$，考虑方程

$$n! = a^b - a^c.$$

不妨设 (n,b,c) 是它的一组正整数解. 想证：n, b, c 均有界.

设 p 为大于 a 的奇素数，则 $(p, a)=1$. 又有

$$n! = a^c \cdot (a^{b-c} - 1).$$

因此 $$v_p(n!) = v_p(a^{b-c} - 1).$$

由于 $$v_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k}\right] \geq \left[\frac{n}{p}\right] > \frac{n}{p} - 1.$$

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

$$= v_p(a^{p-1} - 1) + v_p(b-c), \quad \text{由} p \nmid b$$

$$\frac{n}{p} - 1 < v_p(a^{p-1} - 1) + v_p(b-c). \quad \text{又} \because v_p(a^{p-1} - 1) = \alpha.$$

因此 $$v_p(b-c) > \frac{n}{p} - 1 - \alpha.$$ 从而

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

$n\log_a^n > p^{\frac{n}{p}-1-\alpha}$

从而 $\log_p^{n\log_a^n} > \frac{n}{p}-1-\alpha$. 因此 n 有界，从而 n 的个数有限.

又 $b-c < \log_a^{n!}$，$c < \log_a^{n!}$，从而 b, c 也为有限个！ #

Ex10. 求所有的三元正整数组 (p, x, y)，满足条件：

p 为奇素数，且 $x^{p-1}+y$ 和 $x+y^{p-1}$ 都是 p 的幂.

分析：不妨设

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

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

其次, $p\nmid xy$. 理由: 由于 $x^{p-1}+y=p^{\alpha}$, 则 $v_p(x^{p-1})=v_p(y)$.

即 $(p-1)v_p(x)=v_p(y)$. 又 $x+y^{p-1}=p^{\beta}$. 则 $v_p(x)=v_p(y^{p-1})$, 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 $$\begin{cases} x^{p-1}+y=p^{\alpha}, \\ x+y^{p-1}=p^{\beta}. \end{cases}$$ $x\geq y\geq 1$, $\alpha\geq\beta\geq 1$, $p\nmid xy$.

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, $p \nmid xy$, $x \neq \pm y$, $p \mid x \mp y$. $n \geq 1$, 则

$$v_p(x^n \mp y^n) = v_p(x \mp y) + v_p(n).$$

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

$$= x \cdot (x^{p-1} + y) - y \cdot (y^{p-1} + x) = \underline{x \cdot p^\alpha - y \cdot p^\beta}.$$

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

又 $v_p(xp^\alpha - yp^\beta) = \beta$. 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

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

我们有: $k \cdot p^{\beta-1} + y + y^{p-1} = p^\beta$. (*)

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

从而 $y \mid p-k$, 又 $p \mid y+1$. 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 $1 + (p-1)^{p-2} = p^{\beta-1}$.

$1+(p-1)^{p-2} = p^1 \Rightarrow p=3$.

我们知道:

$$\beta-1 = v_p(p^{\beta-1}) = v_p\left(1+(p-1)^{p-2}\right) = v_p(1+(p-1)) + v_p(p-2) = 1.$$

从而 $\beta=2$.

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 $(3,2,5)$. #

Ex11. 求所有的正整数 n，满足条件：存在正整数 a,b，使得

$$(a+n)(b+n)\mid a^2+b^2.$$

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 $a_1,\dots,a_k$，使得

$$(a_1+n)\cdots(a_k+n)\mid a_1^2+\dots+a_k^2.$$

分析：

(1) $n=1$，不符合条件。理由如下：反证法，如果结论对，那么 $n=1$ 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 $a^2+b^2=(a+1)(b+1)\cdot k$，其中 k 为正整数.

下面要构造矛盾.

构造集合:

$$S_k=\{(u,v)\mid u,v\text{ 均为正整数且 }u^2+v^2=(u+1)(v+1)k\}.$$

因此，$S_k\neq\varnothing$. 理由: $(a,b)\in S_k$.

若 $(u,v)\in S_k$，则 $(v,u)\in S_k$. 而且 $u\neq v$. 否则，若 $u=v$，则

$$2u^2=(u+1)^2\cdot k$$

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 $(u,v)\in S_k$，$u>v\geq 1$，而且 $u+v$ 是最小的.

由于 $(u,v)\in S_k$，那么 $u^2+v^2=(u+1)(v+1)\cdot k$. 因此，

$$u^2-(v+1)k\cdot u+v^2-(v+1)k=0.$$

从而 $x=u$ 为方程

$$x^2-(v+1)k\cdot x+v^2-(v+1)k=0$$

的一个根. 从而有另一个根 $x=w$. 因此，

$$\begin{cases} u+w=(v+1)\cdot k \\ u\cdot w=v^2-(v+1)k. \end{cases}$$

从而 $w\in\mathbb{Z}$，且 $w<v$.

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

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

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

② 如果 $w\geq 1$，那么 $(w,v)\in S_k$，且 $w+v<u+v$，$S(u,v)$ 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

$$(a+n)(b+n)\mid a^2+b^2. \qquad (*)$$

下面构造 (a,b).

我们知道：

$$(*)\iff b+n\mid a^2+b^2,\ \text{且}\ a+n\mid \frac{a^2+b^2}{b+n}.$$

观察：$b+n\mid a^2+b^2=a^2+n^2+b^2-n^2$. 即 $b+n\mid a^2+n^2$.

要求 $b+n=a^2+n^2$. 则 $b=a^2+n^2-n$.

再观察：

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

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

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

$$= \underline{a^2-n^2} + 2n^2-2n+1.$$

因为 $a+n \mid 2n^2-2n+1$. 要求 $a+n = 2n^2-2n+1$.

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

#

Ex12. 证明：n为好数当且仅当 $p+n$，且 p 模 n^p 的阶能被 p 整除.

分析：

(1) 元素的阶.

(i) Euler Th. 设 m 为正整数，$(a,m)=1$，则

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

(ii) 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 $t = \mathrm{ord}_m(a)$.

(iii) 若 $\mathrm{ord}_m(a) = t$，且 $a^r \equiv 1 \pmod{m}$，则 $t \mid r$.

特别，有 $t \mid g(m)$.

(2) 回到原题：对正整数 n，分情况讨论：

(i) 如果 $p \mid n$，那么 n 不是好数. 理由：构造一个正整数 $m \neq n$，使得：

$$\left\{\frac{p^m}{m^p}\right\} = \left\{\frac{p^n}{n^p}\right\} \qquad (*)$$

由于 $p \mid n$，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 $\beta \geq 1$，待定，要求 $(*)$ 成立. 代回去

有 $$\left\{\frac{p^{m-p^\beta}}{n^p}\right\} = \left\{\frac{p^n}{n^p}\right\}.$$

用心 $n^p \mid p^{m-p\beta} - p^n = p^n \cdot (p^{m-n-p\beta} - 1)$ (**)

由于 $n^p = (p^\alpha n_1)^p = p^{p\alpha} \cdot n_1^p$. 显然 $p^{p\alpha} \mid p^n$. $p\alpha \le n$.

从而 (**) 可写为:

$$n_1^p \mid p^{m-n-p\beta} - 1 = p^{p\beta \cdot n - n - p\beta} - 1 = p^{n(a^x - x - 1)} - 1.$$

要求 $\beta = p^{\alpha-1} \cdot n_1 x$, 其中 x 待定. 代回去, 有

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

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

利用第3题，知存在无穷多正整数 x，使得

$$a^x - x \equiv 1 \pmod{\varphi(n_1^p)}.$$

取一个正整数解 x_0，则

$$\varphi(n_1^p) \mid a^{x_0} - x_0 - 1 = p^{p^{\alpha-1} \cdot n_1 \cdot x_0} - x_0 - 1.$$

利用 Euler Th. 有

$$n_1^p \mid p^{a^{x_0} - x_0 - 1} - 1, \text{ 从而 } n_1^p \mid p^{n(a^{x_0} - x_0 - 1)} - 1.$$

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

因此 n 不是如数.