信安数基第一次作业—冯尔宁—2022302181149

13. 证明：设形如 $4k+3$ 的素数有有穷多个，这些素数为 $P_1, P_2 \cdots P_n$，
现考虑：$N = 4(P_1 \cdot P_2 \cdots P_n) - 1$ 显然 N 除以 4 余数为 3，
因而它必然也是 $4k+3$ 的数。由于 $P_1, P_2 \cdots P_n$ 均为形如 $4k+3$ 的数，故它们的乘积也必然可表示为形如 $4k+3$ 的数。
则 N 可表示为 $N = (4k+3)M + R$，其中 M 为一个整数，R 为 N 除以形如 $4k+3$ 的素数的乘积后的余数。又 N 除以形如 $4k+3$ 后的素数的乘积后余数也为 3，故 $N = (4k+3)M + 3$
所以 N 不能被任何形如 $4k+3$ 的素数整除，则 N 也为素数，
又 $N > P_i \ (i = 1, 2, \cdots n)$，故假设不成立，则形如 $4k+3$ 的素数有无穷多个。

17. $(111100011110101)_2$ = 0X78F5

$(10111101001110)_2$ = 0X2F4E

18. $(ABCDEFA)_{16} = (1010\ 1011\ 1100\ 1101\ 1110\ 1111\ 1010)_2$

$(DEFACEDA)_{16} = (1101\ 1110\ 1111\ 1010\ 1100\ 1110\ 1101\ 1010)_2$

$(9A0AB)_{16} = (1001\ 1010\ 0000\ 1010\ 1011)_2$

28. $(20785, 44350) = 5$

$44350 = 2 \times 20785 + 2780$.

$20785 = 7 \times 2780 + 1325$.

$2780 = 2 \times 1325 + 130$

$1325 = 10 \times 130 + 25$.

$130 = 5 \times 25 + 5$.

$25 = 5 \times 5 + 0$.

32. ① $(1613, 3589) = 1$

$3589 = 2\times1613 + 363$
$1613 = 4\times363 + 161$
$363 = 2\times161 + 41$
$161 = 3\times41 + 38$
$41 = 1\times38 + 3$
$38 = 12\times3 + 2$
$3 = 2\times1 + 1$
$1 = 1\times1 + 0$

$1 = 3 - 2\times1$
$= 3 - (38 - 12\times3) = 13\times3 - 38$
$= 13\times(41 - 38) - 38$
$\vdots$
$= 13\times41 - 14\times38$
$= 13\times41 - 14\times(161 - 3\times41)$
$= 13\times41 - 161\times14 + 42\times41$
$= 55\times41 - 161\times14$
$= 55\times(363 - 2\times161) - 161\times14$
$= 55\times363 - 124\times161$
$= 55\times363 - 124\times(1613 - 4\times363)$
$= (55 + 496)\times363 - 124\times1613$
$= 551\times363 - 124\times1613$
$= 551\times(3589 - 2\times1613) - 124\times1613$
$= 551\times3589 - 1226\times1613$

则 $s = -1226$, $t = 551$

② $(2947, 3772) = 1$

$3772 = 1\times2947 + 825$
$2947 = 825\times3 + 472$
$825 = 472 + 353$
$472 = 353 + 119$
$353 = 2\times119 + 115$
$119 = 115 + 4$
$115 = 28\times4 + 3$
$4 = 3 + 1$
$1 = 1 + 0$

$1 = 4 - 3 = 4 - (115 - 28\times4) = 29\times4 - 115$
$= 29\times(119 - 115) - 115 = 29\times119 - 30\times115$
$= 29\times119 - 30\times(353 - 2\times119)$
$= 89\times119 - 30\times353 = 89\times(472 - 353) - 30\times353$
$= 89\times472 - 119\times353 = 89\times472 - 119\times(825 - 472)$
$= 208\times472 - 119\times825 = 208\times(2947 - 3\times825) - 119\times825$
$= 208\times2947 - 743\times825$
$= 208\times2947 - 743\times(3772 - 2947)$
$= 951\times2947 - 743\times3772$

则 $s = 951$, $t = -743$

50. ④ $[132, 253] = \cancel{3036} \frac{132\times 253}{(132,253)} = \frac{132\times 253}{11} = 3036$

$(132, 253) = 11$

$253 = 132 + 121$

$132 = 121 + 11$

$121 = 11\times 11 + 0.$

54.

前5个 Mersenne 素数 2、3、5、7、13.

信安数基第2次作业 - 冯尔宁 - 2022302181149

(2) 证明：∵ $m-1 \equiv -1 \pmod m$

∴ $(m-1)^2 \equiv (-1)^2 \equiv 1 \pmod m$

则 $0^2, 1^2, \cdots (m-1)^2$ 一定不是模m的完全剩余系

(6)

∵ $2^3 = 8 \equiv 1 \pmod 7$

$20030509 = 6676836 \times 3 + 1$

∴ $2^{20030509} = (2^3)^{6676836} \cdot 2 \equiv 2 \pmod 7$

故 $2^{20030509}$ 天是星期日

(13) ∵ $a^2 \equiv b^2 \pmod n$

∴ $n \mid a^2 - b^2$

即 $n \mid (a-b)(a+b)$ 又 $n \nmid a-b$, $n \nmid a+b$

又 $n = pq$, 则 $pq \mid (a-b)(a+b)$，又 p, q 均为素数

则 $p \mid (a-b)$, 或 $p \mid (a+b)$ 故有 $(n, a-b) = (pq, a-b) > 1$

同理有 $q \mid (a-b)$ 或 $q \mid (a+b)$ 以及 $(n, a+b) = (pq, a+b) > 1$

(24) $3^{1000000} \pmod 7$

由欧拉定理：$3^{\varphi(7)} \equiv 3^6 \equiv 1 \pmod 7$

故 $3^{1000000} = (3^6)^{166666} \cdot 3^4 \equiv 81 \equiv 4 \pmod 7$

(25) $137^{113} \pmod{227}$

$113 = (1110001)_2$ $a = 1$, $b = 137$, $m = 227$

$n_0 = 1$ $a_0 = a \times b \equiv 137$, $b_1 = b^2 \equiv 155$, mod 227

$n_1 = 0$ $a_1 = 137$, $b_2 = b_1^2 \equiv 190$, mod 227

$n_2 = 0$ $a_2 = 137$, $b_3 = b_2^2 \equiv 7$ mod 227

$n_3 = 0$, $a_3 = 137$, $b_4 = b_3^2 \equiv 49$, mod 227

$n_4 = 1$, $a_4 = 130$, $b_5 = 131$, mod 227

$n_5 = 1$, $a_5 = 5$, $b_6 = 136$, mod 227

$n_6 = 1$, $a_6 = 226$.

故原式 = 226 mod 227

武漢大學
WUHAN UNIVERSITY
Wuhan 430072, Hubei, P.R. China 中国·武汉 Tel.(027)

信安数基 第3次作业 —冯尔宁—2022302181169

1. $17x \equiv 14 \pmod{21}$

$\because (17, 21) = 1$，先计算 $17x \equiv 1 \pmod{21}$，利用广义欧几里得除法，

$21 = 17 \times 1 + 4$ 解得一个特解 $x_0 \equiv 5 \pmod{21}$

$17 = 4 \times 4 + 1$

$1 = 17 - 4\times 4 = 17 - 4\times(21-17) = 5\times 17 - 4\times 21$

则原方程有一个特解 $x_0' = 14 x_0 \pmod{21} = 14\times 5 \pmod{21} \equiv 7 \pmod{21}$

则原方程的所有解为 $x = 7 + 21t \pmod{21}$，当 $t=0$ 时，解为 $x=7$

10. 证明：同余方程组 $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$ 有解当且仅当 $(m_1, m_2) \mid (a_1 - a_2)$

并证明若有解，该解模 $([m_1, m_2])$ 是唯一的。

证明：(1) 设 $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$ 有解，故 $\begin{cases} x = a_1 + s m_1 & ① \\ x = a_2 + t m_2 & ② \end{cases}$

①-② 有 $a_1 - a_2 + s m_1 - t m_2 = 0$ 故有 $s m_1 - t m_2 = a_2 - a_1$ ③

由贝祖公式的判定条件，若上述方程有解，则有 $(m_1, m_2) \mid (a_1 - a_2)$

(2) 由③ $\dfrac{s m_1}{(m_1, m_2)} - \dfrac{t m_2}{(m_1, m_2)} = \dfrac{a_2 - a_1}{(m_1, m_2)}$ ④ 可化简为

此时 $\left(\dfrac{m_1}{(m_1, m_2)}, \dfrac{m_2}{(m_1, m_2)}\right)$ 互素 $s' \dfrac{m_1}{(m_1, m_2)} - t' \dfrac{m_2}{(m_1, m_2)} = 1$ ⑤

解上述二元一次不定方程 可得到一组特解为 $\begin{cases} s = s_0 \\ t = t_0 \end{cases}$

从而该方程有一组通解 $\begin{cases} s = s_0 + k \dfrac{m_2}{(m_1, m_2)} \\ t = t_0 + k \dfrac{m_1}{(m_1, m_2)} \end{cases}$ 将通解代入①②有 $\begin{cases} x = a_1 + s_0 m_1 + k\dfrac{m_1 m_2}{(m_1, m_2)} = a_1 + s_0 m_1 + k[m_1, m_2] \\ x = a_2 + t_0 m_2 + k\dfrac{m_1 m_2}{(m_1, m_2)} = a_2 + \ldots \end{cases}$

则该解模 $[m_1, m_2]$ 是唯一

1705546

13.(ii) $23x \equiv 1 \pmod{140}$;

原式可转化为同余方程组 $\begin{cases} 23x \equiv 1 \pmod 4 \\ 23x \equiv 1 \pmod 5 \\ 23x \equiv 1 \pmod 7 \end{cases}$ 采用中国剩余定理

$m = 4\times5\times7 = 140$.

$M_1 = 5\times7 = 35$, $M_2 = 4\times7 = 28$, $M_3 = 4\times5 = 20$.

又 $M_i' \cdot M_i \equiv 1 \pmod{m_i}$ 解得 $\begin{cases} M_1' \equiv 3 \pmod 4 \\ M_2' = 2 \pmod 5 \\ M_3' = 6 \pmod 7 \end{cases}$

$\therefore \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$

则 $x \equiv 3\times35\times3 + 2\times28\times2 + 4\times20\times6 = 67 \pmod{140}$

(iii) $17x \equiv 229 \pmod{1540}$

原式可转化为同余式组 $\begin{cases} 17x \equiv 4 \pmod 5 \\ 17x \equiv 1 \pmod 4 \\ 17x \equiv 5 \pmod 7 \\ 17x \equiv 9 \pmod{11} \end{cases}$

$M_1 = 4\times7\times11 = 308$

$M_2 = 5\times7\times11 = 385$

$M_3 = 5\times4\times11 = 220$

$M_4 = 5\times4\times7 = 140$.

$M_1' = 2 \pmod 5$

$M_2' = 1 \pmod 4$

$M_3' \equiv 5 \pmod 7$

$M_4' = 7 \pmod{11}$

$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4 \\ x \equiv 4 \pmod 7 \\ x \equiv 7 \pmod{11} \end{cases}$ 由中国剩余定理

$x \equiv 2\times308\times2 + 1\times385\times1 + 4\times220\times5 + 7\times140\times7$

$\equiv 557 \pmod{1540}$

23. $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod 7$

原式可化为 $r(x) = x^6 + 2x^5 + 2x^3 + 15x^2 + 5x \equiv 0 \pmod 7$

$$
\begin{array}{r|l}
 & 3x^7 + 4x^6 + 2x^4 + x^2 + 3x + 4 \\
x^7 - x & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\
 & 3x^{14} - 3x^8 \\
\hline
 & 4x^{13} + 2x^{11} + x^9 + 3x^8 + x^6 \\
 & 4x^{13} - 4x^7 \\
\hline
 & 2x^{11} + x^9 + 3x^8 + 4x^7 + x^6 \\
 & 2x^{11} - 2x^5 \\
\hline
 & x^9 + 3x^8 + 4x^7 + x^6 + 2x^5 \\
 & x^9 - x^3 \\
\hline
 & 3x^8 + 4x^7 + x^6 + 2x^5 + 2x^3 \\
 & 3x^8 - 3x^2 \\
\hline
 & 4x^7 + x^6 + 2x^5 + 2x^3 + 15x^2 + 4x
\end{array}
$$

$r(0) = 0 \pmod 7$

$r(1) = 4 \pmod 7$

$r(2) = 4 \pmod 7$

$r(3) = 5 \pmod 7$

$r(4) = 1 \pmod 7$

$r(5) = 6 \pmod 7$

$r(6) = 0 \pmod 7$

故同余式的解为 $x \equiv 0, 6 \pmod 7$

24. $f(x) \equiv x^4 + 7x + 4 \equiv 0 \pmod{243}$

$f'(x) = 4x^3 + 7 \pmod{243}$

直接验算 $f(x) \equiv 0 \pmod 3$ 有一解 $x_1 \equiv 1 \pmod 3$

以 $x = 1 + 3t_1$ 代入 $f(x) \equiv 0 \pmod 9$ 可得

$f(1) + 3t_1 f'(1) \equiv 0 \pmod 9$

$\because f(1) \equiv 3 \pmod 9$, $f'(1) \equiv 2 \pmod 9$

故上述同余式可写成 $3 + 3t_1 \cdot 2 \equiv 0 \pmod 9$

即 $2t_1 \equiv -1 \pmod 3$　$t_1 = 1 \pmod 3$

故 $f(x) \equiv 0 \pmod 9$ 解为 $x_2 \equiv 1 + 3t_1 = 4 \pmod 9$

再以 $x = 4 + 9t_2$ 代入 $f(x) \equiv 0 \pmod{27}$ 得

$f(4) + 9t_2 f'(4) \equiv 0 \pmod{27}$

$f(4) \equiv 18 \pmod{27}$　$f'(4) \equiv 20 \pmod{27}$

故上述同余式可写成 $18 + 9t_2 \cdot 20 \equiv 0 \pmod{27}$

即 $20t_2 \equiv -2 \pmod 3$

$t_2 = 2 \pmod 3$

同余式 $f(x) \equiv 0 \pmod{27}$ 解为 $x_3 = 4 + 9t_2 \equiv 22 \pmod{27}$

再以 $x = 22 + 27t_3$ 代入 $f(x) \equiv 0 \pmod{81}$ 得

$f(22) + 27t_3 f'(22) \equiv 0 \pmod{81}$

$f(22) \equiv 0 \pmod{81}$, $f'(22) \equiv 74 \pmod{81}$

即 $27 \times t_3 \times 74 \equiv 0 \pmod{81}$

$74t_3 \equiv 0 \pmod 3$

$t_3 = 0 \pmod 3$　$x_4 = 22 \pmod{81}$

再以 $x = 22 + 81t_4$ 代入 $f(x) \equiv 0 \pmod{243}$

$f(22) = 162 \pmod{243}$　$f'(22) = 74 \pmod{243}$

即 $\cancel{4 + 3t_4 \cdot 7 \equiv 0 \pmod{243}}$　$162 + 81t_4 \times 74 \equiv 0 \pmod{243}$

即 $\cancel{2 + t_4 \equiv -4 \pmod{243}}$　即 $2 + 74t_4 \equiv 0 \pmod 3$

解得 $\cancel{t_4 \equiv 8 \pmod{243}}$　$t_4 \equiv 2 \pmod 3$

$t_4 \equiv$

代入得 $x = 22 + 81 \cdot 2 = 184 \pmod{243}$

信安数基第4次作业-冯[illegible]宇-2022302181149

(4): 2-1: $y^2 = x^3-2x+3 \pmod 7$

$x=0$, $y^2 = 3 \pmod 7$，无解；$x=1$, $y^2=2 \pmod 7$, $y=3,4 \pmod 7$

$x=2$, $y^2=0 \pmod 7$, $y=0 \pmod 7$, $x=3$, $y^2=\cancel{2}\ 3 \pmod 7$，无解

$x=4$, $y^2=3 \pmod 7$，无解，$x=5$, $y^2=6 \pmod 7$，无解

$x=6$, $y^2=4 \pmod 7$，$y=2,5 \pmod 7$

共有5个点 分别是 $(0,3)$, $(0,4)$, $(6,2)$, $(6,5)$, $(2,0)$

(10) 求解同余式 $x^2 \equiv 79 \pmod{105}$

$$x^2 \equiv 79 \pmod{105} \Rightarrow \begin{cases} x^2 \equiv 79 \pmod 5 \equiv 4 \pmod 5 \\ x^2 \equiv 79 \pmod 3 \equiv 1 \pmod 3 \\ x^2 \equiv 79 \pmod 7 \equiv 2 \pmod 7 \end{cases}$$

$M_1=21$, $M_2=35$, $M_3=15$ $\qquad x=x_1=\pm 2 \pmod 5$

$M_1' \equiv 1 \pmod 5$, $M_2' \equiv 2 \pmod 3$, $M_3' \equiv 4 \pmod 7$ $\qquad x=x_2=\pm 1 \pmod 5$, $x=x_3=\pm 3 \pmod 7$

由中国剩余定理，原方程解为 $x=b_1\times 21+b_2\times 70+b_3\times 60 \pmod{105}$

$x_1 \equiv 2\times 21+1\times 70+3\times 60 \pmod{105} \equiv 82 \pmod{105}$

$x_2 \equiv 2\times 21+1\times 70-3\times 60 \pmod{105} \equiv 37 \pmod{105}$

$x_3 \equiv 2\times 21-70+3\times 60 \pmod{105} \equiv 47 \pmod{105}$

$x_4 \equiv 2\times 21-70-3\times 60 \pmod{105} \equiv 2 \pmod{105}$

$x_5 \equiv -2\times 21+70+3\times 60 \pmod{105} \equiv 103 \pmod{105}$

$x_6 \equiv -2\times 21-70+3\times 60 \pmod{105} \equiv 68 \pmod{105}$

$x_7 \equiv -2\times 21+70-3\times 60 \pmod{105} \equiv 58 \pmod{105}$

$x_8 \equiv -2\times 21-70-3\times 60 \pmod{105} \equiv 23 \pmod{105}$

20. $\left(\frac{151}{373}\right) = (-1)^{\frac{151^2-1}{2}\cdot\frac{373^2-1}{2}}\left(\frac{373}{151}\right) = (-1)^{(75\times152)(186\times372)} = 1\times\left(\frac{373}{151}\right) = \left(\frac{71}{151}\right)$

$= (-1)^{\frac{151^2-1}{2}\cdot\frac{71^2-1}{2}}\left(\frac{151}{71}\right) = (-1)^{75\times151\times35\times72} = \left(\frac{151}{71}\right) = \left(\frac{9}{71}\right) = 1$

$\left(\frac{911}{2003}\right) = (-1)^{\frac{911^2-1}{2}\cdot\frac{2003^2-1}{2}}\left(\frac{2003}{911}\right) = (-1)^{455\times912\ 1001\times2004}\left(\frac{2003}{911}\right) = \left(\frac{181}{911}\right) = (-1)^{\frac{90\times152}{2}}\left(\frac{911}{181}\right)$

$= \left(\frac{6}{181}\right)$

$= \left(\frac{2}{181}\right)\left(\frac{3}{181}\right) = (-1)^{\frac{181^2-1}{8}}\left(\frac{1}{3}\right)(-1)^{\frac{3^2-1}{2}\cdot\frac{181^2-1}{2}} = (-1)^{45\times91} = -1$

$\left(\frac{37}{200723}\right) = \left(\frac{200723}{37}\right)(-1)^{\frac{37^2-1}{2}\cdot\frac{200723^2-1}{2}} = \left(\frac{200723}{37}\right)(-1)^{(36\times19)\times100362\times200722}$

$= \left(\frac{13}{37}\right) = (-1)^{40\times18\times18\times38} = \left(\frac{18}{19}\right)$

$= \left(\frac{-1}{19}\right) = -1^{\frac{19-1}{2}} = -1$

(22) ① $x^2 \equiv -2 \pmod{67}$

$\left(\frac{-2}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{-1}{67}\right) = (-1)^{\frac{67^2-1}{8}}(-1)^{\frac{67-1}{2}} = 1$，原方程有2个解

② $x^2 \equiv 2 \pmod{67}$　$\left(\frac{2}{67}\right) = (-1)^{\frac{67^2-1}{8}} = -1$，原方程无解

(26) ① $x^2 \equiv 7 \pmod{227}$　$\left(\frac{7}{227}\right) = (-1)^{\frac{7^2-1}{2}\cdot\frac{227^2-1}{2}}\left(\frac{227}{7}\right) = \left(\frac{3}{7}\right) = (-1)^{\frac{7^2-1}{2}\cdot\frac{3^2-1}{2}}\left(\frac{1}{3}\right) = 1$

有解

② $11x^2 \equiv -6 \pmod{91}$

$\Rightarrow \begin{cases} 11x^2 \equiv -6 \pmod{7} \\ 11x^2 \equiv -6 \pmod{13} \end{cases}$　$\left(\frac{4}{7}\right) = \left(\frac{1}{7}\right) = 1$，

$\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1 = \left(\frac{-6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{6}{7}\right) = \left(\frac{-1}{7}\right) = (-1)^{\frac{7-1}{2}} = -1$

有解

(33) $p=401$, $q=281$ 求解同余式 (1) $x^2 \equiv 11 \pmod{pq}$

$\Rightarrow \begin{cases} x^2 \equiv 11 \pmod{401} \\ x^2 \equiv 11 \pmod{281} \end{cases}$　$\left(\frac{11}{401}\right) = \left(\frac{401}{11}\right)(-1)^{\frac{11^2-1}{2}\cdot\frac{401^2-1}{2}} = \left(\frac{5}{11}\right) = \left(\frac{1}{5}\right) = 1$

$\left(\frac{11}{281}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)^{\frac{11^2-1}{8}}\left(\frac{2}{3}\right) = (-1)(-1) = -1$

故同余式无解

信安数基第五次作业-冯乐子-2022302181149

9. 模47的原根有多少个，求所有模47的原根。

解：共有 $\varphi(\varphi(47))=\varphi(46)=22$ 个原根

$46=2\times 23$，即46有两个质因数 2, 23，

又 $ord_{47}^{-2}=23$，$ord_{47}^{-1}=2$，

故 $ord_{47}^{-2}=46$，故 -2 是模47的一个原根，

当 $(d,p-1)$ 时，d 遍历模 $p-1=46$ 的简化剩余系：

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45.

$(-2)^1=-2\equiv 45$，$(-2)^3=-8\equiv 39$，$(-2)^5=-32\equiv 15$，$(-2)^7=-128\equiv 13$

$(-2)^9\equiv 5$，$(-2)^{11}\equiv 20$，$(-2)^{13}\equiv 33$，$(-2)^{15}\equiv 38$，$(-2)^{17}\equiv 11$

$(-2)^{19}\equiv 44$，$(-2)^{21}\equiv 35$，$(-2)^{25}\equiv 43$，$(-2)^{27}\equiv 31$，$(-2)^{29}\equiv 30$

$(-2)^{31}\equiv 26$，$(-2)^{33}\equiv 10$，$(-2)^{35}\equiv 40$，$(-2)^{37}\equiv 19$，$(-2)^{39}\equiv 29$

$(-2)^{41}\equiv 22$，$(-2)^{43}\equiv 41$，$(-2)^{45}\equiv 23$

10. 设 p，$\frac{p-1}{2}$ 都是素数，设 a 是与 p 互素的整数，如果 $a\not\equiv\pm1$，$a^2\not\equiv 1$，$a^{\frac{p-1}{2}}\not\equiv 1 \pmod{p}$，则 a 是模 p 的原根。

证明：$\because a^2\not\equiv 1$ 且 $a^{\frac{p-1}{2}}\not\equiv 1 \pmod{p}$，$(a,p)=1$

又 $p-1$ 的因子只有 $1, 2, \frac{p-1}{2}, p-1$

$\therefore a^{p-1}\equiv 1 \pmod{p}$ 且 $\varphi(p)=p-1$

$\therefore a$ 为模 p 的原根

(17) $x^{22} \equiv 29 \pmod{41}$ $\varphi(41)=40$

$\because (22,40)=2$, $ind\,29=7$, $(7,2)=1$, 故无解