第1、2、3、4、5章

第1章 整数的可除性

(13)

Question

证明：形如 $4k+3$ 的素数有无穷多个.

Answer

证明：

设 $\forall N \in \mathbf{I}_+$,

设 $p_1, p_2, \cdots, p_n$ 为形如 $4n+3$ 的不大于 N 的所有素数，即形如 $4n+3$ 的素数个数有限.

令 $q = 4 \cdot \prod\limits_{i=1}^{k} p_i - 1$，$p_i$ 显然不为 q 的素因数.

1. 若 q 为素数
   $\because q = 4 \cdot \prod\limits_{i=1}^{k} p_i - 1 = 4(\prod\limits_{i=1}^{k} p_i - 1) + 3$
   则 q 也为形如 $4n+3$ 的素数，显然有 $q > N$，表明存在大于 N 的形如 $4n+3$ 的素数.
2. 若 q 不为素数
   先证明：形如 $4n+3$ 的正整数必有形如 $4n+3$ 的素因数.
   易知一切奇素数可写成 $4k+1$ 或 $4k+3 \quad (k \in I)$ 的形式.
   而 $(4k_1+1)(4k_2+1) = 4(4k_1k_2 + k_1 + k_2) + 1$ 不形如 $4n+3$,
   则 $4n+3$ 分解成的素因数乘积一定含 $4n+3$ 形式的素数.
   则 q 必含形如 $4n+3$ 的素因数 p，且 $p \neq p_i \ (i = 1, 2, \cdots, k)$, 则 $p > N$,
   表明存在大于 N 的形如 $4n+3$ 的素数 p.

由于 N 为任取正整数，则证明形如 $4n+3$ 的素数有无穷多个.

(17)

Question

将二进制 $(111100011110101)_2, (10111101001110)_2$ 转换为十六进制.

Answer

解：

$(0111\ 1000\ 1111\ 0101)_2 = (78\mathrm{F}5)_{16}$.

$(0010\ 1111\ 0100\ 1110)_2 = (2\mathrm{F}4\mathrm{E})_{16}$.

(18)

Question

将十六进制 $(\mathrm{ABCDEFA})_{16}, (\mathrm{DEFACEDA})_{16}, (9\mathrm{A}0\mathrm{AB})_{16}$ 转换为二进制.

Answer

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

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

$(9\mathrm{A}0\mathrm{AB})_{16} = (1001\ 1010\ 0000\ 1010\ 1011)_2$.

(28)

Question

求以下整数对的最大公因数：

④ $(20785, 44350)$.

Answer

解：

$44350 = 2 \times 20785 + 278020785 \quad = 7 \times 2780 + 13252780 = 2 \times 1325 + 1301325 \quad = 10 \times 130 + 25130 = 5 \times 25 + 525 \quad = 5 \times 5$

$\therefore$ 最大公因数是 5.

(32)

Question

运用广义欧几里德除法求整数 s, t 使得 $s \cdot a + t \cdot b = (a, b)$.

① $(1613, 3589)$.　　② $(2947, 3772)$.

Answer

解：

①

$$
\begin{aligned}
3589 &= 2 \times 1613 + 363 \\
1613 &= 4 \times 363 + 161 \\
363 &= 2 \times 161 + 41 \\
161 &= 3 \times 41 + 38 \\
41 &= 1 \times 38 + 3 \\
38 &= 12 \times 3 + 2 \\
3 &= 1 \times 2 + 1 \\
2 &= 2 \times 1
\end{aligned}
$$

$$
\begin{aligned}
(1613, 3589) = 1 &= 3 - 2 \\
&= 3 + 12 \times 3 - 38 \\
&= 13 \times (41 - 38) - 38 \\
&= 13 \times 41 - 14 \times (161 - 3 \times 41) \\
&= 55 \times (363 - 2 \times 161) - 14 \times 161 \\
&= 55 \times 363 - 124 \times (1613 - 4 \times 363) \\
&= 551 \times (3589 - 2 \times 1613) - 124 \times 1613 \\
&= 551 \times 3589 - 1226 \times 1613
\end{aligned}
$$

$\therefore\ (1613, 3589) = 1 = (-1226) \times 1613 + 551 \times 3589$

②

$$
\begin{aligned}
3772 &= 1 \times 2947 + 825 \\
2947 &= 3 \times 825 + 472 \\
825 &= 1 \times 472 + 353 \\
472 &= 1 \times 353 + 119 \\
353 &= 2 \times 119 + 115 \\
119 &= 1 \times 115 + 4 \\
115 &= 28 \times 4 + 3 \\
4 &= 1 \times 3 + 1 \\
3 &= 3 \times 1
\end{aligned}
$$

$$
\begin{aligned}
(2947, 3772) = 1 &= 4 - 3 \\
&= 4 + 28 \times 4 - 115 \\
&= 29 \times (119 - 115) - 115 \\
&= 29 \times 119 - 30 \times (353 - 2 \times 119) \\
&= 89 \times (472 - 353) - 30 \times 353 \\
&= 89 \times 472 - 119 \times (825 - 472) \\
&= 208 \times (2947 - 3 \times 825) - 119 \times 825 \\
&= 208 \times 2947 - 743 \times (3772 - 2947) \\
&= 951 \times 2947 - 743 \times 3772
\end{aligned}
$$

$\therefore\ (2947, 3772) = 1 = 951 \times 2947 - 743 \times 3772$

(50)

Question

求出下列各对数的最小公倍数.

④ $[132, 253]$.

Answer

解：

$$
\begin{aligned}
253 &= 1 \times 132 + 121 \\
132 &= 1 \times 121 + 11 \\
121 &= 11 \times 11
\end{aligned}
$$

$\therefore\ (132, 253) = 11.$

$\therefore\ [132, 253] = \frac{132 \times 253}{(132, 253)} = \frac{11 \times 12 \times 11 \times 23}{11} = 11 \times 12 \times 23 = 29436.$

第2章 同余

(2)

Question

证明：当 $m > 2$ 时，$0^2, 1^2, \cdots, (m-1)^2$ 一定不是模 m 的完全剩余系.

Answer

证明：

$\because\ m > 2, (m-1)^2 = m^2 - 2m + 1 = m(m-2) + 1 \equiv 1 \pmod m$

则 1 和任意 $(m-1)^2$ 在同一剩余类中，则 $m>2$ 时，

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

(6)

Question

2003 年 5 月 9 日是星期五，问第 $2^{20080509}$ 天是星期几？

Answer

解：

$2^1 \equiv 2 \pmod 7, \qquad 2^2 \equiv 4 \pmod 7, \qquad 2^3 \equiv 1 \pmod 7$

$20080509 = 3 \times 6693503$

$\therefore\ 2^{20080509} = (2^3)^{6693503} \equiv 1 \pmod 7$

$\therefore$ 是星期六.

(9)

Question

设 $n=pq$，其中 p, q 是素数. 证明：如果 $a^2 \equiv b^2 \pmod n$，$n \nmid a-b$，$n \nmid a+b$，则 $(n, a-b)>1, (n, a+b)>1$.

Answer

证明：

$\because\ a^2 \equiv b^2 \pmod n$

$\therefore$ 设 $a^2-b^2 = kn = (a+b)(a-b), k \in \mathbf{Z}$

$\Rightarrow\ n \mid (a+b)(a-b), kpq = (a+b)(a-b)$

$\because\ n \nmid (a-b), n \nmid (a+b)$

则如设 $p \mid a-b, q \mid a+b$，则 $p \nmid a+b, q \nmid a-b$.

$\therefore\ (p, a+b) = 1 = (q, a-b)$

$\therefore$

$$
\begin{aligned}
(n, a-b) = (pq, a-b) = (p, a-b) = p > 1 \\
(n, a+b) = (pq, a+b) = (q, a+b) = q > 1
\end{aligned}
$$

(12)

Question

列出 $\mathbf{Z}/7\mathbf{Z}$ 中的加法表和乘法表.

Answer

解：

$\mathbf{Z}/7\mathbf{Z} = \{0, 1, 2, 3, 4, 5, 6\}$.

加法表

⊕	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

乘法表

⊗	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(31)

Question

证明：如果 $c_1, c_2, \cdots, c_{\varphi(m)}$ 是模 m 的简化剩余系，那么

$$c_1 + c_2 + \cdots + c_{\varphi(m)} \equiv 0 \pmod{m}.$$

Answer

证明：

$\because\ C_1, C_2, \cdots, C_{\varphi(m)}$ 是模 m 的简化剩余系.

而对任意 C_i 有 $(m - C_i) + C_i \equiv 0 \pmod{m}$.

而 $m - C_i$ 属于模 m 的简化剩余系.

$\therefore\ c_1 + c_2 + \cdots + c_{\varphi(m)} \equiv 0 \pmod{m}$.

第3章 同余式

(1)

Question

求出下列一次同余方程的所有解.

③ $17x \equiv 14 \pmod{21}$.

Answer

解:

$\because\ (17,21)=1\mid 14$

$\therefore$ 有解.

求出 $7x\equiv 1\pmod{21}$ 的一个特解 $x_0'\equiv 5\pmod{21}$.

则 $17x\equiv 14\pmod{21}$ 的一个特解 $x_0\equiv 14x_0'\equiv 14\cdot 5\equiv 7\pmod{21}$.

所有解为 $x\equiv 7\pmod{21}$.

(10)

Question

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.

Answer

证明:

必要性:

有解 $\Rightarrow\ (m_1,m_2)=1\mid(a_1-a-2)$，显然成立.

充分性:

$x\equiv y_1m_1+a_1\Rightarrow y_1m_1\equiv a_2-a_1\pmod{m_2}$.

有解 $y_1\equiv y_0\pmod{m_2}$.

设 $x_0=a_1+m_1y_0$，则 $x_0\equiv a_1\pmod{m_1}$，且

$x_0=a_1+m_1y_0\equiv a_2\pmod{m_2}$

$\therefore\ x_0$ 为同余方程组的解.

若 x_1,x_2 为方程组的解，则 $x_1\equiv x_2\pmod{m_1},x_1\equiv x_2\pmod{m_2}$.

$\therefore\ x_1\equiv x_2\pmod{[m_1,m_2]}$，解模 $([m_1,m_2])$ 是唯一的.

(16)

Question

求下列一次同余方程组的解.

① $\begin{cases}x+2y\equiv 1\pmod 7\\2x+y\equiv 1\pmod 7\end{cases}$.

Answer

解:

$$\begin{cases}x+2y\equiv 1\pmod 7\\2x+y\equiv 1\pmod 7\end{cases}\Rightarrow\begin{cases}x+y\equiv 3\pmod 7\\x-y\equiv 0\pmod 7\end{cases}$$

$$\therefore \begin{cases} x \equiv 5 \pmod 7 \\ y \equiv 5 \pmod 7 \end{cases}$$

(19)

Question

将同余式方程化为同余式组来求解.

(i) $23x \equiv 1 \pmod{140}$; (ii) $17x \equiv 229 \pmod{1540}$.

Answer

解:

(i)

$$23x \equiv 1 \pmod{140} \Rightarrow \begin{cases} 23x \equiv 1 \pmod 4 \\ 23x \equiv 1 \pmod 5 \\ 23x \equiv 1 \pmod 7 \end{cases} \Rightarrow \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

$\therefore\ m_1 = 4, m_2 = 5, m_3 = 7.$

$\therefore\ M_1 = 35, M_2 = 28, M_3 = 20.$

$$\begin{cases} 35M_1' \equiv 1 \pmod 4 \\ 28M_2' \equiv 1 \pmod 5 \\ 20M_3' \equiv 1 \pmod 7 \end{cases} \Rightarrow \begin{cases} M_1' = 3 \\ M_2' = 2 \\ M_3' = 6 \end{cases}$$

$\therefore\ x \equiv 3 \cdot 3 \cdot 25 + 2 \cdot 2 \cdot 28 + 4 \cdot 6 \cdot 20 \pmod{140} \Rightarrow x \equiv 67 \pmod{140}.$

(ii)

$$17x \equiv 229 \pmod{1540} \Rightarrow \begin{cases} 17x \equiv 1 \pmod 4 \\ 17x \equiv 4 \pmod 5 \\ 17x \equiv 5 \pmod 7 \\ 17x \equiv 9 \pmod{11} \end{cases} \Rightarrow \begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 4 \pmod 7 \\ x \equiv 7 \pmod{11} \end{cases}$$

$\therefore\ m_1 = 4, m_2 = 5, m_3 = 7, m_4 = 11.$

$\therefore\ M_1 = 385, M_2 = 308, M_3 = 220, M_4 = 140.$

$$\begin{cases} 385M_1' \equiv 1 \pmod 4 \\ 308M_2' \equiv 1 \pmod 5 \\ 220M_3' \equiv 1 \pmod 7 \\ 140M_4' \equiv 1 \pmod{11} \end{cases} \Rightarrow \begin{cases} M_1' = 1 \\ M_2' = 2 \\ M_3' = 5 \\ M_4' = 7 \end{cases}$$

$\therefore\ x \equiv 1 \cdot 1 \cdot 385 + 2 \cdot 2 \cdot 308 + 5 \cdot 4 \cdot 220 + 7 \cdot 7 \cdot 140 \pmod{1540} \Rightarrow x \equiv 557 \pmod{1540}.$

(23)

Question

求解同余式

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

Answer

解:

$$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x \equiv 0 \pmod 7$$
$$(x^7-x)(3x^7+4x^6+2x^4+x^2+3x+4)+x^6+2x^5+2x^3+15x^2+5x \equiv 0 \pmod 7$$
$$x^6+2x^5+2x^3+15x^2+5x \equiv 0 \pmod 7$$

代入 $x=0,1,2,3,4,5,6$

得 $x \equiv 0 \pmod 7 \Rightarrow x \equiv 6 \pmod 7$.

(24)

Question

求解同余式

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

Answer

解:

求导 $f'(x)=4x^3+7 \pmod{243}$.

且 $243=3^5$.

$\therefore\ f(x) \equiv 0 \pmod 3 \Rightarrow x_1 \equiv 1 \pmod 3$.

将 $x=1+3\cdot t_1$ 代入 $f(x)\equiv 0 \pmod 9$.

$f(1)+f'(1)t_1\cdot 3 \equiv 0 \pmod 9 \Rightarrow f(1)\equiv 3 \pmod 9, f'(1)\equiv 2 \pmod 9$.

$\therefore\ 3+6t_1 \equiv 0 \pmod 9$ 或 $2t_1 \equiv -1 \pmod 3$.

$\therefore\ t_1 \equiv 1 \pmod 3$.

$\therefore\ f(x)\equiv 0 \pmod 9 \Rightarrow x_2 \equiv 1+3\cdot t_1 \equiv 4 \pmod 9$.

将 $x=4+9\cdot t_2$ 代入 $f(x)\equiv 0 \pmod{27}$.

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

$\therefore\ 18+20t_2\cdot 9 \equiv 0 \pmod{27} \Rightarrow 2t_2 \equiv -2 \pmod 3$.

$\therefore\ t_2 \equiv 2 \pmod 3$.

$\therefore\ x_3 \equiv 4+9\cdot t_2 \equiv 22 \pmod{27}$.

将 $x=22+27\cdot t_3$ 代入 $f(x)\equiv 0 \pmod{81}$.

$f(22)\equiv 0 \pmod{81}, f'(22)\equiv 7 \pmod{81}$.

$\therefore\ 0+7t_3\cdot 1 \equiv 0 \pmod 3$.

$\therefore\ t_3 \equiv 0 \pmod 3$.

$\therefore\ x_4 \equiv x_3+27\cdot t_3 \equiv 22 \pmod{81}$.

$f(22)\equiv 162 \pmod{243}, f'(22)\equiv 6 \pmod{243}$.

$\therefore\ 162+27t_4\cdot 6 \equiv 0 \pmod{243}$.

$\therefore\ t_4 \equiv 2 \pmod 3$.

$\therefore\ x_5 \equiv x_4+81\cdot t_4 \equiv 184 \pmod{243}$.

$\therefore$ 解为 $x \equiv 84 \pmod{243}$.

第4章 二次同余式与平方剩余

(4)

Question

求满足方程 $E: y^2 = x^3 - 2x + 3 \pmod 7$ 的所有点.

Answer

解:

对 $x = 0, 1, 2, 3, 4, 5, 6$ 分别求 y.

$x = 0, y^2 \equiv 3 \pmod 7$，无解.

$x = 1, y^2 \equiv 2 \pmod 7$，$y = 3, 4 \pmod 7$.

$x = 2, y^2 \equiv 0 \pmod 7$，$y = 0 \pmod 7$.

$x = 3, y^2 \equiv 3 \pmod 7$，无解.

$x = 4, y^2 \equiv 3 \pmod 7$，无解.

$x = 5, y^2 \equiv 6 \pmod 7$，无解.

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

$\therefore$ 共 5 个点.

(10)

Question

求解同余式 $x^2 \equiv 79 \pmod{105}$.

Answer

解:

$\because\ 105 = 3 \cdot 5 \cdot 7$

$\therefore$ 原同余式等价于同余式组

$$\begin{cases} x^2 \equiv 79 \equiv 1 \pmod 3 \\ x^2 \equiv 79 \equiv 4 \pmod 5 \\ x^2 \equiv 79 \equiv 2 \pmod 7 \end{cases} \Rightarrow \begin{cases} x = x_1 \equiv \pm 1 \pmod 3 \\ x = x_2 \equiv \pm 2 \pmod 5 \\ x = x_3 \equiv \pm 3 \pmod 7 \end{cases}$$

$\therefore\ m_1 = 3, m_2 = 5, m_3 = 7, m = 105.$

$\therefore\ M_1 = 35, M_2 = 21, M_3 = 15.$

$\therefore\ M_1' = 2, M_2' = 1, M_3' = 1.$

$\therefore\ x \equiv 70b_1 + 21b_2 + 15b_3 \pmod{105} \Rightarrow$

$$
\begin{aligned}
x &\equiv \quad 70+42+45 \equiv 52 \pmod{105} \\
x &\equiv \quad 70+42-45 \equiv 67 \pmod{105} \\
x &\equiv \quad 70-42+45 \equiv 73 \pmod{105} \\
x &\equiv \quad 70-42-45 \equiv 88 \pmod{105} \\
x &\equiv \quad -70+42+45 \equiv 17 \pmod{105} \\
x &\equiv \quad -70+42-45 \equiv 32 \pmod{105} \\
x &\equiv \quad -70-42+45 \equiv 38 \pmod{105} \\
x &\equiv \quad -70-42-45 \equiv 53 \pmod{105}
\end{aligned}
$$

(20)

Question

② $\left(\frac{151}{373}\right)$; ④ $\left(\frac{151}{373}\right)$; ⑤ $\left(\frac{151}{373}\right)$;

Answer

解:

②

$$
\begin{aligned}
&\left(\frac{151}{373}\right) \\
&= \left(\frac{373}{151}\right) \cdot (-1)^{\frac{151-1}{2}\cdot\frac{373-1}{2}} \\
&= \left(\frac{71}{151}\right) \\
&= \left(\frac{151}{71}\right) \cdot (-1)^{\frac{151-1}{2}\cdot\frac{373-1}{2}} \\
&= -\left(\frac{9}{71}\right) \\
&= -\left(\frac{3^2}{71}\right) \\
&= -1
\end{aligned}
$$

④

$$\left(\frac{911}{2003}\right)$$

$$=\left(\frac{2003}{911}\right)\cdot(-1)^{\frac{911-1}{2}\cdot\frac{2003-1}{2}}$$

$$=-\left(\frac{181}{911}\right)$$

$$=-\left(\frac{911}{181}\right)\cdot(-1)^{\frac{181-1}{2}\cdot\frac{911-1}{2}}$$

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

$$=-\left(\frac{2}{181}\right)\cdot\left(\frac{3}{181}\right)$$

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

$$=\left(\frac{1}{3}\right)$$

$$=1$$

⑤

$$\left(\frac{37}{200723}\right)$$

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

$$=\left(\frac{35}{37}\right)$$

$$=\left(\frac{5}{37}\right)\cdot\left(\frac{7}{37}\right)$$

$$=\left(\frac{37}{5}\right)\cdot(-1)^{\frac{5-1}{2}\cdot\frac{37-1}{2}}\cdot\left(\frac{37}{7}\right)\cdot(-1)^{\frac{7-1}{2}\cdot\frac{37-1}{2}}$$

$$=\left(\frac{2}{5}\right)\cdot\left(\frac{2}{7}\right)$$

$$=(-1)^{\frac{5^2-1}{8}}\cdot(-1)^{\frac{7^2-1}{8}}$$

$$=-1$$

(22)

Question

求下列同余方程的解数：

① $x^2 \equiv -2 \pmod{67}$; ② $x^2 \equiv 2 \pmod{67}$;

Answer

解：

①

$$
\begin{aligned}
&\left(\frac{-2}{67}\right) \\
&= \left(\frac{-1}{67}\right) \cdot \left(\frac{2}{67}\right) \\
&= (-1)^{\frac{67-1}{2}} \cdot (-1)^{\frac{67^2-1}{8}} \\
&= 1
\end{aligned}
$$

∴ 有两个解.

②

$$
\begin{aligned}
&\left(\frac{2}{67}\right) \\
&= (-1)^{\frac{67^2-1}{8}} \\
&= -1
\end{aligned}
$$

∴ 无解.

(26)

Question

判断下列同余方程是否有解：

① $x^2 \equiv 7 \pmod{227}$; ③ $11x^2 \equiv -6 \pmod{91}$;

Answer

解：

①

$$\left(\frac{7}{227}\right)$$

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

$$= -\left(\frac{7}{3}\right) \cdot (-1)^{\frac{3-1}{2} \cdot \frac{7-1}{2}}$$

$$= \left(\frac{1}{3}\right)$$

$$= 1$$

$\therefore$ 7 是 227 的平方剩余，有解.

③

$$11x^2 \equiv -6 \pmod{91} \Rightarrow x^2 \equiv 16 \pmod{91}$$
$$\Rightarrow \begin{cases} x^2 \equiv 3 \ (\text{mod } 13) \\ x^2 \equiv 2 \ (\text{mod } 7) \end{cases} \Rightarrow \begin{cases} x = x_1 \equiv \pm 4 \ (\text{mod } 13) \\ x = x_2 \equiv \pm 3 \ (\text{mod } 7) \end{cases}$$

$\therefore\ m_1 = 13, m_2 = 7.$

$\therefore\ M_1 = 7, M_2 = 13.$

$\therefore\ M_1' = 2, M_2' = 5.$

$\therefore\ x \equiv 14b_1 + 65b_2 \ (\text{mod } 91)$

$\therefore$ 有解.

(39)

Question

设 $p = 401, q = 281$，求解下列同余式：

(v) $x^2 = 11 \ (\text{mod } pq)$.

Answer

解：

$x^2 = 11 \ (\text{mod } pq), p = 401, q = 281$

$\Rightarrow \begin{cases} x^2 \equiv 11 \ (\text{mod } 401) \\ x^2 \equiv 11 \ (\text{mod } 281) \end{cases}.$

$$\left(\frac{11}{281}\right)$$

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

$$= \left(\frac{6}{11}\right)$$

$$= \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$$

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

$$= -1$$

$\therefore$ 无解.

第5章 原根与指标

(5)

Question

问模 47 的原根有多少个? 求出模 47 的所有原根.

Answer

解:

$\because$ 47 为素数.

$\therefore$ $\varphi(47) = 46 = 2 \times 43 \Rightarrow q_1 = 2, q_2 = 43.$

原根个数 $n = \varphi(\varphi(m)) = \varphi(46) = \varphi(2) \cdot \varphi(23) = 22.$

只需验证 $g^{23} \equiv 1 \pmod{47}, g^2 \equiv 1 \pmod{47}$ 是否成立.

对 $2, 3, 5$ 等进行验算.

$2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16,$
$2^7 \equiv 34, 2^8 \equiv 21, 2^{16} \equiv 1 \pmod{47}.$

$3^2 \equiv 9, 3^3 \equiv 27, 3^4 \equiv 81,$
$3^7 \equiv 25, 3^8 \equiv 28, 3^{16} \equiv 32, 3^{23} \equiv 1 \pmod{47}.$

$5^2 \equiv 4, 5^3 \equiv 31, 5^4 \equiv 14,$
$5^7 \equiv 11, 5^8 \equiv 8, 5^{16} \equiv 17, 5^{23} \equiv -1 \pmod{47}.$

$\therefore$ $g = 5$ 为模 47 的原根，g^d 遍历 47 的所有原根，其中

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

$$
\begin{aligned}
&5^1 = 5, && 5^3 = 31, && 5^5 = 23, \\
&5^7 = 11, && 5^9 = 40, && 5^{11} = 13, \\
&5^{13} = 43, && 5^{15} = 41, && 5^{17} = 38, \\
&5^{19} = 10, && 5^{21} = 15, && 5^{25} = 22, \\
&5^{27} = 33, && 5^{29} = 26, && 5^{31} = 39, \\
&5^{33} = 35, && 5^{35} = 29, && 5^{37} = 20, \\
&5^{39} = 30, && 5^{41} = 45, && 5^{43} = 44, && 5^{45} = 19 \pmod{47}
\end{aligned}
$$

共 22 个.

(10)

Question

设 p 和 $\frac{p-1}{2}$ 都是素数，设 a 是与 p 互素的正整数. *证明* 如果

$$
a \not\equiv 1, \quad a^2 \not\equiv 1, \quad a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p},
$$

则 a 是模 p 的原根.

Answer

证明:

$\because\ p, \frac{p-1}{2}$ 为素数.

$\therefore\ \varphi(p) = p - 1 = 2 \cdot \frac{p-1}{2}$.

$\therefore\ q_1 = 2, q_2 = \frac{p-1}{2}$.

又 $a^{\frac{\varphi(p)}{2}} \not\equiv 1 \pmod{p}, a^2 = a^{\frac{\varphi(p)}{\frac{p-1}{2}}} \not\equiv 1 \pmod{p}$.

$\therefore\ a$ 为模 p 的原根.

(17)

Question

求解同余式

$$
x^{22} \equiv 29 \pmod{41}
$$

Answer

解:

$\because\ (n, \varphi(m)) = (22, \varphi(41)) = (22, 40) = 2$,

$\text{ind} 29 = 7, (2, 7) = 1$,

$\therefore$ 该同余式无解.