

### 第三章

1. 通过直接计算求下列同余方程的解和解数：

- (1)  $x^5 - 3x^2 + 2 \equiv 0 \pmod{7}$ ;
- (2)  $3x^4 - x^3 + 2x^2 - 26x + 1 \equiv 0 \pmod{11}$ ;
- (3)  $3x^2 - 12x - 19 \equiv 0 \pmod{28}$ ;
- (4)  $3x^2 + 18x - 25 \equiv 0 \pmod{28}$ ;
- (5)  $x^2 + 8x - 13 \equiv 0 \pmod{28}$ ;
- (6)  $4x^2 + 21x - 32 \equiv 0 \pmod{141}$ ;
- (7)  $x^{26} + 7x^{21} - 5x^{17} + 2x^{11} + 8x^5 - 3x^2 - 7 \equiv 0 \pmod{5}$ ;
- (8)  $5x^{18} - 13x^{12} + 9x^7 + 18x^4 - 3x + 8 \equiv 0 \pmod{7}$ 。

答：可用程序语言进行计算。

- (1) 将 0~6 分别代入方程验算可得，该方程有解 1, 5。
- (2) 将 0~10 分别代入方程验算可得，方程有  $x = 10$  为唯一解。
- (3) 将 0~27 分别代入方程验算可得，方程有 4 个解，分别为 1,3,15,17。
- (4) 将 0~27 分别代入方程验算可得，方程有 4 个解，分别为 3,5,17,19。
- (5) 将 0~27 分别代入方程验算可得，方程有 4 个解，分别为 9,11,23,25。
- (6) 将 0~140 分别代入方程验算可得，该方程无解。
- (7) 将 0~4 分别代入方程验算可得，该方程无解。
- (8) 将 0~6 分别代入方程验算可得，该方程无解。

2. 求  $2^x \equiv x^2 \pmod{3}$  的解。

解：6k+2 和 6k+4 (k 为整数) 两种解，即：  $\pm 2 \pmod{6}$

2. 求  $2^x \equiv x^2 \pmod{3}$  的解。

解：将 0,1,2 分别代入方程验算可得， ~~$x = 2 \pmod{3}$~~ 。这种解法错误，比如  $x = 5$  就不是方程的解。

正确的解：

$$2^x \equiv x^2 \pmod{3} \Rightarrow (3-1)^x \equiv x^2 \pmod{3} \Rightarrow (-1)^x \equiv x^2 \pmod{3}.$$

很显然，当  $x$  为 3 的倍数时方程不成立； $x$  为奇数时也不成立， $(2k+1)^2 \pmod{3}$  只可能余 0 或 1，而左边  $\pmod{3}$  余 -1；所以考虑  $x=6k+2$  和  $6k+4$  的情形，通过验证，这两类数都满足方程，即左边和右边  $\pmod{3}$  都余 1。

所以原方程的解为  $x \equiv \pm 2 \pmod{6}$ 。

3. 求解下列一元一次同余方程。

- (1)  $3x \equiv 2 \pmod{7}$ ;
- (2)  $9x \equiv 12 \pmod{15}$ ;

- (3)  $7x \equiv 1(\text{mod } 31)$ ;
- (4)  $20x \equiv 4(\text{mod } 30)$ ;
- (5)  $17x \equiv 14(\text{mod } 21)$ ;
- (6)  $64x \equiv 83(\text{mod } 105)$ ;
- (7)  $128x \equiv 833(\text{mod } 1001)$ ;
- (8)  $987x \equiv 610(\text{mod } 1597)$ ;
- (9)  $57x \equiv 87(\text{mod } 105)$ ;
- (10)  $49x \equiv 5000(\text{mod } 999)$ 。

解：(1) 由于  $(3, 7) = 1$ ,  $3^{-1} \equiv 5(\text{mod } 7)$ , 所以有唯一解  $x \equiv 3(\text{mod } 7)$ 。

$$(2) (9, 15) = 3. 3|12, \text{ 因此, } a' = \frac{9}{3} = 3, m' = \frac{15}{3} = 5, b' = \frac{12}{4}.$$

首先考虑同余方程  $3x \equiv 1(\text{mod } 5)$ , 因为 3 模 5 的逆元为 2, 所以该方程的解为  $x_0 = 2$ 。

因此,

$$x \equiv 2 \times 4 + k \times 5(\text{mod } 15), k = 0, 1, \dots, \text{gcd}(9, 15) - 1$$

是同余方程  $9x \equiv 12(\text{mod } 15)$  的全部解。

所以同余方程  $9x \equiv 12(\text{mod } 15)$  的全部解为 8, 13, 3。

(3) 由于  $(7, 31) = 1$ , 由扩展的欧几里得算法可计算出  $7^{-1} \equiv 9(\text{mod } 31)$ , 所以有唯一解  $x \equiv 9(\text{mod } 31)$ 。

(4)  $(20, 30) = 10$ , 而  $10 \nmid 4$ , 所以方程无解。

(5) 由于  $(17, 21) = 1$ , 由扩展的欧几里得算法可计算出  $17^{-1} \equiv 5(\text{mod } 21)$ , 所以有唯一解  $x = 5 * 14 \equiv 7(\text{mod } 21)$ 。

(6) 由于  $(64, 105) = 1$ , 由扩展的欧几里得算法可计算出  $64^{-1} \equiv 64(\text{mod } 105)$ , 所以有唯一解  $x = 64 * 83 \equiv 62(\text{mod } 105)$ 。

(7) 由于  $(128, 1001) = 1$ , 由扩展的欧几里得算法可计算出  $128^{-1} \equiv 305(\text{mod } 1001)$ , 所以有唯一解  $x = 305 * 833 \equiv 812(\text{mod } 1001)$ 。

(8) 由于  $(987, 1597) = 1$ , 由扩展的欧几里得算法可计算出  $987^{-1} \equiv 610(\text{mod } 1597)$ , 所以有唯一解  $x = 610 * 610 \equiv 1596(\text{mod } 1596)$ 。

4. 求解下列一元一次同余方程。

- (1)  $x \equiv 1(\text{mod } 4)$ ,  $x \equiv 2(\text{mod } 3)$ ,  $x \equiv 3(\text{mod } 5)$ ;
- (2)  $x \equiv 4(\text{mod } 11)$ ,  $x \equiv 3(\text{mod } 17)$ ;
- (3)  $x \equiv 2(\text{mod } 5)$ ,  $x \equiv 1(\text{mod } 6)$ ,  $x \equiv 3(\text{mod } 7)$ ,  $x \equiv 0(\text{mod } 11)$ ;
- (4)  $3x \equiv 1(\text{mod } 11)$ ,  $5x \equiv 7(\text{mod } 13)$ ;
- (5)  $8x \equiv 6(\text{mod } 10)$ ,  $3x \equiv 10(\text{mod } 17)$ ;

$$(6) \quad x \equiv 7(\text{mod}10), \quad x \equiv 3(\text{mod}12), \quad x \equiv 12(\text{mod}15);$$

$$(7) \quad x \equiv 6(\text{mod}35), \quad x \equiv 11(\text{mod}55), \quad x \equiv 2(\text{mod}33)。$$

解：(1) 根据中国剩余定理，令  $m=60$ ，则

$$M_1=60/4=15, \quad M_1^{-1} = 15^{-1} \equiv 3(\text{mod}4);$$

$$M_2=60/3=20, \quad M_2^{-1} = 20^{-1} \equiv 2(\text{mod}3);$$

$$M_3=60/5=12, \quad M_3^{-1} = 12^{-1} \equiv 3(\text{mod}5);$$

$$\text{因此, } x = 3 \times 15 \times 1 + 2 \times 20 \times 2 + 3 \times 12 \times 3(\text{mod}60) \equiv 53(\text{mod}60)。$$

(2) 根据中国剩余定理，令  $m=187$ ，则

$$M_1=17, \quad M_1^{-1} = 17^{-1} \equiv 2(\text{mod}11);$$

$$M_2=11, \quad M_2^{-1} = 11^{-1} \equiv 14(\text{mod}17);$$

$$\text{因此, } x = 4 \times 17 \times 2 + 3 \times 11 \times 14(\text{mod}187) \equiv 37(\text{mod}187)。$$

(3) 根据中国剩余定理，令  $m=5*6*7*11=2310$ ，则

$$M_1=2310/5=462, \quad M_1^{-1} = 462^{-1} \equiv 3(\text{mod}5);$$

$$M_2=2310/6=385, \quad M_2^{-1} = 385^{-1} \equiv 1(\text{mod}6);$$

$$M_3=2310/7=330, \quad M_3^{-1} = 330^{-1} \equiv 1(\text{mod}7);$$

$$M_4=2310/11=210, \quad M_4^{-1} = 210^{-1} \equiv 1(\text{mod}11);$$

$$\text{因此, } x = 2 \times 462 \times 3 + 1 \times 385 \times 1 + 3 \times 330 \times 1 + 0 \times 210 \times 1(\text{mod}2310) \\ \equiv 1837(\text{mod}2310)。$$

(4) 原方程组等价于  $x \equiv 4(\text{mod}11), x \equiv 8(\text{mod}13)$

根据中国剩余定理，令  $m=11*13=143$ ，则

$$M_1=13, \quad M_1^{-1} = 13^{-1} \equiv 6(\text{mod}11);$$

$$M_2=11, \quad M_2^{-1} = 11^{-1} \equiv 6(\text{mod}13);$$

$$\text{因此, } x = 4 \times 13 \times 6 + 8 \times 11 \times 6(\text{mod}143) \equiv 125(\text{mod}143)。$$

(5) 首先求解  $8x \equiv 6(\text{mod}10)$ ，可得该方程有两个解为 2 和 7。

然后分别求解  $x \equiv 2(\text{mod}10), x \equiv 9(\text{mod}17)$  和  $x \equiv 7(\text{mod}10), x \equiv 9(\text{mod}17)$ 。

根据中国剩余定理，第一个方程组的解为  $x = 162(\text{mod}170)$ ，第二个方程组的解为  $x = 77(\text{mod}170)$ 。

(6) 原方程组等价于

$$\begin{cases} x \equiv 7(\text{mod}2) \\ x \equiv 7(\text{mod}5) \\ x \equiv 3(\text{mod}3) \\ x \equiv 3(\text{mod}4) \\ x \equiv 12(\text{mod}3) \\ x \equiv 12(\text{mod}5) \end{cases}$$

即

$$\begin{cases} x \equiv 2(\text{mod}5) \\ x \equiv 0(\text{mod}3) \\ x \equiv 3(\text{mod}4) \end{cases}$$

根据中国剩余定理，可得

$$x = 27(\text{mod}60)。$$

(7) 原方程组等价于

$$\begin{cases} x \equiv 6(\text{mod}5) \\ x \equiv 6(\text{mod}7) \\ x \equiv 11(\text{mod}5) \\ x \equiv 11(\text{mod}11) \\ x \equiv 2(\text{mod}3) \\ x \equiv 2(\text{mod}11) \end{cases}$$

由于第 4 个方程和第 6 个方程矛盾，所以原方程组无解。

5. 把同余方程化为同余方程组来解。

$$(1) \ 23x \equiv 1(\text{mod}140); \quad (2) \ 17x \equiv 229(\text{mod}1540)。$$

解 (1) 由于  $140=4 \times 5 \times 7$ ，所以原同余方程与下列同余方程组同解：

$$\begin{cases} 23x = 1(\text{mod}4) \\ 23x = 1(\text{mod}5) \\ 23x = 1(\text{mod}7) \end{cases}$$

上述同余方程组可以化简为：

$$\begin{cases} 3x = 1(\text{mod}4) \\ 3x = 1(\text{mod}5) \\ 2x = 1(\text{mod}7) \end{cases}$$

可进一步化简为：

$$\begin{cases} x = 3(\text{mod}4) \\ x = 2(\text{mod}5) \\ x = 4(\text{mod}7) \end{cases}$$

根据中国剩余定理，令  $m=140$ ，

$$M_1 = 140/4=35, \quad M_1^{-1} = 3(\text{mod}4)$$

$$M_2 = 140/5=28, \quad M_2^{-1} = 2(\text{mod}5)$$

$$M_3 = 140/7=20, \quad M_3^{-1} = 6(\text{mod}7)$$

$$x = 3 \cdot 35 \cdot 3 + 2 \cdot 28 \cdot 2 + 6 \cdot 20 \cdot 4 \quad (\text{mod}140)$$

$$\equiv 315 + 112 + 480 \quad (\text{mod}140)$$

$$\equiv 67 \pmod{140}$$

(2) 解:  $1540=4*5*7*11$ .

所以  $17x \equiv 229 \pmod{1540}$  等价于

$$\begin{cases} 17x \equiv 229 \pmod{4} \\ 17x \equiv 229 \pmod{5} \\ 17x \equiv 229 \pmod{7} \\ 17x \equiv 229 \pmod{11} \end{cases}$$

即

$$\begin{cases} x \equiv 1 \pmod{4} \\ 2x \equiv 4 \pmod{5} \\ 3x \equiv 5 \pmod{7} \\ 6x \equiv 9 \pmod{11} \end{cases}$$

等价于

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 7 \pmod{11} \end{cases}$$

根据中国剩余定理, 令  $m=1540$ ,

$$M_1=1540/4=385, \quad M_1^{-1} \equiv 1 \pmod{4}$$

$$M_2=1540/5=308, \quad M_2^{-1} \equiv 2 \pmod{5}$$

$$M_3=1540/7=220, \quad M_3^{-1} \equiv 5 \pmod{7}$$

$$M_4=1540/11=140, \quad M_4^{-1} \equiv 7 \pmod{11}$$

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

$$\equiv 12877 \pmod{1540}$$

$$\equiv 557 \pmod{1540}$$

6. 证明: 同余方程组  $x \equiv a_j \pmod{m_j} (j=1,2)$  有解的充要条件是  $(m_1, m_2) | (a_1 - a_2)$ , 若有解则对模  $[m_1, m_2]$  的解数为 1。

证明: 设  $(m_1, m_2) = d$ , 由  $x \equiv a_j \pmod{m_j} (j=1,2)$  可知  $x \equiv a_j \pmod{d} (j=1,2)$ , 因此有  $a_1 - a_2 \equiv 0 \pmod{d}$ , 即  $d | (a_1 - a_2)$ 。

反之, 若  $d | (a_1 - a_2)$ , 由  $x \equiv a_j \pmod{m_j} (j=1,2)$  可设

$$x = k_1 m_1 + a_1, \quad x = k_2 m_2 + a_2$$

则有

$$k_1 m_1 + a_1 = k_2 m_2 + a_2$$

即

$$\frac{a_1 - a_2}{d} = \frac{m_2}{d} k_2 - \frac{m_1}{d} k_1$$

由于  $(\frac{m_2}{d}, \frac{m_1}{d}) = 1$ , 所以一定存在整数  $u, v$ , 使得

$$\frac{m_2}{d} u - \frac{m_1}{d} v = 1$$

取  $k_1 = v \cdot \frac{a_1 - a_2}{d}$ ,  $k_2 = u \cdot \frac{a_1 - a_2}{d}$ , 则不定方程  $\frac{a_1 - a_2}{d} = \frac{m_2}{d} k_2 - \frac{m_1}{d} k_1$  有解,

所以方程  $k_1 m_1 + a_1 = k_2 m_2 + a_2$  也有解, 即方程组  $x \equiv a_j \pmod{m_j} (j=1, 2)$  有解。

下证唯一性。

若方程组  $x \equiv a_j \pmod{m_j} (j=1, 2)$  还有另一解为  $x'$ , 则有

$$x - x' \equiv 0 \pmod{m_1}, \quad x - x' \equiv 0 \pmod{m_2}$$

因此有  $[m_1, m_2] | (x - x')$ , 即  $x \equiv x' \pmod{[m_1, m_2]}$ 。所以原方程组对模  $[m_1, m_2]$  的解数为 1。

7. 求模  $p=13, 23, 37, 41$  的二次剩余, 二次非剩余。

x	1, 12	2, 11	3, 10	4, 9	5, 8	6, 7
$a = x^2 \pmod{13}$	1	4	9	3	12	10

所以, 模 13 的二次剩余为 1, 3, 4, 9, 10, 12, 二次非剩余为 2, 5, 6, 7, 8, 11。

x	1, 22	2, 21	3, 20	4, 19	5, 18	6, 17	7, 16	8, 15
$a = x^2 \pmod{23}$	1	4	9	16	2	13	3	18
x	9, 14	10, 13	11, 12					
$a = x^2 \pmod{23}$	12	8	6					

所以, 模 23 的二次剩余为 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 二次非剩余为 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22。

x	1, 36	2, 35	3, 34	4, 33	5, 32	6, 31	7, 30	8, 29
$a = x^2 \pmod{37}$	1	4	9	16	25	36	12	27
x	9, 28	10, 27	11, 26	12, 25	13, 24	14, 23	15, 22	16, 21
$a = x^2 \pmod{37}$	7	26	10	33	21	11	3	34
x	17, 20	18, 19						
$a = x^2 \pmod{37}$	30	28						

所以, 模 37 的二次剩余为 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 二次非剩余为 2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 31, 35。

x	1, 40	2, 39	3, 38	4, 37	5, 36	6, 35	7, 34	8, 33
---	-------	-------	-------	-------	-------	-------	-------	-------

$a = x^2(\text{mod}41)$	1	4	9	16	25	36	8	23
x	9,32	10,31	11,30	12,29	13,28	14,27	15,26	16,25
$a = x^2(\text{mod}41)$	40	18	39	21	5	32	20	10
x	17,24	18,23	19,22	20,21				
$a = x^2(\text{mod}41)$	2	37	33	31				

所以，模 41 的二次剩余为 1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40 二次非剩余 3, 6, 7, 11, 12, 13, 14, 15, 17, 19, 22, 24, 26, 27, 28, 29, 30, 34, 35, 38。

8. 在不超过 100 的素数  $p$  中，2 是哪些模  $p$  的二次剩余？-2 是哪些模  $p$  的二次剩余？

解：不超过 100 的素数  $p$  有 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97。

当  $p \neq 2$  时， $(2, p) = 1$ ，根据定理 3.2.2，2 是模  $p$  的二次剩余当且仅当  $2^{\frac{p-1}{2}} \equiv 1(\text{mod}p)$ 。依次将  $p$  的值代入验证可得，2 是模 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97 的二次剩余。-2 是模 3, 11, 17, 19, 41, 59, 67, 73, 83, 89, 97 的二次剩余。

9. 证明推论 3.2.1。

证明：推论 3.2.1 设素数  $p > 2$ ， $(p, d_1) = 1$ ， $(p, d_2) = 1$ ，那么

(1) 若  $d_1, d_2$  均为模  $p$  的二次剩余，则  $d_1 d_2$  是模  $p$  的二次剩余；

(2) 若  $d_1, d_2$  均为模  $p$  的二次非剩余，则  $d_1 d_2$  是模  $p$  的二次剩余；

(3) 若  $d_1$  为模  $p$  的二次剩余， $d_2$  为模  $p$  的二次非剩余，则  $d_1 d_2$  是模  $p$  的二次非剩余。

(1) 根据定理 3.2.2， $d_1, d_2$  是模  $p$  的二次剩余，则有  $d_1^{\frac{p-1}{2}} \equiv 1(\text{mod}p)$ ， $d_2^{\frac{p-1}{2}} \equiv 1(\text{mod}p)$ ，因此  $(d_1 d_2)^{\frac{p-1}{2}} \equiv (d_1)^{\frac{p-1}{2}} (d_2)^{\frac{p-1}{2}} \equiv 1(\text{mod}p)$ ，所以  $d_1 d_2$  是模  $p$  的二次剩余。

(2) 根据定理 3.2.2， $d_1, d_2$  是模  $p$  的二次非剩余，则有  $d_1^{\frac{p-1}{2}} \equiv -1(\text{mod}p)$ ， $d_2^{\frac{p-1}{2}} \equiv -1(\text{mod}p)$ ，因此  $(d_1 d_2)^{\frac{p-1}{2}} \equiv (d_1)^{\frac{p-1}{2}} (d_2)^{\frac{p-1}{2}} \equiv 1(\text{mod}p)$ ，所以  $d_1 d_2$  是模  $p$  的二次剩余。

(3) 根据定理 3.2.2， $d_1$  是模  $p$  的二次剩余，则有  $d_1^{\frac{p-1}{2}} \equiv 1(\text{mod}p)$ ， $d_2$  是模  $p$  的二次非剩余，所以  $d_2^{\frac{p-1}{2}} \equiv -1(\text{mod}p)$ ，因此  $(d_1 d_2)^{\frac{p-1}{2}} \equiv (d_1)^{\frac{p-1}{2}} (d_2)^{\frac{p-1}{2}} \equiv -1(\text{mod}p)$ ，所以  $d_1 d_2$  是模  $p$  的二次非剩余。

10. 计算下列 Legendre 符号：

$$\left(\frac{13}{47}\right), \left(\frac{30}{53}\right), \left(\frac{71}{73}\right), \left(\frac{-35}{97}\right), \left(\frac{-23}{131}\right), \left(\frac{7}{223}\right), \left(\frac{-105}{223}\right), \left(\frac{91}{563}\right), \left(\frac{-70}{571}\right), \left(\frac{-286}{647}\right)。$$

$$\text{解：} \left(\frac{13}{47}\right) = (-1)^{\frac{13-1}{2} \frac{47-1}{2}} \left(\frac{47}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{2}{13}\right)^3 = -1$$

$$\begin{aligned}
\left(\frac{30}{53}\right) &= \left(\frac{2}{53}\right)\left(\frac{3}{53}\right)\left(\frac{5}{53}\right) \\
&= (-1)^{\frac{53^2-1}{8}} \cdot (-1)^{\frac{3-1}{2} \cdot \frac{53-1}{2}} \left(\frac{53}{3}\right) (-1)^{\frac{5-1}{2} \cdot \frac{53-1}{2}} \left(\frac{53}{5}\right) \\
&= \left(\frac{2}{3}\right)\left(\frac{3}{5}\right) \\
&= (-1) (-1) \\
&= 1
\end{aligned}$$

$$\begin{aligned}
\left(\frac{71}{73}\right) &= (-1)^{\frac{71-1}{2} \cdot \frac{73-1}{2}} \left(\frac{73}{71}\right) \\
&= \left(\frac{2}{71}\right) \\
&= (-1)^{\frac{71^2-1}{8}} \\
&= 1
\end{aligned}$$

$$\begin{aligned}
\left(\frac{-35}{97}\right) &= \left(\frac{-1}{97}\right)\left(\frac{5}{97}\right)\left(\frac{7}{97}\right) \\
&= (-1)^{\frac{97-1}{2}} \cdot (-1)^{\frac{5-1}{2} \cdot \frac{97-1}{2}} \left(\frac{97}{5}\right) (-1)^{\frac{7-1}{2} \cdot \frac{97-1}{2}} \left(\frac{97}{7}\right) \\
&= \left(\frac{2}{5}\right)\left(\frac{-1}{7}\right) \\
&= (-1) (-1) \\
&= 1
\end{aligned}$$

$$\begin{aligned}
\left(\frac{-23}{131}\right) &= \left(\frac{-1}{131}\right)\left(\frac{23}{131}\right) \\
&= (-1)^{\frac{131-1}{2}} \cdot (-1)^{\frac{23-1}{2} \cdot \frac{131-1}{2}} \left(\frac{131}{23}\right) \\
&= \left(\frac{16}{23}\right) \\
&= 1
\end{aligned}$$

$$\begin{aligned}
\left(\frac{7}{223}\right) &= (-1)^{\frac{7-1}{2} \cdot \frac{223-1}{2}} \left(\frac{223}{7}\right) \\
&= (-1) \left(\frac{-1}{7}\right) \\
&= 1
\end{aligned}$$



$$\begin{aligned}
\left(\frac{-105}{223}\right) &= \left(\frac{-1}{223}\right)\left(\frac{3}{223}\right)\left(\frac{5}{223}\right)\left(\frac{7}{223}\right) \\
&= (-1)^{\frac{223-1}{2}} \cdot (-1)^{\frac{3-1}{2} \cdot \frac{223-1}{2}} \left(\frac{223}{3}\right) (-1)^{\frac{5-1}{2} \cdot \frac{223-1}{2}} \left(\frac{223}{5}\right) (-1)^{\frac{7-1}{2} \cdot \frac{223-1}{2}} \left(\frac{223}{7}\right) \\
&= (-1) \left(\frac{1}{3}\right) \left(\frac{3}{5}\right) \left(\frac{2}{7}\right) \\
&= -1
\end{aligned}$$

$$\begin{aligned}
\left(\frac{91}{563}\right) &= (-1)^{\frac{91-1}{2} \cdot \frac{563-1}{2}} \left(\frac{563}{91}\right) \\
&= (-1) \left(\frac{17}{91}\right) \\
&= (-1) \left(\frac{6}{17}\right) \\
&= (-1) \left(\frac{2}{17}\right) \left(\frac{3}{17}\right) \\
&= 1
\end{aligned}$$

$$\begin{aligned}
\left(\frac{-70}{571}\right) &= \left(\frac{-1}{571}\right)\left(\frac{2}{571}\right)\left(\frac{5}{571}\right)\left(\frac{7}{571}\right) \\
&= (-1)^{\frac{571-1}{2}} \cdot (-1)^{\frac{571^2-1}{8}} \cdot (-1)^{\frac{5-1}{2} \cdot \frac{571-1}{2}} \left(\frac{1}{5}\right) \cdot (-1)^{\frac{7-1}{2} \cdot \frac{571-1}{2}} \left(\frac{4}{7}\right) \\
&= (-1) \cdot (-1) \cdot 1 \cdot 1 \cdot (-1) \cdot 1 \\
&= -1
\end{aligned}$$

$$\begin{aligned}
\left(\frac{-286}{647}\right) &= \left(\frac{-1}{647}\right)\left(\frac{2}{647}\right)\left(\frac{11}{647}\right)\left(\frac{13}{647}\right) \\
&= (-1)^{\frac{647-1}{2}} \cdot (-1)^{\frac{647^2-1}{8}} \cdot (-1)^{\frac{11-1}{2} \cdot \frac{647-1}{2}} \left(\frac{9}{11}\right) \cdot (-1)^{\frac{13-1}{2} \cdot \frac{647-1}{2}} \left(\frac{10}{13}\right) \\
&= (-1) \cdot 1 \cdot (-1) \cdot 1 \cdot 1 \cdot (-1) \\
&= -1
\end{aligned}$$

11. 证明定理 3.2.3 和 3.2.7。

证明：定理 3.2.2

$$(1) \left(\frac{a}{p}\right) = \left(\frac{p+a}{p}\right).$$

因为  $a \equiv p + a \pmod{p}$ ，所以有  $\left(\frac{a}{p}\right) = \left(\frac{p+a}{p}\right)$ 。

$$(2) \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}.$$

由定理 3.2.2 和勒让德符号的定义可知, 结论显然成立。

$$(3) \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

$$\text{由 (2) 知 } \left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod{p} = (a)^{\frac{p-1}{2}} (b)^{\frac{p-1}{2}} \pmod{p} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

$$(4) \text{ 若 } (a, p) = 1, \text{ 则 } \left(\frac{a^2}{p}\right) = 1.$$

$$\text{由 (3) 可得 } \left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^2 = 1.$$

$$(5) \left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

由 (2) 可直接得出结论。

定理 3.2.7 类似可证。

12. 判断下列同余方程是否有解:

$$(1) x^2 \equiv 7 \pmod{227};$$

要判断该方程是否有解, 即要判断 7 是否为模 227 的平方剩余。由于 227 为奇素数, 所以可以通过计算勒让德符号  $\left(\frac{7}{227}\right)$  来判断 7 是否为模 227 的平方剩

余。由于  $\left(\frac{7}{227}\right) = 1$ , 所以原方程有解。

$$(2) x^2 \equiv 11 \pmod{511};$$

由于  $\left(\frac{11}{511}\right) = -1$ , 所以原方程无解。

$$(3) 11x^2 \equiv -6 \pmod{91};$$

原方程等价于

$$\begin{cases} 11x^2 \equiv -6 \pmod{7} \\ 11x^2 \equiv -6 \pmod{13} \end{cases}, \text{ 即 } \begin{cases} 4x^2 \equiv -6 \pmod{7} \\ 11x^2 \equiv -6 \pmod{13} \end{cases}, \text{ 可变形为 } \begin{cases} x^2 \equiv 2 \pmod{7} \\ x^2 \equiv 3 \pmod{13} \end{cases}$$

由于 2 是模 7 的二次剩余, 3 是模 13 的二次剩余, 所以该方程组有解。因此原方程有解。

$$(4) 5x^2 \equiv -14 \pmod{6193}.$$

原方程等价于

$$\begin{cases} 5x^2 \equiv -14(\text{mod } 11) \\ 5x^2 \equiv -14(\text{mod } 563) \end{cases} \text{ 即 } \begin{cases} x^2 \equiv 6(\text{mod } 11) \\ 5x^2 \equiv -14(\text{mod } 563) \end{cases}$$

由于 2 是模 11 的二次剩余, 3 是模 11 的二次非剩余, 所以 6 不是模 11 的二次剩余, 所以该方程组无解。因此原方程无解。

13. (1) 求以 -3 为其二次剩余的全体素数;  
(2) 求以  $\pm 3$  为其二次剩余的全体素数;  
(3) 求以  $\pm 3$  为其二次非剩余的全体素数;  
(4) 求以 3 为其二次剩余、-3 为二次非剩余的全体素数;  
(5) 求以 3 为其二次非剩余、-3 为二次剩余的全体素数;  
(6) 求  $(100)^2 - 3, (150)^2 + 3$  的素因数分解式。

解: 设  $p$  为奇素数。

(1) 以 -3 为二次剩余, 则有  $\left(\frac{-3}{p}\right) = 1$ , 又

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

而由

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1, & p \equiv 1(\text{mod } 6) \\ \left(\frac{-1}{3}\right) = -1, & p \equiv -1(\text{mod } 6) \end{cases}$$

可知以 -3 为其二次剩余的素数为  $p \equiv 1(\text{mod } 6)$ 。

(2) 以 3 为二次剩余, 则有  $\left(\frac{3}{p}\right) = 1$ , 又

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

由

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1, & p \equiv 1(\text{mod } 6) \\ \left(\frac{-1}{3}\right) = -1, & p \equiv -1(\text{mod } 6) \end{cases} \quad \text{及}$$
$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1(\text{mod } 4) \\ -1, & p \equiv -1(\text{mod } 4) \end{cases}$$

可知,  $\left(\frac{3}{p}\right) = 1$  的充要条件是

$$p \equiv 1(\bmod 4), \quad p \equiv 1(\bmod 6)$$

或

$$p \equiv -1(\bmod 4), \quad p \equiv -1(\bmod 6)$$

而由(1)的结论可知 $\left(\frac{-3}{p}\right) = 1$ 的充要条件为 $p \equiv 1(\bmod 6)$ 。所以同时满足 $\left(\frac{3}{p}\right) = 1$

和 $\left(\frac{-3}{p}\right) = 1$ 的充要条件是

$$p \equiv 1(\bmod 4), \quad p \equiv 1(\bmod 6)$$

利用中国剩余定理可知

$$p \equiv 1(\bmod 12)$$

(3) 以 $\pm 3$ 为其二次非剩余, 则有 $\left(\frac{3}{p}\right) = -1$ ,  $\left(\frac{-3}{p}\right) = -1$ , 又

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

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

而由

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1, & p \equiv 1(\bmod 6) \\ \left(\frac{-1}{3}\right) = -1, & p \equiv -1(\bmod 6) \end{cases} \quad \text{及}$$

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1(\bmod 4) \\ -1, & p \equiv -1(\bmod 4) \end{cases}$$

可知, 同时满足 $\left(\frac{3}{p}\right) = -1$ ,  $\left(\frac{-3}{p}\right) = -1$ 的充要条件是

$$p \equiv 1(\bmod 4), \quad p \equiv -1(\bmod 6)$$

由中国剩余定理可知

$$p \equiv 5(\bmod 12)$$

(4) 以3为其二次剩余、-3为二次非剩余的素数的充要条件为

$$p \equiv -1(\text{mod } 4), \quad p \equiv -1(\text{mod } 6)$$

根据中国剩余定理可知

$$p \equiv -1(\text{mod } 12)$$

(5) 以3为其二次非剩余、-3为二次剩余的素数的充要条件是

$$p \equiv -1(\text{mod } 4), \quad p \equiv 1(\text{mod } 6)$$

根据中国剩余定理可知

$$p \equiv 7(\text{mod } 12)$$

(6) 要求 $100^2 - 3$ 的素因子分解, 则每一个素因子  $p$  都满足  $p \mid 100^2 - 3$ , 而且 3 是模  $p$  的二次剩余。所以有  $p \equiv \pm 1(\text{mod } 12)$ , 因此  $p$  有可能为 11, 13, 37 等。通过尝试可知  $100^2 - 3 = 13 \times 769$ 。

同理,  $150^2 + 3$  的素因子满足  $p \equiv 1(\text{mod } 6)$ , 所以  $150^2 + 3 = 3 \times 13 \times 577$ 。

14. 求以3为其二次非剩余, 2为二次剩余的全体素数(即以3为正的最小二次非剩余的全体素数)。

解: 以 2 为二次非剩余的充要条件是  $p \equiv \pm 1(\text{mod } 8)$ , 以 3 为二次非剩余的充要条件是  $p \equiv \pm 5(\text{mod } 12)$ 。

根据中国剩余定理可知, 以3为其二次非剩余, 2为二次剩余的全体素数满足

$$p \equiv \pm 7(\text{mod } 24)$$

15. 证明下列形式的素数具有无穷多个:

(1)  $8k-1, 8k+3, 8k-3$ ;

(2)  $3k+1, 6k+1, 12k+7, 12k+1$ 。

略(超纲了)。