

第3章 同余方程参考答案

计算证明

1. 求解线性同余方程:

$$(1) 27x \equiv 12 \pmod{15} \quad (2) 24x \equiv 6 \pmod{81}$$

解: (1) 由 $(27, 15) = 3, 3 \mid 12$, 故该方程有3个解. 易知有特解 $x_0 \equiv 1 \pmod{15}$, 则这三个解为 $x \equiv 1 + \frac{15}{3}t \pmod{15}, t = 0, 1, 2$, 即 $x \equiv 1, 6, 11 \pmod{15}$.

(2) 由 $(24, 81) = 3, 3 \mid 6$, 故该方程有3个解. 化简得 $8x \equiv 2 \pmod{27}$ 得特解 $x_0 \equiv 7 \pmod{81}$, 则这三个解为 $x \equiv 7 + \frac{81}{3}t \pmod{81}, t = 0, 1, 2$, 即 $x \equiv 7, 34, 61 \pmod{81}$.

2. 求解线性同余方程组:

$$(1) \begin{cases} x \equiv 9 \pmod{12} \\ x \equiv 6 \pmod{25} \end{cases} \quad (2) \begin{cases} x \equiv 2 \pmod{9} \\ 3x \equiv 4 \pmod{5} \\ 4x \equiv 3 \pmod{7} \end{cases} \quad (3) \begin{cases} 2x \equiv 3 \pmod{5} \\ 4x \equiv 2 \pmod{6} \\ 3x \equiv 2 \pmod{7} \end{cases}$$

$$(4) 91x \equiv 419 \pmod{440} \quad (\text{限制为转化成同余方程组求解, 否则不给分})$$

解: 利用中国剩余定理求解:

$$(1) \text{ 记 } m_1 = 12, m_2 = 25, \text{ 则 } m = m_1 m_2 = 300, M_1 = m_2 = 25, M_2 = m_1 = 12.$$

$$\text{求得: } M'_1 \equiv 25^{-1} \equiv 1 \pmod{12}, M'_2 \equiv 12^{-1} \equiv 23 \pmod{25}.$$

$$\text{故方程组的解为 } x \equiv 1 \times 25 \times 9 + 23 \times 12 \times 6 \equiv 81 \pmod{300}.$$

$$(2) \text{ 首先解同余方程得到: } \begin{cases} x \equiv 2 \pmod{9} \\ 3x \equiv 4 \pmod{5} \\ 4x \equiv 3 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 \pmod{9} \\ x \equiv 3 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}.$$

$$\text{记 } m_1 = 9, m_2 = 5, m_3 = 7, \text{ 则 } m = m_1 m_2 m_3 = 315, M_1 = m_2 m_3 = 35, M_2 = m_1 m_3 = 63, M_3 = m_1 m_2 = 45.$$

$$\text{求得: } M'_1 \equiv 35^{-1} \equiv 8 \pmod{9}, M'_2 \equiv 63^{-1} \equiv 2 \pmod{5}, M'_3 \equiv 45^{-1} \equiv 5 \pmod{7}.$$

$$\text{故方程组的解为 } x \equiv 8 \times 35 \times 2 + 2 \times 63 \times 3 + 5 \times 45 \times 6 \equiv 83 \pmod{315}.$$

$$(3) \text{ 首先解同余方程得到: } \begin{cases} 2x \equiv 3 \pmod{5} \\ 4x \equiv 2 \pmod{6} \\ 3x \equiv 2 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{6} \\ x \equiv 3 \pmod{7} \end{cases} \text{ 或 } \begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 3 \pmod{7} \end{cases}.$$

$$\text{记 } m_1 = 5, m_2 = 6, m_3 = 7, \text{ 则 } m = m_1 m_2 m_3 = 210, M_1 = m_2 m_3 = 42, M_2 = m_1 m_3 = 35, M_3 = m_1 m_2 = 30.$$

$$\text{求得: } M'_1 \equiv 42^{-1} \equiv 3 \pmod{5}, M'_2 \equiv 35^{-1} \equiv 5 \pmod{6}, M'_3 \equiv 30^{-1} \equiv 4 \pmod{7}.$$

$$\text{故方程组的解为 } x \equiv 3 \times 42 \times 4 + 5 \times 35 \times 2 + 4 \times 30 \times 3 \equiv 164 \pmod{210} \text{ 或 } x \equiv 3 \times 42 \times 4 + 5 \times 35 \times 5 + 4 \times 30 \times 3 \equiv 59 \pmod{210}, \text{ 即 } x \equiv 59, 164 \pmod{210}.$$

$$(4) 440 = 2^3 \times 5 \times 11$$

$$91x \equiv 419 \pmod{440} \Leftrightarrow \begin{cases} 91x \equiv 419 & (\text{mod } 8) \\ 91x \equiv 419 & (\text{mod } 5) \\ 91x \equiv 419 & (\text{mod } 11) \end{cases} \Leftrightarrow \begin{cases} 3x \equiv 3 & (\text{mod } 8) \\ x \equiv 4 & (\text{mod } 5) \\ 3x \equiv 1 & (\text{mod } 11) \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 & (\text{mod } 8) \\ x \equiv 4 & (\text{mod } 5) \\ x \equiv 4 & (\text{mod } 11) \end{cases}$$

i. 中国剩余定理直接求解, 不再赘述.

ii. 特殊性求解. 观察到 $\text{mod } 5$ 和 $\text{mod } 11$ 相同, $\begin{cases} x \equiv 1 & (\text{mod } 8) \\ x \equiv 4 & (\text{mod } 5) \\ x \equiv 4 & (\text{mod } 11) \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 & (\text{mod } 8) \\ x \equiv 4 & (\text{mod } 55) \end{cases}$, 设 $x = 8n + 1 = 55m + 4 (m, n \in \mathbb{Z})$, 即 $8n = 55m + 3$, 易知 n 是整数的必要条件是 m 是奇数.

当 $m = 1$ 时, $55m + 3 = 58$ 不满足.

当 $m = 3$ 时, $55m + 3 = 168$ 满足. 得到 $x \equiv 169 \pmod{440}$

3. 使用欧拉判别条件判断 a 是否为 p 的二次剩余 (作答时必要的计算步骤应有体现).

$$(1) a = 2, p = 29 \quad (2) a = 5, p = 2003$$

解: (1) 易知, 29 是奇素数且 $(2, 29) = 1$. $2^{\frac{29-1}{2}} = 2^{14} \equiv -1 \pmod{29}$. 故 2 是 29 的二次非剩余. (计算步骤略)

(2) 易知, 2003 是奇素数且 $(5, 2003) = 1$. $5^{\frac{2003-1}{2}} = 5^{1001} \equiv -1 \pmod{2003}$. 故 5 是 2003 的二次非剩余. (计算步骤略)

4. 求下列符号 (首先判断是 Legendre 符号还是 Jacobi 符号, 再写出计算过程):

$$(1) \left(\frac{313}{401} \right) \quad (2) \left(\frac{191}{397} \right) \quad (3) \left(\frac{151}{373} \right) \quad (4) \left(\frac{313}{2023} \right)$$

解: (1) 401 是质数, 该符号为 Legendre 符号. 313 也是质数.

$$\left(\frac{313}{401} \right) = \left(\frac{88}{313} \right) = \left(\frac{2^3 \cdot 11}{313} \right) = \left(\frac{2}{313} \right) \left(\frac{11}{313} \right) = \left(\frac{2}{313} \right) \left(\frac{5}{11} \right) = \left(\frac{2}{313} \right) \left(\frac{1}{5} \right) = 1$$

(2) 397 是质数, 该符号为 Legendre 符号. 191 也是质数.

$$\left(\frac{191}{397} \right) = \left(\frac{15}{191} \right) = \left(\frac{3}{191} \right) \left(\frac{5}{191} \right) = - \left(\frac{-1}{3} \right) \left(\frac{1}{5} \right) = 1$$

(3) 373 是质数, 该符号为 Legendre 符号. 151 也是质数.

$$\left(\frac{151}{373} \right) = \left(\frac{71}{151} \right) = - \left(\frac{9}{71} \right) = - \left(\frac{3^2}{71} \right) = -1$$

(4) $2023 = 7 \times 17^2$, 该符号为 Jacobi 符号. 313 是质数.

$$\left(\frac{313}{2023} \right) = \left(\frac{313}{7} \right) \left(\frac{313}{17} \right) \left(\frac{313}{17} \right) = \left(\frac{5}{7} \right) = \left(\frac{2}{5} \right) = -1$$

5. 求 $E: y^2 \equiv x^3 + 3x + 2 \pmod{7}$ 的所有点. (注: $\pmod{7}$ 表示 x, y 均在 7 的完全剩余系中, 遍历代入 $x = x_1$ 求对应的 y 的二次剩余的解 y_1 , 则 (x_1, y_1) 是 E 上的点. 另外, 本题不需要考虑有限域上的椭圆曲线无穷远点 O .)

解: 当 $x = 0$ 时, $y^2 \equiv 2 \pmod{7}$, 而 $\left(\frac{2}{7} \right) = 1$ 有解, 解得 $y \equiv \pm 3 \pmod{7}$.

当 $x = 1$ 时, $y^2 \equiv 6 \pmod{7}$, 而 $\left(\frac{6}{7} \right) = -1$ 无解.

当 $x = 2$ 时, $y^2 \equiv 2 \pmod{7}$, 而 $\left(\frac{2}{7} \right) = 1$ 有解, 解得 $y \equiv \pm 3 \pmod{7}$.

当 $x = 3$ 时, $y^2 \equiv 3 \pmod{7}$, 而 $\left(\frac{3}{7}\right) = -1$ 无解.

当 $x = 4$ 时, $y^2 \equiv 1 \pmod{7}$, 而 $\left(\frac{1}{7}\right) = 1$ 有解, 解得 $y \equiv \pm 1 \pmod{7}$.

当 $x = 5$ 时, $y^2 \equiv 2 \pmod{7}$, 而 $\left(\frac{2}{7}\right) = 1$ 有解, 解得 $y \equiv \pm 3 \pmod{7}$.

当 $x = 6$ 时, $y^2 \equiv 5 \pmod{7}$, 而 $\left(\frac{5}{7}\right) = -1$ 无解.

综上所述, E 上共有8个点: $(0, 3), (0, 4), (2, 3), (2, 4), (4, 1), (4, 6), (5, 3), (5, 4)$.

6. 若正整数 b 不被奇素数 p 整除, 求 $\left(\frac{b}{p}\right) + \left(\frac{2b}{p}\right) + \left(\frac{3b}{p}\right) + \cdots + \left(\frac{(p-1)b}{p}\right)$.

解: 原式可化为 $\left(\frac{b}{p}\right) \left(\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) \right)$, 而模 p 的缩系中二次剩余和非二次剩余的个数均为 $\frac{p-1}{2}$, 则原式=0.

7. 证明: 若 p 是奇素数, 则有 $\left(\frac{-3}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{6} \\ -1, & p \equiv -1 \pmod{6} \end{cases}$.

证明 $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{(3-1)(p-1)}{2}} \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$. 易知 $p \equiv 1 \pmod{2}$.

当 $p \equiv 1 \pmod{3}$ 即 $p \equiv 1 \pmod{6}$ 时, $\left(\frac{-3}{p}\right) = \left(\frac{1}{3}\right) = 1$.

当 $p \equiv -1 \pmod{3}$ 即 $p \equiv -1 \pmod{6}$ 时, $\left(\frac{-3}{p}\right) = \left(\frac{-1}{3}\right) = -1$. 证毕.

8. * (选做) 求解同余方程: $f(x) = x^3 + 5x^2 + 9 \equiv 0 \pmod{27}$.

解: 易知 $27 = 3^3$. 导式 $f'(x) = 3x^2 + 10x$.

易知, 同余方程 $f(x) \equiv 0 \pmod{3}$ 的解为 $x \equiv 0, 1 \pmod{3}$

当 $x \equiv 0 \pmod{3}$ 时, $f'(0) = 0$, $(f'(0), 3) = 3 \neq 1$.

当 $x \equiv 1 \pmod{3}$ 时, $f'(1) = 13 \equiv 1 \pmod{3}$, $(f'(1), 3) = 1$. $(f'(1))^{-1} \equiv 1 \pmod{3}$

下面进行递归:

$$\begin{cases} t_1 \equiv -\frac{f(x_1)}{3} ((f'(x_1))^{-1} \pmod{3}) \equiv 1 \pmod{3} \\ x_2 \equiv x_1 + 3t_1 \equiv 4 \pmod{9} \end{cases}$$

$$\begin{cases} t_2 \equiv -\frac{f(x_2)}{3^2} ((f'(x_1))^{-1} \pmod{3}) \equiv 1 \pmod{3} \\ x_2 \equiv x_1 + 3^2 t_2 \equiv 22 \pmod{27} \end{cases}$$

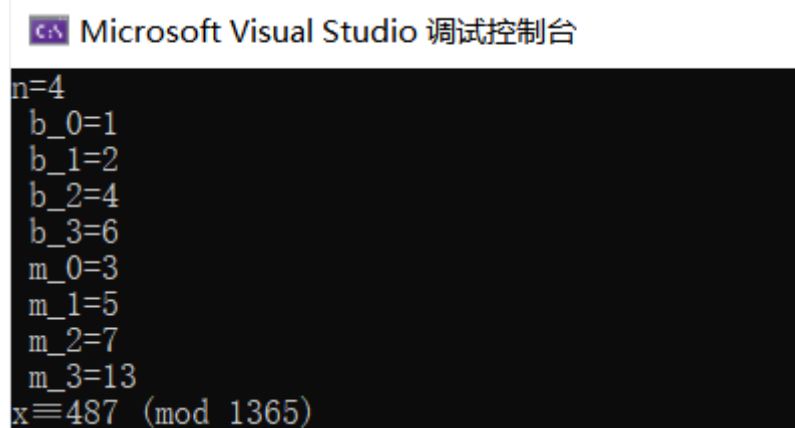
所以原同余方程有解 $x \equiv 13 \pmod{27}$.

另外, 对 $x \equiv 0 \pmod{3}$ 的情况, 进行遍历, 可以得到只有当 $x \equiv 3, 6, 12, 15, 21, 24 \pmod{27}$.

经验证, 该同余方程的解为 $x \equiv 3, 6, 12, 13, 15, 21, 24 \pmod{27}$.

编程练习（基于C/C++）

1. 编程实现中国剩余定理，效果如下图所示（**注意**：实验报告中代码提交的完整性，如自己写的头文件应该说明清楚且给出源码，另外不允许使用第三方封装好的库，需要自己实现）。



```
Microsoft Visual Studio 调试控制台

n=4
b_0=1
b_1=2
b_2=4
b_3=6
m_0=3
m_1=5
m_2=7
m_3=13
x≡487 (mod 1365)
```

```
1  #include<iostream>
2  using namespace std;
3
4  void swap(int& a, int& b)
5  {
6      a = a ^ b;
7      b = a ^ b;
8      a = a ^ b;
9  }
10
11 int extend_Euclid(int a, int b, int& inv_a, int& inv_b)
12 {
13     if (a < b) return extend_Euclid(b, a, inv_b, inv_a);
14     int a0 = a, b0 = b, q = 1;
15     int s0 = 1, s1 = 0, t0 = 0, t1 = 1;
16     while (a % b != 0)
17     {
18         q = a / b;
19         a = a % b;
20         swap(a, b);
21         s0 -= q * s1;
22         swap(s0, s1);
23         t0 -= q * t1;
24         swap(t0, t1);
25     }
26     inv_a = s1 > 0 ? s1 : s1 + b0;
27     inv_b = t1 > 0 ? t1 : t1 + a0;
28     return b;
29 }
30
31 int CRT(int* b, int* m, int n, int& M)
32 {
33     int* Mn = new int[n];
34     int rst = 0;
35     M = 1;
36     for (int i = 0; i < n; i++) M *= m[i];
37     for (int i = 0; i < n; i++) Mn[i] = M / m[i];
```

```

38     for (int i = 0; i < n; i++)
39     {
40         int temp, nop;
41         extend_Euclid(Mn[i], m[i], temp, nop);
42         rst += temp * Mn[i] * b[i];
43     }
44     delete[]Mn;
45     rst %= M;
46     return rst;
47 }
48
49 int main()
50 {
51     int n, M;
52     cout << "n=";
53     cin >> n;
54     int* b = new int[n];
55     int* m = new int[n];
56     for (int i = 0; i < n; i++)
57     {
58         cout << " b_" << i << "=";
59         cin >> b[i];
60     }
61     for (int i = 0; i < n; i++)
62     {
63         cout << " m_" << i << "=";
64         cin >> m[i];
65     }
66     int rst = CRT(b, m, n, M);
67     cout << "x≡" << rst << " (mod " << M << ")";
68     delete[]b;
69     delete[]m;
70     return 0;
71 }

```