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）$27x \equiv 12 \pmod{15}$（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 $x \equiv 1+\dfrac{15}{3}t \pmod{15},\ t=0,1,2$，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$x \equiv 7+\dfrac{81}{3}t \pmod{81},\ t=0,1,2$，即 $x \equiv 7,34,61 \pmod{87}$．

2. 求解线性同余方程组：

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

（4）$91x \equiv 419 \pmod{440}$（**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）记$m_1=12,\ m_2=25$，则$m=m_1m_2=300,\ M_1=m_2=25,\ M_2=m_1=12.$

求得：$M_1' \equiv 25^{-1} \equiv 1 \pmod{12},\ M_2' \equiv 12^{-1} \equiv 23 \pmod{25}$．

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

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

记$m_1=9,\ m_2=5,\ m_3=7$，则$m=m_1m_2m_3=315,\ M_1=m_2m_3=35,\ M_2=m_1m_3=63,\ M_3=m_1m_2=45$．

求得：$M_1' \equiv 35^{-1} \equiv 8 \pmod{9},\ M_2' \equiv 63^{-1} \equiv 2 \pmod{5},\ M_3' \equiv 45^{-1} \equiv 5 \pmod{7}$．

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

记$m_1=5,\ m_2=6,\ m_3=7$，则$m=m_1m_2m_3=210,\ M_1=m_2m_3=42,\ M_2=m_1m_3=35,\ M_3=m_1m_2=30$．

求得：$M_1' \equiv 42^{-1} \equiv 3 \pmod{5},\ M_2' \equiv 35^{-1} \equiv 5 \pmod{6},\ M_3' \equiv 30^{-1} \equiv 4 \pmod{7}$．

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

（4）$440=2^3\times 5\times 11$

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

i. 中国剩余定理直接求解，不再赘述.

ii. 特殊性求解. 观察到 $\bmod\ 5$ 和 $\bmod\ 11$ 相同，$\begin{cases}x\equiv 1 & \pmod 8\\ x\equiv 4 & \pmod 5\\ x\equiv 4 & \pmod{11}\end{cases} \Leftrightarrow \begin{cases}x\equiv 1 & \pmod 8\\ x\equiv 4 & \pmod{55}\end{cases}$，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）$a=2,p=29$ （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) $\left(\dfrac{313}{401}\right)$　　(2) $\left(\dfrac{191}{397}\right)$　　(3) $\left(\dfrac{151}{373}\right)$　　(4) $\left(\dfrac{313}{2023}\right)$

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$\left(\dfrac{2}{7}\right)=1$有解，解得$y\equiv \pm 3 \pmod 7$.

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

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

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

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

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

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

综上所示，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$\left(\dfrac{b}{p}\right)+\left(\dfrac{2b}{p}\right)+\left(\dfrac{3b}{p}\right)+\cdots+\left(\dfrac{(p-1)b}{p}\right)$.

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

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

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

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

当$p\equiv -1 \pmod 3$即$p\equiv -1 \pmod 6$时，$\left(\dfrac{-3}{p}\right)=\left(\dfrac{-1}{3}\right)=-1$. 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$f(x)=0 \pmod 3$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:

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

$$\begin{cases}t_2\equiv -\dfrac{f(x_2)}{3^2}\left((f'(x_1))^{-1} \pmod 3\right)\equiv 1 & \pmod 3\\ x_2\equiv x_1+3^2t_1\equiv 22 & \pmod{27}\end{cases}$$

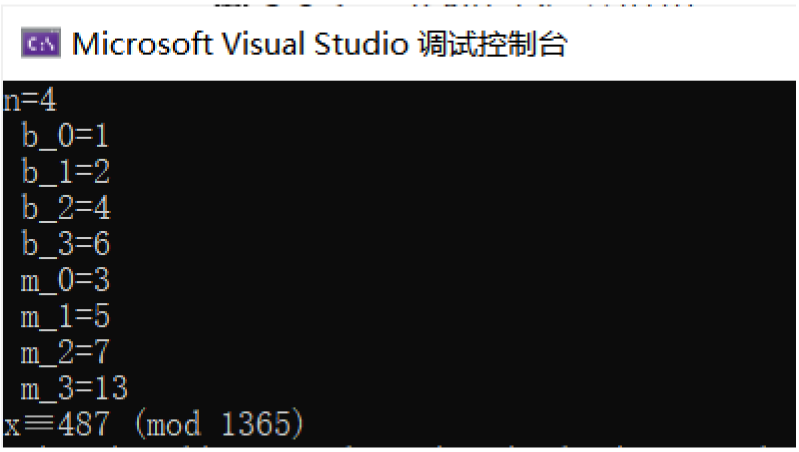
所以原同余方程有解$x\equiv 13 \pmod{27}$.

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）.




```
#include<iostream>
using namespace std;

void swap(int& a, int& b)
{
    a = a ^ b;
    b = a ^ b;
    a = a ^ b;
}

int extend_Euclid(int a, int b, int& inv_a, int& inv_b)
{
    if (a < b)return extend_Euclid(b, a, inv_b, inv_a);
    int a0 = a, b0 = b, q = 1;
    int s0 = 1, s1 = 0, t0 = 0, t1 = 1;
    while (a % b != 0)
    {
        q = a / b;
        a = a % b;
        swap(a, b);
        s0 -= q * s1;
        swap(s0, s1);
        t0 -= q * t1;
        swap(t0, t1);
    }
    inv_a = s1 > 0 ? s1 : s1 + b0;
    inv_b = t1 > 0 ? t1 : t1 + a0;
    return b;
}

int CRT(int* b, int* m, int n, int& M)
{
    int* Mn = new int[n];
    int rst = 0;
    M = 1;
    for (int i = 0; i < n; i++)M *= m[i];
    for (int i = 0; i < n; i++)Mn[i] = M / m[i];
```

```
    for (int i = 0; i < n; i++)
    {
        int temp, nop;
        extend_Euclid(Mn[i], m[i], temp, nop);
        rst += temp * Mn[i] * b[i];
    }
    delete[]Mn;
    rst %= M;
    return rst;
}

int main()
{
    int n, M;
    cout << "n=";
    cin >> n;
    int* b = new int[n];
    int* m = new int[n];
    for (int i = 0; i < n; i++)
    {
        cout << " b_" << i << "=";
        cin >> b[i];
    }
    for (int i = 0; i < n; i++)
    {
        cout << " m_" << i << "=";
        cin >> m[i];
    }
    int rst = CRT(b, m, n, M);
    cout << "x≡" << rst << " (mod " << M << ")";
    delete[]b;
    delete[]m;
    return 0;
}
```