

# 第三章 同余方程

## 计算证明

1. 求解线性同余方程（如果解的个数较多，可以写成通式）：

(1)  $91x \equiv 26 \pmod{169}$

(2)  $24x \equiv 6 \pmod{81}$

2. 求解线性同余方程组：

(1)

$$\begin{cases} x \equiv 9 \pmod{12} \\ x \equiv 6 \pmod{25} \end{cases}$$

(2)

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

(3)

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

3. 求解同余方程  $x^2 + 18x - 823 \equiv 0 \pmod{1800}$ 。

4. 一个数被 3, 5, 7, 11 除所得的余数均为 2, 且为 13 的倍数, 求出符合上述条件的最小正整数。

5. 求满足方程  $E: y^2 = x^3 - 3x + 2 \pmod{7}$  的所有点（本题不需要考虑有限域上的椭圆曲线无穷远点  $O$ ）。

6. 求出同余方程  $x^2 \equiv 8 \pmod{287}$  的所有解。

7. 计算以下符号（首先判断是 Legendre 符号还是 Jacobi 符号, 再写出计算过程）：

(1)  $\left(\frac{17}{37}\right)$ ;

(2)  $\left(\frac{51}{71}\right)$ ;

(3)  $\left(\frac{313}{401}\right)$ ;

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

8. 证明若正整数  $b$  不被奇素数  $p$  整除, 则:  $\left(\frac{b}{p}\right) + \left(\frac{2b}{p}\right) + \left(\frac{3b}{p}\right) + \dots + \left(\frac{(p-1)b}{p}\right) = 0$ 。

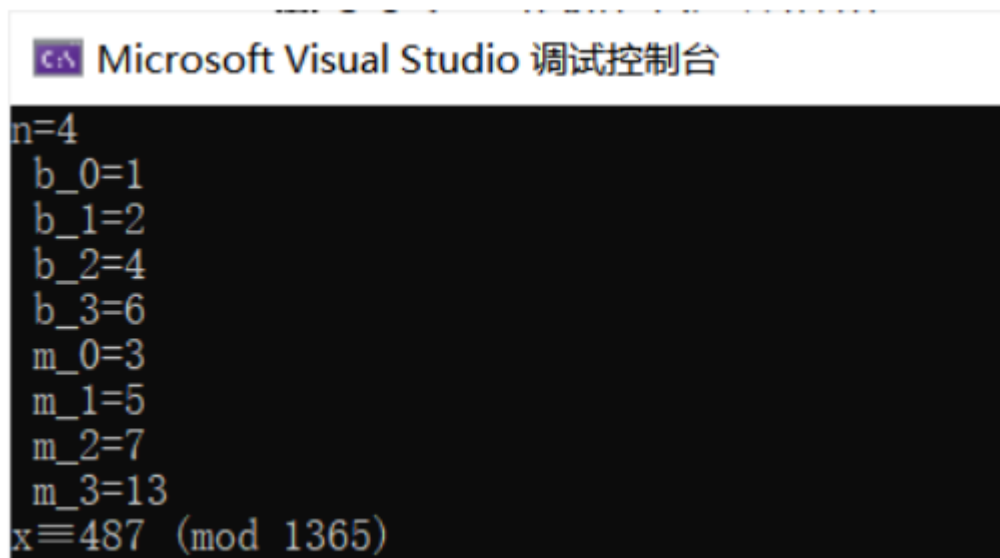
9. 设  $p$  是奇素数, 证明  $x^2 \equiv 3(mod\ p)$  有解的充要条件是  $p \equiv \pm 1(mod\ 12)$ 。
10. 证明: 若  $p$  是奇素数, 则

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

- \*11. 判断同余方程  $x^2 \equiv 191(mod\ 397)$  是否有解。

## 编程练习 (基于C/C++)

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)。



```
C# 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)
```