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) $91x \equiv 26(mod\ 169)$ $x \equiv 4+13t(mod\ 169), t=0,1,...,11,12$
   (2) $24x \equiv 6(mod\ 81)$ $x \equiv 7,34,61(mod\ 81)$
2. 求解线性同余方程组：
   (1)
   $$\begin{cases} x \equiv 9(mod\ 12) \\ x \equiv 6(mod\ 25) \end{cases}$$
   $x \equiv 81(mod\ 300)$
   (2)
   $$\begin{cases} x \equiv 2(mod\ 9) \\ 3x \equiv 4(mod\ 5) \\ 4x \equiv 3(mod\ 7) \end{cases}$$
   $x \equiv 83(mod\ 315)$
   (3)
   $$\begin{cases} 2x \equiv 3(mod\ 5) \\ 4x \equiv 2(mod\ 6) \\ 3x \equiv 2(mod\ 7) \end{cases}$$
   $x \equiv 59,164(mod\ 210)$
3. 求解同余方程 $x^2+18x-823 \equiv 0(mod\ 1800)$。
   $x \equiv 43,439,443,839,943,1339,1343,1739(mod\ 1800)$
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。
   $x \equiv 1157(mod\ 15015)$
   所以 $x=1157$

5. 求满足方程 $E: y^2=x^3-3x+2(mod\ 7)$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）。
$(0,3),(0,4),(1,0),(2,2),(2,5),(5,0),(6,2),(6,5)$
6. 求出同余方程 $x^2\equiv 8(mod\ 287)$ 的所有解。
$x\equiv 34,48,239,253(mod\ 287)$
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)$(\frac{17}{37})$； $L\quad -1$
(2)$(\frac{51}{71})$； $L\quad -1$
(3)$(\frac{313}{401})$； $L\quad 1$
(4)$(\frac{151}{373})$； $L\quad -1$
8. 证明若正整数 b 不被奇素数 p 整除，则：$(\frac{b}{p})+(\frac{2b}{p})+(\frac{3b}{p})+...+(\frac{(p-1)b}{p})=0$。

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.

9. 设 p 是奇素数，证明 $x^2\equiv 3(mod\ p)$有解的充要条件是 $p\equiv\pm1(mod\ 12)$。
同课本72页B组11题
10. 证明：若 p 是奇素数，则

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

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.

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

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)
```