第3章 同余方程

计算证明

1. 求解线性同余方程：

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

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**）

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）$a = 5, p = 2003$

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）$\left(\dfrac{313}{2023}\right)$

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.）

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

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

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

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）.