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) $91x \equiv 26(mod\,169)$
   (2) $24x \equiv 6(mod\,81)$
2. 求解线性同余方程组：
   (1)
$$\begin{cases} x \equiv 9(mod\,12) \\ x \equiv 6(mod\,25) \end{cases}$$
   (2)
$$\begin{cases} x \equiv 2(mod\,9) \\ 3x \equiv 4(mod\,5) \\ 4x \equiv 3(mod\,7) \end{cases}$$
   (3)
$$\begin{cases} 2x \equiv 3(mod\,5) \\ 4x \equiv 2(mod\,6) \\ 3x \equiv 2(mod\,7) \end{cases}$$
3. 求解同余方程 $x^2 + 18x - 823 \equiv 0(mod\,1800)$。
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。
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）。
6. 求出同余方程 $x^2 \equiv 8(mod\,287)$ 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)$(\frac{17}{37})$;
   (2)$(\frac{51}{71})$;
   (3)$(\frac{313}{401})$;
   (4)$(\frac{151}{373})$;
8. 证明若正整数 b 不被奇素数 p 整除，则：$(\frac{b}{p}) + (\frac{2b}{p}) + (\frac{3b}{p}) + ... + (\frac{(p-1)b}{p}) = 0$。

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

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

*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）。