第3章习题

3.1 原根

解答题

1. 34对模37的次数是多少？

2. 2^{12}对模37的次数是多少？

3. 2是模61的一个原根，利用这个事实，在小于61的正整数中，找到所有次数为4的整数.

4. 47, 55, 59的原根是否存在？若存在则求出其所有的原根.

5. 求113的最小原根.

6. 已知2是19的原根，构造19的指数表并求出如下方程的**最小正剩余解**：
(1) $8x^4 \equiv 3 \pmod{19}$；
(2) $5x^3 \equiv 2 \pmod{19}$；
(3) $x^7 \equiv 1 \pmod{19}$.

7. 求解同余方程$x^{22} \equiv 5 \pmod{41}$.

证明题

1. 设$ab \equiv 1 \pmod{m}$，求证$\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

2. 设$m > 1$，$(a, m) = 1$，如果$\mathrm{ord}_m(a) = st$，证明$\mathrm{ord}_m(a^s) = t$.

3. 求证如果g^k是m的原根，那么g也是m的原根.

4. 如果a, b, m是正整数，a, b分别与m互素，且满足$(\text{ord}_m(a), \text{ord}_m(b)) = 1$，证明$\text{ord}_m(ab) = \text{ord}_m(a) \cdot \text{ord}_m(b)$.

5. 证明整数12没有原根.

*6. 证明$\text{ord}_{F_n}(2) \leq 2^{n+1}$，其中$F_n = 2^{2^n} + 1$是第$n$个费马数.

*7. 令p是费马数$F_n = 2^{2^n} + 1$的一个素因子，

(1) 证明$\text{ord}_p(2) = 2^{n+1}$.

(2) 证明p一定形如$2^{n+1}k + 1$.

8. 证明：如果p是一个以g为原根的奇素数，那么$\text{ind}_g(p-1) = (p-1)/2$.

练习题

1. 编写求解奇素数原根的程序.

2. 编写构造指数表的程序.

3.2 二次剩余

解答题

1. 利用欧拉判别条件判断2是否为29的二次剩余.

2. 设p为奇素数，求-1是模p的二次剩余的充要条件.

3. 判断同余方程$x^2 \equiv 191 \pmod{397}$是否有解.

4. 判断同余方程$x^2 \equiv 11 \pmod{511}$是否有解.

5. 求解同余方程$x^2 \equiv 2 \pmod{73}$.

6. 是否存在正整数n使得n^2-3是313的倍数？

7. 计算以下勒让德符号(写出计算过程)：

(1) $\left(\frac{17}{37}\right)$；

(2) $\left(\frac{151}{373}\right)$；

(3) $\left(\frac{191}{397}\right)$；

(4) $\left(\frac{911}{2003}\right)$；

(5) $\left(\frac{37}{20040803}\right)$.

8. 求出所有以5为二次剩余的奇素数p.

9. 不解方程，求满足方程$E:\ y^2 = x^3 - 3x + 10 \pmod{23}$的点的个数.

10. 计算以下雅可比符号(写出计算过程)：

(1) $\left(\frac{51}{71}\right)$；

(2) $\left(\frac{35}{97}\right)$；

(3) $\left(\frac{313}{401}\right)$；

(4) $\left(\frac{165}{503}\right)$.

证明题

1. 设p是奇素数，证明$x^2 \equiv 3 \pmod{p}$有解的充要条件是$p \equiv \pm 1 \pmod{12}$.

2. 证明若$p \equiv 1 \pmod{5}$，则5是模p的二次剩余.

3. 证明：若正整数b不被奇素数p整除，则

$$\left(\frac{b}{p}\right)+\left(\frac{2b}{p}\right)+\left(\frac{3b}{p}\right)+\cdots+\left(\frac{(p-1)b}{p}\right)=0.$$

4. 证明：若p是奇素数，则

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

*5. 证明：若p是素数且$p\geq 7$，则p总有两个差为2的二次剩余.

练习题

1. 编写计算勒让德符号.

2. 编程计算雅可比符号.