第3章习题

3.1 原根

解答题

1. 34对模37的次数是多少？

解：$\varphi(37)=36$，36的非平凡因子有2,3,4,6,9,12,18. 依次检验可知$34^9\equiv 1 \pmod{37}$.

2. 2^{12}对模37的次数是多少？

解：$2^{36}\equiv(2^{12})^3\equiv 1 \pmod{37}$，3没有非平凡因子.

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.

解：$x^4\equiv 1 \pmod{61}$，$(x^2+1)(x^2-1)\equiv 0 \pmod{61}$. 由于$x$的次数为4，那么只能有$x^2\equiv -1 \pmod{61}$. 注意到$2^{60}\equiv 1 \pmod{61}$，明显有$(2^{15})^4\equiv 11^4\equiv 1 \pmod{61}$，而$11^2\equiv -1 \pmod{61}$，于是11的次数是4. 另外马上可知50是另一个满足条件的整数.

4. 47,55,59的原根是否存在？若存在则求出其所有的原根.

解：判断方法：参照教材(机械工业出版社)定理4.2.11，求原根的方法：参照定理4.2.12和例4.2.5.

47的原根为5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45；

55不存在原根；

59的原根为2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56.

5. 求113的最小原根.

解：参照定理4.2.12和例4.2.5. 113的最小原根为3.

6. 已知2是19的原根，构造19的指数表并求出如下方程的解：

(1) $8x^4 \equiv 3 \pmod{19}$；

(2) $5x^3 \equiv 2 \pmod{19}$；

(3) $x^7 \equiv 1 \pmod{19}$.

解：指数表构造方法参照教材(机械工业出版社)例4.3.1.

	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

(1) $x^4 \equiv 17 \pmod{19} \Rightarrow 4\mathbf{ind}_g x \equiv 10 \pmod{18}$，解得$\mathbf{ind}_g x \equiv 7, 16 \pmod{18}$，查表可得$x \equiv 5, 14 \pmod{19}$

(2) $x \equiv 2, 3, 14 \pmod{19}$

(3) $x \equiv 1 \pmod{19}$

7. 求解同余方程$x^{22} \equiv 5 \pmod{41}$.

解：查例4.3.1中的指数表可得$22\mathrm{ind}_g x \equiv 22 \pmod{40}$，解得$\mathrm{ind}_g x \equiv 1, 21 \pmod{40}$，从而查表有$x \equiv 6, 35 \pmod{41}$.

证明题

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

证明：$(ab)^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} b^{\mathrm{ord}_m(a)} \equiv 1 \pmod{m}$. 已知$a^{\mathrm{ord}_m(a)} \equiv 1 \pmod{m}$，那么有$b^{\mathrm{ord}_m(a)} \equiv 1 \pmod{m}$. 又知$b^{\mathrm{ord}_m(b)} \equiv 1 \pmod{m}$，从而有$\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$. 同理可得$\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$，故$\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

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

证明：教材(机械工业出版社)定理4.1.5.

$$\mathrm{ord}_m(a^s) = \frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), s)} = \frac{st}{(st, s)} = \frac{st}{s} = t$$

3. 求证如果g^k是m的原根，那么g也是m的原根.

证明：因为g^k是m的原根，所以有$\text{ord}_m(g^k) = \varphi(m)$. 易知$\text{ord}_m(g) \mid \varphi(m)$. 又有$g^{\text{ord}_m(g)k} \equiv (g^k)^{\text{ord}_m(g)} \equiv 1 \pmod m$，从而有$\text{ord}_m(g^k) \mid \text{ord}_m(g)$，即$\varphi(m) \mid \text{ord}_m(g)$. 综上，有$\text{ord}_m(g) = \varphi(m)$.

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$\text{ord}_m(ab) = \text{ord}_m(a) \cdot \text{ord}_m(b)$.

证明：教材(机械工业出版社)定理4.2.4.

5. 证明整数12没有原根.

证明：(i) 参照教材(机械工业出版社)定理4.2.11，$12 = 2^2 \times 3$，不符合$2, 4, p^l, 2p^l$ 的形式.

(ii) 只有1,5,7,11与12互素，他们的次数是1或2，而$\varphi(12) = 4$.

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.

证明：易知$2^{2^n} + 1 \equiv 0 \pmod{F_n} \Rightarrow 2^{2^n} \equiv -1 \pmod{F_n}$. 将同余式两边平方，有$(2^{2^n})^2 \equiv 1 \pmod{F_n}$，即$2^{2^{n+1}} \equiv 1 \pmod{F_n}$，从而有$\text{ord}_{F_n}(2) \leq 2^{n+1}$.

7*. 令p是费马数$F_n = 2^{2^n} + 1$的一个素因子，证明：

(1) $\text{ord}_p(2) = 2^{n+1}$；

(2) p一定形如$2^{n+1}k+1$.

证明：

(1) 令$d=\text{ord}_p(2)$. 注意到$2^{2^n}\equiv -1 \pmod{F_n}$，那么有$2^{2^n}\equiv -1 \pmod{p}$，所以$(2^{2^n})^2\equiv 2^{2^{n+1}}\equiv 1 \pmod{p}$，于是有$d\mid 2^{n+1}$. 也就是说$d$可表示为$d=2^k$的形式，且$k\le n+1$. 然而当$k<n+1$时，有$2^d\equiv 2^{2^k}\equiv 1 \pmod{p}\Rightarrow 2^{2^n}\equiv 1 \pmod{p}$，矛盾. 故$k=n+1$，即$d=2^{n+1}$.

(2) $2^{n+1}=\text{ord}_p(2)\mid\varphi(p)=p-1$，所以有$p=2^{n+1}k+1$.

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

证明： $g^{p-1}\equiv (g^{(p-1)/2})^2\equiv 1 \pmod{p}$. 因为$g$是原根，所以$p-1$是使得$g^l\equiv 1 \pmod{p}$成立的最小的$l$. 于是可知$g^{(p-1)/2} \pmod{p}$不可能为1，只能有$g^{(p-1)/2}\equiv -1\equiv p-1 \pmod{p}$. 故$\text{ind}_g(p-1)=(p-1)/2$.

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.

解：$2^{\frac{29-1}{2}} \equiv -1 \pmod{29}$

2. 设p为奇素数，求-1是模p的二次剩余的充要条件.

解：$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p \equiv 1 \pmod 4$

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

解：

$$\begin{aligned}
\left(\frac{191}{397}\right) &= (-1)^{\frac{191-1}{2}\frac{397-1}{2}}\left(\frac{397}{191}\right) \\
&= \left(\frac{397}{191}\right) = \left(\frac{15}{191}\right) = \left(\frac{3}{191}\right)\left(\frac{5}{191}\right) \\
&= -\left(\frac{-1}{3}\right)\left(\frac{1}{5}\right) \\
&= 1
\end{aligned}$$

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

解：$\left(\frac{11}{511}\right) = -\left(\frac{5}{11}\right) = -\left(\frac{11}{5}\right) = -1$

5. 求解同余方程$x^2 \equiv 2 \pmod{73}$.

解：$\left(\frac{2}{73}\right) = (-1)^{\frac{73^2-1}{8}} = 1$，有解. 观察可知$9^2 \equiv 8 \pmod{73}$，又有$4x^2 \equiv (2x)^2 \equiv 8 \pmod{73}$，从而可知满足$2x \equiv 9 \pmod{73}$的$x$是原方程的一个解，可求出$x \equiv 41 \pmod{73}$，那么另一个解为$x \equiv -41 \equiv 32 \pmod{73}$.

6. 是否存在正整数n使得$n^2 - 3$是313的倍数？

解：即判断同余方程$n^2 \equiv 3 \pmod{313}$是否有解. $\left(\frac{3}{313}\right) = 1$

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

解：

(1) -1；(2) -1；(3) 1；(4) 1；(5) 1.

8. 求出所有以5为二次剩余的奇素数p.

解：

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\frac{p-1}{2}}\left(\frac{p}{5}\right) = (-1)^{p-1}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

$p \equiv 1, 4 \pmod{5}$时，$\left(\frac{p}{5}\right) = 1$.

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

解：见下表.

x	$x^3 - 3x + 10 \pmod{23}$	$x^3 - 3x + 10$是否为二次剩余	点的个数
0	10		
1	8	✓	2
2	12	✓	2
3	5		
4	16	✓	2
5	5		
6	1	✓	2
7	10		
8	15		
9	22		
10	14		
11	20		
12	0	*	1
13	6	✓	2
14	21		
15	5		
16	10		
17	19		
18	15		
19	4	✓	2
20	15		
21	8	✓	2
22	12	✓	2

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

解：(1) -1;　(2) 1;　(3) 1;　(4) -1.

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$p \equiv \pm 1 \pmod{12}$.

证明：方程有解$\Leftrightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4, p \equiv 1 \pmod 3$或$p \equiv -1 \pmod 4, p \equiv -1 \pmod 3 \Leftrightarrow p \equiv \pm 1 \pmod{12}$.

2. 证明若$p \equiv 1 \pmod 5$，则5是模p的二次剩余，其中p是奇素数.

证明：

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\frac{p-1}{2}}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

$p \equiv 1 \pmod 5$时，$\left(\frac{5}{p}\right) = 1$.

3. 证明：若正整数b不被奇素数p整除，则

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

证明：原式可化为

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

模p的缩系中二次剩余和非二次剩余各有$(p-1)/2$个.

4. 证明：若p是奇素数，则

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

证明：

$$\begin{aligned}\left(\frac{-3}{p}\right)&=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right)\\&=(-1)^{p-1}\left(\frac{p}{3}\right)=\left(\frac{p}{3}\right)\end{aligned}$$

已知$p\equiv 1 \pmod 2$. 当$p\equiv 1 \pmod 3$即$p\equiv 1 \pmod 6$时，$\left(\frac{-3}{p}\right)=1$；当$p\equiv -1 \pmod 3$即$p\equiv -1 \pmod 6$时，$\left(\frac{-3}{p}\right)=-1$.

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.

证明：显然1和4是p的二次剩余. 如果2或3是，那么得证；如果2和3都不是，那么6一定是，因为此时$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=(-1)(-1)=1$，从而得证.