

# 第四章 原根和指数

## 计算证明

- 1. 求 $2^{12}$ 对模37的次数。
- 2. 求模61的最小非负完系中所有次数为4的整数。
- 3. 设 $ab \equiv 1(mod\ m)$ , 求证:  $ord_m(a) = ord_m(b)$ 。
- 4. 设a、b、m是正整数, 如果a、b分别与m互素, 且满足 $(ord_m(a), ord_m(b)) = 1$ , 证明:  $ord_m(ab) = ord_m(a) * ord_m(b)$ 。
- 5. 判断55、103的原根是否存在? 若存在则求出其最小原根。
- 6. 求出47的所有原根。
- 7. 已知2是19的原根, 构造19的指数表并求解:
  - (1)  $8x^4 \equiv 3(mod\ 19)$
  - (2)  $5x^3 \equiv 2(mod\ 19)$
  - (3)  $x^7 \equiv 1(mod\ 19)$
- 8. (1) 若 $g^k$ 是m的原根, 求证: g是m的原根。  
(2) 若p是一个以g为原根的奇素数, 求证:  $ind_g(p-1) = \frac{p-1}{2}$
- 9. 设p是费马数 $F_n = 2^{2^n} + 1$ 的一个素因子, 求证:
  - (1)  $ord_p(2) = 2^{n+1}$ ;
  - (2) p一定形如 $2^{n+1}k + 1$ 。
  - (3) \*当n>1时, p一定形如 $2^{n+2}t + 1$
- 10. 求以下整数的最小原根
  - (1)  $5^2$           (2) 6

## 编程练习 (基于C/C++)

编程实现求解最小原根并基于最小原根构造指数表, 效果如下图所示。

```
Please input n(n>0): 103
The min primitive root of 103: g=5
The ind_table of 103 based on g=5 is:
      0      1      2      3      4      5      6      7      8      9
0      -      0     44     39     88      1     83      4     30     78
1     45     61     25     72     48     40     74     70     20     80
2     89     43      3     24     69      2     14     15     92     86
3     84     57     16    100     12      5     64     93     22      9
4     31     50     87     77     47     79     68     85     11      8
5     46      7     58     97     59     62     34     17     28     98
6     26     36    101     82     60     73     42     13     56     63
7     49     67      6     33     35     41     66     65     53     18
8     75     54     94     38     29     71     19     23     91     99
9     21     76     10     96     27     81     55     32     52     37
10    90     95     51      -      -      -      -      -      -      -
```

Please input  $n(n>0)$ : 169

The min primitive root of 169:  $g=2$

The ind\_table of 169 based on  $g=2$  is:

	0	1	2	3	4	5	6	7	8	9
0	-	0	1	124	2	9	125	107	3	92
1	10	103	126	-	108	133	4	146	93	65
2	11	75	104	130	127	18	-	60	109	40
3	134	21	5	71	147	116	94	151	66	-
4	12	85	76	122	105	101	131	63	128	58
5	19	114	-	120	61	112	110	33	41	35
6	135	140	22	43	6	-	72	37	148	98
7	117	137	95	51	152	142	67	54	-	24
8	13	28	86	45	77	155	123	8	106	91
9	102	-	132	145	64	74	129	17	59	39
10	20	70	115	150	-	84	121	100	62	57
11	113	119	111	32	34	139	42	-	36	97
12	136	50	141	53	23	27	44	154	7	90
13	-	144	73	16	38	69	149	83	99	56
14	118	31	138	-	96	49	52	26	153	89
15	143	15	68	82	55	30	-	48	25	88
16	14	81	29	47	87	80	46	79	78	-