

信息安全数学基础

陈恭亮

上海交通大学信息安全工程学院

电话: 021-62933387, email: chengl@sjtu.edu.cn

2004 年 9 月 4 日

目 录

第一章 整数的可除性	3
§1.1 整除的概念 欧几里得除法	4
§1.2 整数的表示	23
§1.3 最大公因数与广义欧几里得除法	30
§1.4 整除的进一步性质及最小公倍数	57
§1.5 素数 算术基本定理	63
第二章 同余	71
§2.1 同余的概念及基本性质	72
§2.2 剩余类及完全剩余系	79
§2.3 简化剩余系与欧拉函数	86
§2.4 欧拉定理 费马小定理	96
§2.5 模重复平方算法	103
第三章 同余式	107
§3.1 基本概念及一次同余式	108
§3.2 中国剩余定理	115
§3.3 高次同余式的解数及解法	127
§3.4 素数模的同余式	132
第四章 二次同余式与平方剩余	141
§4.1 一般二次同余式	142
§4.2 模为奇素数的平方剩余与平方非剩余	146
§4.3 勒让得符号	150
§4.4 二次互反律的证明	158
§4.5 雅可比符号	162
§4.6 模 p 平方根	167

第五章	原根与指标	175
§5.1	指数及其基本性质	176
§5.2	原根存在的条件	195
§5.3	指标及 n 次剩余	210
第六章	素性检验	223
§6.1	拟素数	224
§6.2	Euler 拟素数	235
§6.3	强拟素数	238
第七章	连分数	241
§7.1	连分数	243
§7.2	简单连分数	253
§7.3	循环周期连分数	265
§7.4	最佳逼近	268
第八章	群	271
§8.1	群	272
§8.2	同态和同构	291
§8.3	商群	295
第九章	群的结构	303
§9.1	循环群	304
§9.2	有限生成交换群	308
§9.3	置换群	311
第十章	环	323
§10.1	环和同态	324
§10.2	分式域	336
§10.3	理想	339
§10.4	多项式环	351

第十一章	域和 Galois 理论	369
§11.1	域的扩张	370
§11.2	基本定理	383
§11.3	可分域 代数闭包	386
第十二章	域的结构	389
§12.1	超越基	390
§12.2	有限域的构造	392
第十三章	椭圆曲线	403
§13.1	椭圆曲线基本概念	404
§13.2	加法原理	410
§13.3	有限域上的椭圆曲线	429

第一章 整数的可除性

本章主要讲述如下问题：

1. 整除 因数 倍数
2. 素数 合数
3. 厄拉托塞师 (Eratosthenes) 筛法
4. 欧 里得除法 不完全商 余数
5. 整数的 b - 进制表示
6. 最大公因数
7. 广义欧 里得除法
8. 整数的性质 最小公倍数
9. 算术基本定理
10. 素数定理

本节考虑关于整数的基本概念和性质：整除和欧几里得除法。

*** 定义 1** 设 a, b 是任意两个整数，其中 $b \neq 0$. 如果存在一个整数 q 使得等式

$$a = bq \quad (1)$$

成立，就称 b **整除** a 或者 a 被 b 整除，记作 $b|a$, 并把 b 叫做 a 的 **因数**, 把 a 叫做 b 的 **倍数**. 这时， q 也是 a 的因数，常将 q 写成 a/b 或 $\frac{a}{b}$. 否则，就称 b 不能整除 a 或者 a 不能被 b 整除，记作 $b \nmid a$.

注 1 整除定义仅与乘法运算有关，与小学整除定义有极大区别。

注 2 本整除定义可推广为现代数学的整除定义。

注 3 当 b 遍历整数 a 的所有因数时, $-b$ 遍历整数 a 的所有因数.

注 4 当 b 遍历整数 a 的所有因数时, a/b 遍历整数 a 的所有因数.

*** 例 1** $30 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6$.

有 2, 3, 5 分别整除 30 或 30 被 2, 3, 5 分别整除, 记作 $2|30$, $3|30$, $5|30$. 这时, 2, 3, 5 都是 30 的因数, 30 是 2, 3, 5 的倍数.

30 的所有因数是 $\{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}$, 或是 $\{\mp 1, \mp 2, \mp 3, \mp 5, \mp 6, \mp 10, \mp 15, \mp 30\}$, 或是 $\{\pm 30 = 30/\pm 1, \pm 15 = 30/\pm 2, \pm 10 = 30/\pm 3, \pm 6 = 30/\pm 5, \pm 5 = 30/\pm 6, \pm 3 = 30/\pm 10, \pm 2 = 30/\pm 15, \pm 1 = 30/\pm 30\}$.

又例如: $7|84$, $-7|84$, $5|20$, $19|171$, $3 \nmid 8$, $5 \nmid 12$, $13|0$, $11|11$.

*** 0 是任何非零整数的倍数. 1 是任何整数的因数. 任何非零整数 a 是其自身的的倍数, 也是其自身的因数.**

例 2 设 a, b 为整数. 若 $b|a$, 则 $b|(-a)$, $(-b)|a$, $(-b)|(-a)$.

证 设 $b|a$, 则存在整数 q 使得 $a = bq$. 因而,

$$(-a) = b(-q), \quad a = (-b)(-q), \quad (-a) = (-b)q.$$

因为 $-q, q$ 都是整数, 根据整除的定义, 有 $b|(-a)$, $(-b)|a$, $(-b)|(-a)$.

*** 定理 1** 设 $a, b \neq 0, c \neq 0$ 是整数. 若 $c|b, b|a$, 则 $c|a$. (**传递性**)

证 设 $c|b, b|a$, 根据整除的定义, 分别存在整数 q_1, q_2 使得

$b = cq_1, \quad a = bq_2$. 因此, 我们有

$$a = bq_2 = (cq_1)q_2 = cq.$$

因为 $q = q_1q_2$ 是整数, 所以根据整除的定义, 有 $c|a$.

注 数学证明的表述.

*** 例 3** 因为 $7|42, 42|84$, 所以 $7|84$.

定理 2 设 $a, b, c \neq 0$ 是整数. 若 $c|a, c|b$, 则 $c|a \pm b$. (**加法运算**)

证 设 $c|a, c|b$, 那么存在整数 q_1, q_2 分别使得 $a = cq_1, b = cq_2$.

因此, $a \pm b = cq_1 \pm cq_2 = c(q_1 \pm q_2)$.

因为 $q_1 \pm q_2$ 是整数, 所以 $a \pm b$ 被 c 整除.

例 4 因为 $7|14, 7|84$, 所以 $7|(84 + 14) = 98, 7|(84 - 14) = 70$.

*** 定理 3** 设 $a, b, c \neq 0$ 是整数. 若 $c|a, c|b$, 则对任意整数 s, t , 有 $c|sa + tb$. (**整系数线性组合**)

证 设 $c|a, c|b$, 那么存在整数 q_1, q_2 分别使得 $a = cq_1, b = cq_2$.

因此,

$$sa + tb = s(cq_1) + t(cq_2) = c(sq_1 + tq_2).$$

因为 $sq_1 + tq_2$ 是整数, 所以 $sa + tb$ 被 c 整除.

例 5 因为 $7|14$, $7|21$, 故 $7|(3 \cdot 21 - 4 \cdot 14) = 7$, $7|(3 \cdot 21 + 4 \cdot 14) = 119$.

*** 例 6** 设 $a, b, c \neq 0$ 是三个整数, $c|a, c|b$. 如果存在整数 s, t , 使得 $sa + tb = 1$, 则 $c = \pm 1$.

证 设 $c|a, c|b$, 因为存在整数 s, t , 使得 $sa + tb = 1$, 根据定 3, 我们有

$$c|sa + tb = 1.$$

因此, $c = \pm 1$.

定 3 可推广为:

定理 4 若整数 $a_1, \dots, a_n$ 都是整数 $c \neq 0$ 的倍数, 则对任意 n 个整数 $s_1, \dots, s_n$, 整数

$$s_1 a_1 + \dots + s_n a_n$$

是 c 的倍数.

例 7 因为 $7|14$, $7|21$, $7|35$, 所以

$$7|(5 \cdot 21 + 4 \cdot 14 - 3 \cdot 35) = 56.$$

*** 定理 5** 设 a, b 都是非零整数. 若 $a|b$, $b|a$, 则 $a = \pm b$.

证 设 $a|b$, $b|a$, 那么存在两个整数 q_1, q_2 分别使得

$$a = bq_1, \quad b = aq_2.$$

从而,

$$a = bq_1 = (aq_2)q_1 = a(q_1q_2).$$

这样, $q_1q_2 = 1$. 因为 q_1, q_2 是整数, 所以 $q_1 = q_2 = \pm 1$. 进而, $a = \pm b$.

前面考虑了整除和因数，现在考虑不能继续分解的整数。

*** 定义 2** 设整数 $n \neq 0, \pm 1$. 如果除了显然因数 ± 1 和 $\pm n$ 外, n 没有其它因数, 则 n 叫做 **素数** (或 **质数** 或 **不可约数**), 否则, n 叫做 **合数**.

因 n 和 $-n$ 同为素数或合数, 故素数总是指正整数, 通常写成 p .

例 8 整数 2, 3, 5, 7 都是素数; 整数 4, 6, 10, 15, 21 都是合数.

下面我们要证明每个合数必有素因子.

*** 定理 6** 设 n 是一个正合数, p 是 n 的一个大于 1 的最小正因数, 则 p 一定是素数, 且 $p \leq \sqrt{n}$.

证 反证法. 若 p 不是素数, 则存在 $q, 1 < q < p$, 使得 $q|p$. 但 $p|n$, 由定理 1, 有 $q|n$. 这与 p 是 n 的最小正因数矛盾. 故, p 是素数.

因为 n 是合数, 所以 $n = pn_1, 1 < p \leq n_1 < n$. 因此, $p^2 \leq n$. 故 $p \leq \sqrt{n}$.

根据定 6, 我们立即得到一个整数为素数的判别法则.

*** 定理 7** 设 $n > 1$. 若对所有的素数 $p \leq \sqrt{n}$, 有 $p \nmid n$, 则 n 是素数.

*** 应用定 7, 我们有一个寻找素数的确定性方法, 通常叫做厄拉托塞师 (Eratosthenes) 筛法.**

对任意给定的正整数 N , 要求出所有不超过 N 的素数. 我们列出 N 个整数, 从中删除 $\leq \sqrt{N}$ 的所有素数 $p_1, \dots, p_k$ 的倍数. 具体地是依次删除,

$$p_1 \text{ 的倍数: } 2p_1, \dots, \left[\frac{N}{p_1}\right]p_1;$$

.....

$$p_k \text{ 的倍数: } 2p_k, \dots, \left[\frac{N}{p_k}\right]p_k,$$

余下的整数 (不包括 1) 就是所要求的不超过 N 的素数.

例 9 求出所有不超过 $N = 100$ 的素数.

解 因为 $\leq \sqrt{100} = 10$ 的所有素数为 2, 3, 5, 7, 所以依次删除 2, 3, 5, 7 的倍数,

$$2 \cdot 2, \quad 3 \cdot 2, \quad 4 \cdot 2, \quad \dots, \quad 49 \cdot 2, \quad 50 \cdot 2$$

$$2 \cdot 3, \quad 3 \cdot 3, \quad 4 \cdot 3, \quad \dots, \quad 32 \cdot 3, \quad 33 \cdot 3$$

$$2 \cdot 5, \quad 3 \cdot 5, \quad 4 \cdot 5, \quad \dots, \quad 19 \cdot 5, \quad 20 \cdot 5$$

$$2 \cdot 7, \quad 3 \cdot 7, \quad 4 \cdot 7, \quad \dots, \quad 13 \cdot 7, \quad 14 \cdot 7.$$

余下的整数 (不包括 1) 就是所要求的不超过 $N = 100$ 的素数.

我们将上述解答列表如下:

对于素数 $p_1 = 2$,

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

对于素数 $p_2 = 3$,

1	2	3	5	7	9
11	13	15	17	19	
21	23	25	27	29	
31	33	35	37	39	
41	43	45	47	49	
51	53	55	57	59	
61	63	65	67	69	
71	73	75	77	79	
81	83	85	87	89	
91	93	95	97	99	

对于素数 $p_3 = 5$,

1	2	3	5	7
11	13		17	19
	23	25		29
31		35	37	
41	43		47	49
	53	55		59
61		65	67	
71	73		77	79
	83	85		89
91		95	97	

对于素数 $p_4 = 7$,

1	2	3	5	7
11	13		17	19
	23			29
31			37	
41	43		47	49
	53			59
61			67	
71	73		77	79
	83			89
91			97	

余下整数 (不包括 1) 就是所求的不超过 $N = 100$ 的素数:

1	2	3	5	7
11		13		17 19
		23		29
31				37
41		43		47
		53		59
61				67
71		73		79
		83		89
				97

即 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

*** 定理 8** 素数有无穷多个.

证 反证法. 假设只有有限个素数. 设它们为 $p_1, p_2, \dots, p_k$.
考虑整数

$$n = p_1 \cdot p_2 \cdots p_k + 1.$$

因为 $n > p_i, \quad i = 1, \dots, k$, 所以 n 一定是合数. 根据定 6, n 的大于 1 的最小正因数 p 是素数. 因此, p 是 $p_1, p_2, \dots, p_k$ 中的某一个, 即存在 $j, 1 \leq j \leq k$, 使得 $p = p_j$. 根据定 3, 我们有

$$p \mid n - p_1 \cdots p_j \cdots p_k = 1.$$

这是不可能的. 故存在有无穷多个素数.

运用上述方法可证明形为 $4k+3$ 的素数有无穷多个, 但无法证明形为 $4k+1$ 的素数有无穷多个. 要更多技巧.

因为不是任意两个整数之间都有整除关系, 所以我们引进 **欧几里得 (Euclid) 除法 或 带余数除法**.

*** 定理 9 (欧 里得除法)** 设 a, b 是两个整数, 其中 $b > 0$. 则存在惟一的整数 q, r 使得

$$a = bq + r, \quad 0 \leq r < b \quad (2)$$

定理 9 之证明: (存在性) 考虑一个整数序列

$$\dots, -3b, -2b, -b, 0, b, 2b, 3b, \dots$$

它们将实数轴分成长度为 b 的区间, 而 a 必定落在其中的一个区间中. 因此存在一个整数 q 使得 $qb \leq a < (q+1)b$.

我们令 $r = a - bq$, 则有 $a = bq + r, \quad 0 \leq r < b$.

(惟一性) 如果分别有整数 q, r 和 q_1, r_1 满足 (2), 则

$$a = bq + r, \quad 0 \leq r < b,$$

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

两式 减, 有 $b(q - q_1) = -(r - r_1)$.

当 $q \neq q_1$ 时, 左边的绝对值 $\geq b$, 而右边的绝对值 $< b$. 这是不可能的. 故 $q = q_1, \quad r = r_1$.

*** 定义 3** (2) 式中的 q 叫做 a 被 b 除所得的 **不完全商**, r 叫做 a 被 b 除所得的 **余数**.

推论 在定 9 的条件下, $b|a \Leftrightarrow r = 0$.

注 欧 里得除法在密码算法中起着核心作用, 其改进关系到密码系统的效率. 如 $b = 2^u + v, v$ 很小.

应用定理 7 和欧几里得除法, 可具体判断一个整数是否为素数.

例 10 证明 $N = 137$ 为素数.

解 因为 $\leq \sqrt{137} < 12$ 的所有素数为 2, 3, 5, 7, 11, 所以依次用 2, 3, 5, 7, 11 去试除:

$$137 = 68 \cdot 2 + 1, \quad 137 = 45 \cdot 3 + 2, \quad 137 = 26 \cdot 5 + 3,$$

$$137 = 19 \cdot 7 + 4, \quad 137 = 12 \cdot 11 + 5.$$

2 $\nmid$ 137, 3 $\nmid$ 137, 5 $\nmid$ 137, 7 $\nmid$ 137, 11 $\nmid$ 137. 由定理 7, $N = 137$ 为素数.

为了更好的描述不完全商和余数, 以及今后表述一些数学概念和问题, 我们引进一个数学符号.

定义 4 设 x 是一个实数. 我们称 x 的整数部分为小于或等于 x 的最大整数, 记成 $[x]$. 这时, 我们有

$$[x] \leq x < [x] + 1.$$

注 定 9 中不完全商 q 可写为 $q = [\frac{a}{b}]$, 余数 r 可写为 $r = a - b[\frac{a}{b}]$.
事实上, 我们是先计算不完全商 $q = [\frac{a}{b}]$, 再计算余数 $r = a - b[\frac{a}{b}]$.

例 11 $[3.14] = 3$, $[-3.14] = -4$, $[3] = 3$, $[-3] = -3$.

例 12 设 $b = 15$.

当 $a = 255$ 时, $a = 17b + 0$, $q = [\frac{255}{15}] = 17$, $r = 0 < 15$;

当 $a = 417$ 时, $a = 27b + 12$, $q = [\frac{417}{15}] = 27$, $0 < r = 12 < 15$;

当 $a = -81$ 时, $a = -6b + 9$, $q = [\frac{-81}{15}] = -6$, $0 < r = 9 < 15$.

实际运用欧 里得除法时, 可根据 要将余数取成其它形式.

定理 10 (欧 里得除法) 设 a, b 是两个整数, 其中 $b > 0$. 则对任意的整数 c , 存在惟一的整数 q, r 使得

$$a = bq + r, \quad c \leq r < b + c$$

注

1. 当 $0 \leq r < b$ 时, r 叫做 **最小非负余数**.
2. 当 $1 \leq r \leq b$ 时, r 叫做 **最小正余数**.
3. 当 $-b + 1 \leq r \leq 0$ 时, r 叫做 **最大非正余数**.
4. 当 $-b \leq r < 0$ 时, r 叫做 **最大负余数**.
5. 当 $-b/2 \leq r < b/2$ 或 $-b/2 < r \leq b/2$ 时, r 叫做 **绝对值最小余数**.

例 13 设 $b = 7$. 则

余数 $r = 0, 1, 2, 3, 4, 5, 6$ 为最小非负余数.

余数 $r = 1, 2, 3, 4, 5, 6, 7$ 为最小正余数.

余数 $r = 0, -1, -2, -3, -4, -5, -6$ 为最大非正余数.

余数 $r = -1, -2, -3, -4, -5, -6, -7$ 为最大负余数.

余数 $r = -3, -2, -1, 0, 1, 2, 3$ 为绝对值最小余数.

例 14 设 $b = 8$. 则

余数 $r = 0, 1, 2, 3, 4, 5, 6, 7$ 为最小非负余数.

余数 $r = 1, 2, 3, 4, 5, 6, 7, 8$ 为最小正余数.

余数 $r = 0, -1, -2, -3, -4, -5, -6, -7$ 为最大非正余数.

余数 $r = -1, -2, -3, -4, -5, -6, -7, -8$ 为最大负余数.

余数 $r = -4, -3, -2, -1, 0, -1, -2, -3$

或 $r = -3, -2, -1, 0, 1, 2, 3, 4$ 为绝对值最小余数.

我们平时遇到的整数通常是以 10 进制表示. 例如 51328 意指

$$5 \cdot 10^4 + 1 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10^1 + 8 \cdot 10^0.$$

中国是世界上最先采用十进制的国家, 春秋战国时期已普遍使用的筹算就严格遵循了十进位制, 见《孙子算经》. 但在计算机中, 51328 要用 2 进制, 8 进制或 2 进制表示. 为此, 我们考虑一般的 b 进制, 再考察特殊的 2 进制, 10 进制和 16 进制.

运用欧几里得除法, 我们可得到如下定理:

定理 1 设 $b > 1$ 是正整数. 则每个正整数 n 可惟一地表示成

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1b + a_0,$$

其中 a_i 是整数, $0 \leq a_i \leq b-1$, $i = 1, \dots, k-1$, 且首项系数 $a_{k-1} \neq 0$.

证 先证明 n 有表达式. 逐次运用欧 里得除法,

首先, 用 b 去除 n 得到 $n = bq_0 + a_0, \quad 0 \leq a_0 \leq b - 1.$

再用 b 去除不完全商 q_0 得到 $q_0 = bq_1 + a_1, \quad 0 \leq a_1 \leq b - 1.$

$$q_1 = bq_2 + a_2, \quad 0 \leq a_2 \leq b - 1,$$

如此可依次得到

$\dots$

$$q_{k-3} = bq_{k-2} + a_{k-2}, \quad 0 \leq a_{k-2} \leq b - 1,$$

$$q_{k-2} = bq_{k-1} + a_{k-1}, \quad 0 \leq a_{k-1} \leq b - 1.$$

因为 $0 \leq q_{k-1} < \dots < q_1 < q_0 < n$, 所以必有整数 k 使得

$q_{k-1} = 0$. 这样, 我们依次得到

$$\begin{aligned} n &= bq_0 + a_0 = b(bq_1 + a_1) + a_0 = b^2q_1 + a_1b + a_0 = \dots \\ &= b^{k-2}q_{k-3} + a_{k-3}b^{k-3} + \dots + a_1b + a_0 \\ &= b^{k-1}q_{k-2} + a_{k-2}b^{k-2} + \dots + a_1b + a_0 \\ &= a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \dots + a_1b + a_0. \end{aligned}$$

再证明这个表示式是惟一的. 如果有两种不同的表示式:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1b + a_0, \quad 0 \leq a_i \leq b-1, \quad i = 1, \dots, k-1.$$

$n = c_{k-1}b^{k-1} + c_{k-2}b^{k-2} + \cdots + c_1b + c_0, \quad 0 \leq c_i \leq b-1, \quad i = 1, \dots, k-1.$ (这里可以取 $a_{k-1} = 0$ 或 $c_{k-1} = 0$.) 两式 减得到

$$(a_{k-1} - c_{k-1})b^{k-1} + (a_{k-2} - c_{k-2})b^{k-2} + \cdots + (a_1 - c_1)b + (a_0 - c_0) = 0.$$

假设 j 是最小的正整数使得 $a_j \neq c_j$, 则

$$b^j((a_{k-1} - c_{k-1})b^{k-1-j} + (a_{k-2} - c_{k-2})b^{k-2-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j)) = 0.$$

或者 $(a_{k-1} - c_{k-1})b^{k-1-j} + (a_{k-2} - c_{k-2})b^{k-2-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0.$

因此 $a_j - c_j = -((a_{k-1} - c_{k-1})b^{k-j-2} + (a_{k-2} - c_{k-2})b^{k-j-3} + \cdots + (a_{j+1} - c_{j+1}))b.$

故 $b|(a_j - c_j), \quad |a_j - c_j| \geq b.$ 但 $0 \leq a_j \leq b-1, \quad 0 \leq c_j \leq b-1,$ 又有 $|a_j - c_j| < b.$ 这不可能. 也就是说 n 的表示式是惟一的.

为了说明整数是关于基 b 的表示式, 我们引进如下符号:

定义 1 我们用 $n = (a_{k-1}a_{k-2}\dots a_1a_0)_b$ 表示展开式:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \dots + a_1b + a_0,$$

其中 $0 \leq a_i \leq b-1$, $i = 1, \dots, k-1$, $a_{k-1} \neq 0$, 并称其为整数 n 的 b 进制表示. 这时, n 的 b -进制位数是 $k = [\log_b n] + 1$. 事实上,

$$b^{k-1} \leq n < b^k \quad \text{或} \quad k-1 \leq \log_b n < k.$$

因此, $k-1 = [\log_b n]$.

例 1 表示整数 642 为 2 进制.

解 逐次运用欧里得除法, 我们有

$$642 = 2 \cdot 321 + 0,$$

$$20 = 2 \cdot 10 + 0,$$

$$321 = 2 \cdot 160 + 1,$$

$$10 = 2 \cdot 5 + 0,$$

$$160 = 2 \cdot 80 + 0,$$

$$5 = 2 \cdot 2 + 1,$$

$$80 = 2 \cdot 40 + 0,$$

$$2 = 2 \cdot 1 + 0,$$

$$40 = 2 \cdot 20 + 0,$$

$$1 = 2 \cdot 0 + 1.$$

因此, $642 = (1010000010)_2$, 或者

$$642 = 1 \cdot 2^9 + 0 \cdot 2^8 + 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0.$$

计算机也常用 8 进制, 或 16 进制, 或 64 进制等. 在 16 进制中, 我们用 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A , B , C , D , E , F 分别表示 0, 1, ..., 15 共 16 个数, 其中 A , B , C , D , E , F 分别对应于 10, 11, 12, 13, 14, 15.

为了方便各进制转换，提高转换效率，可预先制作换算表.

10 进制	16 进制	2 进制	10 进制	16 进制	2 进制
0	0	0000	8	8	1000
1	1	0001	9	9	1001
2	2	0010	10	A	1010
3	3	0011	11	B	1011
4	4	0100	12	C	1100
5	5	0101	13	D	1101
6	6	0110	14	E	1110
7	7	0111	15	F	1111

例 3 转换 16 进制 $(ABC8)_{16}$ 为 2 进制.

因 $A = (1010)_2, B = (1011)_2, C = (1100)_2, 8 = (1000)_2$. 从而 $(ABC8)_{16} = (1010101111001000)_2$.

例 4 转换 2 进制 $(101110111111101001)_2$ 为 16 进制.
由上述换算表可得到

$$(1001)_2 = 9, (1110)_2 = E, (1111)_2 = F, (1101)_2 = D, (101)_2 = (0101)_2 = 5.$$

从而 $(101110111111101001)_2 = (5DFE9)_{16}$.

因为 2 进制的转换比 16 进制要容易些, 所以我们可以先将数作 2 进制表示, 然后, 运用 2 进制与 16 进制之间的换算表, 将 2 进制转换成 16 进制.

例 5 表示整数 642 为 16 进制.

解 根据例 1, 我们有 $642 = (1010000010)_2$.

又查换算表得到

$$(0010)_2 = 2, (1000)_2 = 8, (10)_2 = (0010)_2 = 2.$$

故 $642 = 2 \cdot 16^2 + 8 \cdot 16^1 + 2 = (282)_{16}$.

本节考虑多个整数的公共因数，特别是它们的最大公因数以及最大公因数的计算.

定义 1 设 $a_1, \dots, a_n$ 是 n ($n \geq 2$) 个整数. 若整数 d 是它们中每一个数的因数, 那么 d 就叫做 $a_1, \dots, a_n$ 的一个 **公因数**.

如果整数 $a_1, \dots, a_n$ 不全为零, 那么整数 $a_1, \dots, a_n$ 的所有公因数中最大的一个公因数叫做 **最大公因数**, 记作 $(a_1, \dots, a_n)$. 特别地, 当 $(a_1, \dots, a_n) = 1$ 时, 我们称 $a_1, \dots, a_n$ **互素** 或 **互质**.

实际上, $d = (a_1, \dots, a_n)$ 的数学表达式可叙述为:

- (1) $d|a_1, \dots, d|a_n$. (2) 若 $e|a_1, \dots, e|a_n$, 则 $e|d$.

我们将在定理 7 中给予说明.

例 1 两个整数 14 和 21 的公因数为 $\{\pm 1, \pm 7\}$, 它们的最大公因数 $(14, 21) = 7$.

例 2 两个整数 -15 和 21 的公因数为 $\{\pm 1, \pm 3\}$, 它们的最大公因数 $(-15, 21) = 3$.

例 3 三个整数 $14, -15$ 和 21 的公因数为 $\{\pm 1\}$, 它们的最大公因数 $(14, -15, 21) = 1$. 或者说, 三个整数 $14, -15$ 和 21 是互素的.

例 4 设 a, b 是两个整数, 则 $(b, a) = (a, b)$.

例 5 设 a, b 是两个正整数. 如果 $b|a$, 则 $(a, b) = b$.

例 6 设 p 是一个素数, a 为整数. 如果 $p \nmid a$, 则 p 与 a 互素.

证 设 $(p, a) = d$. 则有 $d|p$ 及 $d|a$.

因为 p 是素数, 所以由 $d|p$, 我们有 $d = 1$ 或 $d = p$.

对于 $d = p$, 由 $d|a$, 我们有 $p|a$, 这与假设 $p \nmid a$ 矛盾.

因此, $d = 1$. 即 $(p, a) = 1$. 结论成立.

定理 1 设 $a_1, \dots, a_n$ 是 n 个不全为零的整数, 则

(i) $a_1, \dots, a_n$ 与 $|a_1|, \dots, |a_n|$ 的公因数 同;

(ii) $(a_1, \dots, a_n) = (|a_1|, \dots, |a_n|)$.

例 7 设 a, b 是整数. 则 $(a, b) = (a, -b) = (-a, b) = (|a|, |b|)$

例 8 我们有

$$1) (-14, 21) = (14, -21) = (-14, -21) = (14, 21) = 7.$$

$$2) (-15, 21) = (15, -21) = (-15, -21) = (15, 21) = 3.$$

*** 定理 2** 设 b 是任一正整数, 则 $(0, b) = b$.

证 因为任何非零整数都是 0 的因数, 而正整数 b 的最大因数为 b , 所以 $(0, b) = b$.

例 9 1) $(0, 21) = 21$. 2) $(-15, 0) = 15$. 3) $(0, b) = |b|$.

*** 定理 3** 设 a, b, c 是三个不全为零的整数. 如果 $a = bq + c$, 其中 q 是整数, 则 $(a, b) = (b, c)$.

证 设 $d = (a, b)$, $d' = (b, c)$, 则 $d|a$, $d|b$. 由 §1.1 定 3,

$$d|a + (-q)b = c,$$

因而, d 是 b, c 的公因数. 从而, $d \leq d'$.

同 , d' 是 a, b 的公因数, $d' \leq d$.

因此, $d = d'$. 于是, 定 3 成立.

例 10 因为 $1859 = 1 \cdot 1573 + 286$, 所以 $(1859, 1573) = (1573, 286)$.

例 11 因为 $1573 = 5 \cdot 286 + 143$, 所以 $(1573, 286) = (286, 143) = 143$.

怎样才能具体计算出两个整数 a, b 的最大公因数？直接应用最大公因数的定义，就要知道整数的因数分解式，这在 a, b 不是很大数时是可行的，见 §1.5 定理 4. 但当 a, b 是很大数时，整数分解本身就是很困难的事. 为此，我们先给出一种算法“广义欧几里得除法或辗转除法”，然后运用它求 a, b 的最大公因数.

* 广义欧几里得除法 设 a, b 是任意两个正整数.

记 $r_{-2} = a, r_{-1} = b$. 反复运用欧几里得除法, 我们有

$$r_{-2} = q_0 r_{-1} + r_0, \quad 0 \leq r_0 < r_{-1},$$

$$r_{-1} = q_1 r_0 + r_1, \quad 0 \leq r_1 < r_0,$$

$$r_0 = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1,$$

$$\dots\dots\dots (1)$$

$$r_{n-4} = q_{n-2} r_{n-3} + r_{n-2}, \quad 0 \leq r_{n-1} < r_{n-2},$$

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, \quad 0 \leq r_{n-1} < r_{n-2},$$

$$r_{n-2} = q_n r_{n-1} + r_n, \quad r_n = 0.$$

经过有限步骤, 必然存在 n 使得 $r_n = 0$, 这是因为

$$0 = r_n < r_{n-1} < \dots < r_1 < r_0 < r_{-1} = b,$$

且 b 是有限正整数.

定理 4 设 a, b 是任意两个正整数, 则 $(a, b) = r_{n-1}$, 其中 r_{n-1} 是广义欧几里得除法 (1) 中最后一个非零余数.

证 根据定理 3, 我们有

$$\begin{aligned}(a, b) &= (r_{-2}, r_{-1}) = (r_{-1}, r_0) \\ &= (r_0, r_1) = \dots \\ &= (r_{n-2}, r_{n-1}) = (r_{n-1}, 0).\end{aligned}$$

再根据定理 2, 我们有

$$(a, b) = (r_{n-1}, 0) = r_{n-1}.$$

因为每个欧几里得除法的运算时间为 $O(\log a \log b)$, 且 $n = O(\log a)$, 所以计算 (a, b) 的时间为 $O(\log^2 a \log b)$.

因为求两个整数的最大公因数在信息安全的实践中起着重要的作用，所以我们将求两个整数的最大公因数之过程详述如下：

首先，根据定理 1, 将求两个整数的最大公因数转化为求两个非负整数的最大公因数；

其次，运用欧几里得除法，并根据定理 3, 我们可以将求两个正整数的最大公因数转化为求两个较小非负整数的最大公因数；

反复运用欧几里得除法，即广义欧几里得除法来，将求两个正整数的最大公因数转化为求 0 和一个正整数的最大公因数；

最后，根据定理 2, 求出两个整数的最大公因数.

例 12 设 $a = -1859$, $b = 1573$, 计算 (a, b) .

解 由定 1, $(-1859, 1573) = (1859, 1573)$. 运用广义欧 里得除法，

$$1859 = 1 \cdot 1573 + 286, \quad 1573 = 5 \cdot 286 + 143, \quad 286 = 2 \cdot 143.$$

根据定 4, $(-1859, 1573) = 143$.

例 14 设 $a = 46480$, $b = 39423$, 计算 (a, b) .

解 利用广义欧里得除法, 方法一: 最小非负余数.

$$46480 = 1 \cdot 39423 + 7057$$

$$1219 = 2 \cdot 481 + 257$$

$$26 = 3 \cdot 7 + 5$$

$$39423 = 5 \cdot 7057 + 4138$$

$$481 = 1 \cdot 257 + 224$$

$$7 = 1 \cdot 5 + 2$$

$$7057 = 1 \cdot 4138 + 2919$$

$$257 = 1 \cdot 224 + 33$$

$$5 = 2 \cdot 2 + 1$$

$$4138 = 1 \cdot 2919 + 1219$$

$$224 = 6 \cdot 33 + 26$$

$$2 = 2 \cdot 1.$$

$$2919 = 2 \cdot 1219 + 481$$

$$33 = 1 \cdot 26 + 7$$

方法二: 绝对值最小余数.

$$46480 = 1 \cdot 39423 + 7057$$

$$1219 = 3 \cdot 481 - 224$$

$$7 = 3 \cdot 2 + 1$$

$$39423 = 6 \cdot 7057 - 2919$$

$$481 = 2 \cdot 224 + 33$$

$$2 = 2 \cdot 1.$$

$$7057 = 2 \cdot 2919 + 1219$$

$$224 = 7 \cdot 33 - 7$$

$$2919 = 2 \cdot 1219 + 481$$

$$33 = 5 \cdot 7 - 2$$

所以, $(46480, 39423) = 1$.

从广义欧几里得除法的演示中，我们观察到

$$r_n = r_{n-2} - r_{n-1}q_{n-1},$$

$$r_{n-1} = r_{n-3} - r_{n-2}q_{n-3},$$

.....

$$r_3 = r_1 - r_2q_2,$$

$$r_2 = r_0 - r_1q_1.$$

这样，逐次消去 $r_{n-1}, r_{n-2}, \dots, r_3, r_2$, 可找到整数 s, t 使得 $sa + tb = (a, b)$.

例 15 设 $a = -1859, b = 1573$, 求整数 s, t , 使得 $sa + tb = (a, b)$.

解 由例 12, 我们有

$$\begin{aligned} 143 &= 1573 - 5 \cdot 286 \\ &= 1573 - 5 \cdot (1859 - 1 \cdot 1573) \\ &= 5 \cdot (-1859) + 6 \cdot 1573. \end{aligned}$$

因此，整数 $s = 5, t = 6$ 满足 $sa + tb = (a, b)$.

例 17 设 $a = 46480$, $b = 39423$, 求整数 s, t , 使得 $sa + tb = (a, b)$.

解 由例 14, 我们有方法一: 最小非负余数.

$$\begin{aligned}
 1 &= 5 & - 2 \cdot 2 \\
 &= 5 & - 2 \cdot (7 - 1 \cdot 5) \\
 &= (-2) \cdot 7 & + 3 \cdot (26 - 3 \cdot 7) \\
 &= 3 \cdot 26 & + (-11) \cdot (33 - 1 \cdot 26) \\
 &= (-11) \cdot 33 & + 14 \cdot (224 - 6 \cdot 33) \\
 &= 14 \cdot 26 & + (-95) \cdot (257 - 1 \cdot 224) \\
 &= (-95) \cdot 257 & + 109 \cdot (481 - 1 \cdot 257) \\
 &= 109 \cdot 481 & + (-204) \cdot (1219 - 2 \cdot 481) \\
 &= (-204) \cdot 7 & + 517 \cdot (2919 - 2 \cdot 1219) \\
 &= 517 \cdot 2919 & + (-1238) \cdot (4138 - 1 \cdot 2919) \\
 &= (-1238) \cdot 4138 & + 1755 \cdot (7057 - 1 \cdot 4138) \\
 &= 1755 \cdot 7057 & + (-2993) \cdot (39423 - 5 \cdot 7057) \\
 &= (-2993) \cdot 39423 & + 16720 \cdot (46480 - 1 \cdot 39423) \\
 &= 16720 \cdot 46480 & + (-19713) \cdot 39423 \\
 &= (16720 - 39423) \cdot 46480 & + (46480 - 19713) \cdot 39423 \\
 &= (-22703) \cdot 46480 & + 26767 \cdot 39423.
 \end{aligned}$$

方法二：绝对值最小余数.

$$\begin{aligned}
 1 &= 7 && - 3 \cdot 2 \\
 &= 7 && - 3 \cdot (-33 + 5 \cdot 7) \\
 &= 3 \cdot 33 && + (-14) \cdot (-224 + 7 \cdot 33) \\
 &= 14 \cdot 224 && + (-95) \cdot (481 - 2 \cdot 224) \\
 &= (-95) \cdot 481 && + 204 \cdot (-1219 + 3 \cdot 481) \\
 &= (-204) \cdot 1219 && + 517 \cdot (2919 - 2 \cdot 1219) \\
 &= 517 \cdot 2919 && + (-1238) \cdot (7057 - 2 \cdot 2919) \\
 &= (-1238) \cdot 7057 && + 2993 \cdot (-39423 + 6 \cdot 7057) \\
 &= (-2993) \cdot 39423 && + 16720 \cdot (46480 - 1 \cdot 39423) \\
 &= 16720 \cdot 46480 && + (-19713) \cdot 39423 \\
 &= (16720 - 39423) \cdot 46480 + (46480 - 19713) \cdot 39423 \\
 &= (-22703) \cdot 46480 + 26767 \cdot 39423.
 \end{aligned}$$

因此，整数 $s = -22703$, $t = 26767$ 满足 $sa + tb = (a, b)$.

*** 定理 5** 设 a, b 是正整数, 则 $s_n a + t_n b = (a, b), \quad (2)$

对于 $n = 0, 1, 2, \dots$, 这里 s_n, t_n 归纳地定义为

$$\begin{cases} s_0 = 1, s_1 = 0, s_j = s_{j-2} - q_{j-1}s_{j-1}, \\ t_0 = 0, t_1 = 1, t_j = t_{j-2} - q_{j-1}t_{j-1}, \end{cases} \quad j = 2, 3, \dots, n \quad (3)$$

其中 q_j 是 (1) 式中的不完全商.

证 只需证明: 对于 $j = 0, 1, 2, \dots, n$, $s_j a + t_j b = r_j, \quad (4)$

其中 r_j 是 (1) 式中的余数. 因为 $(a, b) = r_n$, 所以

$$s_n a + t_n b = (a, b).$$

对 j 作数学归纳法来证明 (4).

$j = 0$ 时, 有 $s_0 = 1, t_0 = 0$, 以及 $s_0 a + t_0 b = a = r_0$. 结论对于 $j = 0$ 成立.

$j = 1$ 时, 有 $s_1 = 0, t_1 = 1$, 以及 $s_1 a + t_1 b = b = r_1$. 结论对于 $j = 1$ 成立.

假设结论对于 $1 \leq j \leq k-1$ 成立. 即

$$s_j a + t_j b = r_j.$$

对于 $j = k$, 我们有

$$r_k = r_{k-2} - r_{k-1}q_{k-1}.$$

利用归纳假设, 我们得到

$$\begin{aligned} r_k &= (s_{k-2}a + t_{k-2}b) - (s_{k-1}a + t_{k-1}b)q_{k-1} \\ &= (s_{k-2} - q_{k-1}s_{k-1})a + (t_{k-2} - q_{k-1}t_{k-1})b \\ &= s_k a + t_k b. \end{aligned}$$

因此, 结论对于 $j = k$ 成立. 根据数学归纳法原理, (4) 对所有的 j 成立. 这就完成了证明.

假设 a, b 是不全为零的非负整数. 我们具体计算 s, t 使得

$$sa + tb = (a, b).$$

首先, 令 $r_{-2} = a, r_{-1} = b, s_{-2} = 1, s_{-1} = 0, t_{-2} = 0, t_{-1} = 1$.

(1) 如果 $r_{-1} = 0$, 则令 $s = s_{-2}, t = t_{-2}$. 否则, 计算

$$q_0 = \left[\frac{r_{-2}}{r_{-1}} \right], \quad r_0 = r_{-2} - q_0 r_{-1}.$$

(2) 如果 $r_0 = 0$, 则令 $s = s_{-1}, t = t_{-1}$. 否则, 计算

$$s_0 = s_{-2} - q_0 s_{-1}, \quad t_0 = t_{-2} - q_0 t_{-1}, \text{ 以及 } q_1 = \left[\frac{r_{-1}}{r_0} \right], \quad r_1 = r_{-1} - q_1 r_0.$$

(3) 如果 $r_1 = 0$, 则令 $s = s_0, t = t_0$. 否则, 计算

$$s_1 = s_{-1} - q_1 s_0, \quad t_1 = t_{-1} - q_1 t_0, \text{ 以及 } q_2 = \left[\frac{r_0}{r_1} \right], \quad r_2 = r_0 - q_2 r_1.$$

.....

(j+1) 若 $r_{j-1} = 0$, ($j \geq 3$), 则令

$$s = s_{j-2}, \quad t = t_{j-2}.$$

否则, 计算

$$s_{j-1} = s_{j-3} - q_{j-1}s_{j-2}, \quad t_{j-1} = t_{j-3} - q_{j-1}t_{j-2},$$

以及

$$q_j = \left[\frac{r_{j-2}}{r_{j-1}} \right], \quad r_j = r_{j-2} - q_j r_{j-1}.$$

最后, 一定有 $r_n = 0$. 这时, 令

$$s = s_{n-1}, \quad t = t_{n-1}.$$

总之, 我们可以找到整数 s, t , 使得

$$sa + tb = r_{n-1} = (a, b).$$

上述过程可以列成如下表格：

j	s_{j-1}	t_{j-1}	q_j	r_j
-2				a
-1	1	0		b
0	0	1	q_0	r_0
1	s_0	t_0	q_1	r_1
2	s_1	t_1	q_2	r_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n-1	s_{n-2}	t_{n-2}	q_{n-1}	r_{n-1}
n	s_{n-1}	t_{n-1}	q_n	r_n

其中，

$$\left\{ \begin{array}{l} s_{j-1} = s_{j-3} - q_{j-1}s_{j-2}, \\ t_{j-1} = t_{j-3} - q_{j-1}t_{j-2}, \\ q_j = \left[\frac{r_{j-2}}{r_{j-1}} \right], \\ r_j = r_{j-2} - q_j r_{j-1}. \end{array} \right.$$

例 18 设 $a = 1859$, $b = 1573$. 计算整数 s, t 使得

$$sa + tb = (a, b).$$

解 根据表格 (5) 及公式 (6), 我们有

j	s_{j-1}	t_{j-1}	q_j	r_j
-2				1859
-1	1	0		1573
0	0	1	1	286
1	1	-1	5	143
2	-5	6	2	0

因此, $s = -5$, $t = 6$ 使得

$$(-5) \cdot 1859 + 6 \cdot 1573 = 143.$$

例 19 设 $a = 737$, $b = 635$. 计算整数 s, t 使得

$$sa + tb = (a, b).$$

解 根据表格 (5) 及公式 (6), 我们有:

j	s_{j-1}	t_{j-1}	q_j	r_j	j	s_{j-1}	t_{j-1}	q_j	r_j
-2				737	2	-6	7	4	10
-1	1	0		635	3	25	-29	2	3
0	0	1	1	102	4	-56	65	3	1
1	1	-1	6	23	5	193	-224	3	0

因此, $s = 193$, $t = -224$ 使得

$$193 \cdot 737 + (-224) \cdot 635 = 1.$$

定 5 的逆命题不成立. 但我们有

*** 定理 6** 整数 a, b 互素的充分必要条件是存在整数 s, t 使得

$$sa + tb = 1.$$

证 根据定 5, 我们立即得到命题的必要性.

反过来, 设 $d = (a, b)$, 则有 $d|a, d|b$. 现在若存在整数 s, t 使得

$$sa + tb = 1.$$

则我们有

$$d|sa + tb = 1.$$

因此, $d = 1$. 即整数 a, b 互素.

例 20 设四个整数 a, b, c, d 满足关系式:

$$ad - bc = 1.$$

则 $(a, b) = 1$, $(a, c) = 1$, $(d, b) = 1$, $(d, c) = 1$.

下面，我们再说明最大公因数的数学定义. 我们有

*** 定理 7** 设 a, b 是任意两个不全为零的整数, d 是正整数. 则 d 是整数 a, b 的最大公因数的充要条件是:

(i) $d|a, d|b$;

(ii) 若 $e|a, e|b$, 则 $e|d$.

证 若 d 是整数 a, b 的最大公因数, 则显然有 (i) 成立; 再由定 5, 存在整数 s, t 使得

$$sa + tb = d.$$

因此, 当 $e|a, e|b$ 时, 有

$$e|sa + tb = d.$$

故 (ii) 成立.

反过来, 假设 (i) 和 (ii) 成立, 那么

(i) 说明 d 是整数 a, b 的公因数;

(ii) 说明 d 是整数 a, b 的公因数中的最大数, 因为 $e|d$ 时, 有 $|e| \leq d$.

因此, d 是整数 a, b 的最大公因数.

*** 定理 8** 设 a, b 是任意两个不全为零的整数,

(i) 若 m 是任一正整数, 则 $(am, bm) = (a, b)m$.

(ii) 若非零整数 d 满足 $d|a, d|b$, 则 $(\frac{a}{d}, \frac{b}{d}) = \frac{(a, b)}{|d|}$. 特别地,

$$* (\frac{a}{(a, b)}, \frac{b}{(a, b)}) = 1.$$

证 设 $d = (a, b)$, $d' = (am, bm)$. 由定 5, 存在整数 s, t 使得 $sa + tb = d$.

两端同乘 m , 得到 $s(am) + t(bm) = dm$. 因此 $d'|dm$.

又显然有 $dm|am, dm|bm$. 根据定 7 (ii), 有 $dm|d'$.

故 $d' = dm$. 即 (i) 成立.

再根据 (i), 当 $d|a, d|b$ 时, 有

$$(a, b) = (\frac{a}{|d|} \cdot |d|, \frac{b}{|d|} \cdot |d|) = (\frac{a}{|d|}, \frac{b}{|d|})|d| = (\frac{a}{d}, \frac{b}{d})|d|.$$

因此, $(\frac{a}{d}, \frac{b}{d}) = \frac{(a, b)}{|d|}$. 特别地, 取 $d = (a, b)$, 有 $(\frac{a}{(a, b)}, \frac{b}{(a, b)}) = 1$. 故 (ii) 成立.

例 21 设 $a = 11 \cdot 200306$, $b = 23 \cdot 200306$. 计算 (a, b) .

解 因为 $(11, 23) = (11, 23 - 11 \cdot 2) = (11, 1) = 1$, 所以

$$(a, b) = (11 \cdot 200306, 23 \cdot 200306) = 200306.$$

前面我们讨论了如何具体求两个整数的最大公因数. 对于 n 个整数 $a_1, \dots, a_n$ 的最大公因数, 我们可以用递归的方法, 将求它们的最大公因数转化为一系列求两个整数的最大公因数. 具体过程如下:

定理 9 设 $a_1, \dots, a_n$ 是 n 个整数, 且 $a_1 \neq 0$. 令

$$(a_1, a_2) = d_2, \quad \dots, \quad (d_{n-1}, a_n) = d_n.$$

则 $(a_1, \dots, a_n) = d_n$.

例 22 计算最大公因数 $(120, 150, 210, 35)$.

解 因为

$$(120, 150) = (120, 30) = 30,$$

$$(30, 210) = 30,$$

$$(30, 35) = (30, 5) = 5,$$

所以最大公因数 $(120, 150, 210, 35) = 5$.

*** 定理 1** 设 a, b, c 是整数, 且 $b \neq 0, c \neq 0$. 如果 $(a, c) = 1$, 则 $(ab, c) = (b, c)$.

证 令 $d = (ab, c)$, $d' = (b, c)$. 有 $d'|b, d'|c$. 进而 $d'|ab, d'|c$. 根据 §1.3 定理 7, 得 $d'|d$.

反过来, 因为 $(a, c) = 1$, 根据 §1.3 定理 6, 存在整数 s, t 使得 $sa + tc = 1$.

两端同乘 b , 得到 $s(ab) + (tb)c = b$. 根据 §1.1 定理 3, 由 $d|ab, d|c$, 我们得到 $d|s(ab) + (tb)c$, 即 $d|b$. 同样根据 §1.3 定理 7, 得到 $d|d'$.

故 $d = d'$.

推论 设 a, b, c 是三个整数, 且 $c \neq 0$. 如果 $c|ab, (a, c) = 1$, 则

$c|b$.

证 根据假设条件和定 1, 有 $c|(ab, c) = (b, c)$. 从而 $c|b$. 证毕.

例 1 因为 $15|2 \cdot 75$, 又 $(2, 15) = 1$, 所以 $15|75$.

*** 定理 2** 设 p 是素数. 若 $p|ab$, 则 $p|a$ 或 $p|b$.

证 若 $p \nmid a$, 则根据 §1.3 例 6, 有 $(p, a) = 1$. 再根据定 1 之推论, 有 $p|b$. 证毕.

例 2 因为 $5|3 \cdot 25$, 又 $5 \nmid 3$ 及 5 为素数, 所以 $5|25$.

问题: 若 $c|ab$, 则 $c|a$ 或 $c|b$?

* **定理 3** 设 $a_1, \dots, a_n, c$ 为整数. 如果 $(a_i, c) = 1, 1 \leq i \leq n$.

则

$$(a_1 \cdots a_n, c) = 1.$$

* **推论** 设 $a_1, \dots, a_n$ 是整数, p 是素数. 若 $p|a_1 \cdots a_n$, 则 p 一定整除某一个 a_k .

* **定义 1** 设 $a_1, \dots, a_n$ 是 n 个整数. 若 m 是这 n 个数的倍数, 则 m 叫做这 n 数的一个 **公倍数**. $a_1, \dots, a_n$ 的所有公倍数中的最小正整数叫做 **最小公倍数**, 记作 $[a_1, \dots, a_n]$.

$m = [a_1, \dots, a_n]$ 的数学表达式是:

(i) $a_i | m, 1 \leq i \leq n$; (ii) 若 $a_i | m', 1 \leq i \leq n$, 则 $m | m'$.

例 3 整数 14 和 21 的公倍数为 $\{\pm 42, \pm 84, \dots\}$, 最小公倍数为 $[14, 21] = 42$.

* **定理 4** 设 a, b 是两个互素正整数. 则

(i) 若 $a | m, b | m$, 则 $ab | m$; (ii) $[a, b] = ab$.

例 4 设 p, q 是两个不同的素数. 则 $[p, q] = pq$.

* **定理 5** 设 a, b 是两个正整数. 则

$$(i) \text{ 若 } a|m, b|m, \text{ 则 } [a, b] | m; \quad (ii) [a, b] = \frac{ab}{(a, b)}.$$

证 令 $d = (a, b)$. 根据 §1.3 定 8, 我们有 $(\frac{a}{d}, \frac{b}{d}) = 1$.

又根据定 4, $[\frac{a}{d}, \frac{b}{d}] = \frac{a}{d} \cdot \frac{b}{d}$, 进而 $[a, b] = \frac{ab}{d}$, 即 (ii) 成立.

再由 $\frac{a}{d} | \frac{m}{d}, \frac{b}{d} | \frac{m}{d}$, 得到 $\frac{a}{d} \cdot \frac{b}{d} | \frac{m}{d}$. 从而 $\frac{ab}{d} | m$, 即 (i) 成立.

对于 n 个整数 $a_1, \dots, a_n$ 的最小公倍数, 我们可以用递归的方法, 将求它们的最小公倍数转化为一系列求两个整数的最小公倍数. 具体过程如下:

定理 6 设 $a_1, \dots, a_n$ 是 n 个整数. 令

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \dots, [m_{n-1}, a_n] = m_n.$$

则 $[a_1, \dots, a_n] = m_n$.

例 5 计算最小公倍数 $[120, 150, 210, 35]$.

解 因为 $[120, 150] = \frac{120 \cdot 150}{(120, 150)} = \frac{120 \cdot 150}{30} = 600$

$$[600, 210] = \frac{600 \cdot 210}{(600, 210)} = \frac{600 \cdot 210}{30} = 4200,$$

$$[4200, 35] = \frac{4200 \cdot 35}{(4200, 35)} = \frac{4200 \cdot 35}{35} = 4200.$$

所以最大公因数 $[120, 150, 210, 35] = 4200$.

*** 定理 7** 设 $a_1, a_2, \dots, a_n$ 是正整数. 如果 $a_1|m, a_2|m, \dots, a_n|m$, 则 $[a_1, a_2, \dots, a_n] \mid m$

前面讨论过素数, 并证明了每个整数都有一个素因数. 下面要证明每个整数一定可以表示成素数的乘积, 而且该表达式是惟一的 (在不考虑乘积顺序的情况下).

*** 定理 1(算术基本定理)** 任一整数 $n > 1$ 都可以表示成素数的乘积, 且在不考虑乘积顺序的情况下, 该表达式是惟一的. 即

$$n = p_1 \cdots p_s, \quad p_1 \leq \cdots \leq p_s, \quad (1)$$

p_i 是素数, 且若 $n = q_1 \cdots q_t$, $q_1 \leq \cdots \leq q_t$, q_j 是素数, 则 $s = t$, $p_i = q_i$, $1 \leq i \leq s$.

证 首先用数学归纳法证明: 任一整数 $n > 1$ 都可以表示成素数的乘积, 即 (1) 式成立. $n = 2$, (1) 式成立. 假设对于 $< n$ 的正整数, (1) 式成立. 对于正整数 n ,

若 n 是素数, 则 (1) 式对 n 成立. 若 n 是合数, 则存在正整数 b, c 使得

$$n = bc, \quad 1 < b < n, \quad 1 < c < n.$$

根据归纳假设, $b = p'_1 \cdots p'_u, \quad c = p'_{u+1} \cdots p'_s$. 于是, $n = p'_1 \cdots p'_s$. 适当改变 p'_i 的次序即得 (1) 式, 故 (1) 式对于 n 成立.

根据数学归纳法原理, (1) 式对于所有 $n > 1$ 的整数成立.

再证明表达式是惟一的. 设还有 $n = q_1 \cdots q_t, \quad q_1 \leq \cdots \leq q_t,$

其中 q_j 是素数, 则

$$p_1 \cdots p_s = q_1 \cdots q_t. \quad (2)$$

因此 $p_1 | q_1 \cdots q_t$. 根据 §1.4 定理 3 之推论, 存在 q_j 使得 $p_1 | q_j$. 但 p_1, q_j 都是素数, 故 $p_1 = q_j$. 同理, 存在 p_k 使得 $q_1 = p_k$. 这样,

$$p_1 \leq p_k = q_1 \leq q_j = p_1,$$

进而 $p_1 = q_1$. 将 (2) 式的两端同时消除 p_1 , 我们有

$$p_2 \cdots p_s = q_2 \cdots q_t.$$

同理可推出 $p_2 = q_2$. 如此类推, 依次得到 $p_3 = q_3, \dots, q_s = p_t$. 以及 $s = t$.

例 1 写出整数 45, 49, 100, 128 的因数分解式.

解 根据定 1, 我们有

$$45 = 3 \cdot 3 \cdot 5, \quad 49 = 7 \cdot 7,$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5, \quad 128 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2.$$

将 同的素数乘积写成素数幂的形式, 定 1 可表述为:

定理 2 任一整数 $n > 1$ 可以惟一地表示成

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0, \quad i = 1, \dots, s, \quad (3)$$

其中 $p_i < p_j$ ($i < j$) 是素数.

(3) 式叫做 n 的 **标准分解式**.

例 2 写出整数 45, 49, 100, 128 的 准分解式.

解 根据定 1 和例 1, $45 = 3^2 \cdot 5$, $49 = 7^2$, $100 = 2^2 \cdot 5^2$, $128 = 2^7$.

在应用中, 为了表述方便起见, 整数的因数分解式常写成

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i \geq 0, \quad i = 1, \dots, s.$$

定理 3 设 n 是大于 1 的一个整数, 且有 准分解式:

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0, \quad i = 1, \dots, s,$$

则 d 是 n 的正因数当且仅当 d 有因数分解式:

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad \alpha_i \geq \beta_i \geq 0, \quad i = 1, \dots, s. \quad (4)$$

定理 4 设 a, b 是两个正整数, 且都有素因数分解式:

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad b = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad \alpha_i \geq 0, \quad \beta_i \geq 0, \quad i = 1, \dots, s,$$

则 a 和 b 的最大公因数和最小公倍数分别有因数分解式:

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_s^{\min(\alpha_s, \beta_s)}, \quad [a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdots p_s^{\max(\alpha_s, \beta_s)}.$$

推论 设 a, b 是两个正整数, 则 $(a, b)[a, b] = ab$.

例 4 计算整数 120, 150, 210, 35 的最大公因数和最小公倍数.

解 根据定 1, $120 = 2^3 \cdot 3 \cdot 5$, $150 = 2 \cdot 3 \cdot 5^2$, $210 = 2 \cdot 3 \cdot 5 \cdot 7$, $35 = 5 \cdot 7$.

再根据定 4, $(120, 150) = 2 \cdot 3 \cdot 5 = 30$, $(30, 210) = 2 \cdot 3 \cdot 5 = 30$, $(30, 35) = 5$,

所以整数 120, 150, 210, 35 的最大公因数为 5.

同样, 根据定 4, $[120, 150] = 2^3 \cdot 3 \cdot 5^2 = 600$, $[600, 210] = 2^3 \cdot 3 \cdot 5^2 \cdot 7 = 4200$, $[4200, 35] = 2^3 \cdot 3 \cdot 5^2 \cdot 7 = 4200$, 所以 $[120, 150, 210, 35] = 4200$.

第二章 同余

本章主要讲述如下问题：

1. 同余的基本概念
2. 模同余的判断：等价关系和模运算等
3. 模同余的基本性质
4. 剩余类与完全剩余系
5. 简化剩余类与简化剩余系
6. 模逆元素 乘法表
7. 欧拉函数及其计算
8. 欧拉定理 费马小定理
9. RSA 解密证明
10. 模重复平方方法

前面讨论了整数的整除性质，现在讨论整数的同余性质，以对整数进行恰当的分类. 同余是数论中的一个十分重要的概念，同余理论在密码学，特别是公钥密码学中有着非常重要的应用.

定义 1 给定一个正整数 m . 两个整数 a, b 叫做模 m **同余**, 如果 $a - b$ 被 m 整除, 或 $m|a - b$, 记作 $a \equiv b \pmod{m}$. 否则, 叫做模 m **不同余**. 记作 $a \not\equiv b \pmod{m}$.

注 模 m 是正整数, 在同余性质的讨论中为一个固定整数.

例 1 我们有 $29 \equiv 1 \pmod{7}$, 因为 $7|29 - 1$. 同样, $27 \equiv 6 \pmod{7}$ 和 $23 \equiv -5 \pmod{7}$. 同余的概念常常出现于日常生活中. 例如, 时针是模 12 或 24 小时. 分针和秒针是模 60.

如何判断两个整数 a, b 模 m 同余呢？

直接运用同余的定义，就必须作欧几里得除法，即计算 $a - b$ 被模 m 除的余数。但这是一项冗长的工作。因此，我们引进一些等价的判别法，以便更快捷地判断两个整数 a, b 模 m 是否同余。

首先，通过整数 a, b 的表达形式来判断整数 a, b 模 m 是否同余。

定理 1 设 m 是正整数，设 a, b 是整数，则 $a \equiv b \pmod{m}$ 的充要条件是存在一个整数 k 使得 $a = b + km$.

例 2 我们有 $39 \equiv 4 \pmod{7}$ ，因为 $39 = 5 \cdot 7 + 4$.

其次，模同余具有一种叫做 **等价关系** 的性质。

定理 2 设 m 是一个正整数，则模 m 同余是等价关系，即

- i). (自反性) 对任一整数 a , $a \equiv a \pmod{m}$;
- ii). (对称性) 若 $a \equiv b \pmod{m}$, 则 $b \equiv a \pmod{m}$;
- iii). (传递性) 若 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 则 $a \equiv c \pmod{m}$.

例 3 因为 $39 \equiv 32 \pmod{7}$, $32 \equiv 25 \pmod{7}$, 所以

$$39 \equiv 25 \pmod{7}. \quad \text{传递性}$$

同时, 我们有

$$39 \equiv 39 \pmod{7}, \quad 25 \equiv 25 \pmod{7}, \quad \text{自反性}$$

以及

$$32 \equiv 39 \pmod{7}, \quad 25 \equiv 32 \pmod{7}. \quad \text{对称性}$$

第三, 运用整数 a, b 模 m 的余数, 可以判断 a, b 模 m 是否同余.

定理 3 设 m 是一个正整数, 则整数 a, b 模 m 同余的充分必要条件是 a, b 被 m 除的余数 同.

例 4 我们有 $39 \equiv 25 \pmod{7}$, 因为 $39 = 5 \cdot 7 + 4$, $25 = 3 \cdot 7 + 4$.

第四，因为模同余是等价关系，所以有整数 a, b 模 m 的加法运算和乘法运算性质，并可运用这个性质来判断 a, b 模 m 是否同余.

定理 4 设 m 是正整数，设 a_1, a_2, b_1, b_2 是整数. 如果

$$a_1 \equiv b_1 \pmod{m}, \quad a_2 \equiv b_2 \pmod{m},$$

则 (i) $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$; (ii) $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

例 5 已知 $39 \equiv 4 \pmod{7}$, $22 \equiv 1 \pmod{7}$, 所以

$$61 = 39 + 22 \equiv 4 + 1 \equiv 5 \pmod{7},$$

$$17 = 39 - 22 \equiv 4 - 1 \equiv 3 \pmod{7},$$

$$858 = 39 \cdot 22 \equiv 4 \cdot 1 \equiv 4 \pmod{7},$$

$$1521 = 39^2 \equiv 4^2 \equiv 2 \pmod{7},$$

$$484 = 22^2 \equiv 1^2 \equiv 1 \pmod{7}.$$

例 6 2003 年 5 月 9 日是星期五，问第 2^{2003} 天是星期 ？

解 因为 $2^1 \equiv 2 \pmod{7}$, $2^2 \equiv 4 \pmod{7}$, $2^3 = 8 \equiv 1 \pmod{7}$, 又 $2003 = 667 \cdot 3 + 2$. 所以

$$2^{2003} = (2^3)^{667} \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod{7}.$$

故第 2^{2003} 天是星期二.

下面, 我们进一步讨论同余的性质.

*** 定理 8** 设 $ad \equiv bd \pmod{m}$. 若 $(d, m) = 1$, 则 $a \equiv b \pmod{m}$.

证 若 $ad \equiv bd \pmod{m}$, 则 $m \mid ad - bd$, 或 $m \mid d(a - b)$. 从而 $m \mid a - b$.

例 11 因为 $95 \equiv 25 \pmod{7}$, $(5, 7) = 1$, 所以 $19 \equiv 5 \pmod{7}$.

定理 9 设 $a \equiv b \pmod{m}$, $k > 0$, 则 $ak \equiv bk \pmod{mk}$.

*** 定理 10** 设 $a \equiv b \pmod{m}$. 若 $d \mid (a, b, m)$, 则 $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

例 13 因为 $190 \equiv 50 \pmod{70}$, 所以取 $d = 10$, 得到 $19 \equiv 5 \pmod{7}$.

*** 定理 11** 设 $a \equiv b \pmod{m}$. 如果 $d \mid m$, 则 $a \equiv b \pmod{d}$.

*** 定理 12** 设 $a \equiv b \pmod{m_i}$, $i = 1, \dots, k$, 则 $a \equiv b \pmod{[m_1, \dots, m_k]}$.

例 15 因 $190 \equiv 50 \pmod{7}$, $190 \equiv 50 \pmod{10}$, 故 $190 \equiv 50 \pmod{70}$.

*** 例 16** 设 p, q 是不同素数. 若 a, b 满足 $a \equiv b \pmod{p}$, $a \equiv b \pmod{q}$, 则 $a \equiv b \pmod{pq}$.

证 设 $a \equiv b \pmod{p}$, $a \equiv b \pmod{q}$, 则 $p|a-b$, $q|a-b$. 因为 p, q 是不同的素数, 所以 $pq|a-b$. 即 $a \equiv b \pmod{pq}$.

定理 13 设 $a \equiv b \pmod{m}$, 则 $(a, m) = (b, m)$.

因为同余是一种等价关系，所以可借助于同余对全体整数进行分类，并将每类作为一个数来看待，进而得到整数的一些新性质.

对任意整数 a , 令 $C_a = \{c \mid c \in \mathbf{Z}, a \equiv c \pmod{m}\}$.

定理 1 i) 任一整数必包含在一个 C_r 中, $0 \leq r \leq m-1$.

ii) $C_a = C_b \Leftrightarrow a \equiv b \pmod{m}$. (1)

iii) $C_a \cap C_b = \emptyset \Leftrightarrow a \not\equiv b \pmod{m}$.

定义 1 C_a 叫做模 m 的 a 的 **剩余类**. 一个剩余类中的任一数叫做该类的 **剩余** 或 **代表元**. 若 $r_0, r_1, \dots, r_{m-1}$ 是 m 个整数, 并且其中任何两个数都不在同一个剩余类里, 则 $r_0, \dots, r_{m-1}$ 叫做

模 m 的一个 **完全剩余系**. 模 m 的剩余类有 m 个

$$C_0, C_1, \dots, C_{m-1}.$$

例 1 对任意整数 a , $C_a = \{a + 10k \mid k \in \mathbf{Z}\}$ 是模 $m = 10$ 的剩余类.

0, 1, 2, 3, 4, 5, 6, 7, 8, 9 为模 10 的一个完全剩余系.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10 为模 10 的一个完全剩余系.

0, -1, -2, -3, -4, -5, -6, -7, -8, -9 为模 10 的一个完全剩余系.

0, 3, 6, 9, 12, 15, 18, 21, 24, 27 为模 10 的一个完全剩余系.

10, 11, 22, 33, 44, 55, 66, 77, 88, 99 为模 10 的一个完全剩余系.

定理 2 m 个整数 $r_0, r_1, \dots, r_{m-1}$ 为模 m 的一个完全剩余系的充分必要条件是它们模 m 两两不同余.

例 2 设 m 是一个正整数. 则

i) $0, 1, \dots, m-1$ 是模 m 的一个完全剩余系, 叫做模 m 的 **最小非负完全剩余系**;

ii) $1, \dots, m-1, m$ 是模 m 的一个完全剩余系, 叫做模 m 的 **最小正完全剩余系**;

iii) $-(m-1), \dots, -1, 0$ 是模 m 的一个完全剩余系, 叫做模 m 的 **最大非正完全剩余系**;

iv) $-m, -(m-1), \dots, -1$ 是模 m 的一个完全剩余系, 叫做模 m 的 **最大负完全剩余系**;

v) 当 m 分别为偶数时, $-m/2, -(m-2)/2, \dots, -1, 0, 1, \dots, (m-2)/2$, 或 $-(m-2)/2, \dots, -1, 0, 1, \dots, (m-2)/2, m/2$, 是模 m 的一个完全剩余系;

当 m 分别为奇数时, $-(m-1)/2, \dots, -1, 0, 1, \dots, (m-1)/2$ 是模 m 的一个完全剩余系, 上述两个完全剩余系统称为模 m 的一个 **绝对值最小完全剩余系**.

定理 3 设 $(a, m) = 1$, b 是任意整数. 若 x 遍历模 m 的一个完全剩余系, 则 $ax + b$ 也遍历模 m 的一个完全剩余系.

证 根据定理 2, 只 证明: 当 $a_0, a_1, \dots, a_{m-1}$ 是模 m 的一个完全剩余系时, m 个整数 $aa_0 + b, aa_1 + b, \dots, aa_{m-1} + b$ 模 m 两两不同余. 事实上, 若存在 a_i 和 a_j ($i \neq j$) 使得

$$aa_i + b \equiv aa_j + b \pmod{m},$$

则 $m|a(a_i - a_j)$. 因为 $(a, m) = 1$, 根据 §1.4 定理 1 之推论, 我们有 $m|a_i - a_j$. 这说明 a_i 与 a_j 模 m 同余, 与假设矛盾. 因此, $ax + b$ 也遍历模 m 的一个完全剩余系.

例 2 设 $m = 10$, $a = 7$, $b = 5$. 则形为 $ax + b$ 的 10 个数 5, 12, 19, 26, 33, 40, 47, 54, 61, 68 构成模 10 的一个完全剩余系.

定理 4 设 $(m_1, m_2) = 1$. 若 x_1, x_2 分别遍历模 m_1, m_2 的完全剩余系, 则 $m_2x_1 + m_1x_2$ 遍历模 m_1m_2 的完全剩余系.

证 因为 x_1, x_2 分别遍历 m_1, m_2 个数时, $m_2x_1 + m_1x_2$ 遍历 m_1m_2 个整数, 所以只 证明这 m_1m_2 个整数模 m_1m_2 两两不同余. 事实上, 若整数 x_1, x_2 和 y_1, y_2 满足

$$m_2x_1 + m_1x_2 \equiv m_2y_1 + m_1y_2 \pmod{m_1m_2},$$

则 $m_2x_1 + m_1x_2 \equiv m_2y_1 + m_1y_2 \pmod{m_1}$, 或者 $m_2x_1 \equiv m_2y_1 \pmod{m_1}$, 进而, $m_1|m_2(x_1 - y_1)$. 因为 $(m_1, m_2) = 1$, 所以 $m_1|x_1 - y_1$. 故 x_1 与 y_1 模 m_1 同余.

同理, x_2 与 y_2 模 m_2 同余. 因此, 定理是成立的. 证毕.

例 3 设 p, q 是不同的素数, $n = pq$. 则对任意整数 c , 存在惟一的一对整数 x, y 满足 $qx + py \equiv c \pmod{n}$, $0 \leq x < p, 0 \leq y < q$.

证 因为 p, q 是两个不同的素数, 所以 p, q 是互素的. 根据定理 4 及其证明, 知 x, y 分别遍历模 p, q 的完全剩余系时, $qx + py$ 遍历模 $n = pq$ 的完全剩余系. 因此, 存在惟一的一对整数 x, y 满足

$$qx + py \equiv c \pmod{n}, \quad 0 \leq x < p, 0 \leq y < q.$$

例 4 设 $m_1 = 2, m_2 = 5$. 则形为 $2x_1 + 5x_2$ 的 10 个数

$$0, 5, 10, 15, 20, 2, 7, 12, 17, 22$$

构成模 10 的一个完全剩余系.

定理 5 设 $m_1, m_2, \dots, m_k$ 是 k 个互素的正整数. 若 $x_1, x_2, \dots, x_k$ 分别遍历模 $m_1, m_2, \dots, m_k$ 的完全剩余系, 则

$$m_2 \cdots m_k x_1 + m_1 m_3 \cdots m_k x_2 + \cdots + m_1 \cdots m_{k-1} x_k$$

遍历模 $m_1 m_2 \cdots m_k$ 的完全剩余系.

在讨论中, 常常假定两个整数 a, m 互素的条件, 即 $(a, m) = 1$. 现在我们讨论剩余与 m 互素的剩余类的性质.

定义 1 设 m 是一个正整数. 则 m 个整数 $0, 1, \dots, m-1$ 中与 m 互素的整数的个数, 记作 $\varphi(m)$, 通常叫做 **欧拉 (Euler) 数**.

例 1 设 $m = 10$. 则 10 个整数 $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ 中与 10 互素的整数为 $1, 3, 7, 9$, 所以 $\varphi(10) = 4$.

定义 2 一个模 m 的剩余类叫做 **简化剩余类**, 如果该类中存在一个与 m 互素的剩余.

定理 1 设 r_1, r_2 是同一模 m 剩余类的两个剩余, 则 r_1 与 m 互素的充分必要条件是 r_2 与 m 互素.

证 依题设, 有 $r_1 = r_2 + km$. 进而 $(r_1, m) = (r_2, m)$. 因此, $(r_1, m) = 1 \Leftrightarrow (r_2, m) = 1$.

定义 3 在模 m 的所有不同简化剩余类中, 从每个类任取一个数组成的整数的集合, 叫做模 m 的一个 **简化剩余系**.

模 m 的简化剩余系的元素个数为 $\varphi(m)$.

例 3 1, 3, 7, 9 是模 10 的简化剩余系, $\varphi(10) = 4$.

例 4 1, 7, 11, 13, 17, 19, 23, 29 是模 30 的简化剩余系, $\varphi(30) = 8$.

例 5 1, 2, 3, 4, 5, 6 是模 7 的简化剩余系, $\varphi(7) = 6$.

例 6 当 $m = p$ 为素数时, $1, 2, \dots, p-1$ 是模 p 的简化剩余系, 所以 $\varphi(p) = p-1$.

定理 2 若 $r_1, \dots, r_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数, 并且两两模 m 不同余, 则 $r_1, \dots, r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

证 依定理假设, 知 $\varphi(m)$ 个整数 $r_1, \dots, r_{\varphi(m)}$ 是模 m 的所有不同简化剩余类的剩余. 故 $r_1, \dots, r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

定理 3 设 $(a, m) = 1$. 如果 x 遍历模 m 的一个简化剩余系, 则 ax 也遍历模 m 的一个简化剩余系.

证 因为 $(a, m) = 1, (x, m) = 1$, 所以 $(ax, m) = 1$. 这说明 ax 是简化剩余类的剩余. 又 $ax_1 \equiv ax_2 \pmod{m}$ 时, 有 $x_1 \equiv x_2 \pmod{m}$. 因此, x 遍历模 m 的一个简化剩余系时, ax 遍历 $\varphi(m)$ 个数, 且它们两两模 m 不同余. 根据定理 2, ax 遍历模 m 的一个简化剩余系.

例 7 已知 1, 7, 11, 13, 17, 19, 23, 29 是模 30 的简化剩余系, $(7, 30) = 1$. 所以

$$\begin{aligned} 7 \cdot 1 &\equiv 7, & 7 \cdot 7 &= 49 \equiv 19, & 7 \cdot 11 &= 77 \equiv 17, \\ 7 \cdot 13 &= 91 \equiv 1, & 7 \cdot 17 &= 119 \equiv 29, & 7 \cdot 19 &= 133 \equiv 13, \\ 7 \cdot 23 &= 161 \equiv 11, & 7 \cdot 29 &= 203 \equiv 23 \pmod{30}. \end{aligned}$$

因此, $7 \cdot 1, 7 \cdot 7, 7 \cdot 11, 7 \cdot 13, 7 \cdot 17, 7 \cdot 19, 7 \cdot 23, 7 \cdot 29$ 是模 30 的简化剩余系.

例 8 设 $m = 7$. 设 a 表示第一列数, 为与 m 互素的给定数. 设 x 表示第一行数, 遍历模 m 的简化剩余系. 设 a 所在行与 x 所在列的交叉位置表示 ax 模 m 最小非负剩余. 则我们得到如下的列表,

$a \setminus x$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

其中 a 所在行的数表示 ax 随 x 遍历模 m 的简化剩余系.

定理 4 设 $(a, m) = 1$. 则存在整数 a' , $1 \leq a' < m$ 使得

$$aa' \equiv 1 \pmod{m}.$$

证一 (存在性证明). 因为 $(a, m) = 1$, 根据定理 3, x 遍历模 m 的一个最小简化剩余系时, ax 也遍历模 m 的一个简化剩余系. 因此, 存在整数 $x = a'$, $1 \leq a' < m$ 使得 aa' 属于 1 的剩余类, 即 $aa' \equiv 1 \pmod{m}$. 证毕.

因为在实际运用中, 我们常常要具体地求出整数, 所以我们运用广义欧几里得除法给出定理 4 的构造性证明.

证二 (构造性证明). 因为 $(a, m) = 1$, 根据 §1.3 定理 5, 运用广义欧几里得除法, 可找到整数 s, t 使得 $sa + tm = (a, m) = 1$. 因此, 整数 $a' = s \pmod{m}$ 满足 $aa' \equiv 1 \pmod{m}$.

例 9 设 $m = 7$, a 表示与 m 互素的整数. 根据定理 4, 我们得

到 应的同余式:

$$\begin{aligned} 1 \cdot 1 &\equiv 1, & 2 \cdot 4 &\equiv 1, & 3 \cdot 5 &\equiv 1, & (\text{mod } 7) \\ 4 \cdot 2 &\equiv 1, & 5 \cdot 3 &\equiv 1, & 6 \cdot 6 &\equiv 1, & (\text{mod } 7). \end{aligned}$$

例 10 设 $m = 737$, $a = 635$. 根据 §1.3 例 19, 由广义欧 里得除法, 可找到整数 $s = -224$, $t = 193$ 使得

$$(-224) \cdot 635 + 193 \cdot 737 = 1.$$

因此, $a' = -224 \equiv 513 \pmod{737}$ 使得

$$635 \cdot 513 \equiv 1 \pmod{737}.$$

定理 5 设 $(m_1, m_2) = 1$. 如果 x_1, x_2 分别遍历模 m_1 和模 m_2 的简化剩余系, 则 $m_2x_1 + m_1x_2$ 遍历模 m_1m_2 的简化剩余系.

证 先证明: $(x_1, m_1) = 1, (x_2, m_2) = 1$ 时, $(m_2x_1 + m_1x_2, m_1m_2) = 1$.

事实上, 因为 $(m_1, m_2) = 1$, 根据 §1.3 定理 3 和 §1.4 定理 1, 我们有

$$(m_2x_1 + m_1x_2, m_1) = (m_2x_1, m_1) = (x_1, m_1) = 1,$$

$$(m_2x_1 + m_1x_2, m_2) = (m_1x_2, m_2) = (x_2, m_2) = 1.$$

因此, 再根据 §1.4 定理 3, 我们得到 $(m_2x_1 + m_1x_2, m_1m_2) = 1$.

其次, 证明模 m_1m_2 的任一简化剩余可表示为 $m_2x_1 + m_1x_2$,

其中 $(x_1, m_1) = 1, (x_2, m_2) = 1$. 事实上, 根据 §2.2 定理 4, 模 m_1m_2 的任一剩余可以表示为 $m_2x_1 + m_1x_2$. 因此, 当 $(m_2x_1 + m_1x_2, m_1m_2) = 1$ 时, 根据 §1.4 定理 1 和 §1.3 定理 3, 有

$$(x_1, m_1) = (m_2x_1, m_1) = (m_2x_1 + m_1x_2, m_1) = 1.$$

同理, $(x_2, m_2) = 1$. 结论成立.

从定理 5 可推出欧拉函数 φ 的性质 (即 φ 是所谓的乘性函数).

定理 6 设 m, n 是互素的两个正整数. 则 $\varphi(mn) = \varphi(m)\varphi(n)$.

证 根据定理 5, 当 x 遍历模 m 的简化剩余系, 共 $\varphi(m)$ 个整数以及 y 遍历模 n 的简化剩余系, 共 $\varphi(n)$ 个整数时, $ym + xn$ 遍历模 mn 的简化剩余系, 其整数个数为 $\varphi(m)\varphi(n)$. 但模 mn 的简化剩余系的元素个数又为 $\varphi(mn)$. 因此, 所以 $\varphi(mn) = \varphi(m)\varphi(n)$.

例 11 $\varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$.

例 12 $\varphi(30) = \varphi(2)\varphi(3)\varphi(5) = 1 \cdot 2 \cdot 4 = 8$.

定理 7 设 n 有 准因数分解式为 $n = \prod_{p|n} p^{\alpha} = p_1^{\alpha_1} \cdots p_k^{\alpha_s}$. 则

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

推论 设 p, q 是不同的素数. 则 $\varphi(pq) = pq - p - q + 1$.

证明 由定理 7, 有 $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1) = pq - p - q + 1$.

注 当 n 为合数, 且不知道 n 的因数分解式时, 通常很难求出 n 的欧拉函数值 $\varphi(n)$.

例 13 设正整数 n 是两个不同素数的乘积. 如果知道 n 和欧拉函数值 $\varphi(n)$, 则可求出 n 的因数分解式.

证 考虑未知数 p, q 的方程组:

$$\begin{cases} p + q = n + 1 - \varphi(n) \\ p \cdot q = n. \end{cases}$$

根据多项式的根与系数之间的关系, 我们可以从二次方程

$$z^2 - (n + 1 - \varphi(n))z + n = 0$$

求出 n 的因数 p, q .

例 1 设 $m = 7$, $a = 2$. 我们有 $(2, 7) = 1$, $\varphi(7) = 6$.

考虑模 7 的最小非负简化剩余系 $1, 2, 3, 4, 5, 6$, 我们有

$$2 \cdot 1 \equiv 2, 2 \cdot 2 \equiv 4, 2 \cdot 3 \equiv 6, 2 \cdot 4 \equiv 1, 2 \cdot 5 \equiv 3, 2 \cdot 6 \equiv 5, \pmod{7}.$$

上述同余式左右对应 乘, 得到

$$(2 \cdot 1)(2 \cdot 2)(2 \cdot 3)(2 \cdot 4)(2 \cdot 5)(2 \cdot 6) \equiv 2 \cdot 4 \cdot 6 \cdot 1 \cdot 3 \cdot 5 \pmod{7}$$

或

$$2^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}.$$

注意到

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv (1 \cdot 6)(2 \cdot 4)(3 \cdot 5) \equiv (-1) \cdot 1 \cdot 1 \equiv -1 \pmod{7},$$

故 $2^6 \equiv 1 \pmod{7}$.

例 2 设 $m = 30$, $a = 7$. 我们有 $(7, 30) = 1$, $\varphi(30) = 8$.

考虑模 30 的最小非负简化剩余系 1, 7, 11, 13, 17, 19, 23, 29, 有

$$\begin{aligned}7 \cdot 1 &\equiv 7, & 7 \cdot 7 &= 49 \equiv 19, & 7 \cdot 11 &= 77 \equiv 17, \\7 \cdot 13 &= 91 \equiv 1, & 7 \cdot 17 &= 119 \equiv 29, & 7 \cdot 19 &= 133 \equiv 13, \\7 \cdot 23 &= 161 \equiv 11, & 7 \cdot 29 &= 203 \equiv 23 \pmod{30}.\end{aligned}$$

上述同余式左右对应 乘, 得到

$$\begin{aligned}&(7 \cdot 1)(7 \cdot 7)(7 \cdot 11)(7 \cdot 13)(7 \cdot 17)(7 \cdot 19)(7 \cdot 23)(7 \cdot 29) \\&\equiv 7 \cdot 19 \cdot 17 \cdot 1 \cdot 29 \cdot 13 \cdot 11 \cdot 23 \pmod{30}\end{aligned}$$

或

$$7^8 \cdot 1 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \equiv 1 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \pmod{30}.$$

注意到 $(1 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29, 30) = 1$, 故 $7^8 \equiv 1 \pmod{30}$.

例 1 和例 2 可推广为一般的结论, 即欧拉定理.

定理 1 (Euler) 如果 $(a, m) = 1$, 则 $a^{\varphi(m)} \equiv 1 \pmod{m}$.

证 取 $r_1, \dots, r_{\varphi(m)}$ 为模 m 的一个最小正简化剩余系, 则当 a 是满足 $(a, m) = 1$ 的整数时, $ar_1, \dots, ar_{\varphi(m)}$ 也为模 m 的一个简化剩余系, 这就是说, $ar_1, \dots, ar_{\varphi(m)}$ 模 m 的最小正剩余是 $r_1, \dots, r_{\varphi(m)}$ 的一个排列. 故乘积 $(ar_1) \cdots (ar_{\varphi(m)})$ 模 m 的最小正剩余和乘积 $r_1 \cdots r_{\varphi(m)}$ 模 m 的最小正剩余 等. 即

$$(ar_1) \cdots (ar_{\varphi(m)}) \equiv r_1 \cdots r_{\varphi(m)} \pmod{m}.$$

因此, $r_1 \cdots r_{\varphi(m)} (a^{\varphi(m)} - 1) \equiv 0 \pmod{m}$. 又从 $(r_1, m) = 1, \dots, (r_{\varphi(m)}, m) = 1$ 及 §1.4 定理 3, 可推出 $(r_1 \cdots r_{\varphi(m)}, m) = 1$. 从而, 根据 §2.1 定理 8, 得到 $a^{\varphi(m)} - 1 \equiv 0 \pmod{m}$.

例 3 设 $m = 11$, $a = 2$. 则 $(2, 11) = 1$, $\varphi(11) = 10$. 故 $2^{10} \equiv 1 \pmod{11}$.

例 4 设 $m = 23$, $23 \nmid a$. 我们有 $(a, 23) = 1$, $\varphi(23) = 22$. 故 $a^{22} \equiv 1 \pmod{23}$.

定理 2 (Fermat) 设 p 是一个素数. 则对任意整数 a , 我们有

$$a^p \equiv a \pmod{p}.$$

证 我们分两种情形考虑.

i) 若 a 被 p 整数, 则同时有 $a \equiv 0 \pmod{p}$ 和 $a^p \equiv 0 \pmod{p}$.

因此, $a^p \equiv a \pmod{p}$.

ii) 若 a 不被 p 整数, 则 $(a, p) = 1$ (见 §1.3 例 4). 根据定理 1,

$$a^{p-1} \equiv 1 \pmod{p}.$$

两端同乘 a , 得到

$$a^p \equiv a \pmod{p}.$$

例 5 设 p, q 是两个不同的奇素数, $n = pq$, a 是与 pq 互素的整数. 如果整数 e 满足 $1 < e < \varphi(n)$, $(e, \varphi(n)) = 1$, 那么存在整数 d , $1 \leq d < \varphi(n)$, 使得

$$ed \equiv 1 \pmod{\varphi(n)}.$$

而且, 对于整数 $a^e \equiv c \pmod{n}$, $1 \leq c < n$, 有 $c^d \equiv a \pmod{n}$.

证 因为 $(e, \varphi(n)) = 1$, 根据 §2.3 定理 4, 存在整数 d , $1 \leq d < \varphi(n)$, 使得

$$ed \equiv 1 \pmod{\varphi(n)}.$$

因此, 存在一个正整数 k 使得 $ed = 1 + k \varphi(n)$. 现在, 根据定理 1, 得到

$$a^{\varphi(p)} \equiv 1 \pmod{p}.$$

两端作 $k(\varphi(n)/\varphi(p))$ 次幂, 并乘以 a 得到

$$a^{1+k \varphi(n)} \equiv a \pmod{p},$$

即

$$a^{ed} \equiv a \pmod{p}.$$

同理,

$$a^{ed} \equiv a \pmod{q}.$$

因为 p 和 q 是不同的素数, 根据 §2.1 定理 12 ,

$$a^{ed} \equiv a \pmod{n},$$

因此,

$$c^d \equiv (a^e)^d \equiv a \pmod{n}.$$

定理 3 (Wilson) 设 p 是一个素数. 则 $(p-1)! \equiv -1 \pmod{p}$.

例 5 设 $p = 17$. 我们有

$$\begin{aligned} 2 \cdot 9 &= 18 \equiv 1, & 3 \cdot 6 &= 18 \equiv 1, & 4 \cdot 13 &= 52 \equiv 1, \\ 5 \cdot 7 &= 35 \equiv 1, & 8 \cdot 15 &= 120 \equiv 1, & 10 \cdot 12 &= 120 \equiv 1, \\ 11 \cdot 14 &= 154 \equiv 1, & 1 \cdot 16 &\equiv -1 & & \pmod{17}. \end{aligned}$$

因此,

$$\begin{aligned} &1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \\ &= (1 \cdot 16)(2 \cdot 9)(3 \cdot 6)(4 \cdot 13)(5 \cdot 7)(8 \cdot 15)(10 \cdot 12)(11 \cdot 14) \\ &\equiv (-1) \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \\ &\equiv -1 \pmod{17}. \end{aligned}$$

在模算术计算中，常常要对大整数模 m 和大整数 n ，计算 $b^n \pmod{m}$ 。当然，可以递归地计算 $b^n \equiv (b^{n-1} \pmod{m}) \cdot b \pmod{m}$ 。

但这种计算较为费时，须作 $n - 1$ 次乘法。现在，将 n 写成二进制：

$$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1},$$

其中 $n_i \in \{0, 1\}$, $i = 0, 1, \dots, k-1$ 。则 $b^n \pmod{m}$ 的计算可归纳为

$$b^n \equiv \underbrace{b^{n_0} (b^2)^{n_1} \cdots (b^{2^{k-2}})^{n_{k-2}} (b^{2^{k-1}})^{n_{k-1}}}_{\pmod{m}}.$$

我们最多作 $2[\log_2 n]$ 次乘法。这个计算方法叫做“**模重复平方算法**”。具体算法如下：

0). 令 $a = 1$ ，并将 n 写成二进制： $n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1}$,

其中 $n_i \in \{0, 1\}$, $i = 0, 1, \dots, k-1$.

1). 如果 $n_0 = 1$, 则计算 $a_0 \equiv a \cdot b \pmod{m}$, 否则取 $a_0 = a$. 即计算 $a_0 \equiv a \cdot b^{n_0} \pmod{m}$. 再计算 $b_1 \equiv b^2 \pmod{m}$.

2). 如果 $n_1 = 1$, 则计算 $a_1 \equiv a_0 \cdot b_1 \pmod{m}$, 否则取 $a_1 = a_0$. 即计算 $a_1 \equiv a_0 \cdot b_1^{n_1} \pmod{m}$. 再计算 $b_2 \equiv b_1^2 \pmod{m}$

k-1). 如果 $n_{k-2} = 1$, 则计算 $a_{k-2} \equiv a_{k-3} \cdot b_{k-2} \pmod{m}$, 否则取 $a_{k-2} = a_{k-3}$. 即计算 $a_{k-2} \equiv a_{k-3} \cdot b_{k-2}^{n_{k-2}} \pmod{m}$. 再计算 $b_{k-1} \equiv b_{k-2}^2 \pmod{m}$.

k). 如果 $n_{k-1} = 1$, 则计算 $a_{k-1} \equiv a_{k-2} \cdot b_{k-1} \pmod{m}$, 否则取 $a_{k-1} = a_{k-2}$. 即计算 $a_{k-1} \equiv a_{k-2} \cdot b_{k-1}^{n_{k-1}} \pmod{m}$.

最后, a_{k-1} 就是 $b^n \pmod{m}$.

例 1 计算 $12996^{227} \pmod{37909}$.

解 设 $m = 37909$, $b = 12996$. 令 $a = 1$. $227 = 1 + 2 + 2^5 + 2^6 + 2^7$.

运用模重复平方法, 依次计算如下:

1). $n_0 = 1$. 计算 $a_0 = a \cdot b \equiv 12996$, $b_1 \equiv b^2 \equiv 11421 \pmod{37909}$.

2). $n_1 = 1$. 计算 $a_1 = a_0 \cdot b_1 \equiv 13581$, $b_2 \equiv b_1^2 \equiv 32281 \pmod{37909}$.

3). $n_2 = 0$. 计算 $a_2 = a_1 \equiv 13581$, $b_3 \equiv b_2^2 \equiv 20369 \pmod{37909}$.

4). $n_3 = 0$. 计算 $a_3 = a_2 \equiv 13581$, $b_4 \equiv b_3^2 \equiv 20065 \pmod{37909}$.

5). $n_4 = 0$. 计算 $a_4 = a_3 \equiv 13581$, $b_5 \equiv b_4^2 \equiv 10645 \pmod{37909}$.

6). $n_5 = 1$. 计算 $a_5 = a_4 \cdot b_5 \equiv 22728$, $b_6 \equiv b_5^2 \equiv 6024 \pmod{37909}$.

7). $n_6 = 1$. 计算 $a_6 = a_5 \cdot b_6 \equiv 24073$, $b_7 \equiv b_6^2 \equiv 9663 \pmod{37909}$.

8). $n_7 = 1$. 计算 $a_7 = a_6 \cdot b_7 \equiv 7775 \pmod{37909}$.

最后, 计算出 $12996^{227} \equiv 7775 \pmod{37909}$.

第三章 同余式

本章主要讲述如下问题：

1. 同余式的基本概念
2. 一次同余式的求解
3. 中国剩余定理
4. 大模计算的简化
5. $x^p - x$ 与高次同余式
6. 高次同余式的解数
7. 模素数幂同余式及解的提升
8. 模素数同余式

现在考虑在模 m 的情况下多项式的求解 (即同余式) .

定义 1 设 m 正整数, $f(x)$ 多项式 $f(x) = a_n x^n + \cdots + a_1 x + a_0$,

其中 a_i 是整数, 则 $f(x) \equiv 0 \pmod{m}$ (1)

叫做模 m **同余式**. 若 $a_n \not\equiv 0 \pmod{m}$, 则 n 叫做 $f(x)$ 的 **次数**, 记为 $\deg f$. 此时, (1) 式又叫做模 m 的 n **次同余式**.

如果整数 a 使得 $f(a) \equiv 0 \pmod{m}$ 成立, 则 a 叫做该 (1) 的 **解**. 事实上, 满足 $x \equiv a \pmod{m}$ 的所有整数都使得 (1) 成立, 即 a 所在剩余类 $C_a = \{c \mid c \in \mathbf{Z}, a \equiv c \pmod{m}\}$ 中的每个剩余都使得 (1) 成立, 因此, (1) 的解 a 常写成 $x \equiv a \pmod{m}$.

在模 m 的完全剩余系中, 使得 (1) 成立的 剩余个数叫做同余式 (1) 的 **解数**.

例 1 $x^5 + x + 1 \equiv 0 \pmod{7}$ 是首项系数为 1 的模 7 同余式. 而 $x \equiv 2 \pmod{7}$ 是该同余式的解. 事实上, 我们有

$$2^5 + 2 + 1 = 35 = 5 \cdot 7 \equiv 0 \pmod{7}.$$

还有解 $x \equiv 2 \pmod{7}$, 解数为 2.

现在我们考虑一次同余式的求解.

定理 1 设 $a \nmid m$. 则一次同余式 $ax \equiv b \pmod{m}$ (2) 有解的充要条件是 $(a, m) | b$. 且当 (2) 有解时, 其解数为 $d = (a, m)$.

证 必要性. 设 (2) 有解 $x \equiv x_0 \pmod{m}$, 即存在整数 y_0 使得 $ax_0 - my_0 = b$. 因为 $(a, m) | a$, $(a, m) | m$, 所以 $(a, m) | ax_0 - my_0 = b$. 因此, 必要性成立. 充分性. 设 $(a, m) | b$. 则 $\frac{b}{(a, m)}$ 为整数.

首先, 我们考虑同余式 $\frac{a}{(a, m)}x \equiv 1 \pmod{\frac{m}{(a, m)}}. \quad (3)$

因为 $(\frac{a}{(a, m)}, \frac{m}{(a, m)}) = 1$, 故存在 x_0 , 使得 (3) 成立. 而且, 同余式 (3) 有惟一解 $x \equiv x_0 \pmod{\frac{m}{(a, m)}}. \quad (4)$

事实上, 若同时有 $\frac{a}{(a, m)}x \equiv 1 \pmod{\frac{m}{(a, m)}} \quad \text{和} \quad \frac{a}{(a, m)}x_0 \equiv 1 \pmod{\frac{m}{(a, m)}}$

成立, 两式 减 $\frac{a}{(a,m)}(x-x_0) \equiv 0 \pmod{\frac{m}{(a,m)}}$. 故 $x \equiv x_0 \pmod{\frac{m}{(a,m)}}$.

其次, 写出同余式 $\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \pmod{\frac{m}{(a,m)}}$ (5)

的惟一解 $x \equiv x_1 \equiv x_0 \frac{b}{(a,m)} \pmod{\frac{m}{(a,m)}}$. (6)

而且, $x \equiv x_1 \equiv x_0 \frac{b}{(a,m)} \pmod{m}$ 是 (2) 的一个特解.

最后, 写出 (2), 即 $ax \equiv b \pmod{m}$ 的全部解

$$x \equiv x_1 + t \frac{m}{(a,m)} \pmod{m}, \quad t = 0, 1, \dots, (a,m)-1.$$

事实上, 如果同时有 $ax \equiv b \pmod{m}$ 和 $ax_1 \equiv b \pmod{m}$, 两式 减 得到 $a(x-x_1) \equiv 0 \pmod{m}$. 根据 §2.1 定理 10 和定理 8, 这等价于

$$x \equiv x_1 \pmod{\frac{m}{(a,m)}}.$$

因此, 同余式 (2) 的全部解可写成 (7) 式. 证毕.

例 2 求解一次同余式 $33x \equiv 22 \pmod{77}$.

解 首先, 计算 $(33, 77) = 11$, 且有 $(33, 77) = 11 | 22$, 故原同余式有解.

其次, 运用广义欧几里得除法, 求出同余式 $3x \equiv 1 \pmod{7}$ 的一个特解 $x'_0 \equiv 5 \pmod{7}$.

第三, 写出同余式 $3x \equiv 2 \pmod{7}$

的一个特解 $x_0 \equiv 2 \cdot x'_0 \equiv 2 \cdot 5 \equiv 3 \pmod{7}$.

最后, 写出原同余式的全部解

$$x \equiv 3 + t \frac{77}{(33, 77)} \equiv 3 + 7t \pmod{77}, \quad t = 0, 1, \dots, 10.$$

或者

$$x \equiv 3, 10, 17, 24, 31, 38, 45, 52, 59, 66, 73 \pmod{77}.$$

根据定理 1, 我们可以更确切地描述 §2.3 定理 4.

定理 2 设 $(a, m) = 1$. 则 $ax \equiv 1 \pmod{m}$ 有惟一解 $x \equiv a' \pmod{m}$.

证 由 $(a, m) = 1, b = 1$, 得 $(a, m) | b$. 故原同余式有惟一解.

定义 2 设 a 是整数. 如果存在整数 a' 使得 $aa' \equiv 1 \pmod{m}$ 成立, 则 a 叫做模 m **可逆元**.

根据定理 2, 在模 m 的意义下, a' 是惟一存在的. 这时 a' 叫做 a 的模 m **逆元**, 记作 $a' = a^{-1} \pmod{m}$.

有了模 m 逆元的说法, 我们可以将同余式 (2) 的求解写成

定理 3 设 $(a, m) | b$. 则一次同余式 $ax \equiv b \pmod{m}$ 的全部解为

$$x \equiv \frac{b}{(a, m)} \cdot \left(\left(\frac{a}{(a, m)} \right)^{-1} \pmod{\frac{m}{(a, m)}} \right) + t \frac{m}{(a, m)} \pmod{m},$$

$$t = 0, 1, \dots, (a, m) - 1.$$

现在我们给出模简化剩余的一个等价描述.

定理 4 设 m 是一个正整数. 则整数 a 是模 m 简化剩余的充要条件是整数 a 是模 m 逆元.

证 必要性. 如果整数 a 是模 m 简化剩余, 则 $(a, m) = 1$. 根据定理 2, 存在整数 a' 使得 $aa' \equiv 1 \pmod{m}$.

因此, 由定义 2, a 是模 m 逆元.

充分性. 如果 a 是模 m 逆元, 则存在整数 a' 使得

$$aa' \equiv 1 \pmod{m}.$$

即同余式 $ax \equiv 1 \pmod{m}$ 有解 $x \equiv a' \pmod{m}$. 根据定理 1, 我们有 $(a, m) | 1$. 从而, $(a, m) = 1$. 因此, 整数 a 是模 m 简化剩余.

§3.2 中国剩余定理

关于中国剩余定理或孙子定理，其最早见于《孙子算经》的“物不知数”题：
今有物不知其数，三三数之有二，五五数之有三，七七数之有二，问物有多少？
答案：二十三.

解答过程为：三三数之有二对应于一百四十，五五数之有三对应于六十三，七七数之有二对应于三十，将这些数相加得到二百三十三，再减去二百一十，即得数之数二十三.

将“物不知数”问题用同余式组表示就是：

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

而解答过程：三三数之有二对应于一百四十，五五数之有三对应于六十三，七七数之有二对应于三十，将这些数相加得到二百三十三，再减去二百一十，即得数之数二十三。就为：

$$\begin{aligned} 2 \cdot 5 \cdot 7 \cdot 2 &= 140, & 1 \cdot 3 \cdot 7 \cdot 3 &= 63, & 1 \cdot 3 \cdot 5 \cdot 2 &= 30, \\ 2 \cdot 3 \cdot 5 \cdot 7 &= 210, & 140 + 63 + 30 &= 233, & 233 - 210 &= 23. \end{aligned}$$

在“数不知数”问题中，如果将

3, 5, 7 分别看作模 m_1, m_2, m_3 ; 2, 3, 2 分别看作 b_1, b_2, b_3 ;
 5·7, 3·7, 3·5 分别看作 M_1, M_2, M_3 ; 2, 1, 1 分别看作 M'_1, M'_2, M'_3 ;
 233 作为所构造的整数; 105 作为模 $m = m_1 \cdot m_2 \cdot m_3$.

则它们满足同余式： $M'_i M_i \equiv 1 \pmod{m_i}, \quad i = 1, 2, 3,$
 和 $x \equiv M'_1 M_1 b_1 + \cdots + M'_k M_k b_k \pmod{m}.$

现在考虑“物不知数”问题的推广形式，即中国剩余定理.

定理 1 (中国剩余定理) 设 $m_1, \dots, m_k$ 是 k 个两两互素的正整数. 则对任意的整数 $b_1, \dots, b_k$, 同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ \dots\dots\dots \\ x \equiv b_k \pmod{m_k}. \end{cases} \quad (1)$$

一定有解，且解是惟一的. 事实上，

(i) 若令 $m = m_1 \cdots m_k$, $m = m_i M_i$, $i = 1, \dots, k$,

则同余式组 (1) 的解可表示为

$$x \equiv M'_1 M_1 b_1 + \cdots + M'_k M_k b_k \pmod{m}, \quad (2)$$

其中 $M'_i M_i \equiv 1 \pmod{m_i}$, $i = 1, 2, \dots, k$.

(ii) 若令

$$N_i = m_1 \cdots m_i, \quad i = 1, \dots, k-1,$$

则同余式组 (1) 的解可表示为:

$$x \equiv x_k \pmod{m_1 \cdots m_k},$$

其中 $N'_i N_i \equiv 1 \pmod{m_{i+1}}$, $i = 1, 2, \dots, k-1$, 而 x_i 是同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ \dots\dots\dots \\ x \equiv b_i \pmod{m_i}. \end{cases}$$

的解, $i = 1, \dots, k$, 并满足递归关系式

$$x_i \equiv x_{i-1} + N_{i-1} (N'_{i-1} (b_i - x_{i-1}) \pmod{m_i}) \pmod{m_1 \cdots m_i}$$

$$i = 2, \dots, k$$

证 首先证解的惟一性. 设 x, x' 都是满足同余式 (1) 式的解, 则 $x \equiv b_i \equiv x' \pmod{m_i}, \quad i = 1, \dots, k.$

因为 $m_1, \dots, m_k$ 是两两互素的, 所以 $x \equiv x' \pmod{m}.$

再证明解的存在性.

(i) 直接构造同余式组的解:

根据假设, 对任意给定的 $i, 1 \leq i \leq k$, 有 $(m_i, m_j) = 1, 1 \leq j \leq k, j \neq i$, 又根据 §1.4 定理 3, 有 $(m_i, M_i) = 1.$

运用广义欧里得除法, 求出整数 M'_i , 使得 $M'_i M_i \equiv 1 \pmod{m_i},$ 这样, 构造出形为 (2) 的整数, 即 $x = M'_1 M_1 b_1 + \dots + M'_k M_k b_k \pmod{m}.$

因为 $m = m_i M_i$ 及 $m_i | M_j, 1 \leq j \leq k, j \neq i$, 所以这个整数 x 满足同余式 $x \equiv M'_i M_i b_i \equiv b_i \pmod{m_i}, \quad i = 1, \dots, k.$

也就是说, 形为 (2) 式的整数是同余式 (1) 式的解.

例 1 求解同余式组

$$\begin{cases} x \equiv b_1 \pmod{5}, \\ x \equiv b_2 \pmod{6}, \\ x \equiv b_3 \pmod{7}, \\ x \equiv b_4 \pmod{11}. \end{cases}$$

解 令 $m = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$,

$$M_1 = 6 \cdot 7 \cdot 11 = 462, \quad M_2 = 5 \cdot 7 \cdot 11 = 385,$$

$$M_3 = 5 \cdot 6 \cdot 11 = 330, \quad M_4 = 5 \cdot 6 \cdot 7 = 210.$$

分别求解同余式 $M'_i M_i \equiv 1 \pmod{m_i}$, $i = 1, 2, 3, 4$.

得到 $M'_1 = 3$, $M'_2 = 1$, $M'_3 = 1$, $M'_4 = 1$.

故同余式组的解为

$$x \equiv 3 \cdot 462 \cdot b_1 + 385 \cdot b_2 + 330 \cdot b_3 + 210 \cdot b_4 \pmod{2310}.$$

例 2 韩信点兵：有兵一队，若列成五行纵队，则末行一人；成六行纵队，则末行五人；成七行纵队，则末行四人；成十一行纵队，则末行十人．求兵数．

解 韩信点兵问题可转化为同余式组

$$\begin{cases} x \equiv 1 \pmod{5}, \\ x \equiv 5 \pmod{6}, \\ x \equiv 4 \pmod{7}, \\ x \equiv 10 \pmod{11}. \end{cases}$$

解一 对 $b_1 = 1, b_2 = 5, b_3 = 4, b_4 = 10$ 应用例 1, 得到

$$\begin{aligned} x &\equiv 3 \cdot 462 + 385 \cdot 5 + 330 \cdot 4 + 210 \cdot 10 \\ &\equiv 6731 \\ &\equiv 2111 \pmod{2310}. \end{aligned}$$

解二: 归纳构造同余式组的解.

令 $N_1 = 5$. 同余式组的第一个同余式有解 $x \equiv x_1 \equiv 1 \pmod{5}$, 将同余式组的解表示为 (y 待定参数) $x = 1 + 5y$. 将 x 代入同余式组的第二个同余式, 有 $1 + 5y \equiv 5 \pmod{6}$, 或 $5y \equiv 4 \pmod{6}$.

对整数 $N_1 = 5$ 及模 $m_2 = 6$, 可求出整数 $N'_1 \equiv N_1^{-1} \equiv 5 \pmod{6}$, 故 $y \equiv 5 \cdot 4 \equiv 2 \pmod{6}$. 同余式组的解为 $x = x_2 = 1 + 5 \cdot 2 \equiv 11 \pmod{30}$.

将它表为 (y 待定参数) $x = x_2 = 11 + 30y$. 代入同余式组的第三个同余式, 有 $11 + 30y \equiv 4 \pmod{7}$, 或 $30y \equiv 4 - 11 \equiv 0 \pmod{7}$. 对整数 $N_2 = 30$ 及模 $m_3 = 7$, 可求出整数 $N'_2 \equiv N_2^{-1} \equiv 4 \pmod{7}$,

故 $y \equiv 4 \cdot 0 \pmod{7}$. 同余式组的解为 $x = x_3 = 11 + 30 \cdot 0 \equiv 11 \pmod{210}$.

将它表示为 (y 待定参数) $x = x_3 = 11 + 210y$. 代入同余式组的

第四个同余式，我们有

$$11 + 210y \equiv 10 \pmod{11}, \quad \text{或} \quad 210y \equiv 10 - 11 \equiv 10 \pmod{11}.$$

运用广义欧几里得除法，对整数 $N_3 = 210$ 及模 $m_4 = 11$ ，可求出整数 $N'_3 \equiv N_3^{-1} \equiv 1 \pmod{11}$ ，我们有

$$y \equiv 1 \cdot 10 \pmod{11}.$$

故同余式组的解为

$$x = x_3 = 11 + 210 \cdot 10 \equiv 2111 \pmod{210}.$$

应用中国剩余定理，可将一些复杂的运算转化为较简单的运算。

例 3 计算 $2^{1000000} \pmod{77}$ 。

解一 利用 Euler 定理及模重复平方算法直接计算。

因为 $\varphi(77) = \varphi(7)\varphi(11) = 60$ ，所以 $2^{60} \equiv 1 \pmod{77}$ 。又 $1000000 = 16666 \cdot 60 + 40$ ，所以 $2^{1000000} = (2^{60})^{16666} \cdot 2^{40} \equiv 2^{40} \pmod{77}$ 。设 $m = 77$ ， $b = 2$ 。令 $a = 1$ 。 $40 = 2^3 + 2^5$ 。

运用模重复平方法，依次计算如下：

- 1). $n_0 = 0$. 计算 $a_0 = a \equiv 1$, $b_1 \equiv b^2 \equiv 4 \pmod{77}$.
- 2). $n_1 = 0$. 计算 $a_1 = a_0 \equiv 1$, $b_2 \equiv b_1^2 \equiv 16 \pmod{77}$.
- 3). $n_2 = 0$. 计算 $a_2 = a_1 \equiv 1$, $b_3 \equiv b_2^2 \equiv 25 \pmod{77}$.
- 4). $n_3 = 1$. 计算 $a_3 = a_2 \cdot b_3 \equiv 25$, $b_4 \equiv b_3^2 \equiv 9 \pmod{77}$.
- 5). $n_4 = 0$. 计算 $a_4 = a_3 \equiv 25$, $b_5 \equiv b_4^2 \equiv 4 \pmod{77}$.
- 6). $n_5 = 1$. 计算 $a_5 = a_4 \cdot b_5 \equiv 23 \pmod{77}$.

最后，计算出 $2^{1000000} \equiv 23 \pmod{77}$ 。

解二 令 $x = 2^{1000000}$. 因为 $77 = 7 \cdot 11$, 所以计算 $x \pmod{77}$ 等价于求解同余式组
$$\begin{cases} x \equiv b_1 \pmod{7} \\ x \equiv b_2 \pmod{11}. \end{cases}$$

因为 Euler 定理给出 $2^{\varphi(7)} \equiv 2^6 \equiv 1 \pmod{7}$, 以及 $1000000 = 166666 \cdot 6 + 4$, 所以 $b_1 \equiv 2^{1000000} \equiv (2^6)^{166666} \cdot 2^4 \equiv 2 \pmod{7}$.

类似地, 因为 $2^{\varphi(11)} \equiv 2^{10} \equiv 1 \pmod{11}$, $1000000 = 100000 \cdot 10$, 所以 $b_2 \equiv 2^{1000000} \equiv (2^{10})^{100000} \equiv 1 \pmod{11}$.

令 $m_1 = 7$, $m_2 = 11$, $m = m_1 \cdot m_2 = 77$, $M_1 = m_2 = 11$, $M_2 = m_1 = 7$, 分别求解同余式 $11M'_1 \equiv 1 \pmod{7}$, $7M'_2 \equiv 1 \pmod{11}$.

得到 $M'_1 = 2$, $M'_2 = 8$. 故

$$x \equiv 2 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 1 \equiv 100 \equiv 23 \pmod{77}.$$

因此, $2^{1000000} \equiv 23 \pmod{77}$.

定理 2 在定理 1 的条件下, 若 $b_1, \dots, b_k$ 分别遍历模 $m_1, \dots, m_k$ 的完全剩余系, 则 $x \equiv M'_1 M_1 b_1 + \dots + M'_k M_k b_k \pmod{m}$ 遍历模 $m = m_1 \cdots m_k$ 的完全剩余系.

证 令 $x_0 = M'_1 M_1 b_1 + \dots + M'_k M_k b_k \pmod{m}$, 则当 $b_1, \dots, b_k$ 分别遍历模 $m_1, \dots, m_k$ 的完全剩余系时, x_0 遍历 $m_1 \cdots m_k$ 个数. 如果能够证明它们模 m 两两不同余, 则定理成立. 事实上, 若 $M'_1 M_1 b_1 + \dots + M'_k M_k b_k \equiv M'_1 M_1 b'_1 + \dots + M'_k M_k b'_k \pmod{m}$, 则根据 §2.1 定理 11, $M'_i M_i b_i \equiv M'_i M_i b'_i \pmod{m_i}$, $i = 1, \dots, k$. 因为 $M'_i M_i \equiv 1 \pmod{m_i}$, $i = 1, \dots, k$, 所以, $b_i \equiv b'_i \pmod{m_i}$, $i = 1, \dots, k$. 但 b_i, b'_i 是同一个完全剩余系中的两个数, 故

$$b_i = b'_i, \quad i = 1, \dots, k.$$

定理成立.

现在我们考虑高次同余式的求解.

定理 1 设 $m_1, \dots, m_k$ 两两互素, $m = m_1 \cdots m_k$. 则

$$f(x) \equiv 0 \pmod{m} \quad (1) \quad \Leftrightarrow \quad \begin{cases} f(x) \equiv 0 \pmod{m_1}, \\ \dots\dots\dots \\ f(x) \equiv 0 \pmod{m_k} \end{cases} \quad (2)$$

若 T_i 为 $f(x) \equiv 0 \pmod{m_i}$ 的解数, T 为 (1) 的解数, 则 $T = T_1 \cdots T_k$.

例 1 解同余式 $f(x) \equiv x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{35}$.

解 由定理 1 知原同余式等价于同余式组
$$\begin{cases} f(x) \equiv 0 \pmod{5}, \\ f(x) \equiv 0 \pmod{7}. \end{cases}$$

直接验算,

$f(x) \equiv 0 \pmod{5}$ 的解为 $x \equiv 1, 4 \pmod{5}$,

$f(x) \equiv 0 \pmod{7}$ 的解为 $x \equiv 3, 5, 6 \pmod{7}$.

根据中国剩余定理, 可求得同余式组
$$\begin{cases} x \equiv b_1 \pmod{5} \\ x \equiv b_2 \pmod{7} \end{cases}$$

的解为 $x \equiv 3 \cdot 7 \cdot b_1 + 3 \cdot 5 \cdot b_2 \pmod{35}$.

故原同余式的解为

$$x \equiv 31, 26, 6, 24, 19, 34 \pmod{35},$$

共 $2 \cdot 3 = 6$ 个.

因为 $m = \pi_p p^\alpha$, 所以要求解同余式 $f(x) \equiv 0 \pmod{m}$, 只须求解同余式 $f(x) \equiv 0 \pmod{p^\alpha}$.

我们讨论 p 为素数时, $f(x) \equiv 0 \pmod{p^\alpha}$ (3) 的解法.

设 $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ 为整系数多项式, 我们记 $f'(x) = na_n x^{n-1} + \cdots + 2a_2 x + a_1$. 称 $f'(x)$ 为 $f(x)$ 的 **导式**.

定理 2 设 $x \equiv x_1 \pmod{p}$ 是同余式 $f(x) \equiv 0 \pmod{p}$ (4) 的一个解, 且 $(f'(x_1), p) = 1$, 则同余式 (3) 有解 $x \equiv x_\alpha \pmod{p^\alpha}$, 其中 x_α 由下面关系式递归得到:

$$\begin{cases} x_i \equiv x_{i-1} + p^{i-1} t_{i-1} & \pmod{p^i}, \\ t_{i-1} \equiv -\frac{f(x_{i-1})}{p^{i-1}} (f'(x_1)^{-1} \pmod{p}) \pmod{p}, \end{cases}$$

$i = 2, \dots, \alpha.$

例 2 求解同余式 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \pmod{27}$.

解一 (按照定理 2 的证明过程)

对于 $f(x) \equiv x^4 + 7x + 4 \pmod{27}$, 有 $f'(x) \equiv 4x^3 + 7 \pmod{27}$.

直接验算, 知同余式 $f(x) \equiv 0 \pmod{3}$ 有一解 $x_1 \equiv 1 \pmod{3}$.

以 $x = 1 + 3t_1$ 代入 $f(x) \equiv 0 \pmod{9}$, 可得 $f(1) + 3t_1 f'(1) \equiv 0 \pmod{9}$.

因为 $f(1) \equiv 3 \pmod{9}$, $f'(1) \equiv 2 \pmod{9}$, 所以上述同余式可写成 $3 + 3t_1 \cdot 2 \equiv 0 \pmod{9}$ 或 $2t_1 \equiv -1 \pmod{3}$. 解得 $t_1 \equiv 1 \pmod{3}$,

故 $f(x) \equiv 0 \pmod{9}$ 的解为 $x_2 \equiv 1 + 3t_1 \equiv 4 \pmod{9}$.

再以 $x = 4 + 9t_2$ 代入 $f(x) \equiv 0 \pmod{27}$, 得 $f(4) + 9t_2 f'(4) \equiv 0 \pmod{27}$.

因为 $f(4) \equiv 18 \pmod{27}$, $f'(4) \equiv 20 \pmod{27}$, 所以上述同余式可写成 $18 + 9t_2 \cdot 20 \equiv 0 \pmod{27}$ 或 $2t_2 \equiv -2 \pmod{3}$. 解得 $t_2 \equiv 2 \pmod{3}$,

因此, 同余式 $f(x) \equiv 0 \pmod{27}$ 的解为 $x_3 \equiv 4 + 9t_2 \equiv 22 \pmod{27}$.

解二 (应用定理 2 的结论)

对于 $f(x) \equiv x^4 + 7x + 4 \pmod{27}$, 有 $f'(x) \equiv 4x^3 + 7 \pmod{27}$.

直接验算, 知同余式 $f(x) \equiv 0 \pmod{3}$ 有一解 $x_1 \equiv 1 \pmod{3}$.

首先, 计算 $f'(x_1) = 4 \cdot 1^3 + 7 \equiv -1 \pmod{3}$, $f'(x_1)^{-1} \equiv -1 \pmod{3}$;

其次, 计算
$$\left\{ \begin{array}{l} t_1 \equiv -\frac{f(x_1)}{3^1} (f'(x_1)^{-1} \pmod{3}) \equiv 1 \pmod{3}, \end{array} \right.$$

$$\left\{ \begin{array}{l} x_2 \equiv x_1 + 3t_1 \equiv 4 \pmod{9}; \end{array} \right.$$

$$\left\{ \begin{array}{l} t_2 \equiv -\frac{f(x_2)}{3^2} (f'(x_1)^{-1} \pmod{3}) \equiv 2 \pmod{3}, \end{array} \right.$$

最后, 计算
$$\left\{ \begin{array}{l} x_3 \equiv x_2 + 3^2 t_2 \equiv 22 \pmod{27}. \end{array} \right.$$

因此, 同余式 $f(x) \equiv 0 \pmod{27}$ 的解为 $x_3 \equiv 22 \pmod{27}$.

考虑 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$ (1) 其中 $p \nmid a_n$.

引理 (多项式欧里得除法) 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 为 n 次整系数多项式, $g(x) = x^m + \cdots + b_1 x + b_0$ 为 $m \geq 1$ 次首一整系数多项式, 则存在整系数多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x) = g(x)q(x) + r(x), \quad \deg r(x) < \deg g(x).$$

证 分两种情形: (I) $n < m$. 取 $q(x) = 0$, $r(x) = f(x)$, 结论成立.

(II) $n \geq m$. 对 $f(x)$ 的次数 n 作数学归纳法. $n = m$. 我们有

$$f(x) - a_n \cdot g(x) = (a_{n-1} - a_n b_{m-1})x^{n-1} + \cdots + (a_1 - a_n b_0)x + a_0.$$

因此, $q(x) = a_n x$, $r(x) = f(x) - a_n x \cdot g(x)$ 为所求.

假设 $n - 1 \geq m$ 时, 结论成立.

对于 $n > m$, 我们有

$$\begin{aligned} & f(x) - a_n x^{n-m} \cdot g(x) \\ &= (a_{n-1} - a_n b_{m-1})x^{n-1} + \cdots + (a_{n-m} - a_n b_0)x^{n-m} \\ & \quad + a_{n-m-1}x^{n-m-1} + \cdots + a_0. \end{aligned}$$

这说明 $f(x) - a_n x^{n-m} \cdot g(x)$ 是次数 $\leq n-1$ 的多项式. 对其运用归纳假设或情形 (I), 存在整系数多项式 $q_1(x)$ 和 $r_1(x)$ 使得

$$f(x) - a_n x^{n-m} \cdot g(x) = g(x)q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x).$$

因此, $q(x) = a_n x^{n-m} + q_1(x)$, $r(x) = r_1(x)$ 为所求.

根据数学归纳法原理, 结论是成立的. 证毕.

因为多项式 $x^p - x \pmod{p}$ 对任何整数取值为零, 所以借助于它以及多项式欧几里得除法, 可将高次多项式的求解转化为次数不超过 $p-1$ 的多项式的求解, 即有

定理 1 同余式 (1) 与一个次数不超过 $p-1$ 模 p 同余式等价.

证 由欧里得除法, 存在 $q(x)$, $r(x)$ 使得 $f(x) = (x^p - x)q(x) + r(x)$, 其中 $\deg r(x) \leq p-1$. 又对任何整数 x , 都有 $x^p - x \equiv 0 \pmod{p}$.

故同余式 $f(x) \equiv 0 \pmod{p}$ 等价于同余式 $r(x) \equiv 0 \pmod{p}$.

例 1 求与同余式 $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod{5}$ 等价的次数 < 5 的同余式.

解 作多项式的欧里得除法, 我们有

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ &= (x^5 - x)(3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5) \\ & \quad + 3x^3 + 16x^2 + 6x. \end{aligned}$$

所以原同余式等价于 $3x^3 + 16x^2 + 6x \equiv 0 \pmod{5}$.

定理 2 设 $1 \leq k \leq n$. 如果 $x \equiv a_i \pmod{p}$ 是 (1) 的 k 个不同解, 则对任何整数 x , 都有 $f(x) \equiv (x - a_1) \cdots (x - a_k) f_k(x) \pmod{p}$, (2)
其中 $f_k(x)$ 是 $n - k$ 次多项式, 首项系数是 a_n .

例 2 我们有同余式

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ & \equiv x(x-1)(x-2)(3x^{11} + 3x^{10} + 3x^9 + 4x^7 + 3x^6 + x^5 + 2x^4 + x^2 + 3x + 3) \pmod{5}. \end{aligned}$$

现在讨论模 p 同余式解数. 首先给出同余式解数的上界估计.

定理 4 同余式 (1) 的解数不超过它的次数.

推论 次数 $< p$ 的整系数多项式对所有整数取值模 p 为零的充要条件是其系数被 p 整除.

现在给出同余式解数的判断.

定理 5 设 $n \leq p$. 则 $f(x) = x^n + \cdots + a_1x + a_0 \equiv 0 \pmod{p}$, (3)

有 n 个解的充分必要条件是 $x^p - x$ 被 $f(x)$ 除所得余式的所有系数都是 p 的倍数.

推论 设 p 是一个素数, d 是 $p-1$ 的正因数. 那么多项式 $x^d - 1$ 模 p 有 d 个不同的根.

证 因为 $d|p-1$, 所以存在整数 q 使得 $p-1 = dq$. 这样, 我们有因式分解式:

$$x^{p-1} - 1 = (x^d - 1)(x^{d(p-1)} + x^{d(p-2)} + \cdots + x^d + 1).$$

根据定理 5, 多项式 $x^d - 1$ 模 p 有 d 个不同的根.

例 3 判断同余式 $2x^3 + 5x^2 + 6x + 1 \equiv 0 \pmod{7}$ 是否有三个解.

解 为应用定理 5, 须将多项式变成首一的. 注意到 $4 \cdot 2 \equiv 1 \pmod{7}$, 我们有 $4(2x^3 + 5x^2 + 6x + 1) \equiv x^3 - x^2 + 3x - 3 \pmod{7}$. 此同余式与原同余式等价. 作多项式的欧里得除法, 我们有

$$x^7 - x = (x^3 - x^2 + 3x - 3)(x^3 + x^2 - 2x - 2)x + 7x(x^2 - 1).$$

根据定理 5, 原同余式的解数为 3.

例 4 求解同余式 $21x^{18} + 2x^{15} - x^{10} + 4x - 3 \equiv 0 \pmod{7}$.

解 首先, 去掉系数为 7 的倍数的项, 得 $2x^{15} - x^{10} + 4x - 3 \equiv 0 \pmod{7}$.

其次, 作多项式的欧里得除法, 我们有

$$2x^{15} - x^{10} + 4x - 3 = (x^7 - x)(2x^8 - x^3 + 2x^2) + (-x^4 + 2x^3 + 4x - 3).$$

原同余式等价于同余式 $x^4 - 2x^3 - 4x + 3 \equiv 0 \pmod{7}$.

直接验算 $x = 0, \pm 1, \pm 2, \pm 3$, 知同余式无解.

例 5 求解同余式 $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod{5}$.

解一 作多项式的欧几里得除法, 我们有

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ &= (x^5 - x)(3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5) + 3x^3 + 16x^2 + 6x \end{aligned}$$

原同余式等价于 $3x^3 + 16x^2 + 6x \equiv 3x^3 + x^2 + x \pmod{5}$.

直接验算, 解为 $x \equiv 0, 1, 2 \pmod{5}$.

解二 由恒等同余式 $x^p - x \equiv 0 \pmod{p}$, 可得, 对于任意正整数 t, k , $x^{t+k(p-1)} \equiv x^t \pmod{p}$. 特别 ($p = 5$),

$$x^{14} \equiv x^{10} \equiv x^6 \equiv x^2, \quad x^{13} \equiv x^9 \equiv x^5 \equiv x, \quad x^{11} \equiv x^7 \equiv x^3, \pmod{5}.$$

因此, 原同余式等价于 $3x^3 + 16x^2 + 6x \equiv 0 \pmod{5}$. 进而等价于 $2(3x^3 + 16x^2 + 6x) \equiv x^3 + 2x^2 + 2x \equiv 0 \pmod{5}$.

直接验算，同余式的解为 $x \equiv 0, 1, 2 \pmod{5}$.

第四章 二次同余式与平方剩余

本章主要讨论如下问题.

1. 二次同余式的基本概念
2. 模平方剩余与模平方非剩余
3. 勒让得符号 二次互反律
4. 二次同余式有解的判断
5. 高斯引理 二次互反律之证明
6. 雅克比符号
7. 模 p 平方根的计算
8. 椭圆曲线点的计算

二次同余式的一般形式是 $ax^2 + bx + c \equiv 0 \pmod{m}$ (1) 其中 $m \nmid a$.

因为 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, 所以二次同余式 (1) 式等价于同余式组:

$$\begin{cases} ax^2 + bx + c \equiv 0 \pmod{p_1^{\alpha_1}}, \\ \dots\dots\dots \\ ax^2 + bx + c \equiv 0 \pmod{p_k^{\alpha_k}}. \end{cases}$$

故只 讨论模为 p^α 同余式: $ax^2 + bx + c \equiv 0 \pmod{p^\alpha}$, $p \nmid a$. (2)

将 (2) 的两端同乘 $4a$, 得到 $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p^\alpha}$ 或 $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p^\alpha}$. 令 $y = 2ax + b$, 有

$$y^2 \equiv b^2 - 4ac \pmod{p^\alpha}.$$

特别地, 当 p 是奇素数时, $(p, 2a) = 1$. 上述同余式等价于 (2).

定义 1 若同余式 $x^2 \equiv a \pmod{m}$, $(a, m) = 1$ (3) 有解, 则 a 叫做模 m 的 **平方剩余**(或 **二次剩余**);

否则, a 叫做模 m 的 **平方非剩余** (或 **二次非剩余**).

问题: 1) 整数 a 模 m 平方剩余与实数中平方根 $\sqrt{a}$ 有什么区别?

2) 如何判断同余式 (3) 有解? 3) 如何求同余式 (3) 的解?

例 1 1 是模 4 平方剩余, -1 是模 4 平方非剩余.

例 2 1, 2, 4 是模 7 平方剩余, -1, 3, 5 是模 7 平方非剩余.

因为 $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 2$, $5^2 \equiv 4$, $6^2 \equiv 1 \pmod{7}$.

例 3 -1, 1, 2, 4, 8, 9, 13, 15 是模 17 平方剩余;

3, 5, 6, 7, 10, 11, 12, 14 是模 17 平方非剩余.

因为 $1^2 \equiv 16^2 \equiv 1$, $2^2 \equiv 15^2 \equiv 4$, $3^2 \equiv 14^2 \equiv 9$, $4^2 \equiv 13^2 \equiv 16 \equiv -1$, $5^2 \equiv 12^2 \equiv 8$, $6^2 \equiv 11^2 \equiv 2$, $7^2 \equiv 10^2 \equiv 15$, $8^2 \equiv 9^2 \equiv 13 \pmod{17}$.

例 4 求满足方程 $E : y^2 = x^3 + x + 1 \pmod{7}$ 的所有点.

解 对 $x = 0, 1, 2, 3, 4, 5, 6$, 分别求出 y .

$$x = 0, y^2 = 1 \pmod{7}, \quad y = 1, 6 \pmod{7},$$

$$x = 1, y^2 = 3 \pmod{7}, \quad \text{无解},$$

$$x = 2, y^2 = 4 \pmod{7}, \quad y = 2, 5 \pmod{7},$$

$$x = 3, y^2 = 3 \pmod{7}, \quad \text{无解},$$

$$x = 4, y^2 = 6 \pmod{7}, \quad \text{无解},$$

$$x = 5, y^2 = 5 \pmod{7}, \quad \text{无解},$$

$$x = 6, y^2 = 6 \pmod{7}, \quad \text{无解}.$$

例 5 求满足方程 $E : y^2 = x^3 + x + 2 \pmod{7}$ 的所有点.

解 对 $x = 0, 1, 2, 3, 4, 5, 6$, 分别求出 y .

$$x = 0, y^2 = 2 \pmod{7}, \quad y = 3, 4 \pmod{7},$$

$$x = 1, y^2 = 4 \pmod{7}, \quad y = 2, 5 \pmod{7},$$

$$x = 2, y^2 = 5 \pmod{7}, \quad \text{无解},$$

$$x = 3, y^2 = 4 \pmod{7}, \quad y = 2, 5 \pmod{7},$$

$$x = 4, y^2 = 0 \pmod{7}, \quad y = 0 \pmod{7},$$

$$x = 5, y^2 = 6 \pmod{7}, \quad \text{无解},$$

$$x = 6, y^2 = 0 \pmod{7}, \quad y = 0 \pmod{7}.$$

讨论模为素数 p 的二次同余式 $x^2 \equiv a \pmod{p}$, $(a, p) = 1$. (1)

定理 1 (欧拉判别条件) 设 p 是奇素数, $(a, p) = 1$. 则

(i) a 是模 p 的平方剩余的充分必要条件是 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$; (2)

(ii) a 是模 p 的平方非剩余的充分必要条件是 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. (3)

并且当 a 是模 p 的平方剩余时, 同余式 (1) 恰有二解.

证 (i) 因为 p 是奇素数, 所以有表达式

$$x^p - x = x\left((x^2)^{\frac{p-1}{2}} - a^{\frac{p-1}{2}}\right) + (a^{\frac{p-1}{2}} - 1)x = (x^2 - a)xq(x) + (a^{\frac{p-1}{2}} - 1)x,$$

其中 $q(x)$ 是 x 的整系数多项式.

若 a 是模 p 的平方剩余, 即 $x^2 \equiv a \pmod{p}$ 有二个解 x , 根据 §3.4 定理 5, 余式的系数被 p 整除, 即 $p | a^{\frac{p-1}{2}} - 1$. 所以 (2) 成立.

反过来, 若 (2) 成立, 则同余式 $x^2 \equiv a \pmod{p}$ 有解, 即 a 是模 p 平方剩余.

(ii) 因为 p 是奇素数, $(a, p) = 1$, 根据欧拉定理, 有

$$(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) = a^{p-1} - 1 \equiv 0 \pmod{p}.$$

再根据 §1.4 定理 2, 我们有 $p \mid a^{\frac{p-1}{2}} - 1$ 或 $p \mid a^{\frac{p-1}{2}} + 1$. 因此, 结论 (i) 告诉我们: a 是模 p 的平方非剩余的充要条件是 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

推论 设 p 是奇素数, $(a_1, p) = 1$, $(a_2, p) = 1$. 则

- (i) 若 a_1, a_2 是模 p 的平方剩余, 则 $a_1 a_2$ 是模 p 的平方剩余;
- (ii) 若 a_1, a_2 是模 p 的平方非剩余, 则 $a_1 a_2$ 是模 p 的平方剩余;
- (iii) 如 a_1 是模 p 平方剩余, a_2 模 p 平方非剩余, 则 $a_1 a_2$ 是模 p 的平方非剩余.

证 因为 $(a_1 a_2)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}}$,

所以由定理 1 即得结论.

例 1 判断 137 是否为模 227 平方剩余.

解 根据定理 1, 我们要计算: $137^{(227-1)/2} = 137^{113} \pmod{227}$.

运用模重复平方法. 设 $m = 227$, $b = 137$. 令 $a = 1$. 将 113 写成二进制, $113 = 1 + 2^4 + 2^5 + 2^6$. 我们依次计算如下:

- 1). $n_0 = 1$. 计算 $a_0 = a \cdot b^{n_0} \equiv 137$, $b_1 \equiv b^2 \equiv 155 \pmod{227}$.
- 2). $n_1 = 0$. 计算 $a_1 = a_0 \cdot b_1^{n_1} \equiv 137$, $b_2 \equiv b_1^2 \equiv 190 \pmod{227}$.
- 3). $n_2 = 0$. 计算 $a_2 = a_1 \cdot b_2^{n_2} \equiv 137$, $b_3 \equiv b_2^2 \equiv 7 \pmod{227}$.
- 4). $n_3 = 0$. 计算 $a_3 = a_2 \cdot b_3^{n_3} \equiv 137$, $b_4 \equiv b_3^2 \equiv 49 \pmod{227}$.
- 5). $n_4 = 1$. 计算 $a_4 = a_3 \cdot b_4^{n_4} \equiv 130$, $b_5 \equiv b_4^2 \equiv 131 \pmod{227}$.
- 6). $n_5 = 1$. 计算 $a_5 = a_4 \cdot b_5^{n_5} \equiv 5$, $b_6 \equiv b_5^2 \equiv 136 \pmod{227}$.
- 7). $n_6 = 1$. 计算 $a_6 = a_5 \cdot b_6^{n_6} \equiv 226 \equiv -1 \pmod{227}$.

因此, 137 为模 227 平方非剩余.

定理 2 设 p 是奇素数. 则模 p 的简化剩余系中平方剩余与平方非剩余的个数各为 $(p-1)/2$, 且 $(p-1)/2$ 个平方剩余与序列:
 $1^2, 2^2, \dots, (\frac{p-1}{2})^2$ (4) 中的一个数同余, 且仅与一个数同余.

§4.2 定理 1 给出了整数 a 是否是模奇素数 p 二次剩余的判别法则, 但需要作较复杂的运算. 我们希望有一种更简单的判别法则.

定义 1 设 p 是素数. 定义 **勒让得 (Legendre) 符号** 如下:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{若 } a \text{ 是模 } p \text{ 的平方剩余;} \\ -1, & \text{若 } a \text{ 是模 } p \text{ 的平方非剩余;} \\ 0, & \text{若 } p|a. \end{cases}$$

例 1 根据 §4.1 例 3, 我们有

$$\left(\frac{-1}{17}\right) = \left(\frac{1}{17}\right) = \left(\frac{2}{17}\right) = \left(\frac{4}{17}\right) = \left(\frac{8}{17}\right) = \left(\frac{9}{17}\right) = \left(\frac{13}{17}\right) = \left(\frac{15}{17}\right) = 1;$$

$$\left(\frac{3}{17}\right) = \left(\frac{5}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{11}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{14}{17}\right) = -1.$$

利用勒让得符号, 可将 §4.2 定理 1 叙述为:

定理 1 (欧拉判别法则) 对任意整数 a , $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

例 2 证明 2 是模 17 平方剩余; 3 是模 17 平方非剩余.

因为 $(17-1)/2 = 2^3$, 且有 $2^2 \equiv 4$, $2^4 \equiv 4^2 \equiv -1$, $2^8 \equiv (-1)^2 \equiv 1$;
 $3^2 \equiv 9$, $3^4 \equiv 9^2 \equiv -4$, $3^8 \equiv (-4)^2 \equiv -1 \pmod{17}$.

推论 1 设 p 是奇素数, 则 (1) $\left(\frac{1}{p}\right) = 1$; (2) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

推论 2 设 p 是奇素数, 那么 $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{若 } p \equiv 1 \pmod{4}; \\ -1, & \text{若 } p \equiv 3 \pmod{4}. \end{cases}$

定理 2 设 p 是奇素数, 则 (i) $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$;
(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$; (iii) 设 $(a, p) = 1$, 则 $\left(\frac{a^2}{p}\right) = 1$.

证 (i) 因为同余式 $x^2 \equiv a + p \pmod{p}$ 等价于同余式 $x^2 \equiv a \pmod{p}$, 所以 $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$.

(ii) 根据欧拉判别法则, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \pmod{p}$ 以及 $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod{p}$. 因此

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}.$$

因为勒让得符号取值 ± 1 , 且 p 是奇素数, 所以有 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

推论 设 p 是奇素数. 若 $a \equiv b \pmod{p}$, 则 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

对与 p 互素的 a , Gauss 给出了另一判别法则, 以判断 a 是否为模 p 二次剩余.

引理 (Gauss) 设 p 奇素数. $(a, p) = 1$. 若 $a \cdot 1, a \cdot 2, \dots, a \cdot \frac{p-1}{2}$ 中模 p 的最小正剩余大于 $\frac{p}{2}$ 的个数是 m , 则 $\left(\frac{a}{p}\right) = (-1)^m$.

定理 3 (i) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. (ii) 若 $(a, 2p) = 1$, 则

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left[\frac{ak}{p}\right]}.$$

推论 设 p 是奇素数, 那么

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{若 } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{若 } p \equiv \pm 3 \pmod{8}. \end{cases}$$

证 根据定理 3 (i), 我们有

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

若 $p \equiv \pm 1 \pmod{8}$, 则存在正整数 k 使得 $p = 8k \pm 1$. 从而

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2(4k^2 \pm k)} = 1.$$

若 $p \equiv \pm 3 \pmod{8}$, 则存在正整数 k 使得 $p = 8k \pm 3$. 从而

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2(4k^2 \pm 3k) + 1} = -1.$$

定理 4 (二次互反律) 若 p, q 是互素奇素数, 则

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) \quad (9)$$

例 3 2 是模 17 平方剩余; 3 是模 17 平方非剩余.

解 根据定理 3 (i), $\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = (-1)^{2 \cdot 18} = 1$.

因此, 2 是模 17 平方剩余.

根据定理 4,

$$\left(\frac{3}{17}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{17-1}{2}} \left(\frac{17}{3}\right).$$

又根据定理 2 (i) 和定理 1 之推论 1 (ii), $\left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$,
因此, $\left(\frac{3}{17}\right) = -1$, 3 是模 17 平方非剩余.

例 4 判断同余式 $x^2 \equiv 137 \pmod{227}$ 是否有解.

解 因为 227 是素数, 根据定理 2,

$$\left(\frac{137}{227}\right) = \left(\frac{-90}{227}\right) = \left(\frac{-1}{227}\right) \left(\frac{2 \cdot 3^2 \cdot 5}{227}\right) = - \left(\frac{2}{227}\right) \left(\frac{5}{227}\right).$$

由定理 3 (i), 我们有

$$\left(\frac{2}{227}\right) = (-1)^{\frac{227^2-1}{8}} = (-1)^{\frac{226 \cdot 228}{8}} = -1.$$

又由定理 4 及定理 3 (i), 我们有

$$\left(\frac{5}{227}\right) = (-1)^{\frac{5-1}{2} \frac{227-1}{2}} \left(\frac{227}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

因此, $\left(\frac{137}{227}\right) = -1$. 同余式 $x^2 \equiv 137 \pmod{227}$ 无解.

例 5 判断 $x^2 \equiv -1 \pmod{365}$ 是否有解, 有解时, 求出其解数.

解 $365 = 5 \cdot 73$ 不是素数, 原同余式等价于:

$$\begin{cases} x^2 \equiv -1 \pmod{5}, \\ x^2 \equiv -1 \pmod{73}. \end{cases}$$

因为 $\left(\frac{-1}{5}\right) = \left(\frac{-1}{73}\right) = 1$, 故同余式组有解. 原同余式有解, 解数为 4.

例 6 判断 $x^2 \equiv 2 \pmod{3599}$ 是否有解, 有解时求出其解数.

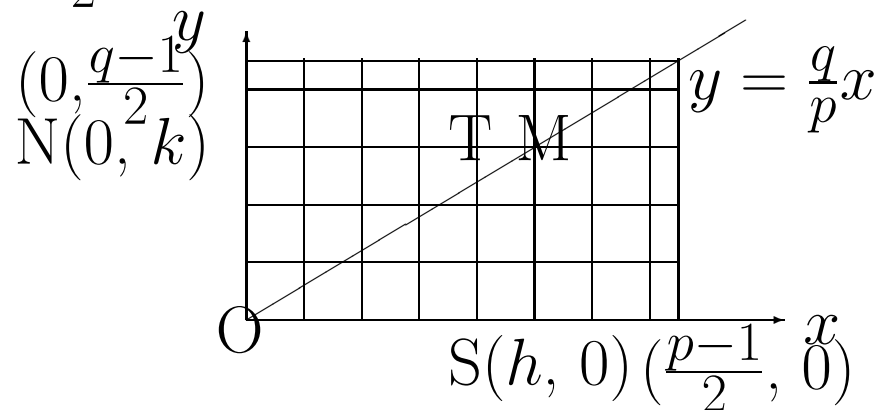
解 $3599 = 59 \cdot 61$ 不是素数, 原同余式等价于:

$$\begin{cases} x^2 \equiv 2 \pmod{59}, \\ x^2 \equiv 2 \pmod{61}. \end{cases}$$

因为 $\left(\frac{2}{59}\right) = (-1)^{(59^2-1)/8} = -1$, 故同余式组无解. 原同余式无解.

§4.3 定理 4 之证明: 要证明: $\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$

因为 $(2, pq) = 1$, 有 $\left(\frac{q}{p}\right) = (-1)^{\sum_{h=1}^{\frac{p-1}{2}} \left[\frac{qh}{p}\right]}, \quad \left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \left[\frac{pk}{q}\right]},$
 所以只需证明 $\sum_{h=1}^{\frac{p-1}{2}} \left[\frac{qh}{p}\right] + \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{pk}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$



考察长为 $\frac{p}{2}$, 宽为 $\frac{q}{2}$ 的长方形内的整点个数: 在垂直直线 ST

上, 整点个数为 $\left[\frac{qh}{p}\right]$, 因此, 下三角形内的整点个数为 $\sum_{h=1}^{\frac{p-1}{2}} \left[\frac{qh}{p}\right];$

在水平直线 NM 上, 整点个数为 $\left[\frac{pk}{q}\right]$, 因此, 上三角形内的整

点个数为 $\sum_{k=1}^{\frac{q-1}{2}} \left[\frac{pk}{q}\right]$.

因为对角线上无整点, 所以长方形内整点个数为

$$\sum_{h=1}^{\frac{p-1}{2}} \left[\frac{qh}{p}\right] + \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{pk}{q}\right] = \frac{p-1}{2} \frac{q-1}{2}.$$

这就完成了定理 1 的证明. 证毕.

例 1 求所有奇素数 p , 它以 3 为其二次剩余.

解 即要求所有奇素数 p , 使得 $\left(\frac{3}{p}\right) = 1$.

根据二次互反律, $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \left(\frac{p}{3}\right)$. 因为

$$(-1)^{(p-1)/2} = \begin{cases} 1, & \text{当 } p \equiv 1 \pmod{4}; \\ -1, & \text{当 } p \equiv -1 \pmod{4}, \end{cases} \text{ 以及 } \left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1, & \text{当 } p \equiv 1 \pmod{6}; \\ \left(\frac{-1}{3}\right) = -1, & \text{当 } p \equiv -1 \pmod{6}, \end{cases}$$

故 $\left(\frac{-1}{p}\right) = 1$ 的充要条件是 $\begin{cases} p \equiv 1 \pmod{4} \\ p \equiv 1 \pmod{6} \end{cases}$ 或 $\begin{cases} p \equiv -1 \pmod{4} \\ p \equiv -1 \pmod{6}. \end{cases}$

这分别等价于 $p \equiv 1 \pmod{12}$, 或 $p \equiv -1 \pmod{12}$.

因此, 3 是模 p 二次剩余的充分必要条件是 $p \equiv \pm 1 \pmod{12}$.

例 2 设 p 是奇素数, d 是整数. 如果 $\left(\frac{d}{p}\right) = -1$, 则 p 一定不能表示为 $x^2 - dy^2$ 的形式.

证 如果 p 有表达式 $p = x^2 - dy^2$, 则由 p 是素数, 可得到 $(x, p) = (y, p) = 1$. 事实上, 若 $(x, p) \neq 1$, 则

$$p|x, \quad p|x^2 - p = dy^2.$$

但 $(d, p) = 1$, 所以 $p|y^2$, 进而 $p|y$. 这样 $p^2|x^2$, $p^2|y^2$. 从而 $p^2|x^2 - dy^2 = p$. 这不可能. 因此,

$$\left(\frac{d}{p}\right) = \left(\frac{d}{p}\right) \left(\frac{y^2}{p}\right) = \left(\frac{dy^2}{p}\right) = \left(\frac{x^2}{p}\right) = 1.$$

这与题设矛盾.

在勒让得符号的计算中, 要求模 p 为素数. 现在将它推广为一般的模 m .

定义 1 设 $m = p_1 \cdots p_r$ 是奇素数 p_i 的乘积. 对任意整数 a , 定义 **雅可比 (Jacobi) 符号** 为

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

雅可比符号形式上是勒让得符号的推广, 但所蕴含的意义已经不同. 雅可比符号为 -1 , 可判断 a 是模 m 平方非剩余; 但雅可比符号为 1 , 却不能判断 a 是模 m 平方剩余. 例如, 3 是模 119 平方非剩余, 但

$$\left(\frac{3}{119}\right) = \left(\frac{3}{7}\right) \left(\frac{3}{17}\right) = (-1)(-1) = 1.$$

定理 1 设 m 是正奇数. 则 (i) $\left(\frac{a+m}{m}\right) = \left(\frac{a}{m}\right)$;
(ii) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$; (iii) 设 $(a, m) = 1$, 则 $\left(\frac{a^2}{m}\right) = 1$.

证 设 $m = p_1 \cdots p_r$, 其中 p_i 为奇素数. 根据定义,

$$(i) \quad \left(\frac{a+m}{m}\right) = \left(\frac{a+m}{p_1}\right) \cdots \left(\frac{a+m}{p_r}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right) = \left(\frac{a}{m}\right).$$

$$(ii) \quad \left(\frac{ab}{m}\right) = \left(\frac{ab}{p_1}\right) \cdots \left(\frac{ab}{p_r}\right) = \left(\frac{a}{p_1}\right) \left(\frac{b}{p_1}\right) \cdots \left(\frac{a}{p_r}\right) \left(\frac{b}{p_r}\right) \\ = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right) \left(\frac{b}{p_1}\right) \cdots \left(\frac{b}{p_r}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right).$$

$$(iii) \quad \left(\frac{a^2}{m}\right) = \left(\frac{a^2}{p_1}\right) \cdots \left(\frac{a^2}{p_r}\right) = 1.$$

引理: 设 $m = p_1 \cdots p_r$ 是奇数. 则

$$\frac{m-1}{2} \equiv \frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2} \pmod{2};$$
$$\frac{m^2-1}{8} \equiv \frac{p_1^2-1}{8} + \cdots + \frac{p_r^2-1}{8} \pmod{2}.$$

定理 2 设 m 是奇数. 则 (i) $\left(\frac{1}{m}\right) = 1$;

(ii) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$; (iii) $\left(\frac{2}{m}\right) \equiv (-1)^{\frac{m^2-1}{8}}$

定理 3 设 m, n 都是奇数. 则 $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \left(\frac{m}{n}\right)$.

例 1 判断同余式

$$x^2 \equiv 286 \pmod{563}$$

是否有解.

解 不用考虑 563 是否为素数, 直接计算雅可比符号. 因为

$$\left(\frac{286}{563}\right) = \left(\frac{2}{563}\right) \left(\frac{143}{563}\right) = (-1)^{\frac{563^2-1}{8}} (-1)^{\frac{143-1}{2} \cdot \frac{563-1}{2}} \left(\frac{563}{143}\right) = \left(\frac{-9}{143}\right) = \left(\frac{-1}{143}\right) = -1,$$

所以原同余式无解.

例 2 求出 $y^2 \equiv x^3 + x + 1 \pmod{17}$ 的所有解及解数.

解 令 $f(x) = x^3 + x + 1$. 根据 §4.1 例 3, 我们有

$$\begin{array}{ll} f(0) = 1, & y = 1, y = 16; \quad f(1) = 3, \text{ 无解;} \\ f(2) = 11, & \text{无解} \quad f(3) = 14, \text{ 无解;} \\ f(4) = 1, & y = 1, y = 16; \quad f(5) = 12, \text{ 无解;} \\ f(6) = 2, & y = 6, y = 11; \quad f(7) = 11, \text{ 无解;} \\ f(8) = 11, & \text{无解;} \quad f(9) = 8, \quad y = 5, y = 12; \\ f(10) = 8, & y = 5, y = 12; \quad f(11) = 0, \quad y = 0; \\ f(12) = 7, & \text{无解;} \quad f(13) = 1, \quad y = 1, y = 16; \\ f(14) = 5, & \text{无解;} \quad f(15) = 8, \quad y = 5, y = 12; \\ f(16) = -1, & y = 4, y = 13 \pmod{17}. \end{array}$$

故原同余式解: $(0, 1), (0, 16), (4, 1), (4, 16), (6, 6), (6, 11), (9, 5), (9, 12), (10, 5), (10, 12), (11, 0), (13, 1), (13, 16), (15, 5), (15, 12), (16, 4), (16, 13)$.

设 p 为奇素数. 对任意给定的整数 a , 应用高斯二次互反律 (§4.3 定理 4) 可以快速判断 a 是否为模 p 平方剩余, 即二次同余式

$$x^2 \equiv a \pmod{p}$$

是否有解, 也就是说解的存在性.

现在在有解的情况下, 即 a 满足

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \pmod{p}$$

的情况下, 考虑二次同余式的具体求解. 求解过程按照下面的算法进行.

对奇素数 p , 将 $p-1$ 写成 $p-1 = 2^t \cdot s$, $t \geq 1$, 其中 s 是奇数.

(i) 任意选取一个模 p 平方非剩余 n , 即整数 n 使得 $\left(\frac{n}{p}\right) = -1$.

再令 $b := n^s \pmod{p}$. 有 $b^{2^t} \equiv 1$, $b^{2^{t-1}} \equiv -1 \pmod{p}$.

即 b 是模 p 的 2^t 次单位根, 但非模 p 的 2^{t-1} 次单位根.

(ii) 计算 $x_{t-1} := a^{\frac{s+1}{2}} \pmod{p}$. 有 $a^{-1}x_{t-1}^2$ 满足同余式 $y^{2^{t-1}} \equiv 1 \pmod{p}$, 即 $a^{-1}x_{t-1}^2$ 是模 p 的 2^{t-1} 次单位根. 事实上,

$$(a^{-1}x_{t-1}^2)^{2^{t-1}} \equiv a^{2^{t-1}s} \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \equiv 1 \pmod{p}.$$

(iii) 如果 $t = 1$, 则 $x = x_{t-1} = x_0 \equiv a^{\frac{s+1}{2}} \pmod{p}$ 满足 $x^2 \equiv a \pmod{p}$.

如果 $t \geq 2$, 要寻找 x_{t-2} 使得 $a^{-1}x_{t-2}^2$ 满足 $y^{2^{t-2}} \equiv 1 \pmod{p}$.

即 $a^{-1}x_{t-2}^2$ 是模 p 的 2^{t-2} 次单位根.

要寻找 x_{t-2} 使得 $a^{-1}x_{t-2}^2$ 满足 $y^{2^{t-2}} \equiv 1 \pmod{p}$.

(a) 如果 $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \pmod{p}$,

令 $j_0 := 0$, $x_{t-2} := x_{t-1} = x_{t-1}b^{j_0} \pmod{p}$, 则 x_{t-2} 即为所求;

(b) 如果 $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \equiv (b^{-2})^{2^{t-2}} \pmod{p}$,

令 $j_0 := 1$, $x_{t-2} := x_{t-1}b = x_{t-1}b^{j_0} \pmod{p}$, 则 x_{t-2} 即为所求.

如此下去,

假设找到整数 x_{t-k} 使得 $a^{-1}x_{t-k}^2$ 满足 $y^{2^{t-k}} \equiv 1 \pmod{p}$,

即 $a^{-1}x_{t-k}^2$ 是模 p 的 2^{t-k} 次单位根: $(a^{-1}x_{t-k}^2)^{2^{t-k}} \equiv 1 \pmod{p}$.

(k+2) 如果 $t = k$, 则 $x = x_{t-k} \pmod{p}$ 满足 $x^2 \equiv a \pmod{p}$.

如果 $t \geq k+1$, 要寻找 x_{t-k-1} 使得 $a^{-1}x_{t-k-1}^2$ 满足

$y^{2^{t-k-1}} \equiv 1 \pmod{p}$. 即 $a^{-1}x_{t-k-1}^2$ 是模 p 的 2^{t-k-1} 次单位根.

寻找 x_{t-k-1} 使得 $a^{-1}x_{t-k-1}^2$ 满足 $y^{2^{t-k-1}} \equiv 1 \pmod{p}$.

(a) 如果 $(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv 1 \pmod{p}$, 令

$$j_{k-1} := 0, \quad x_{t-k-1} := x_{t-k} = x_{t-k} b^{j_{k-1} 2^{k-1}} \pmod{p},$$

则 x_{t-k-1} 即为所求;

(b) 如果 $(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1 \equiv (b^{-2^k})^{2^{t-k-1}} \pmod{p}$, 我们令

$$j_{k-1} := 1, \quad x_{t-k-1} := x_{t-k} b^{2^{k-1}} = x_{t-k} b^{j_{k-1} 2^{k-1}} \pmod{p},$$

则 x_{t-k-1} 即为所求.

特别地, 对于 $k = t - 1$, 有

$$\begin{aligned} x = x_0 &\equiv x_1 b^{j_{t-2} 2^{t-2}} \equiv \dots \equiv x_{t-1} b^{j_0 + j_1 2 + \dots + j_{t-2} 2^{t-2}} \\ &\equiv a^{\frac{s+1}{2}} b^{j_0 + j_1 2 + \dots + j_{t-2} 2^{t-2}} \pmod{p} \end{aligned}$$

满足同余式 $x^2 \equiv a \pmod{p}$.

例 1 应用上述算法求解同余式 $x^2 \equiv 186 \pmod{401}$.

解 因为 $a = 186 = 2 \cdot 3 \cdot 31$, 计算勒让得符号

$$\left(\frac{2}{401}\right) = (-1)^{(401^2-1)/8} = 1, \quad \left(\frac{3}{401}\right) = (-1)^{\frac{3-1}{2} \frac{401-1}{2}} \left(\frac{401}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$
$$\left(\frac{31}{401}\right) = (-1)^{\frac{31-1}{2} \frac{401-1}{2}} \left(\frac{401}{31}\right) = \left(\frac{-2}{31}\right) = \left(\frac{-1}{31}\right) \left(\frac{2}{31}\right) = (-1)^{\frac{31-1}{2}} (-1)^{\frac{31^2-1}{8}} = -1,$$

所以 $\left(\frac{186}{401}\right) = \left(\frac{2}{401}\right) \left(\frac{3}{401}\right) \left(\frac{31}{401}\right) = 1 \cdot (-1) \cdot (-1) = 1.$

故原同余式有解.

下面具体求解:

对 $p = 401$, 写 $p - 1 = 400 = 2^4 \cdot 25$, 其中 $t = 4$, $s = 25$ 是奇数.

(i) 任选一个模 401 平方非剩余 $n = 3$, 即 $n = 3$ 使得 $\left(\frac{3}{401}\right) = -1$.

再令 $b := 3^{25} \equiv 268 \pmod{401}$.

(ii) 计算 $x_3 := 186^{\frac{25+1}{2}} \equiv 103 \pmod{401}$. 以及 $a^{-1} \equiv 235 \pmod{401}$.

(iii) 因为 $(a^{-1}x_3^2)^{2^2} \equiv 98^4 \equiv -1 \pmod{401}$,

我们令 $j_0 := 1$, $x_2 := x_3 b^{j_0} = 103 \cdot 268 \equiv 336 \pmod{401}$,

(iv) 因为 $(a^{-1}x_2^2)^2 \equiv (-1)^2 \equiv 1 \pmod{401}$,

我们令 $j_1 := 0$, $x_1 := x_2 b^{j_1 2} = 336 \pmod{401}$.

(v) 因为 $a^{-1}x_1^2 \equiv -1 \pmod{401}$,

我们令 $j_2 := 1$, $x_0 := x_1 b^{j_2 2^2} = 336 \cdot 268^4 \equiv 304 \pmod{401}$,

则 $x \equiv x_0 \equiv 304 \pmod{p}$ 满足同余式

$$x^2 \equiv 186 \pmod{401}.$$

例 2 设 p 是形为 $4k+3$ 的素数. 如果 $x^2 \equiv a \pmod{p}$ 有解, 则其解是 $x \equiv \pm a^{(p+1)/4} \pmod{p}$.

解 因为 p 是形为 $4k+3$ 的素数, 所以存在奇数 q 使得 $p-1 = 2q$. 现在同余式 $x^2 \equiv a \pmod{p}$ 有解, 则我们有 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, 或者 $a^q \equiv 1 \pmod{p}$.

两端同时乘以 a , 得到

$$a^{q+1} \equiv a \pmod{p}.$$

因此, 同余式的解为

$$x \equiv \pm a^{\frac{q+1}{2}} \equiv \pm a^{(p+1)/4} \pmod{p}.$$

例 3 设 p, q 是形为 $4k + 3$ 的不同素数. 如果整数 a 满足 $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$, 求解同余式 $x^2 \equiv a \pmod{pq}$.

解 因为 $x^2 \equiv a \pmod{pq}$ 等价于同余式组
$$\begin{cases} x^2 \equiv a \pmod{p} \\ x^2 \equiv a \pmod{q}, \end{cases}$$

而同余式 $x^2 \equiv a \pmod{p}$ 的解为 $x \equiv \pm a^{(p+1)/4} \pmod{p}$,

同余式 $x^2 \equiv a \pmod{q}$ 的解为 $x \equiv \pm a^{(q+1)/4} \pmod{q}$,

根据 §3.2 定理 1(中国剩余定理), 原同余式的解为

$$x \equiv \pm(a^{\frac{p+1}{4}} \pmod{p})uq \pm (a^{\frac{q+1}{4}} \pmod{q})vp \pmod{pq},$$

其中整数 u, v 分别满足

$$uq \equiv 1 \pmod{p}, \quad vp \equiv 1 \pmod{q}.$$

本 要讨论的主要内容:

1. 高次同余式
2. 指数
3. 基本性质 (循环群)
4. 原根存在性
5. 原根的构造或生成元的构造
6. 指
7. n 次剩余
8. 乘法表的构造

本 将进一步讨论同余式 $x^n \equiv a \pmod{m}$. (1)

设 $m > 1$ 是整数, $(a, m) = 1$. 根据欧拉定 $a^{\varphi(m)} \equiv 1 \pmod{m}$.

问该 $\varphi(m)$ 是否是使得上式成立的最小正整数以及这个最小正整数具有哪些性质.

定义 1 设 $m > 1$ 是整数, a 是与 m 互素的正整数. 则使得

$$a^e \equiv 1 \pmod{m}$$

成立的最小正整数 e 叫做 a 对模 m 的 **指数**. 记作 $\text{ord}_m(a)$.

如果 a 对模 m 的指数是 $\varphi(m)$, 则 a 叫做模 m 的 **原根**.

例 1 设 $m = 7$. $\varphi(7) = 6$. 则 $1^1 \equiv 1$, $2^3 = 8 \equiv 1$, $3^3 = 27 \equiv -1$, $4^3 \equiv (-3)^3 \equiv 1$, $5^3 \equiv (-2)^3 \equiv -1$, $6^2 \equiv (-1)^2 \equiv 1 \pmod{7}$.

列成表为:

a	1	2	3	4	5	6
$\text{ord}_m(a)$	1	3	6	3	6	2

因此, 3, 5 是模 7 的原根. 但 2, 4, 6 不是模 7 的原根.

例 2 设整数 $m = 14 = 2 \cdot 7$, 这时 $\varphi(14) = 6$. 我们有

$$\begin{aligned}
 1^1 &\equiv 1, & 3^3 &= 27 \equiv -1, & 5^3 &= 125 \equiv -1, \\
 9^3 &\equiv (-5)^3 \equiv 1, & 11^3 &\equiv (-3)^3 \equiv 1, & 13^2 &\equiv (-1)^2 \equiv 1 \pmod{14}.
 \end{aligned}$$

列成表为:

a	1	3	5	9	11	13
$\text{ord}_m(a)$	1	6	6	3	3	2

因此, 3, 5 是模 14 的原根. 但 9, 11, 13 不是模 14 的原根.

例 3 设整数 $m = 15 = 3 \cdot 5$, 这时 $\varphi(15) = 8$. 我们有

$$1^1 \equiv 1, \quad 2^4 = 16 \equiv 1, \quad 4^2 = 16 \equiv 1, \quad 7^2 = 49 \equiv 4, \quad 7^4 \equiv 16 \equiv 1, \\ 8^4 \equiv (-7)^4 \equiv 1, \quad 11^2 \equiv (-4)^2 \equiv 1, \quad 13^4 \equiv (-2)^4 \equiv 1, \quad 14^2 \equiv (-1)^2 \equiv 1 \pmod{15}.$$

列成表为:

a	1	2	4	7	8	11	13	14
$\text{ord}_m(a)$	1	4	2	4	4	2	4	2

因此, 没有模 15 的原根.

例 4 设整数 $m = 9 = 3^2$, 这时 $\varphi(9) = 6$. 我们有

$$1^1 \equiv 1, \quad 2^3 = 8 \equiv -1, \quad 4^3 = 64 \equiv 1, \\ 5^3 \equiv (-4)^3 \equiv -1, \quad 7^3 \equiv (-2)^3 \equiv 1, \quad 8^2 \equiv (-1)^2 \equiv 1 \pmod{9}.$$

列成表为:

a	1	2	4	5	7	8
$\text{ord}_m(a)$	1	6	3	6	3	2

因此, 2, 5 是模 9 的原根.

例 5 设整数 $m = 8 = 2^3$, 这时 $\varphi(8) = 4$. 我们有

$$1^1 \equiv 1, 3^2 = 9 \equiv 1, 5^2 = 25 \equiv 1, 7^2 \equiv (-1)^2 \equiv 1 \pmod{8}.$$

列成表为:

a	1	3	5	7
$\text{ord}_m(a)$	1	2	2	2

因此, 没有模 8 的原根.

例 6 证明: 5 是模 3 及模 6 的原根, 也是模 3^2 , $2 \cdot 3^2$ 的原根.

$\varphi(3) = 2$, 且 $5 \equiv -1, 5^2 \equiv 1 \pmod{3}$; 同样, $\varphi(6) = 2$, 且 $5 \equiv -1, 5^2 \equiv 1 \pmod{6}$;

类似地, 因为 $\varphi(3^2) = 6$, 且

$$5 \equiv 5, 5^2 \equiv 7, 5^3 \equiv 8 \equiv -1, 5^4 \equiv 4, 5^5 \equiv 2, 5^6 \equiv 1 \pmod{3^2};$$

对于模 $2 \cdot 3^2$, 因为 $(5, 2) = 1$, 所以我们有

$$5 \equiv 5, 5^2 \equiv 7, 5^3 \equiv 8 \equiv -1, 5^4 \equiv 4, 5^5 \equiv 2, 5^6 \equiv 1 \pmod{2 \cdot 3^2}.$$

定理 1 设 $(a, m) = 1$. 则整数 d 使得 $a^d \equiv 1 \pmod{m}$ 的充分必要条件是 $\text{ord}_m(a) | d$.

证 充分性. 设 $\text{ord}_m(a) | d$, 则存在 k 使得 $d = k \text{ord}_m(a)$. 因此, $a^d = (a^{\text{ord}_m(a)})^k \equiv 1 \pmod{m}$.

必要性. 如果 $\text{ord}_m(a) \nmid d$ 不成立, 则由欧里得除法, 存在整数 q, r 使得 $d = \text{ord}_m(a)q + r$, $0 < r < \text{ord}_m(a)$.

从而, $a^r \equiv a^r (a^{\text{ord}_m(a)})^q = a^d \equiv 1 \pmod{m}$.

这与 $\text{ord}_m(a)$ 的最小性矛盾. 故 $\text{ord}_m(a) | d$.

推论 1 设 $m > 1$ 是整数, a 是与 m 互素的整数. 则 $\text{ord}_m(a) | \varphi(m)$.

根据推论 1, 整数 a 模 m 的指数 $\text{ord}_m(a)$ 是 $\varphi(m)$ 的因数, 所以可在 $\varphi(m)$ 的因数中求 $\text{ord}_m(a)$.

例 7 求整数 5 模 17 的指数 $\text{ord}_{17}(5)$.

解 $\varphi(17) = 16$, 只需对 16 的因数 $d = 1, 2, 4, 8, 16$, 计算 $a^d \pmod{m}$. 因为

$$5^1 \equiv 5, 5^2 = 25 \equiv 8, 5^4 \equiv 64 \equiv 13 \equiv -4, 5^8 \equiv (-4)^2 \equiv 16 \equiv -1, 5^{16} \equiv (-1)^2 \equiv 1 \pmod{17},$$

所以 $\text{ord}_{17}(5) = 16$. 这说明 5 是模 17 的原根.

推论 2 设 p 是奇素数, 且 $(p-1)/2$ 也是素数. 如果 $(a, p) = 1$, 且 a 不是 1 的模 p 二次同余根, 则 $\text{ord}_p(a) = \frac{p-1}{2}$ 或 $p-1$.

证 根据欧拉定, $a^{\varphi(p)} \equiv 1 \pmod{p}$.

根据推论 1, $\text{ord}_p(a)$ 是 $\varphi(p) = p-1 = 2 \cdot \frac{p-1}{2}$ 的因数, 但 $\text{ord}_p(a) \neq 2$, 所以 $\text{ord}_p(a) = \frac{p-1}{2}$ 或 $p-1$.

性质 1 设 $(a, m) = 1$.

(i) 若 $b \equiv a \pmod{m}$, 则 $\text{ord}_m(b) = \text{ord}_m(a)$.

(ii) 设 a^{-1} 使得 $a^{-1}a \equiv 1 \pmod{m}$, 则 $\text{ord}_m(a^{-1}) = \text{ord}_m(a)$.

例 8 39 模 17 的指数为 $\text{ord}_{17}(39) = \text{ord}_{17}(5) = 16$.

7 模 17 的指数为 16. 因为 $5^{-1} \equiv 7 \pmod{m}$.

定理 2 设 $(a, m) = 1$. 则 $1 = a^0, a, \dots, a^{\text{ord}_m(a)-1}$ 模 m 两两不同余. 特别地, 当 a 是模 m 的原根, 即 $\text{ord}_m(a) = \varphi(m)$ 时, 这 $\varphi(m)$ 个数组成模 m 的简化剩余系.

证 反证法. 如果 $\text{ord}_m(a)$ 个数 $a^0, a, \dots, a^{\text{ord}_m(a)-1}$ 中有两个数模 m 同余, 则存在整数 $0 \leq k, l < \text{ord}_m(a)$ 使得

$$a^k \equiv a^l \pmod{m}.$$

不妨设 $k > l$. 两端同乘 $a^{-l} \pmod{m}$, 有 $a^{k-l} \equiv 1 \pmod{m}$.

但 $0 < k - l < \text{ord}_m(a)$. 这与 $\text{ord}_m(a)$ 的最小性矛盾. 故结论成立.

再设 a 是模 m 的原根, 即 $\text{ord}_m(a) = \varphi(m)$, 则 $\varphi(m)$ 个数 $1 = a^0, a, \dots, a^{\varphi(m)-1}$ 模 m 两两不同余.

根据 §2.3 定 2, 这 $\varphi(m)$ 个数组成模 m 的简化剩余系.

例 9 整数 $\{5^k \mid k = 0, \dots, 15\}$ 组成模 17 的简化剩余系.

解 作计算如下:

$$\begin{aligned}
 5^0 &\equiv 1, & 5^1 &\equiv 5, & 5^2 &= 25 \equiv 8, \\
 5^3 &\equiv 8 \cdot 5 \equiv 6, & 5^4 &\equiv 8^2 \equiv 13, & 5^5 &\equiv 13 \cdot 5 \equiv 14, \\
 5^6 &\equiv 6^2 \equiv 2, & 5^7 &\equiv 2 \cdot 5 \equiv 10, & 5^8 &\equiv 10 \cdot 5 \equiv 40 \equiv -1 \\
 5^9 &\equiv (-1) \cdot 5 \equiv 12, & 5^{10} &\equiv (-1) \cdot 8 \equiv 9, & 5^{11} &\equiv (-1) \cdot 6 \equiv 11, \\
 5^{12} &\equiv (-1) \cdot 13 \equiv 4, & 5^{13} &\equiv (-1) \cdot 14 \equiv 3, & 5^{14} &\equiv (-1) \cdot 2 \equiv 15, \\
 5^{15} &\equiv (-1) \cdot 10 \equiv 7 \pmod{17}.
 \end{aligned}$$

列表为:

5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7	5^8	5^9	5^{10}	5^{11}	5^{12}	5^{13}	5^{14}	5^{15}
1	5	8	6	13	14	2	10	-1	12	9	11	4	3	15	7

定理 3 设 $(a, m) = 1$. 则 $a^d \equiv a^k \pmod{m} \Leftrightarrow d \equiv k \pmod{\text{ord}_m(a)}$.

例 10 $2^{1000000} \equiv 2^{10} \equiv 100 \pmod{231}$. 因为 $\text{ord}_{231}(2) = 30$,

$1000000 \equiv 10 \pmod{30}$.

例 11 $2^{2002} \equiv 2^1 \equiv 2 \pmod{7}$. 因为 $\text{ord}_7(2) = 3$, $2002 \equiv 1 \pmod{3}$.

定理 4 设 $(a, m) = 1$. 设 $d \geq 0$ 为整数, 则 $\text{ord}_m(a^d) = \frac{\text{ord}_m(a)}{(\text{ord}_m(a), d)}$.

例 12 $5^2 \equiv 8 \pmod{17}$ 模 17 的指数为 $\text{ord}_{17}(5^2) = \frac{\text{ord}_{17}(5)}{(\text{ord}_{17}(5), 2)} = 8$.

推论 设 $m > 1$ 是整数, g 是模 m 的原根. 设 $d \geq 0$ 为整数, 则 g^d 是模 m 的原根当且仅当 $(d, \varphi(m)) = 1$.

证 根据定 4, 我们有

$$\text{ord}_m(g^d) = \frac{\text{ord}_m(g)}{(\text{ord}_m(g), d)} = \frac{\varphi(m)}{(\varphi(m), d)}.$$

因此, g^d 是模 m 的原根, 即 $\text{ord}_m(g^d) = \varphi(m)$ 当且仅当 $(d, \varphi(m)) = 1$.

定理 5 如果模 m 有一个原根 g , 则模 m 有 $\varphi(\varphi(m))$ 个不同的原根.

证 设 g 是模 m 的一个原根. 则 $\varphi(m)$ 个整数

$$g, g^2, \dots, g^{\varphi(m)}$$

构成模 m 的一个简化剩余系.

又 g^d 是模 m 的原根当且仅当 $(d, \varphi(m)) = 1$.

因为这样的 d 共有 $\varphi(\varphi(m))$ 个, 所以模 m 有 $\varphi(\varphi(m))$ 个不同的原根.

例 13 求出模 17 的所有原根.

解 由例 7 知道 5 是模 17 的原根. 再由定 5, 得到 $\varphi(\varphi(17)) = \varphi(16) = 8$ 个整数 5, $5^3 \equiv 6$, $5^5 \equiv 14$, $5^7 \equiv 10$, $5^9 \equiv 12$, $5^{11} \equiv 11$, $5^{13} \equiv 3$, $5^{15} \equiv 7 \pmod{17}$ 是模 17 的全部原根.

定理 6 设 $(ab, m) = 1$, $(a, b) = 1$. 如果 $(\text{ord}_m(a), \text{ord}_m(b)) = 1$, 则 $\text{ord}_m(ab) = \text{ord}_m(a)\text{ord}_m(b)$. 反之亦然.

证 因为 $(a, m) = 1$, $(b, m) = 1$, 所以 $(ab, m) = 1$, 故存在 $\text{ord}_m(ab)$.

$$\begin{aligned} \text{又 } a^{\text{ord}_m(b)\text{ord}_m(ab)} &\equiv (a^{\text{ord}_m(b)})^{\text{ord}_m(ab)} (b^{\text{ord}_m(b)})^{\text{ord}_m(ab)} \\ &\equiv ((ab)^{\text{ord}_m(ab)})^{\text{ord}_m(b)} \equiv 1 \pmod{m}, \end{aligned}$$

因此, $\text{ord}_m(a) \mid \text{ord}_m(b)\text{ord}_m(ab)$. 但 $(\text{ord}_m(a), \text{ord}_m(b)) = 1$, 根据 §1.4 定 1 之推论, $\text{ord}_m(a) \mid \text{ord}_m(ab)$.

同, $\text{ord}_m(b) \mid \text{ord}_m(ab)$. 再由 $(\text{ord}_m(a), \text{ord}_m(b)) = 1$ 及 §1.4 定 4, 得到 $\text{ord}_m(a)\text{ord}_m(b) \mid \text{ord}_m(ab)$.

另一方面, $(ab)^{\text{ord}_m(a)\text{ord}_m(b)} = (a^{\text{ord}_m(a)})^{\text{ord}_m(b)} (b^{\text{ord}_m(b)})^{\text{ord}_m(a)}$
 $\equiv 1 \pmod{m}$, 从而 $\text{ord}_m(ab) \mid \text{ord}_m(a)\text{ord}_m(b)$. 故

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

反过来, 如果 $\text{ord}_m(ab) = \text{ord}_m(a)\text{ord}_m(b)$, 那么由

$$(ab)^{[\text{ord}_m(a), \text{ord}_m(b)]} = a^{[\text{ord}_m(a), \text{ord}_m(b)]} b^{[\text{ord}_m(a), \text{ord}_m(b)]} \equiv 1 \pmod{m},$$

推得 $\text{ord}_m(ab) \mid [\text{ord}_m(a), \text{ord}_m(b)]$,

即 $\text{ord}_m(a)\text{ord}_m(b) \mid [\text{ord}_m(a), \text{ord}_m(b)]$.

因此, $(\text{ord}_m(a), \text{ord}_m(b)) = 1$. 结论成立.

例 14 求模 71 的原根.

解 计算整数 2 模 71 的指数为 $\text{ord}_{71}(2) = 35$;

因此, 整数 -2 为模 71 的原根,

因为 -2 模 71 的指数为 $\text{ord}_{71}(-2) = \text{ord}_{71}(-1)\text{ord}_{71}(2) = 70$.

定理 7 设 m, n 都是大于 1 的整数, $(a, m) = 1$. 则

(i) 若 $n|m$, 则 $\text{ord}_n(a) \mid \text{ord}_m(a)$.

(ii) 若 $(m, n) = 1$, 则 $\text{ord}_{mn}(a) = [\text{ord}_m(a), \text{ord}_n(a)]$.

证 (i) 根据 $\text{ord}_m(a)$ 的定义, $a^{\text{ord}_m(a)} \equiv 1 \pmod{m}$.

因此, 当 $n|m$ 时, 可推出 $a^{\text{ord}_m(a)} \equiv 1 \pmod{n}$. 故 $\text{ord}_n(a) \mid \text{ord}_m(a)$.

(ii) 由 (i) 有 $\text{ord}_m(a) \mid \text{ord}_{mn}(a)$, $\text{ord}_n(a) \mid \text{ord}_{mn}(a)$,

从而, $[\text{ord}_m(a), \text{ord}_n(a)] \mid \text{ord}_{mn}(a)$.

又由 $a^{[\text{ord}_m(a), \text{ord}_n(a)]} \equiv 1 \pmod{m}$, $a^{[\text{ord}_m(a), \text{ord}_n(a)]} \equiv 1 \pmod{n}$,

可推出 $a^{[\text{ord}_m(a), \text{ord}_n(a)]} \equiv 1 \pmod{mn}$.

从而, $\text{ord}_{mn}(a) \mid [\text{ord}_m(a), \text{ord}_n(a)]$. 故 $\text{ord}_{mn}(a) = [\text{ord}_m(a), \text{ord}_n(a)]$.

推论 1 设 p, q 是两个不同的奇素数, a 是与 pq 互素的整数.

则 $\text{ord}_{pq}(a) = [\text{ord}_p(a), \text{ord}_q(a)]$.

例 15 设 $p \neq q$ 都是奇素数, $n = pq$, $(a, p) = 1$. 如果整数 e 满足 $1 < e < \varphi(n)$, $(e, \varphi(n)) = 1$, 那么存在整数 $d = d_a$, $1 \leq d < \text{ord}_n(a)$, 使得 $ed \equiv 1 \pmod{\text{ord}_n(a)}$.

而且, 对于整数 $a^e \equiv c \pmod{n}$, $1 \leq c < n$, 有 $c^d \equiv a \pmod{n}$.

证 由 $(e, \varphi(n)) = 1$, $\text{ord}_n(a) \mid \varphi(n)$, 得 $(e, \text{ord}_{pq}(a)) = 1$. 故存在 $d = d_a$, $1 \leq d < \text{ord}_n(a)$, 使得 $ed \equiv 1 \pmod{\text{ord}_n(a)}$. 因此, 存在一个正整数 k 使得 $ed = 1 + k \text{ord}_{pq}(a)$.

现在, 根据指数的定义, 得到 $a^{\text{ord}_p(a)} \equiv 1 \pmod{p}$.

又 $(\text{ord}_{pq}(a)/\text{ord}_p(a))$ 为整数. 两端作 $k(\text{ord}_{pq}(a)/\text{ord}_p(a))$ 次幂, 并乘以 a 得到 $a^{1+k \text{ord}_{pq}(a)} \equiv a \pmod{p}$, 即 $a^{ed} \equiv a \pmod{p}$.

同 , $a^{ed} \equiv a \pmod{q}$. 因为 p 和 q 是不同的素数, 根据 §2.1 定 12, $a^{ed} \equiv a \pmod{n}$, 因此, $c^d \equiv (a^e)^d \equiv a \pmod{n}$.

推论 2 设 $(a, m) = 1$. 则当 $m = 2^n p_1^{\alpha_1} \cdots 2 p_k^{\alpha_k}$ 时, 我们有

$$\text{ord}_m(a) = [\text{ord}_{2^n}(a), \text{ord}_{p_1^{\alpha_1}}(a), \dots, \text{ord}_{p_k^{\alpha_k}}(a)].$$

定理 8 设 $(m, n) = 1$. 则对与 mn 互素的任意整数 a_1, a_2 , 存在整数 a 使得 $\text{ord}_{mn}(a) = [\text{ord}_m(a_1), \text{ord}_n(a_2)]$.

证 考虑同余式组
$$\begin{cases} x \equiv a_1 \pmod{m}, \\ x \equiv a_2 \pmod{n}. \end{cases}$$

根据中国剩余定 理, 这个同余式组有惟一解 $x \equiv a \pmod{mn}$.

根据性质 1 (i), 有 $\text{ord}_m(a) = \text{ord}_m(a_1)$, $\text{ord}_n(a) = \text{ord}_n(a_2)$.

因此, 从定 理 7, $\text{ord}_{mn}(a) = [\text{ord}_m(a), \text{ord}_n(a)] = [\text{ord}_m(a_1), \text{ord}_n(a_2)]$.

注 对于模 m , 不一定有 $\text{ord}_m(ab) = [\text{ord}_m(a), \text{ord}_m(b)]$ 成立.

例如, 由例 2, $\text{ord}_{10}(3 \cdot 3) = 2 \neq [\text{ord}_{10}(3), \text{ord}_{10}(3)] = 4$, $\text{ord}_{10}(3 \cdot 7) = 1 \neq [\text{ord}_{10}(3), \text{ord}_{10}(7)] = 4$. 但有 $\text{ord}_{10}(7 \cdot 9) = 4 = [\text{ord}_{10}(7), \text{ord}_{10}(9)] = 4$.

定理 9 对与 m 互素的任意整数 a, b , 存在整数 c 使得

$$\text{ord}_m(c) = [\text{ord}_m(a), \text{ord}_m(b)].$$

证 根据 §1.5 例 5, 对于整数 $\text{ord}_m(a)$ 和 $\text{ord}_m(b)$, 存在整数 u, v 满足: $u | \text{ord}_m(a), \quad v | \text{ord}_m(b), \quad (u, v) = 1$

使得 $[\text{ord}_m(a), \text{ord}_m(b)] = uv$.

现在令 $s = \frac{\text{ord}_m(a)}{u}, \quad t = \frac{\text{ord}_m(b)}{v},$

根据定 4, 我们有

$$\text{ord}_m(a^s) = \frac{\text{ord}_m(a)}{(\text{ord}_m(a), s)} = u, \quad \text{ord}_m(b^t) = v.$$

再根据定 6, 我们得到

$$\text{ord}_m(a^s b^t) = \text{ord}_m(a^s) \text{ord}_m(b^t) = uv = [\text{ord}_m(a), \text{ord}_m(b)].$$

因此, 取 $c = a^s b^t \pmod{m}$. 即为所求. 证毕.

例 16 设整数 $m = 3631$. m 是素数. 我们有

$$\varphi(3631) = 3630 = 2 \cdot 3 \cdot 5 \cdot 11^2,$$

$$\text{ord}_{3631}(2) = 605 = 5 \cdot 11^2,$$

$$\text{ord}_{3631}(5) = 363 = 3 \cdot 11^2,$$

$$\text{ord}_{3631}(7) = 33 = 3 \cdot 11,$$

$$\text{ord}_{3631}(11) = 330 = 2 \cdot 3 \cdot 5 \cdot 11,$$

$$\text{ord}_{3631}(13) = 1815 = 3 \cdot 5 \cdot 11^2,$$

$$\text{ord}_{3631}(15) = 3630 = 2 \cdot 3 \cdot 5 \cdot 11^2,$$

$$\text{ord}_{3631}(3) = 1210 = 2 \cdot 5 \cdot 11^2,$$

$$\text{ord}_{3631}(6) = 1210 = 2 \cdot 5 \cdot 11^2,$$

$$\text{ord}_{3631}(10) = 1815 = 3 \cdot 5 \cdot 11^2,$$

$$\text{ord}_{3631}(12) = 1210 = 2 \cdot 5 \cdot 11^2,$$

$$\text{ord}_{3631}(14) = 1815 = 3 \cdot 5 \cdot 11^2,$$

$$\text{ord}_{3631}(17) = 1210 = 2 \cdot 5 \cdot 11^2.$$

根据定 9, 取整数 $a = 3$, $b = 5$ 以及 $u = 1210$, $v = 33$, 这时 $s = 1$, $t = 11^2$, 而整数 $c = a^s b^t = 3^1 \cdot 5^{121} \equiv 2623 \pmod{3631}$ 的指数为

$$[\text{ord}_{3631}(3), \text{ord}_{3631}(3)] = [1210, 363] = 3630.$$

因此, $c = 2623$ 是模 3631 的原根.

我们先讨论 m 为奇素数 p 的情形:

定理 1 设 p 是奇素数, 则模 p 的原根存在.

证一(构造性) 在模 p 的简化剩余系 $1, \dots, p-1$ 中, 记

$$e_r = \text{ord}_p(r), \quad 1 \leq r \leq p-1, \quad e = [e_1, \dots, e_{p-1}].$$

那么根据 §5.1 定 8, 存在整数 g , 使得 $g^e \equiv 1 \pmod{p}$.

因此, $e \mid \varphi(p) = p-1$. 又因为 $e_r \mid e$, $r = 1, \dots, p-1$,

从而推出同余式 $x^e \equiv 1 \pmod{p}$ 有 $p-1$ 个解 $x \equiv 1, \dots, p-1 \pmod{p}$.

根据 §3.4 定 4, 我们有 $p-1 \leq e$. 故 g 的指数为 $p-1$, 即 g 是模 p 的原根.

证二(存在性) 设 $d|p-1$. 用 $F(d)$ 表示模 p 的简化剩余系中指数为 d 的元素个数. 要证明: $F(d) = \varphi(d)$.

事实上, 我们有 $\sum_{d|p-1} F(d) = p-1$ $\sum_{d|p-1} \varphi(d) = p-1$

进而, $\sum_{d|p-1} (\varphi(d) - F(d)) = 0$.

如果能证明 $F(d) \leq \varphi(d)$, 则对所有 $d|p-1$, $F(d) = \varphi(d)$.

特别, $F(p-1) = \varphi(p-1)$. 这说明存在模 p 指数为 $p-1$ 的元素, 即模 p 的原根存在. 下证: $F(d) = \varphi(d)$.

因为模 p 指数为 d 的元素满足: $x^d - 1 \equiv 0 \pmod{p}$, (2)

且当 a 是模 p 指数为 d 的元素, (2) 的解可以表示成 $x \equiv a^0, a, \dots, a^{d-1}$.

其中指数为 d 的元素有 $\varphi(d)$. 因此, $F(d) = \varphi(d)$. 而若没有模 p 指数为 d 的元素, 则 $F(d) = 0$. 总之, 有 $F(d) \leq \varphi(d)$.

推论 设 p 是奇素数, $d|p-1$. 则模 p 指数为 d 的元素存在.

定理 2 设 g 是模 p 原根, 则 g 或者 $g + p$ 是模 p^2 的原根.

证 设 g 模 p^2 的指数为 n . 则 $g^n \equiv 1 \pmod{p^2}$, $n \mid \varphi(p^2) = p(p-1)$.

又有 $g^n \equiv 1 \pmod{p}$ 及 g 是原根, 故 $p-1 = \text{ord}_p(g) \mid n$.

因此, $n = p-1$ 或者 $n = p(p-1)$. 如果 $n = p(p-1) = \varphi(p^2)$, 则 g 是模 p^2 的原根. 如果 $n = p-1$, 则 $g^{p-1} \equiv 1 \pmod{p^2}$.

我们要证明 $g + p$ 是模 p^2 的原根. 事实上, 我们有

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + (p-1)g^{p-2}p + \binom{p}{2}g^{p-3}p^2 + \dots + p^{p-1} \\ &\equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2}.\end{aligned}$$

因此, $(g+p)^{p-1} \equiv 1 + (p-1)g^{p-2}p \equiv 1 - g^{p-2}p \pmod{p^2}$. 这说明 $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$.

否则, 如果 $(g+p)^{p-1} \equiv 1 \pmod{p^2}$, 则有 $g^{p-2}p \equiv 0 \pmod{p^2}$, 进而 $g^{p-2} \equiv 0 \pmod{p}$, 这是不可能的. 因此, $\text{ord}_{p^2}(g+p) = p(p-1) = \varphi(p^2)$. $g+p$ 是模 p^2 的原根.

定理 3 设 p 是奇素数, 则对任意 α , 模 p^α 的原根存在. 更确切地说, 如果 g 是模 p^2 原根, 则对任意 α , g 是模 p^α 的原根.

证 已知模 p^2 的原根 g 存在, 并且有 $g^{p-1} \not\equiv 1 \pmod{p^2}$.

现对 α 作数学归纳法, 来证明: $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$. (*)

$\alpha = 2$ 时, 命题成立. 假设 $\alpha \geq 2$ 时, 命题成立, 即 $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$.

这个关系式可写成: $g^{p^{\alpha-2}(p-1)} = 1 + u_{\alpha-2}p^{\alpha-1}, \quad p \nmid u_{\alpha-2}$. 两端作 p 次方, 我们有

$$\begin{aligned} g^{p^{\alpha-1}(p-1)} &= 1 + \binom{p}{1} u_{\alpha-2} p^{\alpha-1} + \binom{p}{2} (u_{\alpha-2} p^{\alpha-1})^2 + \cdots + (u_{\alpha-2} p^{\alpha-1})^p \\ &\equiv 1 + u_{\alpha-2} p^\alpha \pmod{p^{\alpha+1}}. \quad (**) \end{aligned}$$

因为 $p \nmid u_{\alpha-2}$, 所以 $g^{p^{\alpha-1}(p-1)} \not\equiv 1 \pmod{p^{\alpha+1}}$. 即 (*) 对于 $\alpha + 1$ 成立. 根据数学归纳法原理, 关系式 (*) 对所有整数 $\alpha \geq 2$ 成立.

设 g 模 p^α 指数为 d , 则 $g^d \equiv 1 \pmod{p^\alpha}$, 从而 $g^d \equiv 1 \pmod{p^2}$.

因为 g 是模 p^2 原根, 所以 g 模 p^2 指数 $p(p-1) = \varphi(p^2) | d$.

同时, $d | \varphi(p^\alpha)$. 因此, 可将 d 写成 $d = p^{r-1}(p-1)$, $2 \leq r \leq \alpha$.

再将上式代入 (**), 得到

$$1 + u_{r-1}p^r = g^{p^{r-1}(p-1)} \equiv 1 \pmod{p^\alpha}$$

或者

$$u_{r-1}p^r \equiv 0 \pmod{p^\alpha}.$$

因为 $p \nmid u_{r-1}$, 所以 $r \geq \alpha$. 因此, $r = \alpha$. 这就是说, g 是模 p^α 的原根. 证毕.

定理 4 设 $\alpha \geq 1$, g 是模 p^α 的一个原根, 则 g 与 $g + p^\alpha$ 中的奇数是模 $2p^\alpha$ 的一个原根.

证 (i) 设奇数 a 满足同余式 $a^d \equiv 1 \pmod{p^\alpha}$,

又显然有 $a^d \equiv 1 \pmod{2}$,

根据 §2.1 定 12, $a^d \equiv 1 \pmod{2p^\alpha}$. 反之显然.

(ii) 若 g 是奇数, 令 $d = \varphi(p^\alpha)$, 则 $\varphi(2p^\alpha) = \varphi(p^\alpha) = d$.

又当 $g^d \equiv 1 \pmod{p^\alpha}$, $g^r \not\equiv 1 \pmod{p^\alpha}$, $0 < r < d$ 时,

有 $g^d \equiv 1 \pmod{2p^\alpha}$, $g^r \not\equiv 1 \pmod{2p^\alpha}$, $0 < r < d$.

故 g 是模 $2p^\alpha$ 的一个原根.

(iii) 若 g 是偶数, 则 $g + p^\alpha$ 是奇数, 类似 (ii) 可得结论. 证毕.

定理 5 设 a 是一个奇数. 则对任意整数 $\alpha \geq 3$, 有

$$a^{\varphi(2^\alpha)/2} \equiv a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

证 用归纳法来证明这个结论. 将奇数 a 写成 $a = 2b + 1$, 有 $a^2 = 4b(b+1) + 1 \equiv 1 \pmod{2^3}$. 因此, 结论对于 $\alpha = 3$ 成立.

假设对于 $\alpha - 1$, 结论也成立, 即 $a^{2^{(\alpha-1)-2}} \equiv 1 \pmod{2^{\alpha-1}}$

或存在整数 $t_{\alpha-3}$ 使得 $a^{2^{(\alpha-1)-2}} = 1 + t_{\alpha-3}2^{\alpha-1}$.

两端平方, 得到

$$a^{2^{\alpha-2}} = (1 + 2^{\alpha-1}t_{\alpha-3})^2 = 1 + (t_{\alpha-3} + 2^{\alpha-2}t_{\alpha-3}^2)2^\alpha \equiv 1 \pmod{2^\alpha}.$$

这就是说, 结论对 α 成立. 根据数学归纳法原理, 同余式 (10) 对所有的整数 $\alpha \geq 3$ 成立. 证毕.

定理 6 设 $\alpha \geq 3$. 则 $\text{ord}_{2^\alpha}(5) = \varphi(2^\alpha)/2 = 2^{\alpha-2}$.

证 根据定 5, 有 $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$. 从而 $\text{ord}_{2^\alpha}(5) \mid 2^{\alpha-2}$.

因此, 为得到结论, 我们只需证明 $\text{ord}_{2^\alpha}(5) \nmid 2^{\alpha-3}$.

事实上, 我们有 $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}$.

我们对 α 作数学归纳法, 来证明这个关系式.

$\alpha = 3$ 时, $5^{2^{3-3}} \equiv 1 + 2^2 \pmod{2^3}$. 因此, 关系式成立.

假设 $\alpha \geq 3$ 时, 命题成立, 即 $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}$.

这样, 存在一个整数 q 使得 $5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + q2^\alpha$.

两端平方, 我们有

$$5^{2^{(\alpha+1)-3}} = (1 + 2^{\alpha-1})^2 + 2(1 + 2^{\alpha-1})q2^\alpha + (q2^\alpha)^2 = 1 + 2^\alpha + (2^{\alpha-3} + q + q2^{\alpha-1} + q^22^{\alpha-1})2^{\alpha+1}.$$

因此 $5^{2^{(\alpha+1)-3}} \equiv 1 + 2^{(\alpha+1)-1} \pmod{2^{\alpha+1}}$. 即关系式对于 $\alpha + 1$ 成立.

根据归纳法原理, 关系式对所有 $\alpha \geq 3$ 成立. 故 $\text{ord}_{2^\alpha}(5) = 2^{\alpha-2} = \varphi(2^\alpha)/2$.

定理 7 模 m 的原根存在 $\Leftrightarrow m = 2, 4, p^\alpha, 2p^\alpha$, 其中 p 是奇素数.

证 必要性. 设 m 的 准分解式为 $m = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

若 $(a, m) = 1$, 则 $(a, 2^\alpha) = 1, \quad (a, p_i^{\alpha_i}) = 1, \quad i = 1, \dots, k$.

根据欧拉定理及定理 5,
$$\begin{cases} a^\tau \equiv 1 \pmod{2^\alpha} \\ a^{\varphi(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}} \\ \vdots \\ a^{\varphi(p_k^{\alpha_k})} \equiv 1 \pmod{p_k^{\alpha_k}}, \end{cases} \quad \text{其中 } \tau = \begin{cases} \varphi(2^\alpha), & \alpha \leq 2, \\ \frac{1}{2}\varphi(2^\alpha), & \alpha \geq 3. \end{cases}$$

令 $h = [\tau, \varphi(p_1^{\alpha_1}), \dots, \varphi(p_k^{\alpha_k})]$. 根据 §5.1 定 6 之推论, 对所有整数 $a, (a, m) = 1$, 我们有 $a^h \equiv 1 \pmod{m}$.

因此, 若 $h < \varphi(m)$, 则模 m 的原根不存在.

现在讨论何时

$$h = \varphi(m) = \varphi(2^\alpha) \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}).$$

现在讨论何时 $h = \varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$.

(a) 当 $\alpha \geq 3$ 时, $\tau = \frac{\varphi(2^\alpha)}{2}$. 因此, $h \leq \frac{\varphi(m)}{2} < \varphi(m)$.

(b) 当 $k \geq 2$ 时, $2|\varphi(p_1^{\alpha_1}), 2|\varphi(p_2^{\alpha_2})$. 进而,
 $[\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2})] \leq \frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) < \varphi(p_1^{\alpha_1}p_2^{\alpha_2})$. 因此, $h < \varphi(m)$.

(c) 当 $\alpha = 2, k = 1$ 时, $\varphi(2^\alpha) = 2, 2|\varphi(p_1^{\alpha_1})$. 因此,

$$h = \varphi(p_1^{\alpha_1}) < \varphi(2^n)\varphi(p_1^{\alpha_1}) = \varphi(m).$$

故只有在 (α, k) 是 $(1, 0), (2, 0), (0, 1), (1, 1)$ 四种情形之一, 即只有在 m 是 $2, 4, p^\alpha, 2p^\alpha$ 四数之一时, 才有可能 $h = \varphi(m)$. 因此必要性成立.

充分性. 当 $m = 2$ 时, $\varphi(2) = 1$, 整数 1 是模 2 的原根;

当 $m = 4$ 时, $\varphi(4) = 2$, 整数 3 是模 4 的原根;

当 $m = p^\alpha$ 时, 根据定理 3, 模 m 的原根存在;

当 $m = 2p^\alpha$ 时, 根据定理 4, 模 m 的原根存在.

因此, 条件的充分性是成立的.

定理 8 设 $m > 1$, $\varphi(m)$ 的所有不同素因数是 $q_1, \dots, q_k$, 则 g 是模 m 的一个原根的充分必要条件是

$$g^{\varphi(m)/q_i} \not\equiv 1 \pmod{m}, \quad i = 1, \dots, k.$$

证 设 g 是 m 的一个原根, 则 g 对模 m 的指数是 $\varphi(m)$. 但

$$0 < \varphi(m)/q_i < \varphi(m), \quad i = 1, \dots, k.$$

根据 §5.1 定理 2, 我们有 $g^{\varphi(m)/q_i} \not\equiv 1 \pmod{m}$, $i = 1, \dots, k$.

反过来, 若 g 对模 m 的指数 $e < \varphi(m)$. 则根据 §5.1 定理 1, 我们有 $e|\varphi(m)$. 因而存在一个素数 q 使得 $q|\frac{\varphi(m)}{e}$. 即

$$\frac{\varphi(m)}{e} = qu, \quad \text{或} \quad \frac{\varphi(m)}{q} = ue.$$

进而 $g^{\varphi(m)/q} = (g^e)^u \equiv 1 \pmod{m}$. 与假设矛盾.

定理 8 给出了一个找原根的方法.

例 1 求模 41 的所有原根.

解 因为 $\varphi(m) = \varphi(41) = 40 = 2^3 \cdot 5$, 所以 $\varphi(m)$ 的素因数为

$q_1 = 2, q_2 = 5$. 进而, $\varphi(m)/q_1 = 20, \varphi(m)/q_2 = 8$.

故只需验证: g^{20}, g^8 模 m 是否同余于 1. 对 2, 3, ..., 逐个验算:

$$2^8 \equiv 10, 2^{20} \equiv 1, 3^8 \equiv 1, 4^8 \equiv 18, 4^{20} \equiv 1,$$

$$5^8 \equiv 18, 5^{20} \equiv 1, 6^8 \equiv 10, 6^{20} \equiv 40 \pmod{41},$$

故 6 是模 41 的原根.

因为 $(d, \varphi(m)) = 1$ 时, $\text{ord}_m(g^d) = \text{ord}_m(g)$, 因此, 当 d 遍历模 $\varphi(m) = 40$ 的简化剩余系: 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 共 $\varphi(\varphi(m)) = 16$ 个数时, 6^d 遍历模 41 的所有原根:

$$6^1 \equiv 6, 6^3 \equiv 11, 6^7 \equiv 29, 6^9 \equiv 19, 6^{11} \equiv 28, 6^{13} \equiv 24, 6^{17} \equiv 26, 6^{19} \equiv 34,$$

$$6^{21} \equiv 35, 6^{23} \equiv 30, 6^{27} \equiv 12, 6^{29} \equiv 22, 6^{31} \equiv 13, 6^{33} \equiv 17, 6^{37} \equiv 15, 6^{39} \equiv 7.$$

例 2 设 $m = 41^2 = 1681$, 求模 m 的原根.

解 因为 6 是模 $p = 41$ 的原根, 所以 6 或者 $6 + 41 = 47$ 是模 $41^2 = 1681$ 的原根. 事实上, 我们有

$$6^{40} \equiv 143 \equiv 1 + 41 \cdot 3 \pmod{41^2}, \quad 47^{40} \equiv 1518 \equiv 1 + 41 \cdot 37 \pmod{41^2}.$$

这就是说, $6^{40} \not\equiv 1 \pmod{41^2}$, $47^{40} \not\equiv 1 \pmod{41^2}$.

根据定 3 之证明, 6 和 47 都是模 $m = 41^2 = 1681$ 的原根, 它们也都是模 41^α 的原根.

因为 $(d, \varphi(m)) = 1$ 时, $\text{ord}_m(g^d) = \text{ord}_m(g)$, 因此, 当 d 遍历模 $\varphi(41^2) = 1640$ 的简化剩余系时, 6^d 遍历模 41^2 的所有原根.

例 3 设 $m = 2 \cdot 41^2 = 3362$, 求模 m 的原根.

解 这里应用定 3 及例 2, 即可得到 $6 + 41^2 = 1687$ 和 47 是模 $2 \cdot 41^2 = 3362$ 的原根.

例 4 求模 43 的原根.

解 设 $m = 43$, 则 $\varphi(m) = \varphi(43) = 2 \cdot 3 \cdot 7$, $q_1 = 2$, $q_2 = 3$, $q_3 = 7$.

因此, $\varphi(m)/q_1 = 21$, $\varphi(m)/q_2 = 14$, $\varphi(m)/q_3 = 6$.

这样, 只需验证: g^{21} , g^{14} , g^6 模 m 是否同余于 1. 对 2, 3, ... 逐个验算:

$$\begin{aligned} 2^2 &\equiv 4, & 2^4 &\equiv 16, & 2^6 &\equiv 64 \equiv 21, & 2^7 &\equiv 21 \cdot 2 \equiv -1, \\ 2^{14} &\equiv 1, & 3^2 &\equiv 9, & 3^4 &\equiv 81 \equiv -5, & 3^6 &\equiv 9 \cdot (-5) \equiv -2, \\ 3^7 &\equiv -6, & 3^{14} &\equiv (-6)^2 \equiv 36, & 3^{21} &\equiv (-6) \cdot 36 \equiv -1 \pmod{43}. \end{aligned}$$

因此, 3 是模 43 的原根.

当 d 遍历模 $\varphi(m) = 42$ 的简化剩余系: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41 共 $\varphi(\varphi(43)) = 12$ 个数时, 3^d 遍历模 43 的所有原根:

$$\begin{aligned} 3^1 &\equiv 3, & 3^5 &\equiv 28, & 3^{11} &\equiv 30, & 3^{13} &\equiv 12, & 3^{17} &\equiv 26, & 3^{19} &\equiv 19, & 3^{23} &\equiv 34, \\ 3^{25} &\equiv 5, & 3^{29} &\equiv 18, & 3^{31} &\equiv 33, & 3^{37} &\equiv 20, & 3^{41} &\equiv 29 \pmod{43}. \end{aligned}$$

例 5 设 $m = 43^2 = 1849$, 求模 m 的原根.

解 因为已知 3 是模 $p = 43$ 的原根, 所以根据定 2, 可知 3 或者 $3 + 43 = 46$ 是模 $43^2 = 1849$ 的原根. 事实上, 我们有

$$3^{42} \equiv 87 \equiv 1 + 43 \cdot 2 \pmod{43^2}, \quad 46^{40} \equiv 689 \equiv 1 + 43 \cdot 16 \pmod{43^2}.$$

这就是说,

$$3^{42} \not\equiv 1 \pmod{43^2}, \quad 46^{42} \not\equiv 1 \pmod{43^2}.$$

根据定 3 之证明, 3 和 46 都是模 $m = 43^2 = 1849$ 的原根, 也都是模 43^α 的原根.

在 $m = p^\alpha$ 或 $2p^\alpha$ 的情形下, 模 m 的原根 g 是存在的.

利用原根引进指标概念, 并研究 $x^n \equiv a \pmod{m}$, $(a, m) = 1$ 有解的条件及解数.

对任意的整数 a , $(a, m) = 1$, 存在惟一的整数 r , $1 \leq r \leq \varphi(m)$, 使得 $g^r \equiv a \pmod{m}$.

定义 1 设 m 是大于 1 的整数, g 是模 m 的一个原根. 设 a 是一个与 m 互素的整数. 则存在惟一的整数 r 使得

$$g^r \equiv a \pmod{m}, \quad 1 \leq r \leq \varphi(m)$$

成立, 这个整数 r 叫做以 g 为底的 a 对模 m 的一个 **指标**, 记作 $r = \text{ind}_g a$ (或 $r = \text{ind} a$).

例 1 整数 5 是模 17 的原根. 并且我们有

5^1	5^2	5^3	5^4	5^5	5^6	5^7	5^8	5^9	5^{10}	5^{11}	5^{12}	5^{13}	5^{14}	5^{15}	5^{16}
5	8	6	13	14	2	10	-1	12	9	11	4	3	15	7	1

因此, 我们有

$$\begin{aligned} \text{ind}_5 1 &= 16, \text{ind}_5 2 = 6, \text{ind}_5 3 = 13, \text{ind}_5 4 = 12, \text{ind}_5 5 = 14, \text{ind}_5 6 = 3, \\ \text{ind}_5 7 &= 15, \text{ind}_5 8 = 2, \text{ind}_5 9 = 10, \text{ind}_5 10 = 7, \text{ind}_5 11 = 11, \text{ind}_5 12 = 9, \\ \text{ind}_5 13 &= 4, \text{ind}_5 14 = 5, \text{ind}_5 15 = 14, \text{ind}_5 16 = 8. \end{aligned}$$

定理 2 设 g 是原根. 设 $(a, m) = 1$. 如果 r 使得 $g^r \equiv a \pmod{m}$ 成立, 则这个整数 r 满足 $r \equiv \text{ind}_g a \pmod{\varphi(m)}$.

证 因为 $(a, m) = 1$, 所以 $g^r \equiv a \equiv g^{\text{ind}_g a} \pmod{m}$.

从而, $g^{r - \text{ind}_g a} \equiv 1 \pmod{m}$.

又因为 g 模 m 的指数是 $\varphi(m)$, $\varphi(m) \mid r - \text{ind}_g a$. 因此,

$$r \equiv \text{ind}_g a \pmod{\varphi(m)}.$$

推论 设 g 是原根. 设 $(a, m) = 1$. 则 $\text{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$.

证 因为 $g^0 \equiv 1 \pmod{m}$, 根据定理 2, 我们有

$$\text{ind}_g 1 \equiv 0 \pmod{\varphi(m)}.$$

定理 3 设 m 是大于 1 的整数, g 是模 m 的一个原根, r 是一个整数, 满足 $1 \leq r \leq \varphi(m)$. 则以 g 为底的对模 m 有 同指 r 的所有整数全体是模 m 的一个简化剩余类.

定理 4 设 m 是大于 1 的整数, g 是模 m 的一个原根. 若 $a_1, \dots, a_n$ 是与 m 互素的 n 个整数, 则

$$\operatorname{ind}_g(a_1 \cdots a_n) \equiv \operatorname{ind}_g(a_1) + \cdots + \operatorname{ind}_g(a_n) \pmod{\varphi(m)}.$$

特别地, $\operatorname{ind}_g(a^n) \equiv n \operatorname{ind}_g(a) \pmod{\varphi(m)}$.

例 2 作模 41 的指标表.

解 已知 6 是模 41 的原根, 直接计算 $g^r \pmod{m}$:

$$\begin{aligned}
 6^{40} &\equiv 1, & 6^1 &\equiv 6, & 6^2 &\equiv 19, & 6^3 &\equiv 11, & 6^4 &\equiv 25, & 6^5 &\equiv 27, & 6^6 &\equiv 39, & 6^7 &\equiv 29, \\
 6^8 &\equiv 10, & 6^9 &\equiv 19, & 6^{10} &\equiv 32, & 6^{11} &\equiv 28, & 6^{12} &\equiv 4, & 6^{13} &\equiv 24, & 6^{14} &\equiv 21, & 6^{15} &\equiv 3, \\
 6^{16} &\equiv 18, & 6^{17} &\equiv 26, & 6^{18} &\equiv 33, & 6^{19} &\equiv 34, & 6^{20} &\equiv 40, & 6^{21} &\equiv 35, & 6^{22} &\equiv 5, & 6^{23} &\equiv 30, \\
 6^{24} &\equiv 16, & 6^{25} &\equiv 14, & 6^{26} &\equiv 2, & 6^{27} &\equiv 12, & 6^{28} &\equiv 31, & 6^{29} &\equiv 22, & 6^{30} &\equiv 9, & 6^{31} &\equiv 13, \\
 6^{32} &\equiv 37, & 6^{33} &\equiv 17, & 6^{34} &\equiv 20, & 6^{35} &\equiv 38, & 6^{36} &\equiv 23, & 6^{37} &\equiv 15, & 6^{38} &\equiv 8, & 6^{39} &\equiv 7.
 \end{aligned}$$

数的指标: 第一列表示十位数, 第一行表示个位数, 交叉位置表示指标所对应数.

	0	1	2	3	4	5	6	7	8	9
0		40	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

例 3 分别求整数 $a = 28, 18$ 以 6 为底模 41 的指 。

解 根据模 41 的以原根 $g = 6$ 的指数表, 查找十位数 2 所在行, 个位数 8 所在列, 交叉位置的数 11 就是 $\text{ind}_6 28 = 11$. 而查找十位数 1 所在行, 个位数 8 所在列, 交叉位置的数 16 就是 $\text{ind}_6 18 = 16$.

为什么要列表呢? 这是因为从整数 r 计算 $g^r \equiv a \pmod{m}$ 很容易; 但从整数 a 求整数 r 使得 $g^r \equiv a \pmod{m}$ 就非常困难.

定义 2 设 m 是大于 1 的整数, a 是与 m 互素的整数. 如果 n 次同余式

$$x^n \equiv a \pmod{m} \quad (1)$$

有解, 则 a 叫做对模 m 的 n **次剩余**; 否则, a 叫做对模 m 的 n **次非剩余**.

例 4 求 5 次同余式 $x^5 \equiv 9 \pmod{41}$ 的解.

解 从模 41 的指数表, 查找整数 9 的十位数 0 所在的行, 个位数 9 所在的列, 交叉位置的数 30 就是 $\text{ind}_6 9 = 30$. 再令 $x = 6^y \pmod{41}$. 原同余式就变为

$$6^{5y} \equiv 6^{30} \pmod{41}.$$

因为 6 是模 41 的原根, 根据定理 2 我们有

$$5y \equiv 30 \pmod{40} \quad \text{或} \quad y \equiv 6 \pmod{8}.$$

解得 $y \equiv 6, 14, 22, 30, 38 \pmod{40}$. 因此, 原同余式的解为

$$\begin{aligned} x &\equiv 6^6 \equiv 39, \quad x \equiv 6^{14} \equiv 21, \quad x \equiv 6^{22} \equiv 5, \\ x &\equiv 6^{30} \equiv 9, \quad x \equiv 6^{38} \equiv 8, \quad x \equiv 6^{39} \equiv 7 \pmod{41}. \end{aligned}$$

定理 5 设 g 是原根. 设 $(a, m) = 1$. 则 $x^n \equiv a \pmod{m}$ (2)

有解的充分必要条件是 $(n, \varphi(m)) \mid \text{inda}$,

且在有解的情况下, 解数为 $(n, \varphi(m))$.

证 若同余式 (2) 有解 $x \equiv x_0 \pmod{m}$,

则分别存在非负整数 u, r 使得 $x_0 \equiv g^u, a \equiv g^r \pmod{m}$.

由 (2) 得 $g^{un} \equiv g^r \pmod{m}$ 或 $un \equiv r \pmod{\varphi(m)}$.

即同余式 $nX \equiv r \pmod{\varphi(m)}$ (3) 有解 $X \equiv u \pmod{\varphi(m)}$.

因此, $(n, \varphi(m)) \mid \text{inda}$.

反过来, 若 $(n, \varphi(m)) \mid \text{inda}$, 则 (3) 有解 $X \equiv u \pmod{\varphi(m)}$, 且解数为 $(n, \varphi(m))$. 因此, (2) 有解 $x_0 \equiv g^u \pmod{m}$, 解数为 $(n, \varphi(m))$.

推论 在定 5 的假设条件下, a 是模 m 的 n 次剩余的充分必要条件是 $a^{\varphi(m)/d} \equiv 1 \pmod{m}$, $d = (n, \varphi(m))$.

证 由定 5 之证明: 同余式 $x^n \equiv a \pmod{m}$ 有解的充分必要条件是同余式 $nX \equiv r \pmod{\varphi(m)}$ 有解. 而这等价于 $(n, \varphi(m)) \mid \text{inda}$, 即 $\text{inda} \equiv 0 \pmod{d}$. 两端同乘 $\frac{\varphi(m)}{d}$, 得到 $\frac{\varphi(m)}{d} \text{inda} \equiv 0 \pmod{\varphi(m)}$. 这等价于 $a^{\varphi(m)/d} \equiv 1 \pmod{m}$.

例 5 求解同余式 $x^8 \equiv 23 \pmod{41}$.

解 因为 $d = (n, \varphi(m)) = (8, \varphi(41)) = (8, 40) = 8$, $\text{ind}23 = 36$. 又 36 不能被 8 整除, 所以同余式无解.

例 6 求解同余式 $x^{12} \equiv 37 \pmod{41}$.

解 因为

$$d = (n, \varphi(m)) = (12, \varphi(41)) = (12, 40) = 4, \\ \text{ind}37 = 32.$$

又 $4|32$, 所以同余式有解. 现求解等价的同余式:

$$12 \text{ ind}x \equiv \text{ind}37 \pmod{40}$$

或 $3 \text{ ind}x \equiv 8 \pmod{10}$.

得到 $\text{ind}x \equiv 6, 16, 26, 36 \pmod{40}$.

查指 表得原同余式解

$$x \equiv 39, 18, 2, 23 \pmod{41}.$$

定理 6 设 g 是原根, $(a, m) = 1$. 则 a 对模 m 的指数是

$$e = \frac{\varphi(m)}{(\text{inda}, \varphi(m))}.$$

特别地, a 是模 m 的原根当且仅当 $(\text{inda}, \varphi(m)) = 1$.

证 因为模 m 有原根 g , 所以有

$$a = g^{\text{inda}} \pmod{m}.$$

根据 §5.1 定理 3, a 的指数为

$$\text{ord}(a) = \text{ord}(g^{\text{inda}}) = \frac{\text{ord}(g)}{(\text{ord}(g), \text{inda})} = \frac{\varphi(m)}{(\text{inda}, \varphi(m))}.$$

显然, a 是模 m 的原根的充分必要条件是 $\text{ord}(a) = \varphi(m)$, 即

$$(\text{inda}, \varphi(m)) = 1.$$

定理 7 设 g 是模 m 的一个原根. 则模 m 的简化剩余系中, 指数是 e 的整数个数是 $\varphi(e)$. 特别地, 在模 m 的简化剩余系中, 原根的个数是 $\varphi(\varphi(m))$.

证 因为模 m 有原根 g , 根据 §5.1 定 3, 知 $a = g^d$ 的指数为

$$\text{ord}(a) = \text{ord}(g^d) = \frac{\text{ord}(g)}{(\text{ord}(g), d)} = \frac{\varphi(m)}{(d, \varphi(m))}.$$

显然, a 的指数是 e 的充分必要条件是 $\frac{\varphi(m)}{(d, \varphi(m))} = e$, 即

$$(d, \varphi(m)) = \frac{\varphi(m)}{e}.$$

令 $d = d' \frac{\varphi(m)}{e}$, $0 \leq d' < e$. 上式等价于 $(d', e) = 1$. 易知这样的 d' 有 $\varphi(e)$ 个. 从而指数为 $\varphi(m)$ 的整数个数是 $\varphi(\varphi(m))$. 即原根个数是 $\varphi(\varphi(m))$.

第六章 素性检验

在本章，我们研究如何产生以及如何快速产生大素数.

根据 Fermat 小定 理：如果 n 是素数，则对任意整数 b , $(b, n) = 1$, 有

$$b^{n-1} \equiv 1 \pmod{n}.$$

由此：如果有一个整数 b , $(b, n) = 1$ 使得 $b^{n-1} \not\equiv 1 \pmod{n}$, 则 n 是一个合数.

例 1 因为 $2^{62} \equiv 2^{60} \cdot 2^2 \equiv (2^6)^{10} \cdot 2^2 \equiv 64^{10} \cdot 2^2 \equiv 4 \not\equiv 1 \pmod{63}$, 所以 63 一个是合数.

上述说法的否定说法不能成立. 事实上, 我们有

例 2 $8^{62} \equiv (2^6)^{31} \equiv 1 \pmod{63}$.

定义 1 设 n 是一个奇合数. 如果整数 b , $(b, n) = 1$ 使得同余式 $b^{n-1} \equiv 1 \pmod{n}$ (1) 成立, 则 n 叫做对于基 b 的 **拟素数**.

例 3 整数 63 都是对于基 $b = 8$ 的拟素数,

例 4 整数 $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, $645 = 3 \cdot 5 \cdot 43$ 都是对于基 $b = 2$ 的拟素数, 因为

$$2^{340} \equiv 1 \pmod{340}, \quad 2^{560} \equiv 1 \pmod{561}, \quad 2^{644} \equiv 1 \pmod{645}.$$

引理 1 设 d, n 都是正整数. 如果 d 能整除 n , 则 $2^d - 1$ 能整除 $2^n - 1$.

证 因为 $d \mid n$, 所以存在一个整数 q 使得 $n = dq$. 因此, 我们有

$$2^n - 1 = (2^d)^q - 1 = (2^d - 1)((2^d)^{q-1} + (2^d)^{q-2} + \cdots + 2^d + 1).$$

故 $2^d - 1 \mid 2^n - 1$.

定理 1 存在无穷多个对于基 2 的拟素数.

证 (I) 要证: 如果 n 是对于基 2 的拟素数, 则 $m = 2^n - 1$ 也是对于基 2 的拟素数. 事实上, 因为 n 是对于基 2 的拟素数, 所以 n 是奇合数, 并且 $2^{n-1} \equiv 1 \pmod{n}$. 由于 n 是奇合数, 所以有因数分解 $n = dq$, $1 < d < n, 1 < q < n$. 根据引 1, $2^d - 1 \mid 2^n - 1$. 因此 $m = 2^n - 1$ 是合数. 现在验证: $2^{m-1} \equiv 1 \pmod{m}$.

因为 $2^{n-1} \equiv 1 \pmod{n}$, 所以可将 $m - 1 = 2(2^{n-1} - 1) = kn$. 根据引 1, $2^n - 1 \mid 2^{m-1} - 1$. 因此, 同余式 $2^{m-1} \equiv 1 \pmod{m}$ 成立. 故 $m = 2^n - 1$ 是对于基 2 的拟素数.

(II) 取 n_0 为对于基 2 的一个拟素数, 例如 $n_0 = 341$ 是一个对于基 2 的拟素数. 再令 $n_1 = 2^{n_0} - 1$, $n_2 = 2^{n_1} - 1$, $n_3 = 2^{n_2} - 1, \dots$. 根据结论 (I), 这些整数都是对于基 2 的拟素数.

定理 2 设 n 是一个奇合数. 则

(i) n 是对于基 b 的拟素数当且仅当 b 模 n 的阶整除 $n - 1$.

(ii) 如果 n 是对于基 b_1 和基 b_2 的拟素数, 则 n 是对于基 $b_1 b_2$ 的拟素数.

(iii) 若 n 是对于基 b 的拟素数, 则 n 是对于基 b^{-1} 的拟素数.

定理 2 设 n 是奇合数. 则 (iv) 如果有一个整数 b , $(b, n) = 1$, 使 (1) 不成立, 则模 n 的简化剩余系中至少有一半的数使 (1) 不成立.

证(iv) 设 $b_1, \dots, b_s, b_{s+1}, \dots, b_{\varphi(n)}$ 是模的简化剩余系, 其中前 s 个数使得 (1) 成立, 后 $\varphi(n) - s$ 个数使得 (1) 不成立. 根据假设条件, 存在一个整数 b , $(b, n) = 1$, 使得 (1) 不成立, 再根据结论 (ii) 和 (iii), 有 s 个模 n 不同简化剩余 $bb_1, \dots, bb_s$ 使得 (1) 不成立. 因此, $s \leq \varphi(n) - s$, 或者 $\varphi(n) - s \geq \frac{\varphi(n)}{2}$. 这就是说, 模 n 的简化剩余系中至少有一半的数使得 (1) 不成立.

例 5 设 $n = 63$. 求出所有整数 b , $1 \leq b \leq n - 1$ 使得 n 是对于基 b 的拟素数.

b	b^{n-1}	a	a^{n-1}	a	a^{n-1}	a	a^{n-1}	a	a^{n-1}	a	a^{n-1}	a	a^{n-1}
1	1	11	58	21	0	31	16	41	43	51	18	61	4
2	4	12	18	22	43	32	16	42	0	52	58	62	1
3	9	13	43	23	25	33	18	43	22	53	37		
4	16	14	7	24	9	34	22	44	46	54	18		
5	25	15	36	25	58	35	28	45	9	55	1		
6	36	16	4	26	46	36	36	46	37	56	49		
7	49	17	37	27	36	37	46	47	4	57	36		
8	1	18	9	28	28	38	58	48	36	58	25		
9	18	19	46	29	22	39	9	49	7	59	16		
10	37	20	22	30	18	40	25	50	43	60	9		

定 2 (iv) 告知：对于大奇数，如果有一个整数 b , $(b, n) = 1$, 使得 (1) 不成立，则模 n 的简化剩余系中至少有一半的数使得 (1) 不成立. 这就是说，对于随机选取的整数 b , $(b, n) = 1$, 有 50% 以上的机会来判断出 n 是合数，或者说 n 是合数的可能性小于 50% .

现在，给出判断一个大奇整数 n 为素数的方法：

随机选取整数 b_1 , $0 < b_1 < n$, 计算 $d_1 = (b_1, n)$. 如果 $d_1 > 1$, 则 n 不是素数. 如果 $d_1 = 1$, 则计算 $b_1^{n-1} \pmod{n}$, 看看同余式 (1) 是否成立. 如果不成立, 则 n 不是素数. 如果成立, 则 n 是合数的可能性小于 $\frac{1}{2}$ 或者说 n 是素数可能性大于 $1 - \frac{1}{2}$.

重复上述步骤.

再随机选取整数 b_2 , $0 < b_2 < n$, 计算 $d_2 = (b_2, n)$. 如果 $d_2 > 1$, 则 n 不是素数. 如果 $d_2 = 1$, 则计算 $b_2^{n-1} \pmod{n}$, 看看同余式 (1) 是否成立. 如果不成立, 则 n 不是素数. 如果成立, 则 n 是合数的可能性小于 $\frac{1}{2^2}$ 或者说 n 是素数可能性大于 $1 - \frac{1}{2^2}$.

继续重复上述步骤, $\dots$, 直至第 t 步.

随机选取整数 b_t , $0 < b_t < n$, 计算 $d_t = (b_t, n)$. 如果 $d_t > 1$, 则 n 不是素数. 如果 $d_t = 1$, 则计算 $b_t^{n-1} \pmod{n}$, 看看同余式 (1) 是否成立. 如果不成立, 则 n 不是素数. 如果成立, 则 n 是合数的可能性小于 $\frac{1}{2^t}$ 或者说 n 是素数可能性大于 $1 - \frac{1}{2^t}$.

上述过程也可简单归纳为:

Fermat 素性检验

给定奇整数 $n \geq 3$ 和安全参数 t .

1. 随即选取整数 b , $2 \leq b \leq n - 2$;
2. 计算 $r = b^{n-1} \pmod{n}$;
3. 如果 $r \neq 1$, 则 n 是合数.
4. 上述过程重复 t 次.

定义 2 合数 n 称为 **Carmichael 数**, 如果对所有的正整数 b , $(b, n) = 1$, 都有同余式

$$b^{n-1} \equiv 1 \pmod{n}$$

成立.

例 6 整数 $561 = 3 \cdot 11 \cdot 17$ 是一个 Carmichael 数.

证 如果 $(b, 561) = 1$, 则 $(b, 3) = (b, 11) = (b, 17) = 1$. 根据 Fermat 小定, $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$, $b^{16} \equiv 1 \pmod{17}$. 从而,

$$b^{560} \equiv (b^2)^{280} \equiv 1 \pmod{3}, \quad b^{560} \equiv (b^{10})^{56} \equiv 1 \pmod{11}, \quad b^{560} \equiv (b^{16})^{35} \equiv 1 \pmod{17}.$$

因此, $b^{560} \equiv 1 \pmod{561}$.

定理 3 设 n 是一个奇合数.

(i) 如果 n 被一个大于 1 平方数整除, 则 n 不是 Carmichael 数.

(ii) 如果 $n = p_1 \cdots p_k$ 是一个无平方数, 则 n 是 Carmichael 数

的充要条件是

$$p_i - 1 \mid n - 1, \quad 1 \leq i \leq k.$$

定理 4 每个 Carmichael 数是至少三个不同素数的乘积.

注: 1. 存在无穷多个 Carmichael 数.

2. 当 n 充分大时, 区间 $[2, n]$ 内的 Carmichael 数的个数 $\geq n^{2/7}$.

设 n 是奇素数. 根据定 , 有同余式 $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}$ 对任意整数 b 成立.

因此, 如果存在整数 b , $(b, n) = 1$, 使得 $b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}$, 则 n 不是一个素数.

例 1 设 $n = 341$, $b = 2$. 分别计算得到: $2^{170} \equiv 1 \pmod{341}$ 以及 $\left(\frac{2}{341}\right) = (-1)^{(341^2-1)/8} = -1$, 因为 $2^{170} \not\equiv \left(\frac{2}{341}\right) \pmod{341}$. 所以 341 不是一个素数.

定义 1 设 n 是一个正奇合数. 设整数 b 与 n 互素. 如果整数 n 和 b 满足条件: $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}$, 则 n 叫做对于基 b 的 **Euler 拟素数**.

例 2 设 $n = 1105$, $b = 2$. 分别计算得到: $2^{552} \equiv 1 \pmod{1105}$ 以及 $\left(\frac{2}{1105}\right) = (-1)^{(1105^2-1)/8} = 1$. 因为 $2^{552} \equiv \left(\frac{2}{1105}\right) \pmod{1105}$, 所以 1105 是一个对于基 2 的 Euler 拟素数.

定理 1 如果 n 是对于基 b 的 Euler 拟素数, 则 n 是对于基 b 的拟素数.

证 设 n 是对于基 2 的 Euler 拟素数, 则 $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}$. 上式两端平方, 并注意到 $\left(\frac{b}{n}\right) = \pm 1 \pmod{n}$,

$$b^{n-1} \equiv (b^{(n-1)/2})^2 \equiv \left(\frac{b}{n}\right)^2 \equiv 1 \pmod{n},$$

因此, n 是对于基 b 的拟素数.

定 1 的逆不成立, 即不是每个拟素数都是 Euler 拟素数. 例如: 341 是对于基 2 的拟素数, 但不是对于基 2 的 Euler 拟素数.

Solovay-Stassen 素性检验

给定奇整数 $n \geq 3$ 和安全参数 t .

1. 随即选取整数 b , $2 \leq b \leq n - 2$;
2. 计算 $r = b^{(n-1)/2} \pmod{n}$;
3. 如果 $r \neq 1$ 以及 $r \neq n - 1$, 则 n 是合数.
4. 计算 Jacobi 符号 $s = \left(\frac{b}{n}\right)$;
5. 如果 $r \neq s$, 则 n 是合数.
6. 上述过程重复 t 次.

设 n 是正奇整数, 并且有 $n-1=2^s t$, 则有如下因数分解式:

$$b^{n-1}-1=(b^{2^{s-1}t}+1)(b^{2^{s-2}t}+1)\cdots(b^t+1)(b^t-1).$$

因此, 如果 $b^{n-1}\equiv 1 \pmod{n}$, 则如下同余式至少有一个成立:

$$b^t\equiv 1, \quad b^t\equiv -1, \quad b^{2^r t}\equiv -1, \dots, \quad b^{2^{s-1}t}\equiv -1 \pmod{n}.$$

定义 1 设 n 是一个奇合数, 且有表示式 $n-1=2^s t$, 其中 t 为奇数. 设 $(b, n)=1$. 如果整数 n 和 b 满足条件: $b^t\equiv 1 \pmod{n}$, 或者存在一个整数 r , $0\leq r<s$ 使得 $b^{2^r t}\equiv -1 \pmod{n}$, 则 n 叫做对于基 b 的 **强拟素数**.

例 1 整数 $n=2047=23\cdot 89$ 是对于基 $b=2$ 的强拟素数.

解 因为 $2^{2046/2}\equiv (2^{11})^{93}\equiv (2048)^{93}\equiv 1 \pmod{2046}$.

定理 1 存在无穷多个对于基 2 的强拟素数.

定理 2 如果 n 是对于基 b 的强拟素数, n 是对于基 b 的 Euler 拟素数.

定理 3 设 n 是一个奇合数. 则 n 是对于基 b , $1 \leq b \leq n-1$, 的强拟素数的可能性至多为 25%.

Miller-Rabin 素性检验

给定奇整数 $n \geq 3$ 和安全参数 k , 写 $n - 1 = 2^s t$, 其中 t 为奇整数.

1. 随机选取整数 b , $2 \leq b \leq n - 2$;
2. 计算 $r_0 \equiv b^t \pmod{n}$;
3. a) 如果 $r_0 = 1$ 或 $r_0 = n - 1$, 则通过检验, 可能为素数.

回到 1. 继续选取另一个随机整数 b , $2 \leq b \leq n - 2$;

- b) 否则, 有 $r_0 \neq 1$ 以及 $r_0 \neq n - 1$, 计算 $r_1 \equiv r_0^2 \pmod{n}$;
4. a) 如果 $r_1 = n - 1$, 则通过检验, 可能为素数.

回到 1. 继续选取另一个随机整数 b , $2 \leq b \leq n - 2$;

- b) 否则, 有 $r_1 \neq n - 1$, 计算 $r_2 \equiv r_1^2 \pmod{n}$; 如此继续下去,
- s+2. a) 如果 $r_{s-1} = n - 1$, 则通过检验, 可能为素数.

回到 1. 继续选取另一个随机整数 b , $2 \leq b \leq n - 2$;

- b) 否则, 有 $r_{s-1} \neq n - 1$, n 为合数.

第七章 连分数

1. 连分数的定义.
2. 简单连分数的定义.
3. 实数的连分数构造.
4. 最佳逼近.
5. 连分数的应用.

对于实数 $\sqrt{2}$, 如何计算其值呢? 我们可以采用如下方法, 即用有理数来近似.

首先, 作展开式

$$\begin{aligned}
 \sqrt{2} &= 1 + (\sqrt{2} - 1) \\
 &= 1 + \frac{1}{\sqrt{2} + 1} \\
 &= 1 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}} \\
 &= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}}
 \end{aligned}$$

$$\begin{aligned}
 &= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}}} \\
 &= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}}}}.
 \end{aligned}$$

其次，可用有 分数来近似。例如，

$$\begin{aligned}
 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} &= 1 + \frac{1}{2 + \frac{1}{2 + \frac{2}{5}}} = 1 + \frac{1}{2 + \frac{5}{12}} \\
 &= 1 + \frac{12}{29} = \frac{41}{29} = 1.413793103
 \end{aligned}$$

最后，列出 $\sqrt{2}$ (取 10 位十进制) 与 10 个有理数间的误差.

i	a_i	P_i/Q_i	$\sqrt{2} - P_i/Q_i$	i	a_i	P_i/Q_i	$\sqrt{2} - P_i/Q_i$
0	1	1/1	0.414213562	5	2	99/70	-0.000072152
1	2	3/2	-0.085786438	6	2	239/169	0.000012379
2	2	7/5	0.014213562	7	2	577/408	-0.000002124
3	2	17/12	-0.002453105	8	2	1393/985	0.000000364
4	2	41/29	0.000420459	9	2	3363/2378	-0.000000063

定义 1 设 $x_0, x_1, \dots$ 是一个无穷实数列, $x_i > 0, i \geq 1$. 对于整数 $n \geq 0$, 我们将表示式

$$x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \dots + \frac{1}{x_n}}}} \quad (1)$$

叫做 n 阶 **有限连分数**, 它的值是一个实数. 当 $x_0, x_1, \dots, x_n$ 都是整数时, 表示式 (1) 叫做 n 阶 **有限简单连分数**, 它的值是一个有分数. 有 连分数也记作 $[x_0, x_1, \dots, x_n]$. (2)

设 $0 \leq k \leq n$, 我们将有限连分数 $[x_0, x_1, \dots, x_k]$ (3) 叫做有限连分数 (1) 的第 k 个 **渐近分数**. 当 (2) 是有限简单连分数时, 将 x_k 叫做它的第 k 个 **部分商**.

当 (1)(或 (2)) 中的 $n \rightarrow \infty$ 时, 将表示式

$$x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \dots}}} \quad (4)$$

或者简记为 $[x_0, x_1, x_2, \dots]$. (5) 叫做 **无限连分数**. 当 $x_0, x_1, \dots$ 都是整数时, 表示式 (4) 叫做 **无限简单连分数**. 设 $k \geq 0$, 我们将有限连分数 $[x_0, x_1, x_2, \dots, x_k]$ 叫做无限连分数 (4) 的第 k 个 **渐近分数**. 当 (4) 是无限简单连分数时, 将 x_k 叫做它的第 k 个 **部分商**.

如果存在极限 $\lim_{k \rightarrow \infty} [x_0, x_1, x_2, \dots, x_k] = \theta$, (6) 则称无限连分数 (4)(或 (5)) 是收敛的, θ 称为无限连分数 (4)(或 (5)) 的值, 记作 $[x_0, x_1, x_2, \dots] = \theta$. 如果极限 (6) 不存在, 则称无限连分数 (4)(或 (5)) 是发散的.

引理 设 a, b, c 是实数, $b \neq 0$. 设 $f(x) = a + \frac{b}{c+x}$. 则

(i) 当 $b > 0$ 时, $f(x)$ 在 $x > c$ (或 $x < -c$) 上是单调递减函数, 即当 $c < x < x'$ (或 $x < x' < -c$) 时, 有 $f(x) > f(x')$.

(ii) 当 $b < 0$ 时, $f(x)$ 在 $x > c$ (或 $x < -c$) 上是单调递增函数, 即当 $c < x < x'$ (或 $x < x' < -c$) 时, 有 $f(x) < f(x')$.

证 对于 $c < x < x'$ (或 $x < x' < -c$), 我们有

$$f(x') - f(x) = \left(a + \frac{b}{c+x'}\right) - \left(a + \frac{b}{c+x}\right) = \frac{-b(x' - x)}{(c+x')(c+x)}.$$

因为 $(c+x')(c+x) > 0$, 所以 (i) 当 $b > 0$ 时, 有 $f(x') < f(x)$. 而 (ii) 当 $b < 0$ 时, 有 $f(x') > f(x)$. 故结论成立. 证毕.

定理 1 设 $x_0, x_1, \dots$ 是一个无穷实数列, $x_i > 0, i \geq 1$. 则

(i) 对任意整数 $n \geq 1, r \geq 1$, 我们有

$$\begin{aligned} & [x_0, x_1, \dots, x_{n-1}, x_n, \dots, x_{n+r}] \\ &= [x_0, x_1, \dots, x_{n-1}, [x_n, \dots, x_{n+r}]] \\ &= [x_0, x_1, \dots, x_{n-1}, x_n + 1/[x_{n+1}, \dots, x_{n+r}]]. \end{aligned} \quad (7)$$

特别地, $[x_0, x_1, \dots, x_{n-1}, x_n, x_{n+1}] = [x_0, x_1, \dots, x_{n-1}, x_n + 1/x_{n+1}]. \quad (8)$

(ii) 对任意实数 $\eta > 0$ 和整数 $n \geq 0$,

(a) 当 n 是奇数时, $[x_0, x_1, \dots, x_{n-1}, x_n] > [x_0, x_1, \dots, x_{n-1}, x_n + \eta,] \quad (9)$

(b) 当 n 是偶数时, $[x_0, x_1, \dots, x_{n-1}, x_n] < [x_0, x_1, \dots, x_{n-1}, x_n + \eta,] \quad (10)$

(iii) 对整数 $n \geq 0$, 令 $\theta_n = [x_0, x_1, \dots, x_{n-1}, x_n]$,

(a) 对任意整数 $r \geq 1, \theta_{2n+1} > \theta_{2n+1+r}, \quad (b) \text{ 对任意整数 } r \geq 1, \theta_{2n} < \theta_{2n+r},$

(c) $\theta_1 > \theta_3 > \dots \theta_{2n-1} > \dots, \quad (d) \theta_0 < \theta_2 < \dots \theta_{2n} < \dots,$

(e) 对任意整数 $s \geq 1, t \geq 0, \theta_{2s-1} > \theta_{2t}.$

定理 2 设 $x_0, x_1, x_2, \dots$ 是无穷实数列, $x_j > 0, j \geq 1$. 再设

$$P_{-2} = 0, \quad P_{-1} = 1, \quad P_n = x_n P_{n-1} + P_{n-2}, \quad n \geq 0, \quad (11)$$

$$Q_{-2} = 1, \quad Q_{-1} = 0, \quad Q_n = x_n Q_{n-1} + Q_{n-2}, \quad n \geq 0. \quad (12)$$

则 $[x_0, x_1, \dots, x_{n-1}, x_n] = \frac{P_n}{Q_n}, \quad n \geq 0, \quad (13)$

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1}, \quad n \geq -1, \quad (14)$$

$$P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n x_n, \quad n \geq 0. \quad (15)$$

特别地, 我们有

$$[x_0, x_1, \dots, x_{n-1}, x_n] - [x_0, x_1, \dots, x_{n-1}] = \frac{(-1)^{n+1}}{Q_{n-1} Q_n}, \quad n \geq 1, \quad (16)$$

$$[x_0, x_1, \dots, x_{n-2}, x_{n-1}, x_n] - [x_0, x_1, \dots, x_{n-2}] = \frac{(-1)^n x_n}{Q_{n-2} Q_n}, \quad n \geq 2. \quad (17)$$

在知道连分数的部分商的情况下，定 给出了求渐近连分数的方法. 我们用列表的形式给出 $\sqrt{2} = [1, 2, 2, 2, \dots]$ 的渐近连分数：

k	x_k	P_k	Q_k	k	x_k	P_k	Q_k
-2		0	1	3	2	17	12
-1		1	0	4	2	41	29
0	1	1	1	5	2	99	70
1	2	3	2	6	2	239	169
2	2	7	5	7	2	577	408

由此得到

$$1.412011 < \frac{P_6}{Q_6} = \frac{239}{169} < \sqrt{2} < \frac{P_7}{Q_7} = \frac{577}{408} < 1.412157.$$

关于 α 与其渐近连分数, 我们有更准确的公式.

定理 3 设 $x_0, x_1, x_2, \dots, x_n$ 是实数列, $x_j > 0, j \geq 1$. 再设

$$\alpha = [x_0, x_1, x_2, \dots, x_n], \quad \alpha_{k+1} = [x_{k+1}, \dots, x_n] \quad (0 \leq k \leq n).$$

则

$$\alpha - \frac{P_k}{Q_k} = \frac{(-1)^k}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})}.$$

证 根据定 1 (i) 及定 2, 我们有

$$\begin{aligned} \alpha - \frac{P_k}{Q_k} &= \frac{\alpha_{k+1}P_k + P_{k-1}}{\alpha_{k+1}Q_k + Q_{k-1}} - \frac{P_k}{Q_k} \\ &= \frac{-(P_kQ_{k-1} - P_{k-1}Q_k)}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})} = \frac{(-1)^k}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})}. \end{aligned}$$

给定一个实数 x ，我们构造 x 的简单连分数如下：

(i) 令 $a_0 = [x]$, $x_0 = x - a_0$. $0 \leq x_0 < 1$.

(ii) 如果 $x_0 = 0$, 则终止. 否则, 令 $a_1 = [\frac{1}{x_0}]$, $x_1 = \frac{1}{x_0} - a_1$.

(iii) 如果 $x_1 = 0$, 则终止. 否则, 令 $a_2 = [\frac{1}{x_1}]$, $x_2 = \frac{1}{x_1} - a_2$.

如此继续下去, 得到 a_k, x_k .

(k+2) 如果 $x_k = 0$, 则终止. 否则, 令 $a_{k+1} = [\frac{1}{x_k}]$, $x_{k+1} = \frac{1}{x_k} - a_{k+1}$

由此得到 x 的简单连分数为

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n + \dots}}}$$

特别地, 当 $x = \frac{u_{-2}}{u_{-1}}$, $u_{-1} \geq 1$ 时, 我们所构造的 x 的简单连分数 $[a_0, a_1, a_2, \dots, a_n]$ 的部分商 a_k , ($0 \leq k \leq n$) 满足如下关系式:

- (i) $u_{-2} = a_0 u_{-1} + u_0, \quad 0 < u_0 = x_0 u_{-1} < u_{-1}.$
- (ii) $u_{-1} = a_1 u_0 + u_1, \quad 0 < u_1 = x_1 u_0 < u_0.$
- (iii) $u_0 = a_2 u_1 + u_2, \quad 0 < u_2 = x_2 u_1 < u_1.$
-
- (n) $u_{n-3} = a_{n-1} u_{n-2} + u_{n-1}, \quad 0 < u_{n-1} = x_{n-1} u_{n-2} < u_{n-2}.$
- (n + 1) $u_{n-2} = a_n u_{n-1} + u_n, \quad 0 = u_n = x_n u_{n-1} < u_{n-1}.$

因为 $\{u_k\}_{k \geq -2}$ 是关于 k 的严格递减的非负整数列, 所以使得 $u_n = 0$ 的 n 是存在的. 因此, $x_n = 0$. 有 分数 $x = \frac{u_{-2}}{u_{-1}}$ 有有限简单连分数

$$x = [a_0, a_1, a_2, \dots, a_n].$$

当 $a_n \geq 2$ 时, 我们也有

$$x = [a_0, a_1, a_2, \dots, a_n] = [a_0, a_1, a_2, \dots, a_n - 1, 1].$$

这就是说, 有 分数有两种连分数表示式. 是否存在其它形式的表示式呢? 答案是否定的. 我们有如下定 .

定理 1 设 $[a_0, a_1, a_2, \dots, a_n]$ 和 $[b_0, b_1, b_2, \dots, b_m]$ 是两个有限简单连分数, $a_n \geq 2, b_m \geq 2$. 如果 $[a_0, a_1, a_2, \dots, a_n] = [b_0, b_1, b_2, \dots, b_m]$, 则 $n = m, a_i = b_i, i = 0, \dots, n$.

定理 2 任一不是整数的有理数 $x = \frac{u_0}{u_1}$ 有且仅有给出的两种有限简单连分数表示式

$$x = [a_0, a_1, a_2, \dots, a_n], \quad n \geq 1, a_n \geq 2$$

和

$$x = [a_0, a_1, a_2, \dots, a_n - 1, 1], \quad n \geq 1, a_n \geq 2.$$

例 1 求 $x = 7700/2145$ 的有限简单连分数及它的各个渐近分数.

解 根据简单连分数的构造, 我们有

- (i) $a_0 = [7700/2145] = 3, \quad x_0 = x - a_0 = 1265/2145.$
- (ii) $a_1 = [2145/1265] = 1, \quad x_1 = 1/x_0 - a_1 = 880/1265.$
- (iii) $a_2 = [1265/880] = 1, \quad x_2 = 1/x_1 - a_2 = 385/880.$
- (iv) $a_3 = [880/385] = 2, \quad x_3 = 1/x_2 - a_3 = 110/385.$
- (v) $a_4 = [385/110] = 3, \quad x_4 = 1/x_3 - a_4 = 55/110.$
- (vi) $a_5 = [110/55] = 2, \quad x_5 = 1/x_5 - a_5 = 0.$

因此, $7700/2145 = [3, 1, 1, 2, 3, 2] = [3, 1, 1, 2, 3, 1, 1].$

i	a_i	x_i	P_i	Q_i	i	a_i	x_i	P_i	Q_i
0	3	1265/2145	3	1	3	2	110/385	18	5
1	1	880/1265	4	1	4	3	55/110	61	17
2	1	385/880	7	2	5	2	0	140	39

设 $p = 107$, $q = 47$.

i) 求 $\frac{p}{q}$ 的连分数展开式.

ii) 求 $\frac{p}{q}$ 的所有渐进分

数.

解 设 $u_{-2} = p = 107$, $u_{-1} = q = 47$. 我们作广义欧里得除法

$$(i) \quad 107 = 2 \cdot 47 + 13, \quad 0 < 13 = x_0 \cdot 47 < 47.$$

$$(ii) \quad 47 = 3 \cdot 13 + 8, \quad 0 < 8 = x_1 \cdot 13 < 13.$$

$$(iii) \quad 13 = 1 \cdot 8 + 5, \quad 0 < 5 = x_2 \cdot 8 < 8.$$

$$(iv) \quad 8 = 1 \cdot 5 + 3, \quad 0 < 3 = x_3 \cdot 5 < 5.$$

$$(v) \quad 5 = 1 \cdot 3 + 2, \quad 0 < 2 = x_4 \cdot 3 < 3.$$

$$(vi) \quad 3 = 1 \cdot 2 + 1, \quad 0 < 1 = x_5 \cdot 2 < 2.$$

$$(vii) \quad 2 = 2 \cdot 1 + 0, \quad 0 = x_6 \cdot 1 < 1.$$

i) 根据简单连分数的构造, 我们有

$$(i) \ a_0 = [107/47] = 2, \quad x_0 = x - a_0 = 13/47.$$

$$(ii) \ a_1 = [47/13] = 3, \quad x_1 = 1/x_0 - a_1 = 8/13.$$

$$(iii) \ a_2 = [13/8] = 1, \quad x_2 = 1/x_1 - a_2 = 5/8.$$

$$(iv) \ a_3 = [8/5] = 1, \quad x_3 = 1/x_2 - a_3 = 3/5.$$

$$(v) \ a_4 = [5/3] = 1, \quad x_4 = 1/x_3 - a_4 = 2/3.$$

$$(vi) \ a_5 = [3/2] = 1, \quad x_5 = 1/x_4 - a_5 = 1/2.$$

$$(vi) \ a_5 = [2/1] = 2, \quad x_6 = 1/x_5 - a_6 = 0.$$

因此, $\frac{p}{q} = [2, 3, 1, 1, 1, 1, 2]$.

ii)

i	a_i	x_i	P_i	Q_i	i	a_i	x_i	P_i	Q_i
-2			0	1	3	1	3/5	16	7
-1			1	0	4	1	2/3	25	11
0	2	13/47	2	1	5	1	1/2	41	18
1	3	8/13	7	3	6	2	0	107	47
2	1	5/8	9	4					

$$\frac{P_0}{Q_0} = 2, \quad \frac{P_1}{Q_1} = \frac{7}{3}, \quad \frac{P_2}{Q_2} = \frac{9}{4}, \quad \frac{P_3}{Q_3} = \frac{16}{7}, \quad \frac{P_4}{Q_4} = \frac{25}{11}, \quad \frac{P_5}{Q_5} = \frac{41}{18}, \quad \frac{P_6}{Q_6} = \frac{107}{47}.$$

例 2 求 $\alpha = (\sqrt{5} + 1)/2$ 的有限简单连分数及它的各个渐近分数.

$$(\sqrt{5} + 1)/2 = 1 + (\sqrt{5} - 1)/2 = 1 + \frac{1}{(\sqrt{5} + 1)/2}$$

$$= 1 + \frac{1}{1 + \frac{1}{(\sqrt{5} + 1)/2}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{(\sqrt{5} + 1)/2}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{(\sqrt{5} + 1)/2}}}}.$$

i	a_i	x_i	P_i	Q_i	i	a_i	x_i	P_i	Q_i
0	1	$(\sqrt{5} - 1)/2$	1	1	10	1	$(\sqrt{5} - 1)/2$	144	89
1	1	$(\sqrt{5} - 1)/2$	2	1	11	1	$(\sqrt{5} - 1)/2$	233	144
2	1	$(\sqrt{5} - 1)/2$	3	2	12	1	$(\sqrt{5} - 1)/2$	377	233
3	1	$(\sqrt{5} - 1)/2$	5	3	13	1	$(\sqrt{5} - 1)/2$	610	377
4	1	$(\sqrt{5} - 1)/2$	8	5	14	1	$(\sqrt{5} - 1)/2$	987	610
5	1	$(\sqrt{5} - 1)/2$	13	8	15	1	$(\sqrt{5} - 1)/2$	1597	987
6	1	$(\sqrt{5} - 1)/2$	21	13	16	1	$(\sqrt{5} - 1)/2$	2584	1597
7	1	$(\sqrt{5} - 1)/2$	34	21	17	1	$(\sqrt{5} - 1)/2$	4181	2584
8	1	$(\sqrt{5} - 1)/2$	55	34	18	1	$(\sqrt{5} - 1)/2$	6765	4181
9	1	$(\sqrt{5} - 1)/2$	89	55	19	1	$(\sqrt{5} - 1)/2$	10946	6765

定理 3 无限简单连分数 $[a_0, a_1, a_2, \dots]$, 也就是存在一个实数 θ , 使得 $\lim_{n \rightarrow +\infty} [a_0, a_1, a_2, \dots, a_n] = \theta$.

证 对 $n \geq 0$, 记 $\theta_n = [a_0, a_1, a_2, \dots, a_n]$. θ_n 是有 分数. 根据 §7.1 定 1, 我们有 $\theta_1 > \theta_3 > \dots > \theta_{2n-1} > \dots > \theta_0$, 以及 $\theta_0 < \theta_2 < \dots < \theta_{2n} < \dots < \theta_1$.

一方面, $\{\theta_{2n-1}\}_{n \geq 1}$ 是单调递减有下界 θ_0 的有 数列. 从而存在极限 $\lim_{n \rightarrow +\infty} \theta_{2n-1} = \theta'$.

另一方面, $\{\theta_{2n}\}_{n \geq 0}$ 是单调递增有上界 θ_1 的有 数列. 从而存在极限 $\lim_{n \rightarrow +\infty} \theta_{2n} = \theta''$.

因此, $\theta_0 < \theta_2 < \dots < \theta_{2n} < \dots < \theta' \leq \theta'' < \dots < \theta_{2n-1} < \dots < \theta_1$.

但根据 §7.1 定 2, 对任意 $n \geq 1$, 我们有 $|\theta'' - \theta'| \leq |\theta_n - \theta_{n-1}| = \frac{1}{Q_{n-1}Q_n}$. 因此, $\theta' = \theta'' = \theta$.

定理 4 设实数 $\theta > 1$ 的渐近分数为 $\frac{P_n}{Q_n}$. 则对任意 $n \geq 1$,

$$|P_n^2 - \theta^2 Q_n^2| < 2\theta.$$

证 从定 3 之证明, 我们有 θ 介于两渐近分数 $\frac{P_n}{Q_n}$ 和 $\frac{P_{n+1}}{Q_{n+1}}$.

根据 §7.1 定 2,

$$|P_n^2 - \theta^2 Q_n^2| = Q_n^2 \left| \theta - \frac{P_n}{Q_n} \right| \left| \theta + \frac{P_n}{Q_n} \right| < Q_n^2 \frac{1}{Q_n Q_{n+1}} \left(\theta + \left(\theta + \frac{1}{Q_n Q_{n+1}} \right) \right).$$

但

$$2\theta \left(\frac{Q_n}{Q_{n+1}} + \frac{1}{2\theta Q_{n+1}^2} \right) - 2\theta < 2\theta \frac{Q_n + 1}{Q_{n+1}} - 2\theta \leq 2\theta \frac{Q_{n+1}}{Q_{n+1}} - 2\theta = 0,$$

故定 成立. 证毕.

设实数 θ 是无限简单连分数 $[a_0, a_1, a_2, \dots]$. 如果存在整数 $m \geq 0$, 使得对于该整数 m , 存在整数 $k \geq 1$, 使得对于所有 $n \geq m$, 有

$$a_{n+k} = a_n, \quad (1)$$

那么, θ 叫做 **循环简单连分数**, 简称 **循环连分数**. 这时 θ 可写成

$$\theta = [a_0, a_1, \dots, a_{m-1}, \overline{a_m, \dots, a_{m+k-1}}].$$

例 1 $\sqrt{2} = [1, 2, 2, \dots] = [1, \overline{2}]$ 是循环连分数.

如果 $m = 0$, 使得 (1) 式成立, 则 θ 叫做 **纯循环简单连分数**, 简称 **纯循环连分数**.

例 2 $\frac{\sqrt{5}+1}{2} = [1, 1, 1, \dots] = [\overline{1}]$ 是纯循环连分数.

定理 1 设 θ 是循环简单连分数, 则 θ 是二次无理数.

证 设 $\theta = [\overline{a_0, \dots, a_{k-1}}]$ 是纯循环连分数, 则根据 §7.1 定理 2,

$$\theta = [a_0, a_1, \dots, a_{k-1}, \theta] = \frac{P_k}{Q_k} = \frac{\theta P_{k-1} + P_{k-2}}{\theta Q_{k-1} + Q_{k-2}},$$

其中 $P_{k-2}, P_{k-1}, Q_{k-2}, Q_{k-1}$ 是整数. 从而,

$$Q_{k-1}\theta^2 + (-P_{k-1} + Q_{k-2})\theta - P_{k-2} = 0.$$

这说明 θ 是二次无理数.

如果 $\theta = [a_0, a_1, \dots, a_{m-1}, \overline{a_m, \dots, a_{m+k-1}}]$ 是循环连分数, 则 $\theta_0 = [\overline{a_m, \dots, a_{m+k-1}}]$ 是纯循环连分数. 根据 §7.1 定理 2,

$$\theta = [a_0, a_1, \dots, a_{k-1}, \theta_0] = \frac{P_k}{Q_k} = \frac{\theta_0 P_{k-1} + P_{k-2}}{\theta_0 Q_{k-1} + Q_{k-2}},$$

其中 $P_{k-2}, P_{k-1}, Q_{k-2}, Q_{k-1}$ 是整数. 因此, θ 是二次无理数.

定理 2 设 θ 是二次无理数，则 θ 是循环简单连分数.

前面，我们考虑了用有理数来逼近一个实数. 现在，我们对逼近的效果给以定性描述.

定义 1 设 θ 是一个实数. 有理数 $\frac{p}{q}$, ($q > 0$) 称为 θ 的最佳逼近, 如果对所有的有理数 $\frac{p'}{q'}$, $0 < q' \leq q$, 有

$$\left| \theta - \frac{p}{q} \right| < \left| \theta - \frac{p'}{q'} \right|. \quad (1)$$

这说明, 在分母 $q' \leq q$ 的所有有理数 $\frac{p'}{q'}$ 中, $\frac{p}{q}$ 是离 θ 最近的有理数 $\frac{p}{q}$.

在说明 θ 的连分数是 θ 的最佳逼近之前, 我们先给出如下定

:

定理 1 设 θ 是无理实数. 设 $\frac{P_n}{Q_n}$, ($n \geq 1$) 是 θ 的第 n 个渐近分数时. 如果整数 p, q , ($q > 0$) 使得

$$|q\theta - p| < |Q_n\theta - P_n| \quad (2)$$

则 $q \geq Q_{n+1}$.

定理 2 实数 θ 的渐近分数是 θ 的最佳逼近. 即当 $\frac{P_n}{Q_n}$, ($n \geq 1$), 是 θ 的第 n 个渐近分数时, 对所有的有理数 $\frac{p}{q} \neq \frac{P_n}{Q_n}$, $0 < q \leq Q_n$, 有

$$\left| \theta - \frac{P_n}{Q_n} \right| < \left| \theta - \frac{p}{q} \right|. \quad (4)$$

第八章 群

群的基本概念

子群的基本概念

常见的群

已学知识的抽象化

群同态、同构

群同态分解定

定义 1 设 S 是一个非空集合. 那么 $S \times S$ 到 S 的映射叫做 S 的 **结合法** 或 **运算**; 对于这个映射, 元素对 (a, b) 的像叫做 a 与 b 的 **乘积**, 记成 $a \otimes b$ 或 $a \cdot b$ 或 $a * b$ 等, 简记 ab , 叫做 **乘法**.

也常叫做 **加法**, (a, b) 的像叫做 a 与 b 的 **和**, 记成 $a \oplus b$ 或 $a + b$.

始终设 S 是一个具有结合法的非空集合.

如果任意 a, b, c , 都有 $(ab)c = a(bc)$, 则称该结合法满足 **结合律**.

定义 2 如果 S 满足结合律, 那么 S 叫做 S 的 **半群**.

如果对任意 a, b , 都有 $ba = ab$, 则称该结合法满足 **交换律**.

如果 S 中有一个元素 e 使得 $ea = ae = a$ 对 S 中所有元素 a 都成立, 则称该元素 e 为 S 中的 **单位元**.

当 S 的结合法写作加法时, 这个 e 叫做 S 中的 **零元**, 通常记作 0 .

性质 1 : S 中的单位元 e 是惟一的.

证 设 e 和 e' 都是单位元. 则 $e' = ee' = e$. 因此, 单位元是惟一的.
设 a 是 S 中元素. 如果 S 存在一个元素 a' 使得 $aa' = a'a = e$, 则称该元素 a 为 S 中的 **可逆元**, a' 称为 a 的 **逆元**, 通常记作 a^{-1} .
当结合法叫做加法时, 这个 a' 叫做元素 a 的负元, 通常记作 $-a$.

性质 2 : 设 S 是一个有单位元的半群. 则对 S 中任意可逆元 a , 其逆元 a' 是惟一的.

证 设 a' 和 a'' 都是 a 的逆元, 即 $aa' = a'a = e$, $aa'' = a''a = e$.
分别根据 a' 和 a'' 为 a 的逆元及结合律, 得到

$$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''.$$

因此, a 的逆元 a' 是惟一的.

定义 3 设 G 是一个具有结合法的非空集合. 如果满足:

- (i) **结合律**, 即对任意的 $a, b, c \in G$, 都有 $(ab)c = a(bc)$;
 - (ii) **单位元**, 即存在一个元素 $e \in G$, 使得对任意的 $a \in G$, 都有 $ae = ea = a$;
 - (iii) **可逆性**, 即对任意的 $a \in G$, 都存在 $a' \in G$, 使得 $aa' = a'a = e$,
- 那么, G 叫做一个 **群**.

特别地, 当 G 的结合法写作乘法时, G 叫做 **乘群**;

当 G 的结合法写作加法时, G 叫做 **加群**.

群 G 的元素个数叫做群 G 的 **阶**, 记为 $|G|$.

当 $|G|$ 为有限数时, G 叫做 **有限群**, 否则, G 叫做 **无限群**.

如果群 G 中的结合法还满足交换律, 即对任意的 $a, b \in G$, 都有 $ab = ba$, 那么, G 叫做一个 **交换群** 或阿倍尔 (Abel) 群.

例 1 自然数集 $\mathbf{N} = \{1, 2, \dots, n, \dots\}$

对于通常意义下的加法有结合律，但没有零元和逆元；

而对于通常意义下的乘法，有结合律和单位元 $e = 1$ ，但没有可逆元.

$$2^{-1} = ?$$

例 2 整数集 $\mathbf{Z} = \{\dots, -n, \dots, -2, -1, 0, 1, 2, \dots, n, \dots\}$

对于通常意义下的加法，有结合律，交换律和零元 0，并且每个元素 a 有负元 $-a$. 因此， $\mathbf{Z}$ 是一个交换加群.

非零整数集 $\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$ 对于通常意义下的乘法，有结合律，交换律和单位 1，但不是每个元素 a 都有逆元，因此 $\mathbf{Z}^*$ 不是一个群.

例 3 有 数集 $\mathbf{Q}$ 对于加法有结合律, 交换律和零元 0, 并且每个元素 a 有负元 $-a$, 因此, $\mathbf{Q}$ 是交换加群.

非零有 数集 $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$ 对于乘法有结合律, 交换律和单位 1, 并且每个元素 a 都有逆元 $a^{-1} = \frac{1}{a}$, 因此, $\mathbf{Q}^*$ 是交换乘群.

类似地, 实数集 $\mathbf{R}$ 和复数集 $\mathbf{C}$ 都是交换加群. 而非零实数集 $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ 和非零复数集 $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$ 都是交换乘群.

例 4 设 D 是非平方整数. 则集合 $\mathbf{Z}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbf{Z}\}$

对于加法运算: $(a + b\sqrt{D}) \oplus (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$

构成一个交换加群.

但对于乘法运算 $(a + b\sqrt{D}) \otimes (c + d\sqrt{D}) = (ac + bdD) + (bc + ad)\sqrt{D}$ 不构成一个乘群.

例 5 设 n 是正整数. $\mathbf{Z}/n\mathbf{Z} = \{0, 1, 2, \dots, n-1\}$.

证明: 集合 $\mathbf{Z}/n\mathbf{Z}$ 对于加法: $a \oplus b = (a + b \pmod{n})$

构成一个交换加群, 其中 $a \pmod{n}$ 是整数 a 模 n 的最小非负剩余.

零元是 0, a 的负元是 $n - a$. $n = 6$

$a \setminus x$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

例 6 设 p 是一个素数, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. 设 $\mathbf{F}_p^* = \mathbf{F}_p \setminus \{0\}$.

证明: 集合 $\mathbf{F}_p^*$ 对于乘法: $a \otimes b = (a \cdot b \pmod{p})$

构成一个交换乘群.

单位元是 1, a 的逆元是 $(a^{-1} \pmod{p})$. $p = 7$

$a \setminus x$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

例 7 设 n 是一个合数. 证明: 集合 $\mathbf{Z}/n\mathbf{Z} \setminus \{0\}$ 对于乘法:
 $a \otimes b = (a \cdot b \pmod{n})$ 不构成一个乘群.

单位元是 1. 但 n 的真因数 d 没有逆元, 即对任意的 $d' \in \mathbf{Z}/n\mathbf{Z} \setminus \{0\}$, 都有 $d \otimes d' = (d \cdot d' \pmod{n}) \neq 1$. $n = 6$

$a \setminus x$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

例 8 设 n 是一个合数. 设 $(\mathbf{Z}/n\mathbf{Z})^* = \{a \mid a \in \mathbf{Z}/n\mathbf{Z}, (a, n) = 1\}$.

证明: 集合 $(\mathbf{Z}/n\mathbf{Z})^*$ 对于乘法: $a \otimes b = (a \cdot b \pmod{n})$

构成一个交换乘群.

单位元是 1, a 的逆元是 $(a^{-1} \pmod{n})$. $n = 15$

$a \setminus x$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

例 9. 设有元素在数域 $\mathbf{K}$ 中的全体 n 级矩阵组成的集合

$$M_n(\mathbf{K}) = \{(a_{ij})_{1 \leq i \leq n, 1 \leq j \leq n} \mid a_{ij} \in \mathbf{K}, 1 \leq i \leq n, 1 \leq j \leq n\}.$$

设 $A = (a_{ij}), B = (b_{ij}), C = (c_{ij}), \in M_n(\mathbf{K})$. 我们定义

加法:

$$A + B = C, \quad \text{其中 } c_{ij} = a_{ij} + b_{ij}, \quad 1 \leq i \leq n, 1 \leq j \leq n.$$

则 $M_n(\mathbf{K})$ 对于加法构成一个交换群.

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

$$\text{零元 } \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \text{ 负元 } \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$$

例 9' 设 $A = (a_{ij}), B = (b_{ij}), C = (c_{ij}), \in M_n(\mathbf{K})$. 定义乘法:

$$A \cdot B = C, \quad \text{其中 } c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}, \quad 1 \leq i \leq n, 1 \leq j \leq n.$$

则 $M_n(\mathbf{K}) \setminus \{0\}$ 对于乘法不构成一个群.

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

单位元 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, 但 $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 \cdot 0 + 1 \cdot 0 & 0 \cdot 1 + 1 \cdot 0 \\ 0 \cdot 0 + 0 \cdot 0 & 0 \cdot 1 + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

但可逆矩阵 A (即存在 A' 使得 $AA' = A'A = I_n$) 对于矩阵的乘法成一个群, 记为 $GL_n(P)$, 称为 n 级 **一般线性群**;

$GL_n(P)$ 中全体行列式为 1 的矩阵对于矩阵乘法也成一个群, 这个群记为 $SL_n(p)$, 称为 **特殊线性群**.

例 10 设 S 是非空集合. G 是 S 到自身的所有一一对应的映射 f 组成的集合. 对于 $f, g \in G$, 定义 f 和 g 的复合映射 $g \circ f$ 为: 对于任意 $x \in S$, $g \circ f(x) = g(f(x))$.

则 G 对于映射的复合运算, 构成一个群, 叫做 **对 群**.

恒等映射是单位元. G 中的元素叫做 S 的一个 **置换**.

当 S 是 n 元有限集时, G 叫做 n 元 **对 群**, 记作 S_n .

多个元素的运算 设 $a_1, a_2, \dots, a_{n-1}, a_n$ 是群 G 中的 n 个元素.
通常归纳地定义这 n 个元素的乘积为

$$a_1 a_2 \cdots a_{n-1} a_n = (a_1 a_2 \cdots a_{n-1}) a_n.$$

当 G 的结合法叫做加法时, 通常归纳地定义这 n 个元素的和为

$$a_1 + a_2 + \cdots + a_{n-1} + a_n = (a_1 + a_2 + \cdots + a_{n-1}) + a_n.$$

性质 3 : 设 $a_1, \dots, a_n$ 是群 G 中的任意 $n \geq 2$ 个元素. 则对任意的 $1 \leq i_1 < \dots < i_k < n$, 有

$$(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = a_1 a_2 \cdots a_{n-1} a_n.$$

性质 4 : 设 $a_1, a_2, \dots, a_{n-1}, a_n$ 是交换群 G 中的任意 $n \geq 2$ 个元素. 则对 $1, 2, \dots, n$ 的任一排列 $i_1, i_2, \dots, i_n$, 有

$$a_{i_1} a_{i_2} \cdots a_{i_n} = a_1 a_2 \cdots a_n.$$

设 n 是正整数. 如果 $a_1 = a_2 = \cdots = a_n = a$, 则记 $a_1 a_2 \cdots a_n = a^n$, 称之为 a 的 n 次幂. 特别地, 定义 $a^0 = e$ 为单位元, $a^{-n} = (a^{-1})^n$ 为逆元 a^{-1} 的 n 次幂.

性质 5 : 设 $a \in G$, 则对任意 $m, n \in \mathbf{Z}$,

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

定理 1 设 $G \neq \emptyset$ 有结合法. 如果 G 是一个群, 则方程 $ax = b, \quad ya = b$ 在 G 中有解. 反过来, 如果上述方程在 G 中有解, 并且结合法满足结合律, 则 G 是一个群.

定义 4 设 H 是群 G 的一个子集合. 如果对于群 G 的结合法, H 成为一个群, 那么 H 叫做群 G 的 **子群**, 记作 $H \leq G$.

$H = \{e\}$ 和 $H = G$ 都是群 G 的子群, 叫做群 G 的 **平凡子群**. 群 G 的子群 H 叫做群 G 的 **真子群**, 如果 H 不是群 G 的平凡子群.

例 11 设 n 是一个正整数. 则 $n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\}$ 是 $\mathbf{Z}$ 的子群.

例 11' 例 10' 中 H_1, H_2, H_3, H_4 都是 S_3 的真子群.

定理 2 设 H 是群 G 的一个非空子集合. 则 H 是群 G 的子群的充要条件是: 对任意的 $a, b \in H$, 有 $ab^{-1} \in H$.

证 必要性是显然的. 我们来证充分性.

因为 G 非空, 所以 G 中有元素 a . 根据假设, 我们有 $e = aa^{-1} \in H$. 因此, H 中有单位元. 对于 $e \in H$ 及任意 a , 再应用假设, 我们有 $a^{-1} = ea^{-1} \in H$, 即 H 中每个元素 a 在 H 中有逆元. 因此, H 是群 G 的子群. 证毕.

定理 3 设 G 是一个群, $\{H_i\}_{i \in I}$ 是 G 的一族子群. 则

$$\bigcap_{i \in I} H_i = H_1 \cap H_2 \cap \cdots \cap H_n \cap \cdots$$

是 G 的一个子群.

证 对任意的 $a, b \in \bigcap_{i \in I} H_i$, 有

$$a, b \in H_i, \quad i \in I.$$

因为 H_i 是 G 的子群, 根据定 2, 我们有 $ab^{-1} \in H_i, i \in I$. 进而,

$$ab^{-1} \in \bigcap_{i \in I} H_i.$$

根据定 2, $\bigcap_{i \in I} H_i$ 是 G 的一个子群.

定义 5 设 G 是一个群, X 是 G 的子集. 设 $\{H_i\}_{i \in I}$ 是 G 的包含 X 的所有子群. 则

$$\bigcap_{i \in I} H_i$$

叫做 G 的由 X **生成的子群**. 记为 $\langle X \rangle$.

X 的元素称为子群 $\langle X \rangle$ 的 **生成元**.

如果 $X = \{a_1, \dots, a_n\}$, 则记 $\langle X \rangle$ 为 $\langle a_1, \dots, a_n \rangle$.

如果 $G = \langle a_1, \dots, a_n \rangle$, 则称 G 为 **有限生成的**.

特别地, 如果 $G = \langle a \rangle$, 则称 G 为 a 生成的 **循环群**.

定理 4 设 G 是一个群, X 是 G 的非空子集. 则由 X 生成的子群为

$$\langle X \rangle = \{a_1^{n_1} \cdots a_t^{n_t} \mid t \in \mathbf{N}, a_i \in G, n_i \in \mathbf{Z}, 1 \leq i \leq t\}.$$

特别, 对任意的 $a \in G$, 有

$$\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}.$$

例 12 设 $G = \langle g \rangle = \{g^r \mid g^r \neq 1, 1 \leq r < n, g^n = 1\}$. G 是 n 阶循环群. 则 $\langle g^d \rangle = \{g^{dk} \mid k \in \mathbf{Z}\}$ 是 G 的子群.

定义 1 设 G, G' 是两个群, f 是 G 到 G' 的一个映射. 如果对任意的 $a, b \in G$, 都有 $f(ab) = f(a)f(b)$,

那么, f 叫做 G 到 G' 的一个 **同态**.

由所有 G 到 G' 的同态组成的集合记作 $\text{Hom}(G, G')$.

如果 f 是一对一的, 则称 f 为 **单同态**; 如果 f 是满的, 则称 f 为 **满同态**; 如果 f 是一一对应的, 则称 f 为 **同构**.

当 $G = G'$ 时, 同态 f 叫做 **自同态**, 同构 f 叫做 **自同构**.

定义 2 设 G, G' 是两个群. 我们称 G 与 G' **同构**, 如果存在一个 G 到 G' 的同构. 记作 $G \cong G'$.

定理 1 设 f 是群 G 到群 G' 的一个同态. 则

(i) $f(e) = e'$, (ii) 对任意 $a \in G$, $f(a^{-1}) = f(a)^{-1}$.

(iii) $\ker f = \{a \mid a \in G, f(a) = e'\}$ 是 G 的子群,

且 f 是单同态的充要条件是 $\ker f = \{e\}$.

定理 2 设 f 是群 G 到群 G' 的一个同态. 则

(iv) $f(G) = \{f(a) \mid a \in G\}$ 是 G' 的子群,

且 f 是满同态的充要条件是 $f(G) = G'$.

(v) 设 H' 是群 G' 的子群, 则集合 $f^{-1}(H') = \{a \in G \mid f(a) \in H'\}$ 是 G 的子群.

$\ker f$ 叫做同态 f 的 **核子群**, $f(G)$ 叫做 **象子群**.

例 1 加群 $\mathbf{Z}$ 到乘群 $G = \langle g \rangle = \{g^n \mid n \in \mathbf{Z}\}$ 的映射 $f : n \mapsto g^n$ 是 $\mathbf{Z}$ 到 $\langle g \rangle$ 的一个同态.

因为对任意的 $a, b \in \mathbf{Z}$, 有 $f(a+b) = g^{a+b} = g^a g^b = f(a)f(b)$.

例 2 加群 $\mathbf{Z}$ 到乘群 $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ 的映射 $f : a \longmapsto e^a$ 是 $\mathbf{R}$ 到 $\mathbf{R}^*$ 的一个同态.

例 3 加群 $\mathbf{Z}$ 到加群 $\mathbf{Z}/n\mathbf{Z}$ 的映射 $f : n \longmapsto g^n$ 是一个同态.

例 4 加群 $\mathbf{Z}$ 到乘群 $G = \{\theta^k | \theta = e^{\frac{2\pi i}{n}}, k \in \mathbf{Z}\}$ 的映射 $f : k \longmapsto \theta^k$ 是一个同态.

例 5 加群 $\mathbf{Z}/n\mathbf{Z}$ 到乘群 $G = \{\theta^k | \theta = e^{\frac{2\pi i}{n}}, k = 0, 1, \dots, n-1\}$ 的映射 $f : k + n\mathbf{Z} \longmapsto \theta^k$ 是一个同构.

例 6 设 a 是群 G 的一个元. 那么映射

$$f : b \longmapsto aba^{-1}$$

是 G 自同态. 事实上,

$$f(bc) = a(bc)a^{-1} = (aba^{-1})(aca^{-1}) = f(a)f(b).$$

定义 1 设 H 是群 G 的子群, a 是 G 中任意元. 那么集合 $aH = \{ah | h \in H\}$ (对应地 $Ha = \{ha | h \in H\}$) 分别叫做 G 中 H 的左(右)**陪集**. aH (对应地 Ha) 中的元素叫做 aH (对应地 Ha) 的代表元. 如果 $aH = Ha$, aH 叫做 G 中 H 的**陪集**

例 1 设 $n > 1$ 是整数. 则 $H = n\mathbf{Z}$ 是 $\mathbf{Z}$ 的子群, 子集

$$a + n\mathbf{Z} = \{a + nk \mid k \in \mathbf{Z}\}$$

就是 $n\mathbf{Z}$ 的陪集. 这个陪集就是模 n 的剩余类.

定理 1 设 H 是群 G 的子群, 则

(i) 对任意 $a \in G$, 有 $aH = \{c \mid c \in G, c^{-1}a \in H\}$ (对应地 $Ha = \{c \mid c \in G, ac^{-1} \in H\}$);

(ii) 对任意 $a, b \in G$, $aH = bH$ 的充要条件 $b^{-1}a \in H$ (对应地 $Ha = Hb$ 的充要条件 $ab^{-1} \in H$);

(iii) 对任意 $a, b \in G$, $aH \cap bH = \emptyset$ 的充要条件 $b^{-1}a \notin H$ (对应地 $Ha \cap Hb = \emptyset$ 的充要条件 $ab^{-1} \notin H$);

(iv) 对任意 $a \in H$, 有 $aH = H = Ha$.

推论 设 H 是群 G 的子群. 则群 G 可以表示为不交的左 (对应右) 陪集的并集.

定义 2 设 H 是群 G 的子群. 则 H 在 G 中不同左 (对应右) 陪集组成的新集合 $\{aH \mid a \in G\}$, 叫做 H 在 G 中的 **商集**, 记作 G/H . G/H 中不同左 (对应右) 陪集的个数叫做 H 在 G 中的 **指标**, 记为 $[G : H]$.

定理 2 设 $H \leq G$, 则 $|G| = [G : H]|H|$.

更进一步, $K, H \leq G, K \leq H$, 则 $[G : K] = [G : H][H : K]$.
如果其中两个指标是有限的, 则第三个指标也是有限的.

推论 (Lagrange). 设 H 是有限群 G 的子群, 则子群 H 阶是 $|G|$ 的因数.

定理 6 设 N 是群 G 的子群, 则如下条件是等价的:

- (i) 对任意 $a \in G$, 有 $aN = Na$;
- (ii) 对任意 $a \in G$, 有 $aNa^{-1} = N$.
- (iii) 对任意 $a \in G$, 有 $aNa^{-1} \subset N$, 其中 $aNa^{-1} = \{ana^{-1} | n \in N\}$.

证 易知, (i) 蕴含 (ii) 及 (ii) 蕴含 (iii) 是显然的. 现从 (iii) 推出 (i). 对任意 $a \in G$, $n \in N$, 因为 $ana^{-1} \in aNa^{-1} \subset N$, 所以 $ana^{-1} = n'$, $n' \in N$. 进而, $an = n'a \in Na$ 及 $aN \subset Na$. 特别, 也有 $a^{-1}N \subset Na^{-1}$ 或 $Na \subset aN$. 故 $aN = Na$. 定理成立. 证毕.

定义 3 设 N 是群 G 的子群. 我们称 N 为群 G 的 **正规子群**, 如果它满足定理 6 的条件. 记作 $N \triangleleft G$.

定理 7 设 $N \triangleleft G$, $G/N = \{aN \mid a \in G\}$.

则对于结合法 $(aN)(bN) = (ab)N$, G/N 构成一个群.

证 首先, 要证明结合法的定义不依赖于陪集的代表元的选择. 即要证明: $aN = a'N$, $bN = b'N$ 时, $(ab)N = (a'b')N$. 事实上, 根据定理 6, 我们有

$$(ab)N = a(bN) = a(b'N) = a(Nb') = (aN)b' = (a'N)b' = (a'b')N.$$

其次, $eN = N$ 是单位元. 事实上, 对任意 $a \in G$, 有

$$(aN)(eN) = (ae)N = aN, \quad (eN)(aN) = (ea)N = aN.$$

最后, aN 的逆元是 $a^{-1}N$. 事实上,

$$(aN)(a^{-1}N) = (aa^{-1})N = eN, \quad (a^{-1}N)(aN) = (a^{-1}a)N = eN.$$

因此, G/N 构成一个群. 证毕.

定 7 中的群叫做群 G 对于正规子群 H 的 **商群**. 如果群 G 的运算写作加法, 则 G/N 中的运算写作 $(a+N) + (b+N) = (a+b) + N$.

定理 8 设 f 是群 G 到群 G' 的同态, 则 f 的核 $\ker(f)$ 是 G 的正规子群. 反过来, 如果 N 是群 G 的正规子群, 则 G 到 G/N 的映射 $s : a \mapsto aN$ 是核为 N 的同态.

证 对任意 $a \in G, b \in \ker f$, 我们有 $f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)e'f(a)^{-1} = e'$. 这说明 $aba^{-1} \in \ker f$. 根据定理 6, $\ker(f)$ 是 G 的正规子群.

反过来, 设 N 是群 G 的正规子群, 则 G 到 G/N 的映射 s 满足:

$$s(ab) = (ab)N = (aN)(bN) = s(a)s(b),$$

同时, $s(a) = N$ 的充分必要条件是 $a \in N$. 因此, s 是核为 N 的同态. 证毕.

映射 $s : G \longrightarrow G/N$ 称为 G 到 G/N **自然同态**.

定理 9 设 $f \in \text{Hom}(G, G')$, 则存在惟一的 $G/\ker(f)$ 到 $f(G)$ 的同构 $\bar{f}: a\ker(f) \mapsto f(a)$ 使得 $f = i \circ \bar{f} \circ s$, 其中 s 是 G 到 $G/\ker(f)$ 的自然同态, i 是 $f(G)$ 到 G' 的恒等同态. 即有如下的交换图:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ s \downarrow & & \uparrow i \\ G/\ker(f) & \xrightarrow{\bar{f}} & f(G) \end{array}$$

证 因为 $\ker(f) \triangleleft G$, 所以存在商群 $G/\ker(f)$.

要证明: $\bar{f}: a\ker(f) \mapsto f(a)$ 是 $G/\ker(f)$ 到像子群 $f(G)$ 的同构.

首先, $\bar{f}$ 是 $G/\ker(f)$ 到 $f(G)$ 的同态. 事实上, 对任意的 $a\ker(f), b\ker(f) \in G/\ker(f)$,

$$\bar{f}((a\ker(f))(b\ker(f))) = \bar{f}((ab)\ker(f)) = f(ab) = f(a)f(b) = \bar{f}(a\ker(f))\bar{f}(b\ker(f)).$$

其次, $\bar{f}$ 是一一对一. 事实上, 对任意 $a \ker(f) \in \ker(\bar{f})$, 有 $\bar{f}(a \ker(f)) = f(a) = e'$. 由此, $a \in \ker(f)$ 以及 $a \ker(f) = \ker(f)$.

最后, $\bar{f}$ 是满同态. 事实上, 对任意 $c \in f(G)$, 存在 $a \in G$ 使得 $f(a) = c$. 从而, $\bar{f}(a \ker(f)) = f(a) = c$. 即 $a \ker(f)$ 是 c 的像源.

因此, $\bar{f}$ 是同构, 并且有 $f = i \circ \bar{f} \circ s$. 事实上, 对任意 $a \in G$, 有

$$i \circ \bar{f} \circ s(a) = i(\bar{f}(s(a))) = i(\bar{f}(a \ker(f))) = i(f(a)) = f(a).$$

假如还有同构 $g : G / \ker(f) \longrightarrow f(G)$ 使得 $f = i \circ g \circ s$, 则对任意 $a \ker(f) \in G / \ker(f)$, 我们有

$$g(a \ker(f)) = i(g(s(a))) = (i \circ g \circ s)(a) = f(a) = \bar{f}(a \ker(f)).$$

因此, $g = \bar{f}$. 证毕.

第九章 群的结构

定理 1 加群 $\mathbf{Z}$ 的每个子群 H 是循环群. 且有 $H = \{0\}$ 或 $H = \langle m \rangle = m\mathbf{Z}$, 其中 m 是 H 中的最小正整数. 如果 $H \neq \langle 0 \rangle$, 则 H 是无限的.

证 如果 $H = \{0\}$, 结论成立. 如果 $H \neq \{0\}$, 则存在非零整数 $a \in H$. 因为 H 是子群, 所以 $-a \in H$. 这说明 H 中有正整数. 设 H 中的最小正整数为 m . 则一定有 $H = \langle m \rangle = m\mathbf{Z}$.

事实上, 对任意的 $a \in H$, 根据欧里得除法, 存在整数 q, r 使得 $a = qm + r$, $0 \leq r < m$.

如果 $r \neq 0$, 则 $r = a - qm \in H$, 这与 m 的最小性矛盾.

因此, $r = 0$, $a = qm \in m\mathbf{Z}$. 故 $H \subset m\mathbf{Z}$. 但显然有 $m\mathbf{Z} \subset H$. 因此, $H = m\mathbf{Z}$. 证毕.

定理 2 每个无限循环群同构于加群 $\mathbf{Z}$. 每个阶为 m 的有限循环群同构于加群 $\mathbf{Z}/m\mathbf{Z}$.

证 设循环群 $G = \langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$. 考虑映射

$$\begin{aligned} f : \mathbf{Z} &\longrightarrow G \\ n &\longmapsto a^n \end{aligned}$$

因为 $f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$, 所以 f 是 $\mathbf{Z}$ 到 G 的同态, 而且是满的. 根据 §8.3 定理 9, 群 G 同构于 $\mathbf{Z}/\ker(f)$. 根据定理 1, $\ker(f) = \langle 0 \rangle$ 或 $\ker(f) = m\mathbf{Z}$. 前者对应于无限循环群, 后者对应于 m 阶有限循环群. 证毕.

定义 1 设 G 是一个群, $a \in G$. 则子群 $\langle a \rangle$ 的阶称为元素 a 的阶, 记为 $\text{ord}(a)$.

定理 3 设 G 是一个群, $a \in G$. 如果 a 是无限阶, 则

- (i) $a^k = e \Leftrightarrow k = 0$. (ii) 元素 a^k ($k \in \mathbf{Z}$) 两两不同.

如果 a 是有限阶 $m > 0$, 则

- (iii) m 是使得 $a^m = e$ 的最小正整数. (iv) $a^k = e \Leftrightarrow m|k$.
(v) $a^r = a^k \Leftrightarrow r \equiv k \pmod{m}$. (vi) a^k ($k \in \mathbf{Z}/m\mathbf{Z}$) 两两不同.
(vii) $\langle a \rangle = \{a, a^2, a^{m-1}, a^m = e\}$ (viii) $\text{ord}(a^d) = \frac{m}{(m, d)}$.

定理 4 循环群的子群是循环群.

定理 5 设 G 是循环群. 如果 G 是无限的, 则 G 的生成元为 a 和 a^{-1} . 如果 G 是有限阶 m , 则 a^k 是 G 的生成元当且仅当 $(k, m) = 1$.

引理 1 设 G 是有限交换群. 对任意元素 $a, b \in G$,
若 $(\text{ord}(a), \text{ord}(b)) = 1$, 则

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

引理 2 设 G 是有限交换群. 对任意元素 $a, b \in G$, 存在 $c \in G$
使得

$$\text{ord}(c) = [\text{ord}(a), \text{ord}(b)].$$

定理 6 设 G 是有限交换群, 则 G 中存在元素 $a_1, a_2, \dots, a_s$ 使
得它们各自的元素阶 $m_1, m_2, \dots, m_s$ 满足 $m_i | m_{i+1}$, $1 \leq i \leq s-1$,
并且使得

$$G = \langle a_1 \rangle \langle a_2 \rangle \cdots \langle a_s \rangle .$$

对任意的加法交换群 G . 如果 X 是 G 的非空子集, 则由 X 生成的子群是所有的线性组合

$$n_1x_1 + n_2x_2 + \cdots + n_kx_k, \quad k \in \mathbf{N}, n_i \in \mathbf{Z}, x_i \in X$$

组成的集合. 特别, 由一个元生成的循环子群 $\langle x \rangle = \{nx | n \in \mathbf{Z}\}$.

交换群 G 的一个子集 X 叫做 G 的 **基底**, 如果 X 是 G 的最小生成元, 即 (i) $G = \langle X \rangle$; (ii) 对于 X 中的任意不同的元素 $x_1, x_2, \dots, x_k$ 在 $\mathbf{Z}$ 上 **线性无关**, 即不存在不全为零的整数 $n_1, n_2, \dots, n_k$ 使得 $n_1x_1 + n_2x_2 + \cdots + n_kx_k = 0$.

线性无关在乘法运算中对应于 **乘性无关**, 即不存在不全为零的整数 $n_1, n_2, \dots, n_k$ 使得 $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k} = e$.

设 $H_1, \dots, H_k$ 是交换群 G 的 k 个子群. 我们称 $H_1 + \dots + H_k$ 是 $H_1, \dots, H_k$ 的 **直和**, 如果 $(H_1 + \dots + H_{i-1} + H_{i+1} + \dots + H_k) \cap H_i = \{0\}$, $1 \leq i \leq k$. 记作 $H_1 \oplus \dots \oplus H_k$.

写作乘法时, 我们称 $H_1 \cdots H_k$ 是 $H_1, \dots, H_k$ 的 **直积**, 如果 $(H_1 \cdots H_{i-1} H_{i+1} \cdots H_k) \cap H_i = \{e\}$, $1 \leq i \leq k$. 记作 $H_1 \otimes \dots \otimes H_k$.

定理 1 设交换群 G 有一组非空基底, 则 G 是一组循环群的直和.

定 1 中的群叫做 **自由交换群**.

定理 2 自由交换群的任意两个基底所含元素个数 同.

自由交换群 G 的基底的元素个数叫做群 G 的 **秩**.

定理 3 每个交换群 G 都是一个秩为 $|X|$ 的自由交换群的同态象子群, 其中 X 为 G 的生成元集.

定理 4 每个有限生成交换群 G 都是有限个循环群的直和, 并且有限循环群的阶 $m_1, \dots, m_s$ 满足 $m_1 | m_2, \dots, m_{s-1} | m_s$.

进一步研究对称群 S_n . 设 $S = \{1, 2, \dots, n-1, n\}$, σ 是 S 上的一个置换, 即 σ 是 S 到自身的一一对应的映射:

$$\begin{aligned}\sigma : S &\longrightarrow S \\ k &\longmapsto \sigma(k) = i_k\end{aligned}$$

因为 k 在 σ 下的象是 i_k , 所以我们将 σ 表示成

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ i_1 & i_2 & \dots & i_{n-1} & i_n \end{pmatrix}.$$

当然可写成
$$\sigma = \begin{pmatrix} n & n-1 & \dots & 2 & 1 \\ i_n & i_{n-1} & \dots & i_2 & i_1 \end{pmatrix} = \begin{pmatrix} j_1 & j_2 & \dots & j_{n-1} & j_n \\ i_{j_1} & i_{j_2} & \dots & i_{j_{n-1}} & i_{j_n} \end{pmatrix},$$

其中 $j_1, j_2, \dots, j_{n-1}, j_n$ 是 $1, 2, \dots, n-1, n$ 的一个排列.

例 1 设 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix}$. 计算 $\sigma\tau$, $\tau\sigma$, σ^{-1} .

解 $\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix}$
 $= \begin{pmatrix} 5 & 6 & 4 & 2 & 3 & 1 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix}.$

$$\tau \cdot \sigma = \begin{pmatrix} 6 & 5 & 4 & 2 & 1 & 3 \\ 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix}.$$

$$\sigma^{-1} = \begin{pmatrix} 6 & 5 & 4 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 3 & 2 & 1 \end{pmatrix}.$$

定理 1 n 元置换全体组成的集合 S_n 对置换的乘法构成一个群, 其阶是 $n!$.

证 因为一一对应的映射的乘积仍是一一对应的, 且该乘积满足结合律, 所以置换的乘法满足结合律.

又 n 元恒等置换 $e = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix}$ 是单位元.

置换 $\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ i_1 & i_2 & \dots & i_{n-1} & i_n \end{pmatrix}$ 有逆元 $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_{n-1} & i_n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix}$.

因此, S_n 对置换的乘法构成一个群.

因为 $(1, 2, \dots, n-1, n)$ 在置换 σ 下的象 $(\sigma(1), \sigma(2), \dots, \sigma(n-1), \sigma(n))$ 是 $(1, 2, \dots, n-1, n)$ 的一个排列, 这样的排列共有 $n!$ 个, 所以 S_n 的阶为 $n!$. 证毕.

如果 n 元置换 σ 使得 $\{1, 2, \dots, n-1, n\}$ 中的一部分元素 $\{i_1, i_2, \dots, i_{k-1}, i_k\}$ 满足 $\sigma(i_1) = i_2, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$, 又使得余下的元素保持不变, 则称该置换为 k -**轮换**, 简称轮换, 记作

$$\sigma = (i_1, i_2, \dots, i_{k-1}, i_k).$$

k 称为轮换的长度. $k = 1$ 时, 1- 轮换为恒等置换; $k = 2$ 时, 2- 轮换 (i_1, i_2) 叫做 **对换**.

两个轮换 $\sigma = (i_1, i_2, \dots, i_{k-1}, i_k), \tau = (j_1, j_2, \dots, j_{l-1}, j_l)$ 叫做不 交, 如果 $k + l$ 个元素都是不同的.

定理 2 任意一个置换都可以表示为一些不交轮换的乘积. 在不考虑乘积次序的情况下, 该表达式是惟一的.

证 设 σ 是 $S = \{1, 2, \dots, n-1, n\}$ 上的一个置换. 在 S 中任取一个元素, 设为 $i_1^{(1)}$. 因为 $n+1$ 个元素

$$i_1^{(1)}, \sigma^1(i_1^{(1)}), \dots, \sigma^n(i_1^{(1)})$$

都落在 n 元集 S 中, 必有 $k \neq l$ 使得 $\sigma^k(i_1^{(1)}) = \sigma^l(i_1^{(1)})$.

不妨设 $k > l$, 得到 $\sigma^{k-l}(i_1^{(1)}) = i_1^{(1)}$.

取 $k_1 \leq n$ 为使得 $\sigma^{k_1}(i_1^{(1)}) = i_1^{(1)}$ 的最小正整数, 并令

$$i_2^{(1)} = \sigma^1(i_1^{(1)}), \dots, i_{k_1}^{(1)} = \sigma^{k_1-1}(i_1^{(1)}).$$

则 $\sigma_1 = (i_1^{(1)}, i_2^{(1)}, \dots, i_{k_1}^{(1)})$ 就是一个 k_1 -轮换.

如果 $k_1 = n$, 则 $\sigma = \sigma_1$. 结论成立.

如果 $k_1 < n$, 在 $S - \{i_1^{(1)}, i_2^{(1)}, \dots, i_{k_1}^{(1)}\}$ 中任取一个元素, 设为 $i_1^{(2)}$. 取 $k_2 \leq n$ 为使得 $\sigma^{k_2}(i_1^{(2)}) = i_1^{(2)}$ 的最小正整数, 并令

$$i_2^{(2)} = \sigma^1(i_1^{(2)}), \dots, i_{k_2}^{(2)} = \sigma^{k_2-1}(i_1^{(2)}).$$

则 $\sigma_2 = (i_1^{(2)}, i_2^{(2)}, \dots, i_{k_2}^{(2)})$ 是一个与 σ_1 不交的 k_2 -轮换.

如此下去, $\dots$, 可找到与 $\sigma_1, \dots, \sigma_{r-1}$ 不交的 k_r -轮换 σ_r 使得 $k_1 + k_2 + \dots + k_r = n$. 因为对任意 $i \in S$, 有

$$\sigma_1 \sigma_2 \cdots \sigma_r(i) = \sigma(i),$$

所以定理成立. 证毕.

例 2 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix} = (2, 5, 4)(1, 6, 3).$

对于轮换 $\sigma = (i_1, i_2, \dots, i_{k-1}, i_k)$, 有

$$\sigma = (i_1, i_2, \dots, i_{k-1}, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_3)(i_1, i_2).$$

例 2 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix} = (2, 5, 4)(1, 6, 3) = (2, 4)(2, 5)(1, 3)(1, 6).$

定义 1 n 元排列 $i_1, \dots, i_k, \dots, i_l, \dots, i_n$ 的一对有序元素 (i_k, i_l) 叫做 **逆序**, 如果 $k < l$ 时, $i_k > i_l$. 排列中逆序的个数叫做该排列的 **逆序数**, 记为 $[i_1, \dots, i_n]$.

定理 3 任意一个置换 σ 都可以表示为一些对换的乘积, 且对换个数的奇偶性与排列的逆序数 $[\sigma(1), \dots, \sigma(n)]$ 的奇偶性 同.

证明 设 $\tau = (\sigma(k), \sigma(l))$, 其对排列 $\sigma(1), \dots, \sigma(k), \dots, \sigma(l), \dots, \sigma(n)$ 作用得到新排列 $\sigma(1), \dots, \sigma(l), \dots, \sigma(k), \dots, \sigma(n)$ 则发生改变的有序对为

$(\sigma(k), \sigma(k+1)), \dots, (\sigma(k), \sigma(l)), (\sigma(k+1), \sigma(l)), \dots, (\sigma(l-1), \sigma(l)),$
共 $2(l-k)+1$ 对. 因此, 对换改变排列的逆序数 $[\sigma(1), \dots, \sigma(n)]$ 的奇偶性.

再设 $\sigma = \tau_k \cdots \tau_1$ 为 m 个对换的乘积, 那么排列 $1, \dots, n$ 经过 m 个对换变为排列 $\sigma(1), \dots, \sigma(n)$. 因此, 逆序数 $[\sigma(1), \dots, \sigma(n)]$ 的奇偶性与 $[1, \dots, n] + m = m$ 的奇偶性 同. 证毕.

定义 2 一个置换 σ 叫做 **偶置换**, 如果它可以表示为偶数个对换的乘积; σ 叫做 **奇置换**, 如果它可以表示为奇数个对换的乘积.

记 A_n 为 n 元偶置换全体组成的集合.

定理 4 A_n 对置换的乘法构成一个群, 其阶是 $n!/2$.

证 因为偶置换与偶置换的乘积是偶置换, 恒等置换是偶置换, 偶置换的逆置换是偶置换, 所以 A_n 对置换的乘法构成一个群.

因为奇置换与偶置换的乘积是奇置换, 所以 n 元奇置换全体组成的集合为 $\tau A_n = \{\tau\sigma \mid \sigma \in A_n\}$, 其中 τ 是任一给定的奇置换. 因此, 取定一个奇置换 τ , 我们有 $S_n = A_n \cup \tau A_n$ 以及 $|S_n| = |A_n| + |\tau A_n| = 2|A_n|$. 故 $|A_n| = n!/2$. 证毕.

A_n 叫做 **交错群**.

由 n 元置换构成的群叫做 n 元 **置换群**.

例 3 设 $\sigma = (1, 2, 3)$. 则循环群 $G = \langle \sigma \rangle = \{e, (1, 2, 3), (1, 3, 2)\}$ 是 3 元置换群.

例 4 设 $\sigma_1 = (1, 2, 3, 4)$, $\sigma_2 = (1, 3, 2, 4)$. 则循环群 $G_1 = \langle \sigma_1 \rangle = \{e, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\}$ 和 $G_2 = \langle \sigma_2 \rangle = \{e, (1, 3, 2, 4), (1, 2)(3, 4), (1, 4, 2, 3)\}$ 都是 4 元置换群.

定理 5 设 G 是一个 n 元群. 则 G 同构一个 n 元置换群.

第十章 环

定义 1 设 R 是具有两种结合法 (通常表示为加法 (+) 和乘法) 的非空集合. 如果如下条件成立:

- (i) R 对于加法构成一个交换群;
- (ii) (结合律) $\forall a, b, c \in R, (ab)c = a(bc)$;
- (iii) (分配律) $\forall a, b, c \in R, (a+b)c = ac + bc, a(b+c) = ab + ac$;

则 R 叫做 **环**.

如果还满足 (iv)(交换律) $\forall a, b \in R, ab = ba$, 则 R 叫做 **交换环**.

如果 R 中有一个元素 $e = 1_R$ 使得 (v) $\forall a \in R$, 有 $a1_R = 1_Ra = a$, 则 R 叫做 **有单位元环**.

定理 1 设 R 是一个环. 则

- (i) 对任意 $a \in R$, 有 $0a = a0 = 0$;
- (ii) 对任意 $a, b \in R$, 有 $(-a)b = a(-b) = -ab$;
- (iii) 对任意 $a, b \in R$, 有 $(-a)(-b) = ab$;
- (iv) 对任意 $n \in \mathbf{Z}$, 任意 $a, b \in R$, 有 $(na)b = a(nb) = nab$;
- (v) 对任意 $a_i, b_j \in R$, 有

$$\left(\sum_{i=1}^n a_i\right)\left(\sum_{j=1}^m b_j\right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j.$$

证 (i) 因为 $0a = (0 + 0)a = 0a + 0a$, 所以 $0a = 0$. 同样, $a0 = 0$.

(ii) 因为 $(-a)b + ab = ((-a) + a)b = 0a = 0$, $a(-b) + ab = a((-b) + b) = a0 = 0$, 所以 $(-a)b = a(-b) = -ab$.

(iii), (iv) 和 (v) 可有 (i) 和 (ii) 得到.

定理 2 设 R 是有单位元的环. 设 n 是正整数, $a, b, a_1, \dots, a_r \in R$.

(i) 如果 $ab = ba$, 则 $(a + b)^n = \sum_{k=0}^n \frac{n!}{k!(n-k)!} a^k b^{n-k}$.

(ii) 如果 $a_i a_j = a_j a_i$, $1 \leq i, j \leq r$, 则

$$(a_1 + \dots + a_r)^n = \sum_{i_1 + \dots + i_r = n} \frac{n!}{i_1! \dots i_r!} a_1^{i_1} \dots a_r^{i_r}.$$

例 1 整数环 $\mathbf{Z}$.

$\mathbf{Z}$ 对于加法 $a + b$ 构成一个交换加群. 零元为 0 , a 的负元为 $-a$. $\mathbf{Z}$ 对于乘法 $a \cdot b$, 满足结合律和交换律, 有单位元 1 . 并且有分配律. 因此, $\mathbf{Z}$ 是有单位元的交换环.

例 2 多项式环 $\mathbf{R}[X]$. 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$,
 $g(x) = b_n x^n + \cdots + b_1 x + b_0 \in \mathbf{R}[X]$. 在 $\mathbf{R}[X]$ 上定义加法:

$$(f + g)(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0),$$

则 $\mathbf{R}[X]$ 对于该加法构成一个交换加群.

零元为 0, $f(x)$ 的负元为 $(-f)(x) = (-a_n)x^n + \cdots + (-a_1)x + (-a_0)$.

设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_n \neq 0$, $g(x) = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$,

在 $\mathbf{R}[X]$ 上定义乘法: $(f \cdot g)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0$,

其中 $c_k = \sum_{i+j=k} a_i b_j$, $0 \leq k \leq n+m$, 即

$$c_{n+m} = a_n b_m, \quad c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m, \dots, \quad c_0 = a_0 b_0.$$

$\mathbf{R}[X]$ 对于该乘法, 满足结合律和交换律, 有单位元 1. 并且有分配律.

因此, $\mathbf{R}[X]$ 是有单位元的交换环.

定义 2 设 a 是环 R 中的一个非零元. a 称为 **左零因子**(对应地. **右零因子**), 如果存在非零元 $b \in R$ (对应地. $c \in R$) 使得 $ab = 0$ (对应地. $ca = 0$), a 称为 **零因子**, 如果它同时为左零因子和右零因子.

例 4 $\mathbf{Z}/6\mathbf{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ 是一个有零因子环. 因为 $\bar{2} \cdot \bar{3} = \bar{0}$.

定义 3 设 a 是有单位元 1_R 的环 R 中的一个元. a 称为 **左逆元**(对应地. **右逆元**), 如果存在元 $b \in R$ (对应地. $c \in R$) 使得 $ab = 1_R$ (对应地. $ca = 1_R$). 这时, b (对应地. c) 叫做 a 的 **右逆**(对应地. **左逆**). a 称为 **逆元**, 如果它同时为左逆元和右逆元.

定义 4 设 R 是一个交换环. 我们称 R 为 **整环**, 如果 R 中有单位元, 但没有零因子.

定义 5 我们称交换环 R 为一个 **域**, 如果 R 中有单位元, 且每个非零元都是可逆元. 即 R 对于加法构成一个交换群, $R^* = R \setminus \{0\}$ 对于乘法构成一个交换群.

定义 6 设 R 是一个交换环, $a, b \in R, b \neq 0$. 如果一个元素 $c \in R$ 使得 $a = bc$, 就称 b **整除** a 或者 a 被 b 整除, 记作 $b|a$. 这时, 把 b 叫做 a 的 **因子**, 把 a 叫做 b 的 **倍元**.

如果 b, c 都不是单位元, 就 b 称为 a 的 **真因子**.

R 中的元素 p 称为不可约元或素元, 如果 p 不是单位元, 且没有真因子. 也就是说, 如果有元素 $b, c \in R$ 使得 $p = bc$, 则 b 或 c 一定是单位元.

两个元素 $a, b \in R$ 称为 **伴的**, 如果存在可逆元 $u \in R$ 使得 $a = bu$.

定义 7 设 R, R' 是两个环. 我们称映射 $f: R \longrightarrow R'$ 为 **环同态**, 如果 f 满足如下条件:

- (i) 对任意的 $a, b \in I$, 都有 $f(a + b) = f(a) + f(b)$;
- (ii) 对任意的 $a, b \in I$, 都有 $f(ab) = f(a)f(b)$.

如果 f 是一对一的, 则称 f 为 **单同态**; 如果 f 是满的, 则称 f 为 **满同态**; 如果 f 是一一对应的, 则称 f 为 **同构**.

定义 8 设 R, R' 是两个环. 我们称 R 与 R' 同构, 如果存在一个 R 到 R' 的同构.

定义 9 设 R 是一个环. 如果存在一个最小正整数 n 使得对任意 $a \in R$, 都有 $na = 0$, 则称环 R 的 **特征** 为 n . 如果不存在这样的正整数, 则称环 R 的特征为 0.

定理 3 如果域 K 的特征不为零, 则其特征必为素数.

证 设域 K 的特征为 n . 如果 n 不是素数, 则存在整数 $1 < n_1, n_2 < n$, 使得 $n = n_1 n_2$. 从而, $(n_1 1_{\mathbf{K}})(n_2 1_{\mathbf{K}}) = (n_1 n_2) 1_{\mathbf{K}} = 0$. 因为域 $\mathbf{K}$ 无零因子, 所以 $(n_1 1_{\mathbf{K}}) = 0$ 或 $(n_2 1_{\mathbf{K}}) = 0$. 这与特征 n 的最小性矛盾. 证毕.

定理 4 设 R 是有单位元的交换环. 如果环 R 的特征是素数 p , 则对任意 $a, b \in R$, 有

$$(a + b)^p = a^p + b^p.$$

证 根据定 2, 我们有

$$(a + b)^p = a^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k b^{p-k} + b^p.$$

对于 $1 \leq k \leq p-1$, 有 $(p, k!(p-k)!) = 1$, 从而 $p \mid p \frac{(p-1)!}{k!(p-k)!}$. 这样, 由 R 的特征是素数 p , 得到 $\frac{p!}{k!(p-k)!} a^k b^{p-k} = 0$. 因此, 定 2 成立. 证毕.

定理 5 设 p 是一个素数. 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 是整系数多项式. 则

$$f(x)^p \equiv f(x^p) \pmod{p}.$$

证 在域 $\mathbf{F}_p$ 上的多项式环 $\mathbf{F}_p[x]$ 上, 应用定 4, 我们有

$$f(x)^p = (a_n x^n)^p + \cdots + (a_1 x)^p + a_0^p = a_n (x^p)^n + \cdots + a_1 (x^p) + a_0 = f(x^p).$$

也就是,

$$f(x)^p \equiv f(x^p) \pmod{p}.$$

设 A 是一个整环. 令 $E = A \times A^*$. 在 E 上定义关系 R :
 $(a, b)R(c, d)$ 如果 $ad = bc$. 则 R 是 E 上的等价关系, 即有

- (i) 自反性: 对任意 $(a, b) \in E$, 有 $(a, b)R(a, b)$.
- (ii) 对称性: 如果 $(a, b)R(c, d)$, 则 $(c, d)R(a, b)$.
- (iii) 传递性: 如果 $(a, b)R(c, d)$ 和 $(c, d)R(e, f)$, 则 $(a, b)R(e, f)$.

记 $\frac{a}{b} = C_{(a,b)} = \{(e, f) | \in E, (a, b)R(c, d)\}$ 为 (a, b) 的等价类.

我们在商集 E/R 上定义加法和乘法如下:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

则 E/R 关于加法构成一个交换群, 零元为 $\frac{0}{b}$, $\frac{a}{b}$ 的负元为 $\frac{-a}{b}$.

$(E/R)^* = E/R \setminus \{\frac{0}{b}\}$ 关于乘法构成一个交换群, 单位元为 $\frac{b}{b}$,

$\frac{a}{b}$ 的逆元为 $\frac{b}{a}$.

因此, E/R 构成一个域. 叫做 A 的 **分式域**.

定理 1 交换环 A 有分式域的充要条件是 R 为整环.

例 1 取 $A = \mathbf{Z}$, 则 $\mathbf{Z}$ 是一个整环, 从而有分式域, 叫做 $\mathbf{Z}$ 的有理数域, 记为 $\mathbf{Q}$.

例 2 取 $A = \mathbf{Z}/p\mathbf{Z}$, 其中 p 为素数. 则 A 是一个整环, 从而有分式域, 叫做 $\mathbf{Z}/p\mathbf{Z}$ 的 p -元域, 记为 $\mathbf{F}_p$ 或 $GF(p)$.

例 3 设 K 是一个域. 则 $A = \mathbf{K}[X]$ 是一个整环, 从而有分式域, 叫做 $\mathbf{K}[X]$ 的多项式分式域, 记为 $\mathbf{K}(X)$. 即

$$\mathbf{K}(X) = \left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in \mathbf{K}[X], g(X) \neq 0 \right\}.$$

定义 1 设 R 是一个环, I 是 R 的子环. I 称为 R 的 **左理想**, 如果对任意的 $r \in R$ 和对任意的 $a \in I$, 都有 $ra \in I$. I 称为 R 的 **右理想**, 如果对任意的 $r \in R$ 和对任意的 $a \in I$, 都有 $ar \in I$. I 称为 R 的 **理想**, 如果 R 同时为左理想和右理想.

例 1 $\{0\}$ 和 R 都是 R 的理想, 叫做 R 的 **平凡理想**.

定理 1 环 R 的非空子集 I 是左 (对应地. 右) 理想的充要条件是:

- (i) 对任意的 $a, b \in I$, 都有 $a - b \in I$;
- (ii) 对任意的 $r \in R$ 和对任意的 $a \in I$, 都有 $ra \in I$. (对应地. $ar \in I$.)

证 必要性是显然的. 我们证明充分性. 由 (i) 和 (ii) 立即知道 I 是 R 的子环.

推论 设 $\{A_i\}_{i \in I}$ 是环 R 中的一族 (左) 理想. 则 $\bigcap_{i \in I} A_i$ 也是一个 (左) 理想.

定义 2 设 X 是环 R 的一个子集. 设 $\{A_i\}_{i \in I}$ 是环 R 中包含 X 的所有 (左) 理想. 则 $\cap_{i \in I} A_i$ 称为由 X 生成的 (左) 理想. 记为 (X) .

X 中的元素叫做理想 (X) 的 **生成元**. 如果 $X = \{a_1, \dots, a_n\}$, 则理想 (X) 记为 $(a_1, \dots, a_n)$, 称为 **有限生成的**. 由一个元素生成的理想 (a) 叫做 **主理想**.

定理 2 设 R 是交换环, $a \in R, X \subset R$. 则

(i) 主 想 (a) 为

$$(a) = \{ra + ar' + na + \sum_{i=1}^m r_i a s_i \mid r, s, r_i, s_i \in R, m \in \mathbf{N}, n \in \mathbf{Z}\}.$$

(ii) 如果 R 有单位元 1_R 时, 则

$$(a) = \{ \sum_{i=1}^m r_i a s_i \mid r_i, s_i \in R, m \in \mathbf{N}, \}.$$

(iii) 如果 a 在 R 的中心, 则

$$(a) = \{ra + na \mid r \in R, n \in \mathbf{Z}\}.$$

(iv) $Ra = \{ra \mid r \in R\}$ (对应地. $aR = \{ar \mid r \in R\}$) 是 R 中的

的左 (对应地. 右) 想. 如果 R 有单位元, 则 $a \in Ra, a \in aR$.

环 R 叫做 **主理想环**, 如果 R 的所有 想都是主 想.

例 2 $\mathbf{Z}$ 是主 想环.

证 设 I 是 $\mathbf{Z}$ 中的一个非零 想. 当 $a \in I$ 时, 有 $0 = 0a \in I$ 及 $-a = (-1)a \in I$. 因此, I 中有正整数存在. 设 d 是 I 中的最小正整数, 则 $I = (d)$. 事实上, 对任意 $a \in I$, 存在整数 q, r 使得

$$a = dq + r, \quad 0 \leq r < d.$$

这样, 由 $a \in I$ 及 $dq \in I$, 得到 $r = a - dq \in I$. 但 $r < d$ 以及 d 是 I 中的最小正整数. 因此, $r = 0$, $a = dq \in (d)$. 从而 $I \subset (d)$. 又显然有 $(d) \subset I$. 故 $I = (d)$. 故 $\mathbf{Z}$ 是主 想环.

例 3 $\mathbf{Z}[X]$ 是主 想环.

例 4 $\mathbf{Z}[\sqrt{-5}]$ 不是主 想环.

设 R 是一个环. I 是 R 的一个理想. 则 I 是 $(R, +)$ 的一个正规子群. 因此, 对于加法运算 $(a + I) + (b + I) = (a + b) + I$, 商群 R/I 存在.

对于乘法, 当 $a + I = a' + I$, $b + I = b' + I$ 时, 有 $a = a' + r_1$, $b = b' + r_2$, $r_1, r_2 \in I$. 因为 I 是理想, 所以 $r_1 b', a' r_2, r_1 r_2 \in I$. 从而, $ab + I = (a' + r_1)(b' + r_2) + I = a'b' + r_1 b' + a' r_2 + r_1 r_2 + I = a'b' + I$.

因此, 在 R/I 上可定义乘法运算: $(a + I)(b + I) = ab + I$.

易知, 对于乘法, 有结合律成立. 因此, 我们得到:

定理 4 设 R 是一个环. I 是 R 的一个 想. 则 R/I 对于加法运算

$$(a + I) + (b + I) = (a + b) + I,$$

和乘法运算

$$(a + I)(b + I) = ab + I,$$

构成一个环. 当 R 是交换环或有单位元时, R/I 也是交换环或有单位元.

定 中的的环 R/I 叫做 R 关于 I 的 **商环**.

定理 5 设 f 是环 R 到环 R' 的同态, 则 f 的核 $\ker(f)$ 是 R 的理想. 反过来, 如果 I 是环 R 的理想, 则映射

$$\begin{aligned}s : R &\longrightarrow R/I \\ r &\longmapsto r + I\end{aligned}$$

是核为 I 的同态.

映射 $s : R \longrightarrow R/I$ 称为 R 到 R/I **自然同态**.

定理 6 设 f 是环 R 到环 R' 的同态, 则存在惟一的 $R/\ker(f)$ 到像子环 $f(R)$ 的同构 $\bar{f}: r + I \longmapsto f(r)$ 使得 $f = i \circ \bar{f} \circ s$, 其中 s 是环 R 到商环 $R/\ker(f)$ 的自然同态, $i: c \longmapsto c$ 是 $f(R)$ 到 R' 的恒等同态. 即有如下的交换图:

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ s \downarrow & & \uparrow i \\ R/\ker(f) & \xrightarrow{\bar{f}} & f(R) \end{array}$$

定义 3 设 P 是环 R 的理想. P 称为 R 的 **素理想**, 如果 $P \neq R$, 且对任意的理想 A, B , $AB \subset P$, 有 $A \subset P$ 或 $B \subset P$.

定理 7 设 P 是环 R 的理想. 如果 $P \neq R$, 且对任意的 $a, b \in R$, 当 $ab \in P$ 时, 有 $a \in P$ 或 $b \in P$, 则 P 是素理想. 反过来, 如果 P 是素理想, 且 R 是交换环, 则上述结论也成立.

例 5 任意整环的零理想是素理想.

例 6 设 p 是素数. 则 $P = (p) = p\mathbf{Z}$ 是 $\mathbf{Z}$ 的素理想.

证 对任意的整数 a, b , 若 $ab \in P = (p)$, 则 $p|ab$. 根据 §1.4 定理 2, 有 $p|a$ 或 $p|b$. 由此得到, $a \in P$ 或 $b \in P$. 根据定理 7, $P = (p) = p\mathbf{Z}$ 是 $\mathbf{Z}$ 的素理想.

定理 8 在有单位元 $1_R \neq 0$ 的交换环 R 中, 理想 P 是素理想的充要条件是商环 R/P 是整环.

定义 4 设 M 是环 R 的 (左) 理想. M 称为 R 的 **最大 (左) 理想**, 如果 $M \neq R$, 且对任意的理想 N , 使得 $M \subset N \subset R$, 有 $N = M$ 或 $N = R$.

定理 9 在有单位元的非零环 R 中, 最大 (左) 理想总是存在的. 事实上, R 的每个 (左) 理想 ($\neq R$) 都包含在一个最大 (左) 理想中.

定理 10 设 R 是一个局部环. 如果 $R^2 = R$, (特别地, 如果 R 有单位元), 则 R 的每个最大理想是素理想.

定理 11 设 R 是一个有单位元 $1_R \neq 0$ 的环, M 是 R 的一个想.

(i) 如果 M 是最大 想, 且 R 是交换环, 则商环 R/M 是一个域;

(ii) 如果商环 R/M 是一个除子环, 则 M 是一个极大 想.

定理 12 设 R 是一个有单位元 $1_R \neq 0$ 的交换环, 则如下条件等价:

(i) R 是的一个域.

(ii) R 没有真 想.

(iii) 0 是 R 的最大 想.

(iv) 每个非零环同态 $R \rightarrow R'$ 是单同态.

我们考虑整环 R 上的全体多项式组成的集合 $R[X]$.

首先, 定义 $R[X]$ 上的加法. 设

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \quad g(x) = b_n x^n + \cdots + b_1 x + b_0,$$

定义 $f(x)$ 和 $g(x)$ 的加法为

$$(f + g)(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0),$$

则 $R[X]$ 中的零元为 0,

$f(x)$ 的负元为

$$(-f)(x) = (-a_n)x^n + \cdots + (-a_1)x + (-a_0)$$

其次, 定义 $R[X]$ 上的乘法.

设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_n \neq 0$, $g(x) = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$,

定义 $f(x)$ 和 $g(x)$ 的乘法为

$$(f \cdot g)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0,$$

其中 $c_k = \sum_{i+j=k} a_i b_j$, $0 \leq k \leq n+m$, 即

$$c_{n+m} = a_n b_m, \quad c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m, \quad \dots, \quad c_0 = a_0 b_0,$$

则 $R[X]$ 中的单位元为 1.

$R[X]$ 对于上述加法运算和乘法运算构成一个整环.

例 1 设 $f(x) = x^6 + x^4 + x^2 + x + 1$, $g(x) = x^7 + x + 1 \in \mathbf{F}_2[x]$, 则

$$f(x) + g(x) = x^7 + x^6 + x^4 + x^2,$$

$$f(x)g(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1.$$

事实上 $(x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1)$

$$\begin{aligned} &= x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 + x^5 + x^3 + x^2 + x \\ &\quad + x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_n \neq 0$, 则称多项式 $f(x)$ 的 **次数** 为 n , 记为 $\deg f = n$.

例 2 $\mathbf{Z}[X]$ 中的 $2x + 3$ 的次数为 1, $x^2 + 2x + 3$ 的次数为 2, $x^4 + 1$ 的次数为 4, $x^8 + x^4 + x^3 + x + 1$ 的次数为 8.

定义 1 设 $f(x)$, $g(x)$ 是整环 R 上的任意两个多项式, 其中 $g(x) \neq 0$. 如果存在一个多项式 $q(x)$ 使得等式

$$f(x) = g(x)q(x) \quad (1)$$

成立, 就称 $g(x)$ **整除** $f(x)$ 或者 $f(x)$ 被 $g(x)$ 整除, 记作 $g(x)|f(x)$. 这时, 把 $g(x)$ 叫做 $f(x)$ 的 **因式**, 把 $f(x)$ 叫做 $g(x)$ 的 **倍式**. 否则, 就称 $g(x)$ 不能整除 $f(x)$ 或者 $f(x)$ 不能被 $g(x)$ 整除, 记作 $g(x) \nmid f(x)$.

例 3 $\mathbf{Z}[X]$ 中的 $2x + 3 \mid 2x^2 + 3x$, $x^2 + 1 \mid x^4 - 1$.

定义 2 设 $f(x)$ 是整环 R 上的非常数多项式. 如果除了显然因式 1 和 $f(x)$ 外, $f(x)$ 没有其它因式, 那么, $f(x)$ 叫做 **不可约多项式**, 否则, $f(x)$ 叫做 **合式**.

多项式是否可约与所在的环或域 关.

例 4 多项式 $x^2 + 1$ 在 $\mathbf{Z}[x]$ 中是不可约的, 但在 $\mathbf{F}_2[x]$ 中是可约的.

例 5 $\mathbf{F}_2[x]$ 中的一次不可约多项式为 $x, x + 1$.

二次不可约多项式为 $x^2 + x + 1$, 可约多项式为 $x^2, x^2 + 1 = (x + 1)^2, x^2 + x = x(x + 1)$.

三次不可约多项式为 $x^3 + x + 1, x^3 + x^2 + 1$, 可约多项式为 $x^3, x^3 + x, x^3 + x^2, x^3 + x^2 + x, x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1), x^3 + 1 = (x + 1)(x^2 + x + 1)$.

定理 1 设 $f(x) = a_n x^n + \cdots + a_0$, $g(x) = x^m + \cdots + b_0$ 是整环 R 上的多项式, 则存在 $q(x)$ 和 $r(x)$ 使得 $f(x) = g(x)q(x) + r(x)$, $\deg r < \deg g$.

证 对次数 $\deg f = n$ 作归纳法. (i) 设 $\deg f < \deg g$, 取 $q(x) = 0$, $r(x) = f(x)$. 成立.

(ii) 设 $\deg f \geq \deg g$. 假设结论对 $\deg f < n$ 的多项式成立.

对于 $\deg f = n \geq \deg g$, 我们有

$$\begin{aligned} f(x) - a_n x^{n-m} \cdot g(x) &= (a_{n-1} - a_n b_{m-1})x^{n-1} + \cdots + (a_{n-m} - a_n b_0)x^{n-m} \\ &\quad + a_{n-m-1}x^{n-m-1} + \cdots + a_0. \end{aligned}$$

这说明 $f(x) - a_n x^{n-m} \cdot g(x)$ 是次数 $\leq n-1$ 的多项式. 对其运用归纳假设或情形 (I), 存在整系数多项式 $q_1(x)$ 和 $r_1(x)$ 使得

$$f(x) - a_n x^{n-m} \cdot g(x) = g(x)q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x).$$

因此, $q(x) = a_n x^{n-m} + q_1(x)$, $r(x) = r_1(x)$ 为所求.

根据数学归纳法原理, 结论是成立的. 证毕.

定 1 叫做 多项式欧几里得除法.

推论 1 设 $f(x)$ 是整环 R 上的多项式, $a \in R$, 则存在多项式 $q(x)$ 和常数 $c = f(a)$ 使得 $f(x) = (x - a)q(x) + f(a)$.

推论 2 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 是整环 R 上的多项式, $a \in R$, 则 $x - a | f(x)$ 的充要条件是 $f(a) = 0$.

定义 3 (2) 式中的 $q(x)$ 叫做 $f(x)$ 被 $g(x)$ 除所得的 **不完全商**, $r(x)$ 叫做 $f(x)$ 被 $g(x)$ 除所得的 **余式**.

例 6 设 $f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$, $g(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbf{F}_2[x]$, 求 $q_1(x)$ 和 $r_1(x)$ 使得

$$f(x) = g(x)q_1(x) + r_1(x), \quad \deg r_1 < \deg g_1.$$

解 逐次消除最高次项,

$$\begin{aligned} & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 - x^5(x^8 + x^4 + x^3 + x + 1) \\ &= x^{11} + x^4 + x^3 + 1, \end{aligned}$$

$$\begin{aligned} & x^{11} + x^4 + x^3 + 1 - x^3(x^8 + x^4 + x^3 + x + 1) \\ &= x^7 + x^6 + 1. \end{aligned}$$

因此, $q_1(x) = x^5 + x^3$, $r_1(x) = x^7 + x^6 + 1$.

类似于整数中的最大公因数和最小公倍数, 我们可以给出多项式环 $R[x]$ 中的最大公因式和最小公倍式.

设 $f(x), g(x) \in R[x]$. $d(x) \in R[x]$ 叫做 $f(x), g(x)$ 的 **最大公因式**, 如果 (1) $d(x)|f(x), d(x)|g(x)$.

(2) 若 $h(x)|f(x), h(x)|g(x)$, 则 $h(x)|d(x)$.

$f(x), g(x)$ 的最大公因式记作 $(f(x), g(x))$.

设 $f(x), g(x) \in R[x]$. $D(x) \in R[x]$ 叫做 $f(x), g(x)$ 的 **最小公倍式**, 如果 (1) $f(x)|D(x), g(x)|D(x)$.

(2) 若 $f(x)|h(x), g(x)|D(x)$, 则 $D(x)|h(x)$.

$f(x), g(x)$ 的最小公倍式记作 $[f(x), g(x)]$.

多项式广义欧几里得除法

设 $f(x), g(x)$ 是域 $\mathbf{K}$ 上多项式, $\deg g \geq 1$. 记 $r_0(x) = f(x), r_1(x) = g(x)$. 反复运用多项式欧几里得除法, 我们有

$$r_0(x) = r_1(x)q_1(x) + r_2(x), \quad 0 \leq \deg r_2 < \deg r_1,$$

$$r_1(x) = r_2(x)q_2(x) + r_3(x), \quad 0 \leq \deg r_3 < \deg r_2,$$

.....

$$r_{k-2}(x) = r_{k-1}(x)q_{k-1}(x) + r_k(x), \quad 0 \leq \deg r_k < \deg r_{k-1},$$

$$r_{k-1}(x) = r_k(x)q_k(x) + r_{k+1}(x), \quad \deg r_{k+1} = 0.$$

经过有限步骤, 必然存在 k 使得 $r_{k+1}(x) = 0$, 这是因为

$$0 = \deg r_{k+1} < \deg r_k < \deg r_{k-1} < \dots < \deg r_2 < \deg r_1 = \deg g,$$

且 $\deg g$ 是有限正整数.

定理 2 设 $f(x), g(x) \in \mathbf{K}[x]$, $\deg g \geq 1$, 则 $(f(x), g(x)) = r_k(x)$, 其中 $r_k(x)$ 是多项式广义欧里得除法中最后一个非零余式.

从多项式广义欧里得除法中逐次消去

$$r_{k-1}(x), r_{k-2}(x), \dots, r_3(x), r_2(x),$$

可找到 $s(x), t(x) \in \mathbf{K}[x]$ 使得

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)).$$

定理 3 设 $f(x), g(x) \in \mathbf{K}[x]$, 则存在 $s(x), t(x) \in \mathbf{K}[x]$ 使得

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)).$$

$f(x)$ 与 $g(x)$ 叫做 **互素**(或 **互质**) 的, 如果它们的最大公因式 $(f(x), g(x)) = 1$.

例 7 设 $f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$, $g(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbf{F}_2[x]$, 求多项式 $s(x)$, $t(x)$ 使得

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)).$$

解 运用广义多项式欧里得除法, 我们有

$$\begin{aligned} f(x) &= g(x)q_1(x) + r_1(x), & q_1(x) &= x^5 + x^3, & r_1(x) &= x^7 + x^6 + 1, \\ g(x) &= r_1(x)q_2(x) + r_2(x), & q_2(x) &= x + 1, & r_2(x) &= x^6 + x^4 + x^3, \\ r_1(x) &= r_2(x)q_3(x) + r_3(x), & q_3(x) &= x + 1, & r_3(x) &= x^5 + x^3 + 1, \\ r_2(x) &= r_3(x)q_4(x) + r_4(x), & q_4(x) &= x, & r_4(x) &= x^3 + x, \\ r_3(x) &= r_4(x)q_5(x) + r_5(x), & q_5(x) &= x^2, & r_5(x) &= 1. \end{aligned}$$

从而,

$$\begin{aligned}r_5(x) &= r_3(x) + q_5(x)(r_2(x) + r_3(x)q_4(x)) \\&= -q_5(x)r_2(x) + (x^3 + 1)(r_1(x) + r_2(x)q_3(x)) \\&= (x^3 + 1)r_1(x) + (x^4 + x^3 + x^2 + x + 1)(g(x) + r_1(x)q_2(x)) \\&= (x^4 + x^3 + x^2 + x + 1)g(x) + (x^5 + x^3)(f(x) + g(x)q_1(x)) \\&= (x^5 + x^3)f(x) + (x^{10} + x^6 + x^4 + x^3 + x^2 + x + 1)g(x).\end{aligned}$$

因此, $s(x) = x^5 + x^3$, $t(x) = x^{10} + x^6 + x^4 + x^3 + x^2 + x + 1$.

定义 4 给定 $R[X]$ 中一个首一多项式 $m(x)$. 两个多项式 $f(x), g(x)$ 叫做模 $m(x)$ **同余**, 如果 $m(x) \mid f(x) - g(x)$. 记作 $f(x) \equiv g(x) \pmod{m(x)}$. 否则, 叫做模 $m(x)$ **不同余**. 记作 $f(x) \not\equiv g(x) \pmod{m(x)}$.

根据定理 1, 任一多项式 $f(x)$ 都与其被 $m(x)$ 除的余式 $r(x)$ 模 $m(x)$ 同余, 该余式 $r(x)$ 叫做 $f(x)$ 模 $m(x)$ 的 **最小余式**, 记为 $(f(x) \pmod{m(x)})$.

设 $p(x)$ 是 $R[X]$ 中的多项式, 则 $(p(x)) = \{f(x) \mid p(x) \mid f(x)\}$ 是 $R[X]$ 中的理想. 由此得到商环 $R/(p(x))$. 该商环上的运算法则为:
加法:

$$f(x) + g(x) = ((f + g)(x) \pmod{p(x)}),$$

乘法:

$$f(x)g(x) = ((fg)(x) \pmod{p(x)}).$$

定理 4 设 $\mathbf{K}$ 是一个域. $p(x)$ 是 $\mathbf{K}[X]$ 中的不可约多项式. 则商环 $\mathbf{K}[X]/(p(x))$ 对于上述运算法则构成一个域.

证 我们只 证明 $\mathbf{K}[X]/(p(x))$ 中的非零元 $f(x) \pmod{p(x)}$ 为可逆元. 事实上, 对于满足 $f(x) \not\equiv 0 \pmod{p(x)}$ 的多项式 $f(x)$, 有 $(f(x), p(x)) = 1$. 根据定 3, 存在多项式 $s(x), t(x)$ 使得

$$s(x)f(x) + t(x)p(x) = 1.$$

从而,

$$s(x)f(x) \equiv 1 \pmod{p(x)}.$$

这说明 $f(x) \pmod{p(x)}$ 为可逆元, $s(x) \pmod{p(x)}$ 为其逆元.

例 11 设 $\mathbf{K} = \mathbf{Z}/p\mathbf{Z}$ 是一个有限域, 其中 p 是素数. 设 $p(x)$ 是 $\mathbf{K}[X]$ 中的 n 次不可约多项式, 则

$$\mathbf{K}[X]/(p(x)) = \{a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \mid a_i \in \mathbf{K}\}.$$

记为 $\mathbf{F}_{p^n}$. 这个域的元素个数为 p^n .

$\mathbf{F}_{p^n}$ 中的加法和乘法是:

$$f(x) + g(x) = ((f + g)(x) \pmod{p(x)}),$$

$$f(x)g(x) = ((fg)(x) \pmod{p(x)}).$$

例 12 设 $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. 则 $p(x) = x^8 + x^4 + x^3 + x + 1$ 是 $\mathbf{F}_2[X]$ 中的 8 次不可约多项式. 事实上, 我们有

$$\mathbf{F}_{2^8} = \mathbf{F}_2[X]/(x^8 + x^4 + x^3 + x + 1) = \{a_7x^7 + \cdots + a_1x + a_0 \mid a_i \in \{0, 1\}\}.$$

$\mathbf{F}_{2^8}$ 中的加法和乘法是:

$$f(x) + g(x) = ((f + g)(x) \pmod{x^8 + x^4 + x^3 + x + 1}),$$

$$f(x)g(x) = ((fg)(x) \pmod{x^8 + x^4 + x^3 + x + 1}).$$

第十一章 域和 Galois 理论

定义 1 设 F 是一个域. 如果 K 是 F 的子域, 则称 F 为 K 的**扩域**.

如果 F 是 K 的扩域, 则 $1_F = 1_K$. 而且, F 可作为 K 上的线性空间. 我们用 $[F : K]$ 表示 F 在 K 上线性空间的维数. 我们称 F 为 K 的**有限扩张** 或 **无限扩张**, 如果 $[F : K]$ 是有限或无限.

定理 1 设 $\mathbf{E}$ 是 $\mathbf{F}$ 的扩域, $\mathbf{F}$ 是 $\mathbf{K}$ 的扩域. 则

$$[\mathbf{E} : \mathbf{K}] = [\mathbf{E} : \mathbf{F}][\mathbf{F} : \mathbf{K}].$$

如果 $\{\alpha_i\}_{i \in I}$ 是 $\mathbf{F}$ 在 $\mathbf{K}$ 上的基底, $\{\beta_j\}_{j \in J}$ 是 $\mathbf{E}$ 在 $\mathbf{F}$ 上的基底, 则 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 是 $\mathbf{E}$ 在 $\mathbf{K}$ 上的基底.

证 首先, 证明 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 是 $\mathbf{E}$ 在 $\mathbf{K}$ 上的生成元. 事实上, 对任意 $c \in \mathbf{E}$, 根据 $\{\beta_j\}_{j \in J}$ 是 $\mathbf{E}$ 在 $\mathbf{F}$ 上的基底, 存在 $b_j \in \mathbf{F}$, $j \in J$ 使得

$$c = \sum_{j \in J} b_j \beta_j.$$

再根据 $\{\alpha_i\}_{i \in I}$ 是 $\mathbf{F}$ 在 $\mathbf{K}$ 上的基底, 存在 $a_{ij} \in \mathbf{K}$, $i \in I$ 使得

$$b_j = \sum_{i \in I} a_{ij} \alpha_i.$$

从而,

$$c = \sum_{i \in I, j \in J} a_{ij} \alpha_i \beta_j.$$

其次, 证明 $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ 在 $\mathbf{K}$ 上线性无关. 事实上, 若存在 $a_{ij} \in \mathbf{K}$, $i \in I$ 使得

$$\sum_{i \in I, j \in J} a_{ij} \alpha_i \beta_j = 0 \quad \text{或} \quad \sum_{j \in J} \left(\sum_{i \in I} a_{ij} \alpha_i \right) \beta_j = 0.$$

因为 $\{\beta_j\}_{j \in J}$ 是 $\mathbf{E}$ 在 $\mathbf{F}$ 上的基底, 所以

$$\sum_{i \in I} a_{ij} \alpha_i = 0, \quad j \in J.$$

又因为 $\{\alpha_i\}_{i \in I}$ 是 $\mathbf{F}$ 在 $\mathbf{K}$ 上的基底, 得到

$$a_{ij} = 0 \quad i \in I, \quad j \in J.$$

因此，我们有

$$[\mathbf{E} : \mathbf{K}] = [\mathbf{E} : \mathbf{F}][\mathbf{F} : \mathbf{K}].$$

定 成立. 证毕.

推论 $\mathbf{E}$ 是 $\mathbf{K}$ 的有限扩域的充要条件是 $\mathbf{E}$ 是 $\mathbf{F}$ 的有限扩域, 以及 $\mathbf{F}$ 是 $\mathbf{K}$ 的扩域.

例 1 实数域 $\mathbf{R}$ 是有理数域 $\mathbf{Q}$ 的扩域, 复数域 $\mathbf{C}$ 是实数域 $\mathbf{R}$ 的扩域.

例 2 数域 $\mathbf{Q}(\sqrt{2})$ 是 $\mathbf{Q}$ 的有限扩张, 且 $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.

设 $\mathbf{F}$ 是一个域, $X \subset \mathbf{F}$, 则包含 X 的所有子域 (对应地. 子环) 的交集仍是包含 X 的子域, 叫做由 X **生成的子域** (对应地. **子环**). 如果 $\mathbf{F}$ 是 $\mathbf{K}$ 的扩域及 $X \subset \mathbf{F}$, 则由 $\mathbf{K} \cup X$ 生成的子域 (对应地. 子环) 叫做 X **在 $\mathbf{K}$ 上生成的子域** (对应地. **子环**), 记为 $\mathbf{K}(X)$ (对应地. $\mathbf{K}[X]$). 注意到 $\mathbf{K}[X]$ 是一个整环.

如果 $X = \{u_1, \dots, u_n\}$, 则 $\mathbf{F}$ 的子域 $\mathbf{K}(X)$ (对应地. 子环 $\mathbf{K}[X]$) 记为 $\mathbf{K}(u_1, \dots, u_n)$ (对应地. $\mathbf{K}[u_1, \dots, u_n]$). 域 $\mathbf{K}(u_1, \dots, u_n)$ 叫做 $\mathbf{K}$ 的有限扩张. 如果 $X = \{u\}$, 则 $\mathbf{K}(u)$ 称为 $\mathbf{K}$ 的单扩张.

定理 2 设 $\mathbf{F}$ 是域 $\mathbf{K}$ 的扩域, $u, u_1, \dots, u_n \in \mathbf{F}$, 以及 $X \subset \mathbf{F}$, 则

(i) 子环 $\mathbf{K}[u]$ 由形为 $f(u)$ 的元素组成, 其中 f 是系数在 $\mathbf{K}$ 的多项式 (就是 $f \in \mathbf{K}[x]$).

(ii) 子环 $\mathbf{K}[u_1, \dots, u_n]$ 由形为 $f(u_1, \dots, u_n)$ 的元素组成, 其中 f 是系数在 $\mathbf{K}$ 的 n 元多项式 (就是 $f \in \mathbf{K}[x_1, \dots, x_n]$).

(iii) 子环 $\mathbf{K}[X]$ 由形为 $f(u_1, \dots, u_n)$ 的元素组成, 其中 $n \in \mathbf{N}$, $u_1, \dots, u_n \in X$, f 是系数在 $\mathbf{K}$ 的 n 元多项式 (就是 $f \in \mathbf{K}[x_1, \dots, x_n]$).

(iv) 子域 $\mathbf{K}(u)$ 由形为 $\frac{f(u)}{g(u)} f(u)/g(u)$ 的元素组成, 其中 $f, g \in \mathbf{K}[x]$, $g(u) \neq 0$.

- (v) 子域 $\mathbf{K}(u_1, \dots, u_n)$ 由形为 $\frac{f(u_1, \dots, u_n)}{g(u_1, \dots, u_n)}$ 的元素组成, 其中 $f, g \in \mathbf{K}[x_1, \dots, x_n]$, $g(u_1, \dots, u_n) \neq 0$.
- (vi) 子域 $\mathbf{K}(u_1, \dots, u_n)$ 由形为 $\frac{f(u_1, \dots, u_n)}{g(u_1, \dots, u_n)}$ 的元素组成, 其中 $n \in \mathbf{N}$, $f, g \in \mathbf{K}[x_1, \dots, x_n]$, $u_1, \dots, u_n \in X$, $g(u_1, \dots, u_n) \neq 0$.
- (vii) 对每个 $v \in \mathbf{K}(X)$ (对应地. $\mathbf{K}[X]$), 存在一个有限子集 $X' \subset X$, 使得 $v \in \mathbf{K}(X')$ (对应地. $\mathbf{K}[X']$).

定义 2 设 F 是 K 的一个扩域. F 的元素 u 称为 K 上的 **代数数**, 如果存在一个非零多项式 $f \in K[x]$ 使得 $f(u) = 0$. F 的元素 u 称为 K 上的 **超越数**, 如果不存在任何非零多项式 $f \in K[x]$ 使得 $f(u) = 0$. F 称为 K 的 **代数扩张**, 如果 F 的每个元素都是 K 上的代数数. F 称为 K 上的 **超越扩张**, 如果 F 中至少有一个元素是 K 上的超越数.

如果 $u \in K$, 则 u 是 $x - u \in K[x]$ 的根, 因此, u 是 K 上的代数数.

定理 3 如果 $\mathbf{F}$ 是 $\mathbf{K}$ 的扩域, $u \in \mathbf{F}$ 是 $\mathbf{K}$ 上的超越数, 则存在一个在 $\mathbf{K}$ 上为恒等映射的域同构 $\mathbf{K}(u) \cong \mathbf{K}(x)$.

证 因为 u 是 $\mathbf{K}$ 上的超越数, 所以对任意非零多项式 $g(x)$, $g(u) \neq 0$. 考虑 $\mathbf{K}(x)$ 到 $\mathbf{K}(u)$ 的映射

$$\sigma : \frac{F(x)}{g(x)} \longmapsto \frac{F(u)}{g(u)}.$$

易知, σ 是同态, 且 σ 是一一对应的. 故 σ 是同构. 证毕.

引理 设 F 是域 K 的扩域, $u \in F$ 是 K 上的代数数, 则存在惟一的 K 上的首一不可约多项式 $f(x)$ 使得 $f(u) = 0$.

证 因为 $u \in F$ 是 K 上的代数数, 所以存在 K 上的多项式 $f(x)$ 使得 $f(u) = 0$. 在这些多项式中, 有一个次数最小的惟一的首一多项式, 仍记为 $f(x)$. 这个 $f(x)$ 还是不可约的. 因此, $f(x)$ 就是所求的多项式. 证毕.

定义 3 设 F 是域 K 的扩域, $u \in F$ 是 K 上的代数数. 引中的首一不可约多项式称为 u 的**不可约多项式** (或 **极小多项式** 或 **定义多项式**). u 在 K 上的**次数** 是 $\deg f$. u 的极小多项式的其它根叫做 u 的**共轭根**.

定理 4 设 F 是域 K 的扩域, $u \in F$ 是 K 上的代数数, 则

(i) $K(u) = K[u]$.

(ii) $K(u) \cong K[x]/(f)$, 其中 $f \in K[x]$ 是满足 $f(u) = 0$ 的次数为 n 的惟一的首一不可约多项式.

(iii) $[K(u) : K] = n$.

(iv) $\{1, u, u^2, \dots, u^{n-1}\}$ 是 K 上向量空间 $K(u)$ 的基底.

(v) $K(u)$ 的每个元素可惟一地表示为 $a_0 + a_1u + \dots + a_{n-1}u^{n-1}$, $a_i \in$

K .

例 3 多项式 $x^2 - x - 1$ 是 $\mathbf{Q}$ 上的不可约多项式.

例 4 多项式 $x^3 - 3x - 1$ 是 $\mathbf{Q}$ 上的不可约多项式.

定理 5 设 $\sigma : \mathbf{K} \rightarrow \mathbf{L}$ 是域同构. 设 u 是 $\mathbf{K}$ 的某一扩域中的元素, v 是 $\mathbf{L}$ 的某一扩域中的元素. 假设

(i) u 是 $\mathbf{K}$ 上的超越元, v 是 $\mathbf{L}$ 上的超越元, 或者

(ii) u 是不可约多项式 $f \in \mathbf{K}[x]$ 的根, v 是不可约多项式 $\sigma f \in \mathbf{L}[x]$ 的根.

则 σ 可扩充为域同构 $\mathbf{K}(u) \cong \mathbf{L}(v)$, 并将 u 映到 v .

定理 6 设 $\mathbf{E}$ 和 $\mathbf{F}$ 都是域 $\mathbf{K}$ 的扩域, $u \in \mathbf{E}$ 以及 $v \in \mathbf{F}$. 则 u 和 v 是同一不可约多项式 $f \in \mathbf{K}[x]$ 的根当且仅当存在一个 $\mathbf{K}$ 的同构 $\mathbf{K}(u) \cong \mathbf{L}(v)$, 其将 u 映到 v .

定理 7 设 $\mathbf{K}$ 是一个域, $f \in \mathbf{K}[x]$ 是次数为 n 的多项式. 则存在 $\mathbf{K}$ 的单扩域 $\mathbf{F} = \mathbf{K}(u)$ 使得

(i) $u \in \mathbf{F}$ 是 f 的根.

(ii) $[\mathbf{K}(u) : \mathbf{K}] \leq n$, 等式成立当且仅当 f 是 $\mathbf{K}[x]$ 中的不可约多项式.

推论 设 $\mathbf{K}$ 是一个域, $f \in \mathbf{K}[x]$ 是次数为 n 的不可约多项式. 设 α 是 $f(x)$ 的根, 则 α 在 $\mathbf{K}$ 上生成的域为 $\mathbf{F} = \mathbf{K}(\alpha)$, 且 $[\mathbf{K}(\alpha) : \mathbf{K}] = n$.

定义 1 设 $\mathbf{E}$ 和 $\mathbf{F}$ 是 $\mathbf{K}$ 的扩域. 一个非零映射 $\sigma : \mathbf{E} \rightarrow \mathbf{F}$ 叫做 **$\mathbf{K}$ -同态**, 如果 σ 是在 $\mathbf{K}$ 上为恒等映射的域同态. 一个自同构 $\sigma : \mathbf{F} \rightarrow \mathbf{F}$ 叫做 **$\mathbf{K}$ -自同构**, 如果 σ 是 $\mathbf{K}$ -同态. $\mathbf{F}$ 的所有 $\mathbf{K}$ -自同构组成的群叫做 $\mathbf{F}$ 在 $\mathbf{K}$ 上的 **伽略华 (Galois) 群**, 记为 $Aut_{\mathbf{K}}\mathbf{F}$.

定理 1 设 $\mathbf{F}$ 是 $\mathbf{K}$ 的扩域, $f \in \mathbf{K}[x]$. 如果 $u \in \mathbf{F}$ 是 f 的根, $\sigma \in Aut_{\mathbf{K}}\mathbf{F}$, 则 $\sigma(u)$ 也是 f 的根.

证 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{K}[x]$. 对于 $u \in \mathbf{F}$ 及 $\sigma \in Aut_{\mathbf{K}}\mathbf{F}$, 我们有

$$\sigma f(u) = \sigma(a_n)\sigma(u)^n + \cdots + \sigma(a_1)\sigma(u) + \sigma(a_0) = a_n\sigma(u)^n + \cdots + a_1\sigma(u) + a_0 = f(\sigma(u)).$$

因此, 定理成立.

定理 2 设 $\mathbf{F}$ 是 $\mathbf{K}$ 的扩域, $\mathbf{E}$ 是中间域以及 H 是 $Aut_{\mathbf{K}}\mathbf{F}$ 的子群. 则

(i) $\mathbf{E}' = \{v \in \mathbf{F} \mid \sigma(v) = v, \sigma \in H\}$ 是扩域 $\mathbf{F}$ 的中间域.

(ii) $H' = \{\sigma \in Aut_{\mathbf{K}}\mathbf{F} \mid \sigma(u) = u, u \in \mathbf{E}\} = Aut_{\mathbf{E}}\mathbf{F}$ 是 $Aut_{\mathbf{K}}\mathbf{F}$ 的子群.

域 $\mathbf{E}'$ 叫做 H 在 $\mathbf{F}$ 中的不变域.

定义 2 设 $\mathbf{F}$ 是 $\mathbf{K}$ 的扩域. $\mathbf{F}$ 叫做 $\mathbf{K}$ - 的 Galois 扩张, 如果 Galois 群 $Aut_{\mathbf{K}}\mathbf{F}$ 的不变域是 $\mathbf{K}$.

定理 3 (Galois 论的基本定理) 如果 $\mathbf{F}$ 是 $\mathbf{K}$ 的有限维 Galois 扩张, 则在所有中间扩域集到 Galois 群 $Aut_{\mathbf{K}}\mathbf{F}$ 的所有子群集之间存在一个一一对应的映射 $\mathbf{E} \mapsto H' = Aut_{\mathbf{E}}\mathbf{F}$ 使得:

- (i) 两个中间域的 关维数等于对应子群的 关指 , 特别, $Aut_{\mathbf{K}}\mathbf{F}$ 有阶 $[\mathbf{F} : \mathbf{K}]$.
- (ii) $\mathbf{F}$ 是每个中间域 $\mathbf{E}$ 上的 Galois 域, 但 $\mathbf{E}$ 是 $\mathbf{K}$ 上的 Galois 域当且仅当对应的子群 $H' = Aut_{\mathbf{E}}\mathbf{F}$ 是 $G = Aut_{\mathbf{K}}\mathbf{F}$ 的正规子群, 在这个情况下, G/H' (同构意义下) 是 $\mathbf{E}$ 在 $\mathbf{K}$ 上的 Galois 群 $Aut_{\mathbf{K}}\mathbf{E}$.

定义 1 设 K 是一个域, $f \in K[x]$ 是次数 ≥ 1 的多项式. K 的一个扩域 F 叫做 **多项式 f 在 K 上的分裂域**, 如果 f 在 $F[x]$ 中可分解, 且 $F = K(u_1, \dots, u_n)$, 其中 $u_1, \dots, u_n$ 是 f 在 F 中的根.

设 S 是 $K[x]$ 中一些次数 ≥ 1 的多项式组成的集合. K 的一个扩域 F 叫做 **多项式集合 S 在 K 上的分裂域**, 如果 S 中的每个多项式 f 在 $F[x]$ 中可分解, 且 F 由 S 中的所有多项式的根在 K 上生成.

定理 1 设 $\mathbf{K}$ 是一个域, $f \in \mathbf{K}[x]$ 的次数为 $n \geq 1$. 则存在 f 一个分裂域 $\mathbf{F}$ 具有 $[\mathbf{F} : \mathbf{K}] \leq n!$.

定理 2 在域 $\mathbf{F}$ 上的如下条件等价:

- (i) 每个非常数多项式 $f \in \mathbf{F}[x]$ 在 $\mathbf{F}$ 中有根.
- (ii) 每个非常数多项式 $f \in \mathbf{F}[x]$ 在 $\mathbf{F}$ 中可分解.
- (iii) 每个不可约多项式 $f \in \mathbf{F}[x]$ 的次数为一.
- (iv) 不存在 $\mathbf{F}$ 的代数扩张 (除了 $\mathbf{F}$ 自己以外).

定义 2 设 $\mathbf{F}$ 是一个域. $\mathbf{F}$ 叫做代数闭包, 如果域 $\mathbf{F}$ 满足定理 2 的等价条件.

第十二章 域的结构

定义 1 设 F 是域 K 的扩域, $a_1, a_2, \dots, a_n$ 是 F 的一个 n 个元素. $a_1, a_2, \dots, a_n$ 叫做在 K 上 **代数相关**, 如果存在一个非零多项式 $f \in K[x_1, \dots, x_n]$ 使得对于 S 的 n 个不同元素 $a_1, a_2, \dots, a_n$, 有

$$f(a_1, a_2, \dots, a_n) = 0.$$

$a_1, a_2, \dots, a_n$ 叫做 **代数无关**, 如果 $a_1, a_2, \dots, a_n$ 不是代数 关.

注 所谓 $a_1, a_2, \dots, a_n$ 代数无关, 如果有多项式 $f \in K[x_1, \dots, x_n]$ 使得 $f(a_1, a_2, \dots, a_n) = 0$, 则 $f = 0$.

例 1 圆周率 $\pi = 3.14 \cdots$ 在 $\mathbf{Q}$ 上代数无关, 自然对数底 $e = 2.718 \cdots$ 在 $\mathbf{Q}$ 上也代数无关.

定理 1 设 F 是域 K 的有限生成扩域, 则 F 是 K 的代数扩张或者存在代数无关元 $\theta_1, \dots, \theta_t$ 使得 F 是 $K(\theta_1, \dots, \theta_t)$ 的代数扩张.

设 $\mathbf{F}_q$ 是 q 元有限域, 其特征 p 为素数. 则 $\mathbf{F}_q$ 包含素域 $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, 是 $\mathbf{F}_p$ 上的有限维线性空间. 设 $n = [\mathbf{F}_q : \mathbf{F}_p]$, 则 $q = p^n$, 即 q 是其特征 p 的幂.

我们要证明: $\mathbf{F}_q^* = \mathbf{F}_q \setminus \{0\}$ 是 $q - 1$ 阶循环乘群. 为此, 我们先讨论 $\mathbf{F}_q^*$ 的一些性质.

定理 1 $\mathbf{F}_q^*$ 的任意元 a 的阶整除 $q - 1$.

定义 1 有限域 $\mathbf{F}_q$ 的元素 g 叫做 **生成元**, 如果它是 $\mathbf{F}_q^*$ 的生成元, 即阶为 $q - 1$ 的元素.

当 g 是 $\mathbf{F}_q$ 的生成元时, 有 $\mathbf{F}_q = \{0, g^0 = 1, g, \dots, g^{q-2}\}$.

定理 2 每个有限域都有生成元. 如果 g 是 $\mathbf{F}_q$ 的生成元, 则 g^d 是 $\mathbf{F}_q$ 的生成元的当且仅当 d 和 $q-1$ 的最大公因数 $(d, q-1) = 1$. 特别地, $\mathbf{F}_q$ 有 $\varphi(q-1)$ 个生成元.

推论 1 设 $q = p^n$, p 为素数, $d|q-1$, 则有限域 $\mathbf{F}_q$ 中有阶为 d 的元素.

推论 2 设 p 为素数, 则存在整数 g 遍历模 p 的简化剩余系, 即存在模 p 原根.

定理 3 如果 $\mathbf{F}_q$ 是 $q = p^n$ 元域, 则其每个元素满足方程 $x^q - x = 0$. 更确切地说, $\mathbf{F}_q$ 是这个方程的根集合. 反过来, 对每个素数幂 $q = p^n$, 多项式 $x^q - x$ 在 $\mathbf{F}_p$ 上的分裂域是 q 元域.

定理 4 设 $\mathbf{F}_q$ 是 $q = p^n$ 元有限域, 设 σ 是 $\mathbf{F}_q$ 到自身的映射, $\sigma : a \longmapsto a^p$. 则 σ 是 $\mathbf{F}_q$ 的自同构, 且 $\mathbf{F}_q$ 中在 σ 下的不动元是素域 $\mathbf{F}_p$ 的元素, 而 σ 的 n 次幂是恒等映射.

定 4 中的映射 σ 叫做 **Frobenius 自同态**.

定理 5 设 $\mathbf{F}_q$ 是 $q = p^n$ 元有限域, 设 σ 是 $\mathbf{F}_q$ 到自身的映射, $\sigma : a \longmapsto a^p$. 如果 α 是 $\mathbf{F}_q$ 的任意元, 则 α 在 $\mathbf{F}_p$ 上的共轭元是元素 $\sigma^j(\alpha) = \alpha^{p^j}$.

有限域的具体构造. 应用 §10.4 定理 4, 我们可以具体构造素域 $\mathbf{F}_p$ 上的 d 次代数扩张.

取 $p(x)$ 为 $\mathbf{F}_p[X]$ 中的 d 次首一不可约多项式, 在商环 $\mathbf{F}_p[x]/(p(x))$ 上定义加法:

$$f(x) + g(x) = ((f + g)(x) \pmod{p(x)}),$$

和乘法:

$$f(x)g(x) = ((fg)(x) \pmod{p(x)}).$$

则 $\mathbf{F}_p[x]/(p(x))$ 对于上述运算法则构成一个域. 根据 §11.1 定理 2, 这个域在 $\mathbf{F}_p$ 上是 d 次扩张. 我们记这个域为 $\mathbf{F}_q$ 或 $GF(q)$, 其中 $q = p^d$.

$\mathbf{F}_2/(x^4 + x + 1)$ 的生成元是 x ,

例 1 证明 x^4+x+1 是 $\mathbf{F}_2[x]$ 中的不可约多项式, 从而 $\mathbf{F}_2[x]/(x^4+x+1)$ 是一个 $\mathbf{F}_{2^4}$ 域.

因为 $\mathbf{F}_2[x]$ 中的所有次数 ≤ 2 的不可约多项式为 $x, x+1, x^2+x+1$, 且

$$x^4+x+1 = x(x^3+1)+1, \quad x^4+x+1 = (x+1)(x^3+x^2+x)+1,$$

$$x^4+x+1 = (x^2+x+1)(x^2+x)+1,$$

所以 $x \nmid x^4+x+1, x+1 \nmid x^4+x+1, x^2+x+1 \nmid x^4+x+1$. 这说明, x^4+x+1 是 $\mathbf{F}_2[x]$ 中的不可约多项式. 因此, $\mathbf{F}_2[x]/(x^4+x+1)$ 是一个 $\mathbf{F}_{2^4}$ 域.

例 2 求 $\mathbf{F}_{2^4} = \mathbf{F}_2[x]/(x^4 + x + 1)$ 中的生成元 $g(x)$, 并计算 $g(x)^t$, $t = 0, 1, \dots, 14$ 和所有生成元.

解 因为 $|\mathbf{F}_{2^4}^*| = 15 = 3 \cdot 5$, 所以满足

$$g(x)^3 \not\equiv 1 \pmod{x^4 + x + 1}, \quad g(x)^5 \not\equiv 1 \pmod{x^4 + x + 1}$$

的元素 $g(x)$ 都是生成元.

对于 $g(x) = x$, 有

$$x^3 \equiv x^3 \not\equiv 1 \pmod{x^4 + x + 1}, \quad x^5 \equiv x^2 + x \not\equiv 1 \pmod{x^4 + x + 1},$$

所以 $g(x) = x$ 是 $\mathbf{F}_2[x]/(x^4 + x + 1)$ 的生成元.

对于 $t = 0, 1, 2, \dots, 14$, 计算 $g(x)^t \pmod{x^4 + x + 1}$:

$$\begin{aligned}
 g(x)^0 &\equiv 1, & g(x)^1 &\equiv x, & g(x)^2 &\equiv x^2, \\
 g(x)^3 &\equiv x^3, & g(x)^4 &\equiv x + 1, & g(x)^5 &\equiv x^2 + x, \\
 g(x)^6 &\equiv x^3 + x^2, & g(x)^7 &\equiv x^3 + x + 1, & g(x)^8 &\equiv x^2 + 1, \\
 g(x)^9 &\equiv x^3 + x, & g(x)^{10} &\equiv x^2 + x + 1, & g(x)^{11} &\equiv x^3 + x^2 + x, \\
 g(x)^{12} &\equiv x^3 + x^2 + x + 1, & g(x)^{13} &\equiv x^3 + x^2 + 1, & g(x)^{14} &\equiv x^3 + 1.
 \end{aligned}$$

所有生成元为 $g(x)^t$, $(t, \varphi(15)) = 1$:

$$\begin{aligned}
 g(x)^1 &= x, & g(x)^2 &= x^2, & g(x)^4 &= x + 1, \\
 g(x)^7 &= x^3 + x + 1, & g(x)^8 &= x^2 + 1, & g(x)^{11} &= x^3 + x^2 + x, \\
 g(x)^{13} &= x^3 + x^2 + 1, & g(x)^{14} &= x^3 + 1.
 \end{aligned}$$

例 3 求 $\mathbf{F}_{2^8} = \mathbf{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$ 中的生成元 $g(x)$.

解 因为 $|\mathbf{F}_{2^8}^*| = 255 = 3 \cdot 5 \cdot 17$, 所以满足

$$g(x)^{15} \not\equiv 1, \quad g(x)^{51} \not\equiv 1, \quad g(x)^{85} \not\equiv 1 \pmod{x^8 + x^4 + x^3 + x + 1}$$

的元素 $g(x)$ 都是生成元.

对于 $g_1(x) = x$, 有

$$\begin{aligned} g_1(x)^{15} &\equiv x^5 + x^3 + x^2 + x + 1, & g_1(x)^{51} &\equiv 1, \\ g_1(x)^{85} &\equiv x^7 + x^5 + x^4 + x^3 + x^2 + 1 \pmod{x^8 + x^4 + x^3 + x + 1}. \end{aligned}$$

因此, $g_1(x) = x$ 不是 $\mathbf{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$ 中的生成元.

对于 $g_2(x) = x + 1$, 有

$$g_2(x)^2 \equiv x^2 + 1,$$

$$g_2(x)^4 \equiv x^4 + 1,$$

$$g_2(x)^8 \equiv x^4 + x^3 + x,$$

$$g_2(x)^{16} \equiv x^6 + x^4 + x^3 + x^2 + x + 1,$$

$$g_2(x)^{48} \equiv x^6 + x^4 + x + 1,$$

$$g_2(x)^{83} \equiv x^7 + x^6 + x^4,$$

$$g_2(x)^3 \equiv x^3 + x^2 + x + 1,$$

$$g_2(x)^7 \equiv x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1,$$

$$g_2(x)^{15} \equiv x^5 + x^4 + x^2 + 1,$$

$$g_2(x)^{32} \equiv x^7 + x^6 + x^5 + x^2 + 1,$$

$$g_2(x)^{51} \equiv x^3 + x^2,$$

$$g_2(x)^{85} \equiv x^7 + x^5 + x^4 + x^3 + x^2 + 1.$$

因此,

$$g_2(x)^{15} \not\equiv 1, \quad g_2(x)^{51} \not\equiv 1, \quad g_2(x)^{85} \not\equiv 1 \pmod{x^8 + x^4 + x^3 + x + 1}.$$

$g_2(x) = x + 1$ 是 $\mathbf{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$ 中的生成元.

定理 6 $\mathbf{F}_{p^n}$ 的子域为 $\mathbf{F}_{p^d}$, $(d|n)$, 它是 $\mathbf{F}_{p^n}$ 中的元素在 $\mathbf{F}_p$ 上生成的域.

定理 7 对任意 $q = p^n$, 多项式 $x^q - x$ 可在 $\mathbf{F}_p[x]$ 中分解成首一不可约多项式的乘积, 且每个多项式的次数 $d|n$.

推论 如果 n 是素数, 则 $\mathbf{F}_{p^n}[x]$ 中有 $\frac{p^n - p}{n}$ 个不同的次数为 n 的首一不可约多项式的乘积.

定理 8 设 p, r 都是素数. 则在 $\mathbf{F}_p$ 上, 多项式 $\frac{x^r - 1}{x - 1}$ 可分解为次数为 $\text{ord}_r(p)$ 的不可约多项式的乘积.

第十三章 椭圆曲线

设 $\mathbf{K}$ 是一个域. 域 $\mathbf{K}$ 上的 Weierstrass 方程是

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (1)$$

其中 $a_1, a_2, a_3, a_4, a_6 \in \mathbf{K}$.

当域 $\mathbf{K}$ 的特征不为 2 时, 上述方程可变形为

$$(y + \frac{1}{2}a_1x + \frac{1}{2}a_3)^2 = x^3 + (\frac{1}{4}a_1^2 + a_2)x^2 + (\frac{1}{2}a_1a_3 + a_4)x + \frac{1}{4}a_3^2 + a_6$$

或 $(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$

$$\text{其中} \quad \begin{cases} b_2 = a_1^2 + 4a_2, \\ b_4 = a_1a_3 + 2a_4, \\ b_6 = a_3^2 + 4a_6. \end{cases} \quad (2)$$

当域 $\mathbf{K}$ 的特征不为 2, 3 时, 方程可继续变形, 有

$$(2y + a_1x + a_3)^2 = 4(x + \frac{1}{12}b_2)^3 + (-\frac{1}{12}b_2^2 + 2b_4)(x + \frac{1}{12}b_2) + (\frac{1}{216}b_2^3 - \frac{1}{6}b_2b_4 + b_6),$$

$$\text{或 } 108^2(2y + a_1x + a_3)^2 = 36^3(x + \frac{1}{12}b_2)^3 - 27c_4 \cdot 36(x + \frac{1}{12}b_2) - 54c_6,$$

$$\text{其中 } \begin{cases} c_4 = b_2^2 - 24b_4, \\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \end{cases} \quad (3)$$

作变换

$$\begin{cases} X = 36(x + \frac{1}{12}b_2) \\ Y = 108(2y + a_1x + a_3) \end{cases} \quad \text{或} \quad \begin{cases} x = \frac{1}{36}X - \frac{1}{12}b_2 \\ y = \frac{1}{216}Y - \frac{1}{2}a_1(\frac{1}{36}X - \frac{1}{12}b_2) - \frac{1}{2}a_3, \end{cases}$$

$$\text{得到 } Y^2 = X^3 - 27c_4X - 54c_6. \quad (4)$$

$$\text{其判别式为 } 1728\Delta = c_4^3 - c_6^2.$$

对于任意域 $\mathbf{K}$, Weierstrass 方程 (1) 的判别式是

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6, \quad (5)$$

其中

$$b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2 \quad (i.e. \ 4b_8 = b_2 b_6 - b_4^2). \quad (6)$$

定义 1 当 $\Delta \neq 0$, 域 $\mathbf{K}$ 上的点集

$$E := \{(x, y) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\},$$

其中 $a_1, a_2, a_3, a_4, a_6 \in \mathbf{K}$, $\{O\}$ 为无穷远点, 叫做域 $\mathbf{K}$ 上的 **椭圆曲线**. 这时, $j = c_4^3/\Delta$ 叫做椭圆曲线 E 的 **j -不变量**, 记作 $j(E)$.

我们将 Weierstrass 方程写成齐次形式:

$$Y^2Z + a_1XYZ + a_3Y = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \quad (8)$$

其中 $a_1, a_2, a_3, a_4, a_6 \in \mathbf{K}$. 则定义 1 中的无穷远点 O 就是齐次坐点 $[0 : 1 : 0]$.

在对域 $\mathbf{K}$ 上椭圆曲线 E 的研究中, 我们通常取如下形式的 Weierstrass 方程:

(i) 当域 $\mathbf{K}$ 的特征不为 2, 3 时, Weierstrass 方程为

$$y^2 = x^3 + a_4x + a_6, \quad \Delta = -16(4a_4^3 + 27a_6^2), \quad j = 1728 \frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

(ii) 当域 $\mathbf{K}$ 的特征为 2, 且 $j(E) \neq 0$ 时, Weierstrass 方程为

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad \Delta = a_6, \quad j = 1/a_6.$$

(iii) 当域 $\mathbf{K}$ 的特征为 2, 且 $j(E) = 0$ 时, Weierstrass 方程为

$$y^2 + a_3y = x^3 + a_4x + a_6, \quad \Delta = a_3^4, \quad j = 0.$$

(iv) 当域 $\mathbf{K}$ 的特征为 3, 且 $j(E) \neq 0$ 时, Weierstrass 方程为

$$y^2 = x^3 + a_2x^2 + a_6, \quad \Delta = -a_2^3a_6, \quad j = -a_2^3/a_6.$$

(v) 当域 $\mathbf{K}$ 的特征为 3 , 且 $j(E) = 0$ 时, Weierstrass 方程为

$$y^2 = x^3 + a_4x + a_6, \quad \Delta = -a_4^3, \quad j = 0.$$

设 E 是由 Weierstrass 方程 (7) 定义的域 $\mathbf{K}$ 上椭圆曲线, 我们定义 E 上的运算法则, 记作 $\oplus$.

运算法则 设 P, Q 是 E 上的两个点, L 是过 P 和 Q 的直线 (过 P 点的切线, 如果 $P = Q$), R 是 L 与曲线 E 交的第三点. 设 L' 是过 R 和 O 的直线. 则 $P \oplus Q$ 就是 L' 与 E 交的第三点.

定理 1 E 上运算法则 $\oplus$ 具有如下性质:

(i) 如果直线 L 交 E 于点 P, Q, R (不必是不同的), 则

$$(P \oplus Q) \oplus R = O.$$

(ii) 对任意 $P \in E$, $P \oplus O = P$.

(iii) 对任意 $P, Q \in E$, $P \oplus Q = Q \oplus P$.

(iv) 设 $P \in E$, 存在一个点, 记作 $-P$, 使得 $P \oplus (-P) = O$.

(v) 对任意 $P, Q, R \in E$, 有 $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

这就是说, E 对于运算规则 $\oplus$ 构成一个交换群.

更进一步, 如果 E 定义在 K 上, 则

$$E(\mathbf{K}) := \{(x, y) \in \mathbf{K} \times \mathbf{K} \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}, \quad (9)$$

是 E 的子群.

现在我们给出定 1 中群运算的精确公式.

定理 2 设椭圆曲线 E 的一般 Weierstrass 方程为:

$$E := \{(x, y) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}.$$

设 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ 是曲线 E 上的两个点. 则

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3).$$

$$\text{取 } \begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{如果 } x_1 = x_2. \end{cases}$$

如果 $P_3 = (x_3, y_3) = P_1 + P_2 \neq O$, 则 x_3, y_3 可以由公式给出

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - a_1x_3 - y_1 - a_3. \end{cases}$$

证 设 E 是由方程 $F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ 定义的椭圆曲线.

(I) 设 $P_1 = (x_1, y_1) \in E$, 计算点 $-P_1$. 设 L 是过 P_1 和 O 的直线, 则该直线为 $L: x - x_1 = 0$.

将 $x = x_1$ 代入到 $F(x, y)$ 中, 并求关于 y 的两个根 y_1, y'_1 . 比较下列方程关于一次项 y 的系数,

$$F(x_1, y) = (y - y_1)(y - y'_1) = y^2 - (y_1 + y'_1)y + y_1y'_1,$$

有 $y'_1 = -y_1 - a_1x_1 - a_3$, 从而 $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$.

(II) 设 $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$. 如果 $P_1 + P_2 \neq O$, 考虑过 P_1 和 P_2 的直线 $L: y = \lambda x + \mu$.

当 $x_1 \neq x_2$ 时, 直线 L 的斜率 λ 为 $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

当 $x_1 = x_2$ 时, 直线 L 为过点 P 的切线, 其斜率 λ 为

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

将 $y = \lambda x + \mu$ 代入方程 $F(x, y) = 0$ 中, 有

$$F(x, \lambda x + \mu) = -x^3 + (\lambda^2 + a_1\lambda - a_2)x^2 + (2\lambda\mu + a_1\mu - a_4)x + \mu^2 - a_6 = 0.$$

因为 P_1, P_2 和 P_3 是 E 上三个点, 所以上述方程关于 x 有三个解 x_1, x_2, x_3 . $F(x, \lambda x + \mu) = c(x - x_1)(x - x_2)(x - x_3)$.

因此, 有 $c = -1$ 及 $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$. $\mu = y_1 - \lambda x_1$, 故

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - a_1x_3 - y_1 - a_3. \end{cases}$$

实数域 $\mathbf{R}$ 上椭圆曲线及其运算法则的 何意义.

因为 $\text{chap}(\mathbf{R}) \neq 2, 3$, 所以 $\mathbf{R}$ 上椭圆曲线 E 的 Weierstrass 方程可设为 $E: y^2 = x^3 + a_4x + a_6$,

其判别式 $\Delta = -16(4a_4^3 + 27a_6^2) \neq 0$. E 在 $\mathbf{R}$ 上的运算规则为:

设 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ 是曲线 E 上的两个点, O 为无穷远点. 则

$$(1) O + P_1 = P_1 + O; \quad (2) -P_1 = (x_1, -y_1);$$

$$(3) \text{ 如果 } P_3 = (x_3, y_3) = P_1 + P_2 \neq O,$$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1. \end{cases} \quad \text{其中} \begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \frac{3x_1^2 + a_4}{2y_1} & \text{如果 } x_1 = x_2. \end{cases}$$

运算法则的 何意义是:

设 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ 是曲线 E 上的两个点, O 为无穷远点.

则 $-P_1$ 为过点 P_1 和点 O 的直线 L 与曲线 E 的交点, 换句话说, $-P_1$ 是点 P_1 关于 x 轴的对称点.

而点 P_1 与点 P_2 的和 $P_1 + P_2 = P_3 = (x_3, y_3)$ 是过点 P_1 和点 P_2 的直线 L 与曲线 E 的交点 R 关于 x 轴的对称点 $P_3 = -R$.

素域 $\mathbf{F}_p$ ($p > 3$) 上椭圆曲线 E .

因为素域 $\mathbf{F}_p$ 的特征不为 2, 3, 所以素域 $\mathbf{F}_p$ 上椭圆曲线 E 的 Weierstrass 方程可设为 $E: y^2 = x^3 + a_4x + a_6$,

其判别式 $\Delta = -16(4a_4^3 + 27a_6^2) \neq 0$. E 在 $\mathbf{R}$ 上的运算规则为:

设 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ 是曲线 E 上的两个点, O 为无穷远点. 则

$$(1) O + P_1 = P_1 + O; \quad (2) -P_1 = (x_1, -y_1);$$

$$(3) \text{ 如果 } P_3 = (x_3, y_3) = P_1 + P_2 \neq O,$$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1. \end{cases} \quad \text{其中} \begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \frac{3x_1^2 + a_4}{2y_1} & \text{如果 } x_1 = x_2. \end{cases}$$

例 1 设 $\mathbf{F}_{17}$ 上椭圆曲线 $E: y^2 = x^3 + 2x + 3$, 求出该椭圆曲线的全部点以及阶.

解 对 $x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$, 分别求出 y .

$$x = 0, y^2 = 3 \pmod{17}, \quad \text{无解,}$$

$$x = 1, y^2 = 6 \pmod{17}, \quad \text{无解,}$$

$$x = 2, y^2 = 15 \pmod{17}, \quad y = 7, 8 \pmod{17},$$

$$x = 3, y^2 = 2 \pmod{17}, \quad y = 6, 11 \pmod{17},$$

$$x = 4, y^2 = 7 \pmod{17}, \quad \text{无解,}$$

$$x = 5, y^2 = 2 \pmod{17}, \quad y = 6, 11 \pmod{17},$$

$$x = 6, y^2 = 10 \pmod{17}, \quad \text{无解,}$$

$$x = 7, y^2 = 3 \pmod{17}, \quad \text{无解,}$$

$$\begin{aligned}
x = 8, \quad y^2 &= 4 \pmod{17}, \quad y = 2, 15 \pmod{17}, \\
x = 9, \quad y^2 &= 2 \pmod{17}, \quad y = 6, 11 \pmod{17}, \\
x = 10, \quad y^2 &= 3 \pmod{17}, \quad \text{无解}, \\
x = 11, \quad y^2 &= 13 \pmod{17}, \quad y = 8, 9 \pmod{17}, \\
x = 12, \quad y^2 &= 4 \pmod{17}, \quad y = 2, 15 \pmod{17}, \\
x = 13, \quad y^2 &= 16 \pmod{17}, \quad y = 4, 13 \pmod{17}, \\
x = 14, \quad y^2 &= 4 \pmod{17}, \quad y = 2, 15 \pmod{17}, \\
x = 15, \quad y^2 &= 8 \pmod{17}, \quad y = 5, 12 \pmod{17}, \\
x = 16, \quad y^2 &= 0 \pmod{17}, \quad y = 0 \pmod{17}.
\end{aligned}$$

椭圆曲线的阶为

$$\#(E(\mathbf{F}_{17})) = 1 + \sum_{x=0}^{17-1} \left(\frac{x^3 + 2x + 3}{17} \right) = 22.$$

例 2 设 $\mathbf{F}_{17}$ 上椭圆曲线 $E: y^2 = x^3 + 2x + 3$ 上的点 $P = (2, 7)$, $Q = (11, 8)$. 求 $P + Q = (x_3, y_3)$, $2P = (x_4, y_4)$, $4P = (x_5, y_5)$, $8P = (x_6, y_6)$, $10P = (x_7, y_7)$, $11P = (x_8, y_8)$, $22P$.

解 令 $x_1 = 2$, $y_1 = 7$, $x_2 = 11$, $y_2 = 8$, 则 $\lambda_1 = \frac{y_2 - y_1}{x_2 - x_1} = 2$,

$$x_3 = \lambda_1^2 - x_1 - x_2 = 8, \quad y_3 = \lambda_1(x_1 - x_3) - y_1 = 15$$

$$\lambda_2 = \frac{3x_1^2 + a_4}{2y_1} = 1,$$

$$x_4 = \lambda_2^2 - 2x_1 = 14, \quad y_4 = \lambda_2(x_1 - x_4) - y_1 = 15$$

$$\lambda_3 = \frac{3x_4^2 + a_4}{2y_4} = 14,$$

$$x_5 = \lambda_3^2 - 2x_4 = 15, \quad y_5 = \lambda_3(x_4 - x_5) - y_4 = 5$$

$$\lambda_4 = \frac{3x_5^2 + a_4}{2y_5} = 15,$$

$$x_6 = \lambda_4^2 - 2x_5 = 8, \quad y_6 = \lambda_4(x_5 - x_6) - y_5 = 15$$

$$\lambda_5 = \frac{y_6 - y_4}{x_6 - x_4} = 0,$$

$$x_7 = \lambda_5^2 - x_4 - x_6 = 12, \quad y_7 = \lambda_5(x_4 - x_7) - y_4 = 2$$

$$\lambda_6 = \frac{y_7 - y_1}{x_7 - x_1} = 8,$$

$$x_8 = \lambda_6^2 - x_1 - x_7 = 16, \quad y_8 = \lambda_6(x_1 - x_8) - y_1 = 0$$

因为过点 $11P = (x_8, y_8) = (16, 0)$ 的切线垂直于 x 轴, 所以 $22P = 2(11P) = O$ (无穷远点).

例 3 设 $\mathbf{F}_{17}$ 上椭圆曲线 $E: y^2 = x^3 + 3x + 1$, 求出该椭圆曲线的全部点以及阶.

解 对 $x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$, 分别求出 y .

$$x = 0, y^2 = 1 \pmod{17}, \quad y = 1, 16 \pmod{17},$$

$$x = 1, y^2 = 5 \pmod{17}, \quad \text{无解},$$

$$x = 2, y^2 = 15 \pmod{17}, \quad y = 7, 8 \pmod{17},$$

$$x = 3, y^2 = 3 \pmod{17}, \quad \text{无解},$$

$$x = 4, y^2 = 9 \pmod{17}, \quad y = 3, 14 \pmod{17},$$

$$x = 5, y^2 = 5 \pmod{17}, \quad \text{无解},$$

$$x = 6, y^2 = 14 \pmod{17}, \quad \text{无解},$$

$$x = 7, y^2 = 8 \pmod{17}, \quad y = 5, 12 \pmod{17},$$

$$x = 8, y^2 = 10 \pmod{17}, \quad \text{无解},$$

$$x = 9, y^2 = 9 \pmod{17}, \quad y = 3, 14 \pmod{17},$$

$$x = 10, y^2 = 11 \pmod{17}, \quad \text{无解},$$

$$x = 11, y^2 = 5 \pmod{17}, \quad \text{无解},$$

$$x = 12, y^2 = 14 \pmod{17}, \quad \text{无解},$$

$$x = 13, y^2 = 10 \pmod{17}, \quad \text{无解},$$

$$x = 14, y^2 = 16 \pmod{17}, \quad y = 4, 13 \pmod{17},$$

$$x = 15, y^2 = 4 \pmod{17}, \quad y = 2, 15 \pmod{17},$$

$$x = 16, y^2 = 14 \pmod{17}, \quad \text{无解}.$$

椭圆曲线的阶为

$$\#(E(\mathbf{F}_{17})) = 1 + \sum_{x=0}^{17-1} \left(\frac{x^3 + 3x + 1}{17} \right) = 15.$$

例 4 设 $\mathbf{F}_{17}$ 上椭圆曲线 $E : y^2 = x^3 + 3x + 1$ 上的点 $P = (2, 7)$. 求 $2P = (x_2, y_2)$, $3P = (x_3, y_3)$, $4P = (x_4, y_4)$, $5P = (x_5, y_5)$. $6P = (x_6, y_6)$, $7P = (x_7, y_7)$, $8P = (x_8, y_8)$, $9P = (x_9, y_9)$, $10P = (x_{10}, y_{10})$, $11P = (x_{11}, y_{11})$, $12P = (x_{12}, y_{12})$, $13P = (x_{13}, y_{13})$, $14P = (x_{14}, y_{14})$.

解 令 $x_1 = 2$, $y_1 = 7$, 则 $\lambda_2 = \frac{3x_1^2 + a_4}{2y_1} = 12$,

$$x_2 = \lambda_2^2 - 2x_1 = 4, \quad y_2 = \lambda_2(x_1 - x_2) - y_1 = 3$$

$$\lambda_3 = \frac{y_2 - y_1}{x_2 - x_1} = 15,$$

$$x_3 = \lambda_3^2 - x_1 - x_2 = 15, \quad y_3 = \lambda_3(x_1 - x_3) - y_1 = 2$$

$$\lambda_4 = \frac{3x_2^2 + a_4}{2y_2} = 0,$$

$$x_4 = \lambda_4^2 - 2x_2 = 9, \quad y_4 = \lambda_4(x_2 - x_4) - y_2 = 14$$

$$\lambda_5 = \frac{y_4 - y_1}{x_4 - x_1} = 1,$$

$$x_5 = \lambda_5^2 - x_1 - x_4 = 7, \quad y_5 = \lambda_5(x_1 - x_5) - y_1 = 5$$

$$\lambda_6 = \frac{y_4 - y_2}{x_4 - x_2} = 9,$$

$$x_6 = \lambda_6^2 - x_2 - x_4 = 0, \quad y_6 = \lambda_6(x_2 - x_6) - y_2 = 16$$

$$\lambda_7 = \frac{y_6 - y_1}{x_6 - x_1} = 4,$$

$$x_7 = \lambda_7^2 - x_1 - x_6 = 14, \quad y_7 = \lambda_7(x_1 - x_7) - y_1 = 13$$

$$\lambda_8 = \frac{3x_4^2 + a_4}{2y_4} = 10,$$

$$x_8 = \lambda_8^2 - 2x_4 = 14, \quad y_8 = \lambda_8(x_4 - x_8) - y_4 = 4$$

$$\lambda_9 = \frac{y_8 - y_1}{x_8 - x_1} = 4,$$

$$x_9 = \lambda_9^2 - x_1 - x_8 = 0, \quad y_9 = \lambda_9(x_1 - x_9) - y_1 = 1$$

$$\lambda_{10} = \frac{y_8 - y_2}{x_8 - x_2} = 12,$$

$$x_{10} = \lambda_{10}^2 - x_2 - x_8 = 7, \quad y_{10} = \lambda_{10}(x_2 - x_{10}) - y_2 = 12$$

$$\lambda_{11} = \frac{y_{10} - y_1}{x_{10} - x_1} = 1,$$

$$x_{11} = \lambda_{11}^2 - x_1 - x_{10} = 9, \quad y_{11} = \lambda_{11}(x_1 - x_{11}) - y_1 = 3$$

$$\lambda_{12} = \frac{y_8 - y_4}{x_8 - x_4} = 15,$$

$$x_{12} = \lambda_{12}^2 - x_4 - x_8 = 15, \quad y_{12} = \lambda_{12}(x_4 - x_{12}) - y_4 = 15$$

$$\lambda_{13} = \frac{y_{12} - y_1}{x_{12} - x_1} = 15,$$

$$x_{13} = \lambda_{13}^2 - x_1 - x_{12} = 4, \quad y_{13} = \lambda_{13}(x_1 - x_{13}) - y_1 = 14$$

$$\lambda_{14} = \frac{y_{12} - y_2}{x_{12} - x_2} = 15,$$

$$x_{14} = \lambda_{14}^2 - x_2 - x_{12} = 2, \quad y_{14} = \lambda_{14}(x_2 - x_{14}) - y_2 = 10$$

最后, $14P = -P, 15P = O$ (无穷远点).

域 $\mathbf{F}_{2^n}$ ($n \geq 1$) 上椭圆曲线 E , $j(E) \neq 0$.

因为域 $\mathbf{F}_{2^n}$ 的特征为 2, 所以域 $\mathbf{F}_{2^n}$ 上椭圆曲线 E 的 Weierstrass 方程可设为 $E: y^2 + xy = x^3 + a_2x^2 + a_6$.

E 在域 $\mathbf{F}_{2^n}$ 上的运算规则为:

设 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ 是曲线 E 上的两个点, O 为无穷远点. 则

$$(1) O + P_1 = P_1 + O; \quad (2) -P_1 = (x_1, x_1 + y_1);$$

$$(3) \text{ 如果 } P_3 = (x_3, y_3) = P_1 + P_2 \neq O,$$

$$\begin{cases} x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2, \\ y_3 = \lambda(x_1 + x_3) + x_3 + y_1. \end{cases} \quad \text{其中} \begin{cases} \lambda = \frac{y_2 + y_1}{x_2 + x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \frac{x_1^2 + y_1}{x_1} & \text{如果 } x_1 = x_2. \end{cases}$$

域 $\mathbf{F}_{3^n}$ ($n \geq 1$) 上椭圆曲线 E , $j(E) \neq 0$.

因为域 $\mathbf{F}_{3^n}$ 的特征为 3, 所以域 $\mathbf{F}_{3^n}$ 上椭圆曲线 E 的 Weierstrass 方程可设为 $E: y^2 = x^3 + a_2x^2 + a_6$.

E 在域 $\mathbf{F}_{3^n}$ 上的运算规则为:

设 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ 是曲线 E 上的两个点, O 为无穷远点. 则

$$(1) O + P_1 = P_1 + O; \quad (2) -P_1 = (x_1, -y_1);$$

$$(3) \text{ 如果 } P_3 = (x_3, y_3) = P_1 + P_2 \neq O,$$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 - a_2, \\ y_3 = \lambda(x_1 - x_3) - y_1. \end{cases} \quad \text{其中} \begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \frac{3x_1^2 + 2a_2x_1}{2y_1} & \text{如果 } x_1 = x_2. \end{cases}$$

设 $\mathbf{K} = \mathbf{F}_q$ 是 $q = p^n$ 元有限域. 设 E 是定义在 $\mathbf{F}_q$ 上的椭圆曲线. 当 $p > 3$ 时, 其 Weierstrass 方程为

$$y^2 = x^3 + a_4x + a_6.$$

易知, $\mathbf{F}_q$ 上椭圆曲线 E 中的点数 $\#(E(\mathbf{F}_q)) \leq 2q + 1$. 事实上, 对每个 $x \in \mathbf{F}_q$, 至多有两个 $y \in \mathbf{F}_q$ 使得 $P(x, y) \in E$, 再加上无穷远点 O , 我们有 $\#(E) \leq 2|\mathbf{F}_q| + 1 = 2q + 1$.

$$\begin{aligned} \varphi : \quad \overline{\mathbf{F}}_q &\longrightarrow \overline{\mathbf{F}}_q \\ \text{考虑 } \mathbf{F}_q \text{ 上椭圆曲线 } E \text{ 上的映射: } \quad (x, y) &\longmapsto (x^q, y^q) \\ O &\longmapsto O \end{aligned}$$

φ 叫做 q 次幂 **Frobenius 映射**. 易知, φ 将 E 上的点映到 E , 且保持群的运算法则. 这就是说, φ 是 $\mathbf{F}_q$ 上 E 的群同态, 因此, φ 又叫做 q 次幂 **Frobenius 自同态**.

Frobenius 自同态 φ 与其迹 (trace) 在椭圆曲线的研究中起着重要作用. 它们由如下方程联系: $\varphi^2 - [t]\varphi + [q] = [0]$, 也就是, 对椭圆曲线 E 上任意点 $P = (x, y)$, 我们有

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = O.$$

此外, 我们有 $\#(E(\mathbf{F}_q)) = q + 1 - t$.

第一个关于 $E(\mathbf{F}_q)$ 的阶的逼近估计是由下面的 Hasse 定理给出.

定理 1(Hasse). 设 E 是定义在 $\mathbf{F}_q$ ($q = p^n$, p 素数) 上的椭圆曲线, φ_q 次幂 Frobenius 自同态 则椭圆曲线 E 上的点数 $\#(E(\mathbf{F}_q))$ 满足

$$|\#(E(\mathbf{F}_q)) - (q + 1)| \leq 2\sqrt{q}.$$